

Senquip User Guide

Release UNI-Z1

Senquip

Aug 10, 2026

List of Figures	v
1 Introduction	3
1.1 Capability at Scale	3
1.2 Typical Applications	4
1.3 Key Features	5
2 First Connection	7
2.1 Before You Begin	8
2.2 Step 1 - Create or Sign In to Your Senquip Portal Account	8
2.3 Step 2 - Add Your Device to the Senquip Portal	8
2.4 Step 3 - Install the SIM Card	9
2.5 Step 4 - Apply Power	10
2.6 Step 5 - Wait for Cellular Connection.	10
2.7 Step 6 - Put the Device in <i>Setup Mode</i>	11
2.8 Step 7a - Configure the Network Using the Senquip Connect App (Recommended).	11
2.9 Step 7b - Configure the Network Using the Embedded Web Server	17
2.10 Step 8 - Continue Setup in the Senquip Portal.	23
2.11 Troubleshooting.	23
3 Regulatory Information	25
3.1 CE Declaration of Conformity.	25
3.2 RCM Compliance	25
3.3 FCC statement.	25
4 Installation	29
4.1 Opening the Box	29
4.2 Mounting	29
4.3 User Access	31
4.4 SIM Card Installation.	33
4.5 Wiring Guide	34
4.6 Initial Setup	36
4.7 LED Indicators	37
4.8 Firmware Updates	38
4.9 Factory Reset	39
4.10 Passwords	39
5 Setup Mode	41
5.1 Entering Setup Mode.	41
5.2 Configuring the Device	41

6	Power Supply	43
6.1	Permanent power	43
6.2	Internal Rechargeable Battery	44
6.3	Low Power Operation	45
6.4	Freight Mode	46
7	General Setup	49
7.1	Measurement and Transmit Intervals	49
7.2	Power Supply Settings	52
7.3	Settings.	52
8	Internal Sensors	53
8.1	Tamper sensor.	53
8.2	Accelerometer	53
8.3	Temperature sensor.	57
8.4	GPS.	57
8.5	Bluetooth interface	59
8.6	Internal sensor settings.	61
9	External Sensors	65
9.1	Inputs and Outputs.	65
9.2	Serial interface.	71
9.3	CAN Bus interface	75
9.4	Calibration.	77
9.5	Warnings and Alarms	78
9.6	External Sensor Settings	79
10	Scripting	89
10.1	Risks	89
10.2	Access	89
10.3	Writing and deploying a script	90
11	Network Connection	93
11.1	Wi-Fi specification	93
11.2	Cellular specification	93
11.3	Satellite Connectivity.	93
11.4	Network Interfaces and Services	94
11.5	Network Requirements.	94
11.6	Connecting to a Wi-Fi or LTE Network with the Senquip Connect App	95
11.7	Connecting to a Wi-Fi Network with the Embedded Webserver	97
11.8	Connecting to an LTE Network with the Embedded Webserver	100
11.9	Network settings.	101
12	Endpoint Setup	103
12.1	Data security	103
12.2	Data format.	103
12.3	Data Buffer	104
12.4	UDP.	106
12.5	HTTP	106
12.6	HTTPS	106
12.7	MQTT.	106
12.8	MQTT over TLS	106
12.9	Settings	107
13	Senquip Portal	109

13.1	Create a Senquip Portal Account.	112
13.2	Creating a Group	114
13.3	Add Devices to a Group	115
13.4	Finding Devices and Groups.	116
13.5	Group Management.	116
13.6	Senquip Vision Dashboards	124
13.7	Device Data Page	136
13.8	Management and Hosting on the Senquip Portal	157
14	Mechanical Specification	165
15	Maintenance	167
15.1	Replacing the LTO Battery	167
16	Frequently Asked Questions	169
16.1	Introduction	169
16.2	Senquip Portal	169
16.3	Network	172
16.4	GPS / GNSS	174
16.5	Measurements	174
16.6	Power	175
16.7	Setup	178
16.8	Operation.	179
16.9	Scripting	180
17	Glossary	183
	Index	185

Figure 1.1: Senquip UNI-Z1	3
Figure 2.1: First connection workflow	7
Figure 2.2: Portal login prompt	8
Figure 2.3: Device credentials card	9
Figure 2.4: Correct SIM orientation.	9
Figure 2.5: UNI-Z1 power connection	10
Figure 2.6: UNI-Z1 status lights	11
Figure 2.7: Scan the QR code to download the Senquip Connect App	12
Figure 2.8: Scanning for devices.	12
Figure 2.9: Selecting a device	13
Figure 2.10: Entering the password	14
Figure 2.11: Choose Wi-Fi or cellular configuration.	15
Figure 2.12: Configuring Wi-Fi	16
Figure 2.13: Configuring cellular connection	17
Figure 2.14: Connect to the Senquip device access point	18
Figure 2.15: Typical network warning	19
Figure 2.16: Enter the device web server address	20
Figure 2.17: Enter the credentials for the device web server	21
Figure 2.18: Configuring the device network settings.	22
Figure 2.19: Results of a network scan	23
Figure 4.1: UNI-Z1 packaging with intact security seal.	29
Figure 4.2: Bottom view showing UNI mounting points	30
Figure 4.3: UNI mounted within a shipping container corrugation.	31
Figure 4.4: SIM card sizes	33
Figure 4.5: Correct orientation of a Nano-SIM card	34
Figure 4.6: Connector pin numbering.	35
Figure 4.7: Typical wiring arrangement	36
Figure 4.8: Senquip Connect App	37
Figure 4.9: UNI LED locations	38
Figure 4.10: Device credentials card	39
Figure 6.1: Typical UNI-Z1 solar panel	43
Figure 6.2: Entering freight mode	46
Figure 7.1: Timing flowchart.	50
Figure 8.1: Definition of pitch	54
Figure 8.2: Definition of roll	54
Figure 8.3: Definition of tilt	55
Figure 8.4: GPS alert parameters	59
Figure 8.5: Example BLE beacons from ELA	60
Figure 9.1: Switching a resistive load	67
Figure 9.2: Switching a high inductance load	67
Figure 9.3: Pulse counting	68
Figure 9.4: Hysteresis.	69
Figure 9.5: iButton reader connected to IO1	70

Figure 9.6: Hysteresis	79
Figure 10.1: Senquip scripting page	90
Figure 10.2: Feedback on unsuccessful script	91
Figure 11.1: Scanning for Devices	96
Figure 11.2: Configuring the Network	97
Figure 11.3: Save changes and reboot	98
Figure 11.4: Note the IP address on your network.	99
Figure 11.5: Access via local IP	100
Figure 12.1: Example JSON data packet.	104
Figure 12.2: Pending change where the device name has been changed.	107
Figure 13.1: Senquip Vision Dashboard	110
Figure 13.2: Senquip Device Data Page	111
Figure 13.3: Create a Senquip Portal account	112
Figure 13.4: Complete the required fields.	113
Figure 13.5: Your email must be verified	114
Figure 13.6: You must login to activate your account	114
Figure 13.7: Create a new Group.	115
Figure 13.8: Select a meaningful name	115
Figure 13.9: Adding a single device to a group.	115
Figure 13.10: Search by group, name , or device id	116
Figure 13.11: Change Group settings	117
Figure 13.12: Manage devices in a Group.	117
Figure 13.13: Grant appropriate permissions to group users	118
Figure 13.14: Available bulk update options	119
Figure 13.15: Selecting devices for bulk configuration.	119
Figure 13.16: Example JSON input and confirmation before confirming changes.	120
Figure 13.17: Selecting devices from the same firmware family.	121
Figure 13.18: Review and confirm firmware updates.	121
Figure 13.19: Review and confirm configuration import.	122
Figure 13.20: Bulk update of device alerts.	123
Figure 13.21: Bulk file upload.	123
Figure 13.22: Fully customisable Senquip Vision dashboard	124
Figure 13.23: Create a different view for each user function	125
Figure 13.24: Min, max, average, total, difference, and latest metrics are available.	126
Figure 13.25: Time weighted average works well where there are missing samples	127
Figure 13.26: Total, sums all data values	128
Figure 13.27: Accumulation calculates increase even is the source parameter is zeroed.	129
Figure 13.28: Device summary table showing alarms on the fuel level	130
Figure 13.29: Adding metrics to a Device Summary Table	130
Figure 13.30: Press the edit button on each column to edit functionality	131
Figure 13.31: Example Device Summary Table showing warnings and alarms.	131
Figure 13.32: Headline numbers show metrics across all devices in the view	132
Figure 13.33: Headline numbers total and average a source metric across all devices in the view	133
Figure 13.34: Charts show trend data across multiple devices	133
Figure 13.35: A stacked chart shows cumulative contribution of multiple data series over time	134
Figure 13.36: Clusters of device separate as the zoom level increases	134
Figure 13.37: Optimise the layout for different screen sizes.	135
Figure 13.38: Dashboard view optimised for mobile screens	136
Figure 13.39: Device Data Pages provide a detailed view of measured data	137
Figure 13.40: Turn widgets on and off and configure the display order	139
Figure 13.41: Switch between numeric, gauge, and digital display modes	140
Figure 13.42: Numeric data can be shown as a line chart	140
Figure 13.43: Data associated with the selected device shown in a table	141
Figure 13.44: Remote update of device settings via the Senquip Portal	143
Figure 13.45: Remote firmware updates via the Senquip Portal	144
Figure 13.46: Configure event forwarding	145
Figure 13.47: A graphical widget showing tyre status.	146
Figure 13.48: Default blank widget showing temperature	146

Figure 13.49: Settings for our water cart example	147
Figure 13.50: Water Level as shown on the device page.	147
Figure 13.51: Water cart widget text settings.. . . .	148
Figure 13.52: Water cart widget with water level shown in green.	148
Figure 13.53: Settings for water cart level element	149
Figure 13.54: Completed water cart widget.	150
Figure 13.55: Water cart widget shown on the Senquip Portal	150
Figure 13.56: Brushed area chart showing particles in oil.	151
Figure 13.57: Default custom chart.	152
Figure 13.58: Custom chart settings	152
Figure 13.59: Custom chart axis	153
Figure 13.60: Adding series to a custom chart	153
Figure 13.61: Example chart showing generator temperature and pressure	154
Figure 13.62: Example bar chart showing a vibration profile and goal	155
Figure 13.63: Example bar chart showing a vibration profile and goal	155
Figure 13.64: Configuration for bar charts	156
Figure 13.65: Stacked and regular bar chart showing percentage of time the pump operated within each load range.	157
Figure 13.66: Select Account to setup billing details	158
Figure 13.67: A warning is shown if there is no payment method available.	159
Figure 13.68: Select Add Payment Method.. . . .	159
Figure 13.69: Add a payment method.	160
Figure 13.70: Select the subscriptions module	161
Figure 13.71: Select devices to be hosted or for which hosting is to be cancelled.	161
Figure 13.72: Make a selection to change plans.	162

PDF Version of this User Guide.

Introduction

1.1 Capability at Scale



Figure 1.1. Senquip UNI-Z1

The Senquip UNI-Z1 is designed for OEMs and fleets requiring compact, cost-effective telemetry that can be deployed consistently across large numbers of machines. Optimised for repeatable machine designs with defined monitoring and control requirements, the UNI-Z1 delivers the essential sensing, connectivity, and edge processing capabilities required by modern equipment manufacturers.

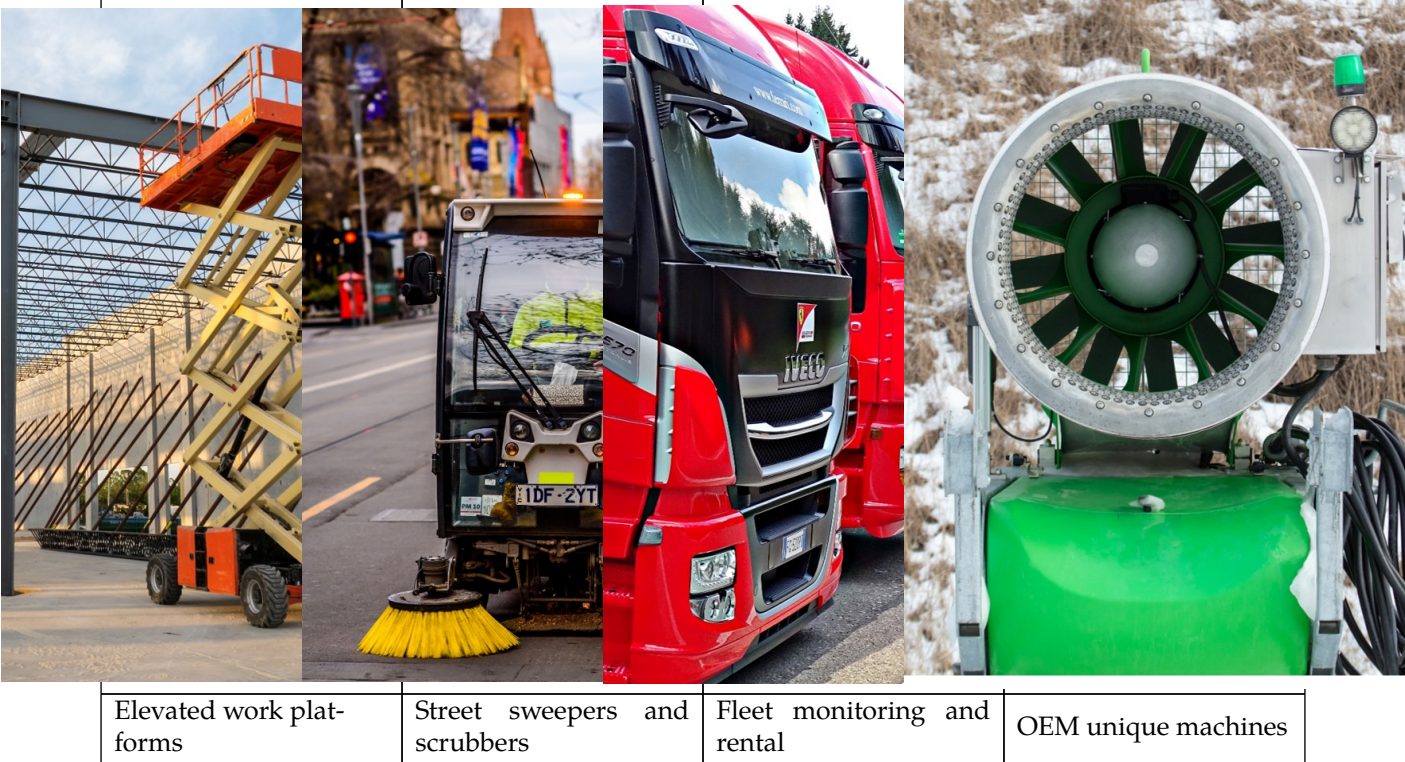
Its compact form factor, integrated Deutsch connector, internal antennas, long-life LTO battery, and satellite-ready connectivity simplify installation while reducing deployment and support costs across large fleets. Whether fitted to a lighting tower, generator, forklift, rental asset, or other OEM machine platform, the UNI-Z1 provides a practical and scalable telemetry solution.

The UNI-Z1 combines monitoring, control, location tracking, communications, and edge processing in a compact package that is easy to install, commission, and deploy at scale.

1.2 Typical Applications

The UNI-Z1 is best suited to repeatable machine designs with defined monitoring and control requirements where ease of deployment, consistency, and cost-effectiveness are important.

			
Lighting towers	Generators	Forklifts	Compressors and blasters



Elevated work plat-
forms

Street sweepers and
scrubbers

Fleet monitoring and
rental

OEM unique machines

1.3 Key Features

- Compact enclosure with integrated Deutsch connector
- Internal Wi-Fi, LTE, Satellite, Bluetooth and GNSS antennas
- Direct-to-Cell satellite-ready connectivity
- Long-life LTO battery with 5000-cycle life
- GNSS location, vibration, pitch, roll and temperature monitoring
- CAN, RS485 and Modbus support
- Bluetooth connectivity
- Programmable edge processing using JavaScript
- Internal memory for buffering and autonomous operation
- SoftSIM, Nano-SIM and eSIM support
- Fast installation and commissioning
- Optimised for repeatable OEM deployment

First Connection

Welcome to your new Senquip UNI-Z1.

This chapter will guide you through connecting your device to the Senquip Portal for the first time. Most installations can be completed in just a few minutes.

If you require detailed information on mounting, wiring or configuration, links are provided throughout this chapter to the relevant sections of this User Guide.

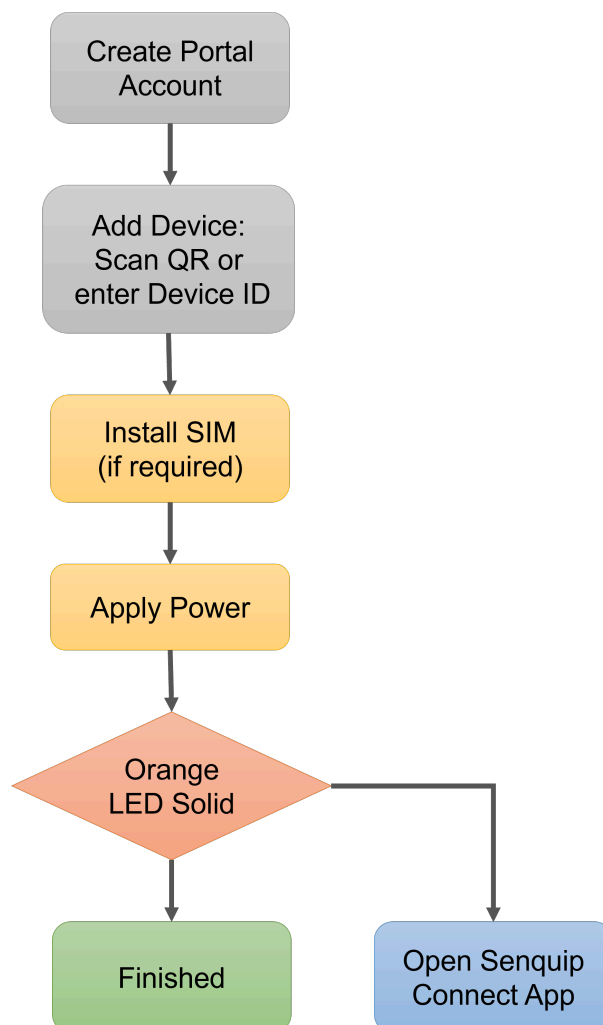


Figure 2.1. First connection workflow

2.1 Before You Begin

Before starting, you will need:

- A power source for your Senquip UNI-Z1
- A mobile phone or computer with Internet access
- A Nano-SIM card unless using eSIM or Wi-Fi only

Hint After initial network setup, it is recommended that all device setup be performed using the Senquip Portal.

2.2 Step 1 - Create or Sign In to Your Senquip Portal Account

If you are new to Senquip, create a free account on the [Senquip Portal](#).

If you already have an account, simply login.

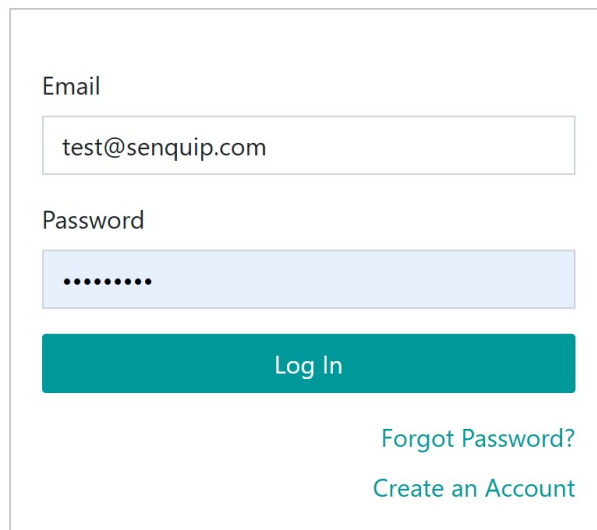
A screenshot of the Senquip Portal login form. It features two input fields: 'Email' with the text 'test@senquip.com' and 'Password' with masked characters. Below the password field is a teal 'Log In' button. At the bottom right, there are two links: 'Forgot Password?' and 'Create an Account'.

Figure 2.2. Portal login prompt

2.3 Step 2 - Add Your Device to the Senquip Portal

If your Senquip distribution partner has already added the device to your account, you can ignore this step.

Note For distribution partners and OEMs, devices are automatically added to your account when shipped from Senquip.

Every UNI-Z1 includes a *Scan to Start* QR code on the supplied security card.

The easiest way to add the device to the Portal is to scan the *Scan to Start* code while signed into the Senquip Portal.

Alternatively, select *Add Device* from the Senquip Vision Dashboard and enter the Device ID and

Setup Password manually.



Figure 2.3. Device credentials card

2.4 Step 3 - Install the SIM Card

If you are using cellular (4G LTE) communications, install a Nano-SIM card before applying power. If you are not using a cellular connection, ignore this step.

The UNI-Z1 automatically configures the APN for most SIM cards. In cases where the APN needs to be added manually, this can be done in a later step.

Note An APN (Access Point Name) identifies the network service that a cellular device should connect to. The APN is normally provided by your SIM or cellular service provider.

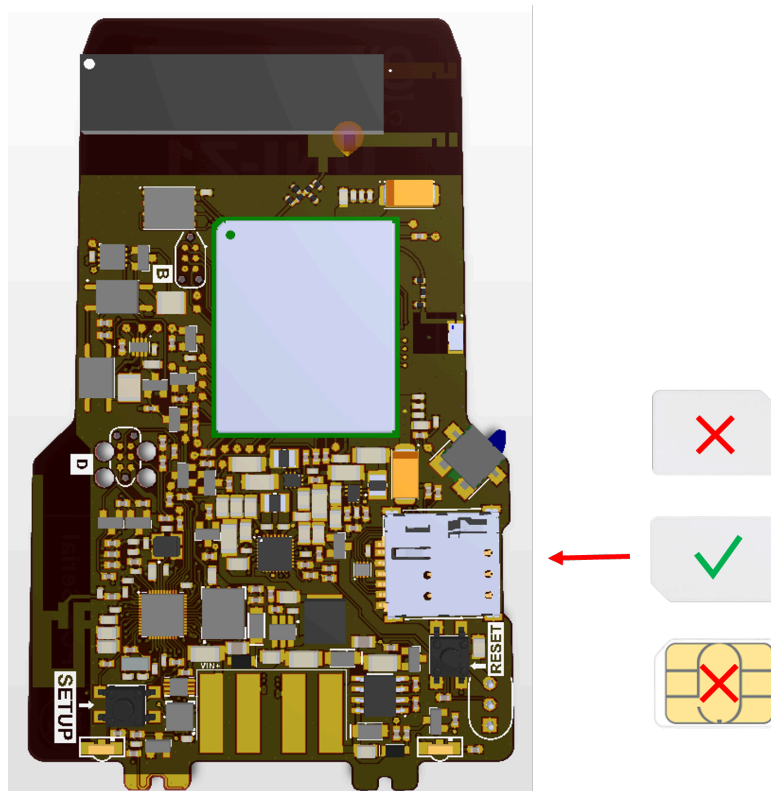


Figure 2.4. Correct SIM orientation

For detailed instructions, see [Section 4.4](#).

2.5 Step 4 - Apply Power

Supply between **10V and 32V DC** to the UNI-Z1.



Figure 2.5. UNI-Z1 power connection

The green Status LED should illuminate.

2.6 Step 5 - Wait for Cellular Connection

Allow up to ten minutes for the UNI-Z1 to resolve the SIM APN and establish a connection.

For most SIM cards, no additional configuration is required.

The orange Network LED indicates progress.

Network LED	Meaning
Flashing	Searching for a network
Pulse	Connected to the network but unable to reach the Senquip Portal
Solid	Connected to the Senquip Portal



Figure 2.6. UNI-Z1 status lights

If the Network LED becomes solid, your UNI-Z1 is connected and no further network configuration is required.

2.7 Step 6 - Put the Device in *Setup Mode*

To enter *Setup Mode*, press the Setup button on the Senquip device. Once the green light starts flashing, the device is in *Setup Mode* and you can proceed.

If connected to external power, the UNI-Z1 will remain in setup mode as long as the lid is open. If no external power is available, the UNI-Z1 will enter sleep mode after 10 minutes of no activity. To re-enable setup mode, press the *Setup* button again for 2 seconds. Setup mode will be exited once the lid has been closed for more than 10 seconds.

Once the UNI-Z1 is in *Setup Mode*, network configuration can be completed using either of the following methods:

- **Senquip Connect App (recommended)** - configure the device using Bluetooth from an Android or iOS mobile device.
- **Embedded Web Server** - configure the device using a web browser over the device's Wi-Fi access point.

Choose either Step 7a or Step 7b below.

2.8 Step 7a - Configure the Network Using the Senquip Connect App (Recommended)

If the UNI-Z1 is to connect with Wi-Fi or the cellular connection does not connect automatically, the Senquip Connect App allows network configuration via Bluetooth.

The Senquip Connect App is available for both Android and iOS.



Figure 2.7. Scan the QR code to download the Senquip Connect App

Network Configuration with the Senquip Connect App:

1. Open the Senquip Connect App.
2. Press *Scan for Devices*, all devices broadcasting Bluetooth or devices in setup mode will be shown.

Note The UNI-Z1 will advertise itself as *UNI-xxxxx*, where xxxxx represents the last 5 digits of the UNI-Z1 device identifier.

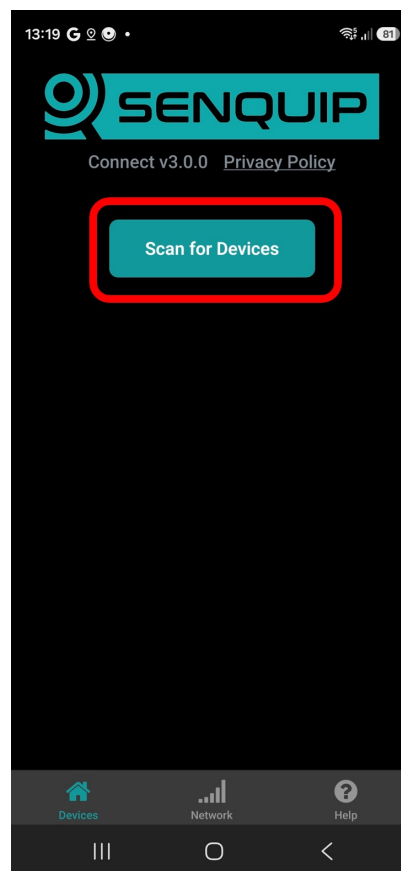


Figure 2.8. Scanning for devices

3. Select the desired device and pair to it

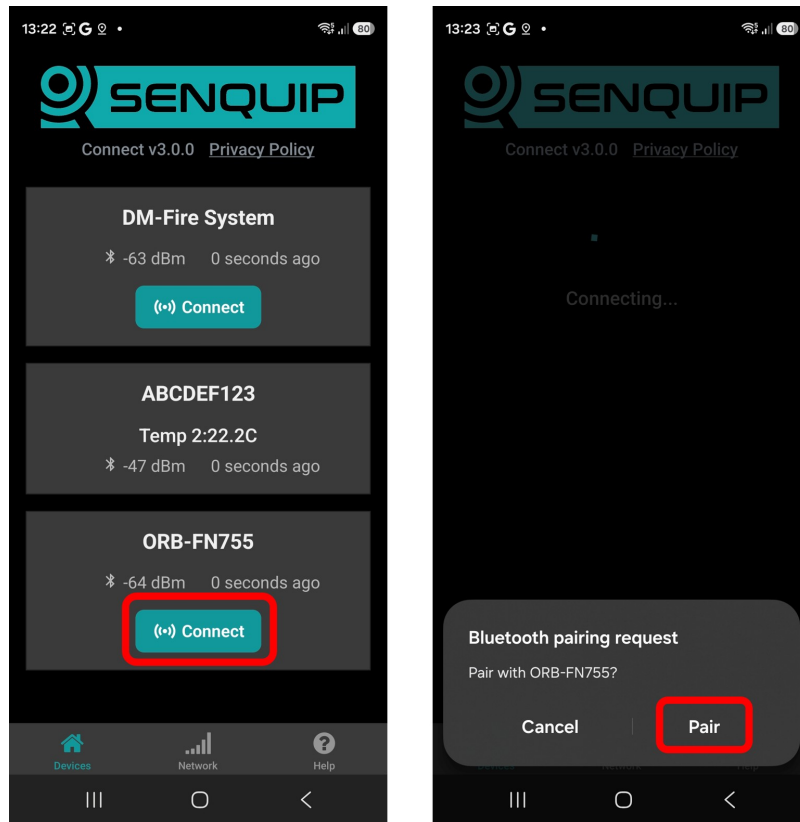


Figure 2.9. Selecting a device

4. Enter the device setup password and press *Submit*.

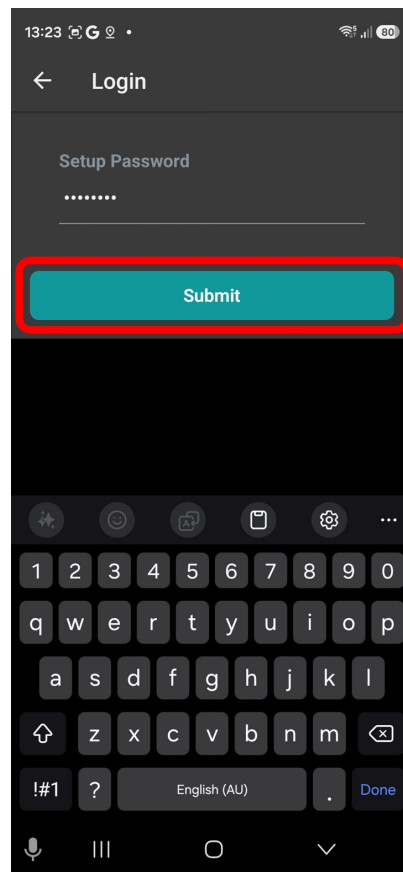


Figure 2.10. Entering the password

Note If the device is in a factory default mode, passwords are not required.

5. Select either *Configure WiFi* or *Configure Cellular / LTE*.

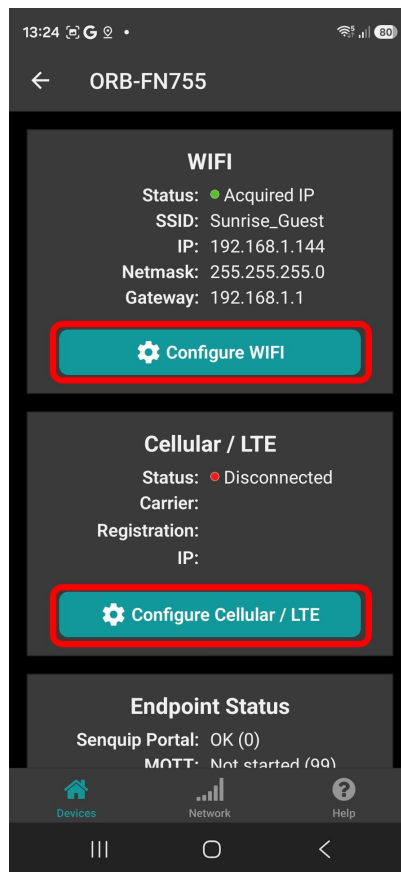


Figure 2.11. Choose Wi-Fi or cellular configuration

6. Enable the connection method.

7a. For Wi-Fi connections, enter the Wi-Fi SSID to which the device is to be connected and the password for that network.

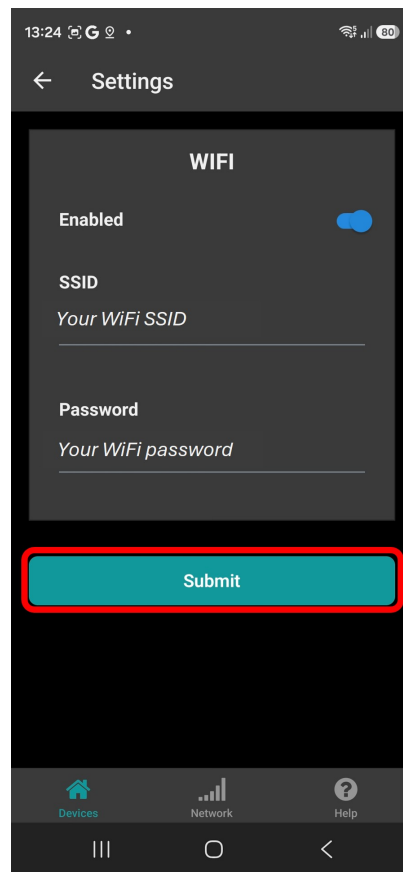


Figure 2.12. Configuring Wi-Fi

Note The UNI-Z1 operates on a 2.4 GHz frequency only

7b. For cellular connection, disable Auto APN and manually enter the APN. In very few setups, the SIM card will require a username and password. Enable roaming if this is a roaming SIM.

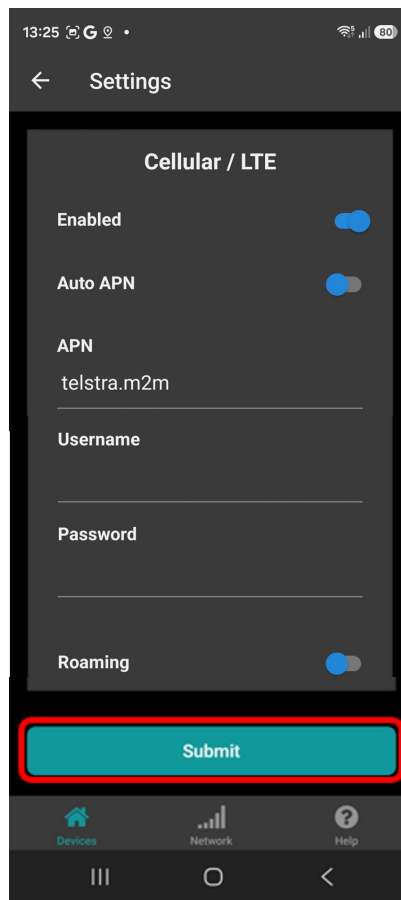


Figure 2.13. Configuring cellular connection

Note Roaming SIMs may be de-prioritised on busy networks

8. Press *Submit*. The device will save the details and will reboot and attempt to connect to the network. Connection progress can be monitored on the Senquip Connect App.

2.9 Step 7b - Configure the Network Using the Embedded Web Server

In setup mode, a device Wi-Fi Access Point (AP) is enabled that allows for initial setup. In this mode, a user can connect to the UNI-Z1 using any computer, tablet or mobile phone that has Wi-Fi and is loaded with a browser.

Note The Senquip UNI-Z1 Wi-Fi Access Point is 2.4 GHz only

Network Configuration with the Embedded Web Server:

1. To connect to the UNI-Z1 access point, search for available Wi-Fi networks on your Wi-Fi enabled device.

Note The UNI-Z1 will advertise itself as *UNI-xxxxx*, where *xxxxx* represents the last 5 digits of the UNI-Z1 device identifier.

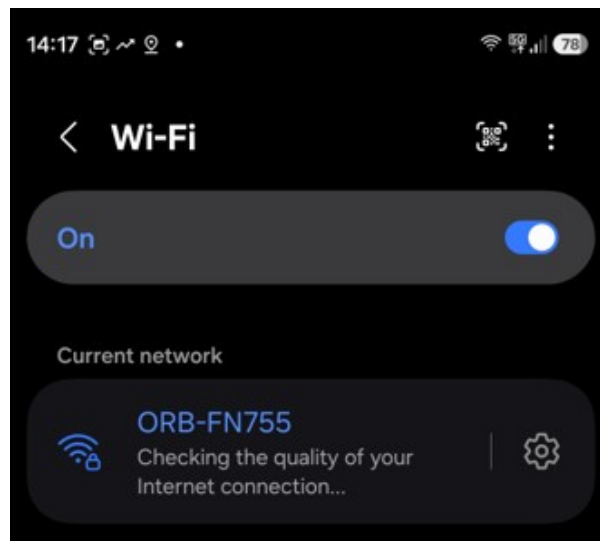


Figure 2.14. Connect to the Senquip device access point

2. Enter the Wi-Fi password as found on the Device Credentials Card.

Warning Modern phones are cautious of unknown and non-internet connected networks. You may need to ignore multiple warnings. You may also need to change mobile device settings to prevent it from switching to an alternate internet connected network.

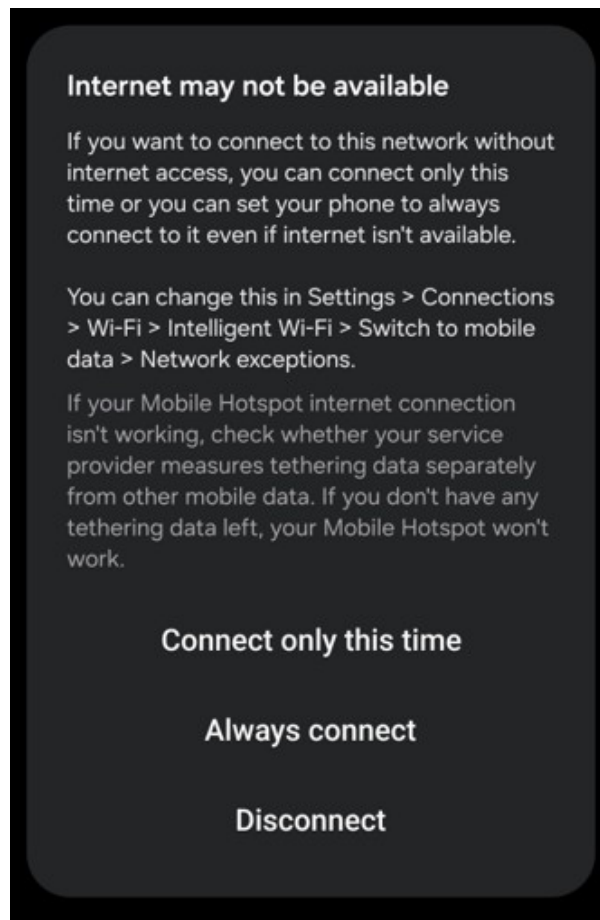


Figure 2.15. Typical network warning

You should now be connected to the device access point. Being connected to the UNI-Z1 access point does not allow you to view or change any data yet.

3. To view and change settings, you need to login to the UNI-Z1 web server. Open your preferred web-browser (Senquip recommends Chrome) and type the address of the UNI-Z1 web server (192.168.4.1) into the address (or search) bar. Expect more warnings that need to be ignored.

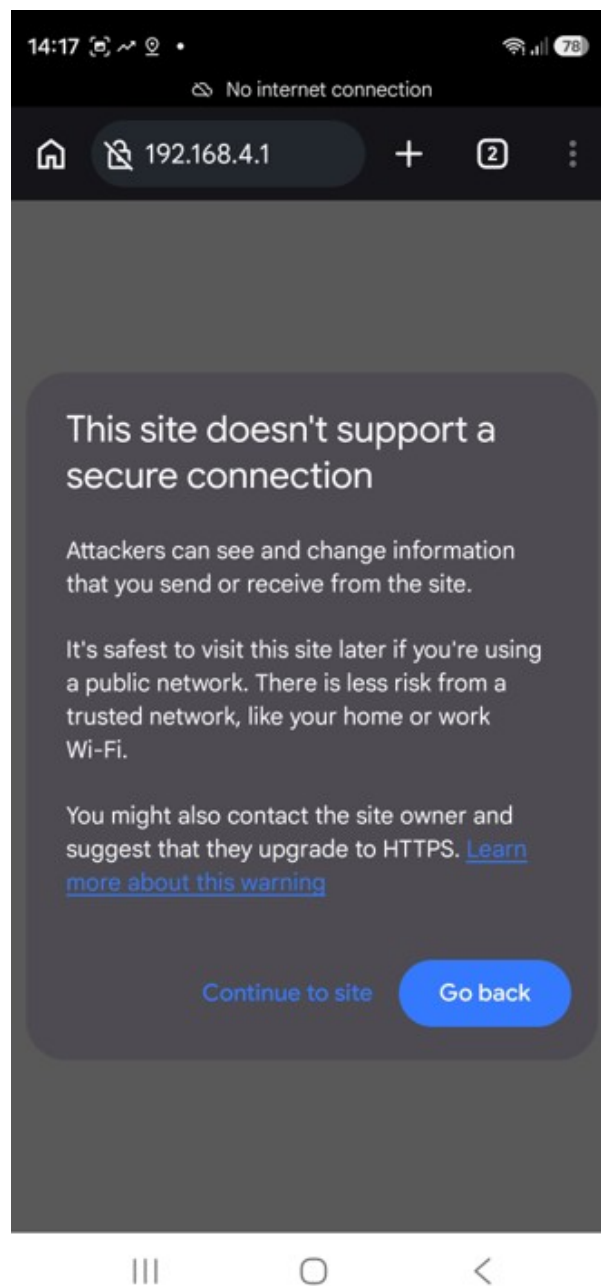


Figure 2.16. Enter the device web server address

4. Login to the device web server with username *Admin* and the *setup* password from the Device Credentials Card. Press *Sign in*.

You should now be connected to the device web server.

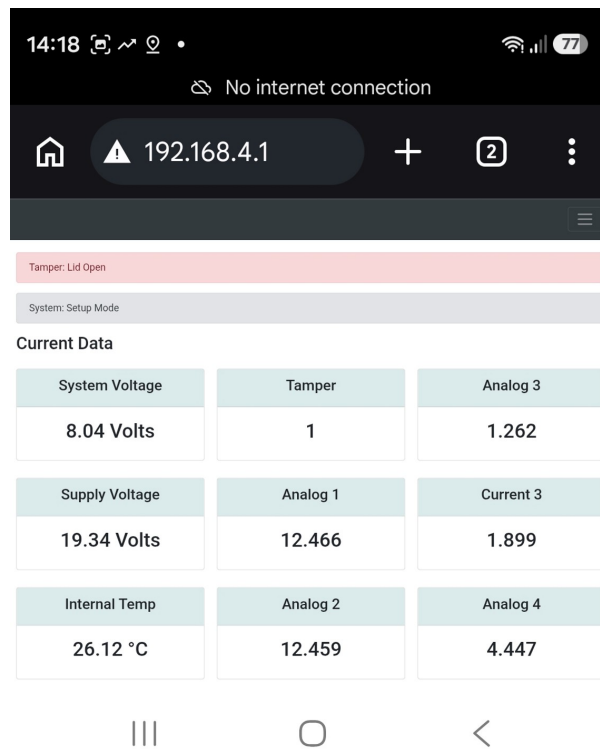


Figure 2.17. Enter the credentials for the device web server

- Using the menu icon (3 horizontal stripes) on the top right, select *Network*. From here you can configure the network settings.

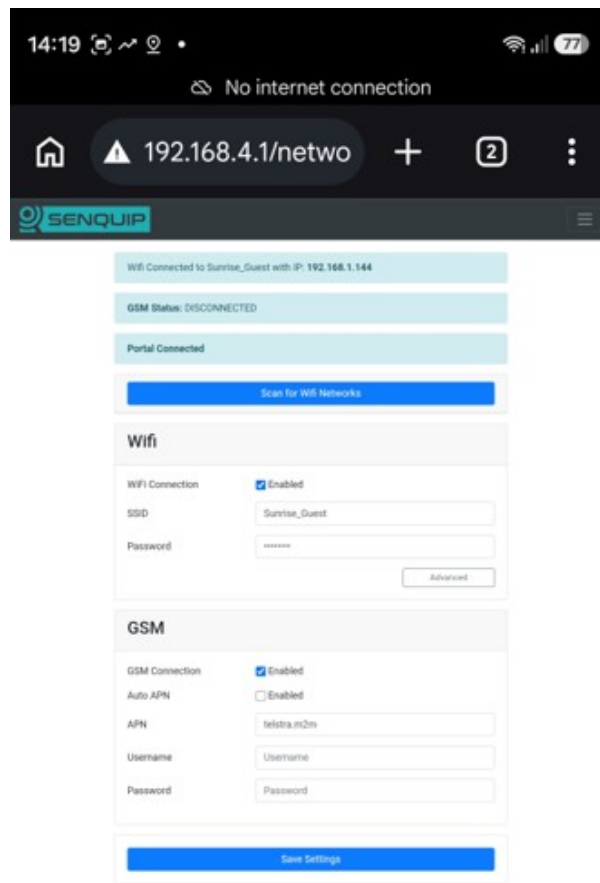


Figure 2.18. Configuring the device network settings

Note You can also configure other device settings, but this is easier to achieve using the Senquip Portal once the device is connected to a network.

Note You can change the device setup password using the *Admin* tab in the menu.

Note Performing a factory reset will reset the passwords to their defaults as found on the Device Credentials Card.

6. Enable the required connection method.

7a. For Wi-Fi connections, you can use the *Scan for WiFi Networks* button and select from available networks or you can enter the Wi-Fi SSID to which the device is to be connected and the password for that network. Additional advanced network settings are available but are rarely used.

Note The UNI-Z1 operates on a 2.4 GHz frequency only

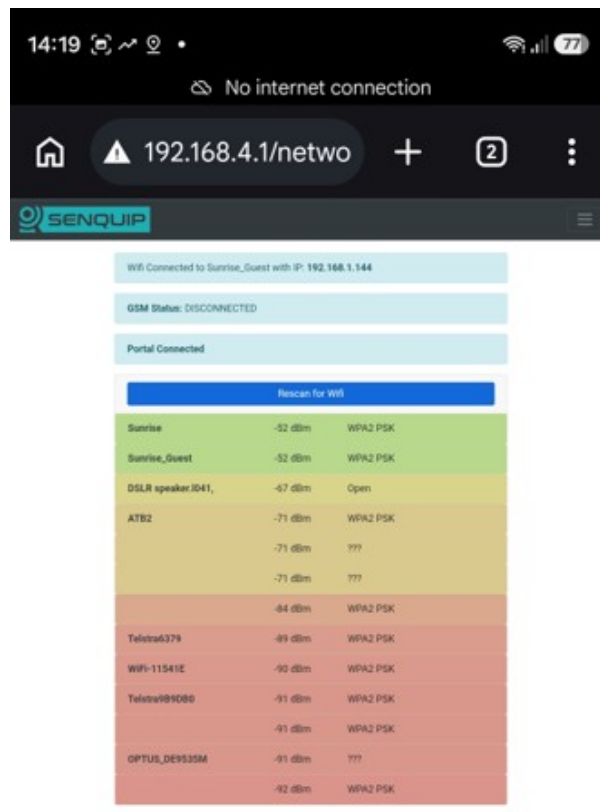


Figure 2.19. Results of a network scan

7b. For cellular connection, disable Auto APN and manually enter the APN. In very few setups, the SIM card will require a username and password.

8. Press *Save Settings*. The device will save the details and will reboot and attempt to connect to the network. If the orange network light goes solid, then the device is connected.

2.10 Step 8 - Continue Setup in the Senquip Portal

Your UNI-Z1 is now connected and ready for use. View measured data and continue device configuration using the Senquip Portal.

For more information, including User Guides, Application Notes, Tech Tips, scripting examples, firmware updates and other technical resources, visit the [Senquip Documentation Page](#).

2.11 Troubleshooting

Problem	Suggested action
Green Status LED is off	Check the power supply and wiring.
Network LED flashes continuously	Check SIM installation, network coverage and SIM activation.
Network LED pulses	Check Internet access, firewall settings or APN configuration.
Device does not appear in the Portal	Confirm that the device has been added to your Portal account.
Automatic connection unsuccessful	Open the Senquip Connect App and complete the network configuration.

Regulatory Information

This device complies with international standards for electromagnetic compatibility and safety, including CE, FCC, and RCM certifications.

3.1 CE Declaration of Conformity

Europe: European Conformity (CE) This device meets the requirements of the Radio Equipment Directive (RED) 2014/53/EU, the Electromagnetic Compatibility Directive (EMC) 2014/30/EU, and the Low Voltage Directive (LVD) 2014/35/EU.

It has been tested to and complies with the applicable harmonised standards for radio equipment, electromagnetic emissions and immunity, and electrical safety.

For products placed on the European market from August 2025, compliance also includes the applicable cybersecurity requirements for internet-connected radio equipment under the Radio Equipment Directive.

A full Declaration of Conformity (DoC) is available on request.

3.2 RCM Compliance

Australia and New Zealand: Regulatory Compliance Mark (RCM) This device complies with the applicable Australian and New Zealand radio communications and electrical safety requirements. It has been tested and meets the relevant ACMA and EESS standards for EMC and radiocommunications.

The RCM indicates that the product meets both electrical safety and electromagnetic compatibility requirements under the Australian Communications and Media Authority (ACMA) and other applicable national regulatory frameworks.

3.3 FCC statement

USA: Federal Communications Commission (FCC) statement

This device complies with FCC part 15 FCC Rules.

Operation is subject to the following two conditions: 1. This device may not cause harmful interference and 2. This device must accept any interference, including interference that may cause undesired operation of the device.

FCC Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

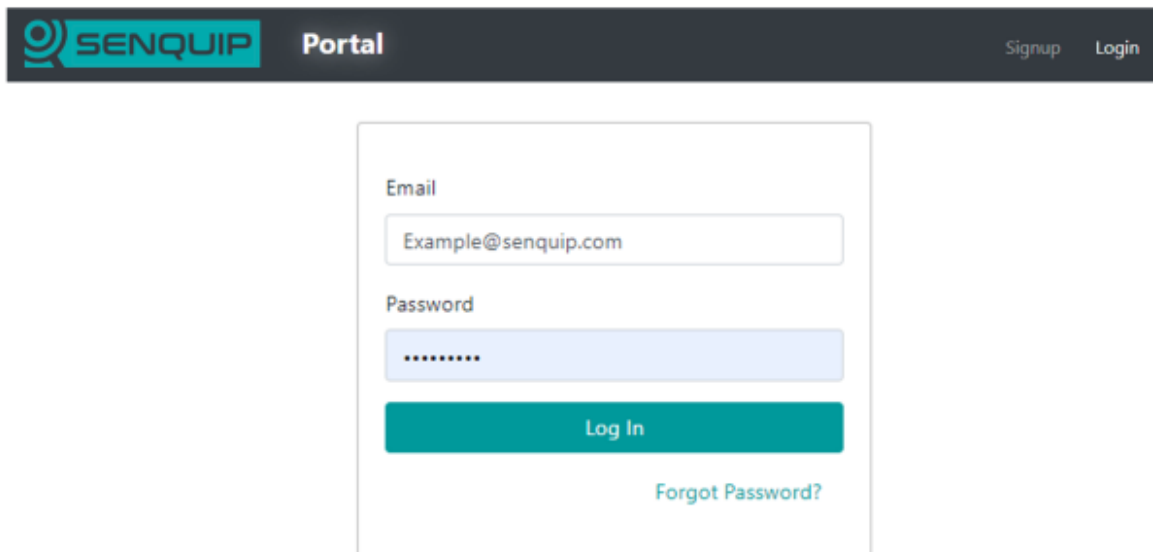
This device meets the FCC and IC requirements for RF exposure in public or uncontrolled environments.

3.3.1 Accessing Regulatory Information

You can access the regulatory information for your device by following this link: <https://portal.senquip.com/fcc>.

Alternatively, you can view the device FCC ID on the Senquip Portal. To view the FCC ID:

1. Launch the [Senquip Portal](#).



2. Browse to the device page

SENQUIP Portal

PlansSupportDocsAccountLogout

Georges Test Devices

+ Add DeviceMapSubscriptions

Name	Device ID	Events	Last Contact	Internal Temperature	Atmospheric Pressure	Tank Level	Supply Voltage	System Voltage
☐ Senquip test C1	QF7BXH531	1	a few seconds ago					
☐ Norman ORB Test 2	EUBD75173	2	an hour ago					
☐ Norman QUAD Test 2	WCTDKUJGE	2	an hour ago				0	
☐ Norman ORB Test 1	ED7C3TBK2	2	an hour ago				0	3.96
☐ Norman QUAD Test 3	WHTDM291E	2	an hour ago					
☐ Norman QUAD Test 1	Q53DC369C	3	an hour ago				0	
☐ Water Tank	HN1AH6A32		3 hours ago	15.74		19.7		
☐ Norman ORB Test 3	UPBD709G3	2	2 days ago					
☐ Senquip Day Night Controller	BN4BK2PM2	2	4 months ago					
☐ Batt Test	XW8918A82	2	4 months ago	3.6	101.79			

< > Page 1 of 3 >> Showing 1 - 10 of 22

MapSatellite

Copyright ©2021 Senquip Pty Ltd. Terms of Use

Select device

3. On the *Device Info* widget, select *Regulatory Information*

SENQUIP Dev Portal

Devices / Senquip test C1 : Data

Senquip test C1

Last Contact: a few seconds ago

Latest Data: 18-Sep-23 08:18:34

Device Info

Asset Image

Events

Triggers

Supply Voltage

System Voltage

Position

Internal Temperature

Select regulatory info

Device ID: QF7BXH531

Model: ORB-C1-G

Firmware: SPW001-7.1.0

Base Interval: 10 seconds

Wifi IP: 192.168.1.101

Wifi Signal: -41 dBm

Regulatory Information

Tamper: Lid Open

18-Sep-23 08:18:34

Send Serial

Hot tub Adjust ONOFF

19.2 Volts

18-Sep-23 08:18:34 [vin]

4.1 Volts

18-Sep-23 08:18:34 [vsys]

Position

MapSatellite

18-Sep-23 08:18:34

27.4 °C

18-Sep-23 08:21:44 [ambient]

Installation

4.1 Opening the Box

The UNI-Z1 is shipped in a box with a security seal that ensures that the packaging has not been opened. If this seal is compromised, the box may have been opened, in which case, a non-authorised party could have had access to the device password. If the device is to be used in a critical application, please ensure that the seal is intact upon receipt and remember to change your password as soon as possible.

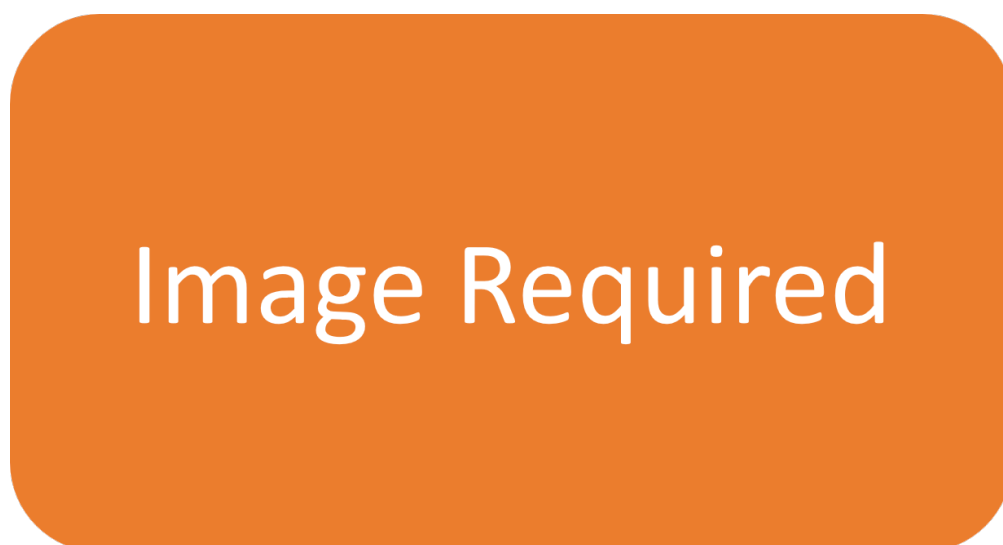


Figure 4.1. UNI-Z1 packaging with intact security seal

4.2 Mounting

The UNI has been designed for permanent installation on industrial equipment and OEM machines. The enclosure incorporates two M5 mounting holes, one on each side of the enclosure, allowing the device to be securely attached to a machine, panel, bracket, or other structure.

The device should be mounted on a rigid surface using suitable M5 fasteners. Care should be taken to ensure that the mounting arrangement can withstand the vibration, shock, and environmental conditions present in the application.

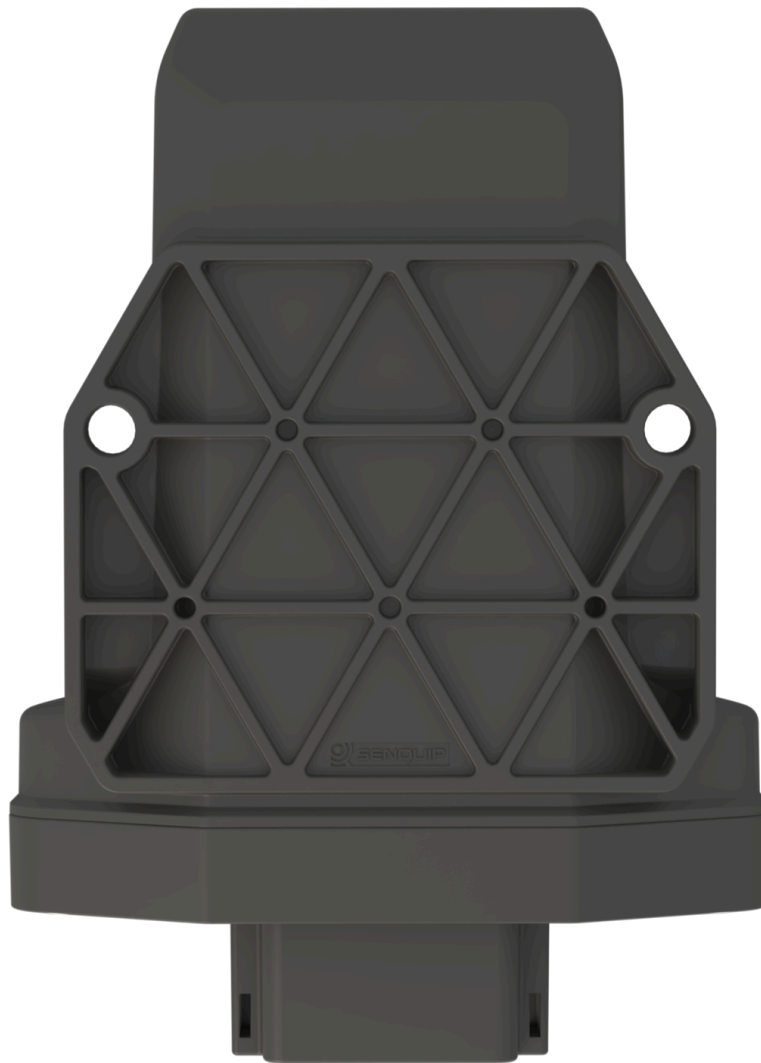


Figure 4.2. Bottom view showing UNI mounting points

For best performance, the device should be mounted such that:

- Wiring is protected from damage and excessive strain.
- The enclosure is not subjected to unnecessary mechanical stress.
- The device is positioned away from significant sources of heat.
- The connector faces downward or sideways where possible to minimise water ingress into the connector cavity during service.

4.2.1 Shipping Container Installation

The UNI enclosure has been designed to fit within the corrugations of a standard shipping container. When mounted within a corrugation, the device does not extend beyond the outer profile of the container, reducing the risk of accidental damage during handling and transport.



Image Required

Figure 4.3. UNI mounted within a shipping container corrugation

This makes the UNI particularly suitable for container monitoring, containerised equipment, and other applications where protection from impact and snagging is important.

Note The installer is responsible for ensuring that the mounting structure and fasteners are suitable for the application and that the installation complies with any applicable safety requirements.

4.3 User Access

The UNI is designed primarily for OEM integration and is not intended to require routine access during normal operation. Access is typically only required during commissioning to install a Nano-SIM card or perform configuration.

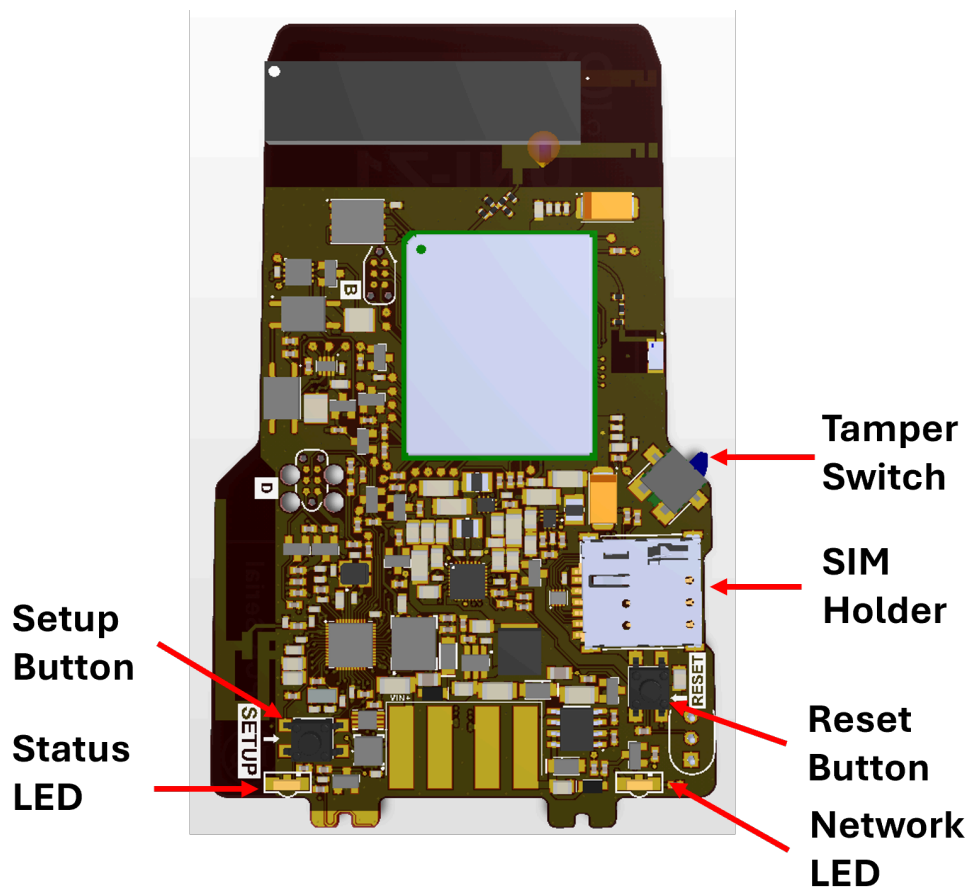
The enclosure is secured using two stainless steel captive screws. To access the electronics, loosen the screws and remove the enclosure from the header.

Opening the enclosure activates the internal tamper switch. Applications requiring tamper detection may use this feature to record or report unauthorised access to the device.



Removing the enclosure

Once the enclosure has been removed, the printed circuit board is exposed. The battery is mounted on the bottom side of the PCB, while the Nano-SIM holder, setup button, reset button, network LED, and setup LED are accessible from the top side.



Internal components

Warning The internal electronics may be damaged by static electricity or improper handling. Avoid touching electronic components, connector contacts, battery terminals, or exposed circuitry. Where possible, handle the PCB by its edges and observe appropriate electrostatic discharge (ESD) precautions.

Before reassembling the device, inspect the enclosure seal to ensure it is clean, correctly seated, and free from damage, dirt, moisture, or other contamination. Failure to correctly fit the seal may compromise the environmental protection of the device.

The setup button, reset button, network LED, and setup LED are described in later sections of this manual.

After any required work has been completed, ensure that the enclosure is correctly fitted to the header, the seal is correctly seated, and both captive screws are tightened before returning the device to service.

4.4 SIM Card Installation

The UNI-Z1 supports both eSIM and Nano-SIM options.

- **eSIM** - Provision is made on the PCB for a customer-supplied MFF2 eSIM component. eSIMs provide excellent reliability in high-vibration environments. Contact Senquip for more information.
- **Nano-SIM** - A Nano-SIM holder is provided for customers wishing to use their own SIM cards. Nano-SIMs offer the greatest flexibility and network choice.

If mobile communications are required and an eSIM is not fitted, a Nano-SIM card must be installed. The UNI-Z1 supports both 1.8V and 3.3V Nano-SIM cards.

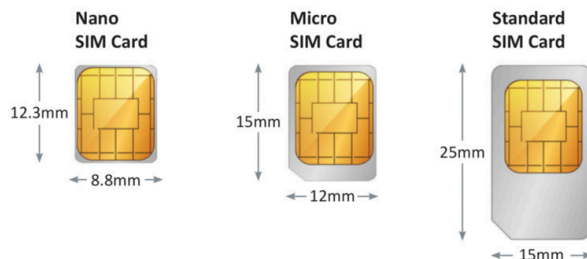


Figure 4.4. SIM card sizes

Note If your UNI-Z1 is fitted with an eSIM, a Nano-SIM card is not required.

To access the Nano-SIM holder, remove the enclosure from the header as described in the User Access section.

The SIM holder is a push-push type. To install a Nano-SIM card, push it fully into the holder until it clicks into place. To remove the SIM card, push it gently and release. The SIM card will eject from the holder.

With the PCB viewed from the SIM holder side and the Deutsch connector closest to you, insert the Nano-SIM card with the contacts facing down and the chamfered corner in the lower-left position, as shown below.

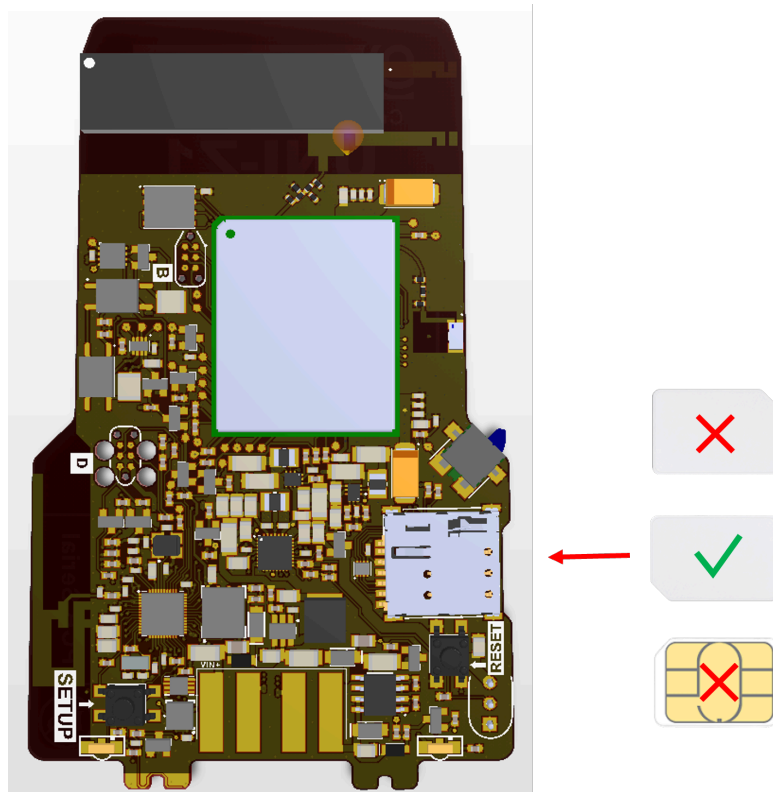


Figure 4.5. Correct orientation of a Nano-SIM card

The enclosure incorporates a retention feature that secures the SIM card when the enclosure is fitted to the header. Ensure that the enclosure is fully seated and both captive screws are tightened after installing the SIM card.

After installing or removing a SIM card, it is recommended that the UNI-Z1 be reset so that the modem can detect the change.

4.5 Wiring Guide

The Senquip UNI-Z1 uses an integrated 8-way Deutsch DT connector to provide power and communications interfaces. Looking into the mating face of the connector, pin 1 is in the upper-left corner and numbering proceeds clockwise.



Figure 4.6. Connector pin numbering

The following pinout applies to the connector:

Pin Number	Signal	Application
1	VIN	Positive supply voltage
2	RS485 B	RS485 B
3	CAN1 L	CAN bus 1 low
4	IO1	General purpose input/output 1
5	IO2	General purpose input/output 2
6	CAN1 H	CAN bus 1 high
7	RS485 A	RS485 A
8	GND	Ground

The mating connector is not supplied with the device and must be purchased separately.

Component	Part Number
Plug Housing	DT06-08SA
Wedge Lock	W8S
Socket Contacts	0462-201-16141

The recommended wire size for the 0462-201-16141 socket contacts is 0.5mm² to 2.0mm² (20 to 14 AWG).

The Deutsch contacts must be crimped using an appropriate Deutsch-compatible crimp tool. Improper crimping can result in increased contact resistance, intermittent operation, or reduced environmental sealing. After crimping, lightly pull each wire to verify correct contact retention before inserting the contact into the connector housing.

To maintain the environmental sealing of the connector:

- Ensure all populated cavities contain correctly installed contacts.
- Ensure the wedge lock is fitted after assembly.
- Ensure the connector is fully mated and latched.
- Fit suitable cavity plugs to any unused cavities if environmental sealing is required.

Warning Ensure that all external power is removed from the device before wiring fitment begins.

Power and ground wires must be rated to at least 1A and should have a voltage rating suitable for the application. A 1A fuse in-line with the power connection is recommended.

Signal wires should be chosen based on the application and may require specific features such as individual shielding, twisted pairs, or impedance matching. In extremely noisy electrical environments, it is recommended that a shielded cable be used and that the shield only be connected to ground at the power supply end. Do not ground the shield at both ends.

The material from which the chosen cable is manufactured should be suitable for the environment in which it is used. Check chemical resistance, UV stability, and flex durability of the cable being used.

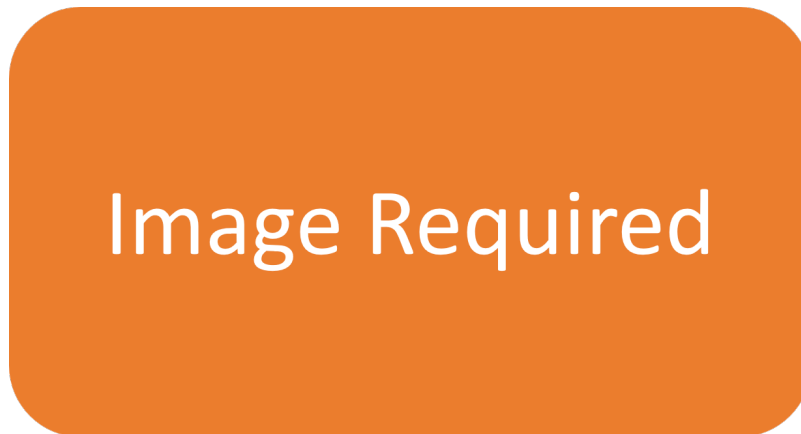


Figure 4.7. Typical wiring arrangement

4.6 Initial Setup

Initial setup can be performed using the integrated web-server using any Wi-Fi enabled phone, tablet or computer or with the Senquip connect App with an Android or iOS device. Once the device is connected to a network, it is recommended that configuration be continued using the Senquip Portal.

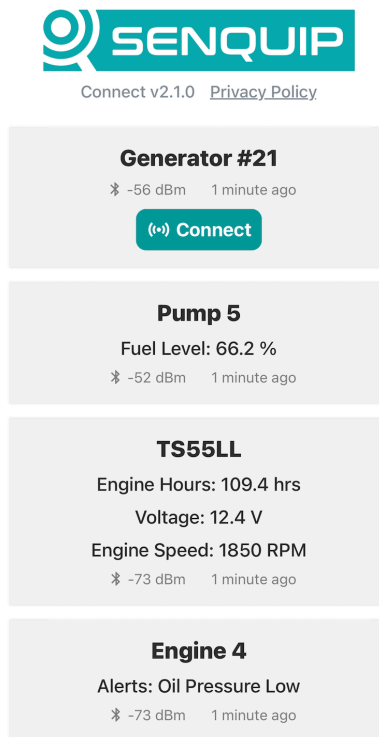


Figure 4.8. Senquip Connect App

Note For volume opportunities, devices can be pre-configured to connect immediately to a network; please contact Senquip to discuss this option.

With the cover open, two push-button switches (setup and reset) and two LEDs (network and status) are available. The switches and LEDs are used to configure the device.

4.7 LED Indicators

The UNI provides two LED indicators that are visible externally through light pipes integrated into the header.

- **Status LED (Green)** - Located to the left of the Deutsch connector.
- **Network LED (Orange)** - Located to the right of the Deutsch connector.



Figure 4.9. UNI LED locations

The LEDs are enabled by default and provide information about device status, configuration mode, and network connectivity. If required, the LEDs may be disabled through the device settings.

When the enclosure is removed from the header, the internal tamper switch is activated and the LEDs will illuminate regardless of the LED enable setting. This allows commissioning, diagnostics, and servicing to be performed even when the LEDs are disabled during normal operation.

The LED flash patterns are identical to those used by the ORB and QUAD products and are described in the tables below.

Status LED (Green)	Network LED (Orange)	Meaning
Off	Off	Device is sleeping or lid is closed
Flash (1Hz)	Off	Setup Mode
On	Flash (1Hz)	Searching for network
On	Pulse off (2 sec)	Attached to network (Wi-Fi or LTE), but not connected to Senquip Portal
On	On	Attached to network and connected to Senquip Portal
Fast Flash	Fast Flash	Factory reset in progress
Off	Fast Flash	Firmware update in progress
Slow Flash	Off	Pre-charge mode

4.8 Firmware Updates

The latest firmware version and a description of changes to firmware can be found in the [Senquip Device Firmware Changelog](#).

Updating to the latest firmware can be performed from the Senquip Portal by selecting *Settings* and *Update* and then pressing the *Update Firmware* button. To update to a specific firmware version, enter the exact firmware number and press *Update Firmware*. During the firmware update, the orange network LED will flash fast. After a firmware update, the LEDs may freeze or remain off for a few minutes. This is normal behaviour and occurs shortly after firmware update when the UNI-Z1 is encrypting the memory.

The firmware update can be seen in the command queue and has been received by the device when the status shows as success. Receipt of the firmware update by the device does not always mean that

the update is correctly applied. To ensure that the update has occurred, check the firmware number in the *Device Info* widget on the device Portal page. You may need to refresh the browser window.

4.9 Factory Reset

To perform a factory reset, press and hold the *Setup* button. While holding the *Setup* button, press and release the *Reset* button. The green status LED and orange network LED will begin to flash fast. Continue to hold the *Setup* button down for 10 seconds. After 10 seconds, the LEDs will stop flashing at which point the *Setup* button can be released. All settings will be changed back to the factory state and the device will restart. Any firmware updates made to the device will be preserved.

Warning Returning the device to factory defaults will remove all network settings, rendering remote updates impossible.

4.10 Passwords

Each UNI-Z1 is supplied with unique factory-generated credentials that protect access to the device and simplify commissioning.

The credentials are generated using a cryptographically secure random number generation process and are unique to each device.

The device is supplied with a credentials card located inside the enclosure containing:

- Device ID
- Setup Password (*SETUP PASS*)
- Wi-Fi Access Point Password (*WIFI PASS*)
- Quick Add QR code
- Quick Start Guide QR code



Figure 4.10. Device credentials card

The Device ID uniquely identifies the device within the Senquip Portal.

The Setup Password is used to access device settings through the Senquip Connect App or device webserver while the device is in setup mode. The Setup Password may also be used to establish administrative access to a device if no administrator has yet been assigned.

The Wi-Fi Password protects access to the device's Wi-Fi Access Point when local wireless configuration is required.

The Quick Add QR code contains the Device ID and Setup Password, allowing an authenticated Senquip Portal user to add the device to their account with a single scan.

The Quick Start Guide QR code links to the latest installation and commissioning instructions for the device.

Warning Store the credentials card in a secure location. Anyone with access to the Device ID and Setup Password may be able to establish administrative access to the device.

4.10.1 Password Management

Authorised administrators may change the Setup Password and Wi-Fi Password through the Senquip Portal.

If a password is forgotten, an administrator may retrieve the current password through the Senquip Portal following identity verification.

4.10.2 Factory Reset

A factory reset restores device settings to their factory defaults, including the factory default passwords.

A factory reset does not change device ownership, user permissions, or the device identity recorded by the Senquip Cloud.

4.10.3 Administrative Recovery

If all administrator accounts are inadvertently removed from a device, administrative access may be re-established using the Setup Password.

Where appropriate verification can be completed, Senquip may also assist in restoring the original administrator account associated with the device.

Setup Mode

Setup Mode enables local configuration of the UNI-Z1 using either the Senquip Connect App via Bluetooth or the device's embedded web server via Wi-Fi.

5.1 Entering Setup Mode

To enter *Setup Mode*, power the UNI-Z1 and wait for the green Status LED to become solid. Press the *Setup* button. When the green Status LED starts flashing, the device is in *Setup Mode*.

If connected to external power, the UNI-Z1 will remain in *Setup Mode* while the lid is open. If external power is not available, the UNI-Z1 will enter sleep mode after 10 minutes of inactivity. To re-enter *Setup Mode*, press the *Setup* button again for 2 seconds.

Setup Mode is exited once the lid has been closed for more than 10 seconds.

5.2 Configuring the Device

Once the UNI-Z1 is in *Setup Mode*, local configuration can be performed using either:

- *Senquip Connect App (recommended)* - connects to the UNI-Z1 via Bluetooth.
- *Embedded Web Server* - connects to the UNI-Z1 via its Wi-Fi access point using a web browser.

For detailed instructions on using either method, see [Chapter 2](#).

Note Once a network connection has been established, it is recommended that further device configuration be performed remotely using the Senquip Portal.

Power Supply

The Senquip UNI-Z1 has been designed to offer maximum flexibility in terms of power supply requirements and is able to run off permanent power and solar.

6.1 Permanent power

A wide input range allows for use in automotive, industrial and telecoms applications. System power is backed up with an internal rechargeable battery in the event of power outages. Supply voltage is monitored to a resolution of 100mV and can be reported on a periodic basis if enabled.

The supply voltage input is reverse polarity protected and is resistant to damage from static and surge.

Parameter	Specification
DC supply voltage range	10 to 32 Volts
Maximum current draw (excluding IO)	500mA at 12V, 250mA at 24V
Maximum current draw (including IO)	700mA at 12V, 350mA at 24V
Hibernate voltage	9.5V

The UNI-Z1 can be used with a solar panel as a source of power. When used with solar, an internal rechargeable battery backs the device up overnight and during cloudy weather. When running on solar, the panel needs to be able to collect enough energy during sunlight hours to power the device through the night and on cloudy days. Keep in mind that solar panels will tend to get dusty and so should be over-rated to avoid regular maintenance. A typical 12V solar panel used to power the UNI-Z1 along with its specifications is shown below:



Figure 6.1. Typical UNI-Z1 solar panel

Parameter	Specification
Maximum power	10W
Voltage at maximum power	17V
Current at maximum power	0.56A
Open-circuit voltage	21.6V
Short-circuit current	0.68A
Width	357mm
Height	302mm

The above solar panel was tested with a UNI-Z1 measuring and reporting 2 input voltages, ambient temperature, ambient pressure and thermocouple temperature at an interval of 5 minutes. To conserve energy in what was a fixed location test, GPS location was measured every 20 base intervals or 100 minutes. The results were transmitted over 4G LTE or Wi-Fi at 5 minute intervals. The solar panel was sufficient to power the UNI-Z1.

Warning The open-circuit voltage of the chosen solar panel MUST be below 32V to avoid damage to the UNI-Z1.

6.2 Internal Rechargeable Battery

An Internal 7.2V, 500mAh rechargeable Lithium Titanate (LTO) battery is charged from system power, making the device ideal in applications where power is intermittent such as solar. The LTO battery can be fully recharged within 4 hours of system power being connected.

If the internal LTO has been allowed to completely discharge; when power is first applied to the UNI-Z1, the battery will go into a pre-charge mode where the battery is charged to a minimum level before the UNI-Z1 starts operating. Pre-charge mode is identified by a slow flash on the green LED with the orange LED off.

An internal protection circuits prevent damage to the LTO battery in the event of a short circuit or due to excessive discharge. A temperature monitoring circuit terminates LTO battery charging at temperatures below 0 °C and above 45°C. It is recommended that the LTO battery be replaced after three years of use or more regularly if the device routinely operates in extended temperatures. The LTO battery should only be replaced by a Senquip replacement part and should only be installed by a suitably trained technician.

System voltage which is closely related to the LTO battery voltage is monitored to a resolution of 100mV and is reported at the base interval.

Parameter	Value	Comment
LTO charge threshold	7.9 V	The LTO voltage below which a charge cycle is initiated
LTO precharge voltage threshold	XXX V	Slow flash on green LED, device not operational below this value
LTO charging voltage	8.2 V	Maximum voltage to which the LTO battery will be charged using <i>Maximum Capacity</i> profile.
LTO charging current	150 mA	Maximum charge current for the LTO battery.
LTO charge current termination	approx. 30 mA	Charge terminates when charge current is below this value.
System shutdown	6.8 V	Device enters freight mode when LTO voltage drops below this value.
Minimum input voltage for charging	10 V	External power must be above this voltage for the LTO battery to charge.
Maximum input current	600 mA	Not suitable for Lithium-thionyl Chloride batteries

Safety timer	8 hours	Time after which charging will cease
Charge temperature range	0 to 45°C	Charging will terminate outside of this range
Operating temperature range	-20 to 80°C	Charging will terminate outside of this range

6.2.1 Internal Battery Profile

An *Internal Battery Profile* setting allows selection between: *Extended Battery Lifespan* (default) and *Maximum Capacity*.

In *Extended Battery Lifespan* mode, the device slightly reduces the maximum charge voltage of the internal battery. Operating lithium cells below their absolute maximum voltage significantly increases cycle life and reduces long-term degradation. This setting is recommended for most applications, particularly in high-temperature environments where elevated temperatures already accelerate battery aging.

Maximum Capacity mode allows the battery to charge to its full rated voltage, providing the longest possible runtime between charges. This may be useful where maximum operating duration is critical, but it may reduce overall battery lifespan compared to the default setting.

6.3 Low Power Operation

The UNI-Z1 has been designed to be suitable for use in applications where permanent power is not available and solar and other sources of intermittent power are the only source of energy. Factors affecting power consumption include the rate at which sensor measurements are made, the number of transmissions of measured data and which internal and external sensors that are connected.

Broadly, the state of the UNI-Z1 can be divided into three modes: sleep, measurement and transmission. Sleep mode is by far the lowest power state where most internal sensors are turned off and the device is waiting for the next measurement period. During a measurement period, the sensors are turned on and power consumption increases dramatically. The actual power consumed during a measurement phase depends on the power requirements of connected sensors and the duration for which they are turned on. For instance, a 4-20mA pressure sensor will, by default, draw between 4mA and 20mA of current when turned on. The sensor will clearly use less energy when measuring 4mA than when measuring 20mA. Transmission is the most energy intense operation performed by the UNI-Z1. During transmission, the Wi-Fi and or 4G LTE radios are turned on and data is transmitted. Limiting the length of radio transmissions has a significant impact on energy consumed.

The following strategies can be used to limit power consumption:

- Limit the rate at which measurements are taken - if the parameter being measured changes slowly, then measuring it regularly will consume additional energy without a benefit.
- Turn off sensors that are not required - the UNI-Z1 contains a rich set of internal sensors. If for example, the GNSS is not required, turn it off.
- Choose external sensors carefully - a 4-20mA sensor may use more energy than a voltage output sensor.
- Limit the number of daily transmissions - consider only transmitting data when warning and alarm conditions are breached.
- Ensure that the device is placed in a position where 4G LTE, Wi-Fi, and GNSS reception is optimal. Far more current is consumed when transmitting and receiving in a poor signal environment.

Measured sleep, measurement, and transmission current is given in the table below. The measurements in the table represent current flowing from the internal battery, with external power to the device removed. Except where stated, the GNSS is assumed off. Actual values will depend on the power source, selected measurements, battery charge state, distance from Wi-Fi or 4G LTE source

and temperature.

Note Perform a factory reset before configuring for low power.

Mode	Current	Time
Sleep	65uA	Up to 24 hours
Measurement (no external sensors, GPS off)	40mA	0.5s
Measurement (no external sensors, GPS cold start)	70mA	54s
Transmit (WiFi from sleep)	97mA	8s
Transmit (4G LTE from sleep)	120mA	20s

6.4 Freight Mode

When shipping the UNI-Z1, it is important that the device is placed in freight mode. In freight mode, the UNI-Z1 is put into sleep mode to reduce battery drain to the minimum, and all transmitting devices are turned off. The UNI-Z1 will exit freight mode when it detects that power has been re-connected.

The freight mode function can be found via two methods:

- From the Senquip Portal, navigate to the Settings page for the device. Go to the Admin tab and open the *Freight Mode* window.
- From the device webserver by pressing the setup button or directly from a browser if the UNI-Z1 webserver is always on and you know the IP address. From the webserver, choose the *Admin* page.

Follow the steps below to enter freight mode:

1. Disconnect all wires including the power input.
2. Press the 'Enter Freight Mode' button from the Senquip Portal or the device webserver.
3. Wait 5 seconds, then check the Status and Network lights remain off.
4. Confirm freight mode has been entered by pressing the *Reset* button; there should be no response from the UNI-Z1.

The screenshot shows the Senquip web interface. At the top, there is a navigation bar with the Senquip logo, the device model 'ORB X1', and several tabs: Status, General, Network, Internal, External, Endpoint, Update, and Admin. The 'Admin' tab is selected. Below the navigation bar, there are two main sections. The first section is titled 'Change Password' and contains a text box explaining that this function allows changing the password to the local web interface, but it does not change the WiFi password in setup mode or any passwords used on the Senquip Portal. It includes three input fields: 'Old Password', 'New Password', and 'Confirm New Password', followed by a blue 'Change Password' button. The second section is titled 'Freight Mode' and contains a text box explaining how to put the device into a low-power freight mode. It lists three steps: 1. Disconnect all wires including the power input. Remove AA batteries (if fitted). 2. Press the 'Enter Freight Mode' button below. 3. Wait 5 seconds, then check the Status and Network lights remain off. It also includes a text box stating that to wake the device up again, power input should be connected to the terminal block. At the bottom of this section is a red 'Enter Freight Mode' button.

Figure 6.2. Entering freight mode

Note A shortcut is provided where pressing the *Setup* button three times, when in setup mode, will cause the UNI-Z1 to enter freight mode. Wait 5 seconds, then confirm freight mode has been entered by pressing the *Reset* button and checking that there are no LEDs or other indicators active.

General Setup

7.1 Measurement and Transmit Intervals

The UNI-Z1 can be configured to take periodic measurements and then to transmit those measurements at various intervals or on exception. When not measuring or transmitting, the UNI-Z1 will remain in a very low power state, referred to as sleep. For example, the UNI-Z1 can be configured to measure temperature at 1 minute intervals, but only to transmit the temperature once an hour or if a warning or alarm level is exceeded (an exception occurs). By allowing a more regular measurement interval and a less frequent transmit interval, the UNI-Z1 is able to reduce power consumption by remaining asleep, thereby maximising battery life. In the event of an exception, a more regular transmit rate can be selected.

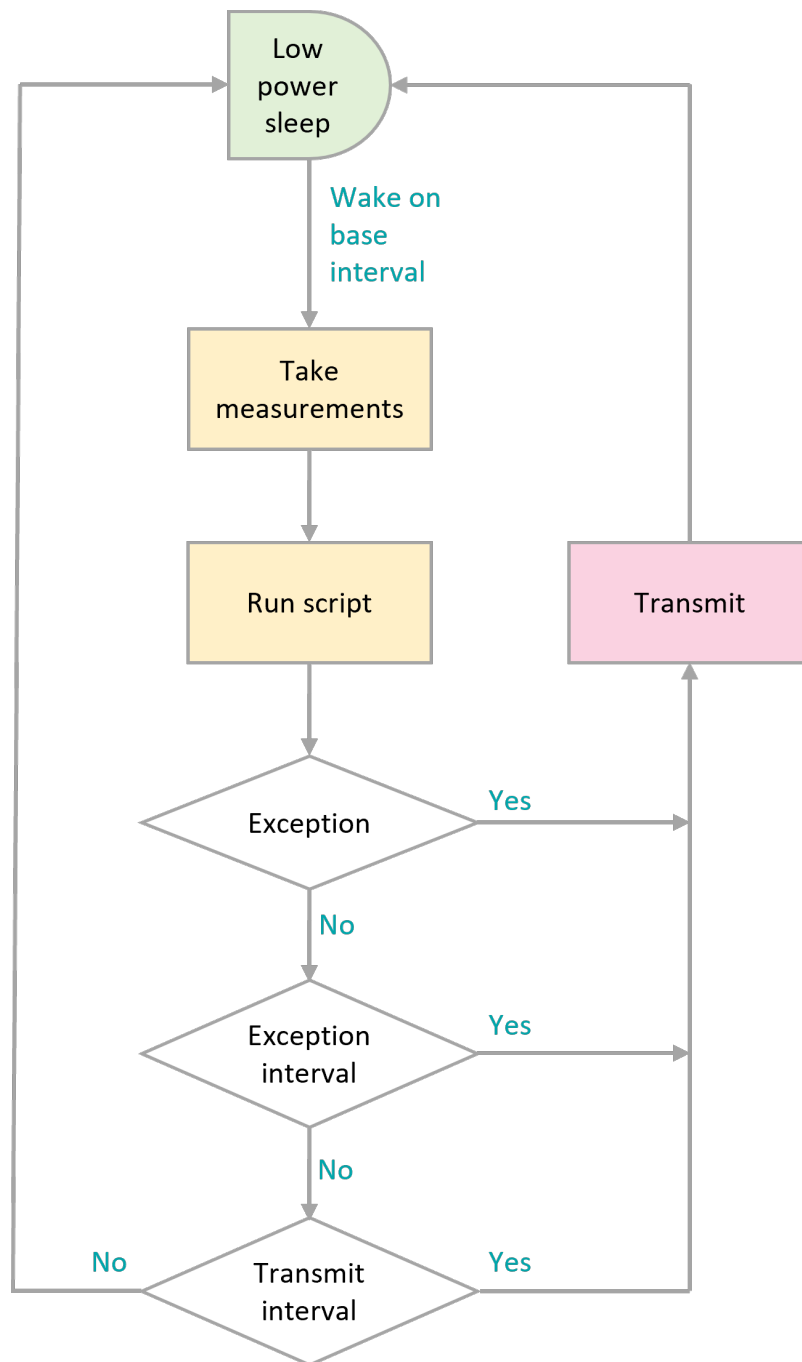


Figure 7.1. Timing flowchart

- Green: Lowest power state; aim to configure the UNI-Z1 to spend maximum time in this state.
- Orange: Moderate power usage; try to reduce the number of times that the UNI-Z1 wakes to measure sensors.
- Pink: Highest power consumption; only transmit data when required.

A summary of wake sources and their behaviour in sleep and hibernate is given in the table below.

TODO

Table

To allow flexible measurement and transmit intervals, whilst ensuring the lowest possible power consumption, the UNI-Z1 has three global and one per-peripheral measurement interval settings.

Base-Interval The base-interval is the period of time after which the UNI-Z1 will wake from sleep in order to check if there are any measurements to perform or if it is time to transmit the latest measured data. In a system where measurements are required often, the base-interval can be as low as 5 seconds. In systems that are slow to respond, the base interval can be as high as 24 hours. It makes sense to set the base interval as long as possible to enable the UNI-Z1 to spend as much time as possible in a low-power sleep state.

Each peripheral, whether internal to the UNI-Z1 or attached to the interface, can be set to only be measured after a number of base-intervals. If a particular peripheral has the interval setting set to 1, then it will be measured at each base-interval. If the interval is set to 0, then that particular peripheral will be turned off. Each time a measurement is taken, the results will be compared with alert, warning and alarm conditions and if an alert or exception occurs, the results will immediately be transmitted.

Note if a base-interval of less than 10 seconds is specified when the UNI-Z1 is communicating via Wi-Fi or 120 seconds over 4G LTE, the UNI-Z1 will remain awake at all times. This setting is not suitable for battery operated installations.

Note if the enabled measurements take longer to complete than interval at which they are scheduled, the UNI-Z1 will not return to sleep and measurements will be sent as fast as possible. This is most likely where the GPS and serial devices are enabled.

Transmit-Interval The transmit-interval is the time between message transmissions. It is a multiple of the base interval and is set as a number of base-intervals. All enabled measurements will be transmitted at the transmit-interval. For example, if the base-interval is 1 minute and the transmit-interval setting is sixty, then all the latest measurements will be transmitted every 60 minutes.

In cases where the UNI-Z1 is configured to measure more often than to transmit, measured data can be saved and transmitted in batches. It is more efficient to batch messages and transmit less regularly than to send individual measurements. Use this option where power use needs to be minimised but all measured data needs to be retrieved.

Note if during a measurement interval, an exception occurs, the UNI-Z1 will immediately transmit the measured data and will switch to the exception interval.

Note if measurement and transmission intervals coincide, measurements will be taken before transmission to ensure the latest values are transmitted.

Exception-Interval If a warning or alarm occurs, the transmit-interval can be shortened in order that measurements are transmitted more often. The exception-interval is a multiple of the base interval and sets the time between message transmissions when an exception is current (warning or alarm). For example, if the base-interval is 1 minute and the transmit-interval setting is sixty, under normal circumstances, measurements will be transmitted every 60 minutes. If the exception-interval setting is 5, then when a warning or alarm condition is current, measurements will be transmitted at 5 minute intervals instead of 60 minute intervals.

Note Only exceptions, which are warnings and alarms will trigger the exception-interval; alert conditions such as low battery will not.

If, on any base interval, a new exception or alert is detected, an immediate transmission will be made

regardless of the transmit-interval.

7.2 Power Supply Settings

The UNI-Z1 continuously monitors its external power source and can be configured to generate alerts, enter hibernate when power is lost, and record operating hours.

7.2.1 Power Loss Alert

When enabled, a power loss alert is generated when the external supply voltage falls below approximately 9.5V.

Where solar power is used, temporary power loss may occur during periods of low sunlight or poor weather conditions. In these applications, power loss alerts may occur when the sun sets or heavy cloud cover reduces solar output.

7.2.2 Hibernate on Power Loss

To conserve energy, the UNI-Z1 can be configured to enter hibernate mode when external power is removed.

When *Hibernate on Power Loss* is enabled, the device continues operating for a configurable number of base intervals after power is lost. This delay is specified by the *Hibernate Delay Intervals* setting.

Once the delay has expired, the device enters hibernate mode to minimise power consumption.

7.2.3 Hibernate Interval

The *Hibernate Interval* setting specifies how often the UNI-Z1 performs a full wake-up cycle while hibernating. During a full wake-up cycle, measurements are taken, alarms are processed, scripts run, and the device transmits.

The interval is configurable between 5 minutes and 24 hours and defaults to 21600 seconds (6 hours).

When hibernating, the UNI-Z1 periodically performs brief wake-ups to check for the return of external power. These wake-ups are optimised for low power consumption and do not perform a normal measurement and transmission cycle.

7.2.4 Count Hours

When enabled, the UNI-Z1 records the number of hours for which external power is present.

This feature can be used as a simple indication of engine or equipment operating hours where a dedicated hour meter is unavailable. More sophisticated utilisation calculations can be implemented using scripts that combine power, vibration, movement, and other measurements.

7.3 Settings

A full list of general settings is given in the table below.

TODO

Table

Internal Sensors

8.1 Tamper sensor

The UNI-Z1 is equipped with an internal tamper switch that is used to activate the setup functions when the lid is opened and to detect tamper attempts. The tamper switch is sampled on a regular basis and does not have an associated measurement interval.

An alert can be generated when the lid is opened.

Note A tamper alert, if enabled will be triggered by a tamper attempt or an authorised entry to change settings.

A full list of tamper switch settings is given in the table at the end of the chapter.

8.2 Accelerometer

The UNI-Z1 contains an integrated 3-axis accelerometer that provides orientation and motion measurements.

The accelerometer can be used to measure:

- Pitch
- Roll
- Tilt
- Vibration Level
- Impact Detection

Although these functions use the same accelerometer, they operate differently and are intended for different applications.

8.2.1 Tilt Measurement

The accelerometer measures acceleration in the X, Y and Z axes. Raw acceleration values are available in G and can be used for custom calculations.

To provide stable orientation measurements, each tilt measurement consists of 10 acceleration samples taken at 1 ms intervals. The average of these samples is used to calculate Pitch, Roll and Tilt.

The X axis passes through the lid of the device, the Y axis passes horizontally through the device and the Z axis passes vertically through the device.

When looking at the front cover, positive pitch is defined as the top of the UNI-Z1 tilting towards

the observer. Negative pitch is defined as the top of the UNI-Z1 tilting away from the observer.



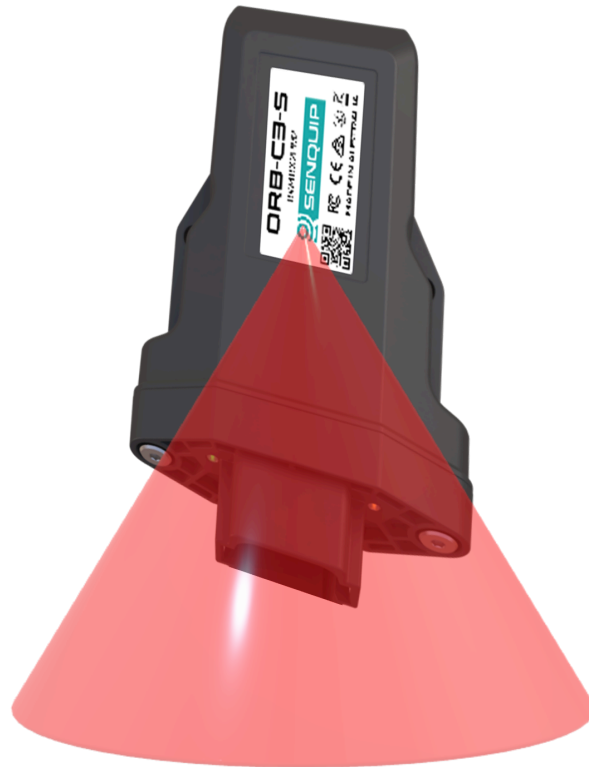
Figure 8.1. Definition of pitch

When looking at the front cover, positive roll is defined as the top of the UNI-Z1 rotating towards the right. Negative roll is defined as the top of the UNI-Z1 rotating towards the left.



Figure 8.2. Definition of roll

Pitch and Roll are useful where the monitored object has a defined front, back, left and right, such as a vehicle. For objects such as poles or masts, Tilt is generally more useful.



Any angle

Figure 8.3. Definition of tilt

8.2.2 Specification

Parameter	Specification
G-force range	+/- 2G
Resolution	1mG
Sensitivity change vs temperature	0.1% per°C
Typical zero-g level offset accuracy	+/- 40mG
Tilt resolution	0.1 deg
Tilt accuracy (0-45 deg)	1.0 deg
Tilt accuracy (45-90 deg)	2.0 deg

8.2.3 Settings

Accelerometer measurements can be scheduled as a multiple of the base interval. Setting the *Interval* to 1 causes measurements to occur every base interval. Increasing the interval reduces power consumption.

Pitch, Roll and Tilt warning and alarm thresholds can be configured. After each measurement, the measured value is compared with the configured warning and alarm limits. If a threshold is exceeded, an alert message is transmitted immediately. While the condition persists, messages are transmitted at the exception interval.

Hysteresis can be configured to prevent repeated alerts when measurements fluctuate around a threshold due to vibration.

Note Pitch and Roll warning and alarm levels may be positive or negative. Tilt warning and alarm levels are always positive.

8.2.4 Vibration Level

The reported Vibration Level provides an indication of the amount of vibration present during the measurement interval. It is intended for long-term condition monitoring, such as detecting increasing vibration caused by bearing wear, imbalance or mechanical deterioration.

Each time a vibration measurement is performed:

1. The latest 32 acceleration samples are read from the accelerometer.
2. A statistical variance calculation is performed on the X, Y and Z measurements.
3. The calculated Vibration Level is reported.

Because only the most recent 32 samples are analysed, the reported Vibration Level represents the vibration at the time the measurement was taken. A short impact that occurs between measurements may not be reflected in the reported value.

Vibration Level is therefore best suited to measuring changes in vibration over time rather than detecting individual impact events.

8.2.5 Impact Detection

Impact Detection is designed specifically to detect short-duration shock events.

Unlike Vibration Level, the accelerometer continuously monitors acceleration in hardware. Two independent impact detectors are available, each with its own configurable acceleration threshold and minimum duration.

Each impact detector has its own acceleration threshold and minimum duration. When both conditions are satisfied, the accelerometer immediately generates an interrupt. The device records the event and can transmit an Impact alert.

Because monitoring is continuous, impacts are detected regardless of when they occur within the base interval.

Note An Impact alert indicates only that the configured threshold has been exceeded. It does **not** report the actual peak acceleration. For example, if an impact threshold is configured for 200 mG and an alert is generated, the actual impact may have been 210 mG, 500 mG or higher.

The two impact detectors allow different severity levels to be configured independently. For example:

- Impact 1: 200 mG for 30 ms
- Impact 2: 400 mG for 200 ms

8.2.6 Choosing the Correct Measurement

Requirement	Recommended Feature
Measure orientation	Pitch, Roll or Tilt
Monitor machine vibration	Vibration Level
Detect long-term vibration trends	Vibration Level
Detect shock or impact events	Impact Detection

Note Vibration Level and Impact Detection are independent functions. It is therefore normal for an Impact alert to be generated while the reported Vibration Level remains relatively low.

8.3 Temperature sensor

An integrated temperature sensor allows for measurement of ambient temperature. Please be aware that the temperature sensor will measure the temperature inside the UNI-Z1 enclosure; this temperature can be subject to fluctuations, for example when the internal battery is charging and so the environment within the device heats up. For accurate external temperature measurement or to measure a wider range of temperatures, use an external temperature sensor.

8.3.1 Specification

Parameter	Specification
Measurement range	-40 - 85°C
Resolution	0.01 deg°C
Absolute accuracy (25°C)	+/-0.5 deg°C
Absolute accuracy (0 - 65°C)	+/-1 deg°C

8.3.2 Settings

Measurements can be scheduled as a multiple of the base-interval. The fastest possible measurement rate is achieved by setting the *interval* to 1 in which case measurements will occur on every base interval. To reduce power consumption, the measurement rate can be turned down by increasing the *interval*.

Warning and *alarm* thresholds for ambient temperature can be enabled. Once enabled, each time a measurement is completed, the returned value will be compared with minimum and maximum *warning* and *alarm* thresholds. If a *warning* or *alarm* level is breached, a message will immediately be transmitted. As long as the warning or alarm condition persists, messages will be transmitted at the exception-interval rather than the transmit-interval. *Hysteresis* can be specified in 1°C increments, to prevent multiple alarms in the presence of fluctuating temperature.

A full list of temperature sensor settings is given in the table at the end of the chapter.

8.4 GPS

Models of the UNI-Z1 that have 4G LTE connectivity also have an integrated Global Navigation Satellite System (GNSS). The GNSS receiver, allows for position and speed based reporting. The internal GNSS receiver uses GPS, GLONASS, BeiDou and Galileo satellites to ensure high accuracy measurement and fast time to first fix. Data available from the GPS includes:

- Latitude, longitude and altitude
- Speed (km/h) and bearing
- Date and time
- Number satellites being tracked

In order to utilise GNSS, the antenna needs to be mounted with clear visibility of the sky. Plastic and fibreglass roof sheeting will have a minimal effect on GNSS performance whereas reinforced concrete and metal roofs will render the GNSS inoperable. Good GNSS signal quality will result in quicker time to position acquisition and lower power use.

8.4.1 Specification

Parameter	Specification
Time to first fix from power up	Typically 20 seconds
Position update rate	Maximum 1Hz
Horizontal position accuracy	<2.5m CEP
Vertical position accuracy	Typically <10m
Maximum Altitude	18000m
Horizontal speed accuracy	<0.1 m/s (<0.36 km/h)
Maximum Velocity:	515m/s
Tracking channels	33
GPS/Galileo L1	1575.42MHz
GLONASS L1	1602.5625MHz
BeiDou	1561.098MHz

Note GNSS accuracy is specified as Circular Error Probable (CEP). A specification of <2.5m CEP indicates that 50% of position fixes will be within 2.5m of the true position. Typical 95% accuracy is better than 5m under open-sky conditions.

8.4.2 Settings

Measurements can be scheduled as a multiple of the base-interval. The fastest possible measurement rate is achieved by setting the *interval* to 1 in which case measurements will occur on every base interval. To reduce power consumption, the measurement rate can be turned down by increasing the *interval*. The GNSS is a high power peripheral and so use should be limited when running on battery power.

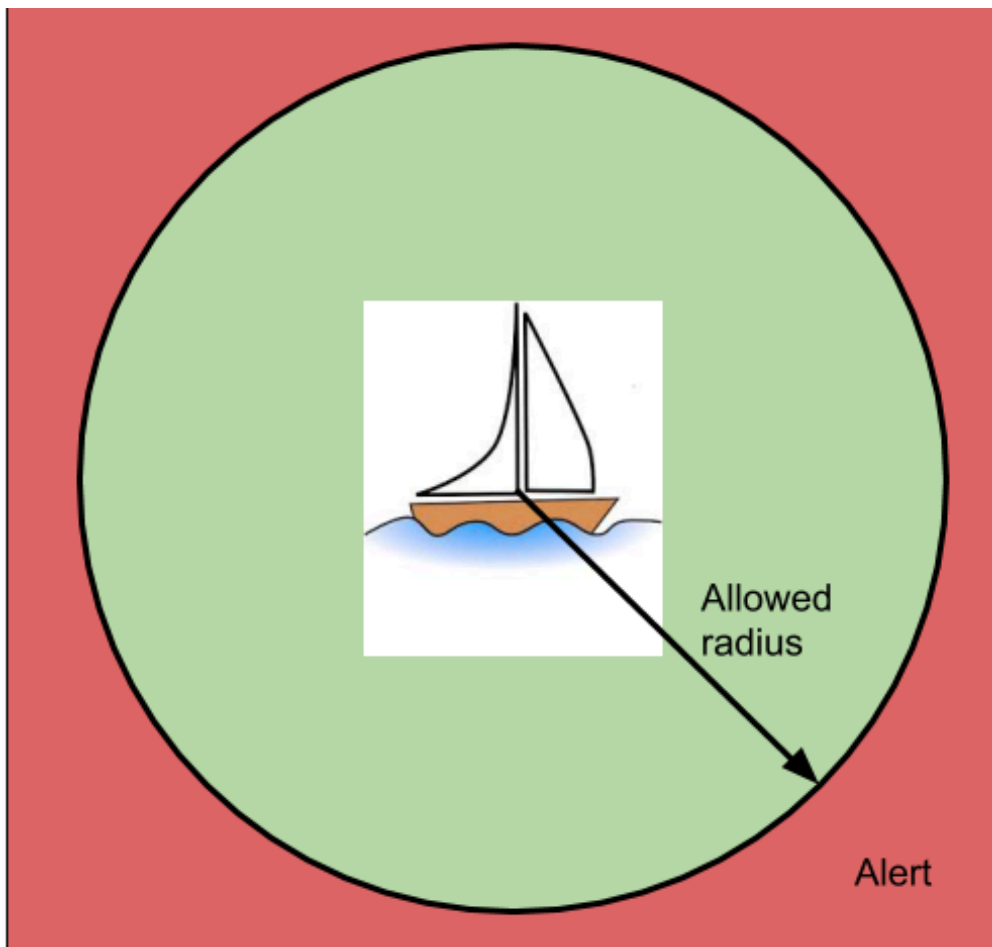


Figure 8.4. GPS alert parameters

The GNSS can create an *alert* based on position and speed. A known position (*expected latitude* and *expected longitude*) can be specified and if the device moves a particular *radius* from that point, an alert can be raised. *Hysteresis* can be specified in 1 meter increments to prevent multiple alerts, for instance as a boat swings on a mooring near the edge of the allowed radius. Likewise, a maximum *speed* can be specified and if the device exceeds that speed, an alert will also be raised. Speed *hysteresis* can be specified in 1km/h increments, to prevent multiple alerts as the speed fluctuates at the alert point. The time that GNSS speed exceeds 2km/h can be counted and used to calculate machine utilisation.

Note In the example above, the UNI-Z1 could also report bilge water level, solar battery voltage and a host of other parameters associated with the yacht.

A full list of GNSS settings is given in the table at the end of the chapter.

8.5 Bluetooth interface

The UNI-Z1 has a Bluetooth peripheral that can transmit and receive Bluetooth Low Energy (BLE) advertising packets. BLE beacons typically use the advertising packets to communicate measured data such as temperatures, voltages, movement, and battery voltage. BLE tags are a special type of beacon that typically only contain identification information and are used to locate items. BLE beacons send advertising messages at different rates. Some report every second and some may be every minute or more. Battery operated BLE devices tend to send at lower rates to save power. Some BLE device are smart and will slow their send rate if they are not being used. A tire pressure moni-

toringdevice may stop sending if the tire is not rotating. Typical protocols used in advertising packets include Eddystone and iBeacon. The UNI-Z1 supports both.

The BLE beacons from ELA shown below enable identification, and measurement of temperature, humidity, voltage, switch position, and more.



Figure 8.5. Example BLE beacons from ELA

The UNI-Z1 will report the beacon address, data, and the strength of the received signal.

- The address (or identifier) is unique and allows individual tags to be recognised.
- The data may contain battery voltage, temperature, humidity, or any other data being conveyed by the beacon.
- The receive signal strength (RSSI) gives an indication of how strong the signal from the beacon is.

For details on using the UNI-Z1 as a BLE beacon to transmit custom advertising packets, please refer to the [Senquip Scripting Guide](#).

Note The BLE module and Wi-Fi module share a common radio. BLE operation will work best when the UNI-Z1 is operated using a cellular network rather than Wi-Fi.

8.5.1 Specification

Parameter	Specification
Bluetooth version	4.2

8.5.2 Settings

Measurements can be scheduled as a multiple of the base-interval. The fastest possible measurement

rate is achieved by setting the *interval* to 1 in which case the Bluetooth peripheral will be sampled on every base interval. To reduce power consumption, the measurement rate can be turned down by increasing the *interval*.

When active, the Bluetooth peripheral will scan for all advertising packets. In a typical environment, phones, computers, and other devices are all advertising. The UNI-Z1 Bluetooth peripheral could easily report a dozen Bluetooth devices even when the one you are searching for is off. A filter allows only the required Bluetooth devices to be reported by filling in the *Address Capture List*. Required addresses should be entered in hexadecimal and should be separated by commas. When the UNI-Z1 wakes for the next measurement interval, the Bluetooth peripheral will be sampled until all the messages listed have been found or the *Capture Time* has been reached. If multiple messages with the same identifier are required in a single measurement interval, place a * followed by the number of messages of that identifier to be returned after the identifier in the list. For example: 98588A10375E*4, 98588a103777, 98588a103888*10 will return 98588A10375E four times, 98588a103777 once and 98588a103888 ten times. Leave the *ID Capture List* blank to receive all messages.

The *Capture Time* setting can be used to set a timeout after which the Bluetooth peripheral will stop listening, allowing the device to transmit received messages and return to sleep. *Capture-time* can be used as a mechanism to allow the UNI-Z1 to sample the environment for devices for a defined time-period.

A full list of Bluetooth settings is given in the table at the end of this chapter.

8.6 Internal sensor settings

A full list of settings for internal sensors is given in the table below.

Name	Item	Function	Range	Unit	Internal Reference
Light Sensor					
Name	text	A name for the light sensor that is meaningful to the user.	25 chars		tamper.name
Tamper Alert	boolean	This parameter determines if an alert is generated when the light sensor detects light or not.			tamper.enable
Ambient Temperature					
Name	text	A name for the input that is meaningful to the user.	25 chars		ambient.name
Interval	integer	The number of base intervals after which the temperature is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.	0 to 10000		ambient.interval
Hysteresis	decimal	The amount by which the measured value has to drop below the threshold to re-enable the alert after an event.	0 to 100	°C	ambient.hysteresis
Warning	text	Warning thresholds. Refer to user guide.	-40 to 100	°C	ambient.warning
Alarm	text	Alarm thresholds. Refer to user guide.	-40 to 100	°C	ambient.alarm
Accelerometer					
Name	text	A name for the input that is meaningful to the user.	25 chars		accel.name

Interval	integer	The number of base intervals after which the accelerometer is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.	0 to 10000		accel.interval
Output XYZ Vectors	boolean	Send X,Y,Z gravity vectors in data output.			accel.outputxyz
Hysteresis	decimal	The amount by which the pitch, roll or angle has to exceed a threshold before triggering alarms or warnings.	0 to 20	Degrees	accel.hysteresis
Pitch Warning	text	Warning thresholds. Refer to user guide.	-90 to 90	Degrees	accel.pitch.warning
Pitch Alarm	text	Alarm thresholds. Refer to user guide.	-90 to 90	Degrees	accel.pitch.alarm
Roll Warning	text	Warning thresholds. Refer to user guide.	-90 to 90	Degrees	accel.roll.warning
Roll Alarm	text	Alarm thresholds. Refer to user guide.	-90 to 90	Degrees	accel.roll.alarm
Angle Warning	text	Warning thresholds. Refer to user guide.	0 to 90	Degrees	accel.angle.warning
Angle Alarm	text	Alarm thresholds. Refer to user guide.	0 to 90	Degrees	accel.angle.alarm
Motion Warning	text	Warning thresholds. Refer to user guide.	0 to 5000	milli-g	accel.motion.warning
Motion Alarm	text	Alarm thresholds. Refer to user guide.	0 to 5000	milli-g	accel.motion.alarm
Wake from Hibernate	boolean	The high warning motion threshold is used to wake the device when hibernating.			accel.motion.wake_from_hiber
Motion Wake Threshold	decimal	The motion threshold above which the device will wake from hibernation.	1 to 2000	milli-g	accel.motion.wake_threshold
Count Motion Hours	boolean	Counts the number of hours the device exceeds the Motion Wake Threshold. Typically used as an machinery work vs idle hour meter.			accel.motion.count_hours
GPS					
Name	text	A name for the GPS signal that is meaningful to the user.	25 chars		gps.name
Interval	integer	The number of base intervals after which the gps is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.	0 to 10000		gps.interval
Max Time	integer	Maximum time the device will wait for a valid GPS fix.	0 to 3600	Seconds	gps.maxtime
Position					
Position Alert	boolean	Sets whether a change in position generates an alert.			gps.position.alert.enable
Radius	integer	An alert will be raised if the device moves further than this value from the expected position.	1 to 10000	Meters	gps.position.alert.radius

Hysteresis	integer	Once the alert is active or inactive, the radius must change by this value to change the alert state.	1 to 10000	Meters	gps.position.alert.hysteresis
Expected Latitude	decimal	Latitude at which the device is expected to be.	-90 to 90	Degrees	gps.position.alert.lat
Expected Longitude	decimal	Longitude at which the device is expected to be.	-180 to 180	Degrees	gps.position.alert.lon
Speed					
Count Movement Hours	boolean	Counts the number of hours the device is moving according to the GPS speed.			gps.speed.count_hours
Speed Alert	boolean	Sets whether a change in speed generates an alert.			gps.speed.alert.enable
Threshold	integer	An alert will be raised if the device's speed goes above this threshold.	1 to 1000	km/h	gps.speed.alert.threshold
Hysteresis	integer	Once the alert is active or inactive, the speed must change by this value to change the alert state.	1 to 1000	km/h	gps.speed.alert.hysteresis
Bluetooth					
Name	text	A name that is meaningful to the user.	25 chars		ble.name
Interval	integer	The number of base intervals after which the Bluetooth module is turned on. Set to 0 to disable.	0 to 10000		ble.interval
Scan Time	integer	The device will capture matching messages for this length of time.		Seconds	ble.capture_time
Address Capture List	text	List of addresses to be captured in HEX format, separated by a comma. Leave blank to capture all.	200 chars		ble.id_list
Send Raw Data	boolean	If ticked, all captured messages will be added to the data message.			

External Sensors

9.1 Inputs and Outputs

The UNI provides two configurable input/output (IO) channels that can be used for measuring voltages, counting pulses, measuring frequency and duty cycle, controlling external devices, and interfacing to 1-Wire sensors.

Pin	Name	Description
4	IO1	Digital input, pulse input, 1-Wire, and output
5	IO2	Voltage input, and output

The available functions are summarised below.

Function	IO1	IO2
Digital measurement	X	
Voltage measurement		X
Pulse count	X	
Frequency	X	
Duty cycle	X	
Wake on change	X	X
Switch to GND	X	X
Pullup	X	
1-Wire	X	

9.1.1 General IO Settings

Each IO can be configured independently.

Measurement Interval

Measurements can be scheduled as a multiple of the base interval. The fastest possible measurement rate is achieved by setting the *Interval* to 1, in which case measurements will occur on every base interval. To reduce power consumption, the measurement rate can be reduced by increasing the *Interval*. To disable an IO, set the *Interval* to 0.

Default State

The default state determines the output state of an IO between measurement cycles.

Note The state of an IO may deviate from the settings if being controlled by a script.

Measurement State

The measurement state determines the state of an IO during a measurement cycle.

Measurement Time

The measurement time determines how long the device hold the IO in the measurement state before taking a measurement. This allows attached sensors to boot, or for measurements to settle before being measured.

9.1.2 IO1

IO1 supports digital measurement, pulse counting, frequency measurement, duty cycle measurement, wake-on-change, 1-Wire communications, and output switching.

Digital inputs are measured using a threshold of approximately 2V. Voltages below the threshold are interpreted as OFF and voltages above the threshold are interpreted as ON.

Pulse counting can be used with flow meters, rain gauges, energy meters, run sensors, and other pulse-output devices. Frequency and duty cycle measurements use the same pulse measurement circuitry.

Many pulse-output sensors, including reed-switch flow meters and rain gauges, use open-collector outputs or voltage-free contacts that switch to ground. In these applications, the internal pullup resistor can be enabled to provide the required bias voltage for pulse detection.

For low-power applications, IO1 may be configured to wake the device when the input changes state.

9.1.3 IO2

IO2 supports voltage measurement, wake-on-change, and output switching.

Voltage measurements may be calibrated into end-use engineering units. For example, a 0-10V level transmitter representing a water level of 0-1m can be configured so that the measured value is reported directly in metres. This allows sensor outputs to be displayed and alarmed in meaningful application units rather than raw voltages.

For low-power applications, IO2 may be configured to wake the device when the input changes state.

9.1.4 Output Functions

The IO can also be used as outputs and can be switched to:

- OFF - High impedance.
- GND - Connects the IO to ground.
- PULLUP - Enables an internal pullup resistor (IO1 only).

OFF disconnects all internal sources from the IO, leaving the pin in a high impedance state.

GND connects the IO to ground through a protected low-side switch and is typically used to activate relays, alarms, indicators, contactors, and other externally powered devices.

PULLUP enables an internal pullup resistor to 3.3V and is typically used with voltage-free contacts, reed switches, and open-collector outputs.

9.1.5 Output Characteristics

Each IO output can switch voltages up to 32V and sink currents up to 250mA.

The outputs are protected against overloads, short circuits, electrostatic discharge, inductive transients, and excessive temperature. If a fault condition occurs, the output automatically protects itself and will automatically resume operation when the fault is removed.

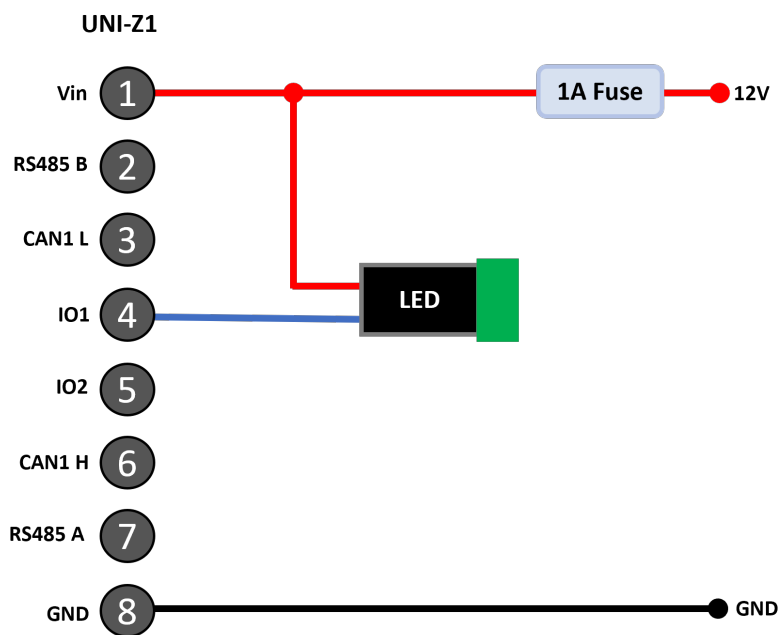


Figure 9.1. Switching a resistive load

The IO are capable of switching inductive loads such as relays and solenoids; however, flyback diodes should always be fitted to inductive loads to minimise electrical stress and improve system reliability.

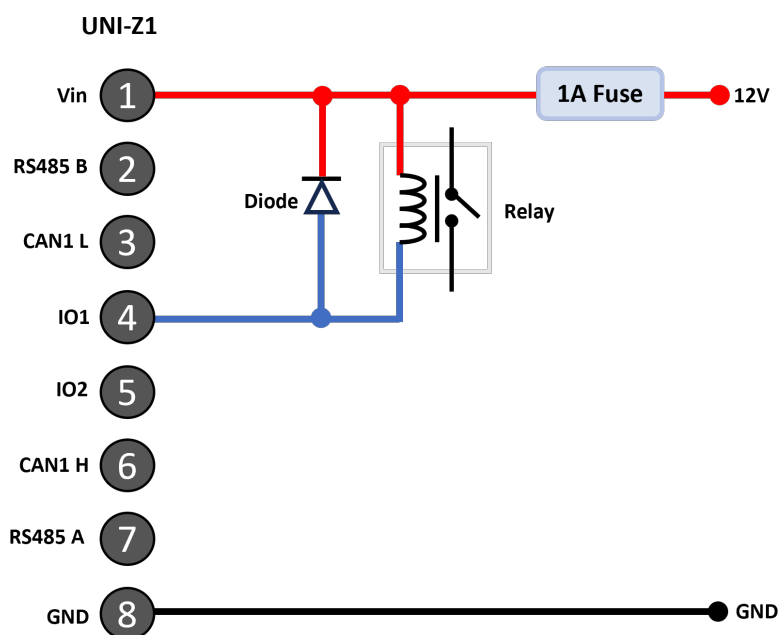


Figure 9.2. Switching a high inductance load

9.1.6 Pulse Measurement

IO1 can be used to measure pulse count, frequency, and duty cycle.

Pulse counting records the number of input transitions occurring during the measurement period. Frequency measurement determines the pulse repetition rate, while duty cycle measurement deter-

minesthe proportion of time the signal remains active.

Input transitions are detected when the signal crosses the digital input threshold of approximately 2V. For reliable operation, input signals should transition cleanly through the threshold voltage and excessive noise around the threshold should be avoided.

The figure shows how to wire a flow meter with a reed-switch using the internal pullup on the UNI-Z1.

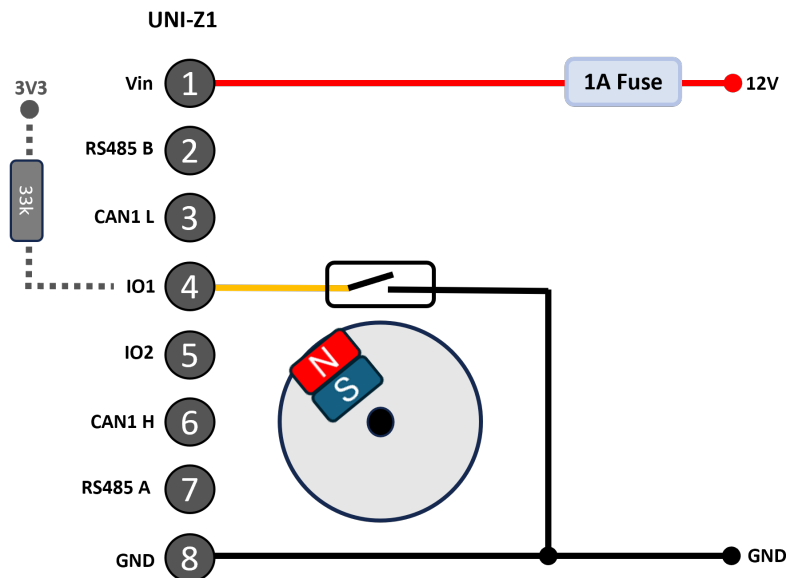


Figure 9.3. Pulse counting

9.1.7 Wake on Change

Wake-on-change allows the UNI to wake from low-power sleep modes when an input changes state.

This feature is particularly useful when monitoring alarm contacts, limit switches, float switches, reed switches, pulse-output sensors, and other event-driven inputs that require immediate response. In many of these applications, the internal pullup resistor on IO1 can be enabled, allowing the sensor to pull the input low when activated.

9.1.8 Calibration

Calibration can be applied to each measurement so that the value returned by the Senquip UNI-Z1 is in units that are meaningful in the end application. For instance, a level sensor that outputs a voltage between 0 and 10V may represent a water level between 0 and 1 metre. The voltage measurement can be calibrated to convert from volts to the more meaningful unit of metres.

In any system, the measurement instrument (the Senquip UNI-Z1), the sensor, and possibly the measured value will be subject to errors that may accumulate to reduce accuracy. To achieve an accurate and meaningful measurement, a calibration can be performed.

In this example, the tank could be calibrated by measuring the sensor output at two known levels. At a level of 0.1m, the measured voltage may be 1.05V. At a level of 0.8m, the measured voltage may be 8.12V. The calibration would then be filled into the IO setting as shown below:

Low In	1.05	This is the value in volts measured by the Senquip UNI-Z1
Low Out	0.1	This is the actual value that we would like to report
High In	8.12	This is the value in volts measured by the Senquip UNI-Z1
High Out	0.8	This is the actual value that we would like to report

Unit	m	The unit to be reported is metres
------	---	-----------------------------------

9.1.9 Warnings and Alarms

For each measurement type, high and low warning and alarm levels can be set. Once enabled, each time a measurement is completed, the returned value will be compared with low and high *warning* and *alarm* thresholds. If a *warning* or *alarm* level is breached, a message will immediately be transmitted. As long as the *warning* or *alarm* condition persists, messages will be transmitted at the *exception-interval* rather than the *transmit-interval*.

Note If calibration has been applied, then the warning and enable thresholds should be set in the calibrated units.

To set a high level warning or alarm only, set the low level to a value that is impossible to achieve. For instance, to set a high-only warning at 50V, set the low warning to -1V, which is an unachievable value.

Hysteresis can be specified in increments of the specified unit, to prevent multiple alarms in the presence of electrical noise.

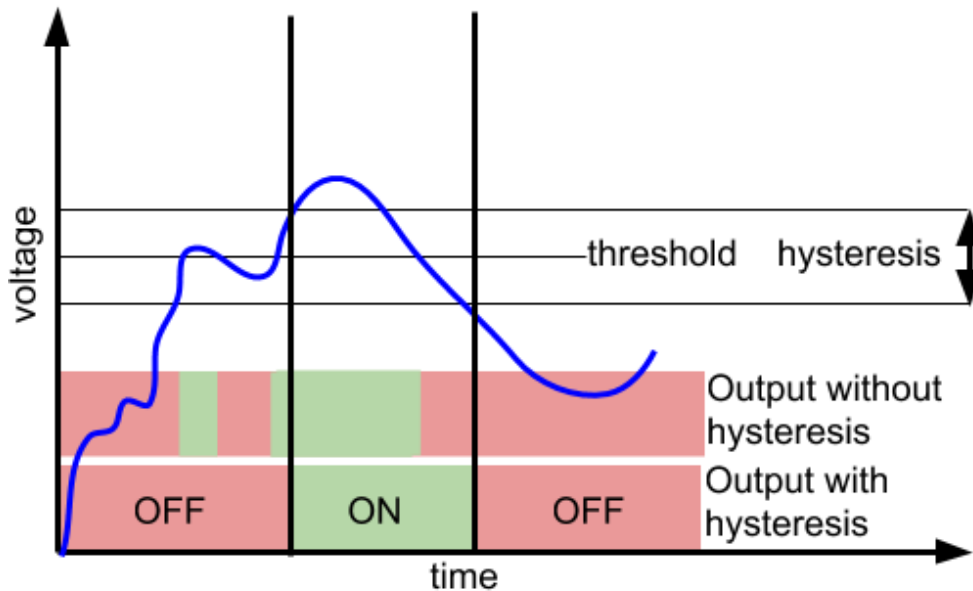


Figure 9.4. Hysteresis

9.1.10 1-Wire

IO1 can be configured for 1-Wire communication by selecting *1WIRE* as the *IO1 Default State*. When 1-Wire is enabled, IO1 is dedicated to 1-Wire operation and all other IO1 measurement and output functions are disabled.

1-Wire is commonly used by digital temperature sensors, identification devices, and other low-speed digital sensors.

The 1-Wire data line is connected to IO1. Multiple 1-Wire devices can share the same bus as each device contains a unique factory-programmed address.

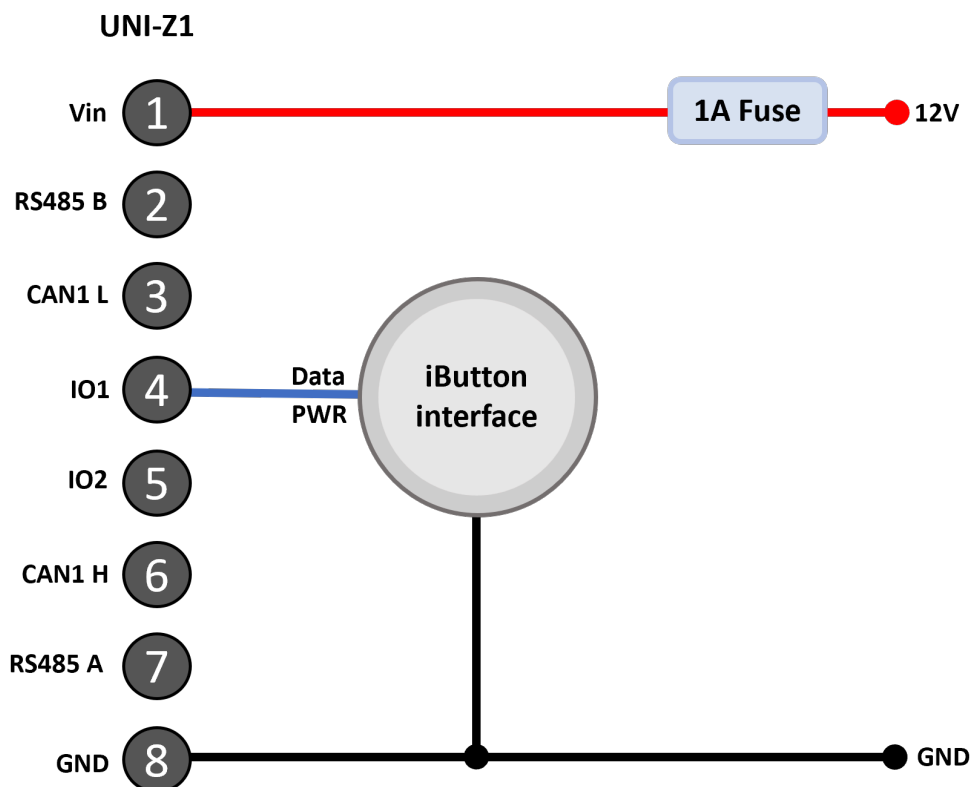


Figure 9.5. iButton reader connected to IO1

Communication with 1-Wire devices is performed entirely from script. The script is responsible for discovering devices, selecting addresses, issuing commands, reading responses, and dispatching measurements.

Note Some 1-Wire devices support parasite power operation. Where reliable operation is important, powering sensors from an external supply is recommended.

9.1.11 Scripting

The IO can be controlled directly from scripts.

Scripts can read measurements and change output states.

Warning If an IO is enabled in the settings and is also used in a script, the behaviour of that IO will be affected by both the settings and the script.

Note In sleep and hibernate modes, the outputs default to *OFF*. If a pullup has been enabled, it will remain active during sleep and hibernate.

9.1.12 Specification

Parameter	Specification
Output	
Open circuit voltage maximum	32V
GND sink current maximum	250mA per pin

Pullup resistor	33k to 3.3V
IO terminal input impedance to ground (without pullup)	>250k ohms
Voltage Measurement (IO2)	
Voltage ADC Type	12 bit SAR
Voltage range	1.5-32VDC
Voltage measurement resolution	10mV
Voltage measurement accuracy	TBD
Threshold for IO to wake from hibernate	2.0V +/-0.5V
Frequency and Pulse	
Frequency measurement range	TBD
Frequency measurement accuracy	TBD
Pulse counting detection threshold	2.0V +/-0.5V
Pulse counting maximum frequency in sleep	TBD
Pulse counting maximum frequency always on	TBD
Pulse minimum width	TBD
Duty cycle measurement range	0% to 100%
Duty cycle accuracy	TBD

Note Due to the characteristics of the ADC used by the UNI-Z1, input voltages below approximately 1.5V on IO2 will be reported as 0V.

9.2 Serial interface

The serial port can be used to capture data that is sent from an external system or to interface to a MODBUS sensor.

The UNI-Z1 provides an RS485 interface on pins 2 and 7 of the header. The pin functions are shown in the table below. When required, an optional 120Ω termination resistor can be enabled in the settings.

Pin	Function
2	RS485-B
7	RS485-A

Note RS485-B is sometimes referred to as D+ or TX+/RX+ and RS485-A as D- or TX-/RX-.

The serial interface supports RS485 operation.

The interface incorporates protection features to improve robustness and reliability in industrial environment with the RS485 receiver offering full failsafe operation for floating, shorted, or terminated inputs.

9.2.1 Specification

Parameter	Specification
RS485 differential output voltage (minimum with load resistance 120Ω)	+2V
RS485 differential input threshold (typical)	+/-200mV
Maximum nodes in RS485 mode	256
RS485 termination resistor	120Ω
ESD protection	+/-16kV

9.2.2 Settings

Measurements can be scheduled as a multiple of the base-interval. The fastest possible measurement rate is achieved by setting the *interval* to 1 in which case measurements will occur on every base interval. To reduce power consumption, the measurement rate can be turned down by increasing the *interval*.

In *serial capture* mode the measurement interval can be used to reduce the number of readings being provided by a connected sensor or system that may be permanently powered. If for instance, a connected system is sending a message every second but it is only required to be read and transmitted every minute, the measurement interval can be set to 1 minute in which case the device will wake on the minute interval, receive a message and return to sleep thereby missing the other 59 messages sent by the attached system. Since serial packets cannot be interrogated by the UNI-Z1 without a customised script, it makes sense to set the measurement interval to the same as the transmit interval in most cases.

An optional 120Ω RS485 termination resistor can be selected by selecting the *Termination resistor* option. The purpose of the termination resistor is to match the impedance of a transmission line to the hardware impedance of the interface to which it is connected. Termination is generally not required in lower speed networks (9600 baud or less) and networks shorter than 500m in length. No more than 2 termination resistors should be used, one at each end of the RS485 transmission line.

A *baud rate* of 4800, 9600, 19200, 38400, 56800 or 115200 needs to be selected using the *baud rate* option. Other settings, including the number of bits, odd or even parity and 1 or 2 stop bits are added in the *settings* field. The most common setup is 8 bits, no parity and 1 stop bit or “8N1”.

The serial interface can be configured in serial capture mode or **MODBUS** mode using the *mode* option. Capture mode is typically used where an external sensor sends serial data and a portion of that serial data is to be captured. MODBUS mode is used to connect to external sensors that are compatible with the MODBUS standard.

In *serial capture mode* The device listens for periodic data and when received, transmits this data at the next send interval. The maximum length of a message that can be captured is 512 characters. Once 512 characters have been received, the UNI-Z1 will terminate the capture and will transmit it on the next transmit interval.

In capture mode, the *max-time* setting can be used to set a timeout after which the serial port will return to sleep. *Max-time* can be used as a way to end serial measurement in the event that no serial data is received, or as a mechanism to allow the device to sample the serial port for a defined time-period.

Note If the serial port needs to be kept on all the time, set the *max-time* to longer than the measurement interval. The contents of the serial buffer is retained as long as the device does not return to sleep.

The operation of the *max chars* option is similar to the *max time* setting except that the serial port stops sampling after a certain number of characters has been received. In most cases where the *max-chars* setting is used to terminate serial capture, the *max-time* setting is also used to end the serial measurement in the event that data does not arrive.

In *Serial capture mode*, in systems where many messages are sent and only a few are of interest, a *start string* of up to 10 characters can be enabled. For instance, in a typical GPS serial NMEA feed, the following are a subset of available messages:

- DTM - Datum being used.
- GGA - Fix information
- GLL - Lat/Lon data
- GSA - Overall Satellite data
- GSV - Detailed Satellite data

- RMC - Recommended minimum data for GPS
- RTE - Route message
- VTG - Vector track an Speed over the Ground

If in the application, the user is only interested in receiving the GGA message, then a *start string* can be set to GGA. In that way, any messages starting with DTM, GLL, GSA or other unwanted messages will be discarded.

Note If a start string is enabled, the device will stay awake until the string is received or until the *max-time* is reached.

In firmware revisions less than 2, serial *start strings* are specified as text, with special characters such as carriage return and line feed being specified by their respective escape sequences. A list of allowable escape sequences is given below:

- \f Form-feed
- \n Newline (Line Feed)
- \r Carriage Return
- \t Horizontal Tab
- \v Vertical Tab
- \\ Backslash

Note Because escape sequences start with a backslash (\), if a capture string contains a backslash, it needs to be escaped and so is represented as a double backslash (\\).

In firmware release 2 and above, serial *start strings* are specified as text, with special characters such as carriage return and line feed being specified by their respective ASCII codes in hexadecimal. A list of example hexadecimal sequences is given below:

- \x0C Form-feed
- \x0A Newline (Line Feed)
- \x0D Carriage Return
- \x09 Horizontal Tab
- \x0B Vertical Tab
- \x08 Backslash

The change to the method used to represent special characters has been made to allow for all ASCII characters to be used, and to allow for hexadecimal data to be captured.

Note In firmware revisions 2 and lower, special characters are specified as escape characters. In revisions 2 and above, special characters are represented by their ASCII representations in hexadecimal.

In some serial protocols, the start of a packet is specified by a preceding period of inactivity on the serial bus. The *Idle Time Before Start* parameter can be used to specify an idle time, which is exceeded will trigger the serial port to start capturing serial data.

Note If the serial port is capturing data and a subsequent idle time occurs, the capture process will restart and captured data will be discarded.

A serial capture *stop string* of up to 10 characters can also be provided. Again using the NMEA example, all NMEA messages end with a carriage return and line feed and so the serial capture *stop strings* in each case will be the same and will be "\r\n" or \x0D\x0A in revision 2 and above firmware. In

most instances, the serial *stop strings* will be the same for all messages.

Note If a *start string* is specified without a *stop string*, or the *stop string* is never encountered, the serial port will capture characters until the *max-time* or *max-chars* is reached, the next measurement interval occurs or 256 characters are received.

An optional serial *request string* can be sent, on each measurement interval, to an external device. The purpose of the *request string* is to request data from an external sensor or system. The *request string* can be a maximum of 10 characters and can be entered as text. Special characters like carriage return and line feed can be inserted using escape sequences or their ASCII representations as described earlier in the chapter.

The UNI-Z1 implements the *MODBUS* communications protocol standard as a master, which enables communication with many slave devices connected to the network. The UNI-Z1 can be configured to periodically request specific data from slave *MODBUS* devices on the network and transmit that data at specified intervals.

Up to fifty *MODBUS* data requests can be configured; these data requests can either be from individual slave devices or multiple requests from the same device. For each of the fifty data reads, the *slave address*, *function* and *register address* need to be specified. The *slave address* will be specified by the manufacturer of the device that is attached to the UNI-Z1; in some cases, slave devices allow their addresses to be configured. The *function* specifies the type of data to be read from the slave device. The UNI-Z1 supports the following types of data reads:

- Disabled - the particular *MODBUS* channel is not used
- Read Coil - a 1 bit data value
- Read Discrete - a 1 bit data value
- Read Holding - a single 16 bit holding register
- Read Input - a 16 bit input register
- Read Holding (32 bits, Little Endian register order) - a 32 bit holding register
- Read Holding (32 bits, Big Endian register order) - a 32 bit holding register
- Read Input (32 bits, Little Endian register order) - a 32 bit input register
- Read Input (32 bits, Little Endian register order) - a 32 bit input register

Endianness is the order or sequence of bytes of digital data in computer storage and will be specified by the sensor that is being connected to the UNI-Z1.

A single *MODBUS* device may have multiple data values that can be read. The *register address* specifies which data the slave device needs to deliver.

In *MODBUS mode*, calibration can be applied so that the registers read by the UNI-Z1 can be scaled to be in the units of what is being measured. For instance, a register that returns 0 to 255 may represent 0% humidity to 100% humidity. The UNI-Z1 can be calibrated to take a number and to convert it to humidity in % and return that as the measured value.

In any system, the sensor and possibly the measured value will be subject to errors that may accumulate to reduce accuracy. In a system that uses the UNI-Z1 to measure fluid volume in a 100 litre tank using a *MODBUS* sensor, the sensor may have offset errors such that with zero liquid in the tank, the UNI-Z1 is showing a small volume. The UNI-Z1 and sensor may also not be perfectly linear in that they may not measure 1 litre in exactly the same way when the tank is empty versus when it is full. The tank itself may also not be perfectly manufactured and may, for instance have walls that are not perfectly straight. All of these errors could add together such that the final system is less accurate than expected. To achieve a more accurate system, a calibration can be performed. In this example, the tank could be calibrated by adding a small amount of liquid, say 10 litres (low Y) and noting the value reported by the UNI-Z1 (low X). Now fill the tank by adding another 99 litres (high y) and note the value being reported by the UNI-Z1 (high X). By filling the high and low X and Y values into the calibration constants associated with *analog mode*, offset and non-linearity errors can be eradicated, resulting in a much more accurate system.

In *MODBUS mode*, *warning* and *alarm* thresholds for can be set for each MODBUS channel. Once enabled, each time a measurement is completed, the returned value will be compared with minimum and maximum *warning* and *alarm* thresholds. If a *warning* or *alarm* level is breached, a message will immediately be transmitted. As long as the *warning* or *alarm* condition persists, messages will be transmitted at the exception-interval rather than the transmit-interval.

Note If calibration has been applied, then the warning and enable thresholds are in the calibrated units.

A full list of serial interface settings is given in the table at the end of the chapter.

9.3 CAN Bus interface

The Senquip UNI-Z1 is equipped with CAN bus that can be used to read data from all kinds of vehicles and sensors. Many sensors, controllers, and electronic devices can be connected to a single CAN network.

In many cases, the protocol that is being used on the CAN bus is known, and so large volumes of understandable data can be extracted from all kinds of vehicles. Common CAN protocols include:

- J1939, the dominating CAN-based protocol for trucks and busses.
- ISO 11783, a J1939 flavor for agricultural tractors.
- ISO 11992, an interface between trucks and trailers.
- NMEA 2000, a protocol based on J1939 for marine use.
- CANopen, provides a standard for industrial machinery commonly used in industrial automation.

The CAN interface on the UNI-Z1 supports Classical CAN. Pins 3 and 6 provide the CAN interface, with pin 6 being CAN High (dominant high) and pin 3 being CAN Low (dominant low).

Pin	Function
3	CAN1 L
6	CAN1 H

In CAN networks, 120Ω termination resistors are installed at each end of the network. In most installations, the required termination will already be present and the internal termination resistor should remain disabled. If the UNI-Z1 is located at the end of a CAN network and termination is required, the internal termination resistor can be enabled in the CAN settings. No external termination resistor is required.

Warning In CAN bus systems, the ground supplied to the Senquip UNI-Z1 must be the same ground as used by the CAN network. High differential voltages between the CAN lines and ground can damage the CAN interface.

9.3.1 Specification

Parameter	Specification
CAN physical layer	High-speed CAN (ISO 11898-2 compatible)
Supported protocols	Classical CAN 2.0A and 2.0B
Maximum bit rate	1Mbit/s
Receiver common mode range	+/-30V
Bus fault protection on CAN High and CAN Low	+/-58V
ESD protection, CAN bus pins, contact discharge	+/-8kV

ESD protection, CAN bus pins, air discharge	+/-15kV
Optional termination resistor	120Ω

9.3.2 Settings

Measurements can be scheduled as a multiple of the base-interval. The fastest possible measurement rate is achieved by setting the *interval* to 1 in which case the CAN network will be sampled on every base interval. To reduce power consumption, the measurement rate can be turned down by increasing the *interval*.

The CAN bus peripheral on Senquip devices supports can bit rates of 125kbit/s, 250kbit/s, 500kbit/s and 1Mbit/s as specified in the *Nominal Baud Rate* field.

Configurable internal 120Ω termination resistors can be enabled.

To ensure minimum intrusion on CAN systems, the CAN peripheral can be set to listen only. In this mode the Senquip device will only receive messages that are acknowledged on the bus by a listening node. Where required, the Senquip device can be made to acknowledge messages by selecting the *TX Enable* option.

The *Capture Time* setting can be used to set a timeout after which the CAN bus peripheral will stop listening, allowing the Senquip device to transmit received messages and return to sleep. *capture-time* can also be used as a mechanism to allow the CAN peripheral to sample the CAN bus for a defined time-period.

A full list of CAN bus settings is given in the table at the end of this chapter.

9.3.3 CAN Filters

Most automotive CAN networks transmit hundreds of different messages, each with a unique identifier. The Senquip device allows you to filter and capture only the messages you need using the *ID Capture List*.

Basic Usage

Enter the CAN IDs you want to capture in *hexadecimal*, separated by commas. For example:

```
18FF20F2, 18FF36F0, 18FF1BF2
```

During each measurement interval, the device listens for the listed messages until either all are received or the *Capture Time* expires.

Capturing Multiple Messages

To capture multiple messages with the same ID, use * followed by the number of each message required:

```
18FF20F2*4, 18FF1BF2*10
```

This captures:

- 4 messages with ID 18FF20F2
- 10 messages with ID 18FF1BF2

To capture all messages of a certain ID received during the interval, use * without a number:

```
18FF1F12*
```

Wildcards and Advanced Filters

- ?? can replace the **Priority** or **Source Address** in a J1939 ID.
For example:

```
??FECA??
```

This matches any J1939 message with a PGN of FECA, regardless of Priority or Source Address.

- # can be placed at the end of the list to match one of any other message not already listed:

```
18FE1451*4, 18FE1256*2, #
```

This captures:

- 4 messages with ID 18FE1451
- 2 messages with ID 18FE1256
- 1 of every other unique ID not already matched

Special Cases

- Leave the list blank to capture one of every message that arrives.
- Use a single * to capture all messages, in the order they arrive.

Warning Capturing all messages may overwhelm the device in high-traffic CAN systems. The number of messages that can be captured in a measurement cycle is internally limited to 128.

9.3.4 Sending CAN Messages

CAN messages can be sent to connected device from within a script. The messages can be sent once, or can be set to repeat at a given time interval. If the device enters sleep or hibernate, repeating messages will be stopped. If the Senquip device is reset, the sending of repeating CAN messages is unaffected. The messages will continue to be sent until a change is applied. For example, if new script is loaded, forcing a reset, the CAN messages will continue to be sent until the new script applies a change. In the case of a malfunction that lasts for more than 30 second, repeating CAN messages will be stopped.

Note To send CAN messages, the *TX Enable* option must be selected.

9.4 Calibration

Calibration can be applied to each measurement so that the value returned by the Senquip UNI-Z1 is in units that are meaningful in the end application. For instance, a fuel level sensor that outputs a voltage between 0 and 5V may represent a level between 0 and 100 litres of diesel. The voltage measurement can be calibrated to convert from Volts to the more meaningful unit of litres.

In any system, the measurement instrument (the Senquip UNI-Z1), the sensor and possibly the measured value will be subject to errors that may accumulate to reduce accuracy. In a system that measures fluid volume in a 100 litre tank using a 4-20mA sensor, offset errors may result in a non-zero or negative reading when the tank is empty. Sensor gain may also not be perfectly linear and so a 1 litre change may be measured differently when the tank is empty versus when it is full. The sensor may report in inches of liquid height where a more meaningful unit may be litres. To achieve an accurate and meaningful measurement, a calibration can be performed.

In this example, the tank could be calibrated by adding a small amount of liquid, say 10 litres at which point the current measured may be 4.1mA. Now add more liquid to take the level to say 80L. The sensor now reads 16.2mA. The calibration would then be filled into the IO setting as shown below:

Low In	4.1	This is the value in mA measured by the Senquip UNI-Z1
Low Out	10	This is the actual value that we would like to report
High In	16.2	This is the value in mA measured by the Senquip UNI-Z1
High Out	80	This is the actual value that we would like to report

Unit	l	The unit to be reported is litres
------	---	-----------------------------------

9.4.1 Unit Names and Symbols

The calibration *Unit* field supports plain text together with a number of commonly used engineering symbols. This allows measurements to be displayed using familiar units such as °C, m³, Ω, μS/cm and N·m.

The following characters are supported:

Letters: a-z, A-Z

Numbers: 0-9

Symbols: /, Ω, ·, μ, Δ, ±, ×, :, °, ², ³, ., %, _ , -

Examples:

Unit	Description
V	Volts
A	Amps
°C	Degrees Celsius
°F	Degrees Fahrenheit
Ω	Ohms
kΩ	Kilohms
m ³	Cubic metres
m ²	Square metres
μS/cm	Microsiemens per centimetre
N·m	Newton metres
kg/m ³	Density
%RH	Relative humidity
L/min	Litres per minute

When entering units on Windows, some special characters can be entered using their **ALT** codes on the numeric keypad.

Character	Windows ALT Code
°	ALT+0176
²	ALT+0178
³	ALT+0179
μ	ALT+0181
±	ALT+0177
×	ALT+0215

The remaining symbols can be copied directly from this guide or inserted using the Windows Character Map (charmap.exe) or the Windows Emoji & Symbols panel (Win + .).

Character	Description
Ω	Ohm
Δ	Uppercase Delta
·	Middle dot

9.5 Warnings and Alarms

For each measurement type, high and low warning and alarm levels can be set. Once enabled, each

time a measurement is completed, the returned value will be compared with low and high *warning* and *alarm* thresholds. If a *warning* or *alarm* level is breached, a message will immediately be transmitted. As long as the *warning* or *alarm* condition persists, messages will be transmitted at the *exception-interval* rather than the *transmit-interval*.

Note If calibration has been applied, then the warning and enable thresholds should be set in the calibrated units.

To set a high level warning or alarm level only, set the low level to a value that is impossible to achieve. For instance to set a high only warning at 50V, set the low warning to -1V which is an unachievable value.

Hysteresis can be specified in increments of the specified unit, to prevent multiple alarms in the presence of electrical noise.

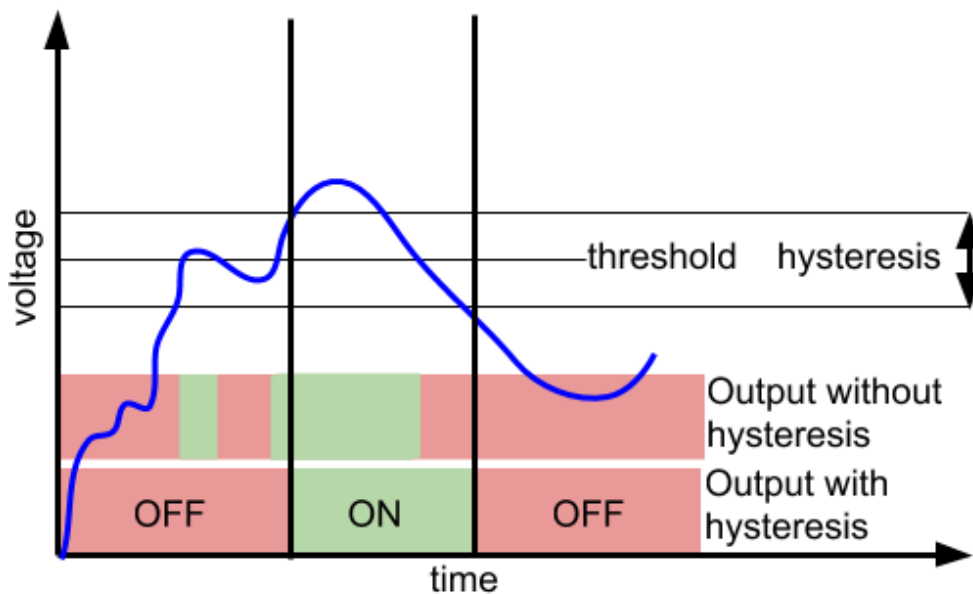


Figure 9.6. Hysteresis

9.6 External Sensor Settings

A full list of settings for external sensors is given in the table below.

Name	Item	Function	Range	Unit	Internal Reference
Input 1					
Name	text	A name for the input that is meaningful to the user.	25 chars		input1.name
Interval	integer	The number of base intervals after which the input is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.	0 to 10000		input1.interval
Mode	preset	Specifies the function of the IN1 terminal. The calibration, warnings and alarms are applied to this mode.			input1.mode
Digital 1					

Digital Threshold	decimal	A threshold against which the input is compared to determine if the input state is ON or OFF.	0 to 30	Volts	input1.digital.threshold
Digital Hysteresis	decimal	Once the input is in a certain state, hysteresis is the amount by which the input has to change before moving to the other state.	0 to 20	Volts	input1.digital.hysteresis
Count Hours	boolean	Counts the number of hours the digital input is ON (above threshold).			input1.digital.count_hours
Digital Change Alert	boolean	Sets whether a change in digital state generates an alert.			input1.digital.alert.enable
Analog 1 Calibration	text	Calibration parameters for Analog 1. Refer to user guide.	30 chars		input1.cal
Unit	text	The unit of measure associated with the calibration. Examples: Litres/min, RPM, Volts			input1.unit
Warning	text	Warning thresholds. Refer to user guide.			input1.warning
Alarm	text	Alarm thresholds. Refer to user guide.			input1.alarm
Alarm/Warning Hysteresis	decimal	Once the input is in a certain state, hysteresis is the amount by which the input has to change before moving to the other state.			input1.hysteresis
Pulse Input					
Pulse Counting	boolean	Enables counting of pulses in addition to frequency measurement.			input1.pulse.enable
Reset Value	integer	The value at which the number of pulses counted on the input is reset to zero.	1 to 200000000	Counts	input1.pulse.reset_value
Pulse Scaling	decimal	Multiplier to convert the pulse count to a useful unit.			input1.pulse.scaling
Pulse Unit	text	The unit of measure associated with the scaled pulse count. Eg: Litres			input1.pulse.unit
Pulse Warning	text	Warning thresholds. Refer to user guide.			input1.pulse.warning
Pulse Alarm	text	Alarm thresholds. Refer to user guide.			input1.pulse.alarm
Input 2					
Name	text	A name for the input that is meaningful to the user.	25 chars		input2.name
Interval	integer	The number of base intervals after which the input is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.	0 to 10000		input2.interval
Mode	preset	Specifies the function of the IN2 terminal. The calibration, warnings and alarms are applied to this mode.			input2.mode
Digital 2					
Digital Threshold	decimal	A threshold against which the input is compared to determine if the input state is ON or OFF.	0 to 30	Volts	input2.digital.threshold

Digital Hysteresis	decimal	Once the input is in a certain state, hysteresis is the amount by which the input has to change before moving to the other state.	0 to 20	Volts	input2.digital.hysteresis
Count Hours	boolean	Counts the number of hours the digital input is ON (above threshold).			input2.digital.count_hours
Digital Change Alert	boolean	Sets whether a change in digital state generates an alert.			input2.digital.alert.enable
Analog 2 Calibration	text	Calibration parameters for Analog 2. Refer to user guide.	30 chars		input2.cal
Unit	text	The unit of measure associated with the calibration. Examples: Litres/min, RPM, Volts			input2.unit
Warning	text	Warning thresholds. Refer to user guide.			input2.warning
Alarm	text	Alarm thresholds. Refer to user guide.			input2.alarm
Alarm/Warning Hysteresis	decimal	Once the input is in a certain state, hysteresis is the amount by which the input has to change before moving to the other state.			input2.hysteresis
Output 1					
Name	text	A name for the input that is meaningful to the user.	25 chars		output1.name
Interval	integer	Does not affect output mode. The number of base intervals at which the input is sampled. Set to 0 to disable. Set to 1 for every base interval.	0 to 10000		output1.interval
Mode	preset	Specifies the function of the OUT1 terminal.			output1.mode
Warnings	boolean	Determines if the output is turned on when a warning is active.			output1.warnings
Alarms	boolean	Determines if the output is turned on when an alarm is active.			output1.alarms
Alerts	boolean	Determines if the output is turned on when an alert is active.			output1.alerts
Hold Time	integer	Sets the time in seconds for which the output is held on after it is triggered. If set to zero, the output remains on while any exceptions are active.		Seconds	output1.hold_time
Digital Change Alert	boolean	If enabled, a change in digital state will generate an alert.			output1.digital.alert.enable
Analog 3 Calibration	text	Calibration parameters for Analog 3. Refer to user guide.	30 chars		output1.cal
Unit	text	The unit of measure associated with the calibration. Examples: Litres/min, RPM, Volts			output1.unit
Warning	text	Warning thresholds. Refer to user guide.			output1.warning
Alarm	text	Alarm thresholds. Refer to user guide.			output1.alarm

Alarm/Warning Hysteresis	decimal	Once the input is in a certain state, hysteresis is the amount by which the input has to change before moving to the other state.			output1.hysteresis
Thermocouple 1					
Name	text	A name for the input that is meaningful to the user.	25 chars		tc1.name
Interval	integer	The number of base intervals after which the thermocouple is measured and events are checked. A value of 1 means that the input is collected every base interval. Set to 0 to disable.	0 to 10000		tc1.interval
Hysteresis	decimal	The amount by which the measured value has to drop below the threshold to re-enable the event.	-1000 to 1000	°C	tc1.hysteresis
Type	text	Determines the type of thermocouple connected. Valid values are: K, J, T, N, S, E, B and R	1 chars		tc1.type
Warning	text	Warning thresholds. Refer to user guide.	-1000 to 1000	°C	tc1.warning
Alarm	text	Alarm thresholds. Refer to user guide.	-1000 to 1000	°C	tc1.alarm
CAN 1					
Name	text	A name that is meaningful to the user.	25 chars		can1.name
Interval	integer	The number of base intervals after which the CAN module is turned on. Set to 0 to disable.	0 to 10000		can1.interval
Nominal Baud Rate	integer	Baud rate for CAN communication. Supported values are: 125, 250, 500, 1000		kbit/s	can1.nominal_baud
Capture Time	integer	The device will capture matching messages for this length of time.		Seconds	can1.capture_time
TX Enable	boolean	Allows the device to transmit and acknowledge messages on the CAN bus.			can1.tx_enable
ID Capture List	text	List of IDs to be captured in HEX format, separated by a comma eg: 18FEE60A. Leave blank to capture all.	200 chars		can1.id_list
Send Raw Data	boolean	If ticked, all captured messages will be added to the data message.			
CAN 2					
Name	text	A name that is meaningful to the user.	25 chars		can2.name
Interval	integer	The number of base intervals after which the CAN module is turned on. Set to 0 to disable.	0 to 10000		can2.interval
Nominal Baud Rate	integer	Baud rate for CAN communication. Supported values are: 125, 250, 500, 1000		kbit/s	can2.nominal_baud
Capture Time	integer	The device will capture matching messages for this length of time.		Seconds	can2.capture_time
					can2.tx_enable

TX Enable	boolean	Allows the device to transmit and acknowledge messages on the CAN bus.	200 chars		can2.id_list
ID Capture List	text	List of IDs to be captured in HEX format, separated by a comma eg: 18FEE60A. Leave blank to capture all.			
Send Raw Data	boolean	If ticked, all captured messages will be added to the data message.			
Current Loop 1			25 chars		current1.name
Name	text	A name for the input that is meaningful to the user.	0 to 10000		current1.interval
Interval	integer	The number of base intervals after which the input is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.			current1.mode
Mode	preset	Specifies the function of the SRC1 terminal.			current1.always_on
Always On	boolean	Determines if Switched Power is to be enabled permanently.	0 to 3600	Seconds	current1.start_time
Start Time	decimal	Time in seconds that the output is turned on before measurements are taken. Allows an external device to stabilise.			current1.digital.alert.enable
Digital Change Alert	boolean	Sets whether a change in digital state generates an alert. (Digital Mode Only)	30 chars		current1.cal
Current 1 Calibration	text	Calibration parameters for Current 1. Refer to user guide.			current1.unit
Unit	text	The unit of measure associated with the calibration. Examples: Percent, Pascals, Meters			current1.warning
Warning	text	Warning thresholds. Refer to user guide.			current1.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			current1.hysteresis
Alarm/Warning Hysteresis	decimal	The amount by which the calibrated current value has to drop below the threshold to re-enable the event.			
Current Loop 2			25 chars		current2.name
Name	text	A name for the input that is meaningful to the user.	0 to 10000		current2.interval
Interval	integer	The number of base intervals after which the input is sampled. A value of 1 means that the input is collected every base interval. Set to 0 to disable.			current2.mode
Mode	preset	Specifies the function of the SRC2 terminal.			current2.always_on
Always On	boolean	Determines if Switched Power is to be enabled permanently.	0 to 3600	Seconds	current2.start_time
Start Time	decimal	Time in seconds that the output is turned on before measurements are taken. Allows an external device to stabilise.			current2.digital.alert.enable

Digital Change Alert	boolean	Sets whether a change in digital state generates an alert. (Digital Mode Only)	30 chars		current2.cal
Current 2 Calibration	text	Calibration parameters for Current 2. Refer to user guide.			current2.unit
Unit	text	The unit of measure associated with the calibration. Examples: Percent, Pascals, Meters			current2.warning
Warning	text	Warning thresholds. Refer to user guide.			current2.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			current2.hysteresis
Alarm/Warning Hysteresis	decimal	The amount by which the calibrated current value has to drop below the threshold to re-enable the event.			
Serial 1			25 chars		serial1.name
Name	text	A name for the input that is meaningful to the user.	0 to 10000		serial1.interval
Interval	integer	The number of base intervals after which the serial port is turned on. Set to 0 to disable.			serial1.type
Type	preset	The electrical interface type.			serial1.termination
Termination Resistor	boolean	This parameter enables the integrated termination resistor.			serial1.mode
Mode	preset	Describes how the serial port is to be handled. CAPTURE: serial data is captured between start and end characters. MODBUS: serial data is treated according to MODBUS RTU standard			serial1.baud
Baud Rate	integer	Baud rate for serial communication. Common values are: 4800, 9600, 19200, 38400, 57600, 115200			serial1.settings
Settings	text	A string describing the number of bytes: 7,8,9. Parity type: N(none), E(even), O(odd). Number of stop bits: 1 or 2. Typically: 8N1			
Capture			32 chars		serial1.capture.start
Start String	text	The serial port starts reading data when it detects these characters. Example: \$GPGGA, serial data will be ignored until \$GPGGA is received after which data will be captured. If nothing is specified, the serial port will capture all data until the timeout period is reached.	0 to 60000	Milliseconds	serial1.capture.start_idle_time
Idle Time Before Start	integer	For a valid start condition, there must be this amount of idle time before receiving serial data. Additionally, the captured data will restarted if the serial port is idle for this time. Set to 0 to disable.	32 chars		serial1.capture.end

End String	text	Once capturing, if these characters are received, the serial port will stop capturing and will return to sleep. For binary data or escape sequences refer to the User Guide.	32 chars		serial1.capture.request
Request String	text	This string will be sent when the serial port is first turned on. Use this function to request data from a remote module.		Seconds	serial1.capture.maxtime
Max Time	integer	The device will wait this length of time for a valid capture.			serial1.capture.maxchars
Max Chars	integer	Maximum number of characters to be captured before the serial port goes back to sleep.			serial1.capture.alert
Alert on Capture	boolean	If checked an alert will be raised on any successful serial capture.			
MODBUS RTU			0 to 10	Seconds	serial1.modbus.timeout
Slave Timeout	decimal	How long to wait for a response from each slave device.			
MODBUS 1			25 chars		mod1.name
Modbus 1 Name	text	A meaningful name for Modbus Channel 1.	18 chars		mod1.settings
Modbus 1 Settings	text	Settings for Modbus Channel 1. Refer to user guide.	30 chars		mod1.cal
Modbus 1 Calibration	text	Calibration paramters for Modbus Channel 1. Refer to user guide.			mod1.unit
Modbus 1 Unit	text	The unit of measure associated with the calibration. Examples: Percent, L/hr, Meters			mod1.warning
Warning	text	Warning thresholds. Refer to user guide.			mod1.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			
MODBUS 2			25 chars		mod2.name
Modbus 2 Name	text	A meaningful name for Modbus Channel 2.	18 chars		mod2.settings
Modbus 2 Settings	text	Settings for Modbus Channel 2. Refer to user guide.	30 chars		mod2.cal
Modbus 2 Calibration	text	Calibration paramters for Modbus Channel 2. Refer to user guide.			mod2.unit
Modbus 2 Unit	text	The unit of measure associated with the calibration. Examples: Percent, L/hr, Meters			mod2.warning
Warning	text	Warning thresholds. Refer to user guide.			mod2.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			
MODBUS 3			25 chars		mod3.name
Modbus 3 Name	text	A meaningful name for Modbus Channel 3.	18 chars		mod3.settings

Modbus 3 Settings	text	Settings for Modbus Channel 3. Refer to user guide.	30 chars		mod3.cal
Modbus 3 Calibration	text	Calibration paramters for Modbus Channel 3. Refer to user guide.			mod3.unit
Modbus 3 Unit	text	The unit of measure associated with the calibration. Examples: Percent, L/hr, Meters			mod3.warning
Warning	text	Warning thresholds. Refer to user guide.			mod3.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			
MODBUS 4			25 chars		mod4.name
Modbus 4 Name	text	A meaningful name for Modbus Channel 4.	18 chars		mod4.settings
Modbus 4 Settings	text	Settings for Modbus Channel 4. Refer to user guide.	30 chars		mod4.cal
Modbus 4 Calibration	text	Calibration paramters for Modbus Channel 4. Refer to user guide.			mod4.unit
Modbus 4 Unit	text	The unit of measure associated with the calibration. Examples: Percent, L/hr, Meters			mod4.warning
Warning	text	Warning thresholds. Refer to user guide.			mod4.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			
MODBUS 5			25 chars		mod5.name
Modbus 5 Name	text	A meaningful name for Modbus Channel 5.	18 chars		mod5.settings
Modbus 5 Settings	text	Settings for Modbus Channel 5. Refer to user guide.	30 chars		mod5.cal
Modbus 5 Calibration	text	Calibration paramters for Modbus Channel 5. Refer to user guide.			mod5.unit
Modbus 5 Unit	text	The unit of measure associated with the calibration. Examples: Percent, L/hr, Meters			mod5.warning
Warning	text	Warning thresholds. Refer to user guide.			mod5.alarm
Alarm	text	Alarm thresholds. Refer to user guide.			
MODBUS 6			18 chars		mod6.settings
Modbus 6 Settings	text	Settings for Modbus Channel 6. Refer to user guide.	30 chars		mod6.cal
Modbus 6 Calibration	text	Calibration paramters for Modbus Channel 6. Refer to user guide.			
MODBUS 7			18 chars		mod7.settings
Modbus 7 Settings	text	Settings for Modbus Channel 7. Refer to user guide.	30 chars		mod7.cal
Modbus 7 Calibration	text	Calibration paramters for Modbus Channel 7. Refer to user guide.			
MODBUS 8			18 chars		mod8.settings

Modbus 8 Settings	text	Settings for Modbus Channel 8. Refer to user guide.	30 chars		mod8.cal
Modbus 8 Calibration	text	Calibration paramters for Modbus Channel 8. Refer to user guide.			
MODBUS 9			18 chars		mod9.settings
Modbus 9 Settings	text	Settings for Modbus Channel 9. Refer to user guide.	30 chars		mod9.cal
Modbus 9 Calibration	text	Calibration paramters for Modbus Channel 9. Refer to user guide.			
MODBUS 10			18 chars		mod10.settings
Modbus 10 Settings	text	Settings for Modbus Channel 10. Refer to user guide.	30 chars		mod10.cal
Modbus 10 Calibration	text	Calibration paramters for Modbus Channel 10. Refer to user guide.			

Scripting

Senquip devices have the ability to run user written scripts, allowing extra flexibility. The scripting language is called mJS and is essentially a restricted JavaScript engine.

Scripting on Senquip devices allows:

- Decoding and parsing of messages from serial and CAN-bus devices
- Mathematical manipulation of measured data
- Controlling connected devices
- Creating complex alerts that may be dependent on more than one variable
- Customisation of data payloads to be compatible with third party dashboards

Scripts can be executed in response to a measurement cycle completing, a trigger button being pressed, or based on a recurring timer function.

For more information about writing JavaScript for a Senquip device, please see the [Senquip Scripting Guide](#).

10.1 Risks

Warning The scripting environment is a powerful tool. If incorrectly used the scripting functions may cause the device to malfunction, or even permanently brick the device.

- The mJS scripting environment provides low level access to the device's memory and CPU. Running a script on the device is not without risk, some of which include:
- Permanent filesystem damage rendering the device unable to boot.
- Malfunction of other functions, such as regular reporting of data to the portal.
- Memory corruption, causing incorrect reporting of data.
- Memory leaks, which may present intermittently or after a period of time.
- Loss of remote control over the device, if your Portal account is compromised.

A good understanding of the environment, language and best practices will help avoid or mitigate these risks.

10.2 Access

Scripts can be written and securely downloaded to the device from the Senquip Portal.

Note You must have ADMIN permissions for a device in order to be able to write scripts.

You can access the scripting page by pressing the scripting icon on the device dashboard.

10.3 Writing and deploying a script

The scripting page on the Senquip Portal allows scripts to be written and downloaded, and custom variables, custom settings, and triggers to be created.

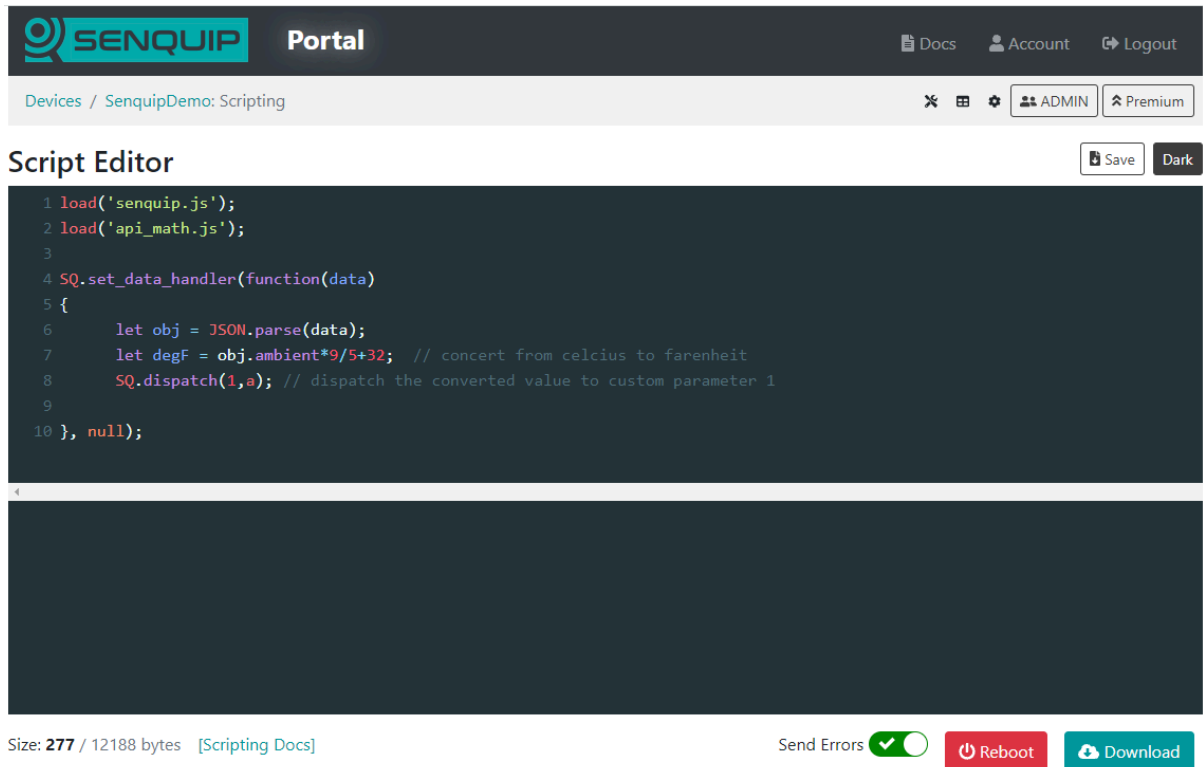


Figure 10.1. Senquip scripting page

Once written, the user can deploy the script to a remote device by pressing the download button and then the reboot button. To enable error reporting, enable the *Send Errors* option. If the script terminates unexpectedly, a message will be sent with a description of the reason that the script failed to complete execution.

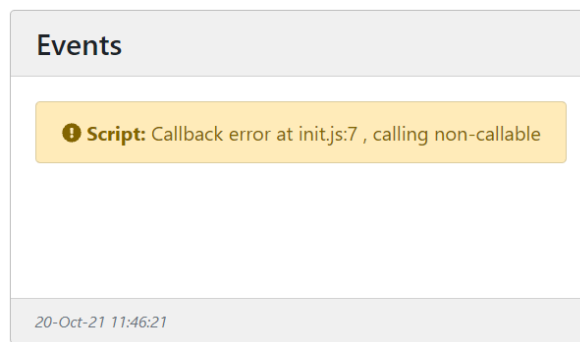


Figure 10.2. Feedback on unsuccessful script

Scripts can be saved to a file using the *Save* button on the scripting page. It is recommended that all scripts are backed up to a secondary storage medium.

Note Remember to backup your scripts.

Network Connection

The Senquip UNI-Z1 can communicate with the Senquip Portal or a remote server using Wi-Fi, cellular networks, and soon, emerging satellite networks. Connectivity is provided using LTE Cat-1 bis, enabling global deployment through a single hardware SKU.

The UNI-Z1 is equipped with a Direct-to-Cell (D2C) capable modem variant designed to support emerging satellite communication services as compatible networks become available.

11.1 Wi-Fi specification

Wi-Fi on the Senquip UNI-Z1 is used to transmit data, to allow settings to be remotely updated, to allow in-field software updates and also to enable setup via an integrated web-server that can be accessed in setup mode via a mobile phone or other Wi-Fi device.

The Wi-Fi implementation supports Wi-Fi 802.11 b/g/n. The Wi-Fi antenna is integrated into the Senquip UNI-Z1. In typical applications, the range achievable with Wi-Fi is 500m.

11.2 Cellular specification

In the absense of Wi-Fi, the UNI-Z1 will attempt to connect using a local cellular network. Senquip devices use cellular networks to transmit data, to allow settings to be remotely updated, and to allow in-field software updates.

The UNI-Z1 implements 4G LTE, and is designed for global operation using Cat 1 bis in the following bands:

Device	Technology	Bands
UNI-Z1-S	CAT-1 bis	B1/B2/B3/B4/B5/B7/B8/B12/B13/B18/B19/B20/B25/B26/B28/B34/B38/B39/B40/B41/B66

LTE Cat 1 bis provides an excellent balance between coverage, performance, power consumption, and cost while maintaining global deployment capability through a single hardware platform.

Cellular antennas are integrated within the UNI-Z1 enclosure, eliminating external antenna connections and improving resistance to vibration, weather, and mechanical damage.

11.3 Satellite Connectivity

The UNI-Z1 is equipped with a Direct-to-Cell (D2C) capable modem variant and is designed to support emerging satellite-to-mobile communication services.

Direct-to-Cell technology allows compatible cellular devices to communicate directly with low Earth

orbit satellites using standard cellular radio technology. As satellite operators continue to deploy D2C services, coverage may become available in locations beyond the reach of terrestrial cellular infrastructure.

Note Direct-to-Cell services are currently being deployed globally and availability varies by country, network operator, and satellite provider.

Note Satellite connectivity depends on service availability, regulatory approvals, modem firmware, SIM compatibility, network operator support, antenna performance, and installation conditions. Availability and performance cannot be guaranteed in all deployments.

11.4 Network Interfaces and Services

The Senquip device provides the following network interfaces:

Interface	Purpose
Cellular	Secure communication with the Senquip Cloud and customer-configured endpoints.
Wi-Fi	Secure communication with the Senquip Cloud and customer-configured endpoints.
Bluetooth Low Energy (BLE)	Local commissioning and configuration using the Senquip Connect App.
Wi-Fi Access Point	Local commissioning and configuration in setup mode.

Network services exposed by the device include:

Service	Availability
Embedded Webserver	Available in setup mode and protected by the device setup password.
BLE Configuration Service	Available in setup mode and protected by the device setup password.
MQTT Client	Outbound communication to authorised cloud or customer-configured endpoints.
HTTP/HTTPS Client	Outbound communication to authorised cloud or customer-configured endpoints.

The device does not provide SSH, Telnet, FTP, remote shell access, or support for arbitrary user-installed network services.

All Senquip Cloud communications use authenticated and encrypted communications. Customer-configured endpoints and services are the responsibility of the endpoint owner.

11.5 Network Requirements

When connected to a Wi-Fi network, the Senquip UNI-Z1 may need to establish secure outbound connections to Senquip services. If your network uses a firewall, the following outbound ports should be permitted.

Function	Port	Description
NTP Time	123	Synchronises the device clock. Accurate time is required for time-stamping measurements and for security functions such as certificate validation.
MQTT (Senquip Portal)	8883	Secure communication between the device and the Senquip Portal.

HTTPS (OTA Updates)	443	Used for Over-the-Air (OTA) firmware updates and other secure web services.
---------------------	-----	---

Note These ports are used for outbound connections only. No inbound ports need to be opened on your firewall.

Note If custom endpoints are enabled, additional ports may need to be opened.

The following Wi-Fi authentication modes are supported:

- WPA
- WPA2
- WPA3

11.6 Connecting to a Wi-Fi or LTE Network with the Senquip Connect App

The Senquip Connect App is a mobile application that allows users to connect to nearby Senquip devices using Bluetooth to configure networks and for data viewing. The app is available for both Android and iOS devices running recent firmware. See the Senquip Device Firmware Changelist for more information on compatible firmware versions.

Network configuration via Bluetooth is available when the Senquip device is in setup mode. To enter setup mode, press the setup button on the device. The green light will start to flash. Open the Senquip Connect App and scan for available devices. Devices in setup mode will allow connection for the purpose of network configuration. Press connect and enter the device setup password.

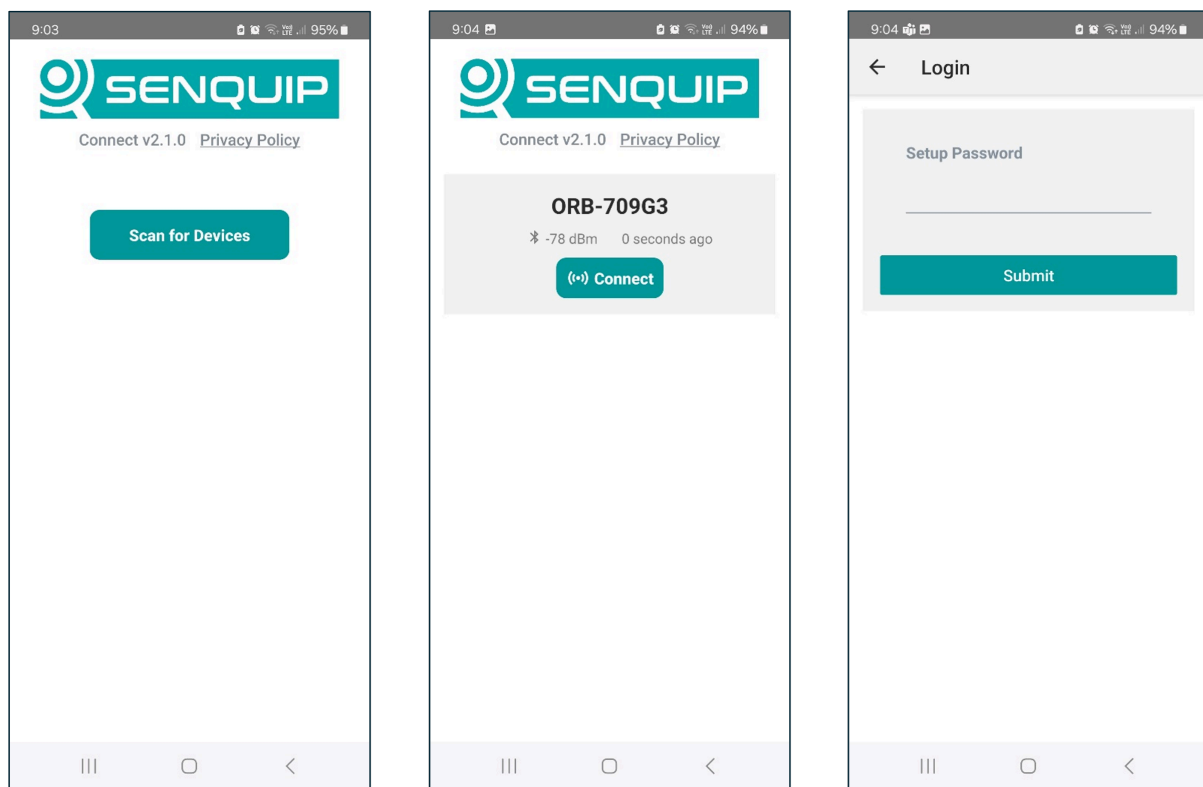


Figure 11.1. Scanning for Devices

Once connected to a device, select *Configure WiFi* or *Configure Cellular / LTE*.

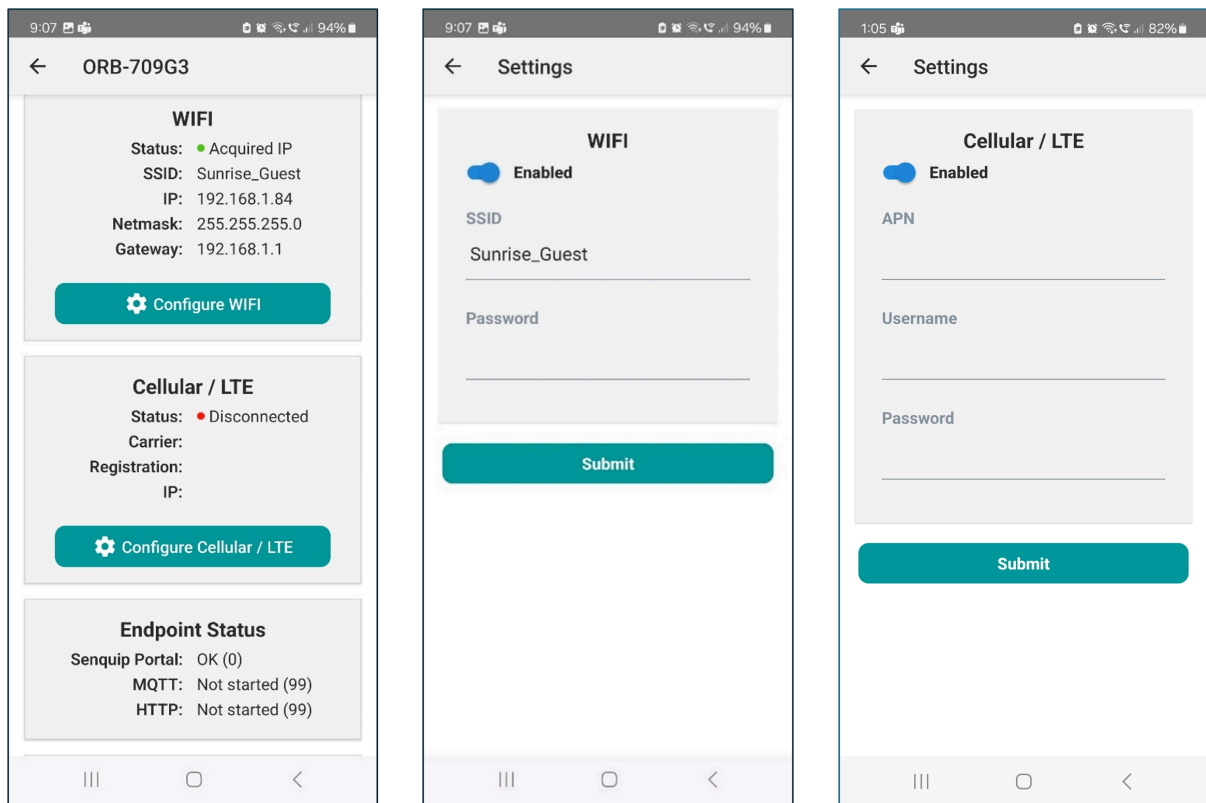


Figure 11.2. Configuring the Network

For Wi-Fi networks, the chosen SSID and password need to be entered. Further advanced Wi-Fi settings are available when using the embedded webserver or Senquip Portal for configuration.

For LTE networks, Auto APN can be enabled in which case the device will attempt to find a suitable APN for the network. Alternatively the APN for the network should be entered. In rare cases, a username and password are required for the SIM.

Press *Submit* to send the settings to the device. The device will save the settings and will reboot back into setup mode. To exit setup mode, press reset on the device. Continue device configuration using the Senquip Portal.

11.7 Connecting to a Wi-Fi Network with the Embedded Webserver

Once in setup mode, use the Network page to connect the Senquip UNI-Z1 to a Wi-Fi network.

On the Network page, press the Scan for Wi-Fi Networks button. After a few seconds, a list of SSIDs for visible Wi-Fi networks will be shown. Select the Wi-Fi network to which you would like to connect by selecting the SSID from the list. The SSID will automatically be copied to the Wi-Fi SSID field and you will be prompted for the network password. After entering the password, press Save Settings. You will be prompted to restart the device; settings will only be applied after a restart. To continue with setup, press *CANCEL* or to restart and apply your settings, press *OK*.

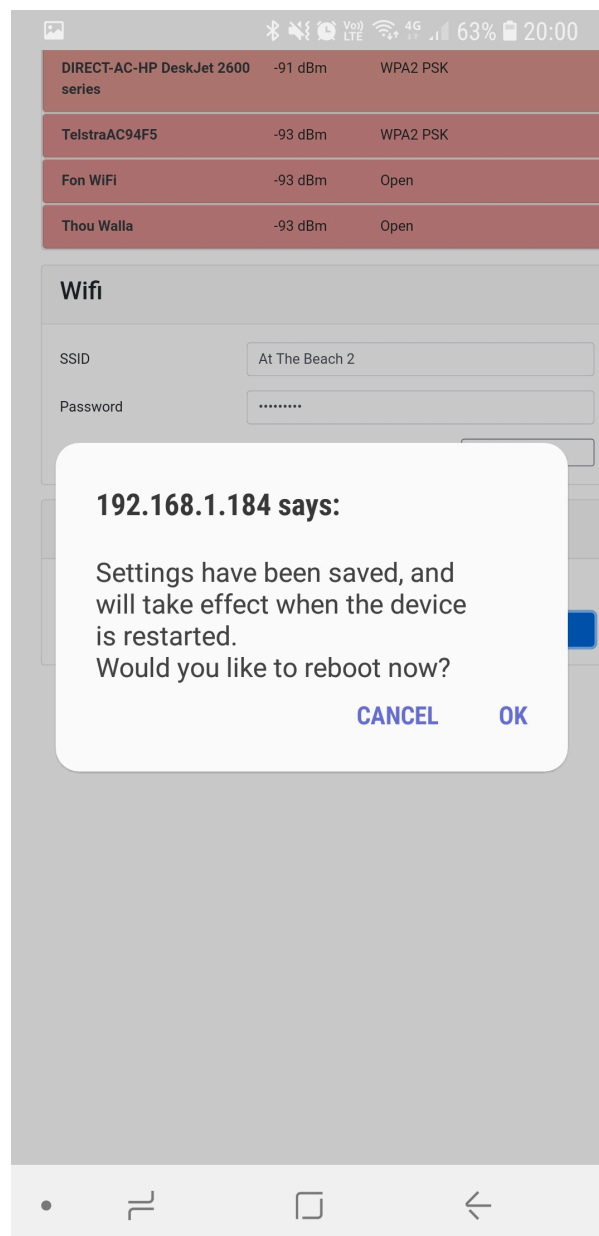


Figure 11.3. Save changes and reboot

After a reboot, the Senquip UNI-Z1 will attempt to connect to the specified Wi-Fi network. You can check if the Senquip UNI-Z1 has successfully connected to the chosen network by placing the device in setup mode and returning to the Network page. At the top of the page, the current network status will be shown. Note the IP address that your Wi-Fi modem has allocated to the Senquip UNI-Z1; you can use this address to access the device directly on your WiFi network.

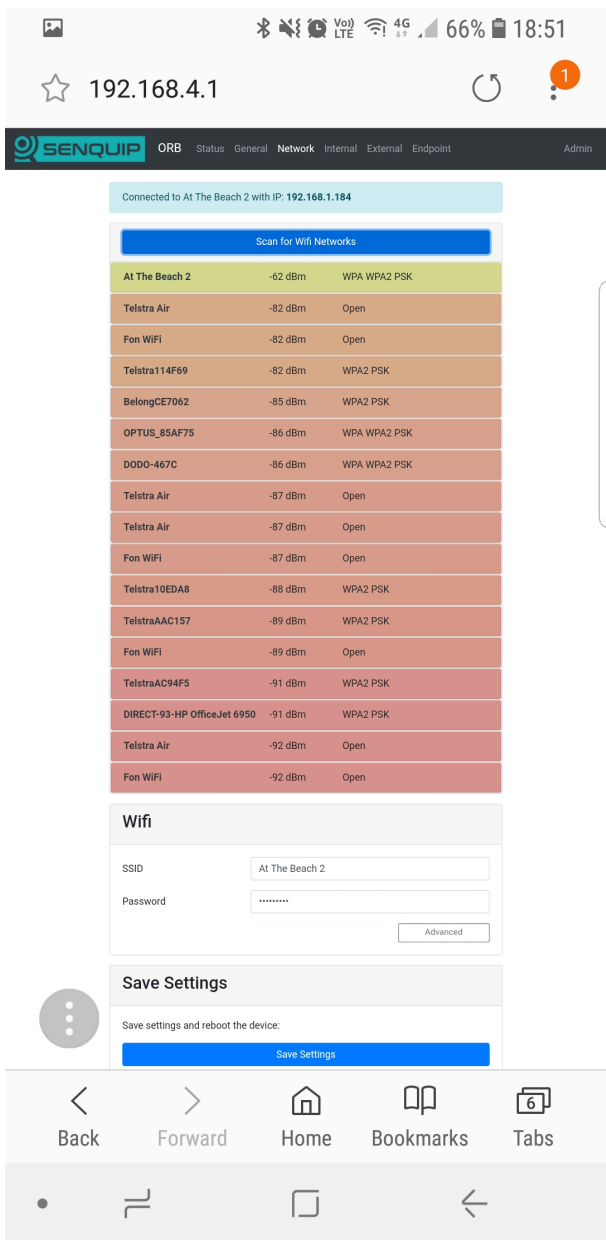


Figure 11.4. Note the IP address on your network

Further Wi-Fi settings are available by selecting the *Advanced* option. Once selected, a static IP address, netmask, gateway and DNS server can be specified.

The integrated web-server is normally only active in setup mode; it can however be made to be always on by setting the web setting to ON. This may be an advantage in systems where permanent power is available and the user wants to be able to make remote changes directly on the Senquip UNI-Z1 without having to access the Senquip Portal. Keeping the web-server active will require that the device remain awake at all times but does mean that the user can make instant changes to settings and see the latest measured data.

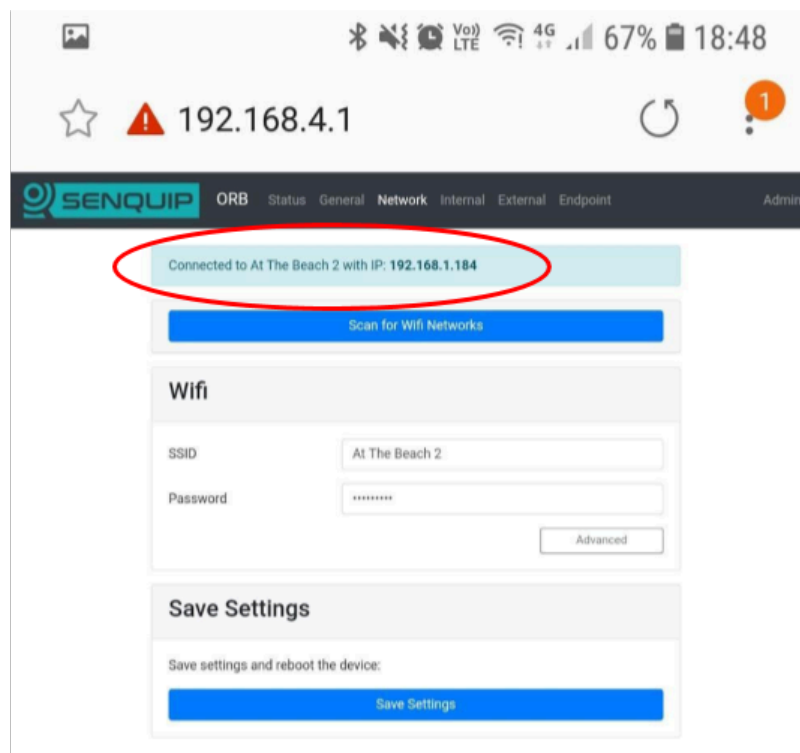


Figure 11.5. Access via local IP

11.7.1 Wi-Fi settings

A full list of Wi-Fi settings is given in the table at the end of the chapter.

11.8 Connecting to an LTE Network with the Embedded Webserver

Once in setup mode, use the Network page to connect the Senquip UNI-Z1 to a mobile network.

In most cases only an APN will be required to establish a 4G LTE connection. Some service providers will require a username and password and some SIM cards will require a pin. If these are not needed, leave them blank.

For CAT-1 devices, an additional *Connection Mode* setting is available. This setting allows the selection of 4G or 2G, 3G, 4G mobile technology. 4G offers higher bandwidth and is recommended unless there are initial connection issues.

A *Roaming* option is available for SIM cards that offer connection to networks other than SIM card home network.

RSSI	Signal Strength	Meaning
0	-113dBm or less	Signal strength poor
1	-111dBm	Signal strength poor
2...30	-109... -53dBm	Medium signal strength
31	-51dBm or greater	Signal strength excellent

11.8.1 4G LTE settings

A full list of 4G LTE settings is given in the table at the end of the chapter.

11.9 Network settings

A full list of network settings is given in the table below.

Name	Item	Function	Internal Reference
Wi-Fi			
Wifi	boolean	Connect to existing Wifi connection specified below.	wifi.sta.enable
SSID	text	Wifi SSID to connect to.	wifi.sta.ssid
Password	password	Wifi password to use for connection.	wifi.sta.pass
Static IP Address	text	Leave blank if assigned by DHCP.	wifi.sta.ip
Static Netmask	text	Leave blank if assigned by DHCP.	wifi.sta.netmask
Static Gateway	text	Leave blank if assigned by DHCP.	wifi.sta.gw
DNS Server	text	Leave blank if assigned by DHCP.	wifi.sta.nameserver
GSM			
GSM	boolean	Enable the GSM connection.	gsm.enable
APN	text	Access Point Name of mobile operator	gsm.apn
Username	text	Username for data connection. Leave blank if not specified	gsm.user
Password	text	Password for data connection. Leave blank if not specified	gsm.pass
Connection Mode	preset	Select mobile technology (CAT-1 devices only)	gsm.scan_mode
Roaming	boolean	Enable network roaming	gsm.roaming

Endpoint Setup

When connected via Wi-Fi or 4G LTE, data measured by a Senquip UNI-Z1 can be sent to the Senquip Portal or a remote server or SCADA system, using UDP, HTTP, HTTPS, MQTT and MQTTS. The endpoint settings allow for configuration of the end server detail and the protocol used to communicate with that server.

12.1 Data security

Devices that connect to company networks and the internet need to be properly secured to mitigate risks and protect organisations from malicious cyber-attacks. Senquip takes the challenge of cyber-security seriously and utilises public-key-infrastructure as a part of their security solution to create a unique, trusted and protected identity for every Senquip device.

Public Key Infrastructure certificates are an important part of developing a complete security solution. By authenticating devices, encrypting confidential data, and maintaining data and system integrity, certificates establish online trust and reliable security.

Authentication: Certificates for devices validate identities to make sure only authorized users, messages, or other types of servers have access to the device.

Encryption: All data stored on the device is encrypted at rest using AES-256. All communication with the Senquip Portal is secured and encrypted using client certificates and Transport Layer Security (TLS).

Integrity: Certificates make sure that any messages or data transferred to and from Senquip devices are not altered.

Each Senquip device is pre-loaded with a unique client certificate, allowing for immediate, out-of-the box, secure communication with the Senquip Portal. Users can then load additional certificates to allow secure communications with other servers, using the encrypted link from the Senquip Portal.

Note For volume applications, certificates can be loaded programmatically via the Senquip Portal Cloud API.

12.2 Data format

Data that is transmitted by the Senquip UNI-Z1 to a remote server is formatted in [JSON](#) format. JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write and it is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

JSON is built on two structures:

- A collection of name/value pairs. In various languages, this is realized as an object, record, struct, dictionary, hash table, keyed list, or associative array.
- An ordered list of values. In most languages, this is realized as an array, vector, list, or sequence.

An example data JSON packet as sent by a Senquip UNI-Z1 is shown below:

```
{
  "deviceid": "4299A5340",
  "humidity": 70.51,
  "vlipo": 4.13,
  "vbat": 2.17,
  "vin": 20.09,
  "analog1": 4.08,
  "digital2": 0,
  "roll": 37.57,
  "pitch": -89.28,
  "angle": 37.57,
  "pressure": 100.4,
  "ambient": 30.4,
  "alarms": {
    "pitch": [
      "Low"
    ],
    "tc1": [
      "Out of Range"
    ]
  },
  "ts": 1544665316.3,
  "tsformat": "13/12/2018 01:41:56"
}
```

Figure 12.1. Example JSON data packet

Users of the Senquip Portal do not need to understand the data format; data can be viewed on the Senquip Portal numerically or graphically or can be downloaded in spreadsheet format.

For users who are sending data to third party servers that require data in a format other than JSON, arbitrary data formats can be scripted on the Senquip device. Application notes are provided that detail the scripting of custom data packet formats for connection to common third party platforms. Further information on scripting for Senquip devices can be found in the [Senquip Scripting Guide](#).

12.3 Data Buffer

When a Senquip device is unable to establish a network connection (Wi-Fi or cellular), if the *Offline Buffer* option is enabled, it will store outgoing data for later transmission. If Offline Buffering is disabled, unsent data is discarded once transmission retries are exhausted.

12.3.1 Buffer Capacity

The available internal data buffer size depends on the firmware version:

- SFW003 firmware: up to 10 MB

Buffered data is stored in internal flash memory. If the buffer becomes full, the device stops logging new data until space becomes available.

When connectivity is restored, buffered data is transmitted automatically, with the most recently stored data sent first.

12.3.2 Normal Message Handling

At each base interval, when new data is generated, the following process occurs:

1. The data packet is placed on a queue for transmission to the Senquip Portal via MQTT.
2. The same packet is also placed on a queue for transmission to any enabled custom endpoints.
3. If the Senquip Portal confirms receipt of the packet, the packet is marked as complete and is discarded.
4. If the Senquip Portal does not confirm receipt after several retries, and the *Offline Buffer* is enabled, the packet is written to the internal data buffer as a file.

Note If a packet is successfully received by the Senquip Portal but fails to reach a custom endpoint, it is not buffered, as successful Portal delivery marks the message as complete.

12.3.3 Buffered Data Transmission

While data is buffered, the device continues attempting to reconnect to:

- The Senquip Portal
- Any configured custom endpoints

Once connectivity is restored:

1. Buffered messages are read from the internal filesystem.
2. Each message is then queued for transmission to the Senquip Portal and any enabled custom endpoints.
3. If the Senquip Portal confirms receipt, the message is marked as sent and removed from the buffer, regardless of whether delivery to a custom endpoint succeeds.

The Senquip Portal therefore acts as the authoritative confirmation point for message delivery.

12.3.4 Operation Without Portal Transmission

If *Send Data to Senquip Portal* is disabled:

- The device waits until it is connected to the configured custom MQTT endpoint.
- Buffered messages are transmitted to the custom endpoint only.
- Once a buffered message is placed on the outgoing queue, it is deleted from the internal buffer.

In this mode, the Senquip Portal does not participate in message acknowledgement or buffering decisions.

12.4 UDP

Data can be sent via raw UDP to a fixed IP address and port. This method is only suitable for a local network Wi-Fi connection as the data is not encrypted and there is no authentication. Raw UDP also provides no acknowledgment that data was received.

12.5 HTTP

An HTTP session is a sequence of network request-response transactions. The Senquip UNI-Z1 initiates a request by establishing a HTTP connection on a particular port on a client server (typically port 80, occasionally port 8080).

12.6 HTTPS

HTTPS is the secure version of HTTP and is sometimes referred to HTTP over TLS. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. Wherever possible, HTTPS should be used as an alternative to HTTP.

HTTPS requires that the [certificate-authority](#) (CA) certificate of the destination be loaded onto the Senquip UNI-Z1.

The main drawback of HTTPS is that it not a persistent connection and requires **a new connection to be established for each data packet sent**. This can lead to increased power consumption and reduced battery life. It can also overload the device when the transmit interval is short (less than 30 seconds) as the device may not have time to establish a new connection before the next data packet is generated. MQTTS is the preferred secure protocol for use with the Senquip UNI-Z1 as it offers a low power and persistent connection.

Note For volume applications, certificates can be loaded programmatically via the Senquip Portal Cloud API.

12.7 MQTT

MQTT is a secure machine-to-machine (M2M) Internet of Things connectivity protocol specifically designed for low data-rate applications and is perfect for implementation on Senquip devices. MQTT is the protocol used when the Senquip UNI-Z1 communicates with the Senquip Portal and is also supported by many open source IoT platforms such as Thingsboard.

Senquip devices implement MQTT Version 3.1.1 client functionality, and work with all popular MQTT server implementations such as AWS IoT, Microsoft Azure, HiveMQ and Mosquitto.

Note Senquip devices can maintain concurrent MQTT connections to the Senquip portal and a customer server or SCADA system.

Consideration must be given to data security on open networks. In applications where data security is critical, the use of MQTTS with encryption and authentication should be considered.

12.8 MQTT over TLS

MQTT over TLS (MQTTS) adds enhanced security as all data is encrypted and secured with SSL

certificates. Most business grade IoT platforms such as AWS (Amazon Web Services) offer MQTTS.

MQTTs is recommended by Senquip as the preferred protocol for use with the Senquip UNI-Z1 as it offers a low power, reliable, secure connection. The Senquip UNI-Z1 is pre-loaded with certificates allowing secure communication with the Senquip Portal.

Note For volume applications, certificates can be loaded programmatically via the Senquip Portal Cloud API.

12.9 Settings

UDP, TCP and HTTP connections require an IP address of the host server and a port on which the host server is listening. Secure protocols like MQTTS and HTTPS require certificates to be loaded on the device. The Senquip UNI-Z1 is pre-loaded with certificates that allow connection to the Senquip Portal that is hosted on Amazon Web Services. Certificates for customer servers can be uploaded using the Senquip Portal.

All messages are time-stamped using the UNIX time standard. Unix time (also known as POSIX time or UNIX Epoch time) is a system for describing a point in time, defined as the number of seconds that have elapsed since 00:00:00, Thursday, 1 January 1970. Every day is treated as if it contains exactly 86400 seconds, so leap seconds are not applied. UNIX time is used to timestamp messages as it is used widely in Unix-like and many other operating systems and file formats.

The Senquip UNI-Z1 automatically updates time by accessing a Network Time Protocol (NTP) server. By default the device will get the time via NTP from pool.ntp.org, on whatever network connection is available (Wi-Fi or 4G LTE). It does this if the time is not valid, for instance, after a reset, and then every 12 hours thereafter. Between updates, time is kept with a high precision real-time clock that is powered by the internal LiPo battery.

Time is UTC (coordinated universal time) - no offsets are applied for local time-zones. The Senquip Portal will apply local time offsets when displaying data as specified by the settings on your computer.

The Senquip Portal can be used to update settings on the Senquip UNI-Z1 remotely. Each time the device makes contact with the Senquip Portal (for example to transmit measurements), the device will check for any settings changes. If there are changes to settings, these will be downloaded and applied. Pending configuration changes are listed on the settings pages on the Senquip Portal.

Command Queue 			
Status	Command	Details	Timestamp
 Pending	Config.Set	{ "device.name": "ORB Water Tank" }	13-Dec-24 10:06:25
Success	Config.Set	{ "endpoint.mqtt.enable": false }	09-Dec-24 14:30:56

Figure 12.2. Pending change where the device name has been changed.

If the Senquip UNI-Z1 is configured to send data to a 3rd party server, the device will by default contact the Senquip Portal to check for settings updates once a day. Set the *Configuration via Senquip Portal* to OFF to prevent the device from contacting the Senquip Portal to check for settings. This setting may be used where power consumption is critical such as when AA batteries are being used

an a very long battery life is required.

Warning Disabling *Configuration via Senquip Portal* will mean that no settings or firmware updates will be able to be performed remotely using the Senquip Portal.

A full list of endpoint settings is given in the table below.

Name	Item	Function	Internal Reference
Data Endpoints			
Configuration via Senquip Portal	boolean	Enables connection to Senquip Portal for remote configuration.	endpoint.config_to_portal
Send Data to Senquip Portal	boolean	Enables data from the device to be sent to the Senquip Portal.	endpoint.data_to_portal
Offline Buffer	boolean	Save data if device is offline, and send when network is available.	endpoint.buffer_enable
Report Network Info	boolean	Add network details and signal strength to data output.	endpoint.network_report
UDP			
UDP	boolean	Enables sending data over UDP to specified address below.	endpoint.udp.enable
UDP Address	text	Address and port to send data to.	endpoint.udp.address
HTTP			
HTTP POST	boolean	Enables sending data via a HTTP POST request to address below.	endpoint.http.enable
HTTP Address	text	Destination address and port for HTTP POST request.	endpoint.http.address
MQTT			
MQTT	boolean	Enables sending data to a MQTT broker.	endpoint.mqtt.enable
Broker Address	text	MQTT Broker Address and Port.	endpoint.mqtt.server
Client ID	text	Client ID to send to the broker. Defaults to device.id if left blank.	endpoint.mqtt.client_id
Username	text	Username for MQTT authentication with username/password. (Optional)	endpoint.mqtt.user
Password	text	Password for MQTT authentication with username/password. (Optional)	endpoint.mqtt.pass

Senquip Portal

The [Senquip Portal](#) is a secure, cloud-based platform hosted on Amazon Web Services (AWS), designed to provide powerful management and visualisation tools for your Senquip devices.

The Portal enables users to:

- View dashboards that display data across groups of devices
- Access detailed device pages showing real-time and historical sensor data
- Perform device management including configuration and firmware updates
- Handle user management with role-based access control
- Maintain long-term data storage for historical analysis and compliance
- Manage events with configurable warnings and alarms
- Manage device subscriptions

The Senquip Portal provides a streamlined and scalable interface used to monitor, manage, and respond to field data from anywhere in the world.

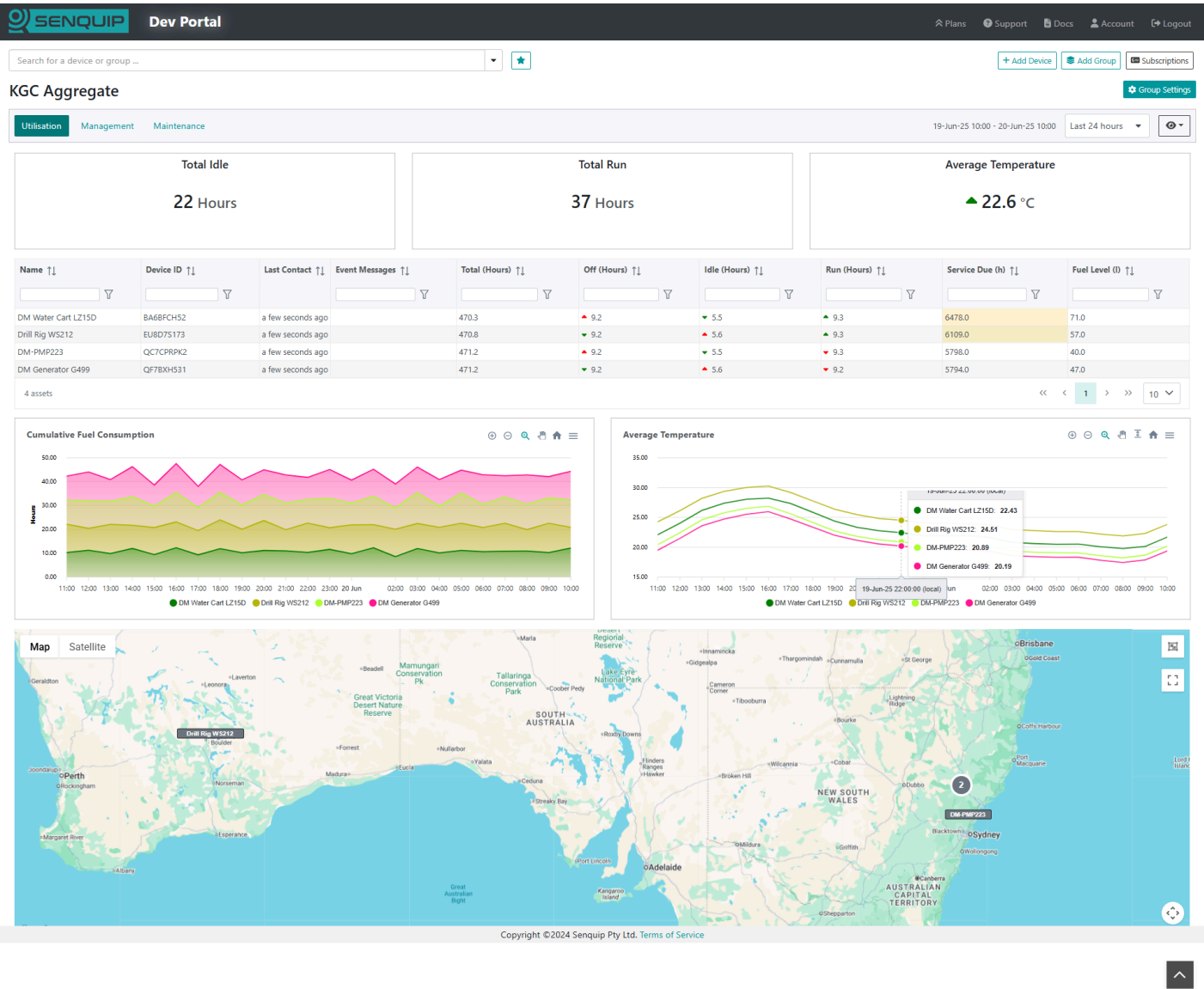


Figure 13.1. Senquip Vision Dashboard

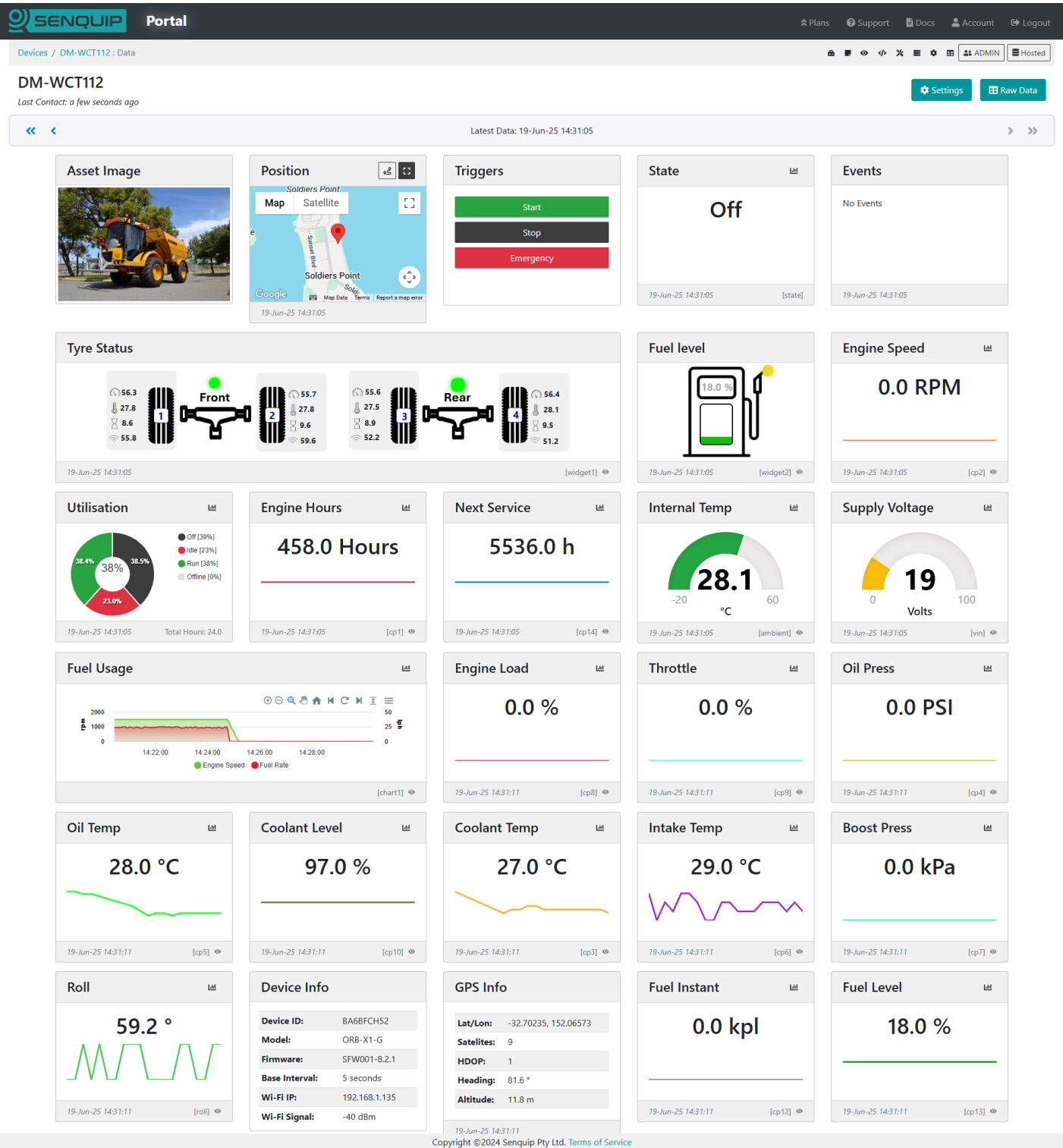


Figure 13.2. Senquip Device Data Page

13.1 Create a Senquip Portal Account

If you do not have an account on the Senquip Portal, you will need to create one. There are no charges for creating an account on the Senquip Portal and a credit card is not required.

1. Go to the [Senquip Portal](#) and select the *Signup* button.



Figure 13.3. Create a Senquip Portal account

2. Complete the required fields and then press *Signup*.

Create Account

Email

test@senquip.com ✓

Given Name

Senquip ✓

Family Name

Test ✓

Mobile Number

+611111222333 ✓

Optional. Required for SMS alerts.
Numbers must be in international format.
For example +61xxxxxxxx in Australia.

Password

..... ✓

Password must be at least 8 characters and contain
uppercase letters, lowercase letters and numbers.

Confirm Password

..... ✓

☒ I have read and agree to the [Terms of Service](#), [Privacy Policy](#) and [Cookie Policy](#)

Signup

Figure 13.4. Complete the required fields

3. A verification email will be sent to the email address provided. Click on the link in the email to verify your account. The email address must be verified as important system updates, alerts, warnings, and alarm messages will be sent to the email address.

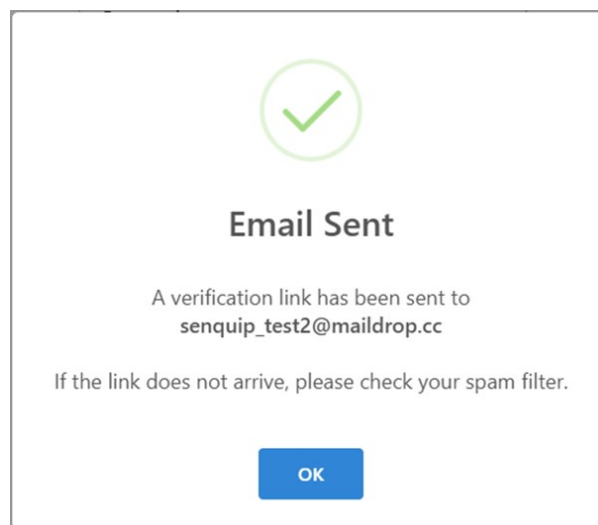


Figure 13.5. Your email must be verified

Note The email may end up in your spam folder or may be blocked by your company firewall.

4. To activate your account, login to the [Senquip Portal](#) once.

A white rectangular form with a thin grey border. It contains two input fields: "Email" with the text "test@senquip.com" and "Password" with masked characters ".....". Below the password field is a teal button labeled "Log In". At the bottom right of the form are two links: "Forgot Password?" and "Create an Account", both in teal text.

Figure 13.6. You must login to activate your account

13.2 Creating a Group

Storing devices in groups facilitates:

- Dashboards that display device data in a way that is meaningful for the application
- User management across a group of devices
- Simultaneous configuration of multiple devices

To create a group:

1. Select the *Add Group* button

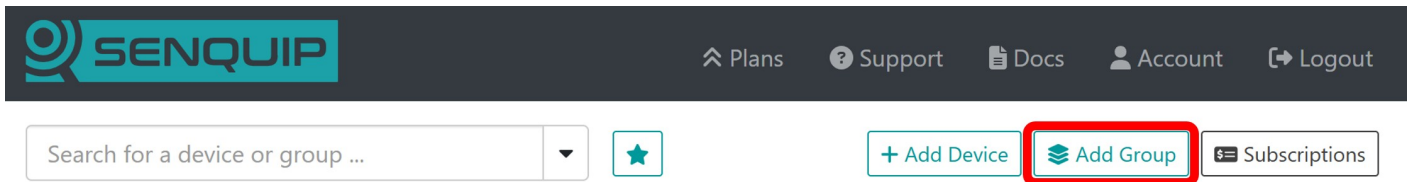


Figure 13.7. Create a new Group

2. Select a name for your group that will be meaningful to the indented user group and press *Create*. The group name can be changed later in the Group Settings.

 A screenshot of a web form titled 'Create New Group'. Below the title is the instruction 'Enter the name of your new group.' There is a text input field with the placeholder text 'Group Name'. Below the input field are two buttons: 'Cancel' and 'Create'.

Figure 13.8. Select a meaningful name

13.3 Add Devices to a Group

You can add devices to a group by either:

1. By pressing the *Add Device* button and entering the device ID. If you are adding a new device to your account, you will be required to enter the setup password.

 A screenshot of a web form titled 'Add New Device'. The form contains the following elements:

- A paragraph: 'To add a device to your Portal account please enter the Device ID which can be found under the lid of your device.'
- A paragraph: 'The Device ID consists of 9 letters and numbers. For example: JDA54E19F' (where 'JDA54E19F' is in red).
- A label 'Device ID' above a text input field with the placeholder 'Enter Device ID'.
- A label 'Group' above a dropdown menu showing 'KGC Aggregate'.
- At the bottom, there are two buttons: 'Cancel' and 'Submit'.

Figure 13.9. Adding a single device to a group

2. Copying or moving devices from another Group for which you have administrator permissions.
3. Requesting that another user give you access to a device or a group of devices.

Note Your account will need to be active for another user to add devices

Note If you have no groups, and devices are added, they will be placed in the default *Ungrouped* Group.

13.4 Finding Devices and Groups

Use the search bar at the top of the page to find devices and groups. Search by group name, device ID, or device name. The *Favourites* button can be used to identify the last few devices and groups accessed, and to mark devices and groups as favourites.

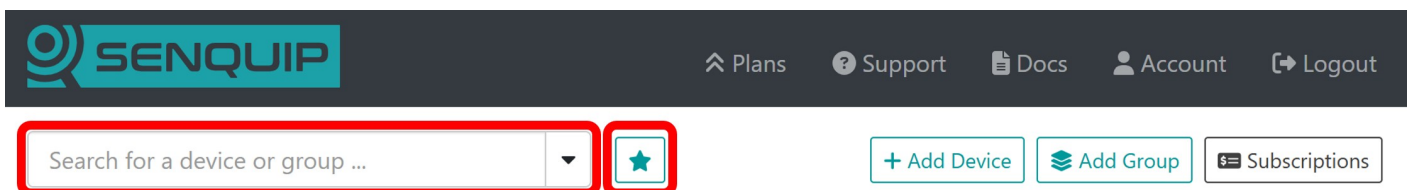


Figure 13.10. Search by group, name , or device id

13.5 Group Management

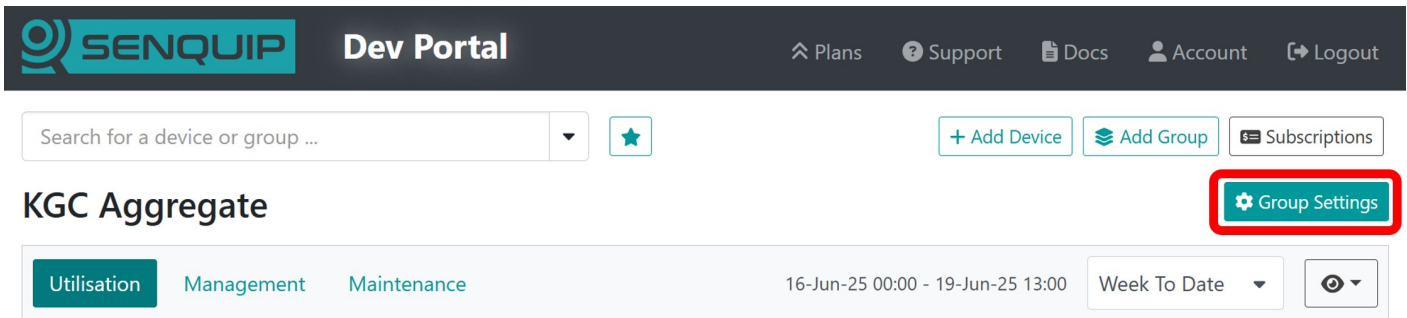
Group functionality simplifies the management of large numbers of devices.

- Groups are collections of devices.
- Devices can belong to multiple groups.
- Private Groups only have one user.
- A group becomes a Public Group when a second user is added to the group.

Groups enable the following functionality:

- Management of user permissions for multiple devices at the same time
- Changing the configuration of multiple devices with a single action
- The standardisation of device data pages across a group
- The creation of dashboards to simplify decision making

Groups are managed by selecting the *Group Settings* button from where group settings, devices, and users can be managed.

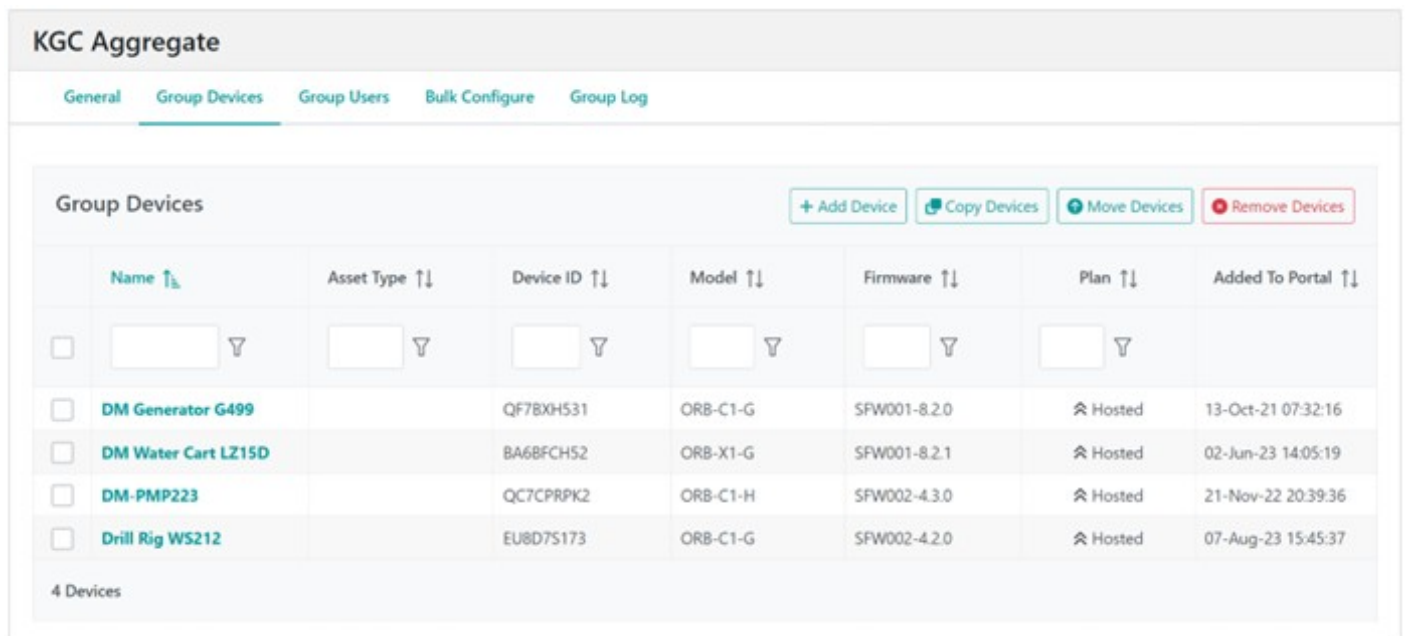


The screenshot shows the Senquip Dev Portal header with navigation links: Plans, Support, Docs, Account, and Logout. Below the header is a search bar and buttons for '+ Add Device', '+ Add Group', and 'Subscriptions'. The main content area is titled 'KGC Aggregate' and features a 'Group Settings' button highlighted with a red box. Below this are tabs for 'Utilisation', 'Management', and 'Maintenance'. A date range '16-Jun-25 00:00 - 19-Jun-25 13:00' and a 'Week To Date' dropdown are also visible.

Figure 13.11. Change Group settings

13.5.1 Device Management

The *Group Devices* option allows devices to be added to the group, copied or moved to another group, or deleted from the group.



The screenshot shows the 'KGC Aggregate' Group Devices management page. It includes tabs for 'General', 'Group Devices', 'Group Users', 'Bulk Configure', and 'Group Log'. The 'Group Devices' tab is active, displaying a table of devices. Above the table are buttons for '+ Add Device', 'Copy Devices', 'Move Devices', and 'Remove Devices'. The table has columns for Name, Asset Type, Device ID, Model, Firmware, Plan, and Added To Portal. Four devices are listed: DM Generator G499, DM Water Cart LZ15D, DM-PMP223, and Drill Rig WS212. A summary at the bottom indicates '4 Devices'.

	Name	Asset Type	Device ID	Model	Firmware	Plan	Added To Portal
☐	DM Generator G499		QF7BXH531	ORB-C1-G	SFW001-8.2.0	Hosted	13-Oct-21 07:32:16
☐	DM Water Cart LZ15D		BA6BFCH52	ORB-X1-G	SFW001-8.2.1	Hosted	02-Jun-23 14:05:19
☐	DM-PMP223		QC7CPRPK2	ORB-C1-H	SFW002-4.3.0	Hosted	21-Nov-22 20:39:36
☐	Drill Rig WS212		EU8D7S173	ORB-C1-G	SFW002-4.2.0	Hosted	07-Aug-23 15:45:37

Figure 13.12. Manage devices in a Group

13.5.2 User Management

The *Group Users* option allows users to be added or removed from a group. Where users are added, they must be allocated appropriate permissions for the group.

Allowed Permission	Admin	User	Operator	View
View data	Yes	Yes	Yes	Yes
Trigger device actions	Yes	Yes	Yes	
View users	Yes	Yes		
Change device settings	Yes	Yes		
View or edit script*	Yes	Yes		
View server log	Yes			
View device passwords	Yes			

Add or remove group users	Yes			
Add or remove group devices	Yes			
Import and export settings	Yes			

Note If you have created a private group and want to share that group, you will need to have administrator permissions for all devices in that group.

Note Users should be added with the minimum permission level required to perform their function.

Warning Anyone who has the device ID and setup password can add the device to their account with Admin permissions.

In the example below, Senquip Test0 is the owner of the group and has *Administrator* access to all devices in the group. Senquip Test1 has been added to the group with permission level *User*.

The screenshot shows the Senquip Dev Portal interface. The top navigation bar includes the Senquip logo, 'Dev Portal', and links for Plans, Support, Docs, Account, and Logout. The breadcrumb trail indicates the current location is 'KGC Aggregate : Group Settings'. The main content area is titled 'KGC Aggregate' and has tabs for General, Group Devices, Group Users (selected), Bulk Configure, and Group Log. The 'Group Users' section displays a table with columns for User Name, User Email, and Group Permission. Two users are listed: 'Senquip Test0' (ADMIN) and 'Senquip Test1' (USER). There are buttons to 'Add User', 'Leave Group', and 'Remove' for the users. A summary bar shows '2 Users' and a 'Permission Types' button.

User Name	User Email	Group Permission
Senquip Test0	Senquip_test0@senquip.cc	ADMIN
Senquip Test1	senquip_test1@maildrop.cc	USER

Figure 13.13. Grant appropriate permissions to group users

13.5.3 Bulk Device Configuration

Bulk configuration of devices allows for settings, firmware, configuration, alerts, and files upload functionality across many devices at the same time.

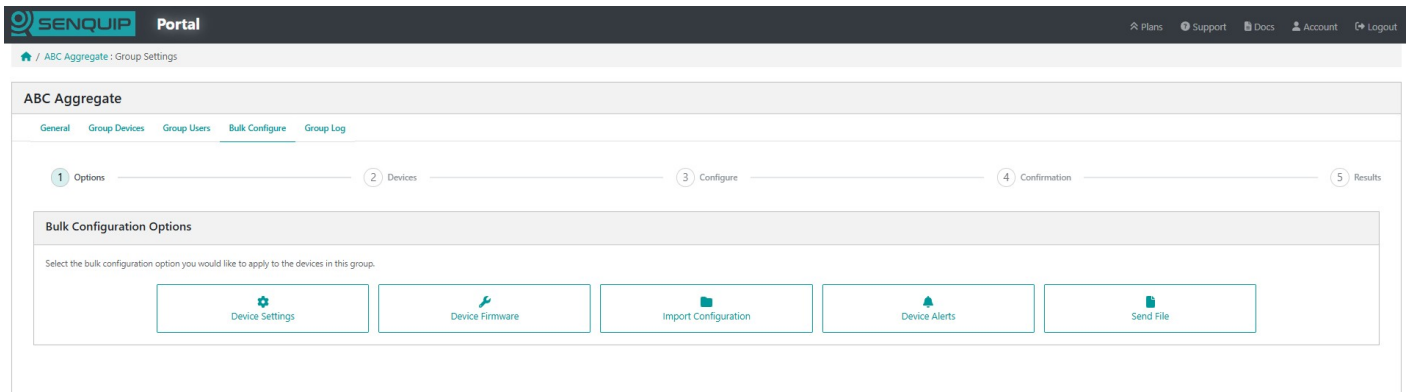


Figure 13.14. Available bulk update options

With each of the bulk configuration options, the devices to be updated can be filtered by:

- Device name
- Firmware version
- Device ID
- Model
- Asset type

After filtering, individual devices can be selected using the checkbox next to each device, or select all devices in the list.

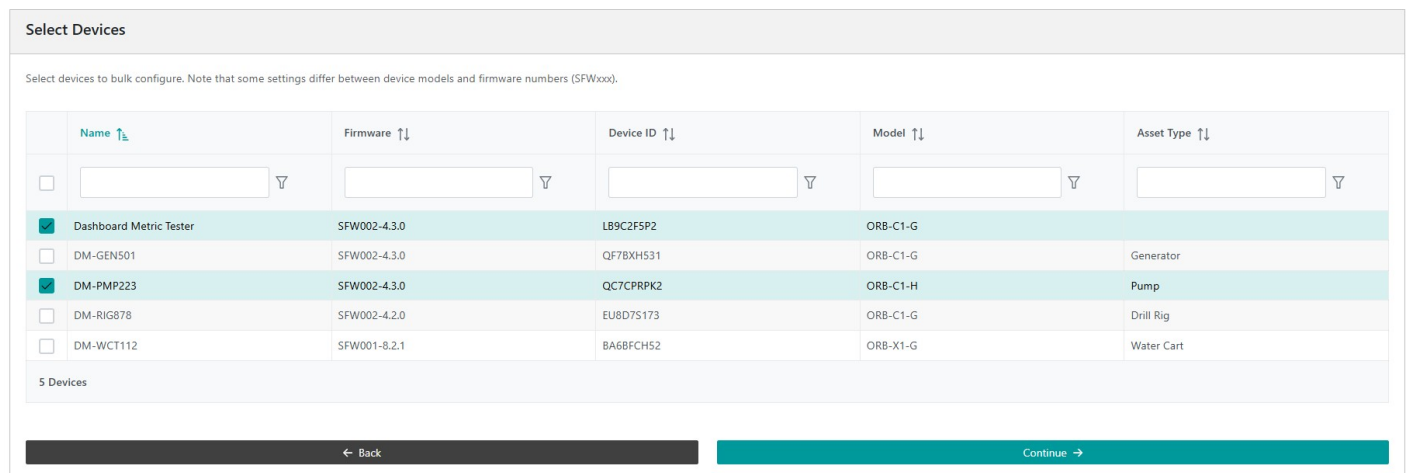


Figure 13.15. Selecting devices for bulk configuration

Warning Bulk Updates Using Groups

When applying settings via the **Groups** feature, changes will be pushed to *all selected devices simultaneously*. This is a powerful tool, but it carries significant risk if configurations have not been properly validated.

Before deploying a Group update:

- Ensure that all devices listed are intended to receive the same configuration.
- Double-check settings such as **network SSID**, **endpoint details**, and **peripheral configurations**.

- Always **test the configuration on a single device first** to confirm safe behaviour.

As shown in the Portal, users must acknowledge the following before applying the update:

- I understand that this update will apply to **all** selected devices shown above.
- I acknowledge that incorrect settings (**for** example: wrong SSID) may cause **all** devices to go offline.
- I have reviewed **and** tested the configuration, **and** confirm it **is** safe to deploy.

Bulk configuration is efficient, but unforgiving. Please review all settings carefully - especially when managing devices in remote or critical environments.

13.5.4 Bulk Settings Update

The Bulk Settings Update feature allows you to apply device settings to multiple devices at once.

Access this feature from the *Group Settings > Bulk Configuration Options* menu by selecting the *Update Device Settings* option.

Settings are applied using a JSON configuration block. You can:

- Copy settings from an existing device using the *View JSON Settings* option under the device Settings menu.
- Paste or enter your own JSON configuration text.

Confirm Changes

The following 1 devices have been selected for bulk configuration.

Name	Device ID	Model	Firmware Version
Dashboard Metric Tester	LB9C2F5P2	ORB-C1-G	SFW002-4.3.0

The following JSON configuration will be merged into the selected devices.

```
{
  "device": {
    "base_interval": 60,
    "vin": {
      "sleep_enable": true
    }
  }
}
```

← Back

Confirm

Figure 13.16. Example JSON input and confirmation before confirming changes.

Once the JSON is entered, review and confirm the changes. Only valid JSON will be accepted.

Refer to the [Senquip Scripting Guide](#) for a list of configuration keys.

Note Always double-check that your JSON settings are compatible with the selected device models and firmware versions before applying them.

13.5.5 Bulk Firmware Update

The Bulk Firmware Update tool allows firmware to be updated across multiple devices simultaneously.

Devices are grouped and filtered based on their firmware family (e.g., SFW001, SFW002, SFW003). A selection button at the top of the interface ensures that only devices within the same base firmware can be chosen.

Note You cannot update between different firmware numbers.

You can filter and sort devices by:

- Name
- Firmware version
- Device ID
- Model
- Asset type

Select Devices

Select devices to apply firmware updates. All devices must have the same base firmware number (SFW00x).

Filter by: SFW001 SFW002

	Name ↑↓	Firmware ↑↓	Device ID ↑↓	Model ↑↓	Asset Type ↑↓
☐					
☒	Dashboard Metric Tester	SFW002-4.3.0	LB9C2F5P2	ORB-C1-G	
☐	DM-GEN501	SFW002-4.3.0	QF7BXH531	ORB-C1-G	Generator
☐	DM-PMP223	SFW002-4.3.0	QC7CPRPK2	ORB-C1-H	Pump
☐	DM-RIG878	SFW002-4.2.0	EU8D7S173	ORB-C1-G	Drill Rig
4 Devices					

← Back

Continue →

Figure 13.17. Selecting devices from the same firmware family.

After selecting devices, you can specify the target firmware version. Options include:

- Entering a specific firmware version (e.g., *SFW002-4.3.0*)
- Leaving the field as **`SFW00x-latest`**, which will automatically apply the latest available version for the selected firmware family

Before updates are applied, a confirmation screen will be shown, listing all selected devices and the firmware version to be installed.

Confirm Changes

The following 1 devices have been selected for bulk configuration.

The selected firmware version SFW002-latest will be applied to each device. For details about what's included in each version, see the [SFW002 Changelog](#).

Name	Device ID	Model	Firmware Version
Dashboard Metric Tester	LB9C2F5P2	ORB-C1-G	SFW002-4.3.0 → SFW002-latest

← Back

Confirm

Figure 13.18. Review and confirm firmware updates.

Once confirmed, the update process begins. Devices will receive the new firmware at their next connection to the Senquip Portal.

13.5.6 Bulk Configuration Import

Device configuration files contain device settings, scripts, Senquip Portal display settings, asset notes, notification settings, and API settings. The Bulk Configuration Import feature allows configuration files that have been exported from a device to be imported into multiple devices at once.

Access this feature from the *Group Settings > Bulk Configuration Options* menu by selecting the *Import Configuration* option.

After selecting a previously exported configuration file, you have the option to

- *Update Firmware to Match Import File* - update the device firmware before importing the configuration file
- *Reset to Factory Defaults Before Importing* - removes all setting from the device before applying the settings in the configuration file

Note Configuration files only contain settings that are different to the defaults. If other settings have previously been changed on the device, these will not be affected by the import. It is therefore suggested that devices be returned to factory default before a configuration is imported.

Note If the imported configuration file does not contain network settings, the device will retain existing network settings.

ABC Aggregate

General Group Devices Group Users Bulk Configure Group Log

1 Options 2 Devices 3 Configure 4 Confirmation 5 Results

Import Configuration

Load and apply settings from a previously exported configuration file.

Choose file

Import File Metadata

```
{
  "fw": "SFW003-6.0.0-beta3",
  "fw_timestamp": "2023-06-05T07:33:28Z",
  "hw": "Q1",
  "id": "QL0C0C160C",
  "model": "QUAD-C2-G",
  "name": "Kensho Controller Test",
  "script_locked": false,
  "contents": [
    "script",
    "Portal Display Settings",
    "Asset Notes",
    "Device Settings",
    "Notification Settings"
  ],
  "comments": ""
}
```

Import Options

Update Firmware to Match Import File ☒ Enabled Import File Firmware: SFW003-6.0.0-beta3

Reset to Factory Defaults Before Importing ☒ Enabled

Warning All existing device settings will be removed before import. Existing network settings will be used if no imported value is available.

Back Continue

Figure 13.19. Review and confirm configuration import.

After a user confirmation, the results of the bulk configuration import are shown.

Warning If the configuration file originates from a different firmware, for example SFW002 from an ORB being applied to SFW003 on a QUAD, device settings may not be compatible.

13.5.7 Bulk Device Alert Configuration

Device Alert settings can be configured for multiple devices at once.

Access this feature from the *Group Settings > Bulk Configuration Options* menu by selecting the *Device*

Alerts option.

Device Alerts

Set recipients for SMS and email alerts with notification timing options.

☐ Change Email Recipients
If unchecked, email recipients will not be changed.

Type an email address for alerts...

☐ Change SMS Recipients
If unchecked, phone numbers will not be changed.

Type a mobile number for alerts...

The following options are available for each event type:

Disabled - No notification sent for this event.

Enabled - Notification sent immediately for any new event.

Enabled with daily reminder - Notification sent immediately and every 24 hours while the event remains continuously active.

☐ Change Alert Notification Settings
If unchecked, existing alert thresholds and frequencies will remain unchanged.

	SMS	Email
Alerts	Disabled	Disabled
Warnings	Disabled	Disabled
Alarms	Disabled	Disabled

← Back

Continue →

Figure 13.20. Bulk update of device alerts.

Options available include:

- Update of email recipients
- Update of SMS recipients
- Enabling of SMS and email alerts and optional reminders

After a user confirmation, the results of the alert updates are shown.

13.5.8 Bulk File upload

User files, typically csv or txt, can be uploaded to multiple devices at the same time. These files may be used in scripts to linearise sensors, update geofences, or a host of other applications.

After choosing a file, the results of the file upload are shown.

Add File to Devices

Download a file to the selected devices. For details on using files in scripting, see the [File Scripting Guide](#).

Select a file to download to the selected devices.

Choose file

No file chosen

← Back

Continue →

Figure 13.21. Bulk file upload.

Note There is a 20k limit on the size of files that can be uploaded to a device.

13.6 Senquip Vision Dashboards

Senquip Vision is a powerful, customisable dashboard that enables businesses to monitor and analyse key operational metrics across a group of devices. Designed for management, maintenance and operational users, it provides a clear and intuitive interface for tracking real-time data, historical trends, and device status, all in one place.

The following are key elements of a Senquip Vision Dashboard:

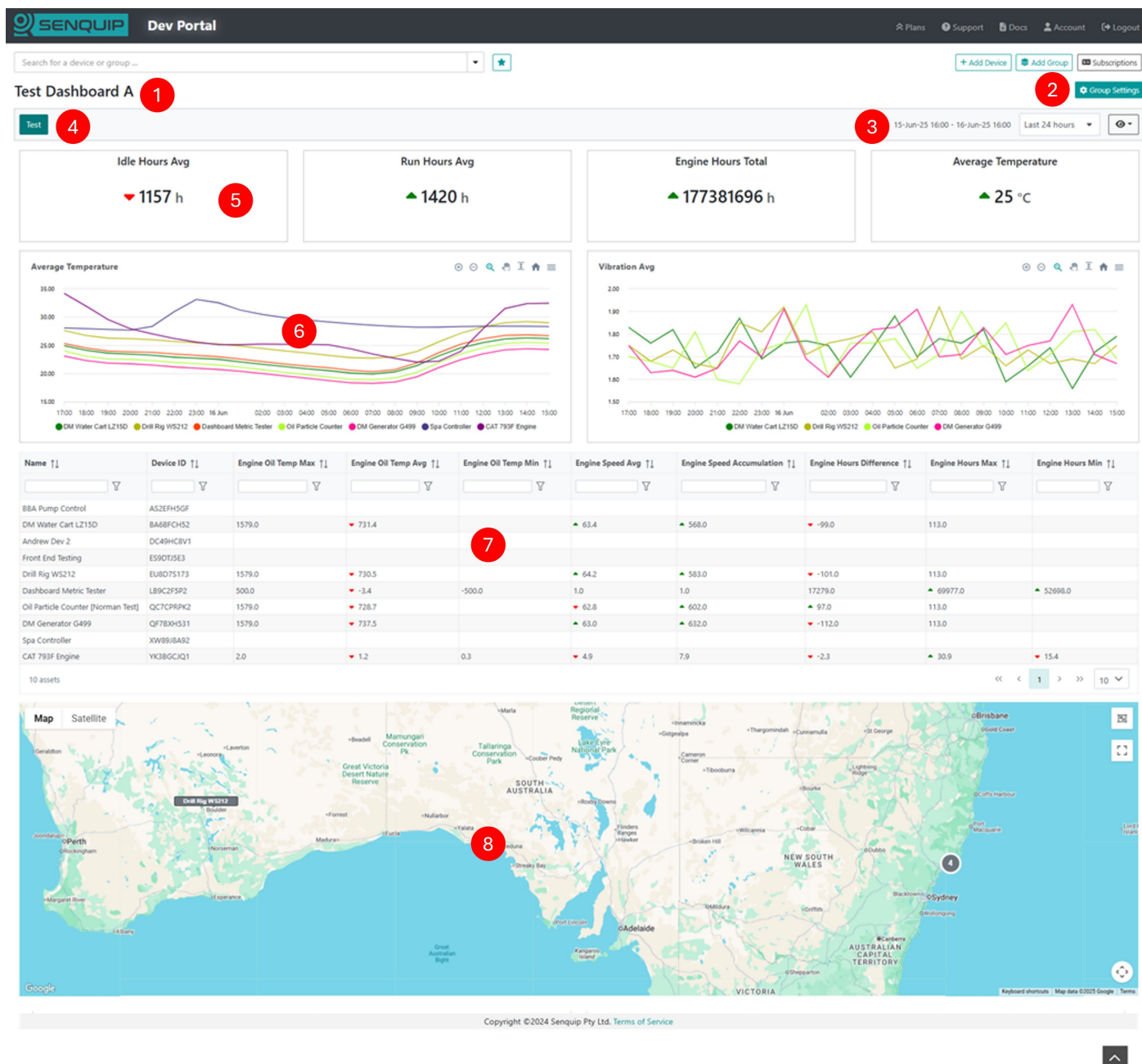


Figure 13.22. Fully customisable Senquip Vision dashboard

Key	Element	Description
1	Dashboard Name	A name that is meaningful to the target user group.

2	Group Settings	Manage the group and perform bulk user management and device configuration.
3	Period	The time range over which data in the dashboard is calculated and shown.
4	View	Multiple views can be created to accommodate users with different roles (e.g. management and maintenance views)
5	Headline Number	Displays key metrics aggregated across all devices in a group.
6	Summary Chart	Visualises data trends over the selected time period.
7	Summary Table	Shows metrics for all devices in the group, calculated over the selected time period.
8	Map	Displays current device locations, with colour indicating device status.

13.6.1 Views

When a new Group is created, a default display with table and map will be generated. Users can then create different views for management, operational, maintenance and other functions. Headline numbers, a customised table, charts, and a map can be added to a view.

KGC Aggregate

[Group Settings](#)


Figure 13.23. Create a different view for each user function

Key	Element	Description
1	Views	Select between the various views that have been created for the dashboard
2	Period	Select the period of time over which data should be calculated and displayed
3	Edit View	Views can be edited by pressing the view settings icon on the right of the view toolbar to expose add, edit, and delete options.

13.6.2 Period

A period of interest can be selected that aligns with the function of the view. For example, when considering rainfall data, month to date may be the most meaningful period. When considering productivity, the last 7 days may be more useful. When a period is selected, calculations on data (metrics) are performed over that time, and data is displayed for that period. Available periods are shown in the table below. Additional periods and previous periods can be selected using the *Custom Range* option.

Period	Description
Last 24 hours	Rolling window of 24 hours
Last 7 days	Rolling window of 7 days
Last 30 days	Rolling window of 30 days
Week to date	Fixed 7-day period, starting at 00:00 on Monday
Month to date	Fixed period starting on the 1st of the month at 00:00
Custom Range	Select your own range

13.6.3 Metrics

Metrics refer to data measured by a device, or values derived from that data by applying operations such as average, total, difference, and others. Metrics are shown in the summary table, on charts, and are the basis for headline numbers. Available metrics include latest data, minimum, maximum, total,

difference, accumulation, and time weighed average. Metrics are selected for a measurement when columns are added to the summary table.

Table Editor

Select and edit columns for the table.

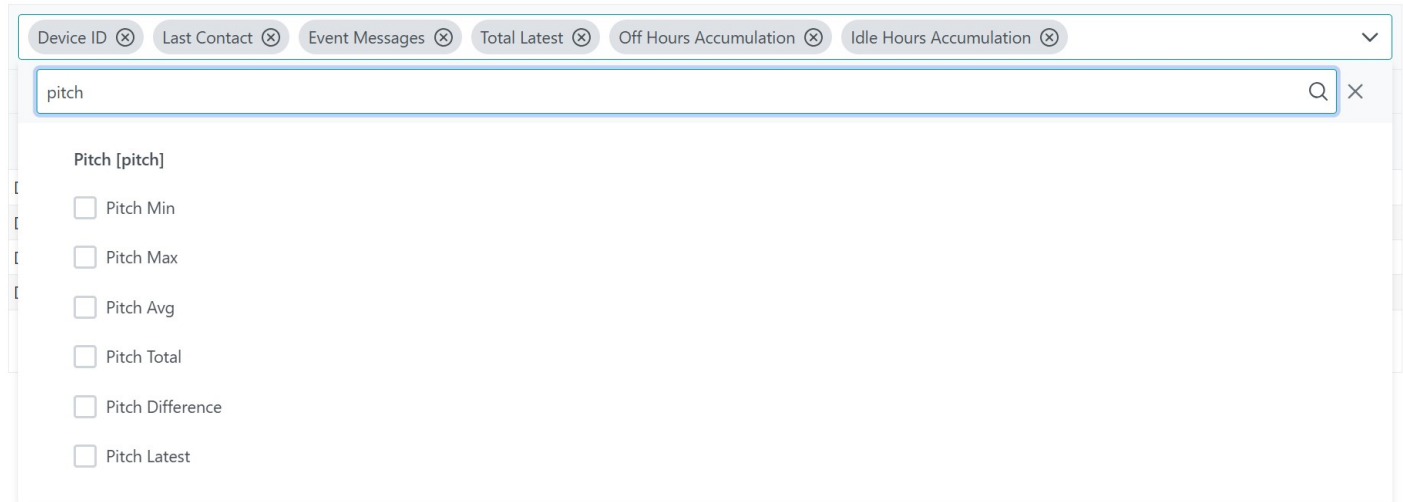


Figure 13.24. Min, max, average, total, difference, and latest metrics are available

Metrics are calculated at the end of each hour for the data collected in that hour and are then collated for the selected period.

Maximum and Minimum

The highest and lowest value measured over the selected period.

Example applications:

- lowest temperature in the last 24 hours
- Lowest tank level so far this month
- Highest engine temperature this week
- Highest engine RPM over the past 24 hours

Note If no samples are available in the period, this value is undefined.

Note If only one sample is available in the period, the minimum and maximum are the same.

Note Maximum and minimum up till the end of the last complete hour.

Latest Data

The latest value measured by the device.

Example applications:

- Current engine hours
- Current tank level
- Current temperature
- Current machine state

Note If there is no current data, then the last available data will be displayed.

Time Weighted Average

The time weighted average considers how long each value was applicable when calculating the average. If for instance, only a few samples are taken in a day, the Time Weighted Average will assume that the previous sample was valid until a new one arrives. This ensures that values occurring for longer durations contribute proportionally more to the average.

In the example below, a dam level is monitored. Actual level samples arrive sporadically. In the absence of a sample, the previous sample is assumed to still be valid. The time weighted average will be the area under the chart divided by the period. Notice that the first sample is 2-Jan-2025 0:00:00 which represents midnight on the 1st Jan. Likewise, the last point is the 1-Feb-2025 0:00:00 which represents midnight on the 31st Jan.



Figure 13.25. Time weighted average works well where there are missing samples

Example applications:

- Average dam level over a month
- Average flow over a month

Note If there is no previous data at the start of the period, the last sample from the previous period will be used.

Note If there is no previous sample, then the first sample will be assumed to have been the value at the beginning of the period.

Integration

The integration function estimates the area under a time-varying signal curve over a measurement period. It is used to calculate the effect or quantity of a signal that represents a rate over time.

For example, a flow meter that outputs a 4 to 20 mA signal proportional to flow rate can be integrated to estimate the total volume.

Internally, integration is performed by multiplying each sampled value by the time between samples (in seconds), using the same technique as the time weighted average.

Note The input signal should represent a *rate per second* (e.g., litres per second), so that the integrated

result is in consistent physical units (e.g., litres or joules). If your sensor reports in units per minute, you must convert to per second (e.g., divide by 60) either in the sensor settings or using a script.

Note The Integration function follows the same sampling approach as shown in the TWA diagram, but it does not divide by time.

Warning Integration accumulates small errors over time.

Total Over a Period

Calculates the total of all the measured samples over a period. In the figure below, daily rainfall is totalised for the month. Notice that the first sample is 2-Jan-2025 0:00:00 which represents midnight on the 1st Jan. Likewise, the last point is the 1-Feb-2025 0:00:00 which represents midnight on the 31st Jan.

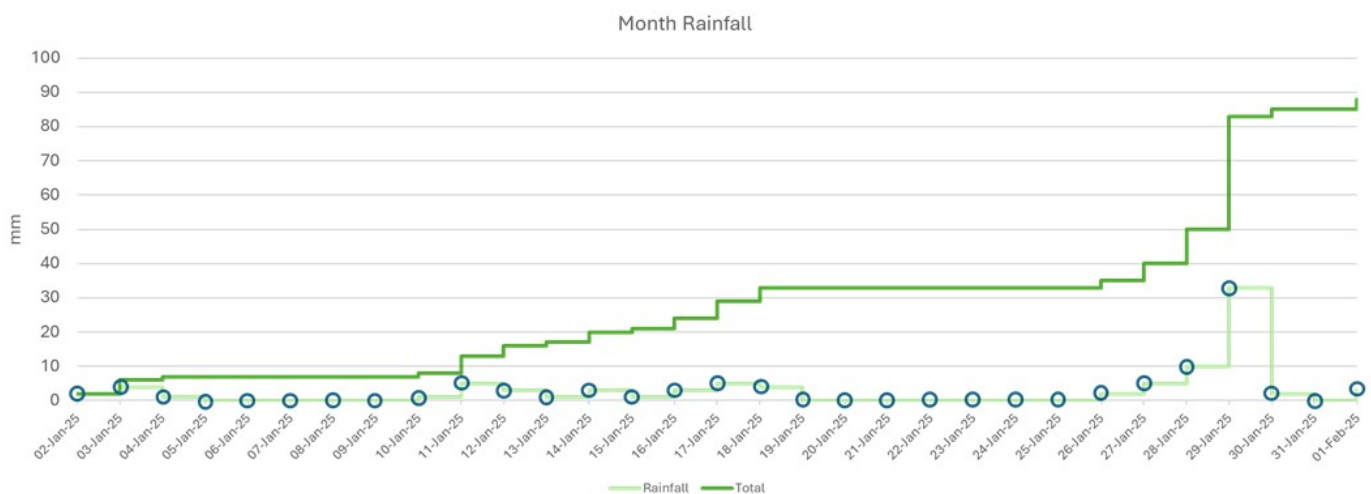


Figure 13.26. Total, sums all data values

Example applications:

- Total rainfall over a period
- Number of times that the pressure has dropped below a threshold.
- How many times a gate has been opened.

Creating a metric to process totals based on historic data simplifies device configuration by offloading totalisation over a period function from the device to the Senquip Portal.

Note If no samples are available in the period, this value is zero.

Note The sum over a period is calculated up to the end of the last complete hour.

Difference Over a Period

The difference between the most recent data and the same data at the end of the previous period.
Example of use:

- Change in dam level over the past month
- Change in engine hours over the past week
- Change in idle hours over the last 7 days

Note If no samples are available in the period, this value is undefined.

Note If no samples are available in the previous period, this value is undefined.

Note The difference over a period is calculated up to the end of the last complete hour.

Accumulation Over a Period

Calculates the total increase in a parameter over the selected period, regardless as to whether the source parameter is reset. For instance, if an engine hour meter is replaced or reset, and returns to zero, the accumulation will not be reset and will continue to climb. In the figure below, engine hours are being read from an hour meter. As the hour meter rises, so does the accumulation. When the hour meter is reset, the accumulation does not change and continues to climb. Accumulation is a good measure of a total where the source data may reset.

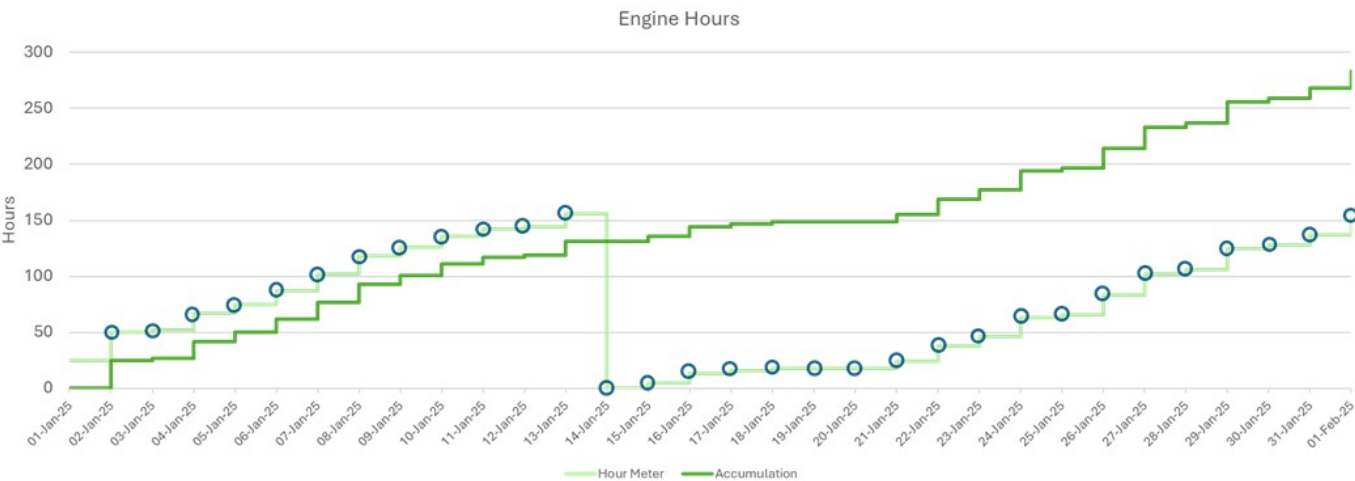


Figure 13.27. Accumulation calculates increase even is the source parameter is zeroed

Example:

- Engine run time where the engine hour meter may be replaced
- Engine idle time where the counter resets to zero when the engine is powered off
- Total distance travelled based on a trip distance meter
- Total flow where the flow meter may get zeroed

Note If no samples are available in the period, the value will remain the same as end of the previous period.

Note If no samples are available in the previous period, the start value will be assumed to be zero.

Note The accumulation over a period is calculated up to the end of the last complete hour.

13.6.4 Summary Table

The summary table widget is the primary element on a view. It shows metrics over the period for all devices in a view. In the example below, we see that fuel is low on some machines, indicated by

the cells being marked red. On 2 machines, the fuel is very low, and alert messages are active. Idle hours when compared with the previous period are down on three machines as marked by the green down arrows. Run hours on 3 machines are up, a good outcome.

Click a device in the table to inspect the device data page.

Name ↑↓	Device ID ↑↓	Last Contact ↑↓	Event Messages ↑↓	Total (Hours) ↑↓	Off (Hours) ↑↓	Idle (Hours) ↑↓	Run (Hours) ↑↓	Service Due (h) ↑↓	Fuel Level (l) ↑↓
DM-WCT112	BA68FCH52	a few seconds ago		398.5	▼ 9.2	▲ 5.6	▲ 9.2	9159.0	69.0
DM-RIG878	EU8D7S173	a few seconds ago	Fuel low	410.5	9.2	▼ 5.6	▲ 9.2	507.0	10.0
DM-PMP223	QC7CPRPK2	a few seconds ago	Fuel low	515.9	▲ 9.3	▼ 5.5	▼ 9.2	3042.0	2.0
DM-GEN501	QF7BXH531	a few seconds ago		410.4	▲ 9.2	▼ 5.5	▲ 9.2	572.0	77.0

4 assets

<< < 1 > >> 10

Figure 13.28. Device summary table showing alarms on the fuel level

Columns are added, removed, and edited using the table editor. In the example below, metrics have been filtered by temp, and the minimum, and average temperature have been chosen to be added to the summary table.

Table Editor

Select and edit columns for the table.

Device ID (X)
Last Contact (X)
Event Messages (X)
Total Latest (X)
Off Hours Accumulation (X)
Internal Temp Min (X)
Internal Temp Avg (X)

temp

Internal Temp [ambient]

☒ Internal Temp Min

☐ Internal Temp Max

☒ Internal Temp Avg

☐ Internal Temp Total

☐ Internal Temp Difference

☐ Internal Temp Latest

Figure 13.29. Adding metrics to a Device Summary Table

The features of table columns can be changed by pressing the edit button at the top of each column in the table editor. Warning and alarm levels can be applied, which when selected will change the cell colour to orange or red. Red and green indicator arrows can be enabled in each cell to show whether a value has increased or decreased when compared to the previous period.

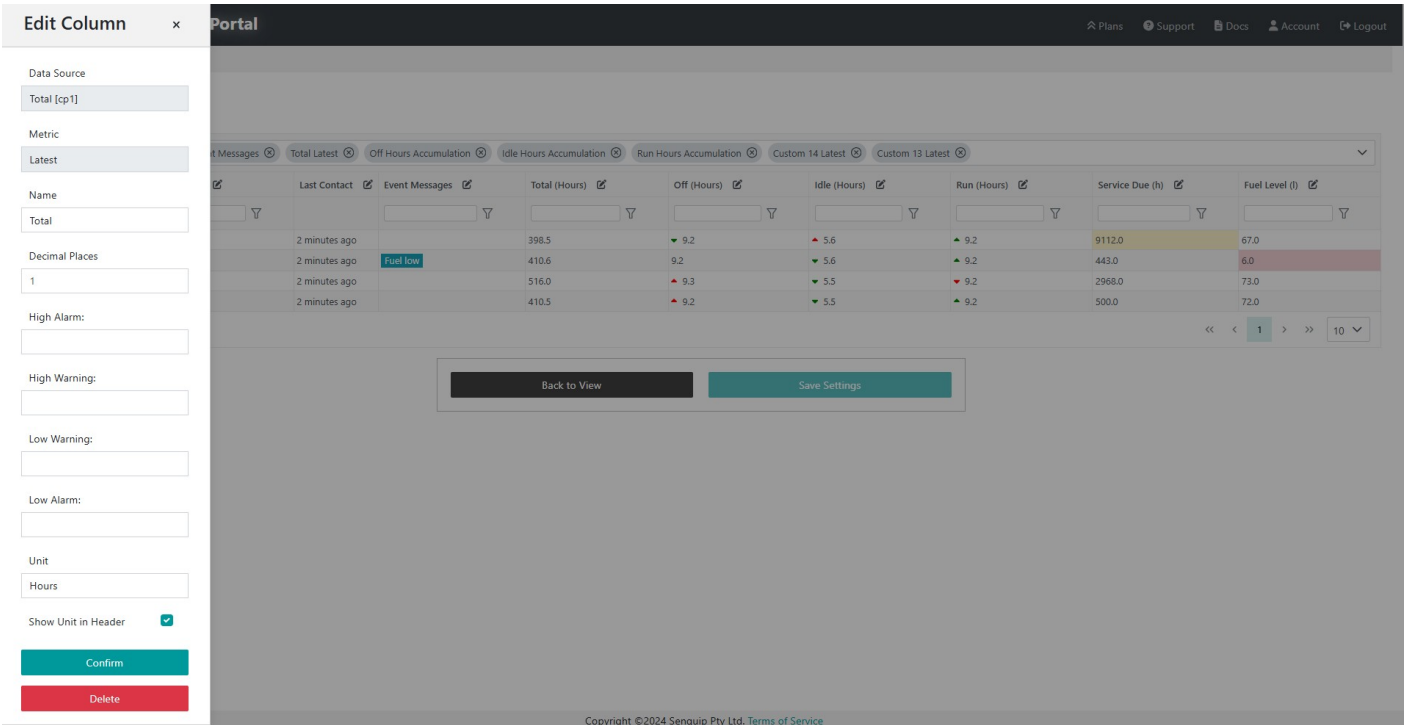


Figure 13.30. Press the edit button on each column to edit functionality

In this example summary table, a warning has been placed when engine hours increase above 6000, and an alarm has been placed on low fuel. Indicator arrows are indicating that idle are down on 3 machines, and run hours are up in most cases.

Name ↑↓	Device ID ↑↓	Last Contact ↑↓	Event Messages ↑↓	Total (Hours) ↑↓	Off (Hours) ↑↓	Idle (Hours) ↑↓	Run (Hours) ↑↓	Service Due (h) ↑↓	Fuel Level (l) ↑↓
DM-WCT112	BA6BFCH52	a few seconds ago		398.5	▼ 9.2	▲ 5.6	▲ 9.2	9159.0	69.0
DM-RIG878	EU8D7S173	a few seconds ago	Fuel low	410.5	9.2	▼ 5.6	▲ 9.2	507.0	10.0
DM-PMP223	QC7CPRPK2	a few seconds ago	Fuel low	515.9	▲ 9.3	▼ 5.5	▼ 9.2	3042.0	2.0
DM-GEN501	QF7BXH531	a few seconds ago		410.4	▲ 9.2	▼ 5.5	▲ 9.2	572.0	77.0
4 assets									

Figure 13.31. Example Device Summary Table showing warnings and alarms

Filters

Filters are used to single out devices from all the devices in the group. Permanent filters can be applied in the table editor, or temporary filters can be applied in the live view. For example, a group may be created that contains all the off-highway assets at a quarry. Different views can then be created to show lighting towers, pumps, and crushers by adding a filters on asset type in the table associated with each view.

Warning Remember to save your settings before returning to the view.

13.6.5 Headline Numbers

Headline numbers show data based on all devices in the current view. In the example below, total idle hours and total run hours across the 4 devices in the table are shown as headline numbers. We can immediately see that idle hours are up over the last 7 days when compared to the previous period, the good news is that run hours are also up. Increased idle hours are bad and are marked

with a red up arrow. Increased run hours are good and are marked with a green up arrow. Hover on the arrow to see the value for the previous period.

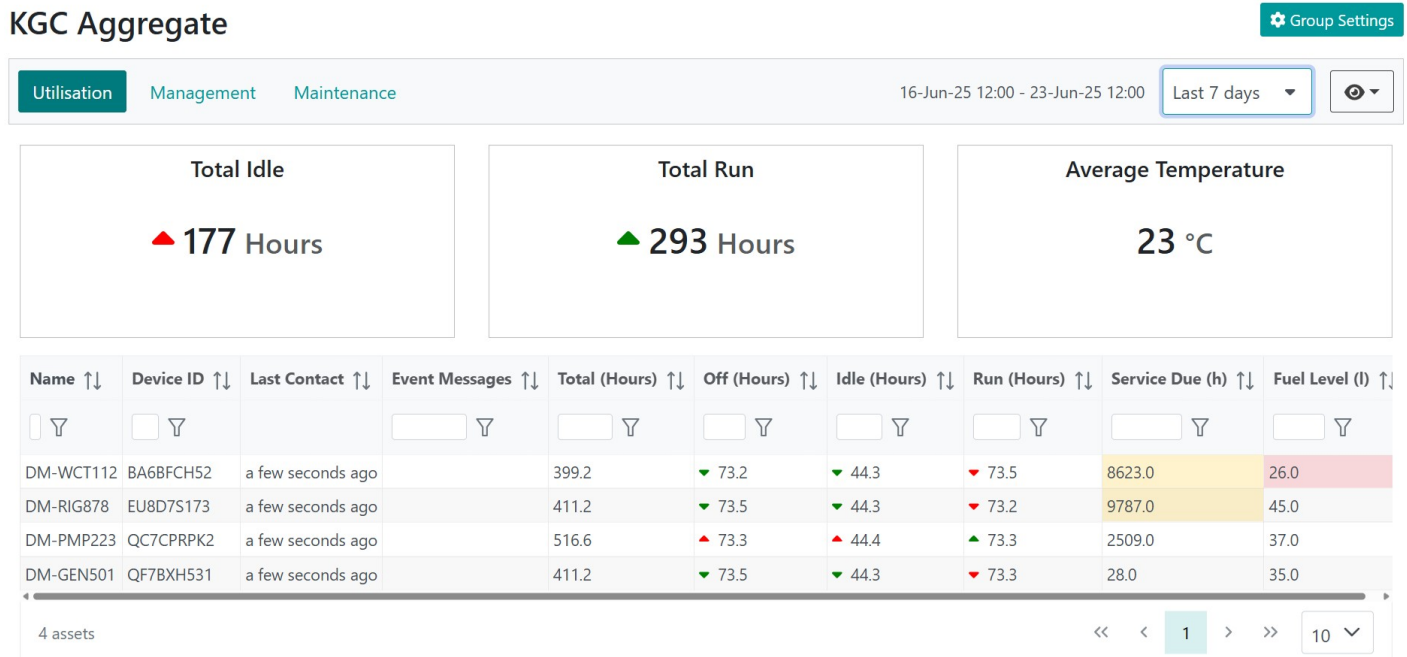


Figure 13.32. Headline numbers show metrics across all devices in the view

Headline numbers are added using the *Edit View* button by selecting *Add headline*. Headline numbers perform operations on all devices in the view. Available operators are:

- Total: Sum a metric across all devices in the view
- Average: Calculate the average across a metric, for all devices in the view
- Minimum: Show the minimum value across all devices in the view
- Maximum: Show the maximum value across all devices in the view

When creating a headline the following steps must be taken:

1. Select the data source from all available metrics. In the example below, the data source chosen is Internal Temperature Average.
2. Choose the operator from either total or average. In the example below, average is chosen and so the headline number will show the average of all the internal temperatures across all devices in the view.
3. Choose a meaningful title, a unit, the number of decimal places to show
4. Select a trend arrow, if required, being careful to choose whether up and down are good or bad

Average Temperature

22 °C

Headline Setup

⚠ Unsaved Changes

Headline Title:

Data Source:

Internal Temp Avg

▼

Operator:

Average

▼

Unit:

Decimal Places:

Trend Arrow Color:

☐ None

☒

☐

☐

☐

Back to View

Save Settings

Figure 13.33. Headline numbers total and average a source metric across all devices in the view

Warning Remember to save your settings before returning to the view.

13.6.6 Charts

Charts can be added to show trend data across the period of interest. Charts show metrics as calculated at the end of each hour. In the example below, a stacked line chart is used to show total fuel used across all machines by the hour. It can be seen that the water cart used 12.09 litres of fuel for the hour ending at 07h00.

Device	Fuel Consumption (Litres)
DM Water Cart LZ15D	12.09
Drill Rig WS212	10
DM-PMP223	11.19
DM Generator G499	12.51

Figure 13.34. Charts show trend data across multiple devices

Charts are added using the *Edit View* button and selecting *Add Chart*. When creating a chart, the following steps must be taken:

1. Select the data source from all available metrics. In the example below, the data source chosen is the average of Custom 11. In this case, Custom 11 is a custom parameter that has been generated in a script on a device and measures instantaneous fuel consumption.
2. Choose the chart type as either line or area, and select whether it is stacked.

13.6. Senquip Vision Dashboards

133

3. Chose a meaningful chart name and configure the y-axis.

Chart Setup

Chart Name:

Data Source:

Chart Type:

Stacked Series: ☒

Stacked Series is limited to 1 axis

Chart Y-Axis

☒ [ax1]

Hours	Min	Max
Tick	dp	Unit

Figure 13.35. A stacked chart shows cumulative contribution of multiple data series over time

Warning Remember to save your settings before returning to the view.

13.6.7 Map

A map will be added to the view by default; it can be removed using the options activated by pressing the *Edit View* button and then selecting *Edit Widgets* and pressing the delete icon on the map. Once removed, an option to add it will appear in the *Edit View* options.



Figure 13.36. Clusters of device separate as the zoom level increases

Where there are many devices in the same area, they will cluster and be shown as the total number of

devices in that area. As the zoom level is increased, the devices will separate.

The colour of the labels on the map indicates if there are any current alerts associated with the device.

- Grey: No alerts
- Blue: Alerts
- Orange: Warnings
- Red: Alarms

Click a device on the map to inspect the device data page.

13.6.8 Customising Layout

Senquip Vision allows you to customise the size and position of dashboard widgets for optimal viewing on desktop, tablet, and mobile screens.

To adjust widget layout:

1. Press the *Edit View* button and select *Edit Widgets*.
2. Choose a display mode: Desktop, Tablet, or Mobile.
3. Reposition widgets by dragging them using the arrow handle at the bottom-left corner.
4. Resize widgets by dragging the bottom-right corner of the widget.
5. When finished, select *Exit Edit* to return to the dashboard view.

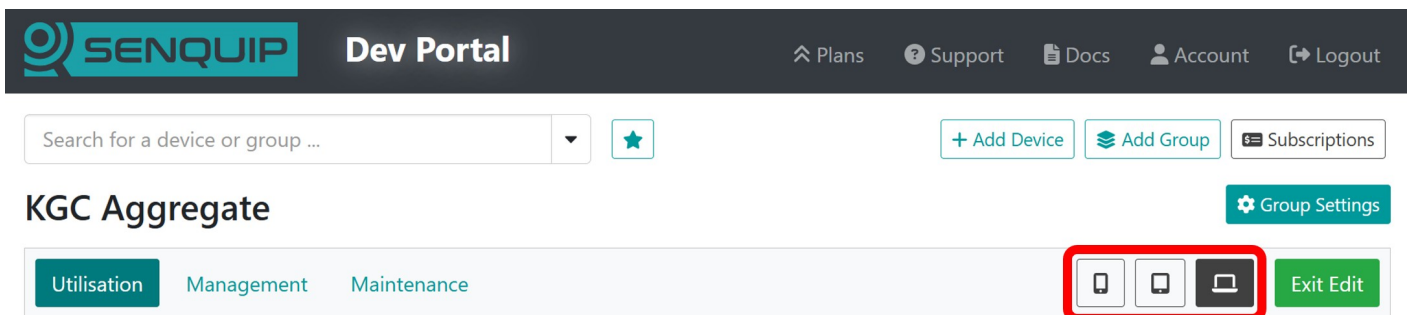


Figure 13.37. Optimise the layout for different screen sizes

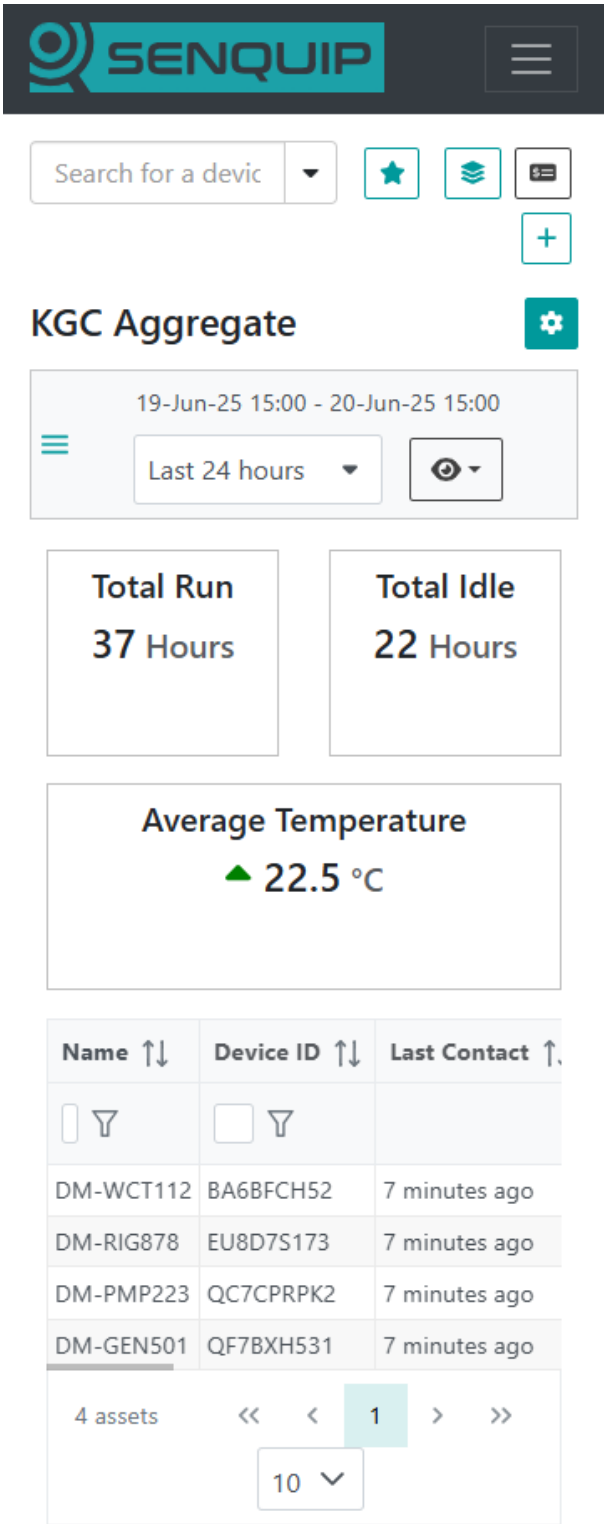


Figure 13.38. Dashboard view optimised for mobile screens

13.7 Device Data Page

The Device Data Page offers a centralised and intuitive view of all real-time and historical measure-

mentsreported by a Senquip device. Data is shown in real time and can be visualised as numbers, gauges, charts, or infographics.

The following are key elements of the Device Data Page:

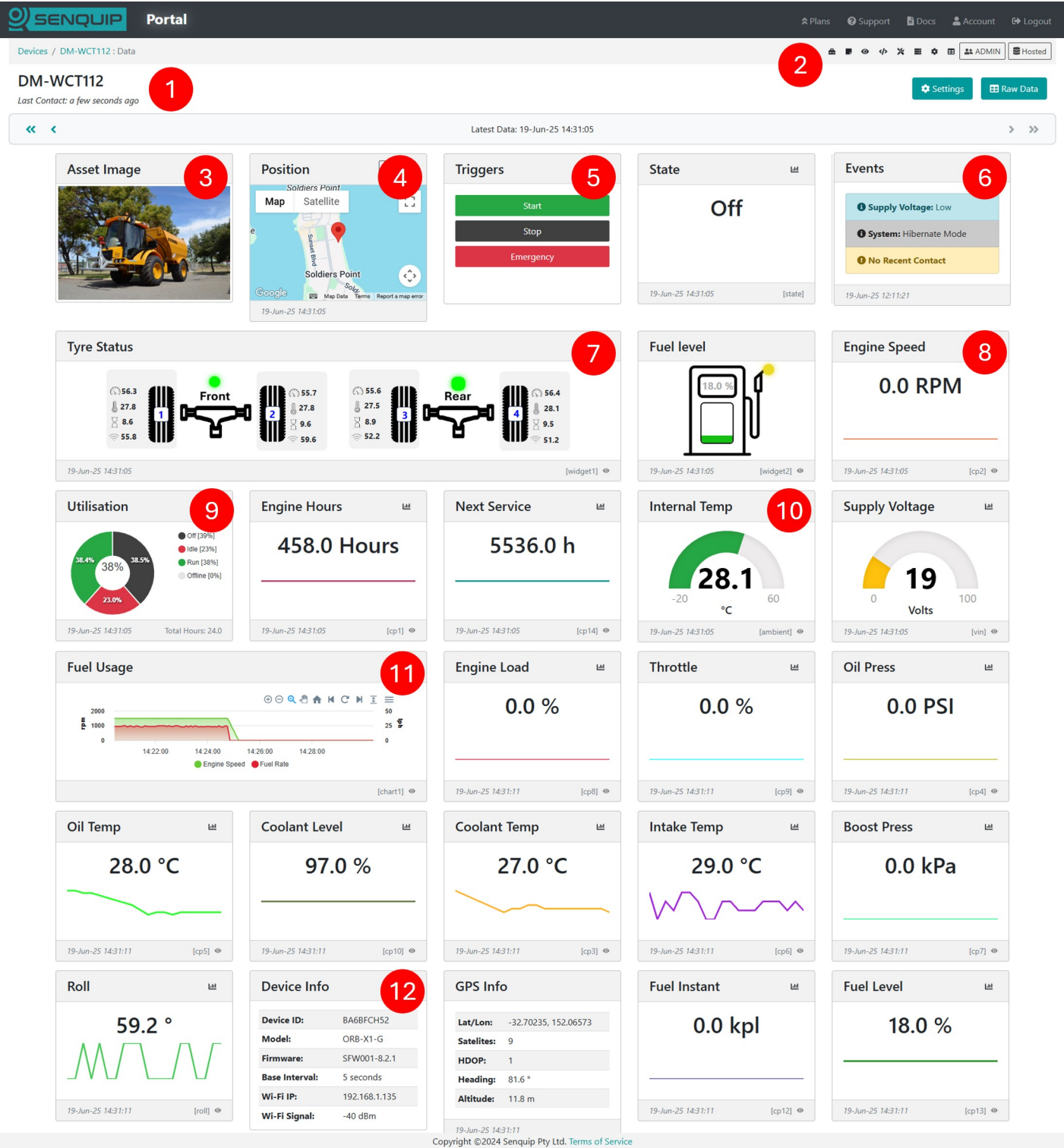


Figure 13.39. Device Data Pages provide a detailed view of measured data

Key	Element	Description
1	Device Name	The name associated with the Senquip device
2	Toolbar Icons	Provide quick access to device settings, scripting, raw data, and more
3	Asset Image	Optional application image
4	Map	Shows the current device location and historic track
5	Trigger Buttons	Allow for remote control by activating functions locally on a remote device
6	Events	Shows all active alerts, warnings, and alarms for a device
7	Infographic	User generated graphical widget that allows information to be shown in a meaningful way
8	Number	Widget displaying numerical data as a number
9	Utilisation	Pie chart showing asset utilisation
10	Gauge	Numerical data shown as a gauge
11	Chart	User generated chart showing trend data
12	Device Info	Shows information about the device
13	Raw Data	(Not shown) The raw JSON data for a device

The Device Data Page is also the central hub for managing device setup. From the toolbar icons on the page, you can select the following:

- Asset Notes: Add notes and images associated with the device application and install.
- Display Settings: Choose which measurements are displayed, and the order in which they are displayed. Create custom Graphical Widgets and Charts.
- Scripting: Link to the device scripting page to customise device operation, create custom parameters, add trigger buttons, and configure states.
- Diagnostics: View device diagnostics information, SIM information, signal strength and more.
- Server Log: Show a log of all user activity including when settings were changed, and when users were added.
- Settings: Change device settings, perform firmware upgrades, and configure events.
- Raw Data: Download historical data and export to CSV if required.

Note Available options will vary depending on user permissions.

13.7.1 Device Data Page Configuration

As measurements are enabled on the Senquip device, associated widgets will automatically appear on the Device Data Page. The widgets can be turned on and off, and the order of display can be changed.

Page Layout

Select the *Display Settings* icon to choose which measurements are displayed, and the order in which they are presented.

Display Settings

Show or hide information on the device page.

Device Page	Display Order	Key	Name
☒	9	[asset_image]	Asset Image
☒	10	[events]	Events
☒	11	[deviceinfo]	Device Info
☒	12	[triggers]	Triggers
☒	12	[utilisation]	Utilisation
☒	12	[state]	State
☒	24	[ambient]	Internal Temp
☒	26	[pressure]	Atmospheric Pressure
☒	27	[vin]	Supply Voltage
☐	28	[vbat]	Battery Voltage
☒	29	[vsys]	System Voltage
☒	50	[cp2]	Vin Drop
☒	50	[cp1]	Run Count
☒	70	[pitch]	Pitch
☒	71	[roll]	Roll
☒	72	[angle]	Angle
☒	73	[motion]	Vibration
☒	90	[raw_json]	Raw Data

Figure 13.40. Turn widgets on and off and configure the display order

Add Asset Image and Logo

Select the Asset Notes icon to upload an image of the asset being monitored, a brand logo, the install location, and to make notes about the install.

Change Widget Display Format

Press the eye icon at the bottom right of the widget to switch between various display formats. Available formats are:

- Hidden - Hide the data if it is not relevant to the application
- Trendline - The default graph that facilitates recognition of change. Allows the user to view longer term trends between date ranges.
- Gauge - Useful when representing measurements that must exist within a range. Can be scaled so that the pointer is vertical under normal conditions. Warning and alarm levels can be set.
- Digital - A simple ON or OFF display that shows the status of a measurement. The threshold at which the display switches from ON to OFF can be set.

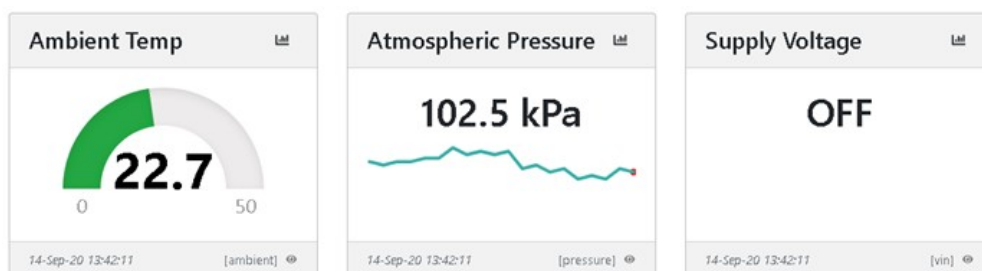


Figure 13.41. Switch between numeric, gauge, and digital display modes

Click on the icon at the top right of each widget to show numerical data on a chart over a selected period. Click on a point on the chart to show values at that point.

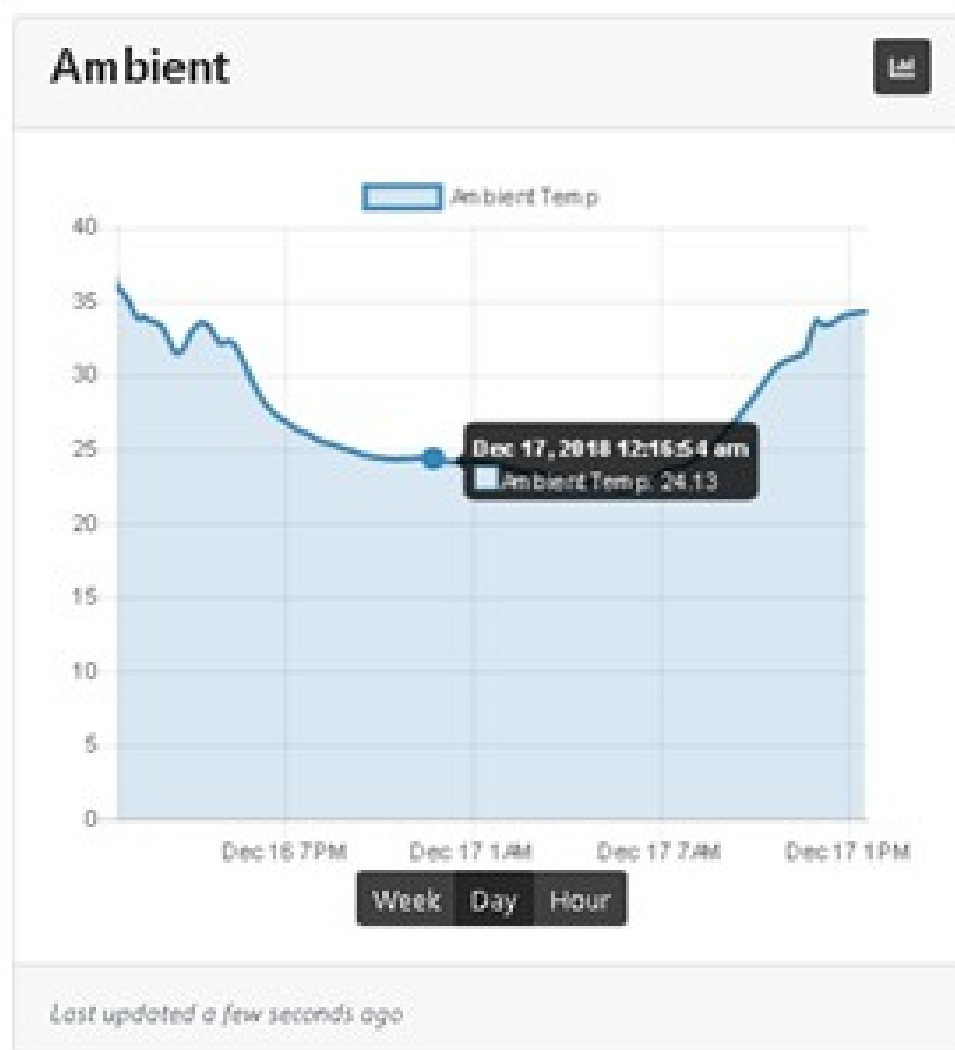


Figure 13.42. Numeric data can be shown as a line chart

13.7.2 Historical Data

To view or download historical data, press the *Raw Data* button on the top right of the dashboard. A table showing all the data associated with the selected device will be shown. To download the data,

press the *Export to CSV* button. The data will be saved to your downloads folder. The downloaded file can be opened and manipulated with any spreadsheet tool.

Raw Data

From: Oct 21, 2021 2:29 PM +11:00 To: Oct 22, 2021 2:29 PM +11:00

Load Data 145 records

Export to CSV All Columns Clear Columns Events Only

Device Date/Time × Events × Water Temperature × Speed × GPS Latitude × GPS Longitude × GPS Satellites × Engine Battery ×

Intruder Alert × Ambient Temp × Supply Voltage × Clean Water ×

Device Date/Time	Events	Water Temperature	Speed	GPS Latitude	GPS Longitude	GPS Satellites	Engine Battery	Intruder Alert	Ambient Temp	Supply Voltage	Clean Water
21/10/2021, 2:33:37 pm AEDT	[WARN] Ambient Temp : High	20.81	0.7	-32.70267	152.0676	6	12.5	0	22.96	12.36	0
21/10/2021, 2:43:48 pm AEDT	[WARN] Ambient Temp : High	20.81	0	-32.70267	152.06755	7	12.5	0	23.02	12.36	0
21/10/2021, 2:54:40 pm AEDT	[WARN] Ambient Temp : High	20.81	0	-32.70262	152.06752	6	12.48	0	23.14	12.36	0
21/10/2021, 3:04:24 pm AEDT	[WARN] Ambient Temp : High	20.94	0	-32.70264	152.06757	7	12.5	0	23.47	12.36	0
21/10/2021, 3:13:54 pm	[WARN] Ambient	21	0	-32.70251	152.06754	7	12.5	0	23.61	12.36	0

Figure 13.43. Data associated with the selected device shown in a table

Note The timestamp in the *timestamp* column is in Unix Time; if you would like a GMT date and time field, enable the timestamp setting in endpoint settings.

13.7.3 Device Level User Administration

In addition to group-level user permissions, permissions can also be managed at the individual device level. This is particularly useful when a user needs access to configure or manage a specific device without being granted administrator rights across the entire group.

To adjust device specific permissions, navigate to the device data page and click the User button. From there, you can assign or modify access for individual users as required.

Warning Anyone who has the device ID and setup password can add the device to their account with Admin permissions.

13.7.4 Configuration via Senquip Portal

Settings associated with a Senquip device can be updated remotely via the Senquip Portal. To change the settings for a selected device, press the *Settings* button on the top right of the dashboard. The selected device settings will be shown and can be changed by clicking in the relevant fields. Once a setting has been changed, press the *Save Settings* button at the bottom of the page.

Senquip devices check for settings changes each time they make a connection to the Senquip Portal. If a device is set to transmit data once an hour, then the settings will be changed up to an hour after the changes have been made on the portal. If quicker changes are required, the device will need to be visited and the changes made via the integrated webserver in setup mode.



Portal

[Upgrade](#) [Docs](#) [Account](#) [Logout](#)

Devices / Gwenie: Settings : General

ADMIN

Premium

Gwenie

General

Network

Internal

External

Endpoint

Events

Update

API

Delete

Senquip

Admin

Command Queue

General

Device ID

MR89FNUQ2

Device Model

ORB-X1-G

Firmware Version

SFW001-3.0.0

Hardware Revision

2

Device Name

Gwenie

Base Interval

600

Seconds

Transmit Interval

1

Exception Interval

1

Device Always On

☐ Enabled

Batch Transmit

☐ Enabled

Web Server

☐ Enabled

Power Input

Power Loss Alert

☒ Enabled

Hibernate on Power Loss

☒ Enabled

Hibernate Delay Intervals

20

Count Hours

☐ Enabled

AA Battery

AA Battery Low Alert

☐ Enabled

Threshold

4.8

Volts

Save Settings

Copyright ©2021 Senquip Pty Ltd. [Terms of Use](#)

Figure 13.44. Remote update of device settings via the Senquip Portal

Note In applications where power is available, a quicker transmit interval will mean that settings changes can be made more quickly.

13.7.5 Remote Firmware Updates

Senquip will routinely make firmware updates to enable new features, enhance security and fix bugs.

Device firmware can be updated via the Senquip Portal. To update the firmware, press the *Update* button on the settings page. You will be directed to a page asking for the firmware number. This number can be found in the [Device Firmware Changelist](#) on the Senquip website or through your preferred distributor.

The screenshot shows the Senquip Portal interface. At the top, there's a navigation bar with the Senquip logo, Margate Marina logo, and the word 'Portal'. On the right, there are links for Upgrade, Docs, Account, and Logout. Below this, a breadcrumb trail shows 'Devices / Gwenie: Settings : Update'. On the right side of this bar are icons for ADMIN and Premium. The main content area is titled 'Gwenie' and contains several tabs: General, Network, Internal, External, Endpoint, Events, Update (highlighted in teal), API, Delete, and Senquip. Below the tabs is a 'Command Queue' section with a refresh icon. The 'Firmware Update' section contains a form with a label 'New firmware number' and a text input field labeled 'Firmware Number'. Below the input field is a large teal button labeled 'Update Firmware'.

Figure 13.45. Remote firmware updates via the Senquip Portal

A Firmware Update typically takes about 5 minutes on Wi-Fi and 20 minutes on 4G LTE. During the update the green light will be off and the orange light will flash fast. Once the device has received the firmware update and is processing it, the lights may appear to freeze. This is normal behaviour. Please allow plenty of time for the device to finish the update and return to normal operation.

Note There is always a risk that something may go wrong during a firmware update; it is not recommended that firmware be updated unless it is suggested by Senquip or a specific new feature is required.

13.7.6 Event Reporting

The Senquip Portal allows forwarding of alert, warning, and alarm events generated on a device to email or SMS endpoints. A Hosted plan is required for this feature. Use the *Events* page on the Senquip Portal to configure event reporting. Events can be configured to be sent once as they occur, or with a daily reminder.

Warning Make sure to add `no-reply@senquip.com` to your safe senders list on your email client to prevent email events from going into spam or junk folders.

Event Reporting

Enable SMS or Email notifications of alerts, warnings and alarms below.

Emails will be sent to:

Remaining emails: **30** (Limit: 30 per month)

SMS events will be sent to:

Remaining SMS: **5** (Limit: 5 per month)

Monthly limits will reset on: **Thu Oct 26 2023 02:55:18 GMT+1100 (Australian Eastern Daylight Time)**

The following options are available for each event type:

Disabled - No notification sent for this event.

Enabled - Notification sent immediately for any new event.

Enabled with daily reminder - Notification sent immediately and every 24 hours while the event remains continuously active.

	SMS	Email
Alerts	Enabled	Enabled with daily reminder
Warnings	Disabled	Disabled
Alarms	Disabled	Disabled

[Save Settings](#)

Figure 13.46. Configure event forwarding

If an event is current, and the event escalates, for example a warning turns into an alarm, the more severe event will be forwarded. If an event is current and it de-escalates, for an example, an alarm turns into a warning, the event will not be forwarded. If a type of event is current, and a new type of event occurs, the new event will be forwarded. For instance, if a high current warning is active and has been forwarded to email or SMS, and a high temperature warning becomes active, the high temperature warning will also be forwarded.

When a device reconnects and sends buffered data, the following rules apply:

- If newer data has already been received, older buffered data is processed but no alerts are sent.
- If no newer data exists, alerts are only sent for buffered data that is less than 12 hours old.

13.7.7 Creating Custom Widgets

Users can create custom widgets that display data graphically in a way that is meaningful to the user. In the example below, the pressure and temperature of each tire on an axle is shown. In the example, the pressure on tyre 2 has dropped and so the pressure field has turned yellow as a warning to the user.

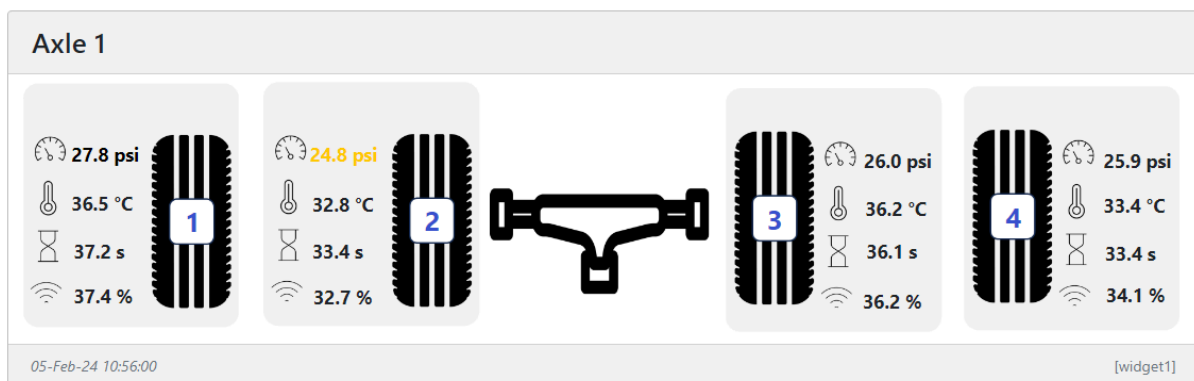


Figure 13.47. A graphical widget showing tyre status

To create a widget, select the *Display Settings* icon on the device data page and chose *Add Custom Widget* at the bottom left of the page. A new custom widget will be generated and you will be taken to the *Widget Editor* page to customise your widget. At the top of the *Widget Editor* page is your widget. It will default to a blank background with an example of how to display temperature shown. The text can be moved to a new location by clicking on it and dragging it.

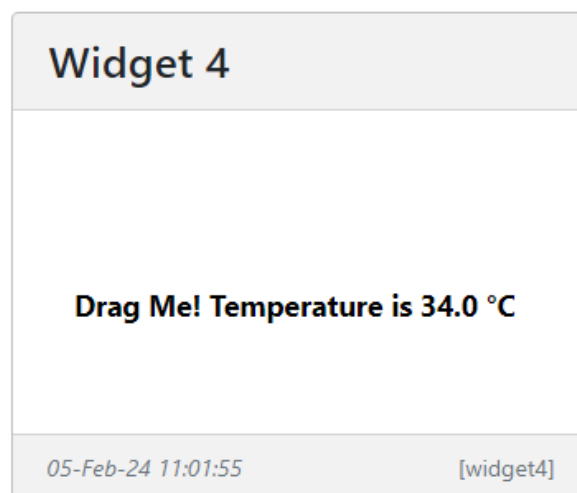
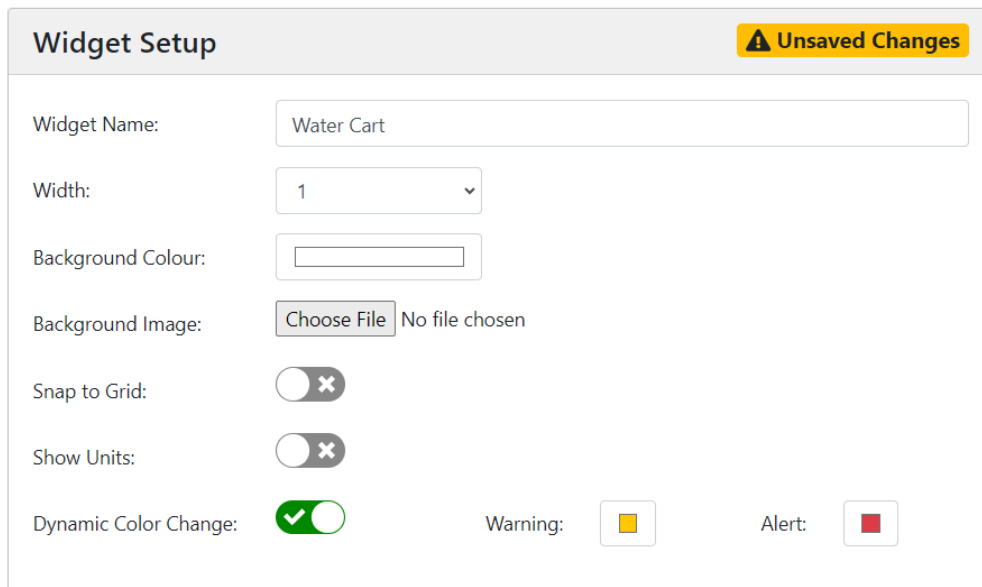


Figure 13.48. Default blank widget showing temperature

As an example, we will generate a widget that shows the level of water in a water cart. In the *Widget Setup* window, we get to name our widget with something meaningful to the user. We will name our widget "Water Cart". We can also set the width of the widget in units of a standard Senquip Portal widget. We will leave the width as 1 unit wide. A background colour can be selected and a background image loaded. We will use the *Choose File* option to load a background image of a water cart. We can choose to show the units associated with values displayed on our widget, or to leave the units off and make the units part of the background image of the text that is displayed along with the value. We will turn off showing units. Selecting *Dynamic Colour Change* automatically changes the colour of values and associated text when a warning or alarm is associated with that value. We will leave this on.



Widget Setup ⚠ Unsaved Changes

Widget Name:

Width:

Background Colour:

Background Image: No file chosen

Snap to Grid: ☐

Show Units: ☐

Dynamic Color Change: ☒

Warning:

Alert:

Figure 13.49. Settings for our water cart example

Note Remember to save your changes.

The *Widget Text* window allows us to insert text and values on the image in the widget. When you created your widget, an example text entry was created “Drag Me! Temperature is $\${data.ambient}$ ”. In this example, the text “Drag Me! Temperature is” will be displayed along with the value of the ambient temperature. The most recent value of ambient temperature is inserted in the text string by using a dollar and curly bracket, followed by the data element, in this example ambient temperature, and a closing bracket “ $\${data.ambient}$ ”. In our example, we will create a script that has a custom variable *cp20* called *Water Level*, and will use this in our example, inserting the unit kl in text as follows “ $\${data.cp20}$ kl”.

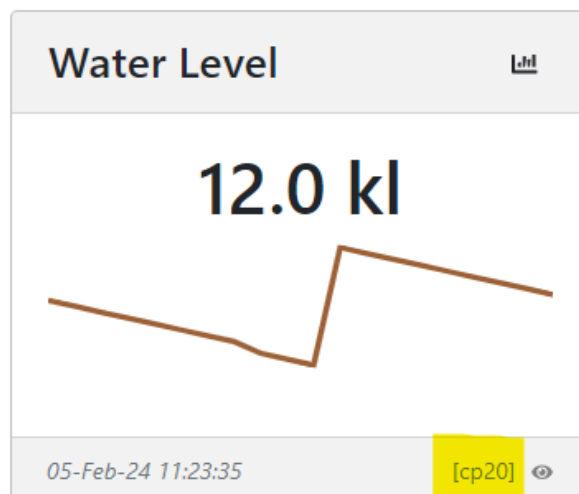


Figure 13.50. Water Level as shown on the device page.

We will choose *Bold*, *20px* font size, and will make the default colour green.

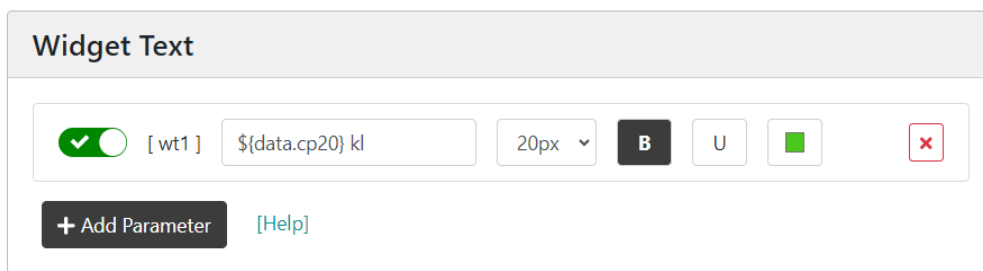


Figure 13.51. Water cart widget text settings.

Note Because we have chosen *Dynamic Colour Change*, the colour of the text will change if there is a warning or alarm current on *cp20*.

Our widget now looks like the image below.

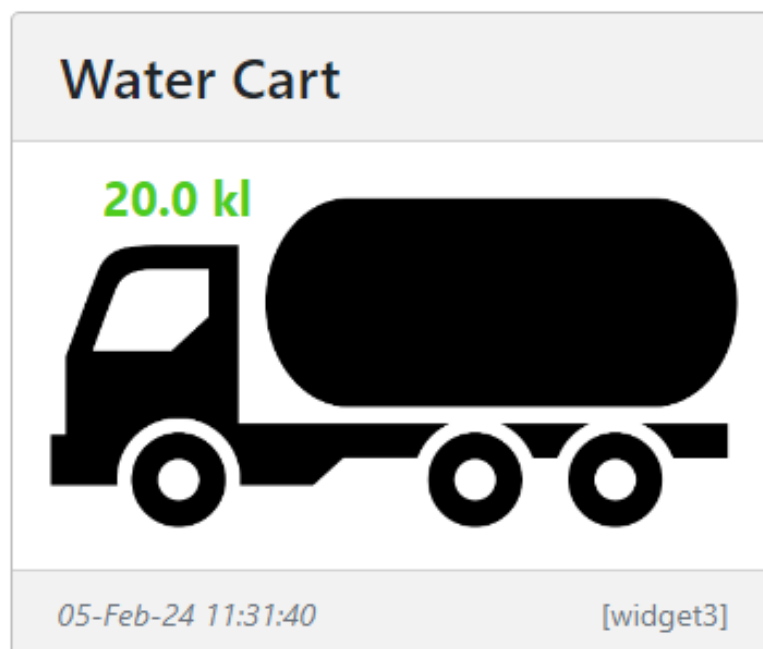
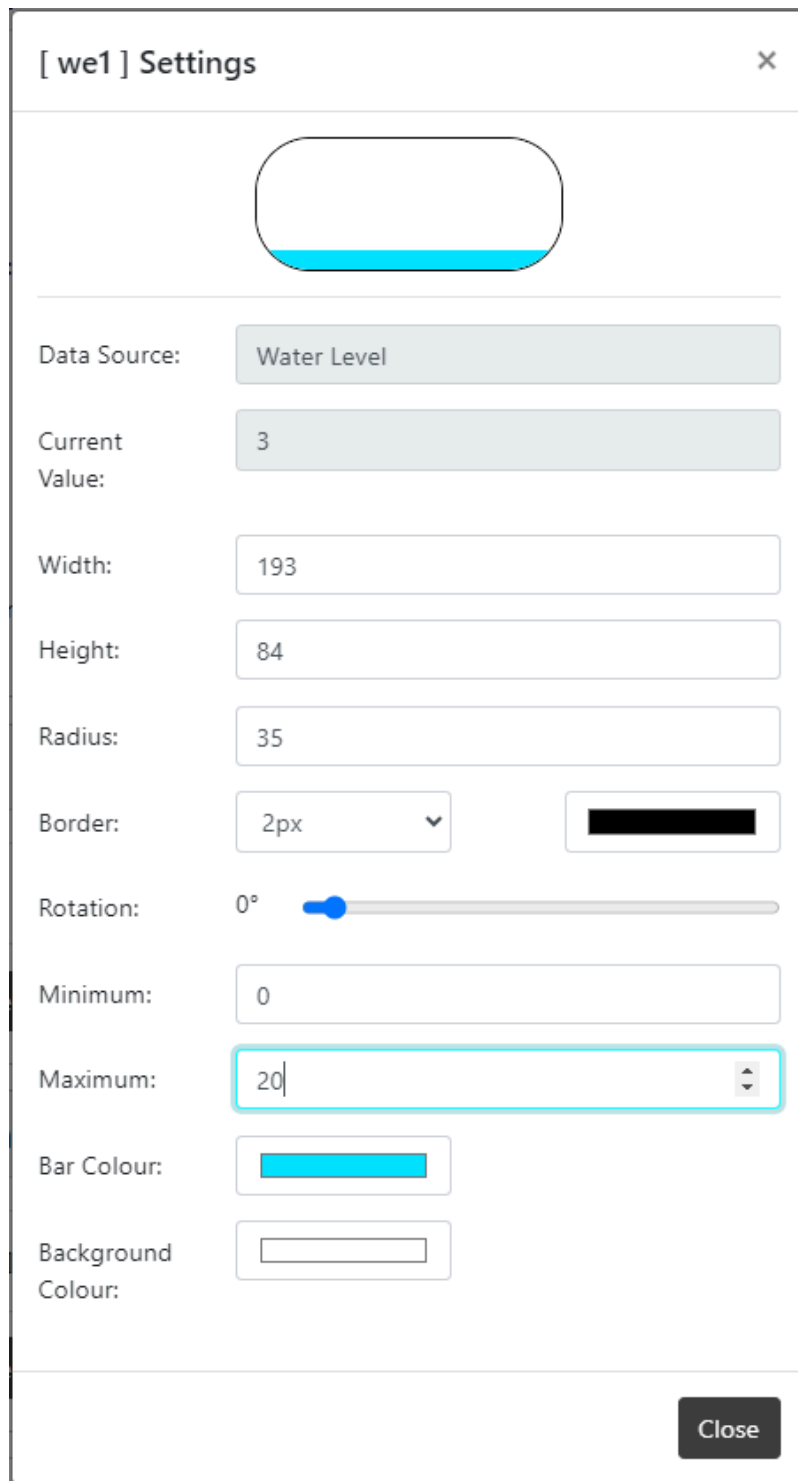


Figure 13.52. Water cart widget with water level shown in green.

We will now use the *Widget Elements* window to add a dynamic level indicator to the tank on the water truck. We will associate the level indicator with the *water level*, *cp20*, and will set the *width*, *height*, and *radius* to match that of the tank on the water truck image. Since the water level parameter created in the script has a range of 0 to 20, we will set the *minimum* and *maximum* levels of the indicator to 0 and 20.



[we1] Settings

Water Level

3

Width: 193

Height: 84

Radius: 35

Border: 2px

Rotation: 0°

Minimum: 0

Maximum: 20

Bar Colour:

Background Colour:

Close

Figure 13.53. Settings for water cart level element

We could also add a status indicator light to the image by adding a *status indicator* element. Status indicators can be associated with data values and can be set to change colour as the data value drops below a threshold.

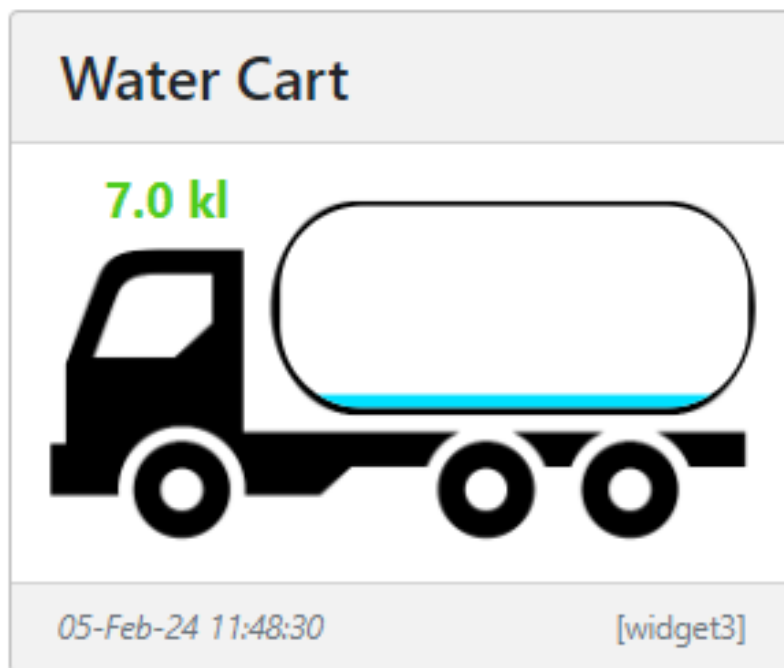


Figure 13.54. Completed water cart widget

Once saved, the water cart widget will appear on the device page alongside all the other enabled widgets.

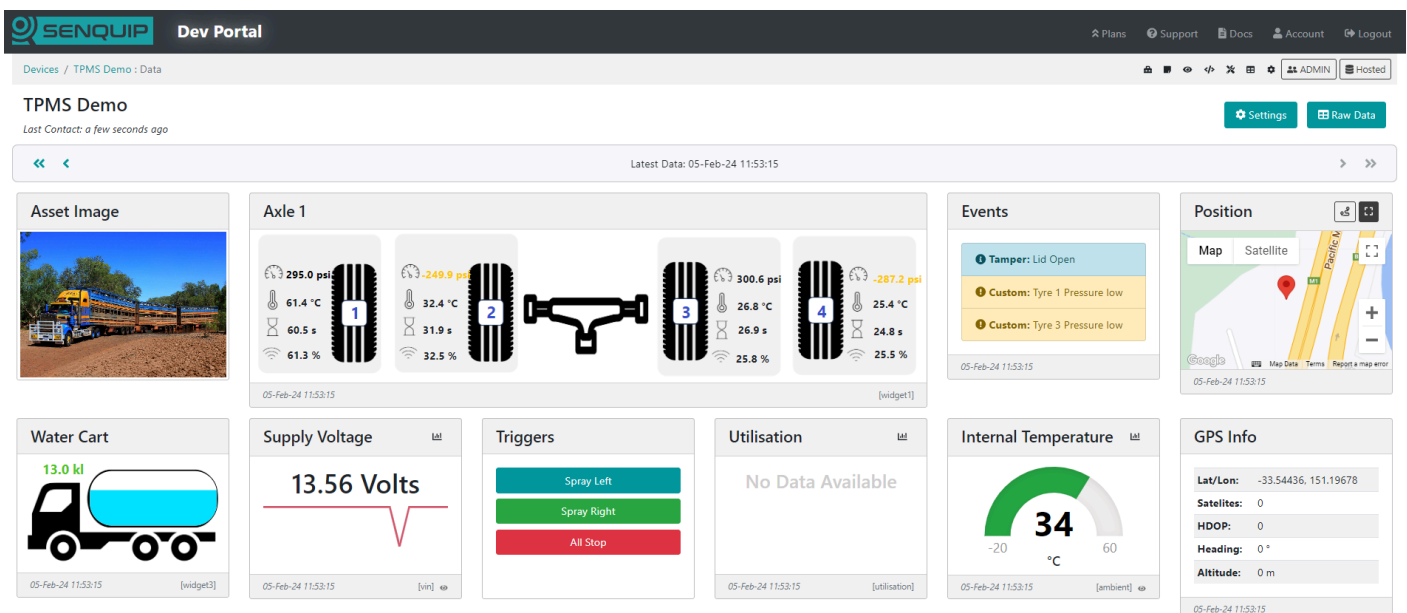


Figure 13.55. Water cart widget shown on the Senquip Portal

To edit the widget, go to the *Display Settings* page and select the widget by clicking on the widget name.

Sizing of widget images

The width of a custom widget can be chosen as 1 to 4 standard widgets in width. The height of the widget is determined by the size of the image uploaded. In the water cart example above,

the image was scaled to result in a widget that is the same height as most of the other standard widgets on the device page. This makes for a neat and consistent looking display. To create a widget the same height as most widgets on the Senquip Portal, use the following ratios for the background image.

Note The image does not have to be these exact sizes as the width will auto scale. The ratio does however need to be correct.

Widget width	Image width	Image height	Ratio
1	320	178	1.8
2	670	178	3.8
3	1020	178	5.7
4	1370	178	7.7

13.7.8 Creating Custom Charts

Users can create custom line, area, and bar charts with multiple axis, and multiple series. In the example below, the number of particles of a particular size in oil is shown on a stacked area chart, with the total of the stack indicating the total number of particles.

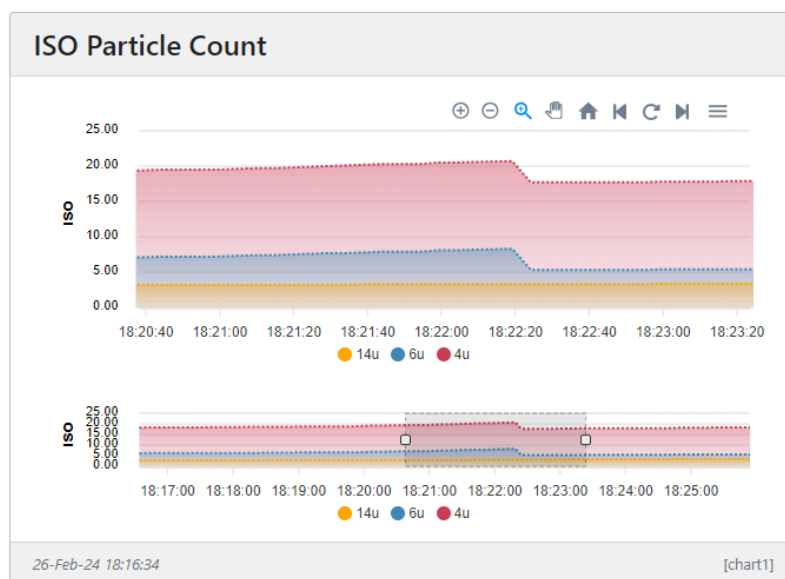


Figure 13.56. Brushed area chart showing particles in oil

Note To speed up render time, all charts are downsampled to show 1000 points across the chart. The algorithm used to downsample the chart data has been selected to retain as many of the features of the original data as possible. It is however possible that details may be missed in a highly compressed timeline.

To create a custom chart, select the *Display Settings* icon on the device data page and chose *Add Custom Chart* at the bottom left of the page. A new custom chart will be generated and you will be taken to the *Chart Editor* page to customise your chart. At the top of the *Chart Editor* page is your custom chart. It will default to a simple chart with no series.

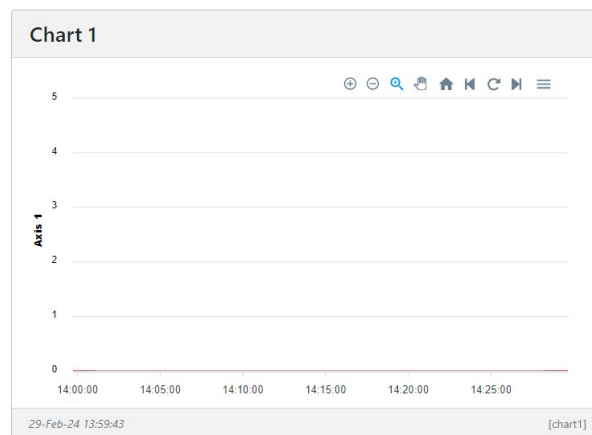


Figure 13.57. Default custom chart

We start by giving the chart a name, in this example, we will generate a chart showing temperature and pressure in a compressor and so we will call the chart “Compressor 2D”. We will choose a *Line* chart, and will give the chart a size of 2 widgets wide by 2 widgets high. We have chosen a time range of *10 minutes*. If we had selected *Brushed Chart*, a magnifying window below the chart would appear that can be dragged left and right to scroll through chart data. The earlier oil particle chart is an example of a brushed chart. If we had selected a *Stacked Series*, the values of the various series would be summed. The example of the oil particle chart is a stacked chart.

Figure 13.58. Custom chart settings

We will now add the axis to the chart. We add 1 axis for temperature and 1 axis for pressure. We have added custom minimum and maximum values for the axis but if we had left them blank, axis values would have been assigned based on the available data. The tick interval has been left blank and will be calculated automatically. One decimal place has been selected for the axis labels, and a colour has been assigned to each axis. Custom axis settings are disabled if the *Brush Chart* option is selected. Only a single axis can be added if *Stacked Series* is selected.

Chart Axis

[ax1]

Temperature

0

20

Tick

1

[ax2]

Pressure

0

30

Tick

1

+ Add Parameter

[\[Help\]](#)

Figure 13.59. Custom chart axis

We will now create a series and will assign an axis to each series. We first select the axis associated with the series. We then select a measurement. In our example, we will add compressor temperature and internal device temperature to the *Temperature* axis and pressure to the *Pressure* axis. We have selected the line type as *Solid*, have selected a line width of 2, and have chosen a colour for each series.

Chart Series

[sr1]

Temperati

Temperature

Solid

2px

[sr2]

Pressure

Pressure

Solid

2px

[sr3]

Temperati

Internal Temper

Solid

2px

+ Add Parameter

[\[Help\]](#)

Figure 13.60. Adding series to a custom chart

Note Remember to save your settings.

We have now generated our first chart.

13.7. Device Data Page

153

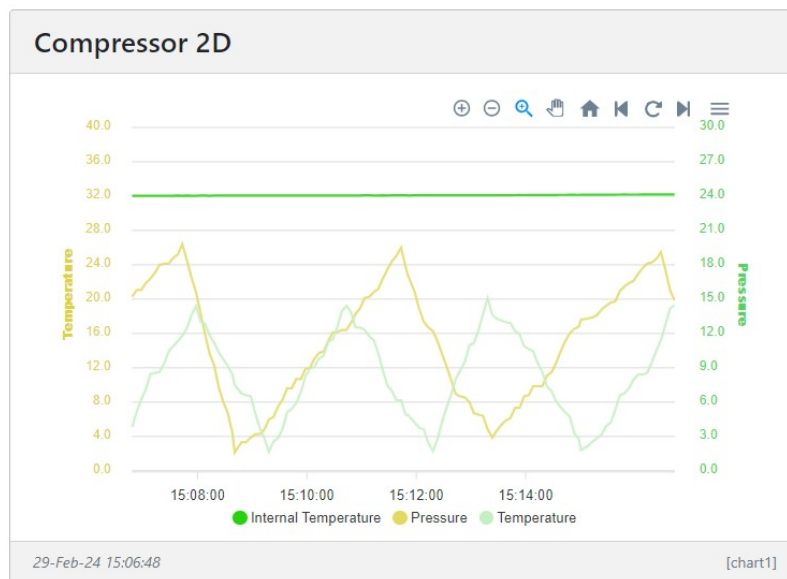


Figure 13.61. Example chart showing generator temperature and pressure

The charts offer controls for zooming, panning, loading previous and new data, and enhancing a zoomed area. The enhance option is provided so that the user can zoom into an area and then select the option to load more data from the server to enhance the chart where the downsizing algorithm may have smoothed detailed features.

The process for creating a bar chart is similar except that the data to be displayed must be sent from the Senquip device as an array of numbers. The array must be turned into a JSON string object before being dispatched. Each element of the array represents the height of the associated bar.

Example - Reading a Vibration Profile and displaying it as a bar chart.

The following vibration chart was created by reading 128 frequency bins from a vibration sensor and sending them as a stringified array. The required code is summarised below. Also in the example below, a goal value within which the vibration profile must remain is dispatched to the Senquip Portal. The goal data is static (does not change often), therefore it does not need to be dispatched on every cycle. To set a series as a goal, use the *Mark as Goal* option in the chart series menu.

[illegible]

A single y axis is generated and vibration and goal data are added as series.

Note The *Mark as Goal* option is ticked to load historic goal data when current values are missing, avoiding the need to resend unchanged data in every packet.

Chart Y-Axis

[ax1]

Vibration

Min

Max

Tick

2

+ Add Parameter

[Help]

Chart Series

[sr1]

Vibration

Vibration Profile

Mark as Goal

[sr2]

Vibration

Goal Profile

Mark as Goal

Bar chart series require data to be sent from the device as a stringified JSON array of numbers.

X

+ Add Parameter

[Help]

Figure 13.62. Example bar chart showing a vibration profile and goal

Vibration

01-Aug-25 09:57:29 [chart2]

Figure 13.63. Example bar chart showing a vibration profile and goal

Example Machine load statistics on a bar chart

13.7. Device Data Page

155

In this example, *states* are used to track how long a pump operates within specific load ranges. These ranges are grouped into bins: 0–25%, 25–50%, 50–75%, and 75–100%. The percentage of time the pump spends in each bin is calculated, and the results are displayed in a bar chart.

```
// Create a load chart
let load25 = [];
let load50 = [];
let load75 = [];
let load100 = [];

// Simulate some data
load25[0] = 20 + 3*Math.random(); // 0 to 25
load50[0] = 30 + 3*Math.random(); // 25 to 50
load75[0] = 30 + 3*Math.random(); // 50 to 75
load100[0] = 100-load25[0] - load50[0] - load75[0];

SQ.dispatch(31,JSON.stringify(load25));
SQ.dispatch(32,JSON.stringify(load50));
SQ.dispatch(33,JSON.stringify(load75));
SQ.dispatch(34,JSON.stringify(load100));
```

A single y axis is specified, and each bar is loaded as a separate series.

The screenshot displays the configuration interface for a bar chart. It is divided into two main sections: 'Chart Y-Axis' and 'Chart Series'.

Chart Y-Axis: This section contains a toggle switch labeled '[ax1]' which is turned on. Below it, there are input fields for '% in Range', 'Min', and 'Max'. The 'Tick' field is set to '2'. At the bottom of this section are buttons for '+ Add Parameter' and '[Help]'.

Chart Series: This section contains four series configurations, each with a toggle switch, a '% in Range' dropdown, a range selection dropdown, a color swatch, and a 'Mark as Goal' checkbox.

- sr1:** Range '0-25', orange color swatch.
- sr2:** Range '25-50', purple color swatch, with a red 'X' icon.
- sr3:** Range '50-75', dark purple color swatch, with a red 'X' icon.
- sr4:** Range '75-100', blue color swatch, with a red 'X' icon.

 At the bottom of this section is a light blue warning banner that reads: 'Bar chart series require data to be sent from the device as a stringified JSON array of numbers.' Below the banner are buttons for '+ Add Parameter' and '[Help]'.

Figure 13.64. Configuration for bar charts

A stacked bar chart may provide a better visual representation of the data rather than the standard bar chart.

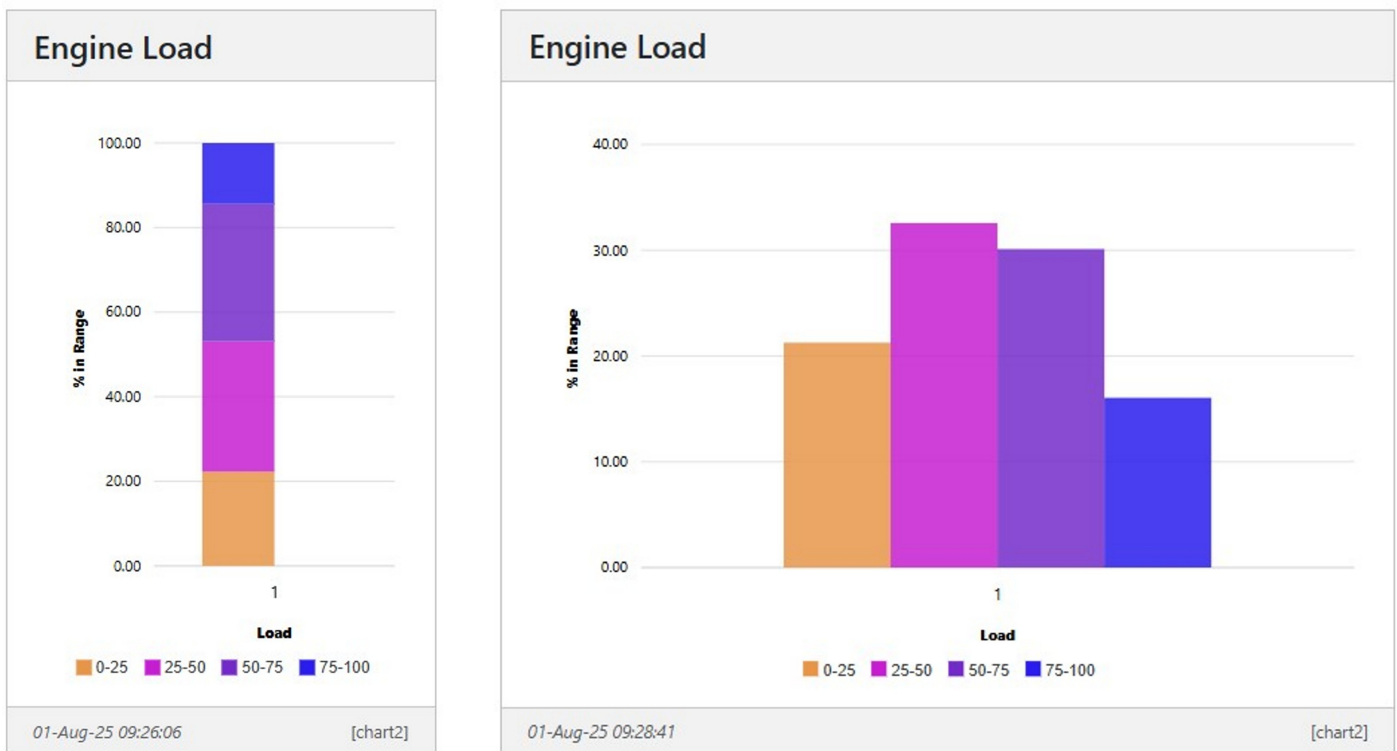


Figure 13.65. Stacked and regular bar chart showing percentage of time the pump operated within each load range.

13.8 Management and Hosting on the Senquip Portal

The Senquip Portal offers hosting of data, a data visualisation dashboard, firmware upgrades, and device management including remote configuration and scripting. Every Senquip device purchased comes with a *managed* plan for the life of the product (10 years). *Managed* plans allow remote configuration and scripting on the Senquip Portal. Users have the option of purchasing a *hosted* plan to enable data hosting and data visualisation on the Senquip Portal. Hosted plans are available on a monthly, yearly, or lifetime basis (10 years), and can be purchased directly off the Senquip Portal or through distributors.

13.8.1 Basic

Zero cost *Basic* plans are most suitable for users who are hosting their data on their own server and have their own dashboards. Features of the management plan include:

- Configure devices from the Senquip Portal
- Connection to a private server
- View current data
- 5 Minute updates to the Senquip Portal
- Device scripting
- Access for 3 users
- Firmware updates

13.8.2 Hosted

Hosted plans are for users who will use the Senquip Portal to store and visualise their data. Features of the hosted plan include:

- Configure devices from the Senquip Portal
- Connection to a private server
- View current and historical data
- 5 second data update limit
- 2 years of data storage
- Device scripting
- Senquip Portal access for 50 users
- Firmware updates
- Export raw data
- Trigger remote actions
- Create custom data widgets
- Create custom charts
- Device to device messaging
- 300 email alerts per month
- 100 SMS alerts per month
- Senquip Cloud API access
- AEMP API access

Note Every device includes 90 days of hosted access from the date of activation.

For the most up to date feature list and to purchase a hosted plan, please visit the [Senquip Portal](#) or contact your preferred distributor.

13.8.3 Adding or Cancelling a Hosted Plan

To add a hosted plan to a device, a user must have a payment method associated with their Senquip Portal account. Billing details are accessed by selecting *Account* from the toolbar at the top of any page on the Senquip Portal.

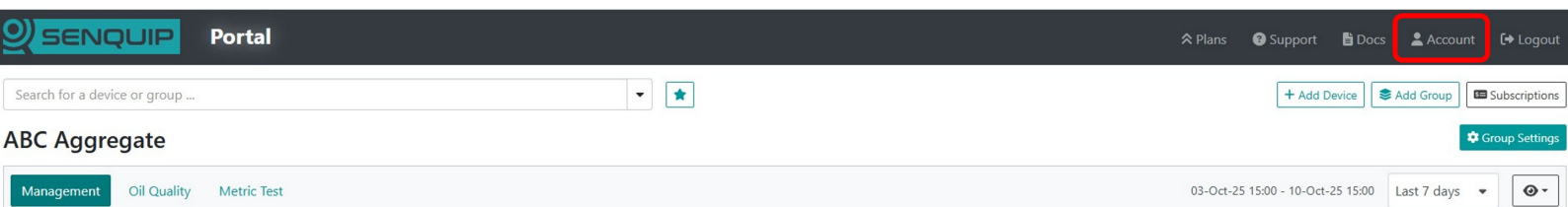


Figure 13.66. Select Account to setup billing details

To add a payment method select *Billing Details*. If no billing detail exists, a warning banner will be displayed.

Billing Details

Billing Name: ABC Enterprise

Billing Email: user@example.com

Billing Address: 1 Sydney Place
Sydney
NSW 2000 AU

Customer ID:



No payment method has been set. A payment method is required for Portal Hosting plans.

Hosting plans for the Senquip Portal are provided by Senquip Pty Ltd and payments are securely processed by Stripe.

Edit Billing Details or View Invoices

Figure 13.67. A warning is shown if there is no payment method available.

Select *Edit Billing Details or View Invoices* and then select *Add payment method*.



Senquip Billing Portal

← Return to Senquip Pty Ltd

PAYMENT METHOD

No payment method.

+ Add payment method

Figure 13.68. Select Add Payment Method.

Enter card details and press *Add*.

Add payment method



Card



AU Direct Debit

Card number

1234 1234 1234 1234





Expiration date

MM / YY

Security code

CVC


123

Country

Australia

By providing your card information, you allow Senquip Pty Ltd to charge your card for future payments in accordance with their terms.

Notwithstanding the logo displayed above, when paying with a co-branded eftpos debit card, your first payment and all future debit payments may be processed through either card network.

You can review important information from Senquip Pty Ltd on their [Terms of Service](#) and [Privacy Policy](#) pages.

Add

Go back

Figure 13.69. Add a payment method.

Note Hosting plans for the Senquip Portal are provided by Senquip Pty Ltd and payments are securely processed by Stripe. Senquip does not store credit card details.

Once a payment method is available, users can add hosted plans to their subscription.

To add or cancel hosting on devices:

- from the Senquip Vision Dashboard, select *Subscriptions*

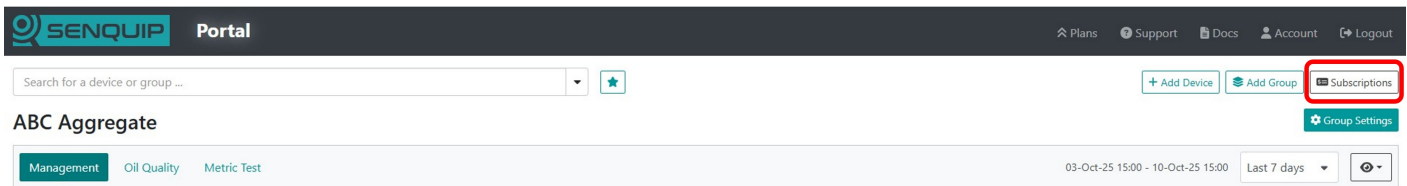


Figure 13.70. Select the subscriptions module

- From the Accounts page, select *Subscriptions* and then *Manage Subscriptions*

Users can use the subscriptions page to:

- confirm which devices are already on hosted plans
- confirm which devices are paid for on your account
- check the expiry date of hosted plans
- Add or cancel hosted plans

Filter and then select devices to be hosted or for which hosting is to be cancelled

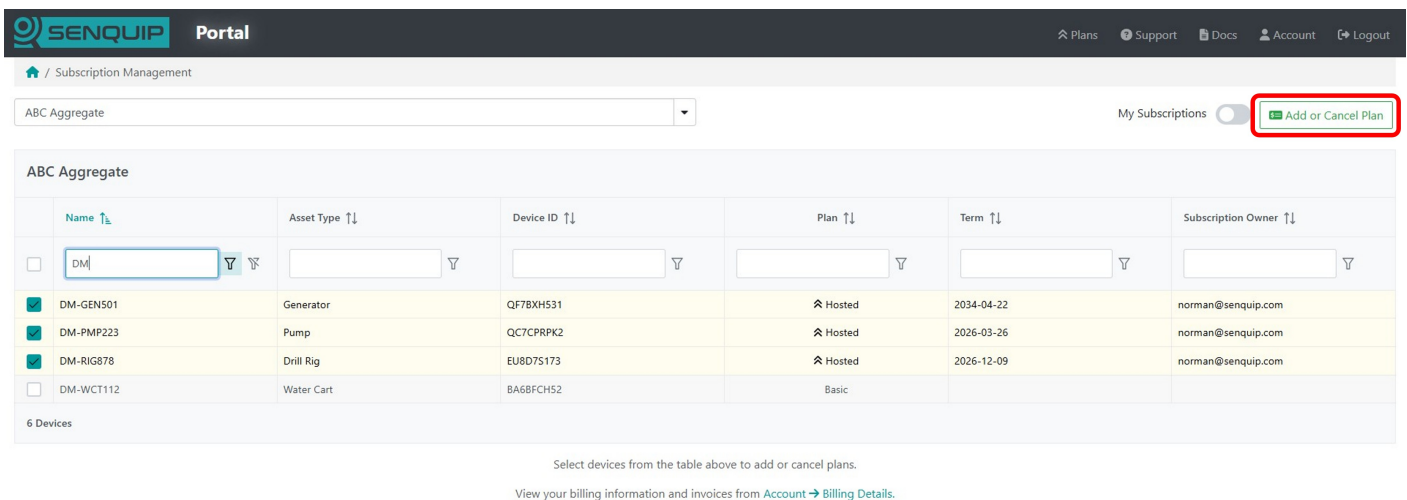


Figure 13.71. Select devices to be hosted or for which hosting is to be cancelled.

On the top right, select *Add or Cancel Plan*. A summary of the current plans for each device is shown.

- To add hosting to a device currently on a basic plan, select *Hosted*.
- To cancel the hosted plan on a device, select a *Basic* plan for that device.

Change Plans

Chosen devices:

Name	Device ID	Current Plan
DM-PMP223	QC7CPRPK2	Basic
DM-GEN501	QF7BXH531	Basic
DM-RIG878	EU8D7S173	Basic

Select the new plan type:

Hosted

Select the Hosted plan term:

Monthly

This is an ongoing subscription service per device.
The minimum term is 1 month.
You can cancel at any time before next renewal date, but no refunds will be given.

Devices will be upgraded to the Hosted plan, effective immediately.
Your Monthly subscription will be updated, and your payment method charged. [Terms of Use](#)

 To avoid multiple charges: select all devices requiring upgrade before proceeding, rather than upgrading one by one.

Hosted Plan price per device:

AUD \$7.50 / month (plus tax)

Cancel Change to Hosted

Figure 13.72. Make a selection to change plans

When adding hosting, select either *Monthly* or *Yearly*. A discount is given for yearly subscriptions.

- To host devices, select *Change to Hosted*
- to cancel hosting and return devices to a basic plan, select *Change to Basic*

Note Plans can be cancelled at any time. The cancellation will be immediate and no further billing will take place. Refunds will not be issued when a plan is cancelled mid term.

Note If a hosted plan is added in the middle of a month, a pro-rate payment for the balance of the month will be invoiced. Once one hosted plan has been added, further hosted plans will be billed on the same date as the first plan.

Warning Where plans are cancelled, any data stored on the Portal for these devices will be lost.

13.8.4 Changing Billing Details

You can update the credit card used for billing at any time through the Senquip Portal.

Updating Your Credit Card

1. Log in to the Senquip Portal at <https://portal.senquip.com/> using your account credentials.
2. In the Portal, click *Account* (typically located at the top-right of the page).
3. Select *Billing Details*.
4. Click *Edit Billing Details* or *View Invoices*. This will open the Senquip secure payment portal.
5. In the secure payment portal you can:
 - *Add a payment method* to enter a new credit card, or
 - *Remove an existing card* by clicking the **X** next to that card.
6. Enter your updated credit card details and save.

Security and Permissions

Senquip uses a secure third-party payment processor (Stripe). Credit card details are *not stored on Senquip servers*.

If you cannot see the *Billing Details* page, your account may not have sufficient permissions. Billing changes typically require *Administrator* access.

13.8.5 Replacing a User Who Has Left

When a staff member leaves an organisation, their access to Senquip devices should be removed and transferred to another user.

If your devices are organised into a Group, replacing a user is simple:

1. Create a Senquip Portal account for the new user if they do not already have one.
2. Add the new user to the Group with the required permissions.
3. Remove the previous user from the Group.

All devices in the Group will automatically inherit the updated permissions.

If the device is **not** part of a Group, the new administrator must be added to each device individually. This can be done in one of two ways.

If the device setup password is available:

1. Create a Senquip Portal account for the new user.
2. Select **Add Device** and enter the Device ID and setup password.
3. The device will be added to the new user's account with ADMIN permissions.
4. Open the device page and select ADMIN to remove the previous user.

If the previous administrator's Portal login is available:

1. Create a Senquip Portal account for the new user.
2. Login using the previous administrator's account.
3. Open the device page and select ADMIN.
4. Add the new user as an ADMIN.
5. Remove the previous user.

6. Login using the new user's account to verify access.

Tip For organisations managing multiple devices, it is recommended that devices are placed into Groups. User access can then be managed at the Group level, allowing staff changes to be made once rather than on every individual device.

Mechanical Specification

TODO

TODO

Maintenance

The Senquip UNI-Z1 has been designed to require a minimum of maintenance. The only serviceable item is the internal LTO backup battery.

15.1 Replacing the LTO Battery

TODO

Battery replacement instructions

Frequently Asked Questions

16.1 Introduction

This document is a collection of responses to questions that are commonly asked by new users of the Senquip telemetry devices. If you cannot find an answer to your question below, please contact us at support@senquip.com. [Table of Contents](#)

16.2 Senquip Portal

16.2.1 I created an account but did not get a confirmation email.

Almost certainly our confirmation email has been blocked by your company server or is in your junk or spam folder. We do see that approximately 2% of accounts are created with incorrect email addresses and so it is possible that you have entered an incorrect email address. If the problem persists, contact support@senquip.com and we will manually confirm your account.

16.2.2 Do I need a hosted subscription to remotely configure my device?

No. The purchase of a Senquip device entitles the owner to make configuration changes, perform firmware updates and view data using the Senquip Portal for the life of the device.

16.2.3 Do I need a hosted subscription to perform firmware updates?

No. The purchase of a Senquip device entitles the owner to perform firmware updates using the Senquip Portal for the life of the device.

16.2.4 Can I view data on the Senquip Portal for free?

Yes, you can view data on the Senquip Portal on a free basic plan. Updates to the Senquip Portal may be limited to 5 minute intervals and the data will not be stored for more than a day.

16.2.5 I cannot see historical raw data on the Senquip Portal.

If your device is on a free basic plan, Senquip will not store more than 1 day of historical data. Continuous backups of data storage becomes expensive so is feature of hosted plans where data will be saved for 2 years. Updating a device plan to hosted can be done on the Senquip Portal by using the subscriptions facility.

16.2.6 What payment methods are available for Hosted Portal plans?

Payment methods vary by region and include Credit Card, Direct Debit, Google Pay, Apple Pay, and

others.

16.2.7 Do I have to use the Senquip Portal to view my data?

Senquip devices can send measured data to any endpoint via UDP, HTTP, and MQTT. Data transfers can be secured through the upload of customer certificates to the device.

16.2.8 Can I completely disconnect from the Senquip Portal?

Yes. To stop sending data to the Senquip Portal, unselect the Send Data to Senquip Portal option in the endpoint settings. To stop configuration settings from the Senquip Portal unselect Configuration via Senquip Portal. Further settings updates will have to be done using the Senquip webserver.

16.2.9 Does Senquip have access to my data?

No. Unless you give a Senquip employee access to a device by giving them view, operator, user, or admin status, Senquip employees will not be able to view your data. Sometimes, you may give a Senquip employee access to your device so that they can assist you in setup. As an administrator, you can remove this access at any time.

16.2.10 Can I secure proprietary scripts?

Yes. You can use the lock feature on the Senquip Portal to lock scripts so that only you can access the content of the script.

16.2.11 I am getting a network error when I try to login to the Senquip Portal

The Senquip Portal requires accurate time to correctly secure your connection. If the time on your PC is out by more than a few minutes, you will get a network error. Correct the time on your PC and retry.

16.2.12 I have added a measurement in the settings, but the widget is not showing in the portal.

Browsers typically cache most of the elements in a webpage. Refresh your Chrome or Edge browser by: * Hold down Ctrl and click the Reload button. * Or Hold down Ctrl and press F5. Check that the widget has not been turned off in the portal display settings. To turn on (or off) a widget, press the eye icon on the device page and select which widgets you would like to show, and the order in which you want to show them. Remember to refresh your browser.

16.2.13 There are measurements missing in the data stored on the Senquip Portal.

When a Senquip device tries to connect to a network but cannot, it will retry several times and then discard the measured data and return to sleep. If you would like data to be stored when there is no coverage, select the Offline Buffer option in endpoint settings. If the transmit interval is different to the base interval, the measurement that coincides with the Transmit Interval is the one that will be sent. If you would like the measurements taken on every base interval to be stored, select the Batch Transmit option under general settings.

16.2.14 I have logged into the Senquip Portal but there is no data showing.

Measurements will only show on a device page in the Senquip portal once a device has published measurements to the portal at least once. When you receive a new device, it will be in freight mode, and it will not have published data to the Senquip Portal. Power the device to exit freight mode, configure the network settings and the device will start to publish data at the specified Base Interval.

16.2.15 I have changed a setting on the Senquip Portal, but the Senquip device has not changed behaviour.

When a setting is changed on the Senquip Portal, it is added to a queue that is stored until the device next makes contact. To see if a setting has been applied by a device, press the command queue button at the top of each settings page. Settings changes shown in green have been applied. For remote configuration using the Senquip Portal to be possible, the Configuration via Senquip Portal option must be selected in the endpoint settings.

16.2.16 I have many Senquip devices and I am struggling to identify them.

Once you have many devices installed, it can be difficult to identify which Senquip device is performing which function. It is highly recommended that each device is named using the Device Name setting when first installed and that devices are added to logical groups on the Senquip Portal. If a device has not been named and it needs to be identified, turn the GPS on to determine its location.

The columns on the device summary page can be customised to show key data for a group of assets. You may, for instance want to show fuel level, utilisation and alerts on the summary page.

16.2.17 How can I increase the number of users on a device?

Devices with hosted plans can have up to 50 users attached to each device. Take out a hosted plan by selecting the subscriptions button on the device summary page, or by contacting your distributor. For more detail on hosted plans, see: [Hosted Plans](#).

16.2.18 How can I find the IMEI number for a Senquip device?

The IMEI number is available on the device diagnostics page for all mobile enabled devices.

16.2.19 How can I find the IMSI and ICCID number for the SIM in a Senquip device?

The IMSI and ICCID are related to the SIM in the Senquip device and will be available on the diagnostics page if a SIM is inserted and the SIM responds to the ICCID and IMSI request commands.

16.2.20 Is my data secure?

Yes. To ensure the highest levels of security, Senquip devices are pre-loaded with unique client certificates allowing for immediate, out-of-the box, secure communication with the Senquip Portal. Users can load additional certificates to allow secure communications with other endpoints.

Data stored on Senquip device is encrypted using AES256 encryption.

16.2.21 Can I use symbols and characters as units on the Senquip Portal?

Yes. To use symbols like the degrees symbol (°) as in °C, create the text in an editor such as Microsoft Word or Notepad and copy it into the field in the Senquip Portal. Alternatively, use the alt code for the symbol you need, for instance, ALT 0167 for the ° symbol.

16.2.22 I can't add a user to a device.

To add a user to a device, you must have administrator privileges for that device. For a user to be added to the Senquip Portal, they must have activated an account on the portal. To add a user, from the device page, press the Users icon in the top right. Enter the email address with which the user has signed up to the Senquip Portal. Select the user permissions as Admin, User and Read. If the email address entered is not associated with an activated account on the Senquip Portal, an error will occur, and the user will not be added.

16.2.23 How do I change the payment details for my subscriptions?

You may want to change your payment method when, for instance, your credit card has expired and you need to add an updated version. To change payment details, login to the Senquip Portal and select the *Account* option at the top right to navigate to your account page. Select the *Billing Detail* option and then press the *Edit Billing Detail or View Invoices* banner. This will take you to the secure payment portal from where you can add payment methods by pressing *Add payment method* and delete payment methods by pressing the cross next to each payment method.

16.2.24 Where can I find copies of invoices for subscription payments?

Login to the Senquip Portal and select the *Account* option at the top right to navigate to your account page. Select the *Billing Detail* option and then press the *Edit Billing Detail or View Invoices* banner. This will take you to the secure payment portal where invoice history can be seen at the bottom of the page. Click on an invoice to open the details of that invoice and to download a copy.

16.2.25 Will I get a warning from Senquip before my hosted plan expires

Yes, you will get an email reminder 30 days and 5 days before your hosted plan expires. Please make sure to add Senquip to your trusted email address list to avoid the reminders going into your junk or spam folders.

16.2.26 How much data can I download?

Each *Raw Data* download is limited to 50MB. For more data, it is recommended to use the API.

16.2.27 Sorting of my *All* group is only sorting the first 10 entries.

The sort functionality is limited to the first page when the *All* category is chosen. This is to prevent delays when a user has hundreds of devices in their *All* group. Create your own groups to execute the sort function correctly.

16.3 Network

16.3.1 I have inserted a SIM card, but the device is not connecting to the network.

Senquip devices that use 4G networks need to be configured with an Access Point Name (APN). The APN is unique to each mobile service provider and should be known by the provider of the SIM. Sometimes a username and password are also needed for a SIM. To configure SIM settings, use the device network settings page.

Later versions of firmware for Senquip devices include a feature called Auto-APN. With Auto-APN, the Senquip device reads data off the SIM and searches a database to try and find a suitable APN. If successful, the Senquip device will connect directly to the network.

Senquip produces devices for 4G LTE CAT-M1 and 2G, 3G, 4G CAT-1 networks. CAT-M1 is a newer protocol supported by most networks and delivers extended range from a given 4G tower. Make sure that the 4G network that you are using supports CAT-M1, sometimes referred to as CAT-M.

16.3.2 What is Auto-APN?

Later versions of firmware for Senquip devices include a feature called Auto-APN. With Auto-APN, the Senquip device reads data off the SIM and searches a database to try and find a suitable APN. If successful, the Senquip device will connect directly to the network.

16.3.3 My APN is not on the list of Auto-APN options.

If you have a SIM card for which Auto-APN does not work, please contact support@senquip.com to have your service provider details added.

16.3.4 How do I know which Senquip variant I should use in my country

Senquip offers two variants of each device, for instance ORB-C1-G and ORB-C1-H. The -G product is for use on 4G LTE CAT-M1 networks, and the -H product is for use on 2G, 3G, 4G LTE CAT-1 networks. If your country has CAT-M1, use it as you will get a range improvement.

You can check for CAT-M coverage using the official global coverage map found here: [Mobile IoT Deployment Map](#)

16.3.5 Can I have a PIN on my SIM

No, the SIM must not have a pin. You can remove a pin from a SIM by inserting it in your phone. Here is a guide on how to remove a PIN from a Vodafone SIM: [Turn use of PIN on or off](#).

16.3.6 Why does Senquip prefer to operate on the 4G LTE CAT-M1 network?

Senquip supports 2G, 3G, 4G, and 5G LTE networks. We prefer to use the 4G and 5G LTE CAT-M1 service where available.

3G networks are being turned-off in many counties including Australia and New Zealand from 2020. 4G and 5G networks are capable of very high-speed data transfer that is not required for IoT devices. The designers of the networks realized this and introduced IoT specific services NB-IoT and CAT-M1. These services use lower power and achieve extended ranges, meaning longer battery life and better coverage in buildings and remote areas. Senquip prefers 4G and 5G CAT-M1 over NB-IoT as the prior has data rates that allow for in-field updates and the technology allows roaming between towers in mobile applications.

16.3.7 I cannot see my Senquip device on my local Wi-Fi network.

If you know a Senquip device IP address on your local Wi-Fi network, then you can login to the device webserver provided it is active. The webserver will only be active in setup mode unless the *Web Server* option has been selected in general settings.

The webserver will be inactive if the Senquip device is sleeping, to prevent the device sleeping, select the *Device Always On* option in general settings.

The webserver will be disabled if 4G communication options have been chosen as it is a significant security risk to leave the webserver active when operating on an open network.

16.3.8 I am not sure if my Wi-Fi network is reliable enough.

Wi-Fi networks can be affected by the number of transceivers, the geometry of the site and the way in which a Senquip device is mounted. To receive information of the quality of the connection made by a Senquip device, enable the Report Network Info option in endpoint settings. You will be able to map network coverage using this feature.

16.3.9 What SIM card should I use?

Senquip devices use a Micro SIM. The SIM can be either 1.8V or 3.3V. The SIM needs to be for an operator that supports either a CAT-1 (-H devices) or CAT-M1 (-G devices) network. Nano SIMs with adapters should not be used as the SIM card can become loose in the carrier, damaging the SIM holder.

For volume applications, Senquip can provide devices with SIM cards that are soldered to the PCB during manufacture. Soldered SIMs are more reliable in high vibration environments.

16.3.10 Why does Senquip not allow the webserver to be on when operating on an LTE network?

When a Senquip device is operating on a public LTE network, it will receive an IP address that is open to the internet. If the webserver is enabled, the device may be exposed to malicious attacks by automated *bots* that will try to break the password and gain access to the Senquip device. By turning off the webserver, the risk of attack is eliminated.

16.3.11 I have been using the hotspot on my phone to test Senquip devices and it is not working anymore.

The Wi-Fi Hotspot feature available on most smartphones is typically limited to between 3 and 5 active device connections. Once this limit is reached, the smartphone will not allow further devices to connect. We note that on some newer smartphones, this limit has been increased to 10. We also note various work arounds to increase this limit.

16.4 GPS / GNSS

16.4.1 Is the Senquip GPS compatible with other GNSS networks?

Yes, the Senquip GPS will receive data from GPS, GLONASS, Bei Dou, Galileo, and QZSS satellites. Senquip uses the term GPS instead of the more correct GNSS because it is more commonly understood.

16.4.2 I have enabled GPS but I am not seeing any GPS data.

To provide GPS data such as position, and speed of satellites, Senquip devices need to connect to satellite constellations. Ensure that the device is mounted in a location where the device has a clear view of the sky, not through metal. Ensure that the device is mounted with the cable gland down.

In poor reception areas, the device may require additional time to acquire satellite data. Try increasing the GPS Max Time to 240 or even 360 seconds in poor reception areas.

16.4.3 Can I attach a GPS or 4G antenna to my Senquip device?

No. The Senquip device has all required antennas internal to the device. This has been done specifically as Senquip devices are expected to be used in harsh conditions where antennas would be damaged. If you need an external antenna, please use a Senquip QUAD.

16.4.4 How accurate is the GPS on my Senquip device?

With a clear view of the sky, the position accuracy of the GPS is better than 2.5m 50% of the time, and better than 5m 95% of the time.

GPS position accuracy depends on many factors such as the mounting position, orientation, visibility of the sky, weather conditions and time of day. The best position accuracy will always be obtained when the Senquip device is mounted vertically in a position where it has a clear view of the sky. To enhance GPS position accuracy, the Senquip devices track GPS, GLONASS, Bei Dou, Galileo and QZSS satellites.

16.5 Measurements

16.5.1 My Modbus readings are failing regularly on RS485.

RS485 networks require 120 Ohm termination resistors at each end of the main run of the network.

Turn on the *Termination Resistor* in *Serial* settings.

16.5.2 My CAN bus data is sometimes corrupted.

CAN Bus networks require 120 Ohm termination resistors at each end of the main run of the network. Ensure that 120 Ohm resistors are in place on your network.

16.5.3 I sent a CAN message and it is spamming the bus.

The CAN protocol will automatically resend CAN messages if they are not acknowledged by a device on the network. Ensure that there is a second CAN device on the network.

16.5.4 I'm powering a Modbus device from a current source on a Senquip device but it takes a while to boot.

Newer firmware versions on SFW002 and greater will delay Modbus reads until the *Start Time* on the Source or IO pin has elapsed. This allows time for externally powered Modbus and other sensor to boot or stabilise measurements.

16.5.5 Modbus float values are only to 2 decimal places.

By default, the Modbus peripheral sends float values with 2 decimal places of precision. To increase this, use the calibration option. For instance, 1.23456V will be dispatched as 1.23V without calibration and 1234.56mV with calibration (0-1 in gives 0-1000 out). If, in the example, you have to have the result shown in Volts, use a script to dispatch the scaled version with the required number of decimal places.

16.5.6 I have enabled IO voltage measurements but there is no data shown

This could be because the *Measurement Time* on the IO is longer than the *Base Interval* and so the measurement cycle is ending before the IO is measured. Reduce the *Measurement Time* or increase the *Base Interval*.

16.6 Power

16.6.1 Do I need to add AA batteries as a backup in a solar installation?

No. Senquip devices have an internal LiPo battery which, in most solar applications, will be sufficient to power the device during the night and in low sunlight conditions. In low power configurations, the internal LiPo battery can power a Senquip device for months. Use the battery calculator on the Senquip website to estimate how long the internal battery will power your solar setup.

Senquip devices report the internal LiPo battery voltage. It is recommended that the LiPo battery be monitored for a while after a solar install to ensure it is being sufficiently charged by the solar panel.

AA batteries are only required in applications where there is no permanent or solar power available. They can be added as an additional backup when using permanent or solar power.

16.6.2 I am running on solar and am losing data at night and on cloudy days.

It is likely that your solar panel is not supplying enough energy to power your application and charge the Senquip device internal LiPo battery. Monitor the LiPo battery voltage on the Senquip Portal. A charged battery will reach approximately 4.2V. A low battery is below 3.5V.

The simplest way to extend battery life is to increase the Base Interval in general settings.

16.6.3 How can I extend battery life on my Senquip device?

A Senquip device should be able to last for many years running on AA batteries. To estimate

the life of your device, see the battery calculator on the Senquip website. For low power installations such as solar and battery installs, to save energy, consider the following:

- Increase your Base Interval. In applications where measured data is not changing quickly, you may be able to increase the base interval. A longer base interval means that the Senquip device spends more time sleeping between measurement intervals and so saves energy.
- Increase your Transmit Interval. In some applications you may not need every measurement that is taken to be reported but are more interested in receiving an alert when a warning or alarm condition occurs. In these cases, increase the transmit interval so that data is not transmitted on every measurement interval. Once a day measurement may be enough.
- Turn off peripherals that are not needed. If you are not using the serial port, GPS or other peripheral, make sure that they are turned off.
- Reduce the interval of peripherals. A Senquip device mounted on a pole is unlikely to move. One GPS update a day may be sufficient. The GPS, serial and current sources are the most power-hungry peripherals, use them sparingly.
- Consider using voltage sensors instead of current sensors. Sensors like liquid level sensors are often available in current or voltage versions. A 4-20mA sensor will draw 20mA at full scale whereas a voltage version may only draw 1mA. Where using the serial and current sensors, reduce the wait times before measurement and before returning to sleep.
- Make sure that the device is not always on, and that the webserver is off.
- Under endpoint settings, do not send human readable time and network info. The smaller the set of data you send, the lower the power of your device. Send to a single endpoint if possible.
- Senquip is constantly working on code improvements to reduce the power of devices. Make sure that your device is running the most recent firmware version.

16.6.4 I wired my Senquip device incorrectly; have I damaged it?

Senquip devices have protection against the most common wiring faults like reversing the voltage. There are some inputs such as the serial, current sense and thermocouple inputs that can be damaged if connected to supply voltages.

16.6.5 Do I need a fuse in-line with the power supply of my Senquip device?

It is always a good idea to include a fuse in the supply to any electronic device. A 1A fuse would be a suitable size for use with the Senquip device.

16.6.6 I have opened my Senquip device, and the lights are not on.

Your device is most likely sleeping; this is good as it conserves power. The lights will come on when the device next wakes for a measurement cycle. If you want to access the device immediately, press the setup button to access the device webserver or press reset to initiate a re-start that will trigger a measurement cycle. If you want to be able to access your device to make settings changes at any time, select the *Always On* option in the general settings.

16.6.7 The device that I am setting up via the webserver keeps switching off.

The device webserver is activated by pressing the setup button and then connecting to the device Wi-Fi. The device will exit the webserver when settings are saved and it executes a reset, when the lid is closed or when no activity is detected for a few minutes. To ensure that the webserver does not close-down when you are configuring a device, make sure that you do not cover the device light sensor and that you are not inactive for extended periods of time.

16.6.8 Can I use AA NiCd batteries in my Senquip device?

NiCd batteries are generally rated at 1.2V. Although the Senquip device will operate from 1.2V batter-

ies, they will not last very long. It is recommended to use high quality Alkaline or Lithium batteries. For longest life, use 1.6V or 3.6V lithium batteries.

16.6.9 Can I use 3.6V lithium batteries in my Senquip device?

Yes. 3.6V Lithium Thionyl Chloride batteries are generally the longest lasting when used with a Senquip device. The improvement in life is however small when compared with lower cost Lithium Energizer and other brand batteries that are widely available.

16.6.10 How long will the internal LiPo battery in the Senquip device last?

The lithium battery is expected to last 5 years without significant degradation. The life of the battery may be reduced if it is exposed to temperatures above 55°C or below -10°C, if it experienced an unusually high number of charge/discharge cycles or if it is left in a discharged state for an extended time. Spare LiPo batteries can be sourced from Senquip and can be replaced by a qualified technician.

16.6.11 I have received my Senquip device, pressed the setup button and nothing happens.

When Senquip devices are shipped, they are placed in freight-mode to preserve the internal battery and to prevent the device from transmitting when being transported. To exit shipping mode, apply power or insert batteries.

16.6.12 How long can I run my Senquip device off AA batteries?

To achieve maximum life, use high quality Lithium batteries such as Ultimate Lithium from Energiser. Battery life will depend entirely on your application, the rate of measurement, transmissions and the types of sensors attached. As a guide, if your Senquip device was to be left sleeping, it could achieve up to 10 years of life. In a typical battery powered application, where the Senquip device is communicating over GSM, with once per hour updates, the Senquip device can be expected to last 2 years on a set of batteries. The Senquip device can be configured to monitor its batteries and report low battery conditions.

Use the battery calculator available on the Senquip Portal to estimate the battery life of your system.

16.6.13 Why is my AA battery voltage reading lower than I expect?

If you have inserted four 1.5V AA batteries into your Senquip device, you would expect the battery voltage shown on the portal to be 6V. It may sometimes instead show 5.5V. There is internal resistance in your battery so that when current is drawn from it, the measured voltage drops. If, for instance, the Senquip device was drawing energy from the AA batteries to charge the internal battery when a measurement was made, the measured battery voltage would be slightly lower than 6V. There is also a small amount of protection circuitry between the battery and the measurement circuit and again, we would expect a small drop across this circuitry.

16.6.14 I haven't used my device for a while, and it is taking a long time to make a first connection.

If you leave a device unpowered for an extended time and you have set the Senquip device in a high-power mode by for instance setting a fast update rate, the internal LiPo battery will have run flat. When the Senquip device first receives power, it evaluates the internal LiPo battery and if it is found to be extremely flat, the Senquip device will pre-condition the LiPo before resuming normal operation. If you open the lid during pre-conditioning, you will see the green light pulsing slowly during pre-conditioning.

16.6.15 How do I make a Senquip device safe for shipping?

Put the device in freight mode. In freight mode, the battery drain is reduced to almost zero and all transmitters are turned off. Enable freight mode via the webserver, on the Senquip Portal in

the Admin page, or from setup mode by pressing the setup button 3 times.

The device will exit freight mode when power is applied or batteries are inserted.

16.6.16 Will my ORB enter hibernate mode if AA batteries are installed

Yes, hibernate mode, if enabled, is triggered when the supply voltage drops below 9.5V whether the device is powered with AA batteries or not. Hibernate can be disabled in the *General* settings.

16.7 Setup

16.7.1 If I perform a factory reset, will I lose my settings?

Yes. A factory reset will remove all your settings including your network settings. After performing a factory reset, you will need to connect to the device via the internal webserver to re-establish an internet connection.

16.7.2 I performed a factory reset and I cannot remember a setting.

Go to the settings page for the device and open the command queue at the top of the page. You will be able to see a log of previous settings applied to the device.

16.7.3 If I perform a firmware update, will I lose my settings?

No. Performing a firmware update preserves your settings. If the firmware update introduces new settings, these will be set to the default value. Note that updates to major firmware revisions may reset some variables such as non-volatile variables used in scripts and hour meters.

16.7.4 Can I save my settings to a file?

Yes. You can export your settings, scripts and Senquip Portal settings to a file using the export settings option in the admin settings. Before exporting your settings, you will need to use the Request Device Settings option to get the latest settings from the Senquip device.

16.7.5 Can I save settings to another device?

Yes. Use the Import Settings option in the admin settings to import settings from another device.

16.7.6 I have lost my password, what can I do?

If you have lost the original device password, please contact support@senquip.com who will assist you in recovery.

If your device is connected to your Senquip Portal account, you can continue to view device data and make configuration changes. If you have changed your password, and have forgotten your new password, a factory reset will restore the original device password.

16.7.7 How long does a firmware update take?

The time taken to perform a software update depends on the network type chosen and the signal strength of the connection. A typical update over Wi-Fi will take 5 minutes and an LTE update will take 15 minutes. The orange light will flash during the update process. If the upload is interrupted, it will need to be restarted. A failed firmware upgrade will not harm the Senquip device.

16.7.8 If a firmware update fails, will my Senquip device be harmed?

No. If a firmware update fails, your Senquip device will not be harmed. The Firmware update will need to be restarted.

16.7.9 My device is not accepting a firmware update.

In some instances with short base intervals and lots of data being transmitted, the Senquip device may not have the capacity to process a firmware update. In this instance, reduce the base interval to 60 seconds and then apply the firmware update. Once complete and with the device reporting the new firmware version, change the base interval back to the required rate.

16.7.10 How can I force a Senquip device to accept a change made on the Portal if it is sleeping?

Since the device will not contact the Senquip Portal during sleep, no changes can be made until the next transmit interval. To force a device to make immediate contact, press the reset button. After reset, contact is made with the Senquip Portal, and any outstanding settings will load. This is most useful when you have set a long sleep period and want to test a quick change before deployment.

16.7.11 I have enabled the webserver in *General* settings but I loose contact with it every few minutes.

The webserver will be terminated when the device enters sleep mode between measurement cycles. To keep the webserver on, select *Device Always On* in the *General* settings.

16.7.12 Android phone will not stay connected to device webserver.

Phones always attempt to connect to the best available Wi-Fi network. Since the Senquip device hotspot does not have internet access, it is not considered a good network and the phone switches to an alternate network. This behaviour can be disabled on Android phones by accessing Wi-Fi settings >> Intelligent Wi-Fi and turning off the option to *Switch to Better Wi-Fi Networks*.

16.8 Operation

16.8.1 Is the time on my Senquip device accurate?

Yes. At boot, the Senquip devices connects to an available network and queries time from NTP server pool.ntp.org. If an NTP server is not available, the device will try to retrieve time from the LTE network and failing that, from the device GPS. Both the NTP server address and check-in interval can be changed using **Settings >> Network >> Advanced*.

16.8.2 How often is time synchronised on a Senquip device?

Senquip devices renew their time sync every 12 hours. Time between refresh is maintained by a crystal derived source in the device.

16.8.3 Why does the first measurement after a reset take longer?

After a reset, a Senquip device needs to load the operating system into memory, configure itself and load user settings. This can take a few seconds.

16.8.4 My device does not go to sleep between measurement cycles.

The minimum time between cycles that warrants the device going to sleep depends on the network settings and peripherals enabled. For instance, if you have GPS enabled and a base interval of 1 minute, the device will not go to sleep because it would likely take longer to re-acquire satellites than the 1 minute sleep time. These are the minimum base intervals that will allow the device to go to sleep:

Parameter	Specification
Operating on Wi-Fi	10 seconds
Operating on LTE	120 seconds
GPS enabled	180 seconds (or the <i>Max Time</i> specified in <i>GPS</i> settings)

16.8.5 When my device wakes from hibernate, will it perform measurements before returning to sleep?

Yes, waking from hibernate is considered a normal measurement cycle and all enabled measurements will be performed. If, in a script, a timer is enabled for a future time, the device will not wait for that timer to trigger before returning to hibernate.

16.9 Scripting

16.9.1 Does my script run in the Senquip Portal?

No. Your script will run on the Senquip device in field. This means that your script will continue to execute even if your device loses contact with the network.

16.9.2 How do I get access to scripting?

Administrators of devices have access to device scripting.

16.9.3 I cannot see the scripting icon on the device page.

To request access to scripting you need to be an administrator for the device.

16.9.4 How can I tell if there is an error in my script?

Limited error detection is available real-time in the scripting page. For feedback on why a script that looks ok in the editor has failed, turn on Send Errors in the scripting window. Errors will show up as script events in the events widget on the device page.

16.9.5 My script looks ok in the editor but is failing to run.

The most common source of problems with scripts is the use of JSON keys that do not exist. If, for instance, GPS speed is used in a script, but the GPS loses satellite lock, the GPS speed key will no longer be available. When the script tries to use GPS speed, the script fails. Use a function like `if ((typeof obj.analog1 === "number"))` to check that a variable exists and is of the correct type before using it.

16.9.6 If my script fails, with my Senquip device fail?

Maybe. In general, if a script fails to end correctly, the script will terminate, and the device will continue to run. Scripting is an advanced feature, and an incorrectly written script can cause a Senquip device to fail or even brick a device. Read the scripting guide carefully before committing a script.

16.9.7 My script looks ok, but I get a calling non-callable error.

Your script may be trying to use a function that is not available in the version of firmware that you are using. Update to the latest firmware version before using scripting.

16.9.8 Can I perform bitwise operation in a script.

Yes, see the application note on bitwise operation.

16.9.9 I'm not seeing the latest script that is loaded in my device.

Empty the cache on your browser. You may need to enable developer tools and do a hard reload of your cache (In Google Chrome, enable developer tools, right click on the refresh icon).

16.9.10 Does a device factory reset erase my script?

Yes, all settings are reset to defaults including wiping of your script.

16.9.11 Can you dispatch custom variables from within a timer function?

Yes, this functionality has been added to newer firmware versions of SFW002 and higher.

Glossary

jubilee-clips

A Jubilee-clip, also known as a hose clamp, is used in conjunction with the supplied brackets when pole mounting the ORB-X1.

certificate-authority

A certificate authority (CA) is a trusted entity that issues digital certificates, which are data files used to cryptographically link an entity with a public key. Certificate authorities are a critical part of the internet's public key infrastructure (PKI) because they issue the Secure Sockets Layer (SSL) certificates that web browsers use to authenticate content sent from web servers.

ASCII

American standard code for information interchange. Developed by American National Standards Institute (ANSI), it is the most common code used by computers to translate text (letters, numbers, and symbols) into a form that can be sent to, and understood by, other computers and devices such as modems and printers.

LTE-M1

LTE Cat M1 is a low-power wide-area (LPWA) air interface that lets you connect IoT and M2M devices with medium data rate requirements (375 kb/s upload and download speeds in half duplex mode). It enables longer battery lifecycles and greater in-building range, as compared to standard cellular technologies such as 2G, 3G, or LTE Cat 1

3G & 4G

3G was the first "high speed" cellular network, and is a name that refers to a number of technologies that meet IMT-2000 standards. 4G is the generation of cellular standards that followed 3G, and is what most people use today for mobile cellular data. You can use 3G and 4G for IoT devices, but the application needs a constant power source or must be able to be recharged regularly.

MODBUS

Modbus RTU is an open, serial (RS-232 or RS-485) protocol derived from the Master/Slave architecture. It is a widely accepted protocol due to its ease of use and reliability. Modbus RTU is widely used within Building Management Systems (BMS) and Industrial Automation Systems (IAS). This wide acceptance is due in large part to MODBUS RTU's ease of use.

JSON

JavaScript Object Notation (JSON) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications (e.g., sending some data from the server to the client, so it can be displayed on a web page, or vice versa).

NIST

The National Institute of Standards and Technology (NIST) is a physical sciences laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

LTO

A lithium titanate (LTO) battery is a type of rechargeable battery that uses lithium titanate as the anode material. LTO batteries are known for their high power density, long cycle life, and more extreme temperature tolerance compared to other lithium-ion batteries.

LiPo

A lithium polymer battery, or more correctly lithium-ion polymer battery (abbreviated as LiPo), is a rechargeable battery of lithium-ion technology using a polymer electrolyte instead of a liquid electrolyte.

MQTT

Message Queuing Telemetry Transport (MQTT) is a lightweight, publish-subscribe network protocol that transports messages between devices. It is designed for connections with remote locations where a small code footprint is required and/or the network bandwidth is limited. MQTT is commonly used in IoT applications for its efficiency and simplicity.

Symbols

3G & 4G, 183

A

ASCII, 183

C

certificate-authority, 183

J

JSON, 183

jubilee-clips, 183

L

LiPo, 184

LTE-M1, 183

LTO, 184

M

MODBUS, 183

MQTT, 184

N

NIST, 183

