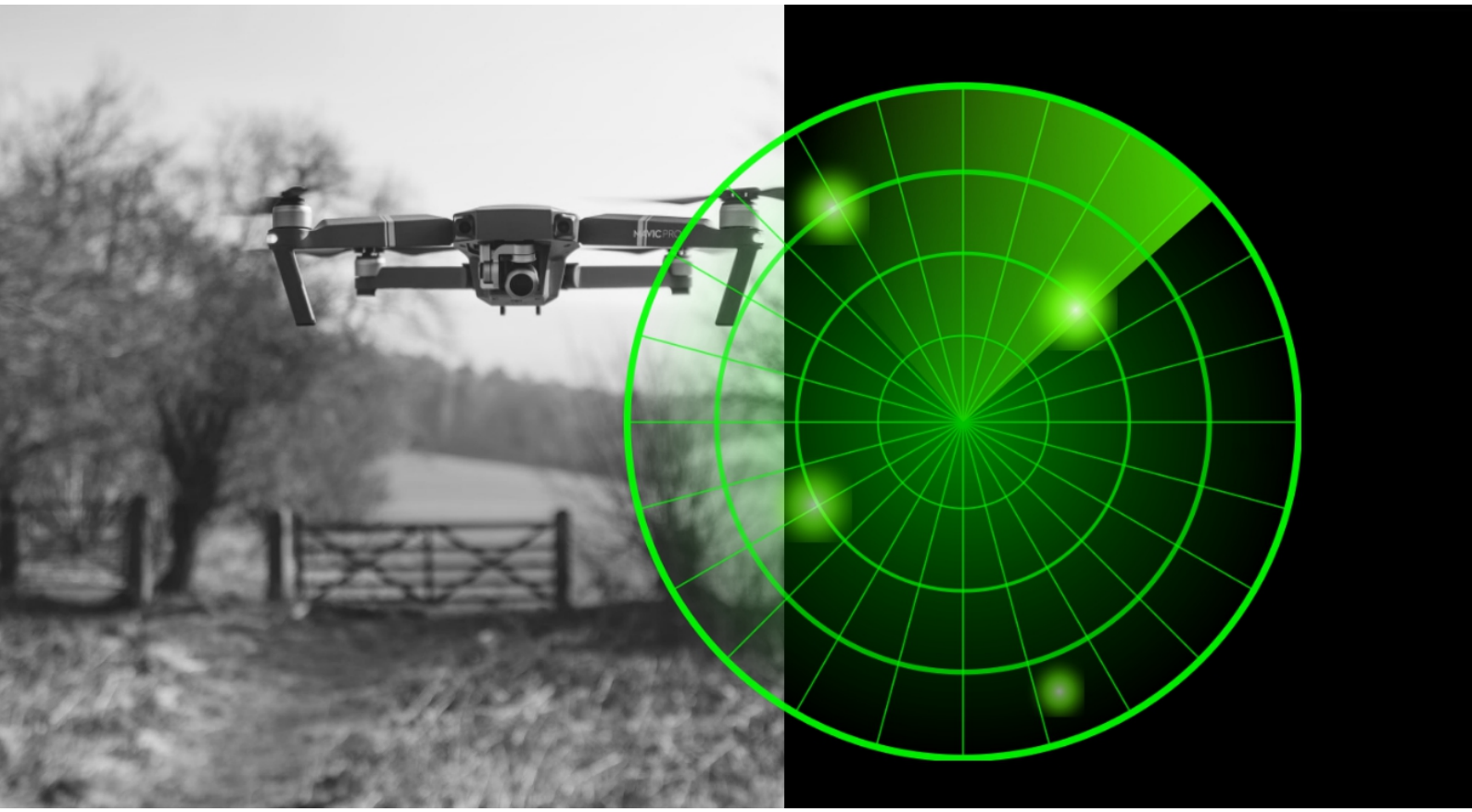
DroneScout - User Manual

November 2021 - version 1.1



The latest version of this manual is located here:
https://download.bluemark.io/dronescout_user_manual.pdf

Intended audience: system integrators, security intelligence firms, professional users with an IT background

Disclaimer: we are not responsible or liable for errors or incomplete information in this document.

Version history

version	date	description
0.9	September 2020	● Initial release
1.0	April 2021	● Adding missing parts ● Updated document with new portal and sensor version
1.1	November 2021	● Updated document with the features of the latest firmware release (web-interface)

Contents

1 INTRODUCTION

1.1 What is it?

DroneScout is a product to detect (consumer) drones near your house or other objects of interest by detecting the wireless signal between drone and remote controller/pilot. Focus of *DroneScout* is on consumer drones (quadcopters) with a live video feed. The product consists of sensors that are installed in the area of interest and a portal for managing sensors and generating alarms.

1.2 Drone detection

There is a large variety of drones: air, water, ground. *DroneScout* focuses on drones that have a wireless *video link* between drone and pilot/remote controller. Those are the ones that affect your privacy most and also transmit continuously wireless video signals (and control signals).

Detection algorithm

DroneScout scans the RF spectrum for drone signals. The detection algorithm identifies RF sources that both suddenly appear and moving. The product does not try to decode the wireless signal, instead it relies on the basic characteristic of a moving RF source.

Consumer drones transmit wireless signals in the 2.4 GHz band and the 5.8 GHz band. The preferred wireless band for drones is 2.4 GHz, as the transmission range is the largest. The 5.8 GHz is typically used as alternative ban. In case there is a lot of RF interference/signals in the 2.4 GHz band, such as in dense urban areas with many WiFi networks, the drone switches to the 5.8 GHz band.

DroneScout is also able to detect control signals, however the detection range for such signals is much less; up to 100 meter due to the lower transmit power.

WiFi interference

WiFi networks use the same 2.4 GHz band. The 5.8 GHz band on the other hand is rarely used by WiFi networks. Nearby WiFi networks will limit the detection range of *DroneScout* as the drone signal needs to be *stronger* than the signal of the WiFi network ('noise floor'), otherwise it can't be detected. It means that the *DroneScout* sensor should be installed at a location where only weak WiFi signals are present. (I.e. the signal strength of nearby WiFi networks should be less than -95 dBm.) In that case, the sensor has maximum detection range. Of course, most drones will try to use the most empty channel for communication, so one strong WiFi network won't affect the performance much. However, the drone and remote controller will determine the best channel based on *their* location, which is different from the sensor location. So there may still be a probability that the drone chooses the frequency of your nearby WiFi network.

Bluetooth interference

Bluetooth signals use also the 2.4 GHz band. Compared to WiFi, Bluetooth uses the whole 2.4 GHz band; it hops very fast to a new channel. WiFi on the other hand has a fixed channel. It means that Bluetooth does not affect much the detection range of DroneScout. Only active Bluetooth connections within 25 meter of the sensor may reduce the maximum detection range to some extend.

2 PRODUCT

DroneScout is a product to detect consumer drones near your house or other objects of interest by detecting the wireless video signal between drone and remote controller/pilot. The product consists of sensors that are installed in the area of interest and a portal for generating alarms and managing sensors.

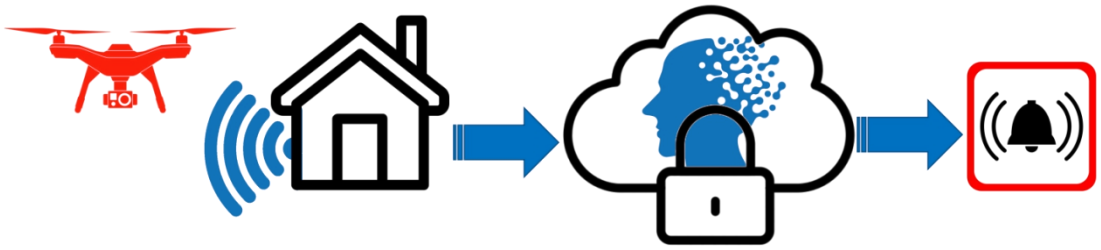


Figure 1 - How does it work? Detect the wireless signal of the video link between drone and remote controller and send it to the portal for generation of alarms.

Sensor

The sensor (DS100) is a device that detects the wireless drone signal. It needs power and internet using PoE (Power over Ethernet/802.3af). For the object of interest you can use one or multiple sensors and divide them into *zones*. For instance use sensor A detect drones in the zone *garden*. And use sensor B for detection in zone *main entrance*. The range of the sensors depends on the type.

Portal

The main purpose of the platform is to generate alarms and manage sensors.

Alarms

DroneScout offers two kinds of alarms. First, there is the daily briefing via mail, that gives an overview of detected drones in the last 24 hours. It is also possible to receive real time alarms via MQTT. MQTT is a popular publish/subscribe protocol for sensor data. (See http://mqtt.org/ for background information.) To receive real time alarms you need to have a MQTT client and subscribe to the alarm topic. For most platforms (*Windows*, *macOS*, *Android*, *iOS*) there are MQTT clients available.

3 SENSOR

The standard hardware is the DS100 sensor. The internal building blocks are a dual-band antenna, a so-called SDR (software-defined radio) and an embedded processing platform to analyze/process the RF signals and generate alarms.

The size of the sensor is 27.2 x 27.6 x 9.6 cm, weight around 1.4 kg (with mast mount 1.9 kg) and the power consumption is less than 5 W. It is powered via Power over Ethernet (PoE, 802.3af). Furthermore, the sensor acts as DHCP client in the network. The network name is the serial number that is printed on back of the sensor(ds0xxxxx) e.g. ds000101.

3.1 Installation

Location - The sensor detects drones from all directions, it is *omnidirectional*. The range is up to 1 km. The detection range can be reduced in the portal. For installation, it is therefore important not to install sensors near the border of the detection area, but instead in the center. It also depends a bit on the situation. If you have nearby WiFi networks, you don't want the sensor nearby it as the WiFi signal will reduce the detection range. Basically, install the sensor away from areas where there are signals in the 2.4/5.8 GHz band or large nearby objects (house) that can block detection of signals/drones from that direction.

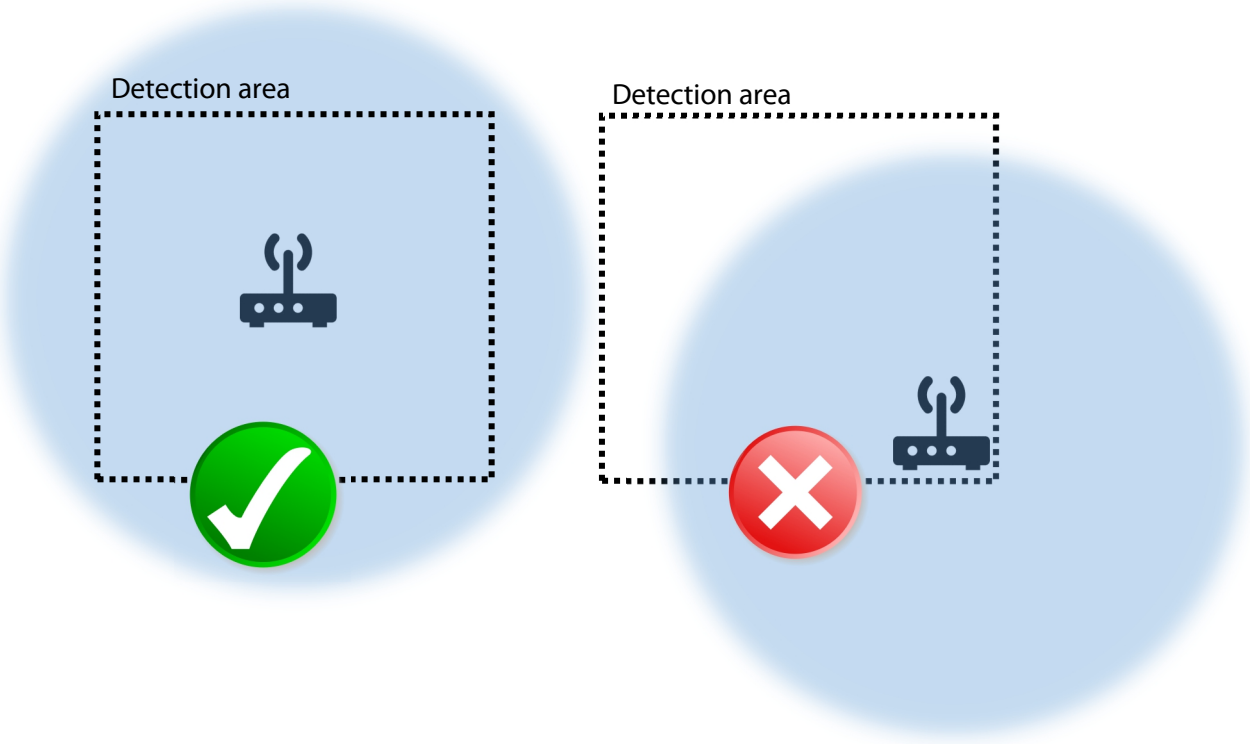


Figure 2 - install the sensor in the center of the detection area.

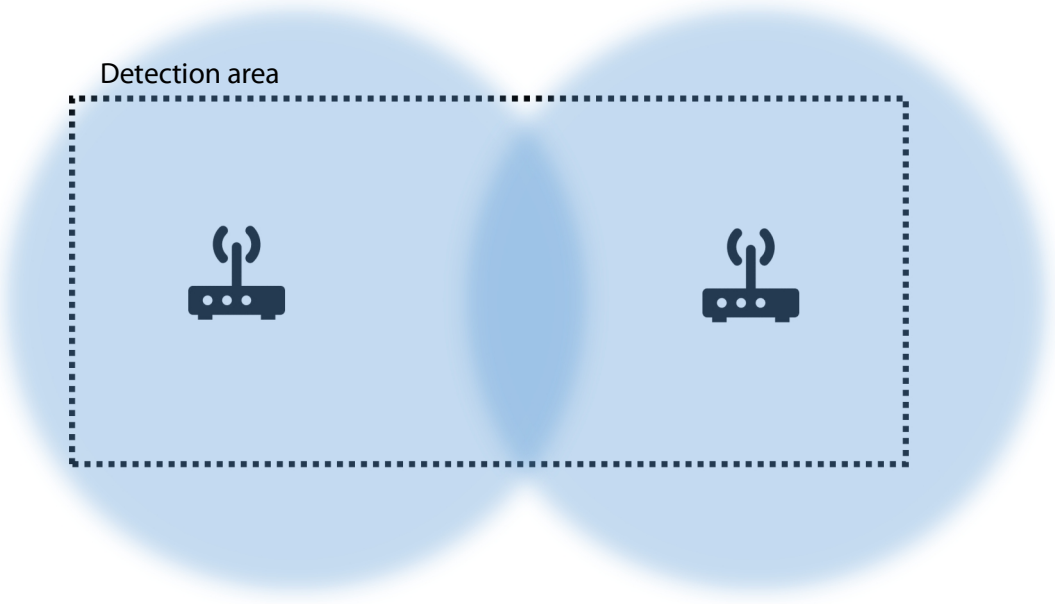


Figure 3 - use multiple sensor to cover the detection area in case the detection area is not square, or circle shape.

Construction materials - Construction materials (wood, concrete) attenuate wireless signals. This means that the detection area is reduced, if a sensor is installed behind or in such an object. This is especially true for the 5.8 GHz band. Also, it may introduce *blind spots* in the detection area where a drone is not detected. Installing multiple sensors is a solution to avoid blind spots.

For optimal performance install the sensor in open space, not surrounded by nearby objects. As a reference please find below a table describing the RF attenuation by various construction materials. For instance, if a drone is detected in the 5.8 GHz band with a 114 mm wooden fence between sensor and drone, the signal strength is 13 dB less compared to no fence.

Material and thickness	2.4 GHz	5.8 GHz
Red brick (hollow), 89 mm	5	15
Window glass (uncoated), 6 mm	1	1
Plasterboard, 13 mm	1	0
Wood dry, 114 mm	7	13
Plywood dry, 13 mm	1	0
Bricks (concrete, hollow), 203 mm	11	15
Concrete (C8 mix), 203 mm	35	56
Reinforcing steel mesh (19 mm Ø, 70-mm-grid)	10	3
Reinforced concrete (C8, 19 mm Ø, 70-mm-grid)	37	58

Table 1: RF attenuation by various construction materials. (source c't 9/2021, page 139 using data from William C. Stone, Electromagnetic Signal Attenuation in Construction Materials, 1997)

Height - Preferred installation height is 2 to 15 meters. Installation lower, near the ground, will reduce the detection area as objects in the detection area will block wireless signals more. Installing the sensor higher on the other hand will increase the detection area.

Angle - The sensor has internally an omnidirectional antenna. Install the sensor with zero angle (vertical plane). This means that the sensor should looks straight ahead. Not down or up under an angle.

Power - The sensor needs power and is powered via Power over Ethernet (PoE), 802.11af. Connect the Ethernet port of the sensor to an PoE capable switch/router to have both power and connectivity.

Connectivity **-** Connect the Ethernet port of the sensor to your router. The sensor needs internet for uploading the detected drones to the portal. It can also be used for management purposes, like pushing configuration updates. The sensor needs internet via Ethernet to a router with internet access.

Mast mount

For each sensor a mast mount is provided. It can be used to install the sensor to a mast or directly to a wall. See details below.

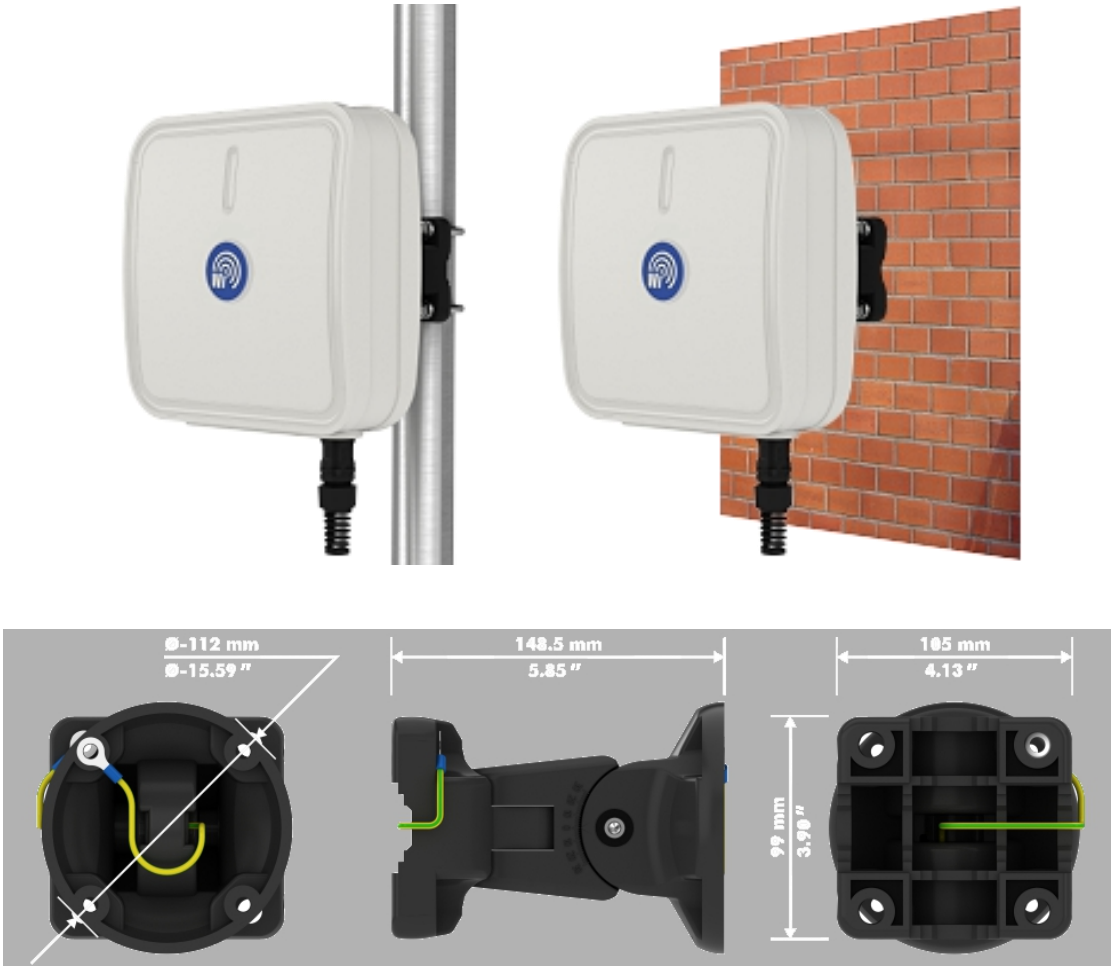


Figure 4 - mast mount to install the sensor to a mast or directly to a wall.

3.2 Configuration

DroneScout products are shipped pre-configured and work out-of-the-box, once they are connected to power and have access to internet. Typically, there is no need to open ports on your router.

Technically, It will use two ports to the server portal.dronescout.co from *inside to the internet*: 10094 for connecting to the MQTT broker and 10090 for remote maintenance (reverse SSH). In addition, it contacts regularly NTP servers on the internet to have the correct time.

Detection range

The detection range of the sensor is handled by the portal. The sensor is configured for maximum sensing distance. The basic model, DS100, has a range up to 1 km. In the portal you can configure a signal threshold for each zone to discard detected drones (or false alarms) outside the detection area. For more information, see the portal section.

Web-interface - In firmware version 20211115-1215 and higher, the sensor has a web-interface to configure the main settings of the sensor: update firmware, configure the network-settings and configure the threshold_override.conf file.

Figure 5 - Screenshot of the web-interface.

The default login is username admin with password bluemark and enter the IP-address of the sensor in your browser. After the log in is successful, the screenshot in Figure 5 is shown. On the main page (status), the state of the sensing information is shown and also the network configuration.

Select the 2.4 GHz threshold to edit the sensing thresholds for the 2.4 GHz band per 1 MHz bin. The same applies for the 5.2 GHz and 5.8 GHz threshold tab. Only signals higher as this threshold will be considered as drone signal. This is useful to reduce false alarms caused by nearby WiFi networks.

In the firmware tab, the firmware can be updated to the latest release. And the network-tab allows to change the network-settings.

Please note that after making changes, the sensing process is restarted and as a result you need to login again.

4 PORTAL

The portal is a central portal used by all *DroneScout* customers. Each customer will receive unique login credentials to manage their own sensors. Typically, the portal is already set up correctly with a project, zone and sensors that have been shipped to you. In that case, you only need to change a few details like project/zone names.

The portal can be reached at: https://portal.dronescout.co/

4.1 Basic concepts

The portal consists of several elements:

- *Sensors* - devices installed around the object of interest
- *Zones* - a virtual sensor configured at the portal. A zone can contain one or more sensors. Also here the signal threshold/detection distance can be configured.
- *Projects* - One or more zones belong to project. A project is typically a location, for instance your house. Each project contains it own specific settings, such as the guard time interval.
- *Settings* - Settings can be configured at two levels. Each project has its own settings, but there are also user settings, for instance email settings.

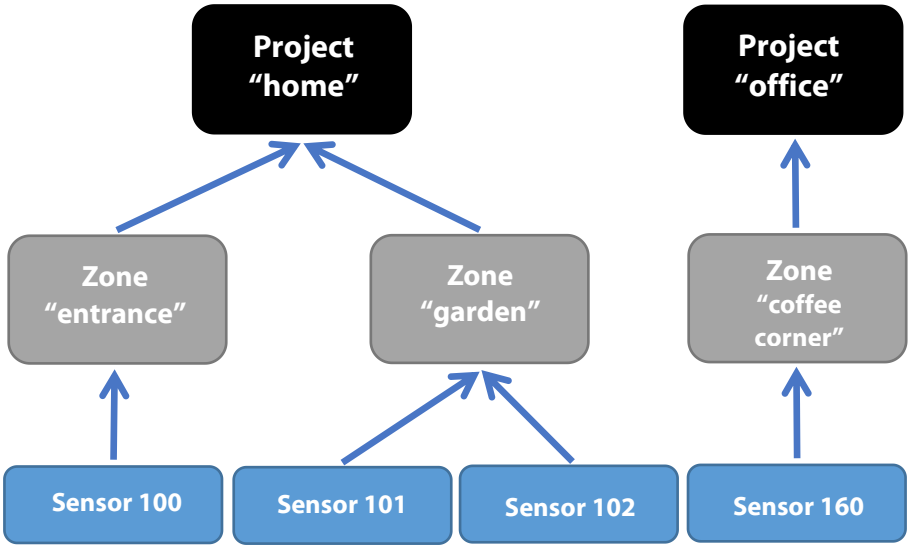


Figure 6 - relation between sensors, zones and projects in the portal

Each customer receives login credentials that are provided by us. The portal is located at: https://portal.dronescout.co/ After login you land on the main portal page. In the middle of the page you see your projects. On the left the main menu is shown. A screenshot of the portal is shown below.

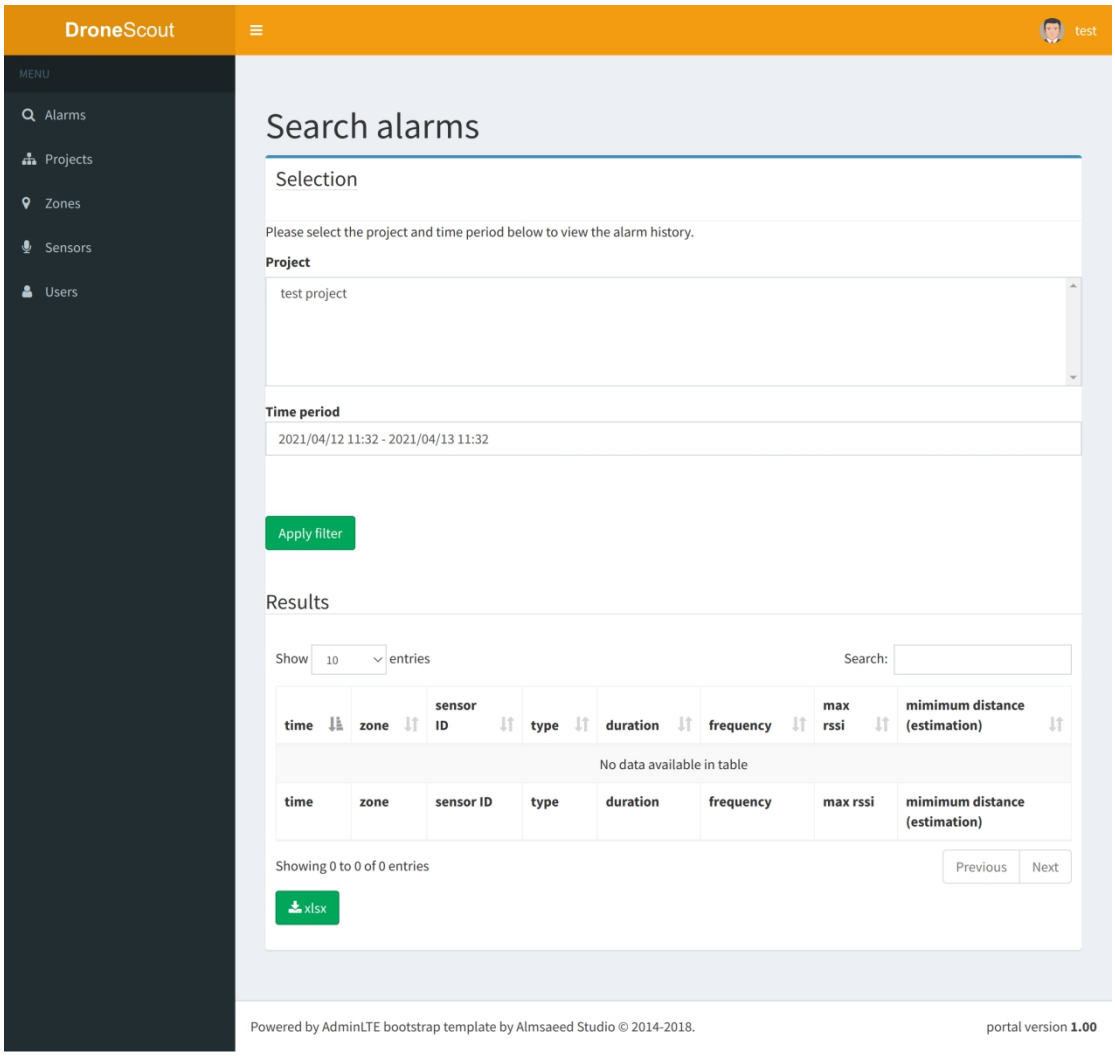


Figure 7 - screenshot of the main portal page.

The main menu contains:

- Alarms - an interactive tool to look up historic alarms.
- Projects - configure projects
- Zones - configure zones
- Sensors - configure sensors
- Users - manage your user account

4.2 Alarms

The *Search alarms* menu item is an interactive tool to display historic drone alarms. On this page, you need to select a project and time period. After pressing *Apply filter* the results are shown.

The *Search* field on the right top of the results allows you to narrow down the results. At the bottom of the page there is a *xlsx* button to export the results to an Excel-sheet.

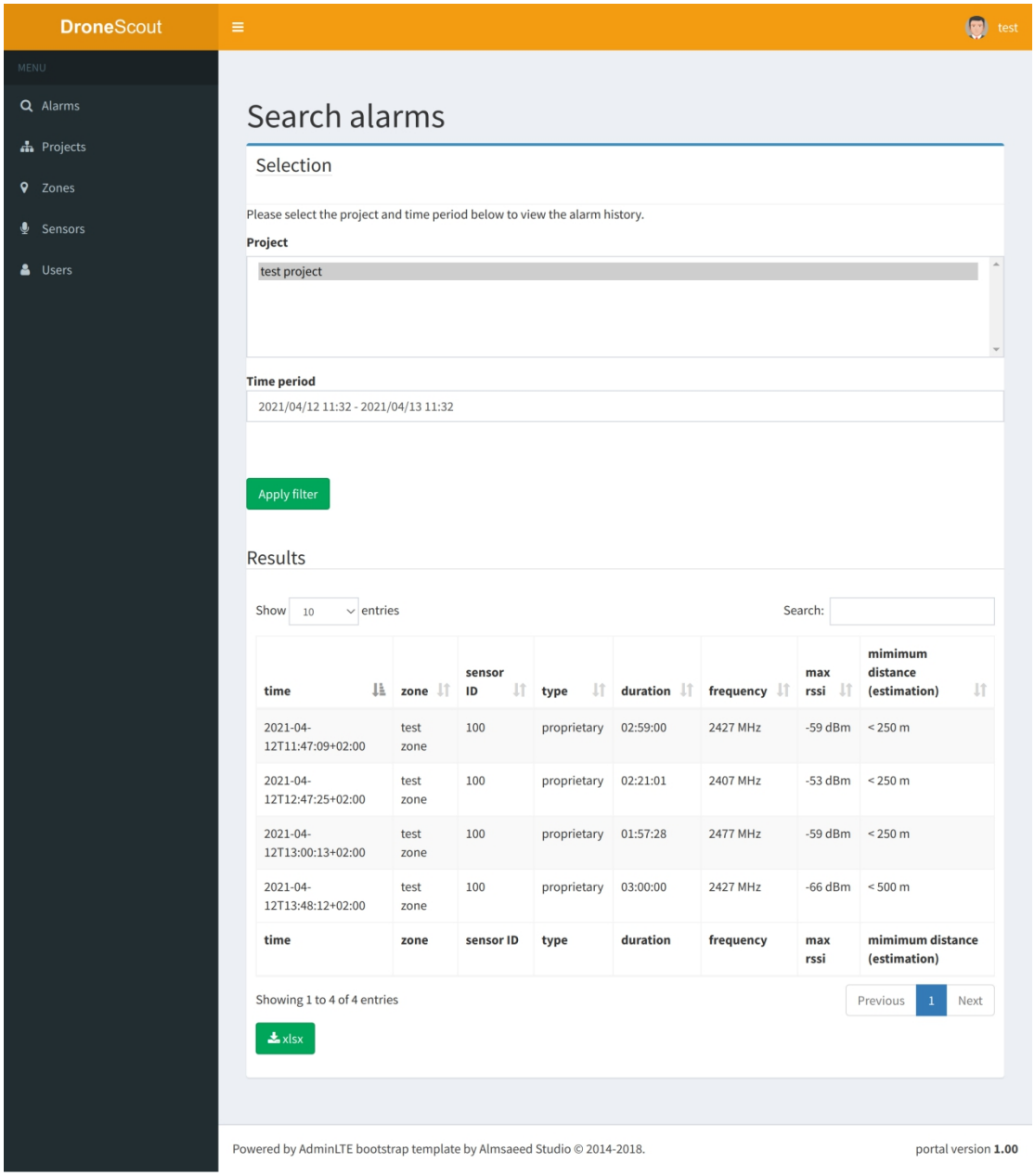


Figure 8 - Search alarms screen

4.3 Projects

If you deploy sensors to a new location, you start configure this location in the portal by adding a new project first.(Typically, a project has already been set up for new customer.) Go to the menu item *Projects* and click on the *New projec*t button. A screen is shown as in the screenshot below. Enter a project name that describes your location. Keep the *Active* project ticked, otherwise sensor data won't be processed. Tick *Realtime,* if you need realtime alarms. Also select the appropriate timezone of your location. This is needed for processing the correct time window.

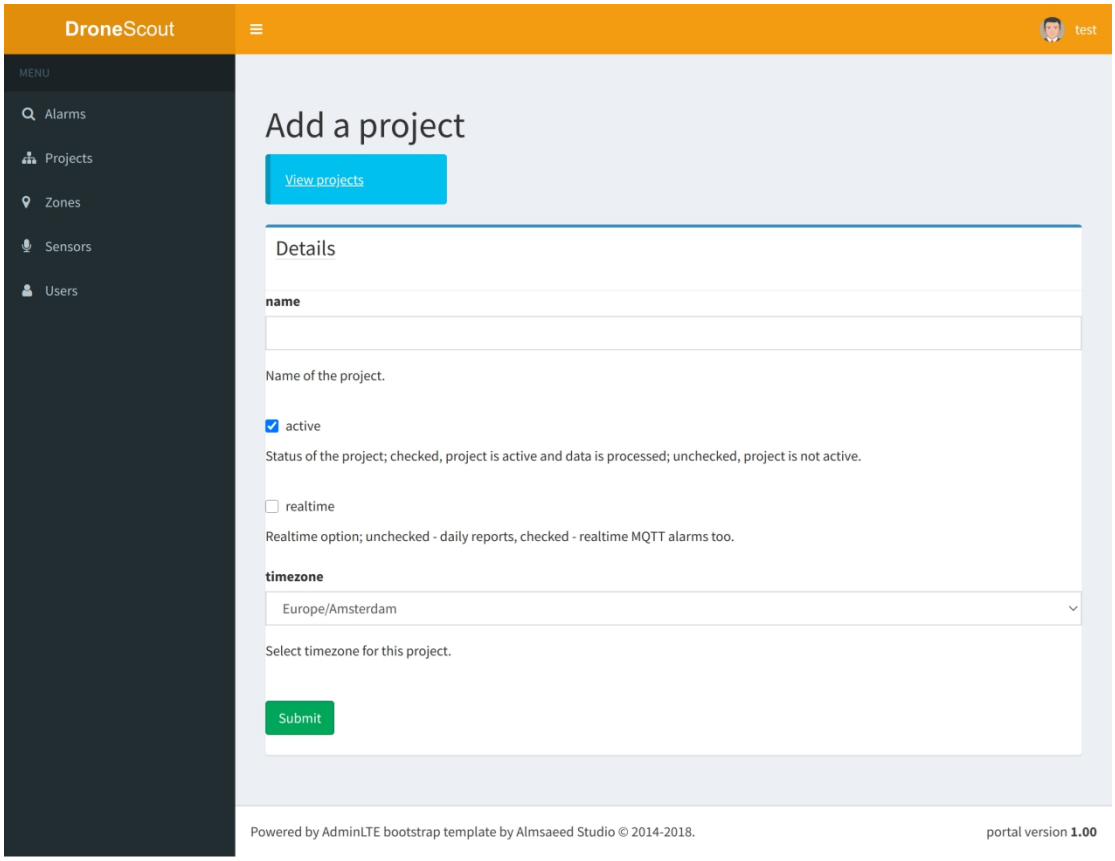


Figure 9 - Add a new project screenshot.

4.4 Zones

After creating a new project, you need to add a new zone. Click on *Add zone* button after creating a new project or go to the Zones menu and press this button.

You need to enter:

- *project* - select the created project to assign it to this project
- *name* - a name describing this zone like *main entrance*.
- *type* - select the sensor type, default DS100 - basic
- *threshold 2.4 GHz/5.8 GHz* - for each signal band, enter the signal threshold that defines the detection area. See the section *Detection range* for more information. The threshold values allow you to discard weak, far away drones or *phantom* detections caused for instance by nearby WiFi networks.
- *250m/500m threshold 2.4 GHz/5.8 GHz* - the distance of the drone is estimated on the received power. For the zone you can set power levels to define the 250 and 500m distance. The received drone transmit levels depends on the country; the USA has for instance higher drone transmit levels, but it also depends on the location. For instance in urban areas, the received power levels are typically higher compared to empty rural areas.
- *GPS mode, latitude, longitude, height, heading* - for the DS100 model set the mode to manual and manual insert the correct GPS location. This information is used for adding GPS data to the alarm messages.

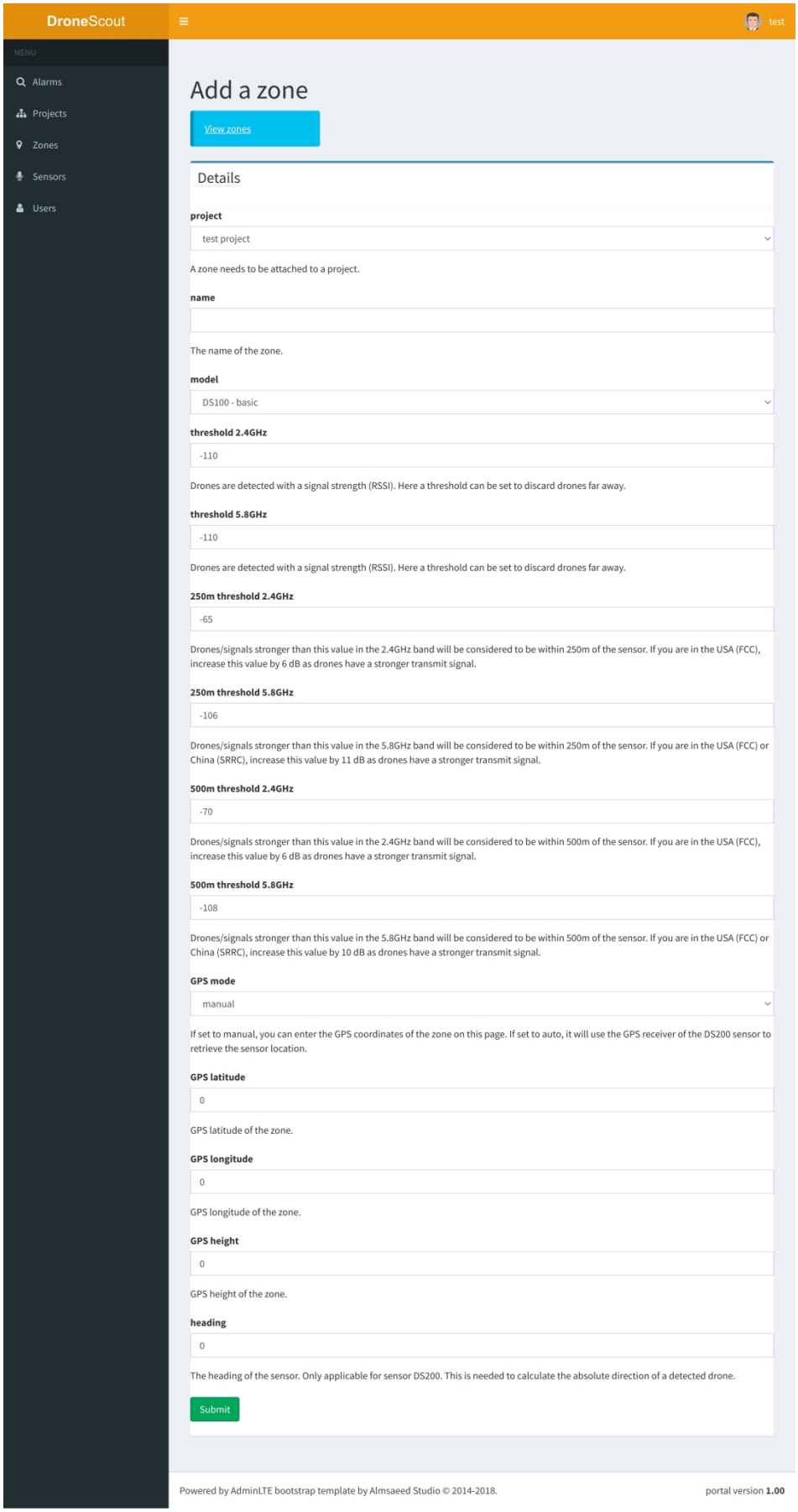


Figure 10 - Add a new zone screenshot.

4.5 Sensors

After configuring the zones attach sensors to it. The sensors section can be seen as a switch board; connect each sensor to the appropriate zone. A sensor can only connected to only one zone, but a zone can contain multiple sensors. Click on *Add sensor* button after creating a new zone or go to the Sensors menu and press this button.

You need to enter:

- *Sensor ID* - this is the numerical code on the back on the sensor without ds, for instance 204.
- *Zone ID* - select the zone in order to attach it to this sensor.
- *Monitor* - Tick *Monitor* if you want to receive messages (by mail and MQTT) when a sensor goes on or offline. Here, you can also select the timeout periods for a warning (*online warning timeout value*) and error message (*online error timeout value*).

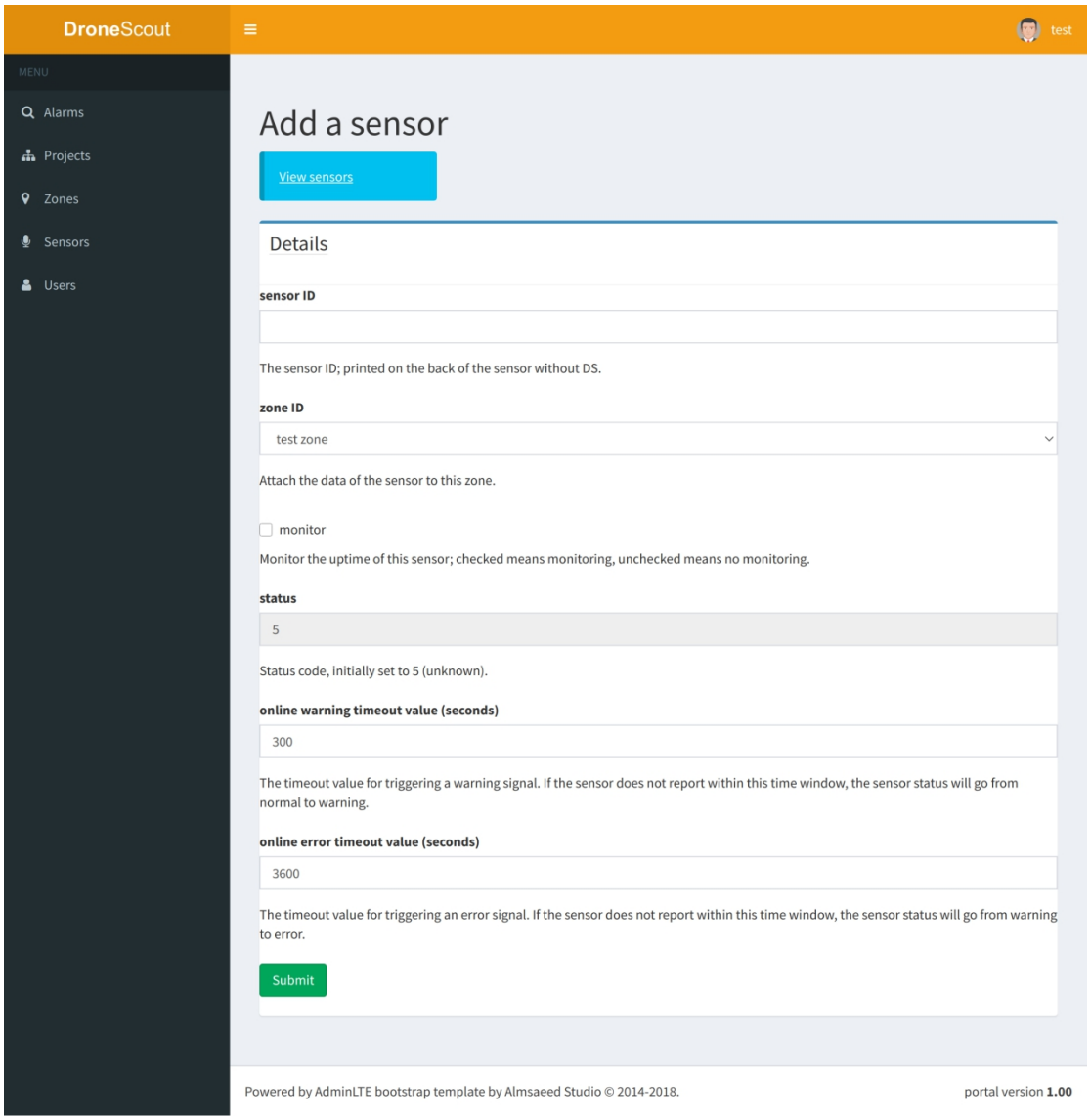


Figure 11 - Add a new sensor screenshot.

Manage sensor

The current status of a sensor can be looked up by going to the manage action. Go to the Sensors page and click on the *Manage* button on the right of the page. The *Last seen* row shows when the sensor is seen last. Every minute a sensor will report to the portal, so typically the last seen row is less than 1 minute old. Please note that the time is shown in *UTC time zone*. This page shows also the current sensor settings.

In addition, it is possible to execute several actions like *power off*, *reboot* or perform a *firmware update*. Note that once you power off a device, you can't power it up remotely anymore! Press on the appropriate buttons to execute a command. The sensor will respond with an acknowledge (ack) message to confirm the action. The *Sensor command history* section at the bottom of the page shows historic commands.

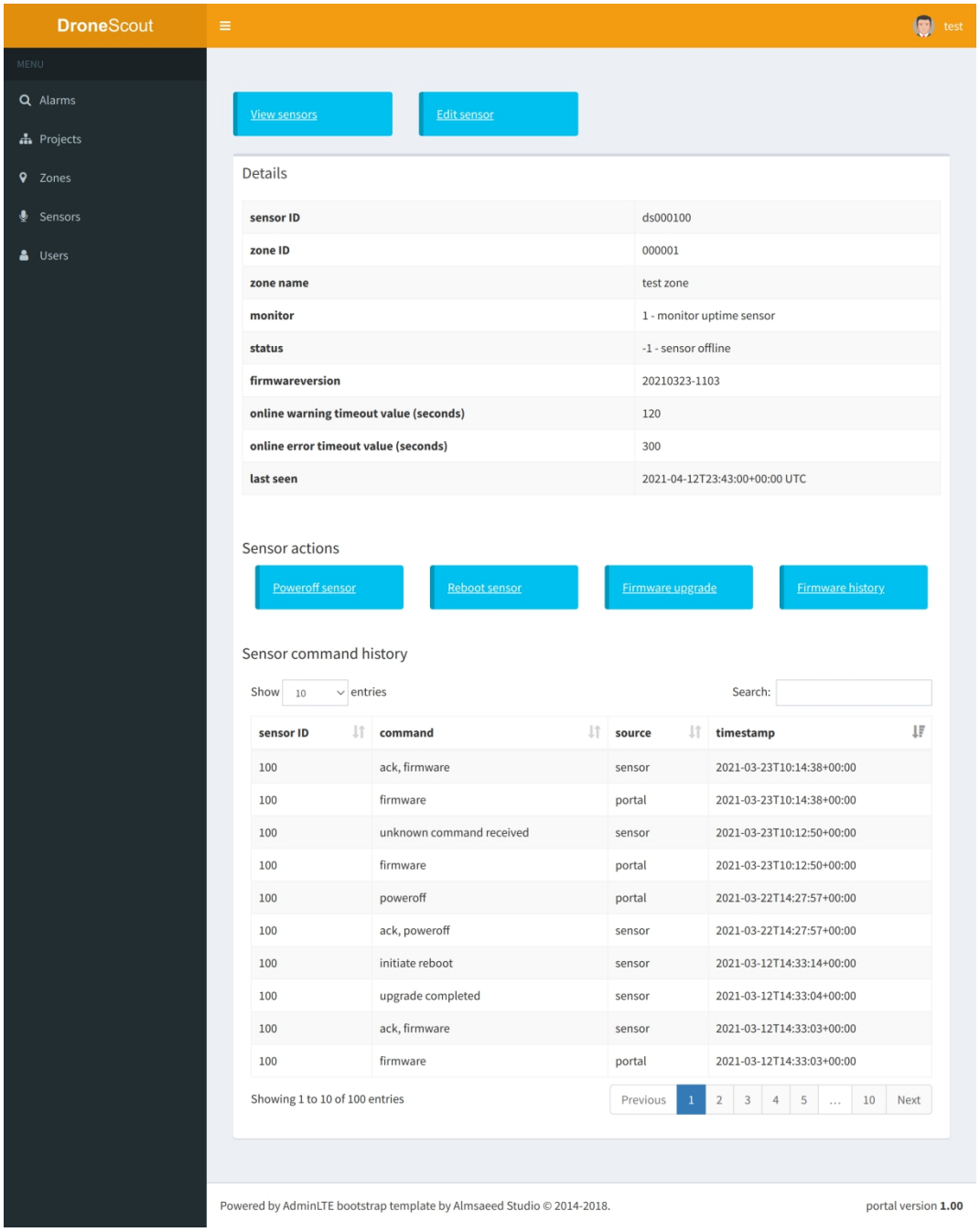


Figure 12 - Manage sensor screenshot.

4.6 Users

Click on the Users menu and click on the Edit button to manage your user settings. On this page you can change username, password, full name and email address. The bottom part of the page allows you to set the MQTT broker configuration. The portal will publish alarm messages to the configured MQTT broker.

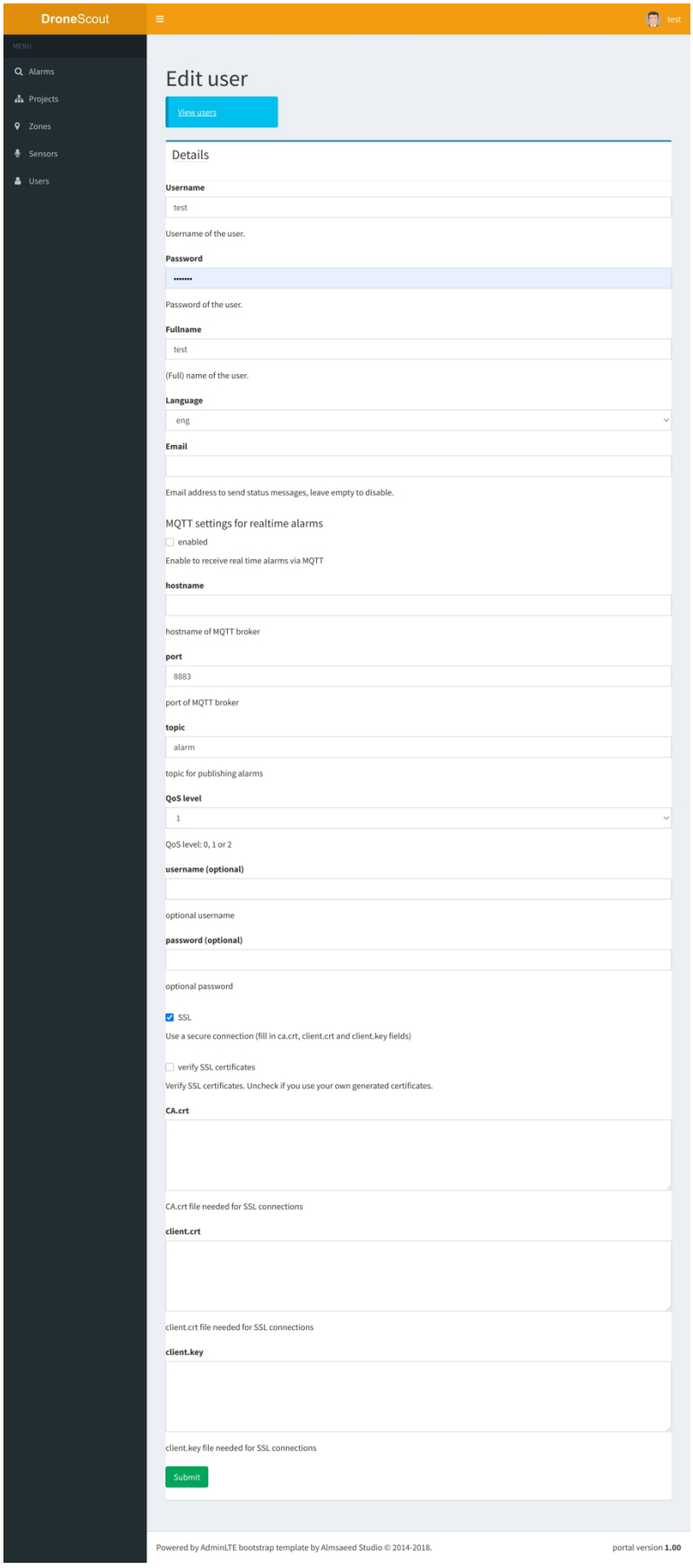


Figure 13 - Edit user screenshot.

4.7 Detection range

An important setting is configuring the detection range of the sensor. The range for the DS100 sensor is up to 1 km for drones in the 2.4 GHz band. In the EU, the 5.8 GHz band has a maximum distance up to 500 meter, due to a much lower drone transmit power in this band.

In the portal the maximum distance can be reduced by discarding weak signals. Drones far away from the sensor, will be detected with a weak signal. The closer a drone is to the sensor, the stronger the detected signal will be. The curve between signal strength and distance depends on a lot of factors. transmit power of the drone, frequency, blocking by a large object etc. Due to these wireless signal characteristics, the detection area can't be configured precisely. There will be a gray area at the border of the detection area, in which some drones get detected and others have too weak signals, although they will be at the same distance to the sensor.

For each zone, multiple thresholds can be set in the portal:

- *threshold 2.4 GHz/5.8 GHz* - drone detections below this threshold don't trigger an alarm and are not shown in the portal.
- *250m/500m threshold 2.4 GHz/5.8 GHz* - the distance is estimated based on the received power. Here, you can set a threshold that defines the 250 and 500m distance. Signals stronger as the 250m threshold are considered to be within the 250m distance. The same applies for the 500m threshold.

There are several approaches to configure the threshold values:

- *standard values* - in case you want to detect every signal, enter -110 for the threshold
- *on-site calibration* - use a drone and do measuring in the detection area.
- *detected devices* - evaluate the detected drones and the detected signal strength after a few weeks/months of operation and set the threshold accordingly.

Standard values

According to the so-called *free-space path loss* model, a wireless signal attenuates 6 dB when the distance doubles in free space. So, if a drone is detected with 0 dBm at 1 meter, it will be detected at -6 dBm at 2 meter, -12 dBm at 4 meters. Outdoor radio propagation is close to the free-space path loss model.

The table below gives the standard values for the EU. Drones in the 5.8 GHz signals band are weaker due to the higher frequency and lower drone transmit power. Add 6 dB to the 2.4 GHz thresholds if the sensor is located in the USA or China and add 10 dB to the 5.8 GHz thresholds for these countries. For other countries outside the EU, USA or China, please check the allowed drone transmit powers in your country and adjust the thresholds accordingly.

max detection distance	threshold 2.4 GHz	threshold 5.8 GHz
250 meter	-65 dBm	-106 dBm
500 meter	-70 dBm	-108 dBm

Table 2: standard threshold values

On-site calibration

Another method for setting up the detection range, is using a test drone (less than 5 years old) which is capable of transmitting in the 2.4 GHz band. Make a flight at the border of the detection area. (The alarm will give the closest signal, so don't fly near the sensor.) Try both bands if possible. Note: an alarm will be visible in the portal 5 minutes after the last detection.

Detected drones

The third and last method is to use the *Search alarms* section. It is an interactive method that can be used stand alone or in combination with the other techniques. Configure all zones to a threshold of -110 dBm. Wait a few weeks and go to the *Search alarms* section. Use the detected signal levels to derive the optimal threshold. The idea is setup the threshold in such a way that you filter away your main sources of false alarms without loosing *real* alarms. Of course, if your desired detection area is less than 500 m, you can start with a higher threshold value.

Drone height

The detected signal strength depends also on the height of the drone. If the drone flies at a height of 50 meter or higher, the signal will be a few dBs weaker.

4.8 Email settings

Daily briefing can be received by mail. An example briefing is shown in the reports section. To receive a daily briefing, make sure:

- the project is active
- enter your email address in the *user* settings page

You can enter your email address, by navigating to the *Users* menu item. Click on Edit in the action column. Edit your mail address in the *Email* field and press Submit. Set the mail address to empty, to receive no daily mails. Note, in case of multiple email addresses, use a comma as separator.

For each project a separate daily briefing will be sent.

4.9 Guard time period

The guard time period is a period of the day in which detected drones will trigger the system to generate an alarm. It is the period that the system is active. Default this time period is from 06:00 to 06:00 next day (24 hours). You can change this period per project; Go to the main *Projects* page. Click on the *View/Settings* button. Here, in the *Related settings* section the start and stop of this time period can be configured.

The *guard_time_start* is the start time in HHMM format. The *guard_time_stop* settings is the end time of the guard period.

Note, the guard time period is only used for the daily briefings.

4.10 Realtime alarms

Realtime alarms can be received, by configuring the MQTT broker. See section *4.6 Users* for more information and *chapter 5 Reports* for example alarms.

5 REPORTS

There are two report types:

- daily briefing by email
- realtime alarms via MQTT

5.1 Daily briefings

An example daily briefing is shown below. It contains several blocks

- Drones that are detected in the guard time window, default the last 24 hours starting with 06:00 each day.
- downtime of sensors that have the monitor option ticked.

From: sensor@bluemark.io <sensor@bluemark.io>
To<sensor@bluemark.io>
Subject: test project detected drones on 11 Apr 2021
Date: Mon, 12 Apr 2021 08:03:02 +0200

```
These drones have been detected in project test project on 11 Apr 2021.

Period 06:00 - 06:00 (next day):
                zone    type           frequency        mimimum distance (estimation)  start   end     duration
           test zone     proprietary    2447.0 MHz                     > 500 meter     13u23   15u22   01u59
           test zone     proprietary    2447.0 MHz                     > 500 meter     15u25   17u25   02u00
           test zone     proprietary    2474.5 MHz                     > 500 meter     17u25   19u25   02u00
           test zone     proprietary    2447.0 MHz                     > 500 meter     17u26   19u26   02u00
           test zone     proprietary    2474.0 MHz                     > 500 meter     19u26   21u26   02u00
           test zone     proprietary    2447.0 MHz                     > 500 meter     19u27   21u27   02u00


Downtime sensors (06:00 to 06:00 next day):
               zone    sensor ID       hour     uptime
```

Figure 14 - Example daily briefing

5.2 Realtime alarms

There are multiple realtime alarms (JSON format):

- *Sensor status* - if the status of the sensor changes (online, offline), a realtime alarm is triggered.
- *Realtime alarm* - every 10 seconds, the system will generate an alarm for currently detected drones
- *Alarm summary* - Five minutes after the last detection of a drone, an alarm summary message is generated.

Alarms are published to the MQTT broker configured by the user. (See section *4.6 Users*). Please note that the guard time period (section *4.9*) does not apply to the realtime alarms; they are always generated.

Sensor status

The portal will publish a sensor status message when the status of a sensor changes and the monitor function is enabled. A example message is shown below.


```
{
 "type":"status",
 "sensor":{
    "id":100,
    "serial number":"ds000100",
    "model":"ds100",
    "firmware version":"20210323-1103"
 },
 "gps":{
    "lat":52.099998,
    "lon":6.100000,
    "alt":75.000000
 },
 "zone":{
    "id":1,
    "name":"test zone",
    "model":"DS100 - basic"
 },
 "project":{
    "id":1,
    "name":"test project",
    "timezone":"Europe/Amsterdam"
 },
 "data":{
    "timestamp":1617105360,
    "time":"2021-03-30 13:56:00",
    "status code":1,
    "status":"normal"
 }
```


Figure 15 - Example sensor status message.

This message contains several sections:

- *type* - "status" for this type of alarm

- *sensor* - this section contains relevant sensor information like serial number, firmware version, model.
- *gps* - GPS data, fetched from GPS location set in the attached zone.
- *zone* - relevant information of the attached zone: name and sensor model.
- *project* - relevant information of the attached project: name and timezone.
- *data* - the data section contains: the time in both unix timestamp and local time (using the timezone configured in the project), the status both in code and text. The status can be -1 - offline, 0 - warning, 1 - online, 2 - license error, 3 - system too hot 4 - RF learning 5- unknown. If the system is too hot, the load on the system is temporarily reduced to prevent overheating. If the sensor is rebooted, the first hours are used to learn the RF environment. For status code 3 and 4, the performance of the system is reduced, a bit less sensitive. In case of status code 2, the detection is disabled.

Realtime alarm

When a drone is detected (and the realtime option is enabled for the project), the portal will generate every 10 seconds an alarm. An example alarm is shown below.


```
{
 "type":"alarm",
 "sensor":{
    "id":100,
    "serial number":"ds000100",
    "model":"ds100",
    "firmware version":"20210323-1103"
 },
 "gps":{
    "lat":52.099998,
    "lon":6.100000,
    "alt":75.000000
 },
 "zone":{
    "id":1,
    "name":"test zone",
    "model":"DS100 - basic"
 },
 "project":{
    "id":1,
    "name":"test project",
    "timezone":"Europe/Amsterdam"
 },
 "data":{
    "timestamp":1617113340,
    "time":"2021-03-30 16:09:00",
    "type":"unknown",
    "frequency MHz":5759.0,
    "bandwidth MHz":2.0,
    "rssi dBm":-114
 }
```


Figure 16 - Example realtime alarm message.

This message contains several sections:

- *type* - "alarm" for this type of alarm
- *sensor* - this section contains relevant sensor information like serial number, firmware version, model.
- *gps* - GPS data, fetched from GPS location set in the attached zone.
- *zone* - relevant information of the attached zone: name and sensor model.
- *project* - relevant information of the attached project: name and timezone.
- *data* - the data section: the time in both unix timestamp and local time (using the timezone configured in the project). Furthermore, the frequency and bandwidth are included, both in MHz values. Based on the bandwidth, the type of the drone is determined. It can be *WiFi*, *proprietary* or *unknown*. Also, the current received signal strength (rssi) is included in dBm value.

Alarm summary

An alarm summary message is generated 5 minutes after the last detection of the drone. An example message is shown below.


```
{
 "type":"alarm summary",
 "sensor":{
    "id":100,
    "serial number":"ds000100",
    "model":"ds100",
    "firmware version":"20210323-1103"
 },
 "gps":{
    "lat":52.099998,
    "lon":6.100000,
    "alt":75.000000
 },
 "zone":{
    "id":1,
    "name":"test zone",
    "model":"DS100 - basic"
 },
 "project":{
    "id":1,
    "name":"test project",
    "timezone":"Europe/Amsterdam"
 },
 "data":{
    "timestamp start":1617108995,
    "timestamp stop":1617109064,
    "time start":"2021-03-30 14:56:35",
    "time stop":"2021-03-30 14:57:44",
    "type":"proprietary",
    "frequency MHz":2469.0,
    "bandwidth MHz":4.0,
    "max rssi dBm":-63
 }
```


Figure 17 - Example alarm summary message.

This message contains several sections:

- *type* - "alarm summary" for this type of alarm
- *sensor* - this section contains relevant sensor information like serial number, firmware version, model.
- *gps* - GPS data, fetched from GPS location set in the attached zone.
- *zone* - relevant information of the attached zone: name and sensor model.
- *project* - relevant information of the attached project: name and timezone.
- *data* - the data section contains: the start and stop detection time in both unix timestamp and local time (using the timezone configured in the project). Furthermore, the frequency and bandwidth are included, both in MHz values. Based on the bandwidth, the type of the drone is determined. It can be *WiFi*, *proprietary* or *unknown*. Also, the maximum received signal strength (rssi) is included in dBm value.

6 MORE INFORMATION

If you need more information, please contact us at info@bluemark.io or by phone: +31 53 711 2104.

All contact information can be found at the *DroneScout* contact page:
https://dronescout.co/contact/