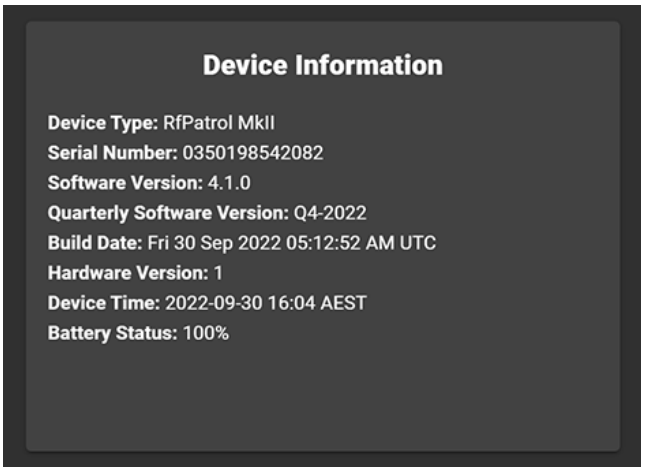
10.4 Device Summary



10.4.1 Device Information

Device Type

Type of DroneShield device (RfPatrol MKII)

Serial Number

The serial number is tied to the device and cannot be changed

Software Version

The software loaded onto the device

Quarterly Software Version

The release cycle of the current software version

Build Date

Date that the software version was built

Hardware Version

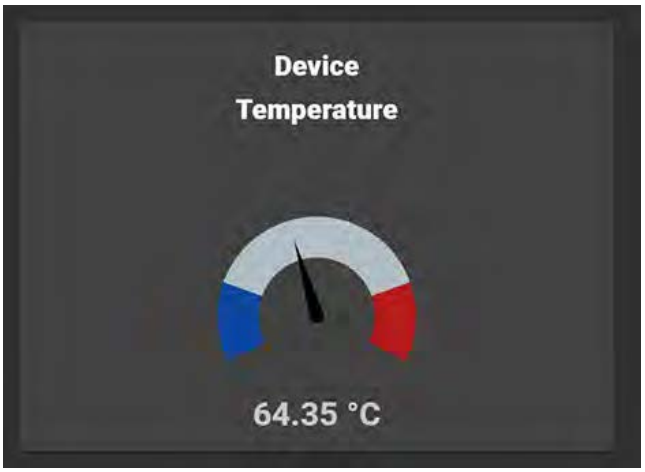
The software version of the internal hardware manager

Device Time

Local time set on the device

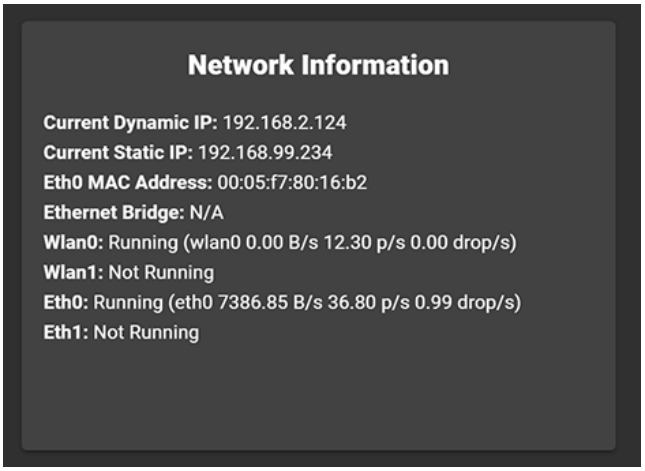
Battery Status

Current battery level of the device



10.4.2 Microcontroller Temp

The current temperature of the RfPatrol MKII device microcontroller, expected range under normal operating conditions between 50-70°C. Higher ambient temperatures may yield higher temperature readings. The device should not surpass 85°C.



10.4.3 Network Information

Current Dynamic IP

This IP address is issued to the device by the DHCP server

Current Static IP

This is 192.168.99.234 by default. It can be changed by user

Eth0 MAC Address

Hardware Adaptor address of the external network interface

Ethernet Bridge

Not used on RfPatrol MKII

Wlan0

Displays the status of the Wi-Fi interface

Wlan1

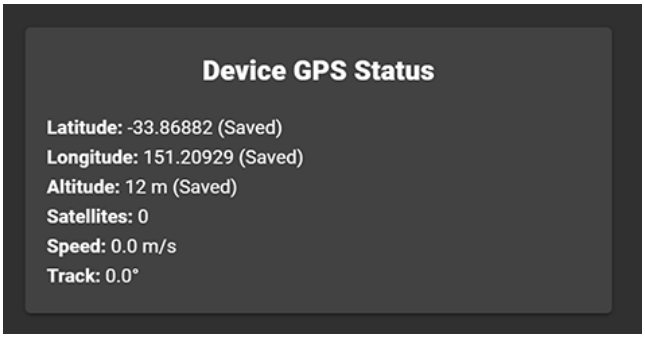
Not used on RfPatrol MKII

Eth0

Displays the status of the network interface, including operation state and network activity

Eth1

Not used on RfPatrol MKII



10.4.4 Device GPS Status

GPS Status will only appear when the RfPatrol MKII device is receiving GPS data or, when applicable from the internal GPS (i.e. for the RfOneMKII and DSX which have an internal GPS module).

Latitude

Latitude reported by the GPS compass

Longitude

Longitude reported by the GPS compass

Altitude

Altitude reported by the GPS compass

Satellites

Number of satellites providing position

Speed

Speed of the device in m/s if live GPS updates are enabled

Track

If the GPS input device provides heading, it will be displayed here

10.5 Filters Tab

Filters can be individually enabled and disabled, edited or deleted entirely. The user can enable/disable specific detectors, which can be useful when in high noise environments causing false detections in specific frequencies.

"10.5.1 RF Detectors"

If the user attaches or dettaches an antenna from the RfPatrol device, the corresponding frequency band must be enabled or disabled from this tab. Individual RF detectors can be enabled/disabled under each frequency band.

"10.5.2 Advanced RF Filters"

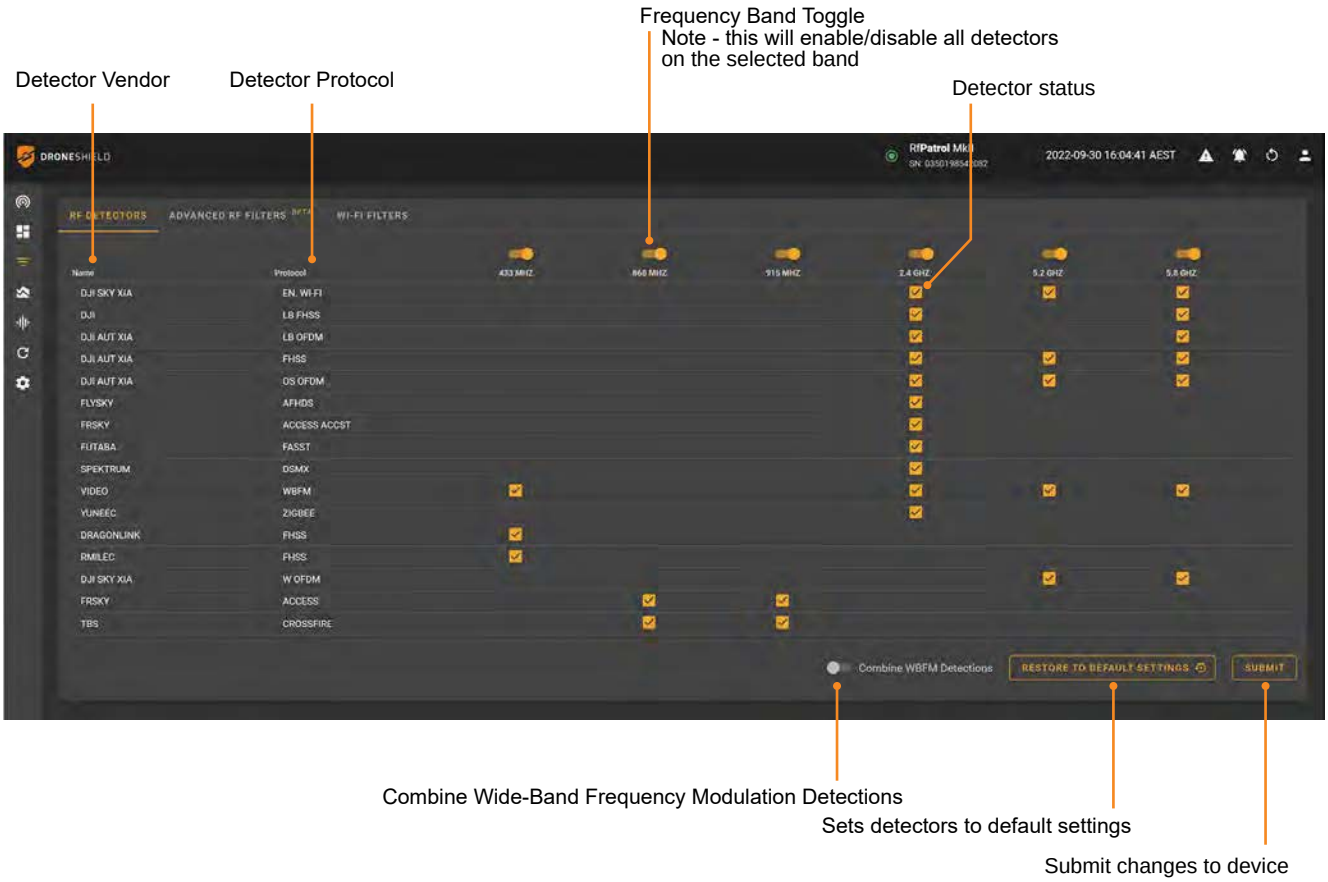
Create targeted RF filters using frequency, vendor, protocol and timeout information. Allows users to refine and target false detections.

"10.5.4 Wi-Fi Filters"

Add filters targeting the SSID to reduce false detections in the Wi-Fi spectrum.

10.5.1 RF Detectors

The supported detectors tab, located under the filters panel, allows the user to enable/disable individual RF detectors or entire bands. If additional antennas are installed or removed from the RfPatrol device, the user should enable/disable the appropriate bands.



Users should disable any frequency band that does not have a matching antenna installed on the RfPatrol MKII or risk false detections.

When multi-drone detector is enabled for FM Video transmitters, multiple signals may be picked up from the same transmitter. This is most common on 2.4GHz signals but can also be present on 5.8GHz signals. The further the transmitter is from the RfPatrol MKII, the less likely this is to occur.

Band Allocations based on region (868MHz / 915MHz)

Users should be aware of the designated frequency based on region, for either 868MHz or 915MHz. Enabling detectors on a frequency band not used in the user's region may cause spurious or unexpected detections.

The band allocations for these frequency bands are as follows:

ISM915 (902MHz - 928MHz)

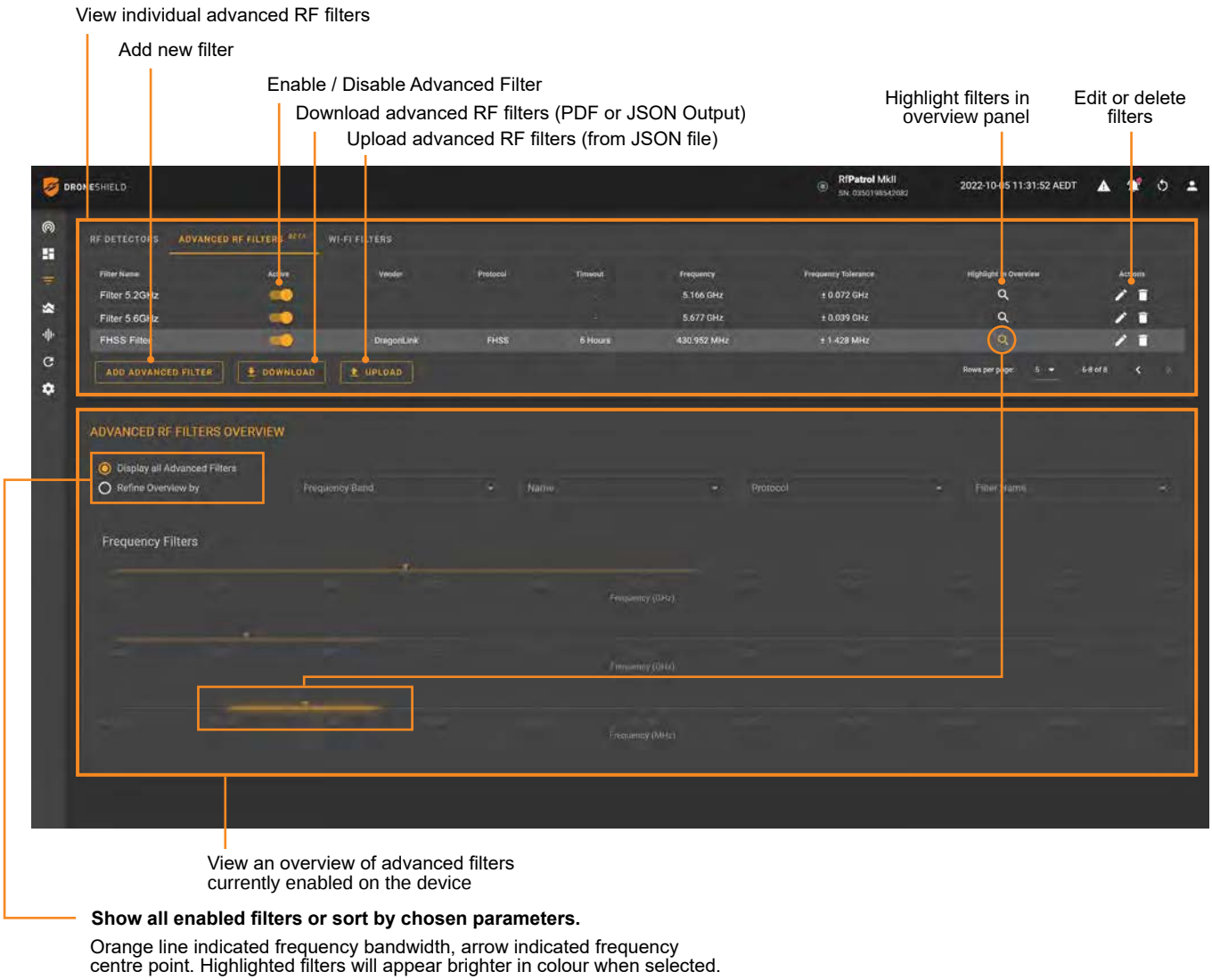
- ITU Region 3 (AUS/NZ) - AUS (915-928MHz)
- ITU Region 2 (USA/CAN) - US (902-928MHz)

ISM/SRD860 (863MHz - 870MHz)

- ITU Region 1 (Europe)

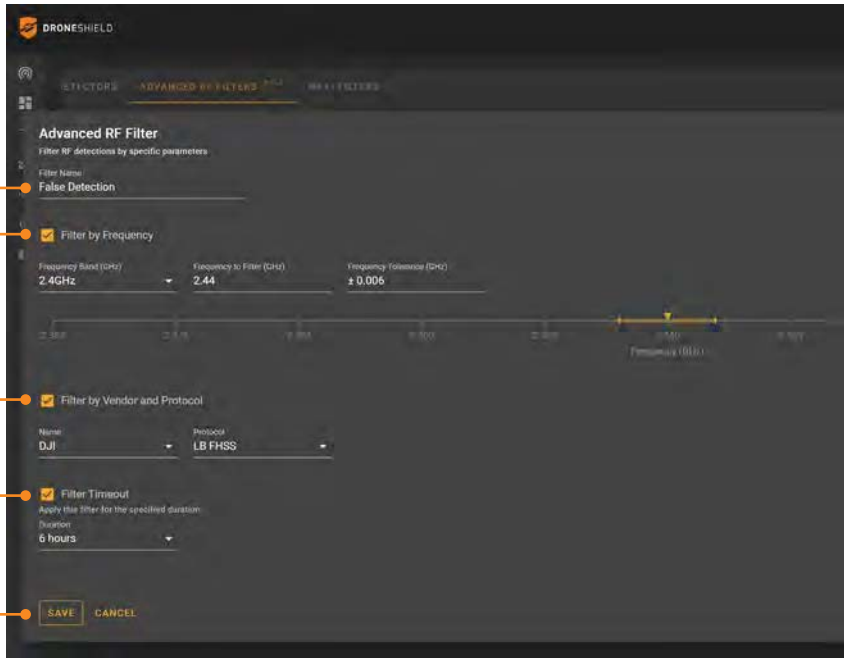
10.5.2 Advanced RF Filters

Advanced RF Filters allow the user to set targeted filters for false detections. Multiple parameters can be set and edited to improve the effectiveness of the filter, including frequency range, vendor, protocol and time-out settings.



RfPatrol MKII Device Manager - Filters Tab

10.5.3 Adding a New Advanced Filter



Name of Filter

Filter by Frequency

To apply a frequency based on frequency, start by selecting a frequency band followed by the centre frequency and tolerance (in GHz).

Filter by Vendor and Protocol

First select the Vendor to filter. Next, select the appropriate protocol to filter.

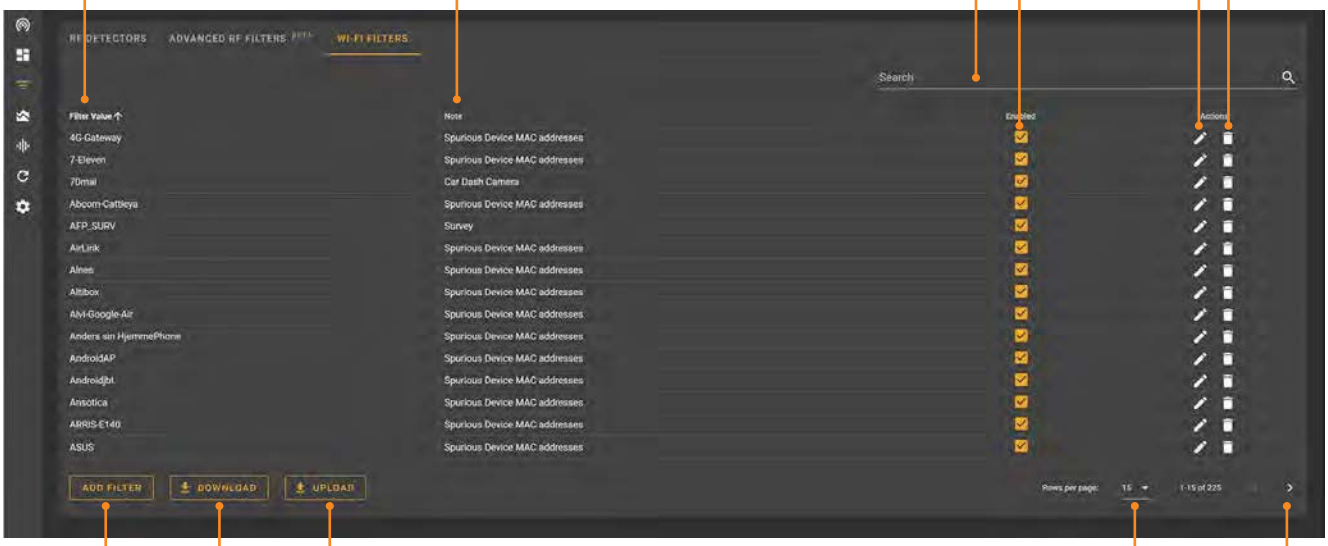
Filter Timeout

Used for temporary filters that automatically disable after a set period of time.

Save Filter

10.5.4 Wi-Fi Filters

Navigating to the device filters tab will display filters currently loaded to the device and their status (enabled or disabled). By default, the filters are sorted by the status.



Filter name

Filter rationale

Search Filters

Filter status

Edit filter

Delete filter

"10.5.5 Add Filter"

Export filter list

Import filter list

Change how many rows are displayed per page

Scroll through pages of filters

10.5.5 Add Filter

1. Click Add 

2. Add network name to Filter (only applicable to Wi-Fi detections)
3. Click Save

Adding a drone to this filter list will mean the user is no longer alerted to this drone's presence
Users should be cautious as to what filters they add.

10.6 Spectrum View

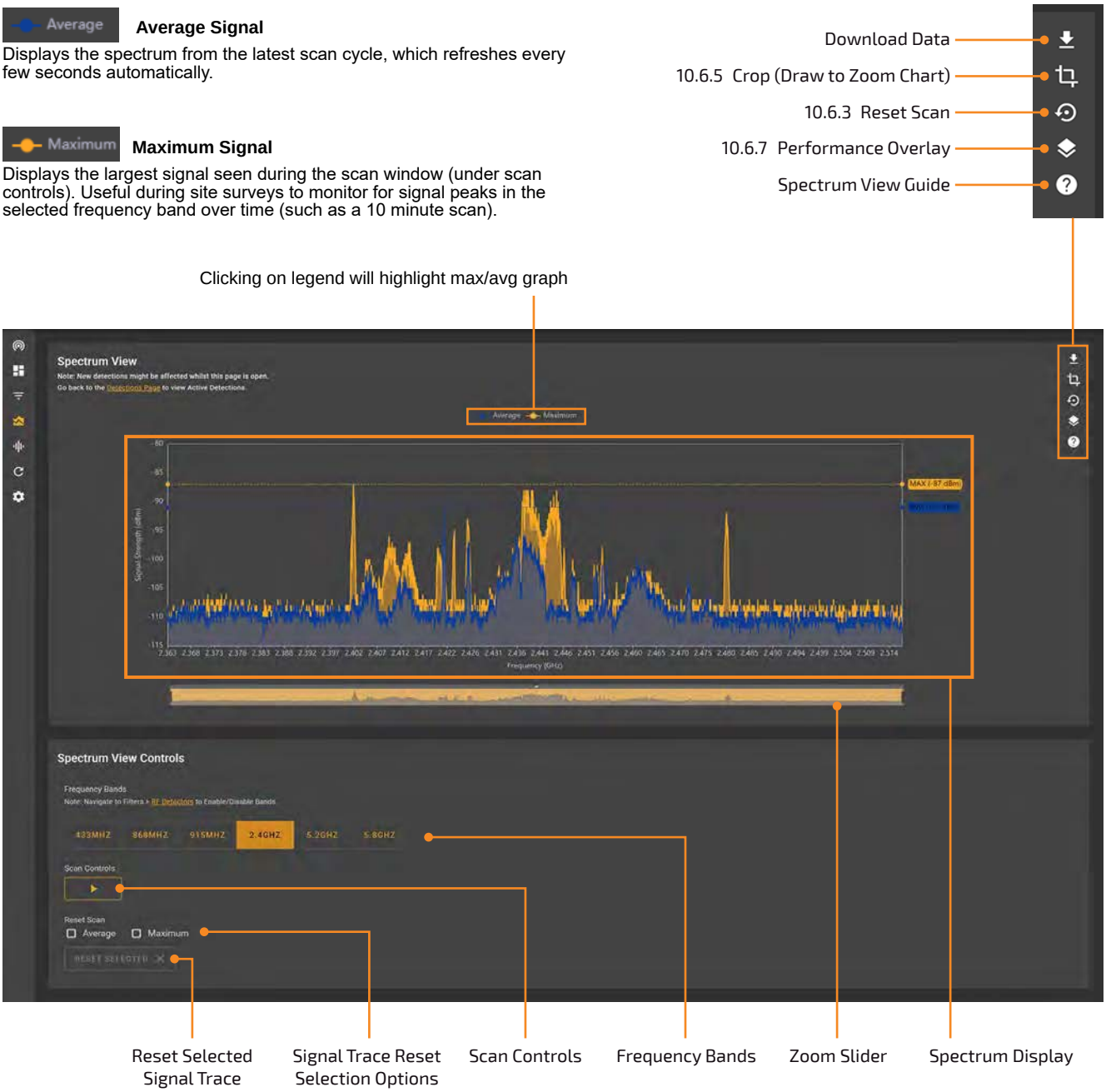
The Spectrum View is a powerful tool to view live radio-frequency spectrum data from the device in real-time. This feature provides the spectrum in a graphed format, displaying maximum and averaged value traces for the selected frequency band.

Average Signal

Displays the spectrum from the latest scan cycle, which refreshes every few seconds automatically.

Maximum Signal

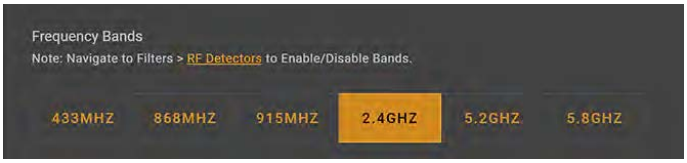
Displays the largest signal seen during the scan window (under scan controls). Useful during site surveys to monitor for signal peaks in the selected frequency band over time (such as a 10 minute scan).



10.6.1 Frequency Bands

Toggle between the available frequency bands that will be scanned. The Spectrum Display will automatically update if the scan control is set to live. If the scan is paused, it must be re-run in order to update the graph interface.

If a desired frequency is greyed out, check that the band is enabled. See "10.5.1 RF Detectors"



10.6.2 Scan Controls

Setting the scan to live will automatically update the graph with each scan cycle.

Setting the scan to pause will freeze spectrum data on the interface.

Note that navigating away from the Spectrum View tab will automatically pause scanning.

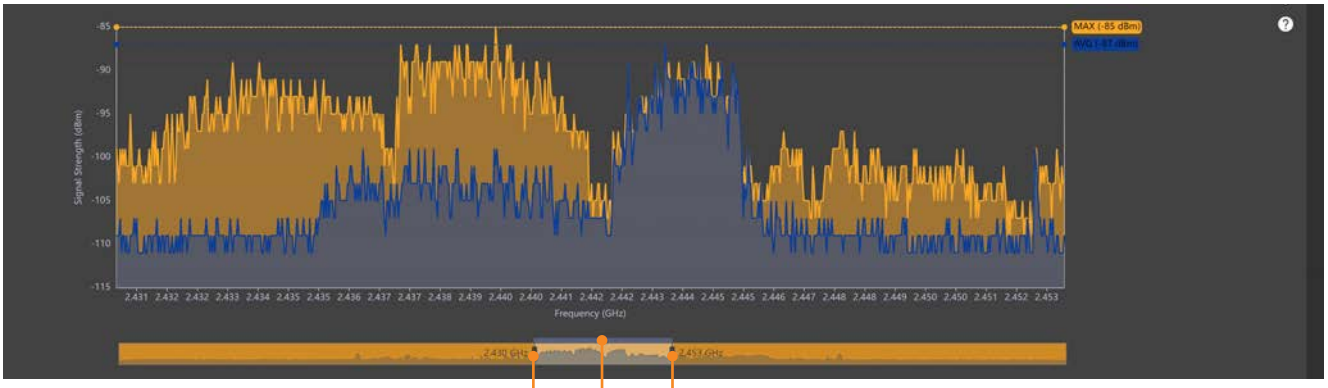
10.6.3 Reset Scan

Select the desired signal trace check-boxes (maximum or average) and click ‘reset selected’ to clear existing signal traces displayed on the spectrum interface. Once a trace has been cleared it will re-calculate on the next spectrum scan-cycle.

10.6.4 Zoom Slider

The zoom slider allows for quick cropping and zoom adjustment of the Spectrum Display to focus on an area of interest.

The slider can be adjusted by clicking and dragging each control tab to the desired upper and lower frequency limits. The spectrum display will zoom to fit the cropped range.



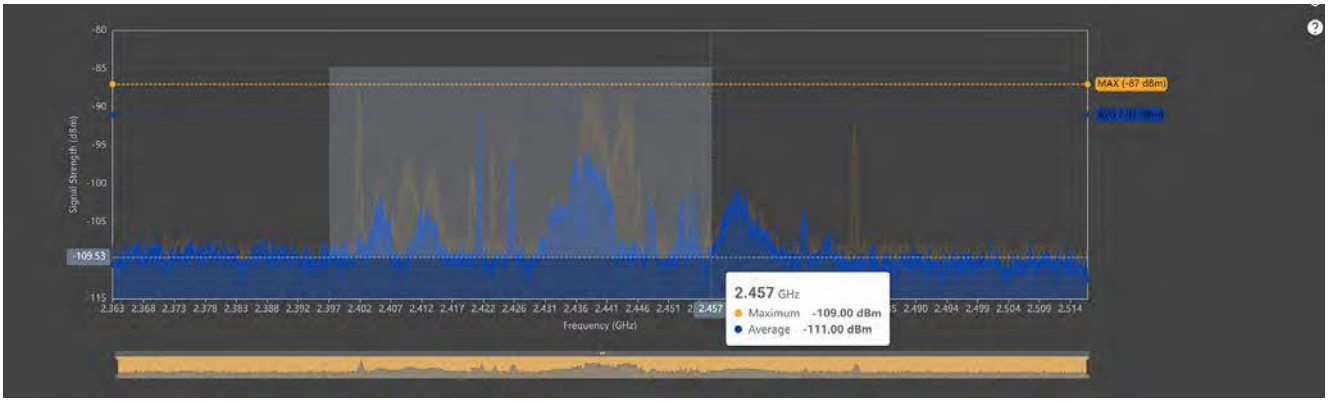
This range can be moved up and down the spectrum by clicking and dragging the slider position control tab.

The zoom slider can also be helpful to visualise where the Spectrum Display is zoomed to when using the 'Draw to Zoom Chart' tool.

Click the 'Reset Graph Zoom' button to reset the graph and the zoom slider.

10.6.5 Crop (Draw to Zoom Chart)

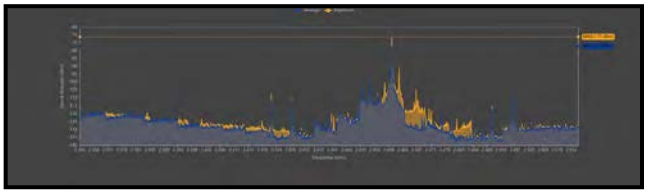
This tool allows the user to drag over an area on the Spectrum Display to zoom the interface to the selected area. This will crop both vertically and horizontally. To reset the interface to view the full spectrum, click 'Reset Graph Zoom'.



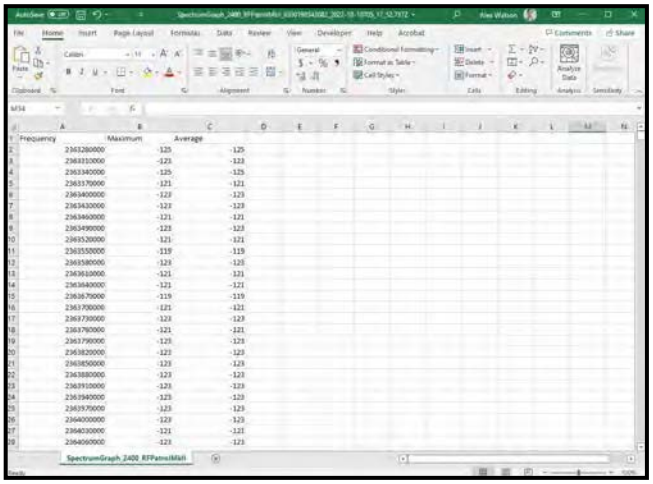
10.6.6 Download Data

Download a .csv spreadsheet file and high resolution snapshot of the Spectrum Display as a .png image.

Exported .png Spectrum View

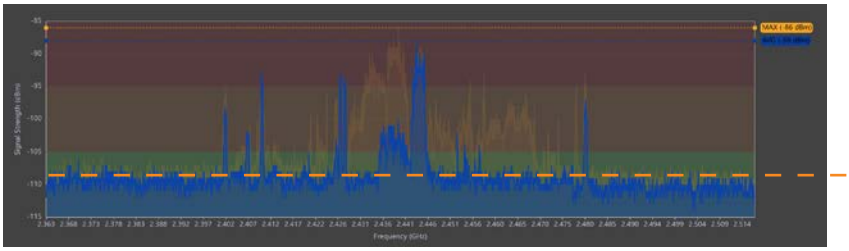


Exported .csv Spectrum View Data



10.6.7 Performance Overlay

Enabling the performance overlay will display a colour gradient on the Spectrum View. The coloured bands help to distinguish low, medium and high spectrum interference. When using the Spectrum View for conducting site surveys, the performance overlay allows the user to quickly distinguish the relative noise levels in each frequency band.



Noise Floor:

The noise floor indicates the level of ambient RF signals in the region of the spectrum. It is represented by the lowest average level on the Spectrum View.

Green
Optimal Performance Region

If the noise floor falls within this region the detection performance of the sensor will be at its best.

Orange
Reduced Performance Region

If the noise floor falls within this region the detection performance of the sensor may be slightly reduced.

Red
Poor Performance Region

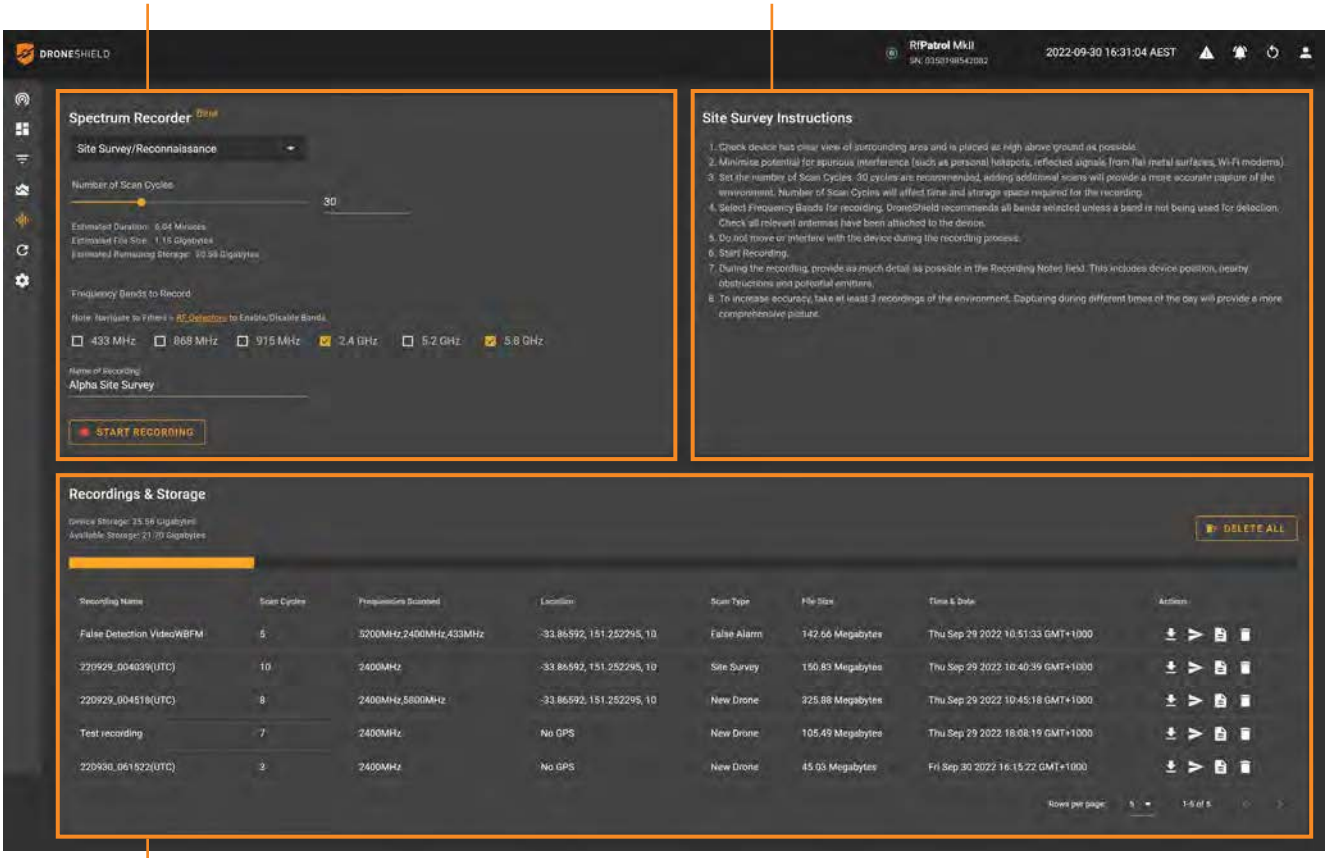
If the noise floor falls within this region the detection performance of the sensor may be greatly reduced.

10.7 Spectrum Recorder

The Spectrum Recorder is a feature which allows the user to record new drones, false alarms or capture site survey data. The tool allows users to configure recordings by frequencies and number of scan cycles, which affect the total recording time and size.

Spectrum Recorder Scan Settings

Instructions for the Selected Recording Type



Saved Spectrum Recordings

10.7.1 Use Scenarios

The Spectrum Recorder can be used under a number of circumstances to collect radio-frequency data from the surrounding environment.

Capturing New Drones

If the user has access to a drone which is not on the DroneShield RFAI Detection Engine, they can conduct a simple recording of its control signature to the controller. This recording can be sent to DroneShield for analysis, additional model training and potentially inclusion in the RFAI Detection Engine. End users should consult with a DroneShield representative before considering a new drone recording.

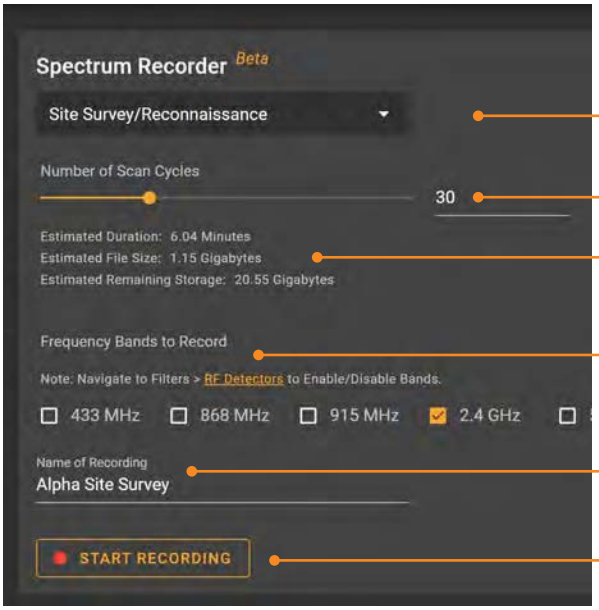
Capturing False Alarm Signatures

If the RF device is capturing repeated false detections (which have been verified not to be originating from a drone), the user may unintended detections. These are sent to DroneShield to improve detection performance and reliability. End users should consult with a DroneShield representative before recording false detection signatures.

Conducting Site Surveys

One of the most utilised scenarios is to conduct a site survey for larger fixed installations. The RfPatrol can be set up in the intended installation point, capturing multiple datasets on the RF noise floor, detectable emissions and cluttered frequency bands.

10.7.2 Recording Settings



Scan Type

New Drone, Site Survey / Reconnaissance or False Alarm.

Scan Cycles

Recommended: 30

The number of times the device will scan using the input parameters. Higher scan cycles give a more accurate picture of the environment, but will increase the recording duration and file size. Only a single recording file will be generated.

Scan Information

This will display the predicted duration, file size and system storage remaining. These figures are based on the number of scan cycles and the selected frequency bands.

Recording Frequency Bands

Select which frequency bands to record on. Before enabling a frequency band, ensure the correct antenna has been attached to the corresponding antenna port.

Recording Name

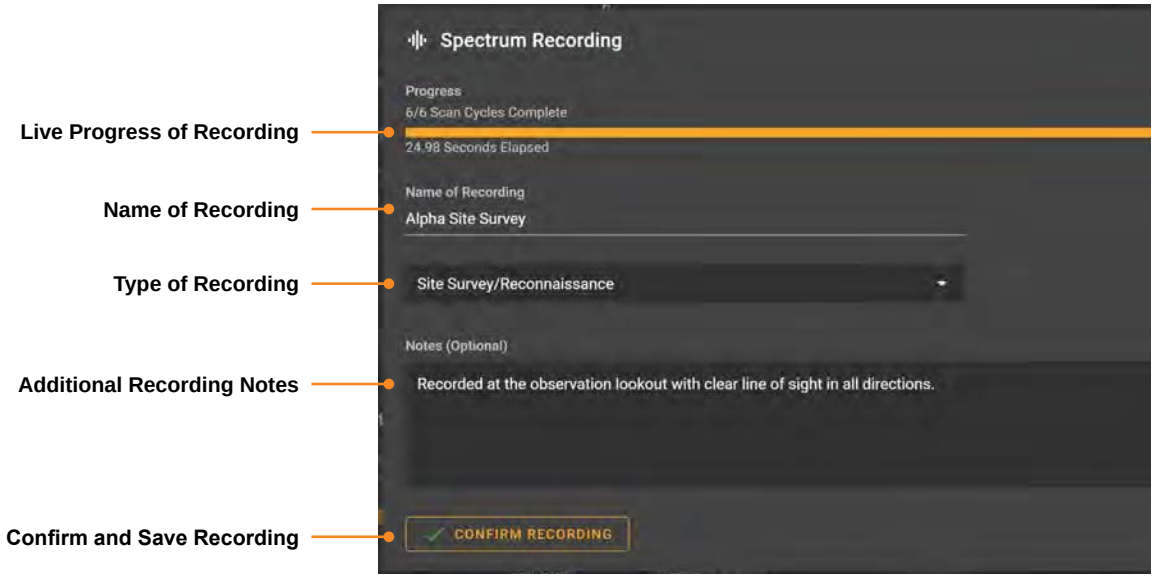
Name the recording and note additional details, such as environmental factors and the placement of the sensor.

Start Recording

Once settings have been configured, select this button to begin the recording process. During a recording, active detections will be temporarily paused.

10.7.3 Progress Interface

When the user starts a spectrum recording, the live progress will be shown on both the device and the device manager interface. A recording can be stopped while in progress, with the existing progress of the recording being saved to the device.



10.7.4 Viewing & Actioning Recordings

Recording Name
Displays the user set recording name

Frequencies Scanned
Lists the frequencies included in the recording

Scan Type
New Drone / Site Survey / False Alarm

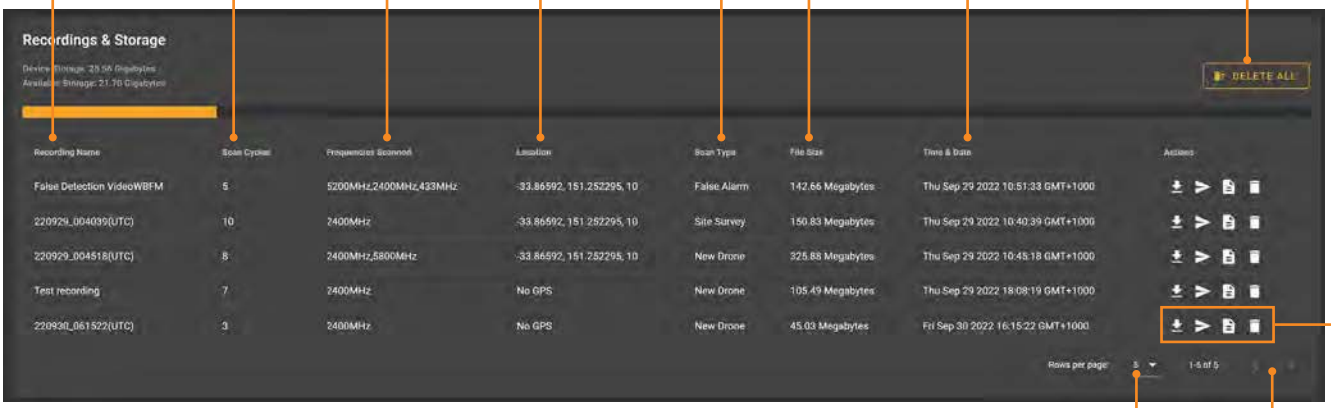
Time & Date
Displays the local time of recording

Scan Cycles
Lists the number of scan cycles completed in the recording

Location
Will automatically populate if the device has access to GPS

File Size
Size of the recording file in MB

Delete All
Deletes all recordings saved on the device



Change how many rows are displayed per page

Scroll through pages of recordings

Download a local copy of the recording file

Send the recording file to DroneShield for analysis (requires an active network connection)

View and edit details of the recording.

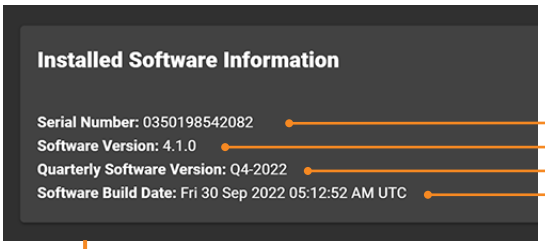
Delete recording from local device

10.8 Updates Tab

The RfPatrol MKII firmware and software can be updated with update files provided by DroneShield.

Users can download the latest software updates, user manuals and brochures from the DroneShield Access Portal at https://portal.droneshield.xyz using the account provided by DroneShield.

If users are unable to access their DroneShield Access Portal account or require an invite, please contact support@droneshield.com



Serial Number
This number is tied to the device and cannot be changed

Software Version
The software loaded onto the RfPatrol MKII

Release Quarter

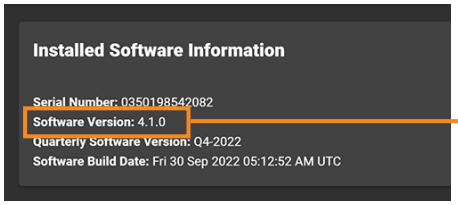
Software Build Date

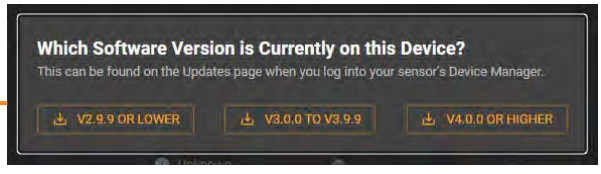
"10.8.1 Perform a Software Update"

Download Product User Manual
(requires an active internet connection)

Link to DroneShield Portal
(requires an active internet connection)

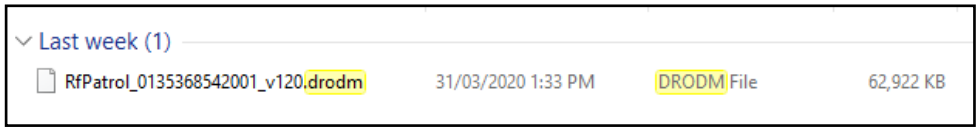
When updating an RF device, ensure the correct software version is downloaded and installed on to the device. If the device is a number of versions behind the latest available, multiple installations may be required. When accessing update files from the DroneShield Portal, the user will be prompted to check what version is currently installed on the device.





10.8.1 Perform a Software Update

1. Click *Choose file*... and match serial label of the *RfPatrol MKII* with the *.drodm* update file.
   For update files, an RfPatrol MKII Annual Software Update subscription must be active (Item No. 112-1).
   For more information, please contact support@droneshield.com or authorised DroneShield distributor.



Do not change the name of the update file or this will cause the software update to fail.

After clicking DEPLOY, do not attempt to re-attempt installation. The installation status screen may take up to 20 minutes to appear, during which time the device may not appear to be installing.

2. Once the update file is selected, click *Deploy*. Allow up to 75 minutes for the device to update at which point it will display "Software Update Complete".

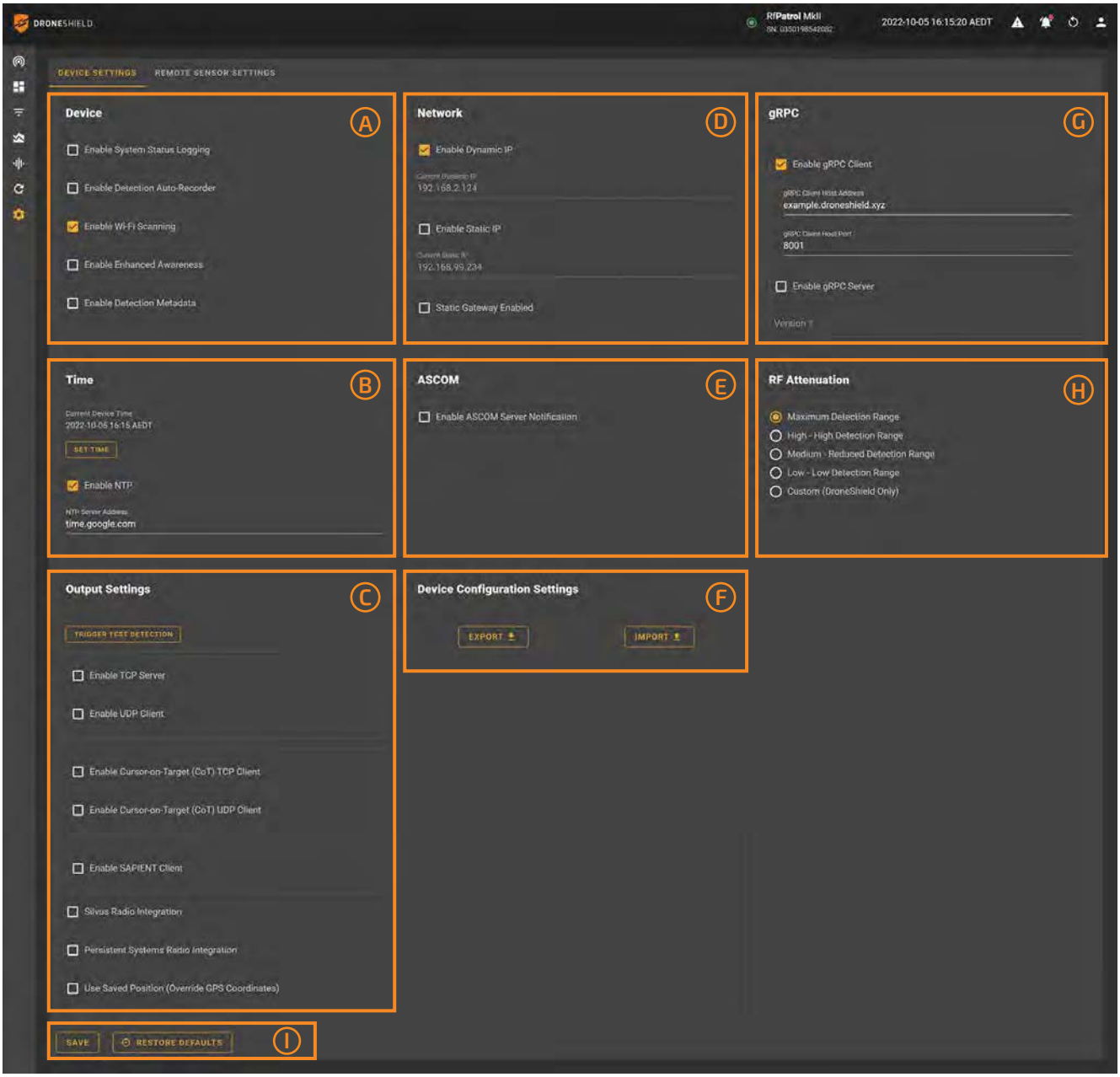
DURING THE UPDATE- Do not cut the power to the RfPatrol MKII during the update process as this may damage the device.

3. After device has automatically restarted, log back into the RfPatrol MKII device and confirm the software version has updated to match the update file.

10.8.2 NTP Clock Reset

If after performing a software update the device does not display the correct time, plug the device into a network with an Internet connection, allowing the clock to reset via NTP.

10.9 Settings



A: Device	
"10.9.1	System Status Logging"
"10.9.2	Detection Auto-Recorder"
"10.9.3	Wi-Fi Scanning"
"10.9.4	Enhanced Awareness"
"10.9.5	Detection Metadata"

B: Time	
"10.9.6	Time Settings"

C: Output Settings	
"10.9.7	Trigger Test Detection"
"10.9.8	TCP"
"10.9.9	UDP"
"10.9.10	CoT TCP Client"

C: Output Settings	
"10.9.11	CoT UDP Client"
"10.9.12	SAPIENT"
"10.9.13	Silvus Radio"
"10.9.14	Persistent Systems Radio"
"10.9.15	Use Saved Position"

D: Network	
"10.9.16	Dynamic IP"
"10.9.17	Static IP"
"10.9.18	Set Subnet"
"10.9.19	Static Gateway"

E: ASCOM	
"10.9.20	ASCOM Server Notifications"

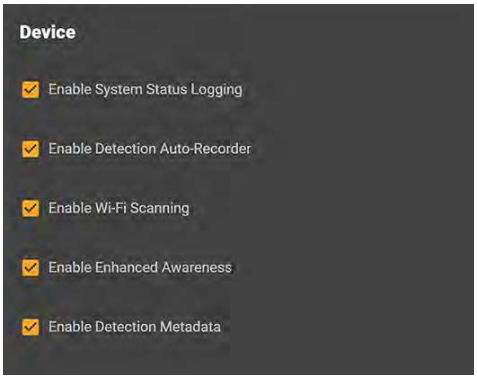
F: Device Configuration Settings	
"10.9.21	Device Configuration Settings"

G: gRPC	
"10.9.22	gRPC Client"
"10.9.23	gRPC Server"

H: RF Attenuation	
"10.9.24	RF Attenuation"

I: Save/Restore Defaults	
"10.9.25	Save/Restore Defaults"

A: Device



10.9.1 System Status Logging

Default: Disabled

Sends system status information to the cloud for sensor diagnostic monitoring.

Caution - when setting is enabled additional network data will be used. Feature is disabled by default.

10.9.2 Detection Auto-Recorder

Default: Disabled

New detections will be automatically recorded and sent to the cloud for diagnostics.

Caution - when setting is enabled additional network data will be used. Feature is disabled by default.

10.9.3 Wi-Fi Scanning

Default: Enabled

Enable device scanning on Wi-Fi channels.

10.9.4 Enhanced Awareness

Default: Disabled

Enhanced Awareness is a feature that displays detected Wi-Fi information under a dedicated table on the 'Detections' page.

Important - device must be power cycled when enabling/ disabling the Enhanced Awareness feature.

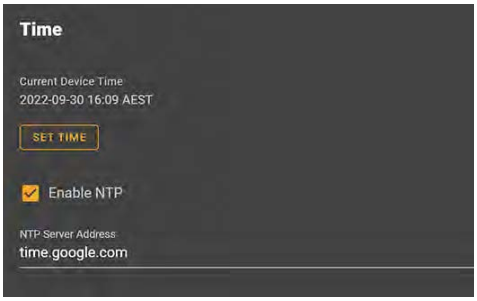
Note - Wi-Fi Scanning must be enabled to use this feature.

10.9.5 Detection Metadata

Default: Disabled

Additional signal features and data points are extracted from RF IQ data streams and appended to valid streamed API data payloads (applies to detection payloads only)

B: Time



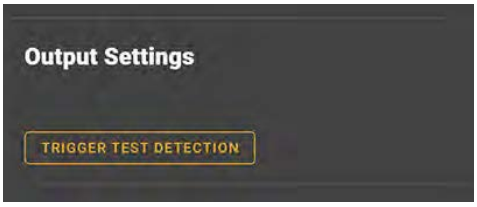
10.9.6 Time Settings

Default: Enabled

NTP Server Address: time.google.com

Determines where the device is to source its network time. The RfPatrol MKII is able to store and maintain time settings when disconnected from power and data.

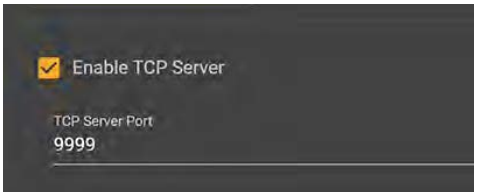
"SET TIME" sets the internal clock to the web-browser time



C: Output Settings

10.9.7 Trigger Test Detection

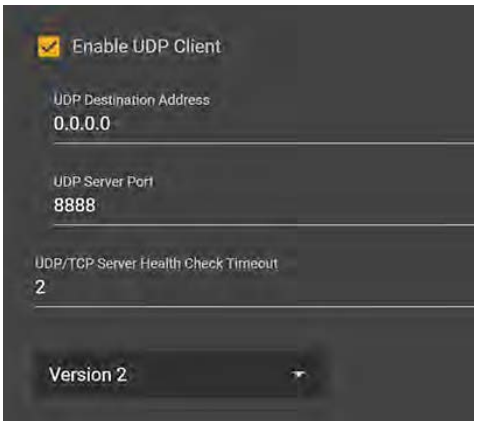
Allows users to test integration methods with the sensor or demonstrate a detection without requiring an active drone. This will trigger a test detection for 20 detection counts.



10.9.8 TCP

Default: Disabled

Enable or disable the TCP server within the device and adjust port



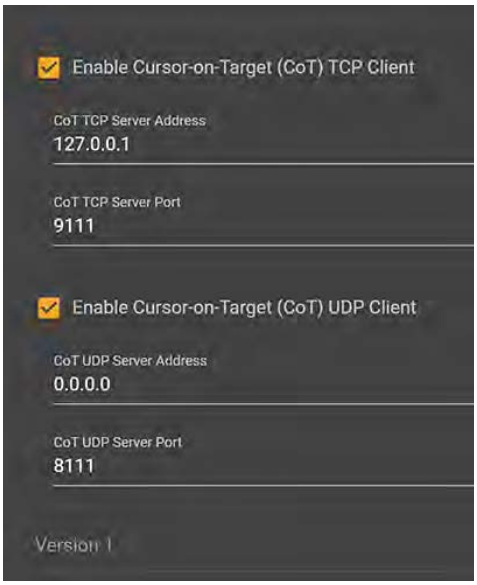
10.9.9 UDP

Default: Disabled

Enable or disable the UDP server within the device and adjust address, port and health-check timeout settings

The API version can be selected, meaning users who have integrated with a previous version can maintain backward compatibility.

For API Version Schema, see "12. APIs"



10.9.10 CoT TCP Client

Default: Disabled

Enable or disable the CoT TCP Client within the device and set address and port values

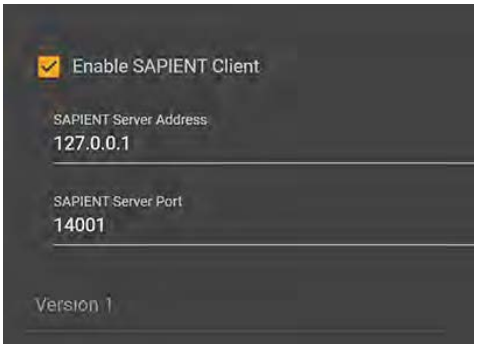
NOTE: Changes will only take affect after the device is rebooted

10.9.11 CoT UDP Client

Default: Disabled

Enable or disable the CoT UDP Client within the device and set address and port values

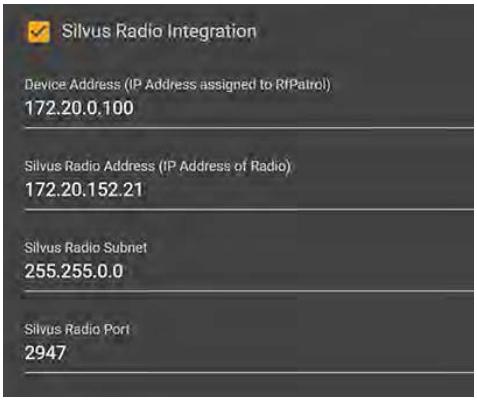
NOTE: Changes will only take affect after the device is rebooted



10.9.12 SAPIENT

Default: Disabled

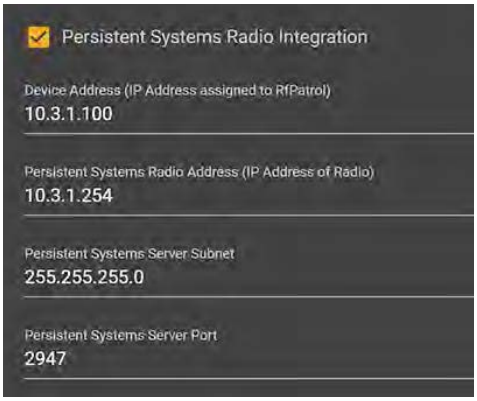
Enable or disable the SAPIENT client within the device and set the destination server address and server port values.



10.9.13 Silvus Radio

Default: Disabled

Set up device to operate with Silvus radio



10.9.14 Persistent Systems Radio

Default: Disabled

Set up device to operate with Persistent Systems radio

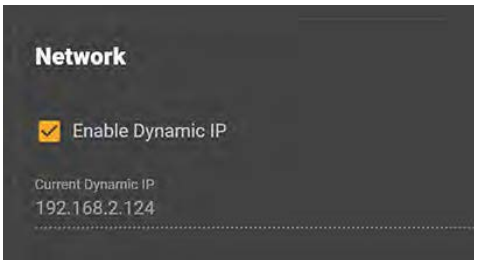
10.9.15 Use Saved Position

Default: Disabled

Set device location manually

NOTE: This will override live coordinates

D: Network



10.9.16 Dynamic IP

Default: Enabled

Allows the device to be allocated a Dynamic IP when plugged into a router. Multiple devices can be accessed simultaneously by logging into the Device Manager via the Dynamic IP.

Note- accessing the device via a Dynamic IP address still requires the user to be on the same network as the device.

10.9.17 Static IP

Default: Enabled

Set static IP: 192.168.99.234

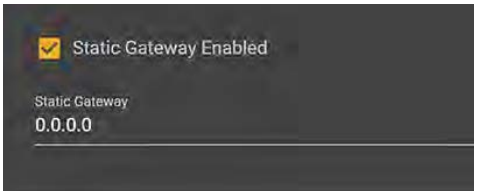
A static address that allows the user to connect to the device when plugged into a router or direct into a PC. Only one device can be accessed at a time with this method.

10.9.18 Set Subnet

Default: Enabled

Set Subnet: 255.255.255.0

Set the static IP subnet



10.9.19 Static Gateway

Default: Disabled

Enable and set the static gateway.

Disabling or changing the static IP can make it difficult to connect to the RfPatrol MKII and may require the customer contact a DroneShield technician. You cannot disable both static and dynamic IP.

E: ASCOM

10.9.20 ASCOM Server Notifications

Default: Disabled

Enable or disable the ASCOM Server Notifications for the RfPatrol MKII device.

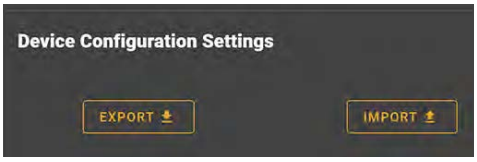
When enabled and configured correctly, the user will receive drone alert notifications via the Unite Axess mobile app.

When a drone is detected by the RfPatrol MKII, a detection notification is sent immediately. When the drone has not been detected for 5 minutes, a second notification is sent alerting the user the drone is no longer present.

The notification alerts are as follows:

English	Norwegian
“Drone Detected”	*“Drone I området!”*
“Drone Disappeared”	*“Drone forlater området!”*

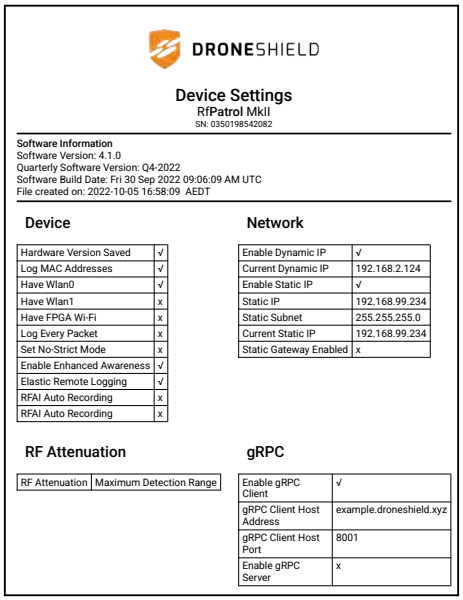
F: Device Configuration Settings



10.9.21 Device Configuration Settings

The configuration of device settings can be exported to PDF or JSON files.

Configurations can also be imported from the local machine as a previously saved JSON file.



DRONESHIELD

Device Settings
RfPatrol MkII
SN: 0350198542082

Software Information
Software Version: 4.1.0
Quarterly Software Version: Q4-2022
Software Build Date: Fri 30 Sep 2022 09:06:09 AM UTC
File created on: 2022-10-05 16:58:09 AEDT

Device

Hardware Version Saved	√
Log MAC Addresses	√
Have Wlan0	√
Have Wlan1	x
Have FPGA Wi-Fi	x
Log Every Packet	x
Set No-Strict Mode	x
Enable Enhanced Awareness	√
Elastic Remote Logging	√
RFAI Auto Recording	x
RFAI Auto Recording	x

Network

Enable Dynamic IP	√
Current Dynamic IP	192.168.2.124
Enable Static IP	√
Static IP	192.168.99.234
Static Subnet	255.255.255.0
Current Static IP	192.168.99.234
Static Gateway Enabled	x

RF Attenuation

RF Attenuation	Maximum Detection Range

gRPC

Enable gRPC Client	√
gRPC Client Host Address	example.droneshield.xyz
gRPC Client Host Port	8001
Enable gRPC Server	x

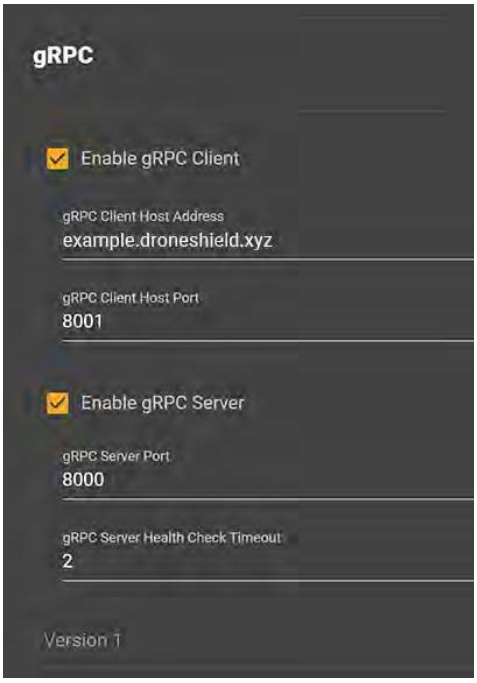
NTP

Enable NTP	√
NTP Server Address	time.google.com

Output Settings

Enable TCP Server	x
Enable UDP Client	x
Enable Cursor-on-Target (CoT) TCP Client	x
Enable Cursor-on-Target (CoT) UDP Client	x
Enable SAPIENT Client	x
Silvus Radio Integration	x
Persistent Systems Radio Integration	x
Use Saved Position (Override GPS Coordinates)	x

Exported RfPatrol MKII device configuration (PDF)



G: gRPC

10.9.22 gRPC Client

Default: Enabled

Client Host address: example.droneshield.xyz

Client Host port: 8001

Determines the location of the gRPC server the device is to communicate with. Host port determins the port used to communicate with the gRPC server.

10.9.23 gRPC Server

Default: Disabled

Enable or disable the gRPC Server within the device and adjust port and healthcheck timeout settings.

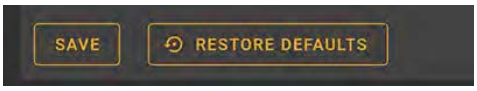
H: RF Attenuation

10.9.24 RF Attenuation

Default: Maximum Detection Range

Determines the level of attenuation for RF detections. By default “Maximum Detection Range” is selected. If the user wishes to limit the RfPatrol MKII’s range, the attenuation can be set to “Medium” or “Low”. “Custom” should only be selected if specifically advised by DroneShield.

I: Save/Restore Defaults

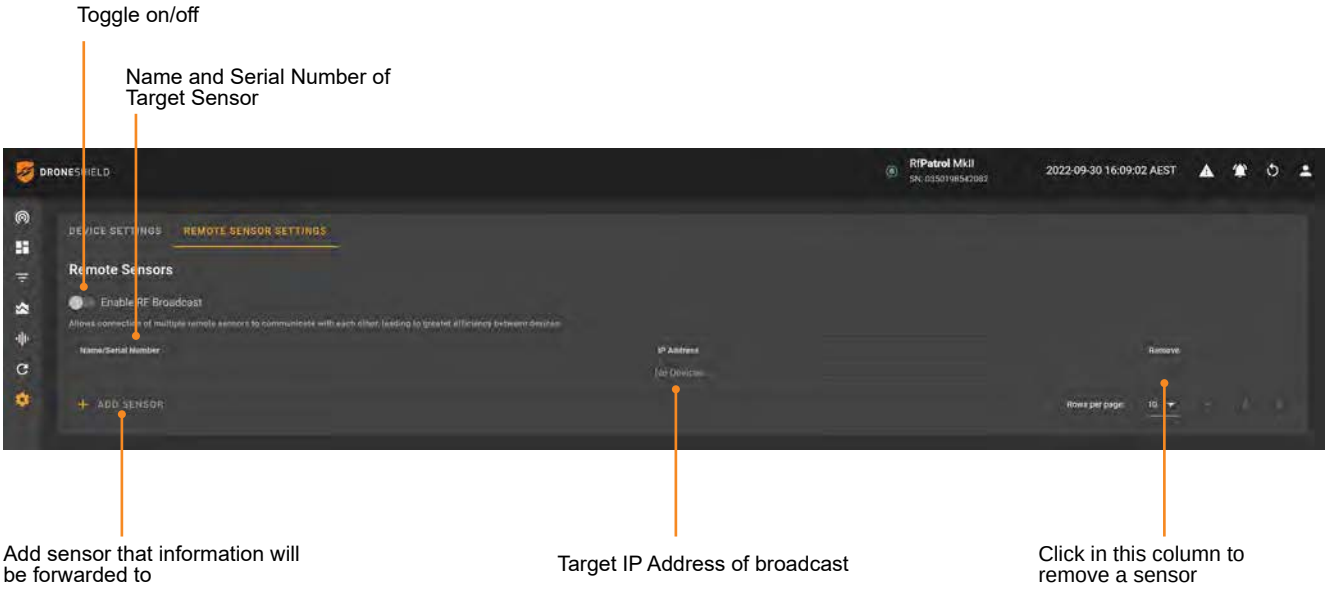


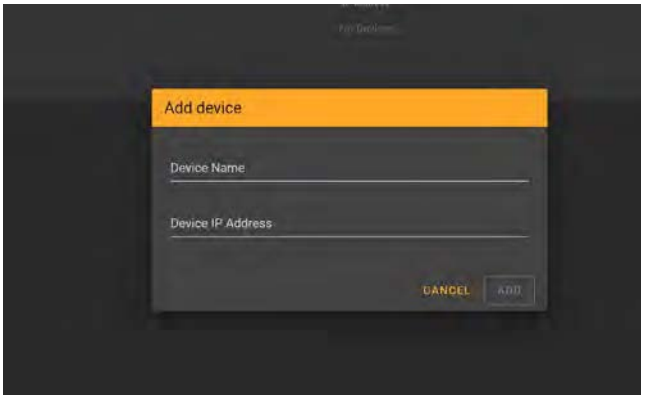
10.9.25 Save/Restore Defaults

Changes to the settings page must be saved before they will take effect. Restoring defaults is a helpful troubleshooting tool if the device is not operating correctly.

10.9.26 Remote Sensor Settings Tab

When enabling ‘RF Broadcast’ the sensor will forward detections to any linked sensors (linked using IP address). A linked sensor will detect a observed signal faster if that signal has already been detected by a sensor that has ‘RF Broadcast’ enabled.





To add a device to RF Broadcast, click ‘ADD SENSOR’.

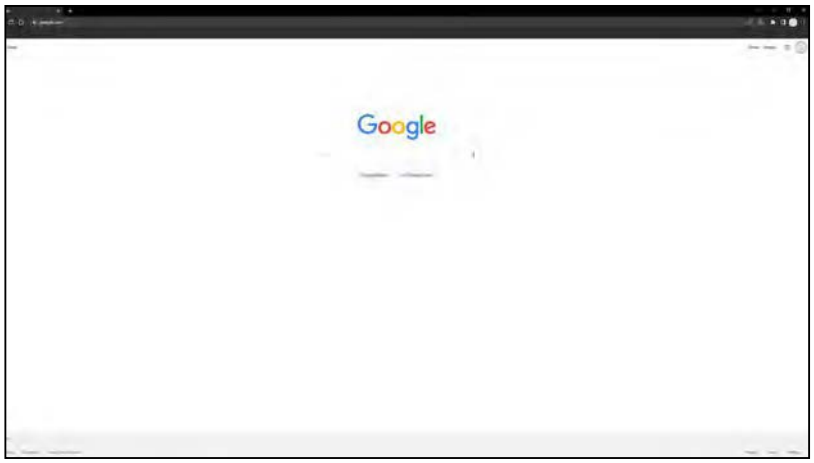
Fill the ‘Device Name’ and ‘Device IP Address’ fields and click ‘ADD’

10.10 Downloading from Device Manager

10.10.1 Changing Download Folder

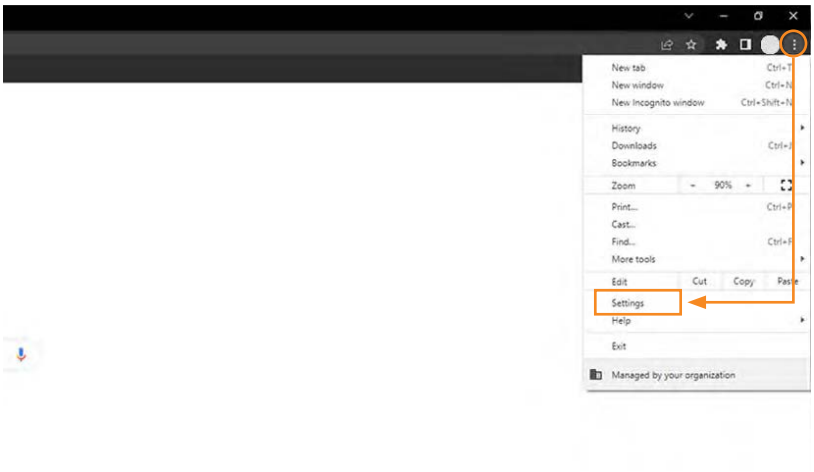
The Device Manager allows the user to download device configurations, detection logs, spectrum views and spectrum recordings. To change the destination folder for downloaded files, the user must change the default location in their browser settings.

Below is a guide on changing the download folder in Google Chrome.



1.

Open the browser that is used to access the Device Manager

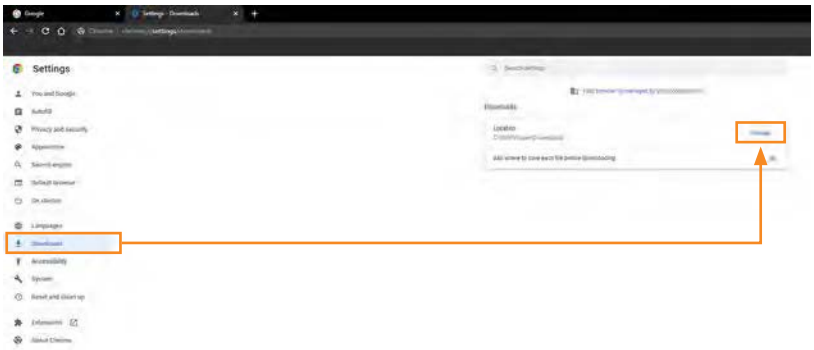


2.

Go to Settings

3.

Select Downloads Settings

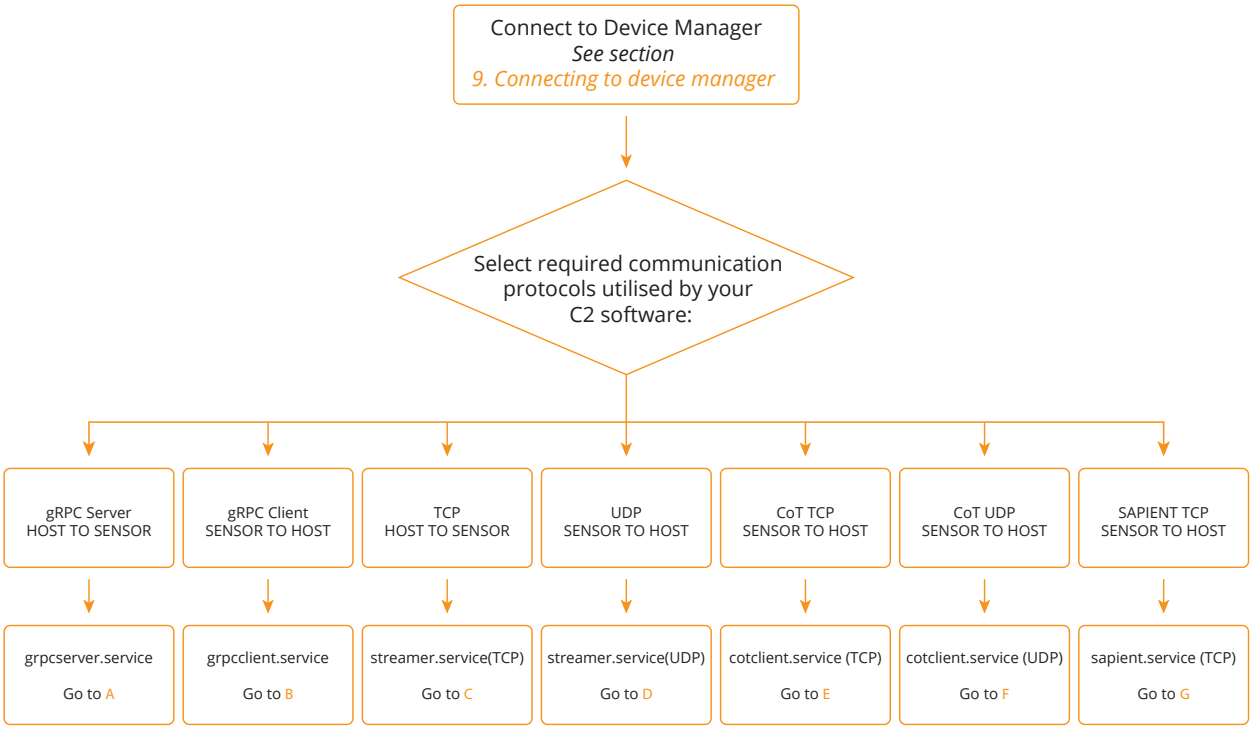


4.

Change the default download folder to the preferred location. Enabling the shown toggle will prompt the user to specify the download location upon each download.

11. Device Integration Overview

When integrating a device into a third party C2, follow the diagram below for information on connecting to the device manager, and where to find relevant communication protocol information and settings:



Option A: Host connects to sensor via gRPC, sensor will stream detections and status to host
See "10.9.23 gRPC Server" on page 83

Option B: Sensor connects to Host via gRPC, sensor will stream detections and status to host
See "10.9.22 gRPC Client" on page 83

Option C: Host connects to sensor via JSON (TCP default port 9999 listener on sensor), sensor will stream detections and status to host
See "10.9.8 TCP" on page 79

Option D: Sensor connects to Host via JSON (UDP default port 8888 listener on host), sensor will stream detections and status to host
See "10.9.9 UDP" on page 79

Option E: Sensor connects to Host via COT XML (TCP default port 9111 listener on host), sensor will stream detections to host
See "10.9.10 CoT TCP Client" on page 79

Option F: Sensor connects to Host via COT XML (UDP default port 8111 listener on host), sensor will stream detections to host
See "10.9.11 CoT UDP Client" on page 79

Option G: Sensor connects to Host via SAPIENT (TCP default port 14001 listener on host), sensor will stream detections to host
See "10.9.12 SAPIENT" on page 80

11.1 RF Signal Metadata Schema

A multitude of signal features can be extracted as metadata from RF IQ data streams. Each extracted data point is produced with a corresponding error or probabilistic confidence score.

Feature	Description	Units	Status
Angle of arrival (AoA)	An angle value indicating the direction from which an emitter is emitting signals and how they may be reflecting within the surrounding physical environment.	Degrees or radians	Implemented in DRO systems
Angular Velocity	The velocity of the radial movement of an emitter derived using AoA over time.	deg/s	Not yet Implemented in DRO systems
Received signal strength indicator (RSSI) – Instantaneous value	A measurement of power indicating how well the signal from an emitter can be detected.	dBm	Implemented in DRO systems
RSSI variation over time	This metric indicates how an emitter's signal power changes over time (e.g. approaching or departing emitter).	dBm/s	Implemented in DRO systems
Signal hopping frequencies	The set of frequencies at which the signal occurs at (defined as signal hops).	MHz	Implemented in DRO systems
Signal hopping distribution type	The type of probability distribution of signal hops during the hopping period.	categorical (e.g. pseudorandom)	Not yet Implemented in DRO systems
Signal hopping rate	The probability distribution of signal hop inter-arrival times during the hopping period.	milliseconds	Not yet Implemented in DRO systems
Signal periodicity	A relative measure of how often a signal appears/disappears throughout its transmission period. This feature can be derived using RSSI, AoA as well as signal hop characteristics.	milliseconds	Not yet Implemented in DRO systems
Convolutional neural network (CNN) prediction score	A probabilistic confidence score of what transmission protocol a given emitter's signal is classified as based on the library of known protocols the CNN has been trained on.	A value in the range of [0,1] for each transmission protocol category.	Implemented in DRO systems
Relative spectral entropy metric	The relative measure of a signal's spectral power distribution used in quantifying the amount of potential information contained in the signal. (e.g. quantify data scrambling, whitening etc.)	A probabilistic score in the range of [0,1] with 0 indicating low entropy and 1 indicating high entropy.	Not yet Implemented in DRO systems
Modulation technique	A score indicating whether a signal has amplitude, frequency or phase modulation characteristics.	A probabilistic score in the range of [0,1] for each categorical value	Not yet Implemented in DRO systems
Signal bandwidth	The range of frequencies used for a signal transmission (being the difference in the upper and lower frequency values used in transmission).	MHz	Not yet Implemented in DRO systems
Signal agility	A relative measure of whether a certain emitter alters its transmission modes during operation. E.g. alternating between two different frequency modulation schemes throughout the same transmission period.	A probabilistic score in the range of [0,1] with 0 indicating constant transmission pattern and 1 indicating high likelihood of at least 2 transmission patterns.	Not yet Implemented in DRO systems
Inherent signal activity	A relative measure of whether a recorded data stream contains 2 or more signals undergoing some form of cooperative or adversarial interaction. For example, a cooperative interaction being controller/receiver scenarios, while adversarial being transmitter/jammer scenarios.	A probabilistic score in the range of [0,1] with 0 indicating no observable signal activity and 1 indicating high likelihood of inherent signal activity. This score is derived by labelling uniquely distinguishable signals with cooperation keys.	Not yet Implemented in DRO systems

12. APIs

Device integrates with DroneSentry-C2. For instructions on connecting to DroneSentry-C2 GUI, contact support@droneshield.com

When using DroneSentry-C2, RfPatrol MKII supports IP-based alerts (email, SMS, XML).

All detections are logged for later evidence retrieval.

12.1 JSON

12.1.1 JSON v1 - Detection

Detection Schema

```
{
   "APIVersion": "string",
   // API Version 1 shown below
   "Data": {
      "AbsoluteAngleOfArrivalRadians": float,
      // The angle in radians of a detection relative to north. Only valid for devices that can determine Angle of Arrival and are connected to a CompassOne
      "AngleOfArrivalErrorRadians": float,
      // Beam width measure of error of the direction of the detection (only applies to RfOne Mk II sensors)
      "AngleOfArrivalRadians": float,
      // The direction of a detection in radians, relative to the sensor
      "CorrelationKey": "string",
      // Identifies repeated detections of the same drone across sensors (e.g. 2004290681)
      "DetectionCount": int,
      // Approximate count of the number of times the same signal has been seen (resets if the detection is lost)
      "EpochTimeMilliSeconds": int,
      // Epoch time
      "FrequencyHertz": int,
      // Frequency in Hz of the detection (e.g 2455000000)
      "IsDrone": bool,
      // Drone or controller (defaults to drone if not known)
      "MacAddress": "string",
      // MAC address of the detected device (only applies to Wi-Fi detections)
      "Name": "string",
      // SSID of the device (applies to Wi-Fi detections only)
      "Protocol": "string",
      // Name of the protocol detected
      "RSSI": int,
      // RSSI signal strength of the detection e.g. ~ -25 to -90
      "SerialNumber": "string",
      // Serial Number of the rf_sensor (13 character string, that is always numeric and can have a leading zero)
      "SignalBars": int,
      // Linear Signal strength approximation per drone type.
      "Type": "string",
      // “Radio” or “Wifi”
      "Vendor": "string"
      // Vendor name as a string e.g “DJI” “Yuneec”
   },
   "Type": "string"
}
```

Detection Sample

```
{
   "APIVersion": "1.1",
   "Data": {
      "AbsoluteAngleOfArrivalRadians": 6.981317007977318,
      "AngleOfArrivalErrorRadians": 0,
      "AngleOfArrivalRadians": 0,
      "CorrelationKey": "2137454737",
      "DetectionCount": 3,
      "EpochTimeMilliSeconds": 1655849442000,
      "FrequencyHertz": 2422000000,
      "IsDrone": true,
      "MacAddress": "60:60:1F:5C:96:BE",
      "Name": "TELLO-5C96BE",
      "Protocol": "Wifi",
      "RSSI": -7,
      "SerialNumber": "0268578542044",
      "SignalBars": 10,
      "Type": "Wifi",
      "Vendor": "DJI"
   },
   "Type": "Detection"
}
```

12.1.2 JSON v1 - Status

Status Schema

```
{
    "APIVersion": "1",
    "Data": {
        "AltitudeMetres": int,
        // Not used
        "BearingDegrees": int,
        // Degrees relative to North (direction the sensor is facing)
        "Disrupting": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming
        "DisruptorBand24Enabled": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming on 2.4GHz
        "DisruptorBand58Enabled": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming on 5.8GHz
        "DisruptorBandGnssEnabled": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming on GNSS
        "DisruptorShutoffTimeoutSeconds": int,
        // Applies to sensor with jamming capabilities showing number of seconds before jamming is timed-out (deactivates)
        "IsAutoDisruptionEnabled": bool,
        // Applies to sensor with jamming capabilities indicating if automatic disruption is enabled on the device
        "LatitudeDegrees": float,
        // Latitude of the sensor (All sensors except RfPatrol have built-in GPS)
        "LongitudeDegrees": float,
        // Longitude of the sensor (All sensors except RfPatrol have built-in GPS)
        "SensorTiltDegrees": int,
        // Tilt of the sensor using internal IMU (only applies to RfOne MkII)
        "SerialNumber": "string",
        // Serial Number of the rf_sensor (13 character string)
        "SoftwareVersion": "string",
        // Sensor software version
        "Status": "string",
        // Status of Sensor
        "TemperatureCelsius": float,
        // Temperature of sensor in degrees celsius
        "UpTimeMilliSeconds": int
        // Milliseconds since the sensor was powered on
    },
    "Type": "string"
}
```

Status Sample

```
{
    "APIVersion": "2",
    "Data": {
        "AltitudeMetres": 0,
        "BearingDegrees": 0,
        "Disrupting": false,
        "DisruptorBand24Enabled": true,
        "DisruptorBand58Enabled": true,
        "DisruptorBandGnssEnabled": true,
        "DisruptorShutoffTimeoutSeconds": 30,
        "IsAutoDisruptionEnabled": false,
        "LatitudeDegrees": -33.8688,
        "LongitudeDegrees": 151.2093,
        "SensorTiltDegrees": 0.0,
        "SerialNumber": "testkey123456",
        "SoftwareVersion": "4.1.0",
        "Status": "Operational",
        "TemperatureCelsius": 58.567405700683594,
        "UpTimeMilliSeconds": 357020
    },
    "Type": "Status"
}
```

12.1.3 JSON v2 - Detection

For information on the types of metadata, see "11.1 RF Signal Metadata Schema".

Detection Schema

```
{
    "APIVersion": "string",
    // API Version 2 shown below
    "Data": {
        "AbsoluteAngleOfArrivalRadians": float,
        // The angle in radians of a detection relative to north. Only valid for devices that can determine Angle of Arrival and are connected to a CompassOne
        "AngleOfArrivalErrorRadians": float,
        // Beam width measure of error of the direction of the detection (only applies to RfOne Mk II sensors)
        "AngleOfArrivalRadians": float,
        // The direction of a detection in radians, relative to the sensor
        "CorrelationKey": "string",
        // Identifies repeated detections of the same drone across sensors (e.g. 2004290681)
        "DetectionCount": int,
        // Approximate count of the number of times the same signal has been seen (resets if the detection is lost)
        "EpochTimeMilliSeconds": int,
        // Epoch time
        "FrequencyHertz": int,
        // Frequency in Hz of the detection (e.g 2455000000)
        "IsDrone": bool,
        // Drone or controller (defaults to drone if not known)
        "MacAddress": "string",
        // MAC address of the detected device (only applies to Wi-Fi detections)
        "Name": "string",
        // SSID of the device (applies to Wi-Fi detections only)
        "Protocol": "string",
        // Name of the protocol detected
        "RSSI": int,
        // RSSI signal strength of the detection e.g. ~ -25 to -90
        "SerialNumber": "string",
        // Serial Number of the rf_sensor (13 character string, that is always numeric and can have a leading zero)
        "SignalBars": int,
        // Linear Signal strength approximation per drone type.
        "Type": "string",
        // “Radio” or “Wifi”
        "Vendor": "string"
        // Vendor name as a string e.g “DJI” “Yuneec”
    },
    "Metadata": dict
    // Dictionary containing RF signal metadata
    "Type": "string"
}
```

Detection Sample


```
{
    "APIVersion": "2",
    "Data": {
        "AbsoluteAngleOfArrivalRadians": 6.981317007977318,
        "AngleOfArrivalErrorRadians": 0.39269908169872414,
        "AngleOfArrivalRadians": 0.0,
        "CorrelationKey": "711338179",
        "DetectionCount": 1,
        "EpochTimeMilliSeconds": 173250000,
        "FrequencyHertz": 5729500000,
        "IsDrone": true,
        "MacAddress": "",
        "Name": "Video",
        "Protocol": "WBFM",
        "RSSI": -60,
        "SerialNumber": "testkey123456",
        "SignalBars": 10,
        "Type": "Radio",
        "Vendor": "Video"
    },
    "Metadata": {
        "AngleOfArrivalDegrees": 0.0,
        "AngleOfArrivalDegreesUncertainty": 22.5,
        "AngularVelocity": null,
        "AngularVelocityUncertainty": null,
        "CNNPredictionScores": {
            "analog_video": 1.0
        },
        "InherentSignalActivity": null,
        "ModulationTechnique": null,
        "RSSIInstantaneous": -60,
        "RSSIInstantaneousUncertainty": 1,
        "RSSITimeVarying": null,
        "RSSITimeVaryingUncertainty": null,
        "SignalAgility": null,
        "SignalBandwidth": null,
        "SignalBandwidthUncertainty": null,
        "SignalFrequencyHz": 5729500000,
        "SignalFrequencyHzUncertainty": 30000,
        "SignalHoppingDistribution": null,
        "SignalHoppingFrequencies": [],
        "SignalHoppingFrequencyUncertainty": 0.03,
        "SignalHoppingRate": null,
        "SignalHoppingRateUncertainty": null,
        "SignalPeriodicity": null,
        "SignalPeriodicityUncertainty": null,
        "SpectralEntropy": null
    },
    "Type": "Detection"
}
```

12.1.4 JSON v2 - Status

Status Schema

```
{
    "APIVersion": "1",
    "Data": {
        "AltitudeMetres": int,
        // Not used
        "BearingDegrees": int,
        // Degrees relative to North (direction the sensor is facing)
        "Disrupting": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming
        "DisruptorBand24Enabled": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming on 2.4GHz
        "DisruptorBand58Enabled": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming on 5.8GHz
        "DisruptorBandGnssEnabled": bool,
        // Applies to sensor with jamming capabilities to tell if sensor is jamming on GNSS
        "DisruptorShutoffTimeoutSeconds": int,
        // Applies to sensor with jamming capabilities showing number of seconds before jamming is timed-out (deactivates)
        "IsAutoDisruptionEnabled": bool,
        // Applies to sensor with jamming capabilities indicating if automatic disruption is enabled on the device
        "LatitudeDegrees": float,
        // Latitude of the sensor (All sensors except RfPatrol have built-in GPS)
        "LongitudeDegrees": float,
        // Longitude of the sensor (All sensors except RfPatrol have built-in GPS)
        "SensorTiltDegrees": int,
        // Tilt of the sensor using internal IMU (only applies to RfOne MkII)
        "SerialNumber": "string",
        // Serial Number of the rf_sensor (13 character string)
        "SoftwareVersion": "string",
        // Sensor software version
        "Status": "string",
        // Status of Sensor
        "TemperatureCelsius": float,
        // Temperature of sensor in degrees celsius
        "UpTimeMilliSeconds": int
        // Milliseconds since the sensor was powered on
    },
    "Type": "string"
}
```

Status Sample

```
{
    "APIVersion": "2",
    "Data": {
        "AltitudeMetres": 0,
        "BearingDegrees": 0,
        "Disrupting": false,
        "DisruptorBand24Enabled": true,
        "DisruptorBand58Enabled": true,
        "DisruptorBandGnssEnabled": true,
        "DisruptorShutoffTimeoutSeconds": 30,
        "IsAutoDisruptionEnabled": false,
        "LatitudeDegrees": -33.8688,
        "LongitudeDegrees": 151.2093,
        "SensorTiltDegrees": 0.0,
        "SerialNumber": "testkey123456",
        "SoftwareVersion": "4.1.0",
        "Status": "Operational",
        "TemperatureCelsius": 58.567405700683594,
        "UpTimeMilliSeconds": 357020
    },
    "Type": "Status"
}
```

12.2 Cursor-on-Target (CoT)

The application must be shape (utilising CoT subschema) aware, one sensor cannot provide an intersection (Point), so a wedge/sector shape is produced. As per CoT documentation the point/radius encompasses the shape.

Link to Cursor on target General guide

Link to Shape Subschema

Link to Sensor Subschema

Workflow

As cursor on target has no status element, only detections are forwarded. When a detection is received the given workflow is adhered too.

If a GPS Compass is present and bearing is given then full CoT is sent with a wedge shape.

Else if a static override is present for bearing (set from the UI)(Will override GPS location) then a full CoT is sent with a wedge shape.

Else failing either of the above send CoT as an omni directional so with the location of sensor and its maximum range for the detection. Omnidirectional devices already adhere to this standard.

For RfPatrol, this sensor has no on-board GPS so a GPS multicast is required for the device.

12.2.1 CoT v1 - Detection

Omnidirectional Detection

```
<?xml version="1.0"?>
<event
    version="2.0"
    uid="DS-RF-1802"
    type="a-s-A-M-F-Q"
    time="2022-10-04T05:07:49.813321884Z"
    start="2022-10-04T05:07:49.813321884Z"
    stale="2022-10-04T05:07:50.813321884Z"
    how="m-g">
    <detail>
        <sensor
            azimuth="0.0"
            fov="360.0" />
        <detection
            absolute_angle_of_arrival_radians="6.981317"
            angle_of_arrival_error_radians="0.3926991"
            angle_of_arrival_radians="0"
            correlation_key="2273514911"
            detection_count="2"
            epoch_time_milli_seconds="278380"
            frequency_hertz="5736500000"
            is_drone="true"
            mac_address=""
            name="DJI AUT XIA"
            protocol="OS OFDM"
            rssi="-58"
            serial_number="testkey123456"
            signal_bars="10"
            type="Radio"
            vendor="DJI AUT XIA" />
    </detail>
<point
    lat="-33.8688000"
    lon="151.2093000"
    ce="1000.0"
    hae="100.0"
    le="0.0" />
</event>
```

Directional Detection

```
<?xml version="1.0"?>
<event
    version="2.0"
    uid="DS-RF-session1"
    type="a-s-A-M-F-Q"
    time="2022-10-04T05:07:49.813321884Z"
    start="2022-10-04T05:07:49.813321884Z"
    stale="2022-10-04T05:07:50.813321884Z"
    how="m-g">
    <detail>
        <shape>
            <polyline closed="true">
                <vertex lat="-33.9477959"
                lon="151.1696472"></vertex>
                <vertex lat="-33.9861640"
                lon="151.1413742"></vertex>
                <vertex lat="-33.9824011"
                lon="151.1350276"></vertex>
            </polyline>
        </shape>
        <detection
            absolute_angle_of_arrival_radians="6.981317"
            angle_of_arrival_error_radians="0.3926991"
            angle_of_arrival_radians="0"
            correlation_key="2273514911"
            detection_count="2"
            epoch_time_milli_seconds="278380"
            frequency_hertz="5736500000"
            is_drone="true"
            mac_address=""
            name="DJI AUT XIA"
            protocol="OS OFDM"
            rssi="-58"
            serial_number="testkey123456"
            signal_bars="10"
            type="Radio"
            vendor="DJI AUT XIA" />
    </detail>
<point
    lat="-33.8688000"
    lon="151.2093000"
    ce="1000.0"
    hae="100.0"
    le="0.0" />
</event>
```

DroneSentry-C2 Intersection Detection

```
<?xml version="1.0"?>
<event
    version="2.0"
    uid="DroneShield-rfx-147"
    type="a-s-A-M-H-Q"
    time="2022-10-04T05:07:49.813321884Z"
    start="2022-10-04T05:07:49.813321884Z"
    stale="2022-10-04T05:07:50.813321884Z"
    how="m-g">
    <detail>
        <uuid tadilj="147" />
        <track course="0.0" speed="0.0" />
        <sensor az="0.0" fov="0.1" />
        <detection frequency_hz="2465500000"
        protocol="LightBridge OFDM"
        vendor="DJI"
        correlation_key="12345678"
        mac_address=""
        is_drone="true"
        rssi="-33" />
    </detail>
    <point
    lat="-33.8688000"
    lon="151.2093000"
    ce="1.89"
    hae="0"
    le="1.87"
    />
</event>
```

12.3 SAPIENT

Sensing for Asset Protection with Integrated Electronic Networked Technology (SAPIENT) is a concept that combines modular autonomous sensing with fusion and sensor management. Like Cursor on Target (CoT), directional sensors will produce a cone detection unless the requirements for this are not met. Without directional information it will produce a detection with an positional error that is the range of the sensor.

Link to SAPIENT interface guide

12.3.1 SAPIENT v1 - Registration

Registration Sample:

```
<?xml version="1.0"?>
<SensorRegistration>
   <timestamp>2022-06-22T11:47:33.4019333Z</timestamp>
   <sensorID>22</sensorID>
   <sensorType></sensorType>
   <name>DroneShield multi sensor</name>
   <shortName>DS</shortName>
   <heartbeatDefinition>
      <heartbeatInterval units="seconds" value="10"></heartbeatInterval>
      <sensorLocationDefinition>
         <locationType units="metres" datum="WGS84" zone="W30">UTM</locationType>
      </sensorLocationDefinition>
      <heartbeatReport category="sensor" type="sensorLocation" units="" onChange="false"></heartbeatReport>
   </heartbeatDefinition>
   <modeDefinition type="Permanent">
      <modeName>Default</modeName>
      <modeDescription>Normal Operation</modeDescription>
      <settleTime units="seconds" value="5"></settleTime>
      <maximumLatency units="seconds" value="2"></maximumLatency>
      <scanType>Fixed</scanType>
      <trackingType>None</trackingType>
      <duration units="units" value="1"></duration>
      <detectionDefinition>
         <locationType units="metres" datum="WGS84" zone="W30">UTM</locationType>
         <geometricError type="Standard Deviation" units="metres" variationType="Linear with Range">
            <performanceValue type="eRmin" value="0.1"></performanceValue>
            <performanceValue type="eRmax" value="0.5"></performanceValue>
         </geometricError>
         <detectionReport category="detection" type="confidence" units="probability" onChange="false"></detectionReport>
      </detectionDefinition>
      <taskDefinition>
         <concurrentTasks>0</concurrentTasks>
         <regionDefinition>
            <regionType>Area of Interest</regionType>
            <regionType>Ignore</regionType>
            <settleTime units="seconds" value="5"></settleTime>
            <locationType units="decimal degrees-metres" datum="WGS84" zone="30U" north="Grid">UTM</locationType>
            <classFilterDefinition type="All">
               <filterParameter name="confidence" operators="All"></filterParameter>
            </classFilterDefinition>
         </regionDefinition>
         <command name="Request" units="Registration, Heartbeat, Stop, Start" completionTime="10" completionTimeUnits="seconds"></command>
      </taskDefinition>
   </modeDefinition>
</SensorRegistration>
```

12.3.2 SAPIENT v1 - Detection

Detection Sample:

```
<?xml version="1.0"?>
<DetectionReport>
    <timestamp>2022-03-02T23:44:36.4204995Z</timestamp>
    <sourceID>1</sourceID>
    <reportID>4</reportID>
    <objectID>12345678</objectID>
    <taskID>0</taskID>
    <rangeBearing>
        <R>1000</R>
        <Az>30.5</Az>
        <Ele>0</Ele>
        <Z>0</Z>
        <eR>0</eR>
        <eAz>45</eAz>
        <eEle>0</eEle>
        <eZ>0</eZ>
    </rangeBearing>
    <detectionConfidence>0.99</detectionConfidence>
    <class type="Drone">
        <confidence>0.99</confidence>
    </class>
    <behaviour type="Flying">
        <confidence>0.99</confidence>
    </behaviour>
</DetectionReport>
```

12.3.3 SAPIENT v1 - Status

Status Sample:

```
<?xml version="1.0"?>
<StatusReport>
   <timestamp>2022-06-22T11:48:57.2817910Z</timestamp>
   <sourceID>22</sourceID>
   <reportID>101</reportID>
   <system>OK</system>
   <info>New</info>
   <sensorLocation>
      <location>
         <X>6.378137e+06</X>
         <Y>0</Y>
         <Z>0</Z>
      </location>
   </sensorLocation>
</StatusReport>
```

12.4 gRPC

RfPatrol MKII outputs data using gRPC.

12.4.1 Repository

The Git repository for gRPC integration can be found at the following link:

Git Clone https://customer:1q7JM7Xez-ymJh4k-1xV@gitlab.com/droneshield/simulator-onpremise.git

This Git repository contains gRPC protocol files required to integrate gRPC as well as gRPC simulator files for testing.

12.4.2 Outputs

Detection

Provides all available information about a detection as well as some identifying information about the RfPatrol MKII should the user have multiple sensors.

Field	Type	Description
serial_number	string	Serial Number of the rf_sensor (13 character string)
epoch_time_seconds	uint64	Seconds since the sensor was powered on
frequency_hertz	uint64	Frequency in hz of the detection e.g. 2455000000
rssi	sint32	RSSI signal strength of the detection e.g. -32
angle_of_arrival_radians	float	Direction of the detection in radians (only applies to RfOne MKII sensors) Negative values = left of boresight Positive values = right of boresight
angle_of_elevation_radians	float	Angle of elevation of the detection in radians (only applies to RfOne MKII sensors)
name	string	SSID of device for Wi-Fi detections
mac_address	string	Mac address of the detected device (Only applies to Wi-Fi detections
detection_type	DetectionType	“RADIO” or “Wi-Fi"
vendor	string	Vendor name as a string e.g “DJI” “Yuneec”
protocol	string	Name of the protocol detected e.g “Lightbridge 2”
angle_of_arrival_error_radians	float	Error of the direction of the detection (only applies to RfOne MKII sensors)
correlation_key	string	Correlation Key identifies the detection to relative uniqueness to be compared across detections and sensors
is_drone	bool	Drone or controller (defaults to drone if not known)
signal_bars	sint32	Normalizing (make linear) RSSI for different drone protocols / frequency / bandwidth, specifically for DS
metadata	bytes	Contains metadata of the detection

FilterSetting

Not currently implemented

Field	Type	Description
enabled	bool	
min_window_range	float	
max_window_range	float	

PriorDetectionSetting

Not currently implemented

Field	Type	Description
enabled	bool	
count	unit32	

StatusUpdate

Status update provides the state of the RF sensor including location

Field	Type	Description
serial_number	string	Serial Number of the rf_sensor (13 character string)
ip_address	string	ip address of the sensor
latitude_degrees	double	latitude of the sensor
longitude_degrees	double	longitude of the sensor
bearing_degrees	double	direction the sensor is facing
up_time_seconds	uint64	time in microseconds since the sensor was powered up
temperature_celsius	float	temperature according to the onboard thermometer
OperationalState	enum	Unspecified = 0 Operating = 1 Testing = 2 Fault = 3
Filters	message	FilterSetting azimuth = 1 FilterSetting elevation = 2
prior_detection_setting	PriorDetectionSetting	Filter based on minimum number of required detections before reporting a detection (not yet provided)
operationalstatus	enum	Unknown = 0 Good = 1
altitude_meters	float	
disrupting	bool	For sensors that are jamming capable such as DSXDir
software_version	string	Device firmware version
disruptor_band_24_enabled	bool	Is 2.4GHz band disruption enabled
disruptor_band_58_enabled	bool	Is 5.8GHz band disruption enabled
disruptor_band_gnss_enabled	bool	Is GNSS band disruption enabled
disruptor_shutoff_timeout_seconds	uint64	The number of seconds the disruptor will automatically timeout when disrupting
auto_disruption_enabled	bool	Is auto disruption enabled on the disruptor
sensor_tilt_degrees	float	Tilt angle of the sensor from horizontal
up_time_milliSeconds	uint64	Up time of the sensor

StatusUpdate.Filters

Filters applied to the sensor (not finalised)

Field	Type	Description
azimuth	FilterSetting	
elevation	FilterSetting	

DetectionType

Field	Number	Description
UNSPECIFIED	0	
RADIO	1	
WIFI	2	

StatusUpdate.OperationalState

State the sensor is in (not finalised)

Field	Number	Description
UNSPECIFIED	0	
OPERATING	1	
TESTING	2	

StatusUpdate.OperationalStatus

Status of the sensor (not finalised)

Field	Number	Description
UNKNOWN	0	
GOOD	1	

ComputeDetectionsRequest

Streamed Detections described in detail elsewhere

Field	Type	Description
detection	Detection	

ComputeDetectionsResponse

Empty, unused message

ComputeStatusRequest

Streamed status updates described in detail elsewhere

Field	Type	Description
update	StatusUpdate	

ComputeStatusResponse

Empty, unused message

Compute

When an RF sensor is configured to call out to a particular server it uses this service. The detections and status updates are streamed in the request and the responses are unused.

Method Name	Request Type	Response Type	Description
Detections	ComputeDetectionsRequest stream	ComputeDetectionsResponse	Detections streams detections from the sensor to the compute server
StatusUpdates	ComputeStatusRequest stream	ComputeStatusResponse	StatusUpdates streams status updates from the sensor to the compute server

RFDetectionsRequest

Empty request

RFDetectionsResponse

Field	Type	Description
detection	Detection	RF Sensor status update

RFStatusRequest

Empty request

RFStatusUpdate

Rf Sensor status update

Field	Type	Description
update	StatusUpdate	RF Sensor status update

RfSensor

When an RfSensor is configured as a server it can be called directly and will respond with a stream of detections and status updates while the requests are empty and unused

Method Name	Request Type	Response Type	Description
Detections	RFDetectionsRequest	RFDetectionsResponse stream	Streams detections from the rf sensor
StatusUpdates	RFStatusRequest	RFStatusUpdate stream	Stream for status updates from the rf sensor

Scalar Value Types

.proto Type	Notes	C++	Java	Python	Go	C#	PHP	Ruby
double		double	double	float	float64	double	float	Float
float		float	float	float	float32	float	float	Float
int32	Uses variable-length encoding. Inefficient for encoding negative numbers – if your field is likely to have negative values, use sint32 instead.	int32	int	int	int32	int	integer	Bignum or Fixnum (as required)

.proto Type	Notes	C++	Java	Python	Go	C#	PHP	Ruby
int64	Uses variable-length encoding. Inefficient for encoding negative numbers – if your field is likely to have negative values, use sint64 instead.	int64	long	int/long	int64	long	integer/ string	Bignum
uint32	Uses variable-length encoding.	uint32	int	int/long	uint32	uint	integer	Bignum or Fixnum (as required)
uint64	Uses variable-length encoding.	uint64	long	int/long	uint64	ulong	integer/ string	Bignum or Fixnum (as required)
sint32	Uses variable-length encoding. Signed int value. These more efficiently encode negative numbers than regular int32s.	int32	int	int	int32	int	integer	Bignum or Fixnum (as required)
sint64	Uses variable-length encoding. Signed int value. These more efficiently encode negative numbers than regular int64s.	int64	long	int/long	int64	long	integer/ string	Bignum
fixed32	Always four bytes. More efficient than uint32 if values are often greater than 2^28.	uint32	int	int	uint32	uint	integer	Bignum or Fixnum (as required)
fixed64	Always eight bytes. More efficient than uint64 if values are often greater than 2^56.	uint64	long	int/long	uint64	ulong	integer/ string	Bignum
sfixed32	Always four bytes.	int32	int	int	int32	int	integer	Bignum or Fixnum (as required)
sfixed64	Always eight bytes.	int64	long	int/long	int64	long	integer/ string	Bignum
bool		bool	boolean	boolean	bool	bool	boolean	TrueClass/ FalseClass
string	A string must always contain UTF-8 encoded or 7-bit ASCII text.	string	String	str/ unicode	string	string	string	String (UTF-8)
bytes	May contain any arbitrary sequence of bytes.	string	ByteString	str	[]byte	ByteString	string	String (ASCII-8BIT)

13. Required Ports

This device may require the following ports to be opened for troubleshooting, support and upgrading purposes. Network administrators should be aware of these requirements.

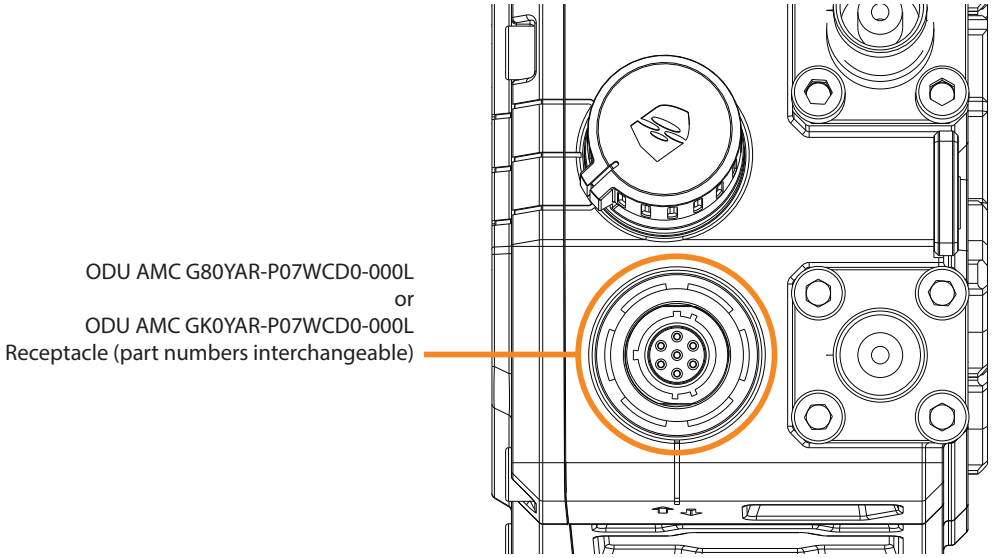
Remote Support Port:	Support Redundancy Ports
UDP 9993	**TCP 3023**
	TCP 3024

14. Third Party Device Integration

14.1 Data Connector Output

The RfPatrol MKII data connector communicates via 10/100 base-T Ethernet standard. The device is provided with a data cable terminated to RJ45 however custom cables can be provided for integration into various battle management systems.

141.1 Data Connector Specification



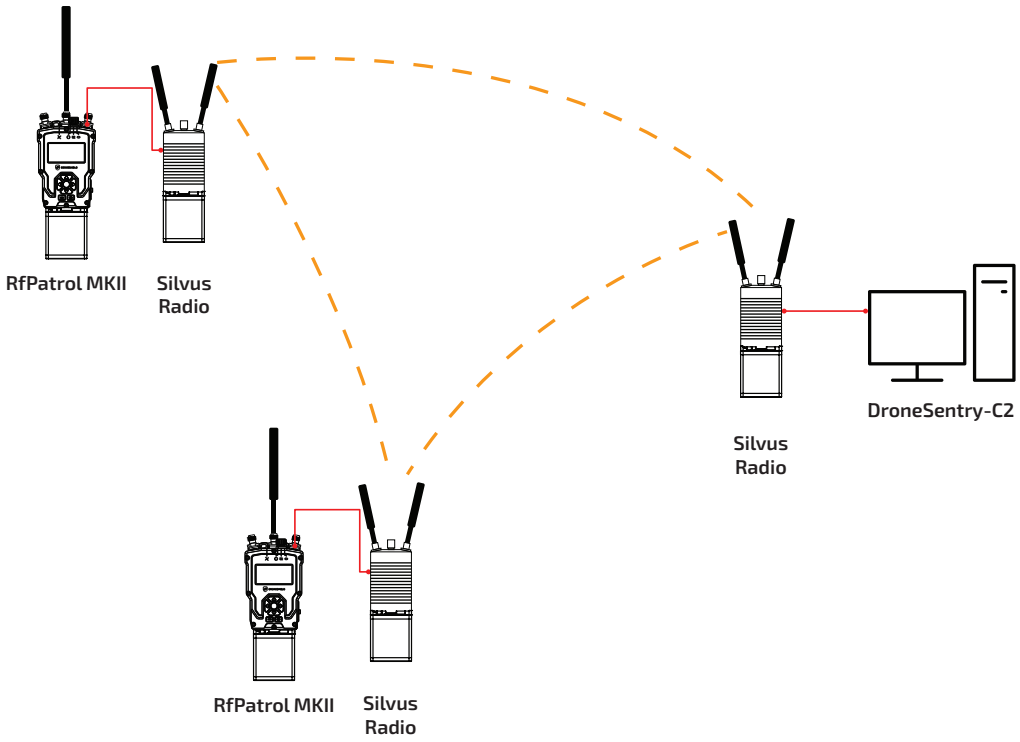
14.1.2 Data Cable Specification

ODU AMC A10YAR-P07XCD0-0000
Plug

14.2 Silvus Radio Integration

The RfPatrol MKII can integrate with the Silvus Radio in order to connect to the DroneSentry-C2 and report the device's position in real time.

Connect to the Silvus radio via the supplied network cables and adaptors.



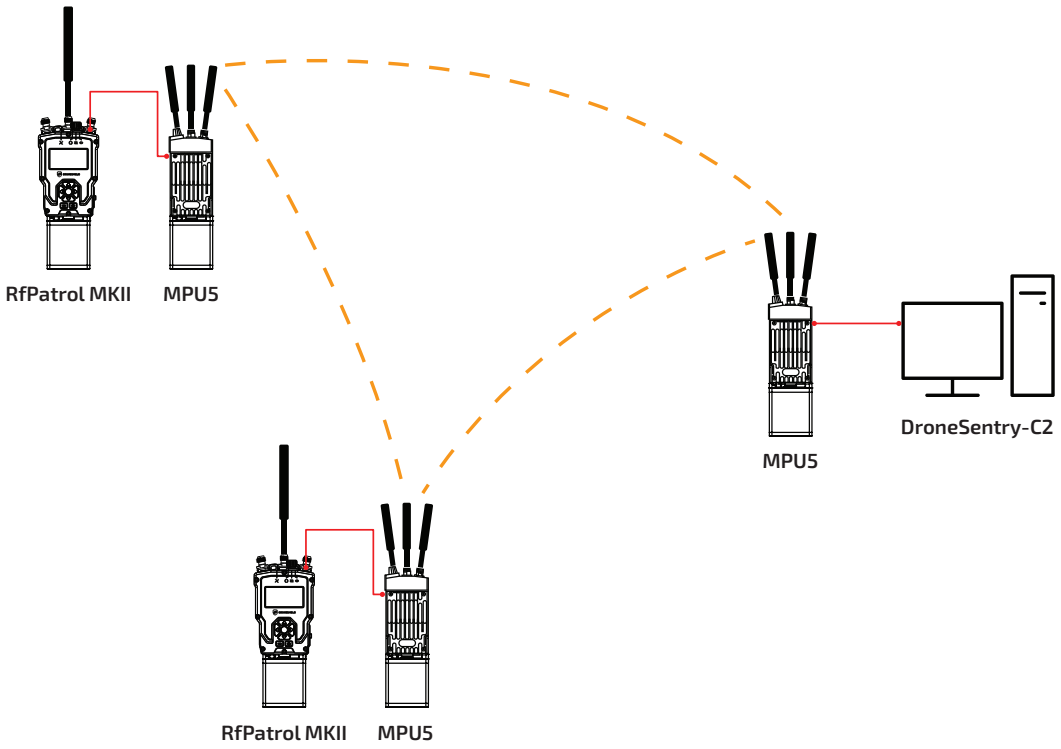
DroneShield recommends that the RfPatrol and Silvus Radio devices are used on the same subnet.

When configuring the network, check the Silvus Radio integration has been enabled under device settings and correct port settings used. See "10.9.13 Silvus Radio"

The Silvus radio must be switched on prior to powering on the RfPatrol MKII. Network cables should be connected when both devices are powered down to correctly configure the network.

14.3 Persistent Systems MPU5 Integration

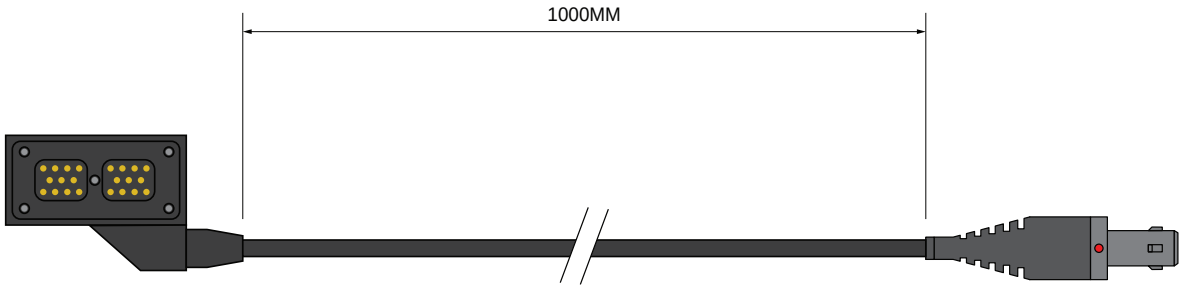
The RfPatrol MKII can integrate with the Persistent Systems MPU5 in order to connect to the DroneSentry-C2 and report the device's position in real time.



When configuring the network, check the Persistent Systems Radio integration has been enabled under device settings and correct port settings used. See "10.9.14 Persistent Systems Radio"

The MPU5 radio must be switched on prior to powering on the RfPatrol MKII. Network cables should be connected when both devices are powered down to correctly configure the network

To connect the RfPatrol MKII to the Persistent Systems MPU5 use the DRO-111-212 Data Cable that can be purchased separately.



NOT TO SCALE

15. Battery Instructions

Supplied Battery: BT-70716BG / BT-70716BV / MP5355-7

Length: 71mm **Width:** 41mm **Height:** 86mm

Weight: BT-70716BG, MP5355-7: 0.36kg (0.80lbs)
BT-70716BV: 0.38kg (0.84lbs)

Battery Notes:

Voltage: 10.8V

Maximum Voltage: 12.6V

Capacity: BT-70716BG: 6.8Ah
BT-70716BV, MP5355-7: 7.0Ah

Operating Temperature: BT-70716BG, BT-70716BV: -30°C to +60°C (-22°F to 140°F)
MP5355-7: -20°C to +60°C (-4°F to 140°F)

Recommended Storage Temperature: -40°C to +40°C (-40°F to +104°F)

Battery Precautions:

Keep the battery away from fire and water

Do not short-circuit the battery pack terminals

Do not force open the battery pack

Provided Battery Charger: 808-064 AC/DC
TS3-022

Specifications

Charger Length: 78mm **Width:** 38mm **Height:** 33mm

Power Supply Length: 144mm **Width:** 31mm **Height:** 60mm

Weight: 0.75kg (1.65lbs)

Battery Charger Notes:

Power Requirements: 100-240VAC, 50/60Hz

Operating Temperature: -30°C to +80°C (-22°F to +176°F)

Battery Charge Time: 6 hours (for depleted battery)

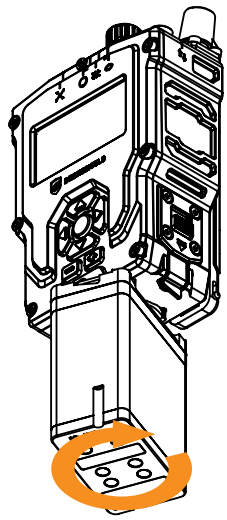
16. Product Acceptance Test

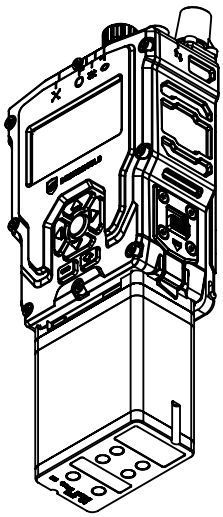
Inspect accessories:

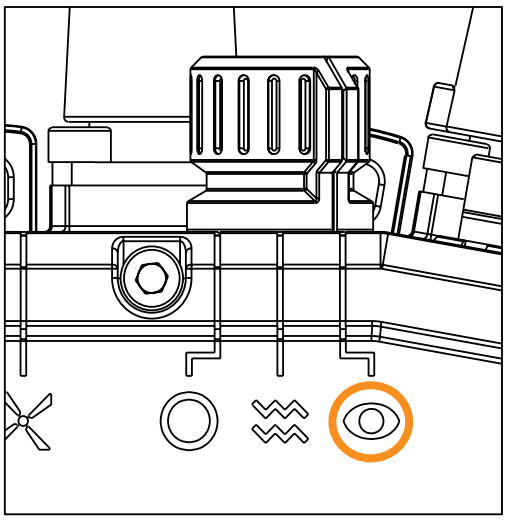
- ☐ All accessories listed in packing list are present
- ☐ All accessories are in good condition

Device power test:

1. Connect *DRO-888-214* Battery to RfPatrol MKII
2. Switch on RfPatrol MKII with rotary power switch







- ☐ RfPatrol MKII powers up and enters scanning display

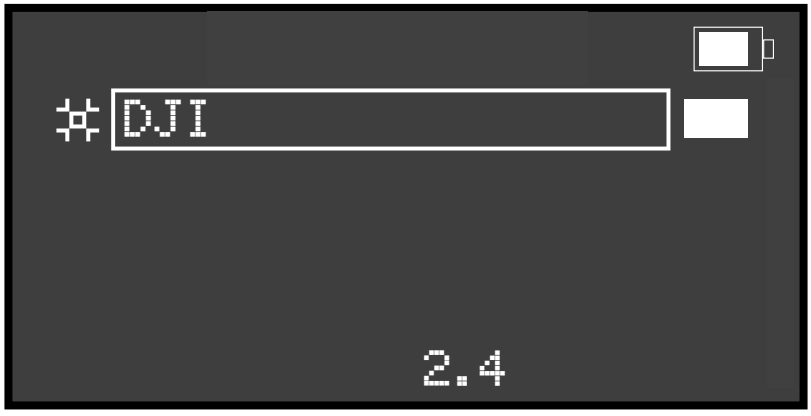
Device data test:

1. Access RfPatrol MKII Device Manager using *DRO-111-210* and *DRO-228-118*
2. Login to Device Manager with Username: user
   Password: user

☐ Login successful
☐ Serial number in Device Manager matches serial label

Operational test detection:

1. Attach *DRO-555-200 ALPHA Antenna* to RfPatrol MKII
2. Turn on DJI Phantom drone



☐ Detection appears on display screen

17. Maintenance

The RfPatrol MKII should undergo routine non technical assessment to ensure its reliable operation.

This assessment can be performed in less than a minute.

17.1 Noncritical Faults

Noncritical faults are faults that will not severely affect the operation of the RfPatrol MKII. They can be repaired at the operator's discretion.

17.1.1 TNC/Military Connector Dust Caps Missing/Damaged

Ensure all three TNC dust caps and two military connector dust caps are intact. If dust caps are damaged or missing, replacements can be purchased from DroneShield or authorised DroneShield distributor.

17.1.2 Display Glass Scratched

Ensure that the display glass is not heavily scratched and no part of the display is obscured by scratches. Heavily scratched display glass can be repaired by DroneShield or authorised DroneShield distributor. (For cracked or shattered screens, refer to "17.2.1 Display Glass Cracked/Shattered" on page 109).

17.1.3 Fogging Behind Display Glass

The RfPatrol MKII display glass may fog up inside if the device changes temperature rapidly. Let the RfPatrol MKII adjust to the ambient temperature and the condensation should disappear. If excessive condensation occurs, the device can be repaired by DroneShield or an authorised DroneShield distributor.

17.1.4 Serial Label

Ensure that the serial label is still attached to the RfPatrol MKII and legible. If the serial label is damaged or missing, a replacement can be sourced from DroneShield or authorised DroneShield distributor.

17.1.5 Connectors Clear of Debris

Ensure that the TNC and military connectors on the top of the RfPatrol MKII device are clear of dirt and debris. Clogged connectors may impact device performance.

17.1.6 Battery Clip

Ensure the battery clip can be raised and lowered and there is no debris in the mechanism. If the battery clip can not be raised and the RfPatrol MKII battery cannot be attached or removed, the battery clip can be disassembled and cleaned. Replacement parts can be purchased from DroneShield or authorised DroneShield distributor.

17.2 Critical Faults

Critical faults may seriously affect the operation of the RfPatrol MKII and should be addressed as soon as possible. Critical faults typically require repair by DroneShield or authorised DroneShield distributors.

17.2.1 Display Glass Cracked/Shattered

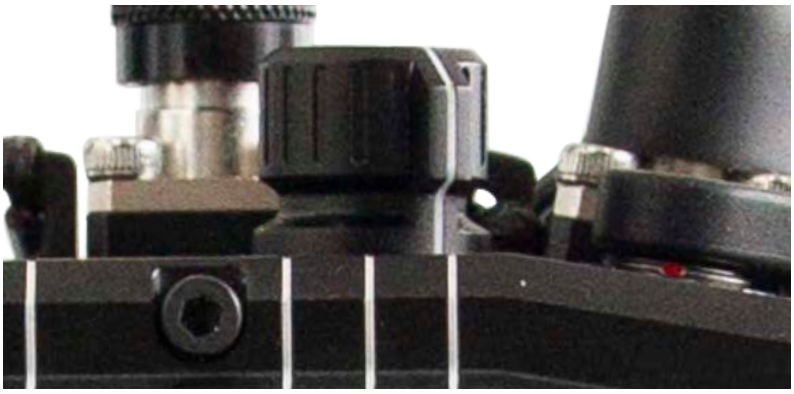
Ensure the display glass is not cracked or shattered. Cracked or shattered display glass can be repaired by DroneShield or authorised DroneShield distributor.

17.2.2 Damaged Battery Connector

Ensure that all three pogo pins on the battery connector are intact and can move freely. If pogo pins are loose, damaged or missing, the RfPatrol MKII may not power on properly. The battery connector can be repaired by DroneShield or authorised DroneShield distributor.

17.2.3 Damaged Rotary Switch

Ensure that the rotary switch can be smoothly turned to each position (OFF, STEALTH, GLIMPSE). If the rotary knob is missing, a replacement can be sourced from DroneShield or authorised DroneShield distributor. If the switch does not turn properly, the RfPatrol MKII should be returned for repair.



17.2.4 RfPatrol MKII Fails to Power On

Ensure the RfPatrol MKII can power on and the display screen activates in the GLIMPSE position. If the RfPatrol MKII fails to power on, check that the battery is connected properly and is charged. If the RfPatrol MKII still fails to power on, the device should be returned to DroneShield or DroneShield distributor.

17.2.5 RfPatrol MKII Displays Error Status

Reboot the RfPatrol MKII. If error persists, see Status Menu and report error to DroneShield or DroneShield distributor.

17.3 Battery Maintenance

Care should be taken with the RfPatrol MKII batteries to ensure they maintain optimum performance through their use and storage.

17.3.1 Battery Storage

RfPatrol MKII batteries should be charged to full every 6 months to ensure optimal battery health. Failure to charge RfPatrol MKII batteries at 6 month intervals may shorten the battery life or result in dead batteries.

Batteries should be stored at -40°C to +40°C (-40°F to +104°F).

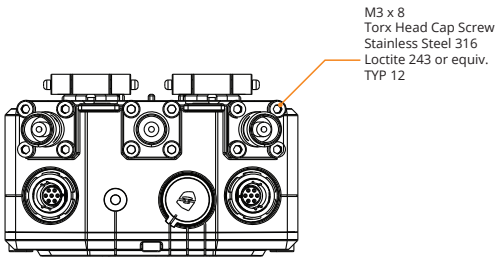
Ensure batteries are stored in a dry location out of direct sunlight.

17.3.2 Battery O-ring

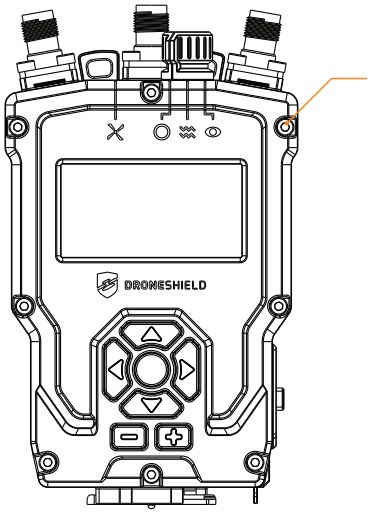
Ensure that the RfPatrol MKII battery O-ring is in place and intact. A damaged battery O-ring may lead to water ingress when attached to the RfPatrol MKII, potentially damaging the battery or the device.

17.4 Fastener Guide

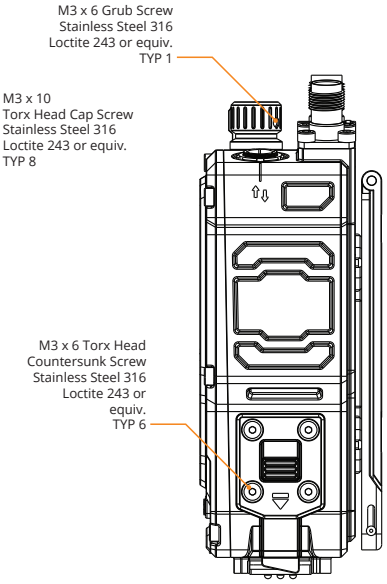
This fastener guide is for the purpose of repair by authorised technical staff only. Any attempt to disassemble or modify the RfPatrol MKII will void the product warranty.



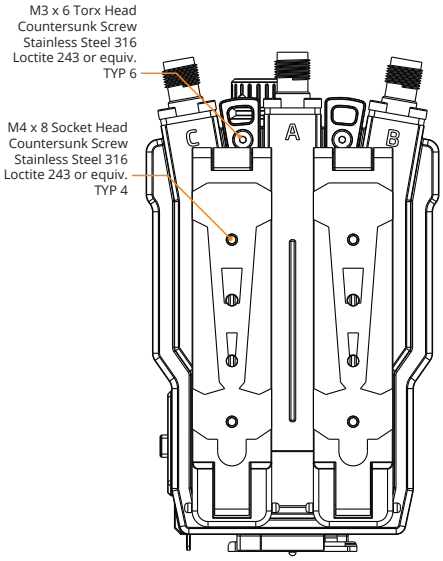
Top View



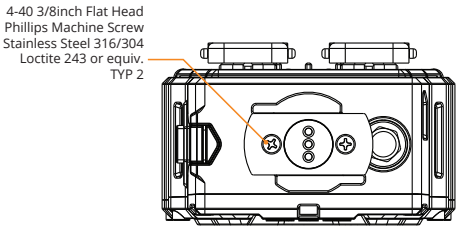
Front View



Side View



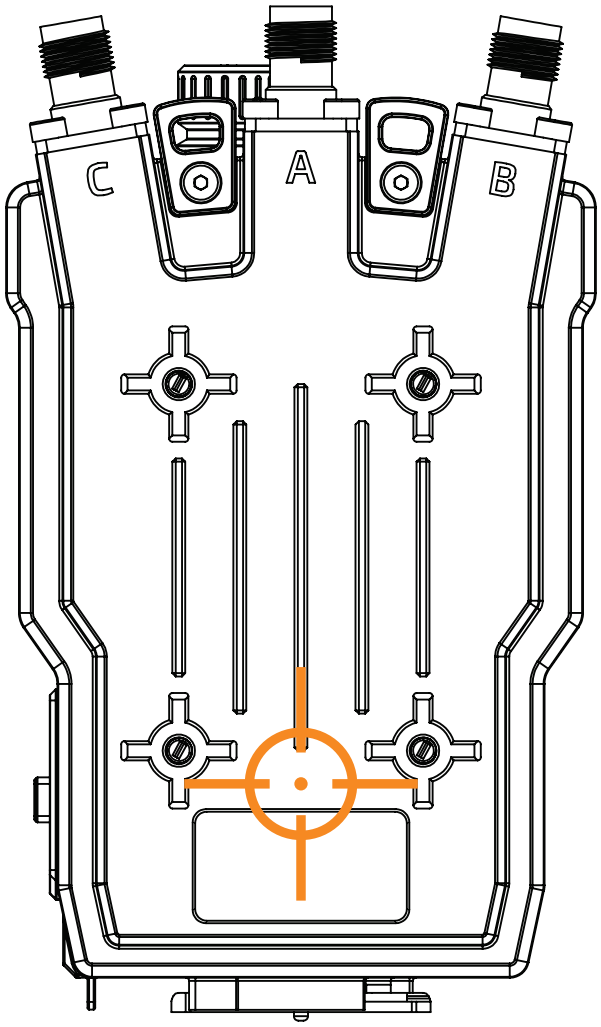
Rear View



Underside View

18. Destruction

Should the RfPatrol MKII need to be destroyed in the field, the device can be drilled in the following location to wipe all recorded data.



19. Specifications

RfPatrol MKII Specifications

Battery Nominal Voltage: 10.8VDC
Effective range:
High RF Environment (Urban): up to 1000m (0.62 miles) line of sight, omni directional
Low RF Environment (Rural): up to 4000m (2.48 miles) line of sight, omni directional
Unit Weight: 780grams (1.72lbs) (without antenna and battery)
User Feedback: LED, OLED display, Vibration, Audio (through headphones)
Unit Colour: Black

Effective Detection Frequencies

2.4GHz ISM
5.2GHz ISM
5.8GHz ISM
433MHz ISM (expansion)
868MHz ISM (expansion)
915MHz ISM (expansion)

Power

Rechargeable Lithium-Ion Battery
NATO-standard military grade battery (common use)
Quick release and reload battery operation
Operating Time: 10+ hour (continuous detection, all bands)

Environment and Operation

Tested to IP67
Tested to MIL-STD-810G: 501.5.i, 502.5.i, 502.5.ii, 503.5.ii, 514.6.i, 516.6.i, MIL-STD-810H: 507.6
Operating temperature: -20°C to +60°C (-4°F to +140°F)

Warranty

12 months from date of shipment

Shipping

Ships in a Rugged Carry Case (IP67)
Carry Case Dimensions: 525mm x 430mm x 215mm (20.6“ x 16.9“ x 8.4“)
Total Shipped Weight: 8.1kg (17.86lbs) - including carry case
HS Code: 85269130

Certifications

FCC ID: 2A9JZ-DRO-035

"This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause interference
- This device must accept any interference, including interference that may cause undesired operation of the device"

20. Contact

For more information, support and technical inquiries please contact your authorised distributor, or DroneShield at **support@droneshield.com**

For product feedback, feature requests and suggestions for improvement, please contact DroneShield at **feedback@droneshield.com**