MILLENIUM
PRODUCTS INC

DRONE DETECTION SYSTEM

WarDragon User Guide

User Guide — Setup, Configuration, and Operation

This guide is the authoritative reference for all current WarDragon systems: Pro and Elite, in Mobile and Drop-In configurations. It covers system setup, networking, detection verification, TAK integration, remote operation, and troubleshooting.

The WarDragon document set

Document	Audience	Use it for
WarDragon User Guide (this document)	Operators, administrators, technical staff	Complete setup, configuration, operation, and troubleshooting. **The source of truth for all technical facts.**
WarDragon Quick Start Guide	New operators	Getting a system running for the first time
WarDragon Drop-In Installation Guide	Installers and integrators	Physical installation of a Drop-In unit: mounting, antennas, DC power, and data connections

> **Note** Where any other document differs from this guide, this guide governs.

Applicability markers

Procedures that differ between configurations are marked. Unmarked content applies to every system.

Marker	Meaning
All systems	Applies to every current WarDragon kit
Mobile only	Ruggedized transport case with a built-in maintenance screen
Drop-In only	DIN-rail integrator enclosure installed into a customer platform
Elite only	Kits with the second SDR (5 GHz and 900 MHz ports)
Legacy Pro v3	Earlier Pro v3 hardware. See Appendix B.

1. System Overview

1.1 What WarDragon Does

WarDragon is a compact, headless RF sensing appliance. It combines dedicated detection radios, a software-defined radio, GPS, and purpose-built software to detect drones across multiple protocols and stream real-time detections into your existing operational picture.

Once configured, it runs unattended and continuously publishes system health, alerts, positions, and track information. No monitor or keyboard is required after initial setup.

1.2 System Variants

Two choices define a kit. **Form factor** is how it deploys. **Tier** is whether it carries the dedicated FPV SDR and x86 compute.

	Pro Mobile	Pro Drop-In	Elite Mobile	Elite Drop-In
Form factor	Hardened carry case	Metal enclosure, DIN-rail	Hardened carry case	Metal enclosure, DIN-rail
Processor	ARM	ARM	x86 Elite	x86 Elite
Dedicated FPV SDR	—	—	Included	Included
FPV awareness	—	—	5 GHz and 900 MHz	5 GHz and 900 MHz
Remote ID	Wi-Fi and Bluetooth	Wi-Fi and Bluetooth	Wi-Fi and Bluetooth	Wi-Fi and Bluetooth
DJI OcuSync	2 and 3, baseline 4	2 and 3, baseline 4	2 and 3, baseline 4	2 and 3, baseline 4
Power	12 V,120 V AC	12 V - 24 V DC	12 V, 120 V AC	12 - 24 V DC
Network	Wi-Fi, Ethernet	DHCP WAN	Wi-Fi, Ethernet	DHCP WAN
TAK output	Yes	Yes	Yes	Yes
DragonScope	Optional	Optional	Optional	Optional

All systems run DragonOS, preloaded. Setup and operation are the same across all variants except where marked.

1.3 What It Detects

Signal	Radio	Band	Kits
Remote ID broadcast	Dual-band Wi-Fi	2.4 and 5 GHz	All
Remote ID broadcast	Bluetooth 5 Long Range	2.4 GHz	All
DJI OcuSync 2 and 3 activity	WarDragon SDR	2.4 and 5.8 GHz	All

Signal	Radio	Band	Kits
DJI OcuSync 4 — baseline awareness	WarDragon SDR	2.4 and 5.8 GHz	All
FPV video activity	Dedicated FPV SDR	5 GHz	Elite
Control and telemetry links	Dedicated FPV SDR	900 MHz	Elite

> **Note** On Elite hardware the front panel is silkscreened **FPV 5.8 Ghz** and **FPV 900**. Those are hardware labels. The 5 GHz port serves FPV video activity; the 900 MHz port serves control and telemetry links.

1.4 System Components

Kits arrive ready to run with DragonOS preloaded. Every kit contains:

- The WarDragon processor — ARM on Pro, x86 Elite on Elite
- WarDragon SDR — DJI OcuSync 2, 3, and 4 activity detection
- Dual-band Wi-Fi adapter — Wi-Fi Remote ID detection, 2.4 and 5 GHz
- Bluetooth 5 Long Range adapter — Bluetooth Remote ID detection
- Dedicated FPV SDR for 5 GHz and 900 MHz — **Elite only**
- Standard paddle antenna set

Mobile adds a hardened carry case with external SMA antenna and GPS connections, external USB and HDMI, integrated cooling fans, a locking external power connector, an AC adapter, and a DC vehicle power adapter.

Drop-In adds a metal enclosure with a DIN-rail clip, a 6-inch DIN-rail strip, and mounting hardware.

> **Note** Antennas are selected and tuned for the configuration and are etched with the port they belong to. Substituting antennas between ports will degrade detection performance.

1.5 DragonScope

DragonScope is an optional annual subscription available on every kit. It decrypts OcuSync 4 to enable full telemetry and drone serial-number identification. Internet connectivity is always required to decrypt DragonScope data.

With DragonScope	Without DragonScope
• OcuSync 4 demodulated and decrypted • Drone serial-number identification and attribution • Full telemetry: drone position (lat/long/altitude), drone velocity (speed/heading/vertical speed), pilot position (lat/long), home point, identification (serial number, drone type), signal data (frequency, RSSI) • Suited to investigative and advanced operations	• OcuSync 4 detected • Per-flight identifier (hash-based) generated for tracking and correlation • Signal-based distance estimation only — no serial-number attribution, no position/velocity telemetry • Suited to general awareness and monitoring

> **Important** DragonScope always requires active internet connectivity to decrypt OcuSync 4 data. Baseline detection does not — it needs no subscription and no cloud connection.

Use the contact form on the website for availability and pricing.

1.6 What WarDragon Will Not Do

- WarDragon is a passive RF sensor for detection and situational awareness. It does not jam, mitigate, interdict, or take control of an aircraft.
- Drones that transmit nothing are not detected.
- Without DragonScope, OcuSync 4 is detected and produces a hash-based per-flight identifier plus a signal-based distance estimate — no position, velocity, or serial-number data. Full telemetry (drone and pilot position, velocity, home point, serial number, signal data) and serial-number attribution require DragonScope and active internet connectivity to decrypt.
- FPV and 900 MHz awareness require the dedicated FPV SDR, which means an Elite kit. It cannot be added to a Pro kit later.
- Detection range depends on antenna, siting, and the RF environment. Performance varies by aircraft type, protocol behavior, and line of sight.

2. Setup Sequence

Complete these steps in order. The first three require a display and keyboard connected to the unit. Everything after that can be done remotely.

1. Connect antennas and apply power
2. Complete local setup
3. Configure networking
4. Verify detection services
5. Configure TAK

Before You Start

Have the following ready:

- A display and cable appropriate to the configuration — see Section 4.1
- A USB keyboard and mouse
- An internet connection for the unit during initial setup
- The default credentials supplied with the kit

> **Important** DJI drones broadcast DroneID only while the motors are spinning. Powering on the aircraft alone does not start the broadcast, so bench testing without spinning motors will show no DJI detections.

3. Antennas and Power

3.1 Connect Antennas

All external RF ports are SMA female pass-through adapters and take antennas with SMA male connectors. For normal operation, connect all required antennas before applying power.

Port	Required for
DragonSDR RX	DJI DroneID detection — primary detection port
WiFi RX	WiFi Remote ID detection
BT5	Bluetooth 5 Long Range Remote ID detection
GPS	External GPS antenna
5 GHz **Elite only**	FPV video activity. Silkscreened FPV 5.8 Ghz.
900 MHz **Elite only**	Control and telemetry links. Silkscreened FPV 900.
TX	Not used. Leave unconnected.

GPS antenna. Drop-In kits ship with a GPS puck antenna, and it should be installed — the enclosure has no sky view of its own. On Mobile kits an external GPS antenna is optional and improves position accuracy and lock time.

Antennas are etched with the name of the port they belong to. Match each antenna to its labelled port. The numbered port map for legacy Pro v3 units is in Appendix B; the Drop-In front panel map is in the Drop-In Installation Guide.

> **Important** Torque SMA connectors to 3–5 in-lb using an SMA torque wrench. If no torque wrench is available, hand-tighten firmly by the connector nut only — never by the antenna body, and never with pliers. Loose connectors are one of the most common causes of missing detections; over-torqued connectors crack the SMA dielectric.

Placement guidance

- Clear line of sight to the sky. Elevate as high as practical.
- Separate antennas by at least one wavelength — about 12 cm at 2.4 GHz.
- Avoid metal surfaces directly behind an antenna.
- For runs over about 1 metre use low-loss coax such as LMR-240. Roughly 3 metres of RG-58 loses about 3 dB at 2.4 GHz.
- Weatherproof all outdoor connections.

3.2 Apply Power

Configuration	Power input
Mobile	12 V through the supplied vehicle adapter, or 120 V AC. Locking external power connector.
Drop-In	12 V / 24 V DC to the front-panel terminal block.

Mobile only.

1. Connect the supplied power source to the unit's locking power connector.
2. Energize the supply.
3. Press and latch the external power button. The button LED should illuminate.

Drop-In only. DC power is wired to the front-panel terminal block. Confirm polarity before energizing — wiring is covered in the WarDragon Drop-In Installation Guide.

Drop-In only. The enclosure cooling fans switch on at **113°F (45°C)**.

The system typically boots within 60–90 seconds. Allow up to 5 minutes on first boot or after an update.

Controls **Mobile only**

Control	Location	Function
External power button	Case exterior	Main power. Must be latched to supply power inside the case.
Compute power button	Inside the case	Local shutdown only.

> **Note** The exhaust fan switch inside the case is frequently mistaken for the main power switch.

> **Note** The BIOS powers the unit on whenever power is applied. USB ports stay powered while the external button is latched.

4. First Boot and Local Setup

> **Important** Kits ship with remote access disabled. This section must be completed locally, with a display and keyboard attached and the unit connected to the internet, before the unit can be reached over SSH or remote desktop. Network reachability alone does not make the unit remotely manageable.

4.1 Connect a Display and Keyboard

Mobile only.

1. Locate the right-angle HDMI adapter on the compute module and remove the HDMI dummy plug from it. Keep the plug — it must go back in.
2. Connect an HDMI cable from the adapter to your monitor, or use the built-in maintenance screen.
3. Remove the protective cap from the USB-C port on the case exterior and insert the supplied USB-C to dual USB-A cable.
4. Connect a USB keyboard and mouse.

Drop-In only. Use the external HDMI port on the front panel. USB connection depends on the compute module: Elite Drop-In units expose USB behind the removable dust cover, while Pro Drop-In units use the external USB port below the HDMI connector. Full detail is in the Drop-In Installation Guide.

> **Note** Some processor variants require an HDMI adapter to reach an external display. The adapter appropriate to your kit is supplied.

4.2 Log In and Secure the Unit

1. Log in with the default credentials supplied with your kit.
2. Change the default password immediately.

> **Important** Default credentials are supplied with the kit and are not published in this guide. Change the password before connecting the unit to any network you do not control.

4.3 Install Remote Access

Command-line access:

```
sudo apt update && sudo apt install openssh-server
sudo systemctl enable ssh
sudo systemctl start ssh
```

Remote desktop:

1. Install RustDesk from the software centre or the RustDesk website.
2. Set a permanent password under Settings, then Security. This is required for unattended access.
3. Enable Allow LAN discovery so the unit can be reached by IP address.
4. Test the connection while the display is still attached.

4.4 Restore the HDMI Dummy Plug

Mobile only.

> **Critical** The dummy plug simulates a connected display. Without it, remote desktop shows a blank screen or fails to connect.

1. Confirm remote access works before disconnecting anything.
2. Disconnect the HDMI cable and reinstall the dummy plug in the adapter.
3. Disconnect the USB-C cable and replace the protective cap.

4.5 Connecting Afterwards

Connection	Method / destination
SSH	ssh dragon@<wardragon-ip>
Remote desktop	Enter the unit's RustDesk ID or IP address, then the permanent password
WiFi hotspot	Join the unit's SSID. The unit is at 192.168.12.1
LAN Ethernet	Read the assigned address from your DHCP lease table

For a direct laptop-to-unit cable with no router in between, DHCP will not assign an address. Set link-local on the unit from the local console, then set your laptop adapter to automatic and connect to the resulting 169.254.x.x address:

```
sudo nmcli connection modify "Wired connection 2" ipv4.method link-local
sudo nmcli connection up "Wired connection 2"
```

5. Network Configuration

> **Critical** Do not modify **Wired connection 1**. This is the dedicated internal link to the DragonSDR — the unit is 172.31.100.1 and the DragonSDR is 172.31.100.2. Changing these addresses breaks DJI DroneID detection.

Configure **Wired connection 2**, the external Ethernet port. It uses DHCP by default. The internal WiFi interface, wlan0, is available for hotspot or client mode. Do not use the detection WiFi adapter for either — it must stay in monitor mode.

5.1 Static IP on the External Port

```
sudo nmcli connection modify "Wired connection 2" \
  ipv4.addresses "<your-ip>/<prefix>" \
  ipv4.gateway "<your-gateway>" \
  ipv4.dns "<dns-server>" \
  ipv4.method manual
sudo nmcli connection down "Wired connection 2"
sudo nmcli connection up "Wired connection 2"
```

5.2 WiFi Client Mode

```
nmcli device wifi list
sudo nmcli device wifi connect "YourNetworkSSID" password "YourPassword"
nmcli connection show --active
```

The connection reconnects automatically on boot.

5.3 WiFi Hotspot

Use hotspot mode where no network infrastructure exists. Check first whether a hotspot is already configured:

```
nmcli connection show | grep -i hotspot
sudo nmcli connection up WarDragon-Hotspot
```

To create one:

```
sudo nmcli connection add \
  type wifi \
  ifname wlan0 \
  con-name "WarDragon-Hotspot" \
  autoconnect no \
  ssid "WarDragon" \
  mode ap \
  ipv4.method shared \
  ipv4.addresses "192.168.12.1/24" \
  wifi-sec.key-mgmt wpa-psk \
  wifi-sec.psk "YourSecurePassword"
```

Set the band — 2.4 GHz gives the best client compatibility — then start it and enable it at boot:

```
sudo nmcli connection modify "WarDragon-Hotspot" wifi.band bg wifi.channel 6
sudo nmcli connection modify "WarDragon-Hotspot" connection.autoconnect yes
sudo nmcli connection up "WarDragon-Hotspot"
nmcli device status
```

Clients receive addresses in 192.168.12.0/24 with the unit at 192.168.12.1 as gateway and DNS. To change the passphrase later:

```
sudo nmcli connection modify "WarDragon-Hotspot" wifi-sec.psk "NewSecurePassword"
```

5.4 Hotspot Plus Ethernet

Recommended for field use. TAK devices connect over the hotspot while the unit reaches a TAK Server or the internet over Ethernet. Address translation is automatic.

```
sudo nmcli connection up "Wired connection 2"
sudo nmcli connection up "WarDragon-Hotspot"
nmcli device status
```

5.5 Finding the Unit

- Check your router's DHCP lease table for hostname wardragon.
- Scan the subnet: nmap -sn <subnet>/24
- On the hotspot, the unit is always at 192.168.12.1.

6. Verify Detection Services

Three services carry the detection pipeline. All start automatically on boot and need no configuration on first boot.

Service	Role
dji-receiver	DJI DroneID from the DragonSDR
zmq-decoder	Unified Remote ID receiver — WiFi, Bluetooth, and DJI
dragonsync	Aggregation, tracking, and output to TAK. Serves the HTTP API on port 8088.

All three should report active (running):

```
sudo systemctl status zmq-decoder dji-receiver dragonsync
```

Confirm the API is responding:

```
curl http://localhost:8088/status
```

With a DJI drone airborne in range, confirm the detection stream is producing data:

```
timeout 10 python3 -c "
import zmq
c = zmq.Context()
s = c.socket(zmq.SUB)
s.connect('tcp://127.0.0.1:4221')
s.setsockopt_string(zmq.SUBSCRIBE, '')
s.setsockopt(zmq.RCVTIMEO, 5000)
try:
    print('DJI DroneID:', s.recv_string()[:100])
except:
    print('DJI DroneID: No data')
"
```

Restart the services if required:

```
sudo systemctl restart zmq-decoder dji-receiver
sudo systemctl restart dragonsync
```

7. WarDragon Console

The Console is a local web interface that shows unit health and live detections, and lets you edit a curated set of configuration without hand-editing files. Tabs cover system health, GPS, per-source receiver status, live drones and signals, configuration with TAK certificate upload and a Restart button, and a read-only version check.

> **Important** Not every kit ships with the Console installed. Confirm whether it is present before relying on it for setup or shutdown. Installation instructions are below.

To install:

```
cd ~/WarDragon
git clone https://github.com/alphafox02/wardragon-console.git
cd wardragon-console
sudo packaging/install.sh
```

The Console binds to loopback and is not exposed on the LAN.

Access from	Address
The unit itself	http://127.0.0.1:4280/
A laptop	SSH tunnel local port 4280 to 127.0.0.1:4280 on the unit
iOS tablet or phone	http://wardragon.local:4280/
Android over USB tether	Use the fixed address shown in the Console's Operator Notes panel

> **Note** http://127.0.0.1:4280/ works only from a browser running on the unit. It will not resolve from a separate laptop.

Receiver indicators. Active sources are WiFi, Bluetooth, and DJI. Legacy source slots not wired up on your kit stay down; that is normal, not a fault.

> **Critical** Anyone with physical access to the USB tether path can write configuration and restart services. Treat physical access as full administrative access.

8. Integration With Your Operational Picture

Detections and system health are published as Cursor on Target messages and appear as drone icons with position, altitude, speed, heading, pilot location, and home point where available. Feeds reach TAK-based common operating pictures including ATAK, WinTAK, and iTAK, either by multicast on the local segment or through a TAK Server for centralized, multi-user operations.

Destination	What it does
Local and standalone	Baseline detection requires no subscription and no cloud connection
ATAK and TAK	Streams detections into TAK-compatible operating pictures via CoT
WarDragon Analytics	Aggregates one kit or many nodes into a central map and dashboard
4DV Analytics	Forwards detection events into 4DV workflows where configured
Your own endpoint	Pushes detections to your middleware, dashboard, or command-center ingestion path

8.1 Multicast — Default

Multicast is enabled by default and needs no change on the unit. On the ATAK device:

1. Open Settings, then Network Preferences, then SA Multicast.
2. Set both Input and Output to 239.2.3.1:6969.
3. Confirm the device is on the same network segment as the unit.

Confirm traffic is leaving the unit:

```
sudo tcpdump -i any host 239.2.3.1 and port 6969
```

> **Note** The unit sends multicast on all active interfaces and rechecks about every 30 seconds, so a newly connected hotspot client or tethered device is picked up automatically.

iTAK: configure SA Multicast input 239.2.3.1:6969. **WinTAK:** Settings, then Network, add multicast input 239.2.3.1:6969.

8.2 TAK Server

Edit /home/dragon/DragonSync/config.ini under [SETTINGS]:

```
tak_host = tak.example.com
tak_port = 8089
tak_protocol = TCP

# TLS using a PKCS#12 bundle
tak_tls_p12 = /home/dragon/certs/client.p12
tak_tls_p12_pass = yourpassword

# Or TLS using PEM files
tak_tls_certfile = /home/dragon/certs/client.crt
tak_tls_keyfile = /home/dragon/certs/client.key
```

```
tak_tls_cafile = /home/dragon/certs/ca.crt
tak_tls_skip_verify = false
```

Place the certificates, restrict permissions, apply, and test:

```
mkdir -p /home/dragon/certs
cp client.p12 /home/dragon/certs/
chmod 600 /home/dragon/certs/*
sudo systemctl restart dragonsync
nc -zv tak.example.com 8089
```

Common ports: TCP 8089 streaming, TCP 8443 TLS, UDP 6969 multicast.

> **Note** Leave tak_tls_skip_verify set to false. If the connection then fails, the certificate authority file is usually missing or wrong.

8.3 WarDragon ATAK Plugin

The plugin adds unit health, enhanced tracks, and pilot locations inside ATAK. CoT continues over multicast or TAK Server independently.

1. Download the plugin from https://github.com/alphafox02/WarDragon-ATAK-Plugin/releases and match the build to your ATAK version.
2. On the device: Settings, then Tool Preferences, then Manage Plugins, then Import Plugin.
3. Enable the WarDragon plugin.
4. Open Tools, then WarDragon, and enter the unit's IP address with API port 8088.

8.4 Reducing Network Load

Each drone is limited to one update every 2 seconds by default. Increase rate_limit in config.ini for large numbers of drones or constrained links, then restart dragonsync.

9. Operation

9.1 Common Commands

Action	Command
Service status	`sudo systemctl status zmq-decoder dji-receiver dragonsync`
Live output logs	`journalctl -u dragonsync -f`
Live Remote ID logs	`journalctl -u zmq-decoder -f`
Live DJI logs	`journalctl -u dji-receiver -f`
Restart detection	`sudo systemctl restart zmq-decoder dji-receiver`
Restart output	`sudo systemctl restart dragonsync`
API health	`curl http://localhost:8088/status`
USB devices	`lsusb`
Network interfaces	`ip addr show`
Disk space	`df -h`
Temperatures	`cat /sys/class/thermal/thermal_zone*/temp`
Clean shutdown	`sudo shutdown -h now`

9.2 Best Practices

- After setup, run the unit headless. No monitor or keyboard is required.
- Manage and monitor remotely over your network or through integrated systems.
- Ensure proper ventilation and a stable power source.
- Keep antennas secure and unobstructed.
- Keep software up to date, monitor system health in your operational picture, and review logs and detections regularly.

9.3 Field Deployment Checklist

1. Pack the unit and every antenna, including GPS and any mission antennas.
2. Connect all antennas to the correct ports before applying power.
3. Apply power. Allow 60 to 90 seconds for boot.
4. Confirm all three services are active.
5. Enable the hotspot if no network is available.
6. Connect TAK devices and confirm detections are arriving.
7. Confirm GPS lock if accurate unit position is required.

9.4 Configuration Backup

```
cp /home/dragon/DragonSync/config.ini ~/config-backup.ini
```

```
sudo cp /etc/NetworkManager/system-connections/WarDragon-Hotspot.nmconnection \
  ~/hotspot-backup.nmconnection
```

To restore the configuration file, copy it back and restart dragonsync. To restore the hotspot profile, copy it back, set owner root and mode 600, then run sudo nmcli connection reload.

9.5 Shutdown

Always shut the operating system down cleanly before removing power. Use whichever method suits the kit.

Command line — all systems:

```
sudo shutdown -h now
```

Console — where the Console is installed: open the System menu, select Shutdown, and wait for the unit to power off.

Once the unit has powered off completely:

- **Mobile only** — delatch the external power button.
- **Drop-In only** — remove DC power at the source.

> **Important** Cutting power without a clean shutdown can corrupt the filesystem.

> **Note** Do not press the compute power button after a command-line shutdown — if the external button is still latched, the unit will boot again.

10. Troubleshooting

10.1 First Steps

```
sudo systemctl status zmq-decoder dji-receiver dragonsync
ip addr show
lsusb
df -h
```

10.2 Power and Boot

Symptom	Likely cause	Action
No indicators	Supply or outlet	Check the adapter and outlet; try another supply
Brief flash then off	Overcurrent protection	Disconnect peripherals and check for shorts
Power on, no boot	Boot failure	Allow 5 minutes, then review journalctl -b and contact support
Random reboots	Power or heat	Verify the supply rating and confirm airflow

10.3 Remote Access

Symptom	Likely cause	Action
SSH refused	OpenSSH not installed	Complete local setup, Section 4
SSH times out	Wrong address or network path	Verify the IP and connectivity
Blank remote desktop	HDMI dummy plug missing	Reinstall the plug in the right-angle adapter (Mobile)
Permission denied	Wrong credentials	Confirm username and password

10.4 No Detections

1. Confirm every antenna is firmly connected to the correct port.
2. Confirm all three services are active.
3. Confirm detection hardware is enumerated: lsusb
4. For DJI: antenna on the DragonSDR RX port, and the drone's motors must be spinning.
5. For WiFi Remote ID: confirm the adapter is in monitor mode with iw dev <iface> info
6. Review logs: journalctl -u dji-receiver -n 50 and journalctl -u zmq-decoder -n 50

Short range: elevate antennas, improve line of sight, consider higher-gain or directional antennas, and reduce nearby RF noise.

10.5 Network and Hotspot

Symptom	Likely cause	Action
Hotspot will not start	Interface in use	Stop other WiFi connections on wlan0
Clients cannot connect	Passphrase mismatch	Verify the passphrase; avoid unusual characters
No address assigned	DHCP not running	Restart NetworkManager
No internet through unit	Forwarding disabled	cat /proc/sys/net/ipv4/ip_forward should return 1

10.6 TAK

1. Confirm the TAK device and unit share a network segment for multicast.
2. Confirm multicast is enabled and the address is correct in config.ini.
3. Test the API: curl http://<wardragon-ip>:8088/status
4. Review logs: journalctl -u dragonsync | grep -i tak
5. For TAK Server, test with nc -zv and verify certificates if TLS is in use.

10.7 GPS

- Check status: gpspipe -w -n 5
- If no data, confirm the device node: ls /dev/ttyACM* /dev/ttyUSB*
- Connect an external GPS antenna if the internal one is obstructed; allow several minutes for first lock.

10.8 Diagnostic Bundle

If support asks for diagnostics:

```
sudo journalctl -b > ~/diag-journal.txt
ip addr > ~/diag-network.txt
lsusb > ~/diag-usb.txt
```

11. Support

Technical support for purchased WarDragon kits and active DragonScope subscriptions is requested through the support page. Scan the code, or go to:

```
https://cemaxecuter.com/support/
```

Include the following when you open a request. Supplying it up front resolves the ticket faster:

- Product and configuration you are running
- Serial number or order reference
- What you expected and what actually happened
- Any error messages or screenshots
- The steps that reproduce the issue
- Output of: sudo systemctl status zmq-decoder dji-receiver dragonsync
- A diagnostic bundle, per Section 10.8

Purchasing, configuration advice, and quote requests do not go through the support queue. Use the contact form on the website instead.

Appendix A — Reference

A.1 Ports

Port	Service	Notes
22	SSH	Installed during local setup
4221	DJI detections	Internal
4224	Unified detection output	Internal — primary input to dragonsync
4225	Unit GPS and status	Internal
4280	WarDragon Console	Loopback and USB tether only
6969 UDP	TAK multicast	Group 239.2.3.1
8088	HTTP API	Read-only; ATAK plugin and Console
8089 / 8443	TAK Server	Outbound from the unit

A.2 File Locations

Item	Path
DragonSync configuration	`/home/dragon/DragonSync/config.ini`
TAK certificates	`/home/dragon/certs/`
Hotspot profile	`/etc/NetworkManager/system-connections/WarDragon-Hotspot.nmconnection`
Hotspot DHCP leases	`/var/lib/NetworkManager/dnsmasq-wlan0.leases`

> **Note** Confirm the configuration path on your kit before scripting against it: sudo systemctl cat dragonsync

A.3 API Endpoints

Read-only and rate-limited: /status for unit health, /drones for active tracks, /signals for signal alerts, /config for sanitized configuration.

A.4 Current System Technical Specifications

Specification	Pro	Elite	Notes
Maximum power draw	15 W	30 W	---
Operating temperature	Up to 60°C (140°F)	Up to 60°C (140°F)	---
Storage temperature	Up to 70°C (158°F)	Up to 70°C (158°F)	---
Mobile environmental protection	NEMA 2 / IP22	NEMA 2 / IP22	Case built to MIL-STD-810H
Drop-in environmental protection	NEMA 1 / IP10	NEMA 1 / IP10	Requires installation within a suitable weatherproof enclosure for outdoor/wet environments

RF: SMA female external ports: SMA male antenna/cables.
Display/USB: Configuration-dependent; see Section 4.1.

Appendix B — Legacy Pro v3 Reference

Legacy Pro v3. This appendix applies only to earlier Pro v3 hardware. It does not describe current kits.

B.1 Antenna Port Map

Case open, viewed from above, front nearest you. All ports are SMA female; use SMA male antennas. Four antennas are supplied.

Side / Port	Label	Purpose
Left 1	ESP32	WiFi Remote ID, secondary
Left 2	RX (Panda)	WiFi Remote ID
Left 3	RX (DragonSDR)	DJI DroneID — primary
Left 4	TX	Not used
Right 1	BT5	Bluetooth 5 Long Range Remote ID
Right 2	GPS	External GPS antenna, optional

B.2 Power and Environment

Item	Specification
Power input	12 V DC, 3 A minimum, 5.5 x 2.1 mm barrel jack
Typical consumption	Approximately 25 W
Operating temperature	0 to 40 °C (32 to 104 °F)

The ESP32 WiFi Remote ID path is present on Pro v3 and may report as an active source in the Console. Second-SDR capabilities are not available on Pro v3.

— End of Guide —

Commercial WarDragon systems are manufactured and distributed by Millenium Products.