DS Series

DETECTION AND SPOOFING SYSTEM

User Manual

V1.0

Reading Tips

This manual applies to the UAV radio countermeasure equipment developed and produced by the company. The manual provides comprehensive specifications, functional design, structure and specification requirements of the system, as well as installation, deployment, and operational requirements, serving as an operational guide for end users.

Symbol Legend

	Supplementary Notes: Additional explanations and annotations to the main text of the manual.
	Safety Notices: Important operational warnings and risk prevention guidelines for users.
	DANGER: Indicates imminent hazards which, if not avoided, will result in death or serious injury and major property damage.

Manual Usage Recommendations

1. Before using the product, please read this manual thoroughly. Retain this manual for future reference to address any operational inquiries.
2. All photographs, graphics, charts, and illustrations in this manual are for explanatory purposes only and may differ from the actual product. Refer to the physical product for exact specifications. The company reserves the right to update this manual due to product version upgrades or other requirements, with the latest electronic version to be distributed to users.
3. The company recommends using this manual under the guidance of qualified personnel.

Safety Notice

Before using the product, please carefully read the following precautions and operate the product correctly as required.

Installation Precautions

Environmental Requirements

Do not install or store the product in any of the following locations:

- Extreme environments: places where temperatures exceed the range of the device operating temperature or where frost may form.
- Near strong electromagnetic interference sources or equipment with large current fluctuations.
- Areas with flammable, explosive, corrosive gases or dust.
- Damp or water-exposed areas. Liquid ingress may cause electric shock or fire hazards.

Operational Guidelines

- Only qualified personnel or designated maintenance staff may open the chassis.
- All antennas must be fully connected and tightened according to the labels. Powering on the device without antennas installed is strictly prohibited.

Usage Precautions

Power and Electrical Safety

- Use only the specified AC 110 V–220 V power supply.
- Do not pull or bend the power cord. Avoid crushing or twisting it, and stop using it if damaged.
- Do not operate the equipment during thunderstorms. Avoid touching power lines or device connectors during lightning to prevent electric shock.

- Always unplug the power cord before moving the device.
- Do not touch the power plug with wet hands.
- When unplugging the power cord, hold the plug body firmly.

Operational Risk Warnings

- If abnormal conditions such as smoke, unusual noises, or burning smells occur, shut off power immediately and contact our after-sales service department.
- Do not install any software unrelated to the software platform; system issues caused by such software are not covered under warranty.
- Do not connect unauthorized USB drives or external hard drives to avoid malware infection. Do not delete server files arbitrarily, change the system time, or shut down or restart the server without authorization.
- Unauthorized personnel are prohibited from disassembling the device to avoid damaging internal components or compromising your rights. If the device malfunctions during use, contact our after-sales service department.

Regulatory Compliance

- This device may cause radio interference during operation. Users must take feasible measures to mitigate such interference.
- If suspected interference occurs with civil-aviation or military frequencies, stop using the device immediately, investigate the cause, and report the incident.

Table of Contents

1 Product Introduction

The DS Series is a stationary detection and spoofing system. Equipped with professional-level waterproof and dustproof design, it can operate reliably and continuously in outdoor harsh environments, and can be widely applied to the area installation and deployment.

1.1 Main Functions

Precise Identification

It can precisely identify different drones of the same brand and model from a long distance and identify the electronic fingerprint of drones.

Spoofing and Defense

After detected the unauthorized drone, it actively emits signals to carry out spoofing, forced landing, driving away and more to protect the safety of the area.

Unattended Function

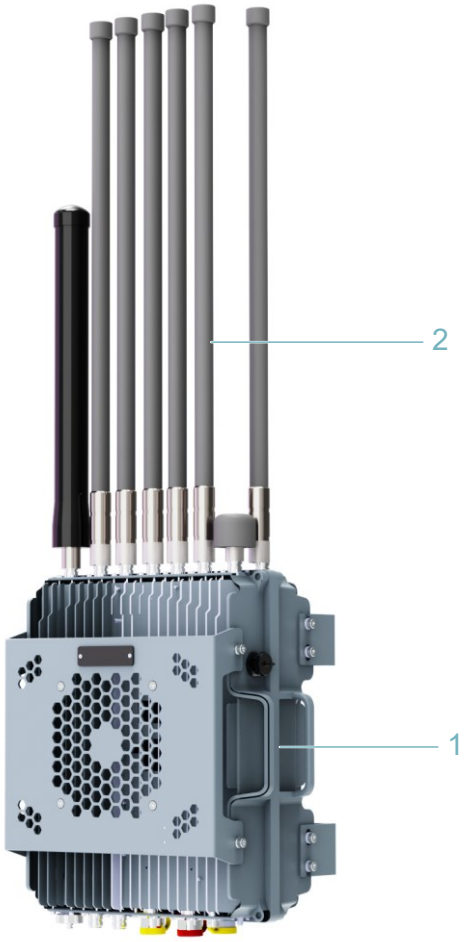
One-click switch to unattended, automatically defend against drone intrusion for 7/24 hours.

Intelligent Spoofing

After detecting the intruding drone, the device actively launches signals to implement deception, forced landing, driving away, and son on, to protect the safety of the defensive zone.

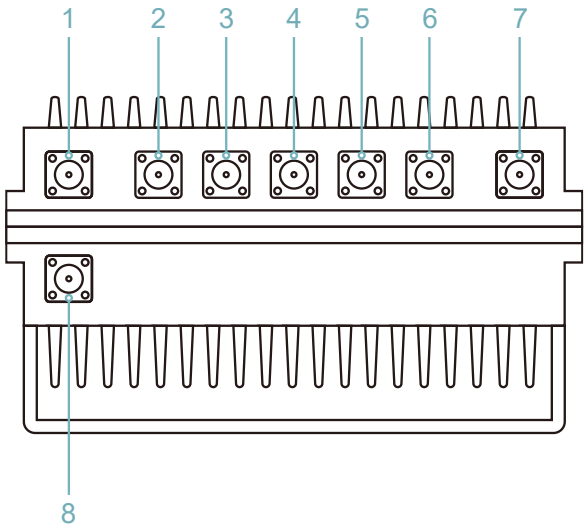
1.2 Product Appearance

The equipment appearance is shown as follows:

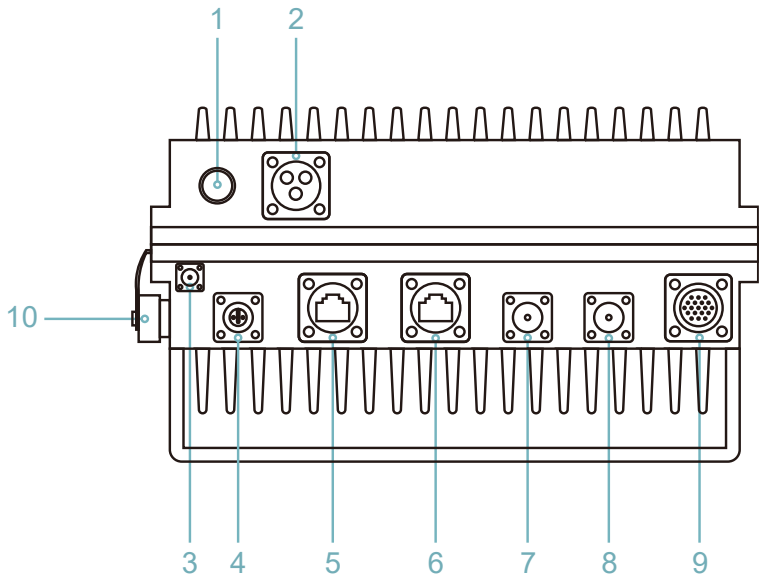


1. Main unit
2. Antennas

1.3 Ports and Antenna Connector



Position	Description	Label	Connector Type
1	GPS receiving antenna connector	GPS	N-type
2	2.4 GHz receiving antenna connector	2.4GHz	N-type
3	5 GHz receiving antenna connector	5GHz	N-type
4	1.4 GHz receiving antenna connector	1.4GHz	N-type
5	433 MHz receiving antenna connector	433 MHz	N-type
6	900 MHz receiving antenna connector	433 MHz	N-type
7	0-6 GHz full band detection receiving antenna connector	0-6GHz	N-type
8	1.5 GHz spoofing antenna connector	1.5G	N-type



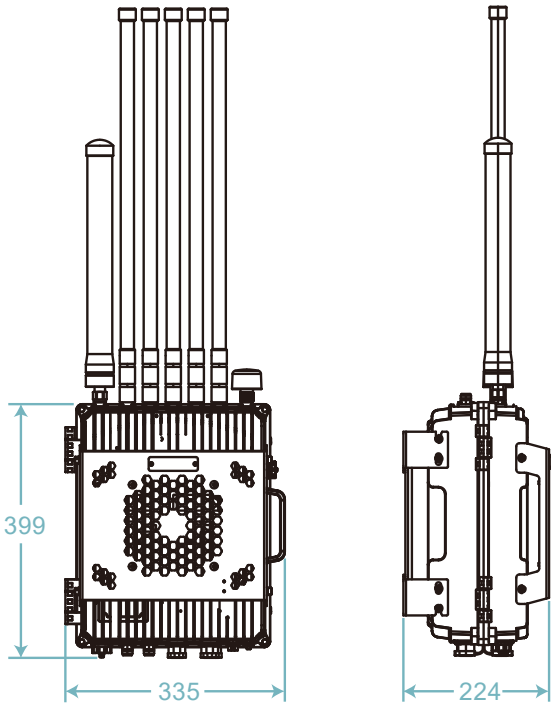
Position	Description	Label	Connector Type
1	Power On/Off button	⏻	—
2	Power connector (AC110V～240V)		3-pin aviation power connector
3	4G antenna connector	—	SMA connector
4	Fan connector	FAN	2-pin circular aviation connector
5	Ethernet port 1	1	RJ45
6	Ethernet port 2	2	RJ45
7	2.4 GHz direction finding data transmission interface	2.4GHz	N-type
8	5.8 GHz direction finding data transmission interface	5.8GHz	N-type
9	Direction finding information control interface	RF	19-pin circular aviation connector

10	SIM card slot	—	nano-SIM

1.4 Mechanical Characteristics

Item	Specification
Size(1)	
Length	399mm
Width	335mm
Thickness	224mm
Weight	
Weight	13kg

(1) The data are of the main unit, excluding fiberglass antenna.



2 Equipment Deployment Preparation

Choose a wide-view area to erect the device. First check the specifications and quantity of all parts and standard parts according to the equipment list, and then assemble them step by step according to the following installation steps.

2.1 Site Selection

The equipment is typically deployed outdoors. A comprehensive site survey must be conducted prior to installation and deployment. Site the equipment should pay attention to the following factors:

Visibility environment: Choose a flat, open highland or building rooftop, ensuring a 360° unobstructed view for the antenna placement.

Electromagnetic environment: Avoid electromagnetic interference zones such as microwave stations, radio transmission towers, and high-voltage power line crossings, as well as areas near glass curtain wall clusters and large metal structures (e.g., bridges, transmission towers).

Natural environment:

- Avoid the wind to reduce the equipment antenna wind load.
- When deploying in thunderstorm-prone areas, avoid locations susceptible to water accumulation and lightning strikes. Install a lightning rod for protection; its height must exceed the overall equipment height by at least 50 cm.

Electrical Environment: Avoid areas near electrified railways, base stations, or any other sources prone to signal interference.

Infrastructure: Ensure the site has mains power access and supports connection to public or dedicated communication networks.

Additional Requirements: The deployment site must be legally designated for construction. The building structure or mounting bracket must have sufficient load-bearing capacity to meet the equipment’s weight requirements.

2.2 Installation Methods

It can be mounted on a pole or wall. Be aware of the surroundings and make sure there are no obvious obstructions or strong jamming devices in the area.

Method 1: Ground Installation.

The equipment features an external mounting bracket on the back, which can be connected and secured to a prepared ground installation bracket using M10 bolts. The ground installation bracket should be firmly installed on the ground.

Method 2: Wall Installation.

The equipment is connected and secured to a wall mounting bracket using bolts, and the wall mounting bracket is fixed to the wall using expansion anchors.

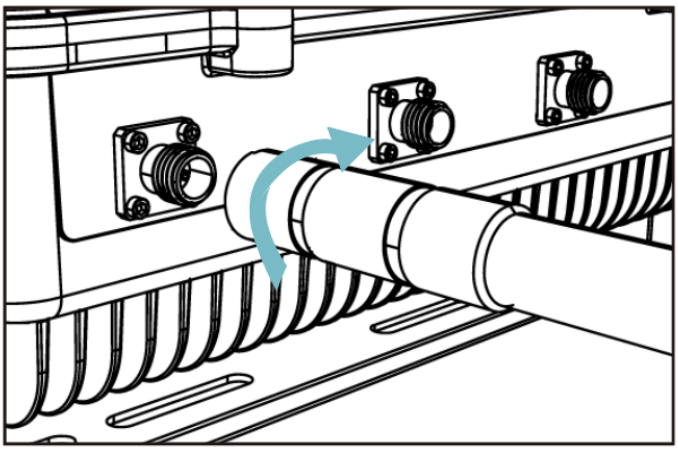
If used in conjunction with a direction-finding unit, the installation height of the Direction-Finding Unit should be higher than that of the main unit's antennas.

3 Deploy the Equipment

3.1 Connect Antennas

1. Screw and tighten the receiving/transmitting antennas onto the main unit one by one in a clockwise direction in accordance with the corresponding labels.

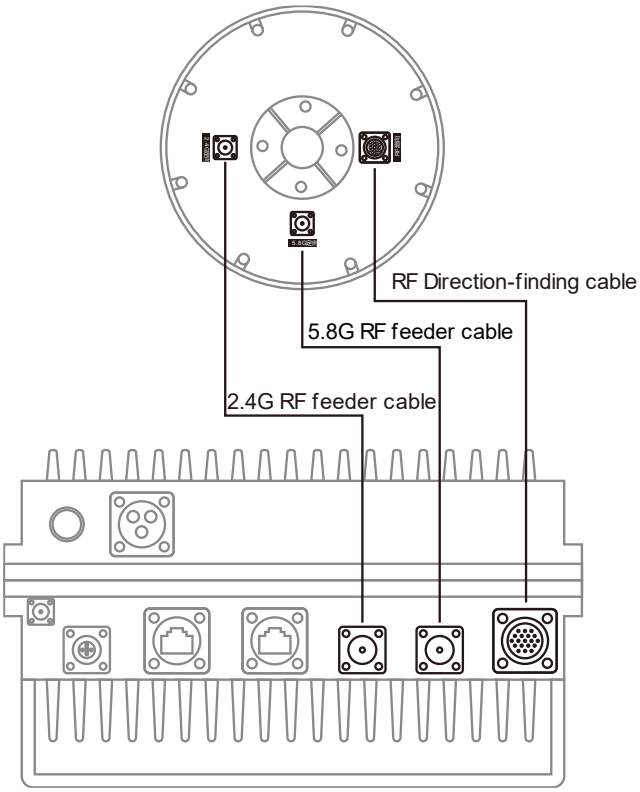
> ⚠ All antennas must be installed on the main unit according to the labeling. If any antenna is missing or damaged, do not operate the equipment; continued use will cause permanent damage.



3.2 (Optional) Install Direction-Finding Antenna

Direction-finding unit can be used with the main unit. Select a suitable location next to the main unit, which is usually fixed with support poles.

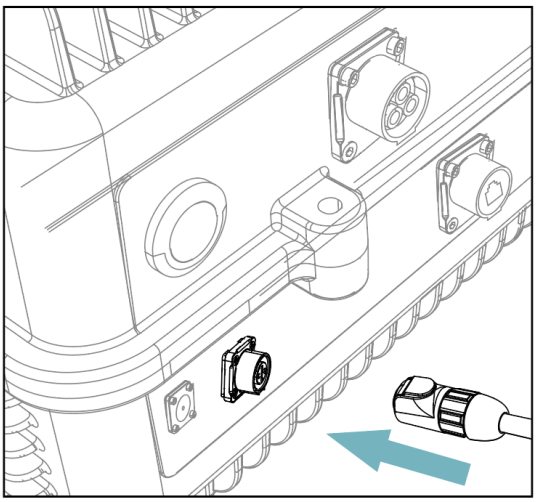
1. Connect the main unit to the direction-finding antenna via two RF transmission cables (2.4 GHz and 5.8 GHz) and one data connection cable.



3.3 Connect Fan

The equipment bracket is equipped with an integrated cooling fan.

1. Connect the power cable of the bracket's built-in side cooling fans.

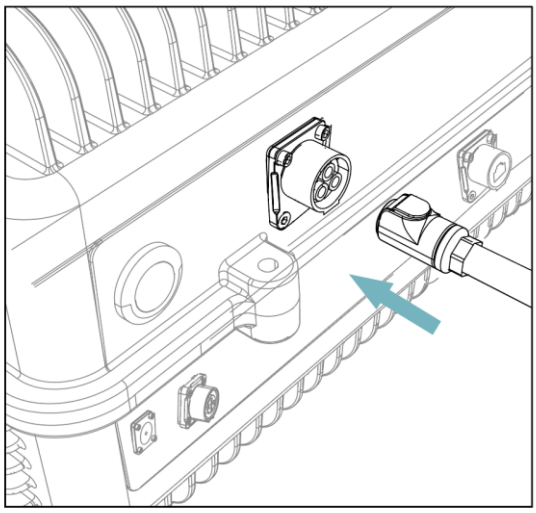


3.4 Connect Power Supply

The equipment can be connected to 220V AC power via power cable using either fixed power supply or UPS.

> ⚠ The main unit must be installed with antennas before power on; otherwise, the device may be damaged.

1. Connect the input end of the power cord to the fixed power supply and insert the output end into the device's power connector. The power connector features a snap-fit design, apply steady pressure until you hear an audible click, confirming a secure connection.



3.5 (Optional) Connect to the Network

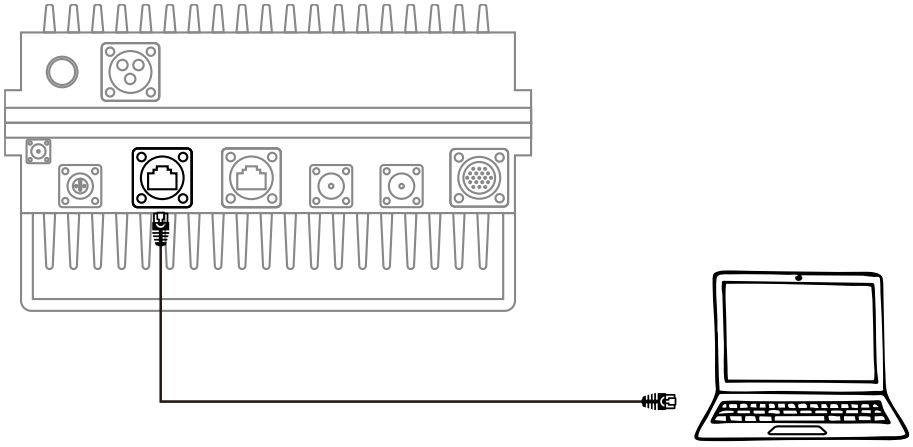
1. Connect the 4G antenna to the corresponding 4G antenna connector.
2. Insert the nano-SIM card into the SIM card slot.

3.6 Connect a Control Terminal

The equipment can be connected to the control terminal via standard ethernet cable through the TCP/IP interface.

1. Plug the control terminal into Ethernet port 1 via ethernet cable.

Ethernet port 2 is a spare port used for networking with other devices into the network. When not in use, keep it sealed with the waterproof plug.



4 Drone Defense Software Platform

Drone defense software platform, which integrates situational awareness, information display, decision-making assistance, command and control. It supports browser access and control of other devices on the LAN, and supports multi-screen and multi-device monitoring.

4.1 Log in to the System

Configure the Network

Before logging into the system, it is necessary to configure the network settings of the drone defense software platform. The IP address should be set within the 192.168.100.x subnet, which is the same subnet as the default access IP of the system: 192.168.100.100.

1. Configure the IP subnet to 192.168.100.x according to the system platform, e.g., Windows, Linux, or macOS.

	Avoid setting the IP address to 192.168.100.100, as this will cause a conflict.

Log in to the System

1. Open a browser and enter the device's IP address https://192.168.100.100 to access the login page.

	Google Chrome is recommended for use.

2. Enter the system account and password, drag the verification slider to verify, and then click the “Sign in” to enter the main interface of the system.

Account:	admin
Password:	lzno1

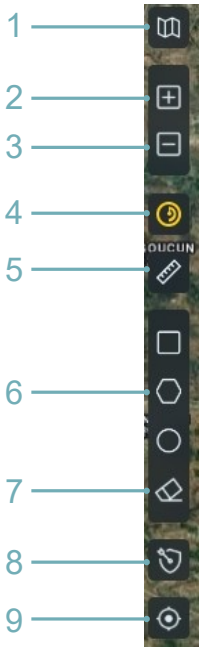
4.2 Main Interface

The main interface is distributed in three functional areas.

1. Operation menu area
2. Information display area
3. Function display area

Operation Menu Area

The operation menu area includes options such as map mode switch and defense-zone settings.



1 Map mode switch	Switch between Google satellite and Google vector.
2 Zoom In	Zoom In the map.
3 Zoom Out	Zoom Out the map.
4 Set Center Point	Sets the center point coordinates for networking. Not applicable for single-device operation.
5 Measuring Distance	Measure the distance and angle between two points on the map, allowing for the measurement of distances and angles between multiple endpoint positions and a starting point.
6 Draw Rectangle / Polygons / Circle (The defensive zone or warning zone)	Set Defensive Zone/Warning Zone on the Map. **Defensive Zone:** Once set, the defensive zone appears as a red inner circle. If a drone enters this zone, it will be highlighted in orange, and audible/visual alarms will activate. **Warning Zone:** Once set, the warning zone appears as a blue inner circle. If a drone enters this zone, it will be highlighted in orange, and audible/visual alarms will activate. Unauthorized drones entering the warning zone will trigger continuous alerts while their position and flight path are monitored.

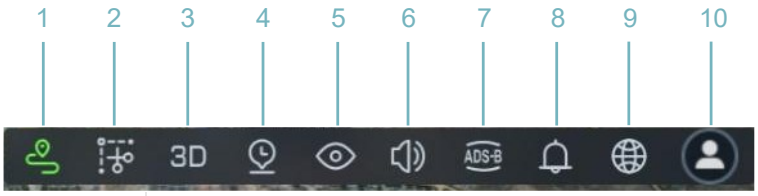
The minimum allowable area for drawing defense/warning zones is 100 square meters.

7 Eraser Defense Zone	Delete the defensive zone or warning zone drawn on the map.
8 Locate the air defense zone	If the device moves too far and loses the defense/warning zone, perform rapid repositioning.
9 Return to center	Return to the center point.

Information Display Area

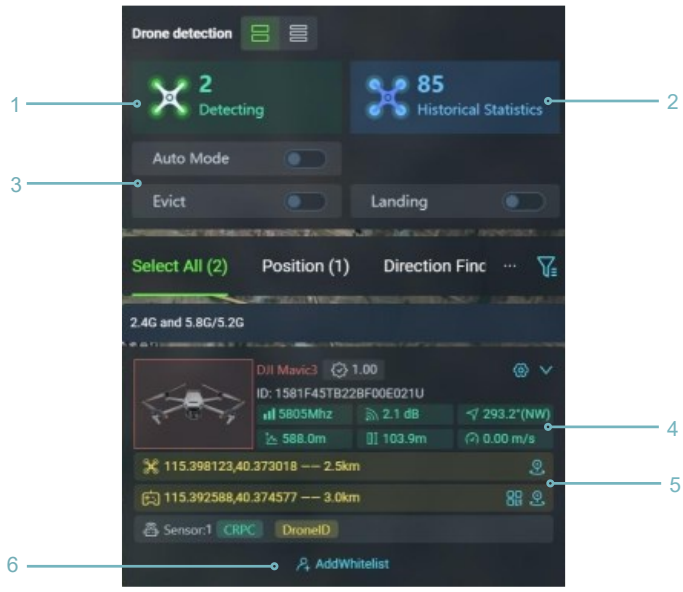
The information display area includes options such as hiding/displaying the menu bar of the main interface, volume, notification switch, language switch, system logon/logoff and other operations.

In addition, this area is mainly responsible for the real-time detection information display and control functions of drones, which can display the number of current detection and historical detection drones, as well as the detailed information of currently detected drones.



1 Show/Hide trajectory	Hide or show the trajectory.
2 Display/Hide Past Flight Trails / Drone Trace Cut Off	Display of hide past flight trails.
3 3D Map	Switch between 3D map view and 2D map view.
4 Historical Drones Detection Setting	Display the historical drone-detection locations on the map and marked with yellow. The date range can be configured by start time and end time.
5 Hide/Show panel	Hide or show the detection area, function area, and map area of the interface.
6 Sound settings	Adjust the alarm volume.
7 ADS-B	Used to receive civil aviation signals transmitted by aircraft, including flight route and schedule information.
8 Notifications	Display device status notifications.

9 Change language	Change system language.
10 Account login	Account login/logout.



1 Currently Detected Drones

2 Cumulative number of drones detected

3 Function Toggle	Toggle the button to activate the corresponding drone defense function.
4 Drone Current Status	Displays detected drone information including reference distance and position.
5 Drone / Pilot Location	Click the corresponding button to navigate to the current location of the drone/pilot.
6 AddWhitelist	Click to add the selected drone to the whitelist; whitelisted drones entering the defensive zone will not trigger alerts

Function Display Area

The function display area includes options such as checking the events, checking the whitelist, checking the statistic, checking the device status and other operations.

Click the button  to expand the function display area menu. Click the same button again to hide the menu.

1	Events	The Drone Events list shows drone details such as type, ID, detection time, duration, and frequency. It supports sorting, time-based expansion, history replay, export drone events, clear drone events on the main screen.
2	Advanced	Includes the unknown UAV WiFi detection, Custom Detectors, Custom Models module.
3	Black/White	Drones added to the blacklist will be flagged with an alert once they enter the defensive zone. Drones on the whitelist will not trigger any alarm when they enter defensive zone.  Whitelist/Blacklist import/export formats: UTF-8 and XLSX. View the exported files in the browser's Downloads list.
4	Statistics	The Drone Statistical Report includes Incidents/Drones, Most Seen Drone Brands, Common UAV, Incident Trends and Critical Incidents. It supports date range configured by start time and end time, and export PDF of the statistics.
5	Devices	The device management window displays the operational status information of controller, engine, sensors and defender. ● Controller: Display the information such as operation status, and detection bands. ● Engine: Display the information such as operation status, GPU and CPU information, and version. ● Sensors: Display the information such as operation

		status, detection bands, and version of the two sensors. ● Spoofer: Display the information such as operation status, faults, and version.
6	Networking	Display the networking information such as Node ID, and Node name. The Networking function icon appears when the site is a Networking Master.
7	Version	Display the version information of UI version, cm, engine, sensor, defender.
8	Settings	Modify passwords and do user management, such as add, edit and delete.
9	Function display area	The functional display area primarily shows the Spectrum, Incident Trends, and Most Seen Drone Brands. The spectrum feature visualizes signals currently detected by the device as a spectrum.

4.3 Check Detection Information

In Information Display Area, it displays the position and direction of the drone. Additionally, the drone model, electronic ID and approximate location information are marked on the electronic map in the main interface.

Add to/Delete from Whitelist

Drones added to the whitelist will not trigger any alarm when they entering the defensive zone.

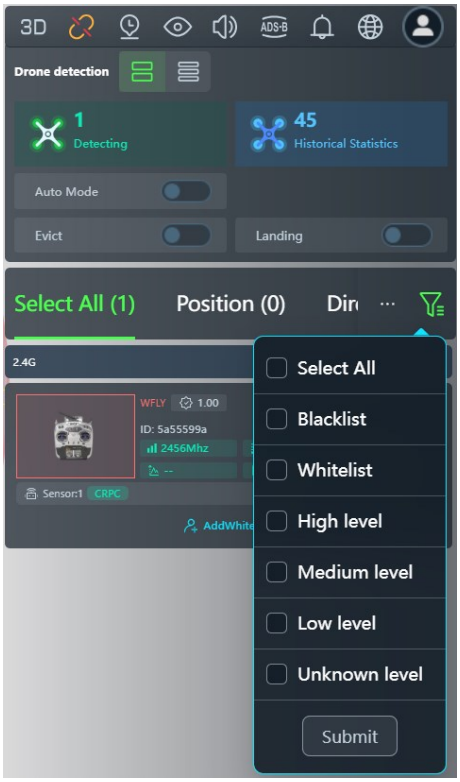
1. Select a drone.
   a) Click **AddWhitelist** button to add the drone to whitelist.
   b) Click **DeleteWhitelist** button to delete the drone from whitelist.

Set Drone Profile

1. Select a drone. Click  button and select **Profile**.
2. On the Drone Profile Setting page, configure the Custom alias, Effective scope, Drone Link ID, and Drone Description.

Filter the Drone List

1. Click  button to pop-up the filter items.



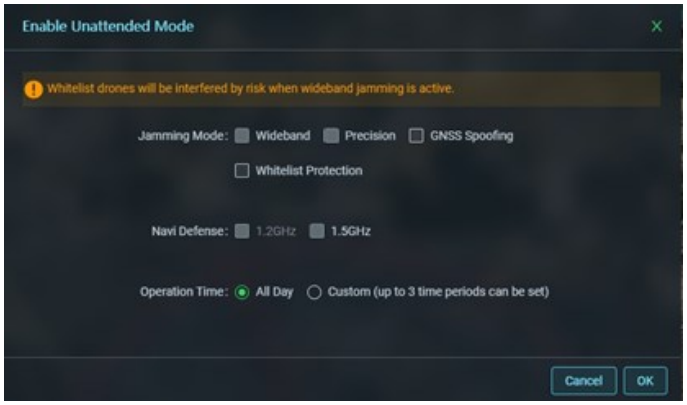
2. Tick the filter criteria and the system displays the drone list accordingly.

4.4 Enable Unattended Function

In unattended mode, the system automatically identifies and filters drones on the whitelist upon detection. For blacklisted drones, it initiates spoofing. The countermeasures will automatically cease once the alarm is no longer triggered.

1. In Information Display Area, toggle the switch of **Auto Mode** to enter the Autonomous Defense Option Confirm page.

2. In the page, set Jamming Mode, Navi Defense, and Operation time.

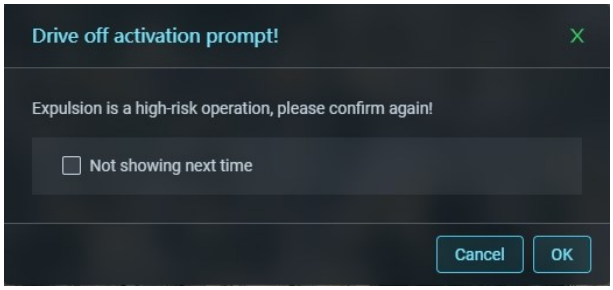


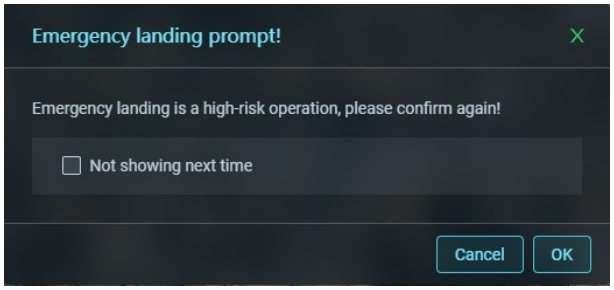
3. Click **OK** button to enable unattended function.

4.5 Spoof Drone

1. In Information Display Area, toggle the switch of **Evict** or **Landing** to interfere with the drone.

2. Read the notice and click **OK** button to confirm.

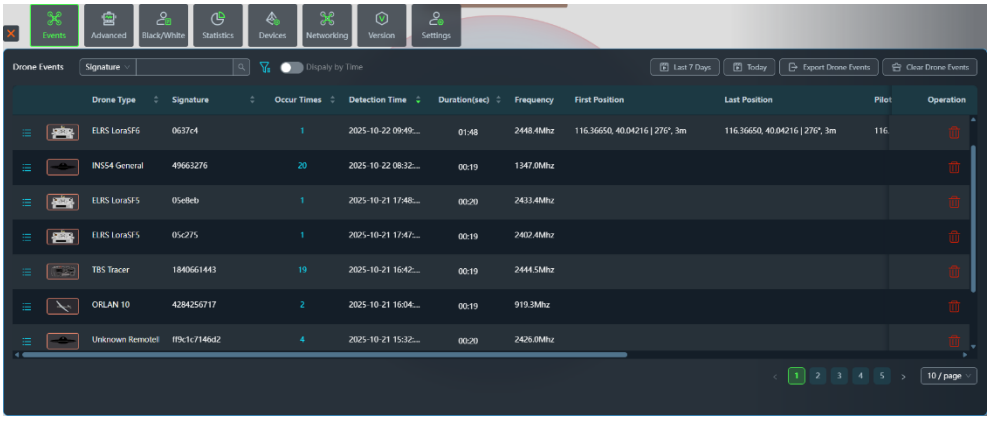




4.6 Check the Events

1. In Function Display area, click **Events**, view the drone events.

> This feature allows one-click expand/collapse of the “Incident Trends” panel on the main interface.



2. Click **Export Drone Events** button to export drone events.

4.7 Mark Danger WiFi Drones

The device can display the drone-like WiFi signals detected in the current environment and allow users to mark them.

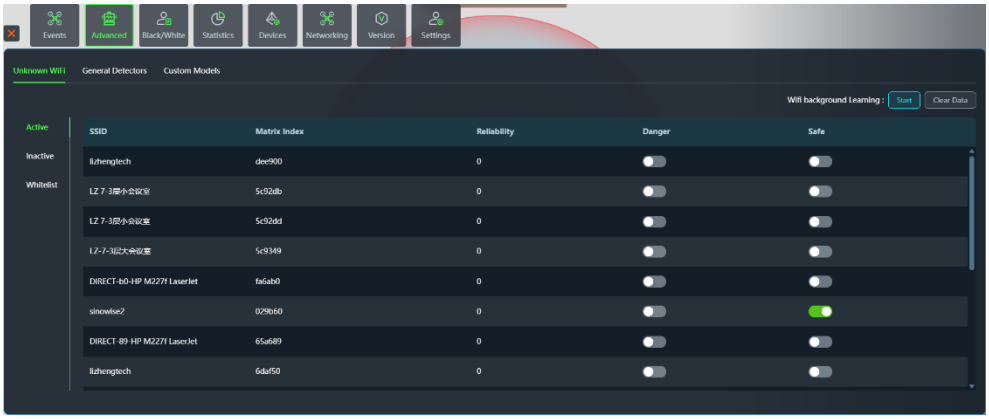
Start WiFi Background Learning

1. In Function Display area, click **Advanced**.
2. Click **Start** button to start Wifi background learning.

3. Click **Stop** button to stop this process.

Mark Danger WiFi Drones

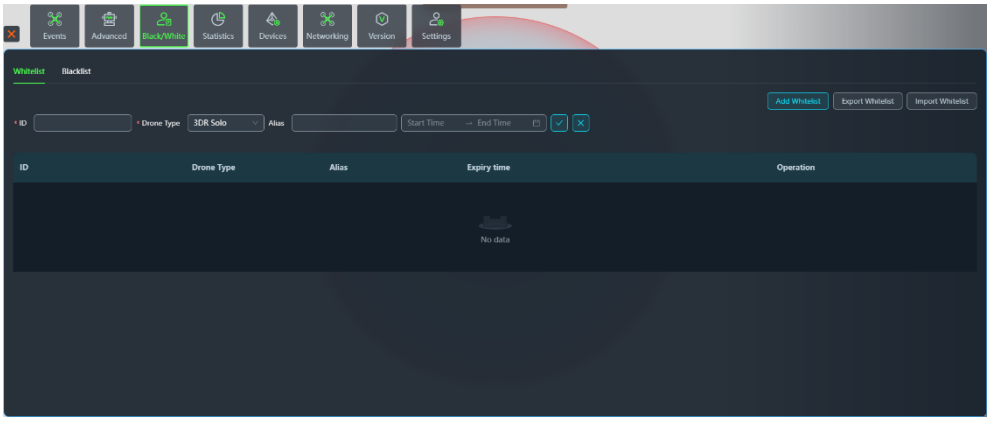
1. In Function Display area, click **Advanced**.
2. Select Unknown WiFi panel to enter the WiFi list.



3. Mark the WiFi signal.
   a) Users may mark an identified non-drone WiFi signal (e.g., a common wireless hotspot) as “Safe.” Once marked, the system will ignore this signal and not trigger alarms.
   b) If a WiFi signal is confirmed to originate from a drone, users can mark it as “Danger”. After marking, the system will trigger an alarm whenever this signal is detected.

4.8 Manage the Whitelist/Blacklist

Drones added to the blacklist will trigger visual alerts when entering the defensive zone, while whitelisted drones will not trigger any alarm when they appear.



Export Whitelist/Blacklist

1. In Function Display area, click **Black/White**.

2. Click **Export Whitelist/Blacklist** button to export whitelist or blacklist file.

Import Whitelist/Blacklist

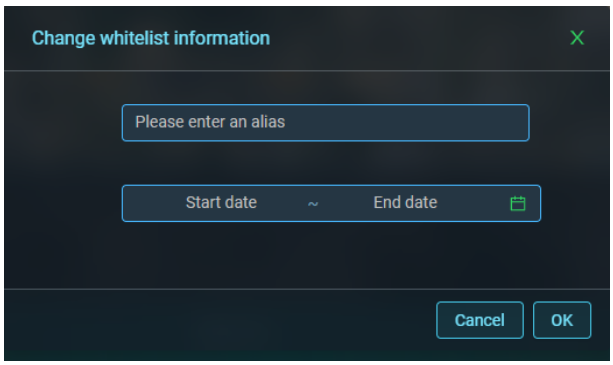
1. In Function Display area, click **Black/White**.
2. Click **Import Whitelist/Blacklist** button to import whitelist or blacklist file. The UTF-8 and XLSX formats are supported.

Add Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Click **Add Whitelist/Add Blacklist** button, enter the ID, Drone Type, Alias, set Effective time, then click  to add.

Update Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Select a list formation to be updated, click  button, update information.
   a) For whitelist, update alias, and effective time range.



   b) For blacklist, update alias.

Delete Whitelist/Blacklist

1. In Function Display area, click **Black/White**.
2. Select a whitelist or blacklist to be deleted, click  button and information will be deleted directly.

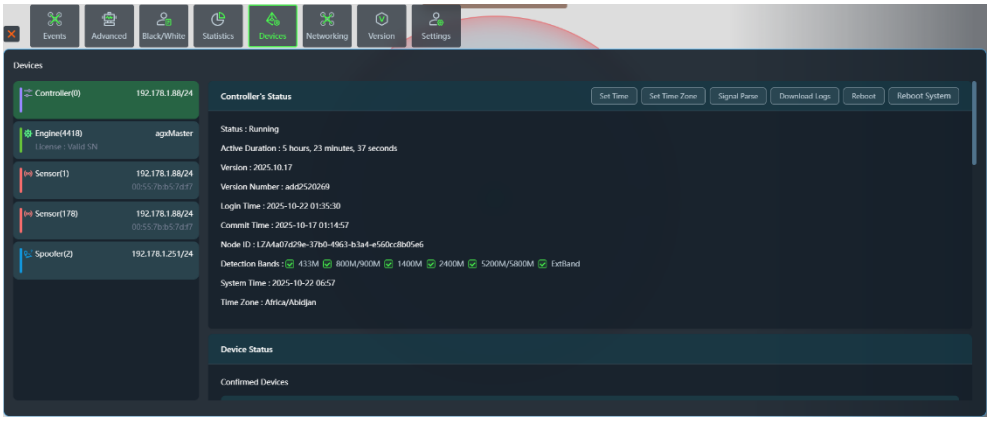
4.9 Check the Statistic Report

1. In Function Display area, click **Statistics**. View the drone event statistics report.

2. Click **Export PDF**, set the time range and export the statistical report in PDF format.

4.10 Check the Device Status

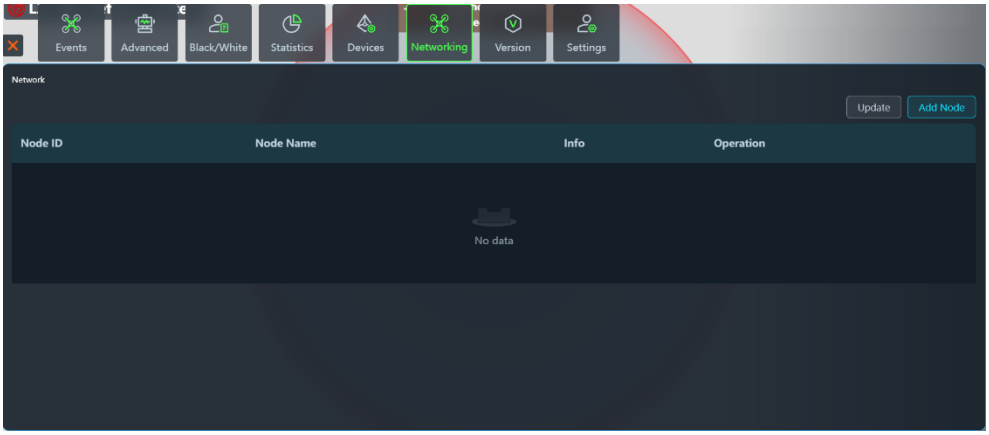
1. In Function Display area, click **Devices**. View the information of Controller, Engine, Sensors and Defender.



4.11 Manage Nodes

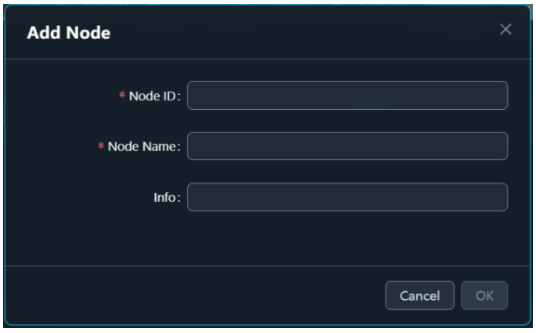
Manage the nodes under Networking function.

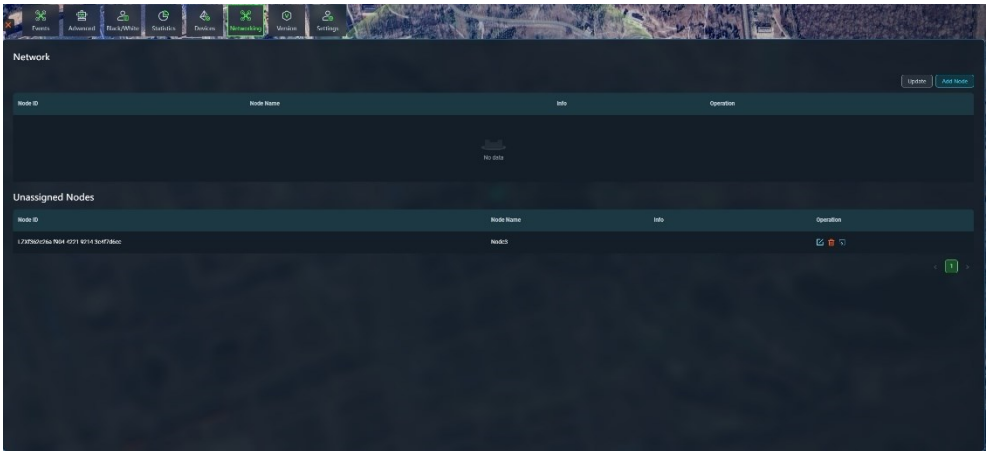
The Networking function icon appears when the site is a Networking Master.



Add Node

1. In Function Display area, click **Networking**.
2. Click **Add Node** button, enter the new node's ID, name and information, then click "OK". The new node appears under Unassigned Nodes.





3. Click  button to move in the node to the networking.

Update Node

1. In Function Display area, click **Networking**.

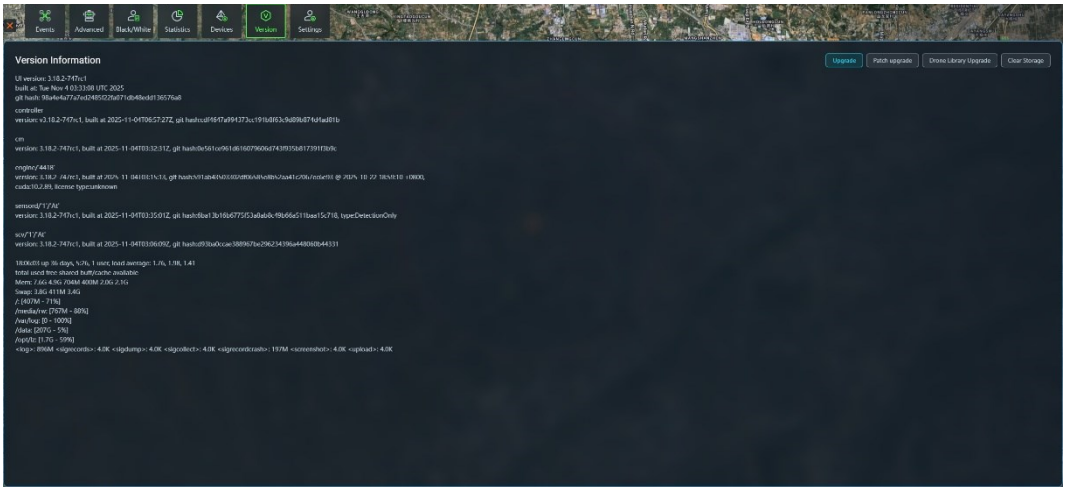
2. Select a node, and click  button to update its Node Name or information.

Delete Node

1. In Function Display area, click **Networking**.
2. Select a node, and click  button to delete this node.

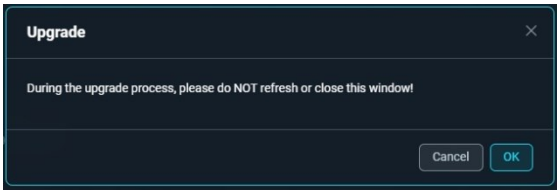
4.12 Check Version

In Function Display area, click **Version** to display the information of UI version, cm, engine, sensor.

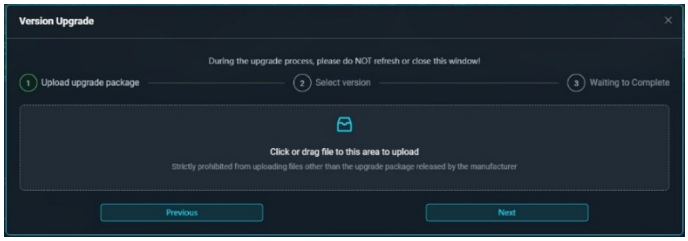


Upgrade Software Version

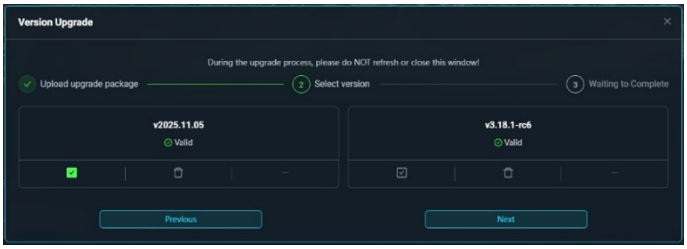
1. Click **Upgrade** button.



2. Click **OK** in the popup.

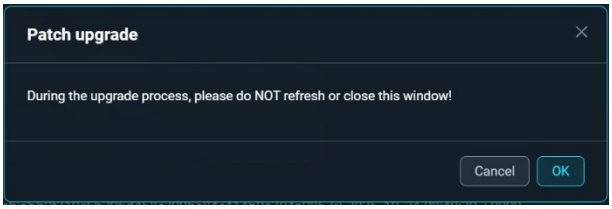


3. Select version to upgrade:
   a) Upload an upgrade package.
   b) Click **Next** button to select a valid software version.

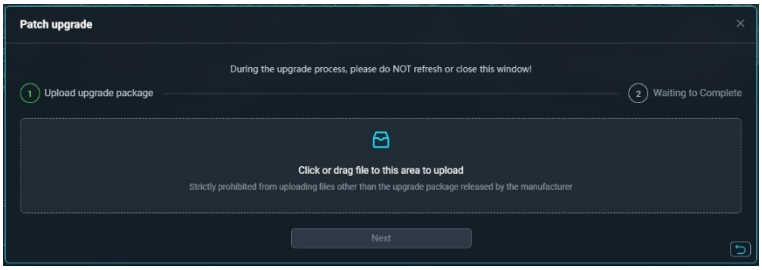


Upgrade Patch

1. Click **Patch Upgrade** button.

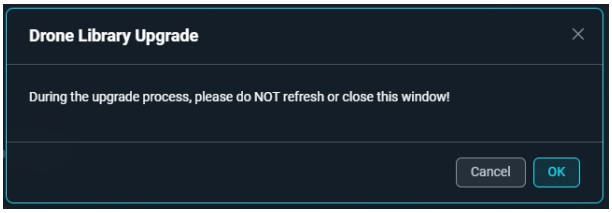


2. Click **OK** in the popup to upload an upgrade package.

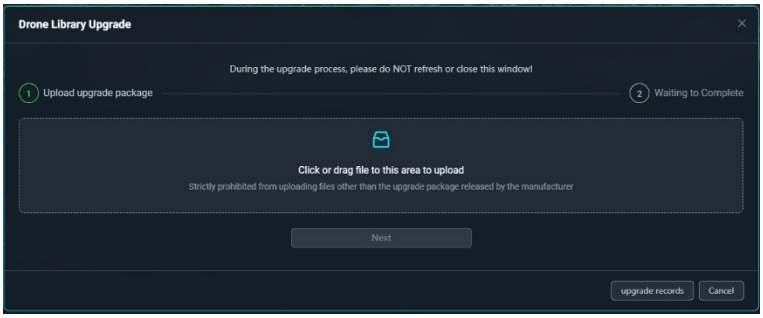


Upgrade Drone Library

1. Click **Drone Library Upgrade** button.

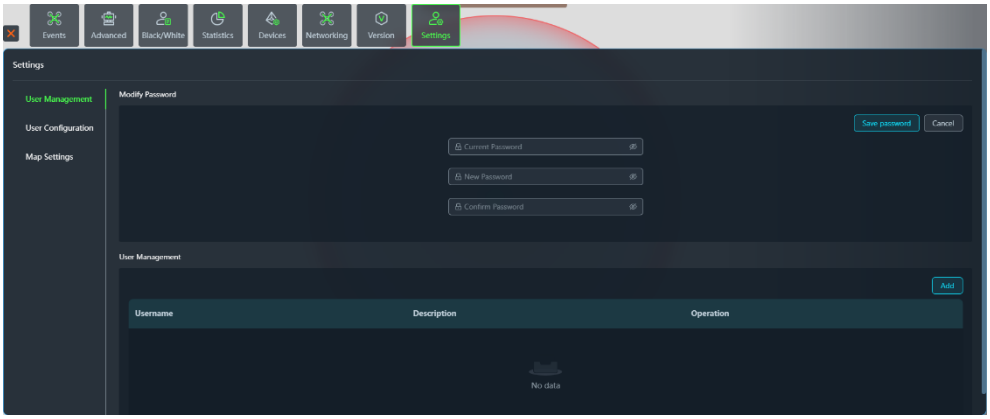


2. Click **OK** in the popup to upload an upgrade package.



4.13 Change Password

1. In Function Display area, click **Settings**.



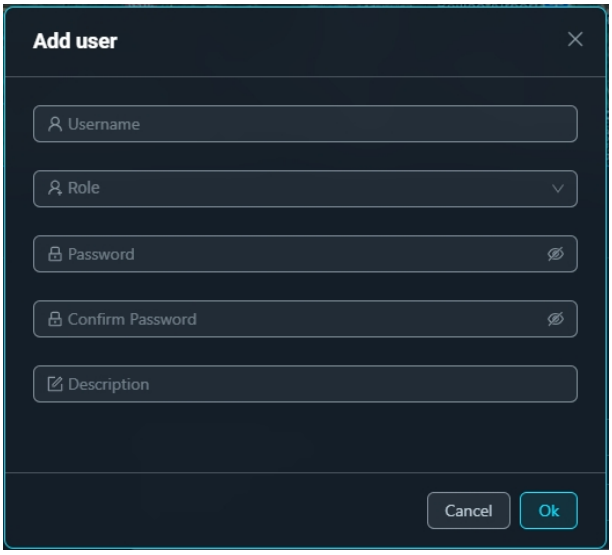
2. Enter the current password and the new password, then click **Save Password** button to set the new password.

4.14 Manage Users

This functionality is restricted to Admin accounts for user management. Normal accounts do not have these permissions.

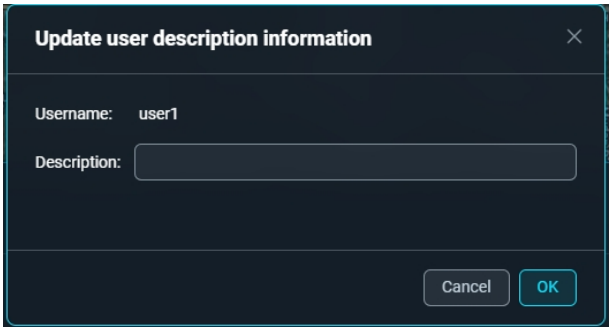
Add Users

1. In Function Display area, click **Settings**.
2. Click **User Management**.
3. Click **Add** button, enter the new user's username, role, password, and description information, then click "OK" to add the new user.



Update User Description Information

1. Select a user to be updated, click **Update** button, update the user's description information.

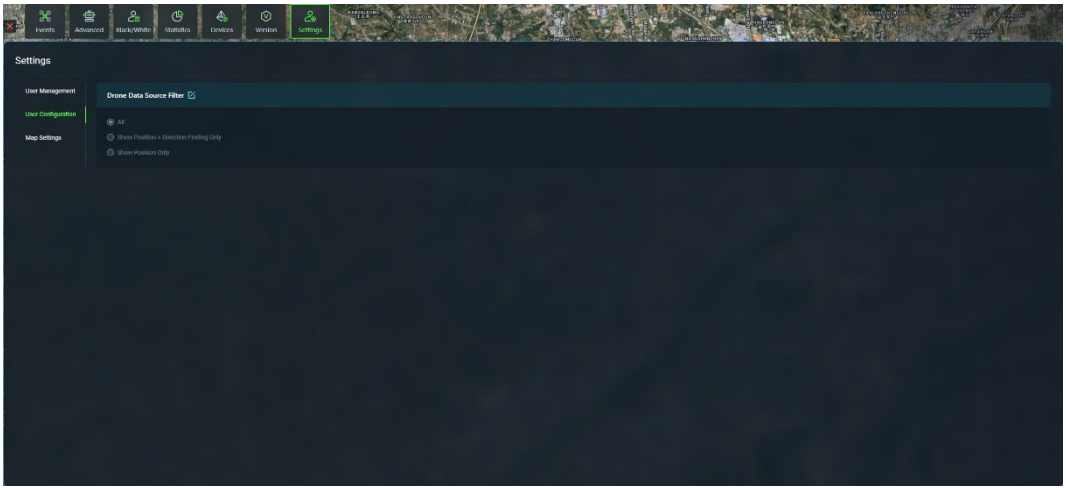


Delete User

1. Select a user to be deleted, click **Delete** button, click **Confirm** to delete the user.

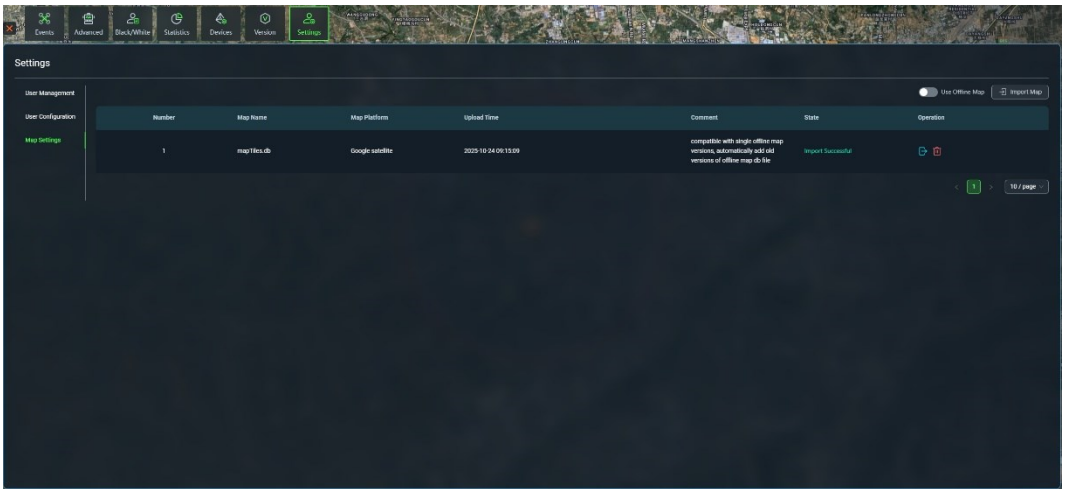
4.15 Configure User

1. In Function Display area, click **Settings**.
2. Click **User Configuration**.
3. Click  icon to select drone data source.



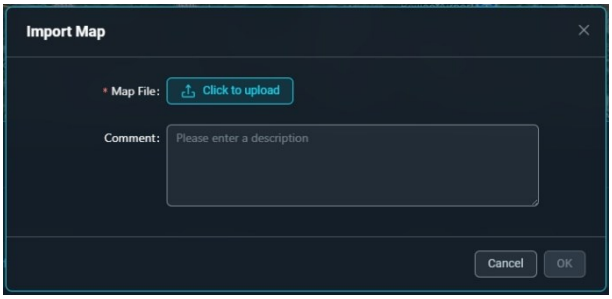
4.16 Manage Maps

The map can be downloaded or imported under Settings.



Import Map

1. In Function Display area, click **Settings**.
2. Click **Map Settings**.
3. Click **Import Map** button.



4. Upload the map file in local directory.

Download Map

1. Click icon to download the map to local directory.

Delete Map

1. Click icon to delete the map.

5 Equipment Maintenance

To ensure stable operation of the equipment, please comply with the following maintenance specifications.

5.1 Routine Maintenance

Maintenance Type	Maintenance Method
Interface protection	Seal unused interfaces with protective covers.
Cable maintenance	● Do not replace antennas without authorization after deployment. ● Ensure cables and interfaces are fully engaged and securely locked. ● Immediately replace any feeder/power/Ethernet cables with damaged jackets or exposed wires. ● Ensure plug pins are not bent or damaged.
Power inspection	Verify that the device is powered normally.

5.2 Basic Troubleshooting

Fault Type	Troubleshooting Method
Power-related fault	● Restart the power switch, boot the server, and launch the related services. ● Power off the device, wait for 30 seconds, and then restart it.
Network disconnection	● Use the *ping* command to test connectivity between the device and the server. ● Unplug and reconnect the network cable, then verify that the port indicator light is on and stable.
System Process	Log in to the "Device" interface to check the process status of the

Exception	controller, engine, and sensors.

If the issue persists, contact our technical support team.

Unauthorized personnel or non-designated maintenance personnel are prohibited from disassembling the chassis.

6 Packaging, Transportation and Storage

The equipment shall comply with the following requirements for packaging, transportation, and storage:

6.1 Packaging

The packing boxes shall be moisture-proof and shock-proof, and contain the following items:

- Delivery list
- Product Inspection Certificate
- User manual.

6.2 Transportation

In the process of transportation, avoid throwing, sun and rain, avoid mixing corrosive substances.

6.3 Storage

The storage shall meet the following requirements:

- Products should be stored in a cool, ventilated, dry warehouse.
- Do not put together with oil, away from heat sources.
- Stacking should be 20cm from the ground and 20cm from the wall.