

DJI FlightHub 2 AIO

User Manual

v1.0

Contents

Using this Manual	3
Read Before Use	3
Product Overview	3
Product Specifications.....	4
Initial Setup.....	5
1 Authorization	5
2 First-Time Activation.....	5
3 Bind Dock to Organization	6
4 Bind Aircraft to Organization	6
Navigating the System Interface	8
1 Language Settings	8
2 Notification Center	8
3 System Maintenance: Updates and Restoration	8
3.1 System Update and Restore Interface	8
3.2 System Update.....	8
3.3 Dongle License Update	9
3.4 Factory Reset.....	9
3.5 Troubleshooting	9
Operation Guide	11
1 Network Management	11
1.1 Wired Network Settings	11
1.2 Wireless Network Settings.....	12
1.3 DHCP Settings	15
1.4 DNS Settings.....	16
1.5 SSH Management	18
2 FlightHub Management	20
2.1 Operations and Maintenance Settings	20
2.2 Basemap Service	22
2.3 Account Settings	24
2.4 Extension Services.....	26
2.5 Access Settings.....	28

2.6 Feature Settings.....	30
2.7 Activation Status.....	31
2.8 Restart FlightHub.....	32
3 Storage Management.....	33
Overview.....	33
Storage Mode Configurations.....	34
3.1 Internal Storage.....	35
3.2 External Storage.....	38
4 Device Information.....	39
4.1 Device Information.....	40
4.2 Device Logs.....	40
4.3 Administrator Password.....	41
4.4 Time Settings.....	42
5 Device Information.....	42
5.1 Overview.....	42
5.2 Navigate to Remote Maintenance.....	43
5.3 Core Feature Operations.....	43
5.4 Notes.....	44

Using this Manual

Read Before Use

Product Overview

The FlightHub 2 AIO is a powerful, all-in-one solution for deploying DJI's FlightHub services on a private, local network. With just a few simple setup steps, you can integrate a full-featured FlightHub platform into your workflow, ensuring all your task data remains securely within your own environment.

The AIO supports connecting with the DJI Pilot 2 app, allowing you to manage and coordinate tasks for up to 20 aircraft and docks.

Product Specifications

CPU	Core Ultra 7 Processor 265
Memory	64 GB × 1
Dedicated Graphics	NVIDIA RTX 2000 Ada
SSD Storage 1	2 TB (System Drive)
SSD Storage 2	2 TB (Data Drive A)
SSD Storage 3	2 TB (Data Drive B)
Wireless Network	802.11be 2×2
Wired Network	1Gbps × 4 PCIe Network Card
Operating System	Ubuntu 24.04.2 LTS Desktop

Initial Setup

Your FlightHub 2 AIO is designed for immediate use. It comes pre-configured with the necessary operating system, drivers, and application software. Follow these steps to get started.

1 Authorization

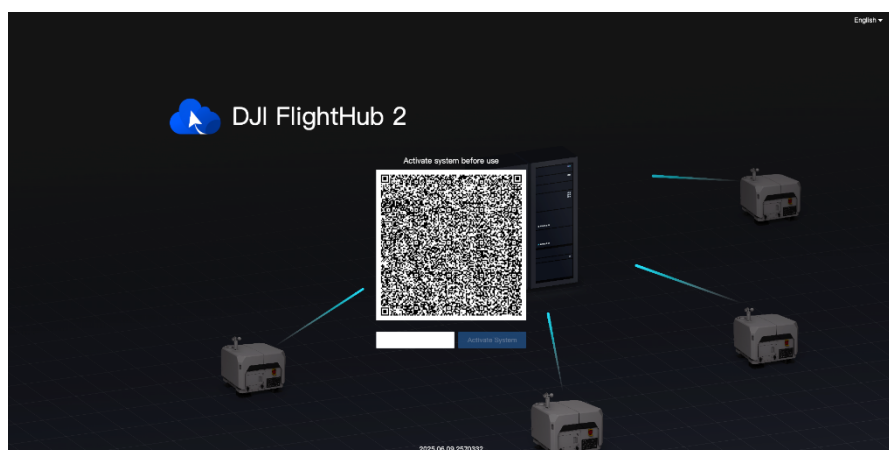
Before powering on the AIO, insert your authorized AIO dongle into any available USB port. Power on the AIO. The system will automatically detect the license and load the necessary services.

The AIO dongle must remain connected to the AIO at all times during operation. Removing the dongle will immediately deactivate the services and interrupt your workflow.

2 First-Time Activation

When first unboxing the AIO and accessing <http://fhaio.net> or 192.168.1.1:30888 on a computer, you will be automatically directed to the setup wizard. Follow the on-screen instructions to complete the initial configuration. This process will take a few minutes to help you further understand how to use the AIO. After completing the configuration, you can jump to the FlightHub page.

When first accessed, or when subsequently upgrading services and authorization, FlightHub will require users to complete the service activation operation. The specific activation method is as follows:



1. Use a mobile browser to access the [remote activation service](#) and enter the real-name account registered on the DJI Developer website.
2. After submitting the account and passing the real-name authentication of the activation service, the activation page will display a QR code. Scan the QR code

to obtain a dynamic activation code (valid for 1 minute).

3. Enter this code on the activation page. Once activation is complete, you will be redirected to the FlightHub 2 login page.
4. You can then begin using FlightHub services.

3 Bind Dock to Organization

Create Organization

1. Open a web browser (Google Chrome 120 or later is recommended.)
2. Enter URL: `http://${SERVICE_DOMAIN}:${FRONTEND_TCP_PORT}`. The default system: `Http://192.168.1.1`
3. Log in with the default credentials:
 - Username: admin
 - Password: Password@
4. Follow the prompts to create an organization. The AIO supports a single organization, so enter your details carefully.
5. Within your organization, create a project to manage your tasks and devices.

Obtain Device Binding Code.

Go to Devices > Dock > Device Binding to obtain device binding code and organization ID.

Cloud Service Configuration

Use a USB-A to USB-C cable to connect the remote controller and the dock, open the DJI Pilot 2 app, navigate to the dock's cloud service settings, select FlightHub 2 On-Premises Version, and fill in the following details:

6. Access Address: `${SERVICE_DOMAIN}:${BACKEND_TCP_PORT}`. The default system: `192.168.1.1:30812`
 - Organization ID: Enter the organization ID obtained in the previous step.
 - Device Binding Code: Enter the organization binding code obtained in the previous step.
 - Dock Name: Enter the dock name.

Bind Device to Organization

Under Project, select a project to bind the device to the organization.

4 Bind Aircraft to Organization

1. Tap the Settings icon in the upper left corner of the Home page and log in to your DJI account.

2. Tap Cloud Services and select FlightHub 2 Cloud Platform. Server address: <http://192.168.1.1:30812> (http:// is required). Please enter the registered FlightHub 2 username and password; the default is admin / Password@.
3. Upon first login, users need to select the organization and project for the task. Subsequent logins will default to the last logged-in organization and project. If the current account has not joined any organization, contact the administrator to add it.
4. After successful login, the DJI Pilot 2 page will display current project information, and users can tap Device Binding to bind an aircraft.
5. Once bound, the aircraft can be viewed and managed on the FlightHub web interface.

Navigating the System Interface

1 Language Settings

You can change the display language to suit your preference. In the upper right corner of the interface, click the Language icon to switch languages. Select from the available options:

- Simplified Chinese
- English
- Spanish

2 Notification Center

The notification center alerts you to important system events, such as disk errors, to help you monitor system health. To view notifications, click the bell icon in the upper right corner.

- A panel will display a list of alerts, showing the issue and the time it occurred. Click View next to a notification to navigate directly to the relevant management page for more details.
- If there are no alerts, the panel will display "No notifications".

3 System Maintenance: Updates and Restoration

The system update and device restore module supports uploading update packages to update the system and restoring factory settings, for system feature iteration, fault repair, or initial configuration.

Note: Data needs to be backed up before operation to avoid loss.

3.1 System Update and Restore Interface

Click System Update & Restore in the left-hand navigation menu to enter the configuration page, which contains three major features: System update, dongle license update, and factory reset.

3.2 System Update

Upload Update Package

Click Upload Update Package. By default, local files are displayed. Select the system update package provided by DJI official (format tar.gz etc.) and click Update. The system will begin the update process and automatically restart when complete. After successful upload, the file will appear in the uploaded update package list.

Update from AIO Local Path

Click Select from AIO Local Path, enter the absolute file path (e.g., C:\Users\Username\Documents\Update package tar.gz).

- If the path is incorrect, a message prompts "File not found. Enter correct path", and the path needs to be re-verified.
- If the path is correct, the file will be automatically uploaded.

3.3 Dongle License Update

The update package update process is as follows:

1. Obtain the dongle license update file (.zip format) from the DJI Developer website.
2. In the Dongle Update section, click Upload File. Select the .zip license file.
3. Once the upload is successful, click Update. The system will apply the new license to the connected USB dongle.

Note: If prompted with "Network error. Upload failed" during the update process, verify the format, integrity, validity, and version of the license file.

Note: When powering on without a dongle inserted and directly entering fhaio.net, a full-screen error will be triggered, prompting "Dongle not detected. Make sure dongle is inserted into AIO". Insert the dongle correctly according to the hardware interface diagram.

3.4 Factory Reset

1. Click Restore Factory Settings. A pop-up window will require you to enter the administrator password for three times.
2. Enter the correct administrator password in sequence.
3. After the third password verification passes, click Confirm Factory Reset, and the system will begin to reset.
4. The factory reset will restore the AIO to its original state, erasing all system configurations and data.

Note: The factory reset only applies to the operating system and does not affect the hardware.

3.5 Troubleshooting

Symptom	Solution
The update process fails with an error message like "Update failed," "Network error," or "Corrupted package".	Check the integrity of the update file. Return to System Update & Restore, re-upload the file, or perform a factory reset and then retry the upload.
You cannot log in or authorize a factory reset because you have forgotten the administrator password.	You can reset the password by running a command directly on the AIO's operating system terminal. curl -X PUT -H "Content-Type:

	<pre>application/json" -d '{"new_pwd":"YourNewPassword123"}'</pre> Note: The new password must be at least 12 characters long and contain uppercase letters, lowercase letters, and numbers.
When uploading the update package, the progress bar gets stuck and a "Transfer failed" message appears.	Switch to a wired network and check network stability. Re-download the package from the DJI Developer website and retry the upload.

Operation Guide

1 Network Management

1.1 Wired Network Settings

Overview

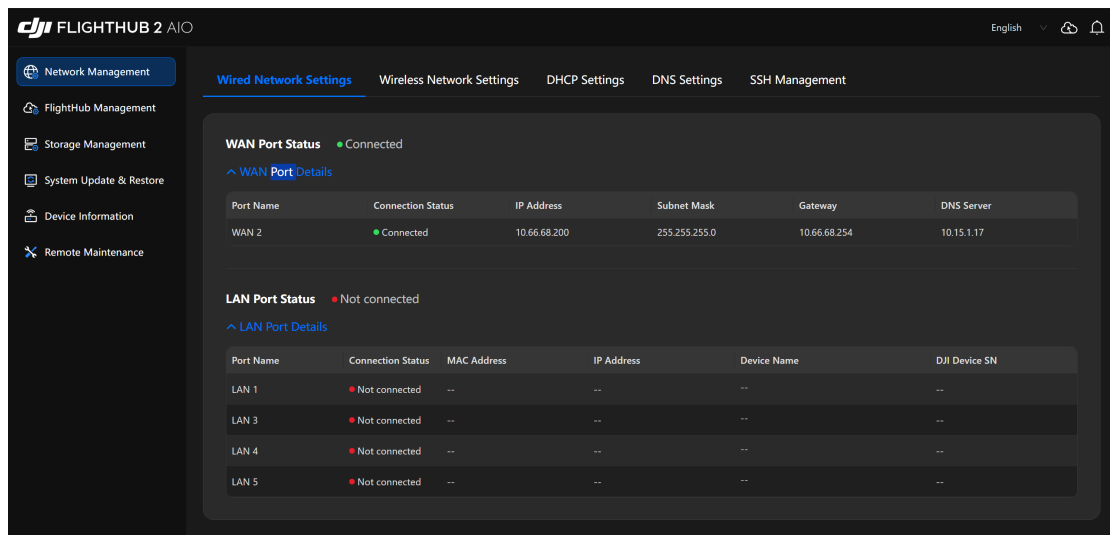
Use this section to monitor the status of your WAN and LAN ports, view network details, and troubleshoot connection issues.

Steps

1. Accessing the Wired Network Settings

Click Network Management in the left-hand navigation menu and select Wired Network Settings.

2. WAN Port Connection Status



Status Indicator	Description	Troubleshooting
Green (Connected)	A green indicator next to the WAN port means it is connected successfully. Click the arrow to expand and view details like its IP address, subnet mask, and gateway.	If parameters are in error, go to DHCP Service Settings or manually configure a static IP (must be compatible with the upstream network).
Red (Not Connected)	A red indicator means the port is not connected.	1. Check that the network cable is securely plugged in and make sure that the router and devices are powered on and functioning correctly.

		2. Restart the FlightHub 2 AIO to re-initiate the connection.
--	--	---

3. LAN Port Connection Status

Status Indicator	Description	Troubleshooting
Green (Connected)	A green indicator signifies that one or more devices are connected. Click the arrow to expand and view details: - MAC address, IP address, subnet mask of each LAN port - Connected device name and SN Note: If one LAN port connects multiple devices, multiple records will be displayed.	1. If the device is not detected, check that the network cable is securely plugged in and make sure that the connected device is powered on and functioning correctly. 2. Make sure there are no IP conflicts. Note: Dynamic IP can be assigned through DHCP Service Settings.
Red (Not Connected)	A red indicator means no devices are connected or a connection error has occurred.	1. Check that the network cable is secure and the connected device is powered on. 2. Restart the FlightHub 2 AIO to re-initiate the connection.

4. Multiple Device Connection Management

- When one LAN port connects multiple devices, expanding LAN Port Details will display data for all connected devices.
- You can locate a specific device by its device name or SN and verify if its network parameters are consistent.

Notes

- Backup Settings: Before adjusting parameters such as IP and DHCP, record the original configuration to prevent the loss of unrecoverable settings.
- Hardware Check: If you experience frequent disconnections, try using a different network cable to rule out a faulty cable or port.
- Multiple Devices: When connecting multiple devices, make sure your DHCP address pool is large enough to prevent IP address conflicts.

1.2 Wireless Network Settings

Overview

The AIO's built-in Wi-Fi can operate in two modes.

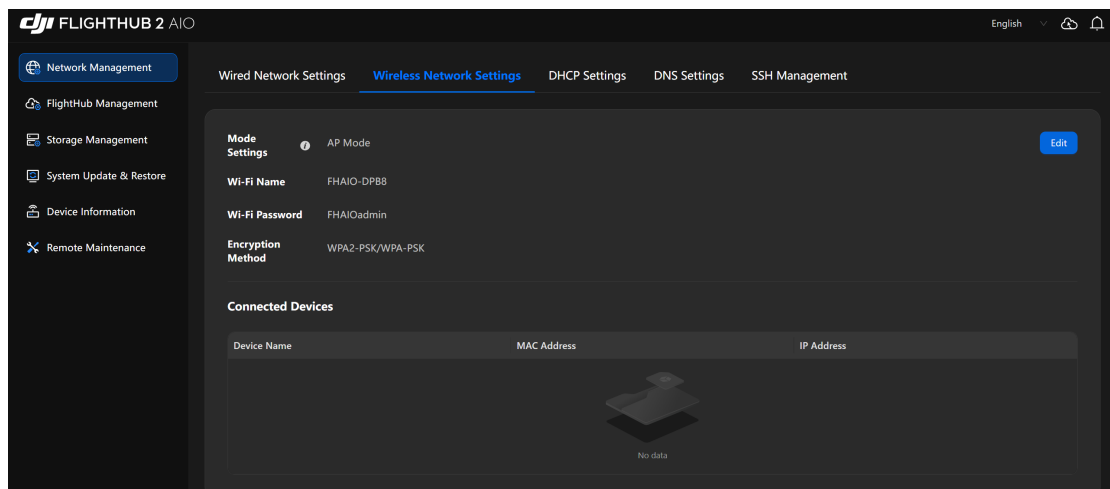
- **AP (Access Point) Mode:** The AIO creates its own Wi-Fi hotspot. This is useful for directly connecting devices like a remote controller or mobile phone for initial setup or management.
- **Station Mode:** The AIO connects to an existing Wi-Fi network. This allows it to access the internet or other network resources wirelessly.

Note: When switching from AP to Station mode, connect your computer directly to the AIO with an Ethernet cable to prevent being unable to access the management backend after the switch.

Steps

1. Accessing the Wireless Network Settings

Navigate to Network Management > Wireless Network Settings.



2. AP Mode Operations

2.1. Configure Hotspot Parameters

1) Click the Edit button.

2) Modify parameters:

- **Wi-Fi Name:** Customize the hotspot SSID (e.g., FHAIO-XXXX. It is recommended to include a device identifier).
- **Wi-Fi Password:** Set a password of 8 or more characters to ensure hotspot security.
- **Encryption Method:** WPA-PSK/WPA2-PSK (Default).

3) Save and Apply:

Click Save, the device will restart the hotspot module, and the new parameters will take effect immediately.

2.2. View Connected Devices

In the connected device list, you can view:

- The name of the connected device, MAC address, and assigned IP address.
- If multiple devices are connected, the list will display all device information for easy management.

3. Station Mode Operations

3.1 Mode Switching

To switch to Station Mode: Click Edit and select Station Mode. After reading the warning, click Switch to enter the Station mode configuration page.

Note: After switching, you will not be able to access the backend via the original hotspot (fhaio.net). You will need to reconnect using one of the following methods:

- Method 1: From another computer on the same LAN, access the device's external IP address on port 30888 (e.g., 192.168.1.101:30888).
- Method 2: Connect your computer to the AIO with an Ethernet cable and navigate to <http://fhaio.net>.

3.2 Select External Wi-Fi

Scan for Wi-Fi: Click Update Wi-Fi to scan for nearby wireless networks.

The list displays available Wi-Fi networks nearby, including:

- Name (SSID), signal strength, and encryption status (Lock icon indicates encrypted; no lock indicates an open network).
- If no Wi-Fi is available, the pop-up window will display "No Wi-Fi available". You can click Search Again.

Select Wi-Fi: Click the Wi-Fi network you want to connect to.

3.3 Enter Wi-Fi Password

Select Encryption Method: A password input box will pop up. Select based on the Wi-Fi type:

- Standard encryption (WEP/WPA2/WPA3): Enter the Wi-Fi password, then click Join.
- Enterprise encryption (EAP-PEAP): Enter the authentication account and password, then click Join.

Password Verification:

- Correct: The device attempts to connect.
- Incorrect: A pop-up will prompt "Incorrect password," requiring re-entry.

3.4 Complete Connection

After a successful connection: The interface displays the Wi-Fi SSID (connected Wi-Fi name), local IP (device's IP on the network), subnet mask, and DHCP server status.

Confirm Switch: Click Save. A prompt box will reappear, reminding you of the reconnection method. Click Switch again to complete the mode change.

3.5 Troubleshooting

Symptom	Solution
No Wi-Fi networks found	Make sure you are within range of a Wi-Fi router. Click Search Again to refresh the list.
Connection fails due to incorrect password	Carefully re-enter the password, paying attention to case sensitivity. For enterprise encryption, make sure to confirm authentication account permissions.
Cannot access the AIO after switching to Station Mode	The easiest solution is to connect your computer to the AIO with an Ethernet cable and navigate to http://fhaio.net . Alternatively, contact the network

	administrator to obtain the device's external IP.
--	---

1.3 DHCP Settings

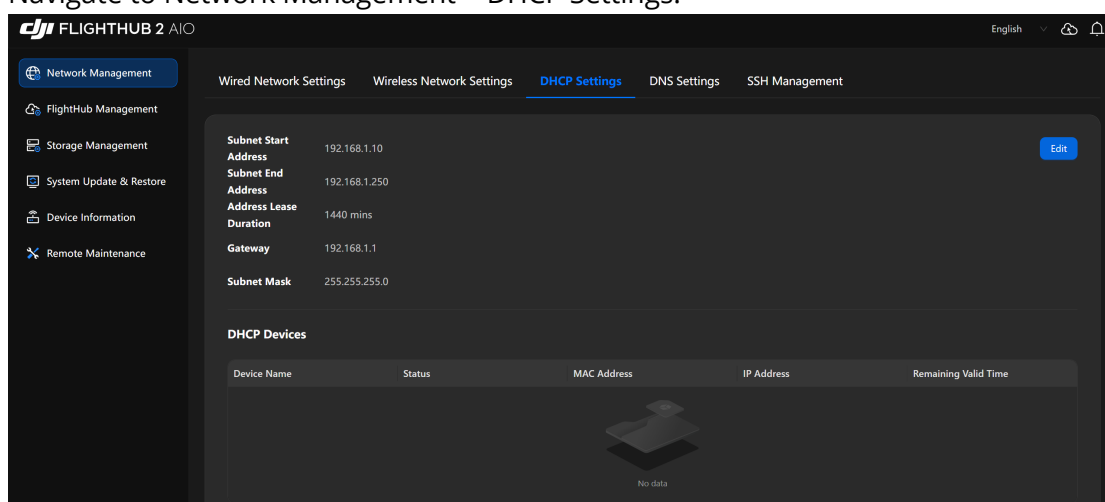
Overview

The DHCP (Dynamic Host Configuration Protocol) service automatically assigns IP addresses and network settings to connected devices, supports configuring IP address ranges, address lease times, gateways, and subnet masks, and displays the real-time statuses of assigned IP addresses, MAC address, and validity period of assigned IP devices, facilitating network management and troubleshooting.

Steps

1. Accessing the DHCP Settings

Navigate to Network Management > DHCP Settings.



2. Viewing Current DHCP Settings

The configuration items are shown in the table below:

Setting	Parameters	Description
Subnet start address	e.g. 192.168.1.2	Defines the range of IP addresses that the AIO can assign to connected devices.
Subnet end address	e.g. 192.168.1.255	
Address lease duration	Range: 1 to 2880 minutes	How long a device can keep an assigned IP address before it needs to be renewed.
Gateway	e.g. 192.168.1.255	The IP address that devices use to communicate with networks outside their own.
Subnet mask	e.g., 255.255.255.0	Defines the size of the local network.

DHCP device list	Shows the parameters for devices that have been assigned IP addresses.	Including device name, status (online/offline), MAC address, IP address, and lease time.
------------------	--	--

3. Edit DHCP Parameters

3.1 Enter Edit Mode

Click the Edit button in the upper right corner.

3.2 Modify Parameters

Parameters	Rules and Recommendations
Subnet start address	Must be a valid IP address, and the start address must be lower than the end address.
Subnet end address	Must be within the same network and avoid conflicts with static IP addresses.
Address lease duration	Supports configuring a lease period of 1-2880 minutes. Shorter lease periods lead to more frequent IP updates, while longer lease periods result in more stable IP addresses.
Gateway	Must be consistent with the LAN gateway (e.g., 192.168.1.255).
Subnet mask	By default is 255.255.255.0.

3.3 Save Configurations

- Click Save. If the parameters are valid, the settings will be applied.
- If there is a parameter error, the parameter needs to be corrected.

After saving, you need to unplug and replug network cables to make sure the devices obtain the new DHCP configurations.

Notes

- Parameter Backup: Back up the original configurations prior to modification to prevent issues like interrupted network.
- Avoid Conflicts: Make sure that the DHCP network segment does not overlap with any static IP addresses. Overlapping segments will cause address conflicts.

1.4 DNS Settings

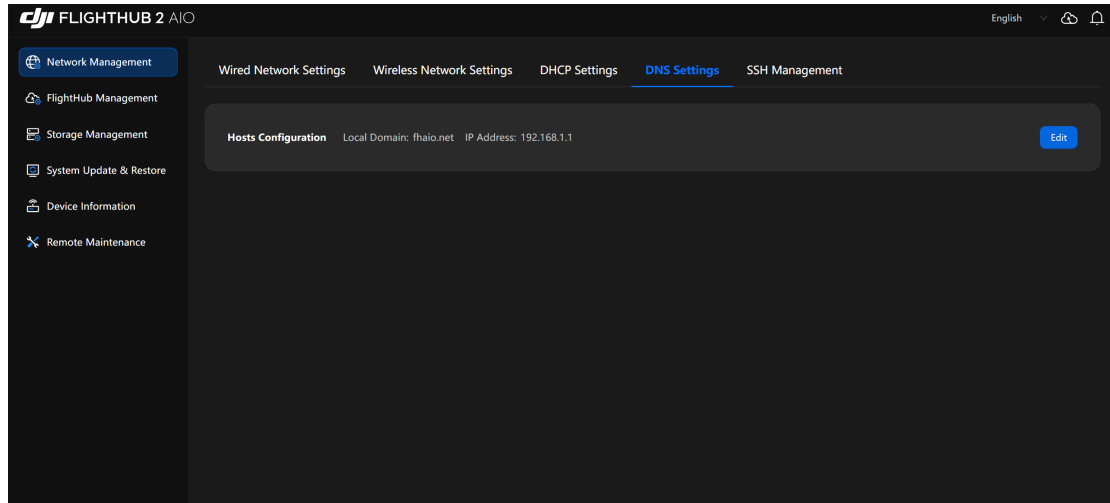
Overview

Domain name resolution settings allow you to create custom domain names that point to specific IP addresses within your local network, commonly used to access intranet services or devices.

Steps

1. Access the Domain Name Resolution Settings

Navigate to Network Management > DNS Settings.



2. Edit Hosts Entries

2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

2.2 Modify Existing Entries

Click directly on the domain name or IP address fields and make your changes.

- Domain Name: Must conform to standard DNS naming conventions (e.g., example.com). Special characters are prohibited.
- IP Address: Must be a valid IPv4 address. Prohibited formats include 0.0.0.0, addresses with segments outside the 0-255 range.

2.3 Add A New Entry

- Click the blue + icon and fill in the desired domain name and the corresponding IP address.
- Enter the new domain name and IP address.

2.4 Delete An Entry

Click the red - icon next to the entry you wish to remove.

Note: Exercise caution, as it cannot be recovered after deletion.

3. Save Configurations

- Click Save to apply your changes.
- If the input format is incorrect, you need to correct it and save again. The interface does not currently provide validation prompts, so manual verification is required.

4. View Saved Hosts Entries

After saving and exiting editing mode, all configured domain-IP mappings will be listed in the interface, enabling simple verification and subsequent management.

Notes

- Domain Uniqueness: Do not assign the same domain name to multiple IP addresses, as this will cause conflicts.
- IP Validity: Ensure the IP address you enter corresponds to a real, accessible device on your network.
- Application Scenarios: These settings apply to the AIO and devices within the same LAN. If public network resolution is required, configurations with a DNS

server or domain name service provider is needed.

1.5 SSH Management

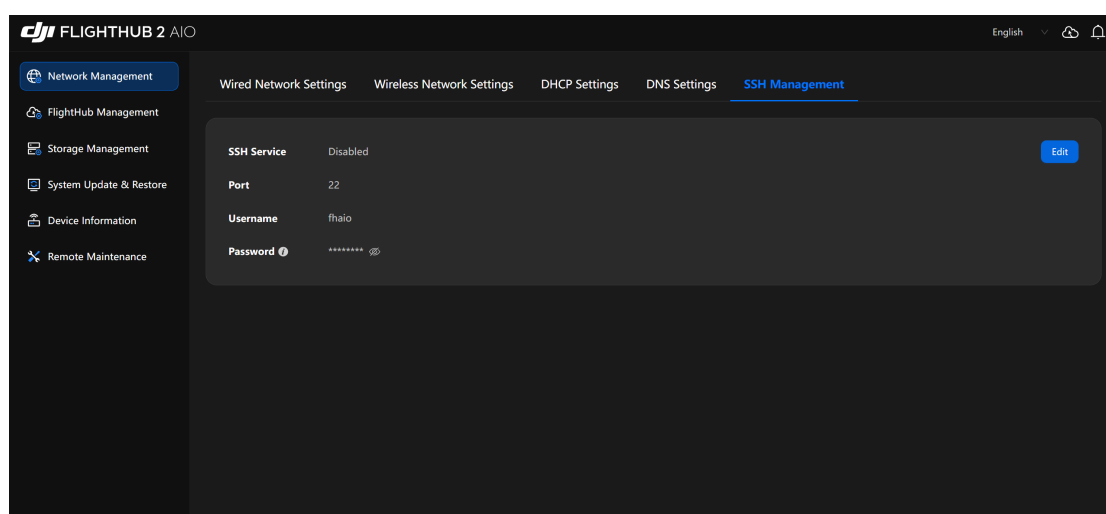
Overview

SSH (Secure Shell) provides secure access to the AIO's underlying operating system. This is an advanced feature intended for troubleshooting and system administration. Enabling SSH exposes your system to potential remote access. Only enable it when necessary and use strong, unique credentials.

Steps

1. Accessing the SSH Management Interface

Navigate to Network Management > SSH Management.



2. View Current SSH Status

The configuration items are shown in the table below:

Item	Parameters	Description
SSH service	Enabled/disabled	Blue indicates enabled, while gray indicates disabled.
Port	22 (Default)	Modifiable. Must be within the port range 0-65535.
Username	Current SSH login account	
Password	Hidden by default	Click the eye icon to temporarily display, and click again to hide.

3. Edit SSH Configurations

3.1 Enter Edit Mode

Click the Edit button in the upper right corner to open the administrator password verification dialog box:

- Enter the system administrator password. This password is the same as the one used for the device management backend.

- Click Confirm to enter editing status.

3.2 Modify Configuration Items

Parameters	Rules and Recommendations
SSH service	Enable/Disable SSH: Use the toggle switch to turn the SSH service on or off. It is highly recommended to keep it disabled during normal operation.
Port	The default port is 22. The valid range is 1-65535.
Username	Set a strong, unique username and password for SSH access. Avoid simple names like admin or root.
Password	The password should be complex and at least 8 characters long, containing uppercase letters, lowercase letters, and numbers. Note: When hovering the mouse over the info icon, a prompt may appear indicating that the frontend and backend passwords might be inconsistent.

3.3 Save Configurations

Click Save to apply your changes.

- If the configuration is valid, it will be saved successfully, and the configuration will take effect immediately.
- If the input format is incorrect, you need to correct it and save again. The interface does not currently provide validation prompts, so manual verification is required.

Notes

- Enable on Demand: Only turn on SSH when you actively need it for maintenance.
- Use a Strong Password: Create a complex password with a mix of uppercase letters, lowercase letters, numbers, and symbols.
 - Passwords should be complex and changed regularly (avoid pure numbers or simple combinations);
 - Change the Default Port: Using a non-standard port makes it harder for attackers to find and target your SSH service.
- Network Isolation: If your AIO is connected to the internet, it is recommended to implement firewall or router rules to permit SSH port access only from trusted IP addresses.

2 FlightHub Management

2.1 Operations and Maintenance Settings

Overview

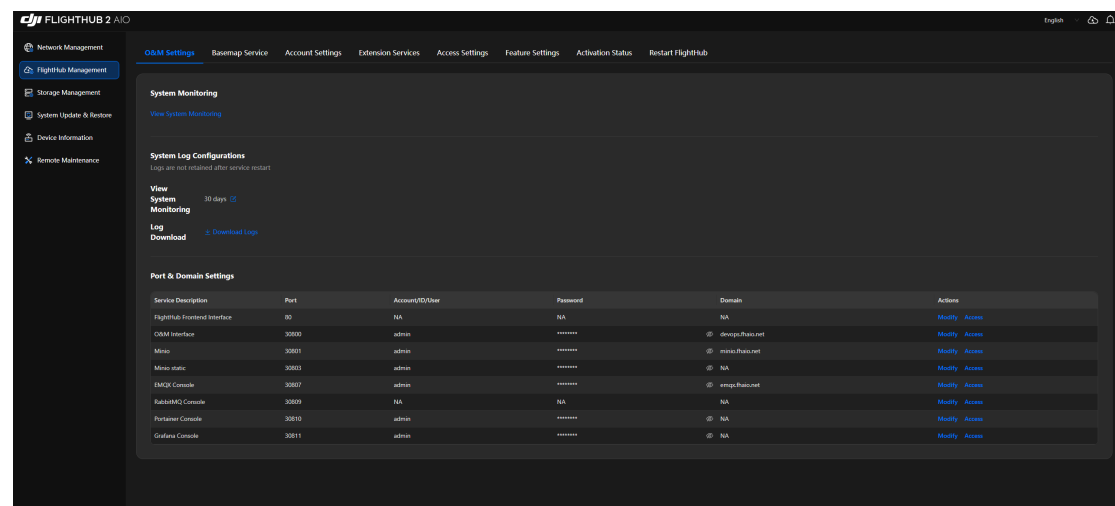
This module provides tools for managing system logs, O&M ports, accounts, domains, and system monitoring, supporting device troubleshooting, remote O&M, and service configuration. **Operate with caution.**

Note: Making changes to most settings within the FlightHub management section will trigger an automatic restart of the FlightHub 2 services. This process can take 2 to 10 minutes, during which time FlightHub 2 will be unavailable.

Steps

1. Accessing the O&M Settings

Navigate to FlightHub Management > O&M Settings.



2. System Log Configurations

2.1 Log Retention

Set how long system logs are kept. Choose from 1, 3, 7, or 30 days.

- Click the desired number of days (e.g., "7 days"). A green checkmark will appear on the right to confirm your selection.
- To cancel, click the red cross that appears next to the selected duration.

Note: Logs are not retained after a service restart. Only O&M logs within the selected duration are recorded.

2.2 Download Logs

Click Download Logs to automatically package and download log files for the current retention period.

3. Service Port and Domain Management

3.1 Service List Overview

Easily manage your services with this interface, which displays essential connection information such as ports, account/ID, passwords, domains, and operation access

points for Operation Interface, MinIO, MinIO Static, EMQX Console, SRS Console, RabbitMQ Console, Portainer Console, Grafana Console, and Traefik Gateway Console.

3.2 Modify Service Configurations

3.2.1 Start the Modification Process

Click the Edit icon next to the service you wish to change. Enter the system administrator password. This password is the same as the one used for the device management backend.

3.2.2 Edit Configuration Items

After entering the edit status, you can modify:

Item	Rules and Recommendations
Port	Enter a valid port (0-65535) to avoid conflicts with other services. The default for the operation and maintenance interface is 30800.
Account/ID/User	Customize login account. For enhanced security against brute-force attacks, it is recommended to use a complex account name.
Password	The password should be complex and at least 8 characters long, containing uppercase letters, lowercase letters, and numbers.
Domain	Enter a valid domain name, which must be compatible with network resolution rules.

3.2.3 Save or Cancel Changes

- Click the green checkmark to save your changes. This will restart the specific service.
- Click the red X to cancel.

4. System Monitoring

Click the View System Monitoring link to access the monitoring dashboard. It displays:

- Device Resource Status: CPU, memory, and storage utilization.
- Service Running Status: Backend service online status and response times.
- Error Alerts: Service errors are highlighted in red.

Notes

- Password Verification: Modifying O&M configurations always requires administrator password verification. If forgotten, refer to the system recovery guide for password reset instructions.
- Service Restart Risk: Modifying ports, accounts, or domains will cause the affected service to restart. Plan these operations during low-usage periods.
- Log Storage: Retaining logs for longer periods consumes more storage space. Regularly download logs for archiving and consider shorter retention periods if storage is a concern.
- Network Adaptation: If you change a service's port or domain, you must update any external clients (e.g., web browsers, O&M tools) that connect to it, or they will lose access.

2.2 Basemap Service

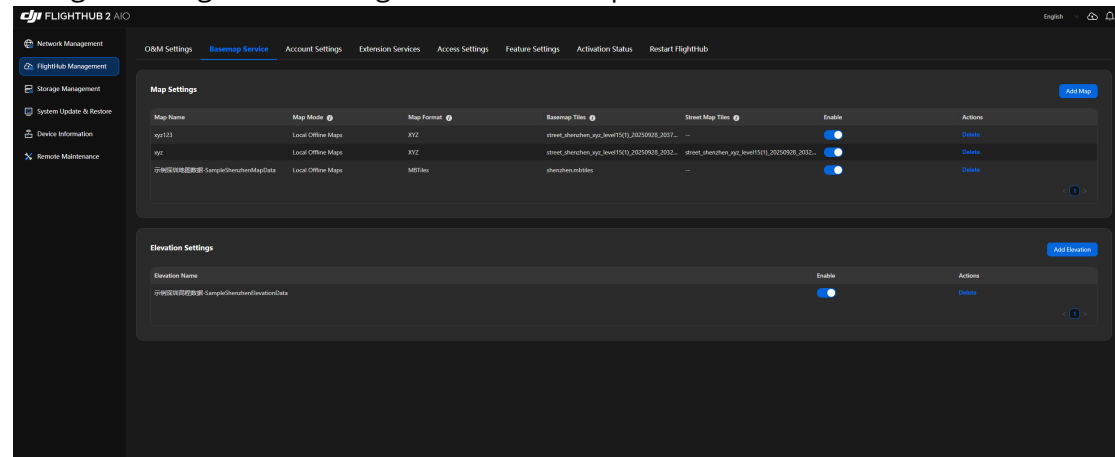
Overview

This module allows you to manage the map and elevation data used within FlightHub 2, supporting various map access modes (offline, online, intranet).

Steps

1. Accessing the Basemap Service

Navigate to FlightHub Management > Basemap Service.



2. Map Settings

2.1 View Existing Map List

Displays all configured maps, including their name, mode, status, and actions.

- Map name
- Map mode
- Map format
- Basemap tiles / street map tiles
- Status
- Actions

2.2. Add New Map

2.2.1 Enter the Add Process

Click Add Map in the upper right corner, and the Add Map configuration box will pop up.

2.2.2 Configure Map Parameters

Item	Operations and Rules
Map name	Provide a custom name for easy identification.
Map mode	Select how the map data is accessed: - Local Offline Maps: Requires you to upload map tile files. - Online Maps: Connects to a public online map service. Requires a service URL and potentially an API key. - Custom Online Maps: Connects to a map service hosted on your local network.

Map format (for local maps only)	Choose between MBTiles (a single database file) or XYZ (a folder structure of individual tile images).
Basemap Tiles / Street Map Tiles (for local maps only)	Click Upload File to select your map tile package (e.g., .mbtiles, .zip format). Street tiles are optional.

2.2.3 Submit and Upload

- Click Add. The system will upload the files (if applicable) and add the map to the list.
- You must then manually enable it.

2.3 Edit Existing Map

- Click the tile link. Enter your system administrator password for verification.
- Modify the map name, mode, or format.

Note: Changing the map mode or format will clear previously uploaded tile files, requiring re-upload.

- Click Save to apply changes.

2.4 Delete Map

- Click the Delete button next to the map. A confirmation dialog will appear.
- Click Delete again to confirm.

Caution: This action is irreversible.

2.5 Enable/Disable Map

Use the toggle switch. Blue indicates the map is active and prioritized. Gray indicates it's deactivated. When multiple maps are enabled, maps higher in the list are prioritized.

3. Elevation Settings

3.1 View Existing Elevation List

The interface displays configured elevation data, including name, latitude/longitude range, status, and actions.

3.2 Add New Elevation Data

Click Add Elevation, and fill in the following information:

- Elevation Name: Custom name.
- Latitude and Longitude Range: Enter a valid range.
- Optionally, click Upload File to submit elevation tile files.

Click Add. The data will be added and needs to be manually enabled.

3.3. Delete Elevation Data

Click the Delete icon.

Caution: This action is immediate and irreversible.

Notes

- File Upload Restrictions:
 - For local tile files, ZIP compression files are recommended. Single files should not exceed 1 GB to avoid upload failures.
 - Make sure file formats are valid.
- Map Mode Switching Risks: Switching a map from local offline to online mode will clear the associated tile files. You will need to reconfigure the online map URL.

- Administrator Password Verification: Editing or deleting maps and elevation data requires administrator password verification for security.
- Map Priority: When multiple maps are enabled, FlightHub 2 will load the map that appears highest in the list. Manual adjustment is supported.

2.3 Account Settings

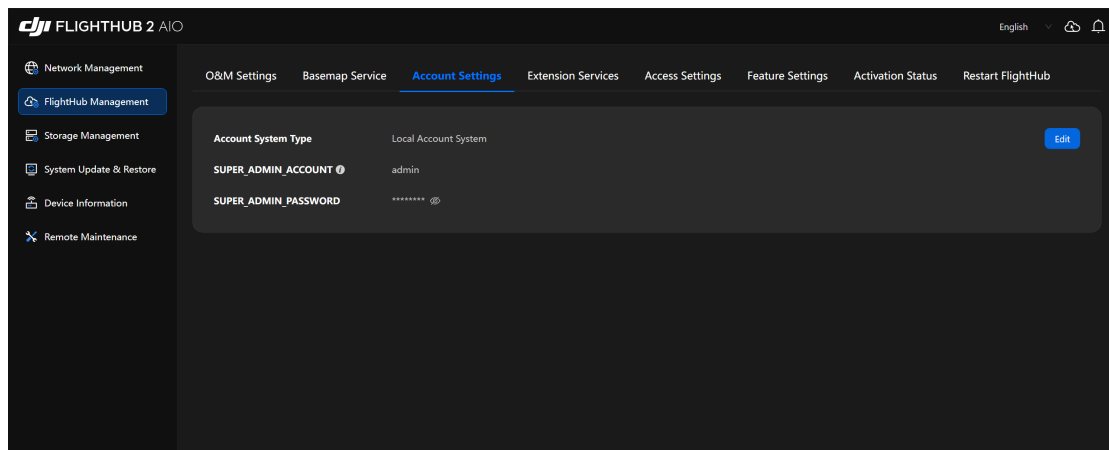
Overview

This module allows you to configure the authentication methods for accessing your FlightHub 2 AIO, supporting either a local account system or integration with a third-party service.

Steps

1. Accessing the Account Settings

Navigate to FlightHub Management > Account Settings.



2. Local Account System

2.1 View Current Status

Displays the SUPER_ADMIN_ACCOUNT (super administrator username) and SUPER_ADMIN_PASSWORD (password, hidden by default).

2.2 Edit Local Account Parameters

2.2.1 Enter Edit Mode;

Click Edit in the upper right corner to enter configuration mode.

2.2.2 Modify Account/Password

Item	Operations and Rules
Account System Type	Keep Local Account System selected.
SUPER_ADMIN_ACCOUNT	You can change the SUPER_ADMIN_ACCOUNT (recommended to use a complex, non-obvious name).
SUPER_ADMIN_PASSWORD	The password should be complex and at least 8 characters long, containing uppercase letters, lowercase letters, and numbers. Note: This SUPER_ADMIN_ACCOUNT has the highest level of privilege. Remember your new password, as

	it controls access to the device.
--	-----------------------------------

2.2.3 Save Changes

Click Save. The new credentials will take effect immediately.

3. Third-party Account System

3.1 Switch to Third-party System

Click the Third-party Account System tab.

Note: This hides the local account configuration.

3.2 Configure Third-party Authentication Parameters

Fill in the required fields with parameters provided by your third-party authentication platform.

Item	Rules and Descriptions
CLIENT_ID	Client ID assigned by the third-party platform (e.g., LvHms6F60). Make sure it matches the platform backend.
CLIENT_SECRET	Client Secret (e.g., zdCETKc4w22RFOvDwlIF58llxpCN4mgl). Keep strictly confidential.
AUTH_URL	Third-party authentication authorization URL (e.g., http://ry.sxldj.com/api/oauth2/authorize). Must be accessible.
TOKEN_URL	Token acquisition address (e.g., http://ry.sxldj.com/api/oauth2/token). Used to exchange access tokens.
USER_URL	User information query URL (e.g., http://ry.sxldj.com/api/userinfo). Used to obtain logged-in user details.
USER_ID_KEY	Key name for the user ID in the returned data. This should match the third-party platform's response format.
USER_ACCOUNT_KEY	Key name for user account in the returned data. This should match the third-party platform's response format.
USE_REDIRECT_URL	Enter the URL where the user will be redirected after authorization. This URI must exactly match the AUTH_URL configured in your application.
SUPER_ACCOUNT	Super admin account for the third-party system, necessary for executing high-privilege actions.

3.3 Save Configurations

After filling all parameters, click Save. The system will attempt to verify the accessibility of the URLs. If invalid, saving will fail.

3.4 Revert to Local System

To switch back, click the Local Account System tab.

Note: Any previously configured third-party parameters will be cleared. You need to reconfigure the local super administrator account.

Notes

- **Permission Risk:** Modifying the account system significantly impacts device login permissions. Always test changes thoroughly in a non-production environment first.

- **Third-Party Parameter Dependency:** The third-party configuration must precisely match your external authentication platform's settings (e.g., CLIENT_ID mismatch or inaccessible URLs will cause login failures).
- **Password Management:** Regularly change local/third-party administrator passwords. Securely store third-party keys.
- **Switching and Rollback:** If switching from a third-party system back to the local system, and the local account was not backed up, you may need to re-register the admin account as the device might not retain the original local account data.

2.4 Extension Services

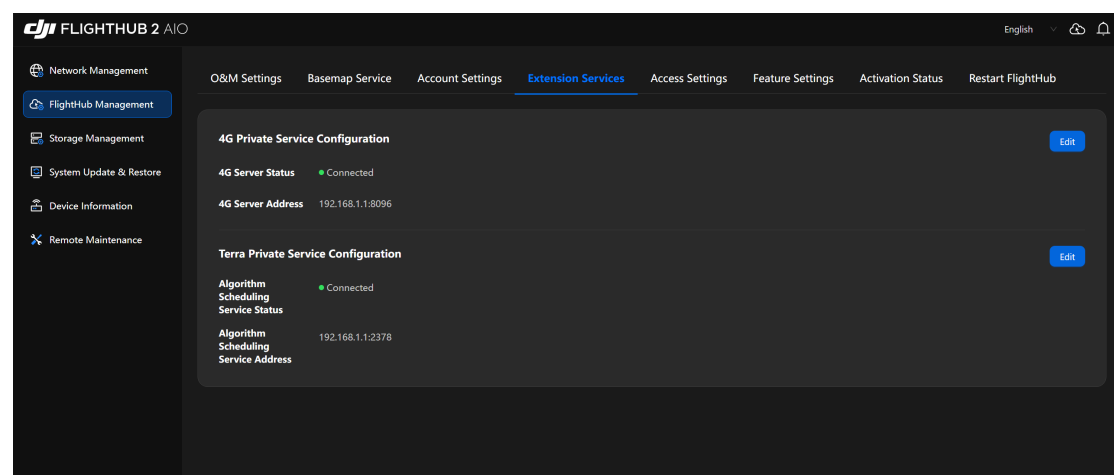
Overview

The section allows you to configure connections to specialized services like a private 4G network or DJI Terra for advanced capabilities.

Steps

1. Accessing the Extension Services

Navigate to FlightHub Management > Extension Services.



2. 4G Private Service

2.1 View Current Status

- **4G Server Status:** Connected (Green), Connection failed, Not connected.
- **4G Server Address:** The network address used to connect to the 4G server. The default is the local address. (Example: devops.fhaio.local)

2.2 Edit 4G Service Parameters

2.2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

2.2.2 Modify Server Address

Enter a new address for your 4G private service. To revert to the AIO's built-in service, click Restore to Local Address to automatically populate the default devops.fhaio.local.

2.2.3 Save and Verify Link

Click Save. The status indicator will turn green if the connection is successful or red if

it fails.

- Connection Successful: The 4G server status remains green and connected.
- Connection Failed: The status indicator will turn red, indicating a failed connection. Verify network accessibility, including network routing and whether the server is powered on.

3. Terra Private Service Configurations

3.1 View Current Status

- Algorithm Scheduling Service Status: Connected (Green), Connection failed.
- Algorithm Scheduling Service Address: The network address used to connect to the algorithm scheduling service. The default is the local address.

3.2 Edit Terra Service Parameters

3.2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

3.2.2 Modify Scheduling Address

Enter a new address for your algorithm scheduling service. To revert to the AIO's built-in service, click Restore to Local Address.

3.2.3 Save and Verify Link

Click Save. The status indicator will turn green if the connection is successful or red if it fails.

- Connection Successful: The algorithm scheduling service status remains green and connected.
- Connection Failed: The status indicator will turn red, indicating a failed connection. Verify network accessibility, including network routing and whether the server is powered on.

Notes

- Address Validity:
 - The 4G or Terra service address must be consistent with the actually deployed server IP or domain name, and the device network must be accessible. It is recommended to first test connectivity using ping or telnet tools.
 - If using a custom domain name, make sure the intranet DNS has been resolved or the hosts file has been configured for mapping.
- Status Monitoring:
 - The service status indicates whether related features like 4G network scheduling and Terra algorithm operation are available. A green (Connected) status means these features can be used normally.
 - If the status is red (Error), check the address spelling and the server's status, ensuring the process is running and the port is not occupied.
- Restore Defaults: If connection fails after changing the address, click Restore to Local Address to revert. This helps quickly diagnose address configuration issues.

2.5 Access Settings

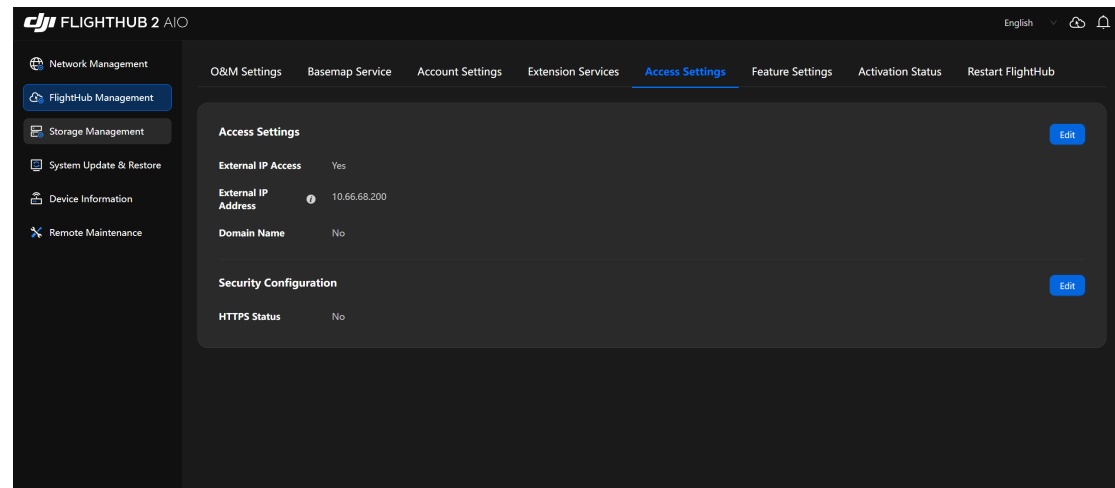
Overview

This section is used to configure the device's network access rules (external IP, domain name) and security authentication (HTTPS, license). Operations must strictly follow the process to ensure access security.

Steps

1. Accessing the Access Settings

Navigate to FlightHub Management > Access Settings.



2. Access Configurations

2.1 View Current Status

- External IP Access: A toggle switch to enable or disable external IP access. The switch is blue when enabled.
- External IP Address: Displays the configured external IP address (e.g., devops.fhaio.local). This address must align with your network topology.
- Domain Name: A toggle switch to enable or disable domain name resolution. The switch is blue when enabled.
- Custom Domain Name: Allows you to specify a custom domain name (e.g., devops.fhaio.local). This domain must be configured to resolve to the device's IP address.

2.2 Edit Access Parameters

2.2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

2.2.2 Adjust Access Rules

Item	Operations and Rules
External IP Access	● Enabled: Allows external networks to access the device via its IP. ● Disabled: Restricts access to only the internal network (enhanced security).

External IP Address	When enabled, enter a valid IP address or domain name. Ensure your network is routable (firewall/router ports are open).
Domain Name	• Enabled: Allows access via a custom domain name. • Disabled: Only allows access via IP (requires disabling domain name resolution simultaneously).
Custom Domain Name	When enabled, enter the resolved domain name (e.g., custom.devops.com). Must be consistent with your DNS configuration.

2.2.3 Save Changes

Click Save. New rules take effect immediately.

- If external IP/domain is enabled, verify connectivity (e.g., via ping).
- If disabled, the device will only respond to internal IP requests, and client access methods may need adjustment.

3. Security Configurations

3.1 View Current Status

- HTTPS Status: A toggle switch to enable or disable HTTPS. The switch is blue when enabled.
- Certificate Import: Indicates if a custom license has been imported. Prior upload is required.
- Server Certificate (crt): Displays the path to the server's SSL/TLS certificate file (e.g., devops.fhaio.local).
- Key File (key): Displays the path to the corresponding private key file (e.g., devops.fhaio.local).

3.2 Edit Security Parameters

3.2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

3.2.2 Adjust Access Rules

Item	Operations and Rules
HTTPS Status	• On: Forces HTTPS access (encrypted transmission, requires a valid certificate). • Off: Downgrades to HTTP (not recommended due to plaintext risk).
Certificate Import	Select from dropdown: • Custom certificate (requires uploading .crt and .key files) • Self-signed certificate (default, lower security, for testing only).
Server Certificate (crt)	When selecting a custom license, upload the .crt file path (e.g., devops.fhaio.local).
Key File (key)	When selecting a custom certificate, specify the .key file path.

3.2.3 Save and Verify HTTPS

Click Save. The system verifies certificate validity.

- Valid Certificate: HTTPS access is normal (browser shows lock icon).
- Invalid Certificate: HTTPS connection fails. Re-upload a correct certificate.

Notes

- Network Dependencies: Before enabling external IP/domain, ensure your network egress (firewall, router) has opened corresponding ports (e.g., 80, 443).
- License Security:
 - Custom certificates should be issued by a trusted CA to avoid browser warnings.
 - Self-signed certificates are for testing only; production environments require compliant ones.
- Access Rollback: If you cannot access the device after making changes, you can log in via a direct local connection to the device's management port to readjust access configurations.

2.6 Feature Settings

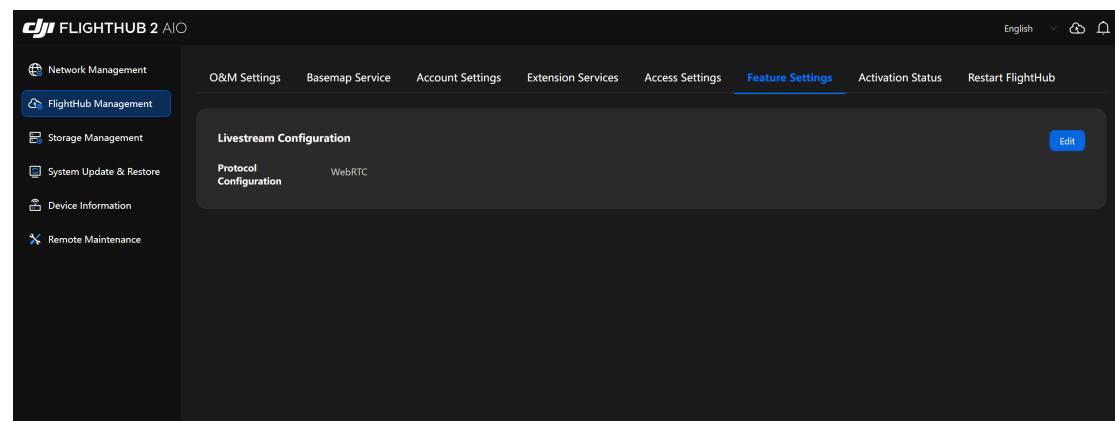
Overview

The section is used to configure livestream feature protocols, supporting switching between WebRTC/RTMP protocols to adapt to different livestream scenarios.

Steps

1. Accessing the Feature Settings

Navigate to FlightHub Management > Feature Settings.



2. Livestream Protocol Configurations

2.1 View Current Protocol

Displays the currently active livestream protocol (default is WebRTC).

2.2 Switch Livestream Protocol

2.2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

2.2.2 Select Protocol Type

Protocol	Applicable Scenarios and Rules
----------	--------------------------------

WebRTC	Highly real-time (low latency), ideal for interactive livestreaming and low-latency scenarios. Natively supported by modern browsers, no extra plugins needed.
RTMP	Good compatibility, adapts to traditional streaming media servers. Suitable for pushing streams to CDNs and livestreaming platforms.

2.2.3 Save Protocol Settings

Click Save. The new protocol takes effect immediately.

- If switching to RTMP, ensure your streaming media server is configured (e.g., port 1935 enabled).
- If retaining WebRTC, ensure your network supports UDP transmission (some intranet environments may restrict UDP, causing stuttering).

Notes

- Protocol Compatibility:
 - WebRTC relies on browser/client support and open UDP ports.
 - RTMP requires a streaming media server.
- Livestream Latency:
 - WebRTC offers less than 1 second latency suitable for real-time control feedback.
 - RTMP has higher latency (approx. 3-10 seconds), suitable for broader broadcasting.
- Network Dependencies:
 - After switching, test the livestream feature.
 - Troubleshoot stuttering/disconnection by checking network bandwidth (RTMP has higher requirements) or firewall blockage (WebRTC relies on UDP).

2.7 Activation Status

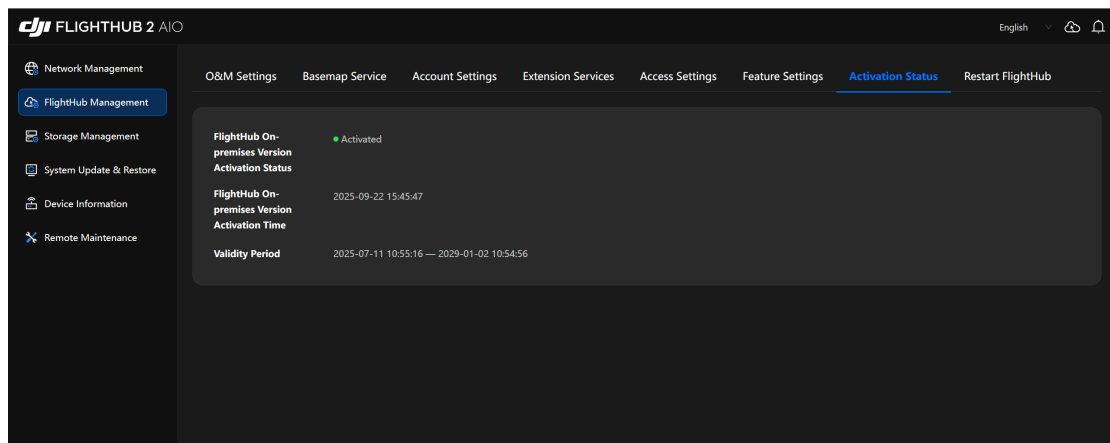
Overview

This section is used for viewing and managing the device's private activation status. Its core features are activating devices and querying validity periods, ensuring normal system usage permissions.

Steps

1. Accessing the Activation Status Page

Navigate to FlightHub Management > Activation Status.



2. View Activation Information

2.1 Activated Status

- FlightHub On-premises Version Activation Status: Displays Activated (green indicator).
- FlightHub On-premises Version Activation Time: Shows the specific activation date and time.
- Validity Period: Displays the valid period of the update service.

2.2 Not Activated status

- FlightHub On-premises Version Activation Status: Displays Not activated (red indicator) and an Activate link.
- FlightHub On-premises Version Activation Time: A default time is shown, which will update upon activation.
- Validity Period: Displays the valid period of the update service.

3. Activate Devices

Click the Activate link to navigate to the activation page. Refer to DJI FlightHub 2 User Manual for details.

Note

Validity Period Management: Regularly check the update validity period. Contact DJI Support to renew your license before it expires to avoid service interruption.

2.8 Restart FlightHub

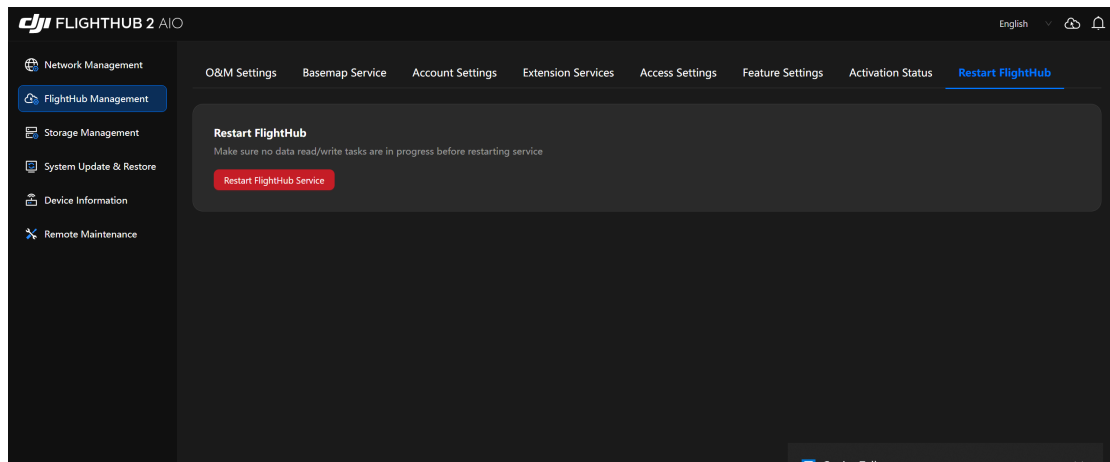
Overview

This module allows you to restart the FlightHub 2 services to resolve system errors, apply configurations, or for other maintenance scenarios.

Steps

1. Accessing the Restart FlightHub Interface

Navigate to FlightHub Management > Restart FlightHub.



2. Initiate the Restart Process

2.1 Confirm Task Status

The interface will prompt: "Make sure no data read/write tasks are in progress before restarting service". You must manually pause or end all data uploads, map tile downloads, and other tasks.

2.2 Verify Administrator Password

Click the Restart FlightHub Service button. A pop-up window will require you to enter the administrator password for three times.

3. Checking Restart Status

3.1 Restart Successful

- The progress bar will disappear. The button will momentarily be grayed out, then turn red and clickable again.
- A top prompt: "FlightHub service restarted successfully" will appear and disappear.

3.2 Restart Failed

- The progress bar may get stuck or disappear, displaying an error message: "FlightHub service failed to restart after multiple attempts". Contact your local dealer or DJI Support.

Notes

- Data Protection: Prioritize pausing all data read/write tasks before restarting to prevent data loss.
- Password Consistency: All three password entries must be identical. An inconsistency will trigger a validation failure, requiring you to restart the verification process.

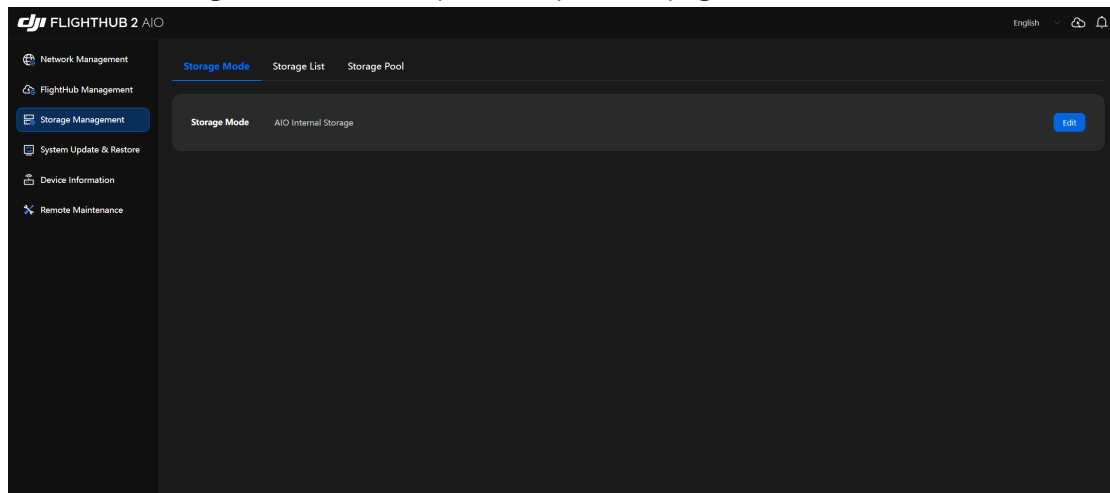
3 Storage Management

Overview

This module allows you to configure your FlightHub 2 AIO's internal or external storage type, set up external storage protocols (NFS, SMB, iSCSI), and monitor the health of your internal disks and RAID arrays. Proper storage configuration is crucial

for data integrity and system performance.

Enter the Storage Management interface: Left navigation bar> Storage Management> select the "Storage Mode" tab to open the operation page.



Storage Mode Configurations

1 View Current Storage Type

- Storage Mode: AIO internal storage, external storage
- Storage Type: Internal storage, external storage

2 Switch Storage Type

2.1 Enter Edit Mode

Click the Edit button in the upper right corner.

2.2 Select Storage Type

Type	Applicable Scenarios and Rules
Internal Storage	Uses the AIO's built-in hard drives. This is the default, plug-and-play option, suitable for smaller data sets and offline operations. No additional configuration is required beyond this step.
External Storage	Allows you to mount network-attached storage (NAS) using NFS/SMB, or an IP SAN using iSCSI. This is suitable for large-scale data and multi-device sharing.

2.3 Save and Verify

- If selecting Internal Storage: Click Save. The system will immediately switch to internal storage.
- If selecting External Storage: Click Save. A pop-up warning will appear, recommending data backup. After reviewing the warning, click Switch. The system will then guide you through the external storage protocol configuration process.

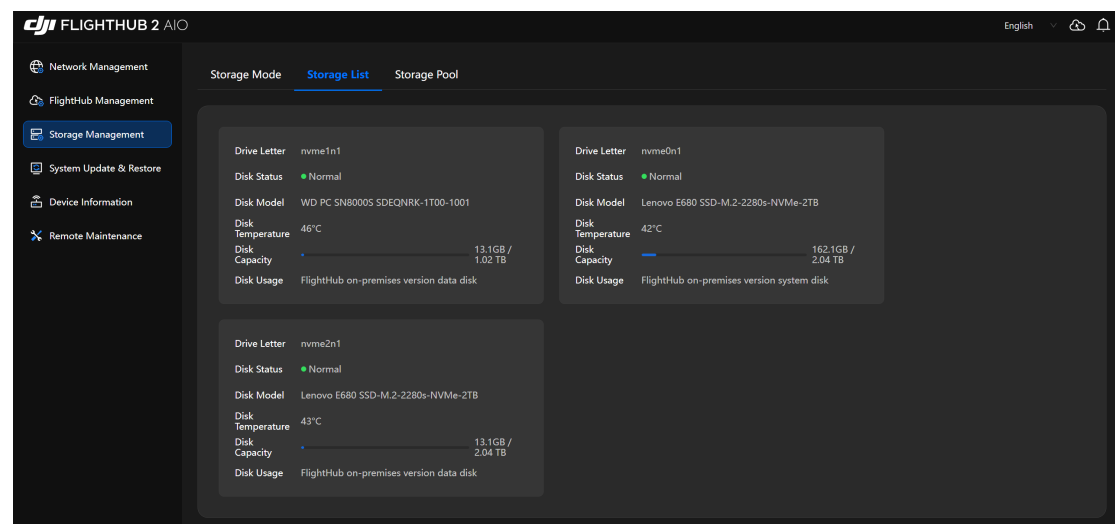
3.1 Internal Storage

Internal Storage List

This section provides detailed information and health status for each physical disk installed in your AIO. The following are the specific operating steps and instructions.

1. Accessing the Internal Storage List

Navigate to Storage Management > Internal Storage. Under the sub-options of Storage Management, select the Internal Storage List tab to enter the operation page.



2. View Storage Disk Information

Each disk is displayed as a card, showing:

- Disk Basic Information
 - Disk Name: System identifier (e.g., nvme0n1).
 - Drive Letter: Corresponding drive identifier.
 - Disk Model: Specific model (e.g., ST4000VN008).
- Disk Status Information
 - Disk Status: Green for normal, and red for error. Hover to see error details.
 - Disk Temperature: Current temperature in Celsius. If outside 0°C to 55°C, the value is highlighted in red, with a warning message.
- Disk Capacity Information
 - Disk Capacity: Shows Used Capacity/Total Capacity (e.g., 3.6TB/4TB).
 - Disk Usage: Describes the disk's usage.

3. Troubleshooting

Symptom	Solution
Disk Status Error: Potential physical damage or malfunction.	Immediately back up important data on this disk. Contact a professional technician for inspection, and replace the disk if necessary to prevent data loss.

Disk Temperature Error: Overheating can damage the disk and lead to data loss. Low temperatures can affect startup.	Check the device's cooling system, ensure proper ventilation, clean internal dust, and verify cooling fan operation. For low temperatures, ensure the disk is within operating range before use.
Insufficient Disk Capacity: Remaining disk space is low (typically below 10%).	Clean up unnecessary files (temp files, cache) or migrate data to other storage devices to ensure normal system operation.

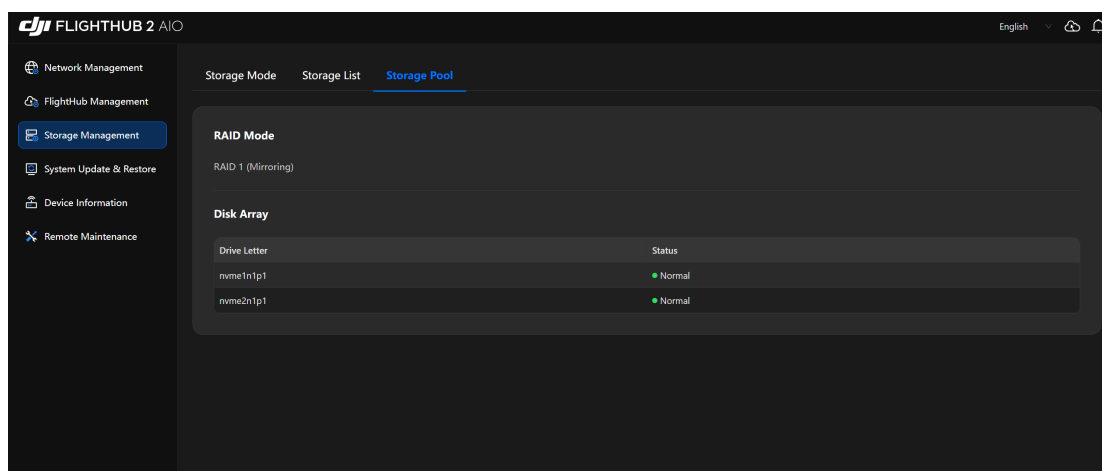
Through the above operational guide, you can effectively keep track of the internal storage disk status of your DJI FlightHub 2 AIO, promptly identify and address potential issues, and ensure the stability and security of device data storage.

Internal Storage Pool Information

This section allows you to manage RAID (Redundant Array of Independent Disks) configuration and status, handle disk failures, and reconstruct or create new storage pools.

1. Accessing the Storage Pool Information

Navigate to Storage Management > Storage Pool.



2. Statuses and Operations

Status 1: All Normal (RAID 1 Healthy)	- Interface Features: - RAID Mode: RAID 1 (Mirroring) - Disk Array: All disks show green (normal). - Operation: Regular inspection (weekly/monthly). No additional operation required.
Status 2: Single or Dual Disk Error (Disk Failure)	- Interface Features: A disk shows red (error). A Remove Faulty Disk button appears. - Operation Process: - Step 1: Remove Faulty Drive

	● Click Remove Faulty Drive to open the faulty drive removal guide ● Follow the guide (record steps with your phone): Power off AIO > Open chassis cover > Disassemble cooling fan/heatsink > Replace faulty hard drive > Reassemble chassis cover and power on AIO Step 2: Add a New Disk (RAID Rebuild) ● After powering on, return to the Storage Pool Information interface. ● Click Add Disk. A pop-up will appear, and after confirming, enter your administrator password for three times. ● The system will begin rebuild. FlightHub service is suspended during rebuild. Step 3: Verify Rebuild Results ● Upon completion, RAID mode restores to RAID 1, all disks are normal, and the storage pool is available. ● RAID mode restores to RAID 1 (Mirroring) ● All disks in the disk array are in normal status, and the storage pool becomes available again.
Status 3: No RAID Status (Not Configured/Array Failed)	● Interface Features: ● RAID Mode: No RAID ● No disk data available. A Create Storage Pool button appears. ● Operation Process: Step 1: Create Storage Pool (RAID 1) ● Click Create Storage Pool. A pop-up will warn that disks will be formatted and added to RAID 1. ● After confirming, enter your administrator password for three times. Step 2: Monitor Storage Pool Rebuild Step 3: Verify Creation Result ● Upon completion, RAID Mode displays RAID 1, all disks are normal, and the storage pool is available. ● RAID Mode displays RAID 1 (Mirroring) ● All disks in the disk array have a normal status, and the storage pool is available.
Status 4: User-defined RAID Status (Custom Configuration)	● Interface Features: ● RAID Mode: RAID X (where X is a user-defined level, e.g., RAID 5/10) ● Disk Array: All disks show green (normal). ● Operation: Only status monitoring. No additional operations are available through this interface (Custom RAID is configured via command line/hardware.)

Status 5: External Storage Status (Mounting NAS/iSCSI)	- Interface Features: - RAID Mode: External storage mounted. - No internal disk information displayed. - Operation: Manage external storage mounts via the Storage Mode tab.
--	---

Notes

- Data Backup: Before replacing disks or reconstructing RAID, always back up critical data to avoid permanent data loss due to formatting.
- Hardware Operations: Replacing hard drives requires strict power-off procedures. Failure to follow them can damage the device or lead to data loss.
- Password Verification: The three password entries must be identical for RAID reconstruction or creation to proceed.

3.2 External Storage

External Storage Protocol Configuration

1. Select Protocol Type

If you selected External Storage, you must configure the protocol that matches your external storage device.

- NFS (Network File System)
 - Applicable to: Linux/Unix-based servers (e.g., FreeNAS, OpenMediaVault).
 - Configuration: Select NFS protocol version (NFSv3/NFSv4), enter server IP (storage server address), and target storage path (server shared directory).
- SMB (Server Message Block)
 - Applicable to: Windows servers or most NAS devices (e.g., Synology, QNAP).
 - Configuration: Select SMB protocol version (SMBv2/SMBv3), enter server IP (storage server address), target storage path (Windows shared directory), and optional username and password (if required by the server).
- iSCSI (IP Storage)
 - Applicable to: IP SAN storage solutions (e.g., Dell EqualLogic, Huawei OceanStor) for high-performance block-level storage.
 - Configuration: Enter target IP, IQN (unique identifier for the target, usually scanned), select security authentication (unidirectional CHAP/No authentication), and choose LUN device selection (logical volumes on the storage server).

Note: Do not switch between NFS and SMB protocols on the same data directory. These protocols use different permission systems and metadata formats. Directly switching can lead to:

- Permission Loss: SMB cannot interpret NFS's UID/GID mapping, potentially

leading to incorrect file permissions.

- Metadata Conflict: Inconsistent timestamp synchronization between protocols.
- Service Error: FlightHub services may fail to read data due to insufficient permissions.

2. Test Connection and Mount

2.1 Test Connection

Click Test Connection.

- Success: A "Connection successful" message appears.
- Failure: A "Connection failed" message appears.
 - Check protocol versions, network reachability (ping server IP), and permissions.
 - Whether the network is reachable (test by pinging the server IP);
 - Whether permissions are correct (SMB username/password, NFS share permissions).

2.2 Mount Now

After a successful connection test, click Mount Now. You will be prompted to enter your administrator password three times.

- Verification Successful: The system will mount the external storage. The Storage Mode will display External Storage, and data can be read/written.
- Verification Failed: Password mismatch will be prompted. You will need to re-initiate the process.

Notes:

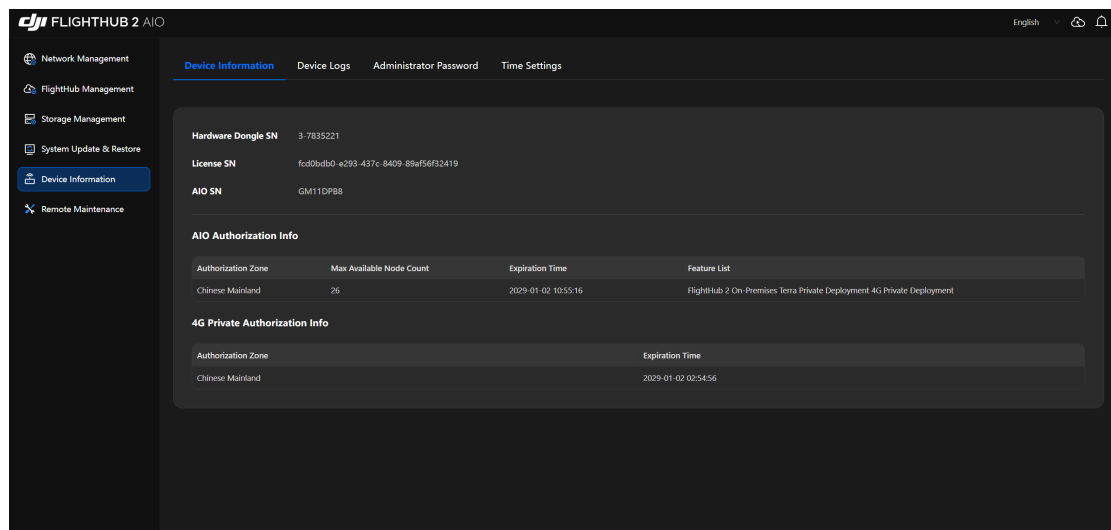
- Data Backup: Before switching to external storage, make sure to back up internal storage data. Otherwise, the original data will be inaccessible after the switch.
- Protocol Compatibility: NFS/SMB/iSCSI must exactly match the storage server's protocol version, permissions, and address. Otherwise, the mount will fail.
- Storage Performance: External storage must meet bandwidth requirements. Otherwise, data read/write will be slow.
- Storage Speed: Read and write speeds should be above 150 MB/s. SSDs are highly recommended for optimal performance.
- Storage Space: Plan capacity based on your usage. For reference, one image is approx. 10-15 MB, and one minute of original video is about 1 GB.
- Network Speed: A 1000 Mb/s (1 GbE) network is standard. Be aware that if read/write operations share a single network port, bottlenecks may occur. Consider upgrading to a higher-specification network card if needed.

4 Device Information

This section allows you to view critical hardware and authorization details, manage system logs, update the administrator password, synchronize system time, and configure remote maintenance settings. These functions are vital for maintaining device compliance, security, and operational integrity.

Navigate to Device Information. This tab displays essential hardware and licensing

details for your FlightHub 2 AIO.



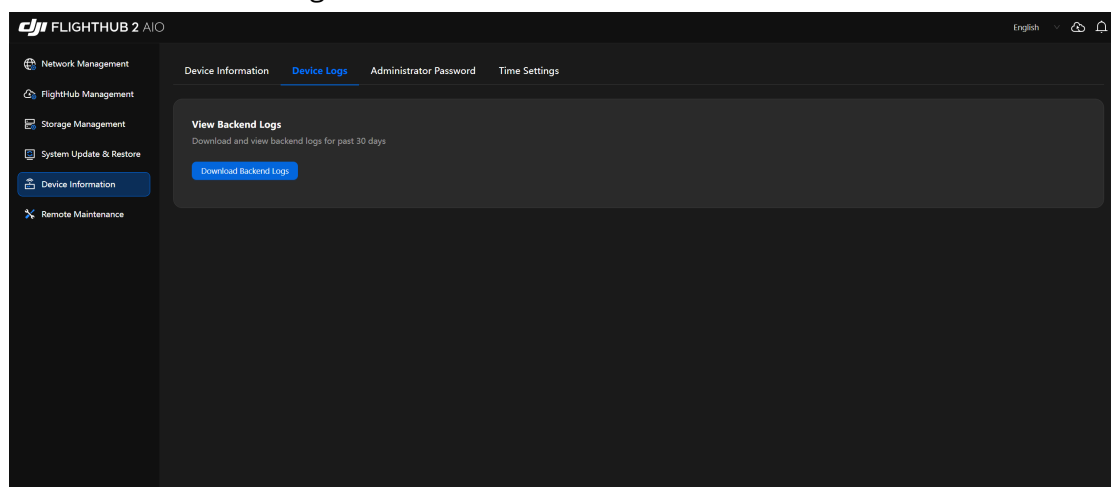
4.1 Device Information

- Hardware Information: Includes the hardware dongle serial number (SN) and the AIO's unique SN.
- AIO SN (DJI Support/management unique code);
- Authorization Details: Shows online device limit, certificate expiration time, and available features (e.g., Terra private deployment).

Note: This section is for viewing only; no direct modifications are possible. It is recommended to regularly check the authorization expiration time to ensure continuous service.

4.2 Device Logs

Switch to the Device Logs tab.

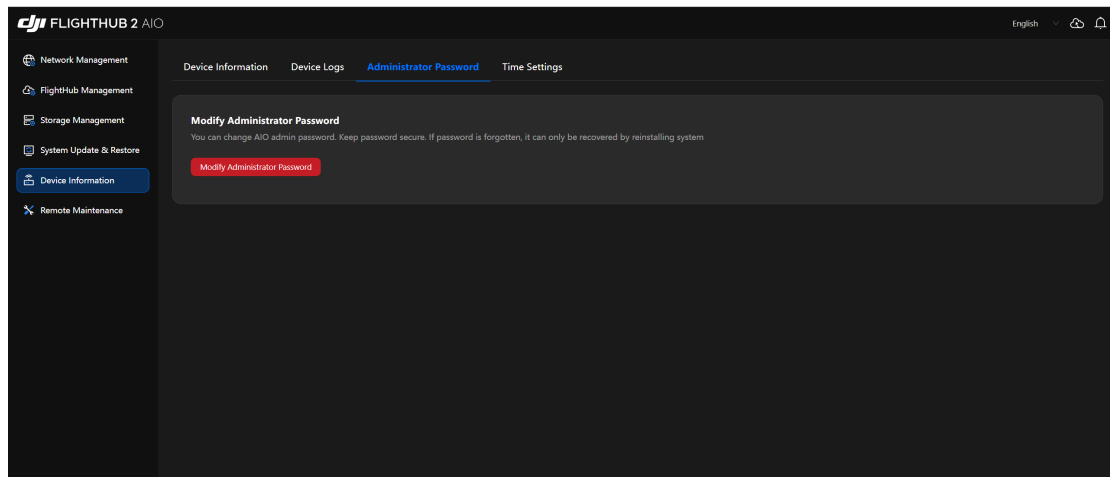


- Click Download Backend Logs to retrieve system operation records from the past 30 days. These logs include error reports and configuration changes.

- Purpose: If you encounter a device error (e.g., feature malfunction, data loss), these logs are crucial for DJI technical support to diagnose and resolve issues.

4.3 Administrator Password

Switch to the Administrator Password tab:



Password Modification Process

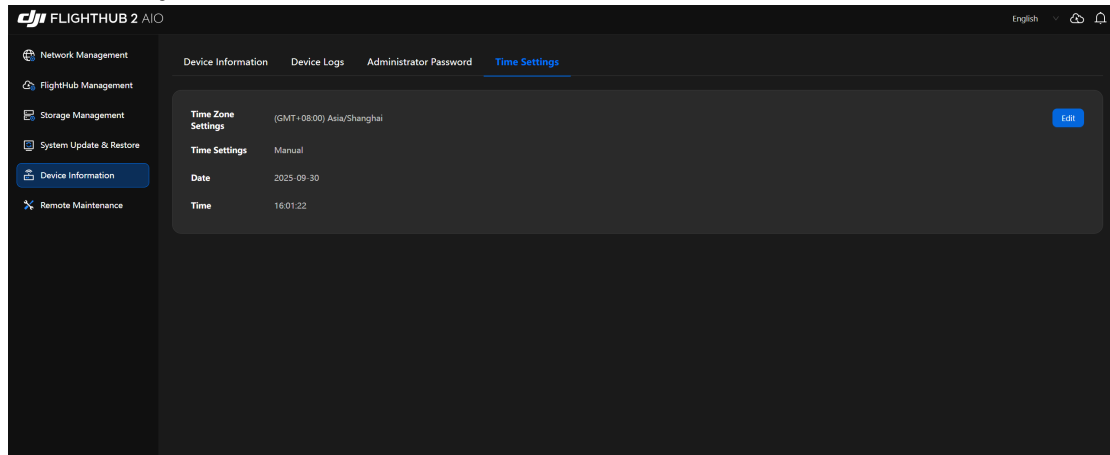
1. Click Modify Administrator Password. A pop-up window will appear.
2. Enter your Original password (current administrator password).
3. Enter your New password. The new password must be at least 12 characters long and include a combination of uppercase letters, lowercase letters, numbers, and special characters (e.g., Admin@2025).
4. Confirm the new password by re-entering it.
5. Click OK. The new password will take effect immediately upon successful verification. An error message will appear if the passwords do not match or complexity requirements are not met.

Notes

- Password Loss: If you forget your administrator password, you will need to reset the system. Refer to the system recovery guide for instructions, and remember to back up all data before proceeding.
- Regular Changes: For enhanced security, it is highly recommended to change your administrator password regularly (e.g., quarterly or semi-annually).

4.4 Time Settings

Switch to the Time Settings tab, which supports manual time adjustment or NTP automatic synchronization.



Manually Set Time

1. Click Edit. Select your desired time zone.
2. Set Time Settings to Manual. Enter the correct date and time.
3. Click Update Now. The system time will be immediately overwritten with your manual input.

NTP Automatic Synchronization

1. Set Time settings to Sync with NTP Server.
2. Enter the server address (default pool.ntp.org or your enterprise's intranet NTP address).
3. Enter the server port (default 8080, ensure it matches your NTP server's port).
4. Click Update Now. The system will attempt to connect to the NTP server.
 - Success: A green pop-up "Time updated successfully" will appear.
 - Failure: A red pop-up "Time update failed" will appear. Check your network connection and the NTP server address/port.

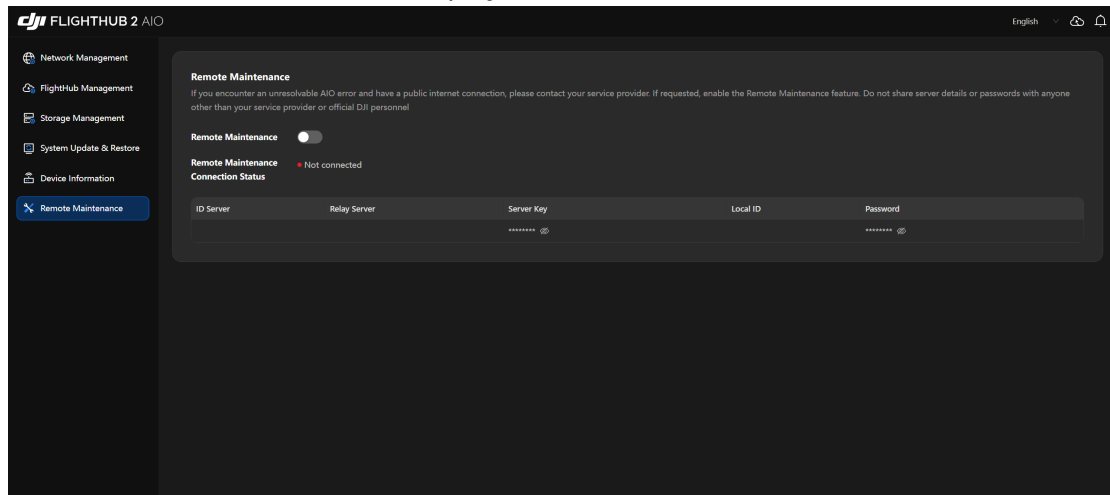
5 Device Information

5.1 Overview

The remote maintenance module allows DJI Support to remotely access your AIO for troubleshooting and issue resolution.

5.2 Navigate to Remote Maintenance

Navigate to Remote Maintenance, which includes the remote maintenance switch, server information, and status display.



5.3 Core Feature Operations

1.1 Remote O&M Switch

- Click the Remote Maintenance button.
 - Blue indicates enabled: The AIO will display connection information (server IP, password) for DJI Support to establish a remote connection.
 - Gray indicates disabled: Server information is hidden, and the remote connection channel is closed.
- Note: AIOs must be connected to a public network to receive remote maintenance.

1.2 Server Information

This section becomes visible only when the remote maintenance is enabled. It provides the necessary credentials for DJI technical support.

- Content Displayed:
 - Server IP (e.g., 24.202.45.26);
 - Server password (masked by default; click the eye icon to view/hide).
 - Case ID, local password (credentials for technical support to verify the device).
- Operations:
 - Provide the server IP, password, and Case ID to DJI technical support. Always re-confirm the identity of the support agent via a trusted channel (e.g., phone call or official email) before sharing this sensitive information.
 - Security Caution: Do not disclose the password unless absolutely necessary. After the troubleshooting session, immediately disable the remote maintenance switch to secure your device.

1.3 Status Display

The bottom of the page displays the remote maintenance connection status:

- Not Connected (Gray): The remote channel is not established (normal standby state).
- Connecting (Blue): DJI technical support is actively attempting to establish a connection.
- Connected (Green): A remote session is established.

5.4 Notes

- Exercise extreme care if operating the device yourself during a connected session, as technical support may also be interacting with the system.
- Confidentiality: The server password and case ID are strictly for DJI technical support. Never disclose them to unauthorized individuals.
- Operation Traceability: During a remote connection, it's recommended to screenshot or record any important configuration changes (e.g., modifications to storage mode) for future reference and fault tracing.