DJI FlightHub 2 AIO

Instrukcja obsługi

v1.0

Spis treści

Korzystanie z niniejszej instrukcji

Przeczytaj przed użyciem

Przegląd produktu

FlightHub 2 AIO to potężne, kompleksowe rozwiązanie do wdrażania usług DJI FlightHub w prywatnej sieci lokalnej. Dzięki kilku prostym krokom konfiguracyjnym można zintegrować w pełni funkcjonalną platformę FlightHub z własnym przepływem pracy, zapewniając bezpieczeństwo wszystkich danych dotyczących zadań w swoim środowisku.

AIO obsługuje połączenie z aplikacją DJI Pilot 2, umożliwiając zarządzanie i koordynowanie zadań dla maksymalnie 20 dronów i stacji dokujących.

Specyfikacja produktu

CPU	Procesor Core Ultra 7 265
Pamięć	64 GB × 1
Dedykowana karta graficzna	NVIDIA RTX 2000 Ada
Pamięć SSD 1	2 TB (dysk systemowy)
Pamięć SSD 2	2 TB (dysk danych A)
Pamięć SSD 3	2 TB (dysk danych B)
Sieć bezprzewodowa	802.11be 2×2
Sieć przewodowa	Karta sieciowa PCIe 1 Gb/s × 4
System operacyjny	Ubuntu 24.04.2 LTS Desktop

Wstępna konfiguracja

Urządzenie FlightHub 2 AIO jest gotowe do natychmiastowego użycia. Jest fabrycznie skonfigurowane z niezbędnym systemem operacyjnym, sterownikami i oprogramowaniem aplikacyjnym. Aby rozpocząć pracę, wykonaj poniższe czynności.

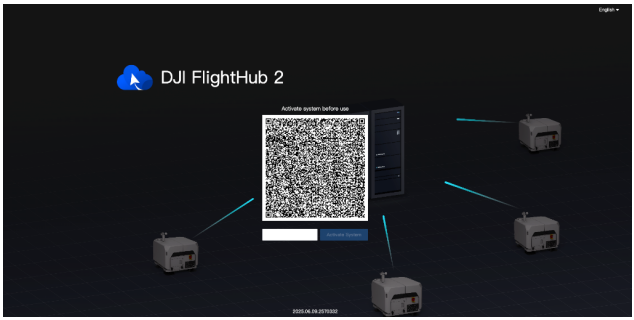
1 Autoryzacja

Przed włączeniem urządzenia AIO należy podłączyć autoryzowany klucz sprzętowy AIO do dowolnego wolnego portu USB. Włącz urządzenie AIO. System automatycznie wykryje licencję i załaduje niezbędne usługi.
Klucz sprzętowy AIO musi pozostawać podłączony do urządzenia AIO przez cały czas jego działania. Wyjęcie klucza spowoduje natychmiastową dezaktywację usług i przerwanie pracy.

2 Pierwsza aktywacja

Po pierwszym rozpakowaniu urządzenia AIO i wejściu na stronę http://fhaio.net lub 192.168.1.1:30888 na komputerze, zostaniesz automatycznie przekierowany do kreatora konfiguracji. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby zakończyć wstępną konfigurację. Proces ten zajmie kilka minut i pomoże Ci lepiej zrozumieć, jak korzystać z urządzenia AIO. Po zakończeniu konfiguracji możesz przejść do strony FlightHub.

Przy pierwszym dostępie lub podczas późniejszej aktualizacji usług i autoryzacji FlightHub wymaga od użytkowników wykonania operacji aktywacji usługi. Konkretna metoda aktywacji jest następująca:



1. Użyj przeglądarki mobilnej, aby uzyskać dostęp do usługi zdalnej aktywacji i wprowadź dane konta zarejestrowanego pod prawdziwym imieniem i nazwiskiem na stronie internetowej DJI Developer.
2. Po przesłaniu danych konta i przejściu procesu weryfikacji tożsamości w usłudze aktywacji na stronie aktywacji wyświetli się kod QR. Zeskanuj kod QR, aby uzyskać dynamiczny kod aktywacyjny (ważny przez 1 minutę).

3. Wprowadź ten kod na stronie aktywacyjnej. Po zakończeniu aktywacji zostaniesz przekierowany na stronę logowania FlightHub 2.
4. Następnie możesz rozpocząć korzystanie z usług FlightHub.

3 Połączenie stacji dokującej z organizacją

Utwórz organizację

1. Otwórz przeglądarkę internetową (zalecana jest przeglądarka Google Chrome 120 lub nowsza).
2. Wprowadź adres URL: http://${SERVICE_DOMAIN}:${FRONTEND_TCP_PORT}. Domyślny system: Http://192.168.1.1
3. Zaloguj się przy użyciu domyślnych danych uwierzytelniających:

- Nazwa użytkownika: admin
- Hasło: Password@

4. Postępuj zgodnie z instrukcjami, aby utworzyć organizację. AIO obsługuje jedną organizację, więc wprowadź swoje dane ostrożnie.
5. W ramach swojej organizacji utwórz projekt, aby zarządzać zadaniami i urządzeniami.

Uzyskaj kod powiązania urządzenia.

Przejdź do sekcji Urządzenia > Stacja dokująca > Powiązanie urządzeń, aby uzyskać kod powiązania urządzenia i identyfikator organizacji.

Konfiguracja usługi w chmurze

Podłącz pilota zdalnego sterowania do stacji dokującej za pomocą kabla USB-A do USB-C, otwórz aplikację DJI Pilot 2, przejdź do ustawień usługi chmurowej stacji dokującej, wybierz FlightHub 2 On-Premises Version i wprowadź następujące dane:

6. Adres dostępu: ${SERVICE_DOMAIN}:${BACKEND_TCP_PORT}.
Domyślny system: 192.168.1.1:30812

- Identyfikator organizacji: Wprowadź identyfikator organizacji uzyskany w poprzednim kroku.
- Kod powiązania urządzenia: Wprowadź kod powiązania organizacji uzyskany w poprzednim kroku.
- Nazwa stacji dokującej: Wprowadź nazwę stacji dokującej.

Powiązanie urządzenia z organizacją

W sekcji Projekt wybierz projekt, aby powiązać urządzenie z organizacją.

4 Przypisanie drona do organizacji

1. Naciśnij ikonę Ustawienia w lewym górnym rogu strony głównej i zaloguj się na swoje konto DJI.

2. Naciśnij Usługi w chmurze i wybierz platformę FlightHub 2 Cloud. Adres serwera: http://192.168.1.1:30812 (wymagany jest protokół http://). Wprowadź zarejestrowaną nazwę użytkownika i hasło FlightHub 2; domyślne ustawienie to admin / Password@.
3. Przy pierwszym logowaniu użytkownicy muszą wybrać organizację i projekt dla zadania. Kolejne logowania będą domyślnie odbywać się do ostatnio zalogowanej organizacji i projektu. Jeśli bieżące konto nie jest przypisane do żadnej organizacji, skontaktuj się z administratorem, aby je dodać.
4. Po pomyślnym zalogowaniu strona DJI Pilot 2 wyświetli aktualne informacje o projekcie, a użytkownicy mogą kliknąć opcję Device Binding (Powiązanie urządzenia), aby powiązać drona.
5. Po powiązaniu drona można wyświetlać i zarządzać nim w interfejsie internetowym FlightHub.

Poruszanie się po interfejsie systemu

1 Ustawienia językowe

Możesz zmienić język wyświetlania zgodnie z własnymi preferencjami. W prawym górnym rogu interfejsu kliknij ikonę Język, aby zmienić język. Wybierz jedną z dostępnych opcji:

- Chiński uproszczony
- Angielski
- Hiszpański

2 Centrum powiadomień

Centrum powiadomień informuje o ważnych zdarzeniach systemowych, takich jak błędy dysku, pomagając monitorować stan systemu. Aby wyświetlić powiadomienia, kliknij ikonę dzwonka w prawym górnym rogu.

Panel wyświetli listę alertów, pokazując problem i czas jego wystąpienia. Kliknij przycisk Wyświetl obok powiadomienia, aby przejść bezpośrednio do odpowiedniej strony zarządzania i uzyskać więcej informacji.

Jeśli nie ma żadnych alertów, panel wyświetli komunikat ”No notifications” (Brak powiadomień).

3 Konserwacja systemu: aktualizacje i przywracanie

Moduł aktualizacji systemu i przywracania urządzenia obsługuje przesyłanie pakietów aktualizacji w celu aktualizacji systemu i przywrócenia ustawień fabrycznych, w celu iteracji funkcji systemu, naprawy usterek lub wstępnej konfiguracji. Uwaga: Przed rozpoczęciem operacji należy wykonać kopię zapasową danych, aby uniknąć ich utraty.

3.1 Interfejs aktualizacji i przywracania systemu

Kliknij opcję Aktualizacja i przywracanie systemu w menu nawigacyjnym po lewej stronie, aby przejść do strony konfiguracji, która zawiera trzy główne funkcje: aktualizacja systemu, aktualizacja licencji klucza sprzętowego i przywrócenie ustawień fabrycznych.

3.2 Aktualizacja systemu

Prześlij pakiet aktualizacji

Kliknij przycisk ”Upload Update Package” (Prześlij pakiet aktualizacji). Domyślnie wyświetlane są pliki lokalne. Wybierz pakiet aktualizacji systemu dostarczony przez firmę DJI (format tar.gz itp.) i kliknij przycisk „Update” (Aktualizuj). System rozpocznie proces aktualizacji i po jego zakończeniu automatycznie uruchomi się ponownie. Po pomyślnym przesłaniu plik pojawi się na liście przesłanych pakietów aktualizacji.

Aktualizacja z lokalnej ścieżki AIO
Kliknij opcję Wybierz z lokalnej ścieżki AIO, wprowadź bezwzględną ścieżkę do pliku (np. C:\Users\Nazwa użytkownika\Dokumenty\Pakiet aktualizacji tar.gz).

- Jeśli ścieżka jest nieprawidłowa, pojawi się komunikat „Nie znaleziono pliku. Wprowadź prawidłową ścieżkę" i należy ponownie sprawdzić ścieżkę.
- Jeśli ścieżka jest prawidłowa, plik zostanie automatycznie przesłany.

3.3 Aktualizacja licencji klucza sprzętowego

Proces aktualizacji pakietu aktualizacji przebiega następująco:

1. Pobierz plik aktualizacji licencji klucza sprzętowego (format .zip) ze strony internetowej DJI Developer.
2. W sekcji Dongle Update (Aktualizacja klucza sprzętowego) kliknij Upload File (Prześlij plik). Wybierz plik licencji .zip.
3. Po pomyślnym przesłaniu pliku kliknij Update (Aktualizuj). System zastosuje nową licencję do podłączonego klucza sprzętowego USB.

Uwaga: Jeśli podczas aktualizacji pojawi się komunikat „Błąd sieci. Nie udało się przesłać danych", sprawdź format, integralność, ważność i wersję pliku licencji. Uwaga: W przypadku włączenia urządzenia bez podłączonego klucza sprzętowego i bezpośredniego wejścia na stronę fhaio.net wyświetli się pełnoekranowy komunikat o błędzie „Nie wykryto klucza sprzętowego. Upewnij się, że klucz sprzętowy jest podłączony do AIO". Podłącz klucz sprzętowy zgodnie ze schematem interfejsu sprzętowego.

3.4 Przywrócenie ustawień fabrycznych

1. Kliknij Przywróć ustawienia fabryczne. W wyskakującym okienku pojawi się prośba o trzykrotne wprowadzenie hasła administratora.
2. Wprowadź poprawnie hasło administratora.
3. Po trzeciej weryfikacji hasła kliknij Potwierdź przywrócenie ustawień fabrycznych, a system rozpocznie resetowanie.
4. Przywrócenie ustawień fabrycznych spowoduje przywrócenie urządzenia AIO do stanu pierwotnego, usuwając wszystkie konfiguracje systemowe i dane.

Uwaga: Przywrócenie ustawień fabrycznych dotyczy wyłącznie systemu operacyjnego i nie ma wpływu na sprzęt.

3.5 Rozwiązywanie problemów

Objaw	Rozwiązanie
Proces aktualizacji kończy się niepowodzeniem i pojawia się komunikat o błędzie, np. „Update failed" (Aktualizacja nie powiodła się), „Network error" (Błąd sieci) lub „Corrupted package" (Uszkodzony pakiet).	Sprawdź integralność pliku aktualizacji. Wróć do sekcji Aktualizacja i przywracanie systemu, ponownie prześlij plik lub przywróć ustawienia fabryczne, a następnie spróbuj ponownie przesłać plik.
Nie możesz się zalogować ani zatwierdzić przywrócenia ustawień fabrycznych, ponieważ zapomniałeś hasła administratora.	Hasło można zresetować, uruchamiając polecenie bezpośrednio w terminalu systemu operacyjnego urządzenia AIO. curl -X PUT -H "Content-Type:

	application/json„ -d »{»new_pwd«:”YourNewPassword123"}« Uwaga: Nowe hasło musi mieć co najmniej 12 znaków i zawierać wielkie litery, małe litery oraz cyfry.
Podczas przesyłania pakietu aktualizacji pasek postępu zatrzymuje się i pojawia się komunikat „”Transfer failed” (Transfer nie powiódł się).	Przejdź na sieć przewodową i sprawdź stabilność sieci. Ponownie pobierz pakiet ze strony internetowej DJI Developer i spróbuj ponownie przesłać pliki.

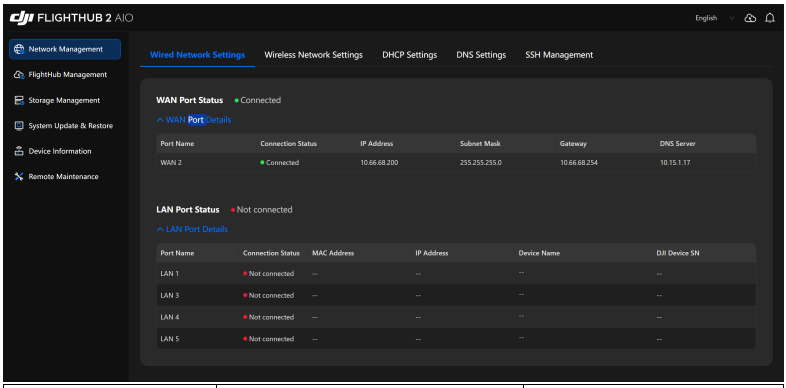
Instrukcja obsługi

1 Zarządzanie siecią

1.1 Ustawienia sieci przewodowej

Przegląd
W tej sekcji można monitorować stan portów WAN i LAN, wyświetlać szczegóły sieci oraz rozwiązywać problemy z połączeniem.
Kroki

1. Dostęp do ustawień sieci przewodowej
Kliknij opcję Zarządzanie siecią w menu nawigacyjnym po lewej stronie i wybierz opcję Ustawienia sieci przewodowej.
2. Stan połączenia portu WAN



Wskaźnik stanu	Opis	Rozwiązywanie problemów
Zielony (podłączony)	Zielony wskaźnik obok portu WAN oznacza, że połączenie zostało nawiązane pomyślnie. Kliknij strzałkę, aby rozwinąć i wyświetlić szczegóły, takie jak adres IP, maska podsieci i brama.	Jeśli parametry są nieprawidłowe, przejdź do ustawień usługi DHCP lub ręcznie skonfiguruj statyczny adres IP (musi być zgodny z siecią upstream).
Czerwony (niepodłączony)	Czerwony wskaźnik oznacza, że port nie jest podłączony.	1. Sprawdź, czy kabel sieciowy jest prawidłowo podłączony i upewnij się, że router i urządzenia są włączone i działają prawidłowo.

		2. Uruchom ponownie FlightHub 2 AIO, aby ponownie zainicjować połączenie.

3. Stan połączenia portu LAN

Wskaźnik stanu	Opis	Rozwiązywanie problemów
Zielony (podłączony)	Zielony wskaźnik oznacza, że podłączone jest co najmniej jedno urządzenie. Kliknij strzałkę, aby rozwinąć i wyświetlić szczegóły: - Adres MAC, adres IP, maska podsieci każdego portu LAN - Nazwa podłączonego urządzenia i numer seryjny Uwaga: Jeśli jeden port LAN łączy wiele urządzeń, wyświetlanych będzie wiele rekordów.	1. Jeśli urządzenie nie zostanie wykryte, sprawdź, czy kabel sieciowy jest prawidłowo podłączony i upewnij się, że podłączone urządzenie jest włączone i działa prawidłowo. 2. Upewnij się, że nie ma konfliktów adresów IP. Uwaga: Dynamiczny adres IP można przypisać za pomocą ustawień usługi DHCP.
Czerwony (niepodłączony)	Czerwony wskaźnik oznacza, że żadne urządzenia nie są podłączone lub wystąpił błąd połączenia.	1. Sprawdź, czy kabel sieciowy jest dobrze podłączony, a podłączone urządzenie jest włączone. 2. Uruchom ponownie FlightHub 2 AIO, aby ponownie zainicjować połączenie.

4. Zarządzanie połączeniami wielu urządzeń

- Gdy jeden port LAN łączy wiele urządzeń, po rozwinięciu sekcji Szczegóły portu LAN wyświetlą się dane wszystkich podłączonych urządzeń.
- Możesz znaleźć konkretne urządzenie według jego nazwy lub numeru seryjnego i sprawdzić, czy jego parametry sieciowe są spójne.

Uwagi

- Ustawienia kopii zapasowej: przed dostosowaniem parametrów, takich jak IP i DHCP, należy zapisać oryginalną konfigurację, aby zapobiec utracie ustawień, których nie można odzyskać.
- Kontrola sprzętu: jeśli często występują rozłączenia, należy spróbować użyć innego kabla sieciowego, aby wykluczyć uszkodzenie kabla lub portu.
- Wiele urządzeń: podczas podłączania wielu urządzeń należy upewnić się, że pula adresów DHCP jest wystarczająco duża, aby zapobiec konfliktom adresów IP.

1.2 Ustawienia sieci bezprzewodowej

Przegląd

Wbudowana funkcja Wi-Fi urządzenia AIO może działać w dwóch trybach.

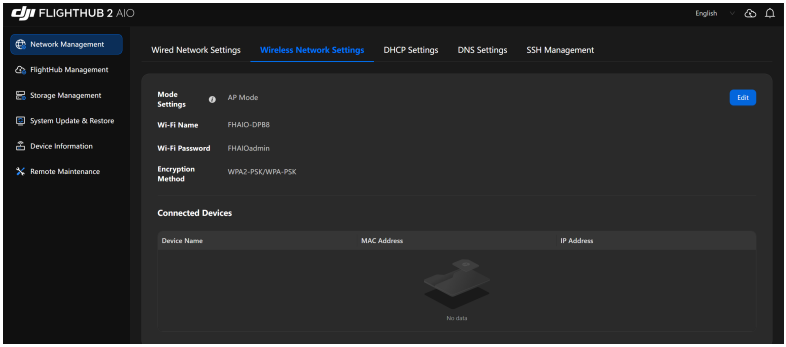
- Tryb AP (punkt dostępowy): Urządzenie AIO tworzy własny hotspot Wi-Fi. Jest to przydatne do bezpośredniego podłączania urządzeń, takich jak pilot zdalnego sterowania lub telefon komórkowy, w celu wstępnej konfiguracji lub zarządzania.
- Tryb stacji: Urządzenie AIO łączy się z istniejącą siecią Wi-Fi. Umożliwia to bezprzewodowy dostęp do Internetu lub innych zasobów sieciowych.

Uwaga: Podczas przełączania z trybu AP do trybu stacji należy podłączyć komputer bezpośrednio do urządzenia AIO za pomocą kabla Ethernet, aby zapobiec utracie dostępu do zaplecza zarządzania po przełączeniu.

Kroki

1. Dostęp do ustawień sieci bezprzewodowej

Przejdź do sekcji Zarządzanie siecią > Ustawienia sieci bezprzewodowej.



2. Działanie w trybie AP

2.1. Konfiguracja parametrów hotspotu

(1) Naciśnij przycisk Edytuj.

2) Zmodyfikuj parametry:

- Nazwa Wi-Fi: Dostosuj identyfikator SSID hotspotu (np. FHAIO-XXXX. Zaleca się uwzględnienie identyfikatora urządzenia).
- Hasło Wi-Fi: Ustaw hasło składające się z co najmniej 8 znaków, aby zapewnić bezpieczeństwo hotspotu.
- Metoda szyfrowania: WPA-PSK/WPA2-PSK (domyślnie).

3) Zapisz i zastosuj:

Naciśnij Zapisz, urządzenie ponownie uruchomi moduł hotspotu, a nowe parametry zaczną obowiązywać natychmiast.

2.2. Wyświetlanie podłączonych urządzeń

Na liście podłączonych urządzeń można wyświetlić:

- Nazwa podłączonego urządzenia, adres MAC i przypisany adres IP.
- Jeśli podłączonych jest wiele urządzeń, lista wyświetli wszystkie informacje o urządzeniach, ułatwiając zarządzanie.

3. Działanie w trybie stacjonarnym

3.1 Przełączanie trybu pracy

Aby przełączyć się do trybu stacji: Naciśnij Edytuj i wybierz Tryb stacji. Po przeczytaniu ostrzeżenia naciśnij Przełącz, aby przejść do strony konfiguracji trybu stacji.

Uwaga: Po przełączeniu nie będzie można uzyskać dostępu do zaplecza za pośrednictwem oryginalnego punktu dostępowego (fhaio.net). Konieczne będzie ponowne połączenie się przy użyciu jednej z następujących metod:

- Metoda 1: Z innego komputera w tej samej sieci LAN uzyskaj dostęp do zewnętrznego adresu IP urządzenia na porcie 30888 (np. 192.168.1.101:30888).
- Metoda 2: Podłącz komputer do urządzenia AIO za pomocą kabla Ethernet i przejdź do strony http://fhaio.net.

3.2 Wybierz opcję Zewnętrzne Wi-Fi

Wyszukaj Wi-Fi: kliknij opcję Aktualizuj Wi-Fi, aby wyszukać pobliskie sieci bezprzewodowe.
Lista wyświetla dostępne sieci Wi-Fi w pobliżu, w tym:

- nazwy (SSID), siły sygnału i statusu szyfrowania (ikona kłódki oznacza szyfrowanie; brak kłódki oznacza sieć otwartą).
- Jeśli żadna sieć Wi-Fi nie jest dostępna, w wyskakującym okienku wyświetli się komunikat „Brak dostępnych sieci Wi-Fi". Możesz kliknąć opcję Wyszukaj ponownie.

Wybierz Wi-Fi: kliknij sieć Wi-Fi, z którą chcesz się połączyć.

3.3 Wprowadź hasło Wi-Fi

Wybierz metodę szyfrowania: Pojawi się okno dialogowe do wprowadzenia hasła. Wybierz metodę w zależności od typu sieci Wi-Fi:

- Standardowe szyfrowanie (WEP/WPA2/WPA3): Wprowadź hasło Wi-Fi, a następnie kliknij Dołącz.
- Szyfrowanie korporacyjne (EAP-PEAP): Wprowadź konto uwierzytelniające i hasło, a następnie kliknij Dołącz.

Weryfikacja hasła:

- Poprawna: urządzenie próbuje nawiązać połączenie.
- Nieprawidłowe: Pojawi się komunikat „Nieprawidłowe hasło" z prośbą o ponowne wprowadzenie hasła.

3.4 Zakończ połączenie

Po pomyślnym nawiązaniu połączenia: interfejs wyświetla identyfikator SSID sieci Wi-Fi (nazwę podłączonej sieci Wi-Fi), lokalny adres IP (adres IP urządzenia w sieci), maskę podsieci i status serwera DHCP.
Potwierdź przełączenie: kliknij przycisk Zapisz. Ponownie pojawi się komunikat z przypomnieniem o metodzie ponownego połączenia. Kliknij ponownie przycisk Przełącz, aby zakończyć zmianę trybu.

3.5 Rozwiązywanie problemów

Objaw	Rozwiązanie
Nie znaleziono sieci Wi-Fi	Upewnij się, że znajdujesz się w zasięgu routera Wi-Fi. Kliknij opcję Wyszukaj ponownie, aby odświeżyć listę
Połączenie nie powiodło się z powodu nieprawidłowego hasła	Wprowadź ponownie hasło, zwracając uwagę na wielkość liter. W przypadku szyfrowania korporacyjnego upewnij się, że potwierdzono uprawnienia konta uwierzytelniającego.
Nie można uzyskać dostępu do urządzenia AIO po przełączeniu do trybu stacji	Najprostszym rozwiązaniem jest podłączenie komputera do urządzenia AIO za pomocą kabla Ethernet i przejście do strony http://fhaio.net. Alternatywnie skontaktuj się z administratorem sieci, aby uzyskać zewnętrzny adres IP urządzenia.

1.3 Ustawienia DHCP

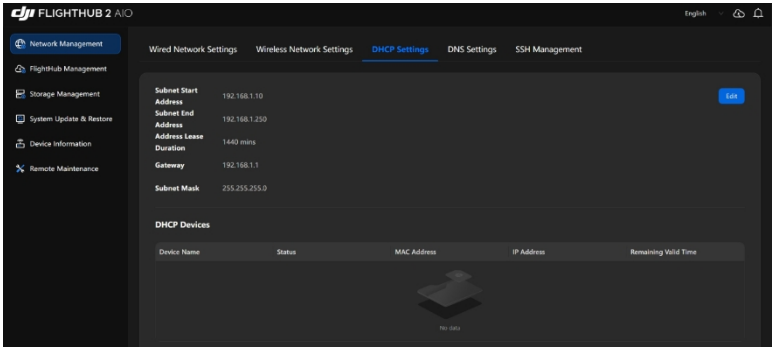
Przegląd

Usługa DHCP (Dynamic Host Configuration Protocol) automatycznie przypisuje adresy IP i ustawienia sieciowe do podłączonych urządzeń, obsługuje konfigurację zakresów adresów IP, czasów dzierżawy adresów, bram i masek podsieci oraz wyświetla w czasie rzeczywistym statusy przypisanych adresów IP, adresów MAC i okresów ważności przypisanych urządzeń IP, ułatwiając zarządzanie siecią i rozwiązywanie problemów.

Kroki

1. Dostęp do ustawień DHCP

Przejdź do sekcji Zarządzanie siecią > Ustawienia DHCP.



2. Wyświetlanie bieżących ustawień DHCP

Elementy konfiguracji przedstawiono w poniższej tabeli:

Ustawienie	Parametry	Opis
Adres początkowy podsieci	np. 192.168.1.2	Określa zakres adresów IP, które urządzenie AIO może przypisać do podłączonych urządzeniom.
Adres końcowy podsieci	np. 192.168.1.255	
Czas trwania dzierżawy adresu	Zakres: od 1 do 2880 minut	Jak długo urządzenie może zachować przypisany adres IP, zanim konieczne będzie odnowić.
Brama	np. 192.168.1.255	Adres IP, którego urządzenia używają do komunikacji z sieciami spoza ich własnej.
Maska podsieci	np. 255.255.255.0	Określa rozmiar lokalnej sieci.

Lista urządzeń DHCP	Wyświetla parametry urządzeń, którym przypisano adresy IP.	W tym nazwę urządzenia, status (online/offline), adres MAC, adres IP i czas dzierżawy.

3. Edytuj parametry DHCP

3.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

3.2 Modyfikacja parametrów

Parametry	Zasady i wskaźniki
Adres początkowy podsieci	Musi być prawidłowym adresem IP, a adres początkowy musi być niższy niż adres końcowy.
Adres końcowy podsieci	Musi znajdować się w tej samej sieci i unikać konfliktów ze statycznymi adresami IP.
Czas trwania dzierżawy adresu	Obsługuje konfigurację okresu dzierżawy od 1 do 2880 minut. Krótsze okresy dzierżawy prowadzą do częstszych aktualizacji adresów IP, natomiast dłuższe okresy dzierżawy skutkują większą stabilnych adresów IP.
Brama	Musi być zgodna z bramą sieci LAN bramą sieci LAN (np. 192.168.1.255).
Maska podsieci	Domyślnie wynosi 255.255.255.0.

3.3 Zapisz konfiguracje

- Kliknij Zapisz. Jeśli parametry są prawidłowe, ustawienia zostaną zastosowane.
- W przypadku wystąpienia błędu parametru należy go skorygować.

Po zapisaniu należy odłączyć i ponownie podłączyć kable sieciowe, aby urządzenia uzyskały nowe konfiguracje DHCP.

Uwagi

- Kopia zapasowa parametrów: Przed modyfikacją należy wykonać kopię zapasową oryginalnych konfiguracji, aby zapobiec problemom, takim jak przerwy w działaniu sieci.
- Unikanie konfliktów: Upewnij się, że segment sieci DHCP nie pokrywa się z żadnymi statycznymi adresami IP. Pokrywające się segmenty spowodują konflikty adresów.

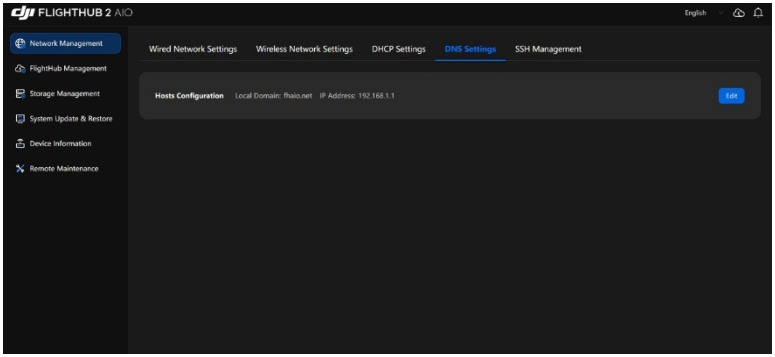
1.4 Ustawienia DNS

Przegląd

Ustawienia rozpoznawania nazw domen umożliwiają tworzenie niestandardowych nazw domen, które odsyłają do określonych adresów IP w sieci lokalnej. Są one powszechnie używane do uzyskiwania dostępu do usług lub urządzeń intranetowych.

Kroki

1. Dostęp do ustawień rozpoznawania nazw domen Przejdź do sekcji Zarządzanie siecią > Ustawienia DNS.



2. Edytuj wpisy hostów

2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

2.2 Zmodyfikuj istniejące wpisy

Kliknij bezpośrednio na pola nazwy domeny lub adresu IP i wprowadź zmiany.

- Nazwa domeny: musi być zgodna ze standardowymi konwencjami nazewnictwa DNS (np. example.com). Znaki specjalne są niedozwolone.
- Adres IP: musi być prawidłowym adresem IPv4. Niedozwolone formaty to 0.0.0.0 oraz adresy z segmentami poza zakresem 0-255.

2.3 Dodaj nowy wpis

- Kliknij niebieską ikonę + i wprowadź żądaną nazwę domeny oraz odpowiedni adres IP.
- Wprowadź nową nazwę domeny i adres IP.

2.4 Usuń wpis

Kliknij czerwoną ikonę - obok wpisu, który chcesz usunąć.

Uwaga: Zachowaj ostrożność, ponieważ po usunięciu nie można go odzyskać.

3. Zapisz konfigurację

- Kliknij przycisk Zapisz, aby zastosować zmiany.
- Jeśli format danych wejściowych jest nieprawidłowy, należy go poprawić i ponownie zapisać. Interfejs nie wyświetla obecnie komunikatów dotyczących sprawdzania poprawności, więc konieczna jest ręczna weryfikacja.

4. Wyświetlać zapisane wpisy hostów

Po zapisaniu i wyjściu z trybu edycji wszystkie skonfigurowane mapowania domen-IP zostaną wyświetlone w interfejsie, umożliwiając prostą weryfikację i późniejsze zarządzanie.

Uwagi

- Unikalność domeny: Nie należy przypisywania tej samej nazwy domeny do wielu adresów IP adresów IP, ponieważ spowoduje to konflikty.
- Ważność adresu IP: Upewnij się, że wprowadzony adres IP odpowiada rzeczywistemu, dostępnemu urządzeniu w sieci.
- Scenariusze zastosowań: Te ustawienia dotyczą urządzenia AIO i urządzeń w tej samej sieci LAN. Jeśli wymagana jest publiczna rozdzielczość sieci, potrzebna jest konfiguracja z serwerem DNS lub dostawcą usług nazw domenowych.

1.5 Zarządzanie SSH

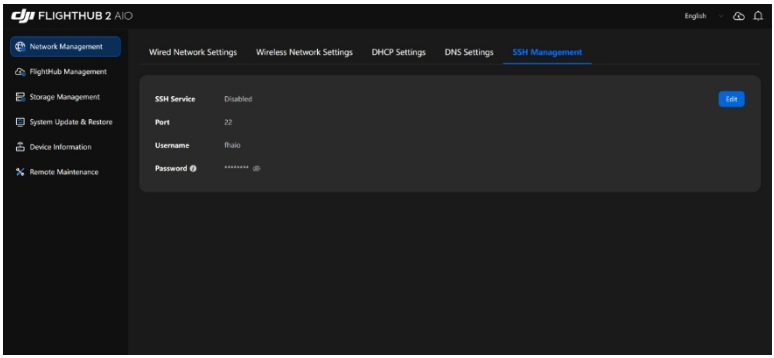
Przegląd

SSH (Secure Shell) zapewnia bezpieczny dostęp do systemu operacyjnego urządzenia AIO. Jest to zaawansowana funkcja przeznaczona do rozwiązywania problemów i administrowania systemem. Włączenie SSH naraża system na potencjalny zdalny dostęp. Włączaj tę funkcję tylko w razie potrzeby i używaj silnych, unikalnych danych uwierzytelniających.

Kroki

1. Dostęp do interfejsu zarządzania SSH

Przejdź do Zarządzanie siecią > Zarządzanie SSH.



2. Wyświetlanie bieżącego stanu SSH

Elementy konfiguracji są przedstawione w poniższej tabeli:

Element	Parametry	Opis
Usługa SSH	Włączona/wyłączona	Kolor niebieski oznacza włączoną usługę, a kolor szary oznacza wyłączenie.
Port	22 (domyślny)	Możliwość modyfikacji. Musi mieścić się w zakresie portów 0-65535.
Nazwa użytkownika	Aktualne konto logowania SSH	
Hasło	Domyślnie ukryte	Kliknij ikonę oka, aby tymczasowo wyświetlić, a kliknij ponownie, aby ukryć.

3. Edytuj konfigurację SSH

3.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu, aby otworzyć okno dialogowe weryfikacji hasła administratora:

- Wprowadź hasło administratora systemu. Hasło to jest takie samo jak hasło używane do zarządzania urządzeniami.

- Kliknij przycisk Potwierdź, aby przejść do trybu edycji.

3.2 Modyfikowanie elementów konfiguracji

Parametry	Zasady i wskaźniki
Usługa SSH	Włącz/Wyłącz SSH: Użyj przełącznika, aby włączyć lub wyłączyć usługę SSH. Zaleca się wskazać pozostawienie wyłączoną podczas normalnej pracy.
Port	Domyślny port to 22. Dopuszczalny zakres to 1-65535.
Nazwa użytkownika	Ustaw silną, unikalną nazwę użytkownika i hasło dla dostępu SSH . Unikaj prostych nazw, takich jak admin lub root.
Hasło	Hasło powinno być złożone i zawierać co najmniej 8 znaków, w tym wielkie litery, małe litery i cyfry. **Uwaga: Po najechaniu myszką na ikonę informacji może pojawić się komunikat wskazujący, że hasła frontendu i backendu mogą być niespójne.**

3.3 Zapisz konfiguracje

Kliknij przycisk Zapisz, aby zastosować zmiany.

- Jeśli konfiguracja jest prawidłowa, zostanie pomyślnie zapisana i natychmiast zacznie obowiązywać.
- Jeśli format danych wejściowych jest nieprawidłowy, należy go poprawić i ponownie zapisać. Interfejs nie wyświetla obecnie komunikatów dotyczących sprawdzania poprawności, dlatego konieczna jest ręczna weryfikacja.

Uwagi

- Włącz na żądanie: włącz SSH tylko wtedy, gdy jest to konieczne do przeprowadzenia konserwacji.
- Użyj silnego hasła: Utwórz złożone hasło, używając wielkich liter, małych liter, cyfr i symboli.
  - Hasła powinny być złożone i regularnie zmieniane (unikaj samych cyfr lub prostych kombinacji);
  - Zmień domyślny port: Korzystanie z niestandardowego portu utrudnia atakującym znalezienie i zaatakowanie usługi SSH.
- Izolacja sieciowa: Jeśli urządzenie AIO jest podłączone do Internetu, wskazać należy wdrożenie reguł zapory sieciowej lub routera, aby zezwolić na dostęp do portu SSH tylko z zaufanych adresów IP.

2 Zarządzanie FlightHub

2.1 Ustawienia operacyjne i konserwacyjne

Przegląd

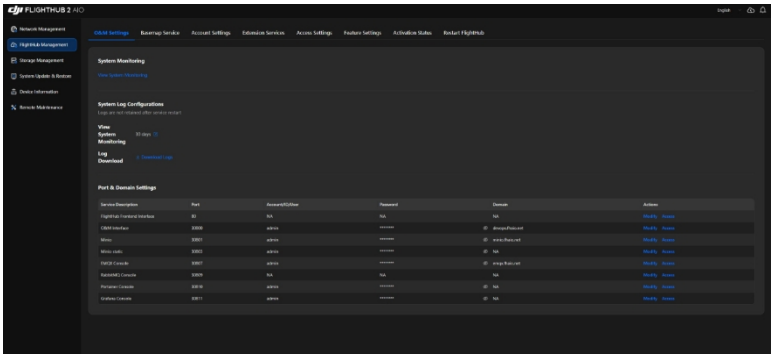
Ten moduł zapewnia narzędzia do zarządzania dziennikami systemowymi, portami O&M, kontami, domenami i monitorowaniem systemu, wspierając rozwiązywanie problemów z urządzeniami, zdalne O&M i konfigurację usług. **Należy zachować ostrożność podczas obsługi.**

Uwaga: Wprowadzenie zmian w większości ustawień w sekcji zarządzania FlightHub uruchomi automatyczne ponowne uruchomienie usług FlightHub 2. Proces ten może potrwać od 2 do 10 minut, podczas których FlightHub 2 będzie niedostępny.

Kroki

1. Dostęp do ustawień O&M

Przejdź do sekcji Zarządzanie FlightHub > Ustawienia O&M.



2. Konfiguracje dziennika systemowego

2.1 Przechowywanie dzienników

Ustaw, jak długo mają być przechowywane logi systemowe. Wybierz 1, 3, 7 lub 30 dni.

- Kliknij żądaną liczbę dni (np. „7 dni"). Po prawej stronie pojawi się zielony znacznik wyboru potwierdzający wybór.
- Aby anulować, kliknij czerwony krzyżyk obok wybranego okresu.

Uwaga: Logi nie są przechowywane po ponownym uruchomieniu usługi. Rejestrowane są tylko logi O&M z wybranego okresu.

2.2 Pobieranie logów

Kliknij Pobierz logi, aby automatycznie spakować i pobrać pliki logów za bieżący okres przechowywania.

3. Zarządzanie portami usług i domenami

3.1 Przegląd listy usług

Łatwo zarządzaj swoimi usługami za pomocą tego interfejsu, który wyświetla podstawowe informacje o połączeniach, takie jak porty, konta/identyfikatory, hasła, domeny i punkty dostępu operacyjnego

dla interfejsu operacyjnego, MinIO, MinIO Static, konsoli EMQX, konsoli SRS, konsoli RabbitMQ, konsoli Portainer, konsoli Grafana i konsoli Traefik Gateway.

3.2 Modyfikowanie konfiguracji usług

3.2.1 Rozpocznij proces modyfikacji

Kliknij ikonę Edytuj obok usługi, którą chcesz zmienić. Wprowadź hasło administratora systemu. Hasło to jest takie samo jak hasło używane do zarządzania urządzeniami.

3.2.2 Edytuj elementy konfiguracji

Po przejściu do trybu edycji można modyfikować:

Pozycję	Zasady i wskaźniki
Port	Wprowadź prawidłowy port (0-65535), aby uniknąć konfliktów z innymi usługami. Domyślnym portem dla interfejsu obsługi i konserwacji jest 30800.
Konto/ID/użytkownik	Dostosuj konto logowania. Aby zwiększyć bezpieczeństwo przed atakami brute-force, wskazano użycie złożonej nazwy konta.
Hasło	Hasło powinno być złożone i zawierać co najmniej 8 znaków, w tym wielkie litery, małe litery i cyfry.
Domena	Wprowadź prawidłową nazwę domeny, która musi być zgodna z zasadami rozdzielczości sieciowej.

3.2.3 Zapisz lub anuluj zmiany

- Kliknij zielony znacznik wyboru, aby zapisać zmiany. Spowoduje to ponowne uruchomienie określonej usługi.
- Kliknij czerwony znak X, aby anulować.

4. Monitorowanie systemu

Kliknij link Wyświetl monitorowanie systemu, aby uzyskać dostęp do pulpitu monitorowania. Wyświetla on:

- Stan zasobów urządzenia: wykorzystanie procesora, pamięci i pamięci masowej.
- Stan działania usługi: stan online usługi zaplecza i czasy odpowiedzi.
- Alerty o błędach: błędy usług są zaznaczone na czerwono.

Uwagi

- Weryfikacja hasła: Modyfikowanie konfiguracji O&M zawsze wymaga weryfikacji hasła administratora. W przypadku zapomnienia hasła należy zapoznać się z instrukcją przywracania systemu, aby uzyskać informacje dotyczące resetowania hasła.
- Ryzyko ponownego uruchomienia usługi: Modyfikacja portów, kont lub domen spowoduje ponowne uruchomienie usługi, której dotyczy zmiana. Operacje te należy planować w okresach niskiego wykorzystania.
- Przechowywanie logów: Dłuższe przechowywanie logów zajmuje więcej miejsca. Regularnie pobieraj logi do archiwizacji i rozważ skrócenie okresu przechowywania, jeśli masz mało miejsca.
- Dostosowanie sieci: W przypadku zmiany portu lub domeny usługi należy zaktualizować wszystkie zewnętrzne klienty (np. przeglądarki internetowe, narzędzia O&M), które łączą się z nią, w przeciwnym razie utracą one dostęp.

2.2 Usługa map bazowych

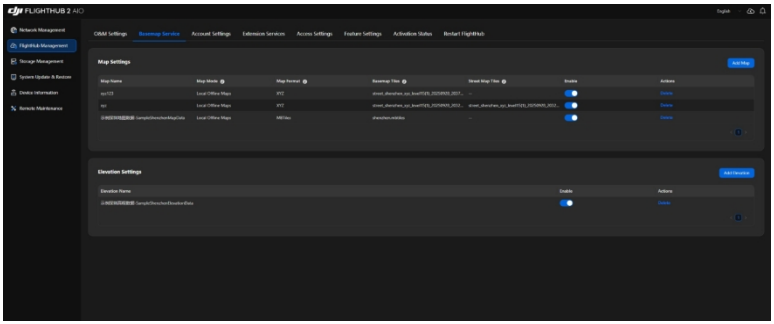
Przegląd

Moduł ten umożliwia zarządzanie danymi mapowymi i wysokościowymi wykorzystywanymi w FlightHub 2, obsługując różne tryby dostępu do map (offline, online, intranet).

Kroki

1. Dostęp do usługi map bazowych

Przejdź do sekcji Zarządzanie FlightHub > Usługa mapy bazowej.



2. Ustawienia mapy

2.1 Wyświetlać listę istniejących map

Wyświetla wszystkie skonfigurowane mapy, w tym ich nazwy, tryby, statusy i działania.

- Nazwa mapy
- Tryb mapy
- Format mapy
- Kafelki mapy bazowej / kafelki mapy ulic
- Status
- Działania

2.2. Dodaj nową mapę

2.2.1 Przejdź do procesu dodawania

Kliknij Dodaj mapę w prawym górnym rogu, a pojawi się okno konfiguracji Dodaj mapę.

2.2.2 Skonfiguruj parametry mapy

Element	Operacje i reguły
Nazwa mapy	Podaj własną nazwę, aby ułatwić identyfikację.
Tryb mapy	Wybierz sposób uzyskiwania dostępu do danych mapy: - Lokalne mapy offline: Wymaga przesłania plików z fragmentami mapy. - Mapy online: łączy się z publiczną usługą map online. Wymaga adresu URL usługi i ewentualnie klucza API. - Niestandardowe mapy online: łączy się z usługą mapową hostowaną w sieci lokalnej.

Format mapy (tylko dla map lokalnych map)	Wybierz między MBTiles (pojedynczy plik bazy danych) a XYZ (strukturę folderów z poszczególnymi obrazami kafelków).
Kafelki mapy bazowej / kafelki mapy ulic (tylko dla map lokalnych)	Kliknij przycisk Prześlij plik, aby wybrać pakiet kafelków mapy (np. format .mbtiles, .zip). Kafelki ulic są opcjonalne.

2.2.3 Prześlij i załaduj

- Kliknij Dodaj. System prześle pliki (jeśli dotyczy) i doda mapę do listy.
- Następnie należy ją ręcznie włączyć.

2.3 Edytuj istniejącą mapę

- Kliknij link kafelka. Wprowadź hasło administratora systemu w celu weryfikacji.
- Zmodyfikuj nazwę, tryb lub format mapy.

Uwaga: Zmiana trybu lub formatu mapy spowoduje usunięcie wcześniej przesłanych plików kafelków, co będzie wymagało ponownego przesłania.

- Kliknij przycisk Zapisz, aby zastosować zmiany.

2.4 Usuń mapę

- Kliknij przycisk Usuń obok mapy. Pojawi się okno dialogowe z prośbą o potwierdzenie.
- Kliknij ponownie przycisk Usuń, aby potwierdzić. Uwaga: tej czynności nie można cofnąć.

2.5 Włączanie/wyłączanie mapy

Użyj przełącznika. Kolor niebieski oznacza, że mapa jest aktywna i ma priorytet. Kolor szary oznacza, że jest wyłączona. Gdy włączonych jest wiele map, priorytet mają mapy znajdujące się wyżej na liście.

3. Ustawienia wysokości

3.1 Wyświetlać istniejącą listę wysokości

Interfejs wyświetla skonfigurowane dane dotyczące wysokości, w tym nazwę, zakres szerokości i długości geograficznej, status oraz działania.

3.2 Dodaj nowe dane dotyczące wysokości

Kliknij Dodaj wysokość i wprowadź następujące informacje:

- Nazwa wysokości: nazwa niestandardowa.
- Zakres szerokości i długości geograficznej: Wprowadź prawidłowy zakres.
- Opcjonalnie kliknij przycisk Prześlij plik, aby przesłać pliki kafelków wysokości.

Kliknij Dodaj. Dane zostaną dodane i należy je ręcznie włączyć.

3.3. Usuń dane dotyczące wysokości

Kliknij ikonę Usuń.

Uwaga: Ta czynność jest natychmiastowa i nieodwracalna.

Uwagi

- Ograniczenia dotyczące przesyłania plików:
  - W przypadku lokalnych plików kafelkowych wskazane jest stosowanie plików skompresowanych w formacie ZIP. Pojedyncze pliki nie powinny przekraczać 1 GB, aby uniknąć błędów podczas przesyłania.
  - Upewnij się, że formaty plików są prawidłowe.
- Ryzyko związane z przełączaniem trybu mapy: Przełączenie mapy z trybu lokalnego offline do trybu online spowoduje usunięcie powiązanych plików kafelkowych. Konieczne będzie ponowne skonfigurowanie adresu URL mapy online.

  URL.

- Weryfikacja hasła administratora: Edycja lub usuwanie map i danych dotyczących wysokości wymaga weryfikacji hasła administratora ze względów bezpieczeństwa.
- Priorytet mapy: Gdy włączonych jest wiele map, FlightHub 2 załaduje mapę, która znajduje się najwyżej na liście. Obsługiwana jest ręczna regulacja.

2.3 Ustawienia konta

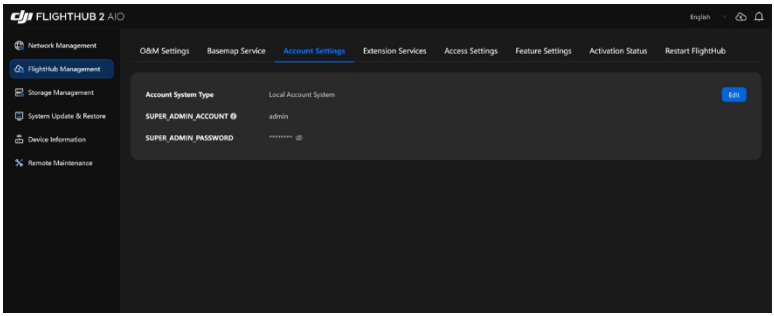
Przegląd

Ten moduł umożliwia skonfigurowanie metod uwierzytelniania dostępu do FlightHub 2 AIO, obsługując lokalny system kont lub integrację z usługami stron trzecich.

Kroki

1. Dostęp do ustawień konta

Przejdź do FlightHub Management > Ustawienia konta.



2. Lokalny system kont

2.1 Wyświetlać aktualny stan

Wyświetla SUPER_ADMIN_ACCOUNT (nazwa użytkownika superadministratora) i SUPER_ADMIN_PASSWORD (hasło, domyślnie ukryte).

2.2 Edytuj parametry konta lokalnego

2.2.1 Przejdź do trybu edycji;

Kliknij przycisk Edytuj w prawym górnym rogu, aby przejść do trybu konfiguracji.

2.2.2 Modyfikacja konta/hasła

Element	Operacje i zasady
Typ systemu kont	Zachowaj wybraną opcję Lokalny system kont.
SUPER_ADMIN_ACCOUNT	Możesz zmienić SUPER_ADMIN_ACCOUNT (wskazać należy użycie złożonej, nieoczywistej nazwy).
SUPER_ADMIN_PASSWORD	Hasło powinno być złożone i zawierać co najmniej 8 znaków, w tym wielkie litery, małe litery i cyfry. Uwaga: SUPER_ADMIN_ACCOUNT ma najwyższy poziom uprawnień. Zapamiętaj nowe hasło, ponieważ steruje ono dostępem do urządzenia.

2.2.3 Zapisz zmiany

Kliknij Zapisz. Nowe dane uwierzytelniające zaczną obowiązywać natychmiast.

3. System kont innych firm

3.1 Przejdź do systemu zewnętrznego

Kliknij kartę System kont zewnętrznych.

Uwaga: spowoduje to ukrycie konfiguracji konta lokalnego.

3.2 Skonfiguruj parametry uwierzytelniania zewnętrznego

Wypełnij wymagane pola parametrami dostarczonymi przez platformę uwierzytelniania zewnętrznego.

Element	Zasady i opisy
CLIENT_ID	Identyfikator klienta przypisany przez platformę zewnętrzną (np. LvHms6F60). Upewnij się, że jest on zgodny z zapleczem platformy.
CLIENT_SECRET	Sekret klienta (np. zdCETKc4w22RFOvDwlIF58llxpCN4mgl). Należy zachować ścisłą poufność.
AUTH_URL	URL autoryzacji uwierzytelniania podmiotu zewnętrznego (np. http://ry.sxldj.com/api/oauth2/authorize). Musi być dostępny.
TOKEN_URL	Adres pozyskiwania tokenów (np. http://ry.sxldj.com/api/oauth2/token). Służy do wymiany tokeny dostępu.
USER_URL	Adres URL zapytania o informacje o użytkowniku (np. http://ry.sxldj.com/api/userinfo). Służy do uzyskania danych zalogowanego.
USER_ID_KEY	Nazwa klucza dla identyfikatora użytkownika w zwróconych danych. Powinna odpowiadać formatowi odpowiedzi platformy zewnętrznej.
USER_ACCOUNT_KEY	Nazwa klucza dla konta użytkownika w zwróconych danych. Powinna odpowiadać formatowi odpowiedzi platformy zewnętrznej.
USE_REDIRECT_URL	Wprowadź adres URL, pod który użytkownik zostanie przekierowany po autoryzacji. Ten adres URI musi dokładnie odpowiadać adresowi AUTH_URL skonfigurowany w Twojej aplikacji.
SUPER_ACCOUNT	Konto superadministratora dla systemu zewnętrznego, niezbędne do wykonywania działań wymagających wysokich uprawnień.

3.3 Zapisz konfiguracje

Po wypełnieniu wszystkich parametrów kliknij Zapisz. System spróbuje zweryfikować dostępność adresów URL. Jeśli będą one nieprawidłowe, zapisanie nie powiedzie się.

3.4 Powrót do systemu lokalnego

Aby powrócić, kliknij kartę System kont lokalnych.

Uwaga: Wszystkie wcześniej skonfigurowane parametry podmiotu zewnętrznego zostaną wyczyszczone. Konieczne będzie ponowne skonfigurowanie lokalnego konta administratora nadrzędnego.

Uwagi

- Ryzyko związane z uprawnieniami: Modyfikacja systemu kont ma znaczący wpływ na uprawnienia logowania do urządzenia. Zawsze najpierw dokładnie testuj zmiany w środowisku nieprodukcyjnym.

- Zależność od parametrów podmiotu zewnętrznego: Konfiguracja podmiotu zewnętrznego musi dokładnie odpowiadać ustawieniom zewnętrznej platformy uwierzytelniającej (np. niezgodność CLIENT_ID lub niedostępne adresy URL spowodują błędy logowania).
- Zarządzanie hasłami: Regularnie zmieniaj hasła administratorów lokalnych/podmiotów zewnętrznych. Bezpiecznie przechowuj klucze podmiotów zewnętrznych.
- Przełączanie i przywracanie: W przypadku przełączania się z systemu zewnętrznego z powrotem do systemu lokalnego, jeśli nie utworzono kopii zapasowej konta lokalnego, może być konieczne ponowne zarejestrowanie konta administratora, ponieważ urządzenie może nie zachować oryginalnych danych konta lokalnego.

2.4 Usługi rozszerzeń

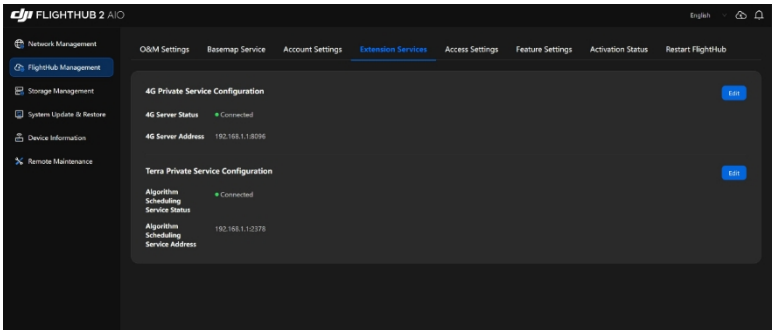
Przegląd

W tej sekcji można skonfigurować połączenia ze specjalistycznymi usługami, takimi jak prywatna sieć 4G lub DJI Terra, aby uzyskać zaawansowane możliwości.

Kroki

1. Dostęp do usług rozszerzeń

Przejdź do FlightHub Management > Usługi rozszerzeń.



2. Prywatna usługa 4G

2.1 Wyświetlać aktualny stan

- Stan serwera 4G: Połączono (zielony), Nie udało się nawiązać połączenia, Nie połączono.
- Adres serwera 4G: adres sieciowy używany do połączenia z serwerem 4G. Domyślnym adresem jest adres lokalny. (Przykład: devops.fhaio.local)

2.2 Edytuj parametry usługi 4G

2.2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

2.2.2 Zmiana adresu serwera

Wprowadź nowy adres dla prywatnej usługi 4G. Aby powrócić do wbudowanej usługi AIO, kliknij przycisk Przywróć adres lokalny, aby automatycznie wypełnić domyślny adres devops.fhaio.local.

2.2.3 Zapisz i sprawdź łącze

Kliknij Zapisz. Wskaźnik stanu zmieni kolor na zielony, jeśli połączenie się powiodło, lub na czerwony, jeśli

nie powiodło się.

- Połączenie nawiązane: Status serwera 4G pozostaje zielony i jest podłączony.
- Połączenie nie powiodło się: Wskaźnik stanu zmieni kolor na czerwony, sygnalizując nieudane połączenie. Sprawdź dostępność sieci, w tym routing sieciowy i czy serwer jest włączony.

3. Konfiguracje usługi Terra Private

3.1 Wyświetlać aktualny status

- Status usługi planowania algorytmów: Połączono (zielony), Nie udało się nawiązać połączenia.
- Adres usługi planowania algorytmów: Adres sieciowy używany do połączenia z usługą planowania algorytmów. Domyślnym adresem jest adres lokalny.

3.2 Edytuj parametry usługi Terra

3.2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

3.2.2 Zmiana adresu planowania

Wprowadź nowy adres dla usługi planowania algorytmów. Aby powrócić do wbudowanej usługi AIO, kliknij przycisk Przywróć adres lokalny.

3.2.3 Zapisz i sprawdź połączenie

Kliknij przycisk Zapisz. Wskaźnik stanu zmieni kolor na zielony, jeśli połączenie się powiodło, lub na czerwony, jeśli zakończyło się niepowodzeniem.

- Połączenie nawiązane: Status usługi planowania algorytmów pozostaje zielony i połączony.
- Połączenie nie powiodło się: wskaźnik stanu zmieni kolor na czerwony, wskazując nieudane połączenie. Sprawdź dostępność sieci, w tym routing sieciowy i czy serwer jest włączony.

Uwagi

- Ważność adresu:
  - Adres usługi 4G lub Terra musi być zgodny z faktycznie wdrożonym adresem IP lub nazwą domeny serwera, a sieć urządzenia musi być dostępna. Wskazać należy najpierw przetestowanie łączności za pomocą narzędzi ping lub telnet.
  - W przypadku korzystania z niestandardowej nazwy domeny należy upewnić się, że intranetowy DNS został rozwiązany lub plik hosts został skonfigurowany do mapowania.
- Monitorowanie statusu:
  - Status usługi wskazuje, czy powiązane funkcje, takie jak planowanie sieci 4G i działanie algorytmu Terra. Zielony status (Połączono) oznacza, że funkcje te mogą być używane prawidłowo.
  - Jeśli status jest czerwony (Błąd), sprawdź pisownię adresu i status serwera, upewniając się, że proces działa, a port nie jest zajęty.
- Przywróć ustawienia domyślne: Jeśli po zmianie adresu połączenie nie działa, kliknij Przywróć adres lokalny, żeby wrócić do poprzednich ustawień. To pomaga szybko zdiagnozować problemy z konfiguracją adresu.

2.5 Ustawienia dostępu

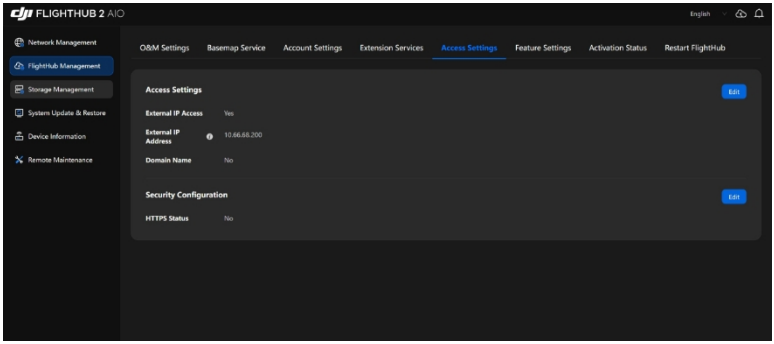
Przegląd

Ta sekcja służy do konfigurowania reguł dostępu do sieci urządzenia (zewnętrzny adres IP, nazwa domeny) oraz uwierzytelniania bezpieczeństwa (HTTPS, licencja). Operacje muszą być wykonywane ściśle zgodnie z procedurą, aby zapewnić bezpieczeństwo dostępu.

Kroki

1. Dostęp do ustawień dostępu

Przejdź do FlightHub Management > Ustawienia dostępu.



2. Konfiguracje dostępu

2.1 Wyświetlanie bieżącego stanu

- Dostęp do zewnętrznego adresu IP: przełącznik umożliwiający włączenie lub wyłączenie dostępu do zewnętrznego adresu IP. Przełącznik jest niebieski, gdy funkcja jest włączona.
- Zewnętrzny adres IP: Wyświetla skonfigurowany zewnętrzny adres IP (np. devops.fhaio.local). Adres ten musi być zgodny z topologią sieci.
- Nazwa domeny: przełącznik umożliwiający włączenie lub wyłączenie rozpoznawania nazw domen. Przełącznik ma kolor niebieski, gdy jest włączony.
- Niestandardowa nazwa domeny: umożliwia określenie niestandardowej nazwy domeny (np. devops.fhaio.local). Domena ta musi być skonfigurowana tak, aby przekierowywała do adresu IP urządzenia.

2.2 Edytuj parametry dostępu

2.2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

2.2.2 Dostosuj reguły dostępu

Element	Operacje i reguły
Dostęp zewnętrzny przez adres IP	• Włączone: Zezwala sieciom zewnętrznym na dostęp do urządzenia za pośrednictwem jego adresu IP. • Wyłączone: ogranicza dostęp wyłącznie do sieci wewnętrznej (zwiększone bezpieczeństwo).

Zewnętrzny adres IP	Po włączeniu tej opcji wprowadź prawidłowy adres IP lub domenę. nazwa. Upewnij się, że Twoja sieć jest routowalna (porty zapory sieciowej/routera są otwarte).
Nazwa domeny	• Włączone: umożliwia dostęp za pośrednictwem niestandardowej nazwy domeny. • Wyłączone: Zezwala wyłącznie na dostęp za pośrednictwem adresu IP (wymaga jednoczesnego wyłączenia rozpoznawania nazw domen).
Niestandardowa nazwa domeny	Po włączeniu tej opcji wprowadź rozpoznaną nazwę domeny (np. custom.devops.com). Musi być zgodna z konfiguracją DNS.

2.2.3 Zapisz zmiany

Kliknij Zapisz. Nowe reguły zaczną obowiązywać natychmiast.

- Jeśli włączono zewnętrzny adres IP/domenę, sprawdź łączność (np. za pomocą polecenia ping).
- Jeśli opcja jest wyłączona, urządzenie będzie odpowiadać tylko na żądania wewnętrznego adresu IP, a metody dostępu klienta mogą wymagać dostosowania.

3. Konfiguracje zabezpieczeń

3.1 Wyświetlać aktualny stan

- Stan HTTPS: Przełącznik do włączania lub wyłączania protokołu HTTPS. Przełącznik jest niebieski, gdy funkcja jest włączona.
- Import certyfikatu: Wskazuje, czy zaimportowano niestandardową licencję. Wymagane jest wcześniejsze przesłanie pliku.
- Certyfikat serwera (crt): Wyświetla ścieżkę do pliku certyfikatu SSL/TLS serwera (np. devops.fhaio.local).
- Plik klucza (key): Wyświetla ścieżkę do odpowiedniego pliku klucza prywatnego (np. devops.fhaio.local).

3.2 Edytuj parametry bezpieczeństwa

3.2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

3.2.2 Dostosuj reguły dostępu

Element	Operacje i reguły
Status HTTPS	• Włączone: wymusza dostęp HTTPS (szyfrowana transmisja, wymaga ważnego certyfikatu). • Wyłączone: Obniża poziom do HTTP (nie należy wskazać ze względu na...) ryzyka związanego z tekstem jawnym).
Import certyfikatu	Wybierz z listy rozwijanej: • Certyfikat niestandardowy (wymaga przesłania plików .crt i .key) • Certyfikat z podpisem własnym (domyślny, niższy poziom bezpieczeństwa, tylko do testów).
Certyfikat serwera (crt)	W przypadku wyboru licencji niestandardowej należy przesłać plik .crt ścieżkę do pliku .crt (np. devops.fhaio.local).
Plik klucza (key)	Wybierając certyfikat niestandardowy, określ ścieżkę do pliku .key ścieżkę do pliku .key.

3.2.3 Zapisz i zweryfikuj HTTPS

Kliknij przycisk Zapisz. System zweryfikuje ważność certyfikatu.

- Ważny certyfikat: dostęp HTTPS działa prawidłowo (w przeglądarce wyświetlana jest ikona kłódki).
- Nieważny certyfikat: połączenie HTTPS nie działa. Prześlij ponownie prawidłowy certyfikat.

Uwagi

- Zależności sieciowe: przed włączeniem zewnętrznego adresu IP/domeny upewnij się, że wyjście sieciowe (zapora sieciowa, router) ma otwarte odpowiednie porty (np. 80, 443).
- Zabezpieczenia licencji:
  - Certyfikaty niestandardowe powinny być wydawane przez zaufany urząd certyfikacji, aby uniknąć ostrzeżeń przeglądarki.
  - Certyfikaty z podpisem własnym służą wyłącznie do celów testowych; środowiska produkcyjne wymagają certyfikatów zgodnych z normami.
- Cofnięcie dostępu: Jeśli po wprowadzeniu zmian nie możesz uzyskać dostępu do urządzenia, możesz zalogować się poprzez bezpośrednie połączenie lokalne z portem zarządzania urządzenia, aby ponownie dostosować konfiguracje dostępu.

2.6 Ustawienia funkcji

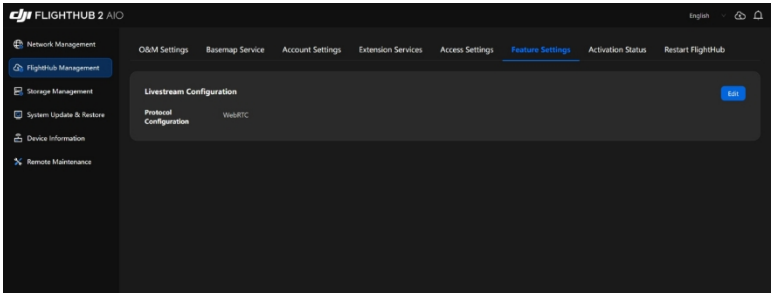
Przegląd

Ta sekcja służy do konfigurowania protokołów funkcji transmisji na żywo, umożliwiając przełączanie między protokołami WebRTC/RTMP w celu dostosowania się do różnych scenariuszy transmisji na żywo.

Kroki

1. Dostęp do ustawień funkcji

Przejdź do FlightHub Management > Ustawienia funkcji.



2. Konfiguracje protokołów transmisji na żywo

2.1 Wyświetlać bieżący protokół

Wyświetla aktualnie aktywny protokół transmisji na żywo (domyślnie WebRTC).

2.2 Zmień protokół transmisji na żywo

2.2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

2.2.2 Wybierz typ protokołu

Protokół	Odpowiednie scenariusze i zasady

WebRTC	Wysoka jakość czasu rzeczywistego (niskie opóźnienia), idealny do interaktywnych transmisji na żywo i scenariuszy wymagających niskich opóźnień. Obsługiwany natywnie przez nowoczesne przeglądarki, nie wymaga dodatkowych wtyczek.
RTMP	Dobra kompatybilność, dostosowuje się do tradycyjnych serwerów mediów strumieniowych. Odpowiedni do przesyłania strumieni do CDN i platform transmisji na żywo.

2.2.3 Zapisz ustawienia protokołu

Kliknij Zapisz. Nowy protokół zacznie działać od razu.

- W przypadku przechodzenia na RTMP upewnij się, że serwer strumieniowy jest skonfigurowany (np. port 1935 jest włączony).
- W przypadku zachowania protokołu WebRTC upewnij się, że Twoja sieć obsługuje transmisję UDP (niektóre środowiska intranetowe mogą ograniczać protokół UDP, powodując przerywanie transmisji).

Uwagi

- Zgodność protokołów:
  - WebRTC wymaga obsługi przeglądarki/klienta oraz otwartych portów UDP.
  - RTMP wymaga serwera strumieniowego przesyłania multimediów.
- Opóźnienie transmisji na żywo:
  - WebRTC oferuje opóźnienie poniżej 1 sekundy, odpowiednie do sterowania sprzężenia zwrotnego w czasie rzeczywistym.
  - RTMP ma większe opóźnienie (około 3–10 sekund), odpowiednie do szerszej transmisji.
- Zależności sieciowe:
  - Po przełączeniu przetestuj funkcję transmisji na żywo.
  - Rozwiązuj problemy związane z zacinaniem się/rozłączaniem, sprawdzając przepustowość sieci (RTMP ma wyższe wymagania) lub blokady zapory sieciowej (WebRTC opiera się na UDP).

2.7 Status aktywacji

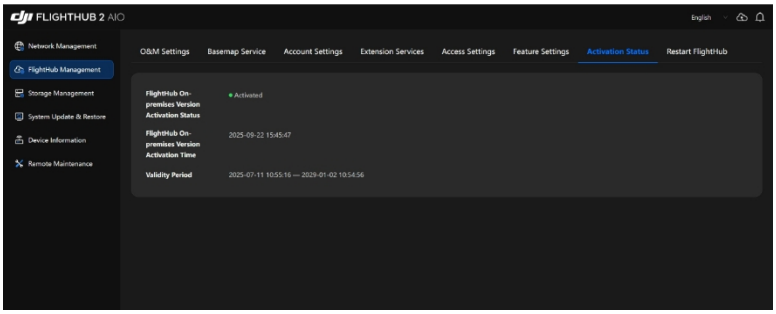
Przegląd

Ta sekcja służy do wyświetlania i zarządzania prywatnym statusem aktywacji urządzenia. Jej podstawowe funkcje to aktywacja urządzeń i sprawdzanie okresów ważności, zapewniające prawidłowe uprawnienia użytkowania systemu.

Kroki

1. Dostęp do strony stanu aktywacji

Przejdź do FlightHub Management > Status aktywacji.



2. Wyświetlać informacje dotyczące aktywacji

2.1 Status aktywacji

- Status aktywacji lokalnej wersji FlightHub: Wyświetla komunikat „Aktywowano” (zielony wskaźnik).
- Czas aktywacji lokalnej wersji FlightHub: Wyświetla konkretną datę i godzinę aktywacji.
- Okres ważności: Wyświetla okres ważności usługi aktualizacji.

2.2 Status nieaktywowany

- Status aktywacji lokalnej wersji FlightHub: Wyświetla komunikat Nieaktywna (czerwony wskaźnik) oraz link Aktywuj.
- Czas aktywacji lokalnej wersji FlightHub: Wyświetlany jest czas domyślny, który zostanie zaktualizowany po aktywacji.
- Okres ważności: Wyświetla okres ważności usługi aktualizacji.

3. Aktywuj urządzenia

Kliknij link Aktywuj, aby przejść do strony aktywacji. Szczegółowe informacje można znaleźć w instrukcji obsługi DJI FlightHub 2.

Uwaga

Zarządzanie okresem ważności: Regularnie sprawdzaj okres ważności aktualizacji. Skontaktuj się z pomocą techniczną DJI, aby odnowić licencję przed jej wygaśnięciem, aby uniknąć przerw w świadczeniu usług.

2.8 Uruchomienie ponowne FlightHub

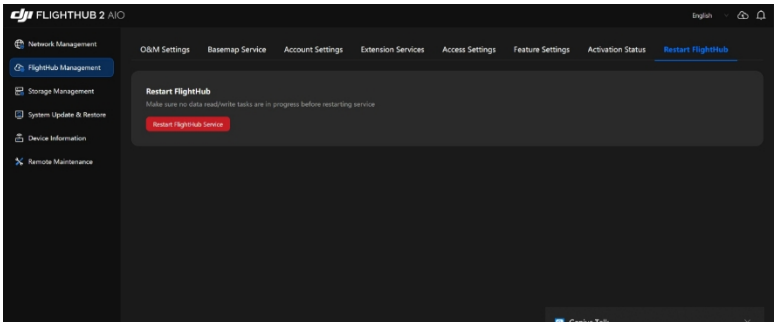
Przegląd

Ten moduł umożliwia ponowne uruchomienie usług FlightHub 2 w celu usunięcia błędów systemowych, zastosowania konfiguracji lub w innych sytuacjach związanych z konserwacją.

Kroki

1. Dostęp do interfejsu ponownego uruchamiania FlightHub

Przejdź do sekcji Zarządzanie FlightHub > Uruchom ponownie FlightHub.



2. Rozpocznij proces ponownego uruchamiania

2.1 Potwierdź status zadania

Interfejs wyświetli komunikat: „Przed ponownym uruchomieniem usługi upewnij się, że nie są wykonywane żadne zadania odczytu/zapisu danych". Należy ręcznie wstrzymać lub zakończyć wszystkie operacje przesyłania danych, pobierania kafelków map i inne zadania.

2.2 Weryfikacja hasła administratora

Kliknij przycisk „Restartuj usługę FlightHub". W wyskakującym oknie pojawi się prośba o trzykrotne wprowadzenie hasła administratora.

3. Sprawdzanie statusu ponownego uruchomienia

3.1 Ponowne uruchomienie zakończone sukcesem

- Pasek postępu zniknie. Przycisk zostanie chwilowo wyszarzony, a następnie zmieni kolor na czerwony i będzie można go ponownie kliknąć.
- Pojawi się komunikat „Usługa FlightHub została pomyślnie ponownie uruchomiona", który następnie zniknie.

3.2 Ponowne uruchomienie nie powiodło się

- Pasek postępu może utknąć lub zniknąć, wyświetlając komunikat o błędzie: „Usługa FlightHub nie została ponownie uruchomiona po wielu próbach". Skontaktuj się z lokalnym sprzedawcą lub pomocą techniczną DJI.

Uwagi

- Ochrona danych: Przed ponownym uruchomieniem należy wstrzymać wszystkie zadania odczytu/zapisu danych, aby zapobiec utracie danych.
- Spójność hasła: Wszystkie trzy hasła muszą być identyczne. Brak spójności uruchomi niepowodzenie weryfikacji i konieczność ponownego rozpoczęcia procesu weryfikacji.

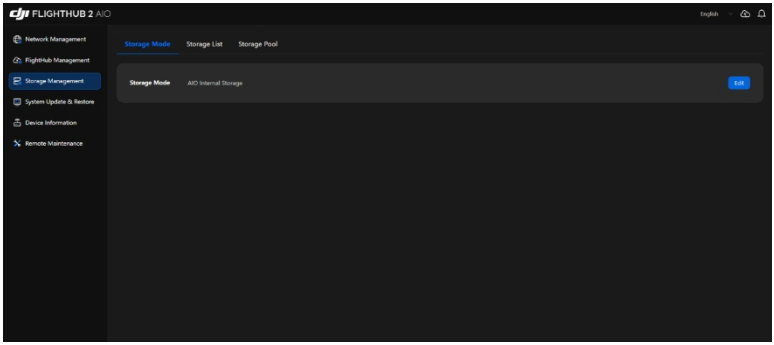
3 Zarządzanie pamięcią masową

Przegląd

Moduł ten umożliwia konfigurację wewnętrznego lub zewnętrznego typu pamięci masowej urządzenia FlightHub 2 AIO, ustawienie protokołów pamięci zewnętrznej (NFS, SMB, iSCSI) oraz monitorowanie stanu dysków wewnętrznych i macierzy RAID. Prawidłowa konfiguracja pamięci masowej ma kluczowe znaczenie

dla integralności danych i wydajności systemu.

Wejdź do interfejsu zarządzania pamięcią masową: Lewy pasek nawigacyjny> Zarządzanie pamięcią masową> wybierz zakładkę „Tryb pamięci masowej", aby otworzyć stronę operacyjną.



Konfiguracje trybu pamięci masowej

1 Wyświetlać aktualny typ pamięci

- Tryb pamięci masowej: pamięć wewnętrzna AIO, pamięć zewnętrzna
- Typ pamięci: Pamięć wewnętrzna, pamięć zewnętrzna 2

Przełącz typ pamięci

2.1 Przejdź do trybu edycji

Kliknij przycisk Edytuj w prawym górnym rogu.

2.2 Wybierz typ pamięci

Typ	Odpowiednie scenariusze i zasady
Pamięć wewnętrzna	Wykorzystuje wbudowane dyski twarde urządzenia AIO. Jest to domyślna opcja typu plug-and-play, odpowiednia dla mniejszych zestawów danych i operacji offline. Po wykonaniu tego kroku nie jest wymagana żadna dodatkowa konfiguracja poza tym krokiem.
Pamięć zewnętrzna	Umożliwia zamontowanie sieciowej pamięci masowej (NAS) przy użyciu NFS/SMB lub IP SAN przy użyciu iSCSI. Jest to odpowiednie rozwiązanie do udostępniania danych na dużą skalę i wielu urządzeniach.

2.3 Zapisz i sprawdź

- W przypadku wyboru pamięci wewnętrznej: kliknij Zapisz. System natychmiast przełączy się na pamięć wewnętrzną.
- W przypadku wyboru pamięci zewnętrznej: kliknij przycisk Zapisz. Pojawi się wyskakujące okienko z ostrzeżeniem wskazującym wykonanie kopii zapasowej danych. Po zapoznaniu się z ostrzeżeniem kliknij przycisk Przełącz. System poprowadzi Cię przez proces konfiguracji protokołu pamięci zewnętrznej.

3.1 Pamięć wewnętrzna

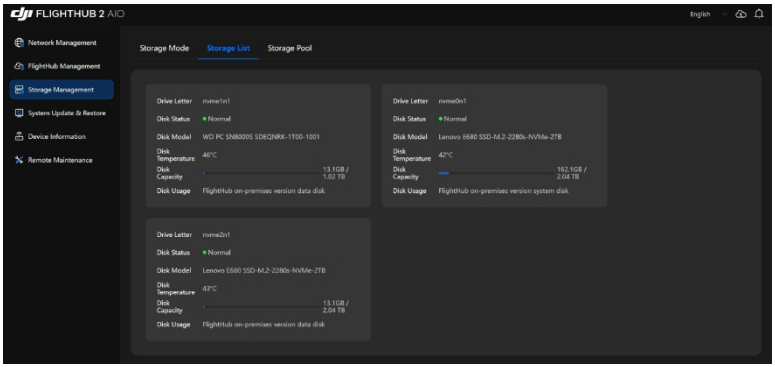
Lista pamięci wewnętrznej

W tej sekcji znajdują się szczegółowe informacje i stan kondycji każdego dysku fizycznego zainstalowanego w urządzeniu AIO. Poniżej przedstawiono konkretne kroki i instrukcje dotyczące obsługi.

1. Dostęp do listy pamięci wewnętrznej

Przejdź do opcji Zarządzanie pamięcią > Pamięć wewnętrzna. W podmenu opcji Zarządzanie pamięcią wybierz kartę Lista pamięci wewnętrznej, aby przejść do strony operacyjnej.

2. Wyświetlać informacje o dyskach pamięci



Każdy dysk jest wyświetlany w formie karty zawierającej następujące informacje:

- Podstawowe informacje o dysku
  - Nazwa dysku: identyfikator systemu (np. nvme0n1).
  - Litera dysku: Odpowiedni identyfikator dysku.
  - Model dysku: konkretny model (np. ST4000VN008).
- Informacje o stanie dysku
  - Stan dysku: zielony oznacza prawidłowy stan, a czerwony oznacza błąd. Najedź kursorem, aby wyświetlić szczegóły błędu.
  - Temperatura dysku: aktualna temperatura w stopniach Celsjusza. Jeśli temperatura wykracza poza zakres od 0°C do 55°C, wartość jest podświetlona na czerwono i wyświetlany jest komunikat ostrzegawczy.
- Informacje o pojemności dysku
  - Pojemność dysku: pokazuje pojemność używaną/całkowitą (np. 3,6 TB/4 TB).
  - Wykorzystanie dysku: opisuje wykorzystanie dysku.

3. Rozwiązywanie problemów

Objaw	Rozwiązanie
Błąd stanu dysku: Potencjalne uszkodzenie fizyczne lub nieprawidłowe działanie.	Natychmiast wykonaj kopię zapasową ważnych danych na tym dysku. Skontaktuj się z profesjonalnym technikiem w celu przeprowadzenia kontroli i W razie potrzeby wymień dysk, aby zapobiec utracie danych.

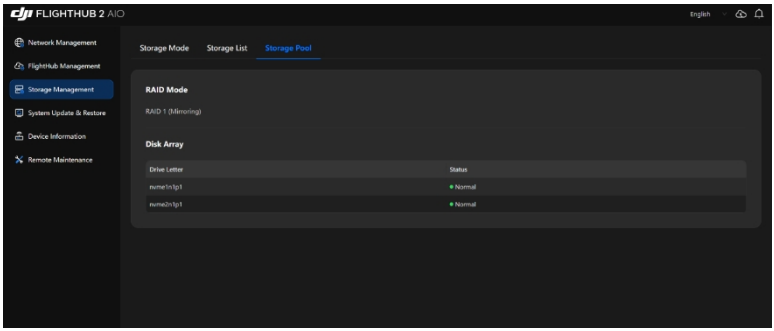
Błąd temperatury dysku: Przegrzanie może spowodować uszkodzenie dysku i utratę danych. Niskie temperatury mogą wpływać na uruchamianie.	Sprawdź system chłodzenia urządzenia, zapewnij odpowiednią wentylację, wyczyść kurz z wnętrza i sprawdź działanie wentylatora chłodzącego. W przypadku niskich temperatur przed użyciem upewnij się, że dysk znajduje się w zakresie roboczym.
Niewystarczająca pojemność dysku: Pozostała przestrzeń dyskowa jest mała (zazwyczaj poniżej 10%).	Należy usunąć niepotrzebne pliki (pliki tymczasowe, pamięć podręczną) lub przenieść dane na inne urządzenia pamięci masowej, aby zapewnić prawidłowego działania systemu.

Dzięki powyższej instrukcji obsługi można skutecznie nadzorować stan wewnętrznego dysku pamięci masowej urządzenia DJI FlightHub 2 AIO, szybko identyfikować i rozwiązywać potencjalne problemy oraz zapewnić stabilność i bezpieczeństwo przechowywania danych w urządzeniu.

Informacje o wewnętrznej puli pamięci

W tej sekcji można zarządzać konfiguracją i stanem macierzy RAID (Redundant Array of Independent Disks), obsługiwać awarie dysków oraz odtwarzać lub tworzyć nowe pule pamięci masowej.

1. Dostęp do informacji o puli pamięci masowej Przejdź do sekcji Zarządzanie pamięcią masową > Pula pamięci masowej.



2. Stany i operacje

Stan 1: Wszystko Normal (RAID 1 sprawny)	• Funkcje interfejsu: ◦ Tryb RAID: RAID 1 (dublowanie) ◦ Macierz dyskowa: Wszystkie dyski mają kolor zielony (prawidłowo). • Działanie: Regularna kontrola (co tydzień/co miesiąc). Nie wymagane żadne dodatkowe czynności.
Stan 2: Błąd pojedynczego lub podwójnego dysku (awaria dysku)	• Funkcje interfejsu: Dysk świeci się na czerwono (błąd). Pojawia się przycisk „Usuń uszkodzony dysk”. • Proces działania: Krok 1: Wyjmij uszkodzony dysk

	● Kliknij przycisk „Usuń uszkodzony dysk”, aby otworzyć instrukcję usuwania uszkodzonego dysku. ● Postępuj zgodnie z instrukcją (zapisz kroki za pomocą telefonu): Wyłącz urządzenie AIO > Otwórz pokrywę obudowy > Zdemontuj wentylator chłodzący/radiator > Wymień uszkodzony dysk twardy > Zamontuj pokrywę obudowy i włącz urządzenie AIO Krok 2: Dodaj nowy dysk (odbudowa macierzy RAID) ● Po włączeniu zasilania wróć do interfejsu informacji o puli pamięci masowej. ● Kliknij Dodaj dysk. Pojawi się okno dialogowe, a po potwierdzeniu wprowadź trzykrotnie hasło administratora. ● System rozpocznie odbudowę. Usługa FlightHub zostanie zawieszona na czas odbudowy. Krok 3: Sprawdź wyniki odbudowy ● Po zakończeniu tryb RAID zostanie przywrócony do RAID 1, wszystkie dyski będą działać prawidłowo, a pula pamięci masowej będzie dostępna. ● Tryb RAID zostanie przywrócony do RAID 1 (mirroring). ● Wszystkie dyski w macierzy dyskowej są w prawidłowym stanie, a pula pamięci masowej jest ponownie dostępna.
Stan 3: Brak stanu RAID (nie skonfigurowano/awaria macierzy)	• Funkcje interfejsu: ● Tryb RAID: Brak RAID ● Brak dostępnych danych dysku. Pojawia się przycisk Utwórz pulę pamięci masowej. • Proces operacyjny: Krok 1: Utwórz pulę pamięci masowej (RAID 1) ● Kliknij przycisk Utwórz pulę pamięci masowej. Pojawi się wyskakujące okienko z ostrzeżeniem, że dyski zostaną sformatowane i dodane do RAID 1. ● Po potwierdzeniu wprowadź trzykrotnie hasło administratora. Krok 2: Monitorowanie odbudowy puli pamięci masowej Krok 3: Sprawdzanie wyniku utworzenia ● Po zakończeniu tryb RAID wyświetla RAID 1, wszystkie Dyski działają prawidłowo, a pula pamięci masowej jest dostępna. ● Tryb RAID wyświetla RAID 1 (mirroring) ● Wszystkie dyski w macierzy dyskowej mają prawidłowy status, a pula pamięci masowej jest dostępna.
Stan 4: Stan RAID zdefiniowany przez użytkownika (konfiguracja niestandardowa)	• Funkcje interfejsu: ● Tryb RAID: RAID X (gdzie X oznacza poziom zdefiniowany przez użytkownika, np. RAID 5/10) ● Macierz dyskowa: Wszystkie dyski mają kolor zielony (prawidłowo). • Działanie: Tylko monitorowanie stanu. Za pośrednictwem tego interfejsu nie są dostępne żadne dodatkowe operacje (konfiguracja RAID jest wykonywana za pomocą w RAID jest konfigurowany za pomocą wiersza poleceń/sprzętu).

Stan 5: Stan pamięci zewnętrznej (montowanie NAS/iSCSI)	• Funkcje interfejsu: ● Tryb RAID: Zewnętrzna pamięć masowa zamontowana. ● Nie są wyświetlane żadne informacje o dyskach wewnętrznych. • Obsługa: Zarządzaj zewnętrznymi urządzeniami pamięci masowej za pomocą karty Tryb pamięci masowej.

Uwagi

- Kopia zapasowa danych: Przed wymianą dysków lub rekonstrukcją macierzy RAID należy zawsze wykonać kopię zapasową ważnych danych, aby uniknąć ich trwałej utraty w wyniku formatowania.
- Operacje sprzętowe: Wymiana dysków twardych wymaga ścisłego przestrzegania procedur wyłączania zasilania. Nieprzestrzeganie tych procedur może spowodować uszkodzenie urządzenia lub utratę danych.
- Weryfikacja hasła: Trzy wprowadzone hasła muszą być identyczne, aby można było kontynuować odbudowę lub utworzenie macierzy RAID.

3.2 Pamięć zewnętrzna

Konfiguracja protokołu pamięci zewnętrznej

1. Wybierz typ protokołu

Jeśli wybrano opcję Pamięć zewnętrzna, należy skonfigurować protokół odpowiadający zewnętrznemu urządzeniu pamięci masowej.

- NFS (sieciowy system plików)
  - Dotyczy: serwerów opartych na systemie Linux/Unix (np. FreeNAS, OpenMediaVault).
  - Konfiguracja: Wybierz wersję protokołu NFS (NFSv3/NFSv4), wprowadź adres IP serwera (adres serwera pamięci masowej) oraz docelową ścieżkę pamięci masowej (udostępniony katalog serwera).
- SMB (Server Message Block)
  - Dotyczy: serwerów Windows lub większości urządzeń NAS (np. Synology, QNAP).
  - Konfiguracja: Wybierz wersję protokołu SMB (SMBv2/SMBv3), wprowadź adres IP serwera (adres serwera pamięci masowej), ścieżkę docelową pamięci masowej (udostępniony katalog systemu Windows) oraz opcjonalnie nazwę użytkownika i hasło (jeśli wymaga tego serwer).
- iSCSI (pamięć masowa IP)
  - Dotyczy: rozwiązań pamięci masowej IP SAN (np. Dell EqualLogic, Huawei OceanStor) do wysokowydajnej pamięci masowej na poziomie bloków.
  - Konfiguracja: Wprowadź docelowy adres IP, IQN (unikalny identyfikator docelowego urządzenia, zazwyczaj skanowany), wybierz uwierzytelnianie bezpieczeństwa (jednokierunkowe CHAP/bez uwierzytelniania) i wybierz urządzenie LUN (woluminy logiczne na serwerze pamięci masowej).

Uwaga: Nie należy przełączać się między protokołami NFS i SMB w tym samym katalogu danych. Protokoły te wykorzystują różne systemy uprawnień i formaty metadanych. Bezpośrednie przełączanie może prowadzić do:

- Utrata uprawnień: SMB nie może interpretować mapowania UID/GID protokołu NFS, co może

nieprawidłowych uprawnień do plików.

- Konflikt metadanych: niespójna synchronizacja znaczników czasu między protokołami.
- Błąd usługi: Usługi FlightHub mogą nie odczytać danych z powodu niewystarczających uprawnień.

2. Sprawdź połączenie i zamontuj

2.1 Test połączenia Kliknij

przycisk Test połączenia.

- Powodzenie: Pojawi się komunikat „Połączenie nawiązane".
- Niepowodzenie: pojawi się komunikat „Połączenie nie powiodło się".
  - Sprawdź wersje protokołów, dostępność sieci (ping IP serwera) i uprawnienia.
  - Czy sieć jest dostępna (sprawdź, wysyłając ping do adresu IP serwera);
  - Czy uprawnienia są prawidłowe (nazwa użytkownika/hasło SMB, uprawnienia udostępniania NFS).

2.2 Podłącz teraz

Po pomyślnym teście połączenia kliknij opcję Zamontuj teraz. Zostaniesz poproszony o wprowadzenie hasła administratora trzykrotnie w komunikacie.

- Weryfikacja zakończona powodzeniem: system zamontuje pamięć zewnętrzną. W trybie pamięci masowej wyświetli się komunikat Pamięć zewnętrzna, a dane będą mogły być odczytywane/zapisywane.
- Weryfikacja nie powiodła się: pojawi się komunikat o niezgodności hasła. Konieczne będzie ponowne zainicjowanie procesu.

Uwagi:

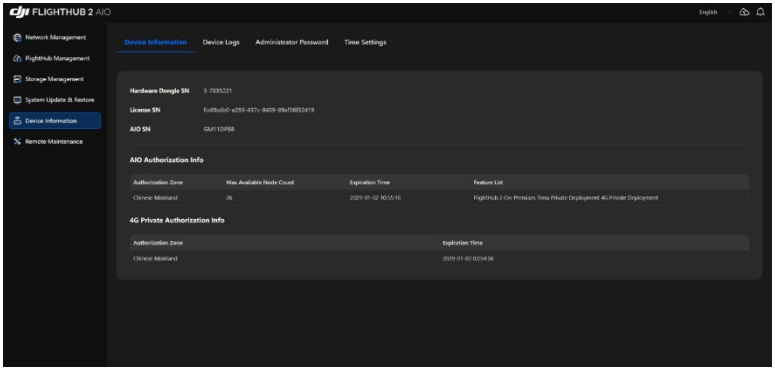
- Kopia zapasowa danych: Przed przełączeniem na pamięć zewnętrzną należy wykonać kopię zapasową danych z pamięci wewnętrznej. W przeciwnym razie po przełączeniu nie będzie można uzyskać dostępu do oryginalnych danych.
- Zgodność protokołów: NFS/SMB/iSCSI muszą dokładnie odpowiadać wersji protokołu, uprawnieniom i adresowi serwera pamięci masowej. W przeciwnym razie zamontowanie nie powiedzie się.
- Wydajność pamięci masowej: Pamięć zewnętrzna musi spełniać wymagania dotyczące przepustowości. W przeciwnym razie odczyt/zapis danych będzie przebiegał wolno.
- Szybkość pamięci masowej: Szybkość odczytu i zapisu powinna wynosić powyżej 150 MB/s. Aby uzyskać optymalną wydajność, zdecydowanie wskazuje się stosowanie dysków SSD.
- Przestrzeń dyskowa: Zaplanuj pojemność w oparciu o swoje potrzeby. Dla porównania, jeden obraz zajmuje około 10–15 MB, a jedna minuta oryginalnego filmu filmowego około 1 GB.
- Szybkość sieci: Standardem jest sieć 1000 Mb/s (1 GbE). Należy pamiętać, że jeśli operacje odczytu/zapisu współdzielą jeden port sieciowy, mogą wystąpić wąskie gardła. W razie potrzeby należy rozważyć modernizację karty sieciowej do wyższej specyfikacji.

4 Informacje o urządzeniu

W tej sekcji można wyświetlać kluczowe informacje dotyczące sprzętu i autoryzacji, zarządzać dziennikami systemowymi, aktualizować hasło administratora, synchronizować czas systemowy oraz konfigurować ustawienia zdalnej konserwacji. Funkcje te mają kluczowe znaczenie dla utrzymania zgodności urządzenia, bezpieczeństwa i integralności operacyjnej.

Przejdź do sekcji Informacje o urządzeniu. Ta karta zawiera podstawowe informacje o sprzęcie i licencjach.

Szczegóły dotyczące urządzenia FlightHub 2 AIO.



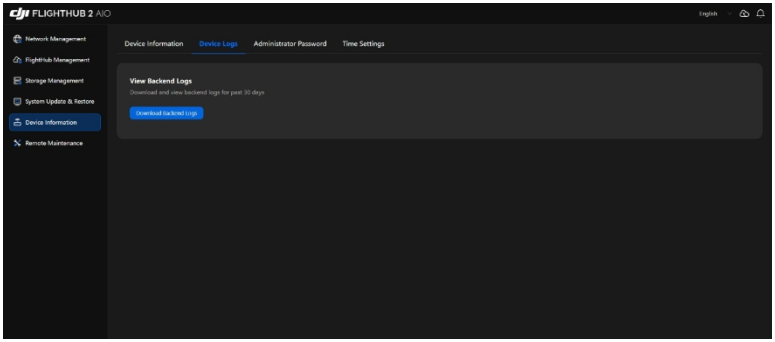
4.1 Informacje o urządzeniu

- Informacje o sprzęcie: Obejmują numer seryjny klucza sprzętowego (SN) oraz unikalny numer seryjny urządzenia AIO.
- Numer seryjny urządzenia AIO (unikalny kod wsparcia/zarządzania DJI);
- Szczegóły autoryzacji: Pokazuje limit urządzeń online, czas wygaśnięcia certyfikatu i dostępne funkcje (np. prywatne wdrożenie Terra).

Uwaga: ta sekcja służy wyłącznie do wyświetlania; nie można wprowadzać w niej żadnych bezpośrednich zmian.
Wskazać regularne sprawdzanie daty wygaśnięcia autoryzacji, aby zapewnić ciągłość działania usługi.

4.2 Dzienniki urządzenia

Przejdź do zakładki Dzienniki urządzenia.

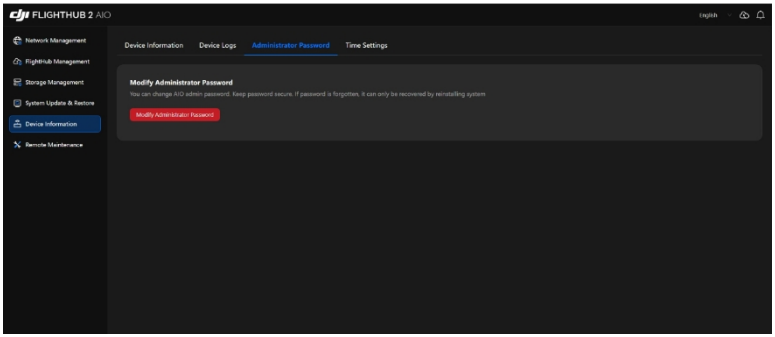


- Kliknij Pobierz dzienniki zaplecza, aby pobrać zapisy działania systemu z ostatnich 30 dni. Dzienniki te zawierają raporty o błędach i zmiany konfiguracji.

- Cel: W przypadku wystąpienia błędu urządzenia (np. nieprawidłowego działania funkcji, utraty danych) dzienniki te mają kluczowe znaczenie dla pomocy technicznej DJI w diagnozowaniu i rozwiązywaniu problemów.

4.3 Hasło administratora

Przejdź do zakładki Hasło administratora:



Proces zmiany hasła

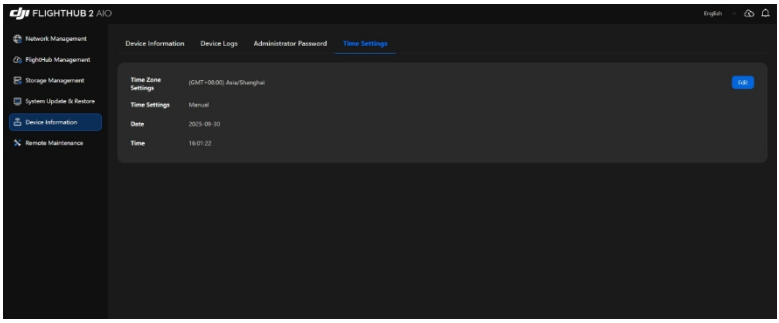
1. Kliknij opcję Modyfikuj hasło administratora. Pojawi się okno podręczne.
2. Wprowadź swoje oryginalne hasło (aktualne hasło administratora).
3. Wprowadź nowe hasło. Nowe hasło musi mieć co najmniej 12 znaków i zawierać kombinację wielkich liter, małych liter, cyfr i znaków specjalnych (np. Admin@2025).
4. Potwierdź nowe hasło, wprowadzając je ponownie.
5. Kliknij OK. Nowe hasło zacznie obowiązywać natychmiast po pomyślnej weryfikacji. Jeśli hasła nie będą się zgadzać lub nie będą spełniać wymagań dotyczących złożoności, pojawi się komunikat o błędzie.

Uwagi

- Utrata hasła: Jeśli zapomnisz hasła administratora, konieczne będzie zresetowanie systemu. Zapoznaj się z instrukcją odzyskiwania systemu i pamiętaj, aby przed przystąpieniem do tej czynności wykonać kopię zapasową wszystkich danych.
- Regularne zmiany: W celu zwiększenia bezpieczeństwa zdecydowanie zaleca się regularną zmianę hasła administratora (np. co kwartał lub co pół roku).

4.4 Ustawienia czasu

Przejdź do zakładki Ustawienia czasu, która obsługuje ręczną regulację czasu lub automatyczną synchronizację NTP.



Ręczne ustawianie czasu

1. Kliknij przycisk Edytuj. Wybierz żądaną strefę czasową.
2. Ustaw opcję Ustawienia czasu na Ręczne. Wprowadź prawidłową datę i godzinę.
3. Kliknij Aktualizuj teraz. Czas systemowy zostanie natychmiast zastąpiony ręcznie wprowadzonymi danymi.

Automatyczna synchronizacja NTP

1. Ustaw opcję Czas na Synchronizuj z serwerem NTP.
2. Wprowadź adres serwera (domyślnie pool.ntp.org lub adres NTP intranetu Twojej firmy).
3. Wprowadź port serwera (domyślnie 8080, upewnij się, że jest zgodny z portem serwera NTP).
4. Kliknij przycisk „Aktualizuj teraz”. System spróbuje połączyć się z serwerem NTP.
   - Powodzenie: pojawi się zielone okienko „Czas zaktualizowany pomyślnie”.
   - Niepowodzenie: pojawi się czerwone okienko „Aktualizacja czasu nie powiodła się”. Sprawdź połączenie sieciowe oraz adres/port serwera NTP.

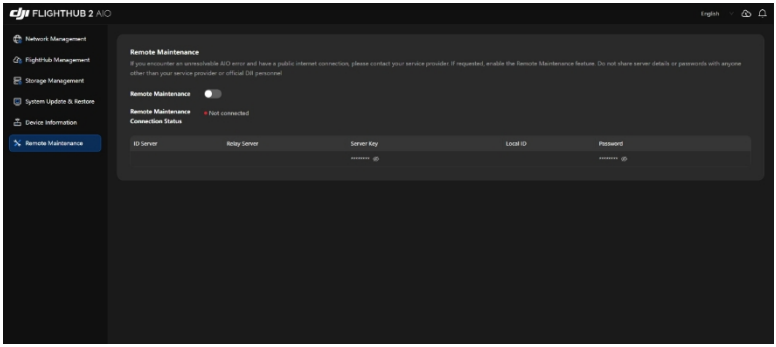
5 Informacje o urządzeniu

5.1 Przegląd

Moduł zdalnej konserwacji umożliwia działowi pomocy technicznej DJI zdalny dostęp do urządzenia AIO w celu diagnostyki i rozwiązywania problemów.

5.2 Przejście do zdalnej konserwacji

Przejdź do sekcji Zdalna konserwacja, która zawiera przełącznik zdalnej konserwacji, informacje o serwerze i wyświetlacz stanu.



5.3 Podstawowe funkcje

1.1 Przełącznik zdalnej obsługi i konserwacji

- Kliknij przycisk zdalnej konserwacji.
  - Kolor niebieski oznacza, że funkcja jest włączona: urządzenie AIO wyświetli informacje o połączeniu (adres IP serwera, hasło) dla pomocy technicznej DJI w celu nawiązania połączenia zdalnego.
  - Kolor szary oznacza wyłączenie: informacje o serwerze są ukryte, a kanał połączenia zdalnego jest zamknięty.
- Uwaga: Urządzenia AIO muszą być podłączone do sieci publicznej, aby można było przeprowadzić zdalną konserwację.

1.2 Informacje o serwerze

Ta sekcja jest widoczna tylko wtedy, gdy włączona jest zdalna konserwacja. Zawiera ona niezbędne dane uwierzytelniające dla pomocy technicznej DJI.

- Wyświetlane treści:
  - Adres IP serwera (np. 24.202.45.26);
  - Hasło serwera (domyślnie ukryte; kliknij ikonę oka, aby wyświetlać/ukryć)
  - Identyfikator sprawy, hasło lokalne (dane uwierzytelniające dla pomocy technicznej w celu weryfikacji urządzenia).
- Czynności:
  - Podaj adres IP serwera, hasło i identyfikator sprawy do pomocy technicznej DJI. Zawsze ponownie potwierdź tożsamość agenta pomocy technicznej za pośrednictwem zaufanego kanału (np.
    telefonicznie lub oficjalnym e-mailem) przed udostępnieniem tych poufnych informacji.
  - Ostrzeżenie dotyczące bezpieczeństwa: Nie należy ujawniać hasła, chyba że jest to absolutnie konieczne. Po zakończeniu sesji rozwiązywania problemów natychmiast wyłącz przełącznik zdalnej konserwacji, aby zabezpieczyć urządzenie.

1.3 Wyświetlanie statusu

W dolnej części strony wyświetlany jest status połączenia zdalnej konserwacji:

- Niepołączone (szare): Kanał zdalny nie został ustanowiony (normalne czuwanie).
- Łączenie (niebieski): Pomoc techniczna DJI aktywnie próbuje nawiązać połączenie.
- Połączono (zielony): Nawiązano sesję zdalną.

5.4 Uwagi

- Należy zachować szczególną ostrożność podczas samodzielnej obsługi urządzenia w trakcie sesji, ponieważ dział pomocy technicznej może również mieć dostęp do systemu.
- Poufność: Hasło serwera i identyfikator sprawy są przeznaczone wyłącznie dla pomocy technicznej DJI. Nigdy nie ujawniaj ich osobom nieuprawnionym.
- Identyfikowalność operacji: Podczas zdalnego połączenia wskazać należy wykonywanie zrzutów ekranu lub rejestrowanie wszelkich ważnych zmian konfiguracji (np. modyfikacji trybu przechowywania) w celu wykorzystania ich w przyszłości i identyfikacji usterek.

UPROSZCZONA DEKLARACJA ZGODNOŚCI UE

SZ DJI Technology Co., Ltd niniejszym oświadcza, że typ urządzenia radiowego [DJI FlightHub 2 AIO] jest zgodny z dyrektywą 2014/53/UE. Pełny tekst deklaracji zgodności UE jest dostępny pod następującym adresem internetowym: https://files.innpro.pl/dji

Adres producenta: Lobby of T2, DJI Sky City, No. 53 Xianyuan Road, Xili Community, Xili Street, Nanshan District, Shenzhen, Chiny

Dane dot. częstotliwości:

2.4GHz
2400-2483,5 MHz

5GHz:
5150-5350 MHz & 5470-5725 MHz

WIFI 6:
Pasma 2,4G i 5G
2,4G: od 2400 MHz do 2483,5 MHz
5G: 5150-5350 MHz & 5470-5725 MHz oraz od 5725 do 5850 MHz

Maks. moc częstotliwości radiowej: <20 dBm

Ochrona środowiska

Zużyty sprzęt elektroniczny oznakowany zgodnie z dyrektywą Unii Europejskiej, nie może być umieszczany łącznie z innymi odpadami komunalnymi. Podlega on selektywnej zbiórce i recyklingowi w wyznaczonych punktach. Zapewniając jego prawidłowe usuwanie, zapobiegasz potencjalnym, negatywnym konsekwencjom dla środowiska naturalnego i zdrowia ludzkiego. System zbierania zużytego sprzętu zgodny jest z lokalnie obowiązującymi przepisami ochrony środowiska dotyczącymi usuwania odpadów. Szczegółowe informacje na ten temat można uzyskać w urzędzie miejskim, zakładzie oczyszczania lub sklepie, w którym produkt został zakupiony.

Produkt spełnia wymagania dyrektyw tzw. Nowego Podejścia Unii Europejskiej (UE), dotyczą-cych zagadnień związanych z bezpieczeństwem użytkowania, ochroną zdrowia i ochroną środo-wiska, określających zagrożenia, które powinny zostać wykryte i wyeliminowane.

Niniejszy dokument jest tłumaczeniem oryginalnej instrukcji obsługi, stworzonej przez produ-centa.

Szczegółowe informacje o warunkach gwarancji dystrybutora / producenta dostępne na stronie internetowej https://serwis.innpro.pl/gwarancja

Importer: INNPRO

INNPRO Robert Błędowski sp. z o.o.
Rudzka 65c
44-200 Rybnik, Polska
tel. +48 533 234 303
hurt@innpro.pl
www.innpro.pl

Podmiot odpowiedzialny w UE:
DJI Europe B.V.
LA 2992
24569 Barendrecht,
Holandia
dealer.nl@dji.com