Hanwha Vision

AIBox

Instrukcja obsługi

AIB-800A
AIB-800

CE

AIBox
Instrukcja obsługi

WAŻNE ZALECENIA DOTYCZĄCE BEZPIECZEŃSTWA

Przed rozpoczęciem eksploatacji urządzenia należy uważnie przeczytać niniejsze instrukcje dotyczące obsługi.

Należy przestrzegać poniższych instrukcji bezpieczeństwa.

Niniejszą instrukcję obsługi należy zachować do użycia w przyszłości.

1) Przeczytać tę instrukcję.
2) Zachować instrukcję.
3) Zwrócić uwagę na wszystkie ostrzeżenia.
4) Przestrzegać wszystkich instrukcji.
5) Nie używać urządzenia w pobliżu wody.
6) Zabrudzoną powierzchnię produktu wyczyść miękką, suchą szmatką lub wilgotną szmatką.
(Nie używaj żadnych detergentów ani produktów kosmetycznych zawierających alkohol, rozpuszczalniki, surfaktanty lub substancje oleiste, ponieważ mogą one spowodować odkształcenie lub uszkodzenie produktu).
7) Nie zasłaniać otworów wentylacyjnych; zamontować zgodnie z instrukcjami producenta.
8) Nie montować w pobliżu źródeł ciepła, takich jak grzejniki, promienniki, piece lub inne urządzenia (również wzmacniacze) wytwarzające ciepło.
9) W żadnym wypadku nie próbować obchodzić zabezpieczeń konstrukcyjnych wtyczki i gniazda z bolcem uziemiającym. Wtyczka ma dwa bolce i otwór na bolec uziemiającym. Bolec uziemiający chroni przed porażeniem prądem elektrycznym. W celu zapewnienia bezpieczeństwa urządzenie wyposażono we wtyczką ze stykiem uziemiającym. Jeśli wtyczka dołączona do urządzenia nie pasuje do gniazdka, należy zwrócić się do elektryka celem wymiany przestarzałego gniazdka ściennego.
10) Zabezpieczyć przewód sieciowy, tak aby nie być przydeptywany ani ściskany; szczególną uwagę należy zwrócić na wtyczki, rozgałęźniki i miejsce, w których przewód wychodzi z urządzenia.
11) Używać wyłącznie elementów wyposażenia/akcesoriów zalecanych przez producenta.
12) Urządzenie umieszczać tylko na wózku, stojaku, trójnogu, półce lub stole zalecanym przez producenta lub sprzedawanym razem z urządzeniem. W przypadku użycia wózka podczas przemieszczania zestawu wózekurządzenie należy zachować ostrożność, aby uniknąć obrażeń spowodowanych jego wywróceniem.

13) W czasie burzy z wyładowaniami atmosferycznymi lub w przypadku nieużywania urządzenia przez dłuższy czas należy odłączyć urządzenie od zasilania.
14) Wszelkie czynności serwisowe należy powierzyć wykwalifikowanym pracownikom serwisu.
W przypadku uszkodzenia urządzenia w jakikolwiek sposób, np. w razie uszkodzenia przewodu zasilającego lub wtyczki, rozlania płynu lub upadku przedmiotów na urządzenie, wystawiania urządzenia na działanie deszczu lub wilgoci, nieprawidłowości w działaniu lub upadku urządzenia, należy oddać urządzenie do serwisu.

INFORMACJE NA TEMAT INSTRUKCJI OBSŁUGI

Niniejszy dokument zawiera instrukcje dotyczące produktu AIBox. Przed rozpoczęciem korzystania z produktu należy uważnie przeczytać niniejszą instrukcję.

- Niniejszy dokument objaśnia, jak używać produktu w oparciu o jego domyślne ustawienia oraz domyślne ekrany.
- Informacje zawarte w niniejszej instrukcji mogą się różnić w zależności od aktualizacji oprogramowania produktu oraz naszych zasad i mogą ulec zmianie bez powiadomienia użytkownika.

INFORMACJE NA TEMAT GRUPY DOCELOWEJ

Niniejsza instrukcja zawiera informacje przeznaczone dla użytkowników AIBox.

INFORMACJE NA TEMAT UŻYTKOWANIA PRODUKTU

Użytkownicy tego produktu mogą wykonywać następujące działania:

- Monitoring w czasie rzeczywistym nagrań wideo z kamer zarejestrowanych w AIBox
- Wysyłanie danych wideo, metadanych AI i BestShot do urządzeń podłączonych do AIBox

Przed użyciem tego produktu należy upewnić się, że zainstalowana jest najnowsza wersja oprogramowania. Najnowszą wersję oprogramowania można sprawdzić i pobrać na stronie internetowej firmy Hanwha Vision (www.HanwhaVision.com).

SPIS TREŚCI

INFORMACJE OGÓLNE 3

3 Ważne zalecenia dotyczące bezpieczeństwa
3 Informacje na temat instrukcji obsługi
3 Informacje na temat grupy docelowej
3 Informacje na temat użytkowania produktu
4 Spis treści

URUCHAMIANIE PRZEGLĄDARKI WEB VIEWER 5

5 Co to jest Web Viewer?
5 Wymagania systemowe
5 Sprawdzanie adresu IP
5 Ustawianie hasła
6 Podłączenie Web Viewera

PRZEGLĄDARKA NA ŻYWO 7

7 Rozkład ekranu przeglądarki na żywo

KONFIGURACJA PRZEGLĄDARKI 8

8 Rozkład ekranu konfiguracji przeglądarki
8 Konfiguracja kamery
- 8 Konfiguracja kanału
- 11 Informacje o profilu
- 11 Hasło kamery

12 Konfiguracja zdarzenia
- 12 Konfiguracja reguły zdarzenia
- 13 Wejście alarmowe
- 13 Harmonogram
- 13 MQTT

15 Konfiguracja sieci
- 15 IP & Port
- 17 DDNS
- 18 Filtr IP
- 18 HTTPS
- 19 802.1x
- 19 FTP
- 20 E-MAIL
- 20 SNMP
- 21 Zarządzanie certyfikatem

22 Konfiguracja systemu
- 22 Data / godzina / język
- 22 Użytkownik
- 23 Zarządzanie systemem
- 24 Zaloguj się

25 Konfiguracja otwartych platform
- 25 Otwórz platformę

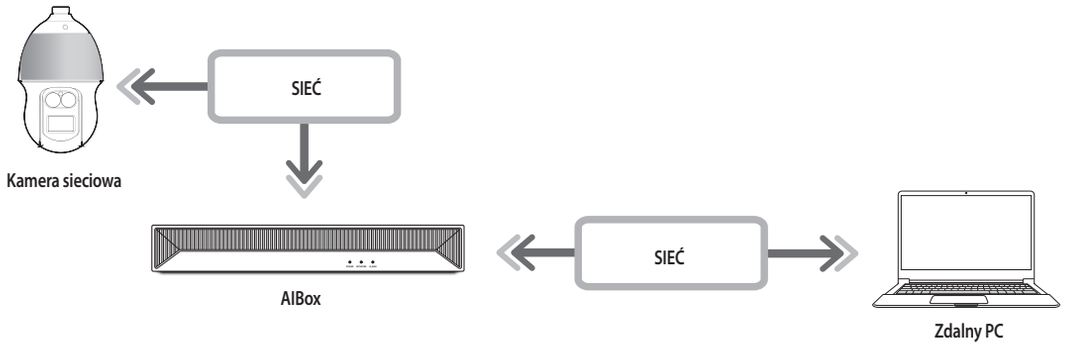
DODATEK 26

26 Rozwiązywanie problemów

uruchamianie przeglądarki web viewer

CO TO JEST WEB VIEWER?

Web Viewer to oprogramowanie, które pozwala na zdalny dostęp do urządzeń poprzez przeglądarkę na komputerze PC w celu monitorowania lub konfiguracji w czasie rzeczywistym.



WYMAGANIA SYSTEMOWE

Lista poniżej podaje zalecenia minimalne dla sprzętu i systemu operacyjnego potrzebnego do korzystania z Web Viewera.

- Korzystać z przeglądarki zalecanej przez system operacyjny.
  Np. przeglądarka zalecana przez Microsoft: Microsoft Edge
- Obsługiwane przeglądarki: Chrome, Edge, oraz Safari
- Obsługiwane OS: działa we wszystkich środowiskach Windows, Linux i OS X, biorąc pod uwagę niezależny od platformy charakter sieci.
- Przetestowane środowiska: testowano i certyfikowano do pracy na systemie Windows® 10 z przeglądarką Edge 117, Google Chrome™ 117, z procesorem Intel® Core™ i7-7700 3,60 Ghz i kartą graficzną NVIDIA® GeForce® GTX™ 1050 lub Intel™ HD Graphics 630.
- Ograniczenia wydajności: wydajność CPU/GPU użytkowników może mieć wpływ na wydajność odtwarzania wideo przeglądarki Web Viewer.
  Podczas oglądania wideo H.265 w Chrome, jakość wideo może ulec pogorszeniu w zależności od ustawień takich jak wysoka rozdzielczość czy prędkość przesyłu.

SPRAWDZANIE ADRESU IP

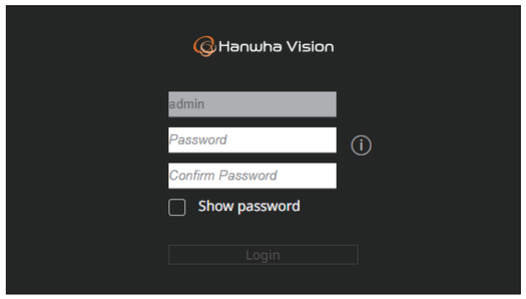
Adres IP AIBox umożliwiający dostęp do Web Viewera można sprawdzić w „Wisenet Device Manager".
Program "Wisenet Device Manager" można zainstalować, wchodząc na stronę internetową firmy Hanwha Vision (www.HanwhaVision.com) i pobierając go z menu „**Support** > **Online Tool**".

1. Uruchom program „Wisenet Device Manager".
2. Kliknij przycisk <**Search**>, aby wyświetlić połączone urządzenia.
3. Sprawdź adres IP AIBox na liście.

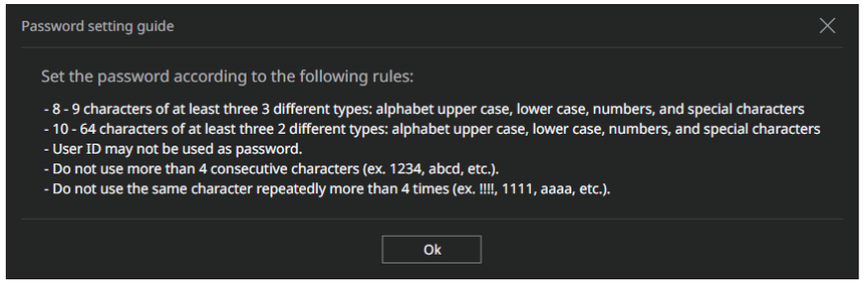
USTAWIANIE HASŁA

Przy pierwszym dostępie do Web Viewera lub po przywróceniu ustawień fabrycznych należy ustawić hasło do AIBox.

1. Otwórz przeglądarkę internetową i w pasku adresowym wprowadź adres IP AIBox.
2. Wprowadź hasło do konta administratora i kliknij przycisk <**Login**>.



3. Kliknij przycisk < ⓘ >, aby wyświetlić podstawowy przewodnik dotyczący ustawiania hasła. Zapoznaj się z zasadami ustawienia hasła.

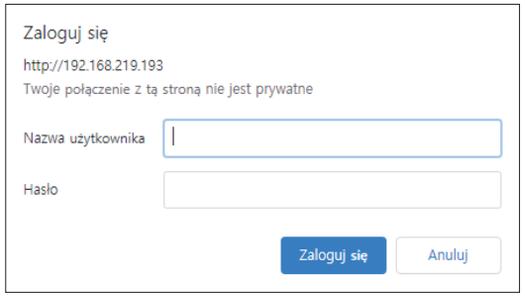


■ Hasło należy zapamiętać lub zapisać, aby go nie stracić.

uruchamianie przeglądarki web viewer

PODŁĄCZENIE WEB VIEWERA

1. Otwórz przeglądarkę internetową i w pasku adresowym wprowadź adres IP AIBox. Pojawi się okno <**Zaloguj się**>.
2. Wprowadź <**Nazwę użytkownika**> i <**Hasło**>, po czym kliknij przycisk <**Zaloguj się**>.
   - Nazwa użytkownika: wprowadź „admin”.
   - Hasło: wprowadź ustawione hasło.



3. Po zalogowaniu pojawi się ekran główny przeglądarki na żywo.

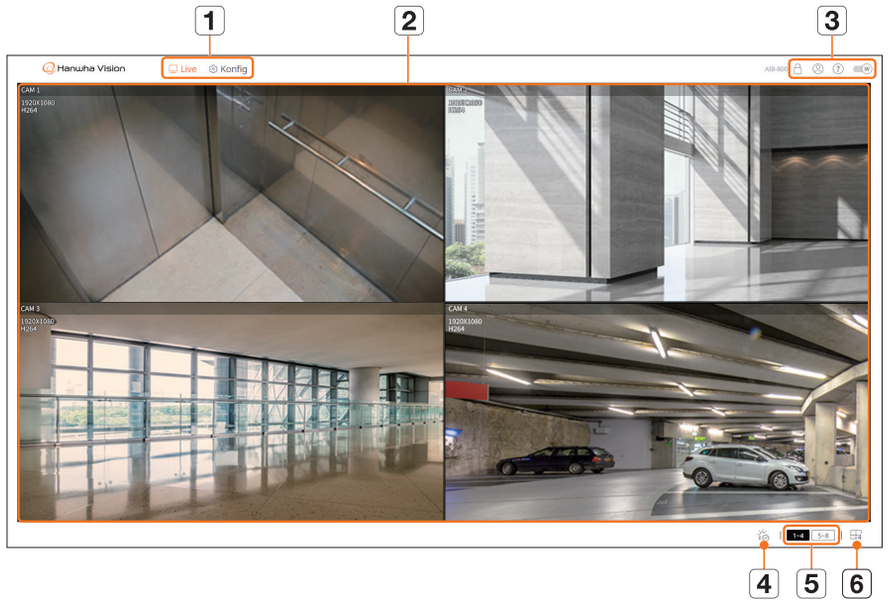
- Wszystkie ustawienia są stosowane zgodnie z ustawieniami AIBox.
- Po zmianie portu WWW podczas łączenia z Web Viewerem dostęp może zakończyć się niepowodzeniem, ponieważ port może być zablokowany. W takiej sytuacji zmień port na inny.
- W celu zapewnienia ochrony danych osobowych i nie dopuszczenia do kradzieży danych hasło należy zmieniać co trzy miesiące. Pamiętaj, że odpowiedzialność za bezpieczeństwo i wszelkie szkody wynikające z braku dbałości o hasło ponosi użytkownik.

- Hasło administratora można zmienić w menu „**Konfig** > **System** > **Użytkownik**”.

przeglądarka na żywo

Pozwala oglądać obraz wideo z kamer zarejestrowanych w AIBox.

ROZKŁAD EKRANU PRZEGLĄDARKI NA ŻYWO



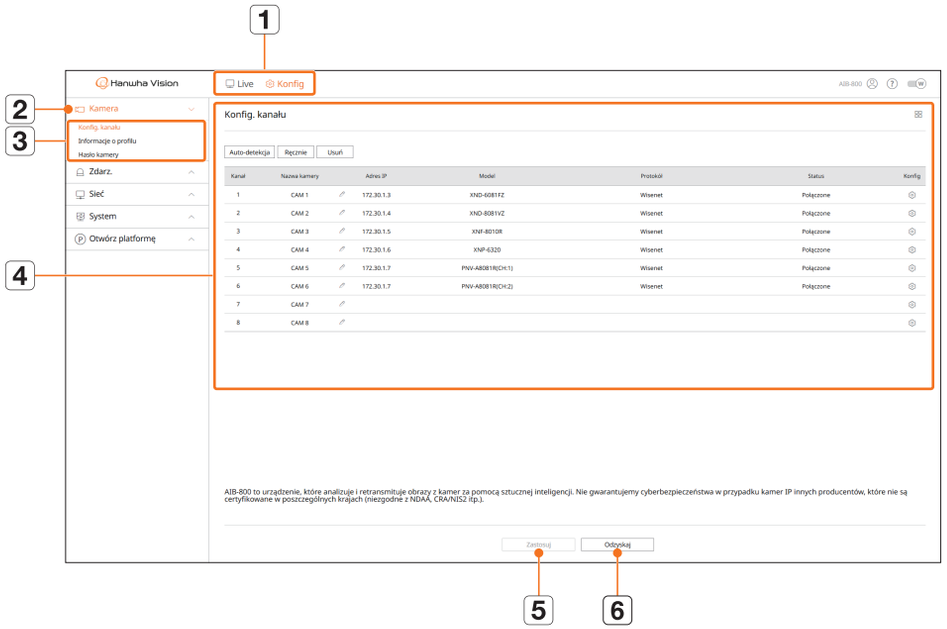
Menu		Opis
1	**Menu**	Kliknięcie każdego menu powoduje przejście do odpowiedniego ekranu menu.
2	**Okno wideo**	Wyświetla obraz wideo z kamer połączonych z AIBox. • Aby przełączyć widok na pojedynczy ekran, kliknij dwukrotnie żądane wideo na podzielonym ekranie wideo. Dwukrotne kliknięcie wideo na pojedynczym ekranie spowoduje ponowne wyświetlenie ekranu podzielonego.
3		Wyświetla adres IP i status wspólnego uwierzytelnienia przeglądarki odbierającej sygnały wideo z AIBox. • : połączenie ze wspólnym uwierzytelnieniem z wykorzystaniem certyfikatu urządzenia WISENET. • : połączenie ze wspólnym uwierzytelnieniem bez korzystania z certyfikatu urządzenia WISENET. • – : połączenie bez wzajemnego uwierzytelnienia. • Brak podłączonej przeglądarki: z AIBox nie jest połączona żadna przeglądarka.
		Pojawia się ID połączonego użytkownika.
		Połączenie bezpośrednio ze stroną internetową firmy Hanwha Vision (www.HanwhaVision.com).
	W	Zmienia motyw kolorów Web Viewera.

Menu		Opis
4		Zatrzymuje alarm lub sygnał dźwiękowy w przypadku wystąpienia zdarzenia lub zmiany stanu systemu.
5	1~4 5~8	Wybrany kanał jest widoczny w oknie wideo.
6		Wybrany podzielony ekran zostanie zastosowany do okna wideo. • : wyświetla kanały od 1 do 8 na jednym ekranie. • : wyświetla kanały od 1 do 4 oraz od 5 do 8 na ekranie podzielonym na 4.

konfiguracja przeglądarki

Pozwala konfigurować ustawienia kamer, zdarzeń, sieci, systemów i otwartych platform.

ROZKŁAD EKRANU KONFIGURACJI PRZEGLĄDARKI



Pozycja		Opis
1	**Menu**	Kliknij menu, aby przejść do odpowiedniego ekranu menu.
2	**Lista menu nadrzędnych**	Skonfiguruj ustawienia lub wybierz element nadrzędny, aby zmienić istniejące ustawienia.
3	**Lista menu podrzędnych**	Wybierz element ustawień z menu podrzędnego wybranego menu nadrzędnego.
4	**Menu szczegółowe**	Kliknij pole wejścia elementu, aby zmienić i wprowadzić odpowiednią wartość.
5	**Zastosuj**	Zastosuje zmodyfikowane ustawienia.
6	**Odzyskaj**	Odzyskuje ustawienia używane przed zmianą.

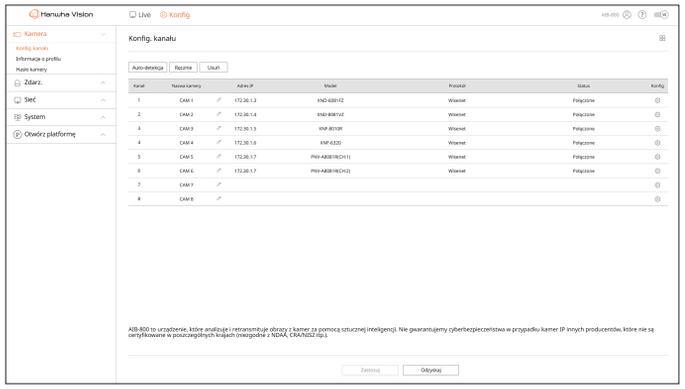
KONFIGURACJA KAMERY

Skonfigurować można ustawienia kanałów, profili i haseł kamer.

Konfiguracja kanału

Możesz zarejestrować kamerę sieciową dla każdego kanału i połączenia pomiędzy nimi.

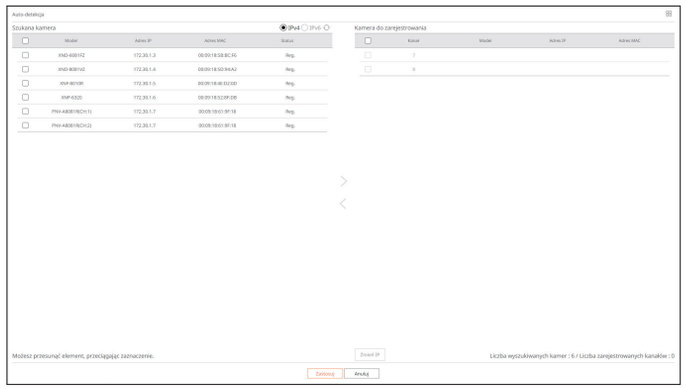
Konfig. > Kamera > Konfig. kanału



- : wyświetla kamery w danym kanale w postaci listy lub miniatur.
  - Kamera wyszukiwana w ONVIF nie umożliwia podglądów.
- Nazwa kamery: wyświetla nazwę kamery. Kliknij przycisk < >, aby zmienić nazwę kamery.
  - Można wprowadzić do 15 znaków ze spacjami.
- Adres IP: wyświetla adres IP kamery sieciowej.
- Model: wyświetla nazwę modelu kamery.
- Protokół: wyświetla informacje o protokole zarejestrowanej kamery sieciowej.
- Status: wyświetla status połączenia.
- Konfig.: kliknij przycisk < >, aby zmienić informacje o połączeniu kamery.

- Jeśli nie możesz zarejestrować kamery po zainicjowaniu systemu, sprawdź ustawienia sieci. Po zainicjowaniu systemu i zresetowaniu ustawień sieci, przepust sieci kamery jest inny niż przepust sieci produktu, więc rejestracja kamery jest niemożliwa.

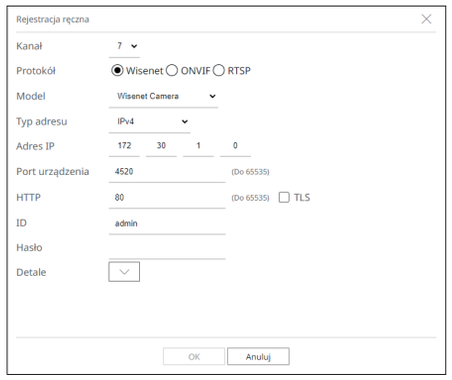
Automatyczna rejestracja kamer sieciowych



1. Kliknij przycisk <**Auto-detekcja**> w polu <**Konfig. kanału**>.
   Pojawi się okno <**Auto-detekcja**>.
2. Wybierz kamerę do zarejestrowania na liście <**Szukana kamera**> i kliknij przycisk >.
   Wybraną kamerę można sprawdzić na liście <**Kamera do zarejestrowania**>.
   - W przypadku ponownego wyszukiwania kamery lub jeżeli adres IP to stary adres IP, który nie został przypisany przez serwer DHCP (np. 192.168.1.100), kliknij przycisk < ↻ >, aby sprawdzić, czy został on przypisany, czy nie.
   - Opcja <**Status**> wyświetla status uwierzytelnienia kamery. W przypadku wystąpienia stanu <**Niepow. uw.**> kliknij przycisk < ✎ >, aby wprowadzić ID kamery i hasło.
   - Kliknij nagłówek u góry listy, aby posortować listę ponownie według wybranego nagłówka.
3. Aby zmienić adres IP kamery, wybierz żądaną kamerę z listy <**Kamera do zarejestrowania**> i naciśnij przycisk <**Zmień IP**>.
4. Kliknij przycisk <**Zastosuj**>, aby zarejestrować wybraną kamerę.

- Aby zmienić ID kamery i hasło w Web Viewerze, o ile kamera jest już zarejestrowana w AIBox, zmień ID i hasło na takie same jak dla kamery.
- Jeżeli stan kamery to przywrócenie ustawień fabrycznych, kamera domyślnie przyjmuje ID i hasło ustawione w menu „**Konfig.** > **Kamera** > **Hasło kamery**”.
- Jeśli ustawiono już ID i hasło kamery, należy użyć tych samych wartości, które ustawiono w menu „**Konfig.** > **Kamera** > **Hasło kamery**”. (maks. 3 zestawy)
- Kamera Wisenet jest zarejestrowana za pomocą protokołu Wisenet, podczas gdy kamera innej firmy zarejestrowana jest za pomocą protokołu ONVIF.

Ręczna rejestracja kamer sieciowych



1. Kliknij przycisk <**Ręcznie**> w polu <**Konfig. kanału**>.
   Pojawi się okno <**Rejestracja ręczna**>.
2. Wybierz kanał oraz protokół wykorzystywany przez kamerę.
   Wprowadzane dane mogą się różnić zależnie od wybranego protokołu.
   - Wisenet: można użyć protokołu kamery Wisenet.
   - ONVIF: oznacza, że kamera obsługuje protokół ONVIF. Podłączając kamerę, która nie występuje na liście, należy wybrać <**ONVIF**>.

     - Gdy kamera jest zarejestrowana za pomocą ONVIF, jeżeli różnica w czasie systemowym między kamerą a AIBox wynosi 2 minuty lub więcej, rejestracja nie jest możliwa. W takim wypadku należy zsynchronizować godzinę w kamerze i AIBox.

   - RTSP: jeden z protokołów „Real Time Streaming Protocol (RTSP)” do strumieniowania w czasie rzeczywistym, zgodny z RFC 2326.
3. Jeśli wybierze się opcję <**Wisenet**>, należy ustawić następujące elementy.
   - Model: wybierz model kamery.
     – Nieznane: tę opcję należy wybrać, gdy nie można zidentyfikować modelu kamery.
     – Wisenet Camera: możliwa jest rejestracja kamer marki Hanwha Vision.
     – Wisenet Multi-Channel: możliwa jest rejestracja kamer wielokierunkowych lub kamer wieloobiektywowych marki Hanwha Vision. Kamera wielokanałowa to kamera z wieloma modułami w jednym korpusie. Automatyczna rejestracja kamer w AIBox umożliwia zarejestrowanie wielu kanałów jednocześnie. Jeśli jednak chcesz ją zarejestrować ręcznie, należy zarejestrować jeden kanał na raz.
   - Typ adresu: wybierz format adresu połączeniowego kamery.
     - Obsługiwany typ adresu może się różnić w zależności od typu podłączonego produktu.
     – IPv4/IPv6: wykorzystywany do bezpośredniego wprowadzania adresu IP kamery.
     – Wisenet DDNS: dostępny tylko wtedy, gdy kamera jest zarejestrowana przez serwer Wisenet DDNS (ddns.hanwhasecurity.com). Podaj zarejestrowaną domenę DDNS ID.
     Np. w przypadku https://ddns.hanwha-security.com/snb5000, jako Wisenet DDNS wprowadź „snb5000”.
     – URL: służy do wprowadzania adresu URL.

- Specyfikacje DDNS każdej kamery można sprawdzić w instrukcji użytkownika odpowiedniej kamery.

- Adres IP: wpisz adres IP kamery.
- Port urządzenia: wprowadź port urządzenia kamery.
  - W zależności od typu kamery niektóre porty urządzenia mogą nie być obsługiwane.
- HTTP/HTTPS: wprowadź port HTTP/HTTPS kamery.
  - Jeśli TLS jest włączony, można ustawić port HTTPS.
- TLS: zaznacz, aby używać zabezpieczenia TLS (Transport Layer Security).
- ID: podaj ID rejestrowanej kamery.
- Hasło: wprowadź hasło rejestrowanej kamery.
- Detale: kliknij przycisk < ⌄ >, aby wybrać metodę strumieniowania.
  - Tryb przesyłania strumieniowego: TCP, UDP, HTTP, Multicast

4. Jeśli wybierze się opcję <**ONVIF**>, należy ustawić następujące elementy.

- Typ adresu: wybierz format adresu połączeniowego kamery.
- Adres IP: pozwala wprowadzić adres IP kamery.
- HTTP/HTTPS: wprowadź port HTTP/HTTPS kamery.
  - Jeśli TLS jest włączony, można ustawić port HTTPS.
- TLS: zaznacz, aby używać zabezpieczenia TLS (Transport Layer Security).
- Kanał: wprowadź kanał, w którym kamera ma być zarejestrowana.
- ID: wprowadź ID kamery.
- Hasło: wprowadź hasło kamery.
- Detale: Kliknij przycisk < ⌄ >, aby wybrać tryb uwierzytelniania i metodę strumieniowania.
  - Tryb uwierzytelniania: Token nazwy użytkownika, Skrót
  - Tryb przesyłania strumieniowego: TCP, UDP, HTTP

5. Jeśli wybierze się opcję <**RTSP**>, należy ustawić następujące elementy.

- URL: wprowadź swój adres RTSP. Więcej informacji można znaleźć w instrukcji użytkownika kamery.
- ID: wprowadź ID kamery.
- Hasło: wprowadź hasło kamery.
- Detale: kliknij przycisk < ⌄ >, aby wybrać metodę strumieniowania.
  - Tryb przesyłania strumieniowego: TCP, UDP, HTTP, HTTPS

- W sekcji <**Detale**> można wybrać tryb przesyłania strumieniowego spośród następujących:
  - TCP: połączenie z kamerą sieciową działa w trybie „RTP przez TCP".
  - UDP: połączenie z kamerą sieciową działa w trybie „RTP przez UDP".
  - HTTP: połączenie z kamerą sieciową działa w trybie „RTP przez TCP (HTTP)".
  - HTTPS: połączenie z kamerą sieciową działa w trybie „RTP przez TCP (HTTPS)".
  - Multicast: można efektywnie wykorzystać przepustowość sieci, wysyłając ten sam strumień wideo do wielu użytkowników w tym samym czasie.
    Zarówno AIBox, jak i kamera muszą obsługiwać Multicast.
- Po wybraniu protokołu ONVIF można wybrać tryb uwierzytelniania w <**Detale**>.
  - Token nazwy użytkownika: ta metoda uwierzytelniania wykorzystuje identyfikator użytkownika i hasło. Uwierzytelnianie może się nie powieść, jeśli synchronizacja czasu między urządzeniami nie działa.
  - Skrót: ta metoda uwierzytelniania jest używana w protokole HTTP i jest zalecana w przypadku korzystania z protokołu ONVIF.

Aby sprawdzić szczegóły błędów rejestracji kamery

Jeżeli rejestracja kamery nie powiodła się, wyświetlony zostanie powód.

- **Połączenie nie powiodło się z nieznanego powodu.** : taki komunikat pojawia się, gdy kamera nie została zarejestrowana ze względu na nieznany status połączenia.
- **Odłączony ze względu na zablokownie kamery.** : komunikat pojawia się po pięciokrotnym wprowadzeniu błędnego ID / hasła konta kamery.
  Spróbuj zalogować się ponownie po 30 sekundach. Jeżeli ten komunikat pojawia się nadal, należy sprawdzić, czy ktoś nie próbuje uzyskać dostępu do kamery z zewnątrz.
- **Połączenie udane.** : taki komunikat pojawia się, gdy kamera jest podłączona poprawnie.
- **Informacje o modelu są niepraw. Wpisz prawidł. nazw modelu.** : taki komunikat pojawia się, gdy informacja o modelu podana przy rejestracji kamery nie jest poprawna.
- **Login nie zweryfikowany.** : taki komunikat pojawia się, gdy ID lub hasło podane przy rejestracji kamery nie jest poprawne.
- **Połączenie zerwane z powodu maks. liczby użytkowników.** : taki komunikat pojawia się, gdy liczba jednoczesnych użytkowników przekracza górny limit.
- **Połączenie nienawiązane - niepr. port HTTP.** : taki komunikat pojawia się, gdy port HTTP kamery jest niepoprawny.
- **Połączenie nie nawiązane. Nieznany błąd połączenia.** : taki komunikat pojawia się, gdy kamera nie połączyła się ze względu na nieznany błąd.
- **Zmiana modelu użytkownika** : jeśli użytkownik ustawił model na <**Wisenet Camera**>, podczas rejestrowania nowej kamery zostaje ona nazwana zgodnie domyślną nazwą urządzenia. W przypadku problemu z automatyczną rejestracją użytkownik może zmienić nazwę modelu kamery, którą chce zarejestrować.

Edycja profilu kamery

Więcej informacji na temat zmiany profilu znajduje się na stronie „**Podgląd ustawień** > **Ustawianie kamery** > **Informacje o profilu**".

- W przypadku kamer, jeśli zastosowano tylko jeden profil, szybkość klatek jest stała i zgodna z profilem. Jeśli występuje wiele profili, szybkość klatek wytwarzanego strumienia wideo nie jest gwarantowana. Na przykład jeśli występują 2 profile 30 fps, kamera może przesyłać strumienie z prędkością 20 fps.

Usuwanie kamery sieciowej

1. Kliknij przycisk <**Usuń**> w polu <**Konfig. kanału**>.

2. Po wyświetleniu okna usunięcia wybierz kanał kamery do usunięcia.

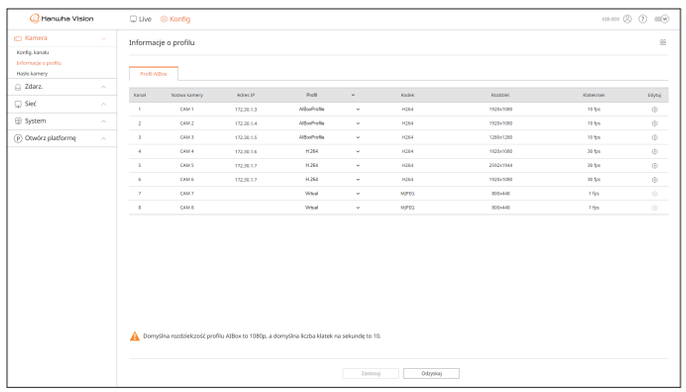
- Aby wybrać kamery dla wszystkich kanałów, kliknij przycisk <**Wszystkie kanały**>.

3. Aby usunąć kamerę z wybranego kanału, kliknij przycisk <**OK**>.

Informacje o profilu

Można wybrać profil do analizy zdarzeń AI, a wybrany profil jest wyświetlany w AIBox Live Viewer.

Konfig. > Kamera > Informacje o profilu



■ Można skonfigurować ustawienia tylko dla profili obsługiwanych przez kamerę.

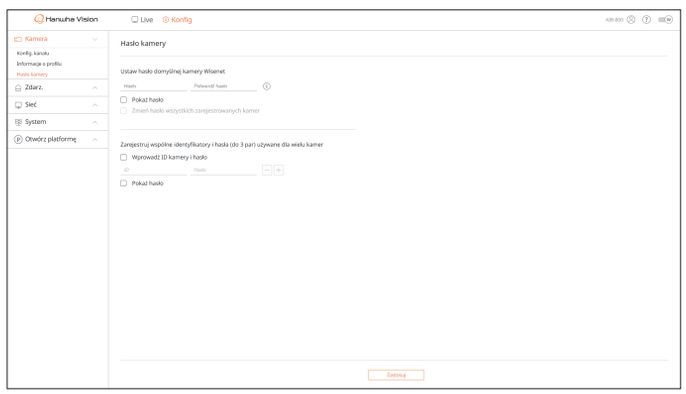
- : wyświetla kamery w danym kanale w postaci listy lub miniatur.
- Nazwa kamery: wyświetla nazwę kamery.
- Adres IP: wyświetla adres IP kamery sieciowej.
- Profil: można wybrać profil dla wybranego kanału.
- Kodek: wyświetla kodek wybranego kanału.
- Rozdziel.: wyświetla rozdzielczość wybranego kanału.
- Klatek/sek: wyświetla szybkość klatek wybranego profilu.
- Edytuj: po kliknięciu przycisku < > w Web Viewerze wybranej kamery, możliwe jest dodawanie, usuwanie i modyfikowanie profilu wideo.

Hasło kamery

Istnieje możliwość jednoczesnej zmiany haseł wszystkich zarejestrowanych kamer.

Można zarejestrować ID i hasło kamery.

Konfig. > Kamera > Hasło kamery



- Hasło: wprowadź nowe hasło zgodne z zasadami tworzenia haseł jako ustawienie fabryczne. Należy wprowadzić hasło początkowe kamery.
- Potwierdź hasło: wprowadź hasło ponownie.
- ID: wprowadź ID kamery, której ID i hasło są ustawione.
- Hasło: wprowadź hasło kamery, której ID i hasło są ustawione.

■ Gdy hasło jest przywracane do ustawień fabrycznych, można je zmieniać i zarządzać nimi partiami.
■ Po kliknięciu przycisku < ⓘ > zostanie wyświetlony domyślny przewodnik dotyczący ustawiania hasła.
■ Po zaznaczeniu opcji <**Pokaż hasło**> bieżące hasło zostanie wyświetlone jako rzeczywiste wprowadzone znaki.
■ Po zaznaczeniu opcji <**Zmień hasło wszystkich zarejestrowanych kamer**> hasła wszystkich kamer zostaną zmienione na wprowadzone hasło.
■ Można zarejestrować maksymalnie 3 zestawy ID kamery z hasłem.
ID kamery i hasło pozwala automatycznie wyszukiwać kamery w celu rejestracji na ekranie „**Konfig. kanału** > **Auto-detekcja**”.
■ Hasła kamery zarejestrowanej za pośrednictwem protokołu ONVIF nie można zmienić.

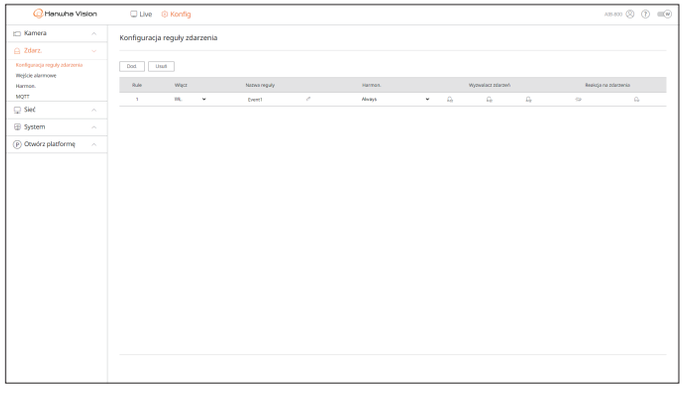
KONFIGURACJA ZDARZENIA

Pozwala konfigurować ustawienia dotyczące zdarzeń, na przykład włączyć lub wyłączyć wykrywanie zdarzeń dla poszczególnych kanałów lub sygnalizację alarmów.

Konfiguracja reguły zdarzenia

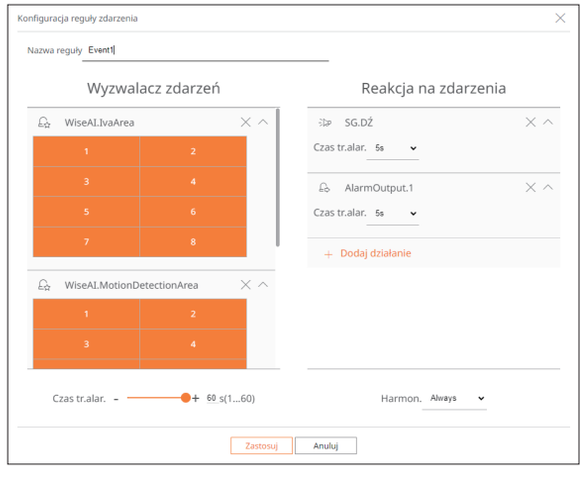
Pozwala ustawić wyzwalacz zdarzeń i regułę działania w taki sposób, aby w razie wystąpienia zdarzenia sygnalizowany był alarm.

Konfig. > Zdarz. > Konfiguracja reguły zdarzenia



- Dod.: aby dodać regułę zdarzenia, wybierz przycisk <**Stwórz regułę**> lub <**Skopiuj regułę**>.
- Usuń: usuwanie wybranej reguły zdarzenia.
- Włącz: wybierz, czy dana reguła zdarzenia ma być włączona, czy wyłączona.
- Nazwa reguły: wyświetla nazwę reguły zdarzenia. Nazwę reguły zdarzenia można zmienić, klikając przycisk < ✎ >.
- Harmon.: pozwala zmienić harmonogram ustawiony w regule zdarzenia.
- Wyzwalacz zdarzeń: pozwala zmienić wyzwalacz zdarzeń ustawiony w regule zdarzenia.
  - Wyświetlane pozycje wyzwalacza zdarzeń mogą się różnić w zależności od zdarzeń, które mogą wystąpić w aplikacji AI (WiseAI lub otwartej aplikacji) zainstalowanej dla każdego kanału.
  - W przypadku wybrania wyzwalacza zdarzenia <**OpenSDKAppStatus.WiseAI**> jako <**Inactive**>, zatrzymanie aplikacji zostanie wykryte jako zdarzenie. Zdarzenie można potwierdzić za pomocą żądanej akcji zdarzenia.
- Reakcja na zdarzenia: pozwala zmienić reakcję na zdarzenia ustawioną w regule zdarzenia.
  - AlarmOutput (Wyjście alarmu), Sg.dź, FTP, MQTT, E-MAIL

Rejestrowanie nowej reguły zdarzenia

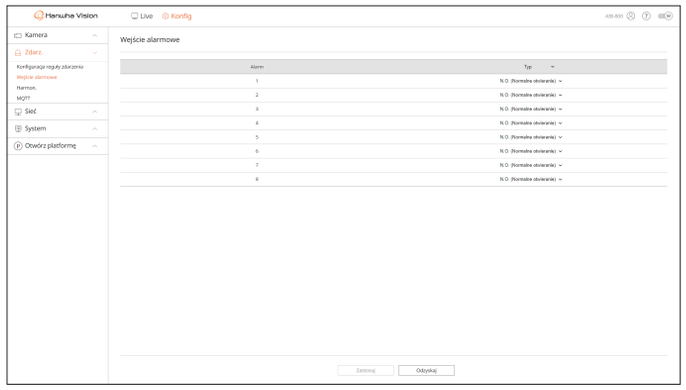


1. Kliknij przycisk <**Dod.**> w polu <**Konfiguracja reguły zdarzenia**>.
2. Kliknij <**Stwórz regułę**>.
   - Skopiuj regułę: wybierz stworzoną regułę zdarzenia, którą chcesz dodać do listy zdarzeń. Klikając przycisk < ✎ > możesz zmienić nazwę reguły.
3. Jeśli pojawi się okno <**Konfiguracja reguły zdarzenia**>, skonfiguruj w nim detale.
   - Nazwa reguły: pozwala wprowadzić nazwę reguły zdarzenia.
   - Wyzwalacz zdarzeń: aby ustawić wyzwalacz zdarzeń oraz kanał, kliknij przycisk <**+ Dodaj wyzwalacz**>.
     - Można dodać maksymalnie trzy wyzwalacze zdarzeń.
     - Czas wykonania oznacza czas oczekiwania na rozpoznanie wystąpienia wybranego zdarzenia. Wybierz wiele wyzwalaczy zdarzeń dla celów konfiguracji.
       Reakcja na zdarzenia uruchamia się tylko wówczas, gdy wszystkie wybrane wyzwalacze zdarzeń wystąpią w czasie wykonania.
     - Aby wybrać kanał do wykrywania wyzwalacza zdarzeń, kliknij lub przeciągnij wybrany kanał w tabeli kanałów. Wybrany kanał będzie wyświetlany na pomarańczowo.
   - Reakcja na zdarzenia: aby ustawić reakcję na zdarzenia, kliknij przycisk <**+ Dodaj działanie**>.
     - AlarmOutput (Wyjście alarmu): wybór portu wyjściowego alarmu i konfiguracja czasu wykonania alarmu.
     - Sg.dź: po wystąpieniu zdarzenia zabrzmi sygnał dźwiękowy.
     - FTP: w przypadku wystąpienia zdarzenia obraz zostanie wysłany przez skonfigurowany serwer FTP.
     - MQTT: w razie wystąpienia zdarzenia wysłany zostanie komunikat MQTT.
     - E-MAIL: konfiguracja użytkowników, którzy będą otrzymywali powiadomienie e-mail, gdy wystąpi zdarzenie.
       - Odbiorcę na wypadek zdarzenia można ustawić w menu „**Konfig.** > **Sieć** > **E-MAIL**".
     - Reakcja na zdarzenia będzie uruchamiana tylko wówczas, gdy wystąpią wszystkie ustawione wyzwalacze zdarzeń. Jeśli wystąpi tylko jedno spośród wielu ustawiony zdarzeń, reakcja na zdarzenia nie zostanie uruchomiona.
     - Reakcję na zdarzenia należy ustawiać tylko w razie konieczności.
   - Harmon.: wybór harmonogramu uruchamiania reakcję na zdarzenia.
4. Kliknij przycisk <**Zastosuj**>, aby zarejestrować regułę zdarzenia.

Wejście alarmowe

Pozwala skonfigurować obsługę czujnika alarmowego.

Konfig. > Zdarz. > Wejście alarmowe

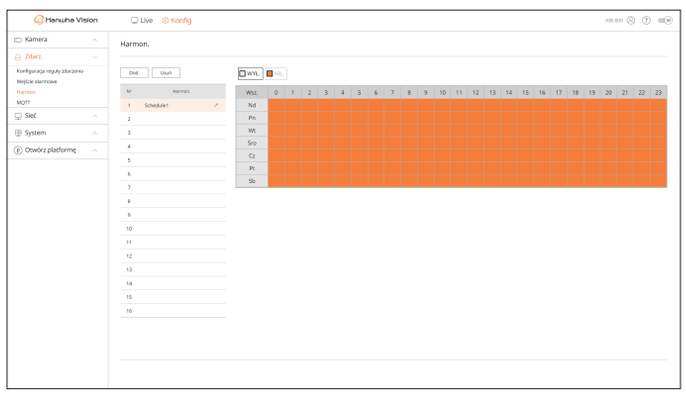


- Typ: wybór trybu włączania czujnika alarmowego.
  - N.O. (Normalne otwieranie): czujnik jest zawsze otwarty. Jeżeli czujnik zostanie zamknięty, pojawi się alarm.
  - N.C. (Normalne zamykanie): czujnik jest zawsze zamknięty. Jeżeli czujnik zostanie otwarty, pojawi się alarm.
  - Wyłącz: czujnik alarmu jest wyłączony. Alarm jest nieużywany.

Harmonogram

Podczas ustawiania reguły zdarzenia można ustawić czas działania reakcji na zdarzenia.

Konfig. > Zdarz. > Harmon.



- Dod.: dodawanie harmonogramu poprzez ustawienie żądanej daty i godziny.
  - WYŁ.: wyświetlane na biało. Alarm nie jest sygnalizowany, nawet jeśli wystąpi zdarzenie.
  - WŁ.: wyświetlane na pomarańczowo. Alarm jest sygnalizowany tylko w przypadku wystąpienia zdarzenia.
    - Aby zmienić nazwę harmonogramu, kliknij przycisk < >.
- Usuń: usunięcie wybranego harmonogramu.

- Nie można usunąć używanego harmonogramu.

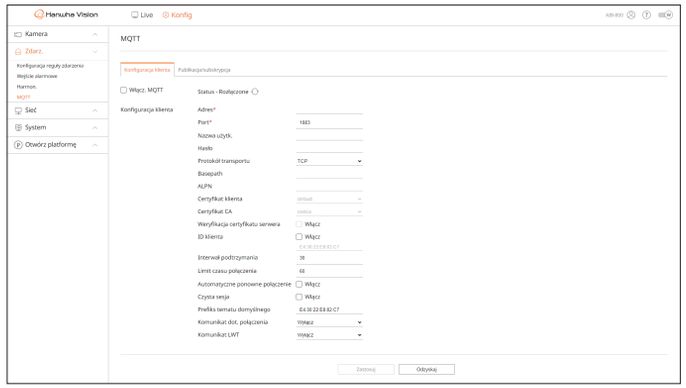
MQTT

MQTT (Message Queueing Telemetry Transport) to protokół przesyłania komunikatów oparty na publikacji/subskrypcji.
Ze względu na to, że został zaprojektowany do przesyłania lekkich wiadomości, wymaga niewielkiej przestrzeni kodowej lub minimalnej przepustowości sieci, aby połączyć zdalne urządzenia. Ponadto umożliwia łatwą wymianę danych z wieloma urządzeniami.

Ustawianie klienta

Pozwala ustawić informacje o kliencie MQTT i wprowadzić informacje o brokerze MQTT, z którym mają łączyć się klienci AIBox. Broker MQTT otrzymuje od klienta deklaracje subskrypcji komunikatów dotyczących określonych tematów i przekazuje je dalej.

Konfig. > Zdarz. > MQTT > Konfiguracja klienta



- Włącz. MQTT: jeśli zaznaczone, ustawiony broker jest połączony.
  - Kliknij przycisk < >, aby zaktualizować status połączenia z brokerem.
- Adres: wprowadź domenę i adres IP brokera. To pole jest wymagane.
- Port: wprowadź numer portu, przez który nastąpi połączenie z brokerem. To pole jest wymagane.
- Nazwa użytk.: wprowadź ID klienta.
- Hasło: wprowadź hasło klienta.
- Protokół transportu: wybierz jedną z opcji: TCP, TLS, WebSocket lub WebSocketSecure.
- Basepath: konfiguracja jest dozwolona, gdy włączony jest protokół WebSocket i WebSocketSecure. Adres URL brokera ostatecznego to Adres:port/ścieżka bazowa.
- ALPN: wprowadź ALPN obsługiwany przez brokera. Konfiguracja jest dozwolona, gdy włączony jest protokół TLS lub WebSocket.
- Certyfikat klienta: wybór jednego z certyfikatów klienta zainstalowanych w AIBox. Konfiguracja jest dozwolona, gdy włączony jest protokół TLS lub WebSocket.
  Certyfikaty można dodawać w menu „**Sieć** > **Zarządzanie certyfikatem** > **Certyfikat klienta**”.
- Certyfikat CA: wybór jednego z certyfikatów CA zainstalowanych w AIBox. Konfiguracja jest dozwolona, gdy włączony jest protokół TLS lub WebSocket.
  Certyfikaty można dodawać w menu „**Sieć** > **Zarządzanie certyfikatem** > **Certyfikat CA**”.

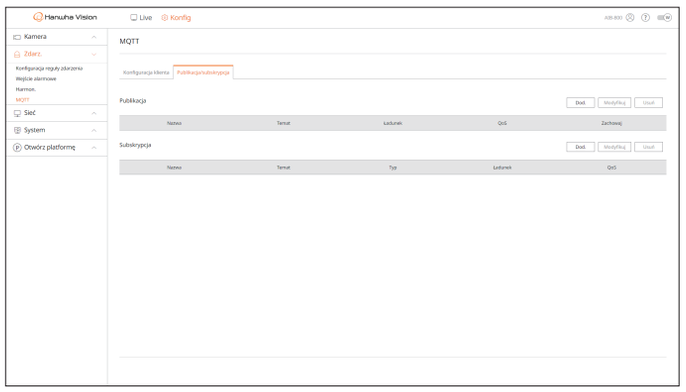
- Weryfikacja certyfikatu serwera: gdy włączony jest protokół TLS lub WebSocket, zaznacz opcję <**Włącz**>, aby wyświetlić certyfikat serwera.
- ID klienta: gdy broker jest podłączony, używany jest ID klienta zdefiniowany przez użytkownika. Zaznacz opcję <**Włącz**> i wprowadź pożądany ID. W przeciwnym razie nastąpi połączenie z losowym ID.
- Interwał podtrzymania: co zadany czas sprawdza, czy broker jest połączony. Czas wprowadź w sekundach.
- Limit czasu połączenia: w przypadku braku odpowiedzi od brokera w zadanym czasie broker zostaje rozłączony. Czas wprowadź w sekundach i ustaw wartość większą niż <**Interwał podtrzymania**>.
- Automatyczne ponowne połączenie: zaznacz opcję <**Włącz**>, aby co minutę następowała automatyczna próba nawiązania połączenia z brokerem.
- Czysta sesja: zaznacz opcję <**Włącz**>, aby po nawiązaniu połączenia między klientem a brokerem usunąć wszystkie informacje (np. ID klienta, komunikaty) pozostałe z poprzedniej sesji.
  Jeśli opcja nie zostanie zaznaczona, informacje z poprzedniej sesji będą zachowane.
  Na przykład, po ponownym połączeniu sesji, klient może odbierać komunikaty na dany temat bez subskrypcji tematu poprzedniej sesji.
- Prefiks tematu domyślnego: gdy ustawiony jest prefiks tematu domyślnego, ostateczny temat jest tworzony przez połączenie prefiksu tematu domyślnego i tematu komunikatu. W przypadku dodatkowego publikowania MQTT można ustawić, czy ma być używany prefiks tematu domyślnego.
- Komunikat dot. połączenia: komunikat ten jest wysyłany przez klienta do brokera po nawiązaniu połączenia. Komunikaty można dodawać w menu „**Zdarz.** > **MQTT** > **Publikacja/subskrypcja** > **Publikacja**”.
- Komunikat LWT: komunikat LWT (Last Will and Testament) jest deklarowany z wyprzedzeniem, aby broker mógł wysłać ustawiony komunikat do określonego tematu, gdy klient zostanie odłączony od brokera. Komunikaty można dodawać w menu „**Zdarz.** > **MQTT** > **Publikacja/subskrypcja** > **Publikacja**”.

Konfiguracja publikacji/subskrypcji

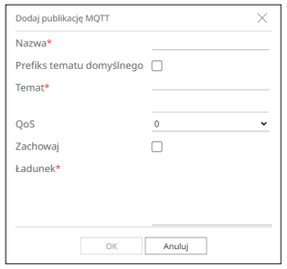
Istnieje możliwość dodawania, modyfikowania lub usuwania komunikatów publikacji i subskrypcji, aby klient MQTT mógł publikować i subskrybować komunikaty dotyczące określonych tematów za pośrednictwem protokołu MQTT.

Gdy wydawca publikuje temat i komunikaty w brokerze, broker dostarcza temat subskrybentom, a subskrybenci subskrybują komunikaty na ten temat. Każdy klient może być wydawcą lub subskrybentem, ponieważ nie jest to określone.

Konfig. > Zdarz. > MQTT > Publikacja/subskrypcja

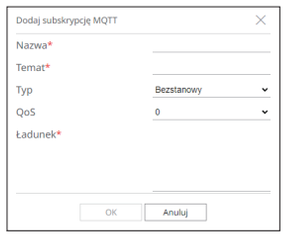


Dodawanie publikacji MQTT



1. W menu Publikacja kliknij przycisk <**Dod.**>. Pojawi się okno <**Dodaj publikację MQTT**>.
   - Nazwa: wprowadź nazwę komunikatu do opublikowania.
   - Prefiks tematu domyślnego: zaznacz, aby przy publikacji komunikatów uwzględniać ustawiony prefiks tematu domyślnego. W tym przypadku prefiks tematu domyślnego jest wysyłany w połączeniu z tematem publikacji.
     Np. jeśli prefiks tematu domyślnego to „AIBox”, a temat publikacji to „połączenie”, wysyłany jest komunikat „AIBox/połączenie”.
   - Temat: wprowadź temat publikacji.
   - QoS (Quality of Service): wybierz pożądany poziom dla publikacji MQTT.
     – 0: nie są podejmowane żadne dodatkowe kroki dla klienta i brokera w celu sprawdzenia otrzymanych elementów i udzielenia odpowiedzi klientowi, gdy klient wysyła komunikaty wraz z tematem, więc nie ma gwarancji rezultatów.
     – 1: wysyłanie tego samego tematu i komunikatu wielokrotnie, aż klient, który wysłał temat i komunikat, otrzyma potwierdzenie jego otrzymania od brokera.
     – 2: gwarantowane jest, że broker otrzyma ten sam temat i komunikaty tylko jeden raz poprzez uzgodnienie między klientem a brokerem.
   - Zachowaj: zaznacz, jeśli chcesz, aby broker przechowywał opublikowane komunikaty i później przesyłał je do nowych subskrybentów tematu.
   - Ładunek: wprowadź zawartość komunikatu do opublikowania.
2. Kliknij przycisk <**OK**>, aby go uzupełnić.
   - Aby zmodyfikować informacje o publikacji MQTT, zaznacz żądane elementy i kliknij przycisk <**Modyfikuj**>.
   - Aby usunąć informacje o publikacji MQTT, zaznacz żądane elementy i kliknij przycisk <**Usuń**>.

Dodawanie subskrypcji MQTT



1. W menu Subskrypcja kliknij przycisk <**Dod.**>. Pojawi się okno <**Dodaj subskrypcję MQTT**>.
   - Nazwa: wprowadź nazwę komunikatu do zasubskrybowania.
   - Temat: wprowadź temat do zasubskrybowania.
   - Typ: wybierz typ subskrypcji.
     - Bezstanowy: konwertuje komunikat MQTT na komunikat bezstanowy.
     - Stanowy: konwertuje komunikat MQTT na warunek. Jako stan używany jest ładunek.
   - QoS (Quality of Service): wybierz pożądany poziom dla subskrypcji MQTT.
     - 0: nie są podejmowane żadne dodatkowe kroki dla klienta i brokera w celu sprawdzenia otrzymanych elementów i udzielenia odpowiedzi klientowi, gdy klient wysyła temat, więc nie ma gwarancji rezultatów.
     - 1: wysyłanie tego samego tematu wielokrotnie, aż klient, który wysłał temat, otrzyma potwierdzenie jego otrzymania od brokera.
     - 2: gwarantowane jest, że broker otrzyma ten sam temat tylko jeden raz poprzez uzgodnienie między klientem a brokerem.
   - Ładunek: wprowadź zawartość komunikatu do zasubskrybowania.
2. Kliknij przycisk <**OK**>, aby go uzupełnić.
   - Aby zmodyfikować informacje o subskrypcji MQTT, zaznacz żądane elementy i kliknij przycisk <**Modyfikuj**>.
   - Aby usunąć informacje o subskrypcji MQTT, zaznacz żądane elementy i kliknij przycisk <**Usuń**>.

KONFIGURACJA SIECI

Użytkownik może ustawić różne funkcje sieci, takie jak monitorowanie wideo na żywo poprzez połączenie z siecią z poziomu lokalizacji zdalnej i otrzymywanie zdarzeń pocztą elektroniczną.

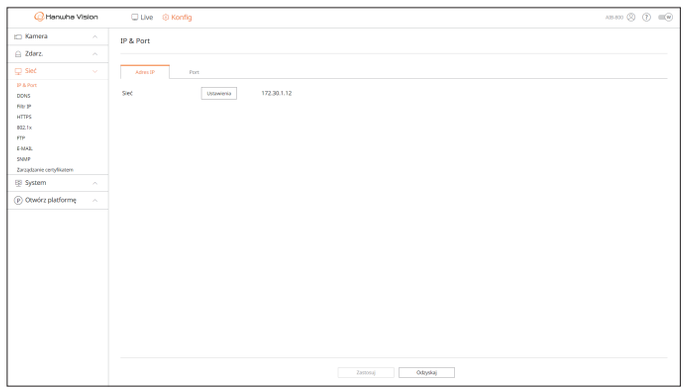
IP & Port

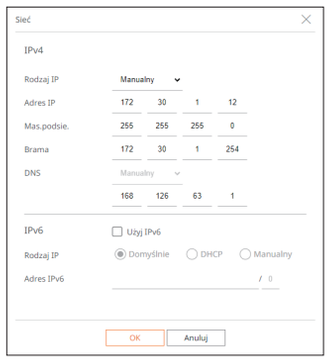
Możesz ustawić drogę połączenia sieciowego oraz protokół.

Konfiguracja połączenia sieciowego

Ustawia protokół i środowisko sieciowe.

Konfig. > Sieć > IP & Port > Adres IP





- Ustawienia: pozwala zmieniać ustawienia sieciowe.
- Sieć: daje dostęp do Web Viewera przy użyciu informacji o sieci.
  - Rodzaj IP: Wybierz typ dostępu do sieci.
    - Manualny: adres IP, maskę podsieci, bramę i DNS można wprowadzić bezpośrednio.
    - DHCP: adres IP, maska podsieci i brama mogą być ustawione automatycznie.
      Wartość DNS można wprowadzić bezpośrednio tylko wtedy, gdy wybrano opcję <**Manualny**>.

konfiguracja przeglądarki

Łączenie i ustawienie sieci

Ustawienia sieci zależą od metody połączenia, przed ustawieniem trybu łączności sprawdź otoczenie sieciowe.

Gdy nie wykorzystywany jest żaden router

- **Tryb manualny**
  - Połączenie internetowe: statycz.IP, dzierżawiona linia i środowiska LAN umożliwiają połączenie między AIBox a użytkownikami zdalnymi.
  - Ustawienia sieciowe: ustaw <**Rodzaj IP**> połączonego AIBoxa na <**Manualny**>.
    - Skonsultuj IP, bramę i maskę podsieci z administratorem sieci.
- **Tryb DHCP**
  - Połączenie internetowe: podłącz AIBox bezpośrednio do modemu kablowego, modemu ADSL DHCP lub światłowodowej sieci LAN.
  - Ustawienia sieciowe: ustaw <**Rodzaj IP**> połączonego AIBoxa na <**DHCP**>.

Gdy wykorzystywany jest router

- Aby uniknąć konfliktu adresu IP ze statycznym adresem IP AIBoxa, sprawdź następujące elementy:

- **Konfiguracja AIBoxa za pomocą statycznego IP**
  - Połączenie internetowe: AIBox można podłączyć do routera IP podłączonego do modemu kablowego lub routera w środowisku sieci lokalnej (LAN).

- **Ustawianie sieci AIBox**

1. ustaw <**Rodzaj IP**> połączonego AIBoxa na <**Manualny**>.
2. Sprawdź, czy ustawiony adres IP jest w zakresie statycznych IP udostępnianych przez router.
   Adres IP, Brama, Mas.podsie.: skonsultuj się z administratorem sieci.

- Jeżeli serwer DHCP ma skonfigurowany adres początkowy (192.168.0.100) adres końcowy na (192.168.0.200), należy ustawić adres IP poza skonfigurowanym zakresem DHCP (192.168.0.2 ~ 192.168.0.99 oraz 192.168.0.201 ~ 192.168.0.254).

3. Sprawdź, czy adres bramy i maska podsieci są zgodne z ustawieniami w routerze IP.

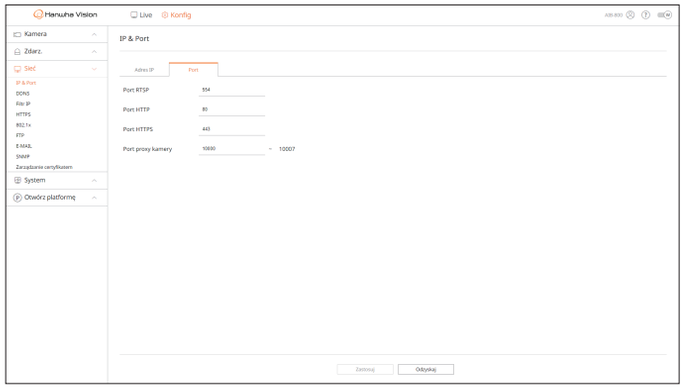
- **Konfiguracja adresu IP DHCP routera**

1. Aby wejść do konfiguracji routera IP, otwórz przeglądarkę na lokalnym komputerze PC podłączonym do routera IP i wprowadź adres routera (np. https://192.168.1.1).
2. Na tym etapie wykonaj konfiguracje lokalnego komputera PC, jak w przykładzie poniżej:
   np. Adres IP: 192.168.1.2
   Mas.podsie.: 255.255.255.0
   Brama: 192.168.1.1
   - Po połączeniu z routerem IP, nastąpi żądanie o hasło. Aby wejść na stronę konfiguracji routera, pozostaw puste pole nazwy użytkownika i wprowadź „**admin**” w polu hasła, po czym kliknij <**OK**>.
   - Wejdź do menu konfiguracji routera i włącz serwer DHCP oraz wpisz adresy początkowe i końcowe.
     - Adres początkowy: 192.168.0.100
     - Adres końcowy: 192.168.0.200

- Powyższe kroki mogą być inne, zależnie od wykorzystywanego routera.

Konfiguracja ustawień portów

Konfig. > Sieć > IP & Port > Port



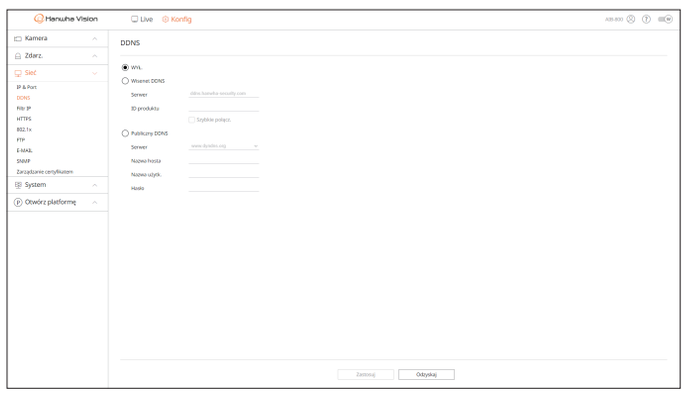
- Port RTSP: służy do przesyłania obrazu wideo przez sieć. Wartość początkowa to <**554**>.
- Port HTTP: pozwala wprowadzić wartość portu dla przeglądarki HTTP Web Viewer. Wartość początkowa to <**80**>.
- Port HTTPS: pozwala wprowadzić wartość portu dla przeglądarki HTTPS Web Viewer. Wartość początkowa to <**443**>.
  - HTTPS to udoskonalona wersja protokołu komunikacji sieciowej HTTP. Jeśli istotne jest zabezpieczenie dostępu do przeglądarki Web Viewer, należy włączyć port HTTPS.
- Port proxy kamery: umożliwia ustawienie portu proxy kamery. Wartość domyślna to <**10000**>.

DDNS

Jeżeli użytkownik zdalny wchodzi do sieci, możesz ustawić, czy używać DDNS i miejsca, do którego jest włączony.

- DDNS to skrót od Dynamic DNS (Domain Name System).
  DNS (Domain Name System) umożliwia adresowanie sekwencjami rozpoznawalnych okiem znaków (np. www.google.com) do numerycznych adresów IP (64.233.189.104). DDNS (Dynamic DNS) rejestruje nazw domeny i dynamiczny adres IP na serwerze DDNS i pozwala na adresowanie nazwą bez względu na zmiany adresu IP.
- Aby użyć DDNS, włącz funkcje przekazywania portów i UPnP routera. Więcej informacji można znaleźć w instrukcji użytkownika routera.

Konfig. > Sieć > DDNS



- WYŁ.: zaznacz, jeśli nie używasz DDNS.

Konfiguracja Wisenet DDNS

- Wisenet DDNS: zaznacz, jeśli używasz serwera DDNS firmy Hanwha Vision. Aby używać Wisenet DDNS, zaloguj się na stronie internetowej (ddns.hanwha-security.com) i zarejestruj produkt w sekcji „**My DDNS** > **Register Product**”.
- Serwer: wyświetla nazwę serwera DDNS, który ma być używany.
- ID produktu: wprowadź ID produktu zarejestrowanego na serwerze Wisenet DDNS.
- Szybkie połącz.: w przypadku korzystania z routera obsługującego funkcję UPnP (Universal Plug and Play), automatycznie obsługuje on otwieranie portów dla połączeń zewnętrznych.
  Podczas łączenia przy użyciu funkcji Szybkie połączenie, pojawi się komunikat o postępie.
  - **Quick connect powiódł się.** : komunikat o sukcesie połączenia.
  - **Sprawdź środowisko sieciowe.** : występuje, gdy ustawienia sieciowe są błędne. Sprawdź ustawienia sieciowe.
  - **Włącz funkcję UPnP w routerze.** : komunikat pojawia się, jeżeli router wymaga dostępu do UPnP.
  - **Nie znaleziono routera.** : komunikat pojawia się, gdy router jest niewidoczny. Sprawdź konfiguracje routera.
  - **Restartuj router.** : komunikat pojawia się, gdy router powinien restartować.
  - **Nie udało się połączyć.** : taki komunikat pojawia się, gdy połączenie nie powiodło się ze względu na nieznany błąd.
  - Jeśli router nie obsługuje funkcji UPnP lub chcesz korzystać z serwera DDNS bez użycia funkcji <**Szybkie połącz.**>, ustaw przekazywanie portów routera na <**Manualny**>.

- Jeśli nie jest używane środowisko podwójnego NAT lub port routera nie został ustawiony, status DDNS zostanie wyświetlony jako <**Udana**>. Jednak połączenie DDNS z przeglądarki do AIBoxa może się nie powieść.
- Aby możliwe było połączenie DDNS, musi być podłączona sieć zewnętrzna.
- Jeśli konfigurujesz port, który jest już w użyciu, połączenie może się nie udać. Sprawdź konfigurację portu routera.
- W razie konfliktu port automatycznie zmienia się na inny. Sprawdź zmienione informacje o porcie AIBox w menu „**Konfig.** > **Sieć** > **IP & Port** > **Port**”.
- Jeśli występuje konflikt portów, zapoznaj się z instrukcją użytkownika podłączonego routera i sprawdź ustawienia przekazywania portów lub UPnP.

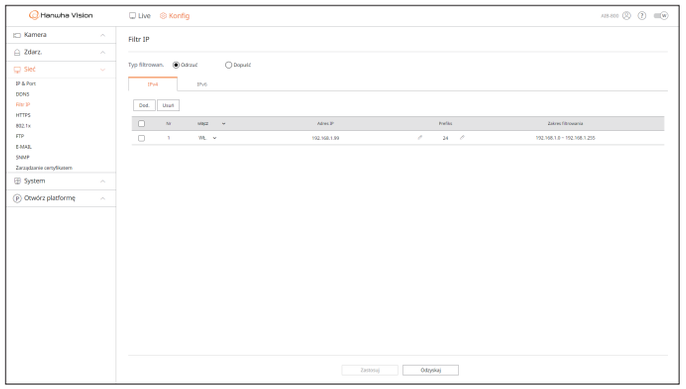
Konfiguracja publicznego DDNS

- Publiczny DDNS: zaznacz, jeśli używasz serwera DDNS publicznej strony. Możesz go używać po zarejestrowaniu się w usłudze.
- Serwer: wybierz serw. DDNS, który ma być używany.
- Nazwa hosta: wprowadź nazwę hosta zarejestrowaną na serw. DDNS.
- Nazwa użytk.: nazwę użytkownika zarejestrowaną na serw. DDNS.
- Hasło: wprowadź hasło użytkownika zarejestrowane na serw. DDNS.

Filtr IP

Możesz przygotować listę adresów IP dostępnych bądź zabronionych dla komunikacji ze wskazanymi zewnętrznymi adresami IP. Adresami IP można zarządzać oddzielnie dla protokołów IPv4 i IPv6.

Konfig. > Sieć > Filtr IP



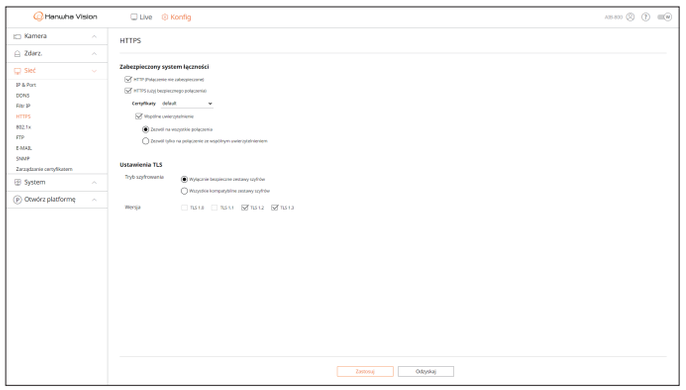
- Typ filtrowan.
  - Odrzuć: ogranicza dostęp dla zarejestrowanych IP.
  - Dopuść: dopuść dostęp dla zarejestrowanych IP.
- IPv4/IPv6: wybrać zakładkę dla typu IP, który ma zostać zarejestrowany.
- Dod.: można dodać więcej elementów do filtrowania.
- Usuń: pozwala usunąć dowolny zarejestrowany filtr.
- Włącz: włączanie lub wyłączanie filtrowania zarejestrowanych adresów IP.
- Adres IP: wyświetla zarejestrowany adres IP. Ustawienie można zmienić, klikając dwukrotnie adres IP lub klikając < ✎ >.
- Prefiks: wyświetla prefiks do filtrowania. Ustawienie można zmienić, klikając dwukrotnie prefiks lub klikając < ✎ >.
- Zakres filtrowania: po wprowadzeniu adresu IP lub prefiksu, wyświetlone zostaną zakresy adresów IP do zablokowania lub dopuszczenia.

- Jeżeli adres IP kamery nie jest włączony do listy Pozwól bądź występuje na liście Odrzuć, dostęp do kamery będzie odrzucony.
- W przypadku IPv4 filtrowanie IP kamery przez port PoE nie jest stosowane natychmiast. (Poprzednie połączenia są zachowywane, a filtrowanie jest stosowane przy następnym logowaniu).

HTTPS

Można wybrać zabezpieczony system łączności lub zainstalować certyfikat.

Konfig. > Sieć > HTTPS



- Zabezpieczony system łączności: zważywszy na poziom bezpieczeństwa, w zależności od środowiska można wybrać metodę bezpiecznego połączenia.
  HTTPS (Hypertext Transfer Protocol Secure) to lepiej zabezpieczona wersja protokołu HTTP, w którym dane wymieniane są z zastosowaniem mechanizmów szyfrowania i odszyfrowania żądania ze strony użytkownika w warstwie TLS (Transport Layer Security).
  - HTTP (Połączenie nie zabezpieczone): dane przesyłane są bez szyfrowania.
  - HTTPS (użyj bezpiecznego połączenia): służy do nawiązania połączenia zabezpieczonego przy użyciu niepowtarzalnego certyfikatu dostarczonego przez AIBox.
    - Wspólne uwierzytelnienie: służy do użytkowania ze zwiększonymi zabezpieczeniami. Jeśli wybrano opcję <**Zezwól na wszystkie połączenia**>, AIBox może się łączyć bez wspólnego uwierzytelnienia. Jeśli wybrano opcję <**Zezwól tylko na połączenie ze wspólnym uwierzytelnieniem**>, AIBox może się łączyć tylko w przypadku udanego wspólnego uwierzytelnienia.
- Ustawienia TLS: można wybrać Tryb szyfrowania lub wersję TLS do zastosowania podczas komunikacji szyfrowanej.
  - Tryb szyfrowania: zapewnia zestawy szyfrów w kilku algorytmicznych kombinacjach do wykorzystania w szyfrowanej komunikacji TLS, takiej jak wymiana kluczy, uwierzytelnianie i szyfrowanie.
    Opcja <**Wyłącznie bezpieczne zestawy szyfrów**> wykorzystuje tylko zestawy szyfrów z wysokimi zabezpieczeniami.
    Na potrzeby kompatybilności wstecznej wybierz opcję <**Wszystkie kompatybilne zestawy szyfrów**>. Może to jednak stanowić zagrożenie dla bezpieczeństwa, ponieważ opcja ta obejmuje wszystkie zestawy szyfrów, niezależnie od tego, czy są one bezpieczne, czy nie.
  - Wersja: można wybrać wersję z protokołem TLS do zastosowania podczas komunikacji szyfrowanej.
    - Jeśli <**Tryb szyfrowania**> jest ustawiony na <**Wyłącznie bezpieczne zestawy szyfrów**>, do wyboru są wersje <**TLS 1.2**> lub <**TLS 1.3**>.

- Jeśli AIBox jest podłączony do zewnętrznego Internetu lub zainstalowany w środowisku, w którym bezpieczeństwo ma duże znaczenie, zalecane jest połączenie HTTPS.

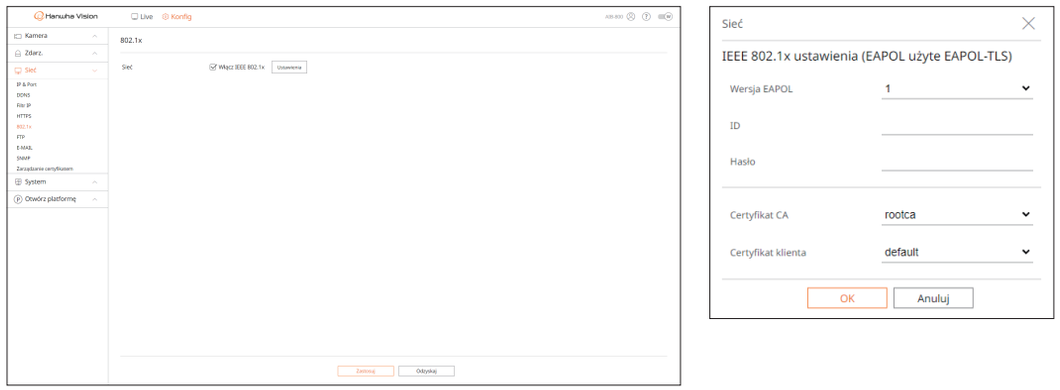
802.1x

Przy łączeniu z siecią możesz wskaż, czy korzystać z protokołu 802.1x i zainstalować odpowiedni certyfikat.

802.1x to system uwierzytelniania między serwerem a klientem, którego celem jest zapobieganie atakom hakerskim, infekowaniu wirusami oraz wyciekom przesyłanych i odbieranych danych sieciowych.

System 802.1x można wykorzystać do blokowania dostępu nieupoważnionym klientom i zwiększenia poziomu bezpieczeństwa poprzez dopuszczenie do komunikacji wyłącznie uwierzytelnionych użytkowników.

Konfig. > Sieć > 802.1x



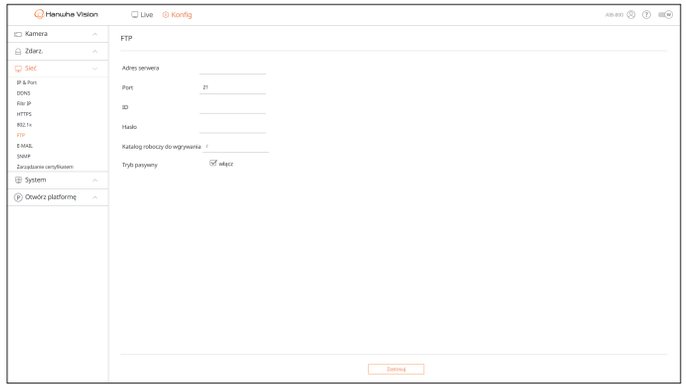
- Ustawienia: jeśli zaznaczona jest opcja <**Włącz IEEE 802.1x**>, można zmienić ustawienia.
- Wersja EAPOL: wybierz protokół w wersji EAPOL.
  - Niektóre z hubów nie działają w ustawieniu z wersją <**2**>. Wybierz wersję <**1**>, która jest wersją domyślą EAPOL.
- ID: wprowadź ID podane przez operatora serwera RADIUS.
  - Jeżeli wprowadzone ID różni się od ID na certyfikacie klienta, nie zostanie właściwie przetworzone.
- Hasło: wprowadź hasło podane przez operatora serwera RADIUS.
  - Jeżeli wprowadzone hasło nie odpowiada kluczowi prywatnemu klienta, nie będzie właściwie przetworzone.
- Certyfikat CA: zaznacz, jeżeli posiadany certyfikat publiczny zawiera też klucz publiczny.
- Certyfikat klienta: wskaż, gdy certyfikat publiczny zawiera też klucz uwierzytelnienia klienta.

- Aby wdrożenie środowiska 802.1x powiodło się, administrator musi korzystać z serwera RADIUS. Ponadto, hub połączony do serwera musi obsługiwać 802.1x.
- Jeśli ustawienia godzin serwera RADIUS, koncentratora przełączającego i AIBoxa nie będą zgodne, komunikacja między nimi może nie działać.
- Protokół 802.1x przyjęty przez AIBox to EAP-TLS.
- Aby korzystać z protokołu 802.1x, należy zainstalować obydwa certyfikaty.

FTP

Jeśli do zdarzenia dojdzie podczas zapisu wideo przez kamerę, pliki obrazów można przesyłać z wykorzystaniem serwera FTP.

Konfig. > Sieć > FTP

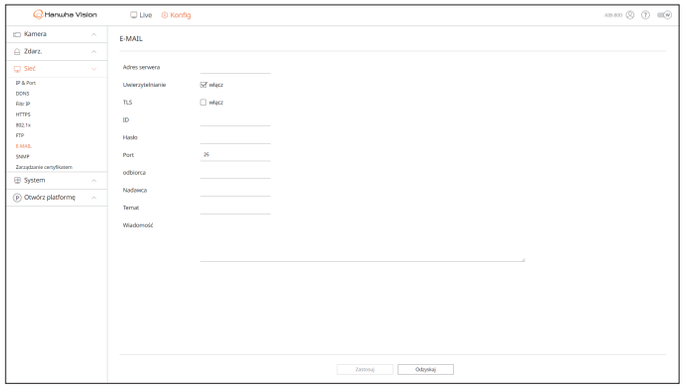


- Adres serwera: wprowadź adres serwera FTP, na który ma zostać przesłane wideo po wystąpieniu zdarzenia.
- Port: wprowadź wartość portu dla Web Viewera serwera FTP. Domyślna wartość to <**21**>, ale można wprowadzić wartość z przedziału od 1 do 65535.
- ID: wprowadź ID użytk. w celu uwierzytelnienia podczas łączenia z serwerem FTP.
- Hasło: wprowadź hasło użytk. w celu uwierzytelnienia podczas łączenia z serwerem FTP.
- Katalog roboczy do wgrywania: wprowadź ścieżkę serwera FTP, pod którą mają być zapisywane przesyłane obrazy zdarzeń.
- Tryb pasywny: zaznacz opcję <**Włącz**>, jeśli z uwagi na firewall lub ustawienia serwera FTP wymagany jest tryb pasywny.
- Zastosuj: uruchamia test transmisji do określonego serwera.

E-MAIL

Jeśli do zdarzenia dojdzie podczas zapisu wideo przez kamerę, pliki obrazów można przesyłać z systemu e-mail.

Konfig. > Sieć > E-MAIL

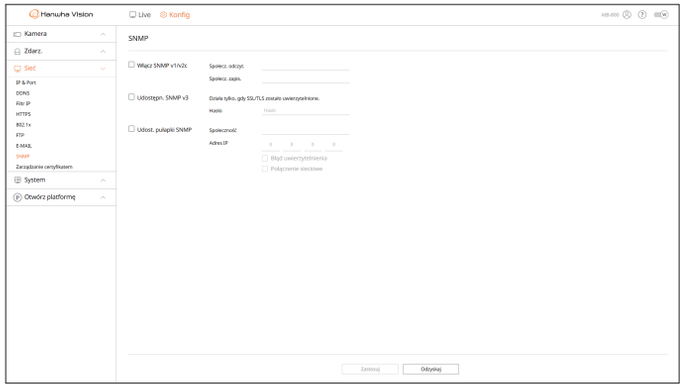


- Adres serwera: wprowadź adres serwera SMTP, na który ma zostać przesłane wideo po wystąpieniu zdarzenia.
- Uwierzytelnianie: zaznacz opcję <**Włącz**>, gdy transmisja e-mail jest uwierzytelniana za pomocą ID i hasła.
- TLS: w przypadku serwera poczty e-mail, który wymaga zabezpieczeń, zaznacz opcję <**Włącz**>.
- ID: wprowadź ID w celu uwierzytelnienia podczas łączenia z serwerem.
- Hasło: wprowadź hasło w celu uwierzytelnienia podczas łączenia z serwerem.
- Port: wprowadź port połączenia.
- Odbiorca: wprowadź adres e-mail odbiorcy.
- Nadawca: wprowadź adres e-mail nadawcy.
- Temat: wprowadź temat wiadomości e-mail.
- Wiadomość: wprowadź treść wiadomości.
- Zastosuj: uruchamia test transmisji do określonego serwera.

SNMP

Za pomocą protokołu SNMP administratorzy systemu lub sieci mogą zdalnie monitorować i konfigurować urządzenia sieciowe.

Konfig. > Sieć > SNMP

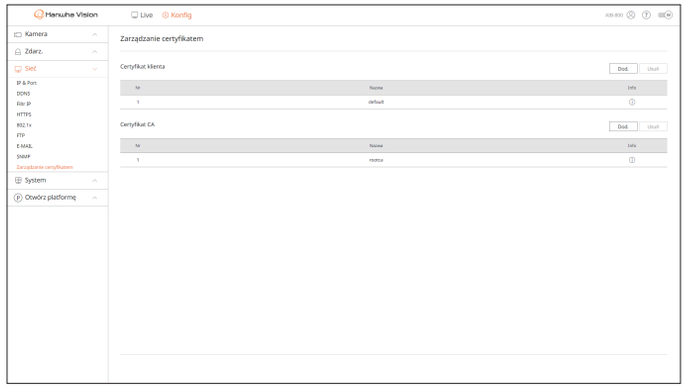


- Włącz SNMP v1/v2c: SNMP v1 lub SNMP v2c jest użyty.
  - Społecz. odczyt.: wprowadź nazwę społeczności z uprawnieniami tylko do odczytu informacji SNMP.
  - Społecz. zapis.: wprowadź nazwę społeczności z uprawnieniami tylko do zapisu informacji SNMP.
- Udostępn. SNMP v3: SNMP v3 jest użyty. Działa tylko wtedy, gdy SSL/TLS został uwierzytelniony.
  - Hasło: ustaw początkowe hasło użytkownika SNMP v3.
- Udost. pułapki SNMP: służy do wysyłania ważnych zdarzeń i statusów do administratora systemu.
  - Społeczność: wprowadzić nazwę społeczności pułapek odbierającej wiadomości.
  - Adres IP: wprowadź adres IP, na który ma być wysłany komunikat.
  - Błąd uwierzytelnienia: jeśli informacje o społeczności są nieprawidłowe, zdarzenie jest dostarczane na wprowadzony adres IP.
  - Połączenie sieciowe: jeśli sieć jest ponownie połączona, zdarzenie jest dostarczane na wprowadzony adres IP.

Zarządzanie certyfikatem

Certyfikatami klienta i certyfikatami CA można zarządzać osobno, a także dodawać je i usuwać.

Konfig. > Sieć > Zarządzanie certyfikatem

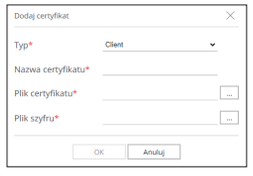


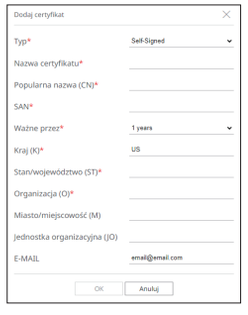
- Info: kliknij przycisk < ⓘ >, aby zobaczyć detale certyfikatu.

Certyfikat klienta

Certyfikat klienta jest tworzony lub stosowany przez użytkownika.

Certyfikat urządzenia dostarczony przez firmę Hanwha Vision jest zarejestrowany domyślnie i nie można go usunąć.



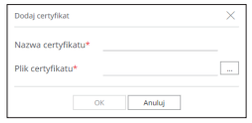


1. Aby dodać certyfikat, kliknij <**Dod.**>. Pojawi się okno <**Dodaj certyfikat**>.
2. Jeśli istnieje jakikolwiek plik certyfikatu, jako typ wybierz <**Client**>.
   - Nazwa certyfikatu: wprowadź nazwę certyfikatu.
   - Plik certyfikatu: kliknij przycisk < ... > i wybierz plik certyfikatu.
   - Plik szyfru: kliknij przycisk < ... > i wybierz plik szyfru.
3. Aby stworzyć certyfikat, jako typ wybierz <**Self-Signed**>.
   - Nazwa certyfikatu: wprowadź nazwę certyfikatu.
   - Popularna nazwa (CN): wprowadź popularną nazwę certyfikatu.
   - SAN: wprowadź SAN (nazwę alternatywną tematu) certyfikatu.
   - Ważne przez: wybierz datę wygaśnięcia certyfikatu.
   - Kraj (K): wprowadź kraj. Dozwolone są maksymalnie dwie litery.
   - Stan/województwo (ST): wprowadź stan lub województwo.
   - Organizacja (O): wprowadź nazwę organizacji.
   - Miasto/miejscowość (M): wprowadź informacje o lokalizacji (miasto/miejscowość).
   - Jednostka organizacyjna (JO): wprowadź jednostkę organizacyjną.
   - E-MAIL: wprowadź adres e-mail.
4. Kliknij przycisk <**OK**>.
   Certyfikat dodany do listy certyfikatów klienta można sprawdzić.
   - Aby usunąć certyfikat, zaznacz certyfikat do usunięcia i kliknij przycisk <**Usuń**>.

Certyfikat CA

Certyfikat CA jest wydawany przez urząd certyfikacji CA (Certificate Authority).

Certyfikat Root CA dostarczony przez firmę Hanwha Vision jest zarejestrowany domyślnie i nie można go usunąć.



1. Aby dodać certyfikat, kliknij <**Dod.**>. Pojawi się okno <**Dodaj certyfikat**>.
   - Nazwa certyfikatu: wprowadź nazwę certyfikatu.
   - Plik certyfikatu: kliknij przycisk < ... > i wybierz plik certyfikatu.
2. Kliknij przycisk <**OK**>.
   Certyfikat dodany do listy certyfikatów CA można sprawdzić.
   - Aby usunąć certyfikat, zaznacz certyfikat do usunięcia i kliknij przycisk <**Usuń**>.

konfiguracja przeglądarki

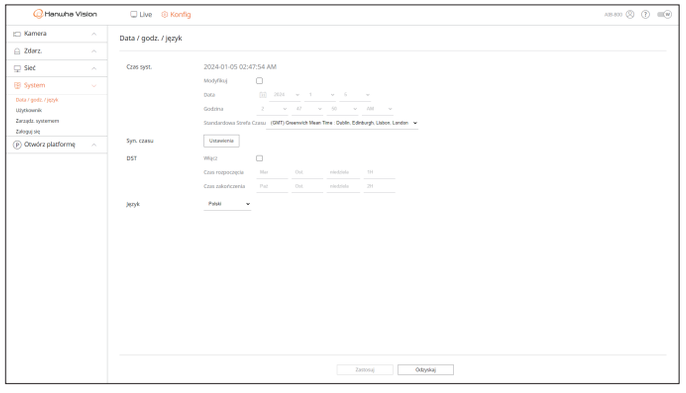
KONFIGURACJA SYSTEMU

Można skonfigurować datę, godzinę i język wyświetlane podczas użytkowania systemu, a także informacje o systemie zapytań i informacje z rejestru.

Data / godzina / język

Możesz sprawdzić i ustawić bieżącą datę/godzinę i parametry związane z czasem oraz język interfejsu.

Konfig. > System > Data / godz. / język



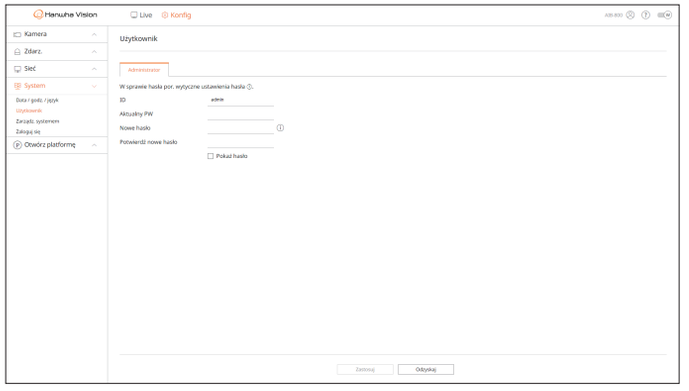
- Czas syst.: wyświetla datę i godzinę wybraną w obszarze <**Standardowa Strefa Czasu**>.
  Jeśli zaznaczona jest opcja <**Modyfikuj**>, możliwa jest zmiana daty i godziny na ekranie.
  - GMT (Czas Greenwich) to standardowy czas ogólnoświatowy względem którego definiowane są strefy czasowe.
- Syn. czasu: określ, czy chcesz korzystać z funkcji synchronizacji z serwerem czasu.
  Aby przejść do ekranu <ustawień synchr. czasu>, kliknij przycisk <**Ustawienia**>.
  Jeśli używana jest opcja <**Synchronizuj z serwerem NTP**>, aktualny czas AIBoxa jest synchronizowany przez serwer ustawiony w obszarze <**Adres serwera NTP**>. W związku z tym godziny nie można zmienić ręcznie.
  - Synchronizuj z serwerem NTP: wskaż, czy używać synchronizacji z serwerem czasu, czy nie.
  - Adres serwera NTP: wprowadź adres IP bądź URL serwera czasu.
- DST: ustaw czas letni wraz z okresem obowiązywania, aby był wcześniejszy o godzinę niż GMT strefy.
  - W zależności od wybranej strefy czasowej, informacje o DST mogą być wyświetlane inaczej.
- Język: wybierz język. Ustawia język interfejsu.

- W zależności od lokalizacji wydania produktu język i standardowe ustawienia czasu mogą się różnić.

Użytkownik

Pozwala zmieniać ID i hasło administratora. Administrator może używać i ustawiać elementy menu i funkcje.

Konfig. > System > Użytkownik > Administrator



- ID: zmiana ID admina. Po zmianie używanego ID użytkownik zostanie wylogowany automatycznie.
- Aktualny PW: wprowadź aktualne hasło.
- Nowe hasło: wprowadź nowe hasło.
- Potwierdź nowe hasło: pozwala ponownie wprowadzić nowe hasło.
  - Po zaznaczeniu opcji <**Pokaż hasło**> hasło do zaszyfrowania zostanie wyświetlone jako rzeczywiste wprowadzone znaki.

- Początkowe ID administratora to „**admin**”, a hasło musi zostać ustawione podczas pierwszego logowania.
- Hasło należy zmieniać co trzy miesiące, aby zapewnić ochronę danych osobowych i zapobiec szkodom wynikającym z kradzieży informacji. Należy pamiętać, że to użytkownik odpowiada za bezpieczeństwo oraz wszelkie inne problemy wynikające z nieprawidłowego posługiwania się hasłem.
- Po kliknięciu przycisku < ⓘ > zostanie wyświetlony domyślny przewodnik dotyczący ustawiania hasła.

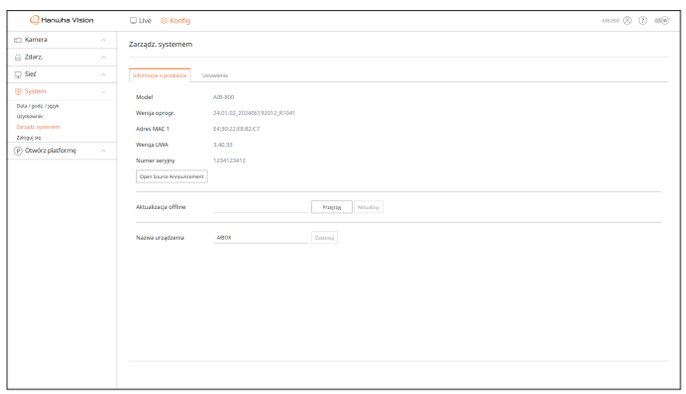
Zarządzanie systemem

Użytkownik może sprawdzić bieżącą wersję systemu, zaktualizować system do nowej wersji, wyeksportować dane, zainicjować ustawienia itp.

Sprawdzenie informacji systemowej

Przed podjęciem aktualizacji możesz sprawdzić aktualna wersję systemu oraz adresy MAC.

Konfig. > System > Zarządz. systemem > Informacje o produkcie



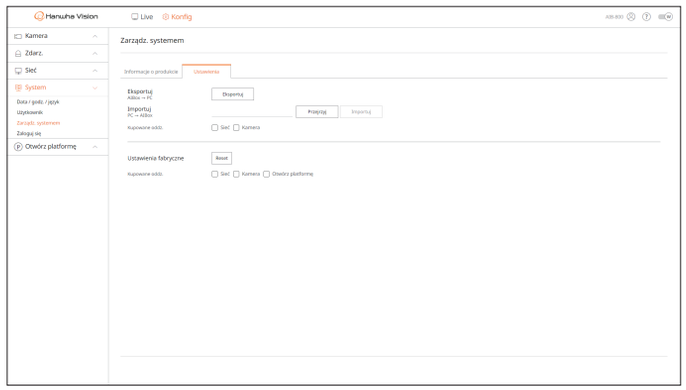
- Model: wyświetla nazwę modelu produktu.
- Wersja oprogr.: wyświetla wersję oprogramowania produktu. Możesz sprawdzić wersję oprogramowania i zaktualizować do najnowszej wersji.
- Adres MAC: wyświetla adres MAC produktu.
- Wersja UWA: wyświetla wersję UWA produktu.
- Numer seryjny: wyświetla numer seryjny produktu.
- Open Source Announcement: licencja open source produktu jest zapisywana jako plik.
- Aktualizacja offline: pozwala zaktualizować oprogramowanie, jeśli istnieje wersja wyższa niż obecna.
  - Kliknij przycisk <**Przejrzyj**> i wybierz plik oprogramowania na komputerze PC lub pamięci USB. Kliknięcie przycisku <**Aktualizuj**> spowoduje aktualizację oprogramowania i automatyczne ponowne uruchomienie systemu po jej zakończeniu. Nie należy wyłączać zasilania, dopóki system nie zakończy ponownego uruchamiania.
- Nazwa urządzenia: wyświetla nazwę używanego urządzenia. Ponadto możliwa jest zmiana nazwy urządzenia. Wprowadź żądaną nazwę i kliknij przycisk <**Zastosuj**>.
  - Aby rozróżnić wiele urządzeń AIBox w VMS, menedżerze urządzeń itp., zaleca się wprowadzenie innej nazwy urządzenia dla każdego urządzenia.

- Wyświetlane informacje systemowe mogą się różnić w zależności od modelu AIBox.

Zarządzanie ustawieniami

Informacje ustawione w urządzeniu AIBox można wyeksportować do komputera PC, a następnie zastosować je w innych jednostkach AIBox.

Konfig. > System > Zarządz. systemem > Ustawienia



- AIBox → PC: ustawienia AIBox są przechowywane na komputerze PC użytkownika.
  - Naciśnięcie przycisku <**Eksportuj**> spowoduje wyświetlenie okna z potwierdzeniem. Kliknij przycisk <**OK**>, aby zapisać ustawienia AIBox do pliku.
- PC → AIBox: ustawienia zapisane na komputerze PC zostaną zastosowane w urządzeniu AIBox.
  - Jeśli wybierzesz ustawienie wyjątku, możesz zaimportować wszystkie informacje oprócz informacji wybranych.
  - Kliknij przycisk <**Przejrzyj**> i wybierz plik konfiguracji na komputerze PC. Kliknij przycisk <**Importuj**>, a wyświetli się okno z potwierdzeniem. Kliknij przycisk <**OK**>, aby zastosować ustawienia w urządzeniu AIBox.
    - Ustawienia <**Eksportuj**> i <**Importuj**> mogą być używane tylko w tej samej wersji oprogramowania.
- Ustawienia fabryczne: przywraca produkt do fabrycznych ustawień. Jednak logi nie zostaną zresetowane. Wszystkie pozycje zaznaczone jako wyjątek nie zostaną objęte resetem do ustawień fabrycznych. Po kliknięciu przycisku <**Reset**> pojawi się wyskakujące okienko z potwierdzeniem. Kliknij przycisk <**OK**>, aby zresetować wybrane pozycje.

konfiguracja przeglądarki

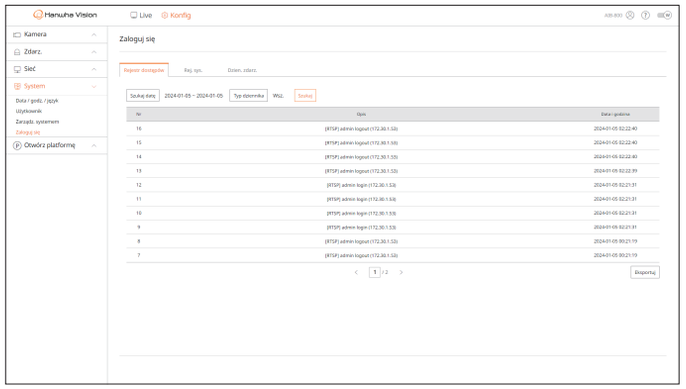
Zaloguj się

Istnieje możliwość sprawdzenia rejestrów związanych z logowaniem / wylogowaniem, systemem i zdarzeniami oraz zapisania ich do plików.

Sprawdzanie rejestrów dostępów

W rejestrze dostępów wyświetlane są informacje o logowaniu / wylogowaniu użytkownika oraz data i godzina wykonania.

Konfig. > System > Zaloguj się > Rejestr dostępów

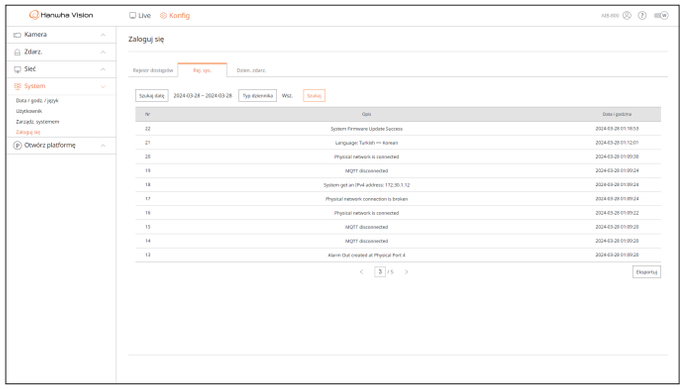


- Szukaj datę: wybierz datę wyszukiwania.
- Typ dziennika: wybierz typ rejestru do wyszukiwania.
- Szukaj: wyświetla wyniki wyszukiwania w liście rejestrów.
- Eksportuj: zapisanie wyszukanych rejestrów na komputerze PC.

Sprawdzanie rejestrów systemowych

Rejestr systemowy zawiera informacje systemowe, takie jak uruchomienie systemu, zamknięcie systemu, sieć, aktualizacja oprogramowania, przywrócenie ustawień fabrycznych, połączenie MQTT i zmiana ustawień menu, a także datę i godzinę wykonania.

Konfig. > System > Zaloguj się > Rej. sys.

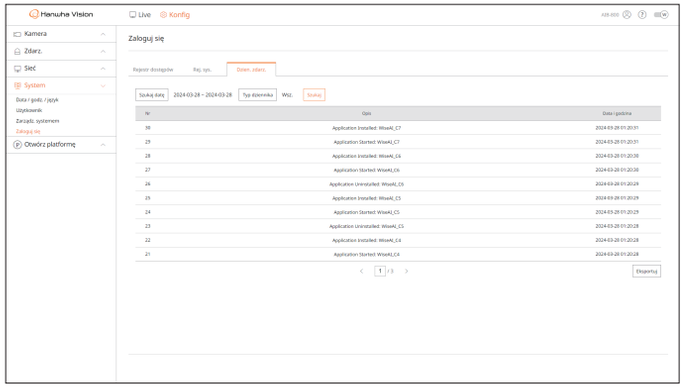


- Szukaj datę: wybierz datę wyszukiwania.
- Typ dziennika: wybierz typ rejestru do wyszukiwania.
- Szukaj: wyświetla wyniki wyszukiwania w liście rejestrów.
- Eksportuj: zapisanie wyszukanych rejestrów na komputerze PC.

Sprawdzanie rejestrów zdarzeń

W rejestrze zdarzeń wyświetlane są informacje o zdarzeniach, takich jak wejścia/wyjścia alarmowe i zdarzenia kamery, a także data i godzina wykonania.

Konfig. > System > Zaloguj się > Dzien. zdarz.



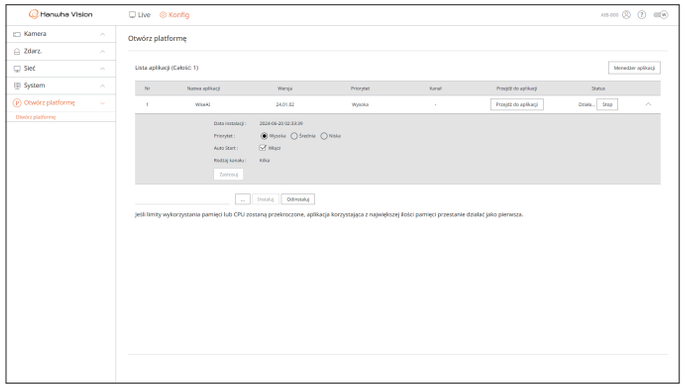
- Szukaj datę: wybierz datę wyszukiwania.
- Typ dziennika: wybierz typ rejestru do wyszukiwania.
- Szukaj: wyświetla wyniki wyszukiwania w liście rejestrów.
- Eksportuj: zapisanie wyszukanych rejestrów na komputerze PC.

KONFIGURACJA OTWARTYCH PLATFORM

Oprócz aplikacji WiseAI firmy Hanwha Vision zainstalowanej domyślnie w urządzeniu AIBox, istnieje możliwość korzystania z różnych funkcji poprzez zainstalowanie dodatkowych aplikacji.

Otwórz platformę

Konfig. > Otwórz platformę > Otwórz platformę



- Menedżer aplikacji: wyświetla nazwę używanej aplikacji, obciążenie pamięci, obciążenie procesora, liczbę utworzonych wątków i czas trwania.
  - Jeśli obciążenie pamięci lub procesora jest bliskie 100%, aplikacje o największym obciążeniu pamięci mogą zostać zatrzymane w celu ochrony systemu.
  - Jeśli używana aplikacja uruchamia wiele funkcji lub rozdzielczość profilu analizy AI przekracza 1080p, może to spowodować przeciążenie pamięci lub wykorzystania CPU. W takim przypadku należy zredukować część funkcji aplikacji, która została zatrzymana z powodu dużego wykorzystania pamięci. Jeśli rozdzielczość profilu AIBox przekracza 1080p, należy zmienić ją na 1080p w menu „**Konfig** > **Kamera** > **Informacje o profilu**”.
- Nazwa aplikacji: wyświetla nazwę aplikacji.
- Wersja: wyświetla wersję aplikacji.
- Priorytet: wyświetla priorytety uruchomionych aplikacji. Jeśli wartość <**Całość**>, którą można sprawdzić w sekcji <**Menedżer aplikacji**>, wzrośnie, aplikacje o niższym priorytecie zostaną przymusowo zakończone w pierwszej kolejności.
  Wartość <**Całość**> to całkowity udział zasobów, w tym główne zadania i aplikacje AIBox.
- Przejdź do aplikacji: przechodzi do ekranu ustawień zdarzeń dostarczanego przez aplikację.
- Status: wyświetla status działań aplikacji. Aby zatrzymać lub uruchomić aplikację, kliknij odpowiednio przycisk <**Stop**> lub <**Start**>.
- V: wyświetla szczegółowe informacje o aplikacji. Aby zmienić ustawienia, należy zmienić je na żądane, a następnie kliknąć <**Zastosuj**>.
  - Data instalacji: wyświetla datę zainstalowania aplikacji.
  - Priorytet: można zmienić priorytet aplikacji. Wybrać <**Wysoka**>, <**Średnia**> lub <**Niska**>.
  - Auto Start: jeśli wybrana jest opcja <**Włącz**>, aplikacja jest uruchamiana automatycznie podczas wykonywania głównego zadania AIBox.
  - Rodzaj kanału: jest wyświetlany jest jako <**Kilka**> lub <**Pojedynczy**> w zależności od liczby kanałów obsługiwanych przez aplikację.
    W przypadku aplikacji, które obsługują tylko jeden kanał, można zmienić kanał na żądany. Przed zmianą kanału należy najpierw zatrzymać uruchomione aplikacje.
- [...] / Instaluj: aplikacja zostanie zainstalowana w danym kanale. Kliknij przycisk < [...] >, wybierz plik aplikacji do zainstalowania i kliknij przycisk <**Instaluj**>.
- Odinstaluj: aby zainstalować aplikację inną niż bieżąca, należy najpierw usunąć używaną aplikację. Kliknij przycisk <**Odinstaluj**>, zaznacz kanały do usunięcia i kliknij przycisk <**Zastosuj**>.
  - Dla każdego kanału można zainstalować tylko jedną aplikację.

- Można rozpoznać sytuację, w której aplikacja zatrzymuje się w celu podjęcia możliwych działań. W menu „**Konfig** > **Zdarz.** > **Konfiguracja reguły zdarzenia**” ustawić wyzwalanie zdarzenia <**OpenSDKAppStatus.WiseAI**> na <**Inactive**>. Zatrzymanie aplikacji zostanie wykryte jako zdarzenie, a zdarzenie można potwierdzić za pomocą żądanej akcji zdarzenia.

ROZWIĄZYWANIE PROBLEMÓW

Objaw	Działanie
Zdarzenie analizy AI nie występuje, a dokładność analizy spada.	• Zalecana rozdzielczość profilu ustawionego dla analizy AI w menu „**Konfig** > **Kamera** > **Informacje o profilu**" to co najmniej 1080p, 10 fps. Jeśli ustawienie jest niższe, należy je zmienić na zalecaną wartość. • Jeśli rozdzielczość kamery jest niższa niż 1080p, należy ją zmienić na wartość maksymalną. • Podczas jednoczesnego przesyłania wielu profili kamer, liczba klatek na sekundę kanału może spaść poniżej 10 fps ze względu na zwiększone obciążenie przetwarzania. Upewnić się, że kamera utrzymuje liczbę klatek na sekundę na poziomie 10 fps. Jeśli kamera nie może utrzymać transmisji na poziomie 10 fps do AIBox, należy zmniejszyć liczbę przesyłanych profili lub przejść do menu „**Konfig** > **Kamera** > **Informacje o profilu**" i wybrać tylko profil używany wcześniej, aby zmniejszyć obciążenie przetwarzania. Ponadto należy sprawdzić, czy rozdzielczość i liczba klatek na sekundę wybranego profilu są zgodne z zalecanymi specyfikacjami (lub zbliżone do nich). • Uruchamianie wielu aplikacji może zwiększyć obciążenie NPU, co może zmniejszyć dokładność analizy AI. W przypadku zauważenia spadku wydajności, należy zatrzymać wszelkie dodatkowe aplikacje poza podstawowymi aplikacjami WiseAI i sprawdzić ponownie. Informacje o zainstalowanych aplikacjach można wyświetlić w menu „**Konfig** > **Otwórz platformę** > **Otwórz platformę**".
Wideo spowalnia lub urywa się.	• Liczba klatek ustawiona dla zwielokrotnionej transmisji danych w kamerze lub w ustawieniach sieciowych, może różnić się od faktycznej prędkości przesyłu. • Jeżeli wideo wyraźnie zwalnia lub zanika, sprawdź środowisko sieciowe lub warunki pracy kamery.
System się nie włącza, a wyświetlacz na przednim panelu nie działa.	• Sprawdź, czy źródło zasilania jest prawidłowo podłączone. • Sprawdź napięcie wejściowe systemu ze źródła zasilania. • Jeśli po wykonaniu powyższych czynności urządzenie się nie włącza, sprawdź źródło zasilania i w razie potrzeby zmień je. • Sprawdź w środku, czy przewody są prawidłowo podłączone. (PRZÓD)
Wejście wideo jest sprawne, ale filmy na niektórych kanałach są wyświetlane nieprawidłowo (np. czarny ekran, C-B ekran).	• Sprawdź, czy kamera jest prawidłowo zasilana. • Sprawdź stan kabla podłączonego do kamery i podłącz go ponownie po wymianie lub odłączeniu. • Sprawdzić sygnał wyjściowy łącząc się z oprogramowaniem Web Viewer kamery. • Sprawdzić, czy gniazdo sieciowe jest prawidłowo podłączone oraz czy ustawienia sieciowe są prawidłowe. • Zmiana koncentratora obsługującego kartę Gigabit może rozwiązać problem.
Kamera nie jest podłączona lub komputer nie może nawiązać połączenia.	• Sprawdź, czy przewód sieciowy jest prawidłowo podłączony. • Sprawdź ustawienia sieciowe. • Sprawdź ustawienie IP komputera i kamer. • Spróbuj przeprowadzić test sieci. • Sprawdź, czy w pobliżu urządzenia znajduje się inne urządzenie wykorzystujące ten sam numer IP.
Obraz wideo jest zbyt jasny lub zbyt ciemny.	• Kliknij przycisk < ⚙ > w żądanym kanale w menu „**Konfig.** > **Kamera** > **Informacje o profilu**", przejdź do Web Viewera danej kamery i zmień konfigurację.
Nie pamiętam hasła.	• Skontaktuj się z administratorem AIBox w celu uzyskania pomocy.


Hanwha
Vision