Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

A05 ACCESS CONTROL TERMINAL

Administrator Guide

Dziękujemy za wybranie terminala kontroli dostępu Akuvox serii A05. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować terminal kontroli dostępu. Niniejsza instrukcja dotyczy wersji 105.30.10.13 i zawiera wszystkie konfiguracje funkcji i cech terminali kontroli dostępu serii A05. Odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe.

Przegląd produktów

Seria Akuvox A05 to oparty na systemie Linux telefon kontroli dostępu z wyświetlaczem. Obejmuje kontrolę dostępu i nadzór wideo. Precyzyjnie dostrojona technologia SmartPlus i technologia komunikacji oparta na sztucznej inteligencji pozwalają na lepsze dostosowanie do nawyków operacyjnych klientów. Seria A05 ma wiele portów, takich jak RS485 i porty Wiegand, które można wykorzystać do łatwej integracji zewnętrznych systemów cyfrowych, takich jak kontroler windy i czujnik alarmu przeciwpożarowego, pomagając w stworzeniu całościowej kontroli wejścia do budynku i jego otoczenia oraz dając użytkownikom duże poczucie bezpieczeństwa poprzez różnorodny dostęp, taki jak dostęp kartą, NFC, kod QR i nowo dodany dostęp do drzwi w połączeniu z pomiarem temperatury ciała. Terminal kontroli dostępu z serii A05 ma zastosowanie w budynkach mieszkalnych, biurowych i ich kompleksach.

Specyfikacja modelu

Model	A05
Wyświetlacz	5" IPS
Ekran dotykowy	X
Przycisk	X
Materiał obudowy	Tworzywo sztuczne
Wyjście przekaźnika	1
Alarm wł.	1
RS485	√
PoE	√
Rozdzielczość	1280x720
Jasność	500 cd/m2
RAM	1GB
ROM	8 GB
Czytnik kart	13,56 MHz
Wi-Fi	X
Bluetooth	Opcjonalnie
Stopień ochrony IP	IP65
Wykrywanie temperatury	Opcjonalnie
Rozpoznawanie twarzy	√
LTE	X
USB	X
Zewnętrzna karta SD	X

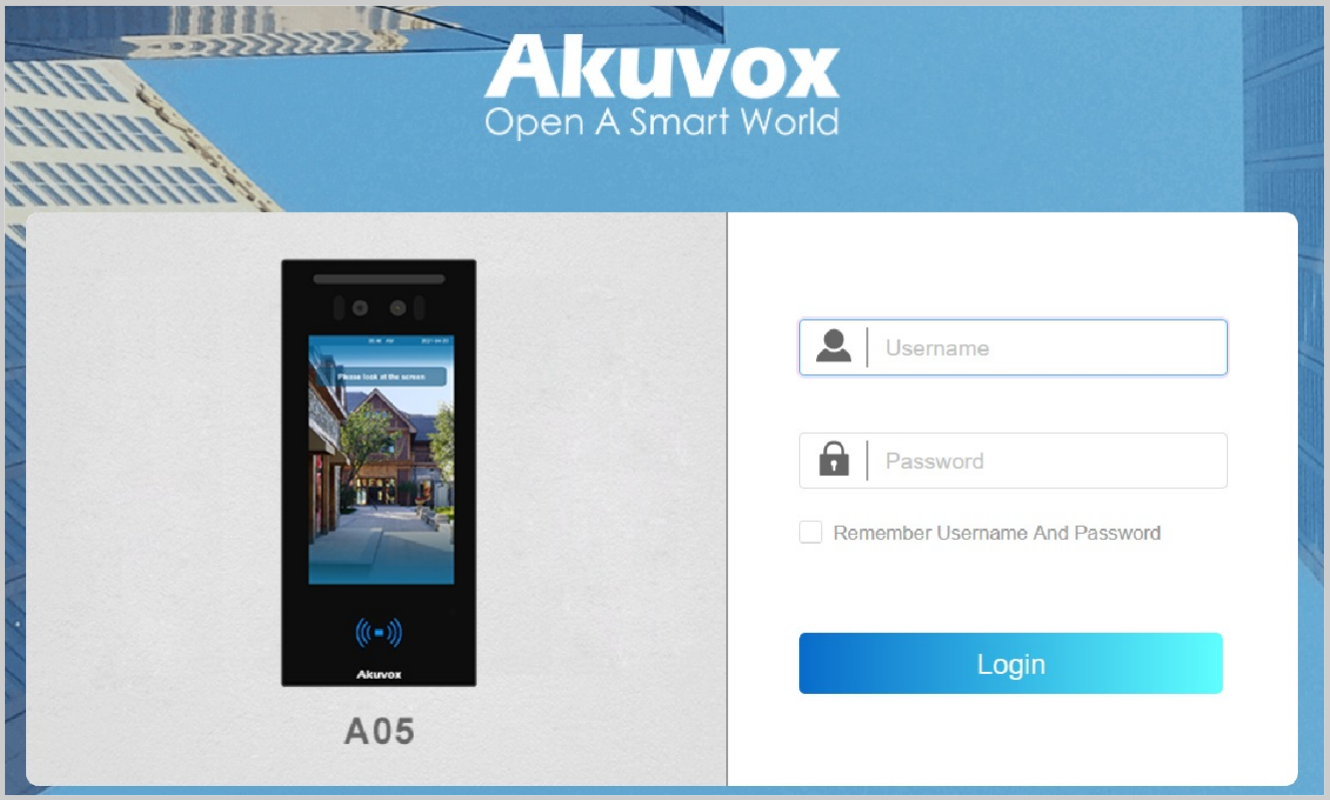
Zasilanie rezerwowe POE	5.5W
Zużycie energii przy pełnym obciążeniu POE	9.8W
Zasilacz Zasilanie w trybie gotowości	5.5W
Zużycie energii przez zasilacz przy pełnym obciążeniu	10W

Wprowadzenie do menu konfiguracji

- **Status** : Ta sekcja zawiera podstawowe informacje, takie jak informacje o produkcie, informacje o sieci i konfiguracje związane z dziennikami, takie jak dzienniki dostępu.
- **Sieć** : Ta sekcja dotyczy głównie ustawień DHCP i statycznego adresu IP, wdrażania sieci urządzeń itp.
- **Nadzór** : Ta sekcja zawiera ustawienia związane z dźwiękiem i wideo, takie jak Live stream, RTSP, ONVIF i MJPEG.
- **Kontrola dostępu**: Ta sekcja zawiera ustawienia wejścia, ustawienia przekaźnika i kontrolę dostępu do drzwi w zakresie rozpoznawania twarzy, karty RF, ustawień Bluetooth i ustawień temperatury ciała.
- **Katalog**: Ta sekcja obejmuje zarządzanie harmonogramem dostępu i zarządzanie użytkownikami.
- **Urządzenie** : Ta sekcja obejmuje oświetlenie, Wiegand, sterowanie windą, LCD, audio itp.
- **Ustawienia**: Ta sekcja dotyczy harmonogramu przekaźnika, ustawień powiadomień bezpieczeństwa, przekaźnika internetowego, czasu, akcji i ustawień HTTP API.
- **System**: Ta sekcja obejmuje aktualizację oprogramowania układowego, resetowanie urządzenia, ponowne uruchamianie, automatyczne dostarczanie pliku konfiguracyjnego, dziennik systemowy, zdalny serwer debugowania, PCAP, modyfikację hasła, a także tworzenie kopii zapasowych urządzenia.

Dostęp do urządzenia

Przed konfiguracją Akuvox A05 należy upewnić się, że urządzenie jest prawidłowo zainstalowane i podłączone do normalnej sieci. Za pomocą narzędzia skanera IP Akuvox wyszukaj adres IP urządzenia w tej samej sieci LAN. Następnie użyj adresu IP, aby zalogować się do przeglądarki internetowej przy użyciu nazwy użytkownika i hasła **admin** i **admin**.



Uwaga

- Pobierz skaner IP: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Zobacz szczegółowy przewodnik: **https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via- ip-scanner?highlight=IP%20Scanner**
- Zdecydowanie zalecana jest przeglądarka Google Chrome.
- Prosimy o uważne wprowadzanie nazwy użytkownika i hasła.

Ustawienia języka i czasu

Język

Język wyświetlacza LCD urządzenia można wybrać w interfejsie **Setting> Time/Lang > LCD Language**.

Obsługiwane są następujące języki:

- Angielski, chiński uproszczony, koreański, hiszpański, japoński i ukraiński.

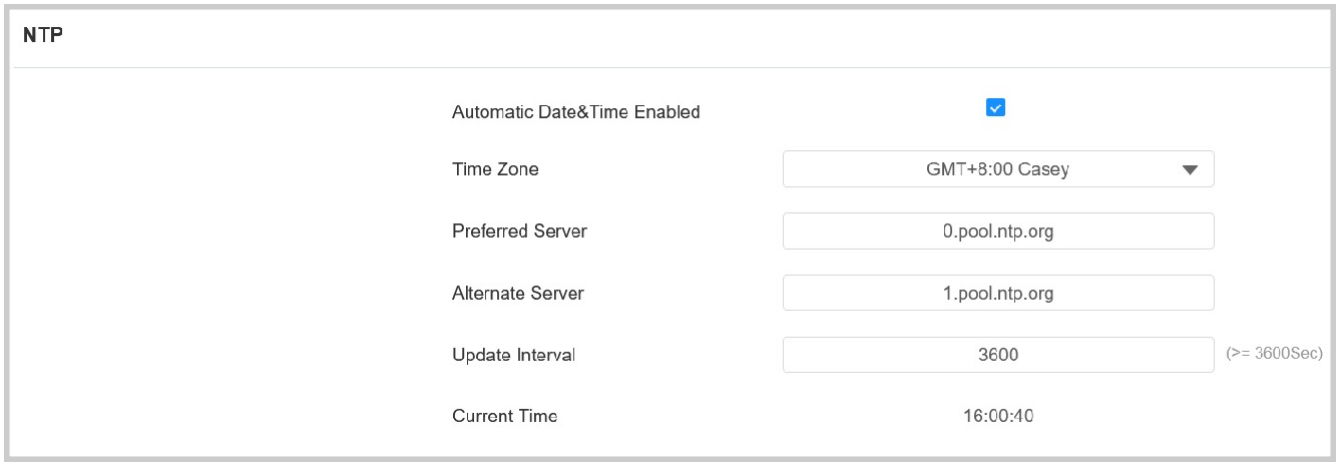
Język internetowy można zmienić w prawym górnym rogu.

Obsługiwane są następujące języki: Angielski, chiński uproszczony, hiszpański i japoński.

Czas

Ustawienia czasu w interfejsie internetowym umożliwiają skonfigurowanie adresu serwera NTP uzyskanego w celu automatycznej synchronizacji czasu i daty. Po wybraniu strefy czasowej urządzenie automatycznie powiadomi serwer NTP o strefie czasowej, aby serwer NTP mógł zsynchronizować ustawienia strefy czasowej w urządzeniu.

Aby skonfigurować czas, przejdź do opcji **Ustawienia >** Interfejs **czasu/języka**.



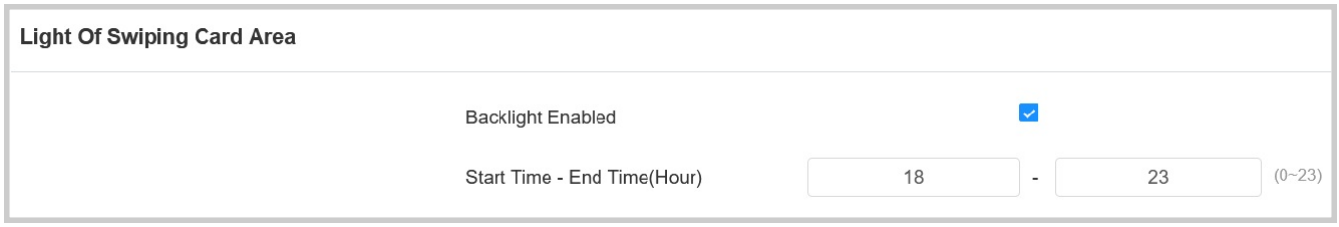
- **Automatic Date&Time Enabled**: Ustawienie, czy urządzenie ma automatycznie aktualizować czas za pośrednictwem serwera Network Time Protocol (NTP).
- **Data/godzina**: ręczne ustawienie daty i godziny dla urządzenia po wyłączeniu usługi automatycznej daty i godziny.
- **Strefa czasowa**: Wybierz określoną strefę czasową w zależności od tego, gdzie urządzenie jest używane. Domyślną strefą czasową jest GMT+0:00.
- **Preferred Server** (**Preferowany serwer**): Wprowadź adres głównego serwera NTP do aktualizacji czasu. Domyślny adres serwera NTP to 0.pool.ntp.org.
- **Alternate Server**: Wprowadź adres zapasowego serwera NPT, gdy podstawowy ulegnie awarii.
- **Interwał aktualizacji**: Ustawienie interwału aktualizacji czasu. Na przykład, jeśli ustawisz 3600s, urządzenie będzie wysyłać żądanie do serwera NPT w celu aktualizacji czasu co 3600 sekund.
- **Bieżący** czas: wyświetla bieżący czas urządzenia.

Ustawienie LED

Ustawienie diody LED w obszarze czytnika kart

W interfejsie internetowym można włączyć lub wyłączyć oświetlenie LED w obszarze czytnika kart. Tymczasem, jeśli nie chcesz, aby światło LED w obszarze czytnika kart pozostawało włączone, możesz również ustawić dokładny czas, w którym światło LED może być wyłączone w celu zmniejszenia zużycia energii elektrycznej.

Aby ją skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **Light**.



- **Backlight Enabled**: Włączenie/wyłączenie diody LED w obszarze czytnika kart.
- **Czas rozpoczęcia - Czas zakończenia (godzina)**: Wprowadź zakres czasu, w którym oświetlenie LED ma obowiązywać, np. jeśli zakres czasu wynosi od 18-22, oznacza to, że światło LED pozostanie włączone w przedziale czasowym od 18:00 do 22:00 w ciągu jednego dnia (24 godziny).

Ustawienie białego światła LED

Białe światło LED jest używane głównie do wzmocnienia oświetlenia dostępu do kodu QR i dla większej widoczności odwiedzających, gdy widzą swoje zdjęcia z wnętrza w ciemnym otoczeniu.

Aby ją skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **Light**.

- **Tryb** :
  - **Auto** : Białe światło zostanie włączone automatycznie podczas rozpoznawania twarzy i skanowania kodu QR w celu otwarcia drzwi.

- **Wyłączone**: Białe światło jest wyłączone.

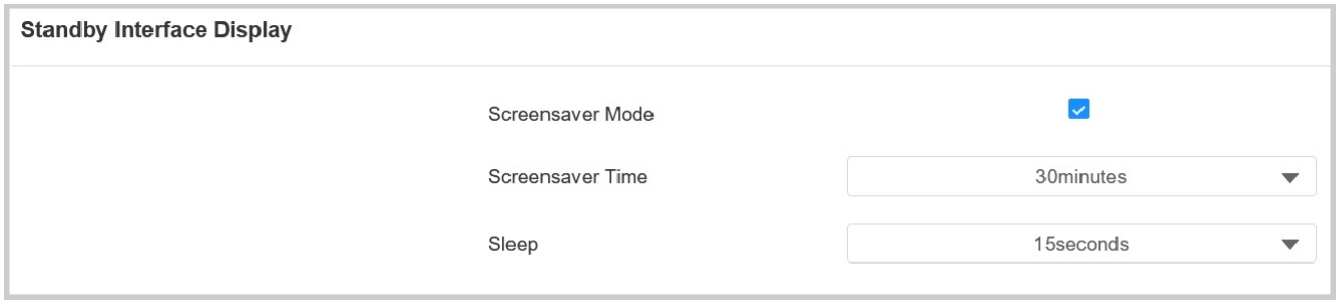
- **Maksymalna wartość światła** białego: Ustaw wartość światła białego w zakresie 1-5, a domyślna wartość światła białego to 3. Im większa wartość, tym jaśniejsze będzie światło.

Konfiguracja ekranu

Konfiguracja wygaszacza ekranu

Konfigurację ekranu oczekiwania można przeprowadzić w interfejsie internetowym, w którym można ustawić czas trwania wygaszacza ekranu, a także czas wyłączenia ekranu zarówno w celu ochrony ekranu, jak i zmniejszenia zużycia energii.

Aby ją skonfigurować, przejdź do opcji **Urządzenie > LCD > Interfejs wyświetlacza w** trybie **gotowości**.



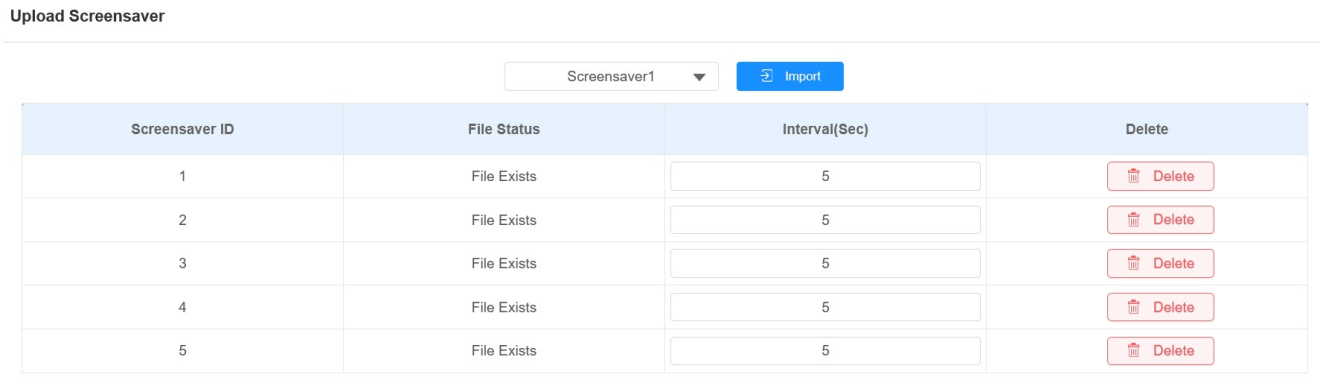
- **Czas wygaszacza ekranu (sek.)**: Ustaw czas uruchomienia wygaszacza ekranu w zakresie od 5 sekund do 2 godzin. Na przykład, jeśli ustawisz czas rozpoczęcia na 5 minut, wygaszacz ekranu uruchomi się, jeśli na urządzeniu nie będą wykonywane żadne operacje lub nikt nie zbliży się do urządzenia w ciągu pięciu minut.

- **Uśpienie** : Ustaw czas trwania wygaszacza ekranu przed wyłączeniem ekranu urządzenia. Czas trwania wygaszacza ekranu można wybrać w zakresie od 2 sekund do 30 minut.

Prześlij wygaszacz ekranu

Obrazy wygaszacza ekranu można przesyłać osobno lub partiami do urządzenia i do interfejsu internetowego urządzenia w celach reklamowych lub dla lepszych wrażeń wizualnych.

Aby go skonfigurować, przejdź do interfejsu **Device > LCD > Upload Screensaver**. Kliknij Import, aby załadować plik i kliknij **Delete**, aby usunąć istniejący plik.



Uwaga

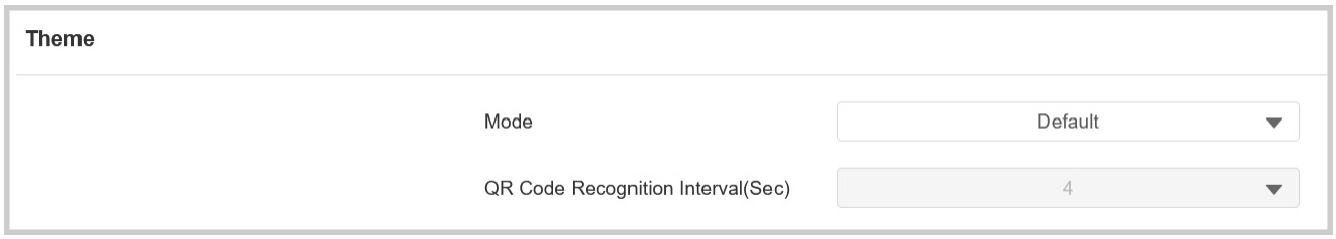
- Przesłane zdjęcia powinny być w formacie JPG lub PNG z maksymalnie 2M pikseli.
- Zalecana rozdzielczość: 600×1024.
- Poprzednie zdjęcia z określoną kolejnością ID zostaną nadpisane, gdy nastąpi powtarzające się oznaczenie zdjęć do tej samej kolejności ID.

Tryb wyświetlania ekranu

Można wybrać tryb wyświetlania Domyślny lub Kod QR odpowiednio dla rozpoznawania twarzy i skanowania kodu QR.

Aby ją

- skonfigurować, przejdź do opcji **Urządzenie > LCD >** Interfejs **motywu**.

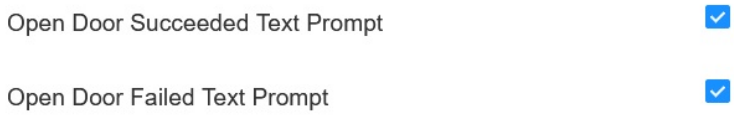


- **QR Code Recognition Interval(Sec)**: Ustawienie interwału rozpoznawania pomiędzy skanowaniem kodu QR, gdy wybrany jest tryb QR Code.

Tekst monitu dostępu do drzwi

Komunikat tekstowy o otwarciu drzwi można włączyć zarówno w przypadku pomyślnego, jak i niepomyślnego otwarcia drzwi. Aby ją skonfigurować, przejdź do opcji **Access Control > Relay > Door Setting General** interface.

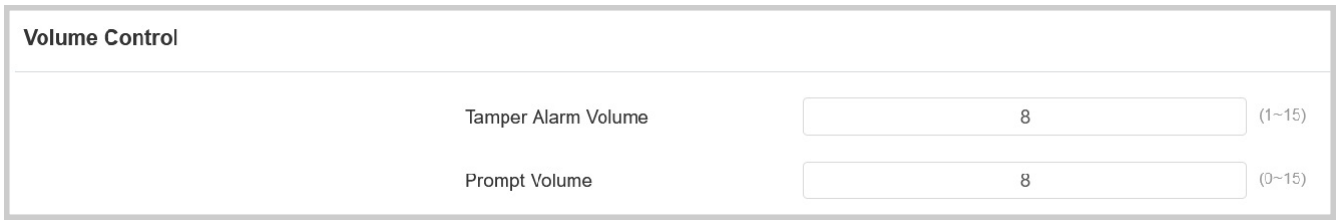
Door Setting General



Konfiguracja głośności i tonów obejmuje ustawienia alarmu sabotażowego i głośności monitu. Ponadto można przesłać dźwięki dzwonka otwierania drzwi.

Konfiguracja głośności

Aby go skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **audio**.



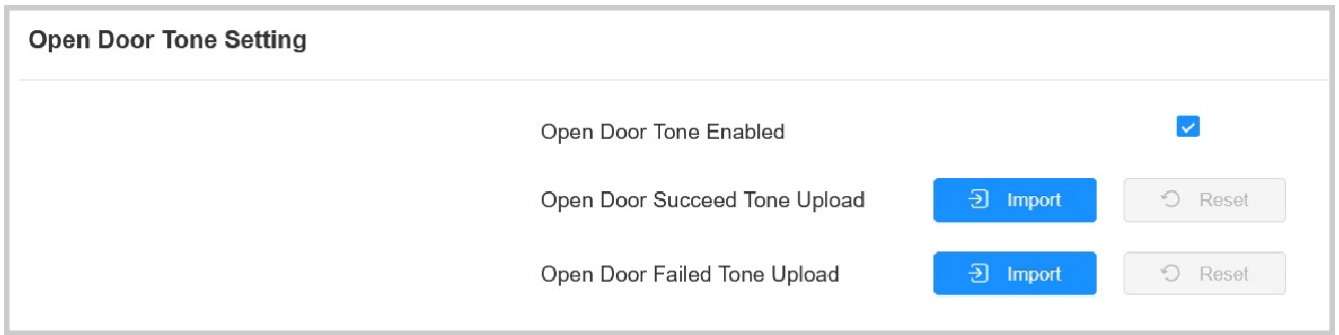
- **Głośność alarmu** sabotażowego: Ustaw głośność, gdy alarm sabotażowy jest wyzwalany. Domyślna głośność to 8.

- **Głośność komunikatów**: Ustaw głośność komunikatów głosowych. Domyślna głośność to 8.

Prześlij dźwięk otwartych drzwi

Sygnał dźwiękowy informujący o niepowodzeniu i powodzeniu otwarcia drzwi można przesłać w interfejsie internetowym urządzenia.

Aby go skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **audio**. Kliknij **Importuj**, aby przesłać plik i kliknij **Resetuj**, aby usunąć plik.



Uwaga

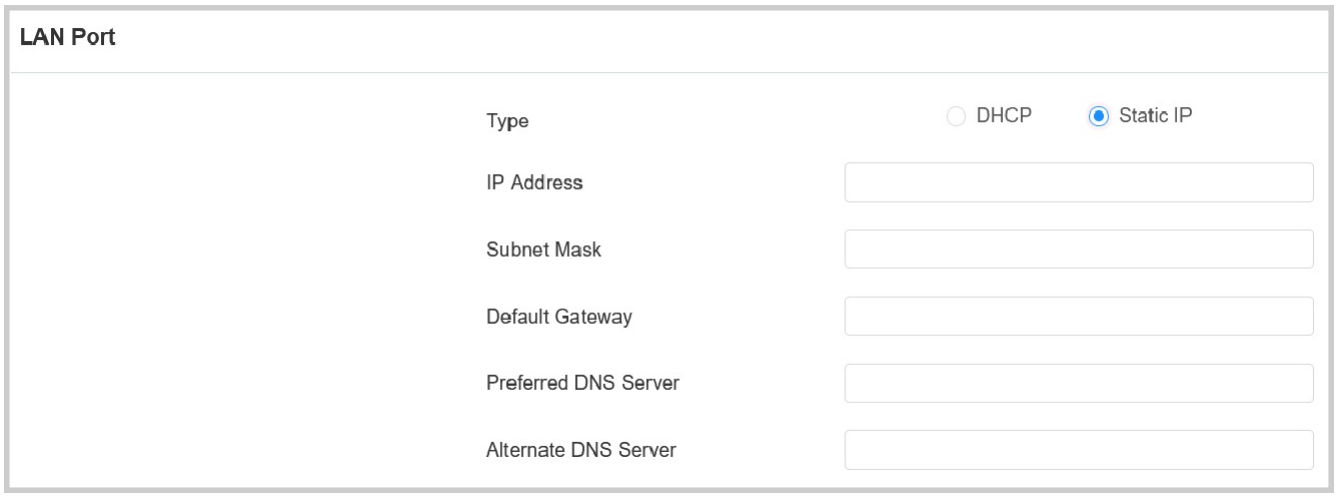
Format pliku: wav, rozmiar: < 200KB, częstotliwość próbkowania: 16000, Bity: 16

Ustawienia sieciowe

Urządzenie Połączenie sieciowe

Aby zapewnić normalne działanie, należy upewnić się, że adres IP urządzenia jest ustawiony prawidłowo lub został uzyskany automatycznie z serwera DHCP.

Aby go skonfigurować, przejdź do opcji **Sieć > Podstawowe >** Interfejs **portu LAN**.

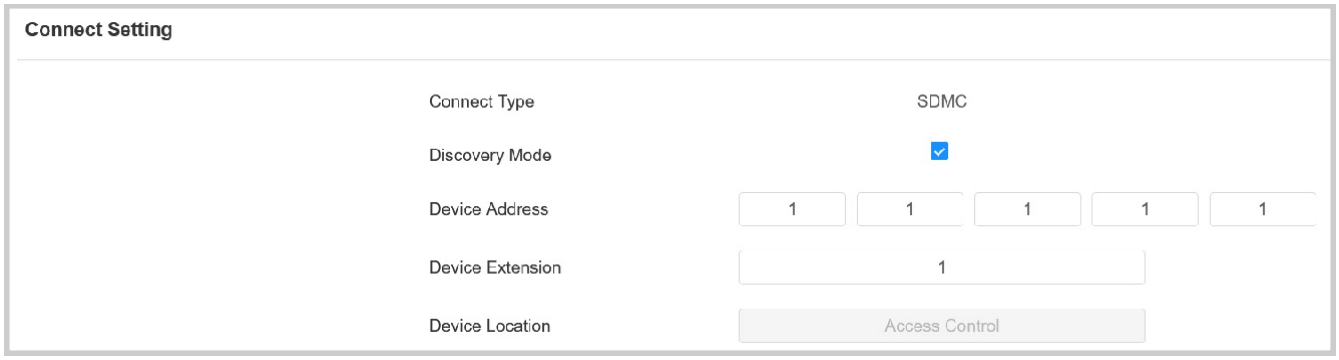


- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Po wybraniu trybu DHCP terminal kontroli dostępu zostanie automatycznie przypisany przez serwer DHCP z adresem IP, maską podsieci, bramą domyślną i adresem serwera DNS.
- **Statyczne IP**: Po wybraniu trybu statycznego IP, adres IP, maska podsieci, brama domyślna i adres serwera DNS powinny być skonfigurowane zgodnie ze środowiskiem sieciowym.
- **Adres IP**: Ustawienie adresu IP w przypadku wybrania statycznego trybu IP.
- **Maska podsieci**: Ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Brama domyślna**: Ustaw prawidłową bramę zgodnie z adresem IP.
- **Preferowany/alternatywny serwer DNS**: Skonfiguruj preferowany lub alternatywny serwer DNS (Domain Name Server) zgodnie z rzeczywistym środowiskiem sieciowym. Preferowany serwer DNS jest serwerem podstawowym, podczas gdy alternatywny serwer DNS jest serwerem dodatkowym. Serwer dodatkowy służy do tworzenia kopii zapasowych.

Wdrażanie urządzeń w sieci

Aby ułatwić kontrolę i zarządzanie urządzeniami, skonfiguruj urządzenia interkomowe Akuvox, podając szczegóły, takie jak lokalizacja, tryb pracy, adres i numery wewnętrzne.

Aby ją skonfigurować, przejdź do interfejsu **Network > Basic > Connect Setting**.



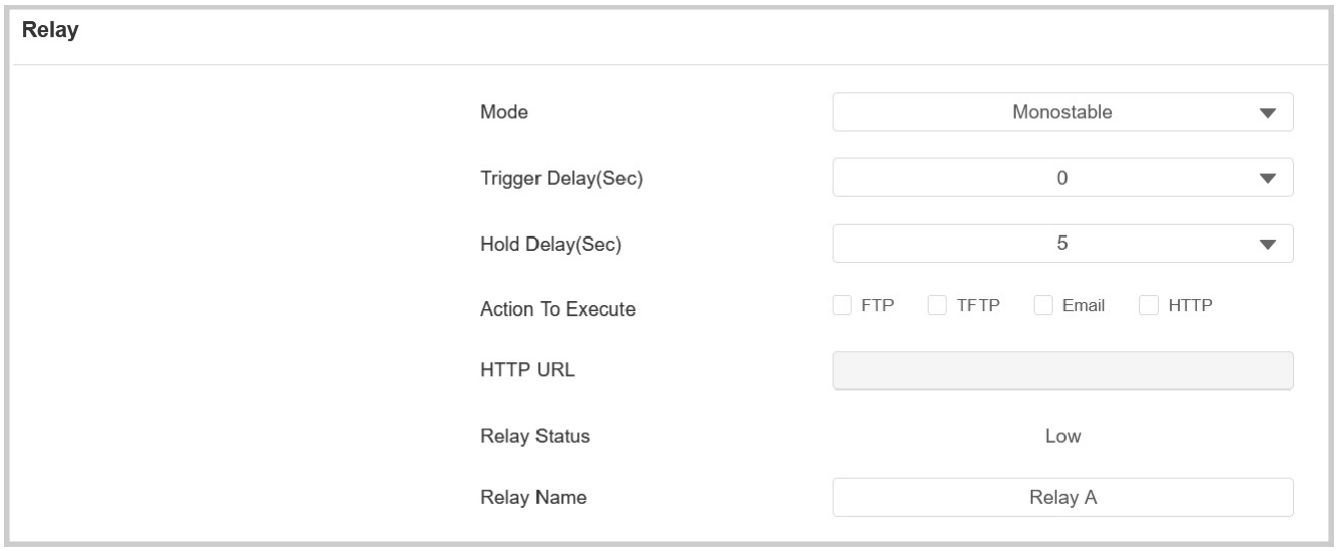
- **Typ połączenia** : Jest automatycznie konfigurowany zgodnie z rzeczywistym połączeniem urządzenia z określonym serwerem w sieci, takim jak SDMC, Cloud lub None. Brak jest domyślnym ustawieniem fabrycznym wskazującym, że urządzenie nie jest podłączone do żadnego typu serwera.
- **Tryb wykrywania** : Po włączeniu urządzenie może być wykrywane przez inne urządzenia w sieci. Po wyłączeniu urządzenie będzie ukryte i nie będzie wykrywane przez inne urządzenia.
- **Adres urządzenia** : Określ adres urządzenia, wprowadzając informacje o lokalizacji urządzenia od lewej do prawej: Community (Społeczność), Unit (Jednostka), Stair (Schody), Floor (Piętro) i Room (Pokój) w kolejności.
- **Rozszerzenie urządzenia**: Numer wewnętrzny urządzenia.
- **Lokalizacja urządzenia**: Lokalizacja, w której urządzenie jest zainstalowane i używane.

Ustawienie przekaźnika

Przełączniki przekaźnikowe dostępu do drzwi można skonfigurować w interfejsie internetowym.

Przełącznik przekaźnika

Aby skonfigurować przekaźnik, przejdź do opcji **Kontrola dostępu > Przekaźnik >** Interfejs **przekaźnika**.



- **Tryb** : Określa warunki automatycznego resetowania stanu przekaźnika.
    - **Monostabilny**: Status przekaźnika resetuje się automatycznie w czasie opóźnienia przekaźnika po aktywacji.
    - **Bistabilny**: Stan przekaźnika resetuje się po ponownym wyzwoleniu przekaźnika.
- **Trigger Delay(Sec)**: Ustaw czas opóźnienia przed wyzwoleniem przekaźnika. Na przykład, jeśli ustawiono 5 sekund, przekaźnik aktywuje się 5 sekund po naciśnięciu przycisku odblokowania.
- **Hold Delay(Sec)**: Określa, jak długo przekaźnik pozostaje aktywny. Na przykład, jeśli ustawione na 5 sekund, przekaźnik pozostanie otwarty przez 5 sekund przed zamknięciem.
- **Akcja do wykonania**: Sprawdź akcję, która ma zostać wykonana po wyzwoleniu przekaźnika.
    - **FTP**: wysłanie zrzutu ekranu na wstępnie skonfigurowany serwer FTP.
    - **TFTP**: wysłanie zrzutu ekranu na wstępnie skonfigurowany serwer TFTP.
    - **E-mail**: Wyślij zrzut ekranu na wstępnie skonfigurowany adres e-mail.

- **HTTP**: Po uruchomieniu, komunikat HTTP może zostać przechwycony i wyświetlony w odpowiednich pakietach. Aby skorzystać z tej funkcji, należy włączyć serwer HTTP i wprowadzić treść wiadomości w wyznaczonym polu poniżej.

- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/Treść wiadomości.
- **Status** przekaźnika: Wskazuje stany przekaźnika, które są normalnie otwarte i zamknięte. Domyślnie pokazuje stan niski dla normalnie zamkniętego (NC) i wysoki dla normalnie otwartego (NO).

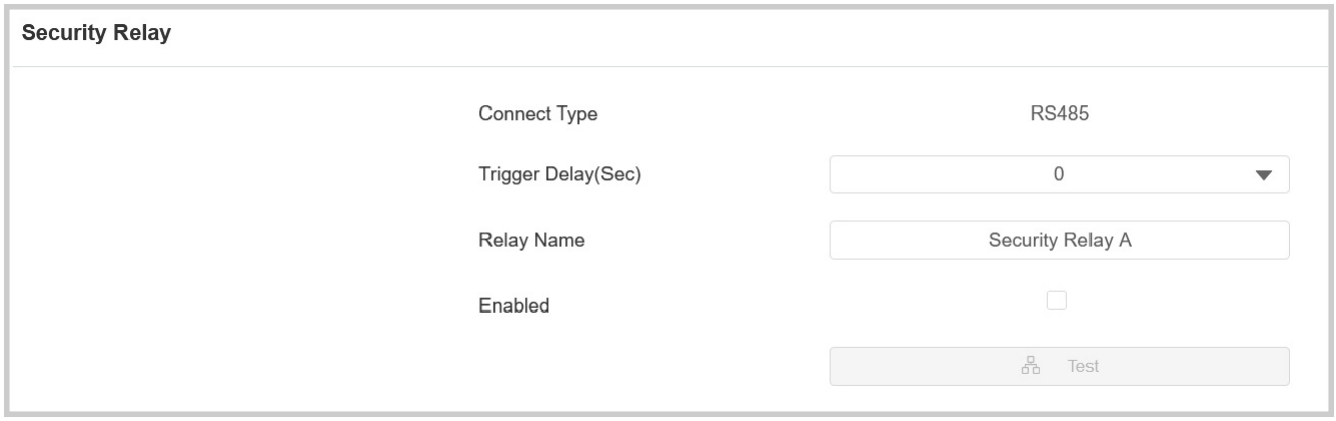
- **Nazwa przekaźnika**: Przypisz odrębną nazwę w celu identyfikacji.

> **Uwaga**
>
> Urządzenia zewnętrzne podłączone do przekaźnika wymagają osobnych zasilaczy.

Przekaźnik bezpieczeństwa

Przekaźnik bezpieczeństwa, znany jako Akuvox SR01, to produkt zaprojektowany w celu wzmocnienia bezpieczeństwa dostępu poprzez zapobieganie nieautoryzowanym próbom wymuszonego wejścia. Zainstalowany wewnątrz drzwi, bezpośrednio steruje mechanizmem otwierania drzwi, zapewniając, że drzwi pozostaną bezpieczne nawet w przypadku uszkodzenia urządzenia.

Aby go skonfigurować, przejdź do opcji **Kontrola dostępu > Przekaźnik >** Interfejs **przekaźnika zabezpieczeń**.



- **Typ połączenia** : Przekaźnik bezpieczeństwa domyślnie łączy się z urządzeniem za pomocą RS485.

- **Trigger Delay(Sec)**: Ustaw czas opóźnienia przed wyzwoleniem przekaźnika. Na przykład, jeśli ustawiono 5 sekund, przekaźnik aktywuje się 5 sekund po naciśnięciu przycisku odblokowania.

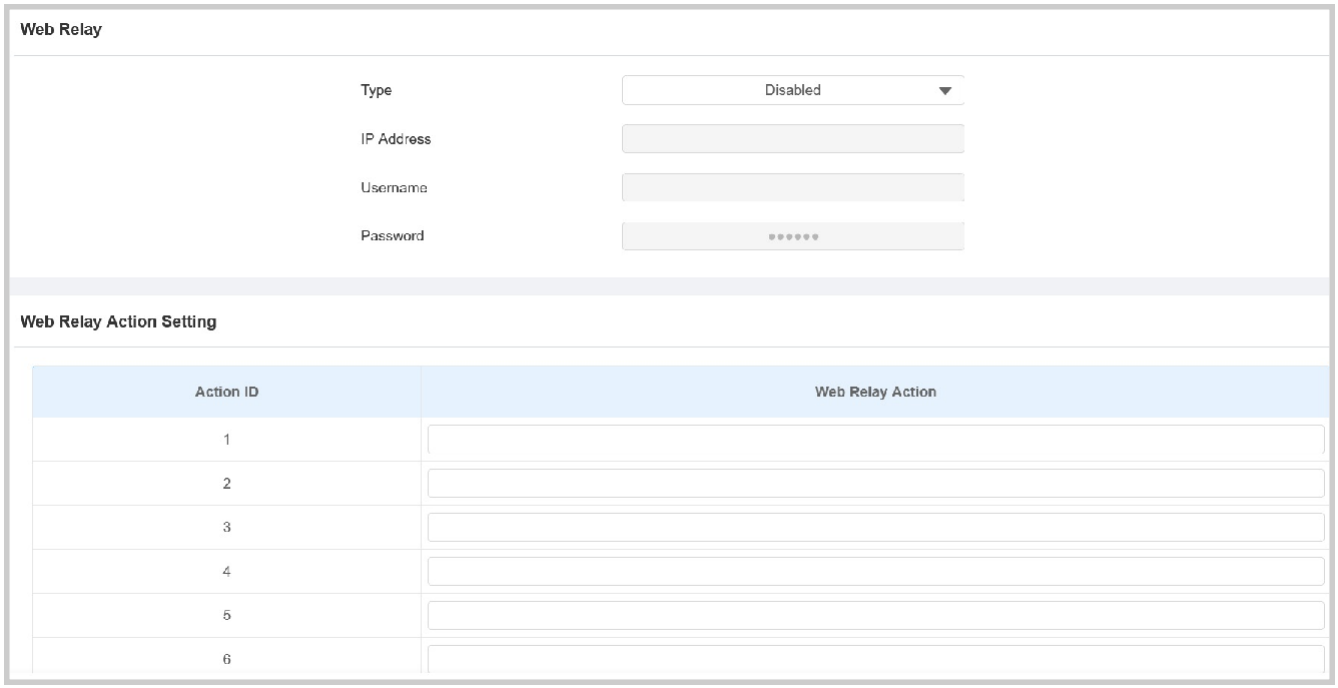
- **Nazwa przekaźnika** : Nazwa przekaźnika bezpieczeństwa. Nazwa może być wyświetlana w dziennikach otwarcia drzwi.

  Podczas łączenia się z chmurą SmartPlus Cloud serwer chmury automatycznie przypisze nazwę przekaźnika.

Przekaźnik internetowy

Przekaźnik sieciowy ma wbudowany serwer sieciowy i może być sterowany przez Internet lub sieć lokalną. Urządzenie może używać przekaźnika sieciowego do sterowania lokalnym przekaźnikiem lub zdalnym przekaźnikiem w innym miejscu w sieci.

Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu >** Interfejs **Web Relay**.



- **Typ** : Określa typ przekaźnika aktywowanego podczas korzystania z metod dostępu do drzwi.
    - **Wyłączone**: Aktywuje tylko lokalny przekaźnik.
    - **Przekaźnik sieciowy**: Aktywuj tylko przekaźnik sieciowy.
    - **Przekaźnik lokalny+przekaźnik sieciowy**: Aktywuje zarówno przekaźnik lokalny, jak i internetowy. Zazwyczaj najpierw uruchamiany jest przekaźnik lokalny, a następnie przekaźnik sieciowy w celu wykonania wcześniej skonfigurowanych działań.
- **Adres IP**: Adres IP przekaźnika sieciowego dostarczony przez producenta przekaźnika sieciowego.
- **Nazwa użytkownika**: Nazwa użytkownika podana przez producenta przekaźnika sieciowego.
- **Hasło** : Klucz uwierzytelniania dostarczony przez producenta dla przekaźnika internetowego. Uwierzytelnianie odbywa się za pośrednictwem protokołu HTTP. Pozostawienie pustego pola Hasło oznacza nieużywanie uwierzytelniania HTTP. Hasło można zdefiniować za pomocą HTTP GET w polu Web Relay Action.
- **Web Relay Action**: Skonfiguruj akcje, które mają być wykonywane przez przekaźnik sieciowy po wyzwoleniu. Wprowadź dostarczone przez producenta adresy URL dla różnych działań, zawierające do 50 poleceń.

Uwaga

Jeśli adres URL zawiera pełną zawartość HTTP (np. http://admin:admin@192.168.1.2/state.xml? relayState=2), nie opiera się na adresie IP wprowadzonym powyżej. Jeśli jednak adres URL jest prostszy (np. "state.xml?relayState=2"), przekaźnik używa wprowadzonego adresu IP.

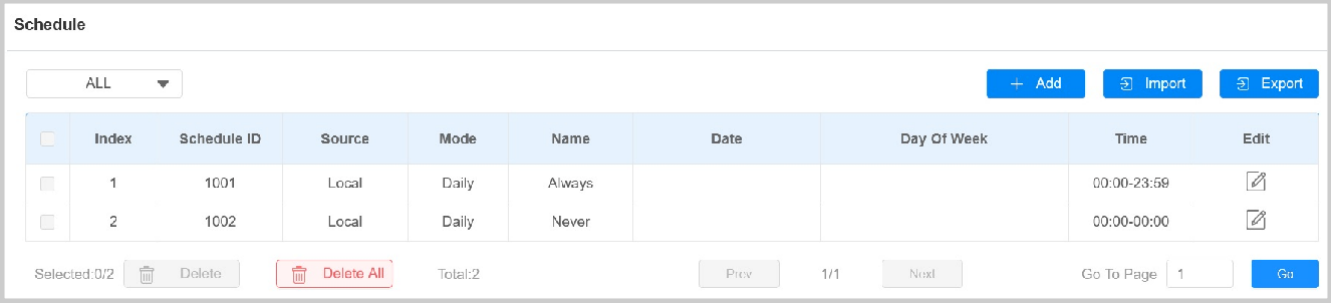
Zarządzanie harmonogramem dostępu do drzwi

Harmonogram dostępu do drzwi

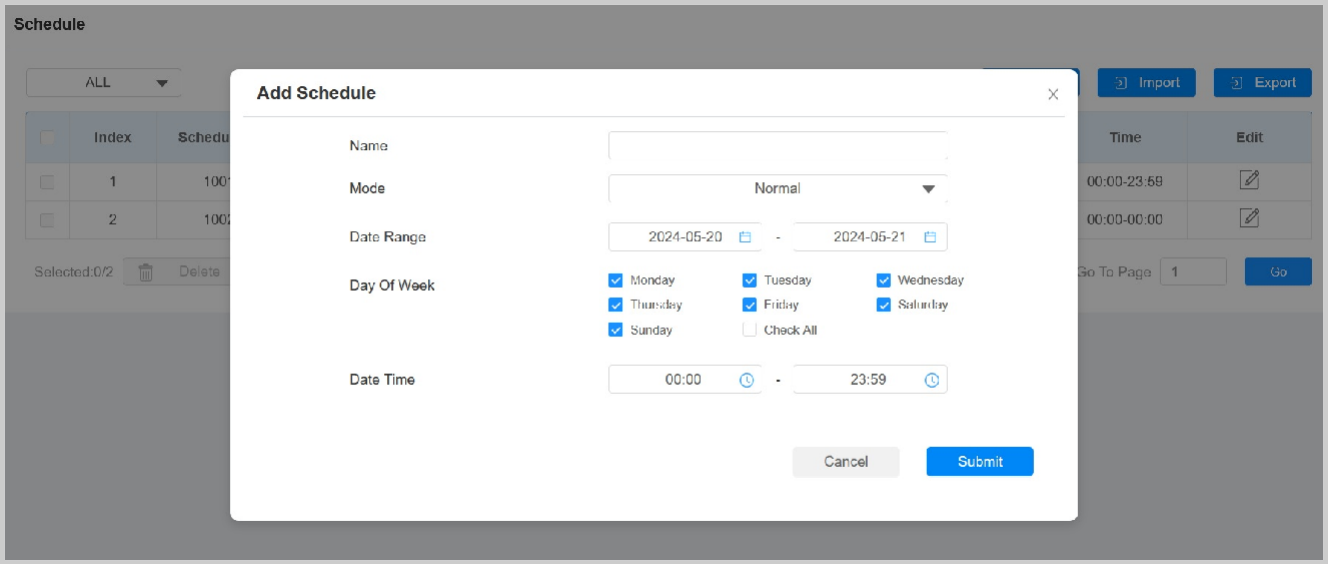
Harmonogram dostępu do drzwi pozwala zdecydować, kto i kiedy może otworzyć drzwi. Dotyczy to zarówno pojedynczych osób, jak i grup, zapewniając, że użytkownicy w ramach harmonogramu mogą otwierać drzwi przy użyciu autoryzowanej metody tylko w wyznaczonych okresach czasu.

Tworzenie harmonogramu dostępu do drzwi

Aby utworzyć harmonogram dostępu do drzwi, przejdź do interfejsu **Setting > Schedule**.



Kliknij **+Dodaj**, aby utworzyć harmonogram.



- **Nazwa**: Nazwa harmonogramu.
- **Tryb** :
  - **Normalny**: Ustaw harmonogram na podstawie miesiąca, tygodnia i dnia. Służy do tworzenia harmonogramów na długie okresy.

- **Tygodniowy**: Ustaw harmonogram na podstawie tygodnia.
- **Codziennie**: Ustaw harmonogram w oparciu o 24 godziny na dobę.

Harmonogram importu i eksportu dostępu do drzwi

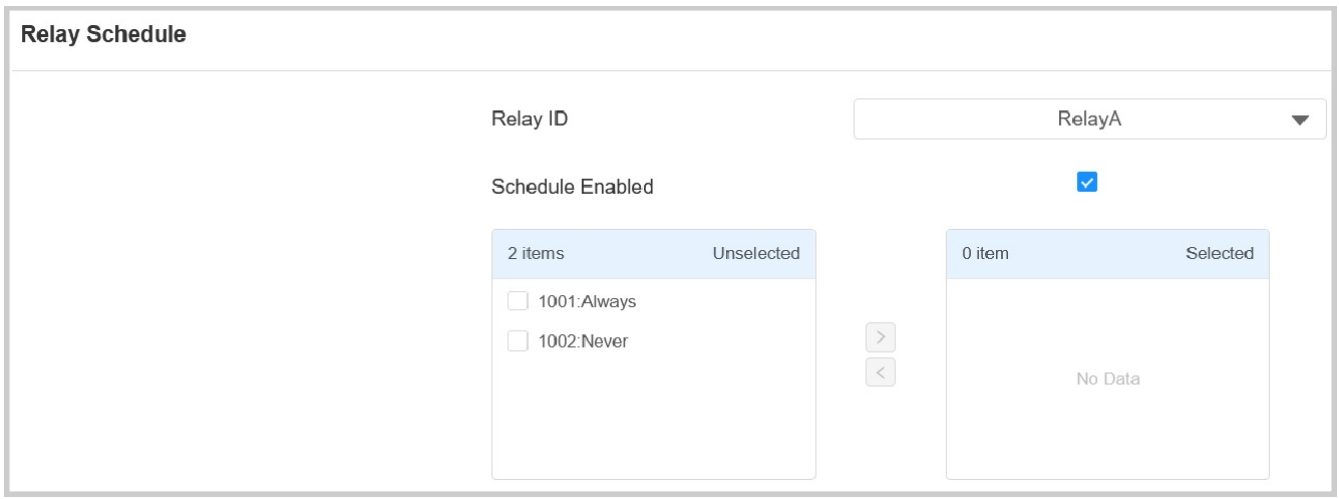
Harmonogramy dostępu do drzwi można tworzyć pojedynczo lub zbiorczo. Można wyeksportować bieżący plik harmonogramu, edytować go lub dodać więcej harmonogramów zgodnie z formatem, a następnie zaimportować nowy plik do wybranych urządzeń. Ułatwia to zarządzanie harmonogramami dostępu do drzwi.

Aby go skonfigurować, przejdź do interfejsu **Ustawienia > Harmonogram**. Plik eksportu jest w formacie **TGZ**. Plik importu powinien być w formacie **XML**.

Harmonogram przekaźników

Harmonogram przekaźnika umożliwia ustawienie konkretnego przekaźnika tak, aby zawsze otwierał się o określonej godzinie. Jest to przydatne w takich sytuacjach, jak utrzymywanie otwartej bramy po szkole lub utrzymywanie otwartych drzwi w godzinach pracy.

Aby ją skonfigurować, przejdź do interfejsu **Access Control > Relay > Relay Schedule**.



- **Identyfikator przekaźnika**: Określ przekaźnik, który chcesz skonfigurować.
- **Schedule Enabled:** Przypisz określone harmonogramy dostępu do drzwi do wybranego przekaźnika. Wystarczy przenieść je do pola Selected Schedules (Wybrane harmonogramy).

Instrukcje dotyczące tworzenia harmonogramów można znaleźć w sekcji Tworzenie harmonogramu dostępu do drzwi.

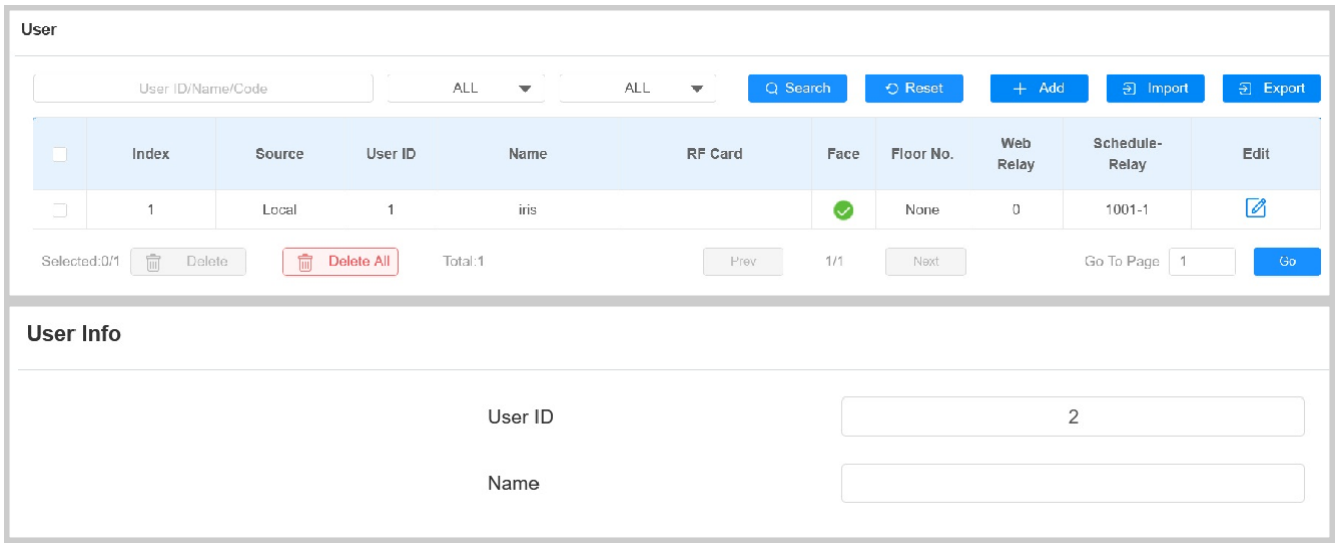
Konfiguracja odblokowania drzwi

Metody dostępu specyficzne dla użytkownika

Prywatna karta RF i ustawienie twarzy powinny być przypisane do konkretnego użytkownika w celu otwarcia drzwi.

Podczas dodawania użytkownika można również dostosować ustawienia, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenie, który przekaźnik ma zostać otwarty.

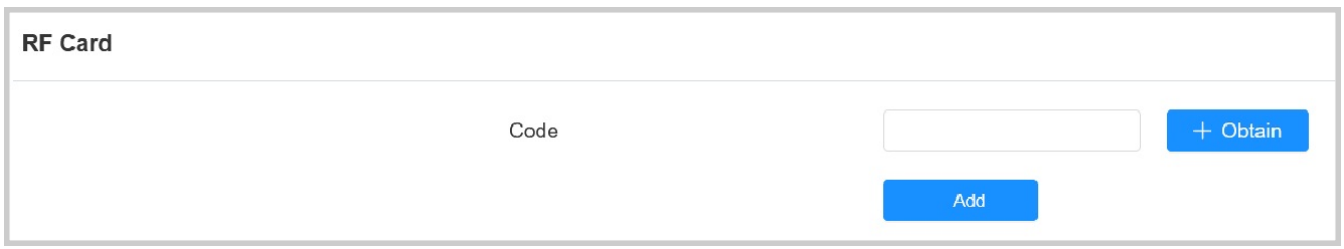
Aby dodać użytkownika, przejdź do **Katalog >** Interfejs **użytkownika** i kliknij **+Dodaj** .



- **Identyfikator użytkownika**: unikalny numer identyfikacyjny przypisany do użytkownika.
- **Nazwa**: nazwa tego użytkownika.

Odblokowanie za pomocą karty RF

W interfejsie **Directory > User > +Add** przewiń do sekcji **RF Card**.



- **Kod** : Numer karty odczytywany przez czytnik kart.

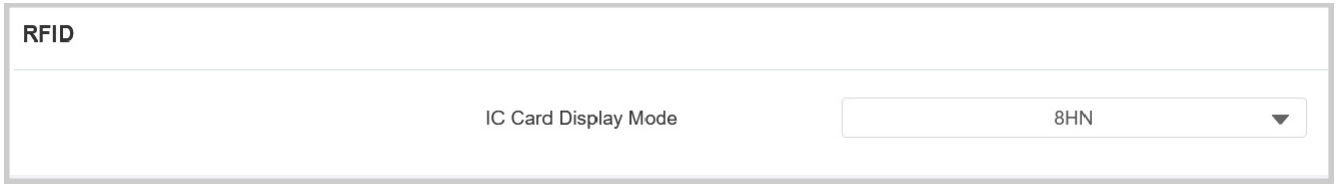
Uwag

- Każdy użytkownik może dodać maksymalnie 5 kart.
- Urządzenie pozwala na dodanie 20 000 użytkowników.
- Karty RF działające na częstotliwościach 13,56 MHz są kompatybilne z urządzeniem w zakresie dostępu.
- A05 obsługuje tylko karty IC.

Format kodu karty RF

Aby zintegrować dostęp do drzwi za pomocą karty RF z systemem interkomowym innej firmy, należy dopasować format kodu karty RF do formatu używanego przez system innej firmy.

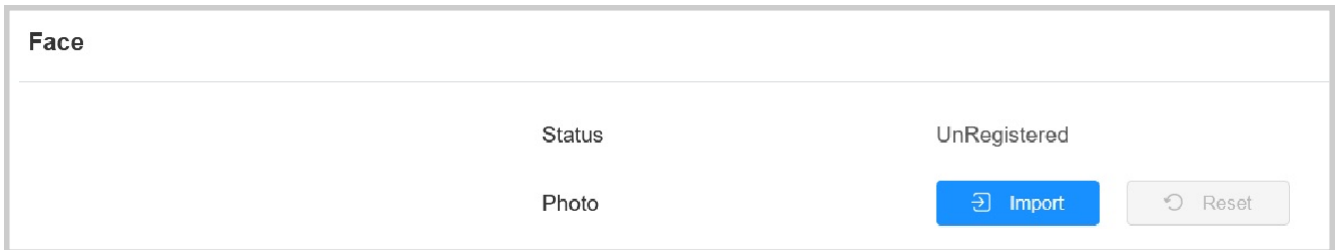
Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu > Ustawienia karty >** Interfejs **RFID**.



- **Tryb wyświetlania karty IC** : Ustaw format numeru karty spośród dostępnych opcji. Domyślnym formatem w urządzeniu jest 8HN.

Odblokowywanie przez rozpoznawanie twarzy

W interfejsie **Directory > User > +Add** przewiń do sekcji **Face**. Kliknij **Importuj**, aby przesłać plik i kliknij **Resetuj**, aby go usunąć.



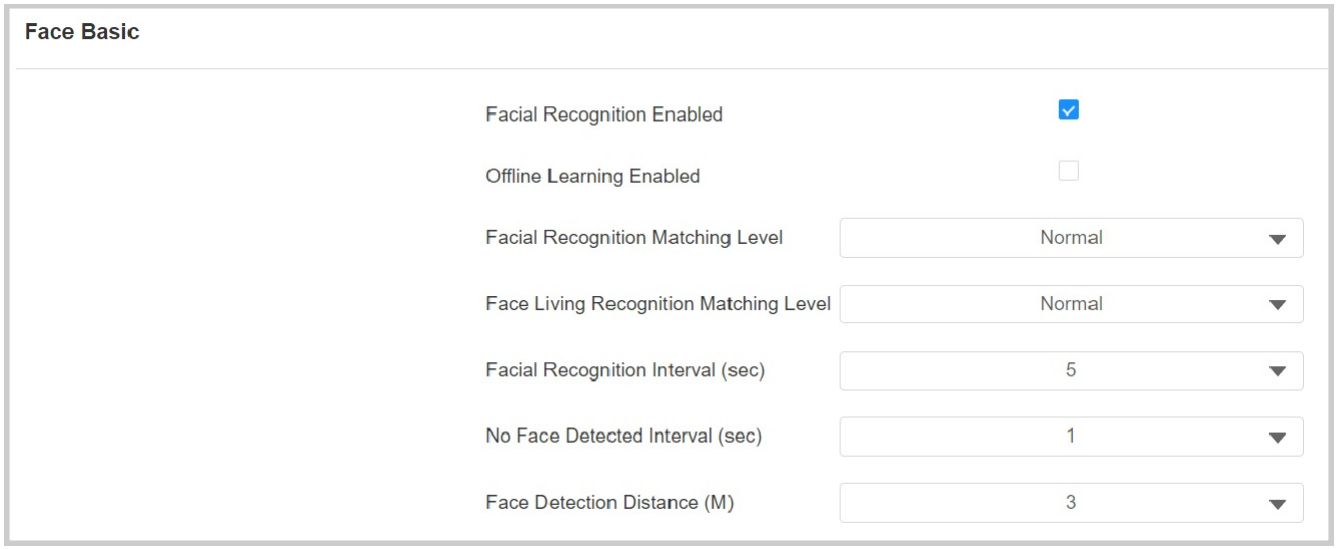
Uwaga

Obsługiwane formaty: jpg, png, bmp i jpeg.

Ustawienia twarzy

Możesz dostosować dokładność rozpoznawania twarzy, interwały rozpoznawania i wiele więcej, aby poprawić komfort użytkowania.

Aby ją skonfigurować, przejdź do interfejsu **Access Control > Face Setting**.



- **Facial Recognition Enabled**: Włączenie/wyłączenie funkcji rozpoznawania twarzy.
- **Offline Learning Enabled**: Dokładność rozpoznawania twarzy poprawia się wraz ze wzrostem liczby rozpoznań twarzy.
- **Poziom dopasowania rozpoznawania twarzy**: Określa, jak rygorystyczny jest system rozpoznawania twarzy w porównywaniu twarzy osoby z przesłanymi danymi twarzy. Każdy poziom pozwala na inny stopień różnicy lub zakrycia twarzy (**z wyjątkiem obszaru ust**), aby przejść rozpoznanie.

- Niski: pozwala na niewielkie różnice w stosunku do przesłanych danych twarzy, przy niewielkim pokryciu twarzy.

- Najwyższy: Wymaganie, aby twarz była identyczna z przesłaną, z minimalnym lub zerowym zakryciem.

- Pozostałe dwa poziomy znajdują się pomiędzy nimi.

- **Poziom dopasowania rozpoznawania twarzy**: Określa, jak rygorystyczny jest system w zapobieganiu fałszywym twarzom.

- Zamknij: Wyłączenie funkcji antyspoofingu twarzy. Weryfikacja twarzy może zostać przeprowadzona przy użyciu nieożywionych substytutów twarzy autoryzowanej osoby, takich jak zdjęcie.

- Najwyższy: System nie może zostać oszukany przez żadne nieożywione substytuty twarzy autoryzowanej osoby.

- Pozostałe trzy poziomy znajdują się pomiędzy nimi.

Interwał rozpoznawania twarzy(sek): Umożliwia dostosowanie odstępu czasu między kolejnymi próbami rozpoznania twarzy w zakresie od 1 do 8 sekund.

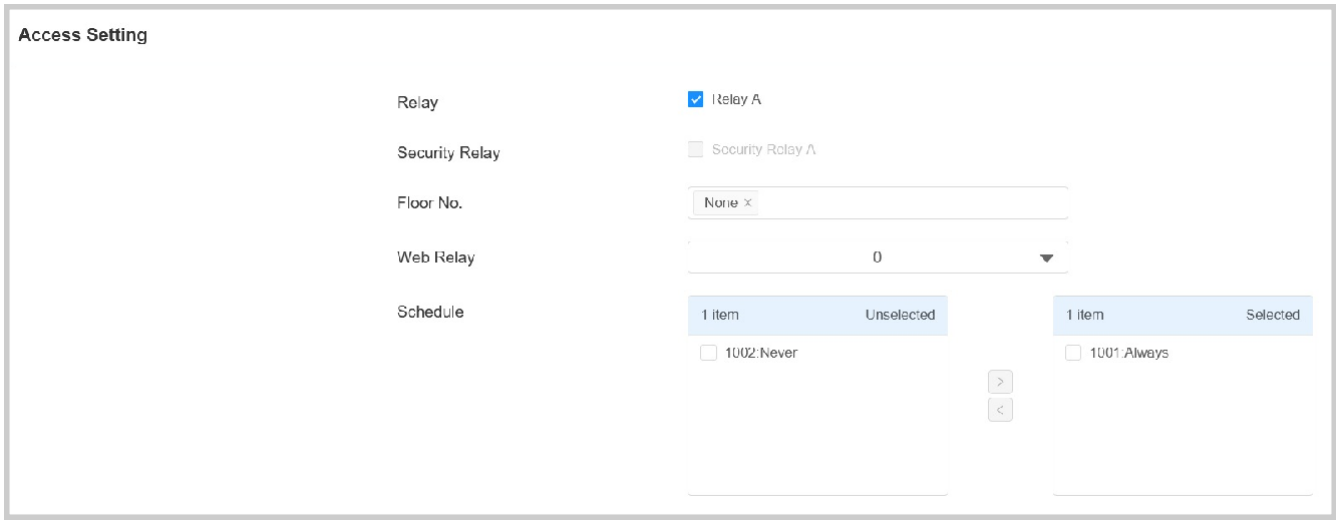
No Face Detected Interval(sec): Umożliwia dostosowanie odstępu czasu między kolejnymi próbami rozpoznania twarzy po pomiarze temperatury.

- **Odległość wykrywania twarzy (M)**: Określa efektywną odległość rozpoznawania twarzy.

Ustawienia dostępu

Możesz dostosować ustawienia dostępu, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenie, który przekaźnik ma zostać otwarty.

W interfejsie **Directory > User > +Add** przewiń do sekcji **Access Setting**.



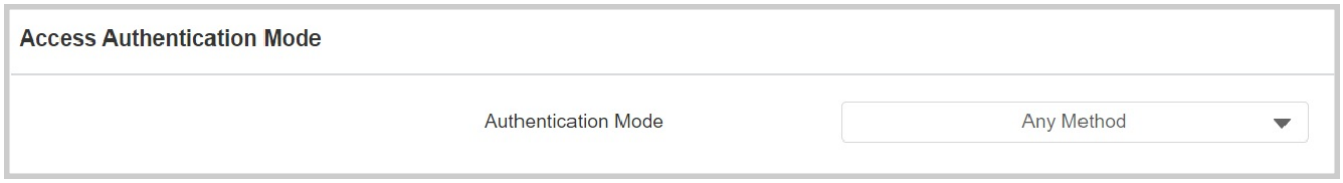
- **Przekaźnik**: Określenie przekaźników, które mają zostać odblokowane przy użyciu metod otwierania drzwi przypisanych do użytkownika.
- **Przekaźnik zabezpieczeń**: Zaznacz Security Relay A, jeśli został skonfigurowany na interfejsie Security Relay.
- **Nr piętra**: Określ piętro (piętra) dostępne dla użytkownika za pośrednictwem windy.
- **Web Relay**: Określa identyfikator poleceń akcji web relay skonfigurowanych w interfejsie Web Relay. Domyślna wartość 0 oznacza, że przekaźnik sieciowy nie będzie uruchamiany.
- **Harmonogram** : Przyznaj użytkownikowi dostęp do otwierania wyznaczonych drzwi w ustalonych okresach, przenosząc żądany harmonogram (harmonogramy) z lewego pola do prawego. Oprócz niestandardowych harmonogramów dostępne są 2 opcje domyślne:

- **Zawsze** : Zezwala na otwieranie drzwi bez ograniczeń liczby otwarć drzwi w ważnym okresie.
- **Nigdy**: Zabrania otwierania drzwi.

Tryb uwierzytelniania dostępu

Urządzenie umożliwia podwójne uwierzytelnianie dostępu do drzwi, wykorzystując kombinację rozpoznawania twarzy i karty RF. Po skonfigurowaniu trybu użytkownicy muszą odblokować drzwi w kolejności wybranych metod.

Aby ją skonfigurować, przejdź do interfejsu **Access Control > Relay > Access Authentication Mode**.



- **Tryb uwierzytelniania** : Określ sposób odblokowania drzwi przy użyciu różnych metod. Należy pamiętać, że kolejność uwierzytelniania dwuskładnikowego ma znaczenie.
  - **Dowolna metoda**: zezwala na wszystkie metody dostępu.
  - **Twarz + karta RF**: najpierw przejdź przez rozpoznawanie twarzy, a następnie przesuń kartę RF.

Odblokowanie przez NFC

NFC (Near Field Communication) to popularny sposób dostępu do drzwi. Wykorzystuje fale radiowe do interakcji transmisji danych. Urządzenie można odblokować za pomocą NFC. Telefon komórkowy można trzymać bliżej urządzenia w celu uzyskania dostępu do drzwi.

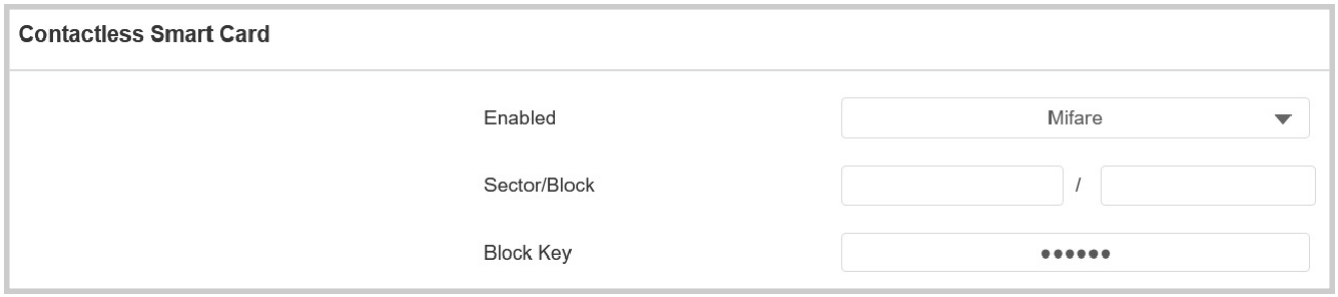
Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu > Ustawienia karty >** Interfejs **zbliżeniowej karty inteligentnej**.

- **Enabled** : Wybierz NFC z listy.

Karta Mifare

Bramofon może szyfrować karty Mifare w celu zwiększenia bezpieczeństwa. Gdy ta funkcja jest włączona, odczytuje dane w wyznaczonych sektorach i blokach karty, a nie identyfikator UID.

Aby ją skonfigurować, przejdź do opcji **Access Control > Card Setting > Contactless Smart Card** interface. Wybierz **Mifare** z listy.



- **Sector/Block**: Określa lokalizację, w której przechowywane są zaszyfrowane dane karty. Karta Mifare ma 16 sektorów (ponumerowanych od 0 do 15), a każdy sektor ma 4 bloki (ponumerowane od 0 do 3).

- **Block Key (Klucz bloku)**: Ustawienie hasła dostępu do danych zapisanych we wstępnie zdefiniowanym sektorze/bloku.

Odblokowanie przez Bluetooth

Aplikacja SmartPlus z obsługą Bluetooth umożliwia użytkownikom otwieranie drzwi bez użycia rąk. Mogą oni otwierać drzwi z aplikacją w kieszeni lub machać telefonem w kierunku urządzenia, gdy zbliżają się do drzwi.

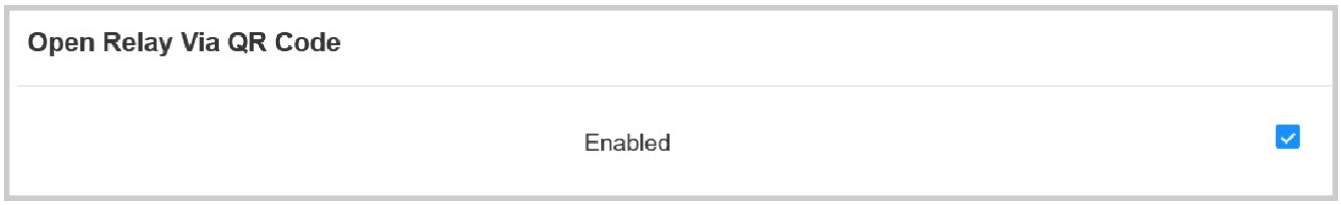
Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu >** Interfejs **BLE**.

- **Próg RSSI**: Ustawienie siły odbieranego sygnału. Wyższe wartości oznaczają większą siłę sygnału, co ułatwia odbieranie sygnału Bluetooth.

- **Open Door Interval (Sec)**: Ustawienie odstępu czasu między kolejnymi próbami uzyskania dostępu do drzwi przez Bluetooth.

Odblokowanie za pomocą kodu QR

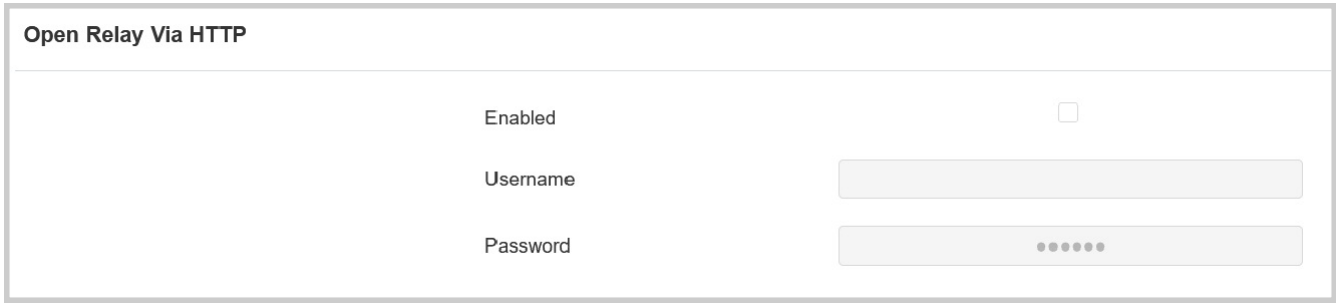
- Do otwarcia drzwi można użyć kodu QR. Ta metoda wymaga usługi w chmurze Akuvox SmartPlus. Przed użyciem tej funkcji należy ją aktywować.



Odblokowanie za pomocą polecenia HTTP

Możesz odblokować drzwi zdalnie, bez fizycznego zbliżania się do urządzenia w celu wejścia do drzwi, wpisując utworzone polecenie HTTP (URL) w przeglądarce internetowej, aby uruchomić przekaźnik, gdy nie jesteś dostępny przy drzwiach w celu wejścia do drzwi.

Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu > Przekaźnik > Otwórz przekaźnik przez** interfejs **HTTP**.



- **Nazwa użytkownika** : Ustaw nazwę użytkownika do uwierzytelniania w adresach URL poleceń HTTP.
- **Hasło**: ustawienie hasła do uwierzytelniania w adresach URL poleceń HTTP.

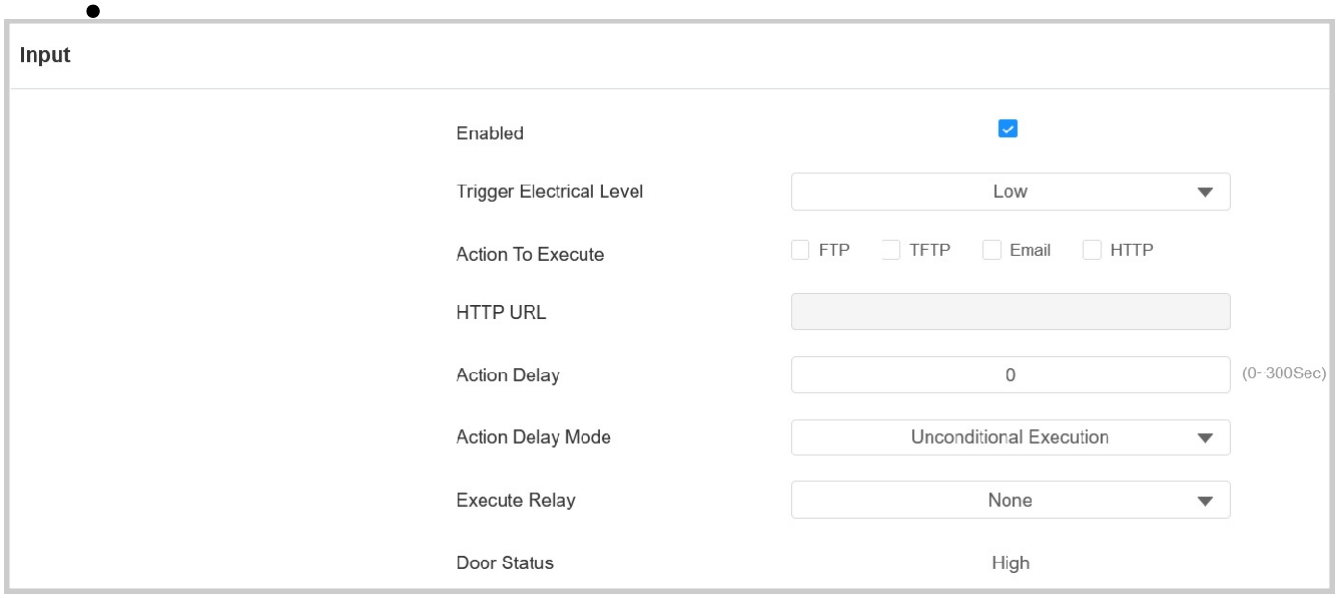
Wskazówka:

Oto przykład adresu URL polecenia HTTP dla wyzwalania przekaźnika.

Odblokowanie przyciskiem wyjścia

Gdy użytkownicy muszą otworzyć drzwi od wewnątrz, naciskając przycisk wyjścia, należy skonfigurować terminal wejściowy, który odpowiada przyciskowi wyjścia, aby aktywować przekaźnik dostępu do drzwi.

Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu >** Interfejs wejści**owy**.



- **Poziom wyzwalania elektrycznego**: Ustawienie wyzwalania interfejsu wejściowego na niskim lub wysokim poziomie elektrycznym.

- **Action To Execute**: Ustaw żądane działania, które wystąpią po wyzwoleniu określonego interfejsu wejściowego.

    - **FTP**: wysłanie zrzutu ekranu na wstępnie skonfigurowany serwer FTP.

    TFTP: wysłanie zrzutu ekranu na wstępnie skonfigurowany serwer TFTP.

    E-mail: Wyślij zrzut ekranu na wstępnie skonfigurowany adres e-mail.

    - **HTTP**: Po uruchomieniu, komunikat HTTP może zostać przechwycony i wyświetlony w odpowiednich pakietach. Aby skorzystać z tej funkcji, należy włączyć serwer HTTP i wprowadzić treść wiadomości w wyznaczonym polu poniżej.

- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/Treść wiadomości.

- **Opóźnienie akcji**: Określa, o ile sekund ma zostać opóźnione wykonanie wstępnie skonfigurowanych działań.

- **Tryb opóźnienia działania** :

    - **Bezwarunkowe wykonanie**: Akcja zostanie wykonana, gdy wejście zostanie wyzwolone.

    - **Execute If Input Still Triggered**: Akcja zostanie wykonana, gdy wejście pozostanie wyzwolone. Na przykład, jeśli drzwi pozostaną otwarte po wyzwoleniu wejścia, zostanie wysłana akcja, taka jak wiadomość e-mail, aby

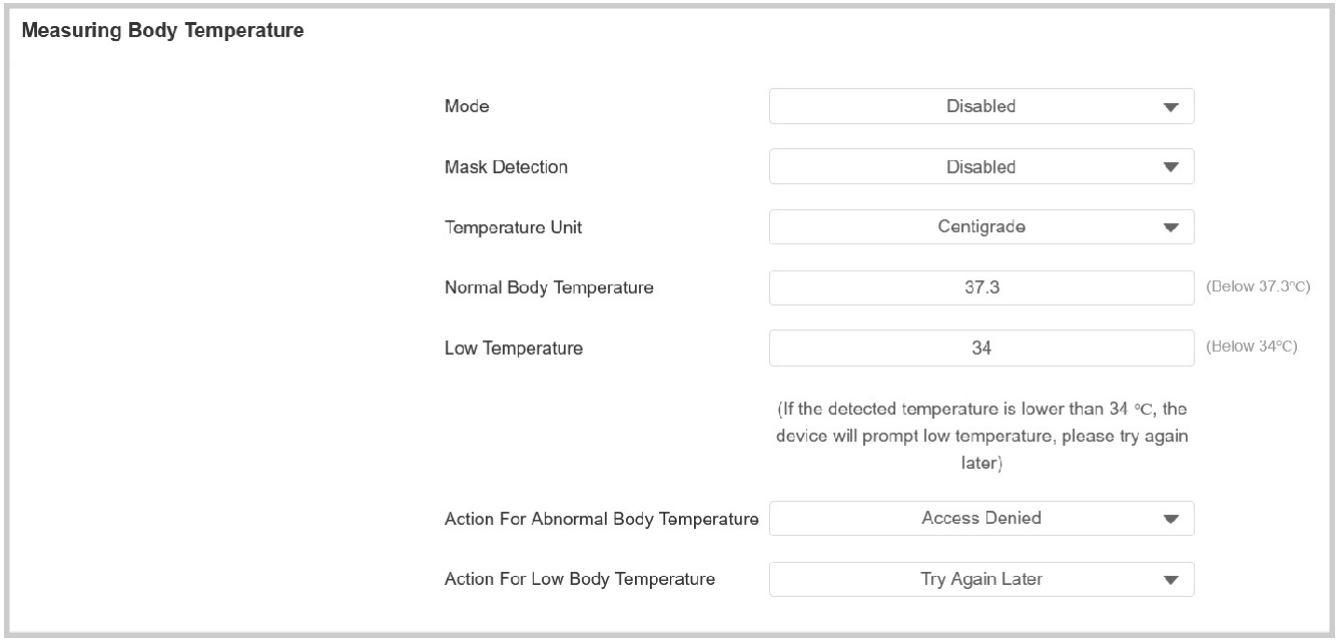
powiadomić odbiorcę.

- **Wykonaj przekaźnik**: Określa przekaźnik, który ma być wyzwalany przez akcje.
- **Stan drzwi**: Wyświetla stan sygnału wejściowego.

Pomiar temperatury ciała na potrzeby dostępu do drzwi (opcja)

Seria A05 oferuje opcjonalną funkcję pomiaru temperatury ciała zaprojektowaną do zastosowania w sytuacji, gdy pomiar staje się niezbędny dla bezpieczeństwa mieszkańców i gości itp. Mieszkańcy i goście muszą przejść pomiar temperatury wraz z opcjonalną kontrolą wykrywania maski, zanim uzyskają dostęp do drzwi.

Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu >** Interfejs **temperatury ciała**.



- **Tryb** : Urządzenie można zainstalować z cyfrowym czujnikiem temperatury na czole.
  - **Wyłączone**: Wyłączenie funkcji.
  - **Czoło**: Sprawdź temperaturę ciała na czole.
  - **Nadgarstek**: Sprawdź temperaturę ciała na nadgarstku.
- **Wykrywanie maski**:
  - **Wyłączone**: Urządzenie nie będzie wykrywać, czy użytkownik nosi maskę.
  - **Ustaw noszenie maski jako obowiązkowe**: Użytkownicy muszą nosić maskę do pomiaru temperatury. Urządzenie najpierw wykryje, czy użytkownik nosi maskę. Jeśli nie, nie przejdzie do następnego kroku.

- **Wyświetlanie monitu** o **noszenie maski**: Noszenie maski nie jest obowiązkowe. Urządzenie najpierw wykryje, czy użytkownik nosi maskę. Jeśli nie, pojawi się komunikat "Proszę założyć maskę" i urządzenie przejdzie do następnego kroku.

- **Normalna temperatura ciała**: Ustaw temperaturę ciała jako podstawę pomiaru w stopniach Fahrenheita lub Celsjusza. Na przykład, jeśli ustawisz temperaturę 37,3 stopni Celsjusza jako temperaturę normalną, wówczas każda temperatura ciała zmierzona powyżej 37,3 stopni Celsjusza zostanie uznana za temperaturę nienormalną.

- **Niska temperatura**: Ustaw temperaturę ciała jako podstawę pomiaru w stopniach Fahrenheita lub Celsjusza. Na przykład, jeśli ustawisz temperaturę 34 stopni Celsjusza jako próg, wówczas każda temperatura ciała zmierzona poniżej 34 stopni Celsjusza zostanie uznana za niską temperaturę ciała.

- **Działanie w przypadku nieprawidłowej temperatury ciała** :
    - **Odmowa dostępu**: W przypadku wykrycia nieprawidłowej temperatury drzwi nie zostaną otwarte.
    - **Dla przypomnienia**: Pojawi się komunikat przypominający o nieprawidłowej temperaturze. Drzwi zostaną otwarte.

- **Działanie w przypadku niskiej temperatury ciała** :
    - **Spróbuj ponownie później**: Użytkownicy zostaną poproszeni o ponowne zmierzenie temperatury, gdy wykryją niską temperaturę. Drzwi nie zostaną otwarte.
    - **Dla przypomnienia**: Pojawi się komunikat przypominający o niskiej temperaturze. Drzwi zostaną otwarte.

Monitor i obraz

MJPEG i RTSP to główne typy strumieni monitorowania omówione w tym rozdziale.

MJPEG lub Motion JPEG to format kompresji wideo, który wykorzystuje obrazy JPEG dla każdej klatki wideo. Urządzenia Akuvox wyświetlają strumienie na żywo w interfejsie internetowym i przechwytują zrzuty ekranu monitorowania w formacie MJPEG. Ustawienia związane z MJPEG określają jakość wideo oraz stan włączenia/wyłączenia funkcji transmisji na żywo.

RTSP to skrót od Real Time Streaming Protocol. Może być używany do strumieniowego przesyłania obrazu i dźwięku z kamer innych firm do urządzenia. Możesz dodać strumień z kamery, dodając jej adres URL. Format adresu URL urządzeń Akuvox to rtsp://Device's IP/live/ch00_0

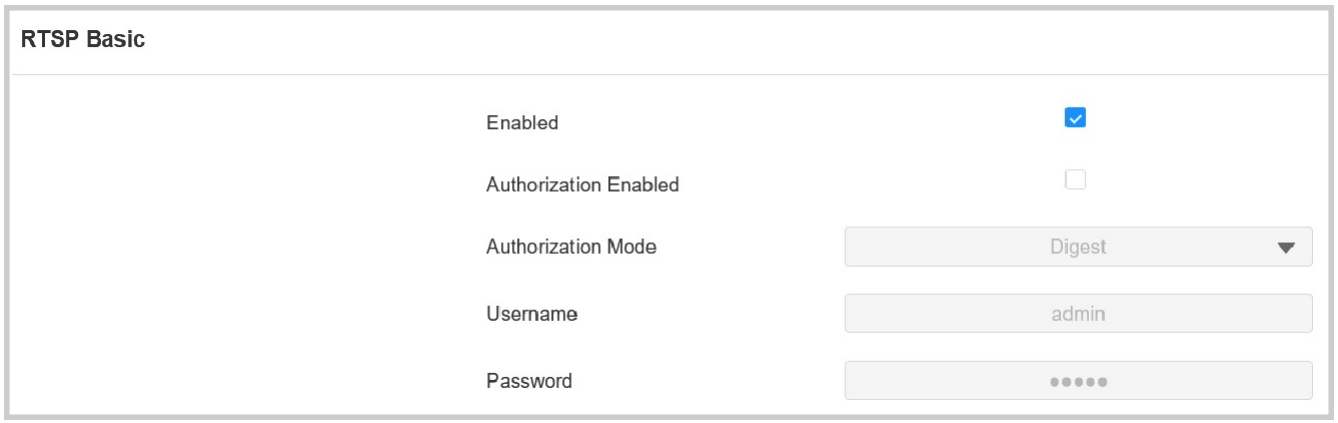
ONVIF to Otwarte Forum Sieciowego Interfejsu Wideo. Umożliwia urządzeniu skanowanie i wykrywanie kamer lub urządzeń domofonowych z aktywowanymi funkcjami ONVIF. Strumienie na żywo uzyskane za pośrednictwem ONVIF są zasadniczo w formacie RTSP.

Monitorowanie strumienia RTSP

Możesz użyć RTSP do oglądania strumienia wideo na żywo z innych urządzeń interkomowych na urządzeniu.

Podstawowe ustawienia RTSP

Aby ją skonfigurować, przejdź do **Surveillance > RTSP** interface.



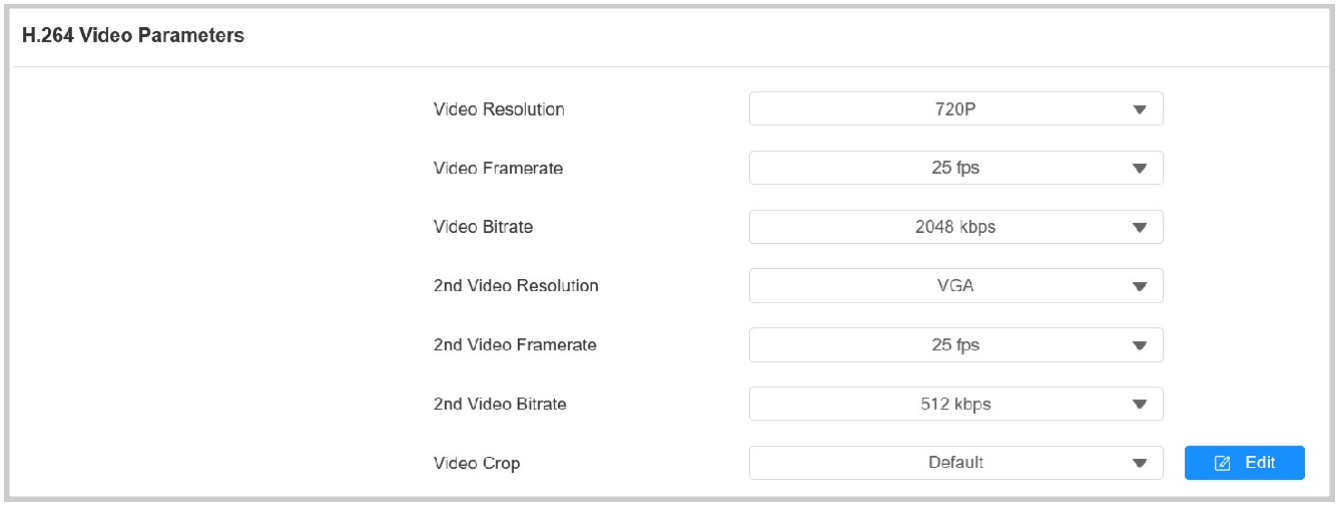
- **Włączona autoryzacja**: Po włączeniu autoryzacji RTSP wymagane jest skonfigurowanie trybu uwierzytelniania RTSP, nazwy użytkownika RTSP i hasła do autoryzacji.
- **Tryb uwierzytelniania** : Dostępne są dwie opcje: Basic i Digest. **Basic** jest domyślnym typem uwierzytelniania.

- **Nazwa użytkownika**: Ustaw nazwę użytkownika do uwierzytelniania.
- **Hasło**: ustawienie hasła uwierzytelniania.

Ustawienia strumienia RTSP

Strumień RTSP może wykorzystywać kodek wideo H.264 lub Mjpeg. W przypadku wybrania H.264 można również dostosować rozdzielczość wideo, szybkość transmisji i inne ustawienia.

Aby skonfigurować strumień RTSP, przejdź do interfejsu Web **Surveillance > RTSP**.



- **Rozdzielczość wideo**: Określa rozdzielczość obrazu, od najniższej QCIF (176x144 pikseli) do najwyższej 1080P (1920x1080 pikseli).
- **Szybkość klatek wideo** : Liczba klatek na sekundę odnosi się do liczby klatek wyświetlanych w jednej sekundzie wideo. Domyślna liczba klatek na sekundę wynosi 25.
- **Szybkość transmisji wideo** : Ilość danych wideo przesyłanych w określonym czasie. Wyższy bitrate wideo oznacza wyższą możliwą jakość, ale także większe rozmiary plików i większą przepustowość.
- **2. rozdzielczość wideo**: Określa rozdzielczość obrazu dla drugiego kanału strumienia wideo.
- **2nd Video Framerate**: Ustaw częstotliwość odświeżania dla drugiego kanału strumienia wideo.
- **2nd Video Bitrate** : Ustaw szybkość transmisji dla drugiego kanału strumienia wideo. Domyślnie jest to 512 kb/s.
- **Video Crop** :

- **Oryginał**: Wyświetlanie pełnoekranowego wideo.

- **Domyślnie**: Wybierz określony obszar wideo do wyświetlenia. Kliknij Edytuj, aby przyciąć wideo.

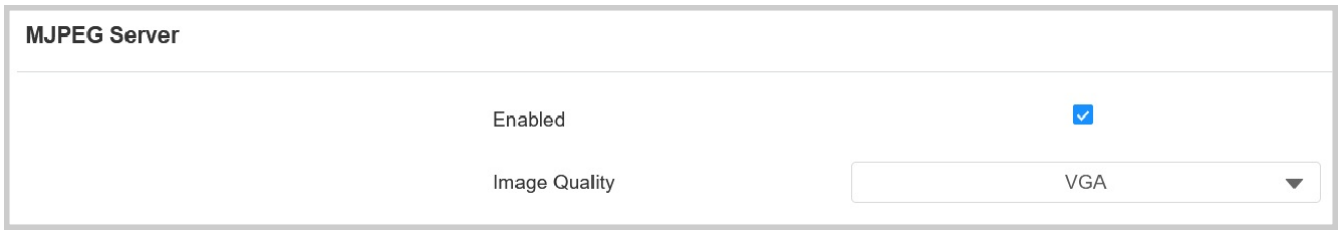
Wskazówka

Aby wyświetlić strumień audio i wideo za pomocą
- RTSP: Pierwszy kanał: rtsp://Device's
- IP/live/ch00_0
  Drugi kanał: rtsp://Device's IP/live/ch00_1

Przechwytywanie obrazu MJPEG

Za pomocą urządzenia można wykonać zdjęcie z monitoringu w formacie Mjpeg. W tym celu należy włączyć funkcję Mjpeg i wybrać jakość obrazu.

Aby ją skonfigurować, przejdź do opcji **Nadzór >** Interfejs **MJPEG**.



- **Enabled**: Wpisanie określonego adresu URL w przeglądarce umożliwia uzyskanie dostępu do obrazu lub wideo z kamery.

Wskazówka

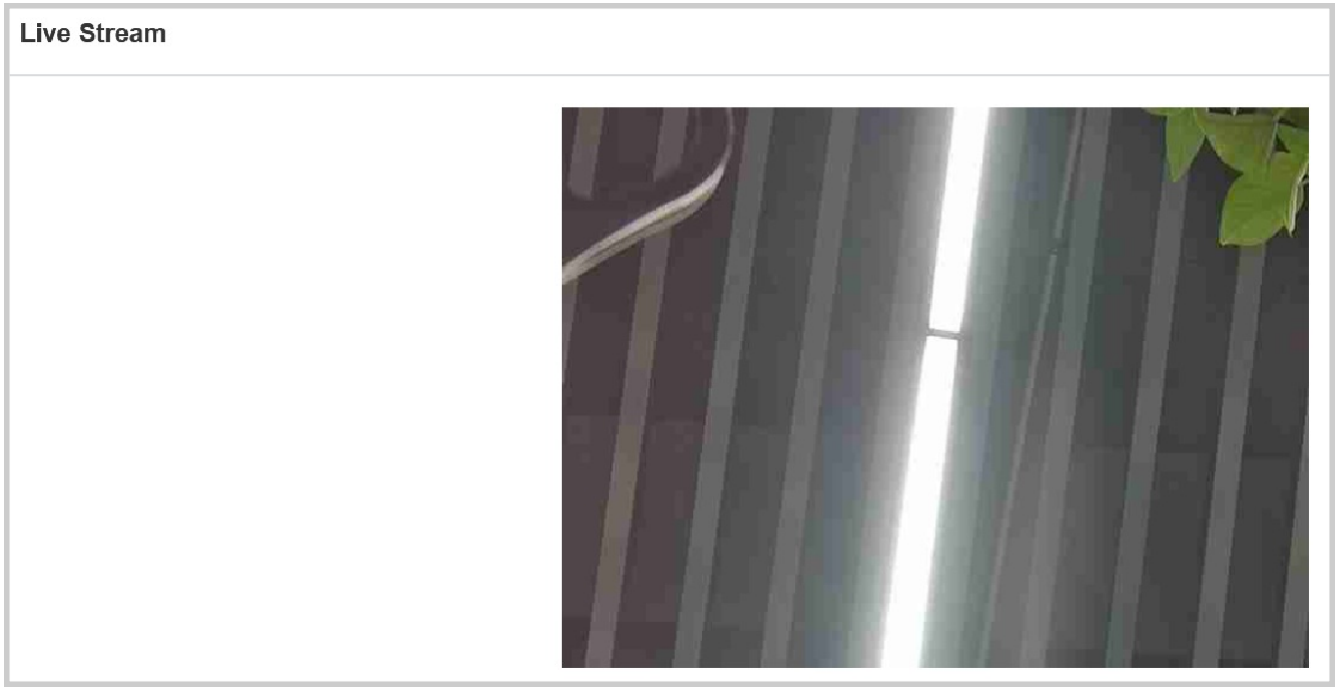
- Aby wyświetlić dynamiczny strumień, użyj adresu URL http://device_IP:8080/video.cgi.
- Aby przechwycić zrzut ekranu, użyj następujących adresów URL, przy czym formaty obrazu różnią się odpowiednio:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi

- **Jakość obrazu**: Określa rozdzielczość obrazu, od najniższej QCIF (176x144 pikseli) do najwyższej 1080P (1920x1080 pikseli).

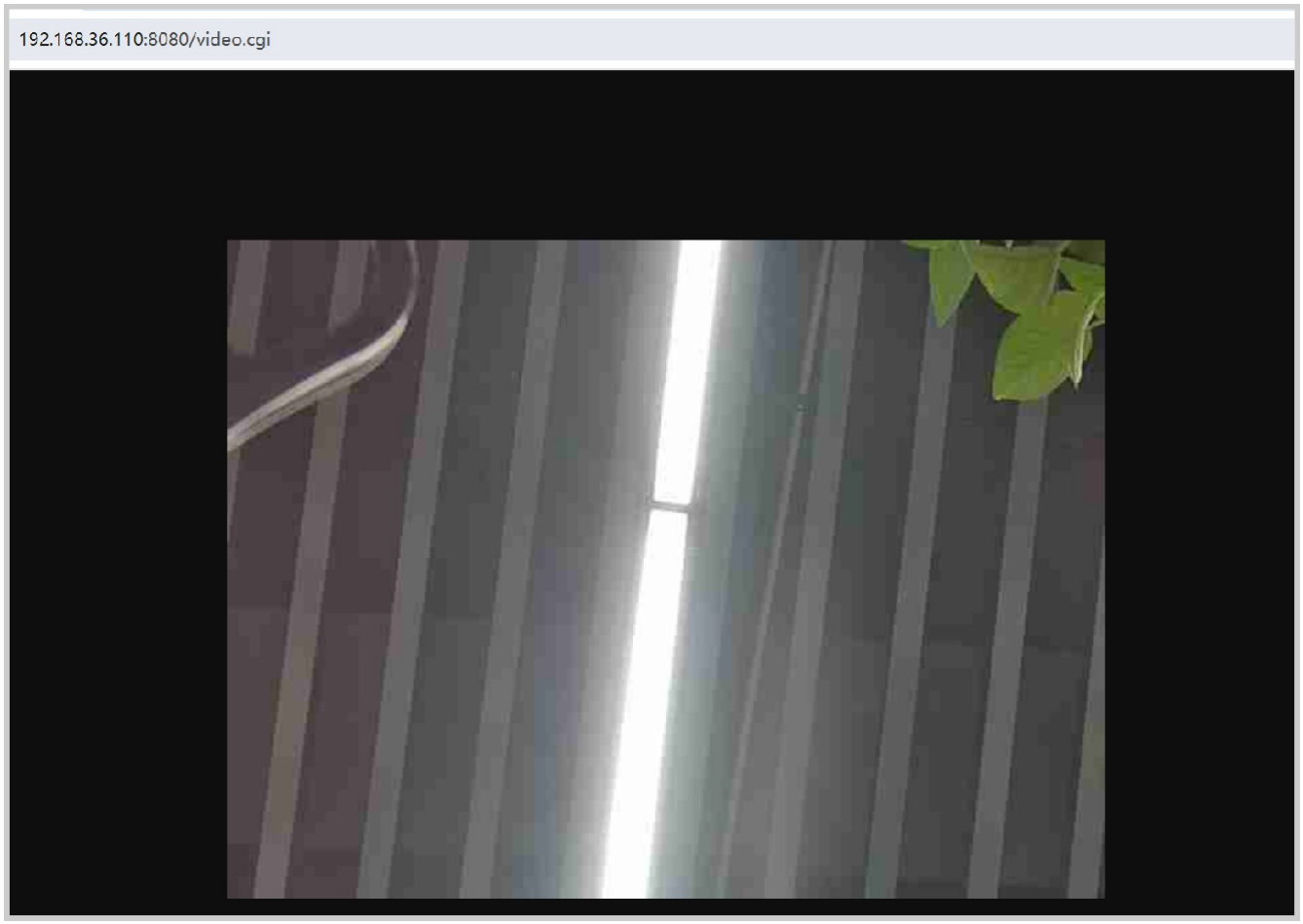
Transmisja na żywo

Istnieją dwa sposoby sprawdzania obrazu wideo w czasie rzeczywistym z urządzenia. Jednym z nich jest przejście do interfejsu internetowego urządzenia i wyświetlenie tam wideo. Drugim jest wpisanie prawidłowego adresu URL w przeglądarce internetowej i uzyskanie bezpośredniego dostępu do wideo.

Transmisja na żywo jest dostępna w interfejsie **Surveillance > Live Stream**.



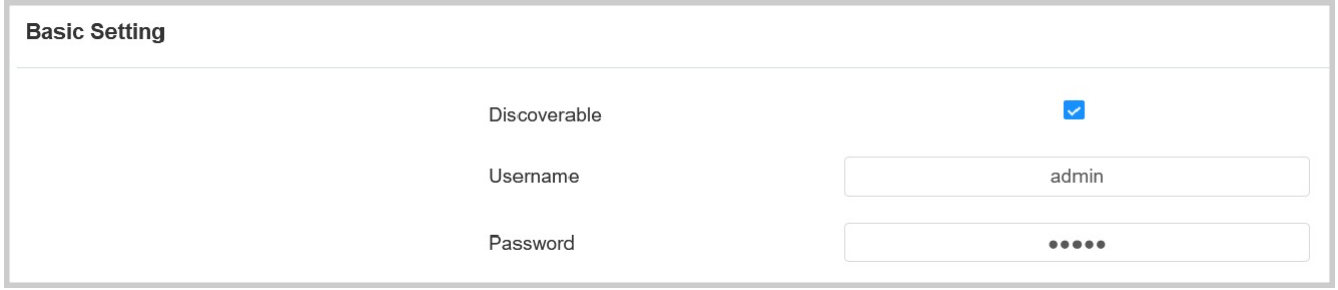
Alternatywnie, jak opisano w sekcji Przechwytywanie obrazu MJPEG, wprowadź prawidłowy adres URL w przeglądarce internetowej.



ONVIF

Dostęp do obrazu w czasie rzeczywistym z kamery urządzenia można uzyskać za pomocą monitora wewnętrznego Akuvox lub innych urządzeń innych firm, takich jak sieciowy rejestrator wideo (**NVR**). Włączenie i skonfigurowanie funkcji ONVIF na urządzeniu pozwoli na wyświetlanie jego wideo na innych urządzeniach.

Aby ją skonfigurować, przejdź do interfejsu **Surveillance > ONVIF > Basic Setting**.



- **Discoverable**: Po włączeniu tej opcji wideo z kamery urządzenia może być wyszukiwane przez inne urządzenia.
- **Nazwa użytkownika**: Ustaw nazwę użytkownika wymaganą do uzyskania dostępu do strumienia wideo urządzenia na innych urządzeniach. Domyślnie jest to admin.

- **Hasło**: Ustaw hasło wymagane do uzyskania dostępu do strumienia wideo urządzenia na innych urządzeniach. Domyślnie jest to admin.

> **Wskazówka**
>
> Po skonfigurowaniu ustawień, aby uzyskać dostęp do strumienia wideo na urządzeniu innej firmy, wystarczy wprowadzić adres URL ONVIF: http://Device's IP:80/onvif/device_service.

Tryb kamery

Tryb kamery można wybrać w zależności od miejsca instalacji urządzenia.

Aby ją wybrać, przejdź do **Surveillance > ONVIF > Camera** interface.

- **Liniowy**: Utrzymuje bezpośrednią, liniową zależność między światłem wejściowym a wyjściowymi wartościami pikseli. Innymi słowy, obrazy są bezpośrednio powiązane z rzeczywistymi poziomami światła w scenie.
- **WDR**: Uchwycenie szerszego zakresu jasnych i ciemnych obszarów w ramach jednego obrazu.

Bezpieczeństwo

Alarm sabotażowy

Funkcja alarmu sabotażowego zapobiega usuwaniu urządzeń przez osoby niepowołane. Odbywa się to poprzez uruchomienie alarmu sabotażowego i wykonanie połączenia do wyznaczonej lokalizacji, gdy urządzenie wykryje zmianę wartości grawitacji w stosunku do pierwotnej.

Aby ją skonfigurować, przejdź do **System > Bezpieczeństwo >** Interfejs **alarmu sabotażowego**.

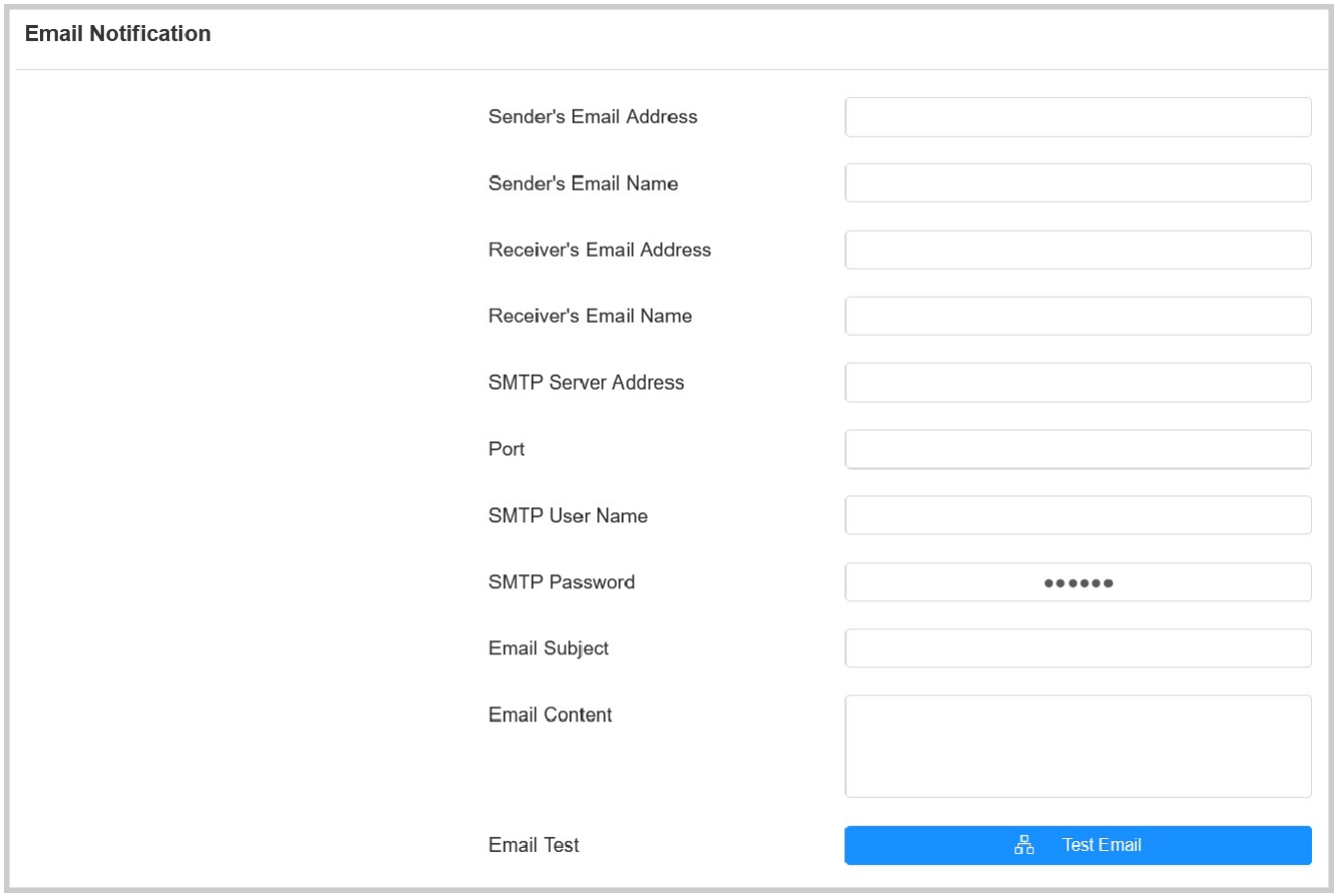
- **Enabled** : Zaznacz, aby włączyć funkcję alarmu sabotażowego. Aby wyłączyć alarm, można kliknąć przycisk **Rozbrój**.
- **Stan klucza**: Alarm sabotażowy nie zostanie wyzwolony, jeśli stan klucza nie zostanie zmieniony z **niskiego** na **wysoki.**

Powiadomienie o zabezpieczeniach

Powiadomienie e-mail

Skonfiguruj powiadomienia e-mail, aby otrzymywać zrzuty ekranu nietypowego ruchu z urządzenia.

Przejdź do **Ustawienia > Akcja >** Interfejs **powiadomień e-mail**.

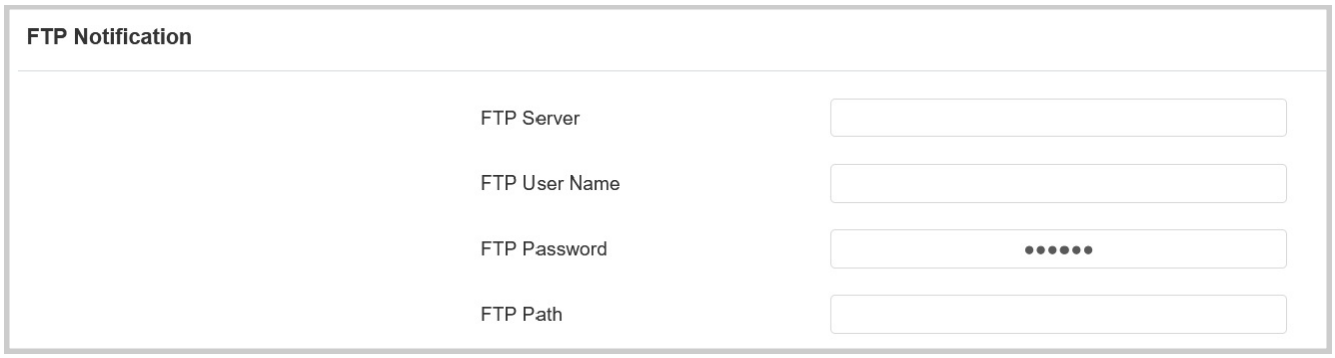


- **Nazwa użytkownika SMTP**: Nazwa użytkownika SMTP jest zwykle taka sama jak adres e-mail nadawcy.
- **Hasło SMTP** : Hasło serwera SMTP, które jest takie samo jak adres e-mail nadawcy.

Ustawienia powiadomień FTP

Aby otrzymywać powiadomienia za pośrednictwem serwera FTP, należy skonfigurować ustawienia FTP. Urządzenie prześle zrzut ekranu do określonego folderu FTP, jeśli wykryje jakikolwiek nietypowy ruch.

Aby ją skonfigurować, przejdź do interfejsu internetowego **Ustawienia > Akcja > Powiadomienie FTP.**



- **Ścieżka FTP**: Nazwa folderu utworzonego na serwerze FTP.

Powiadomienie TFTP

Aby otrzymywać powiadomienia bezpieczeństwa za pośrednictwem serwera TFTP, należy wprowadzić adres serwera TFTP.

Aby ją skonfigurować, przejdź do **Ustawienia > Akcja >** Interfejs **powiadomień TFTP**.

Adres URL akcji

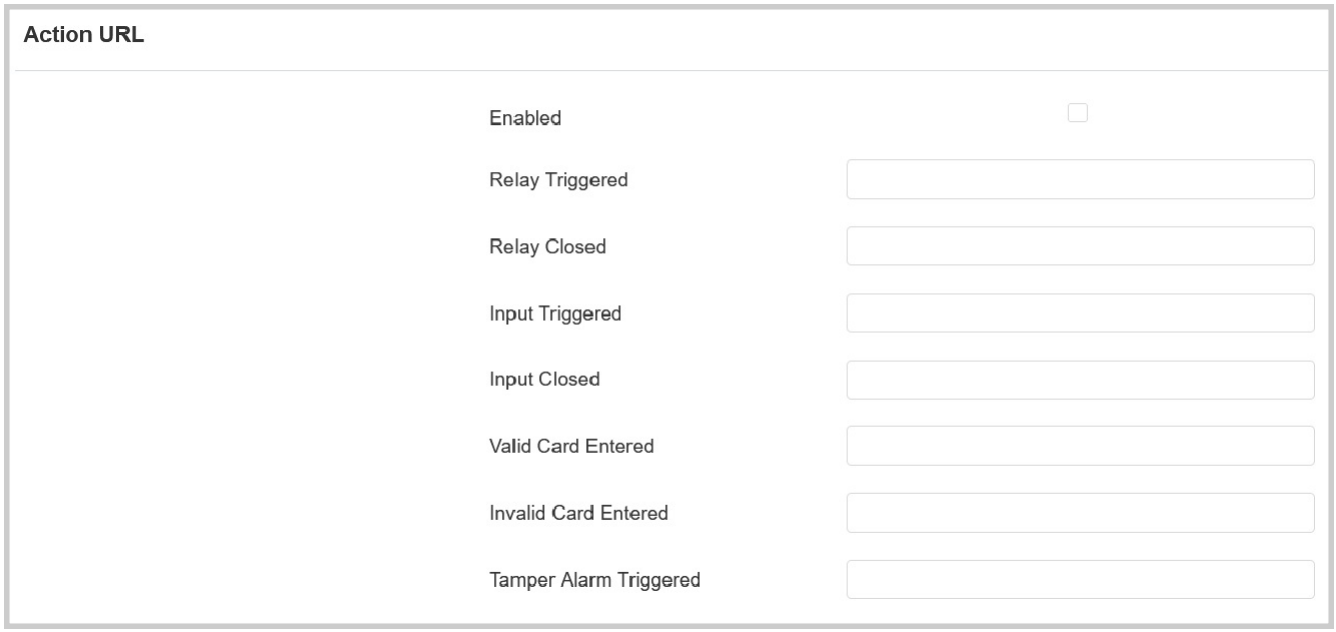
Za pomocą urządzenia można wysyłać określone polecenia HTTP URL do serwera HTTP w celu wykonania określonych działań. Działania te będą wyzwalane, gdy zmieni się stan przekaźnika, stan wejścia, kod PIN lub dostęp do karty RF.

Akuvox Action URL:

Nie.	Wydarzenie	Format parametrów	Przykład
1	Przekaźnik wyzwolony	$relay1status	Http://server ip/relaytrigger=$relay1status
2	Przekaźnik zamknięty	$relay1status	Http://server ip/relayclose=$relay1status
3	Wejście wyzwalane	$input1status	Http://server ip/inputtrigger=$input1status
4	Wejście zamknięte	$input1status	Http://server ip/inputclose=$input1status
5	Wprowadzona ważna karta	$card_sn	Http://server ip/validcard=$card_sn
6	Wprowadzono nieprawidłową kartę	$card_sn	Http://server ip/invalidcard=$card_sn
7	Wyzwolenie alarmu sabotażowego	status alarmu	Http://server ip/tampertrigger=$alarm status

Na przykład: http://192.168.16.118/help.xml?
mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

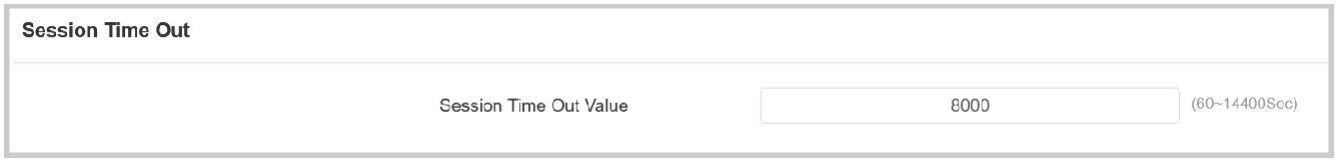
Aby ją skonfigurować, przejdź do opcji **Ustawienia >** Interfejs **Action URL**.



Interfejs sieciowy Automatyczne wylogowanie

Dla celów bezpieczeństwa lub wygody obsługi można skonfigurować automatyczne wylogowywanie interfejsu internetowego, wymagające ponownego zalogowania poprzez wprowadzenie nazwy użytkownika i hasła.

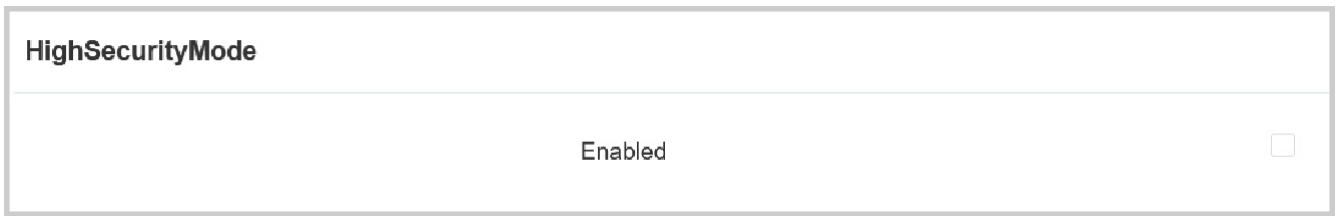
Przejdź do interfejsu internetowego **System > Security**.



Tryb wysokiego bezpieczeństwa

Tryb wysokiego bezpieczeństwa został zaprojektowany w celu zwiększenia bezpieczeństwa. Wykorzystuje on szyfrowanie w różnych aspektach, w tym w procesie komunikacji, poleceniach otwierania drzwi, metodach przechowywania haseł i nie tylko.

Aby włączyć ten tryb, przejdź do interfejsu **System > Security > High Security Mode**.



Ważne uwagi

1. Tryb High Security jest domyślnie wyłączony po uaktualnieniu urządzenia z wersji bez tego trybu do wersji z tym trybem. Jeśli jednak zresetujesz urządzenie do ustawień fabrycznych, tryb ten będzie domyślnie włączony.

2. Ten tryb sprawia, że stare wersje narzędzi są niekompatybilne. Aby z nich korzystać, należy uaktualnić je do następujących wersji lub wyższych.

-PC Manager: 1.2.0.0

-IP Scanner: 2.2.0.0

-Upgrade Tool: 4.1.0.0

-SDMC: 6.0.0.34

3. Obsługiwany format HTTP dla wyzwalania przekaźnika różni się w zależności od tego, czy tryb wysokiego bezpieczeństwa jest włączony czy wyłączony.

Jeśli tryb jest włączony, urządzenie akceptuje tylko nowe formaty HTTP podane poniżej dla otwierania drzwi.

- l http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- l http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

Jeśli tryb jest wyłączony, urządzenie może używać zarówno nowego formatu powyżej, jak i starego formatu poniżej:

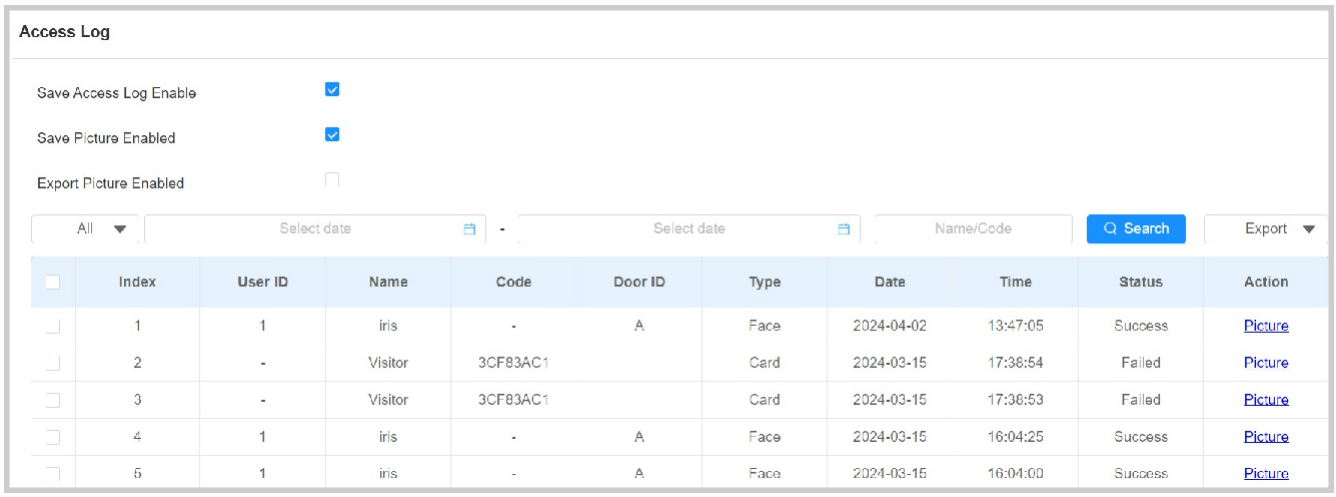
- l http://deviceIP/fcgi/do?
  action=OpenDoor&UserName=username&Password=password&DoorNum=1

4. Niedozwolone jest importowanie/eksportowanie plików konfiguracyjnych w formacie tgz. między urządzeniem z trybem wysokiego bezpieczeństwa a innym bez niego. Aby uzyskać pomoc dotyczącą przesyłania plików, skontaktuj się z pomocą techniczną Akuvox.

Dzienniki

Dziennik dostępu

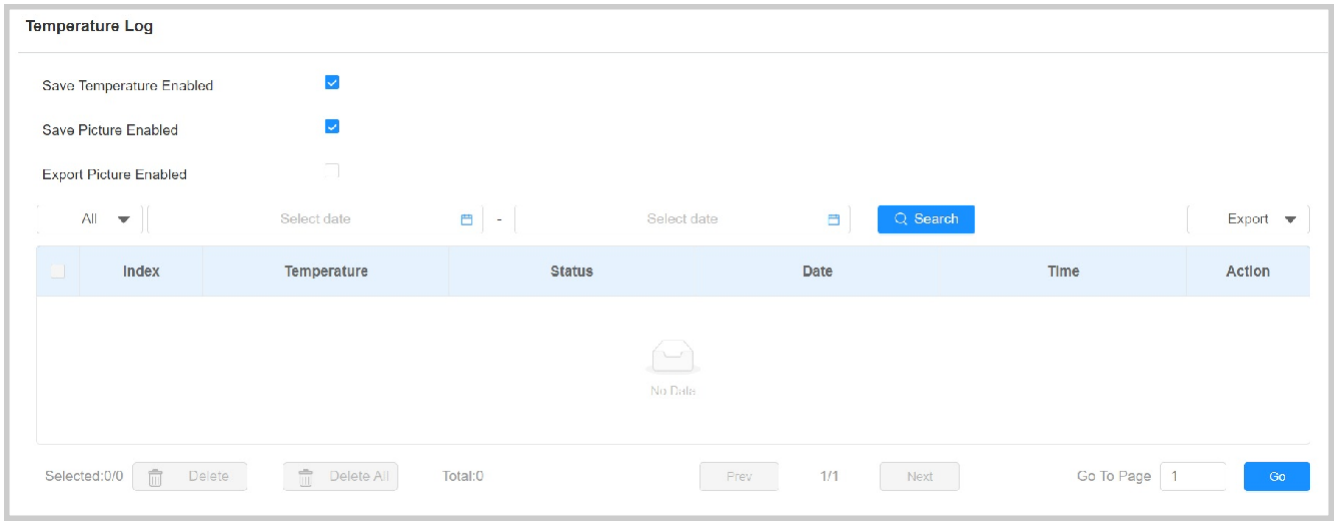
Dzienniki drzwi można wyszukiwać i sprawdzać w interfejsie internetowym urządzenia **Status > Access Log**. Można również eksportować dzienniki drzwi w plikach CSV lub XML.



- **Status**: opcje **Success (sukces)** i **Failed (niepowodzenie)** oznaczają odpowiednio udany dostęp do drzwi i nieudany dostęp do drzwi.
- **Czas**: Wybierz konkretny okres dzienników drzwi, który chcesz przeszukać, sprawdzić lub wyeksportować.
- **Nazwa/kod** : Przeszukuj dziennik według nazwy użytkownika lub kodu PIN.
- **ID drzwi**: Wyświetla nazwę drzwi.
- **Typ** : Wyświetla typ dostępu, np. karta.
- **Działanie**: Kliknij Obraz, aby wyświetlić zrzut ekranu.

Dziennik temperatury

Dzienniki temperatury można przeszukiwać w interfejsie **Status > Temperature Log**. Można również eksportować dzienniki temperatury w plikach CSV lub XML.



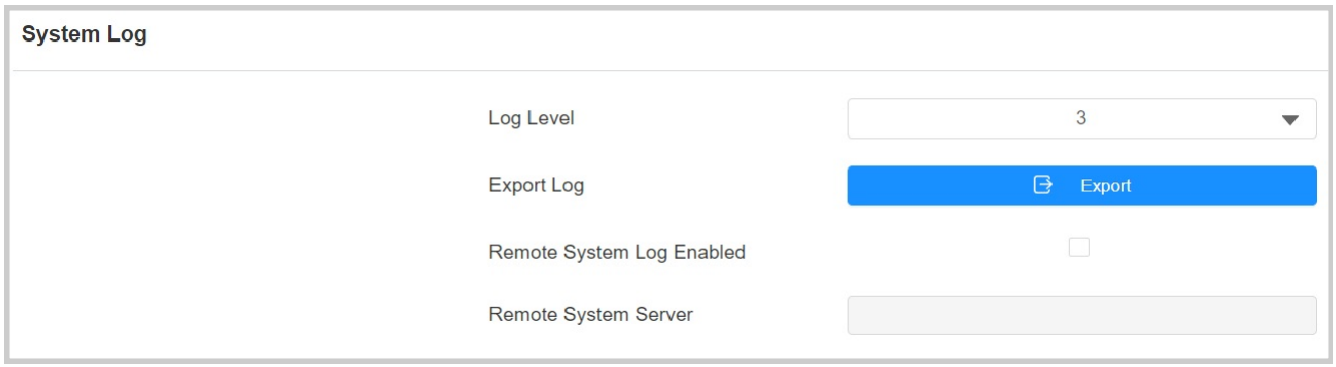
- **Status**: Wyświetlanie stanu normalnego, nieprawidłowego lub niskiej temperatury.
- **Temperatura**: Wyświetlanie danych temperatury.
- **Działanie**: Kliknij Obraz, aby wyświetlić zrzut ekranu.

Debugowanie

Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Aby ją skonfigurować, przejdź do opcji **System > Konserwacja >** Interfejs **dziennika systemowego**.

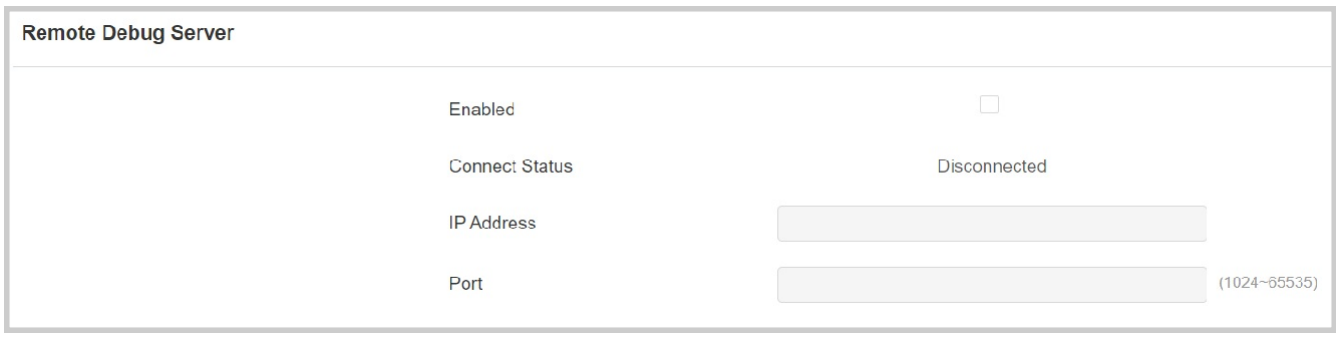


- **Poziom dziennika**: Poziomy dziennika wahają się od 1 do 7. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić do celów debugowania. Domyślny poziom dziennika to 3. Im wyższy poziom, tym bardziej kompletny jest dziennik.
- **Eksportuj dziennik**: Kliknij kartę **Eksportuj**, aby wyeksportować tymczasowy plik dziennika debugowania do lokalnego komputera.
- **Zdalny serwer systemu**: Ustaw adres zdalnego serwera, na który ma być przesyłany dziennik urządzenia. Adres serwera zdalnego zostanie dostarczony przez pomoc techniczną Akuvox.

Zdalny serwer debugowania

Gdy urządzenie ma problem, można użyć zdalnego serwera debugowania, aby uzyskać zdalny dostęp do dziennika urządzenia w celu debugowania.

Aby ją skonfigurować, przejdź do **System > Konserwacja >** Interfejs **serwera zdalnego debugowania**.

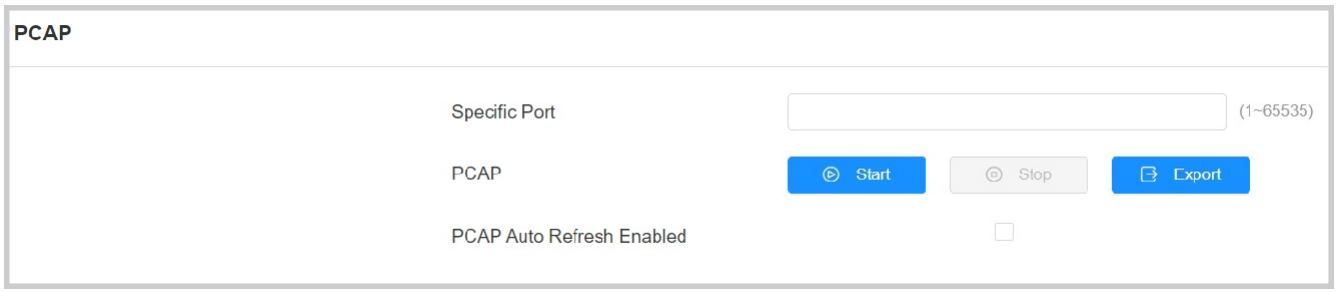


- **Connect Status**: Wyświetla stan połączenia ze zdalnym serwerem debugowania.
- **Adres IP**: Ustaw adres IP zdalnego serwera debugowania. Zapytaj zespół techniczny Akuvox o adres IP serwera.
- **Port**: Ustawia port zdalnego serwera debugowania.

PCAP do debugowania

PCAP służy do przechwytywania pakietów danych wchodzących i wychodzących z urządzeń w celu debugowania i rozwiązywania problemów.

Aby ją skonfigurować, przejdź do **System > Konserwacja >** Interfejs **PCAP**.

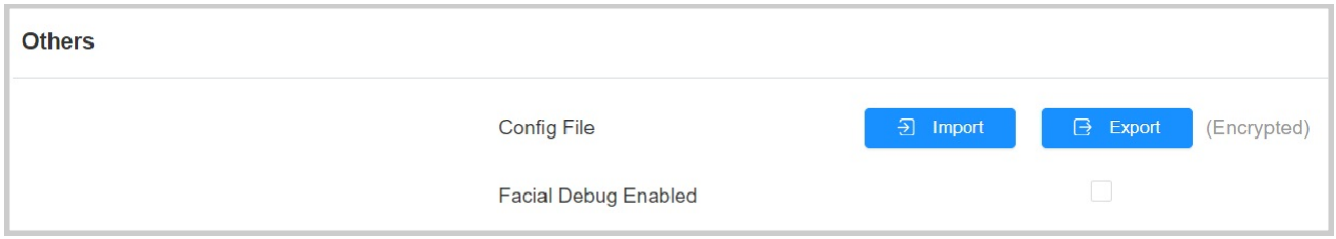


- **Określony port**: Wybierz określone porty z zakresu 1-65535, aby można było przechwytywać tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.
- **PCAP**: Kliknij kartę **Start** i **Stop**, aby przechwycić określony zakres pakietów danych przed kliknięciem karty **Eksport**, aby wyeksportować pakiety danych do lokalnego komputera.
- **PCAP Auto Refresh Enabled**: Po włączeniu tej opcji, PCAP będzie kontynuował przechwytywanie pakietów danych nawet po osiągnięciu maksymalnej pojemności 50M. Po

wyłączeniu, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycone pakiety danych osiągną maksymalną pojemność 1 MB.

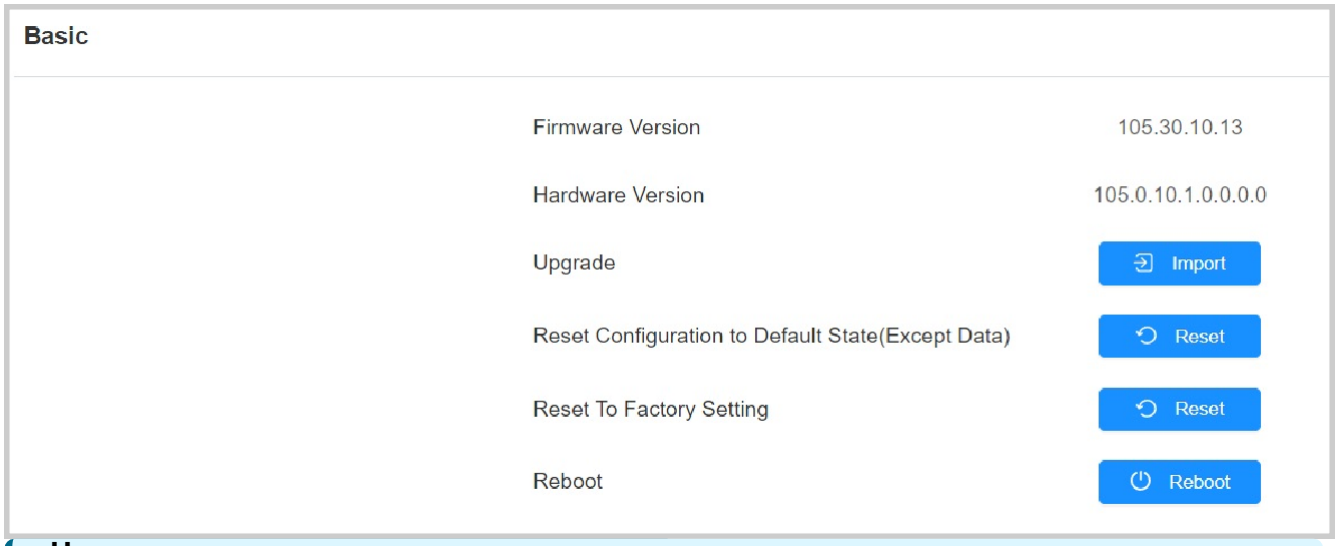
Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować do komputera lokalnego. Aby to skonfigurować, przejdź do **System > Maintenance > Others** interface.



Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można aktualizować w interfejsie internetowym urządzenia. Aby zaktualizować urządzenie, przejdź do **System >** Interfejs **aktualizacji**.



Uwaga

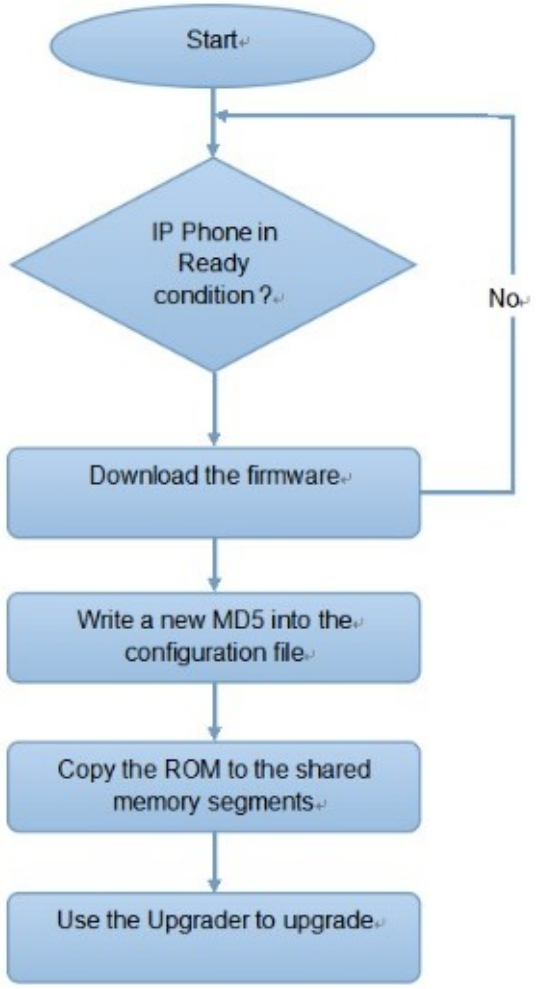
Pliki oprogramowania sprzętowego powinny być w formacie **.rom**.

Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

Zasada udostępniania

Automatyczne dostarczanie to funkcja używana do konfiguracji lub aktualizacji urządzeń w partii za pośrednictwem serwerów innych firm. **DHCP, PNP, TFTP, FTP i HTTPS** to protokoły używane przez urządzenia Akuvox do uzyskiwania dostępu do adresu URL serwera innej firmy, który przechowuje pliki konfiguracyjne i oprogramowanie układowe, które zostaną następnie wykorzystane do aktualizacji oprogramowania układowego i odpowiednich parametrów na urządzeniu.

Zobacz poniższy schemat blokowy:



Wprowadzenie do plików konfiguracyjnych automatycznego przydzielania uprawnień

Pliki konfiguracyjne mają dwa formaty automatycznego provisioningu. Jeden to ogólne pliki konfiguracyjne używane do ogólnego provisioningu, a drugi to provisioning konfiguracji opartej na MAC.

Różnica między tymi dwoma typami konfiguracji jest niewielka:

- **Udostępnianie konfiguracji ogólnej**: plik ogólny jest przechowywany na serwerze, z którego wszystkie powiązane urządzenia będą mogły pobrać ten sam plik konfiguracyjny w celu aktualizacji parametrów na urządzeniach. Na przykład cfg.
- **Udostępnianie konfiguracji opartej na MAC**: Pliki konfiguracyjne oparte na MAC są używane do automatycznego udostępniania na określonym urządzeniu, zgodnie z jego unikalnym numerem MAC. Pliki konfiguracyjne nazwane za pomocą numeru MAC urządzenia zostaną automatycznie dopasowane do numeru MAC urządzenia przed pobraniem w celu udostępnienia na określonym urządzeniu.

Uwaga

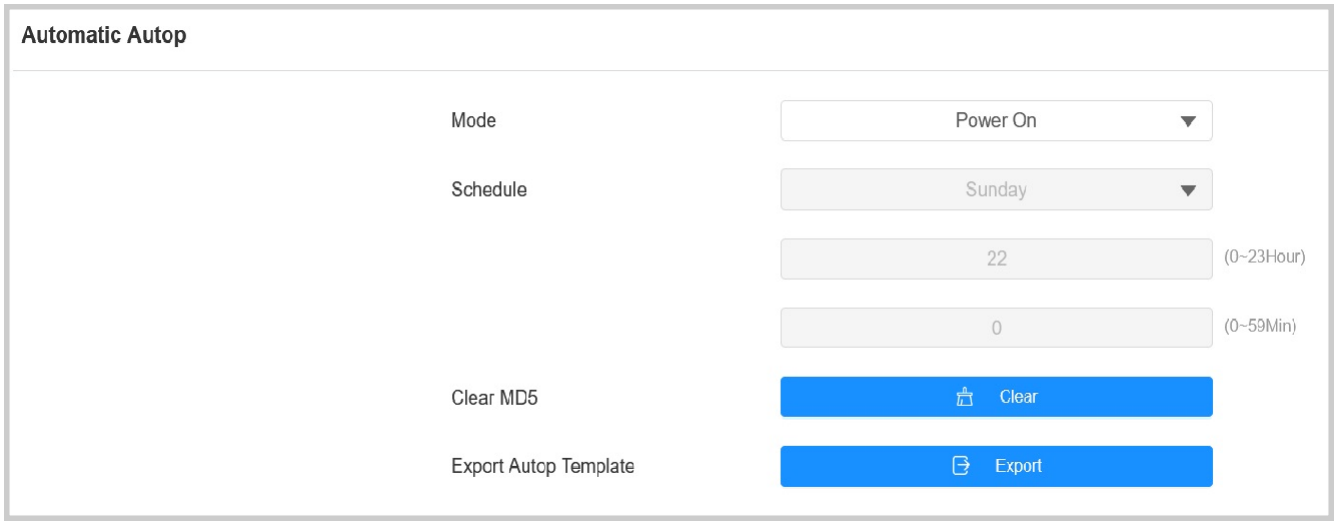
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny udostępniania wsadowego różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC dla określonego udostępniania urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer posiada te dwa typy plików konfiguracyjnych, urządzenia będą najpierw uzyskiwać dostęp do ogólnych plików konfiguracyjnych przed uzyskaniem dostępu do plików konfiguracyjnych opartych na MAC.

Możesz kliknąć **tutaj**, aby zobaczyć szczegółowy format i kroki.

Harmonogram Autop

Akuvox zapewnia różne metody Autop, które umożliwiają urządzeniu samodzielne wykonywanie aprowizacji zgodnie z harmonogramem.

Aby ją skonfigurować, przejdź do **System > Auto Provisioning > Automatic Autop** interface.

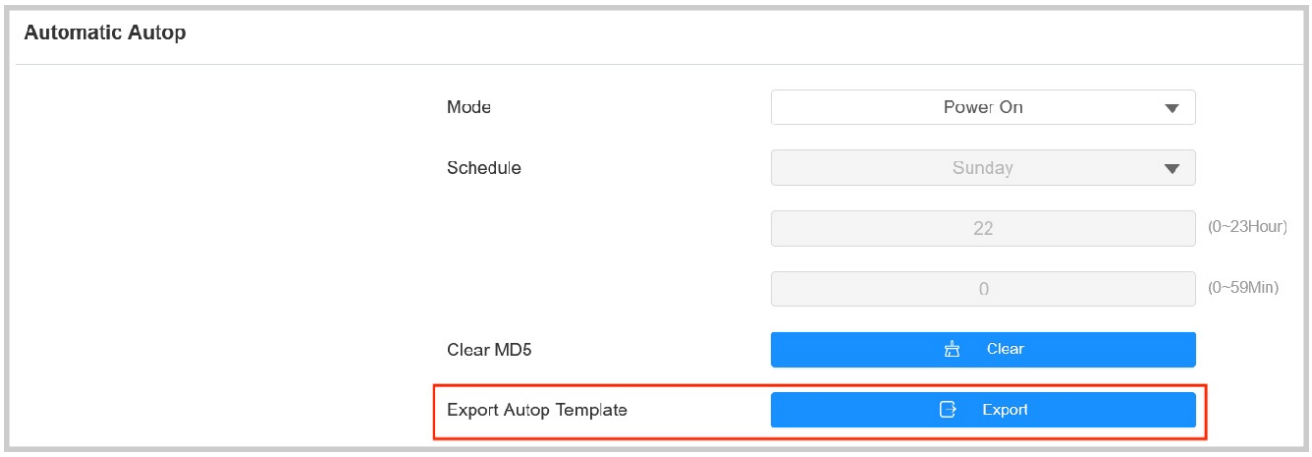


- **Tryb** :
    - **Power On**: Urządzenie wykona Autop przy każdym uruchomieniu.
    - **Wielokrotnie**: Urządzenie wykona funkcję Autop zgodnie z ustawionym harmonogramem.
    - **Power On + Repeatedly**: Połączenie trybów **Power On** i **Repeatedly**, które umożliwią urządzeniu wykonywanie funkcji Autop przy każdym uruchomieniu lub zgodnie z ustawionym harmonogramem.
    - **Hourly Repeat (Powtarzanie co godzinę)**: Urządzenie będzie wykonywać funkcję Autop co godzinę.

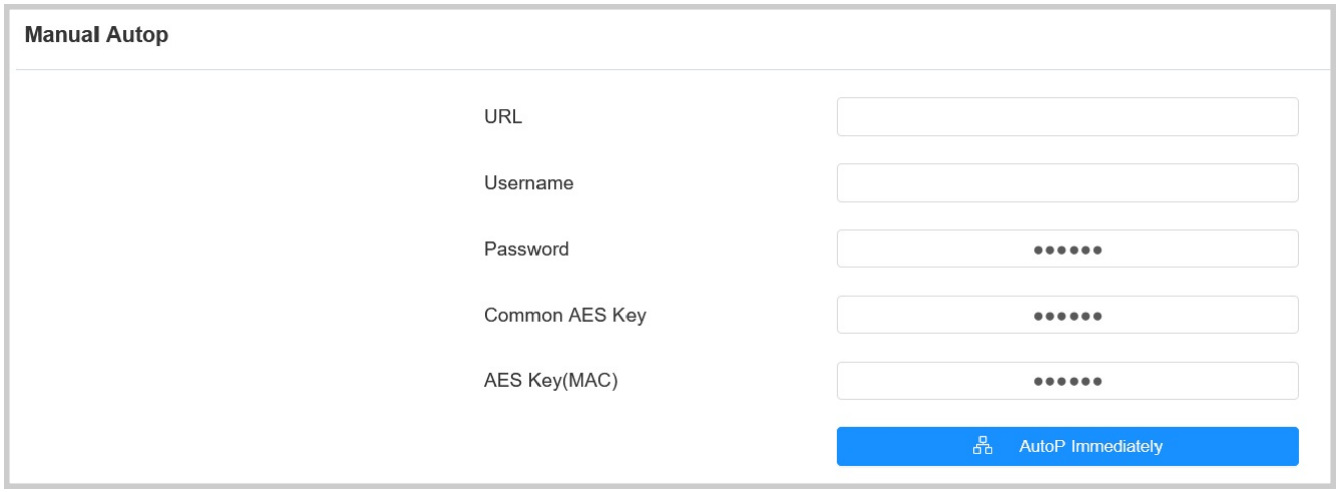
Udostępnianie statyczne

Można ręcznie skonfigurować określony adres URL serwera w celu pobrania oprogramowania sprzętowego lub pliku konfiguracyjnego. Jeśli skonfigurowano harmonogram automatycznego dostarczania, urządzenie wykona automatyczne dostarczanie w określonym czasie zgodnie z ustawionym harmonogramem automatycznego dostarczania. Ponadto TFTP, FTP, HTTP i HTTPS to protokoły, które mogą być używane do aktualizacji oprogramowania układowego i konfiguracji urządzenia.

Aby ją skonfigurować, należy najpierw pobrać szablon w menu **System > Auto Provisioning > Automatic Autop**.



Skonfiguruj serwer Autop w interfejsie **System > Auto Provisioning > Manual Autop**.



- **URL** : Określa adres serwera TFTP, HTTP, HTTPS lub FTP dla provisioningu.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika, jeśli serwer wymaga nazwy użytkownika, aby uzyskać do niego dostęp.
- **Hasło** : Wprowadź hasło, jeśli dostęp do serwera wymaga podania hasła.
- **Wspólny klucz AES**: Służy do odszyfrowywania przez urządzenie ogólnych plików konfiguracyjnych Autop.
- **Klucz AES (MAC)**: Służy do odszyfrowania przez urządzenie pliku konfiguracyjnego Autop opartego na MAC.

Uwaga

- AES jako jeden z typów szyfrowania powinien być skonfigurowany tylko wtedy, gdy plik konfiguracyjny jest zaszyfrowany za pomocą AES.
- Format adresu serwera:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(umożliwia anonimowe logowanie) ftp://username:password@192.168.0.19/(wymaga nazwy użytkownika i hasła)
  - HTTP: http://192.168.0.19/ (użyj domyślnego portu 80) http://192.168.0.19:8080/ (użyj innych portów, takich jak 8080)
  - HTTPS: https://192.168.0.19/ (użyj domyślnego portu 443)

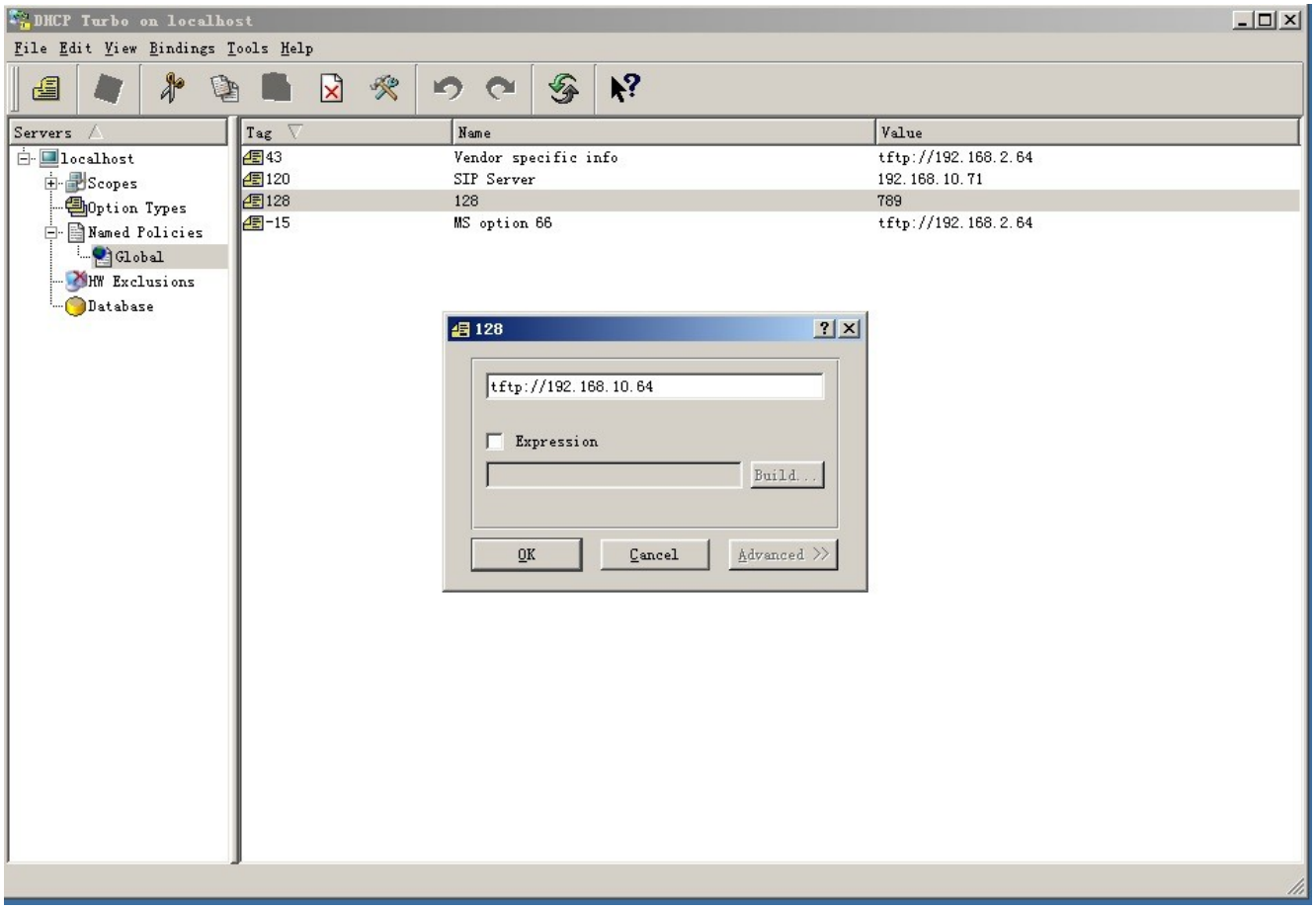
Wskazówka

Akuvox nie zapewnia serwera określonego przez użytkownika. Należy samodzielnie przygotować serwer TFTP/FTP/HTTP/HTTPS.

Udostępnianie DHCP

Adres URL automatycznego dostarczania można również uzyskać za pomocą opcji DHCP, która umożliwia urządzeniu wysłanie żądania do serwera DHCP dla określonego kodu opcji DHCP. Jeśli chcesz użyć

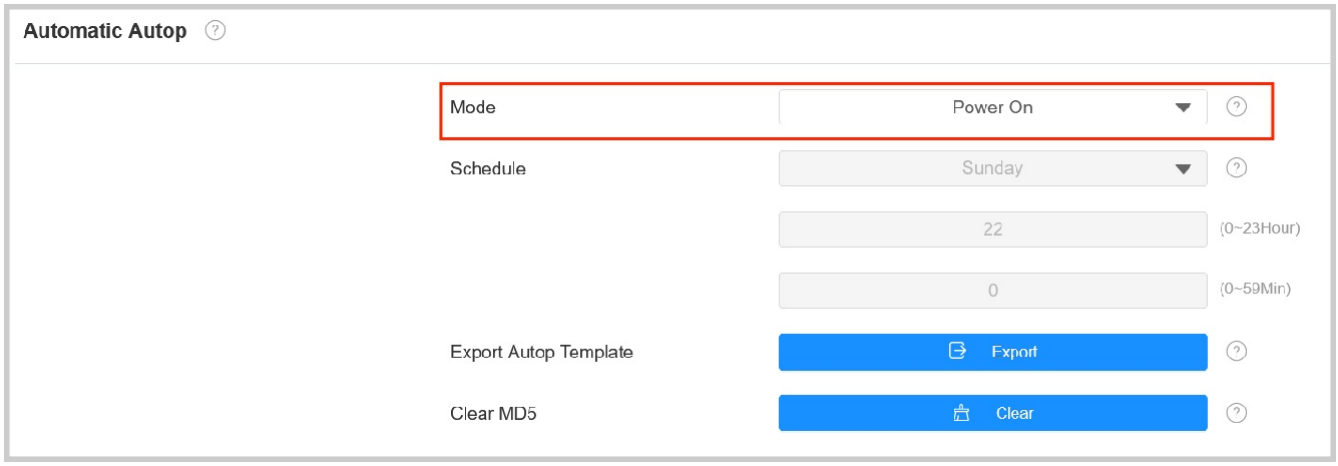
Opcja nie**standardowa** zdefiniowana przez użytkowników z kodami opcji w zakresie 128-255), należy skonfigurować opcję niestandardową DHCP w interfejsie internetowym.



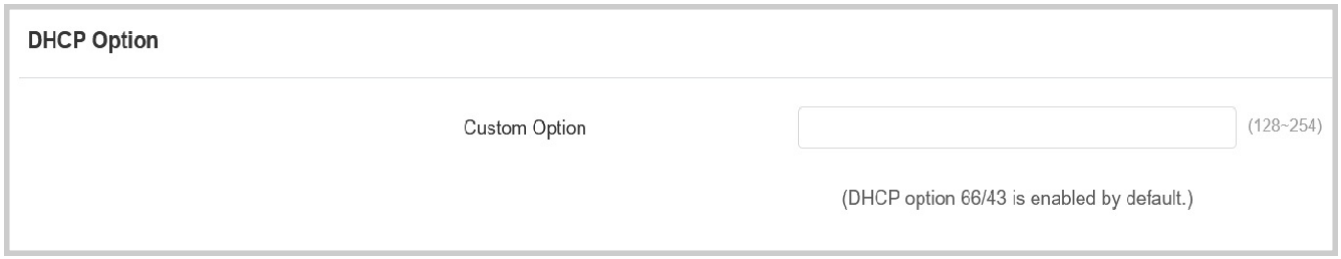
Uwaga

- Typ opcji niestandardowej musi być ciągiem znaków. Wartością jest adres URL serwera TFTP.

Aby skonfigurować DHCP Autop z trybem **Power On**, przejdź do interfejsu **System > Auto Provisioning > Automatic Autop**.



Aby skonfigurować opcję DHCP, przewiń do sekcji **Opcja DHCP**.



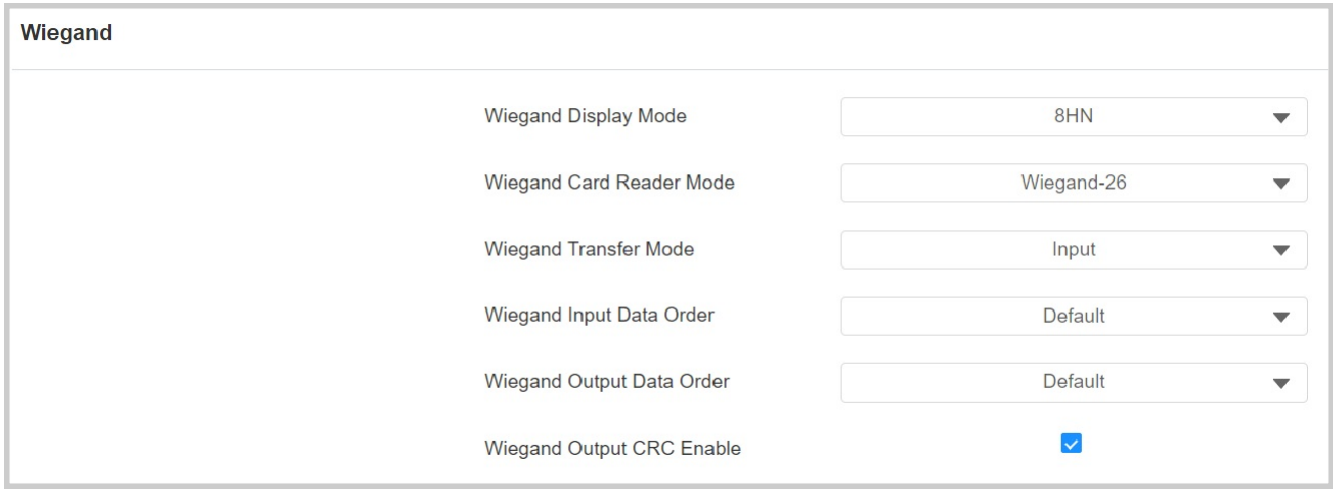
- **Opcja niestandardowa**: Wprowadź kod DHCP pasujący do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych do konfiguracji lub aktualizacji.
- **Opcja 43 DHCP**: Jeśli urządzenie nie otrzyma adresu URL z Opcji 66 DHCP, automatycznie użyje Opcji 43 DHCP. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 43 z adresem URL serwera aktualizacji.
- **Opcja 66 DHCP**: Jeśli żadna z powyższych opcji nie jest ustawiona, urządzenie automatycznie użyje Opcji 66 DHCP, aby uzyskać adres URL serwera aktualizacji. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 66 z adresem URL serwera aktualizacji.

Integracja z urządzeniami innych firm

Integracja przez Wiegand

Terminal kontroli dostępu A05 można zintegrować z urządzeniami innych firm za pośrednictwem Wiegand.

Aby go skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **Wiegand**.



- **Tryb wyświetlania Wiegand** : Wybierz format kodu karty Wiegand spośród dostępnych opcji.
- **Tryb czytnika kart Wiegand**: Format transmisji powinien być identyczny między terminalem kontroli dostępu a urządzeniem innej firmy. Jest on konfigurowany automatycznie.
- **Tryb transferu Wiegand** :
    - **Wejście**: Urządzenie służy jako odbiornik.
    - **Wyjście**: Urządzenie służy jako nadajnik, a użytkownicy mogą otworzyć drzwi tylko po wprowadzeniu kodu PIN lub przeciągnięciu karty RF.
    - **Wyjście Convert To Card No**: Urządzenie służy jako nadawca, a użytkownicy są przypisywani za pomocą wielu metod otwierania drzwi, takich jak rozpoznawanie twarzy i Bluetooth.
- **Kolejność danych wejściowych Wiegand**: Ustawienie kolejności danych wejściowych Wiegand pomiędzy Normal i Reversed. W przypadku wybrania opcji Reversed numer karty wejściowej zostanie odwrócony.
- **Kolejność danych wyjściowych Wiegand:** Określa kolejność numeru karty.

- **Normalnie**: Numer karty jest wyświetlany w takiej postaci, w jakiej został odebrany.
- **Odwrócona**: Kolejność numerów kart jest odwrócona.

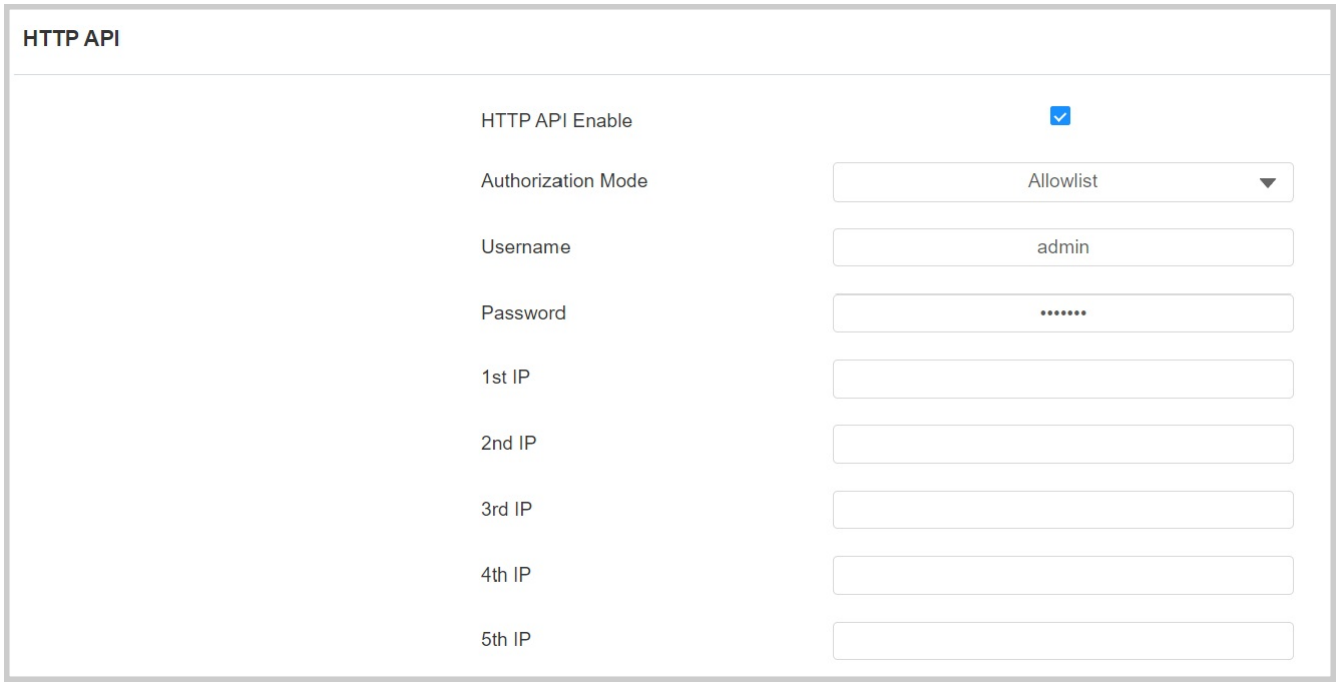
- Wiegand **Output CRC Enable**: Jest domyślnie włączona dla kontroli danych Wiegand. Wyłączenie go może prowadzić do niepowodzenia integracji z urządzeniami innych firm.

> **Uwaga**
>
> Kliknij **tutaj**, aby zobaczyć szczegółowe kroki konfiguracji.

Integracja przez HTTP API

Interfejs API HTTP został zaprojektowany w celu osiągnięcia integracji sieciowej między urządzeniem innej firmy a urządzeniem Akuvox.

Aby go skonfigurować, przejdź do **Ustawienia >** Interfejs **API HTTP**.



- **HTTP API Enable** : Włącz lub wyłącz funkcję HTTP API dla integracji z innymi firmami. Jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.
- **Tryb autoryzacji** : Wybierz jedną z następujących opcji: None, Allowlist, Basic, Digest i Token dla typu autoryzacji, które zostaną szczegółowo wyjaśnione w poniższej tabeli.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic** lub **Digest**. Domyślna nazwa użytkownika to admin.

- **Hasło**: Wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic** lub **Digest**. Domyślne hasło to admin.
- **1st IP-5th IP**: Wprowadź adres IP urządzeń innych firm, gdy dla integracji wybrano autoryzację **Allowlist**.

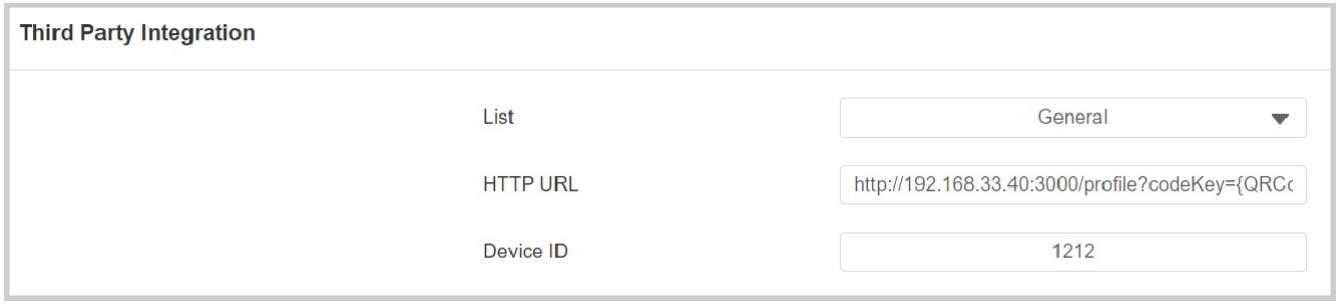
Poniższy opis dotyczy trybu uwierzytelniania:

NIE.	Tryb autoryzacji	Opis
1	Brak	Uwierzytelnianie nie jest wymagane dla HTTP API, ponieważ jest ono używane tylko do testów demonstracyjnych.
2	Lista dozwolonych	Po wybraniu tego trybu wymagane jest jedynie podanie adresu IP urządzenia innej firmy w celu uwierzytelnienia. Lista zezwoleń jest odpowiednia do pracy w sieci LAN.
3	Podstawowy	W przypadku wybrania tego trybu wymagane jest podanie nazwy użytkownika i hasła w celu uwierzytelnienia. W polu Authorization nagłówka żądania HTTP należy użyć metody kodowania Base64 do zakodowania nazwy użytkownika i hasła.
4	Digest	Metoda szyfrowania hasła obsługuje tylko MD5. MD5(Message Digest Algorithm) W polu Authorization nagłówka żądania HTTP: WWW-Authenticate: Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
5	Token	Ten tryb jest używany wyłącznie przez programistów Akuvox.

Integracja z podmiotami zewnętrznymi

Urządzenie obsługuje odczytywanie kodów QR i przesyłanie ich do serwera innej firmy. Generowanie i walidacja kodów QR są obsługiwane na serwerze innej firmy.

Aby ją skonfigurować, przejdź do opcji **Access Control > Relay > Third Party Integration** interface.



- **Lista**:

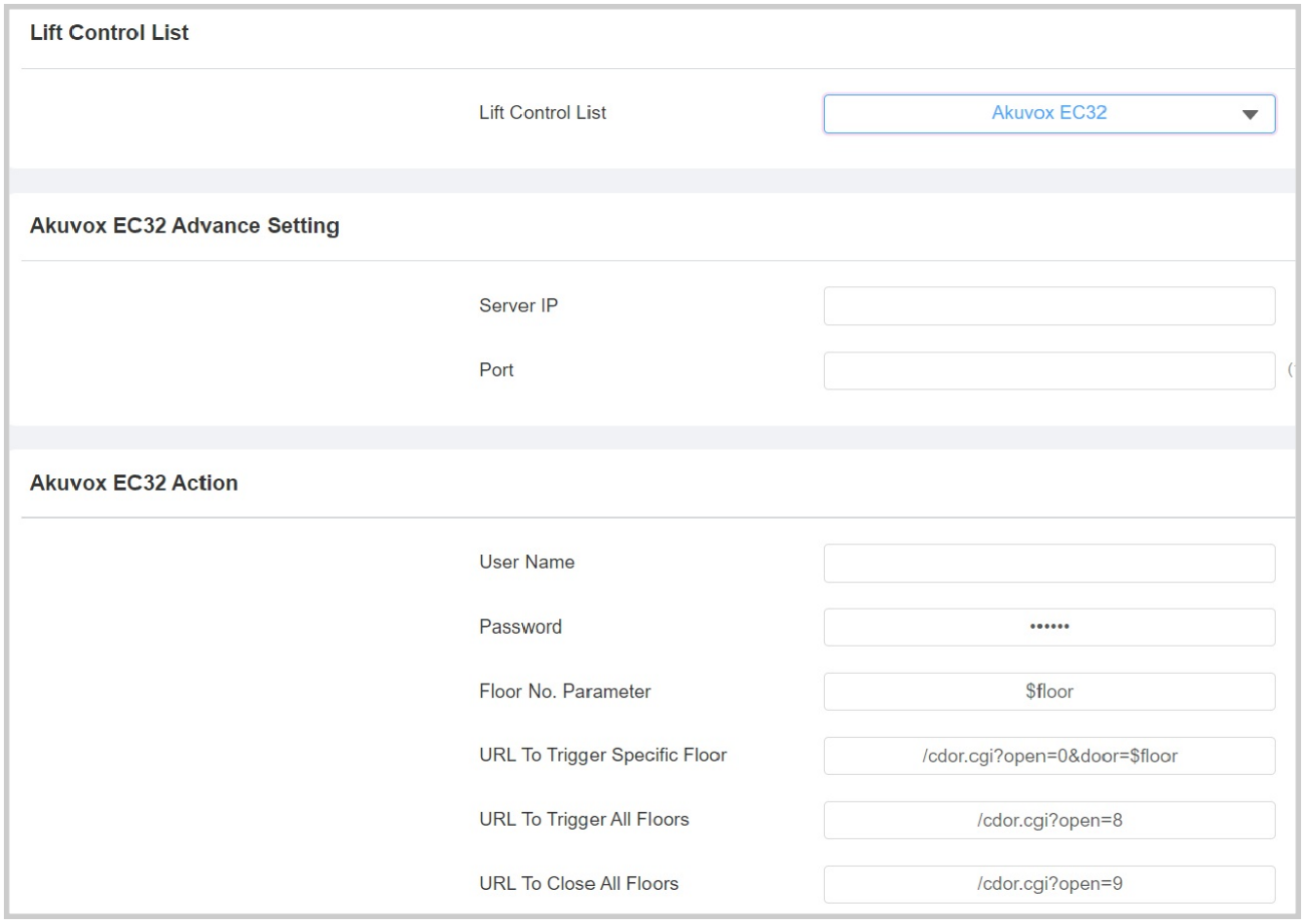
- **Brak** : Wyłączenie funkcji.
- **Ogólne**: Obsługa skanowania kodów QR innych firm. Po włączeniu wymagane jest wypełnienie adresu URL żądania i identyfikatora urządzenia.

- **HTTP URL**: Adres URL wysyłany do serwera strony trzeciej. Formaty URL są następujące:
  - http://server address/api/vistor/scan?codeKey={QRCode}&deviceId={DeviceID}
  - https://server address/api/vistor/scan?codeKey={QRCode}&deviceId={DeviceID}
- **Identyfikator urządzenia**: jako część adresu URL HTTP jest dostarczany przez dostawcę usług serwera zewnętrznego.

Kontrola podnoszenia

Urządzenie można podłączyć do kontrolera windy Akuvox lub innej firmy w celu sterowania windą. Użytkownicy mogą wezwać windę, aby zjechała na parter, gdy uzyskają dostęp za pomocą metod dostępu.

Aby skonfigurować sterowanie windą, przejdź do interfejsu **Device > Lift Control**.



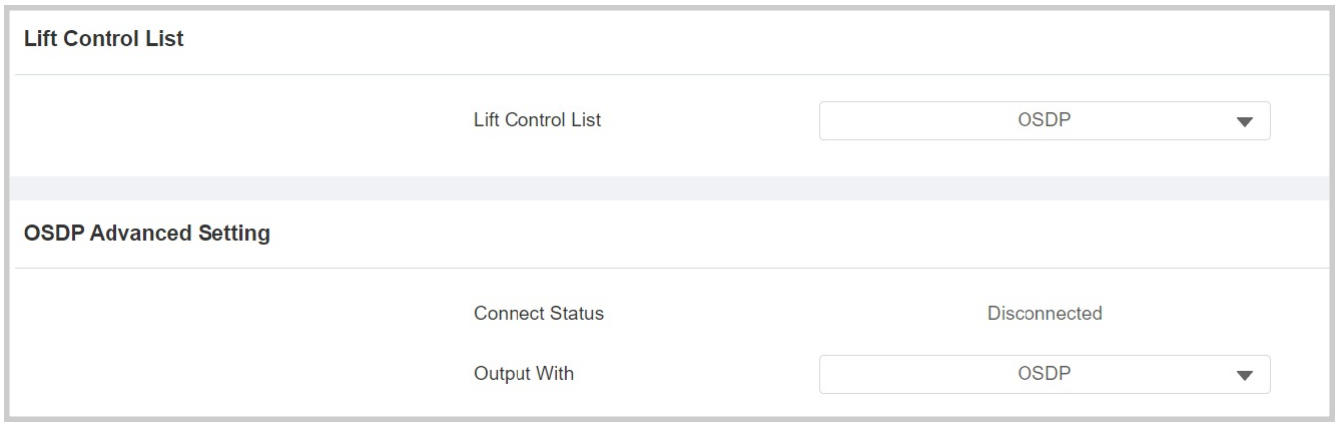
- **Lista sterowania windą**: Wybierz Akuvox EC32 w celu integracji z kontrolerem windy Akuvox.
- **IP serwera**: Wprowadź adres IP serwera kontrolera windy Akuvox.
- **Port**: Wprowadź port serwera kontrolera windy Akuvox.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika kontrolera windy w celu uwierzytelnienia.
- **Hasło** : Wprowadź hasło kontrolera windy w celu uwierzytelnienia.
- **Floor NO. Parametr**: Wprowadź parametr Floor number dostarczony przez Akuvox.
- **URL To Trigger Specific Floor**: Wprowadź adres URL, aby wyzwolić określone piętro.
- **URL do wyzwalania wszystkich pięter** : Wprowadź adres URL do wyzwalania wszystkich pięter.

• **URL do zamknięcia wszystkich pięter** : Wprowadź adres URL używany do zamykania wszystkich pięter.

Ustawienia OSDP

Urządzenie można zintegrować ze sterownikiem windy innej firmy za pośrednictwem protokołu OSDP. Należy sprawdzić protokół integracji urządzenia i upewnić się, że są one takie same.

Aby ją skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **Lift Control**.

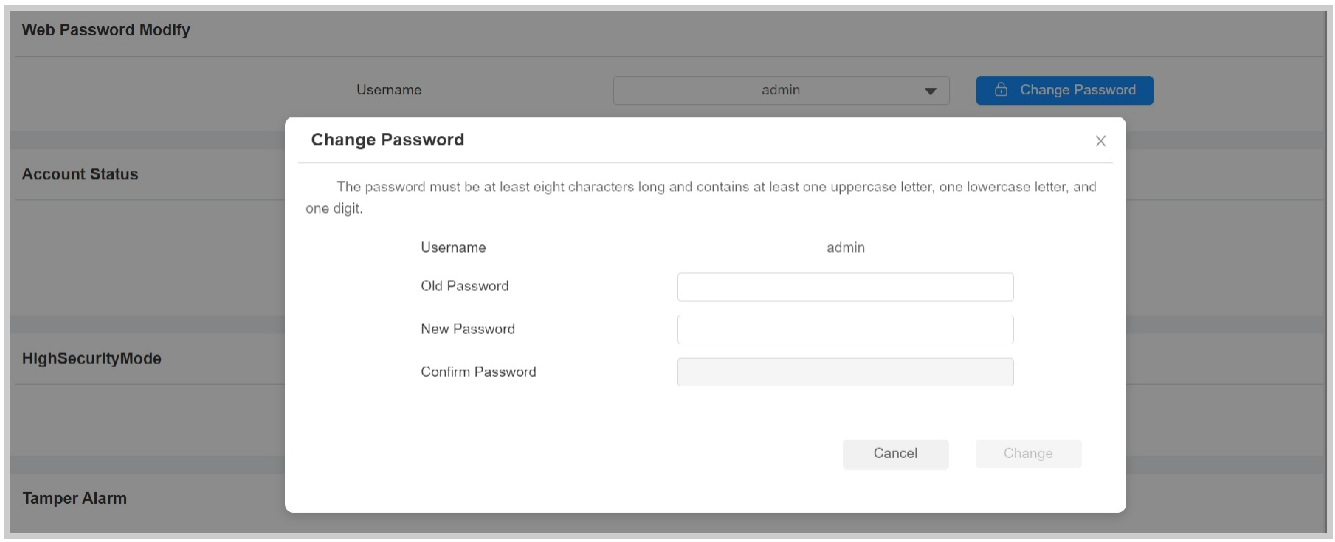


- **Lift Control List**: Wybierz OSDP z listy.
- **Stan połączenia**: Wskazuje stan połączenia.
- **Output With**: Wybierz sposób wysyłania numeru karty.
    - **OSDP**: Numer karty zostanie wysłany do urządzenia innego producenta przez RS485.
    - **Brak**: Numer karty nie zostanie wysłany, ale pozostanie w systemie.

Modyfikacja hasła

Hasło internetowe urządzenia można modyfikować zarówno dla konta administratora, jak i konta użytkownika. Aby je skonfigurować, przejdź do interfejsu **System > Security > Web Password Modify**.

Kliknij przycisk **Zmień hasło**, aby zmodyfikować hasło.

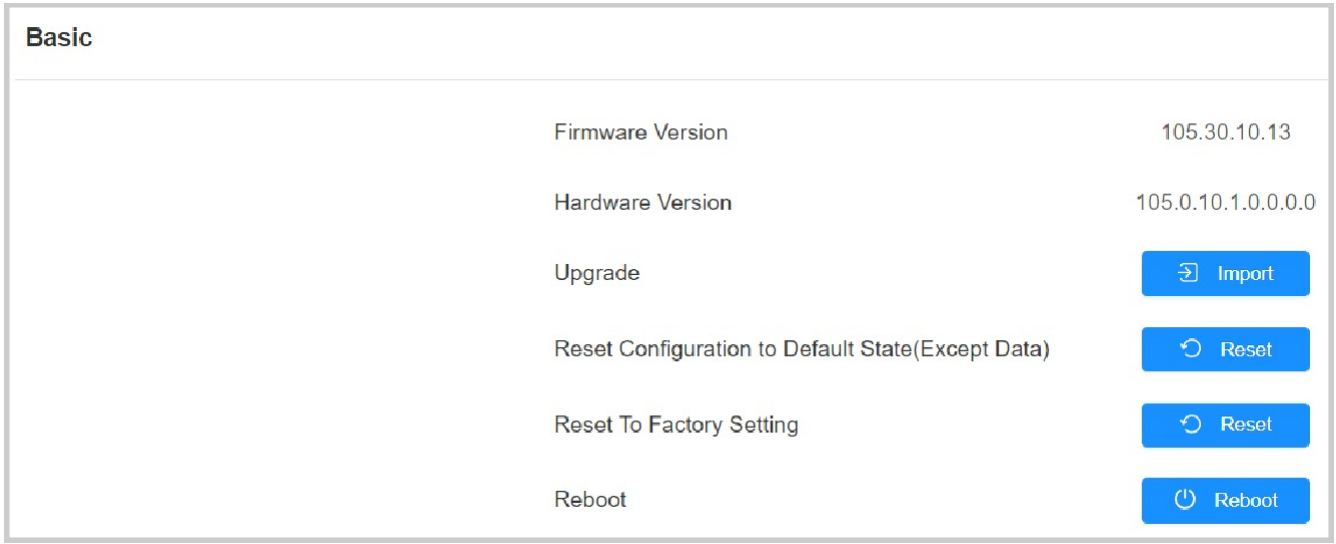


Aby włączyć lub wyłączyć konto użytkownika, przewiń do sekcji **Stan konta**.

Ponowne uruchamianie i resetowanie systemu

Reboot

Ponownie uruchom urządzenie w interfejsie **System > Aktualizacja**.



Aby skonfigurować harmonogram ponownego uruchamiania urządzenia, przejdź do interfejsu **System > Auto Provisioning > Reboot Schedule**.

Reset

Możesz wybrać **Reset To Factory Setting**, jeśli chcesz zresetować urządzenie (usuwając zarówno dane konfiguracyjne, jak i dane użytkownika, takie jak karty RF, dane twarzy itp.) Można też wybrać **Reset Configuration to Default State (Except Data) Reset**, aby zresetować urządzenie (zachowując dane użytkownika).

Zresetuj urządzenie w interfejsie **System > Aktualizacja**.