Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX X912S DOOR PHONE

Administrator Guide

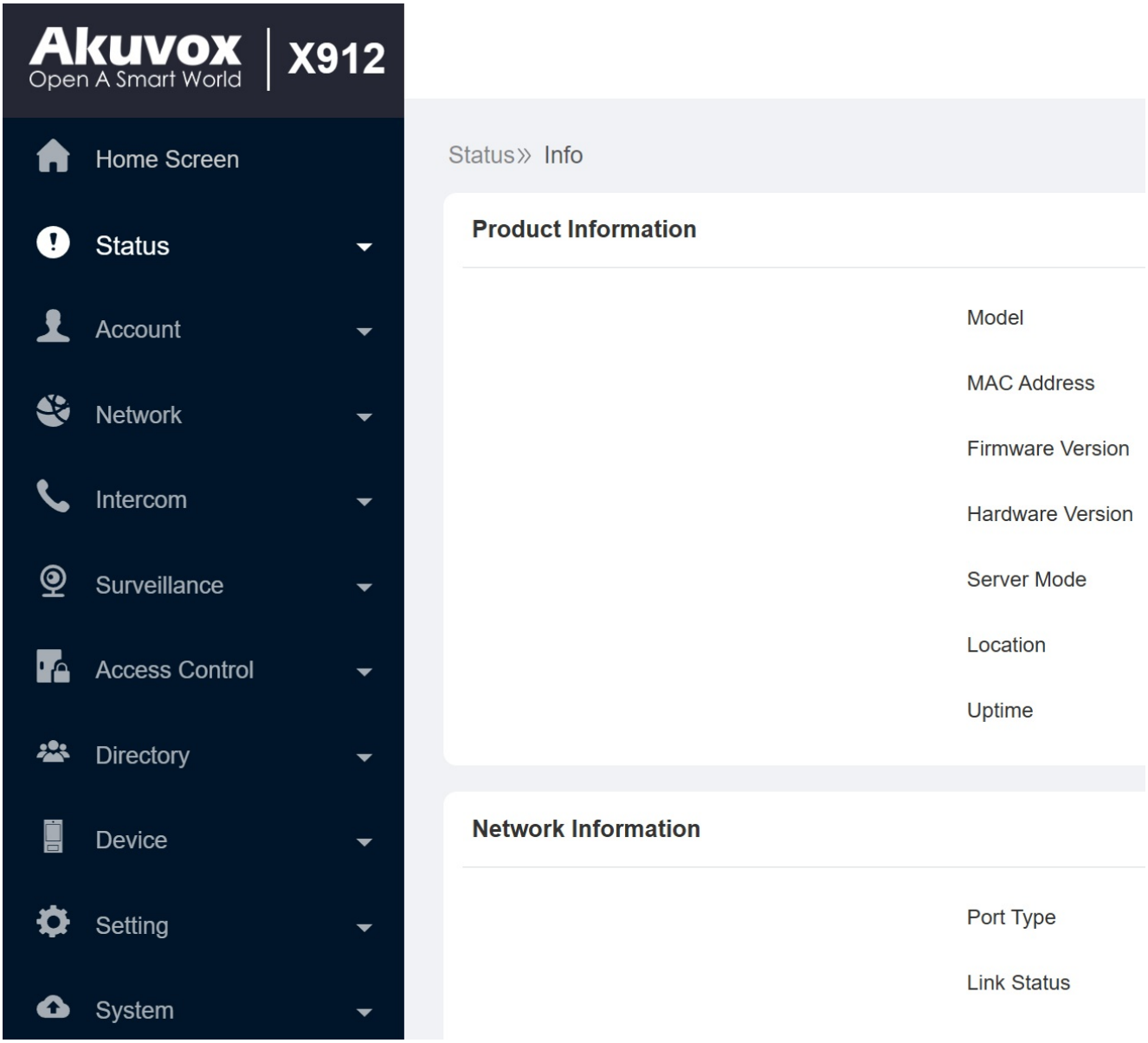
Dziękujemy za wybranie bramofonu Akuvox serii X912. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja została napisana w oparciu o wersję 912.30.1.118 i zawiera wszystkie konfiguracje funkcji i cech bramofonu serii X912. Aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe, odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną.

Przegląd produktów

Akuvox X912 to wideodomofon IP Linux z 4-calowym ekranem dotykowym i fizyczną klawiaturą. Obejmuje komunikację audio i wideo, kontrolę dostępu i nadzór wideo. Precyzyjnie dostrojony system operacyjny Linux, technologia komunikacji oparta na chmurze i sztucznej inteligencji umożliwiają dostosowanie urządzenia do własnych potrzeb. X912 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 duże poczucie bezpieczeństwa dzięki różnym rodzajom dostępu, takim jak dostęp za pomocą karty, rozpoznawanie twarzy NFC, Bluetooth, kod QR. Bramofony z serii X912 mają zastosowanie w budynkach mieszkalnych klasy średniej i wyższej oraz w ekskluzywnych budynkach mieszkalnych z jednym najemcą.

Wprowadzenie do menu konfiguracji

- **Status** : ta sekcja zawiera podstawowe informacje, takie jak informacje o produkcie, informacje o sieci, rejestr połączeń i rejestr drzwi itp.
- **Konto**: ta sekcja dotyczy konta SIP, serwera SIP, serwera proxy, typu protokołu transportowego, kodeka audio i wideo, DTMF, licznika sesji itp.
- **Sieć**: ta sekcja dotyczy głównie ustawień DHCP i statycznego adresu IP, ustawień portu RTP oraz wdrażania urządzeń itp.
- **Interkom: ta sekcja** obejmuje ustawienia interkomu, funkcję połączeń i plan
- wybierania. **Nadzór**: ta sekcja obejmuje wykrywanie ruchu, RTSP, MJPEG, ONVIF, transmisję na żywo itp.
- **Kontrola dostępu**: ta sekcja obejmuje kontrolę wejścia, przekaźnik, ustawienia karty, ustawienia rozpoznawania twarzy, prywatny kod PIN itp.
- **Katalog**: ta sekcja obejmuje zarządzanie użytkownikami, kartą RF, kodem PIN, rozpoznawaniem twarzy i kontaktami.
- **Urządzenie**: ta sekcja zawiera ustawienia oświetlenia, LCD i audio, sterowanie windą, połączenie Wiegand.
- **Ustawienia**: ta sekcja zawiera czas i język, ustawienia akcji, harmonogram kontroli dostępu, wyświetlanie ekranu, HTTP API.
- **System**: ta sekcja obejmuje aktualizację oprogramowania układowego, resetowanie i ponowne uruchamianie urządzenia, automatyczne dostarczanie pliku konfiguracyjnego, diagnostykę błędów, bezpieczeństwo, PCAP, dziennik systemowy, wywołanie sieciowe, alarm temperamentu i modyfikację hasła.


Akuvox
Open A Smart World
X912
Home Screen
Status
Account
Network
Intercom
Surveillance
Access Control
Directory
Device
Setting
System
Status» Info
Product Information
Model
MAC Address
Firmware Version
Hardware Version
Server Mode
Location
Uptime
Network Information
Port Type
Link Status

Specyfikacja modelu

Model	X912
Ekran dotykowy	✓
Wejście przekaźnika	3
Wyjście przekaźnika	2
Alarm wł.	X
RS485	✓
Czytnik kart	13,56 MHz i 125 kHz, NFC
Wi-Fi	X
Bluetooth	✓
Wykrywanie temperatury	X
Rozpoznawanie twarzy	✓
LTE	X
USB	X
Zewnętrzna karta SD	X

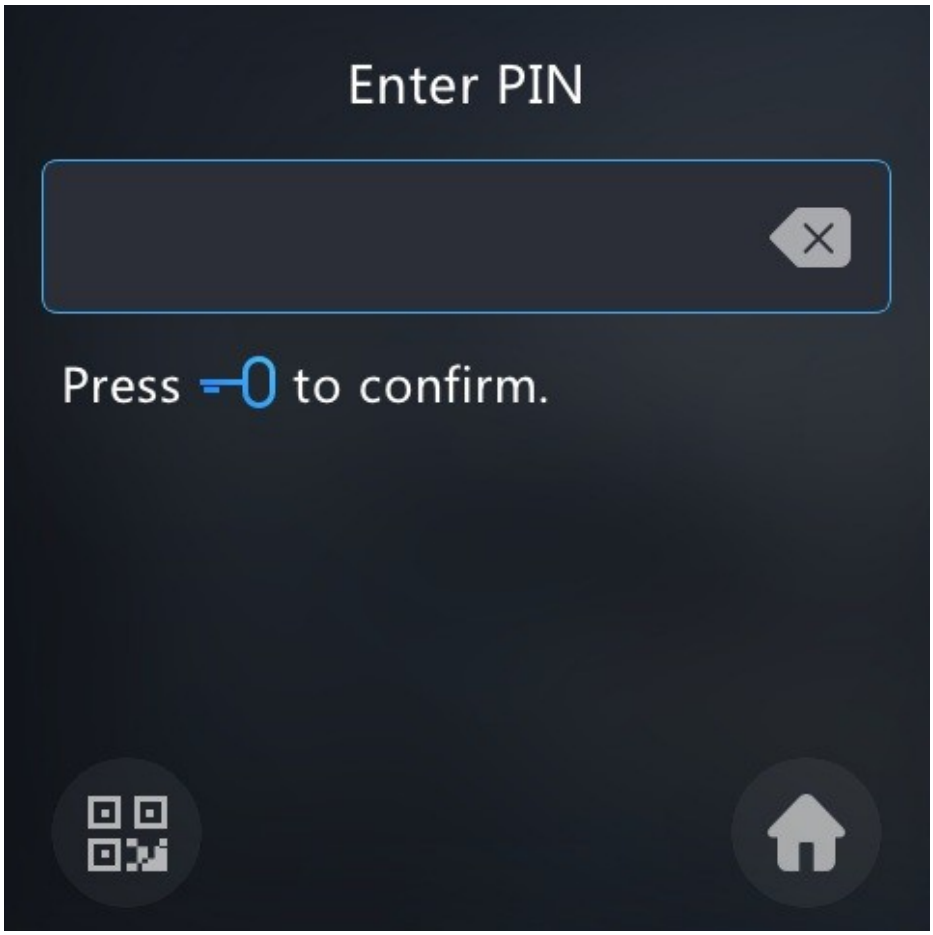
Dostęp do urządzenia

Dostęp do ustawień systemowych bramofonów można uzyskać bezpośrednio na urządzeniu lub za pośrednictwem interfejsu internetowego urządzenia.

Dostęp do ustawień urządzenia na urządzeniu

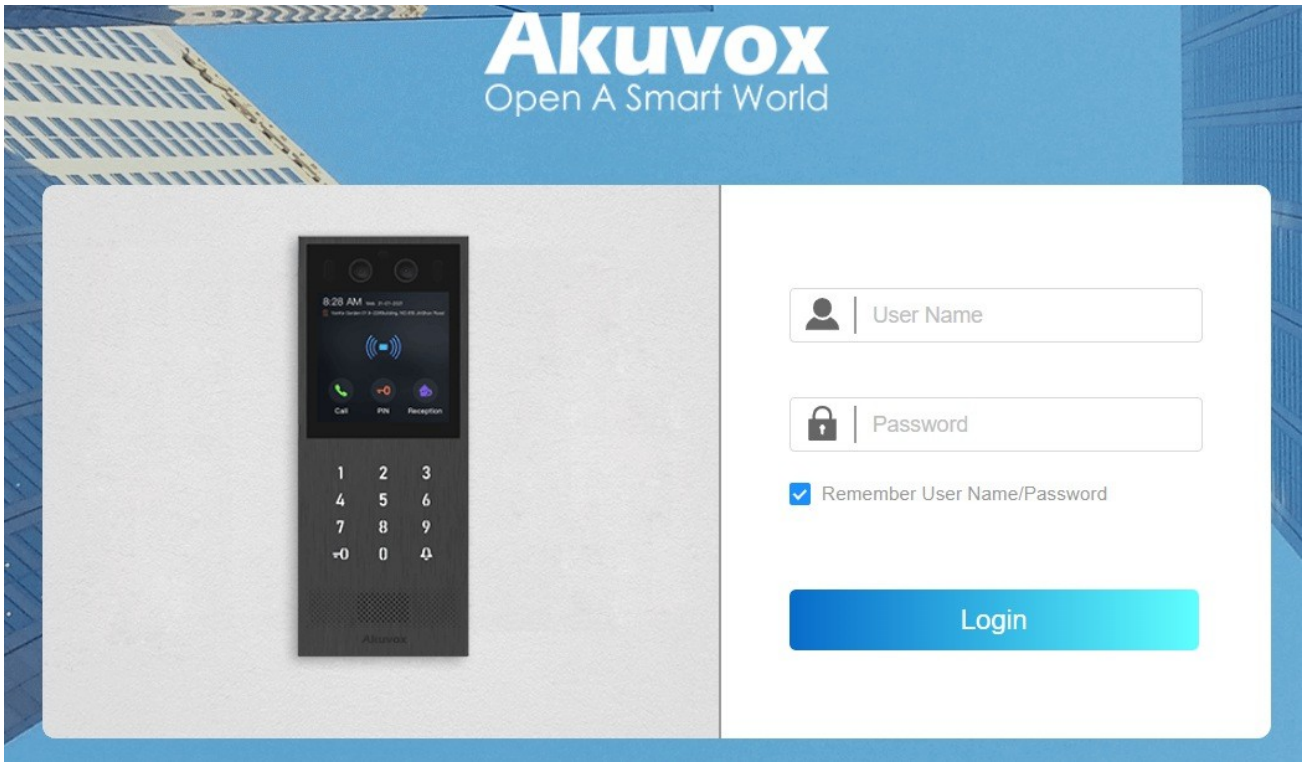
Przed konfiguracją bramofonu należy upewnić się, że urządzenie jest prawidłowo zainstalowane i podłączone do normalnej sieci. Za pomocą narzędzia skanera IP Akuvox wyszukaj adres IP urządzenia w tej samej sieci LAN. Następnie użyj adresu IP, aby zalogować się do przeglądarki internetowej za pomocą nazwy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

Aby uzyskać dostęp do ustawień systemowych urządzenia, można nacisnąć ikonę na ekranie lub na klawiaturze wprowadzić domyślny systemowy kod PIN **2396**, a następnie nacisnąć przycisk w celu potwierdzenia. Aby uzyskać dostęp do ekranu ustawień, naciśnij następnie wprowadź domyślny kod PIN ustawień **3888** .



Dostęp do ustawień urządzenia w interfejsie sieciowym

Można również wprowadzić adres IP urządzenia w przeglądarce internetowej, aby zalogować się do interfejsu internetowego urządzenia, gdzie można skonfigurować i dostosować parametry itp.



Uwaga

Adres IP urządzenia można również uzyskać za pomocą skanera Akuvox IP, aby zalogować się do interfejsu internetowego urządzenia.

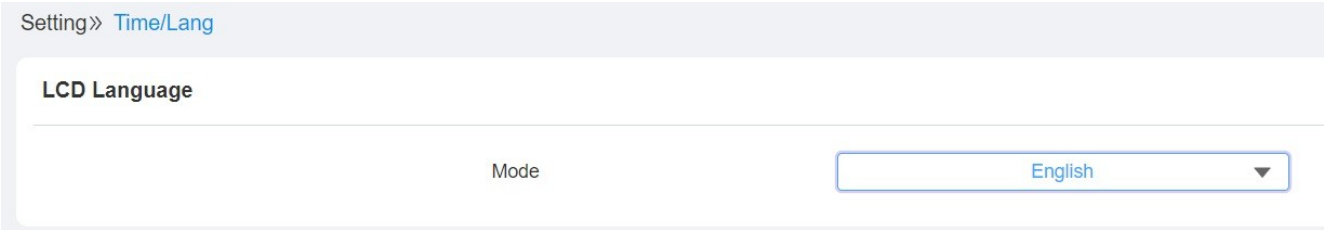
- Pobierz skaner IP: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Zobacz szczegółowy przewodnik: **https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner**
- Zdecydowanie zalecana jest przeglądarka Google Chrome.
- Początkowa nazwa użytkownika i hasło to **admin** i należy zwracać uwagę na wielkość liter we wprowadzanych nazwach użytkowników i hasłach.

Ustawienia języka i czasu

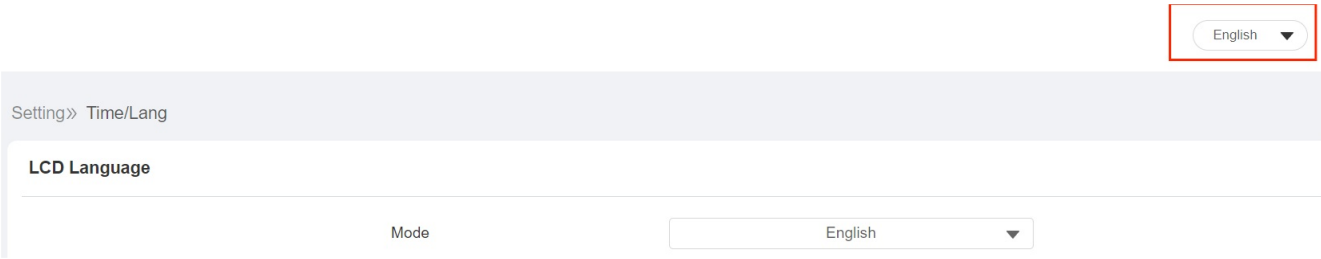
Ustawienia języka

Ustaw język podczas początkowej konfiguracji urządzenia lub później za pomocą urządzenia lub interfejsu internetowego zgodnie z własnymi preferencjami.

Aby wybrać język wyświetlania ekranu urządzenia, przejdź do opcji **Ustawienia >Czas/Lang >** Interfejs **języka LCD.**



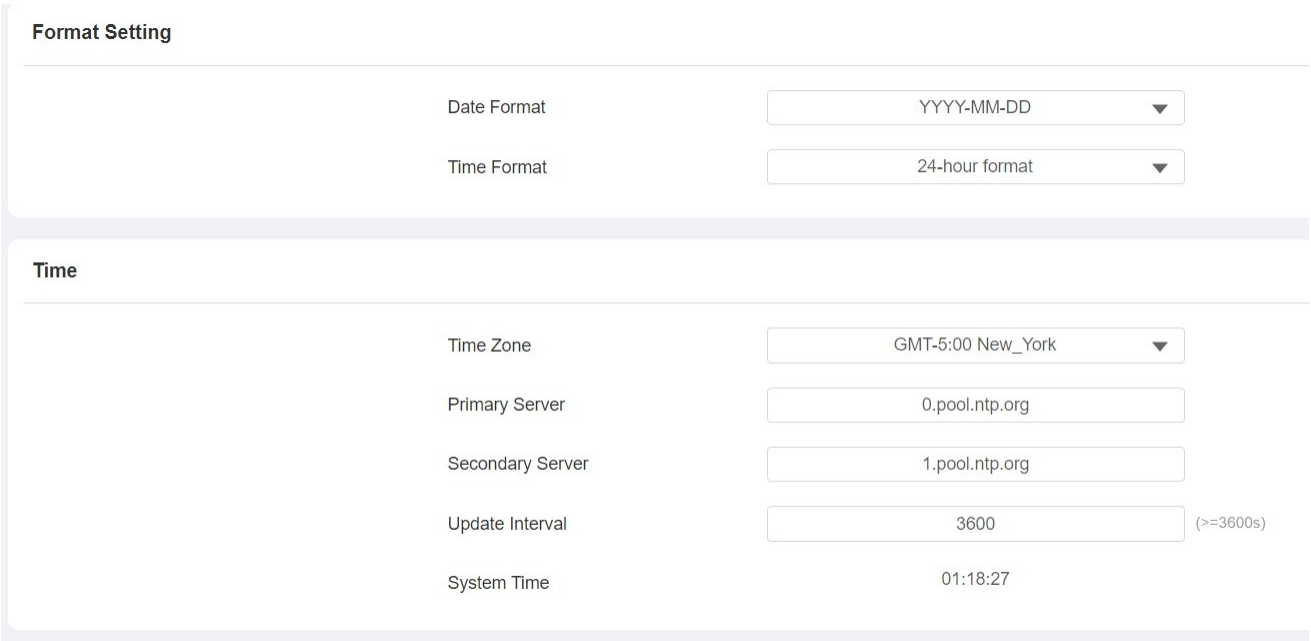
Język internetowy można również wybrać w prawym górnym rogu tego samego interfejsu internetowego.



Ustawienie czasu

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 go w interfejsie **Ustawienia >Czas/Lang.**



Konfiguracja parametrów :

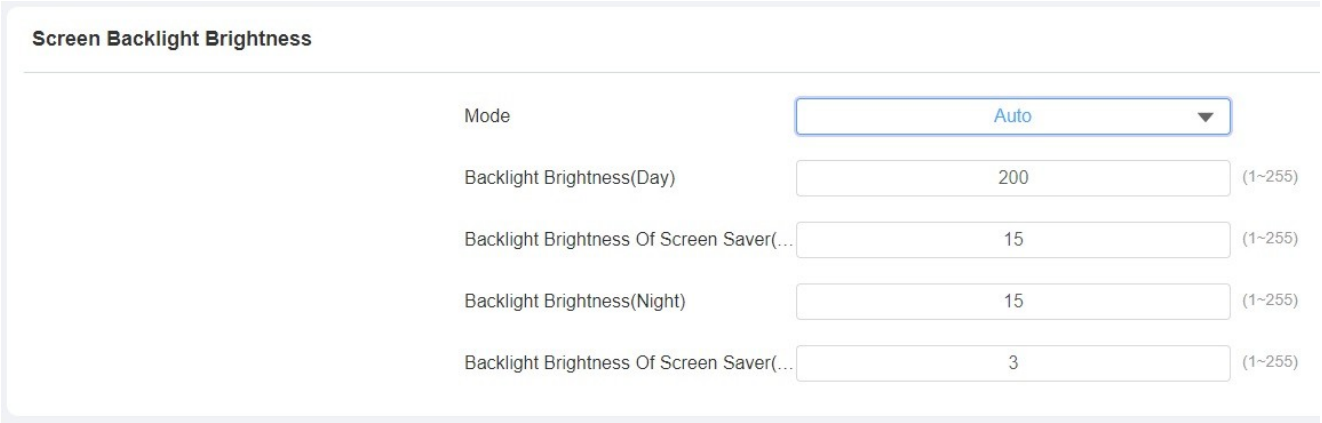
- **Primary/Secondary Server**: serwer strefy czasowej, zwykle automatycznie uzyskuje czas podczas łączenia się z siecią. Serwer alternatywny zacznie działać, gdy serwer podstawowy będzie nieprawidłowy.
- **Update Interval (Interwał aktualizacji**): konfiguracja interwału między dwoma kolejnymi żądaniami NTP.

Ustawienia LCD

Ustawienie jasności ekranu LCD w interfejsie internetowym

W interfejsie internetowym można ustawić i dostosować jasność podświetlenia ekranu i wygaszacza ekranu.

Aby skonfigurować konfigurację w sieci Web **Urządzenie > LCD > Jasność podświetlenia ekranu** .



Konfiguracja parametrów :

- **Tryb** : kliknij, aby wybrać tryb **ręczny** lub **automatyczny** podświetlenia. Po wybraniu opcji

Auto podświetlenie zostanie automatycznie dostosowane do jasności ekranu i odwrotnie.

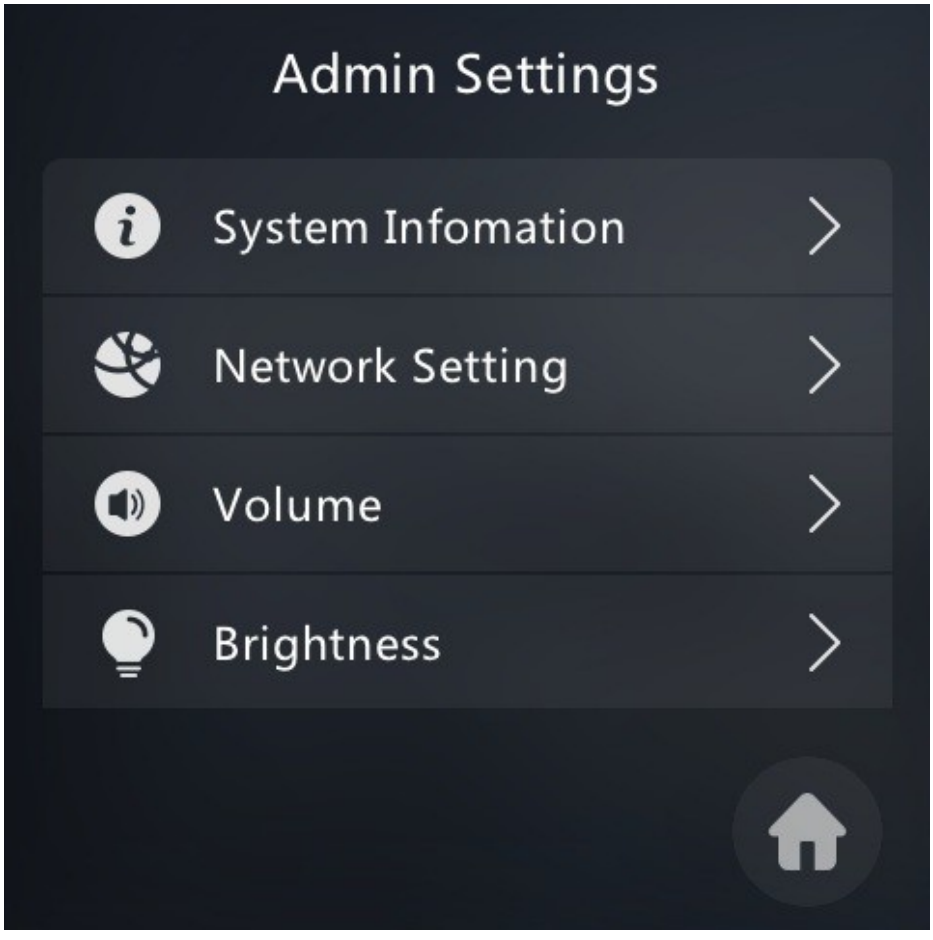
- **Jasność podświetlenia (dzień)**: wybierz wartość jasności z zakresu 1-255. Wartość domyślna to

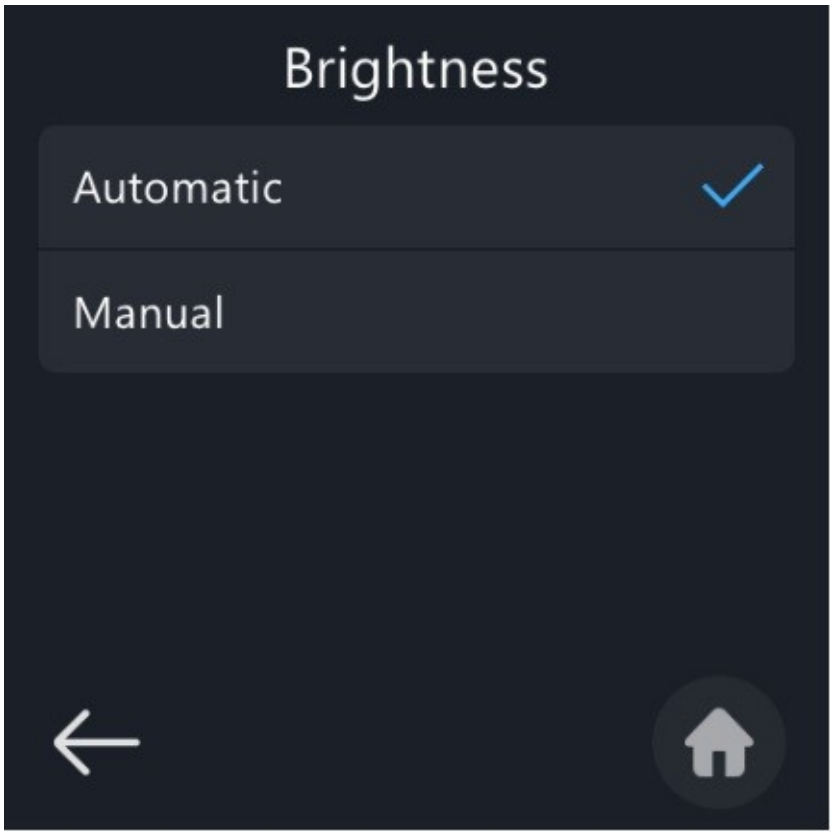
  200. Im większa wartość, tym jaśniejszy ekran.
- **Backlight Brightness Of Screensaver (Day) (Jasność podświetlenia wygaszacza ekranu w dzień)**: regulacja podświetlenia wygaszacza ekranu w ciągu dnia przy użyciu wartości z zakresu (1-255).
- **Jasność podświetlenia (noc)**: regulacja podświetlenia wygaszacza ekranu w nocy za pomocą wartości z zakresu (1-255).
- **Backlight Brightness Of Screensaver (Night) (Jasność podświetlenia wygaszacza ekranu w nocy)**: regulacja jasności podświetlenia wygaszacza ekranu w nocy w zakresie (0-255).

Ustawienie jasności ekranu LCD na urządzeniu

W urządzeniu można ustawić i dostosować jasność podświetlenia ekranu.

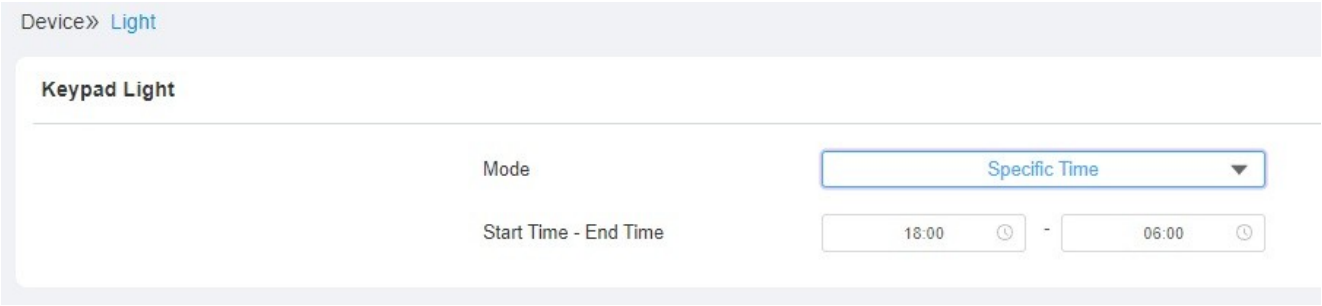
Wybierz opcję **Jasność** , a następnie opcję **Automatycznie** w celu automatycznej regulacji jasności lub opcję **Ręcznie** w celu ręcznej regulacji jasności.





Ustawienie podświetlenia klawiatury

Możesz sterować podświetleniem klawiatury, aby je włączać/wyłączać lub włączać/wyłączać zgodnie z harmonogramem. Aby to zrobić, przejdź do opcji **Urządzenie > Światło > Podświetlenie klawiatury**.



Konfiguracja parametrów :

- **Tryb** : wybierz **Zawsze wyłączone**, aby klawiatura pozostawała wyłączona. Wybierz **Auto,** aby podświetlenie klawiatury włączało się automatycznie po wyłączeniu ekranu. Wybierz **Określony czas**, aby podświetlenie klawiatury włączało się/wyłączało zgodnie z harmonogramem (Czas rozpoczęcia-Czas zakończenia). Podświetlenie klawiatury przejdzie jednak w tryb **automatyczny** w czasie nieobjętym harmonogramem.

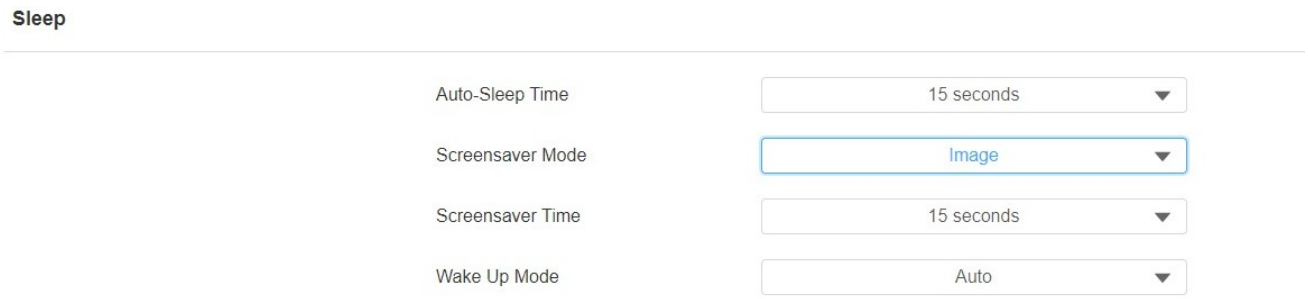
Konfiguracja ekranu

Bramofon umożliwia korzystanie z różnych ekranów, aby wzbogacić wrażenia wizualne i operacyjne poprzez dostosowanie ustawień do własnych preferencji.

Konfiguracja wygaszacza ekranu

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

W interfejsie internetowym przejdź do **Urządzenie > LCD > Uśpienie** .



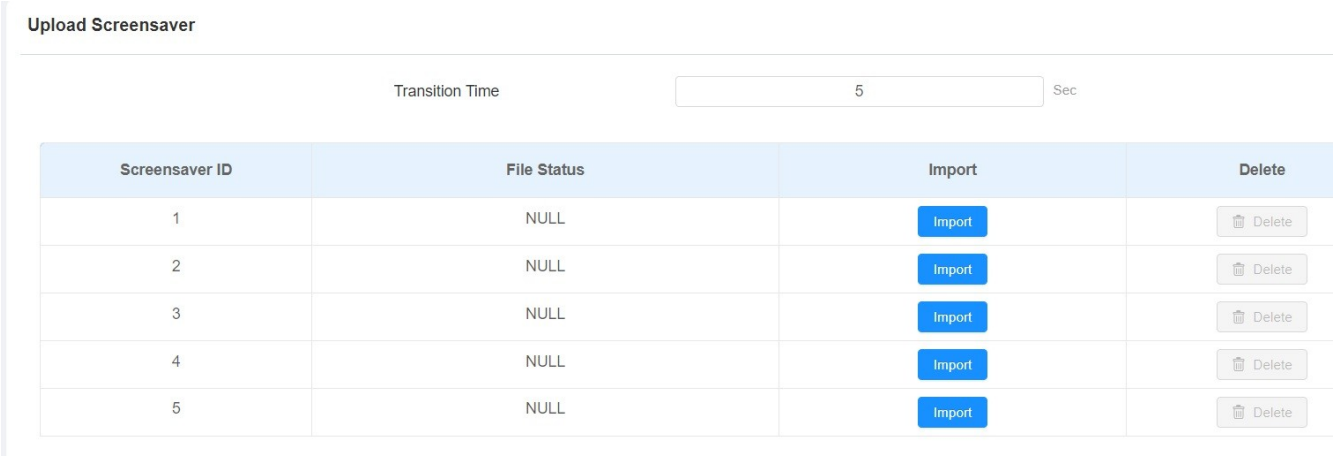
Konfiguracja parametrów :

- **Czas automatycznego uśpienia**: jeśli ustawisz czas uśpienia, na przykład 15 sekund, urządzenie przejdzie w tryb wygaszacza ekranu (wyświetlając wygaszacz ekranu w określonym czasie), gdy urządzenie nie wykryje żadnej operacji lub żadnego zbliżającego się obiektu przez kolejne 15 sekund.
  Jeśli jednak tryb wygaszacza ekranu jest wyłączony, ekran urządzenia zostanie wyłączony bezpośrednio po 15 sekundach. Czas automatycznego uśpienia wynosi od 5 sekund do 30 minut.
- **Tryb wygaszacza ekranu** : wybierz opcję **Obraz,** aby wyświetlić spersonalizowane zdjęcia przesłane do urządzenia; wybierz opcję **Wyłącz**, aby wyłączyć funkcję wygaszacza ekranu.
- **Screensaver Time(Sec)**: wybór czasu trwania wygaszacza ekranu. Zakres czasu: 5 sekund do 30 min.
- **Tryb wybudzania** : Po wybraniu trybu **Auto** ekran zostanie automatycznie wybudzony, gdy urządzenie wykryje zbliżający się obiekt lub operację. Wybierz opcję **Ręcznie**, aby wybudzić ekran za pomocą dotyku.

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 przeprowadzić konfigurację w interfejsie internetowym **Urządzenie > LCD > Prześlij wygaszacz ekranu.**



Konfiguracja parametrów:

- **Czas przejścia** : ustaw czas wyświetlania każdego przesłanego zdjęcia w **Interwał (sek.)**, zakres czasu wyświetlania wynosi od **1 do 120** sekund. Ustawienie domyślne to **5** sekund.

Uwaga

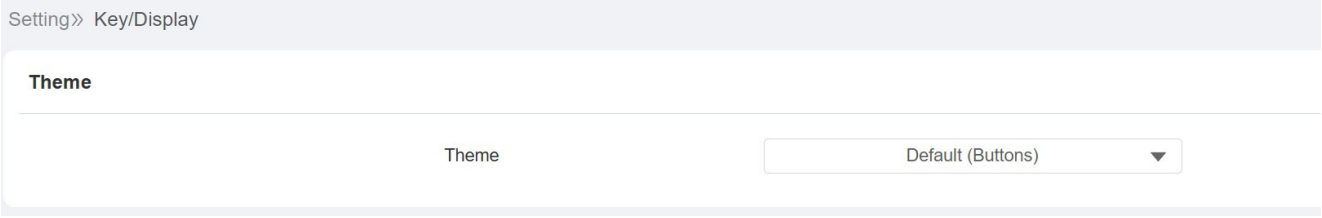
- Przesyłane zdjęcia powinny być w **formacie JPG** o maksymalnej rozdzielczości 2 mln pikseli.

Uwaga

- Poprzednie zdjęcia o określonej kolejności ID zostaną nadpisane podczas powtarzania.

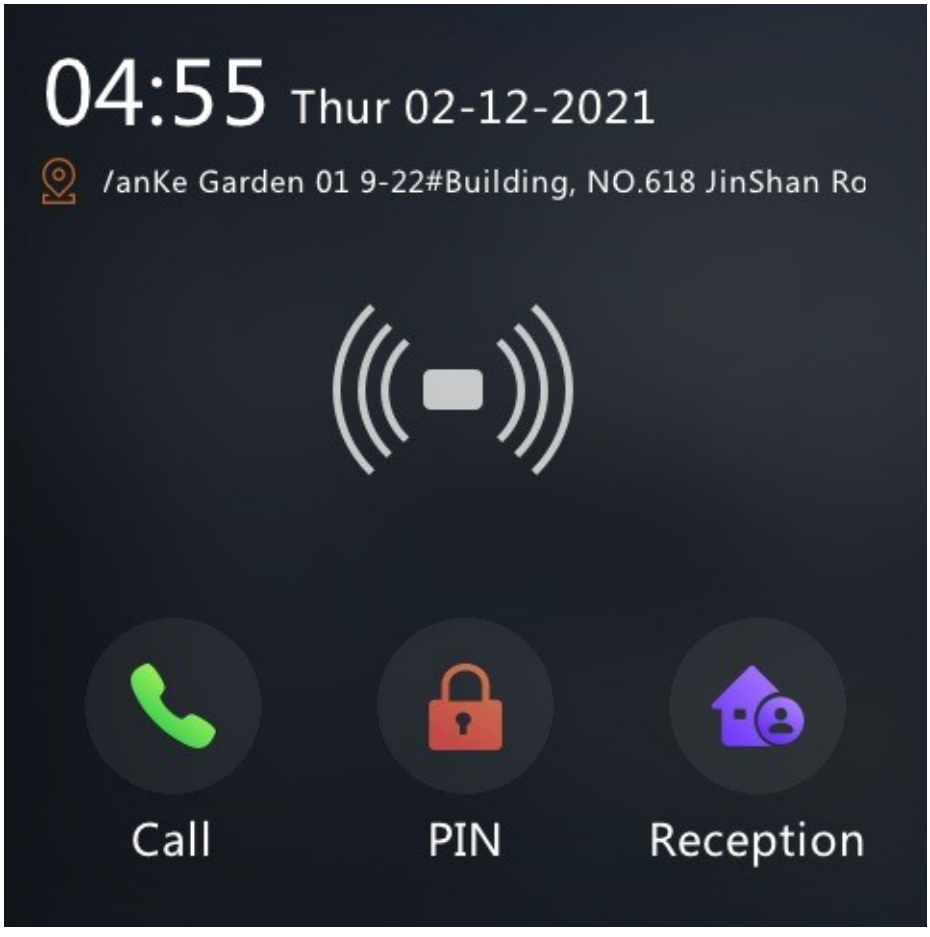
Konfiguracja trybu wyświetlania ekranu opartego na scenariuszu

Bramofony X912 oferują cztery rodzaje trybów wyświetlania ekranu do różnych zastosowań: Tryb **domyślny (przyciski)**, tryb **bezpośredni,** tryb **szybkiego wybierania** i tryb **niestandardowego tekstu.** W interfejsie internetowym przejdź do **Ustawienia >**

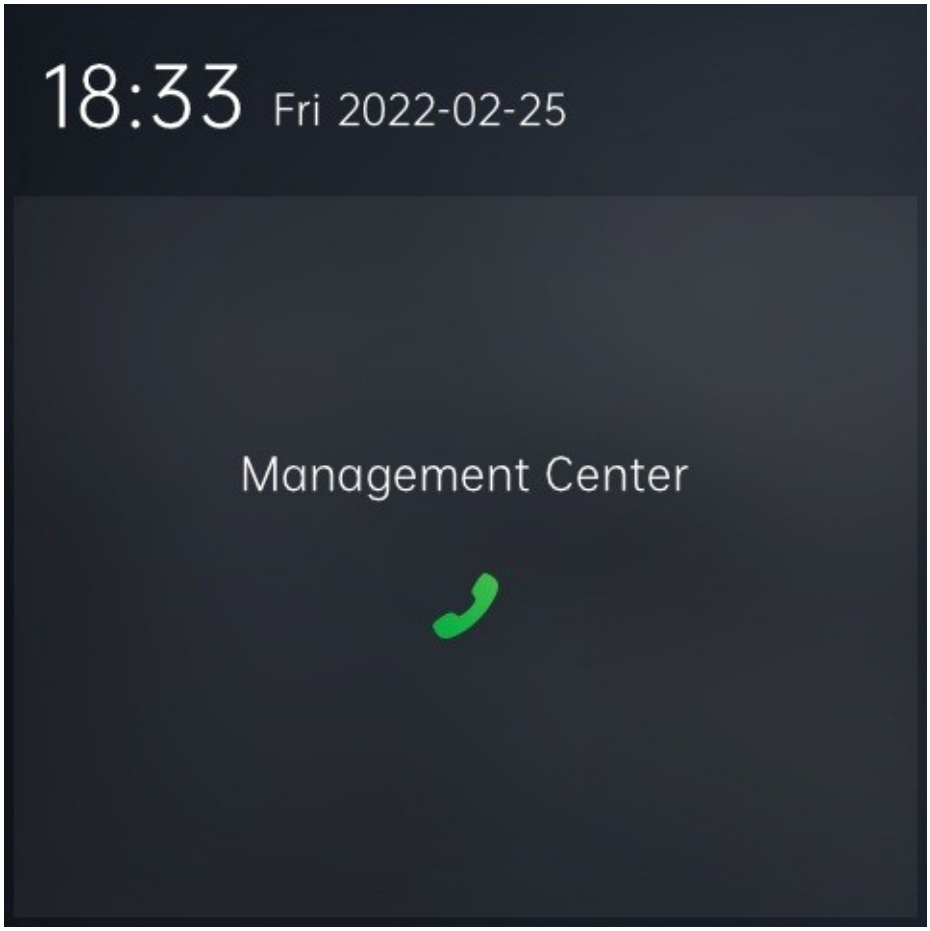


Tryb katalogu

Tryb domyślny (przyciski)



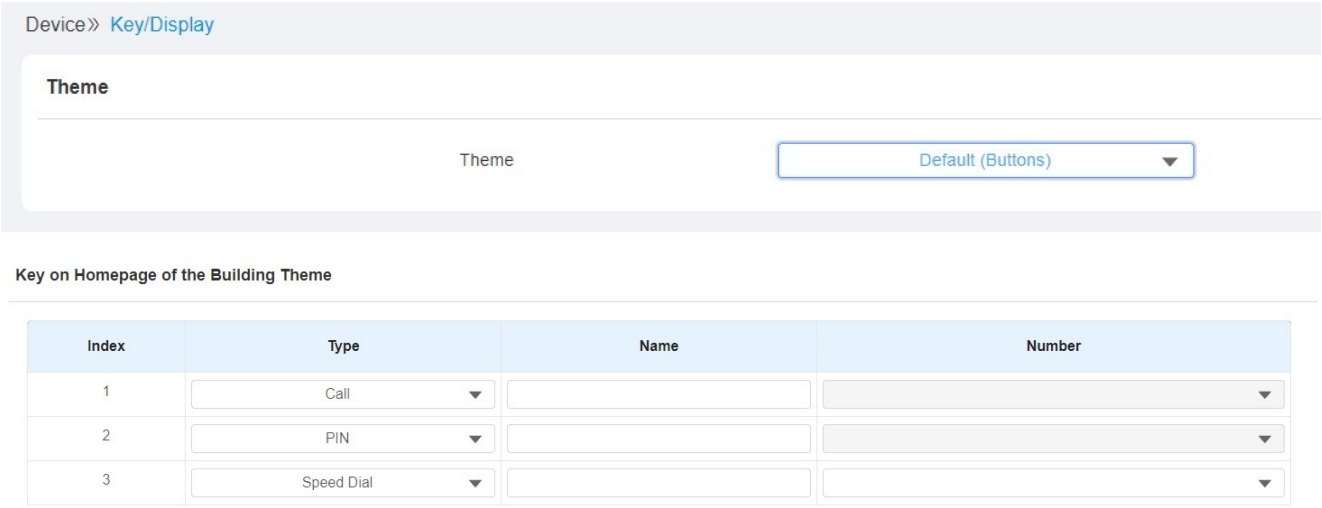
Tryb szybkiego wybierania



Dostosowany tryb tekstowy

Tryb domyślny (przyciski) Wyświetlanie ekranu głównego

Wyświetlanie ekranu głównego można zmienić poprzez konfigurację układu kart i wyświetlanie ikon języka zgodnie z potrzebami w witrynie internetowej urządzenia **Ustawienia > Klawisze/Wyświetlanie > Klawisze na stronie głównej motywu budynku** .

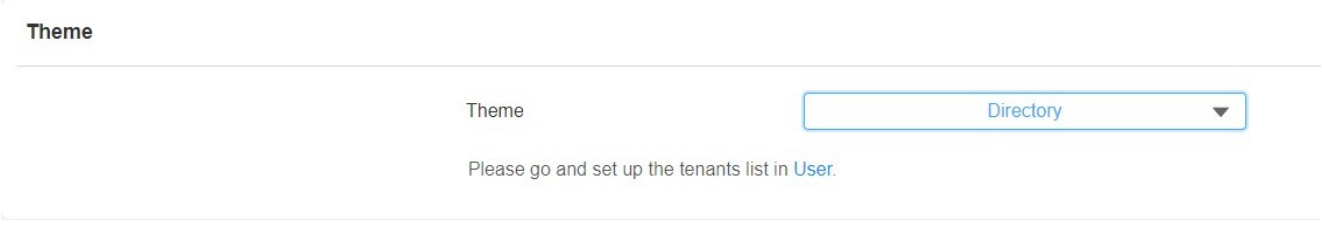


Konfiguracja parametrów :

- **Typ** : wybierz typ karty (Połączenie, PIN, Szybkie wybieranie, Katalog i Kod Temp Key-QR) odpowiadający kolejności ID, która wskazuje pozycję karty. Na przykład, jeśli chcesz, aby zakładka **Temp Key** była wyświetlana w pozycji pierwszej wiersza zakładek, możesz kliknąć, aby wybrać typ kolejności ID 1. Inne pozycje zakładek można odpowiednio zmienić.
- **Nazwa** : wprowadź nową nazwę, aby zastąpić oryginalną nazwę typu, ale nie zmienia atrybutu typu.
- **Numer**: jest dostępny dla tych funkcji, które wymagają skonfigurowania numerów, takich jak funkcja **szybkiego wybierania.**

Wyświetlanie ekranu głównego w trybie katalogu

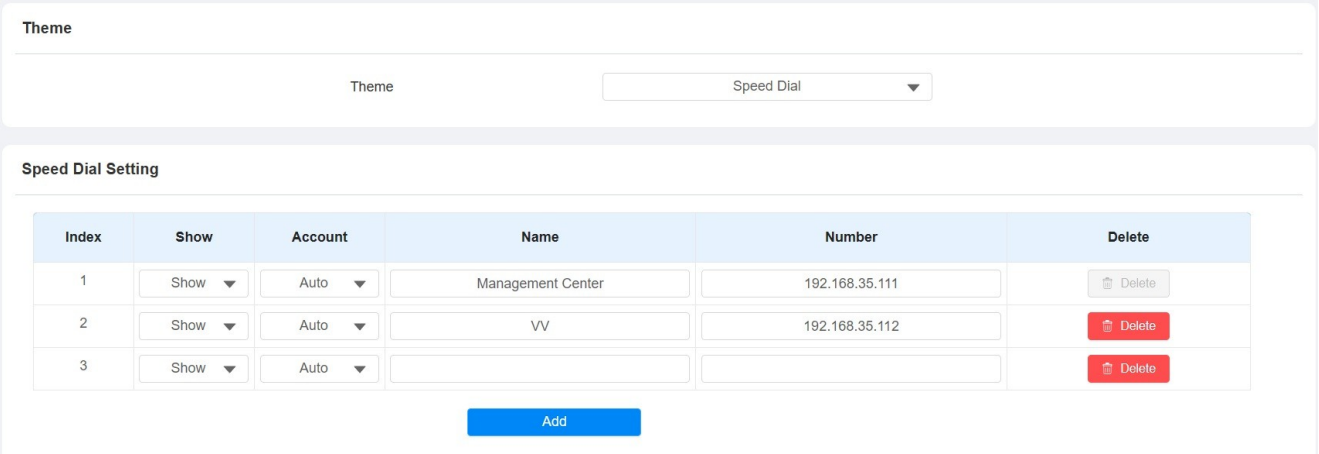
Katalog kontaktów można ustawić jako ekran główny, aby można było łatwo wybrać numer kontaktu. Aby to ustawić, przejdź do opcji **Ustawienia > Klawisze/Wyświetlacz > Motyw** .



Wyświetlanie ekranu głównego w trybie szybkiego wybierania

Po ustawieniu trybu szybkiego wybierania dla ekranu głównego, numery szybkiego wybierania będą wyświetlane na ekranie głównym, dzięki czemu można łatwo wybierać numery do

określonych kontaktów. Można przejść do opcji **Ustawienia > Klawisze/Wyświetlacz > Ustawienia szybkiego wybierania** .

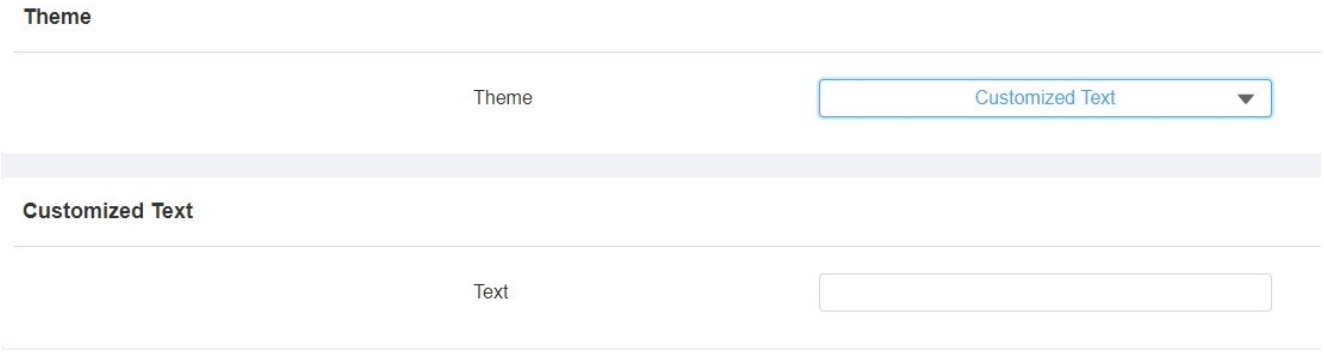


Uwaga

X912 obsługuje do pięciu numerów szybkiego wybierania na ekranie.

Ekran główny w trybie tekstowym

X912 umożliwia wyświetlanie imion osób lub nazw firm itp. na ekranie głównym w celu identyfikacji. Aby to zrobić, przejdź do **Ustawienia > Klawisze/Wyświetlacz > Tekst niestandardowy**.

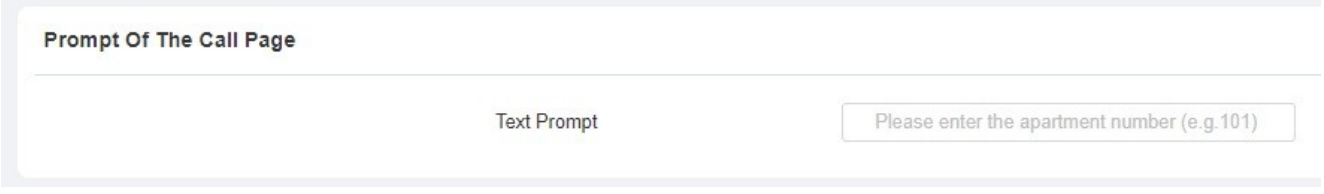


Uwaga

- X912 obsługuje maksymalnie 63-znakową długość niestandardowego tekstu.

Wyświetlanie monitu na ekranie wybierania

W razie potrzeby można dostosować monit wyświetlany na ekranie wybierania. Aby to zrobić, przejdź do **Ustawienia > Klawisz/Wyświetlacz > Monit strony połączenia** .



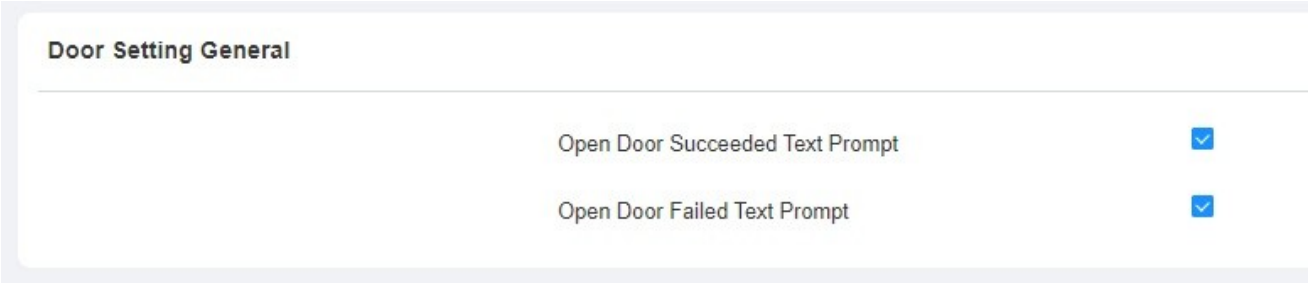
Uwaga

- X912 obsługuje monit tekstowy o maksymalnej długości 128 znaków.

Wyświetlanie komunikatu tekstowego otwartych drzwi

Można włączyć monit tekstowy o otwarciu drzwi zarówno w przypadku powodzenia, jak i niepowodzenia otwarcia drzwi. Można także włączyć wyświetlanie przez bramofon informacji o użytkowniku, gdy korzysta on z danych uwierzytelniających, takich jak karty RF.

Aby to zrobić, przejdź do opcji **Kontrola dostępu > Przekaźnik > Ogólne ustawienia drzwi.**



Konfiguracja głośności i tonów

Konfiguracja głośności i tonów obejmuje głośność mikrofonu, głośność AD, głośność klawiatury, głośność głośnika, głośność alarmu sabotażowego i konfigurację dźwięku otwartych drzwi. Co więcej, możesz przesłać swój ulubiony dźwięk, aby wzbogacić spersonalizowane wrażenia użytkownika.

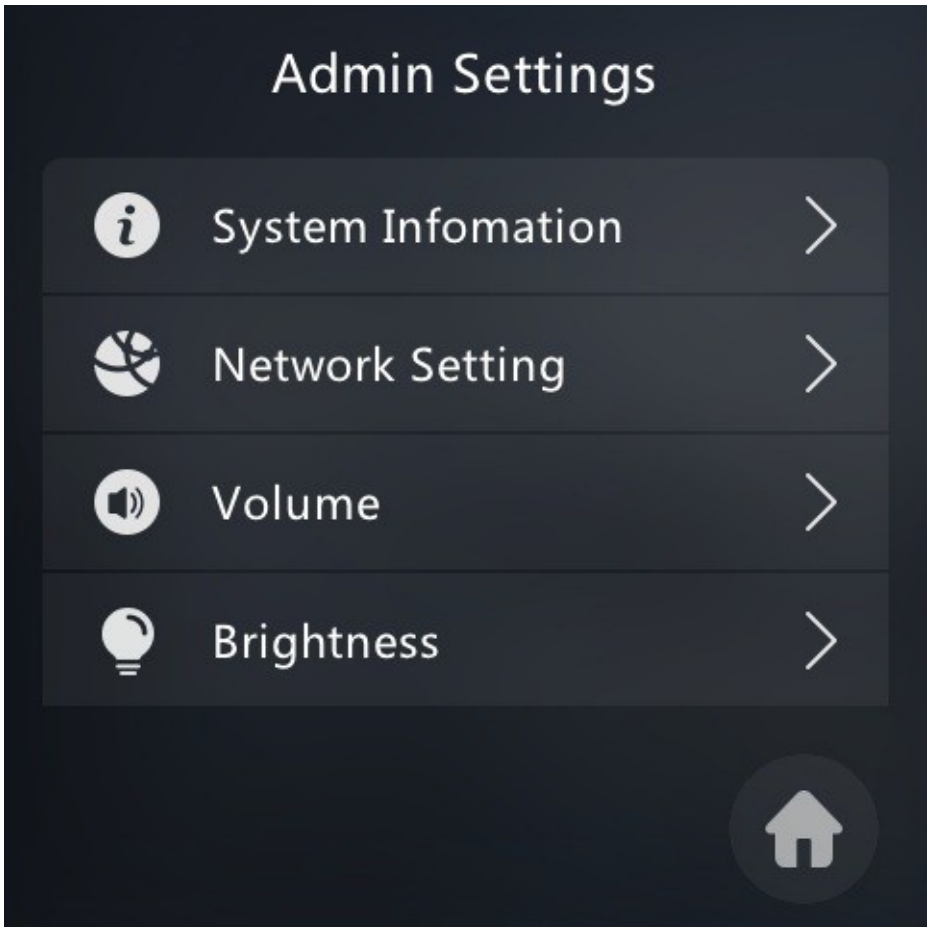
Konfiguracja głośności

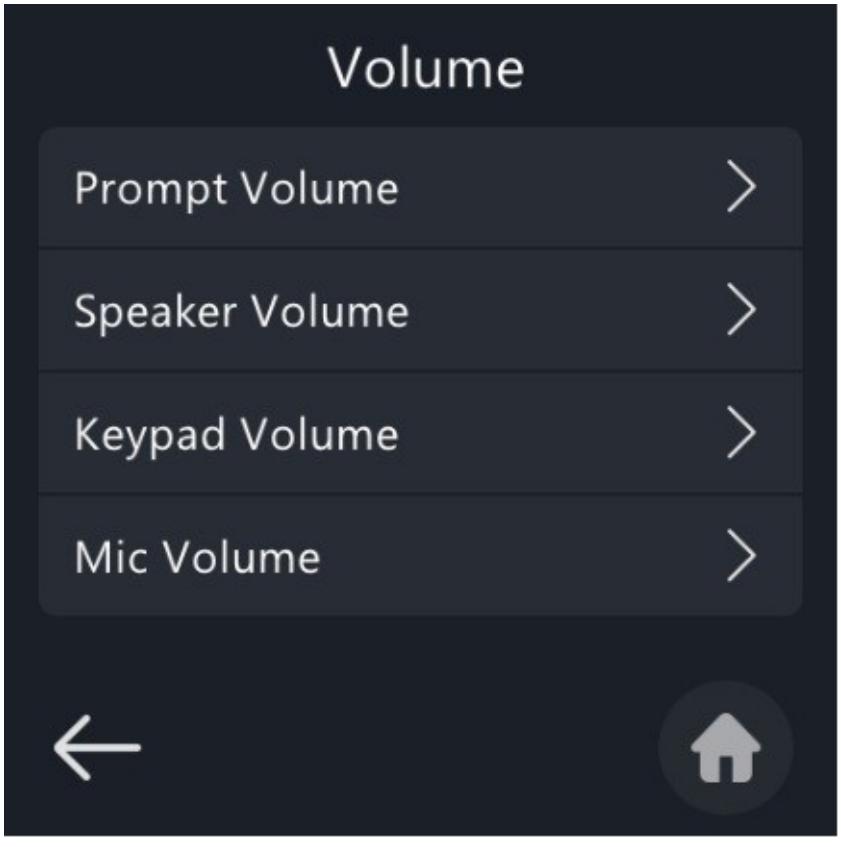
Głośność Mic można skonfigurować zgodnie z potrzebami powiadamiania o otwartych drzwiach. Co więcej, można również ustawić głośność alarmu sabotażowego, gdy nastąpi niepożądane usunięcie terminala kontroli dostępu.

Konfiguracja głośności na urządzeniu

W urządzeniu można regulować głośność mikrofonu, głośność głośnika, głośność klawiatury i głośność AD.

Aby skonfigurować na urządzeniu **Ustawienia administratora >** Interfejs **głośności.**



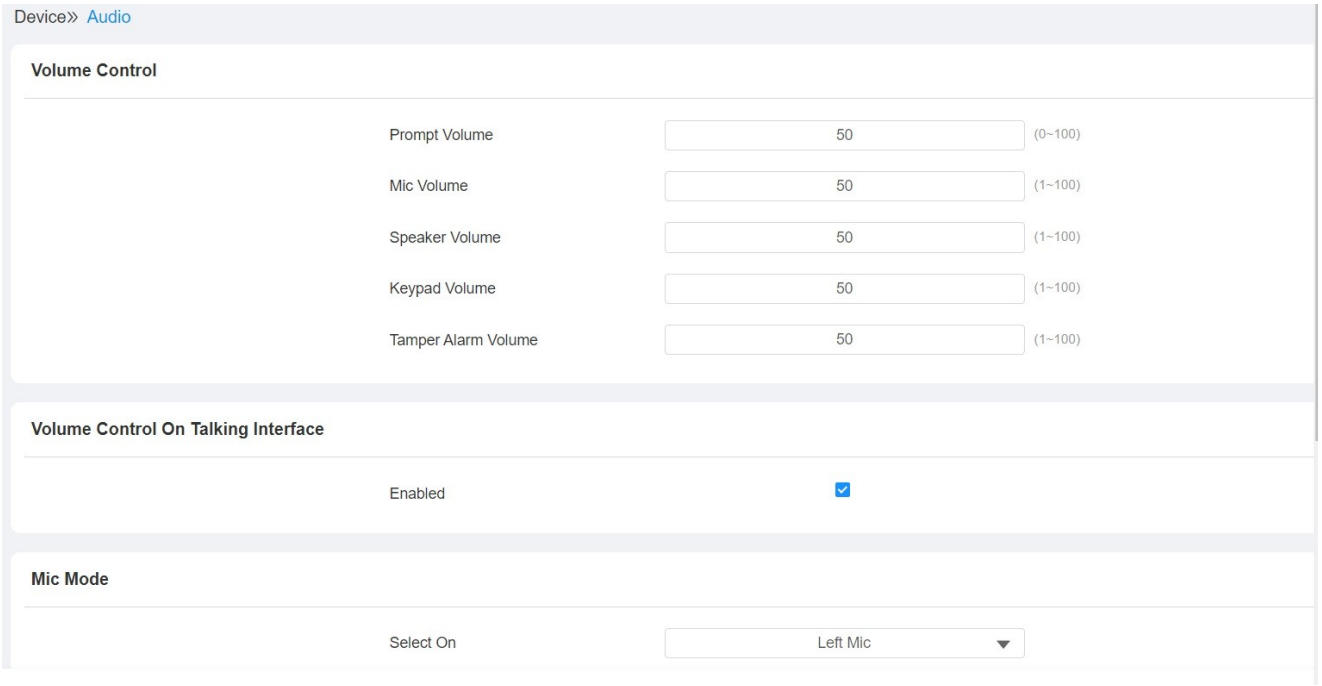


Konfiguracja parametrów :

- **Głośność monitu**: obejmuje **sygnał monitu, dzwonka, otwarcia drzwi** itp. Domyślna głośność monitu wynosi 50.

Konfiguracja głośności w interfejsie internetowym

Aby skonfigurować konfigurację w sieci Web **Urządzenie >** Interfejs **audio.**



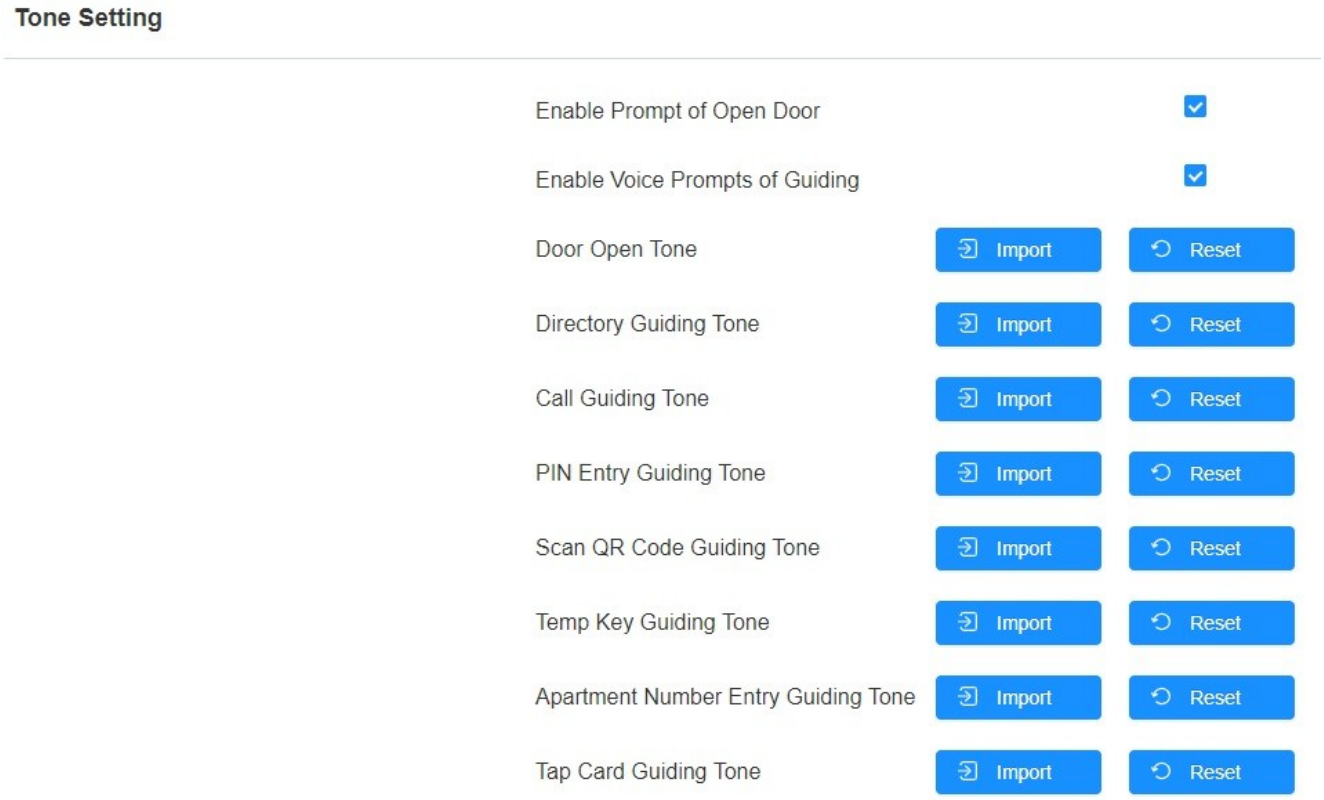
Konfiguracja parametrów:

- **Głośność monitu**: obejmuje sygnał monitu, sygnał zwrotny, czas otwarcia drzwi itp. Domyślna głośność monitu wynosi 50.
- **Enabled** : zaznacz pole wyboru, jeśli zezwalasz na regulację głośności połączenia na ekranie rozmowy podczas połączenia.

Prześlij dźwięk otwartych drzwi

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

Przejdź do interfejsu **Device > Audio > Tone Setting.**



Konfiguracja parametrów :

- **Enable Voice Prompt of Guiding**: po włączeniu tej opcji, po dotknięciu **ikony połączenia** na ekranie odtwarzana będzie promocja głosowa, na przykład "Please enter the number, then press the call button" (Wprowadź numer, a następnie naciśnij przycisk połączenia).
- **Door Open Tone** (**Dźwięk otwarcia drzwi)**: Prześlij dźwięk otwarcia drzwi. Kliknij **Reset**, aby zresetować dźwięk do domyślnego.
- **Directory Guiding Tone** : prześlij komunikat głosowy dotyczący pomyślnego
- otwarcia drzwi. **Call GuidingTone** : prześlij komunikat głosowy dla połączenia, który zostanie odtworzony po dotknięciu ikony połączenia.
- **PIN Entry Guiding Tone**: Prześlij dostosowany dźwięk monitu głosowego na ekranie wprowadzania kodu PIN.
- **Scan QR Code Guiding Tone**: przesłanie komunikatu głosowego dla ekranu kodu
- QR. **Temp Key Guiding Tone** : prześlij dostosowany dźwięk monitu na ekranie tymczasowego wprowadzania kodu PIN.
- **Dźwięk** prowadzący **do wprowadzenia numeru** apartamentu: przesłanie sygnału zachęty do wprowadzenia numeru apartamentu.
- **Tap Card Guiding Tone**: Prześlij dźwięk monitu głosowego dla podwójnego uwierzytelniania przy wejściu do drzwi. Zostanie on odtworzony po zakończeniu pierwszego uwierzytelnienia. Na przykład, podwójne uwierzytelnianie Face+Card.

Uwaga

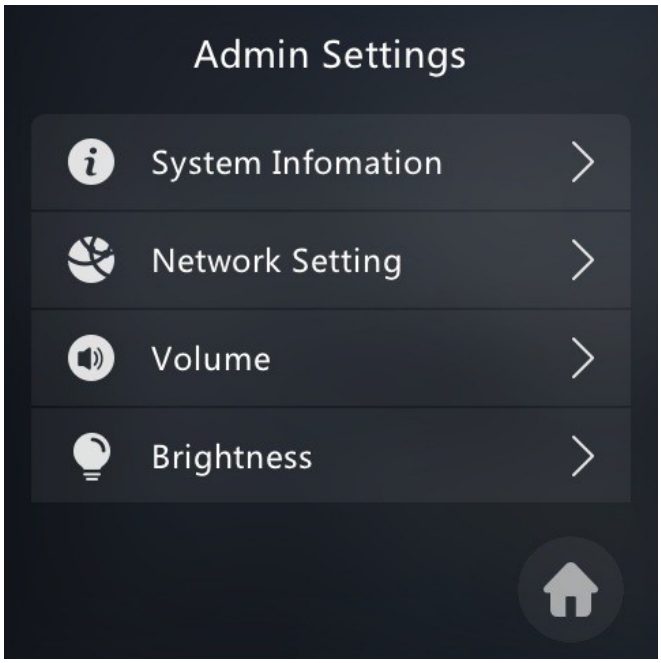
- Wszystkie przesłane pliki dźwiękowe powinny być w formacie .wav, o rozmiarze 200 KB, częstotliwości próbkowania: 16000, bitach: 16

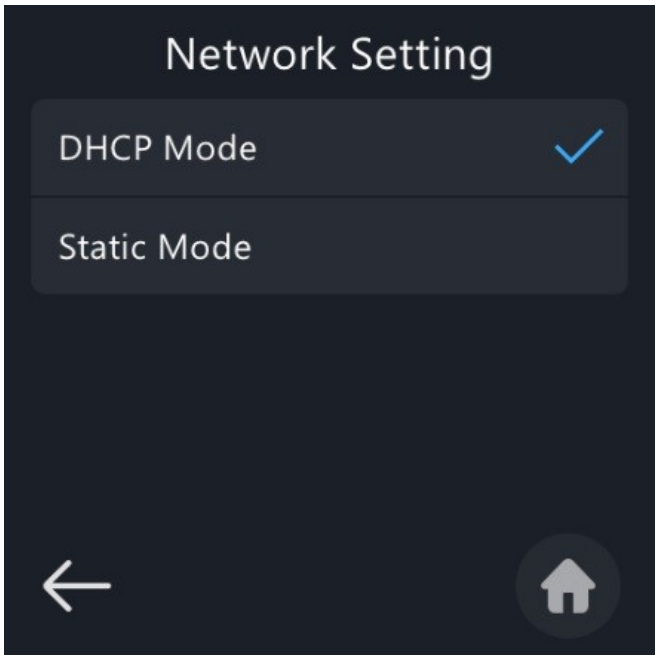
Ustawienia sieciowe

Konfiguracja sieci urządzenia

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

Wybierz opcję **Ustawienia sieci** na ekranie urządzenia.

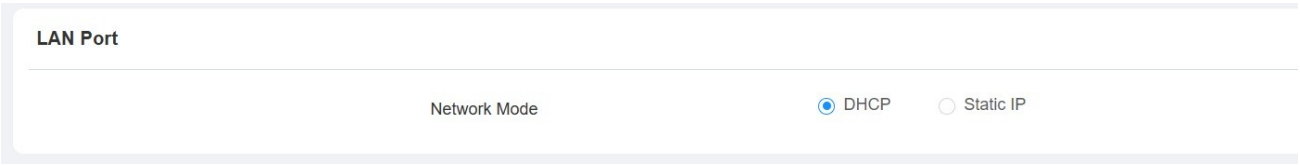




Konfiguracja parametrów :

- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Jeśli tryb DHCP jest włączony, bramofon zostanie automatycznie przypisany przez serwer DHCP z adresem IP, maską podsieci, domyślną bramą i adresem serwera DNS.
- **Statyczny adres IP**: Po wybraniu trybu statycznego adresu IP, adres IP, maska podsieci, brama domyślna i adres serwerów DNS muszą zostać skonfigurowane ręcznie zgodnie z rzeczywistym środowiskiem sieciowym.
- **Adres IP** : ustawienie adresu IP w przypadku wybrania statycznego trybu IP.
- **Maska podsieci**: ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Domyślna brama**: ustaw prawidłową domyślną bramę zgodnie z adresem IP domyślnej bramy.
- **DNS1/2** : skonfiguruj preferowany lub alternatywny serwer DNS (**Domain Name Server**) zgodnie z rzeczywistym środowiskiem sieciowym. Serwer DNS1 jest podstawowym adresem serwera DNS, podczas gdy DNS2 jest adresem serwera pomocniczego, a bramofon połączy się z serwerem DNS2, gdy podstawowy serwer DNS 1 będzie niedostępny.

Aby skonfigurować konfigurację w interfejsie **Sieć > Podstawowe > Port LAN.**

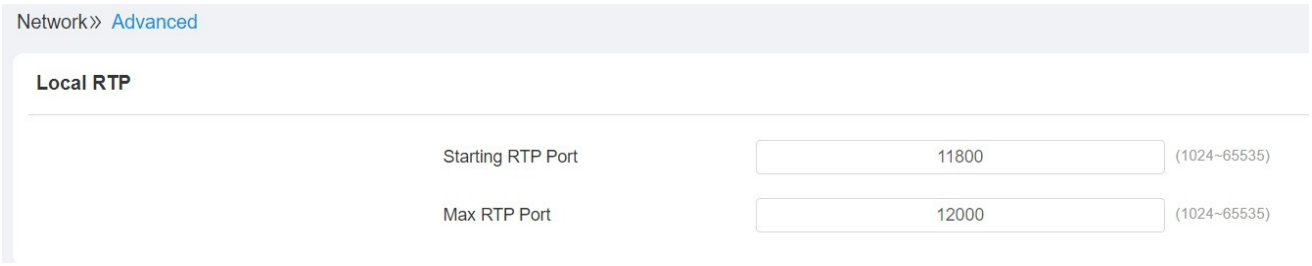


Lokalna konfiguracja RTP urządzenia

Protokół transportowy czasu rzeczywistego (**RTP**) umożliwia urządzeniom strumieniowe przesyłanie danych audio i wideo przez sieć w czasie rzeczywistym.

Aby korzystać z protokołu RTP, urządzenia potrzebują szeregu portów. Port jest jak kanał dla danych w sieci. Konfigurując porty RTP w urządzeniu i routerze, można uniknąć zakłóceń sieciowych i poprawić jakość dźwięku i obrazu.

Aby skonfigurować konfigurację w sieci **Sieć > Zaawansowane > Lokalny** interfejs **RTP.**



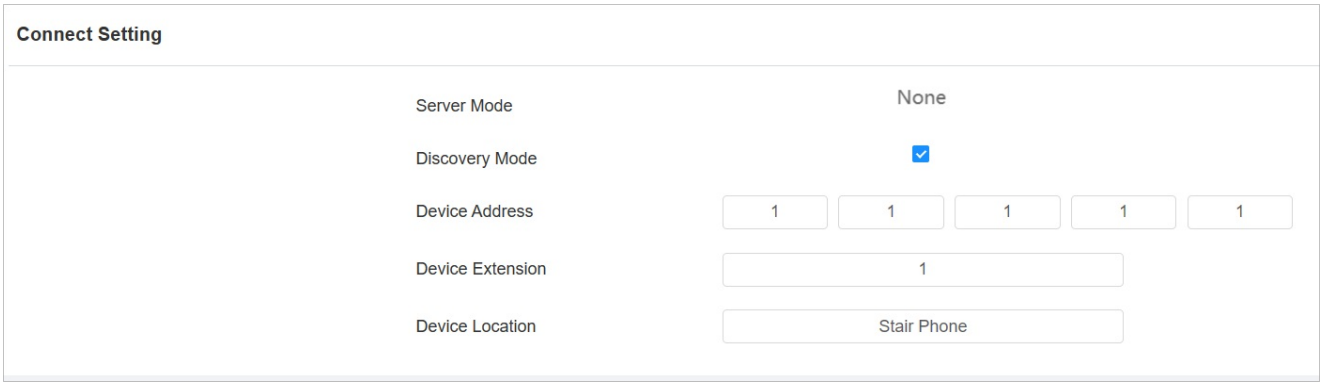
Konfiguracja parametrów :

- **Startowy port RTP**: wprowadź wartość Port, aby ustalić punkt początkowy dla wyłącznego zakresu transmisji danych.
- **Max RTP Port**: wprowadź wartość Port, aby ustalić punkt końcowy dla wyłącznego zakresu transmisji danych.

Wdrażanie urządzeń w sieci

Aby ułatwić kontrolę i zarządzanie urządzeniami, należy skonfigurować urządzenia interkomowe Akuvox z takimi szczegółami, jak lokalizacja, tryb pracy, adres i numery wewnętrzne.

Aby skonfigurować konfigurację w interfejsie **Sieć > Zaawansowane > Ustawienia połączenia.**



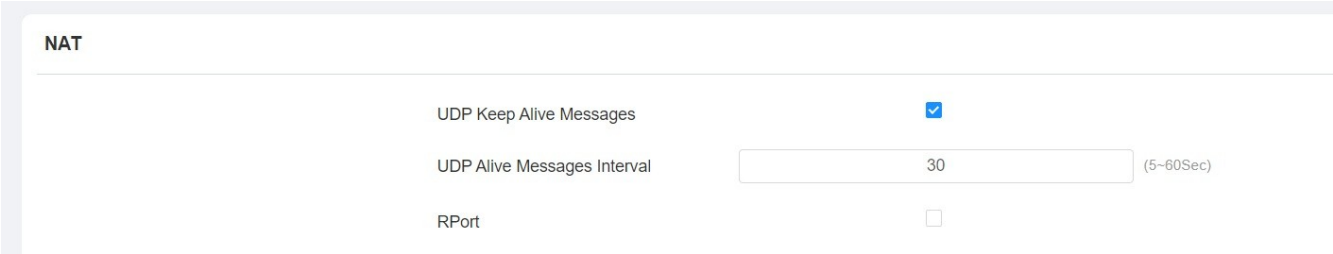
Konfiguracja parametrów :

- **Tryb** serwera: jest automatycznie konfigurowany zgodnie z rzeczywistym połączeniem urządzenia z określonym serwerem w sieci, takim jak **SDMC** lub **Cloud** i **Brak**. **Brak** jest domyślnym ustawieniem fabrycznym.
- **Discovery Mode (Tryb wykrywania**): kliknij Enable **(Włącz)**, aby włączyć tryb wykrywania urządzenia, tak aby mogło być wykrywane przez inne urządzenia w sieci, lub kliknij Disable (Wyłącz), jeśli chcesz ukryć urządzenie, aby nie było wykrywane przez inne urządzenia.
- **Adres urządzenia** : określ adres urządzenia, wprowadzając informacje o lokalizacji urządzenia od lewej do prawej: **Community (Wspólnota), Unit (Jednostka), Stair (Schody), Floor (Piętro), Room (Pokój)** w kolejności.
- **Device Extension**: wprowadź numer wewnętrzny zainstalowanego urządzenia.
- **Lokalizacja urządzenia**: wprowadź lokalizację, w której urządzenie jest zainstalowane i używane.

Ustawienie NAT

Translacja adresów sieciowych (**NAT**) umożliwia urządzeniom w sieci prywatnej korzystanie z jednego publicznego adresu IP w celu uzyskania dostępu do Internetu lub innych sieci publicznych. NAT zapisuje ograniczone publiczne adresy IP i ukrywa wewnętrzne adresy IP i porty przed światem zewnętrznym.

Ścieżka: **Konto > Zaawansowane > NAT**.



Konfiguracja parametrów :

- **UDP Keep Alive Messages**: jeśli włączone, urządzenie wyśle wiadomość do serwera SIP, aby serwer SIP rozpoznał, że urządzenie jest w stanie online.
- **UDP Alive Messages Interval**: ustawienie interwału wysyłania wiadomości w zakresie 5-60 sekund, domyślnie 30 sekund.
- **RPort**: włącz RPort, gdy serwer SIP znajduje się w sieci WAN (**Wide Area Network**).

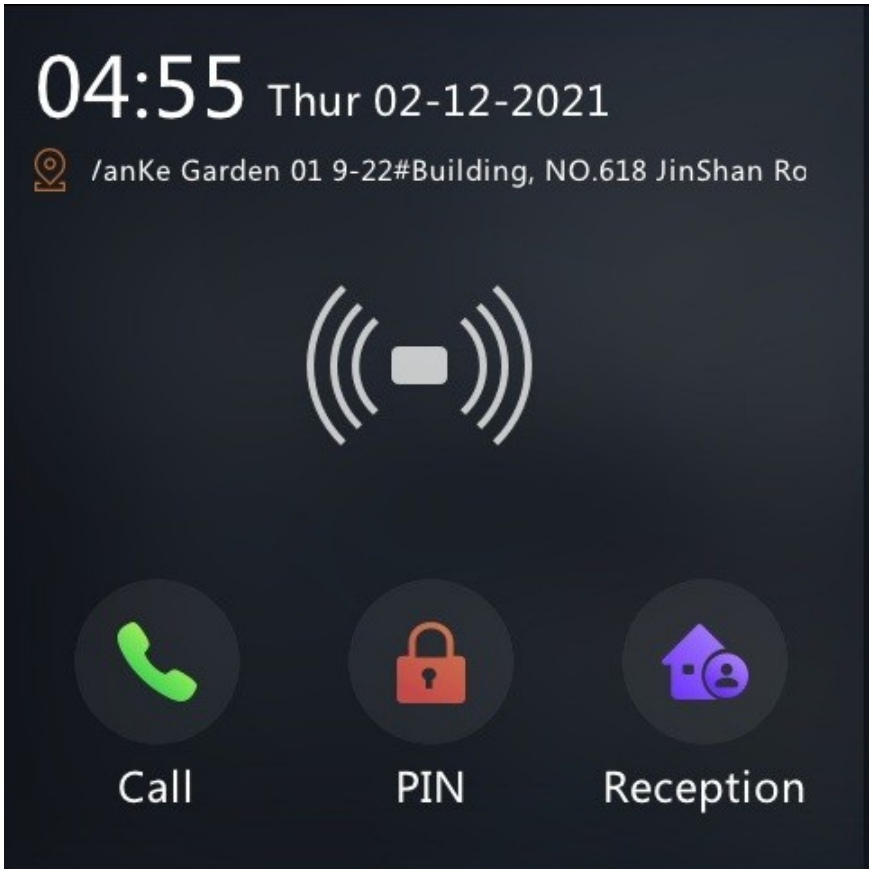
Konfiguracja połączeń interkomowych

Konfiguracja połączeń IP i połączeń IP

Połączenie IP to bezpośrednie połączenie między dwoma urządzeniami interkomowymi przy użyciu ich adresów IP, bez serwera lub centrali PBX. Połączenia IP działają, gdy urządzenia znajdują się w tej samej sieci.

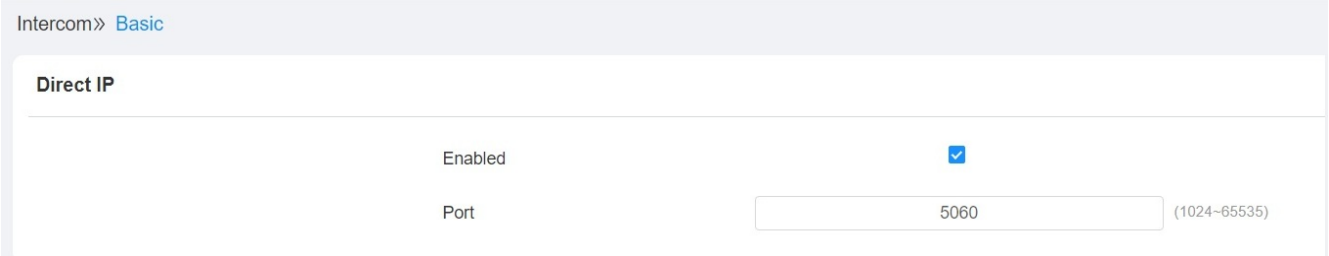
Wykonywanie połączeń IP

Aby nawiązywać połączenia SIP lub IP na urządzeniu, klikając przycisk wybierania lub ekran główny.



Konfiguracja połączeń IP

Aby skonfigurować bezpośrednie połączenie IP na urządzeniu **Interkom > Podstawowe > Bezpośredni** interfejs **IP.**



Konfiguracja parametrów :

- **Port**: bezpośredni port IP to domyślnie 5060 z zakresem portów od 1024-65535. Po wprowadzeniu dowolnej wartości z zakresu innego niż 5060 należy sprawdzić, czy wprowadzona wartość jest zgodna z odpowiednią wartością na urządzeniu, z którym ma zostać nawiązana transmisja danych.

Konfiguracja połączeń SIP i połączeń SIP

Session Initiation Protocol (**SIP**) to protokół transmisji sygnałów używany do inicjowania, utrzymywania i kończenia połączeń.

Połączenie SIP wykorzystuje protokół SIP do wysyłania i odbierania danych między urządzeniami SIP i może wykorzystywać Internet lub sieć lokalną w celu zapewnienia wysokiej jakości i bezpiecznej komunikacji. Inicjowanie połączenia SIP wymaga konta SIP, adresu SIP dla każdego urządzenia i skonfigurowania ustawień SIP na urządzeniach.

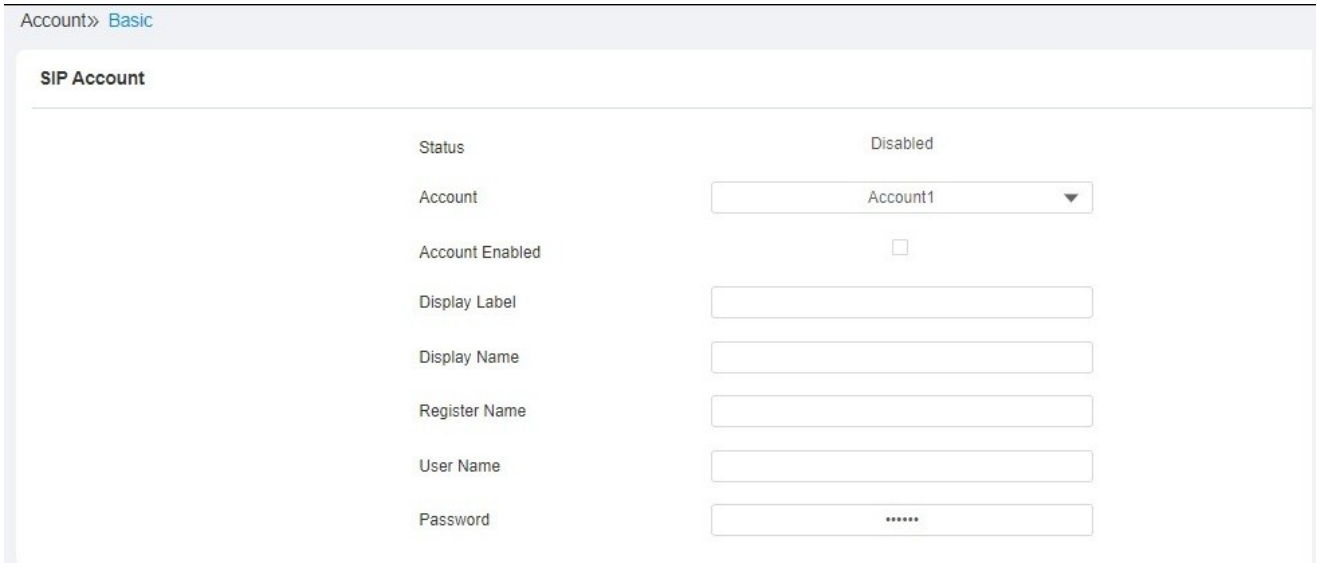
Rejestracja konta SIP

Każde urządzenie potrzebuje konta SIP do wykonywania i odbierania połączeń SIP.

Urządzenia interkomowe Akuvox obsługują konfigurację dwóch kont SIP, które mogą być zarejestrowane na dwóch niezależnych serwerach.

Konfiguracja konta SIP

Aby skonfigurować konto SIP, przejdź do interfejsu **Konto > Podstawowe > Konto SIP. Nazwa rejestru, nazwa użytkownika** i **hasło są uzyskiwane** od administratora konta SIP.



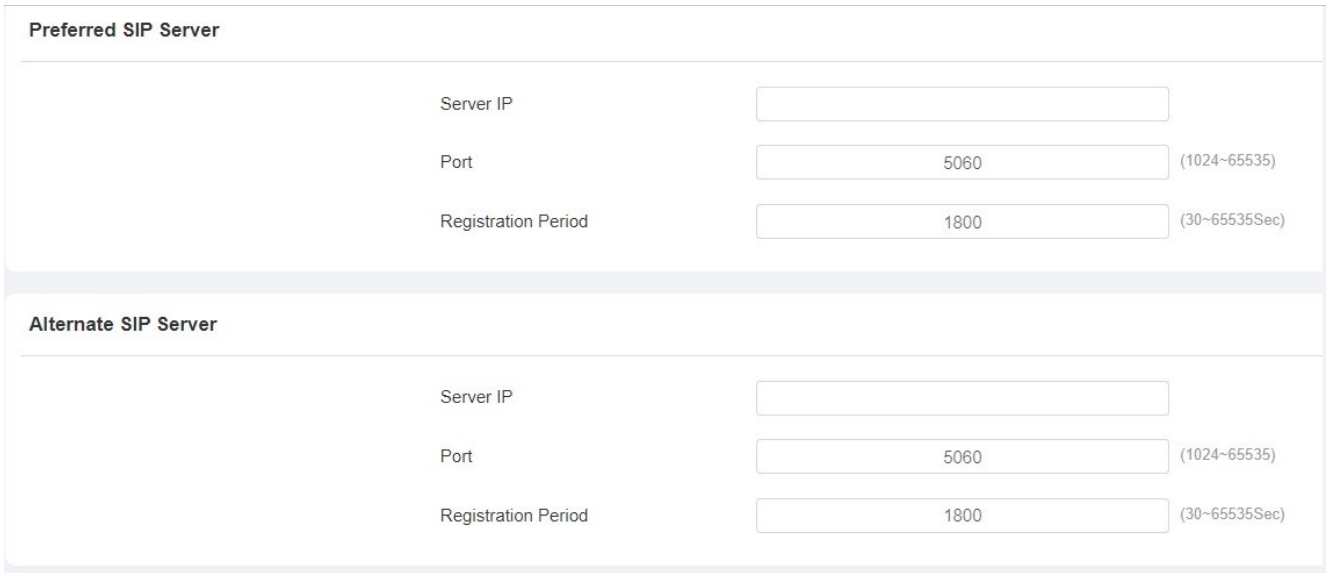
Konfiguracja parametrów :

- **Konto**: wybierz konto 1 lub konto 2, które ma być skonfigurowane do wykonywania lub odbierania połączeń SIP. • **Display Label**: skonfiguruj etykietę urządzenia, która będzie wyświetlana na ekranie urządzenia.
- **Display Name (Wyświetlana nazwa)**: skonfiguruj nazwę urządzenia, która będzie wyświetlana na stronie wywoływanej.

Konfiguracja serwera SIP

Serwery SIP umożliwiają urządzeniom nawiązywanie i zarządzanie sesjami połączeń z innymi urządzeniami interkomowymi przy użyciu protokołu SIP. Mogą to być serwery innych firm lub wbudowane centrale PBX w monitorach wewnętrznych Akuvox.

Aby skonfigurować go w interfejsie **Konto** internetowe **> Podstawowe > Preferowany/Alternatywny serwer SIP.**



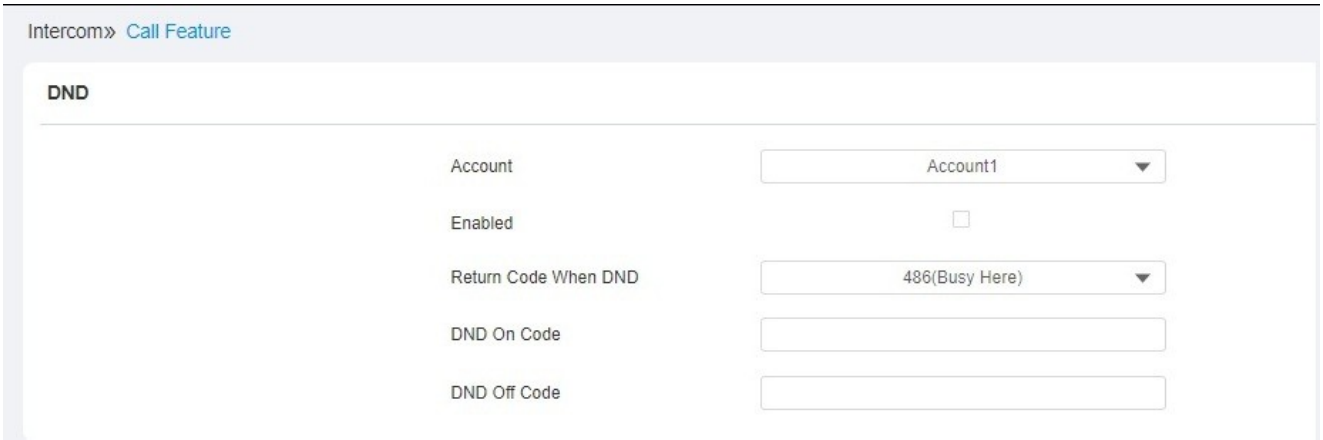
Konfiguracja parametrów :

- **Preferred SIP Server**: wprowadź numer adresu IP serwera podstawowego lub jego adres URL. • **Alternate SIP Server**: wprowadź adres IP zapasowego serwera SIP lub jego adres URL.
- **Port**: ustawienie portu serwera SIP dla transmisji danych.
- **Registration Period** : ustaw okres rejestracji konta SIP. Ponowna rejestracja SIP rozpocznie się automatycznie, jeśli rejestracja konta nie powiedzie się w okresie rejestracji. Domyślny okres rejestracji wynosi 1800 i mieści się w zakresie 30-65535s.

Konfiguracja DND

Funkcja Nie przeszkadzać (**DND**) zapobiega niechcianym połączeniom przychodzącym SIP, zapewniając nieprzerwaną koncentrację. Umożliwia ona również ustawienie kodu wysyłanego do serwera SIP w przypadku odrzucenia połączenia.

Aby skonfigurować konfigurację w interfejsie web **Intercom > Call Feature > DND.**



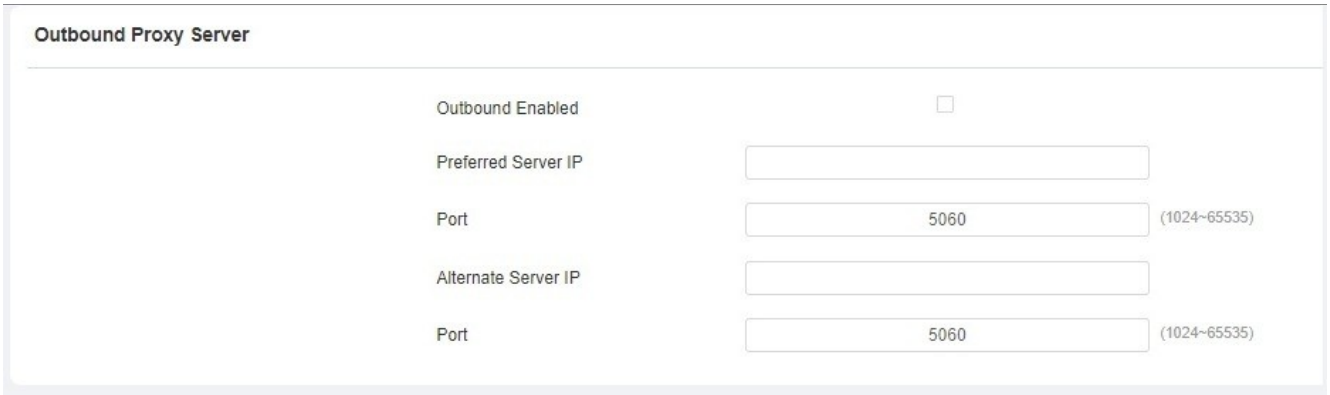
Konfiguracja parametrów :

- **Konto**: wybierz konto, dla którego chcesz zastosować funkcję DND.
- **Return Code When DND** : wybierz, jaki kod ma być wysyłany do urządzenia dzwoniącego przez serwer SIP. 404 dla "nie znaleziono"; 480 dla "tymczasowo niedostępny"; 486 dla "zajęty"; 603 dla "odrzuć".
- **Kod włączenia DND**: wprowadź kod włączenia DND, aby włączyć funkcję DND na serwerze SIP. Kod włączenia DND to 78.
- **Kod wyłączenia DND**: wprowadź kod wyłączenia DND, aby wyłączyć funkcję DND na serwerze SIP. Kod wyłączenia DND to 79.

Konfiguracja serwera proxy połączeń wychodzących

Wychodzący serwer proxy służy do odbierania wszystkich inicjujących komunikatów żądań i kierowania ich do wyznaczonego serwera SIP w celu ustanowienia sesji połączenia za pośrednictwem transmisji danych opartej na portach.

Aby skonfigurować konfigurację w interfejsie **Konto** internetowe **> Podstawowe > Serwer proxy połączeń wychodzących.**



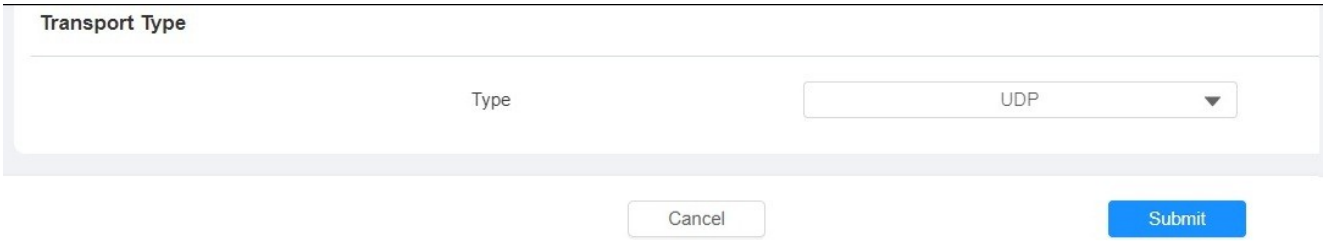
Konfiguracja parametrów :

- **Preferred Server IP** : wprowadź adres SIP głównego serwera proxy połączeń wychodzących.
- **Alternatywny adres IP serwera**: skonfiguruj adres IP serwera zapasowego dla zapasowego wychodzącego serwera proxy.

Konfiguracja typu transmisji danych

Komunikaty SIP mogą być przesyłane w trzech protokołach transmisji danych: **UDP** (**User Datagram Protocol**), **TCP** (**Transmission Control Protocol**), **TLS** (**Transport Layer Security**),
i **DNS-SRV.** W międzyczasie można również zidentyfikować serwer, z którego pochodzą dane.

Aby skonfigurować konfigurację w interfejsie **Konto** internetowe **> Podstawowe > Typ transportu.**



Konfiguracja parametrów :

- **UDP** : wybierz UDP dla zawodnego, ale bardzo wydajnego protokołu warstwy

transportowej. UDP jest domyślnym protokołem transportowym.

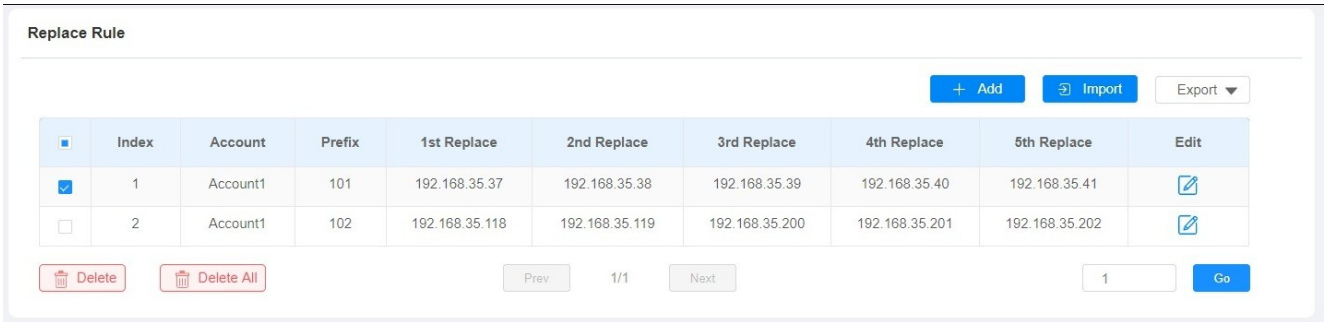
- **TCP**: wybierz TCP dla niezawodnego, ale mniej wydajnego protokołu
- warstwy transportowej. **TLS:** wybierz TLS dla bezpiecznego i niezawodnego protokołu warstwy transportowej.

Konfiguracja opcji wybierania numeru

Szybkie wybieranie numeryczne

Funkcja zastępowania numerów wybierania upraszcza długie i złożone numery wybierania urządzenia, zapewniając krótsze i bardziej przyjazne dla użytkownika alternatywy do wykonywania połączeń. Umożliwia ona zastąpienie wielu numerów wybierania, takich jak adresy IP lub numery SIP, jednym, uproszczonym numerem.

Aby skonfigurować konfigurację w interfejsie web **Intercom > Dial Plan > Replace Rule.**



Konfiguracja parametrów :

- **Konto**: wybierz konto, dla którego ma zostać zastosowana zamiana numeru wybierania. Domyślnie jest to konto **Auto** (wybieranie z konta, na którym zarejestrowano wybierany numer). Możesz wybrać konto 1 lub konto 2, z którego numer może być wybierany. Jeśli numer wybierania został zarejestrowany zarówno na koncie 1, jak i na koncie 2, numer będzie domyślnie wybierany z konta 1.
- **Prefiks**: wprowadź krótki numer, który ma zastąpić wybierany numer.
- **Replace 1/2/3/4/5** : wprowadź numery wybierania, które chcesz zastąpić. Obsługuje maksymalnie 5 numerów do zastąpienia w konfiguracji urządzenia. Na przykład, jeśli zastąpisz pięć oryginalnych numerów wybierania wspólnym krótkim numerem, takim jak **101**, pięć urządzeń interkomowych z tym numerem wybierania zostanie wywołanych w tym samym czasie po wybraniu **101** .

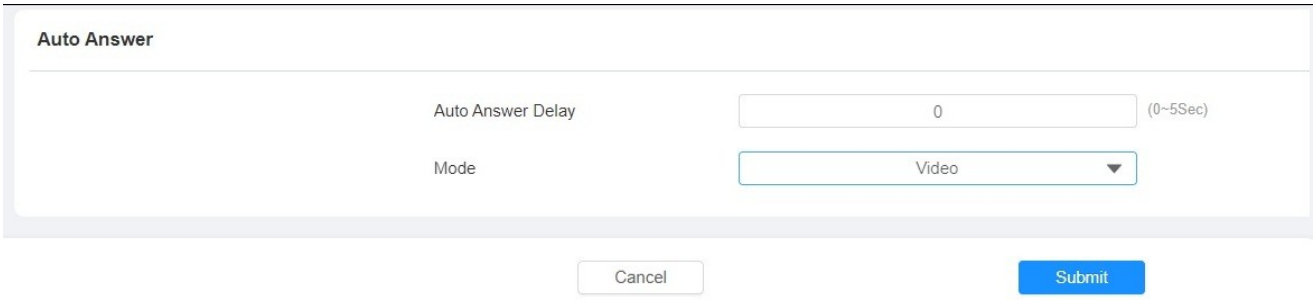
Uwaga

- Pole wyboru dla każdego wiersza **Prefiksu** powinno być zaznaczone przed wyświetleniem opcji Edytuj.

Konfiguracja automatycznego odbierania połączeń

Funkcja automatycznego odbierania pozwala bramofonom na automatyczne odbieranie połączeń przychodzących bez konieczności ręcznej interwencji. Można również dostosować tę funkcję, ustawiając czas trwania automatycznego odbierania i wybierając tryb komunikacji między audio i wideo.

Aby skonfigurować konfigurację w interfejsie web **Intercom > Call Feature > Auto Answer.**



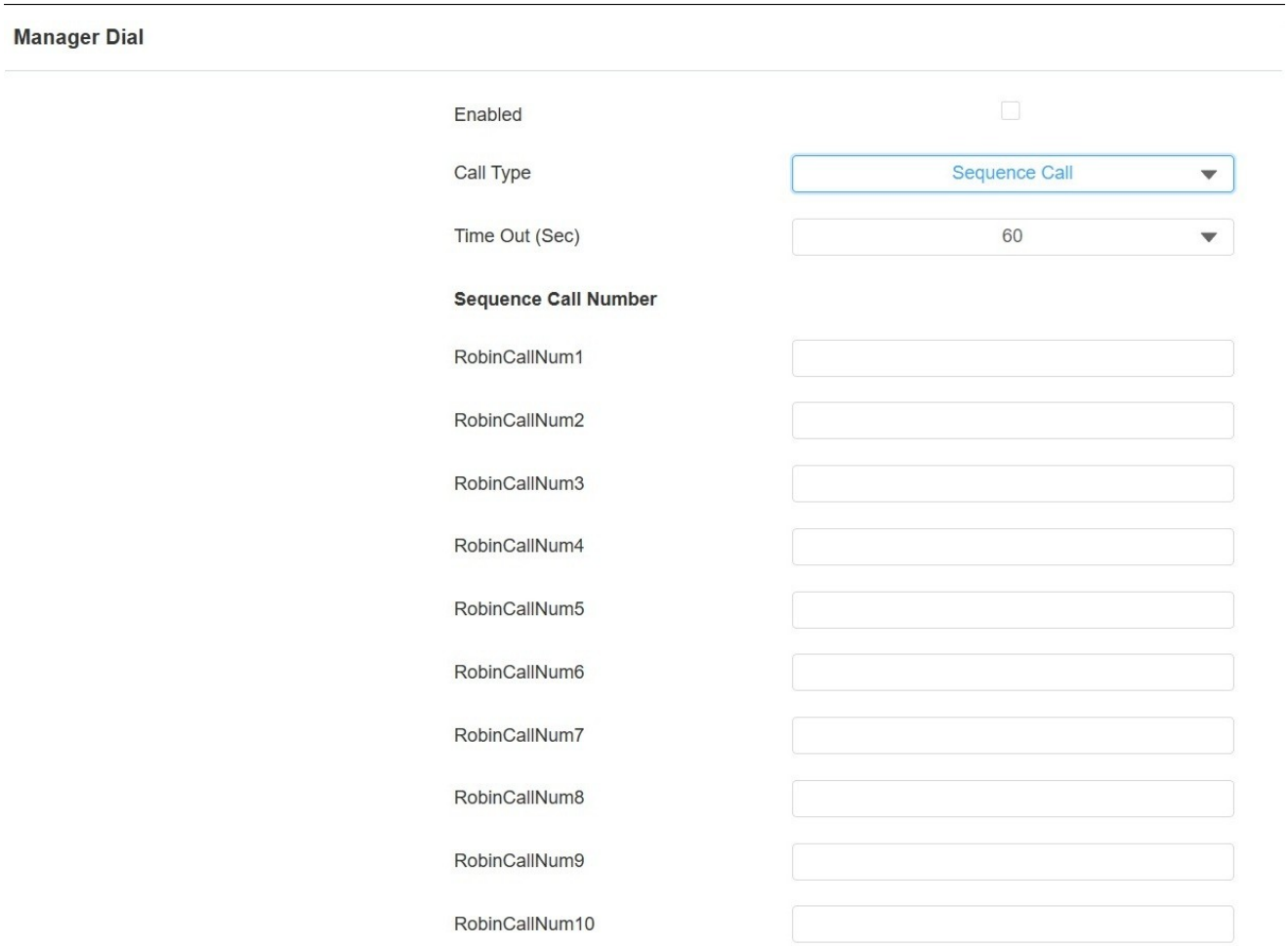
Konfiguracja parametrów :

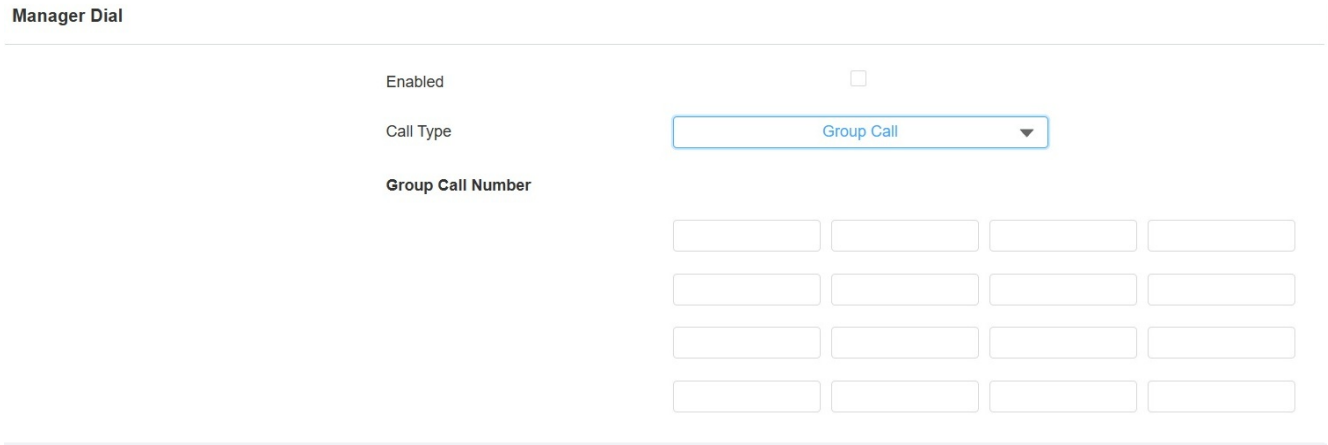
- **Auto Answer Delay**: ustaw czas opóźnienia (od 0 do 5 sekund) przed automatycznym odebraniem połączenia. Na przykład, jeśli ustawisz czas opóźnienia na 1 sekundę, połączenie zostanie automatycznie odebrane w ciągu 1 sekundy.
- **Tryb** : ustawienie preferowanego trybu wideo lub audio dla automatycznego odbierania połączeń.

Wybieranie połączenia przez menedżera

Funkcja Manager Dial Call obejmuje dwa rodzaje połączeń: Połączenie sekwencyjne i połączenie grupowe. Umożliwia szybkie inicjowanie wstępnie skonfigurowanych numerów poprzez naciśnięcie przycisku Management na bramofonie.

Można utworzyć maksymalnie 10 numerów. Aby przeprowadzić konfigurację w interfejsie web **Intercom > Basic > Manager Dial.**





Konfiguracja parametrów :

- **Timeout (Sec) (Limit czasu (sek.))**: kliknij, aby wybrać interwał czasowy między kolejnymi numerami połączeń w docelowej grupie połączeń sekwencyjnych. Na przykład, jeśli ustawisz interwał czasowy na 10 sekund, wówczas połączenie (jeśli nie zostanie odebrane w ciągu 10 sekund) zostanie automatycznie zakończone i przeniesione sekwencyjnie do następnego numeru połączenia sekwencyjnego w docelowej grupie połączeń sekwencyjnych.
- **Typ połączenia**: wybierz połączenie grupowe lub sekwencyjne dla połączenia wybieranego przez menedżera.

- **Połączenie** sekwencyjne: połączenie sekwencyjne służy do inicjowania wielu numerów po naciśnięciu przycisku

  przycisk wybierania menedżera. Jeśli poprzedni rozmówca nie odbierze połączenia w ciągu limitu czasu połączenia sekwencyjnego, połączenie zostanie przeniesione do następnego. Jeśli połączenie zostanie odebrane przez jednego z rozmówców, połączenie nie zostanie już przeniesione. W każdej linii można wprowadzić maksymalnie pięć numerów połączeń sekwencyjnych.
- **Połączenie grupowe**: połączenie grupowe służy do inicjowania połączeń z wieloma numerami jednocześnie po naciśnięciu przycisku wybierania menedżera. Lokalne numery połączeń grupowych to numery dodane lokalnie z poziomu interfejsu internetowego. Połączenia grupowe w chmurze to numery utworzone w chmurze SmartPlus.

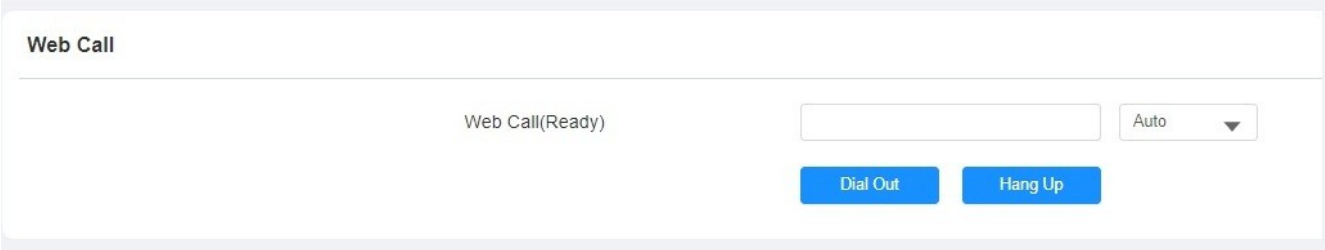
Uwaga

- Funkcja wywoływania sekwencyjnego powinna być obsługiwana przez SmartPlus, prosimy o kontakt
  Więcej informacji można uzyskać w dziale pomocy technicznej Akuvox.

Połączenie internetowe

Funkcja połączeń internetowych umożliwia wykonywanie połączeń za pośrednictwem interfejsu internetowego urządzenia, powszechnie używanego do zdalnego testowania połączeń.

Aby nawiązać połączenie internetowe, przejdź do **System > Maintenance > Web Call.**



Konfiguracja parametrów :

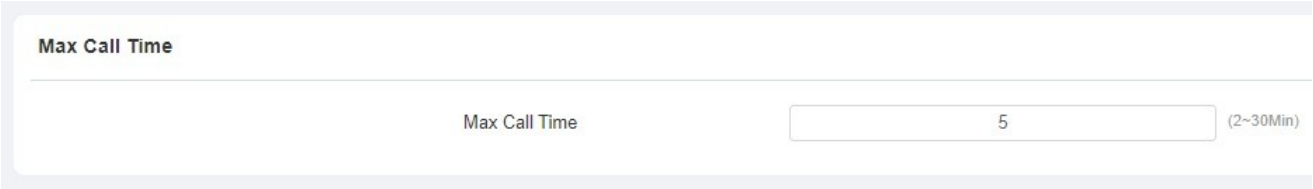
- **Web Call (Ready)**: wprowadź numer IP/SIP, aby się połączyć.

Ustawienia połączeń

Ustawienie maksymalnego czasu trwania połączenia

Bramofon umożliwia ustawienie czasu trwania połączenia podczas odbierania połączenia z urządzenia wywołującego, ponieważ strona dzwoniąca może zapomnieć o odłożeniu słuchawki urządzenia interkomowego. Gdy czas połączenia zostanie osiągnięty, bramofon automatycznie zakończy połączenie.

Aby skonfigurować konfigurację w interfejsie web **Intercom > Call Feature > Max Call Time.**



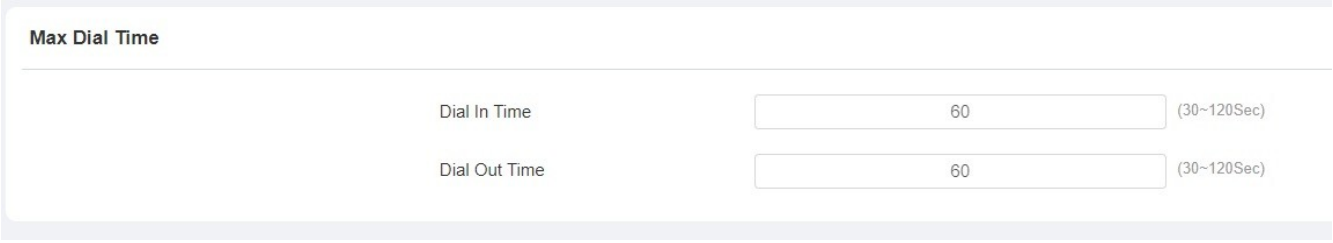
Konfiguracja parametrów :

- **Maksymalny czas połączenia**: wprowadź czas trwania połączenia zgodnie z potrzebami (w zakresie **2-30 min.**). Domyślny czas trwania połączenia wynosi 5 minut.

Ustawienie maksymalnego czasu wybierania numeru

Maksymalny czas wybierania to limit czasu dla połączeń przychodzących i/lub wychodzących na bramofonie. Jeśli zostanie skonfigurowany, bramofon automatycznie zakończy połączenie, jeśli nikt nie odbierze połączenia w ustawionym czasie, niezależnie od tego, czy jest to połączenie przychodzące, czy wychodzące.

Aby skonfigurować konfigurację w interfejsie web **Intercom > Call Feature > Max Dial Time.**



Konfiguracja parametrów :

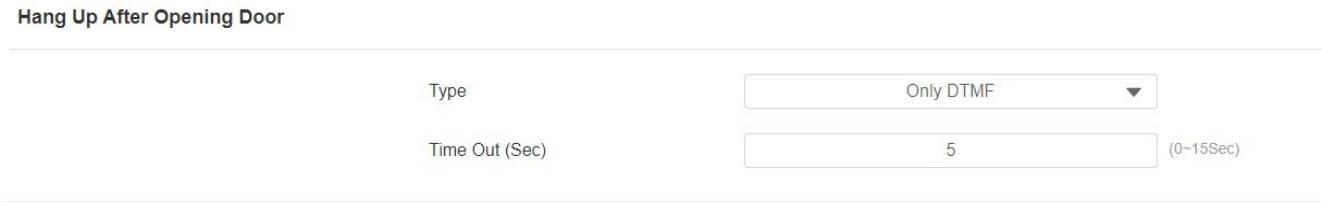
- **Dial In Time** (**Czas wybierania)**: wprowadź czas wybierania dla bramofonu (w zakresie **30-120** sekund), na przykład jeśli ustawisz czas wybierania na 60 sekund w bramofonie, wówczas bramofon automatycznie rozłączy połączenie przychodzące, jeśli połączenie nie zostanie odebrane przez bramofon w ciągu 60 sekund. Domyślnym czasem wybierania jest 60 sekund.

- **Dial** Out **Time** (**Czas wybierania)**: wprowadź czas wybierania dla bramofonu (w zakresie od **30 do 120** sekund), na przykład, jeśli ustawisz czas wybierania na 60 sekund w bramofonie, wówczas bramofon automatycznie rozłączy się z wybranym połączeniem, jeśli nie zostanie ono odebrane przez rozmówcę.

Odłóż słuchawkę po otwarciu drzwi

Funkcja ta automatycznie kończy połączenie po zwolnieniu drzwi, umożliwiając płynne odbieranie kolejnych połączeń.

Aby wykonać tę konfigurację w interfejsie web **Intercom > Call Feature > Hang Up After Opening Door.**



Konfiguracja parametrów :

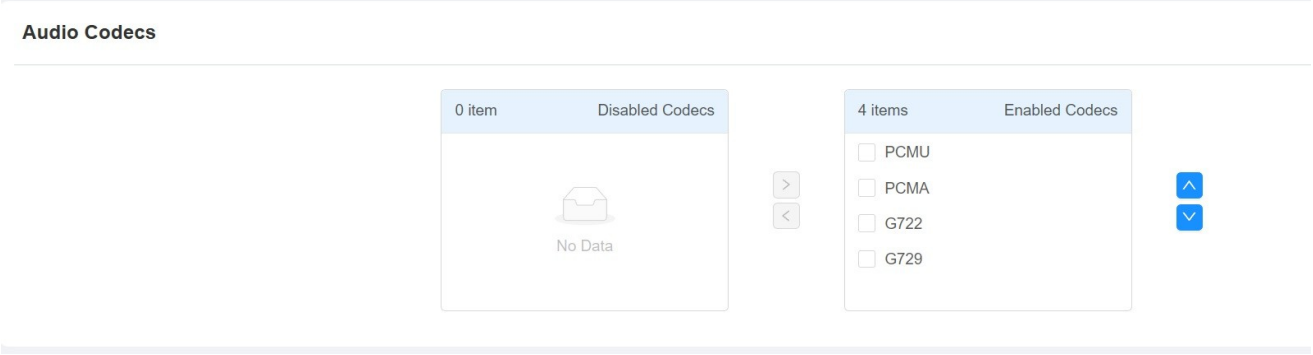
- **Typ**: wybierz typ otwartych drzwi. Drzwi można odblokować za pomocą **Tylko DTMF, Tylko HTTP, DTMF i HTTP** oraz **Wejście, DTMF i HTTP**.
- **Limit czasu**: wartość limitu czasu można ustawić w zakresie od 0 sekund do 15 sekund. Domyślnie jest to 5 sekund. Ustaw wartość 0, jeśli chcesz wyłączyć tę funkcję. Połączenie zostanie automatycznie rozłączone w tym czasie po otwarciu drzwi.

Konfiguracja kodeka audio i wideo dla połączeń SIP

Konfiguracja kodeka audio

Bramofon obsługuje cztery typy kodeków (PCMU, PCMA, G729 i G722) do kodowania i dekodowania danych audio podczas sesji połączenia. Każdy typ kodeka różni się jakością dźwięku. Można elastycznie wybrać konkretny kodek z różnymi szerokościami pasma i częstotliwościami próbkowania w zależności od rzeczywistego środowiska sieciowego.

Aby skonfigurować go w interfejsie **Konto** internetowe **> Zaawansowane > Konto SIP.**



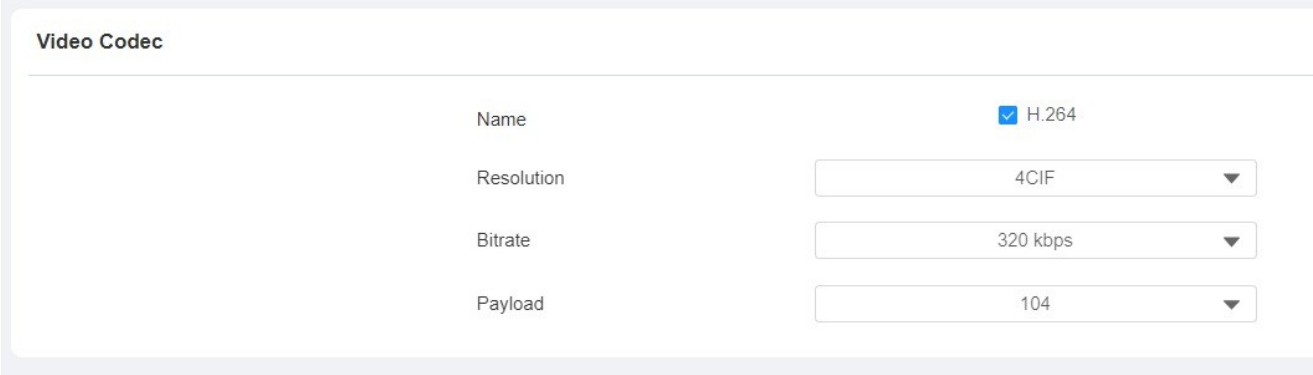
Poniżej znajdują się informacje na temat zużycia pasma i częstotliwości próbkowania dla **czterech typów kodeków:**

Typ kodeka	Zużycie przepustowości	Częstotliwość próbkowania
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Konfiguracja kodeka wideo

Bramofon obsługuje kodek H264, który zapewnia lepszą jakość wideo przy znacznie niższej szybkości transmisji z inną jakością wideo i ładunkiem.

Aby skonfigurować konfigurację w interfejsie **Konto** internetowe **> Zaawansowane > Kodek wideo.**



Konfiguracja parametrów :

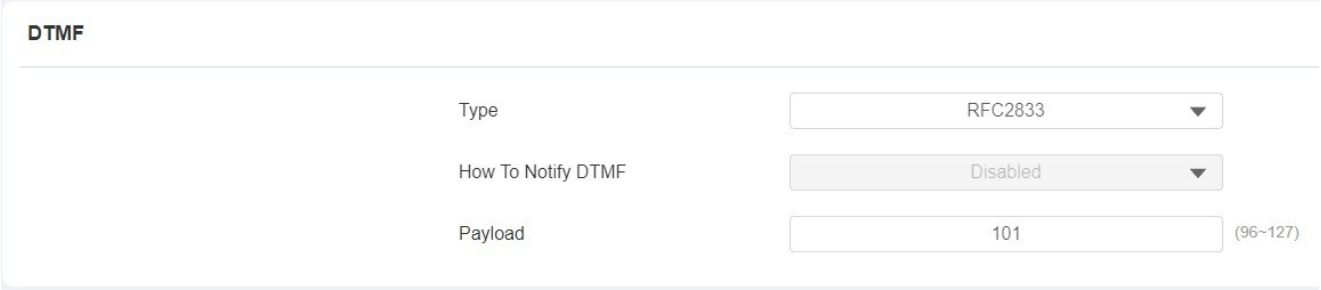
- **Nazwa** : zaznacz, aby wybrać format kodeka wideo H264 dla strumienia wideo z bramofonu. Domyślnym kodekiem wideo jest H264.
- **Rozdzielczość**: wybór rozdzielczości kodu dla jakości wideo spośród pięciu opcji: **QCIF , CIF, VGA**, **4CIF** i **720P w** zależności od rzeczywistego środowiska sieciowego. Domyślną rozdzielczością kodu jest **VGA** .

- **Bitrate** : wybierz szybkość transmisji strumienia wideo (w zakresie **128-2048**). Im większa szybkość transmisji bitów, tym większa ilość danych przesyłanych w każdej sekundzie, dzięki czemu obraz wideo będzie wyraźniejszy. Domyślna szybkość transmisji
- kodu wynosi 2048.
  Payload (Ładunek): wybierz typ ładunku (w zakresie **90-119**), aby skonfigurować plik konfiguracyjny audio/wideo. Domyślny ładunek to 104.

Konfiguracja transmisji danych DTMF

Aby uzyskać dostęp do drzwi za pomocą kodu DTMF lub innych aplikacji, wymagana jest prawidłowa konfiguracja DTMF w celu ustanowienia transmisji danych opartej na DTMF między bramofonem a innymi urządzeniami interkomowymi w celu integracji z innymi firmami.

Aby skonfigurować konfigurację na stronie **Konto > Zaawansowane >** Interfejs **DTMF.**



Konfiguracja parametrów :

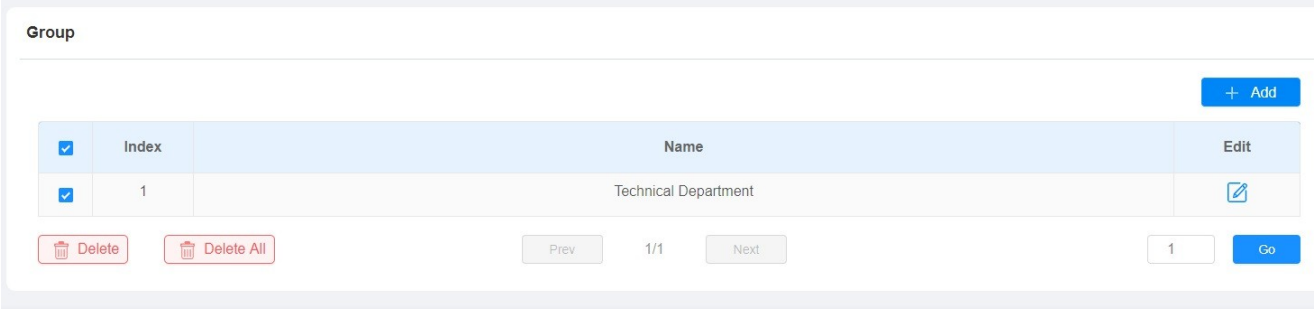
- **Tryb** : wybór trybu DTMF spośród pięciu opcji: **Inband, RFC 2833, Info+Inband**, **Info+RFC 2833** oraz **Info w** oparciu o określony typ transmisji DTMF urządzenia zewnętrznego, które ma być dopasowane do strony odbierającej dane sygnału. Domyślnym ustawieniem jest **RFC 2833** .
- **Jak powiadomić DTMF**: wybierz jeden z czterech typów: **Disable (Wyłącz), DTMF**, **DTMF-Relay (Przekaźnik DTMF)** i **Telephone-Event (Zdarzenie telefoniczne)** zgodnie z konkretnym typem przyjętym przez urządzenie innej firmy. Konfiguracja jest
- wymagana tylko wtedy, gdy dopasowywane urządzenie zewnętrzne przyjmuje tryb **Info. Payload** (Ładunek): ustaw ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą i odbiorcą podczas transmisji danych. Domyślny ładunek 101. Zakres ładunku wynosi od 96 do 127.

Konfiguracja książki telefonicznej

Zarządzanie grupami kontaktów

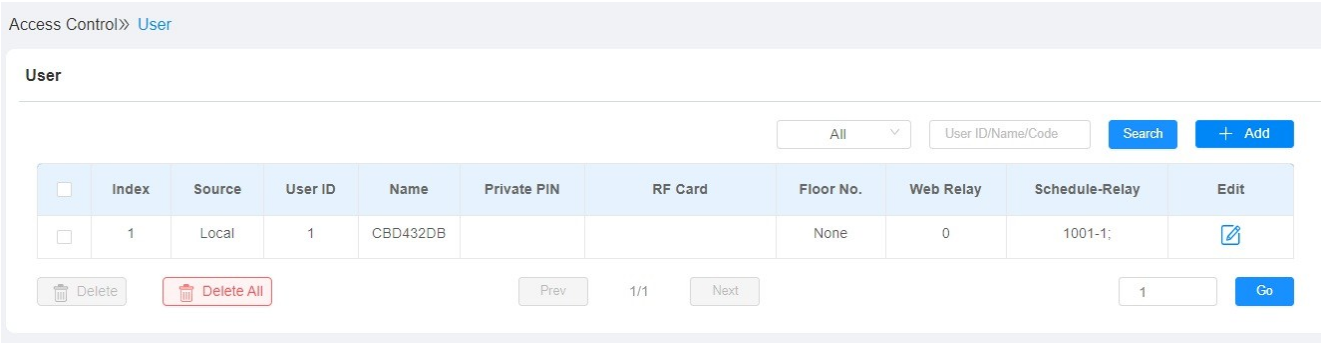
Można utworzyć i edytować grupę kontaktów dla kontaktów. Grupa kontaktów będzie używana podczas dodawania użytkownika.

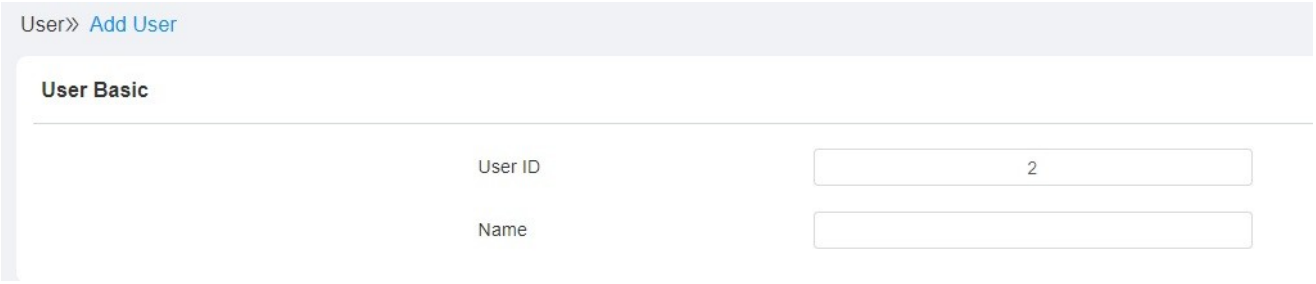
Aby to zrobić, przejdź do **Katalog > Użytkownik > Grupa** .

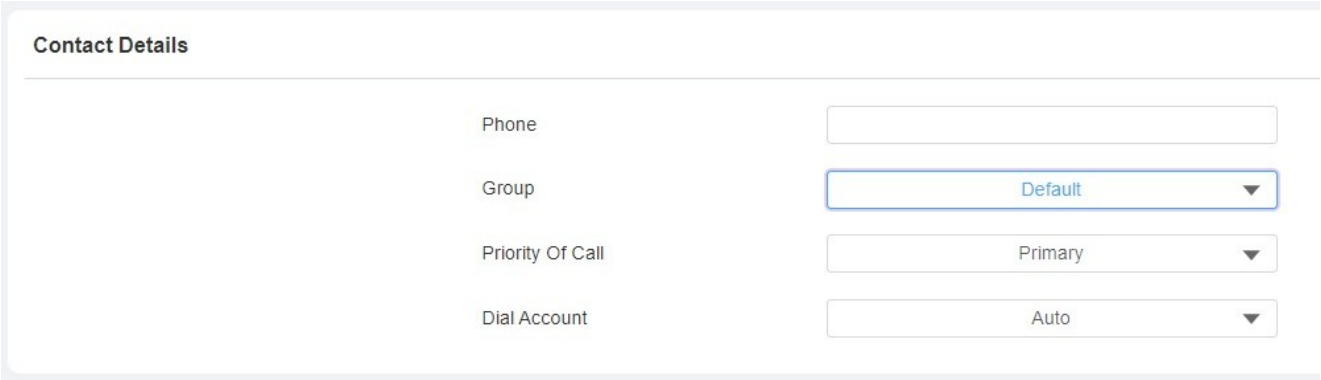


Konfiguracja kontaktu

Po utworzeniu grupy kontaktów można rozpocząć konfigurowanie kontaktu użytkownika, który będzie wyświetlany na ekranie głównym trybu **Directory.** Przed skonfigurowaniem kontaktu użytkownika należy dodać użytkowników, wprowadzając ich ID użytkownika i nazwę użytkownika. Aby to zrobić, przejdź do **Directory > User**, kliknij **+Add** , a następnie przejdź do **User Basic > Contact Details** .







Konfiguracja parametrów :

- **Grupa** : wybierz grupę kontaktów. Wybierz określoną grupę kontaktów dla użytkownika. Wybierz domyślną grupę dla użytkownika.
- **Priorytet połączenia**: ustawienie priorytetu połączenia spośród trzech opcji: Primary**,** **Secondary** i **Terra**. Na przykład, jeśli ustawisz priorytet połączenia dla jednego z kontaktów w określonej grupie kontaktów jako **Podstawowy**, wówczas kontakt ten będzie wywoływany jako pierwszy spośród wszystkich kontaktów w tej samej grupie kontaktów, gdy ktoś naciśnie grupę kontaktów w celu wykonania połączenia grupowego.
- **Wybierz konto**: wybierz konto, z którego ma być wykonywane połączenie.

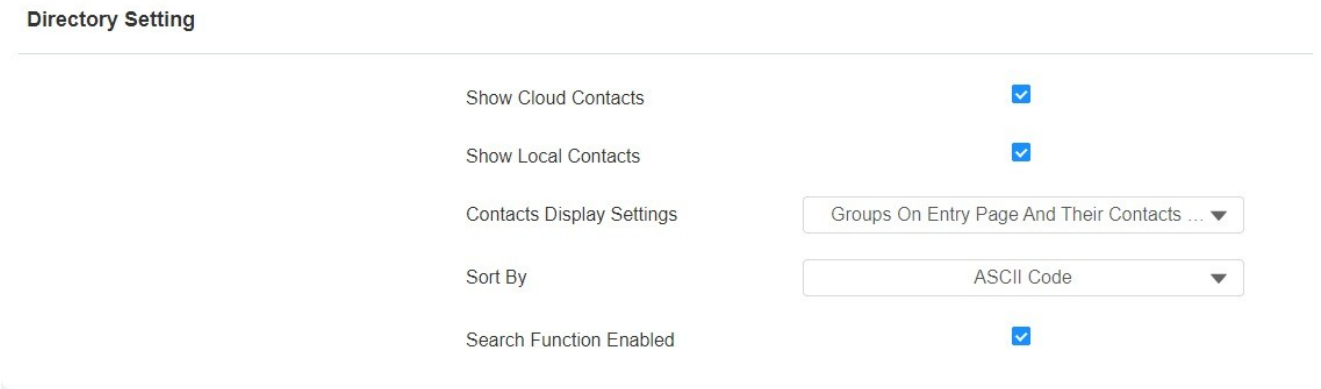
Uwaga

- Wszystkie kontakty bez określonej grupy trafią do grupy domyślnej.

Ustawienia wyświetlania listy kontaktów

Jeśli chcesz dostosować wyświetlanie listy kontaktów do swoich preferencji wizualnych. Możesz przejść do interfejsu internetowego, aby przeprowadzić konfigurację.

Przejdź do interfejsu **Directory > Directory Setting.**



Konfiguracja parametrów :

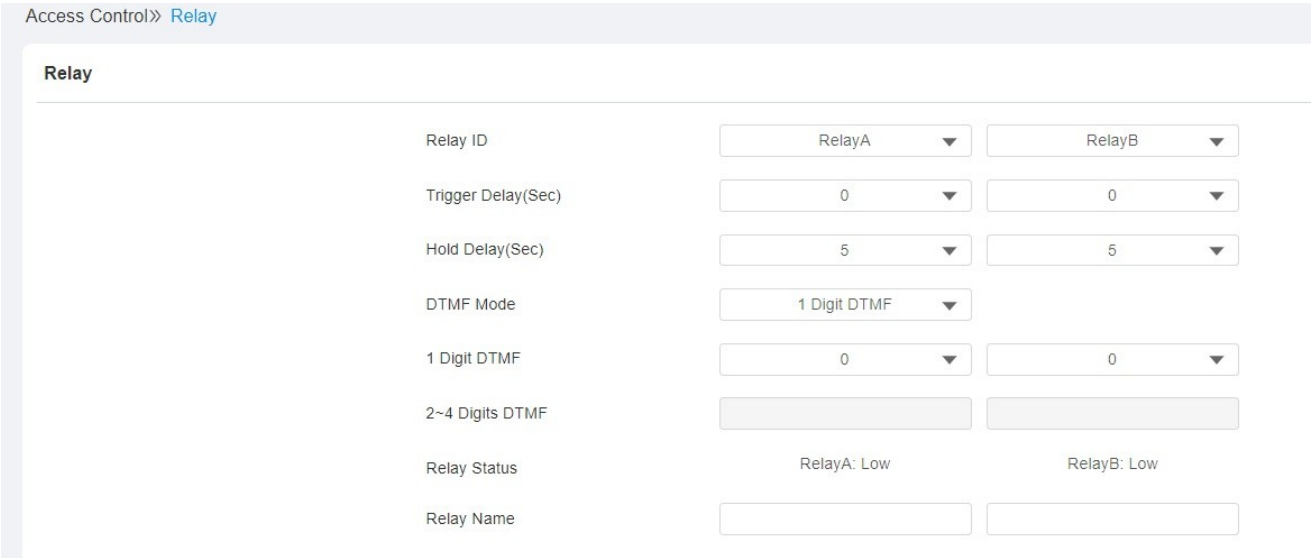
- **Pokaż kontakty w chmurze** : zaznacz pole wyboru, aby wyświetlić kontakty zsynchronizowane z chmurą SmartPlus.
- **Pokaż kontakty lokalne** : zaznacz pole wyboru, aby wyświetlić listę **kontaktów** lokalnych.
- **Ustawienia wyświetlania kontaktów**: wybierz opcję **Wszystkie kontakty**, aby wyświetlić wszystkie kontakty. Wybierz **Groups Only (Tylko grupy),** jeśli chcesz wyświetlić tylko grupę kontaktów i naciśnij, aby nawiązać połączenie grupowe. Wybierz **Groups On Entry Page And Their Contacts On Subpage**, aby wyświetlić kontakty według grup, a następnie naciśnij przycisk, aby wyświetlić listę kontaktów.
- **Sortuj według**: wybierz **Kod ASCII**, **Nr pokoju** lub **Importuj**. Po wybraniu opcji **Kod** ASCII najemcy zostaną wyświetleni według nazwisk w kolejności kodu **ASCII**. Po wybraniu opcji **Room No.** najemcy zostaną posortowani według numerów pokoi.
- **Funkcja wyszukiwania włączona** : włącz funkcję wyszukiwania kontaktów. Na ekranie pojawi się ikona wyszukiwania.

Ustawienie przekaźnika

Ustawienie przełącznika przekaźnika

Przełączniki przekaźnikowe i DTMF dla dostępu do drzwi można skonfigurować w aplikacji Web **Access Control.**

> Interfejs **przekaźnika.**



Konfiguracja parametrów :

- **Trigger Delay (Sec)**: ustaw czas opóźnienia wyzwolenia przekaźnika (w zakresie od 0 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia na 5 sekund, przekaźnik zostanie wyzwolony dopiero po **5** sekundach od naciśnięcia przycisku **odblokowania.**
- **Opóźnienie** wstrzymania **(sek.)**: ustaw czas opóźnienia wstrzymania przekaźnika (w zakresie od 1 do 10 sek.) Na przykład, jeśli ustawisz czas opóźnienia wstrzymania na **5** sekund, przekaźnik powróci do stanu początkowego po utrzymaniu stanu wyzwolenia

przez 5 sekund.

- **Tryb DTMF**: wybór liczby cyfr DTMF dla kontroli dostępu do drzwi (w zakresie od 1 do 4 cyfr). Można na przykład wybrać 1-cyfrowy kod DTMF lub 2-cyfrowy kod DTMF itp. w zależności od potrzeb.
- **1 Digit DTMF**: ustaw 1-cyfrowy kod DTMF z zakresu (**0-9 i *,#**), jeśli opcja DTMF jest ustawiona jako **1-cyfrowa.**
- **2~4 Digits DTMF** : ustaw kod DTMF zgodnie z ustawieniem **opcji DMTP.** Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli **opcja DTMP** jest ustawiona jako 3-cyfrowa.
- **Status przekaźnika**: status przekaźnika jest domyślnie niski, co oznacza stan normalnie zamknięty (NC). Jeśli stan przekaźnika jest wysoki, oznacza to, że jest on normalnie otwarty (NO).

- **Nazwa przekaźnika**: nazwij przełącznik przekaźnika zgodnie z potrzebami. Dla wygody można na przykład nazwać przełącznik przekaźnika zgodnie z jego lokalizacją.

Uwaga

- Tylko urządzenia zewnętrzne podłączone do przełącznika przekaźnikowego muszą być zasilane przez
- zasilane adaptery, ponieważ przełącznik przekaźnika nie dostarcza zasilania. Jeśli tryb DTMF jest ustawiony jako **1 Digit DTMF**, nie można edytować kodu DTMF w polu **2~4 Digits DTMF.** Jeśli tryb DTMF jest ustawiony na 2-4 w polu **2~4 Digits DTMF, nie** można edytować kodu DTMF w polu **1 Digit DTMF.**

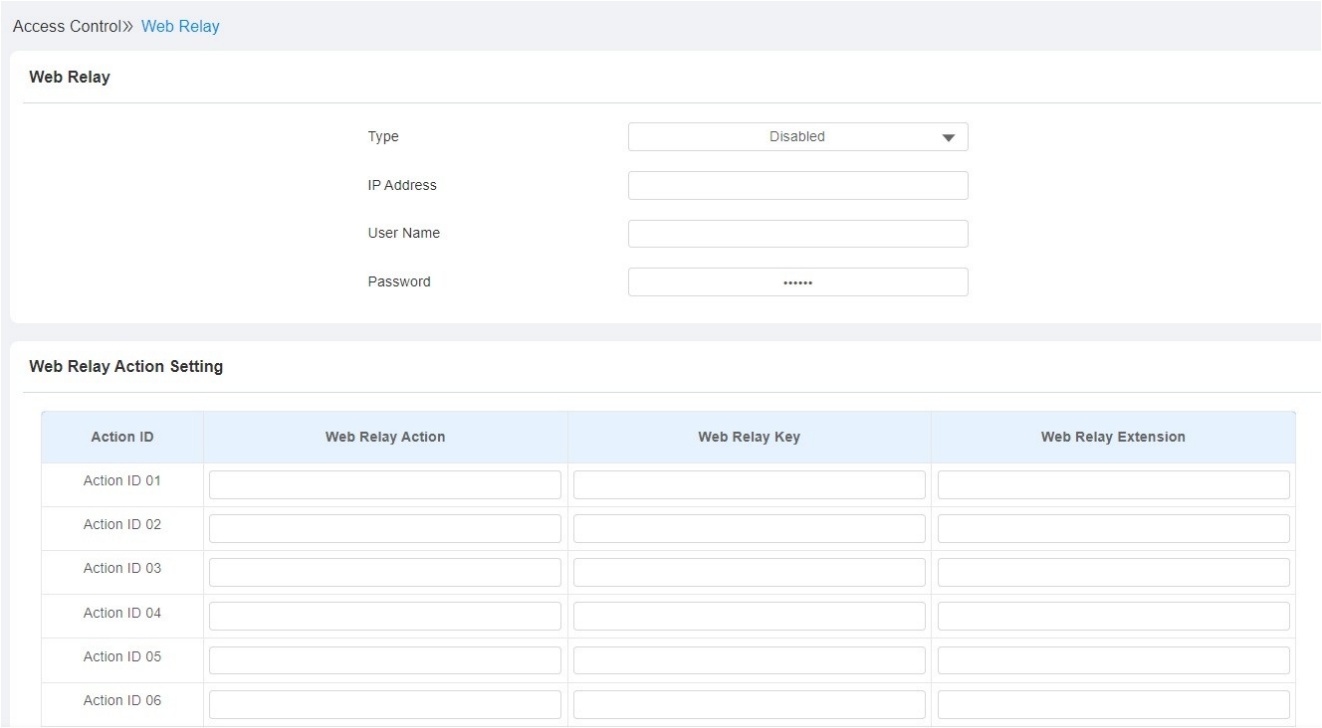
Ustawienia przekaźnika internetowego

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

Konfiguracja funkcji Web Relay

Przekaźnik sieciowy należy skonfigurować w interfejsie sieciowym, w którym należy podać takie informacje, jak adres IP przekaźnika, hasło, działanie przekaźnika sieciowego itp. Przed uzyskaniem dostępu do drzwi za pośrednictwem przekaźnika internetowego.

Aby skonfigurować konfigurację w interfejsie Web **Access Control > Web Relay. Adres IP** i **nazwa użytkownika są** dostarczane przez producenta przekaźnika sieciowego.



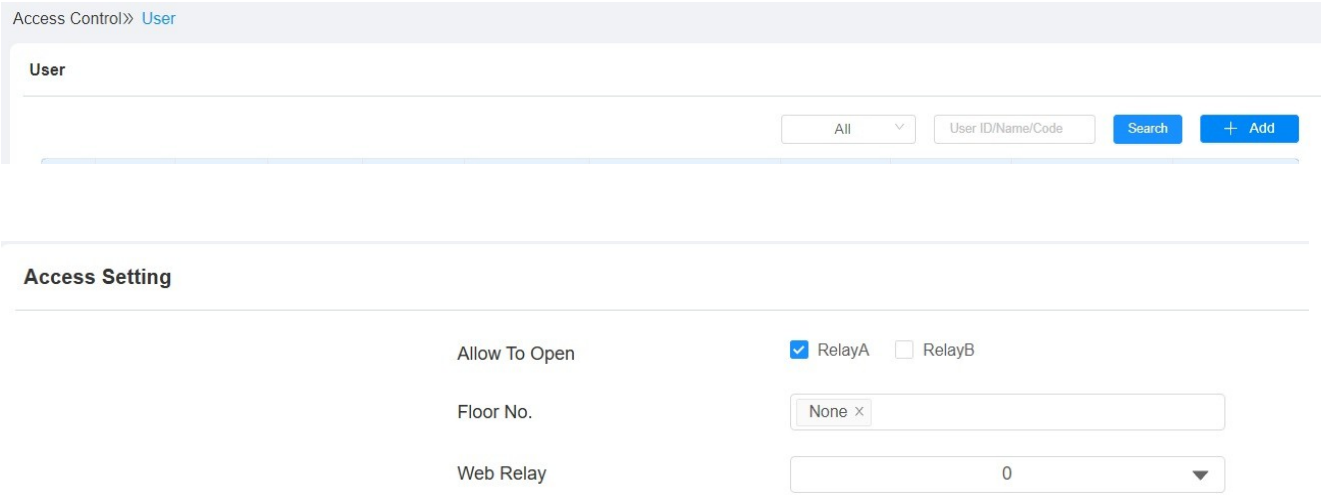
Konfiguracja parametrów :

- **Typ**: wybierz jedną z trzech opcji: **Wyłączone, WebRelay** i **Oba.** Wybierz **Web Relay,** aby włączyć przekaźnik sieciowy. Wybierz **Disable,** aby wyłączyć przekaźnik sieciowy. Wybierz **Both,** aby włączyć zarówno przekaźnik lokalny, jak i internetowy.
- **Password** : wprowadź hasło dostarczone przez producenta przekaźnika sieciowego. Hasło jest uwierzytelniane przez HTTP i można je zdefiniować za pomocą **HTTP Get** in Action.
- **Web Relay Action (Akcja przekaźnika sieciowego)**: wprowadź określone polecenie akcji przekaźnika sieciowego dostarczone przez producenta sieci w celu wykonania różnych akcji przez przekaźnik sieciowy.
- **Klucz** przekaźnika **internetowego**: wprowadź skonfigurowany kod DTMF, gdy drzwi zostaną odblokowane za pomocą kodu DTMF, polecenie akcji zostanie automatycznie wysłane do przekaźnika internetowego.
- **Web Relay Extension**: wprowadź informacje o rozszerzeniu przekaźnika, które może

być nazwą użytkownika konta SIP urządzenia interkomowego, takiego jak monitor wewnętrzny, aby określone polecenie akcji zostało wysłane po odblokowaniu urządzenia interkomowego, podczas gdy to ustawienie jest opcjonalne.

Zapoznaj się z poniższym przykładem: http://admin:admin@192.168.1.2/state.xml?relayState=2.

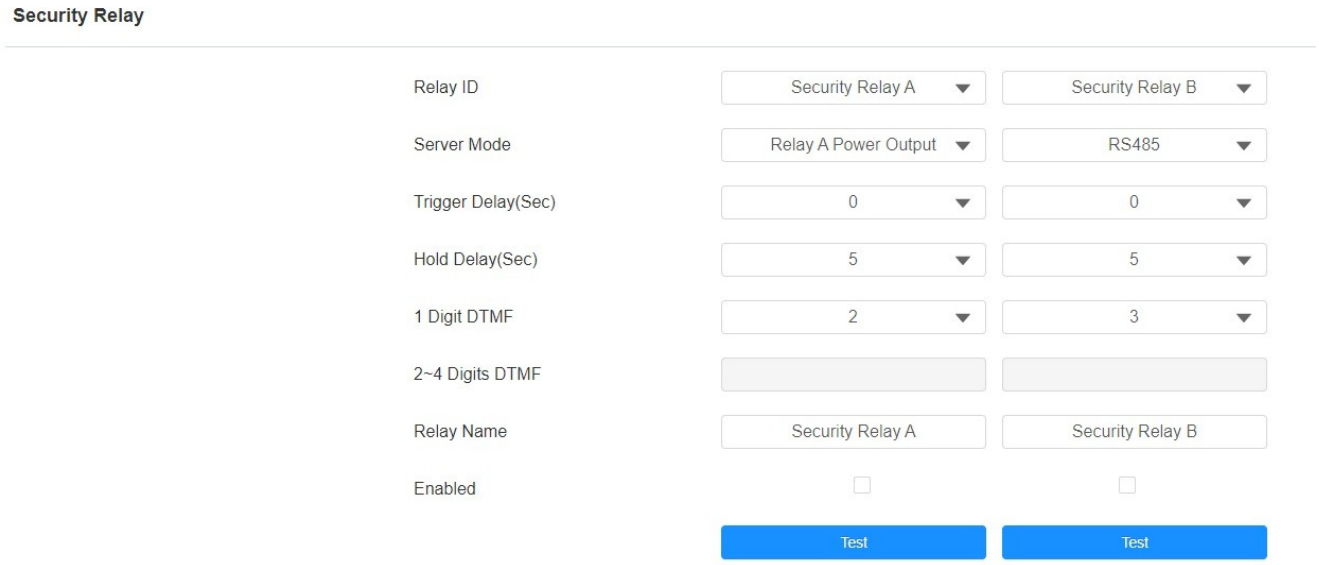
Po skonfigurowaniu przekaźnika sieciowego można skonfigurować określony przekaźnik sieciowy, który ma być wyzwalany na podstawie lokalizacji przekaźnika dostępu do drzwi. Aby to zrobić, przejdź do **Directory > User**, kliknij **+ Add** , a następnie przewiń w dół do **Access Setting** .



Konfiguracja przekaźnika zabezpieczeń

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 bramofonu.

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



Konfiguracja parametrów :

- **Tryb serwera**: wybór typu połączenia między przekaźnikiem bezpieczeństwa a bramofonem. Można wybrać połączenie przez **wyjście zasilania przekaźnika A** lub **RS485**.
- **Trigger Delay (Sec)**: ustaw czas opóźnienia wyzwolenia przekaźnika (w zakresie od 1 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia na **5** sekund, przekaźnik zostanie wyzwolony dopiero 5 sekund po naciśnięciu zakładki **Unlock.** Domyślną wartością jest 0, co oznacza wyzwolenie przekaźnika zaraz po naciśnięciu przycisku odblokowania.
- **Opóźnienie** wstrzymania **(sek.)**: ustaw czas opóźnienia wstrzymania przekaźnika (w zakresie od 1 do 10 sek.) Na przykład, jeśli ustawisz czas opóźnienia wstrzymania na **5** sekund, przekaźnik zostanie opóźniony o 5 sekund po odblokowaniu drzwi.
- **1-cyfrowy DTMF**: ustaw 1-cyfrowy kod DTMF w zakresie od (**0-9 i *,#**).
- **2~4 cyfry DTMF**: ustaw kod DTMF zgodnie z ustawieniem **opcji DMTP.** Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli **tryb DTMP** jest ustawiony jako 3-cyfrowy.
- **Nazwa przekaźnika**: w razie potrzeby nadaj nazwę przekaźnikowi. Nazwę przekaźnika można edytować w chmurze SmartPlus i SDMC.

Uwaga

- Szczegółowe informacje na temat okablowania można znaleźć w **skróconej instrukcji obsługi SR01**.

Zarządzanie harmonogramem dostępu do drzwi

Konfiguracja harmonogramu dostępu do drzwi

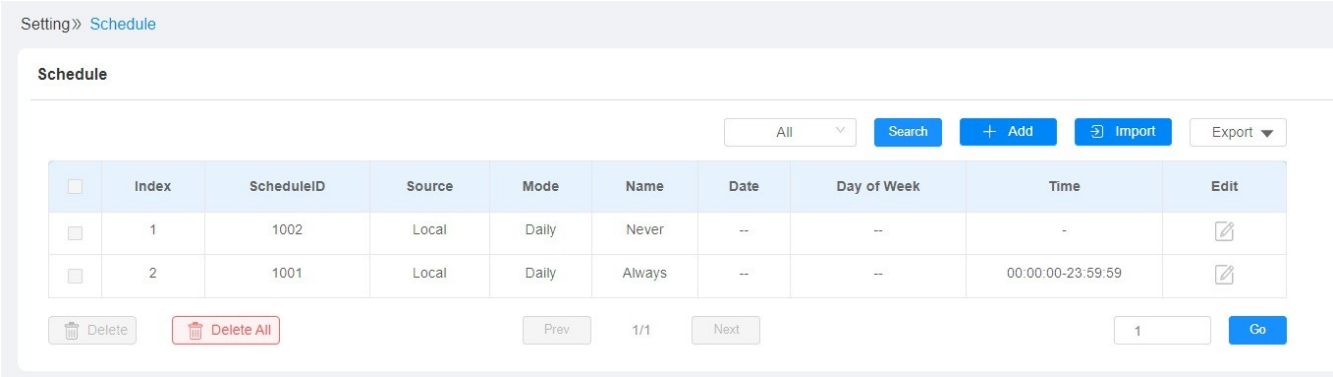
Harmonogram dostępu do drzwi pozwala zdecydować, kto i kiedy może otworzyć drzwi. Dotyczy to zarówno pojedynczych osób, jak i grup, zapewniając, że użytkownicy w ramach harmonogramu mogą otwierać drzwi przy użyciu autoryzowanej metody tylko w wyznaczonych okresach czasu.

Tworzenie harmonogramu dostępu do drzwi

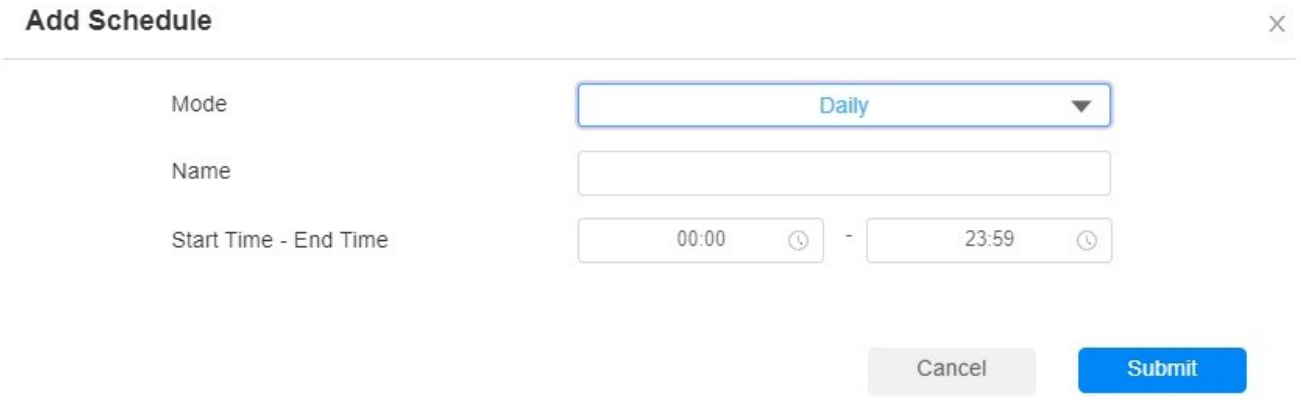
Harmonogramy dostępu do drzwi można tworzyć dla okresów dziennych,

tygodniowych lub niestandardowych. Aby to zrobić, przejdź do **Ustawienia >**

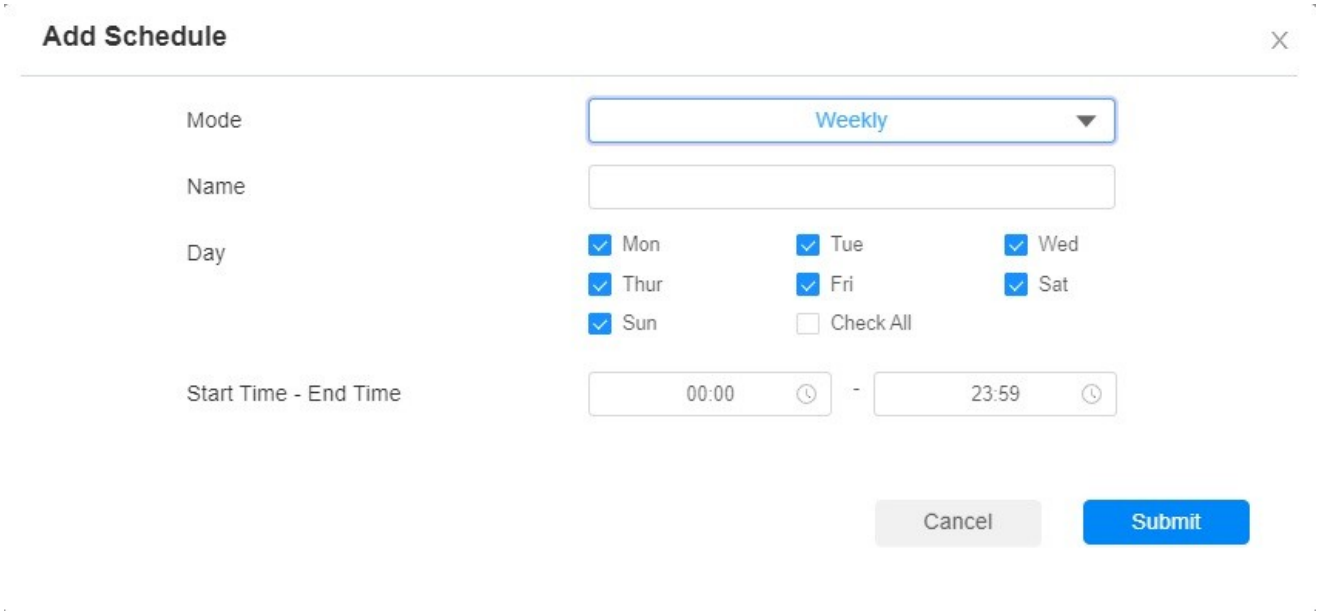
Harmonogram , a następnie kliknij **+ Dodaj** .



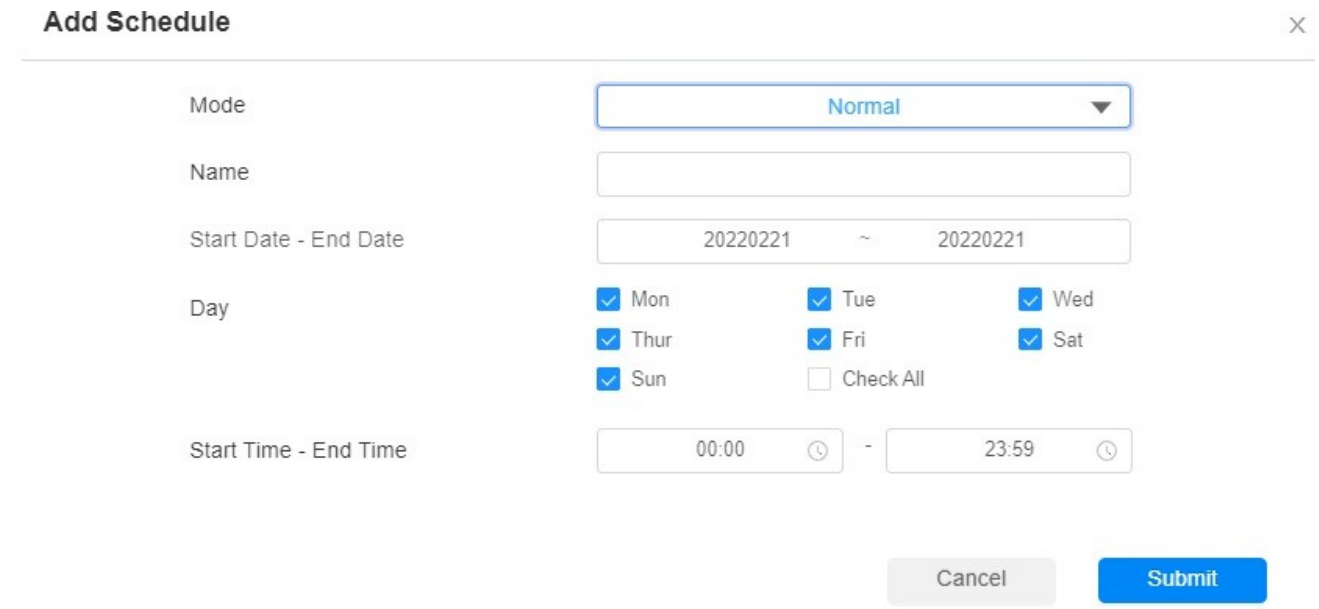
Aby utworzyć harmonogram dzienny, można wykonać następujące czynności:



Aby utworzyć harmonogram tygodniowy:



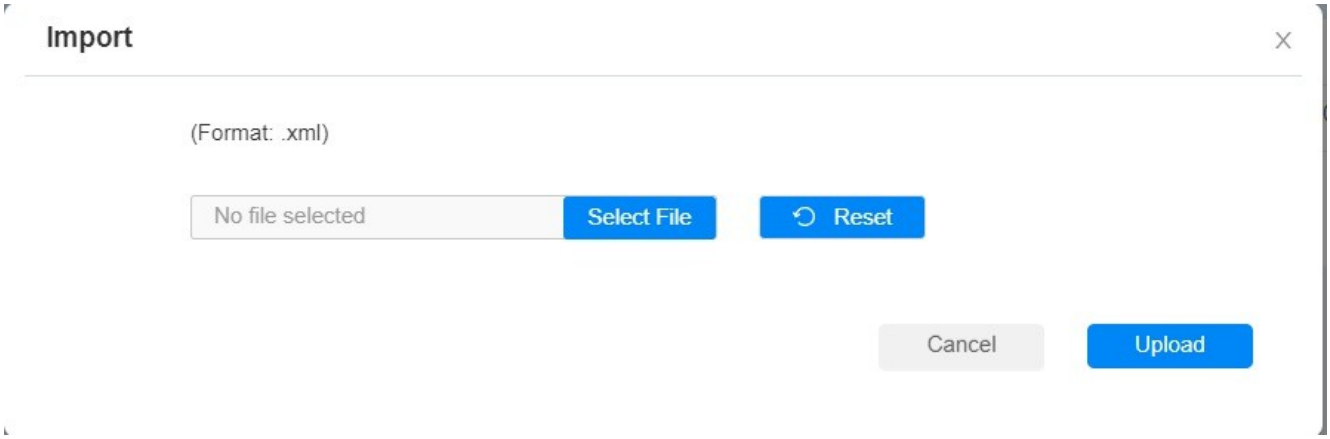
Aby utworzyć harmonogram na dłuższy okres:



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 to zrobić, przejdź do opcji **Ustawienia > Harmonogram** , a następnie kliknij przycisk **Importuj**.

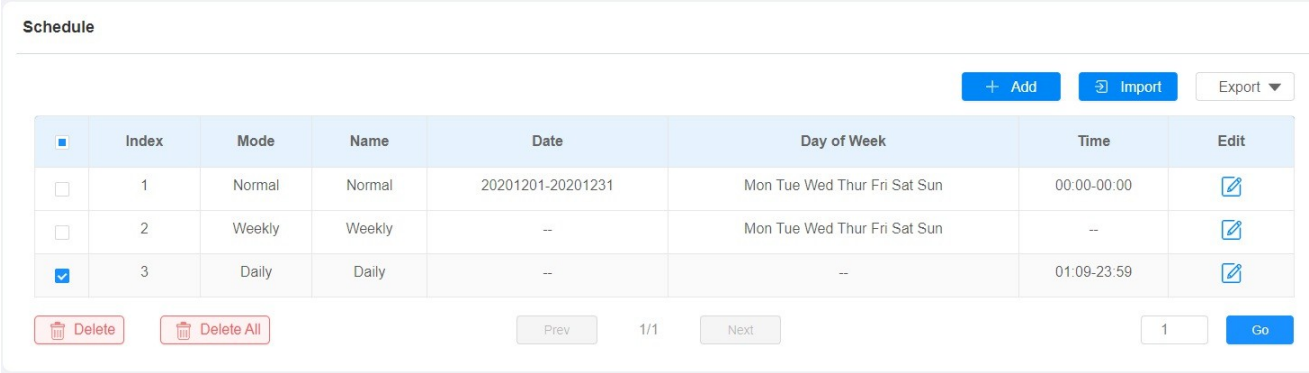


Uwaga:

- Obsługuje tylko plik w formacie .xml do importowania i eksportowania harmonogramu.

Edycja harmonogramu dostępu do drzwi

Przejdź do opcji **Ustawienia >** Interfejs **harmonogramu.**



Uwaga

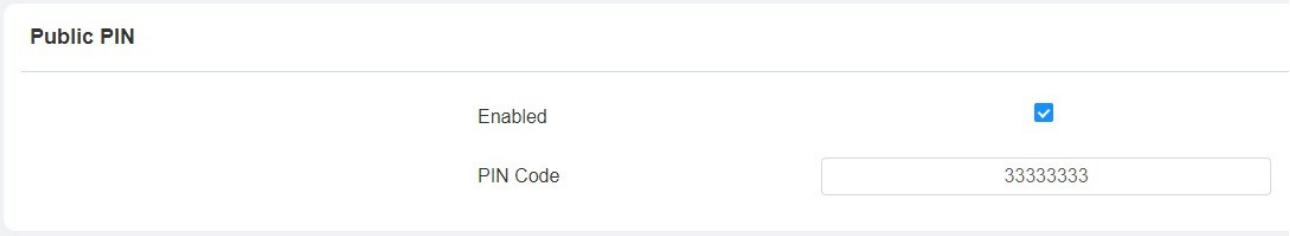
- Obsługuje tylko plik w formacie .xml do importowania i eksportowania harmonogramu.
- Harmonogram kontroli dostępu zsynchronizowany z aplikacją SmartPlus nie może być edytowany ani usuwany.

Konfiguracja odblokowania drzwi

Konfiguracja kodu PIN do odblokowywania drzwi

Istnieją dwa rodzaje kodów PIN dostępu do drzwi: publiczny i prywatny. Prywatny kod PIN jest unikalny dla każdego użytkownika, podczas gdy publiczny jest współdzielony przez mieszkańców tego samego budynku lub kompleksu. Można tworzyć i modyfikować zarówno publiczne, jak i prywatne kody PIN.

Przejdź do opcji **Kontrola dostępu > Ustawienia PIN > Publiczny** interfejs **PIN.**



Konfiguracja parametrów :

- **Kod PIN**: ustawienie kodu PIN z limitem cyfr w zakresie od **4 do 8**.

Uwaga:

- Publiczny kod PIN będzie ważny dopiero po włączeniu tej funkcji.

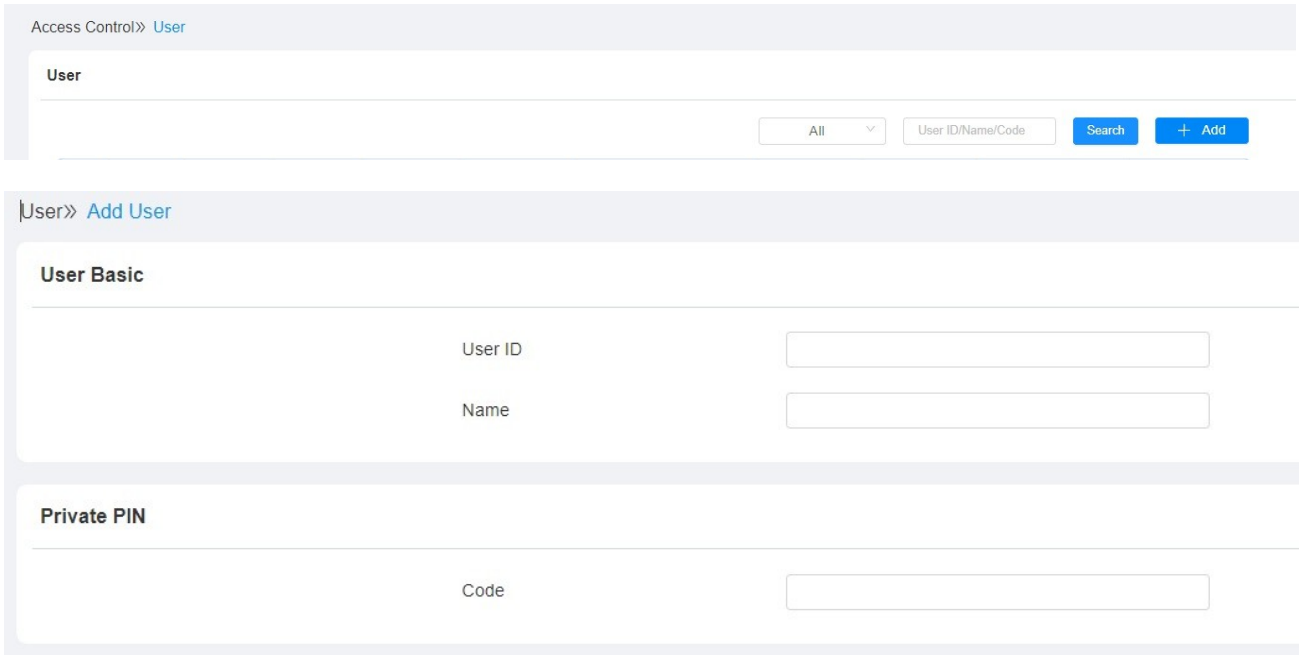
Dodaj użytkownika

Przed skonfigurowaniem prywatnego kodu PIN, karty RF i danych twarzy użytkownika należy utworzyć użytkownika. Można również skonfigurować ustawienia kontroli dostępu i powiązane ustawienia połączeń dla użytkownika.

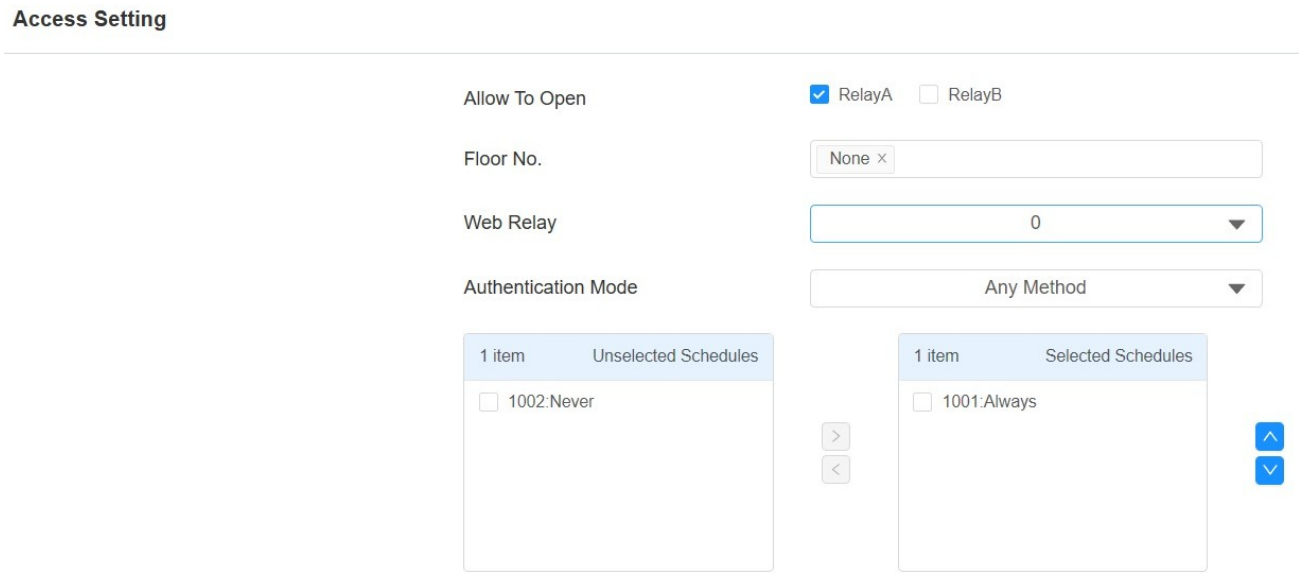
Konfiguracja prywatnego kodu PIN

W interfejsie internetowym można utworzyć kod PIN i dostosować dodatkowe ustawienia, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenia, który przekaźnik ma zostać otwarty.

Aby skonfigurować konfigurację w sieci Web **Directory > User**, kliknij **+Add** .



Następnie przewiń w dół do opcji **Ustawienia dostępu** i wybierz przekaźniki oraz harmonogram dostępu do drzwi dla kodu PIN.



Konfiguracja parametrów :

- **Zezwalaj na otwarcie**: wybierz przekaźniki, które mają być uruchamiane przez kod PIN.

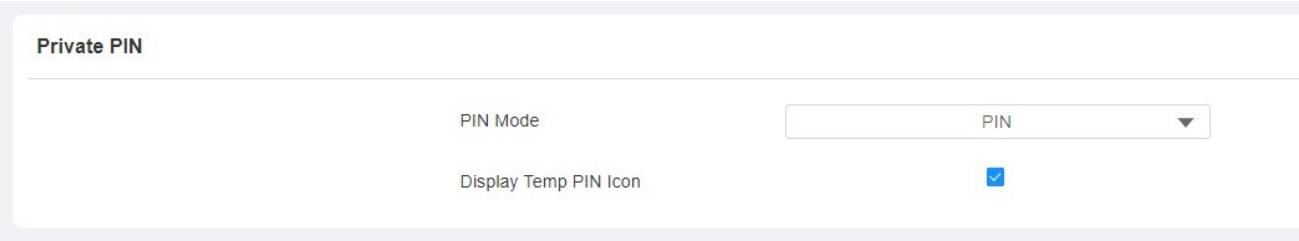
Uwa

- Ten krok ma zastosowanie do dostępu do drzwi za pomocą karty RF i rozpoznawania twarzy, ponieważ są to identyczne w konfiguracji.

Konfiguracja prywatnego trybu dostępu PIN

Bramofon zapewnia dwie metody uwierzytelniania w celu uzyskania dostępu do prywatnego kodu PIN: PIN i APT# + PIN. Ta ostatnia wymaga od użytkowników wprowadzenia numeru mieszkania, a następnie prywatnego kodu PIN w celu odblokowania drzwi.

Aby skonfigurować konfigurację w interfejsie Web **Access Control > PIN Setting > Private PIN.**



Konfiguracja parametrów :

- **Tryb PIN** : wybierz tryb dostępu pomiędzy **PIN** i **APT#+PIN**. W przypadku wybrania opcji PIN wymagane jest jedynie wprowadzenie kodu PIN bezpośrednio w celu uzyskania dostępu do drzwi, natomiast w przypadku wybrania opcji **APT#+PIN** wymagane jest wprowadzenie numeru apartamentu przed wprowadzeniem kodu PIN w celu uzyskania dostępu do drzwi.
- **Display Temp PIN Icon**: włącz, jeśli chcesz wyświetlać ikonę kodu QR, którą możesz nacisnąć, aby uzyskać dostęp do kodu QR na ekranie.

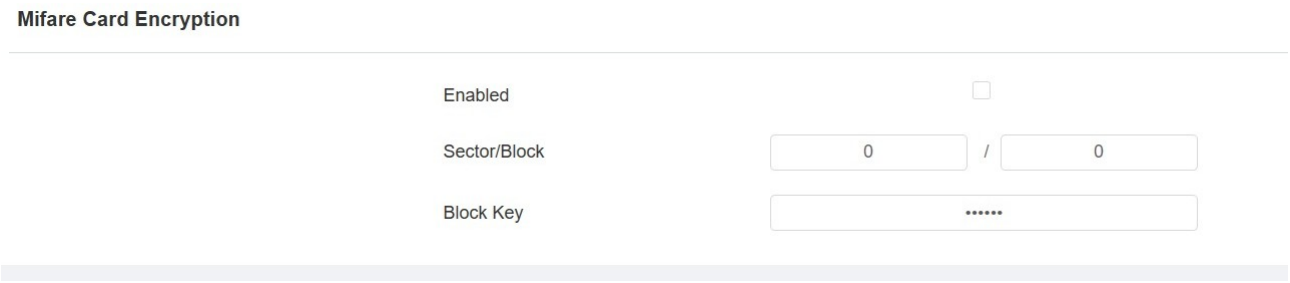
Uwaga:

- **Kod QR** może mieć zastosowanie tylko wtedy, gdy urządzenie jest dodane do Akuvox SmartPlus.

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 to zrobić, przejdź do opcji **Kontrola dostępu > Ustawienia karty > Szyfrowanie karty Mifare**.



Konfiguracja parametrów :

- **Sector/Block** : wprowadź sektor i blok, w którym znajduje się numer karty na karcie Mifare. Na przykład numer karty może znajdować się w sektorze 3 i bloku 3 na karcie.
- **Klucz bloku**: wprowadź hasło bloku, aby uzyskać dostęp do bloku w celu uzyskania kodu.

Uwaga

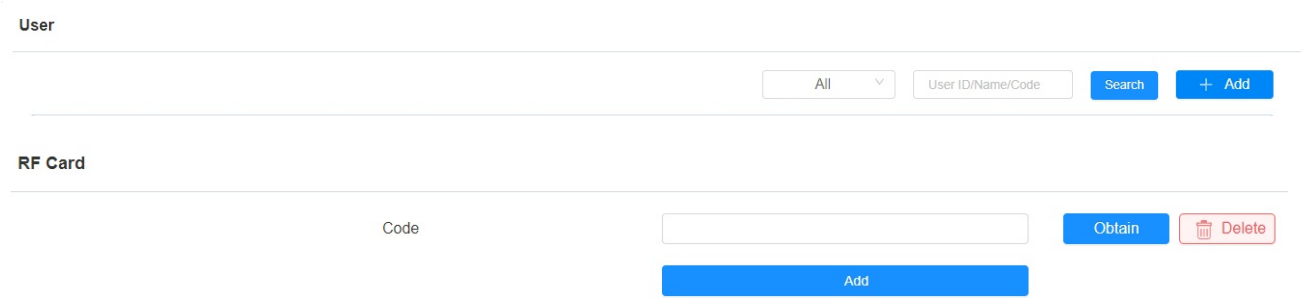
- Karta Mifare musi być najpierw zaszyfrowana, w przeciwnym razie czytnik kart nie będzie w stanie jej odczytać.

Konfiguracja karty RF do odblokowywania drzwi

Konfiguracja karty RF w interfejsie internetowym

Aby skonfigurować kartę RF, przejdź do **Directory > User**, a następnie kliknij **+Add.**

Następnie wprowadź informacje o użytkowniku i uzyskaj kod QR.



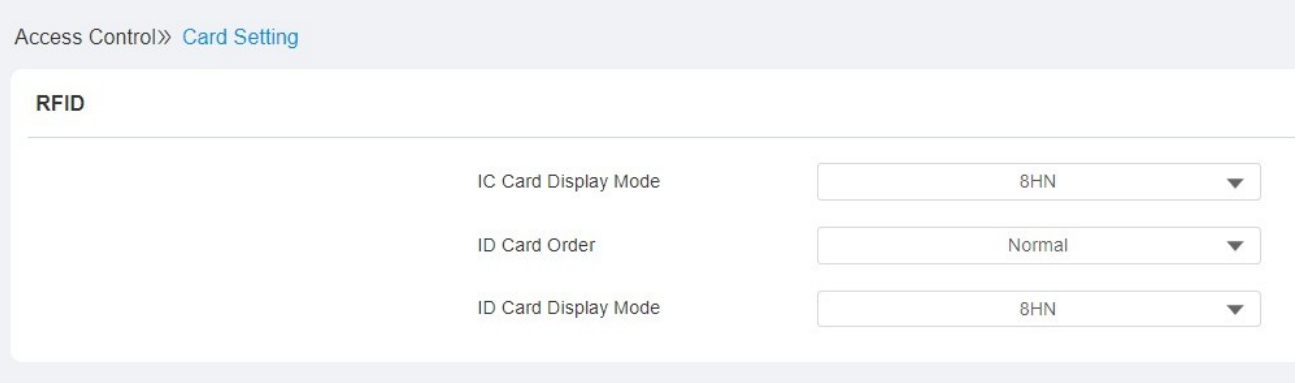
Uwaga

- Informacje na temat wyboru harmonogramu dostępu za pomocą kodu PIN dla użytkownika(-ów) karty RF można znaleźć w części Wybór harmonogramu dostępu za pomocą kodu PIN.
- Karta RF o częstotliwości 13,56 MHz i 125 kHz może być stosowana do bramofonu w celu uzyskania dostępu do drzwi.

Konfiguracja formatu 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 skonfigurować konfigurację w interfejsie Web **Access Control > Card Setting.**



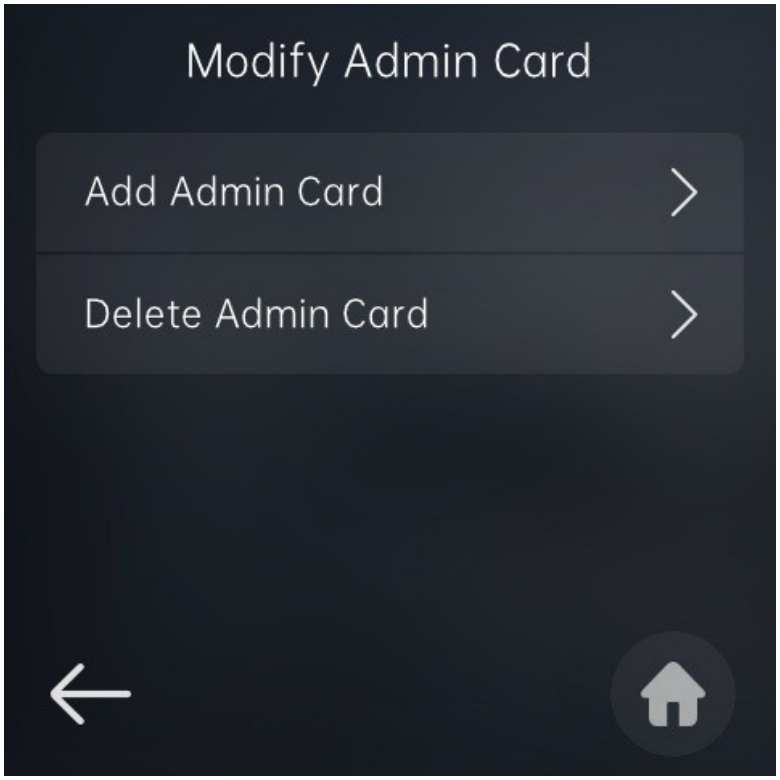
Konfiguracja parametrów :

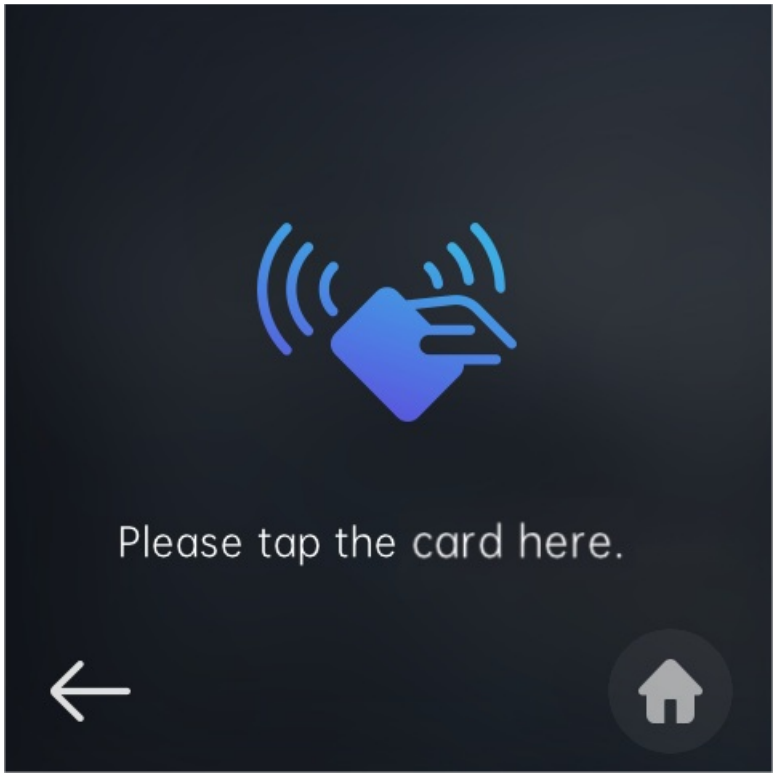
- **Tryb wyświetlania karty IC**: wybór formatu kodu **karty IC** dostępu do drzwi spośród siedmiu opcji formatu: **8H10D; 6H3D 5D(W26); 6H8D; 8HN; 8HR; 6H3D 5D-R(W26); 8HR10D** . Domyślny format kodu karty w bramofonie to **8HN.**
- **Kolejność karty ID**: wybór normalnego lub odwróconego wyświetlania karty ID.
- **Tryb wyświetlania karty ID**: wybór formatu **karty ID** dla dostępu do drzwi spośród siedmiu opcji formatu: **8H10D; 6H3D 5D(W26); 6H8D; 8HN; 8HR; 6H3D 5D-R(W26); 8HR10D** . Domyślny format kodu karty w bramofonie to **8HN.**

Konfiguracja karty RF w urządzeniu

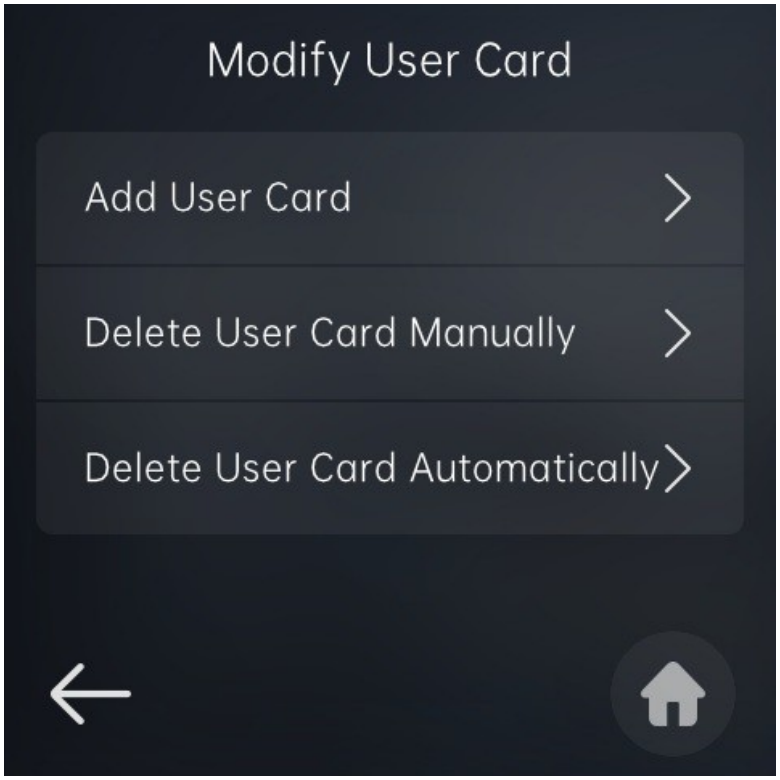
Kartę RF można skonfigurować bezpośrednio na urządzeniu w celu uzyskania dostępu do drzwi, ustawiając harmonogram ważności dostępu do karty RF wraz z przekaźnikiem sieciowym, który może być wyzwalany za pomocą karty RF itp.

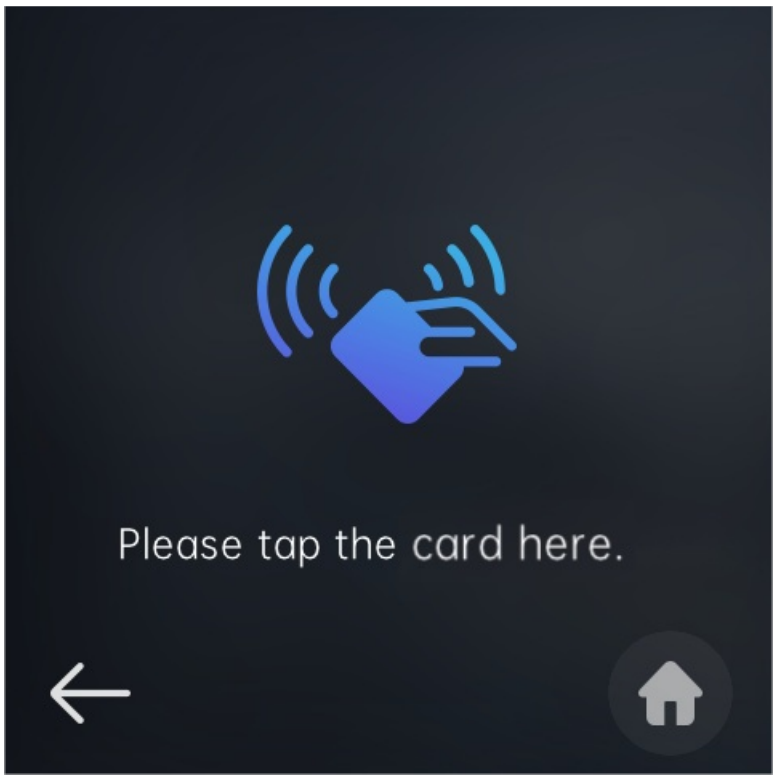
Aby skonfigurować kartę administratora, przejdź do **Ustawienia zaawansowane > Dostęp administratora > Modyfikuj kartę administratora > Dodaj kartę administratora** .





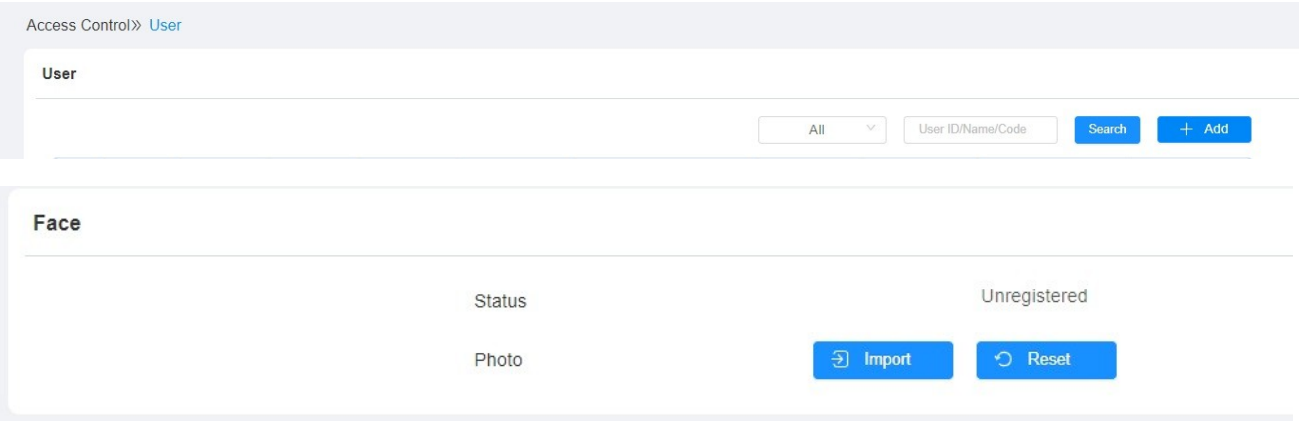
Aby skonfigurować kartę użytkownika, naciśnij ikonę na ekranie głównym, a następnie wprowadź ustawienia domyślne hasło 3888, a następnie naciśnij ikonę na klawiaturze. Następnie wybierz opcję **Modify User Card** , a następnie wprowadź kod PIN systemu, który domyślnie wynosi **2396.** Następnie naciśnij **Dodaj kartę użytkownika** .





Konfiguracja rozpoznawania twarzy do odblokowywania drzwi

Dane twarzy można zaimportować do urządzenia w interfejsie internetowym. Aby to zrobić, przejdź do **Katalog > Użytkownik**, a następnie kliknij **+Dodaj** . Następnie wprowadź informacje o użytkowniku i prześlij zdjęcia rozpoznawania twarzy.



Konfiguracja parametrów :

- **Status** : będzie wyświetlany jako **Zarejestrowany**, jeśli przesłane zdjęcie jest zgodne z formatem i standardem, w przeciwnym razie domyślnie będzie wyświetlany jako **Niezarejestrowany.** Status zostanie jednak zmieniony z powrotem na **Niezarejestrowany,** jeśli przesłane zdjęcie zostanie wyczyszczone po naciśnięciu zakładki **Reset.**
- **Zdjęcie** : wybierz zdjęcie w formacie jpg lub png, które ma zostać przesłane do urządzenia i naciśnij przycisk , jeśli chcesz usunąć przesłane zdjęcie.

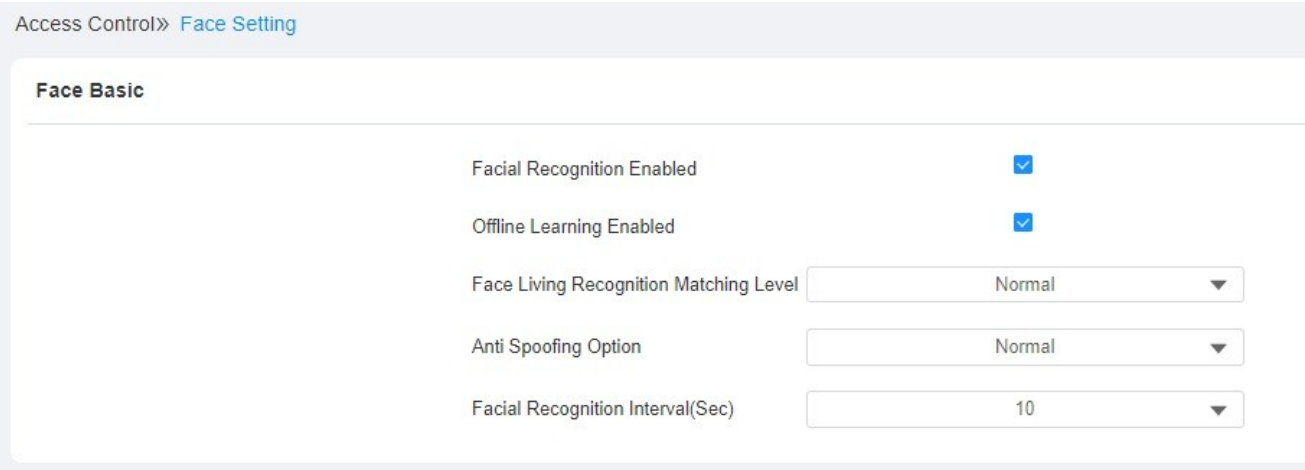
Uwaga

- Przesyłane zdjęcia powinny być w formacie jpg lub png.
- Informacje na temat wyboru harmonogramu dostępu za pomocą kodu PIN dla dostępu do drzwi specyficznego dla użytkownika(-ów) rozpoznającego(-ych) twarz znajdują się w części Wybór harmonogramu dostępu za pomocą kodu PIN.

Podstawowa konfiguracja funkcji rozpoznawania twarzy w interfejsie internetowym

Bramofon umożliwia dostosowanie dokładności rozpoznawania twarzy, interwałów rozpoznawania i nie tylko, aby poprawić komfort użytkowania.

Przejdź do opcji **Kontrola dostępu > Ustawienia twarzy >** Interfejs **podstawowy twarzy.**



Konfiguracja parametrów:

- **Offline Learning Enabled** : włącz tę opcję, jeśli chcesz poprawić zdolność rozpoznawania urządzenia, koncentrując się na głównych cechach twarzy, pomijając drobne zmiany, które zaszły na twarzy. Dokładność rozpoznawania twarzy poprawia się wraz ze wzrostem liczby rozpoznań twarzy.
- **Face Living Recognition Matching Level**: kliknij, aby wybrać poziom dokładności rozpoznawania twarzy spośród czterech opcji: **Low, Normal, High, Highest**. Na przykład, jeśli wybierzesz **Najwyższy**, będzie najmniejsze prawdopodobieństwo, że ktoś inny zostanie pomylony z tobą przez pomyłkę lub w inny sposób podczas rozpoznawania twarzy.
- **Opcja antyspoofingu**: wybierz poziom **antyspoofingu** spośród czterech opcji: **Low, Normal, High, Highest, Close** . Na przykład, jeśli wybierzesz **Najwyższy**, będzie najmniejsze prawdopodobieństwo, że urządzenie zostanie oszukane przez obrazy cyfrowe lub zdjęcia dowolnego rodzaju.
- **Facial Recognition Interval(Sec) (Interwał rozpoznawania twarzy (sek.))**: wybierz interwał czasowy między każdym rozpoznaniem twarzy z zakresu 2-60 sek. Na przykład, jeśli wybierzesz **5**, musisz poczekać 5 sekund. Zanim będzie można ponownie wykonać rozpoznawanie twarzy.

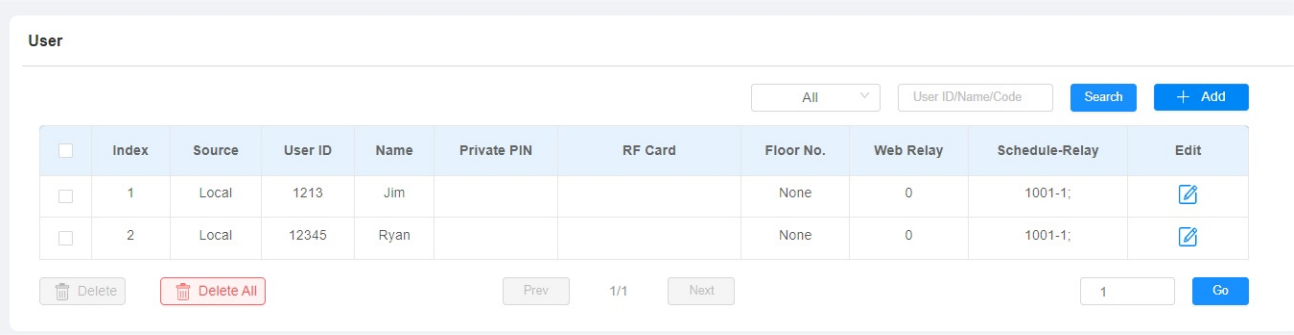
Uwaga

- Więcej informacji na ten temat znajduje się w części Wybór harmonogramu dostępu do kodu PIN dla użytkownika(-ów) rozpoznającego(-ych) twarz.

Edycja danych dostępu do drzwi specyficznych dla użytkownika

Można wyszukiwać dostęp do drzwi dla poszczególnych użytkowników i edytować dane dostępu do drzwi w **katalogu** internetowym.

> Interfejs **użytkownika.**



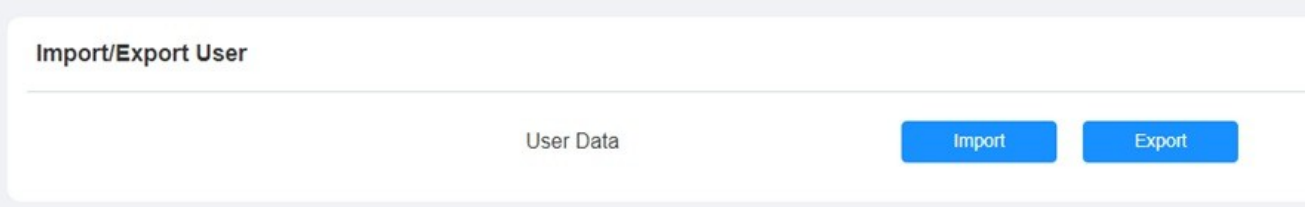
Uwaga

- Użytkowników zsynchronizowanych z aplikacją SmartPlus nie można edytować ani usuwać.

Import i eksport danych użytkownika kontroli dostępu

Bramofon obsługuje dane użytkownika kontroli dostępu, które mogą być współdzielone między bramofonami Akuvox poprzez import i eksport, a także można eksportować dane twarzy z bramofonu, a następnie importować je do urządzenia innej firmy.

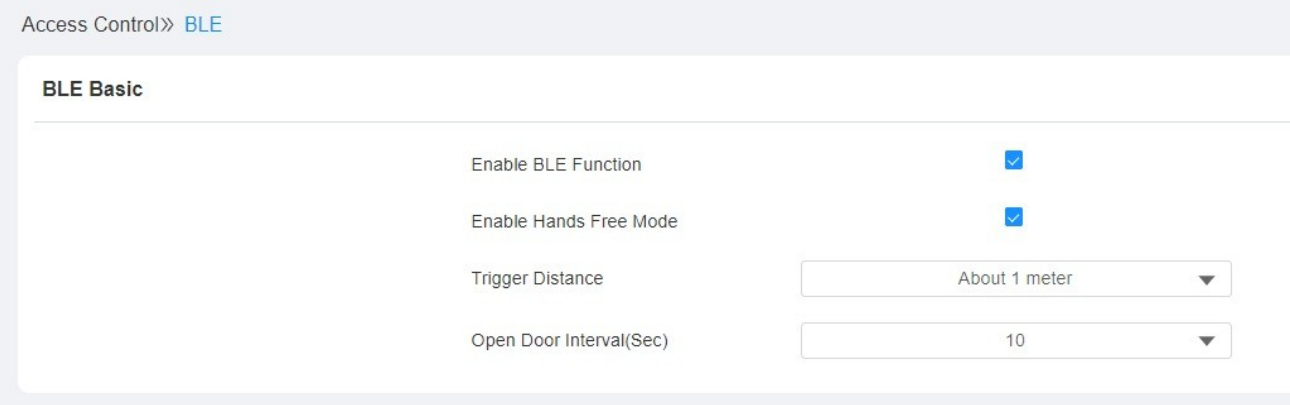
Aby skonfigurować konfigurację w interfejsie Web **Directory > User > Import/Export User.**



Konfiguracja Bluetooth do odblokowywania drzwi

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 drzwi, zbliżając się do nich.

Aby skonfigurować funkcję, przejdź do **Kontrola dostępu > BLE > BLE Basic** .



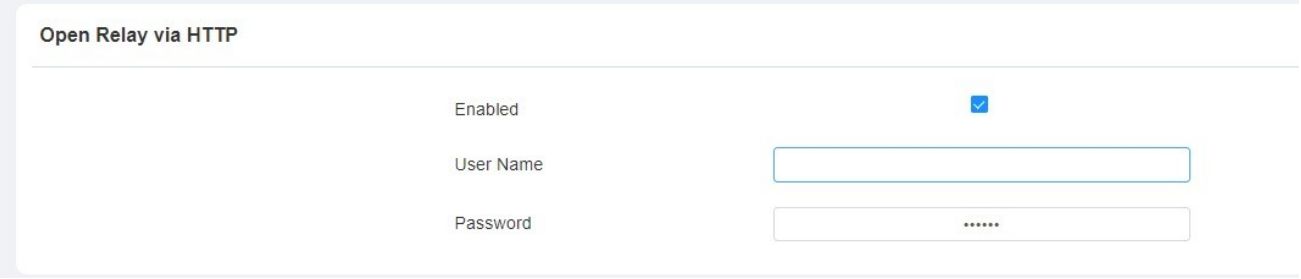
Konfiguracja parametrów:

- **Enable Hands Free Mode (Włącz tryb głośnomówiący):** jeśli opcja ta jest włączona, można uzyskać dostęp do drzwi bez użycia rąk. Jeśli jest wyłączony, aby uzyskać dostęp do drzwi, należy pomachać ręką przed bramofonem.
- **Odległość wyzwalania**: ustawienie odległości wyzwalania Bluetooth dla dostępu do drzwi. Do wyboru są opcje **Około 1 metra, W promieniu 1 metra** i **Ponad 2 metry**. Odległość wyzwalania wynosi **maksymalnie 3 metry**.
- **Interwał otwarcia drzwi (sek.)**: wybór interwału czasowego między kolejnymi dwoma otwarciami drzwi Bluetooth.

Konfiguracja Open Relay przez HTTP do odblokowywania drzwi

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 skonfigurować konfigurację w sieci Web **Access Control > Relay > Open Relay via HTTP** interface.



Konfiguracja parametrów :

- **Nazwa użytkownika** : wprowadź nazwę użytkownika interfejsu internetowego
- urządzenia, na przykład **admin**. **Hasło** : wprowadź hasło dla polecenia HTTP. Na przykład **12345** .

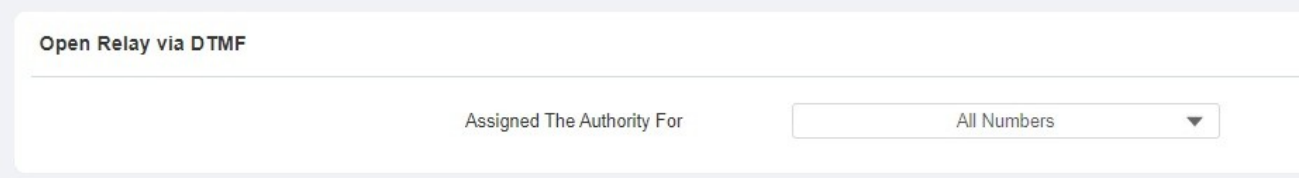
Zapoznaj się z poniższym przykładem:

http://192.168.35.127/fcgi/do?
action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

> **Uwaga**
>
> **DoorNum** w powyższym poleceniu HTTP odnosi się do numeru przekaźnika #1, który ma zostać wyzwolony w celu uzyskania dostępu do drzwi.

Konfiguracja przekaźnika otwarcia poprzez DTMF dla odblokowania drzwi

W razie potrzeby można autoryzować styki, aby mogły odblokować drzwi za pomocą DTMF lub odmówić wszystkim stykom odblokowania DTMF. Aby to zrobić, przejdź do **Kontrola dostępu > Przekaźnik > Otwórz przekaźnik przez DTMF** .



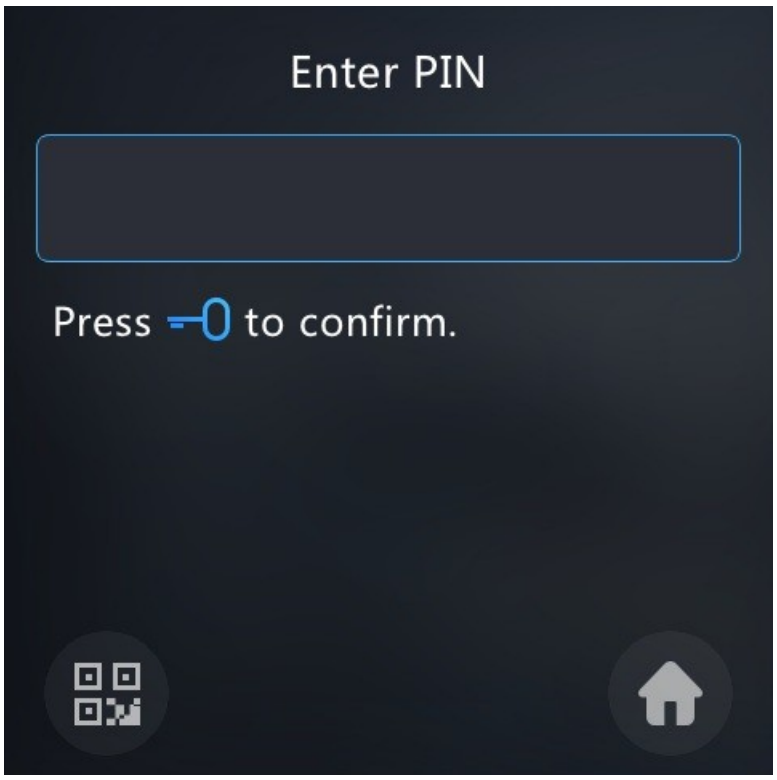
Konfiguracja parametrów :

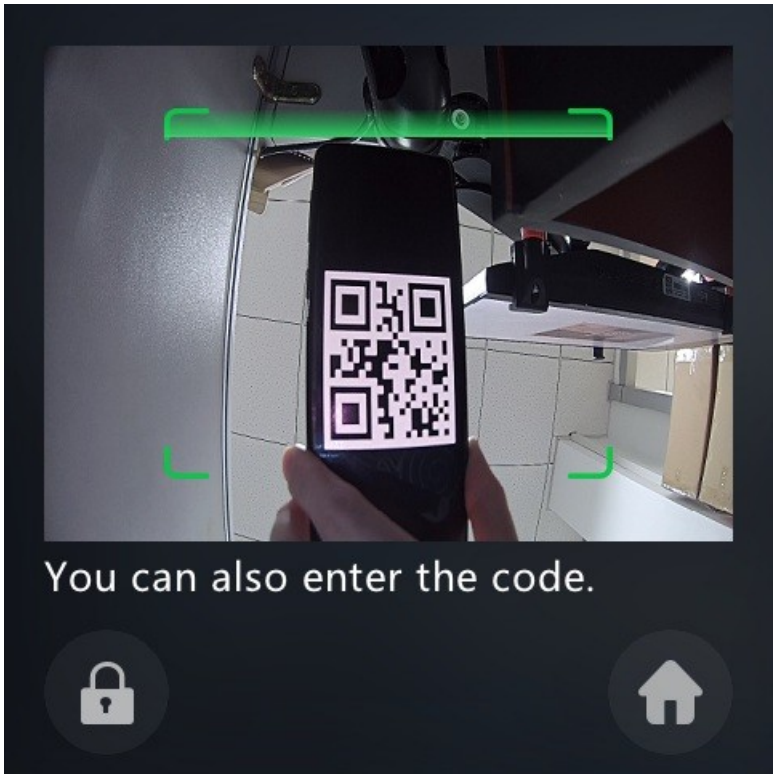
Wybierz **Wszystkie numery, Brak** lub **Tylko lista kontaktów**, aby umożliwić odblokowanie drzwi DTMF.

Odblokowanie za pomocą kodu QR

Możesz użyć kodu QR, aby odblokować drzwi za pomocą bramofonu. Ta metoda wymaga usługi w chmurze Akuvox SmartPlus. Przed użyciem tej funkcji należy ją aktywować.

Naciśnij ikonę kodu QR w lewym dolnym rogu.





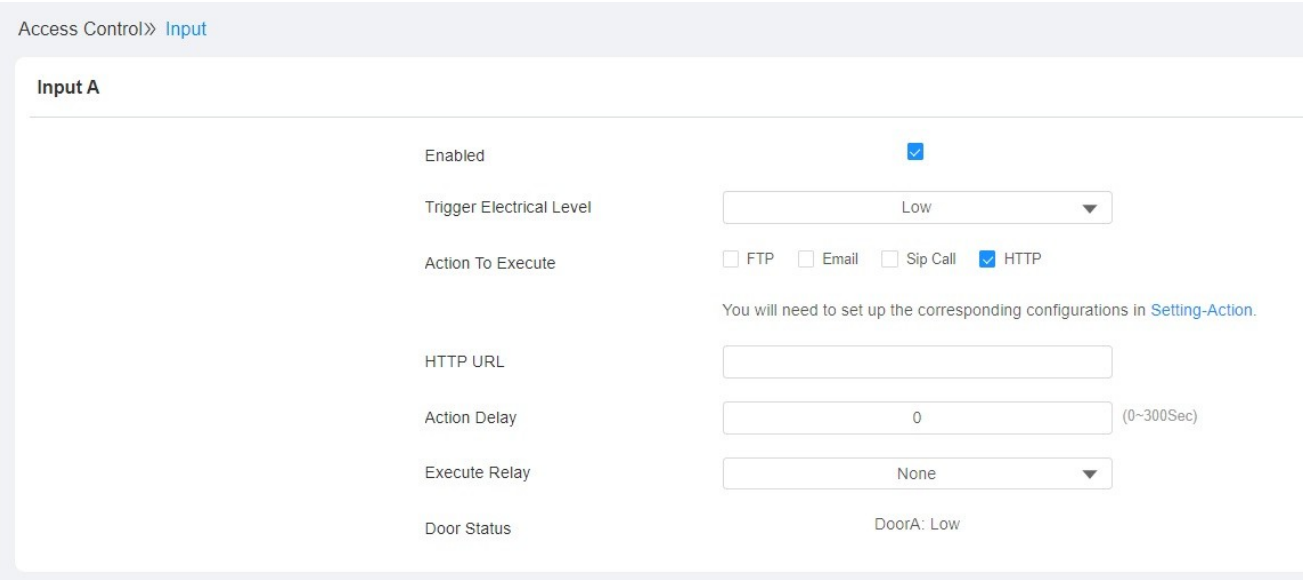
Uwaga

- Funkcja powinna działać z Akuvox SmartPlus. Aby uzyskać więcej informacji, prosimy skontaktować się z pomocą techniczną Akuvox.

Konfiguracja przycisku wyjścia do odblokowywania drzwi

Gdy konieczne jest otwarcie drzwi od wewnątrz za pomocą przycisku wyjścia zainstalowanego przy drzwiach, można skonfigurować wejście domofonowe tak, aby wyzwalało przekaźnik dostępu do drzwi.

Aby skonfigurować konfigurację w sieci Web **Access Control > Input > Input** interface.



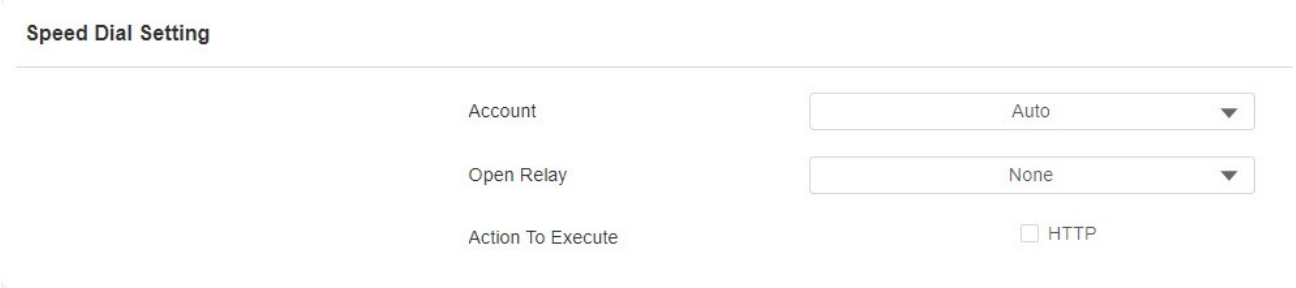
Konfiguracja parametrów :

- **Poziom wyzwalania** elektrycznego: wybierz opcje poziomu wyzwalania elektrycznego między **wysokim** i **niskim** zgodnie z rzeczywistym działaniem przycisku wyjścia.
- **Action to Execute** : wybierz metodę wykonania akcji spośród czterech opcji: **FTP, Email, HTTP** i **SIP Call**.
- **HTTP URL** : wprowadź adres URL, jeśli wybierzesz HTTP do wykonania akcji.
- **Action Delay (Opóźnienie akcji)**: ustawienie czasu opóźnienia wykonania akcji. Na przykład, jeśli ustawisz czas opóźnienia działania na 5 sekund, odpowiednie działania zostaną wykonane 5 minut po naciśnięciu przycisku.
- **Execute Relay**: konfigurowanie przekaźników wyzwalanych przez wejście.

Konfiguracja karty odbioru dla odblokowywania drzwi

Przycisk Recepcja to zakładka na ekranie głównym, która umożliwia mieszkańcom i gościom kontakt z recepcjonistą lub ochroniarzem budynku. Mogą oni dotknąć tego przycisku, aby poprosić o pomoc lub dostęp do drzwi.

Aby skonfigurować konfigurację w sieci Web, wybierz kolejno opcje **Ustawienia > Klawisze/Wyświetlacz > Ustawienia szybkiego wybierania** .

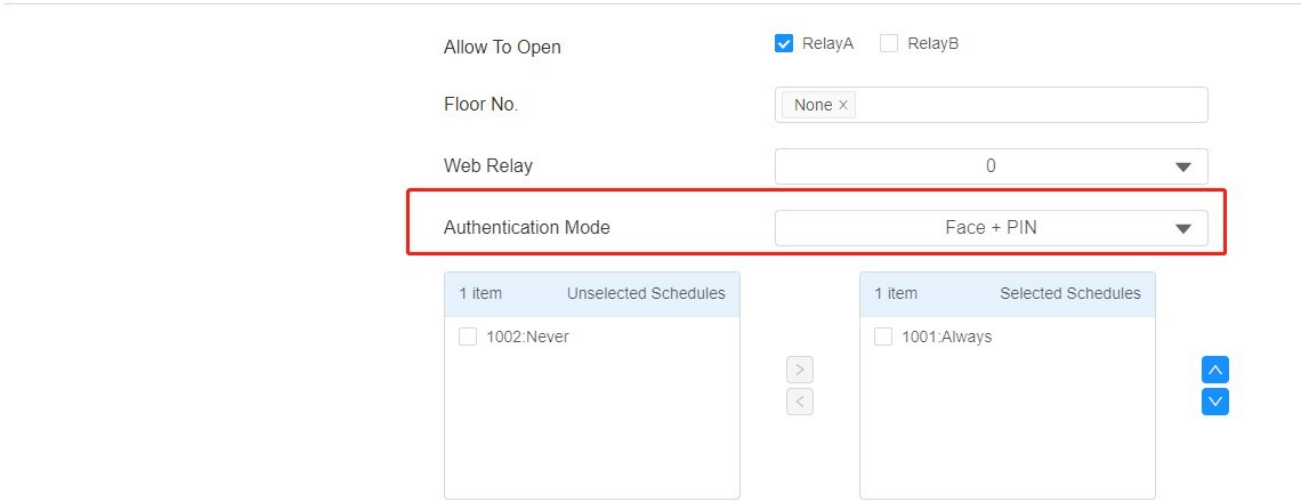


Konfiguracja parametrów :

- **Konto**: wybierz konto, z którego chcesz wykonać połączenie.
- **Open Relay (Otwórz przekaźnik)**: wybierz przekaźnik(i), które mają zostać wyzwolone, naciskając ikonę **odbioru.** • **Action To Execute**: zaznacz pole wyboru, aby włączyć opcję HTTP.
- **HTTP URL** : wprowadź polecenie URL, które ma zostać wysłane w celu uzyskania dostępu do drzwi. Na przykład: http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Uwierzytelnianie wejścia przez drzwi

Dostęp do drzwi można uzyskać poprzez pojedyncze lub podwójne uwierzytelnienie. Dla większego bezpieczeństwa można skonfigurować podwójne uwierzytelnianie. Aby ją skonfigurować, przejdź do opcji **Katalog > Użytkownik**, kliknij przycisk **+Dodaj** , a następnie przewiń w dół do opcji **Ustawienia dostępu** .



Konfiguracja parametrów :

- **Authentication Mode (Tryb uwierzytelniania)**: wybierz tryb uwierzytelniania dostępu do drzwi (**Any Method (Dowolna metoda), Face+PIN (Twarz+PIN), Face+RF**

Card (**Twarz+karta RF)** i **RF Card+PIN (Karta RF+PIN)**). W przypadku wybrania opcji **Dowolna metoda** można uzyskać dostęp do drzwi przy użyciu dowolnej z ustawionych metod dostępu (pojedynczej metody).

uwierzytelnianie). W przypadku wybrania jednego z trybów podwójnego uwierzytelniania, takiego jak **Face+PIN**, wymagane jest przejście zarówno uwierzytelniania za pomocą twarzy, jak i kodu PIN w celu otwarcia drzwi.

Bezpieczeństwo

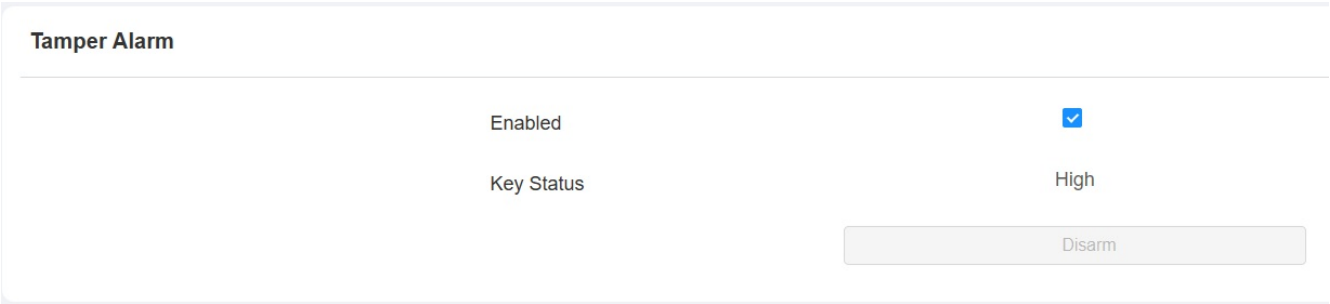
Ustawienie alarmu sabotażowego

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

Konfiguracja alarmu sabotażowego w sieci Web urządzenia

W interfejsie internetowym można dostosować alarm sabotażowy i ustawienia czujnika.

Aby skonfigurować konfigurację w interfejsie sieci Web **System > Security > Tamper Alarm.**



Konfiguracja parametrów :

- **Stan klucza**: alarm sabotażowy nie zostanie wyzwolony, jeśli stan klucza nie zostanie zmieniony z **niskiego** na **wysoki.**

Adres URL akcji

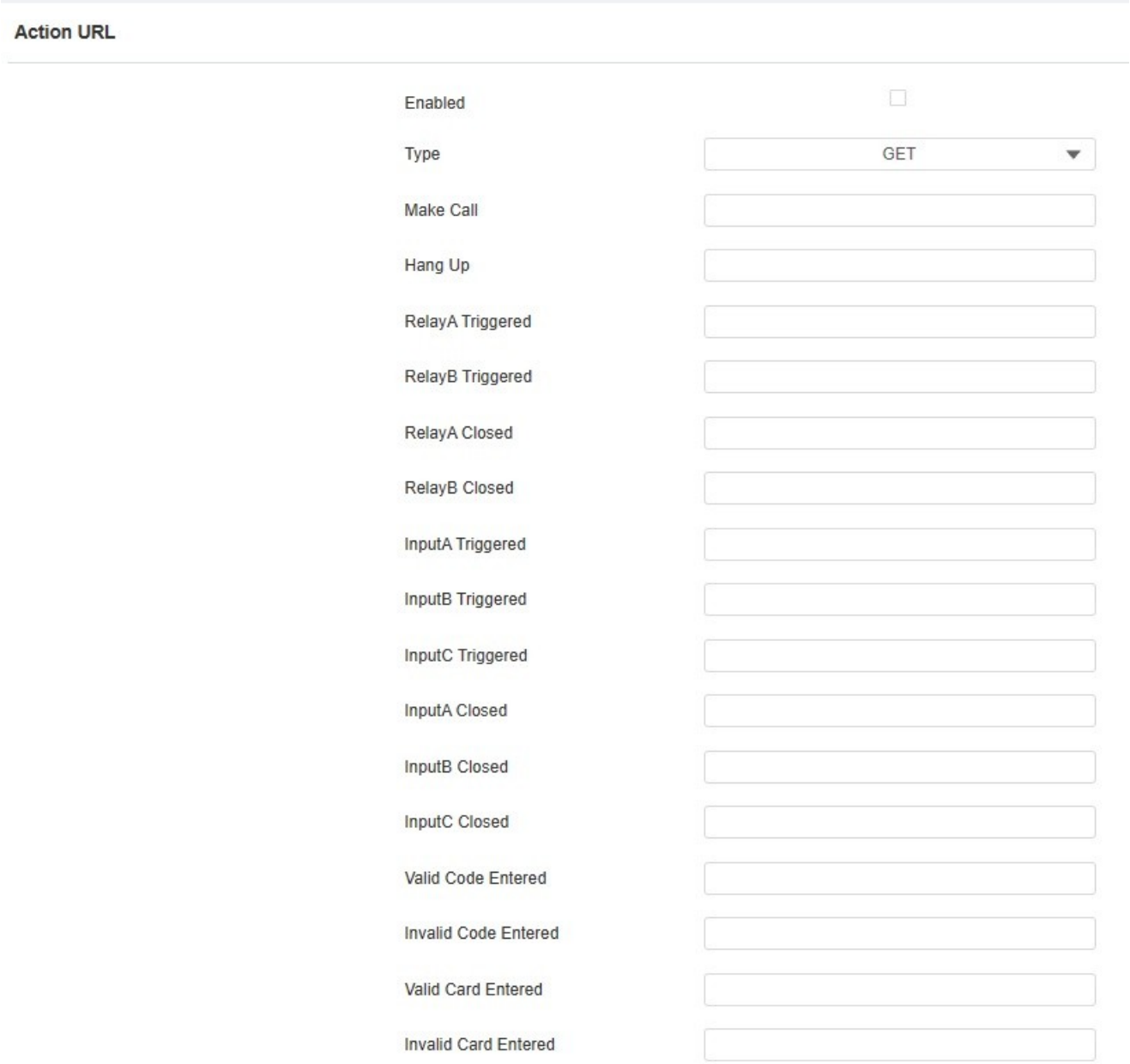
Za pomocą urządzenia można wysyłać określone polecenia HTTP URL do serwera HTTP w celu wykonania określonych działań. Działania te będą wyzwalane, gdy zmieni się stan przekaźnika, stan wejścia, kod PIN lub dostęp do karty RF.

Akuvox Action URL:

Nie	Wydarzenie	Format parametrów	Przykład
1	Wykonaj połączenie	$remote	Http://server ip/ Callnumber=$remote
2	Rozłącz się	$remote	Http://server ip/ Callnumber=$remote
3	Przekaźnik wyzwolony	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Przekaźnik zamknięty	$relay1status	Http://server ip/ relayclose=$relay1status
5	Wejście wyzwalane	$input1status	Http://server ip/ inputtrigger=$input1status
6	Wejście zamknięte	$input1status	Http://server ip/ inputclose=$input1status
7	Wprowadzony prawidłowy kod	$code	Http://server ip/ validcode=$code
8	Wprowadzono nieprawidłowy kod	$code	Http://server ip/ invalidcode=$code
9	Wprowadzona ważna karta	$card_sn	Http://server ip/ validcard=$card_sn
10	Wprowadzono nieprawidłową kartę	$card_sn	Http://server ip/ invalidcard=$card_sn
11	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

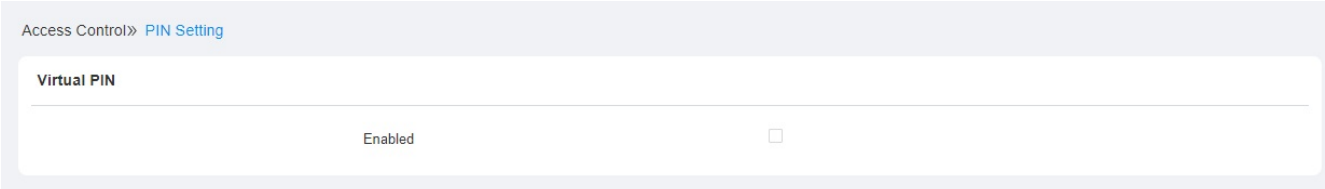
Możesz przejść do **Ustawienia > URL akcji** .



Wirtualny kod PIN

Wirtualny kod PIN pozwala chronić kod PIN przed wyciekiem do innej osoby.

Aby włączyć funkcję wirtualnego kodu PIN, przejdź do opcji **Kontrola dostępu > Ustawienia kodu PIN > Wirtualny kod PIN.**



Konfiguracja parametrów :

- **Enabled (Włączone)**: jeśli opcja ta jest włączona, użytkownik może umieszczać fałszywe liczby po obu stronach kodu PIN w celu jego ochrony. Na przykład, jeśli twoje hasło to 1234567, możesz umieścić 99 i 88 po obu stronach **(99123456788**). Wirtualne hasło jest dopasowywane do użytkowników na podstawie liczby pasujących cyfr. Na przykład, jeśli użytkownik A ma większą liczbę cyfr pasujących do wprowadzonego hasła wirtualnego niż użytkownik B, zostanie ono uznane za hasło użytkownika A. Jednak w przypadku zastosowania podwójnego uwierzytelniania, wirtualne hasło zostanie dopasowane do użytkowników, którzy przejdą pierwszy poziom uwierzytelniania, na przykład Face + PIN.

Uwaga

- Ta funkcja nie jest używana w przypadku publicznych kodów PIN i Apartment+PIN.

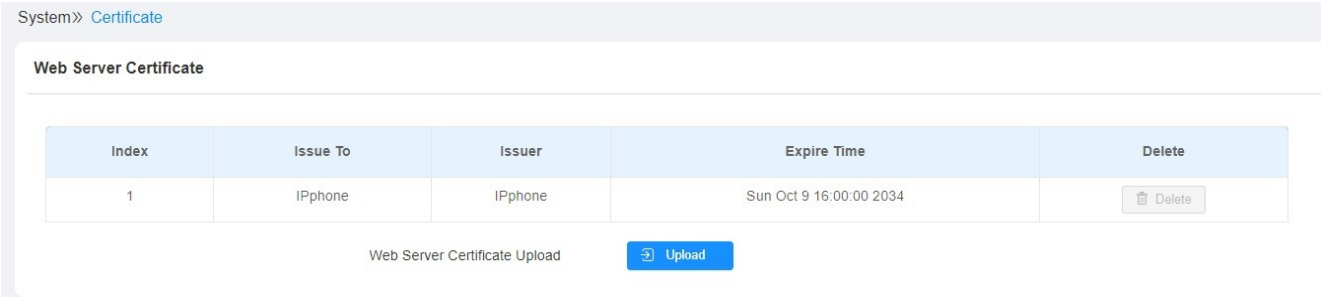
Ustawienia certyfikatu klienta

Certyfikaty zapewniają integralność komunikacji i prywatność. Aby korzystać z protokołu SSL, należy przesłać odpowiednie certyfikaty do weryfikacji.

Certyfikat serwera WWW

Jest to certyfikat wysyłany do klienta w celu uwierzytelnienia, gdy klient żąda połączenia SSL z bramofonem Akuvox. Bramofon Akuvox akceptuje tylko certyfikaty w formacie pliku *.PEM.

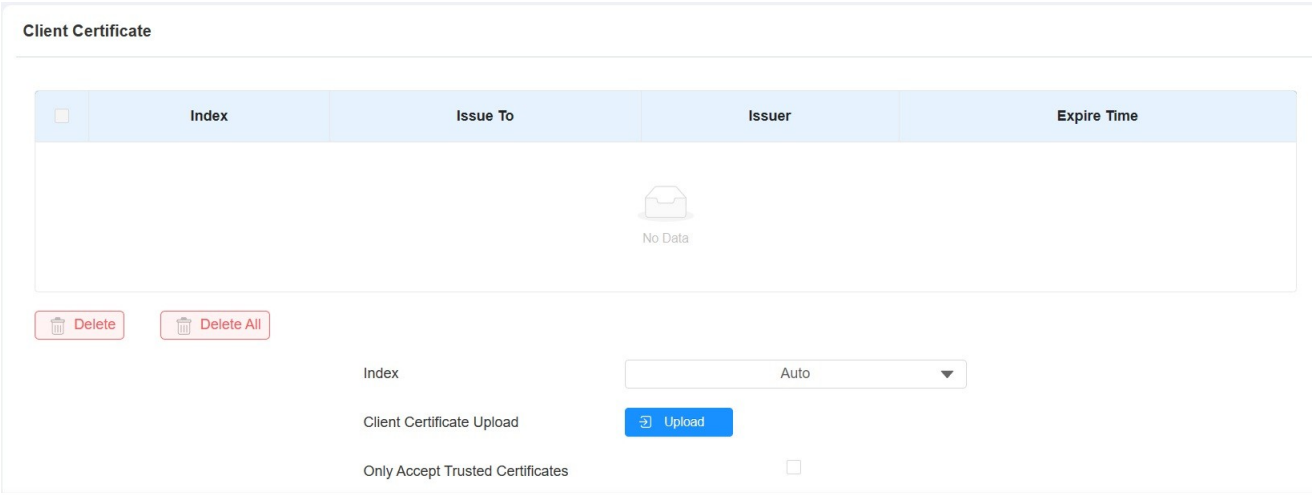
Aby przesłać certyfikat serwera WWW na urządzenie, należy kliknąć **System > Certyfikat > Certyfikat serwera WWW**.



Certyfikat klienta

Ten certyfikat weryfikuje serwer dla telefonu bramowego Akuvox, gdy chcą połączyć się przy użyciu protokołu SSL. Bramofon weryfikuje certyfikat serwera z listą certyfikatów klienta.

Aby przesłać i skonfigurować certyfikaty klienta na tej samej stronie.



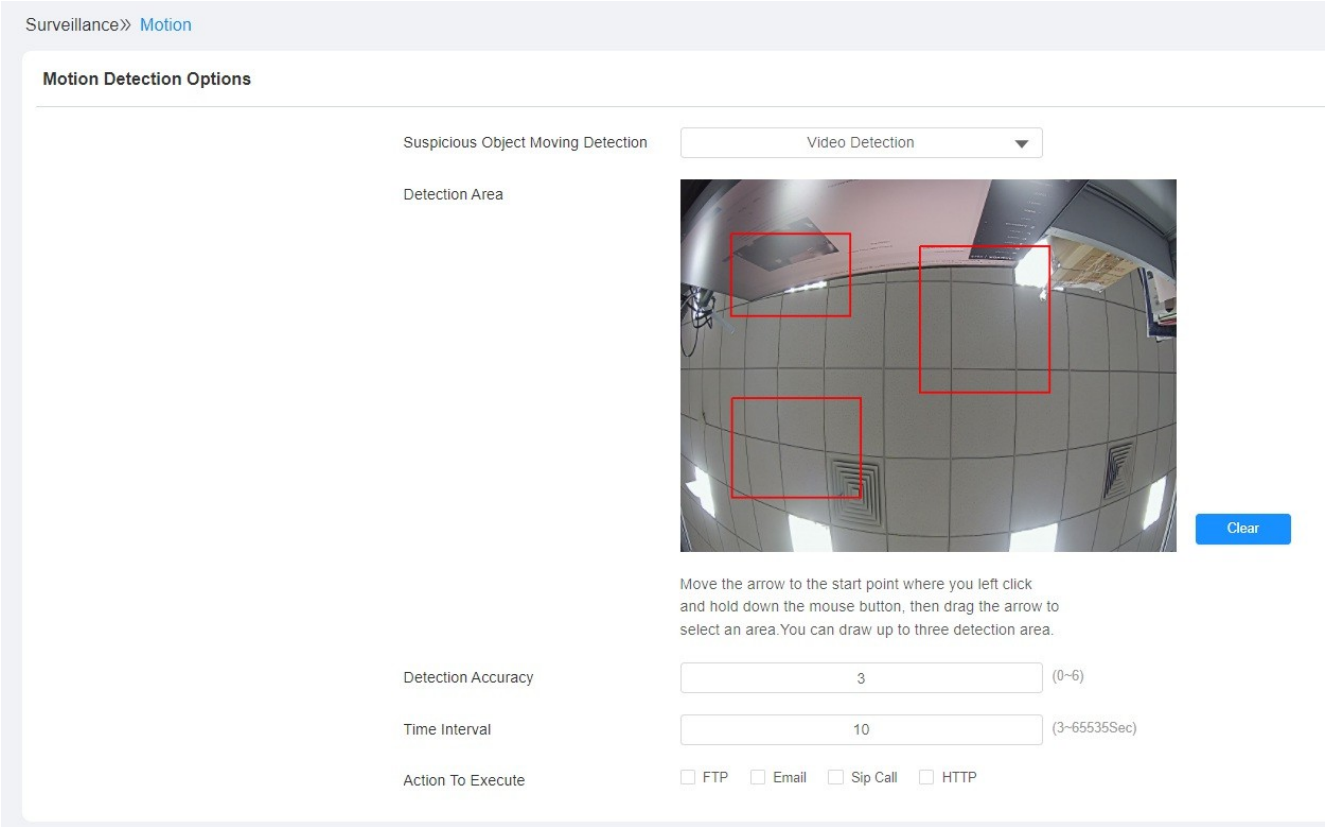
Konfiguracja parametrów :

- **Indeks**: wybierz żądaną wartość z rozwijanej listy Indeks. W przypadku wybrania wartości **Auto** przesłany certyfikat zostanie wyświetlony w kolejności numerycznej. W przypadku wybrania wartości od **1 do 10** przesłane certyfikaty będą wyświetlane zgodnie z wartością wybraną przez użytkownika.
- **Client Certificate Upload**: zlokalizuj i prześlij żądany certyfikat (tylko *.pem).
- **Tylko akceptuj zaufane certyfikaty**: w przypadku wybrania opcji **Włączone** telefon będzie weryfikował certyfikat serwera na podstawie listy certyfikatów klienta, o ile uwierzytelnianie się powiedzie. W przypadku wybrania opcji **Disabled** (**Wyłączone)** telefon nie będzie weryfikował certyfikatu serwera bez względu na to, czy certyfikat jest ważny, czy nie.

Wykrywanie ruchu

Detekcja ruchu to funkcja umożliwiająca nienadzorowany nadzór wideo i automatyczne alarmy. Wykrywa ona wszelkie zmiany w obrazie zarejestrowanym przez kamerę, takie jak przejście osoby lub poruszenie obiektywu, i aktywuje system w celu wykonania odpowiedniej akcji.

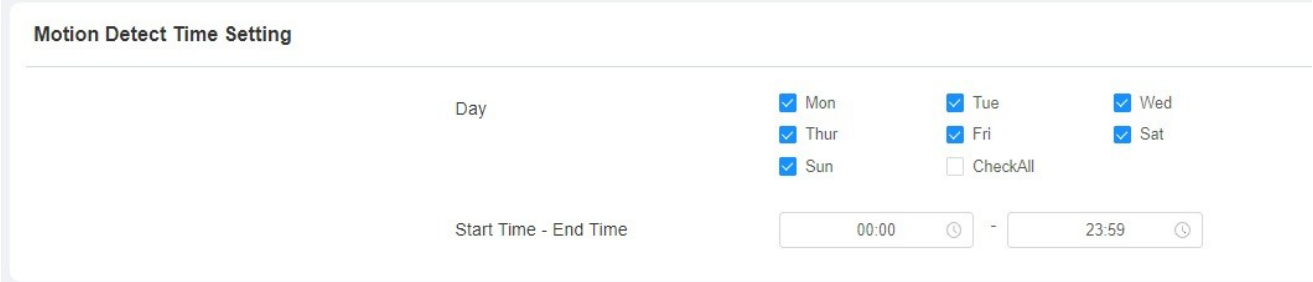
Aby skonfigurować wykrywanie ruchu, przejdź do **Surveillance > Motion > Motion Detection Options** .



Konfiguracja parametrów :

- **Wykrywanie podejrzanych ruchomych obiektów**: wybierz spośród opcji **Wykrywanie wideo, Wykrywanie podczerwieni** i **Wyłączone** . Wykrywanie podczerwieni opiera się na wykrywaniu promieniowania podczerwonego emitowanego lub odbijanego przez obiekty, podczas gdy wykrywanie wideo koncentruje się na analizie informacji wizualnych przechwyconych przez kamery.
- **Obszar detekcji** : wybór obszaru detekcji na obrazie wideo. Można wybrać maksymalnie trzy obszary detekcji.
- **Interwał** czasowy: ustaw interwał czasowy w taki sam sposób, jak na urządzeniu.
- **Dokładność wykrywania**: ustawienie dokładności wykrywania dla czułości wykrywania. Im wyższa wartość, tym większa czułość. Domyślna wartość dokładności wykrywania to **3** .
- **Akcja do wykonania**: wybierz typ powiadomienia: FTP**, Email, HTTP, SIP Call**. Jeśli wybierzesz **FTP** , powiadomienie FTP zostanie wysłane na wskazany serwer. Jeśli wybierzesz **Email**, powiadomienie zostanie wysłane w formie wiadomości e-mail po wyzwoleniu detekcji ruchu.

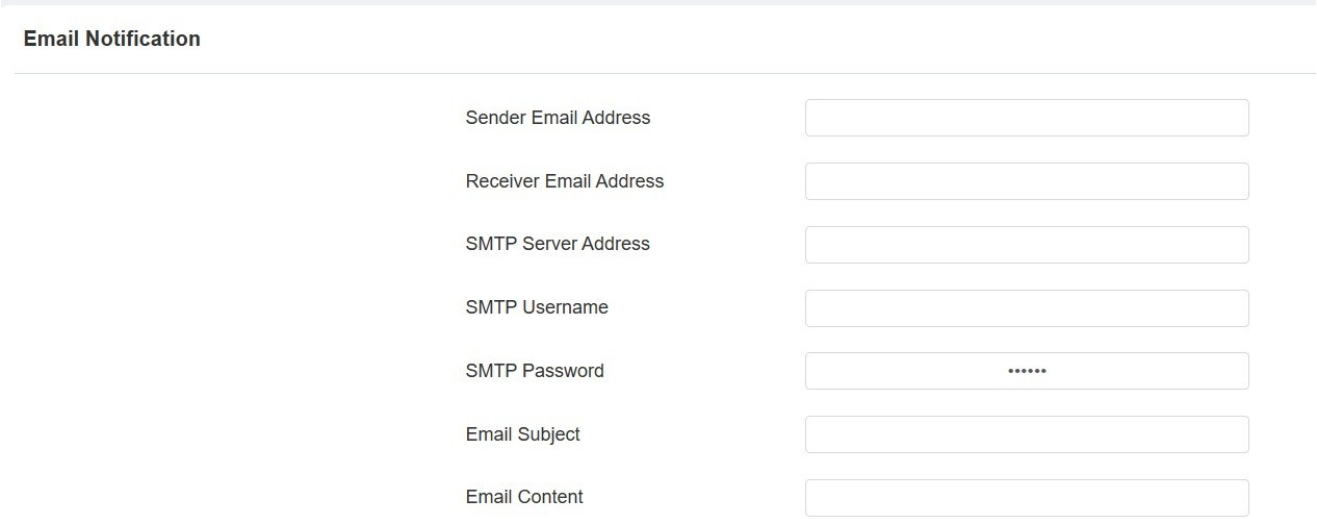
Przewijając stronę w dół, można również ustawić harmonogram wykrywania ruchu.



Ustawienia powiadomień bezpieczeństwa

Ustawienia powiadomień e-mail

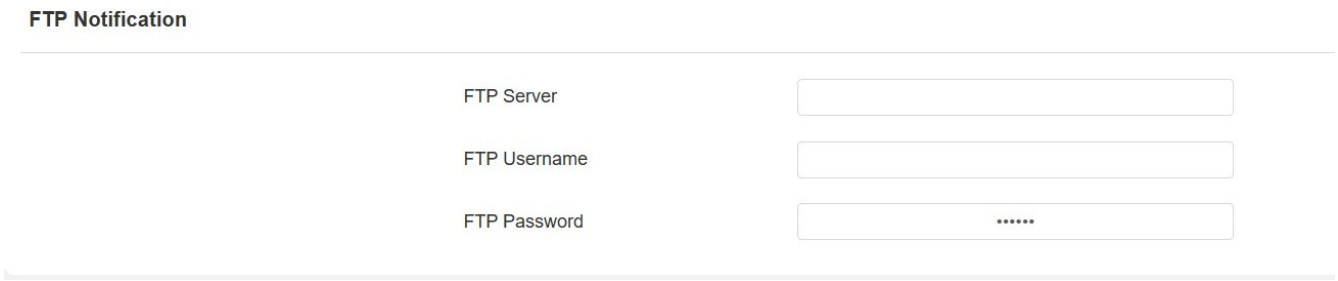
Skonfiguruj powiadomienia e-mail, aby otrzymywać zrzuty ekranu nietypowych ruchów z bramofonu. Przejdź do interfejsu **Setting > Action > Email Notification.**



Ustawienia powiadomień FTP

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

Przejdź do opcji **Ustawienia > Akcja >** Interfejs **powiadomień FTP.**



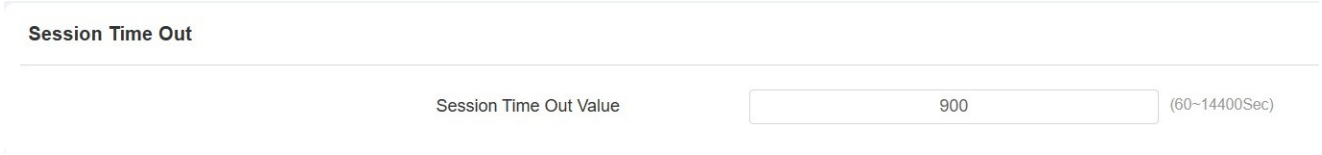
Konfiguracja parametrów :

- **Serwer FTP**: wprowadź adres (URL) serwera FTP dla powiadomienia FTP.

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.

Aby skonfigurować konfigurację w interfejsie sieci Web **System > Security > Session Time Out.**



Konfiguracja parametrów :

- **Session Time Out Value**: ustawienie czasu automatycznego wylogowania interfejsu sieciowego w zakresie od 60 sekund do 14400 sekund. Wartość domyślna to 900.

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. Bramofony 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 strumienia na żywo.

RTSP to skrót od Real Time Streaming Protocol. Może on być używany do strumieniowego przesyłania obrazu i dźwięku z kamer innych firm do bramofonu. Można dodać strumień z kamery, dodając jej adres URL.

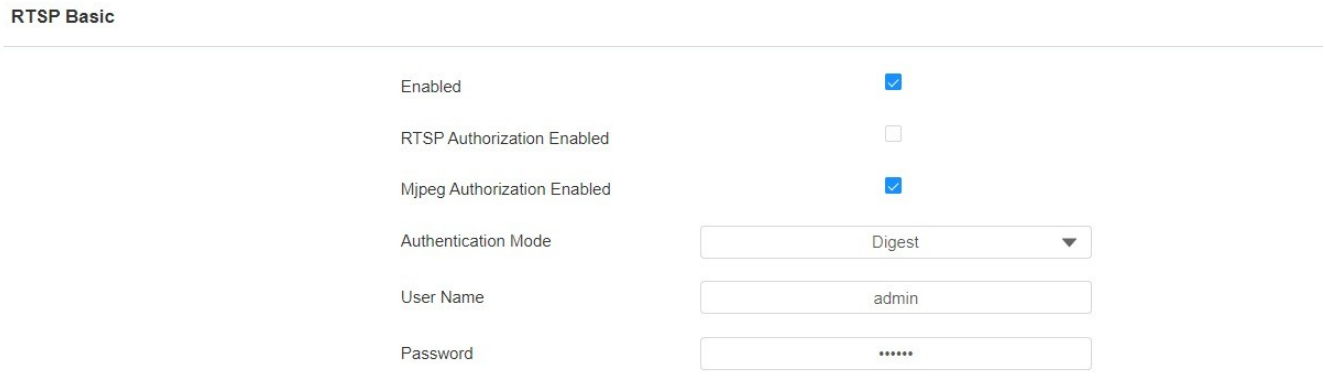
ONVIF to Open Network Video Interface Forum. Umożliwia on bramofonowi skanowanie i wykrywanie kamer lub urządzeń domofonowych z aktywowanymi funkcjami ONVIF. Strumienie na żywo uzyskiwane za pośrednictwem ONVIF są zasadniczo w formacie RTSP.

Monitorowanie strumienia RTSP

Możesz użyć RTSP do oglądania strumienia wideo na żywo z innych urządzeń domofonowych na bramofonie.

Podstawowe ustawienia RTSP

Aby skonfigurować konfigurację w interfejsie internetowym **Surveillance > RTSP > RTSP Basic.**



Konfiguracja parametrów :

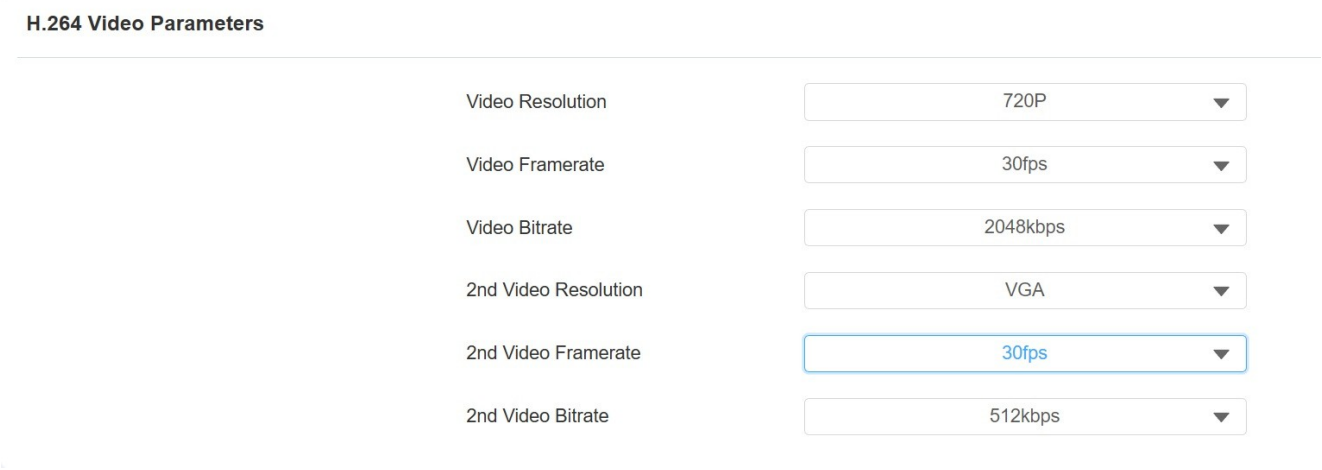
- **RTSP Authorization Enabled** : włączenie autoryzacji RTSP. Po włączeniu autoryzacji RTSP wymagane jest wprowadzenie typu uwierzytelniania RTSP, nazwy użytkownika RTSP i hasła RTSP na urządzeniu interkomowym, takim jak monitor wewnętrzny, w celu autoryzacji.

- **Tryb uwierzytelniania**: wybierz typ uwierzytelniania RTSP pomiędzy **Basic** i **Digest. Basic** jest domyślnym typem 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 parametry kodeka H.264 w interfejsie internetowym **Surveillance > RTSP > H.264 Video Parameters.**



Konfiguracja parametrów :

- **Rozdzielczość wideo**: wybór rozdzielczości wideo spośród siedmiu opcji: **"QCIF", "QVGA", "CIF", "VGA", "4CIF", "720P"** i "**1080P** ". Domyślną rozdzielczością wideo jest "**720P"**. Jeśli rozdzielczość zostanie ustawiona na wyższą niż "**720P"**, wideo z bramofonu może nie być wyświetlane na monitorze wewnętrznym.
- **Częstotliwość klatek wideo**: "**25 klatek na sekundę**" to domyślna częstotliwość klatek wideo.
- **Szybkość transmisji wideo**: wybierz szybkość transmisji wideo spośród sześciu opcji: "**128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs" w** zależności od środowiska sieciowego. Domyślną szybkością transmisji wideo jest "**2048 kpbs**".
- **2 nd Video Resolution**: wybór rozdzielczości wideo dla drugiego kanału strumienia wideo. Domyślną rozdzielczością wideo jest "**VGA**".
- **2 nd Video Framerate** : wybierz liczbę klatek na sekundę dla drugiego kanału strumienia wideo. "**30 klatek na sekundę**" to domyślna liczba klatek na sekundę dla drugiego kanału strumienia wideo.
- **2 nd Video Bitrate** : wybierz bitrate wideo spośród sześciu opcji dla drugiego kanału strumienia wideo. Drugi kanał strumienia wideo ma domyślnie wartość "**512 kpbs**".

Uwaga

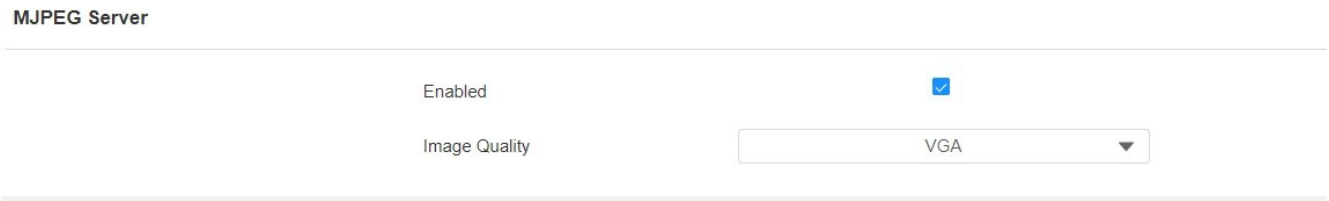
- X912 posiada dwa kanały strumieniowania wideo RTSP w dwóch formatach.

Na przykład:
Kanał 1: rtsp://192.168.1.40/live/ch00_0.
Kanał 2: rtsp://192.168.1.40/live/ch00_1.

Przechwytywanie obrazu MJPEG

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

Przejdź do opcji **Nadzór >** Interfejs **MJPEG.**



Konfiguracja parametrów :

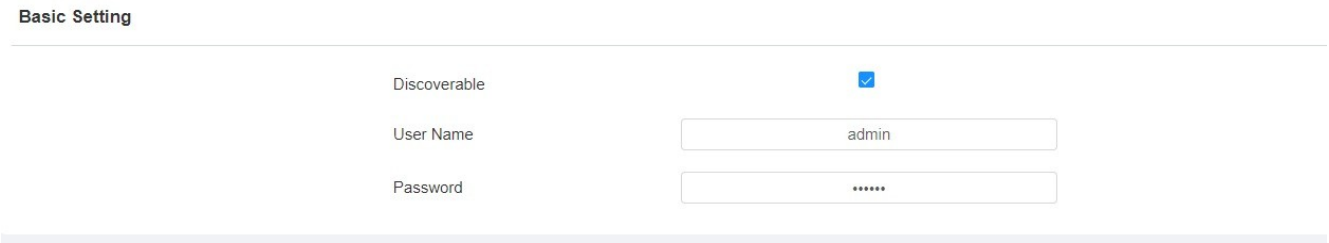
- **Jakość obrazu**: wybór jakości przechwytywanego obrazu spośród sześciu opcji: **QCIF, QVGA, CIF, VGA, 4CIF, 720P** ,
  Po włączeniu usługi MJPEG można przechwytywać obraz z telefonu przy użyciu następujących trzech typów formatu URL:
- http:// urządzenie ip:8080/picture.cgi
- http://device ip:8080/picture.jpg
- http://device ip:8080/jpeg.cgi

Na przykład, jeśli chcesz przechwycić obraz w formacie JPG z bramofonu o adresie IP: 192.168.1.104, można wpisać "http://192.168.1.104:8080/picture.jpg" w przeglądarce internetowej.

ONVIF

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

Aby skonfigurować konfigurację w interfejsie Web **Surveillance > ONVIF.**



Konfiguracja parametrów :

- **Discoverable** : zaznacz pole wyboru, aby włączyć tryb Discoverable ONVIF. Po wybraniu opcji "**Discoverable** " wideo z kamery telefonu może być wyszukiwane przez inne urządzenia.
- **Nazwa użytkownika** : wprowadź nazwę użytkownika. Domyślna nazwa użytkownika to "**admin**". • **Hasło** : wprowadź hasło. Domyślne hasło to "**admin**".

  Po zakończeniu ustawień można wprowadzić adres URL ONVIF na urządzeniu innej firmy, aby wyświetlić strumień wideo.

Na przykład: **http://IP address:80/onvif/device_service**

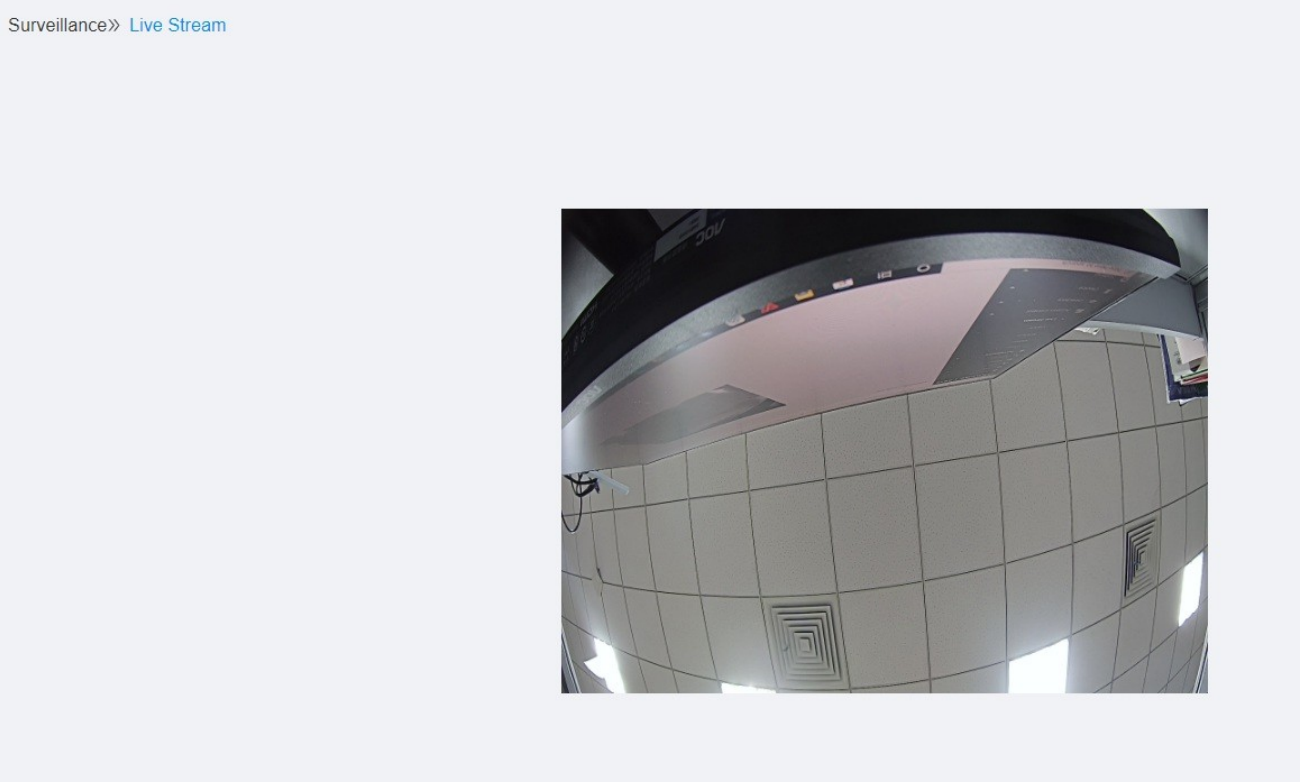
Uwaga:

- Wpisz konkretny adres IP telefonu w adresie URL.

Transmisja na żywo

Istnieją dwa sposoby sprawdzania obrazu wideo w czasie rzeczywistym z bramofonu. 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.

Aby wyświetlić wideo w czasie rzeczywistym w interfejsie internetowym **Surveillance > Live Stream.**

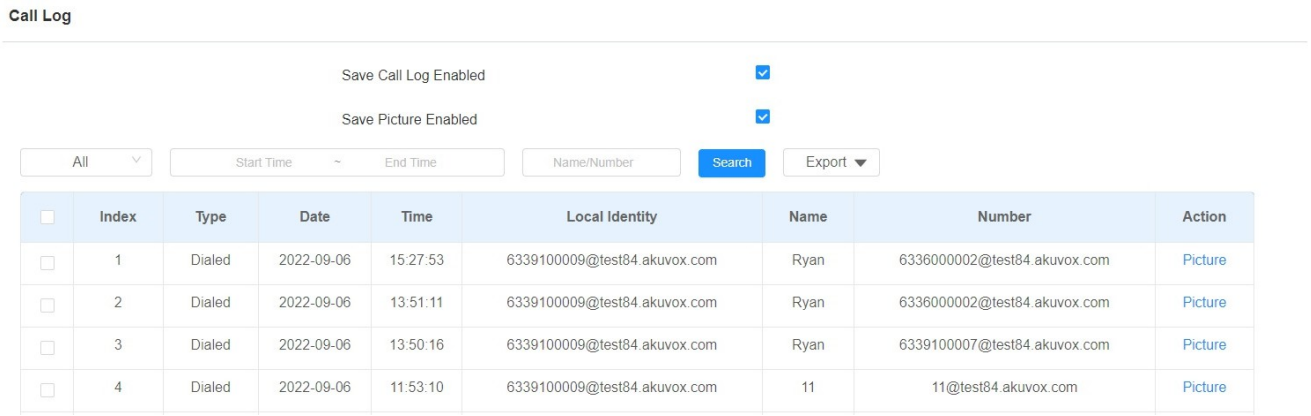


Dzienniki

Dzienniki połączeń

Jeśli chcesz sprawdzić połączenia, w tym połączenia wychodzące, odebrane i nieodebrane w określonym czasie, możesz sprawdzić i przeszukać rejestr połączeń w interfejsie internetowym urządzenia, a w razie potrzeby wyeksportować rejestr połączeń z urządzenia.

Aby sprawdzić rejestr połączeń w interfejsie sieci Web **Status > Call Log.**



Index	Type	Date	Time	Local Identity	Name	Number	Action
1	Dialed	2022-09-06	15:27:53	6339100009@test84.akuvox.com	Ryan	6336000002@test84.akuvox.com	Picture
2	Dialed	2022-09-06	13:51:11	6339100009@test84.akuvox.com	Ryan	6336000002@test84.akuvox.com	Picture
3	Dialed	2022-09-06	13:50:16	6339100009@test84.akuvox.com	Ryan	6339100007@test84.akuvox.com	Picture
4	Dialed	2022-09-06	11:53:10	6339100009@test84.akuvox.com	11	11@test84.akuvox.com	Picture

Konfiguracja parametrów :

- **Historia połączeń**: wybierz historię połączeń spośród czterech opcji: "**Wszystkie**", "**Wybrane** ", "**Odebrane** " i "**Nieodebrane** " dla określonego typu rejestru połączeń, który ma być wyświetlany.
- **Godzina rozpoczęcia ~ Godzina zakończenia** : wybierz określony przedział czasowy

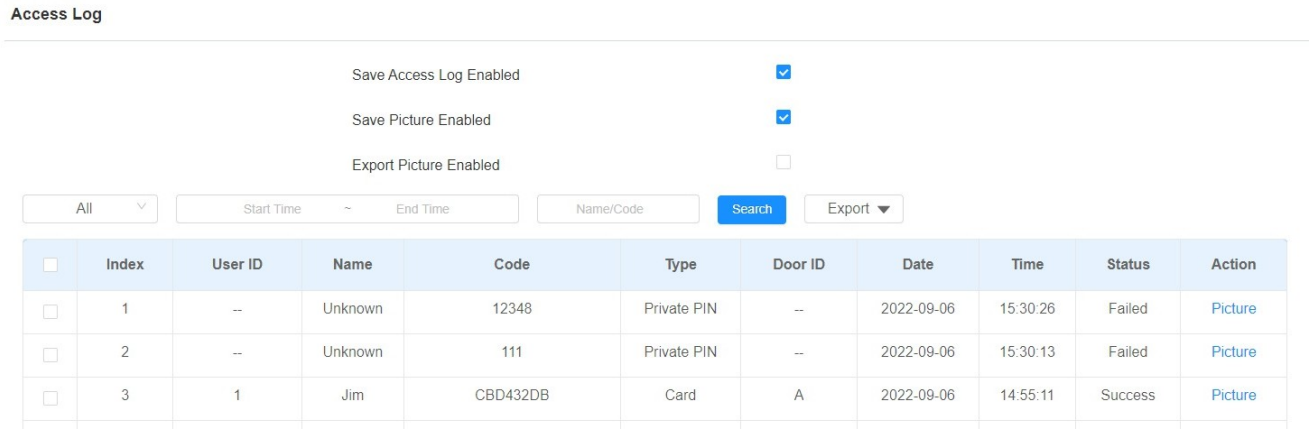
dzienników połączeń, które chcesz wyszukać, sprawdzić lub wyeksportować.

- **Nazwa/Numer**: wybierz opcje "**Nazwa**" i "**Numer**", aby przeszukiwać rejestr połączeń według nazwy lub numeru SIP lub IP.

Dzienniki drzwi

Jeśli chcesz wyszukać i sprawdzić różne rodzaje historii dostępu do drzwi, możesz wyszukać i sprawdzić dzienniki drzwi w Internecie urządzenia.

Przejdź do interfejsu **Status > Access Log.**



Konfiguracja parametrów :

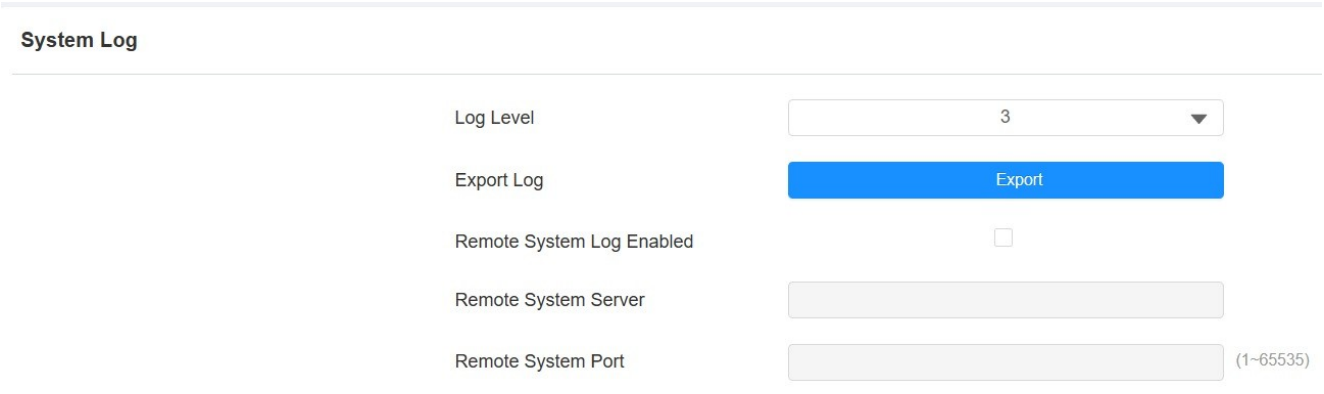
- **Status** : wybierz pomiędzy opcjami **Udany** i **Nieudany**, aby wyszukać udane lub nieudane dostępy do drzwi.
- **Nazwa/Kod** : wybierz opcje **Nazwa** i **Kod,** aby przeszukać dziennik drzwi według nazwy lub kodu PIN.

Debugowanie

Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Funkcję tę można skonfigurować w interfejsie sieci Web **System > Maintenance > System Log.**

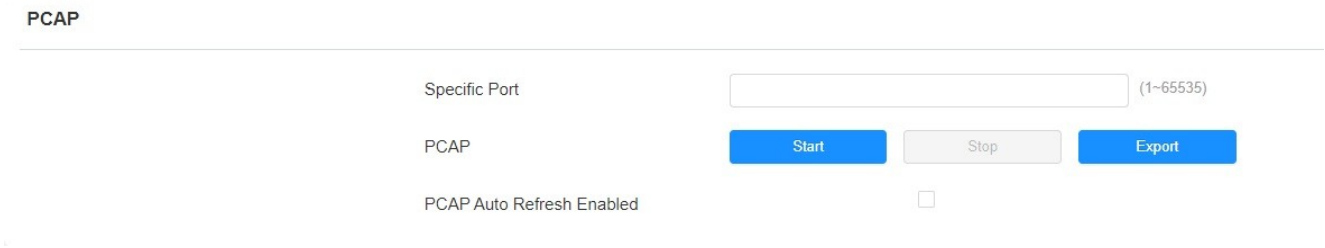


Konfiguracja parametrów :

- **Log Level (Poziom dziennika)**: wybierz poziom dziennika od 1 do 7. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić w celu 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. • **Eksportuj dziennik debugowania**: kliknij kartę **Eksportuj**, aby wyeksportować plik dziennika debugowania do komputera lokalnego.
- **Zdalny serwer systemu**: wprowadź adres zdalnego serwera, aby otrzymywać dziennik urządzenia. Adres serwera zdalnego zostanie podany przez pomoc techniczną Akuvox.

PCAP do debugowania

PCAP służy do przechwytywania pakietów danych wchodzących i wychodzących z urządzeń w celu debugowania i rozwiązywania problemów.
PCAP można skonfigurować w witrynie internetowej urządzenia **System > Konserwacja > PCAP** przed jego użyciem.

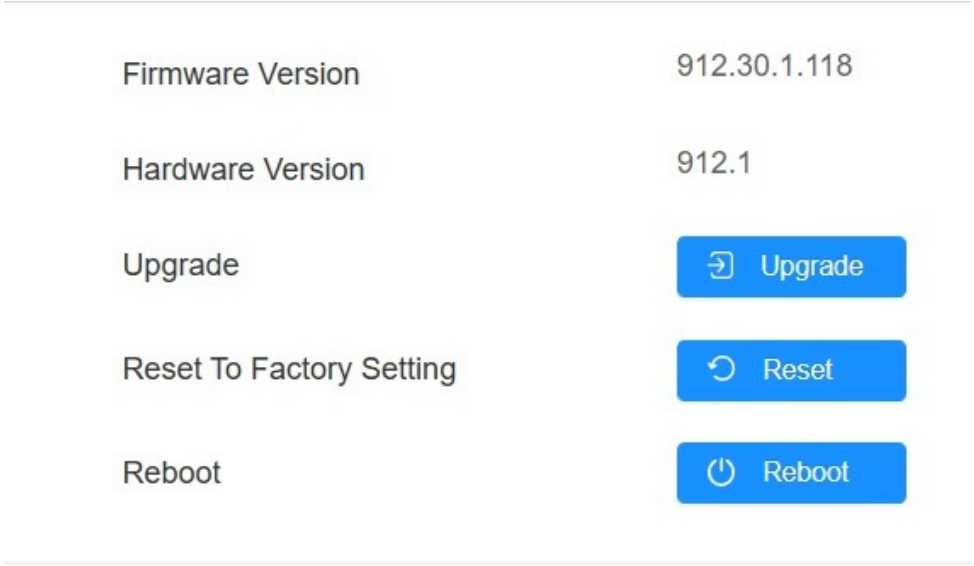


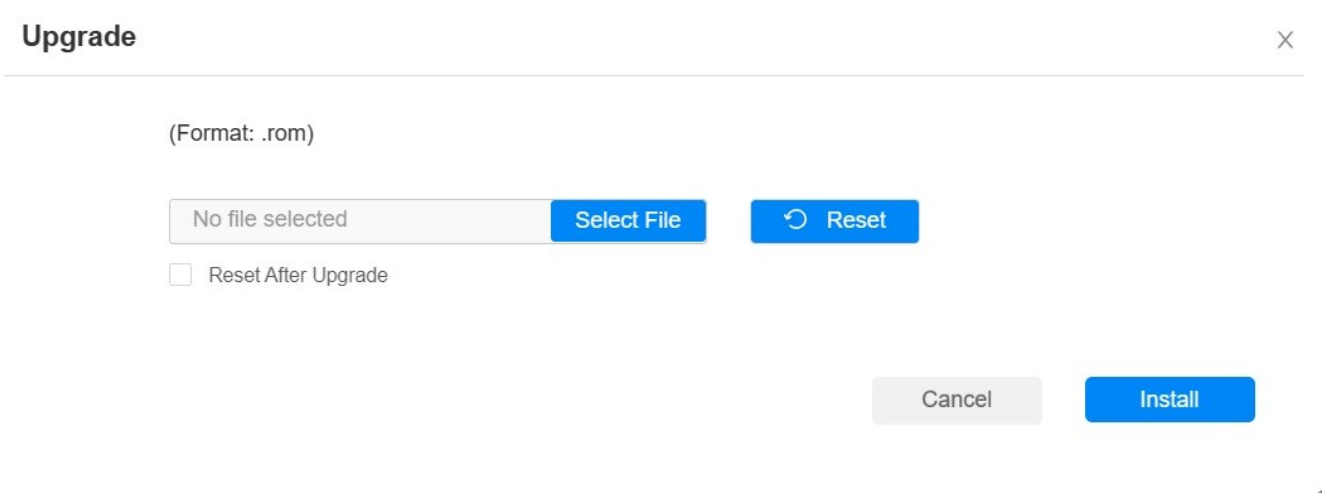
Konfiguracja parametrów :

- **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 zakładkę **Start** i zakładkę **Stop**, aby przechwycić określony zakres pakietów danych przed kliknięciem zakładki **Export**, aby wyeksportować pakiety danych do lokalnego komputera.
- **PCAP Auto Refresh**: wybierz **Enable** lub **Disable,** aby włączyć lub wyłączyć funkcję automatycznego odświeżania PCAP. Jeśli opcja ta zostanie ustawiona jako **Enable**, PCAP będzie kontynuował przechwytywanie pakietów danych nawet po osiągnięciu maksymalnej pojemności 1M pakietów danych. W przypadku ustawienia tej opcji jako **Disable**, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycony pakiet danych osiągnie maksymalną pojemność 1 MB.

Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można zaktualizować w interfejsie internetowym urządzenia. Przejdź do **System > Aktualizacja > Interfejs podstawowy.**





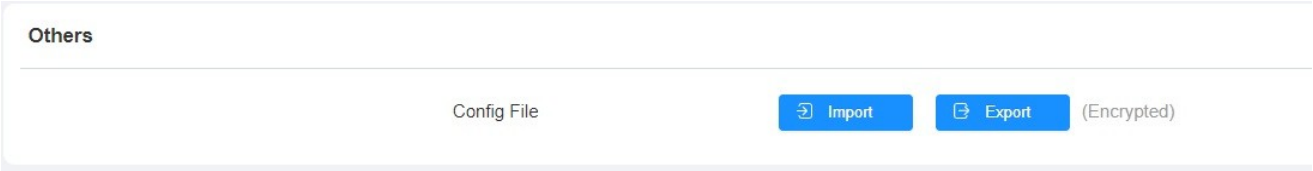
Uwaga:

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

Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować

do komputera lokalnego. Przejdź do **System > Konserwacja > Inne** .



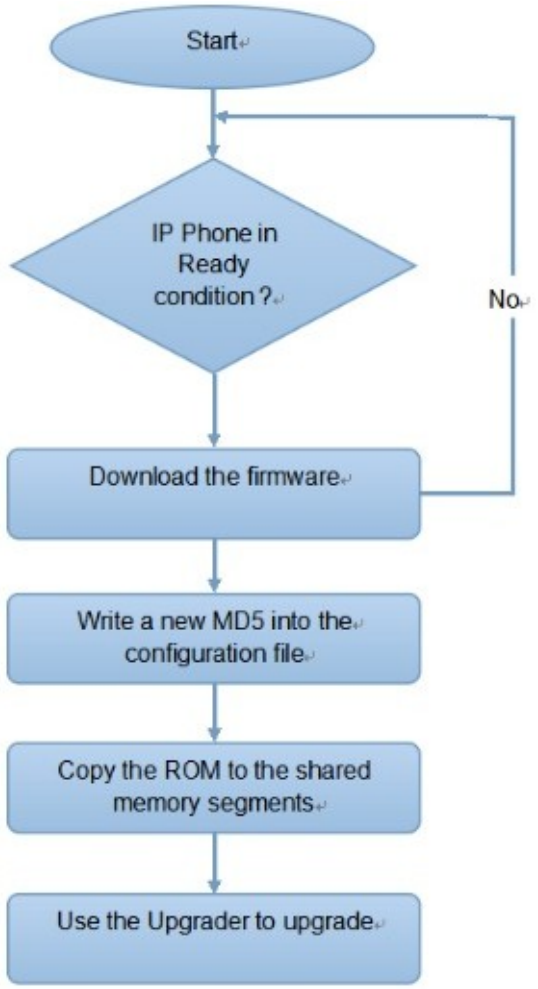
Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

Bramofon można skonfigurować i zaktualizować w interfejsie internetowym za pomocą jednorazowego automatycznego udostępniania i zaplanowanego automatycznego udostępniania za pomocą plików konfiguracyjnych, co pozwala uniknąć konieczności ręcznego konfigurowania poszczególnych ustawień w bramofonie.

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 interkomowe 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:



Pliki konfiguracyjne dla automatycznego przydzielania

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

Poniżej przedstawiono różnicę między tymi dwoma typami plików konfiguracyjnych:

- **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, takich jak 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

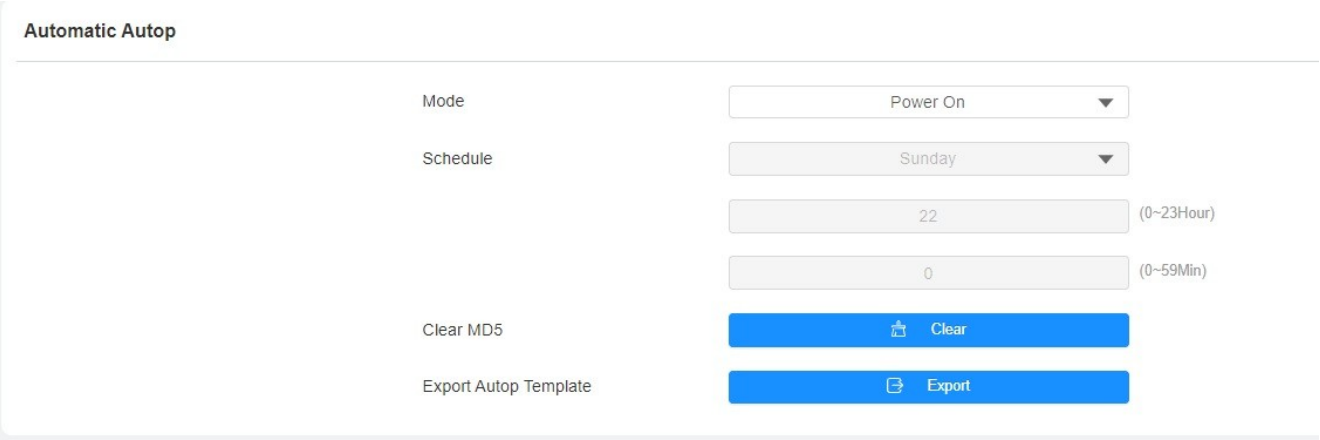
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny udostępniania wsadowego różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC dla określonego udostępniania urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer posiada te dwa typy plików konfiguracyjnych, 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 skonfigurować konfigurację w interfejsie sieci Web **System > Auto Provisioning > Automatic Autop**.



Konfiguracja parametrów :

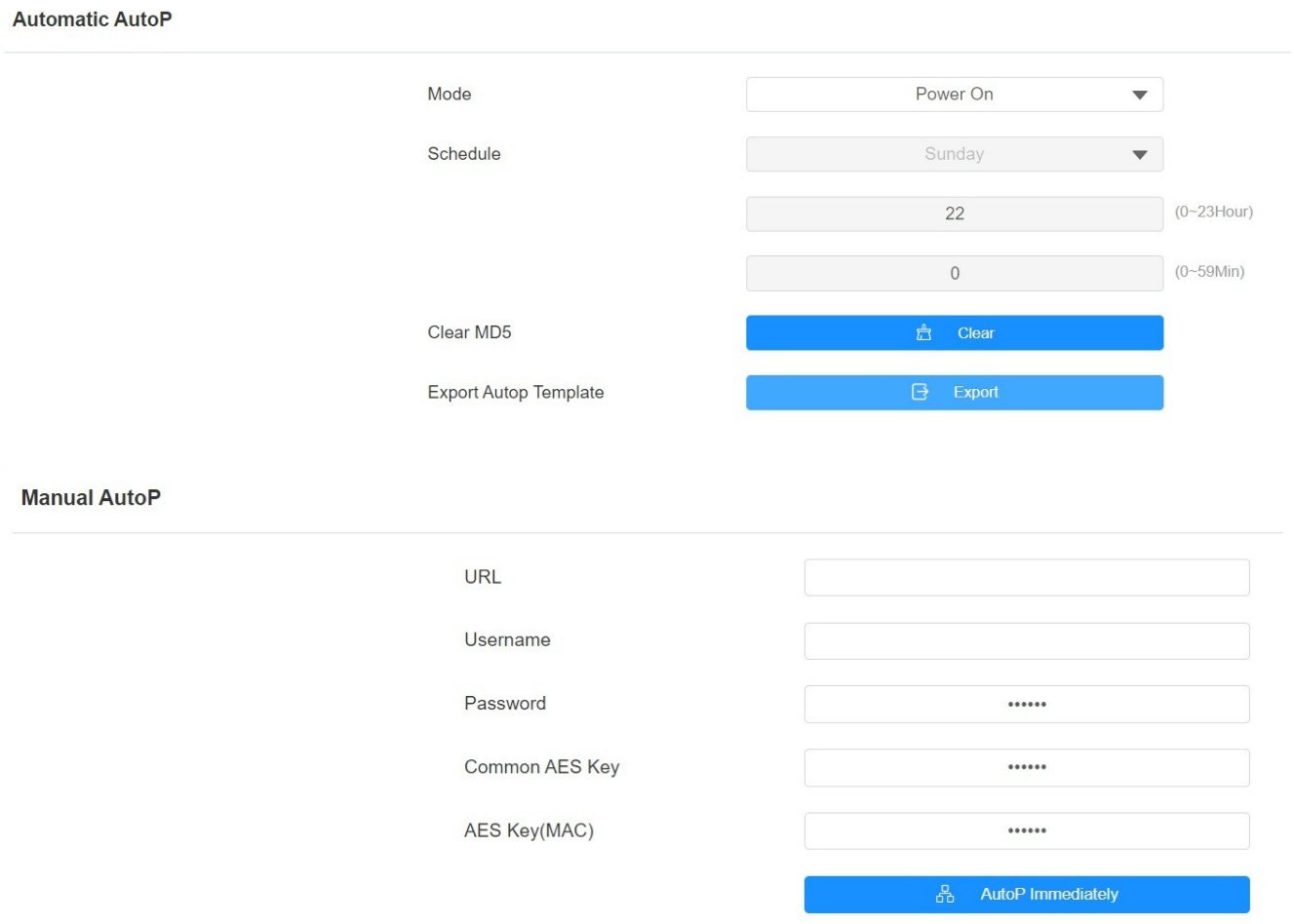
- **Tryb** :
  - **Power On**: pozwala urządzeniu na wykonanie Autop przy każdym
  - uruchomieniu. **Wielokrotnie**: umożliwia urządzeniu wykonywanie
  - automatycznego zatrzymania zgodnie z harmonogramem. **Power On + Repeatedly**: łączy tryby **Power On** i **Repeatedly**, umożliwiając urządzeniu wykonywanie Autop przy każdym uruchomieniu lub zgodnie z harmonogramem.
  - **Hourly Repeat (Powtarzanie co godzinę)**: umożliwia urządzeniu wykonywanie automatycznego zatrzymania co godzinę.
- **Harmonogram**: po wybraniu trybu **Power On** + **Repeatedly** można wybrać konkretny dzień i godzinę automatycznego włączenia.

- **Clear MD 5** : służy do porównywania istniejącego pliku autop z plikiem autop na serwerze, jeśli pliki są takie same, provisioning zostanie zatrzymany, co pozwoli uniknąć niepotrzebnego automatycznego provisioningu.

Konfiguracja udostępniania statycznego

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 pobrać szablon Autop w interfejsie **System > Auto Provisioning > Automatic Autop** i skonfigurować serwer Autop w interfejsie **System > Auto Provisioning > Manual Autop**.



Konfiguracja parametrów :

- **URL** : adres serwera TFTP, HTTP, HTTPS, lub FTP dla provisioningu.
- **Nazwa użytkownika** : ustaw nazwę użytkownika, jeśli serwer wymaga nazwy

użytkownika, aby uzyskać do niego dostęp.

- **Hasło**: ustaw hasło, jeśli serwer wymaga hasła dostępu.
- **Common AES Key**: ustawienie kodu AES dla interkomu w celu odszyfrowania ogólnego Auto Plik konfiguracyjny Provisioning.
- **Klucz AES (MAC)**: ustawienie kodu AES dla interkomu w celu odszyfrowania pliku konfiguracyjnego automatycznego udostępniania 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)

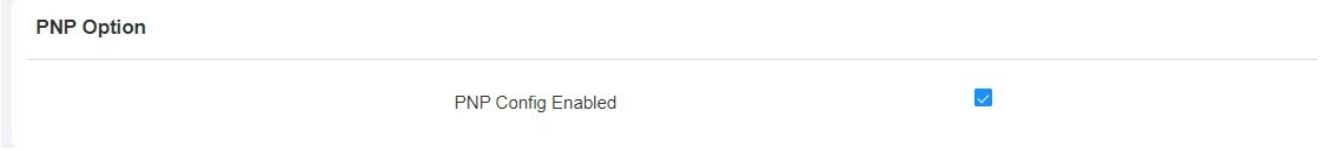
Wskazówka

- Akuvox nie zapewnia serwera określonego przez użytkownika. Prosimy o przygotowanie TFTP/FTP/HTTP/HTTPS.

Konfiguracja PNP

Plug and Play (PNP) to połączenie wsparcia sprzętowego i programowego, które umożliwia systemowi komputerowemu rozpoznawanie i dostosowywanie się do zmian konfiguracji sprzętowej przy niewielkiej lub żadnej interwencji użytkownika.

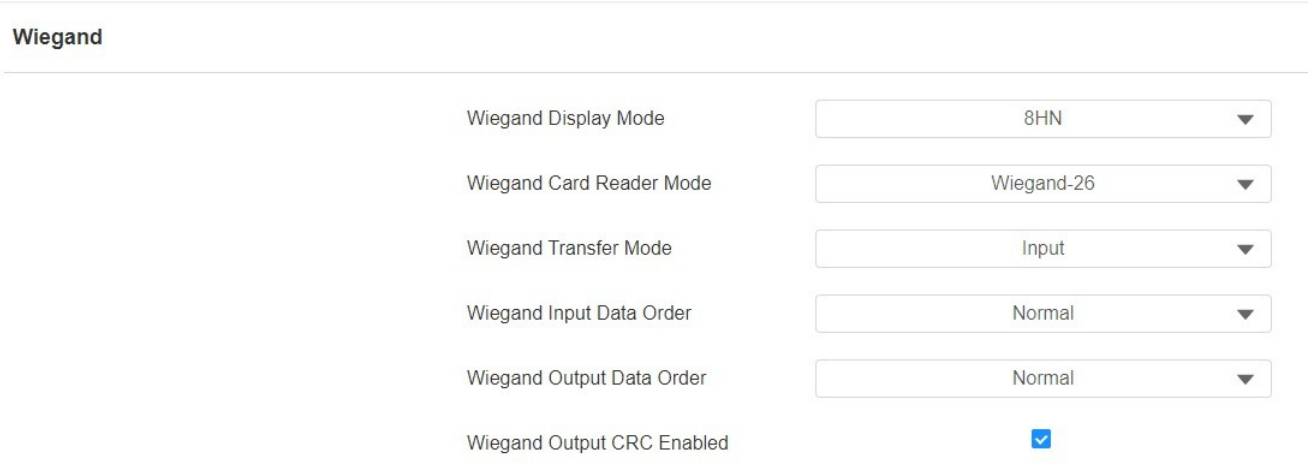
Aby skonfigurować konfigurację w interfejsie sieci Web **System > Auto Provisioning > PNP Option.**



Integracja z urządzeniami innych firm

Integracja przez Wiegand

Funkcja Wiegand umożliwia bramofonowi Akuvox działanie jako kontroler lub czytnik kart. Aby przeprowadzić konfigurację w sieci Web **Device > Wiegand > Wiegand** interface.



Konfiguracja parametrów :

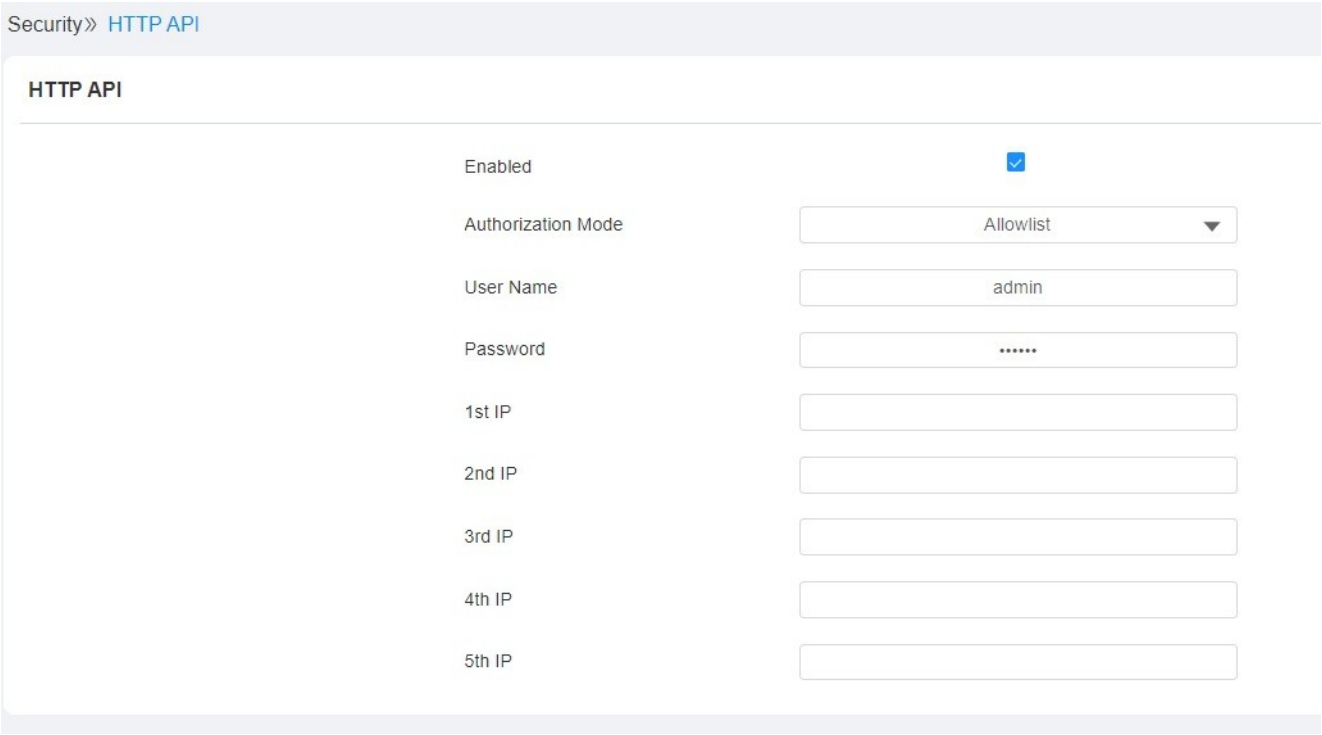
- **Tryb wyświetlania** Wiegand: wybór formatu kodu karty Wiegand spośród **8H10D; 6H3D 5D; 6H8D; 8HN; 8HR; 6H3D 5D-R(W26); 8HR10D; RAW.**
- **Tryb czytnika kart Wiegand**: ustawienie formatu transmisji danych Wiegand spośród trzech opcji: **Wiegand 26, Wiegand 34, Wiegand 58** . Format transmisji powinien być identyczny między bramofonem a urządzeniem, które ma zostać zintegrowane.
- **Tryb transferu Wiegand**: wybierz **Wejście, Wyjście, Konwertuj na kartę nr Wyjście Wiegand**. Jeśli bramofon jest używany jako odbiornik, ustaw go jako **Wejście** dla bramofonu. Wybierz **Wyjście,** jeśli bramofon ma być nadawcą. Wybierz **Convert to Card No.Output Wiegand,** jeśli chcesz, aby dane wyjściowe wiegand zostały przekonwertowane na numer karty przed wysłaniem ich z bramofonu do odbiornika.
- **Kolejność danych wejściowych** Wiegand: ustawienie kolejności danych wejściowych Wiegand pomiędzy **Normal** i **Reversed**. W przypadku wybrania opcji **Reversed** numer karty wejściowej zostanie odwrócony i odwrotnie.
- **Kolejność danych wyjściowych** Wiegand: ustawia kolejność danych wyjściowych Wiegand pomiędzy **Normal i Reversed,** jeśli wybierzesz **Reversed**, numer karty wejściowej zostanie odwrócony i odwrotnie.
- Wiegand **Output CRC Enabled**: Ta funkcja służy do kontroli danych Wiegand. Jest to

jest domyślnie włączona. Jeśli nie jest ona włączona, integracja urządzenia z urządzeniami innych firm może okazać się niemożliwa.

Integracja przez HTTP API

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

Funkcję HTTP API można skonfigurować w interfejsie Web **Setting > HTTP API** dla integracji.



Konfiguracja parametrów :

- **Enabled** : włączenie lub wyłączenie funkcji API HPTT dla integracji innej firmy. Na przykład, jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.
- **Tryb autoryzacji**: wybierz jedną z następujących opcji: **None, Normal, 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.** Domyślna nazwa użytkownika to Admin.
- **1st IP-5th IP**: wprowadź adres IP urządzeń innych firm, gdy **Allowlist**

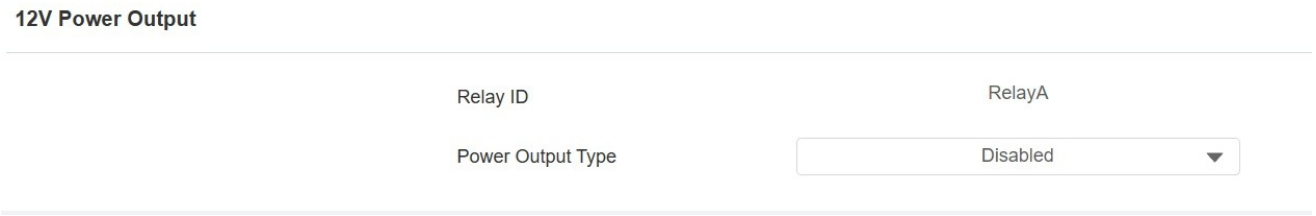
autoryzacja jest wybrana do integracji.

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	Normalny	Ten tryb jest używany tylko przez deweloperów Akuvox
3	Lista dozwolonych	Po wybraniu tego trybu wymagane jest jedynie podanie adresu IP urządzenia zewnętrznego w celu uwierzytelnienia. Lista zezwoleń jest odpowiednia do pracy w sieci LAN.
4	Podstawowy	Jeśli wybrano ten tryb, 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.
5	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".
6	Token	Ten tryb jest używany wyłącznie przez programistę Akuvox.

Kontrola mocy wyjściowej

Bramofon może służyć jako źródło zasilania dla zewnętrznych przekaźników. Można przejść do opcji **Access Control > Relay >12V Power Output** (**Kontrola dostępu > Przekaźnik > Wyjście zasilania 12 V).**



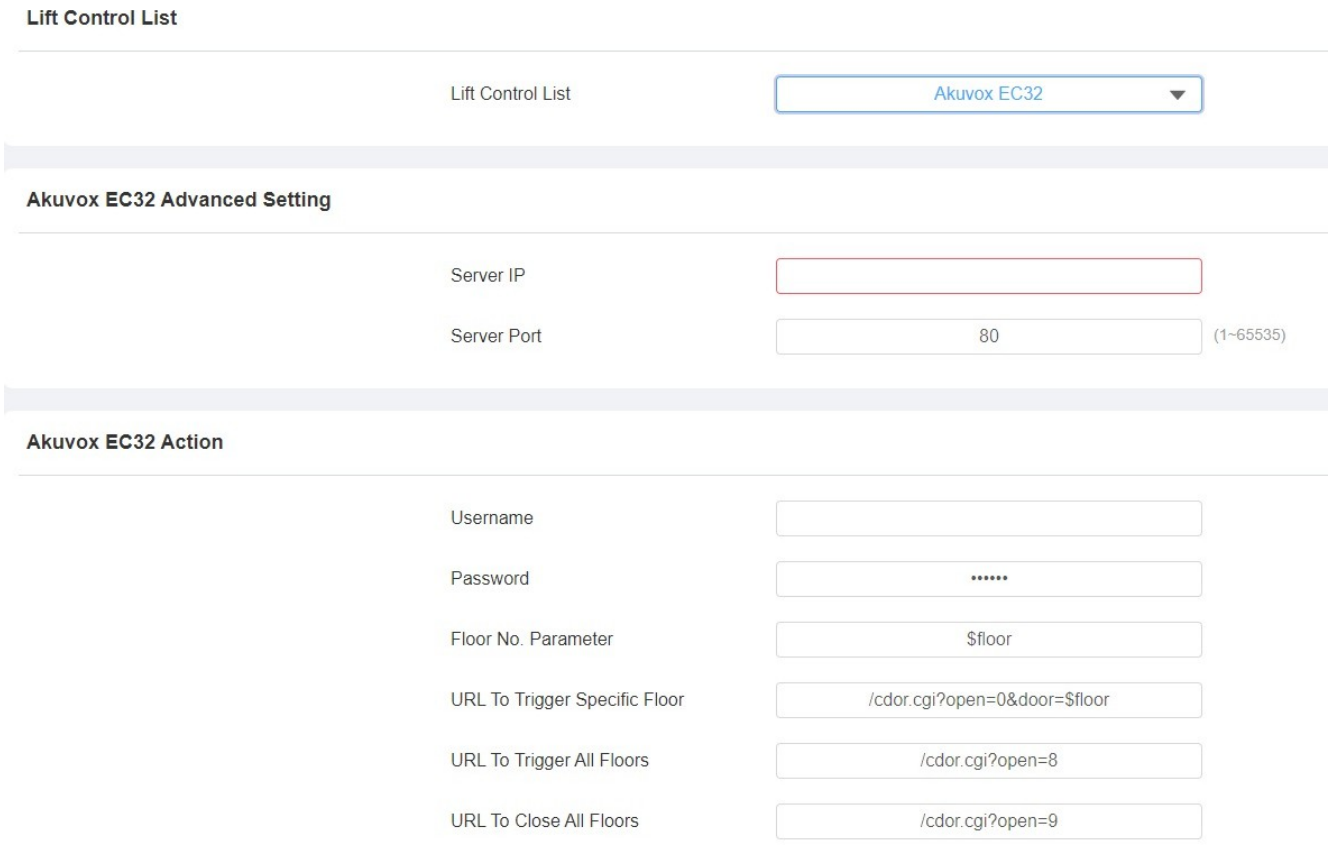
Konfiguracja parametrów :

- **Typ wyjścia zasilania**: wybierz **Wyłączone,** aby wyłączyć funkcję wyjścia zasilania. Wybierz opcję **Always,** aby umożliwić kontrolerowi dostępu ciągłe zasilanie urządzenia innej firmy. Wybierz **Triggered By Open Relay,** jeśli chcesz, aby X912 dostarczał zasilanie do urządzenia zewnętrznego za pośrednictwem wyjścia 12 i interfejsu GND podczas limitu czasu, gdy stan przekaźników zostanie zmieniony z niskiego na wysoki. Wybierz **Security Relay A,** jeśli chcesz skonfigurować przekaźnik bezpieczeństwa.

Kontrola podnoszenia

Bramofony można podłączyć do sterownika windy Akuvox w celu sterowania windą. Użytkownicy mogą wezwać windę, aby zjechała na parter, gdy uzyskają dostęp za pomocą różnych metod dostępu na bramofonie.

Aby skonfigurować sterowanie windą, przejdź do opcji **Urządzenie > Sterowanie windą**.



Konfiguracja parametrów :

- **Lift Control List**: wybierz **None**, aby wyłączyć funkcję i wybierz **Akuvox E32**, aby zintegrować bramofon z kontrolerem Akuvox EC32.
- **Server IP**: adres IP serwera kontrolera Akuvox. **Server**
- **Port**: port serwera kontrolera Akuvox.
- **Nazwa użytkownika** : nazwa użytkownika kontrolera windy do
- uwierzytelniania. **Hasło**: hasło kontrolera windy do uwierzytelniania.
- **Floor NO. Parametr**: wprowadź parametr numeru piętra dostarczony przez Akuvox. Domyślny ciąg parametru to "$floor". W razie potrzeby można zdefiniować własny ciąg parametrów.
- **URL To Trigger Specific Floor**: wprowadź adres URL sterowania windą Akuvox w celu wyzwolenia określonego piętra.

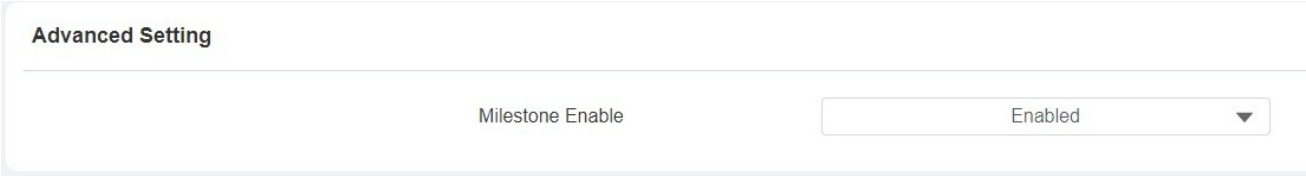
floor. Adres URL to /cdor.cgi?open=0&door= $ floor, ale ciąg "$floor" na końcu musi być identyczny z ciągiem parametrów zdefiniowanym przez użytkownika.

- **URL To Trigger All Floors** : wprowadź adres URL Akuvox do wyzwalania wszystkich pięter.
- **URL To Close All Floors** : wprowadź adres URL Akuvox używany do zamykania wszystkich pięter, co oznacza, że wszystkie przyciski uruchamiane dla odpowiednich pięter staną się nieważne.

Integracja z Milestone

Jeśli chcesz, aby bramofon był monitorowany przez Milestone lub urządzenia innych firm, które zostały zintegrowane z Milestone, musisz włączyć tę funkcję.

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

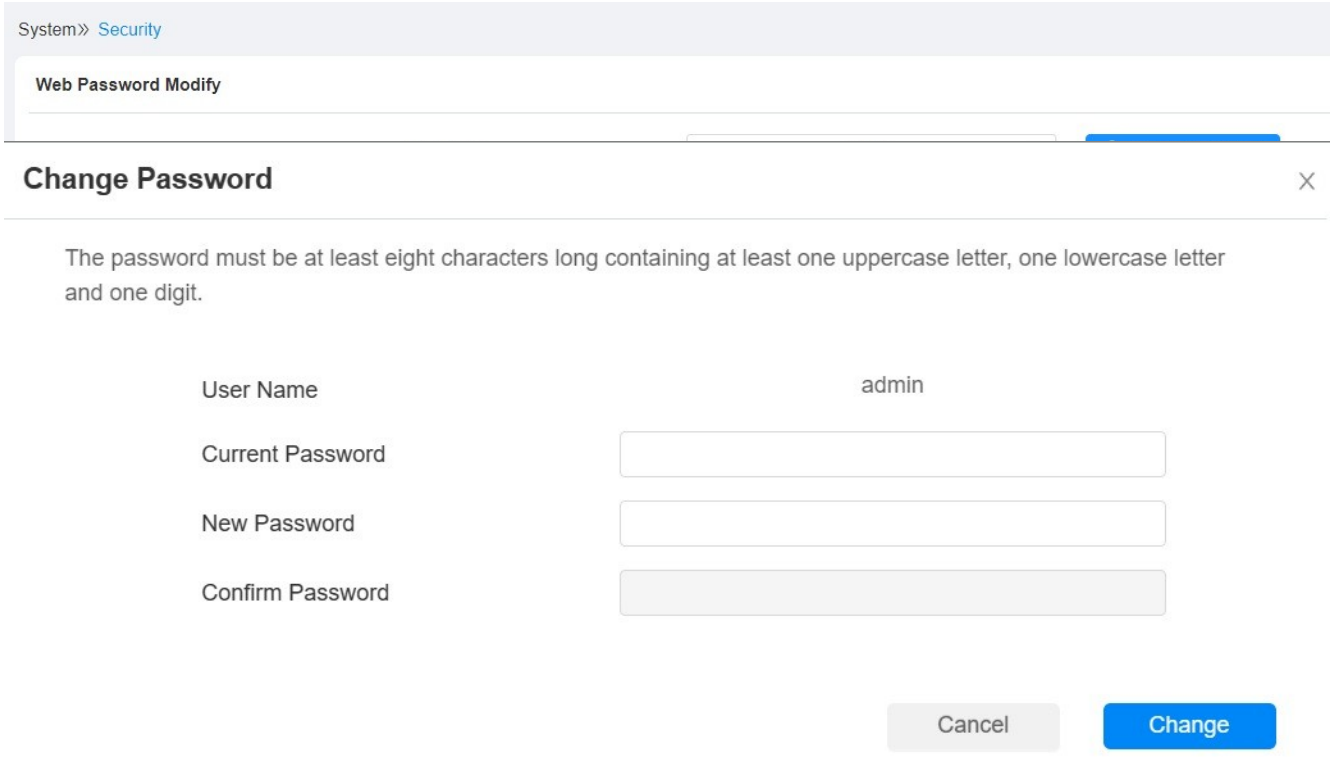


Modyfikacja hasła

Modyfikowanie hasła interfejsu sieciowego urządzenia

Aby zmienić domyślne hasło internetowe w interfejsie **System > Bezpieczeństwo > Modyfikacja hasła internetowego.**

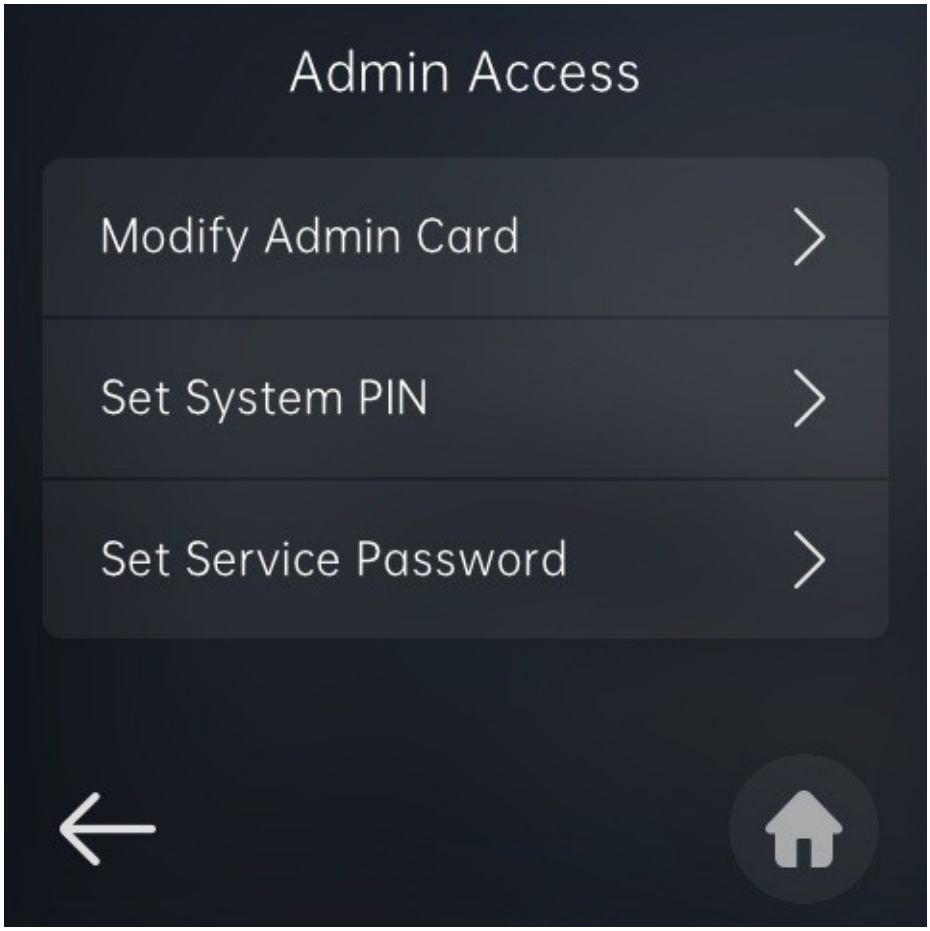
Wybierz **admin** dla konta administratora i **User** dla konta użytkownika. Kliknij kartę **Zmień hasło**, aby zmienić hasło.

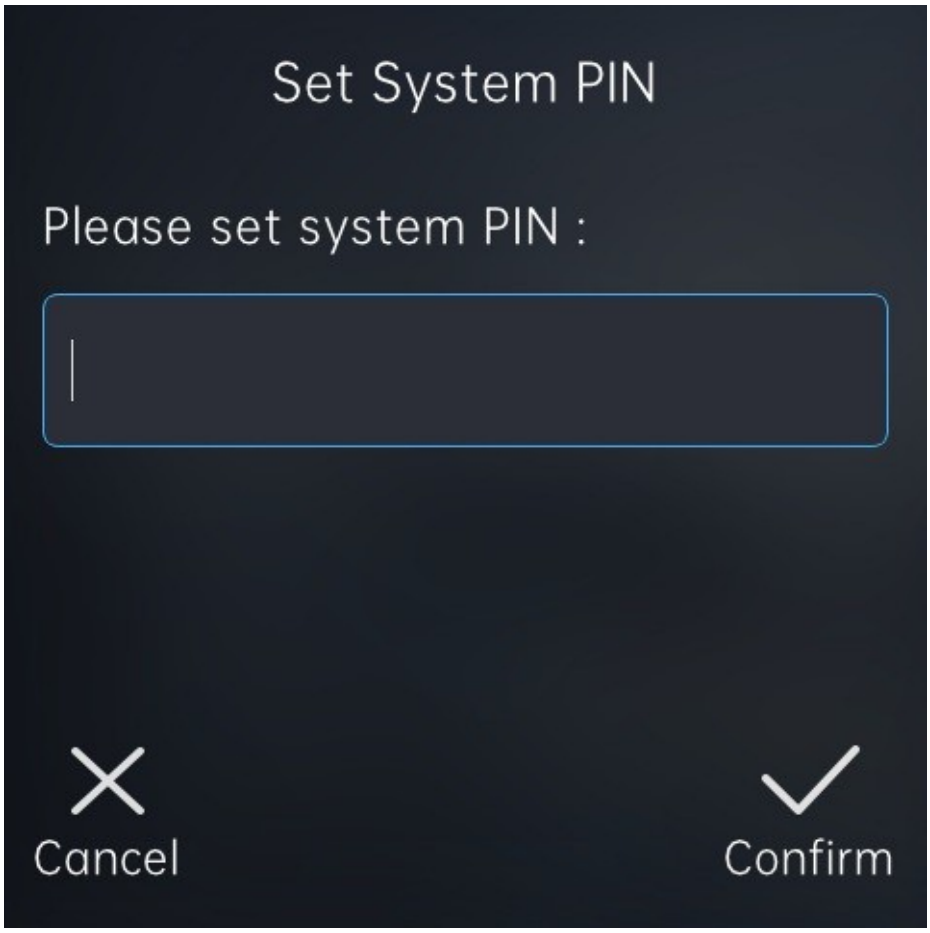


Modyfikowanie hasła systemowego

Systemowy kod PIN służy do uzyskiwania dostępu do systemu urządzenia. Systemowy kod PIN można modyfikować na urządzeniu i w interfejsie internetowym.

Przejdź do **Advance Settings > Admin Access > Set System PIN.**

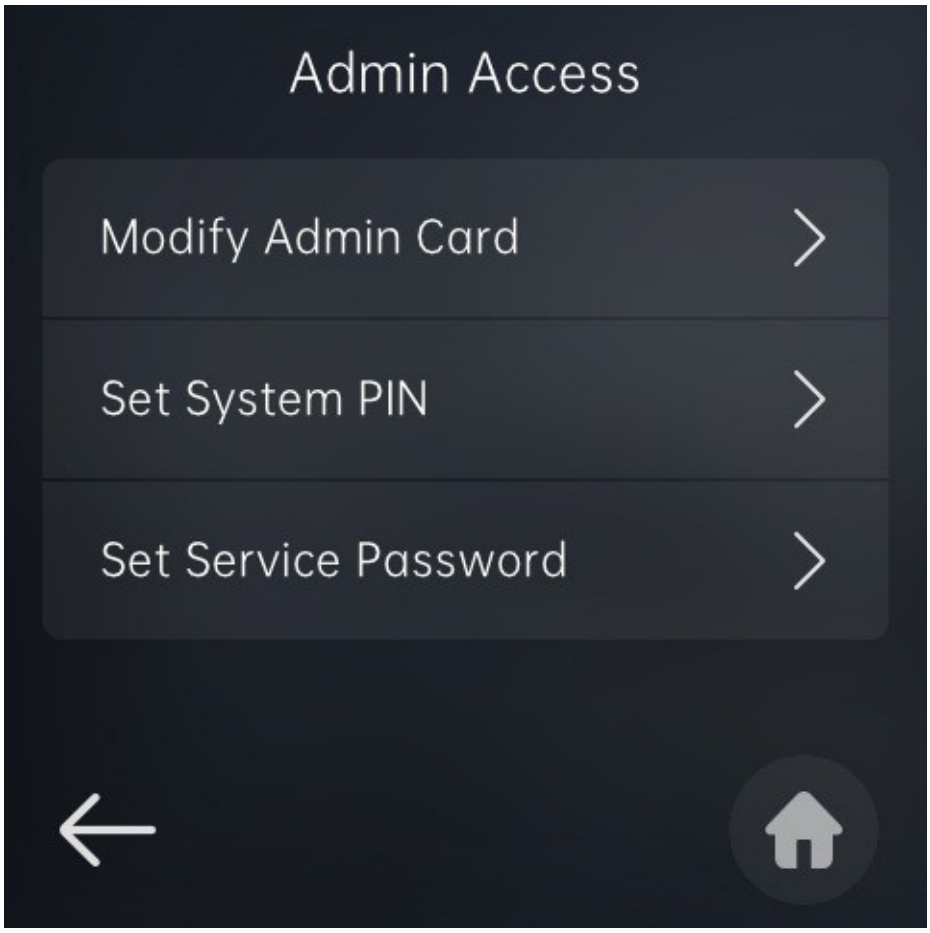


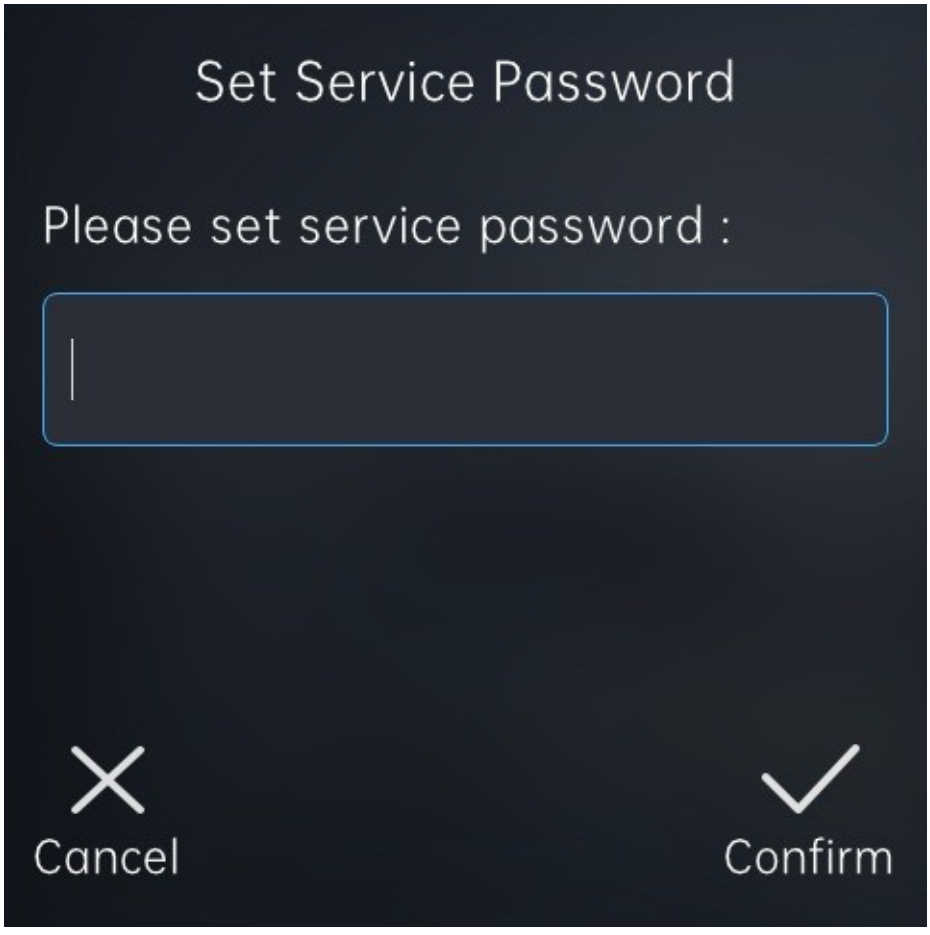


Modyfikowanie hasła ustawień

Ustawienie kodu PIN służy do uzyskiwania dostępu do ustawień urządzenia. Systemowy kod PIN można modyfikować na urządzeniu i w interfejsie internetowym.

Przejdź do **Ustawienia zaawansowane> Dostęp administratora > Ustaw hasło usługi** .


Admin Access
Modify Admin Card
Set System PIN
Set Service Password

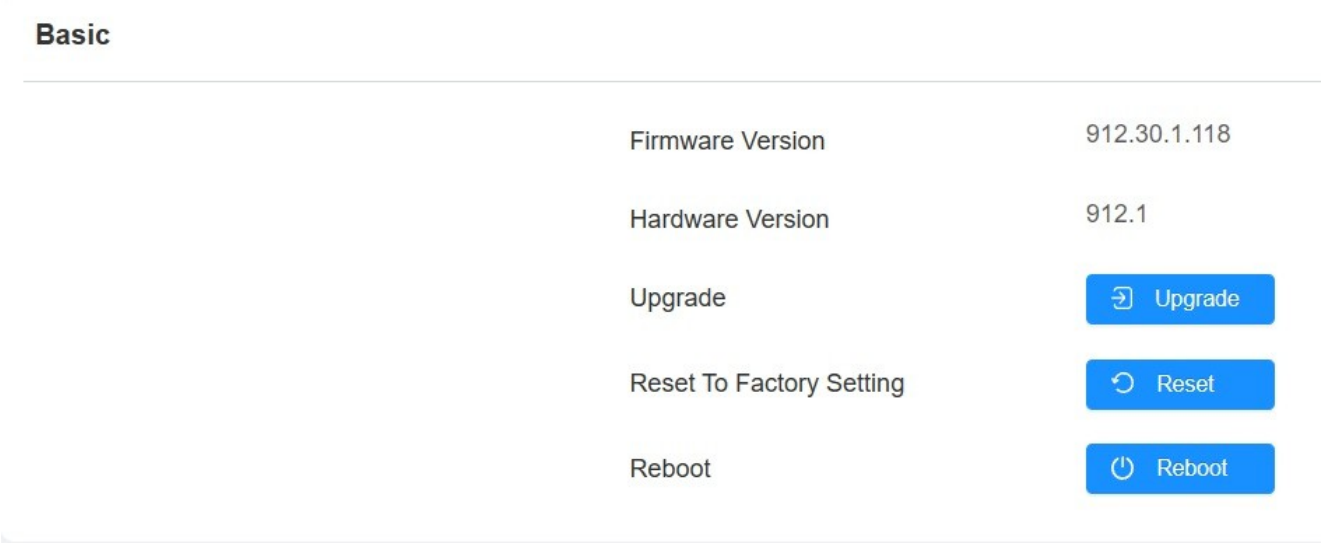

Set Service Password
Please set service password :
Cancel
Confirm

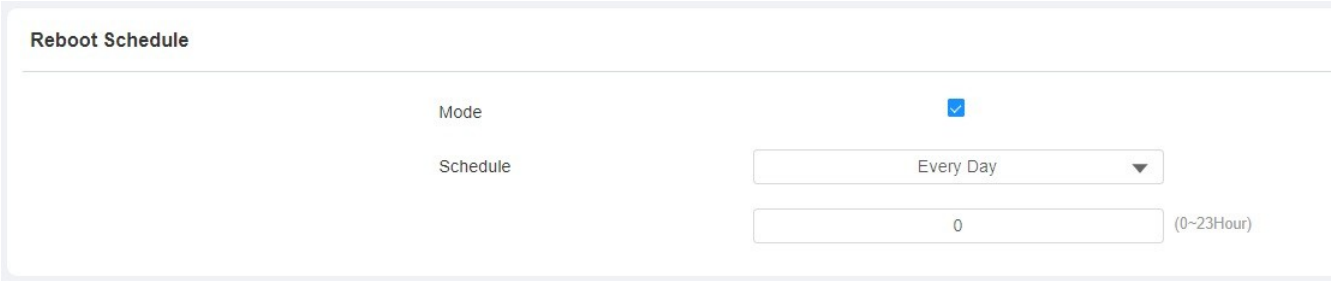
Ponowne uruchamianie i resetowanie systemu

Reboot

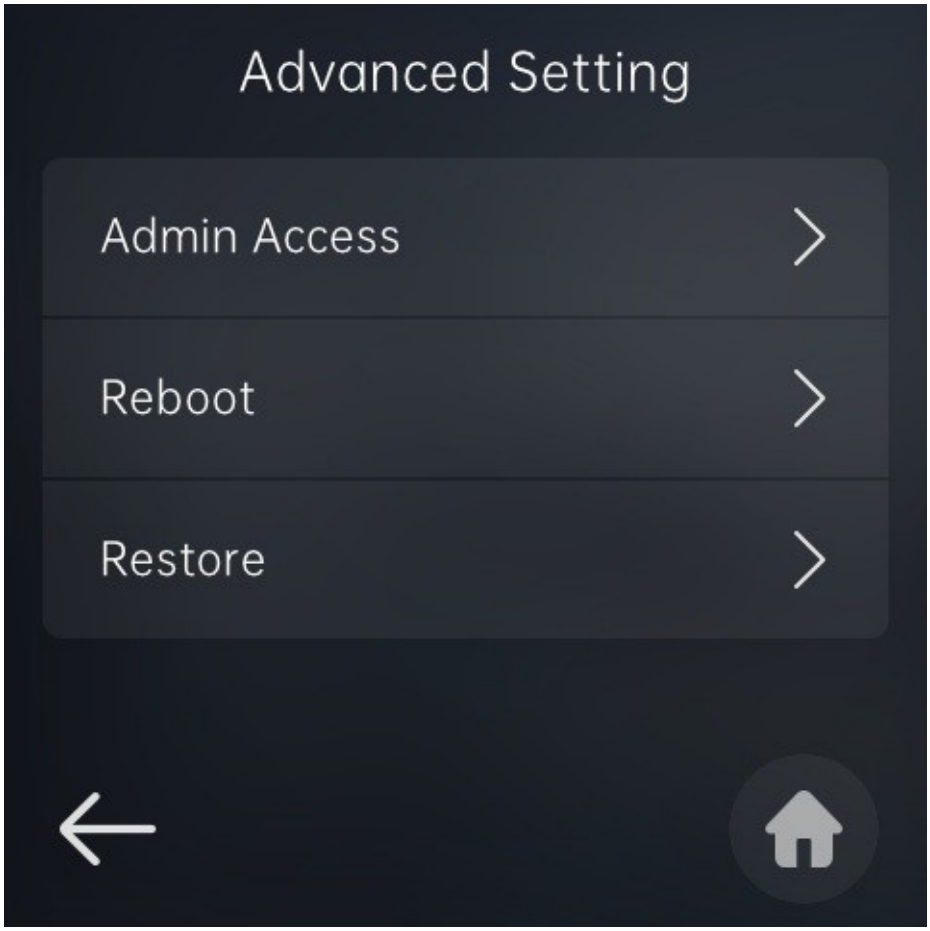
Jeśli chcesz ponownie uruchomić system urządzenia, możesz to również zrobić za pomocą interfejsu internetowego urządzenia. Ponadto można skonfigurować harmonogram ponownego uruchamiania urządzenia.

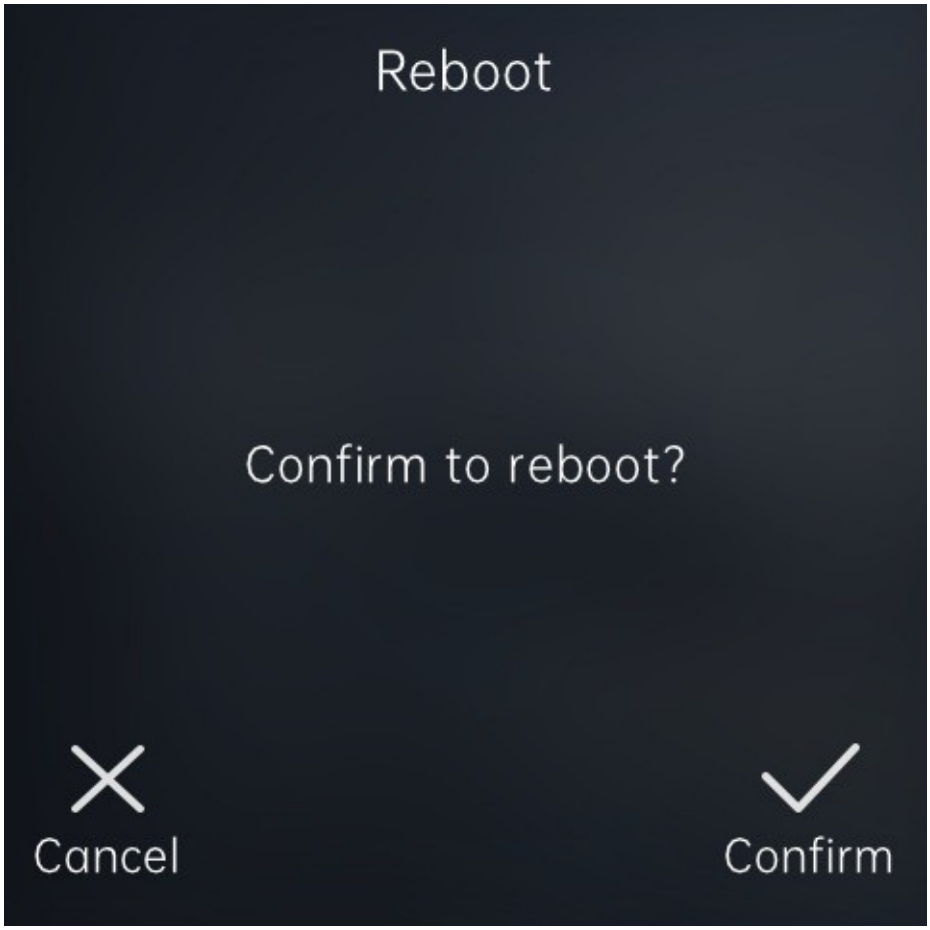
Aby ponownie uruchomić system w interfejsie internetowym **System > Upgrade > Basic.** Aby ustawić harmonogram w System **> Auto Provisioning > Reboot Schedule** .





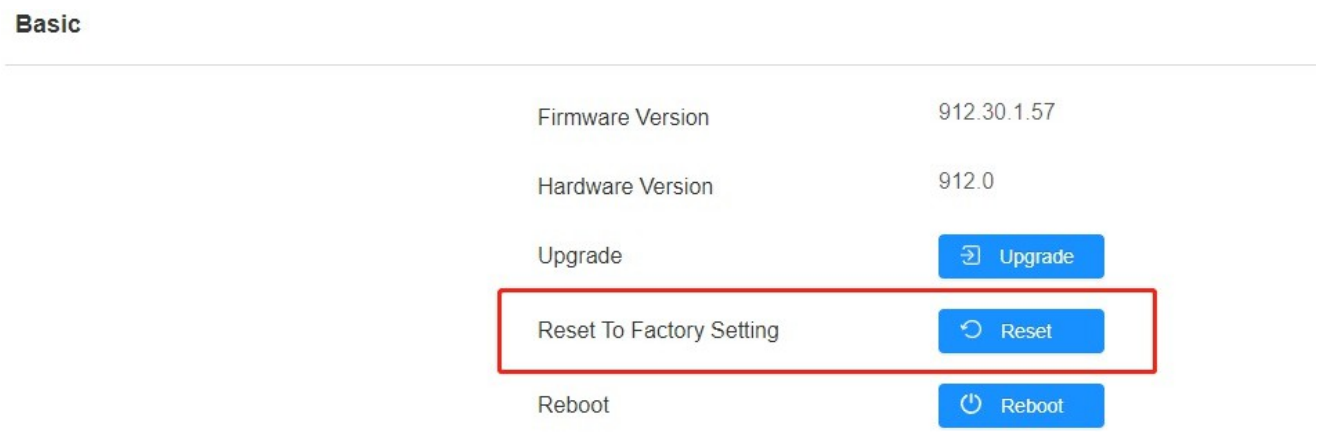
Aby ponownie uruchomić urządzenie, przejdź do opcji **Ustawienia zaawansowane > Uruchom ponownie**.


Advanced Setting
Admin Access
Reboot
Restore

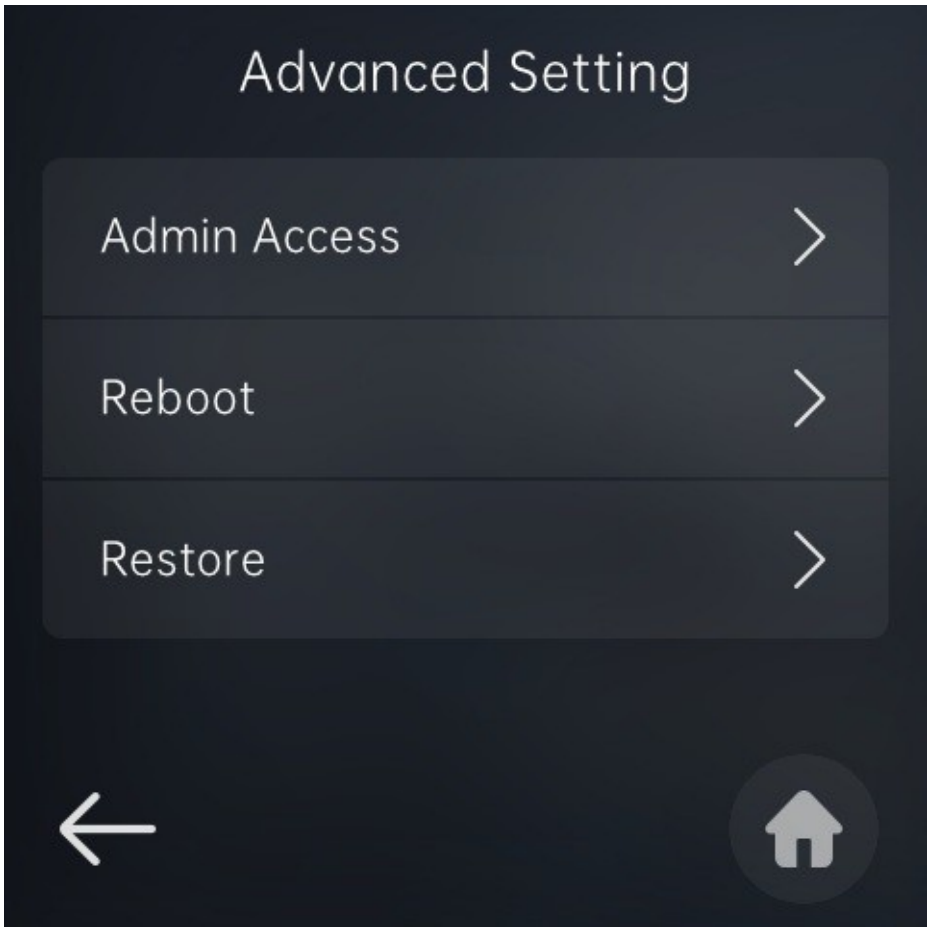

Reboot
Confirm to reboot?
Cancel
Confirm

Reset

Jeśli chcesz zresetować system urządzenia do ustawień fabrycznych, możesz to zrobić w interfejsie internetowym **System > Upgrade > Basic.**



Aby przywrócić ustawienia fabryczne urządzenia, przejdź do opcji **Ustawienia zaawansowane > Przywróć** .




Restore
Please confirm if you want to restore to the factory settings.
Cancel
Confirm