Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX E18C DOOR PHONE

Administrator Guide

Akuvox
Open A Smart World

Dziękujemy za wybranie bramofonu Akuvox E18C. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy wersji 18.30.10.8 i zawiera wszystkie konfiguracje funkcji i cech bramofonów E18C. Odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe.

Przegląd produktów

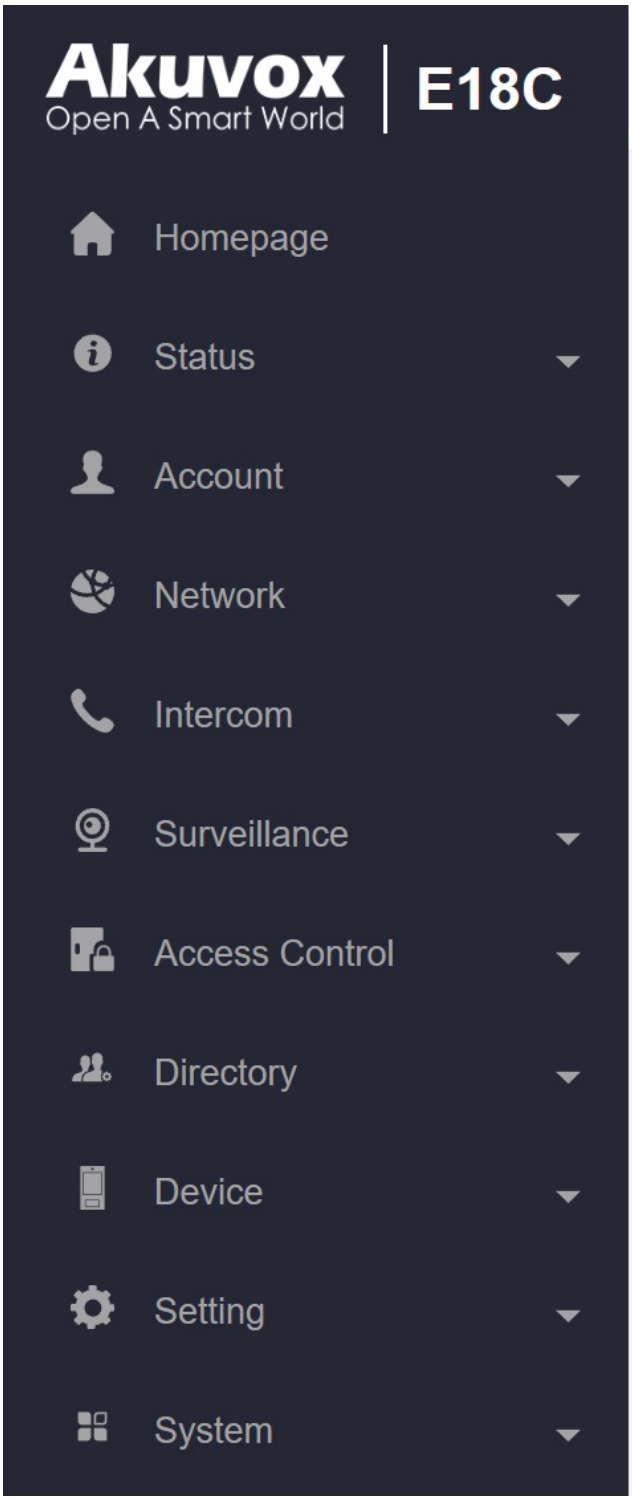
Akuvox E18C jest oparty na systemie Linux z ekranem dotykowym. Obejmuje komunikację audio i wideo, kontrolę dostępu i nadzór wideo. Jego precyzyjnie dostrojona technologia SmartPlus i technologia komunikacji oparta na sztucznej inteligencji pozwalają na lepsze dostosowanie do potrzeb użytkownika. Wiele portów E18C, takich jak RS485 i porty Wiegand, 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 kartą, NFC, Bluetooth, kod QR i nowo dodany dostęp do drzwi w połączeniu z pomiarem temperatury ciała. Bramofon E18C ma zastosowanie w budynkach mieszkalnych, biurowych i ich kompleksach.

Specyfikacja modelu

Model	E18C
Wyjście przekaźnika	2
Wejście przekaźnika	3
RS485	✓
Czytnik kart	13,56 MHz, 125 kHz i NFC
Wi-Fi	X
Bluetooth	✓
Wykrywanie temperatury	Opcjonalnie
Rozpoznawanie twarzy	✓
LTE	Opcjonalnie
USB	X
Zewnętrzna karta SD	✓

Wprowadzenie do menu konfiguracji

- **Status** : ta sekcja zawiera podstawowe informacje, takie jak informacje o produkcie, informacje o sieci i informacje o koncie, dziennik połączeń, dziennik dostępu i dziennik temperatury.
- **Konto**: ta sekcja dotyczy konta SIP, serwera SIP, serwera proxy, typu protokołu transportowego, wychodzącego serwera zbliżeniowego.
- **Sieć**: ta sekcja dotyczy głównie ustawień DHCP i statycznego adresu IP oraz wdrażania urządzeń itp.
- **Interkom**: ta sekcja obejmuje ustawienia połączeń interkomowych, funkcje połączeń, plan
- wybierania itp. **Nadzór**: ta sekcja zawiera ustawienia związane z audio i wideo, takie jak strumień na żywo, RTSP, ONVIF, MJPEG.
- **Kontrola dostępu**: ta sekcja obejmuje ustawienia typu wejścia, ustawienia przekaźnika, ustawienia przekaźnika internetowego, prywatny kod PIN, rozpoznawanie twarzy, kartę RF, ustawienia BLE, temperaturę ciała itp.
- **Directory (Katalog)**: ta sekcja umożliwia dodawanie użytkowników i konfigurowanie kontroli dostępu do drzwi dla poszczególnych użytkowników. Umożliwia także konfigurowanie grup kontaktów, a kontakty są wyświetlane na bramofonie.
- **Urządzenie**: ta sekcja dotyczy oświetlenia LED, Wiegand, sterowania windą, wyświetlacza LCD, dźwięku itp.
- **Ustawienia**: ta druga sekcja dotyczy czasu, języka, ustawień powiadomień bezpieczeństwa, ustawień tekstu monitu do drzwi, adresu URL akcji, harmonogramu i interfejsu API HTTP i tak dalej.
- **System**: ta sekcja obejmuje aktualizację oprogramowania układowego, resetowanie i ponowne uruchamianie urządzenia, automatyczne dostarczanie pliku konfiguracyjnego, modyfikację hasła PCAP, alarm sabotażowy i automatyczne wylogowanie interfejsu internetowego.



Status » Info

Product Information

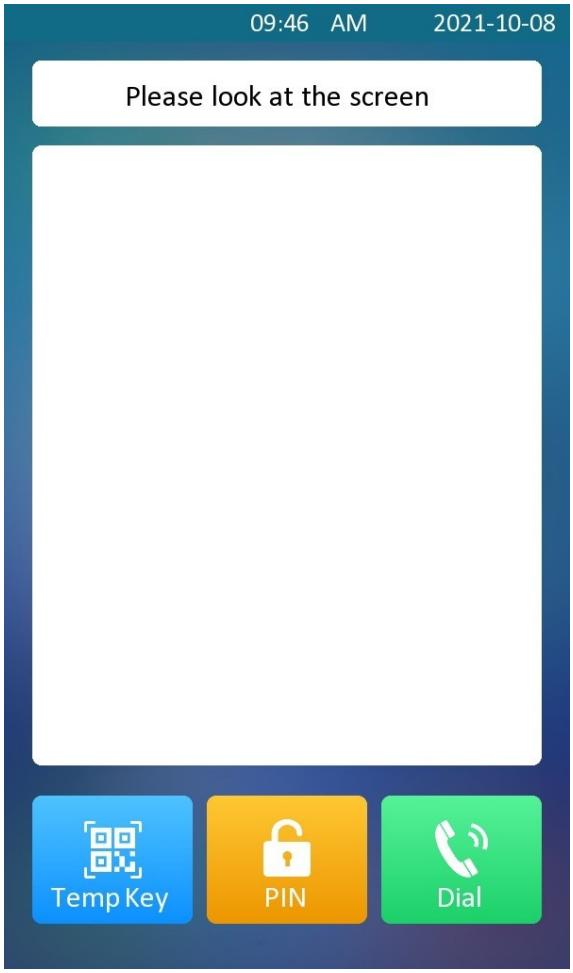
Network Information

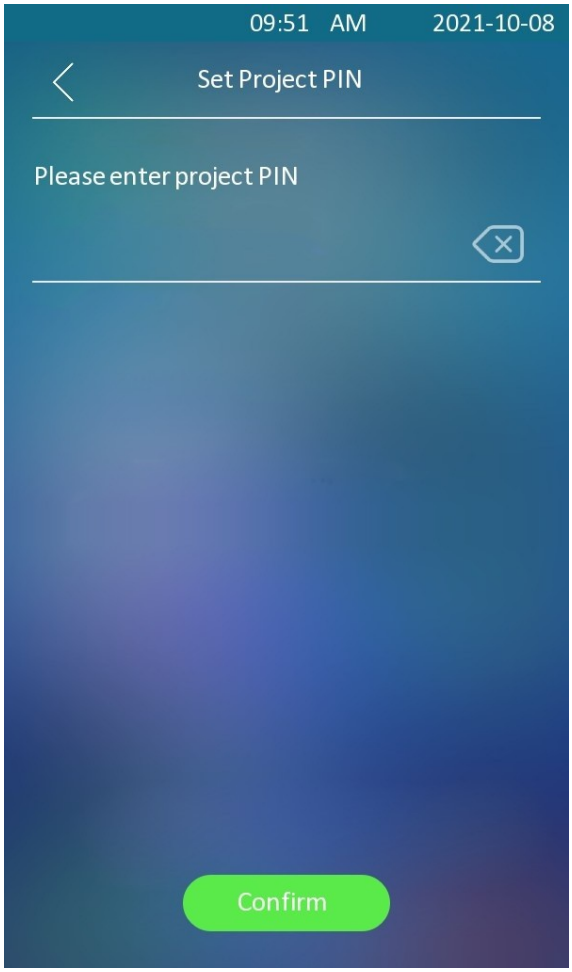
Dostęp do urządzenia

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

Dostęp do ustawień urządzenia na urządzeniu

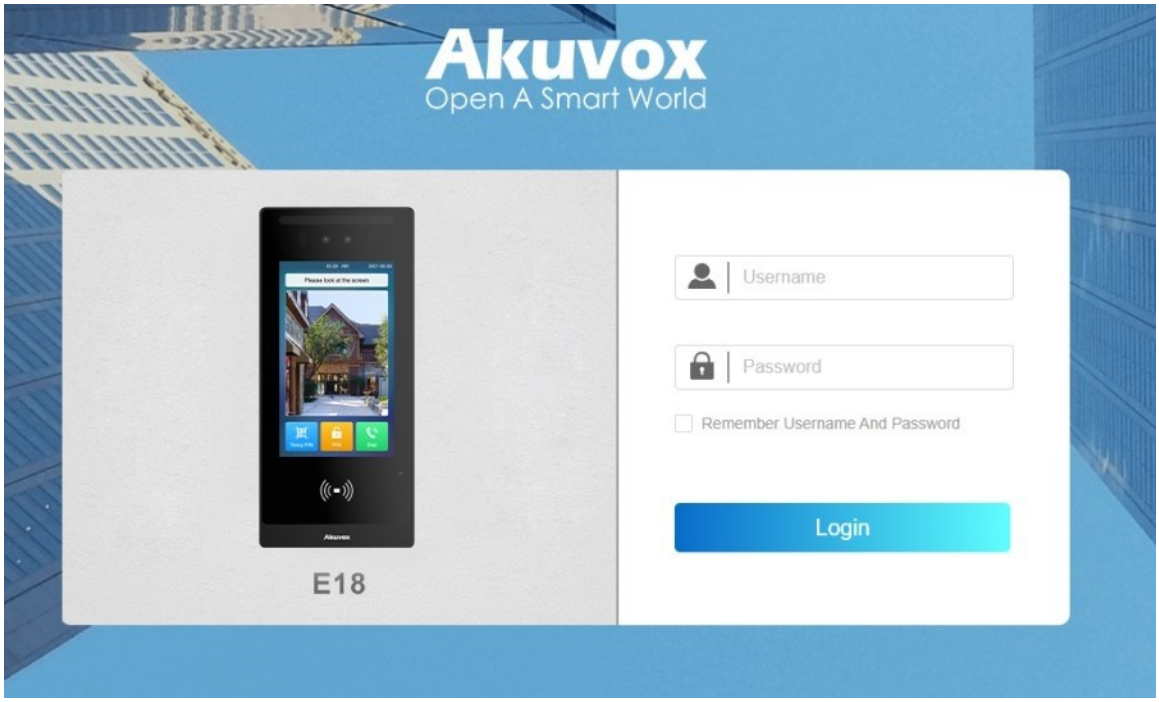
Jeśli chcesz uzyskać dostęp do ustawień urządzenia, aby skonfigurować i dostosować parametry, możesz to zrobić bezpośrednio na urządzeniu. Można nacisnąć dowolne miejsce na ekranie początkowym przez około pięć sekund, wprowadzić domyślny kod PIN **admin**, a następnie nacisnąć przycisk **Potwierdź.**





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 uzyskać za pomocą skanera Akuvox IP w celu zalogowania się do 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 czasu i języka

Ustawienia języka

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

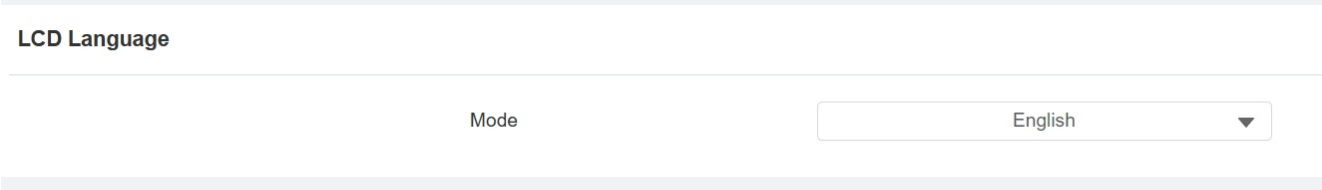
Ustawienia języka na urządzeniu

Język urządzenia można skonfigurować na urządzeniu i w interfejsie internetowym urządzenia, co pozwala wybrać lub zmienić język wyświetlania ekranu zgodnie z własnymi preferencjami. Ścieżka: **Display&Sounds > Language** .

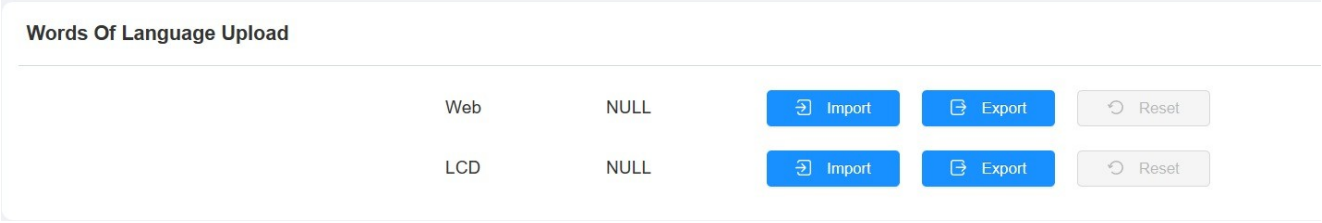
Ustawienia języka w interfejsie internetowym urządzenia

Można wybrać język urządzenia i ikony języka urządzenia, a także dostosować tekst interfejsu, w tym nazwy konfiguracji i tekst monitu.

Przejdź do **Ustawienia >Czas/język > Język LCD** .



Aby dostosować nazwy konfiguracji i tekst monitu, należy wyeksportować i edytować plik .json przed przesłaniem pliku do urządzenia. Ścieżka: **Setting > Time/Lang > Words Of Language**

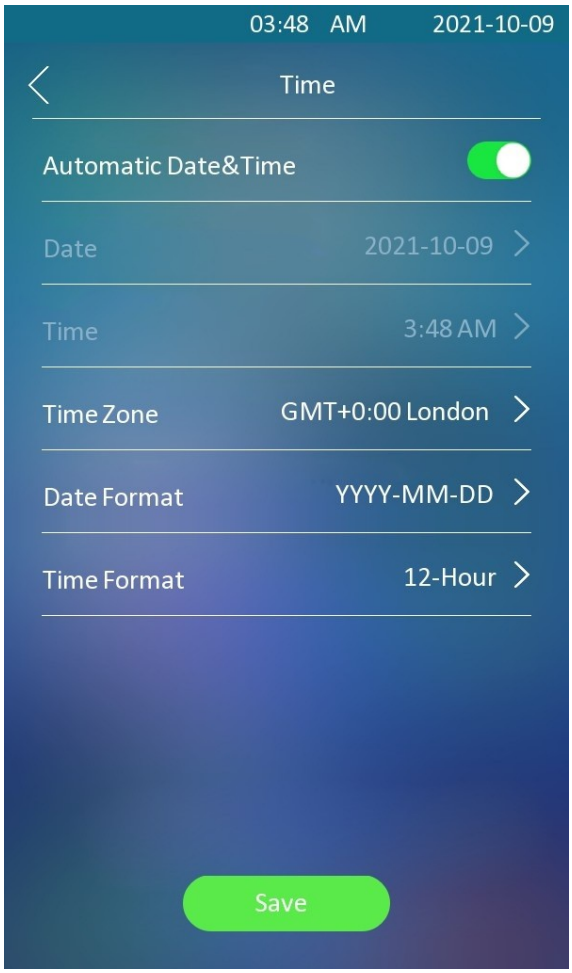


Ustawienie czasu

Ustawienia czasu, w tym strefę czasową, format daty i godziny i inne, można skonfigurować na urządzeniu lub w interfejsie internetowym.

Konfiguracja ustawień czasu na urządzeniu

Ścieżka: **Display&Sounds > Time** .



Konfiguracja parametrów :

- **Automatyczna data i czas**: Automatyczna data i czas są domyślnie włączone, co pozwala na automatyczną konfigurację daty i czasu oraz synchronizację z domyślną strefą czasową i serwerem NTP (**Network Time Protocol**). Można ją również skonfigurować ręcznie, najpierw wyłączając przełącznik, a następnie wprowadzając żądaną godzinę i datę przed naciśnięciem zakładki **Zapisz** w celu zatwierdzenia.

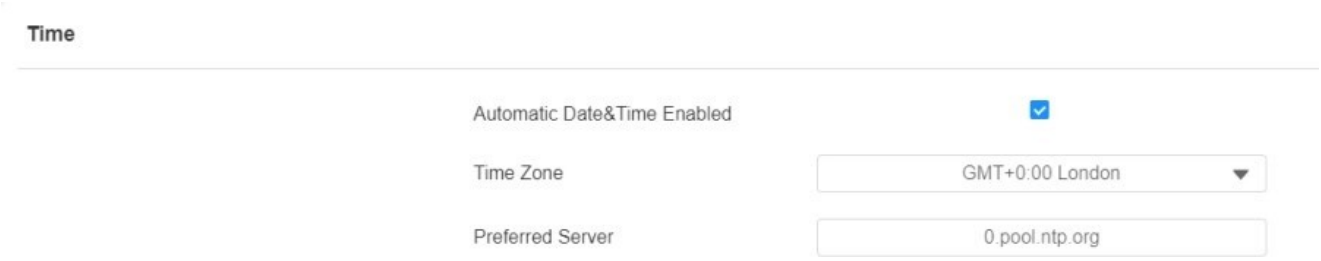
Uwaga

- Gdy przełącznik **automatycznej daty i godziny** jest wyłączony, parametry związane z serwerem NTP nie będą mogły być edytowane. Po włączeniu przełącznika godzina i data nie będą mogły być edytowane.

Ustawienia czasu w interfejsie internetowym urządzenia

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.

Przejdź do opcji **Ustawienia >** Interfejs **czasu/języka.**



Konfiguracja parametrów :

- **Automatic Date&Time Enabled** : zaznacz to pole wyboru, aby zezwolić na automatyczną konfigurację daty i godziny w urządzeniu oraz ich synchronizację z domyślną strefą czasową i serwerem NTP (**Network Time Protocol**). Odznaczenie tego pola wyboru umożliwia ręczne ustawienie czasu w interfejsie internetowym.
- **Preferred Server (Preferowany serwer)**: wprowadź uzyskany serwer NTP w polu NTP Server (Serwer NTP).

Uwaga

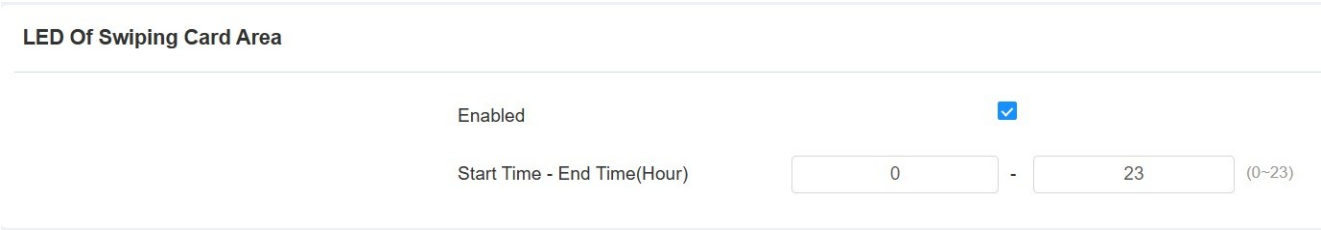
- Gdy pole wyboru Automatic Date&Time nie jest zaznaczone, parametry związane z serwerem NTP nie będą edytowalne. A gdy pole wybodu jest zaznaczone, edycja czasu i daty będzie zabroniona.

Ustawienia LED i LCD

Konfiguracja ustawień diody LED czytnika kart

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

Ścieżka: **Device > Light > LED of Swiping Card Area** .



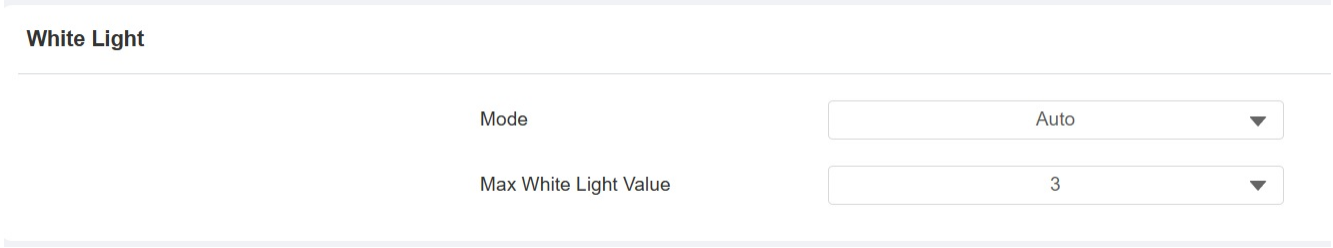
Konfiguracja parametrów :

- **Start Time - End Time (H)**: wprowadź przedział czasowy, w którym oświetlenie LED ma obowiązywać, np. jeśli przedział czasowy wynosi od **18-22**, oznacza to, że światło LED pozostanie włączone w przedziale czasowym od **18:00** do 22**:00** w ciągu jednego dnia (24 godziny).

Konfiguracja ustawień białego światła LED

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

Ścieżka: **Urządzenie > Światło > Światło białe**.



Konfiguracja parametrów:

- **Tryb**: wybierz **Auto** lub **OFF**. Jeśli wybierzesz Auto, białe światło włączy się na 5 minut w celu rozpoznania twarzy i zeskanowania kodu QR. W przypadku wybrania opcji **Wył.** białe światło zostanie wyłączone na 5 minut.

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

Uwaga

- Dioda LED IR powinna zostać uruchomiona jako pierwsza, zanim białe światło będzie mogło być używane w rozpoznawaniu twarzy. Jednakże, dioda LED IR nie musi być uruchomiona dla funkcji białego światła podczas skanowania kodu QR.

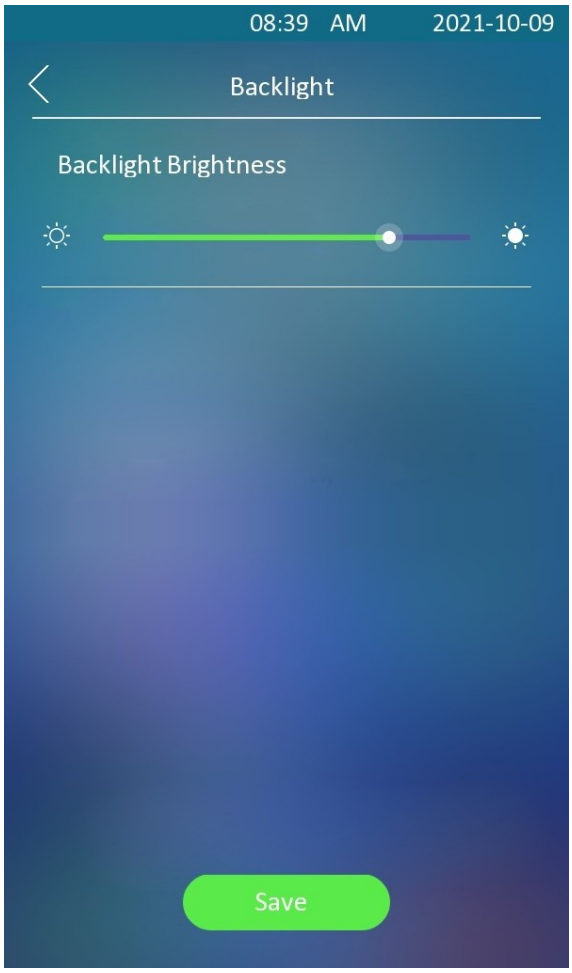
Ustawienie jasności ekranu LCD

Jeśli chcesz rozjaśnić ekran, aby lepiej widzieć ekran w środowisku o większym natężeniu światła, musisz skonfigurować odpowiednie parametry.

Ustawienie jasności ekranu LCD na urządzeniu

W urządzeniu można ustawić i dostosować jasność podświetlenia ekranu.

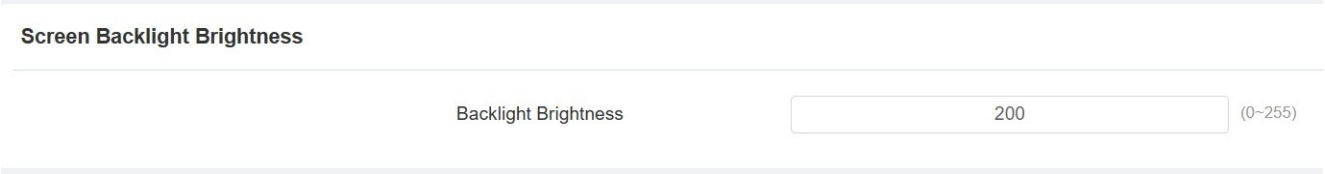
Ścieżka: **Wyświetlacz i dźwięki > Podświetlenie**.



Ustawienie jasności ekranu LCD w interfejsie sieciowym

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

Ścieżka: **Urządzenie > Światło > Jasność podświetlenia ekranu** .



Konfiguracja parametrów :

- **Jasność podświetlenia (dzień)**: ustawienie jasności podświetlenia ekranu w ciągu dnia przy użyciu wartości z zakresu (0-255).

Konfiguracja ekranu

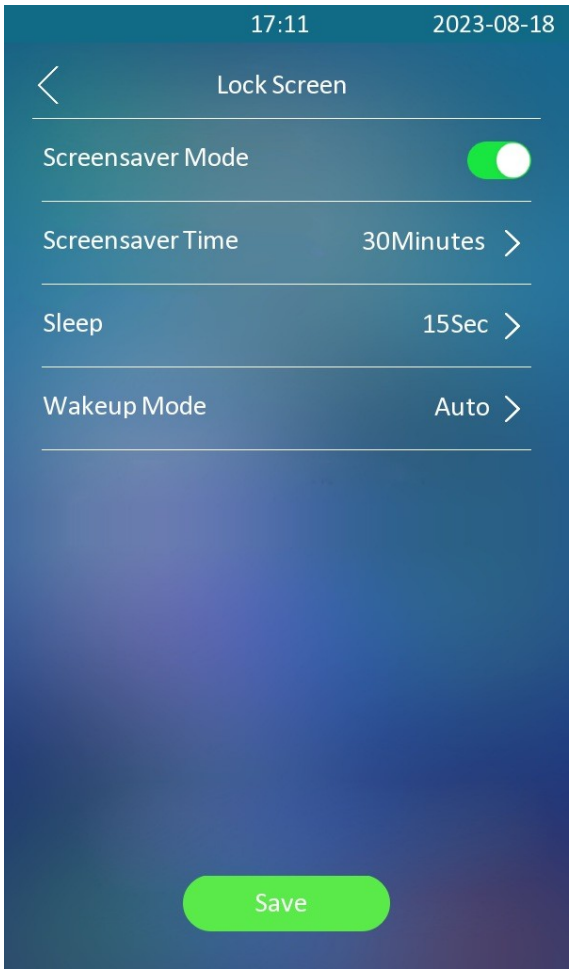
Możesz skonfigurować funkcje wyświetlania ekranu urządzenia, takie jak wygaszacz ekranu, aby zapewnić użytkownikom lepsze wrażenia wizualne i operacyjne.

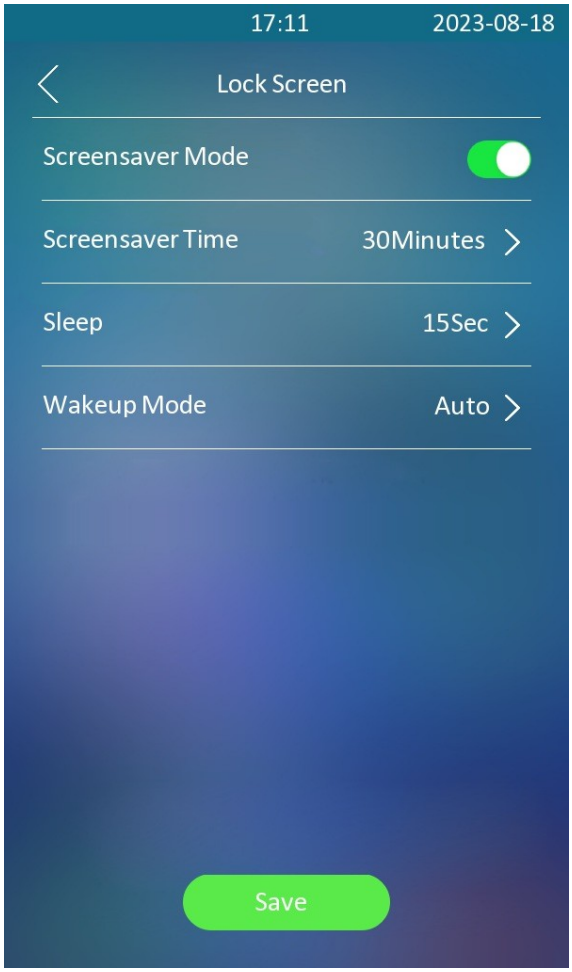
Konfiguracja wygaszacza ekranu

Konfiguracja wygaszacza ekranu na urządzeniu

Tryb uśpienia i wygaszacz ekranu służą do ochrony ekranu. Można ustawić te dwa tryby, aby zapobiec przegrzaniu ekranu urządzenia i zmniejszyć zużycie energii. Można zdefiniować, kiedy urządzenie ma przechodzić w tryb uśpienia, tryb wygaszacza ekranu i wyłączać ekran.

Ścieżka: **Display&Sounds > Screensaver > Lock Screen**.





Konfiguracja parametrów :

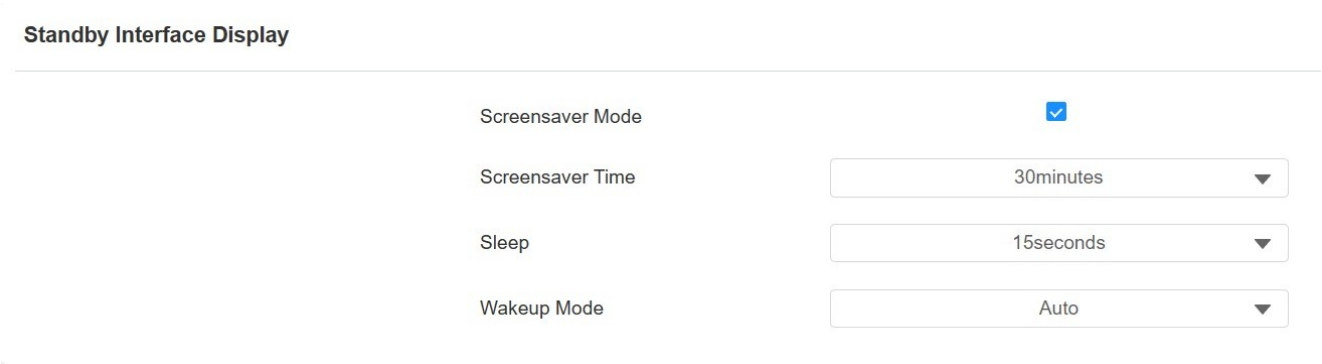
- **Tryb wygaszacza ekranu**: przesuń przełącznik w prawo, aby włączyć funkcję wygaszacza ekranu.
- **Czas wygaszacza ekranu**: ustawienie czasu trwania wygaszacza ekranu po przejściu urządzenia w tryb uśpienia.

  Ustawienie domyślne to 30 minut.
- **Uśpienie**: wybierz czas spośród **5 s, 10 s** i **15 s**. Na przykład, jeśli ustawisz 10 sekund, urządzenie przejdzie w tryb wygaszacza ekranu po 10 sekundach, gdy na urządzeniu nie będzie wykonywana żadna operacja lub nikt nie wykryje zbliżania się urządzenia.
- **Tryb wybudzania**: jeśli wybierzesz tryb **automatyczny**, ekran zostanie wybudzony, gdy ktoś się do niego zbliży bez dotykania go, a jeśli wybierzesz tryb **ręczny**, musisz dotknąć i wybudzić ekran.

Konfiguracja wygaszacza ekranu w interfejsie sieciowym

Można ustawić czas trwania wygaszacza ekranu, a także czas wyłączenia ekranu zarówno w celu ochrony ekranu, jak i zmniejszenia zużycia energii.

Aby skonfigurować wygaszacz ekranu w interfejsie internetowym, można przejść do opcji **Urządzenie > LCD > Wyświetlacz interfejsu czuwania.**



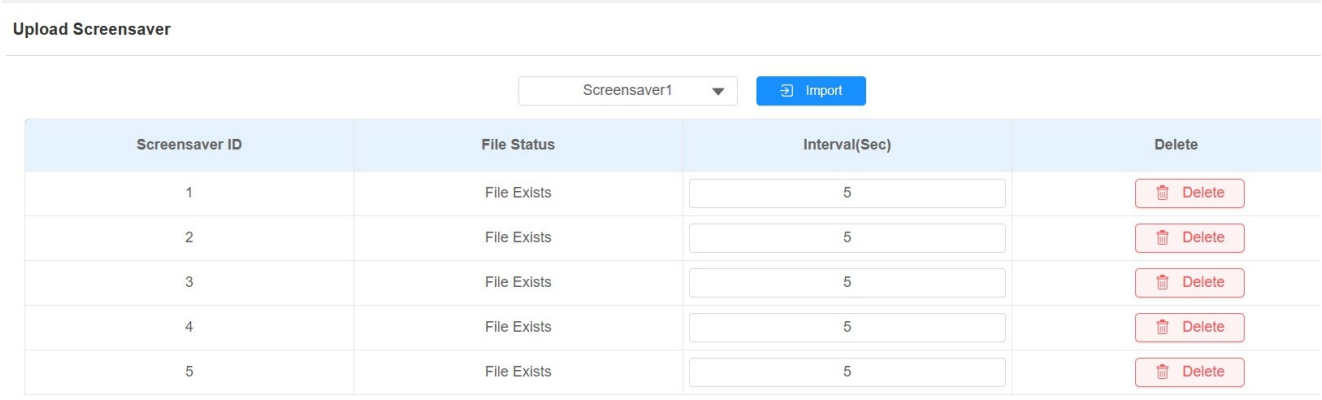
Konfiguracja parametrów :

- **Czas wygaszacza ekranu**: ustawienie czasu trwania wygaszacza ekranu po przejściu urządzenia w tryb uśpienia.

  Czas trwania wygaszacza ekranu wynosi od **5 sekund** do **2 godzin** w interfejsie internetowym. Ustawienie domyślne to **30 minut**.
- **Uśpienie**: wybierz czas spośród **5 s, 10 s** i **15 s**. Na przykład, jeśli ustawisz 10 sekund, urządzenie przejdzie w tryb wygaszacza ekranu po 10 sekundach, gdy na urządzeniu nie będą wykonywane żadne operacje lub nikt nie wykryje zbliżania się urządzenia.
- **Tryb wybudzania**: jeśli wybierzesz tryb **automatyczny**, ekran zostanie wybudzony, gdy ktoś się do niego zbliży bez dotykania go, a jeśli wybierzesz tryb **ręczny**, musisz dotknąć i wybudzić ekran.

Dostosowywanie wygaszacza ekranu w interfejsie internetowym

Obrazy wygaszacza ekranu można przesyłać i dostosowywać oddzielnie lub zbiorczo do urządzenia w celach publicznych lub dla lepszych wrażeń wizualnych. Można przesłać maksymalnie 5 obrazów, a każdy z nich będzie wyświetlany rotacyjnie zgodnie z kolejnością ID i określonym czasem trwania (Time Interval). Można przejść do opcji **Urządzenie > LCD > Prześlij wygaszacz ekranu**.



Konfiguracja parametrów :

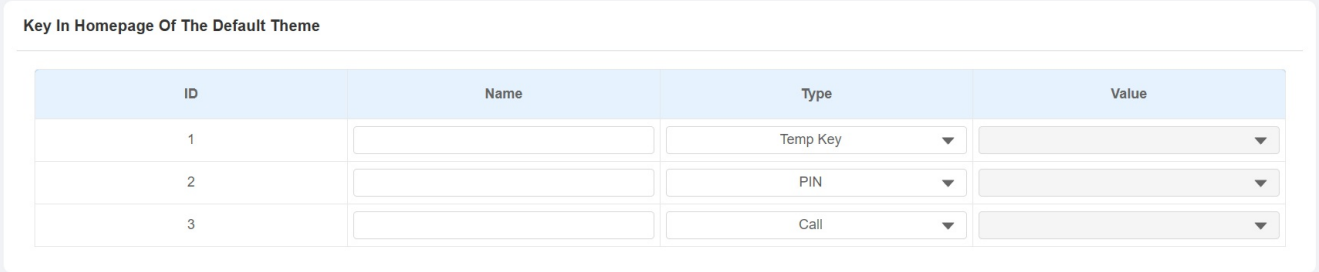
- **Interval(Sec)**: ustawienie czasu wyświetlania każdego przesłanego zdjęcia w **Interval (Sec.).** Zakres czasu wyświetlania wynosi od **1 do 120** sekund. Ustawienie domyślne to 5 sekund.

Uwaga

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

Konfiguracja ekranu głównego

W razie potrzeby można zmienić wyświetlanie ekranu głównego poprzez konfigurację nazwy karty i układu kart w interfejsie internetowym urządzenia. Ścieżka: **Device > LCD > Key In Homepage Of The Building Theme** .



Konfiguracja parametrów :

- **Typ**: wybierz typ zakładki odpowiadający numerowi indeksu, który wskazuje pozycję zakładki. Na przykład, jeśli chcesz, aby zakładka **Speed Dial** była wyświetlana w pozycji pierwszej, możesz zmienić typ w indeksie numer 1 na **Speed Dial**. Można również odpowiednio zmienić inną pozycję zakładki.
- **Nazwa** : wprowadź nową nazwę, aby zastąpić oryginalną nazwę typu, ale nie zmienia atrybutu typu.
- **Wartość** : wprowadź numer IP lub SIP, który ma zostać dołączony do ikony odbioru w celu szybkiego wybierania. Wprowadzony numer zostanie wybrany po naciśnięciu ikony odbioru na ekranie głównym. To pole jest ważne tylko dla szybkiego wybierania.

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.

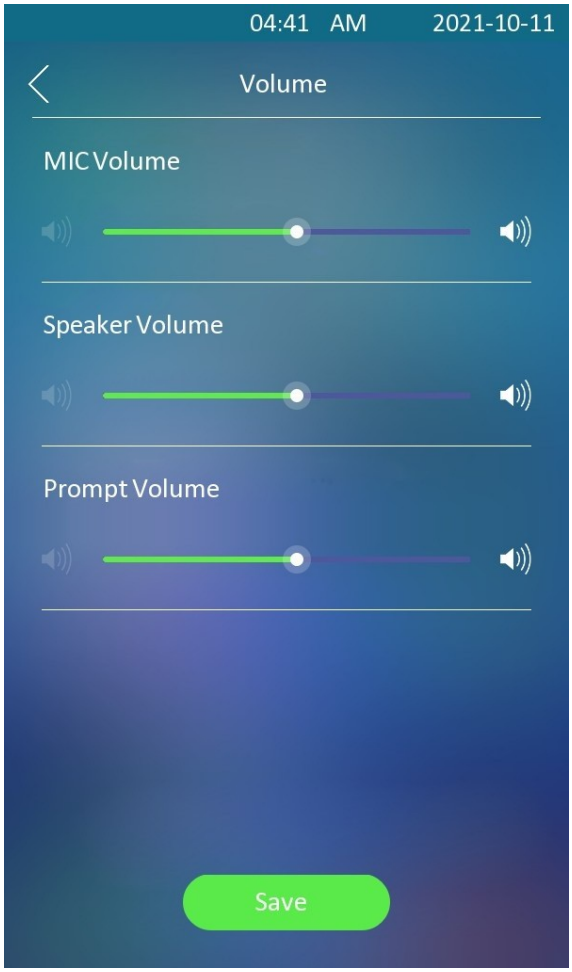
Konfiguracja głośności

Głośność Mic można skonfigurować zgodnie z potrzebami powiadamiania o otwartych drzwiach. Co więcej, można również ustawić głośność alarmu sabotażowego, gdy dojdzie do niepożądanego usunięcia terminala kontroli dostępu.

Konfiguracja głośności na urządzeniu

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

Ścieżka: **Display&Sounds > Sounds** .

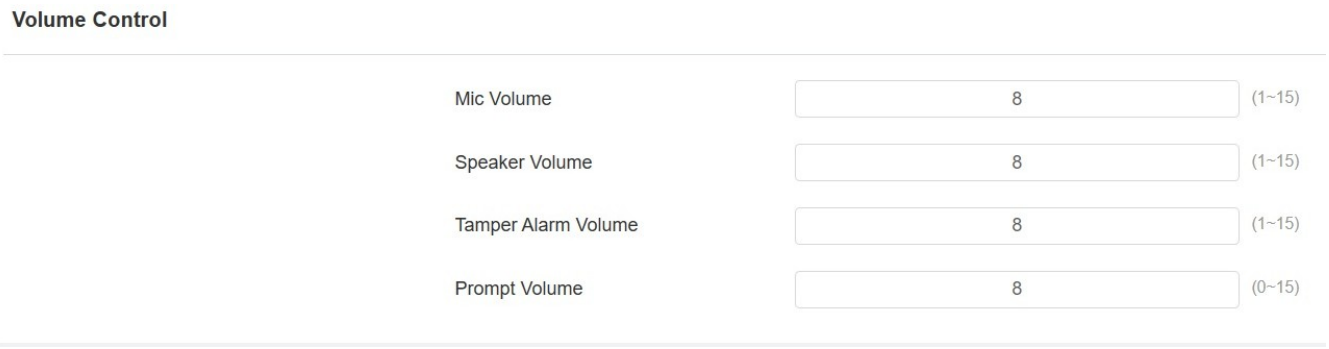


Konfiguracja parametrów :

- **Głośność** monitu: dostosuj głośność monitu, który obejmuje różne rodzaje dźwięków monitu o pomyślne i nieudane otwarcie drzwi, dźwięk zwrotny, dźwięk pomiaru temperatury itp.

Konfiguracja głośności w interfejsie internetowym

W interfejsie internetowym można ustawić głośność alarmu sabotażowego, głośność mikrofonu itp. Ścieżka: **Urządzenie > Audio > Regulacja głośności**.

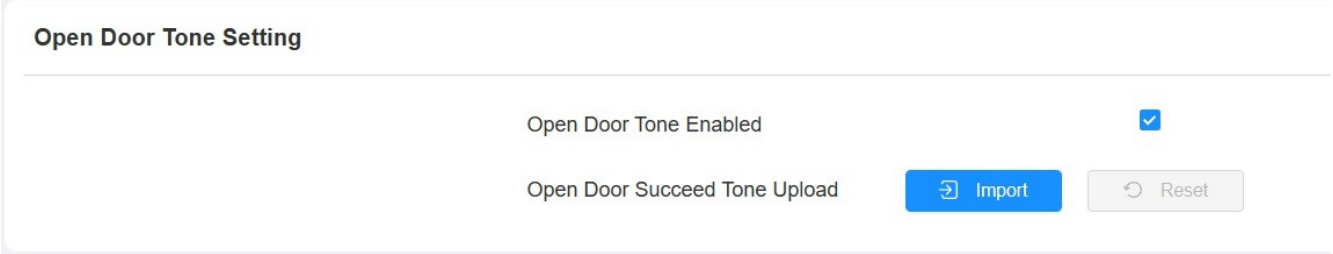


Konfiguracja parametrów:

Głośność komunikatów: regulacja głośności komunikatów, w tym różnych rodzajów dźwięków informujących o pomyślnym i nieudanym otwarciu drzwi, dzwonka, pomiaru temperatury itp.

Prześlij dźwięk otwartych drzwi

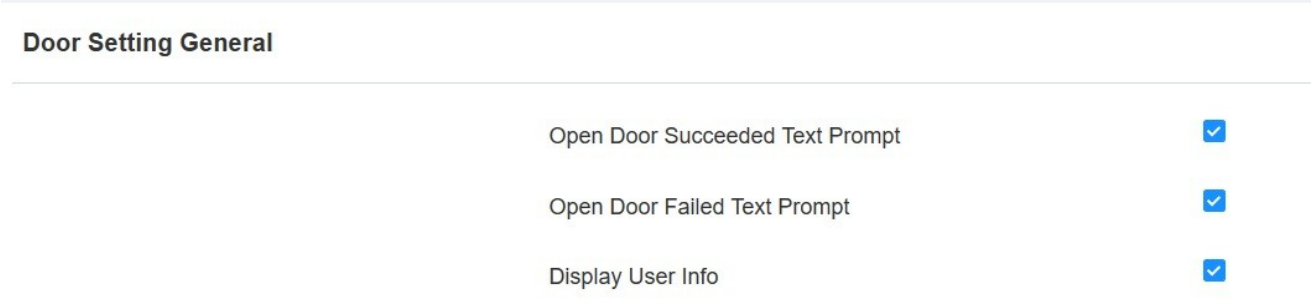
Sygnał dźwiękowy informujący o niepowodzeniu i powodzeniu otwarcia drzwi można przesłać w interfejsie internetowym urządzenia. Ścieżka: **Device >Audio > Open Door Tone Ustawienie.**



Konfiguracja tekstu monitu o otwarcie 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.

Ścieżka: **Kontrola dostępu > Przekaźnik > Ustawienia drzwi Ogólne**.

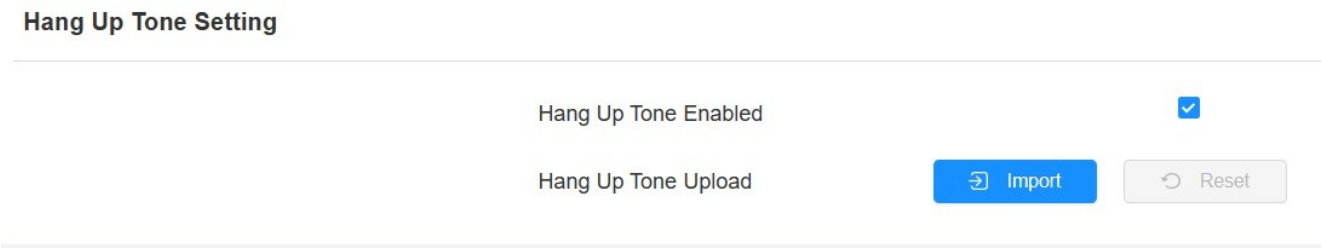


Konfiguracja parametrów :

- **Open Door Succeeded Text Prompt**: zaznacz pole wyboru, jeśli chcesz zobaczyć monit tekstowy po pomyślnym otwarciu drzwi i odwrotnie.
- **Open Door Failed Text Prompt**: zaznacz to pole wyboru, jeśli chcesz wyświetlać słowa zachęty po niepowodzeniu otwarcia drzwi i odwrotnie.

Konfiguracja sygnału rozłączenia

W razie potrzeby można dostosować dźwięk rozłączenia połączenia. Ścieżka: **Device > Audio > Hang Up Tone Setting** .



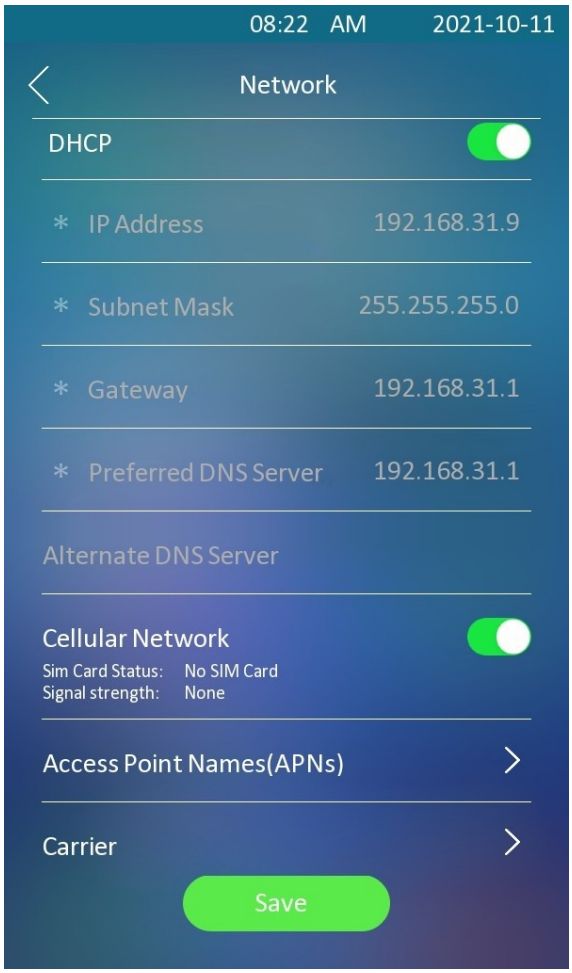
Konfiguracja parametrów :

- **Przesyłanie sygnału** rozłączenia: prześlij plik sygnału rozłączenia w formacie .wav. Rozmiar pliku nie może przekraczać 200 KB. Możesz kliknąć **Resetuj,** jeśli chcesz usunąć przesłany plik, a następnie zmienić go z powrotem na domyślny dźwięk rozłączenia.

Ustawienia sieciowe

Ustawienia połączenia sieciowego urządzenia

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

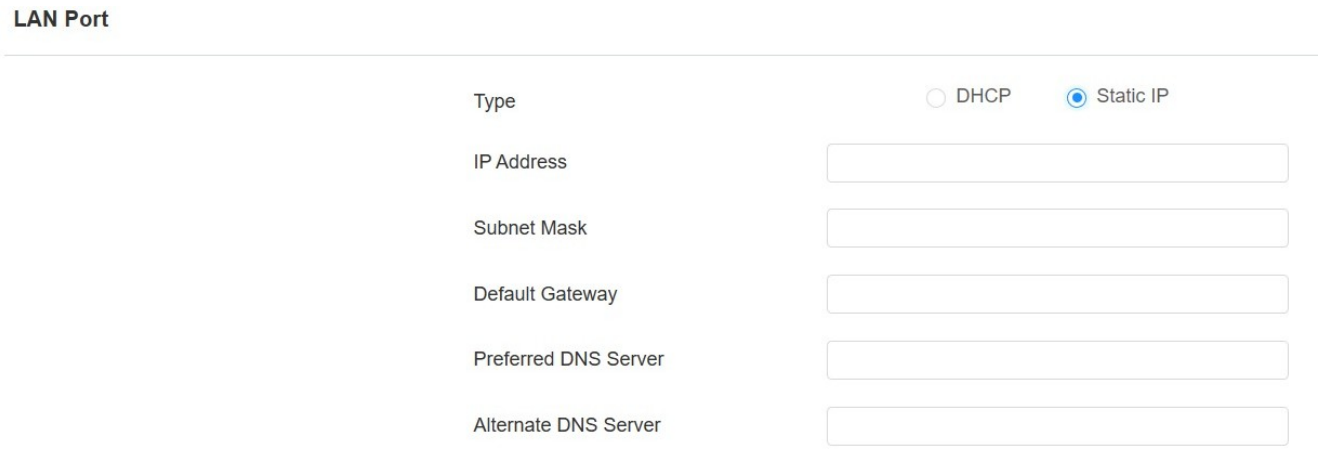


Konfiguracja parametrów :

- **DHCP** : wybierz tryb DHCP, przesuwając przełącznik w prawo. Tryb DHCP jest domyślnym połączeniem sieciowym. Jeśli tryb DHCP jest włączony, bramofon zostanie automatycznie przypisany przez serwer DHCP z adresem IP, maską podsieci, bramą domyślną 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. • **Default Gateway**: ustaw właściwą bramę zgodnie z adresem IP.
- **Preferred&Alternate DNS Server**: skonfiguruj preferowany lub alternatywny serwer DNS (**Domain Name Server**) zgodnie z rzeczywistym środowiskiem sieciowym. Preferowany serwer DNS to adres podstawowego serwera DNS, podczas gdy alternatywny serwer DNS to adres serwera pomocniczego, a bramofon połączy się z serwerem alternatywnym, gdy podstawowy serwer DNS będzie niedostępny.

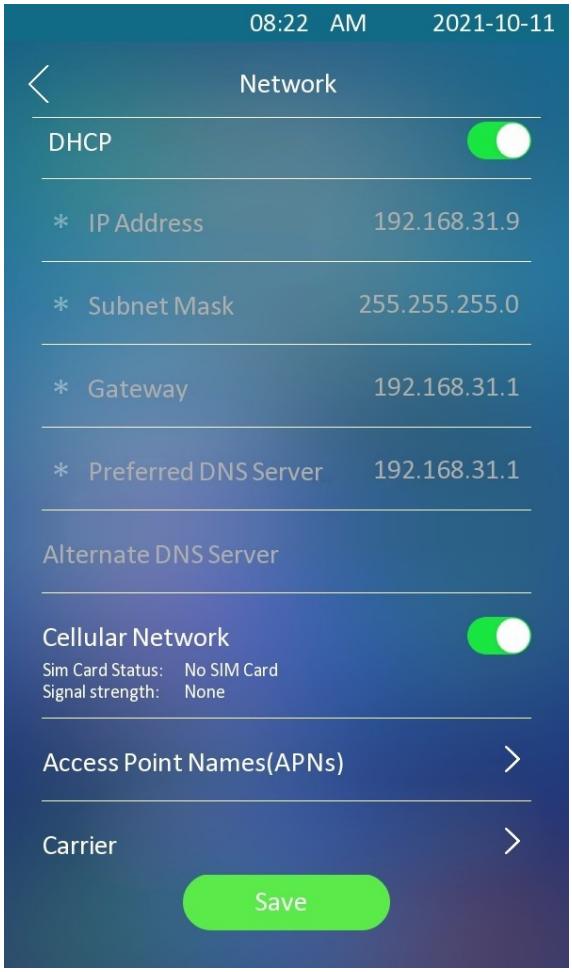
Można również skonfigurować ustawienia pracy sieci w interfejsie internetowym. Ścieżka: **Network > Basic > LAN Port**.

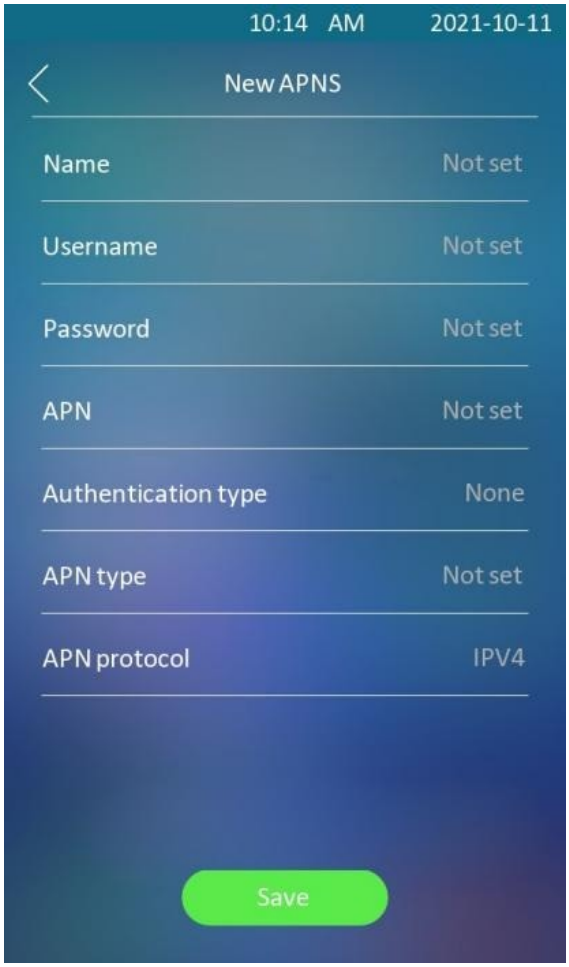


Ustawienia połączenia bezprzewodowego LTE

Moduł LTE umożliwia łączność urządzenia z siecią komórkową w obszarach, w których sieci przewodowe są niedostępne, co jest szczególnie korzystne w przypadku instalacji w starszych budynkach.

Ścieżka: **Sieć > Sieć komórkowa** .

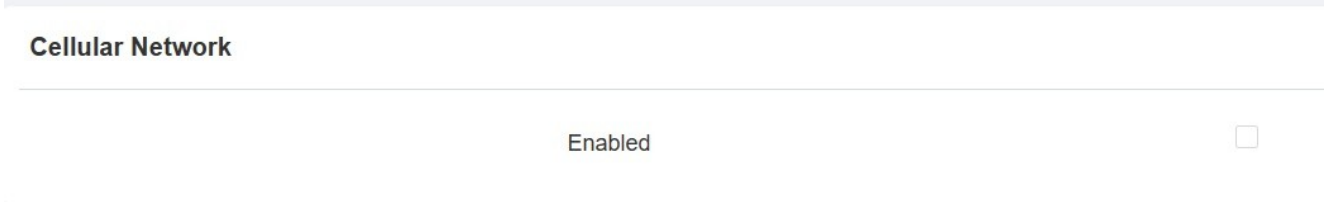




Konfiguracja parametrów :

- **Sieć komórkowa** : włączanie i wyłączanie przełącznika, aby włączyć lub wyłączyć funkcję LTE. Siła sygnału ma cztery poziomy: Słaby, Słaby, Dobry i Doskonały.
- **Nazwa punktu dostępu (APN)**: sprawdź dostawcę sieci komórkowej dla punktu dostępu. W razie potrzeby można również dodawać i usuwać APN-y ręcznie.
- **Przewoźnik**: włączenie lub wyłączenie sieci dostarczanej przez dostawcę usług sieciowych.

Można również włączyć lub wyłączyć sieć komórkową 4G. Ścieżka: **Sieć > Zaawansowane > Sieć komórkowa** .

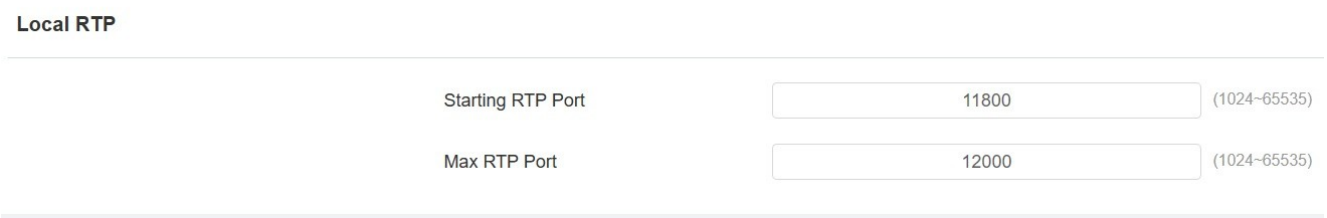


Konfiguracja lokalnego protokołu RTP urządzenia

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.

Ścieżka: **Sieć > Zaawansowane > Lokalny** interfejs **RTP.**



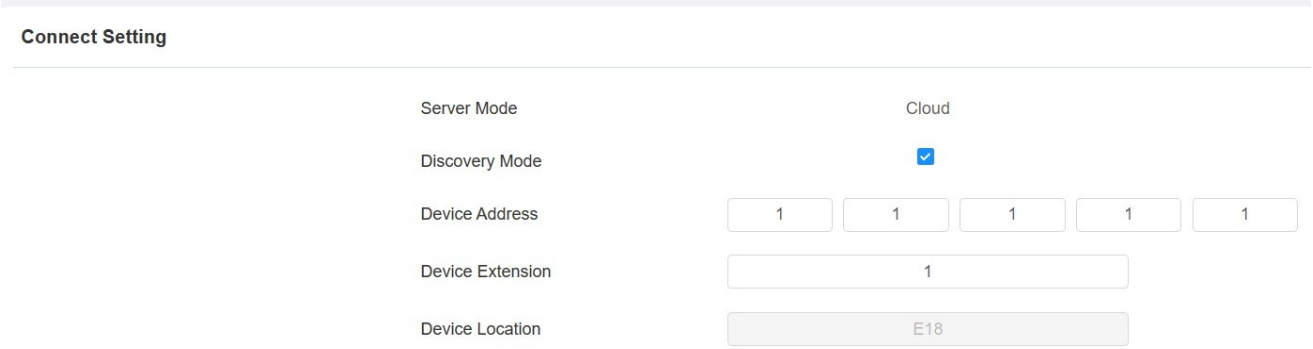
Konfiguracja parametrów :

- **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, skonfiguruj urządzenia interkomowe Akuvox, podając szczegóły, takie jak lokalizacja, tryb pracy, adres i numery wewnętrzne.

Ścieżka: **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 wskazującym, że urządzenie nie jest w żadnym typie

serwera. W związku z tym można

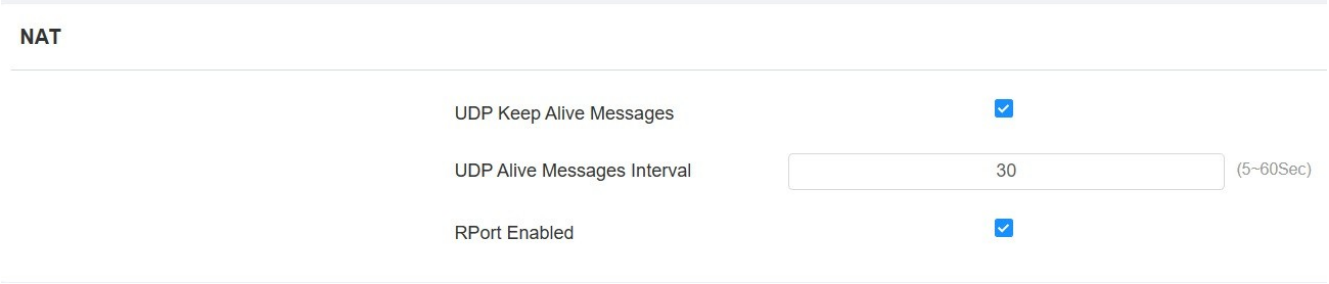
wybierz **Cloud** lub **SDMC** w trybie wykrywania.

- **Discovery Mode (Tryb wykrywania**): kliknij opcję **Enabled** (**Włączone)**, aby włączyć tryb wykrywania urządzenia, tak aby mogło być wykrywane przez inne urządzenia w sieci, lub kliknij opcję **Disabled (Wyłączone)**, jeśli chcesz ukryć urządzenie, aby nie było wykrywane przez inne urządzenia.
- **Węzeł urządzenia**: określ adres urządzenia, wprowadzając informacje o lokalizacji urządzenia od lewej do prawej: **Community (Społeczność), Unit (Jednostka), Stair (Schody)**, **Floor (Piętro)** i **Room (Pokój)** w kolejności.
- **Rozszerzenie urządzenia:** wprowadź numer rozszerzenia zainstalowanego urządzenia. • **Lokalizacja**: 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**).

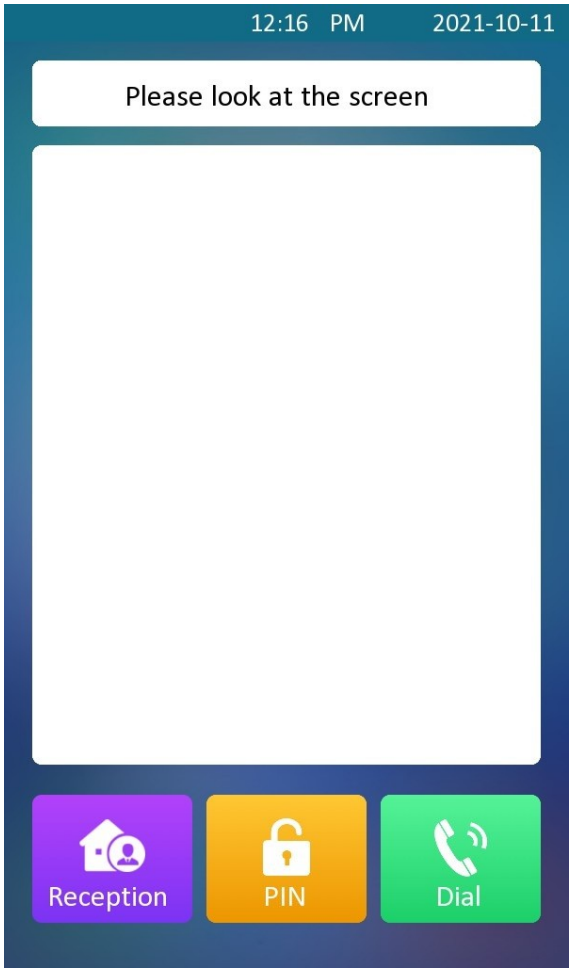
Konfiguracja połączeń interkomowych

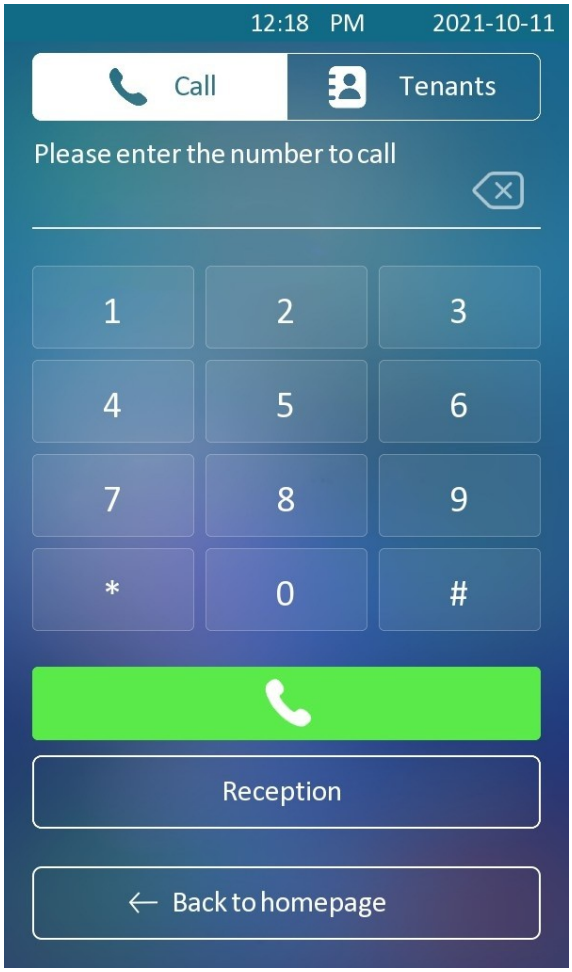
Konfiguracja połączeń IP i połączeń IP

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/SIP

Można nacisnąć kartę wybierania i wykonywać połączenia IP lub SIP.

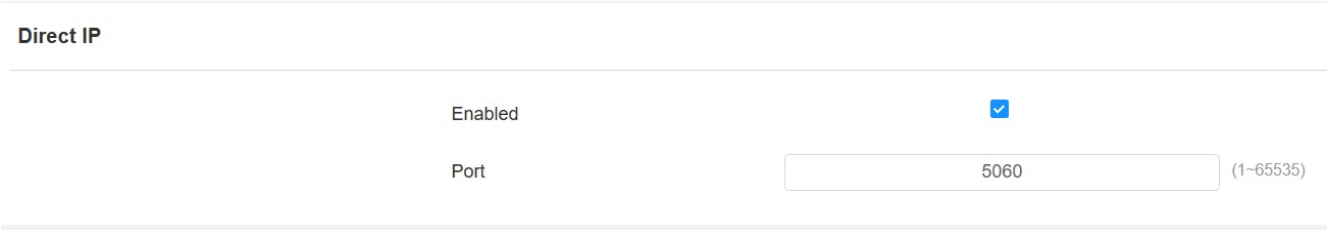




Konfiguracja połączeń IP

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.

Ścieżka: **Interkom > Podstawowe > Bezpośrednie IP** .



Konfiguracja parametrów :

- **Enabled** : zaznacz pole wyboru, aby **włączyć** lub **wyłączyć** bezpośrednie połączenie IP. Na przykład, jeśli nie zezwalasz na wykonywanie bezpośrednich połączeń IP na urządzeniu, możesz wyłączyć tę funkcję.
- **Bezpośredni port IP**: domyślny bezpośredni port IP to **5060** z zakresem portów od **1-65535**. Jeśli wprowadzisz jakiekolwiek wartości w zakresie innym niż 5060, musisz sprawdzić, czy wprowadzona wartość jest zgodna z odpowiednią wartością na

urządzeniu, z którym chcesz nawiązać połączenie.

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.

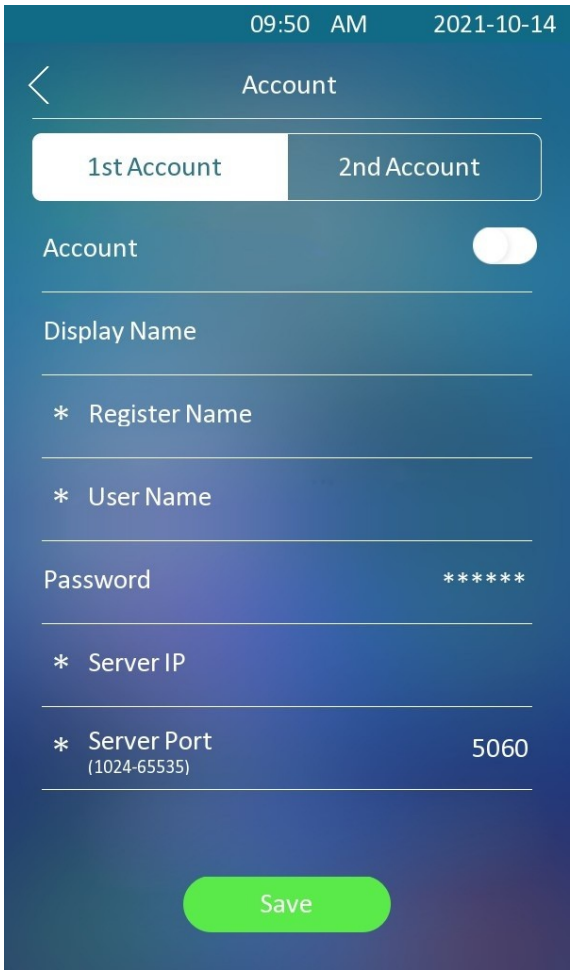
Rejestracja konta SIP

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 na urządzeniu

Aby skonfigurować konto SIP na urządzeniu. Ścieżka: **Konto**. **Nazwa rejestru, nazwa użytkownika** i **hasło** są dostarczane przez administratora konta SIP.

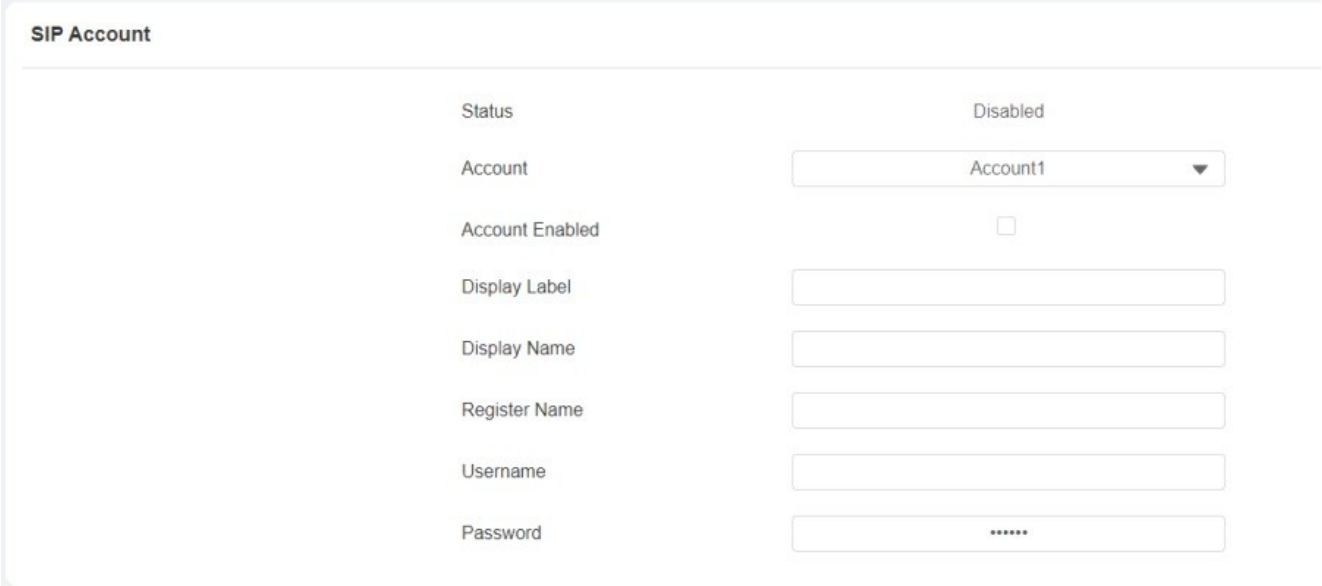


Konfiguracja parametrów :

- **Display Name** : skonfiguruj nazwę, na przykład nazwę urządzenia, która będzie wyświetlana na urządzeniu, z którym nawiązywane jest połączenie.
- **Server IP** : wprowadź adres serwera SIP dla wybranego konta SIP.
- **Port serwera**: wprowadź port serwera SIP do komunikacji. Domyślny port SIP to 5060.

Konfiguracja konta SIP w interfejsie internetowym

Aby przeprowadzić konfigurację w interfejsie internetowym, należy przejść do opcji **Konto > Podstawowe >** Interfejs **konta SIP. Nazwa rejestru, nazwa użytkownika** i **hasło** są dostarczane przez administratora konta SIP. Można wprowadzić maksymalnie 63 bajty znaków.



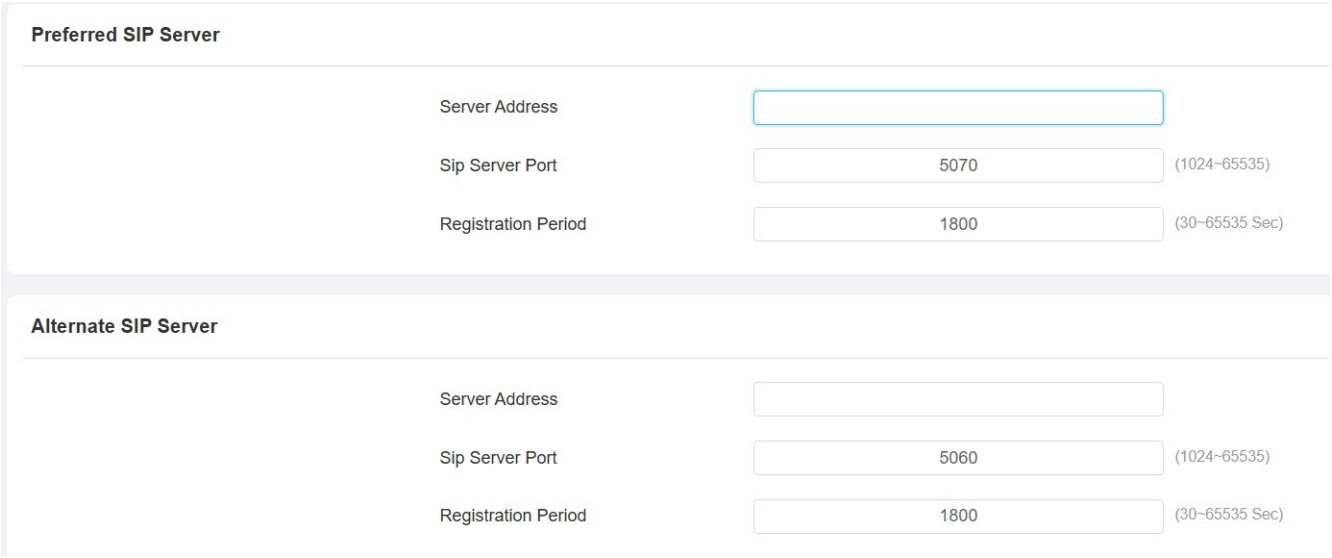
Konfiguracja parametrów :

- **Status**: sprawdza, czy konto SIP jest zarejestrowane, czy nie.
- **Konto**: wybierz dokładne konto (Konto 1 i 2), które ma zostać skonfigurowane.
- **Account Enabled** : zaznacz pole wyboru, aby włączyć lub wyłączyć zarejestrowane konto SIP.
- **Display Name** : skonfiguruj nazwę, na przykład nazwę urządzenia, która będzie wyświetlana na urządzeniu, z którym nawiązano połączenie. Można wpisać maksymalnie 63 bajty znaków.
- **Display Label**: skonfiguruj etykietę urządzenia, która będzie wyświetlana na ekranie urządzenia. Można wprowadzić maksymalnie 63 bajty znaków.

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.

Ścieżka: **Konto > Podstawowe > Preferowany serwer SIP**.

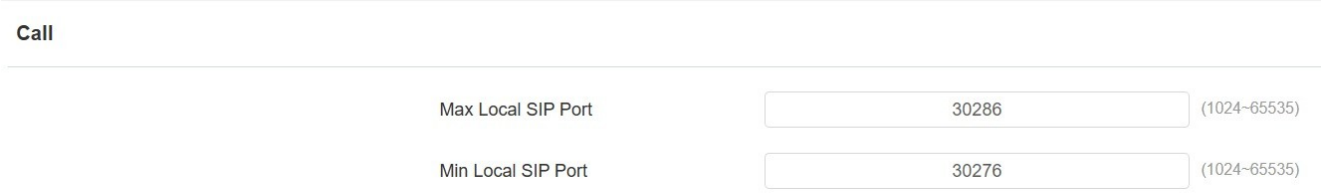


Konfiguracja parametrów :

- **Server Address (Preferowany serwer SIP)**: wprowadź numer adresu IP głównego serwera lub jego adres URL.
- **Server Address (Alternate SIP server)**: wprowadź adres IP zapasowego serwera SIP lub jego adres URL.
- **SIP Server 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**, w zakresie **30-65535s**.

Konfiguracja portów SIP dla połączeń SIP

Wymagane jest skonfigurowanie zakresu portów SIP do wykonywania połączeń SIP.
Przejdź do **Konto > Zaawansowane > Połączenie**.



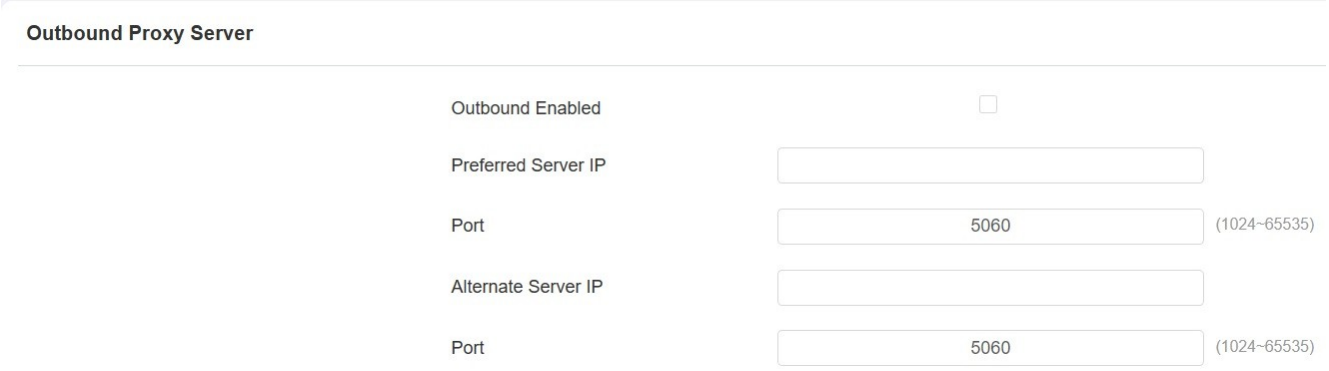
Konfiguracja parametrów :

- **Max Local SIP Port**: wprowadź maksymalny port SIP w zakresie od **1024** do **65535**. Domyślne ustawienie portu to 5062.
- **Min. lokalny port SIP**: wprowadź minimalny port SIP w zakresie od **1024** do **65535**. Domyślne ustawienie portu to 5062.

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.

Ścieżka: **Account > Basic > Outbound Proxy Server**.



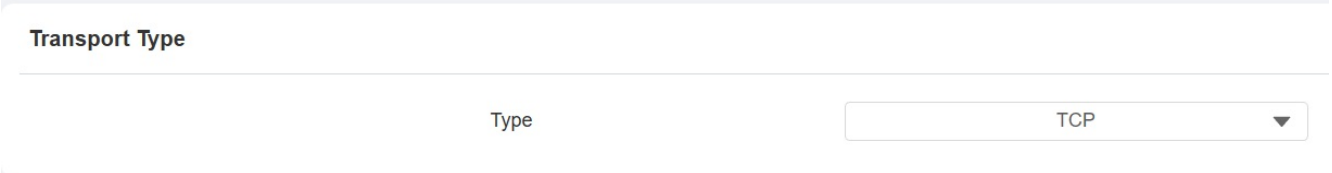
Konfiguracja parametrów :

- **Preferred Server IP** : wprowadź adres SIP serwera proxy połączeń wychodzących.
- **Port**: wprowadź numer portu do nawiązywania sesji połączeń przez wychodzący serwer proxy• **Alternate Server IP**: skonfiguruj adres IP serwera zapasowego dla zapasowego wychodzącego serwera proxy.
- **Port:** wprowadź numer portu, aby ustanowić sesję połączenia za pośrednictwem zapasowego serwera proxy wychodzącego.

Konfiguracja typu transmisji danych

Urządzenia interkomowe Akuvox obsługują cztery protokoły transmisji danych: **User Datagram Protocol(UDP)**, **Transmission Control Protocol(TCP**), **Transport Layer Security**(**TLS**) oraz **DNS-SRV** .

Ścieżka: **Konto > Podstawowe > Typ transportu** .



Konfiguracja parametrów :

- **UDP** : wybierz **UDP** dla zawodnego, ale bardzo wydajnego protokołu warstwy transportowej. UDP jest domyślnym protokołem transportowym.

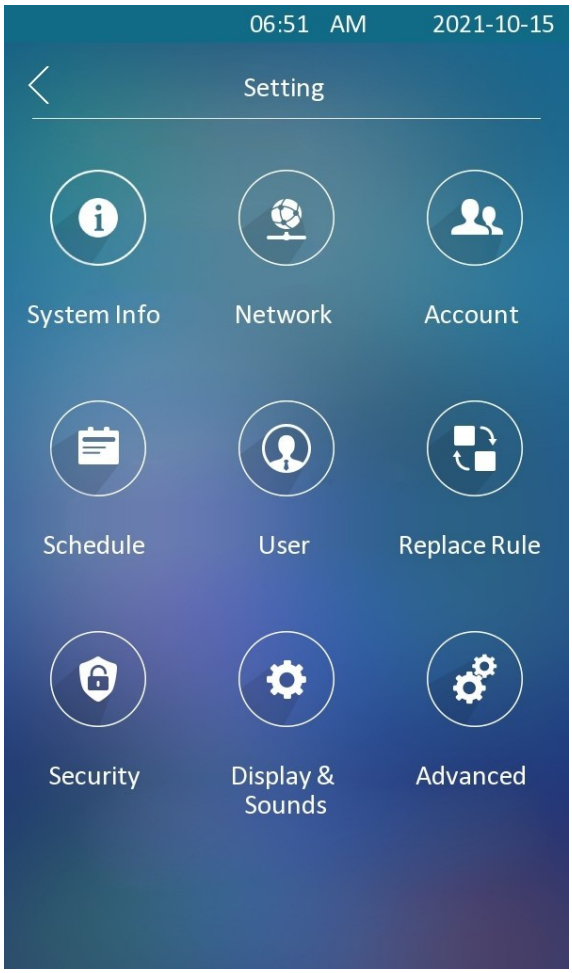
- **TCP** : wybierz **TCP** dla niezawodnego, ale mniej wydajnego protokołu warstwy transportowej. • **TLS** : wybierz **TLS** dla bezpiecznego i niezawodnego protokołu warstwy transportowej.
- **DNS-SRV** : wybierz **DNS-SRV**, aby uzyskać rekord DNS określający lokalizację usług. SRV rejestruje nie tylko adres serwera, ale także port serwera. Ponadto SRV może być również używany do konfigurowania priorytetu i wagi adresu serwera.

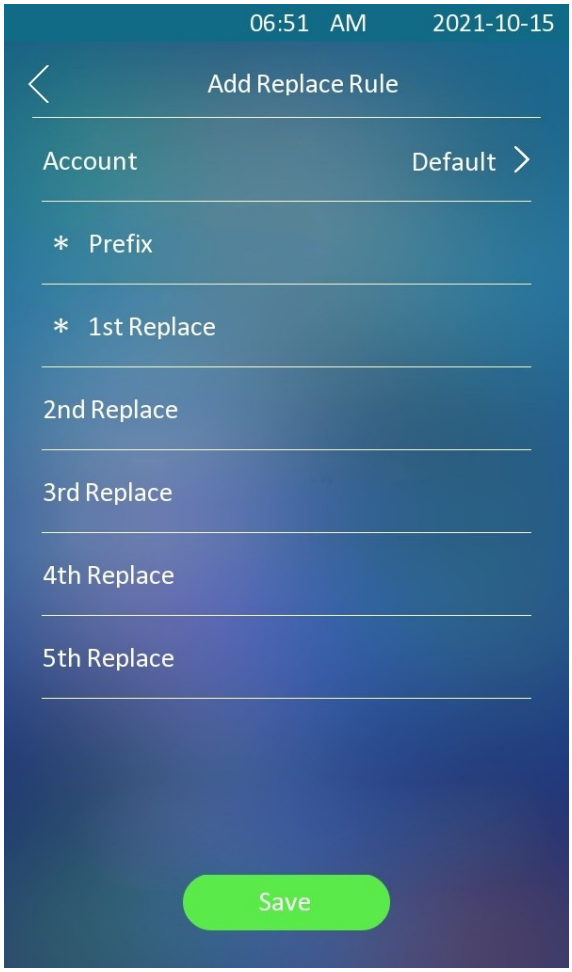
Konfiguracja opcji wybierania numeru
Szybkie wybieranie numeryczne

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, pojedynczym, uproszczonym numerem.

Szybkie wybieranie według numeru na urządzeniu

Długi numer SIP/IP można zastąpić krótkim numerem na urządzeniu. Ścieżka: **Zastąp regułę > Dodaj regułę zastępowania** .





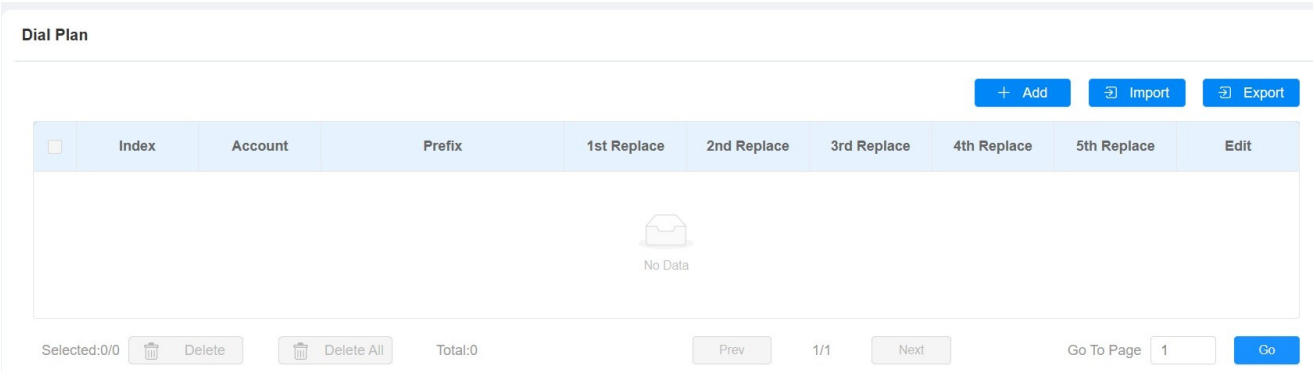
Konfiguracja parametrów :

- **Konto**: wybierz konto, do którego ma zostać zastosowana zamiana numeru wybierania. Domyślnie jest to konto **Auto** (wybieranie z konta, na którym zarejestrowano wybierany numer). Można wybrać konto 1 lub konto 2, z którego numer ma być wybierany. Jeśli wybierany numer 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 wybrany numer.
- **Replace 1/2/3/4/5** : wprowadź wybierane numery, 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 wybranym numerem zostanie wywołanych w tym samym czasie po wybraniu **101** .

Szybkie wybieranie przez zamianę numeru w sieci

Można nie tylko dodać numer szybkiego wybierania osobno, ale także zaimportować numer szybkiego wybierania do urządzenia wsadowo. Ponadto w razie potrzeby można edytować i usuwać numery.

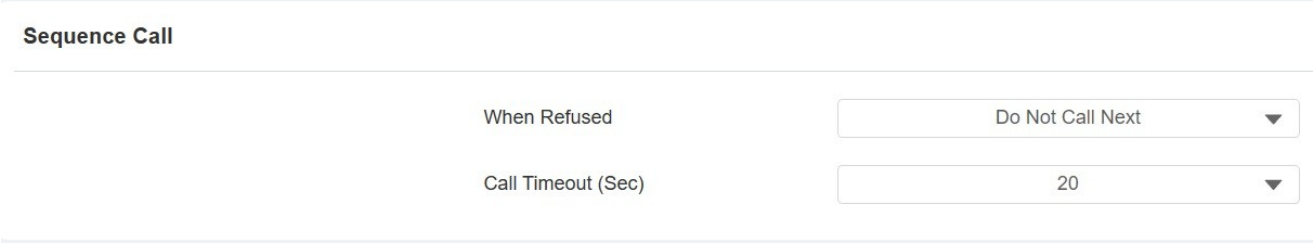
Ścieżka: **Interkom > Plan wybierania**.



Wywołanie sekwencji

Połączenie sekwencyjne to funkcja, która umożliwia wybieranie grupy numerów w określonej kolejności, aż jeden z nich odbierze połączenie. Funkcja ta jest obsługiwana przez aplikację Akuvox SmartPlus, która zapewnia zestaw numerów połączeń sekwencyjnych dla aplikacji.

Aby przeprowadzić konfigurację w interfejsie internetowym **Intercom > Basic > Sequence Call.**



Konfiguracja parametrów:

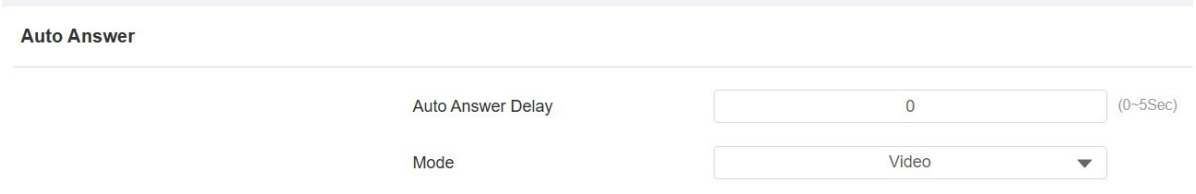
- **W przypadku odmowy**: w przypadku wybrania opcji **Nie dzwoń dalej**, połączenie sekwencyjne zostanie zakończone, jeśli zostanie odrzucone przez rozmówcę. Jeśli wybierzesz opcję **Call Next**, połączenie sekwencyjne będzie kontynuowane do następnego rozmówcy, jeśli zostanie odrzucone przez pierwszego rozmówcę.

Konfiguracja automatycznego odbierania połączeń

Funkcja automatycznego odbierania pozwala urządzeniu 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.

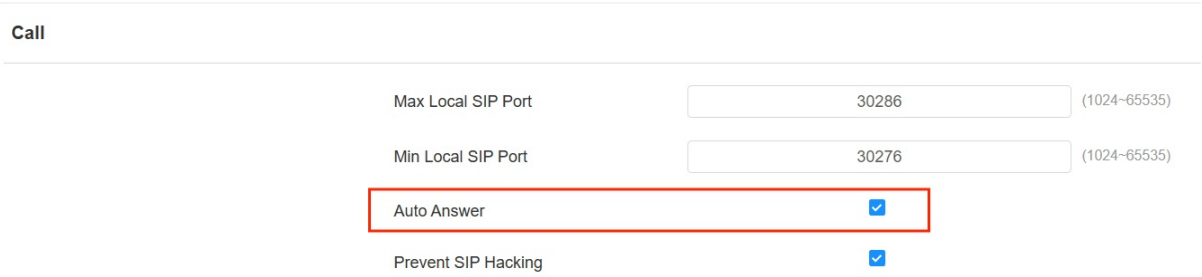
Konfiguracja funkcji automatycznego odbierania połączeń

Ścieżka: **Interkom > Funkcja połączenia > Automatyczne odbieranie** .



- Włącz tryb automatycznej odpowiedzi

Ścieżka: **Konto > Zaawansowane > Połącz**.



Konfiguracja parametrów :

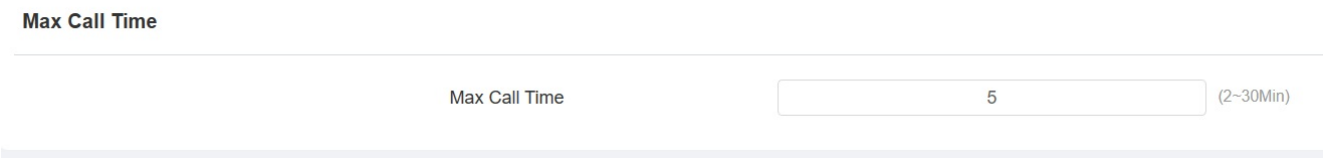
- **Auto Answer Delay**: ustaw czas opóźnienia (**od 0 do 5 sekund**) przed automatycznym odebraniem połączenia. Na przykład, jeśli ustawisz czas opóźnienia na 1 sekundę, połączenie zostanie automatycznie odebrane w ciągu 1 sekundy.
- **Tryb automatycznego odbierania połączeń**: ustaw preferowany tryb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

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.

Ścieżka: **Interkom > Funkcja połączenia > Maksymalny czas połączenia**



Konfiguracja parametrów:

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

Uwaga

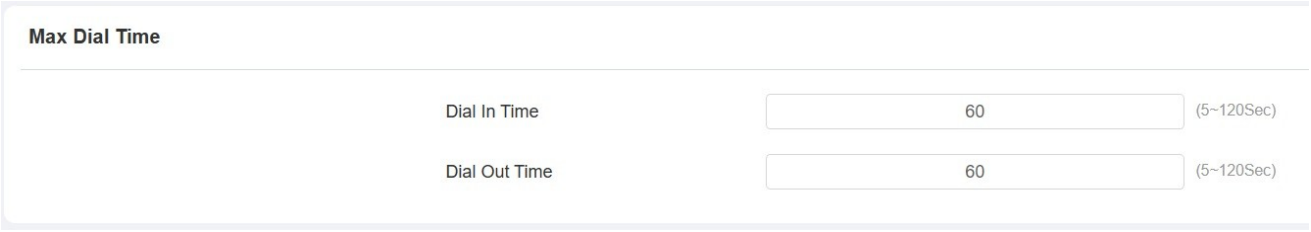
- Maksymalny czas połączenia urządzenia jest również powiązany z maksymalnym czasem połączenia serwera SIP. Jeśli
  Korzystając z konta SIP do nawiązywania połączeń, należy zwrócić uwagę na maksymalny czas połączenia serwera SIP. Jeśli maksymalny czas połączenia serwera SIP jest krótszy niż maksymalny czas połączenia urządzenia, dostępny jest krótszy czas.

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.

Ścieżka: **Interkom > Funkcja połączenia> Maksymalny czas wybierania** .



Konfiguracja parametrów :

- **Dial In Time** : wprowadź czas wybierania numeru dla bramofonu (**w zakresie od 30 do 120 sekund**). Na przykład, jeśli ustawisz czas wybierania numeru na 60 sekund w swoim bramofonie, wówczas bramofon automatycznie rozłączy połączenie przychodzące, jeśli połączenie nie zostanie odebrane przez bramofon w ciągu 60 sekund. Domyślnym czasem wybierania numeru jest 60 sekund.
- **Dial Out Time** : wprowadź czas wybierania numeru dla bramofonu (**w zakresie 5-120 sekund**). Na przykład, jeśli ustawisz czas wybierania na 60 sekund w swoim bramofonie, wówczas bramofon automatycznie rozłączy wybrane połączenie, jeśli nie zostanie ono odebrane przez urządzenie, z którym nawiązano połączenie.

Uwaga

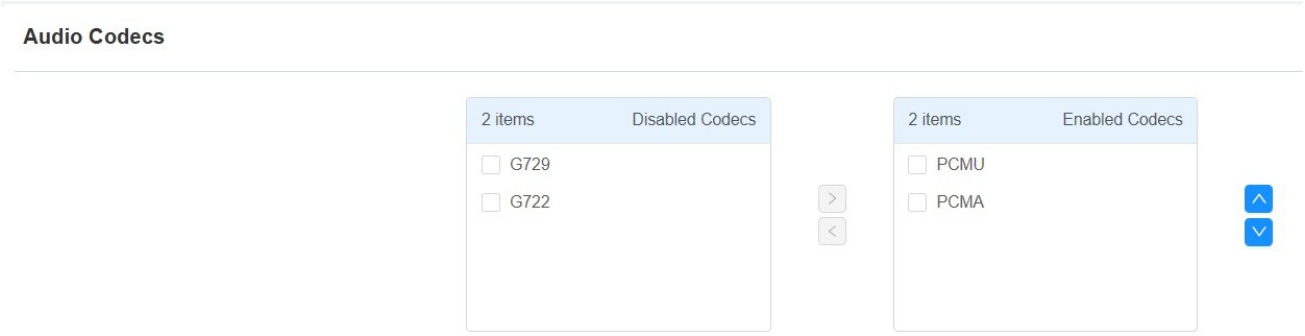
- Maksymalny czas wybierania numeru urządzenia jest również związany z maksymalnym czasem wybierania numeru serwera SIP. Jeśli używasz konta SIP do wykonywania połączeń, zwróć uwagę na maksymalny czas wybierania numeru serwera SIP. Jeśli maksymalny czas wybierania numeru serwera SIP jest krótszy niż maksymalny czas wybierania numeru urządzenia, obowiązuje ten krótszy czas.

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.

Ścieżka: **Konto > Zaawansowane > Kodeki audio** .



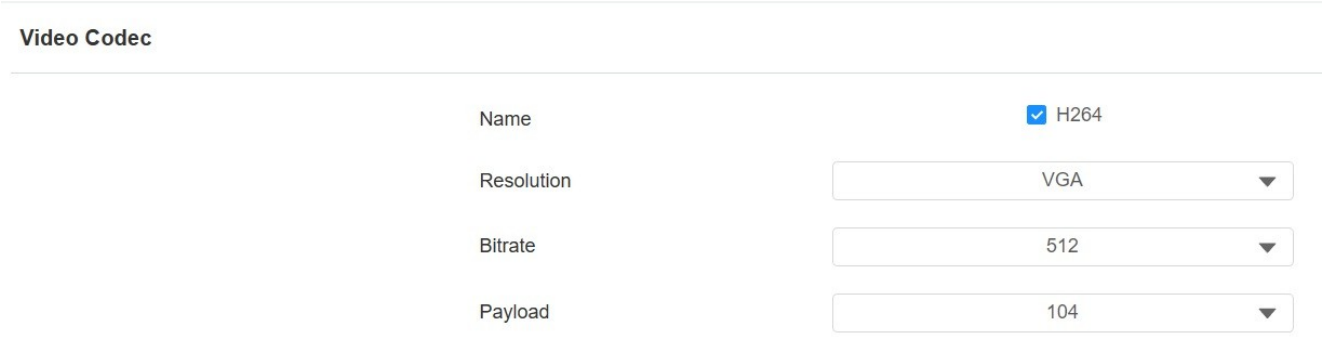
Poniżej znajdują się informacje na temat zużycia pasma **i częstotliwości próbkowania dla czterech typów kodeków:**

Codec Type	Bandwidth Consumption	Sample Rate
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.

Ścieżka: **Konto > Zaawansowane > Kodeki wideo** .



Konfiguracja parametrów :

- **Nazwa** : Zaznacz, aby wybrać format kodeka wideo H264 dla strumienia wideo z bramofonu. Domyślnym kodekiem wideo jest H264.
- **Rozdzielczość**: wybierz rozdzielczość kodu dla jakości wideo spośród pięciu opcji: **QCIF, CIF, VGA, 4CIF** , i **720P** zgodnie z rzeczywistym środowiskiem sieciowym.

Domyślną rozdzielczością jest **VGA** .

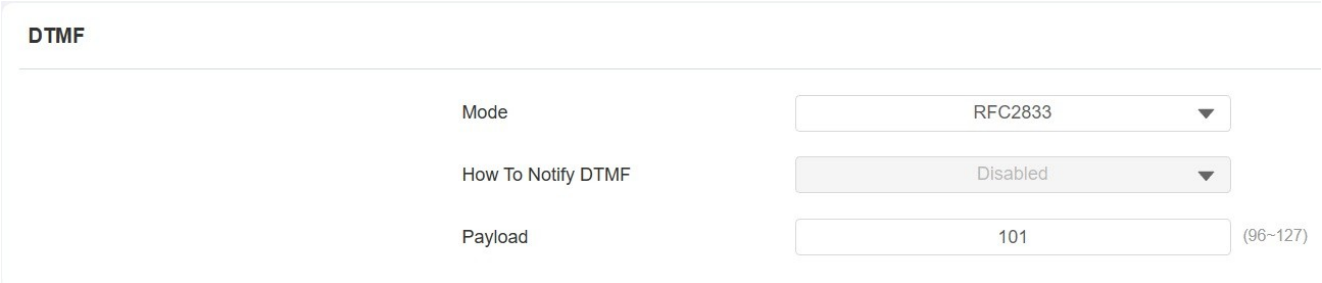
- **Bitrate**: wybór szybkości transmisji strumienia wideo (w zakresie **128-2048**). Im większa szybkość transmisji bitów, tym większa ilość danych przesyłanych w każdej sekundzie, dzięki czemu obraz wideo będzie wyraźniejszy. Domyślna szybkość transmisji kodu wynosi 512.

- **Payload (Ładunek)**: wybierz typ ładunku (w zakresie **90-119**), aby skonfigurować ładunek kodeka audio. Ładunek między bramofonem a odpowiednim urządzeniem interkomowym powinien być identyczny. 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.

Ścieżka: **Konto > Zaawansowane > DTMF** .



Konfiguracja parametrów :

- **Tryb** : wybór trybu DTMF spośród sześciu opcji: **Inband, RFC 2833, Info, Info+Inband**, **Info+RFC 2833** oraz **Info+Inband+RFC 2833 w** oparciu o określony typ transmisji DTMF urządzenia strony trzeciej, z którym ma zostać nawiązane połączenie jako strona odbierająca dane sygnału.
- **Jak powiadamiać DTMF**: wybierz jeden z czterech typów: **Disable, DTMF, DTMF-Relay** i **Telephone-Event** zgodnie z określonym typem przyjętym przez urządzenie zewnętrzne.

Konfiguracja jest wymagana tylko wtedy, gdy urządzenie innej firmy, z którym ma zostać nawiązane połączenie, przyjmuje tryb **Info.**

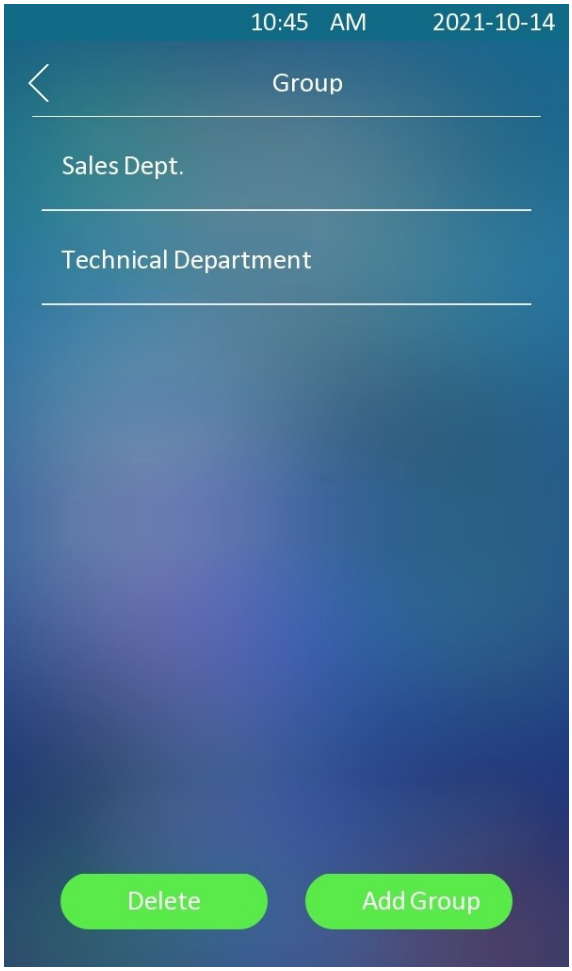
- **Payload**: ustawia ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą i odbiorcą podczas transmisji danych.

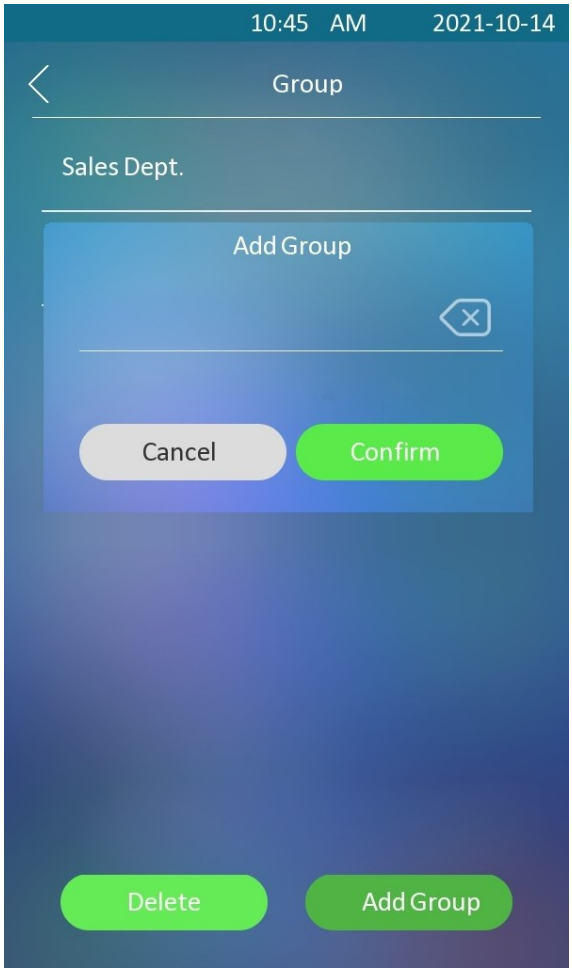
Konfiguracja książki telefonicznej

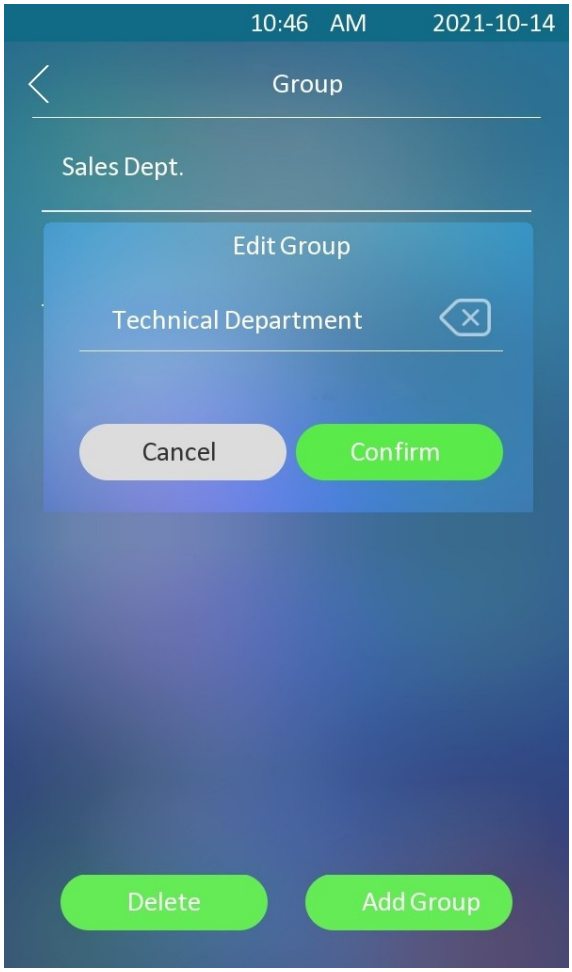
Konfiguracja książki telefonicznej na urządzeniu

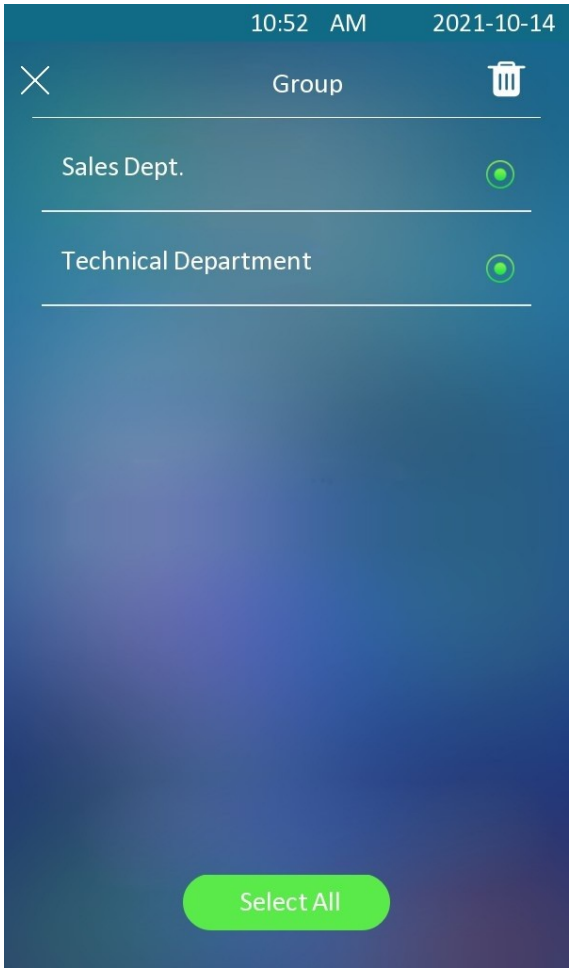
Można tworzyć grupy kontaktów dla użytkowników.

Aby skonfigurować książkę telefoniczną na urządzeniu **Użytkownik > Grupa** .




10:45 AM 2021-10-14
Group
Sales Dept.
Add Group
Cancel
Confirm
Delete
Add Group


10:46 AM 2021-10-14
Group
Sales Dept.
Edit Group
Technical Department
Cancel
Confirm
Delete
Add Group

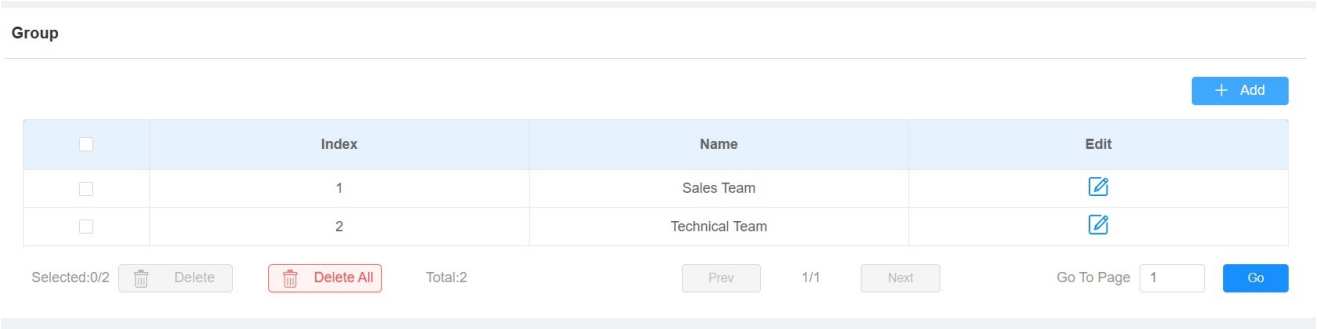


Konfiguracja książki telefonicznej w interfejsie sieciowym

Zarządzanie grupami kontaktów w interfejsie internetowym

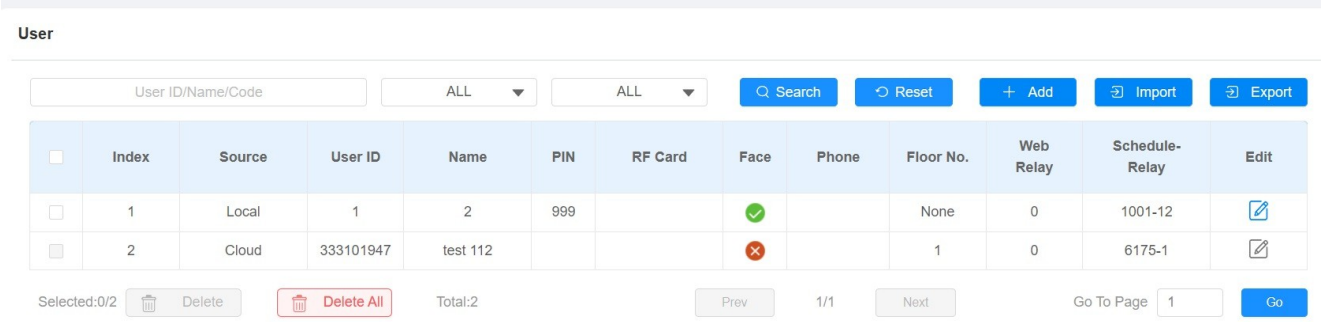
Można utworzyć i edytować grupę kontaktów dla kontaktów. Grupa kontaktów będzie używana podczas dodawania użytkownika.

Ścieżka: **Katalog > Użytkownik> Grupa** .



Konfiguracja listy kontaktów w interfejsie internetowym

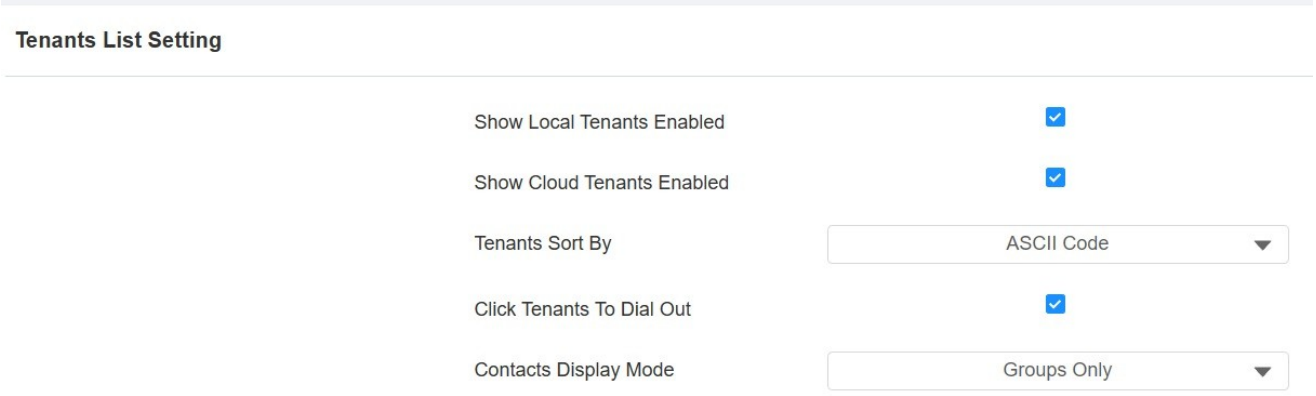
Kontakt można również skonfigurować w interfejsie internetowym, gdzie w razie potrzeby można również przesłać zdjęcia kontaktu. Aby skonfigurować konfigurację w **katalogu** internetowym **>**



Ustawienia wyświetlania listy kontaktów

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

Ścieżka: **Directory > Directory Setting> Tenants List Setting** .



Konfiguracja parametrów :

- **Show Local Tenants Enabled** : zaznacz lub odznacz pole wyboru, aby kontrolować wyświetlanie etykiety grupy. Po odznaczeniu tego pola wyboru wyświetlana będzie tylko karta grupy, a karta kontaktu będzie ukryta i odwrotnie.
- **Show Cloud Tenants Enabled**: zaznacz pole wyboru, aby wyświetlić dzierżawców chmury na liście dzierżawców. Po usunięciu zaznaczenia pola wyboru najemcy w chmurze zostaną ukryci. **Tenants Sort By**: wybierz **ASCII Code, Room No.** lub **Import**. Po wybraniu opcji **ASCII Code** najemcy zostaną wyświetleni według nazw w kolejności kodu **ASCII**. Po wybraniu opcji **Room No.** najemcy zostaną posortowani według numerów pokoi. Po wybraniu opcji **Import** kontakty zostaną posortowane zgodnie z kolejnością w pliku importu.
- **Kliknij Tenants to Dial Out**: zaznacz pole wyboru, aby włączyć funkcję wybierania

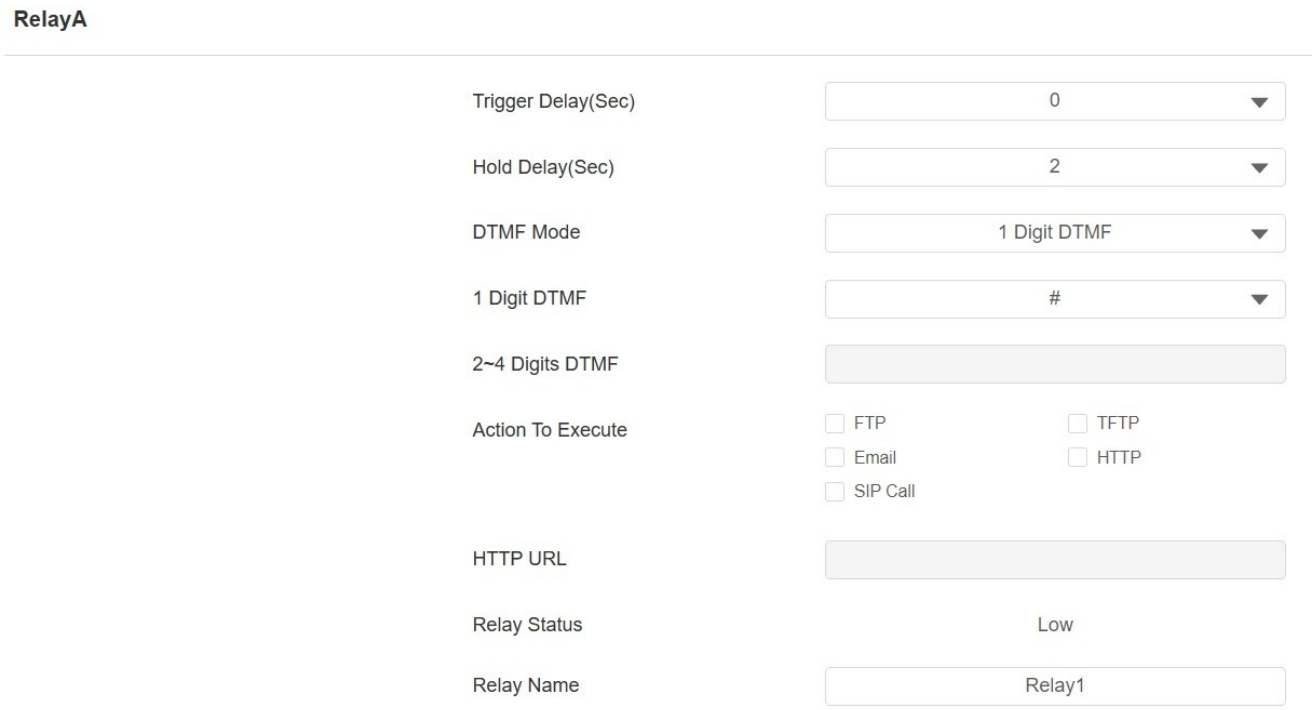
numeru poprzez naciśnięcie karty kontaktu. Gdy ta funkcja jest włączona, można nacisnąć dowolne miejsce na karcie kontaktu, aby wybrać. Ta funkcja zostanie wyłączona po odznaczeniu pola wyboru, a gdy jest wyłączona, należy nacisnąć ikonę połączenia, aby wybrać numer.

Tryb wyświetlania kontaktów : Wybierz spośród opcji **Tylko grupy, Wszystkie kontakty** i **Grupa na stronie wejściowej i ich kontakty na podstronie**. W przypadku wybrania opcji **Tylko grupy** można stuknąć grupę, aby zadzwonić do wszystkich kontaktów. Nazwa grupy jest wyświetlana podczas nawiązywania połączenia.

Ustawienie przekaźnika

Ustawienie przełącznika przekaźnika

Możesz odblokować drzwi za pomocą kodu DTMF podczas połączenia. W tym celu należy skonfigurować kod DTMF wraz z przekaźnikami. Ścieżka: **Kontrola dostępu > Przekaźnik >**



PrzekaźnikA

Konfiguracja parametrów :

- **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 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 zostanie opóźniony o 5 sekund po odblokowaniu drzwi.
- **Tryb DTMF**: wybór liczby cyfr DTMF dla kontroli dostępu do drzwi (w zakresie od 1 do 4 cyfr) Na przykład można wybrać 1-cyfrowy kod DTMF lub 2-cyfrowy kod DTMF itp. w zależności od potrzeb.
- **1 Digit DTMF**: ustawienie 1-cyfrowego kodu DTMF z zakresu (**0-9 i *,#**).

- **2~4 Digits 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.
- **Stan przekaźnika**: domyślnie stan przekaźnika jest niski, co oznacza normalnie zamknięty (NC). Jeśli stan przekaźnika jest wysoki, to jest w stanie normalnie otwartym (NO).
- **Nazwa przekaźnika**: nazwij przełącznik przekaźnika zgodnie z potrzebami. Dla wygody można na przykład nazwać przełącznik przekaźnika zgodnie z jego lokalizacją.

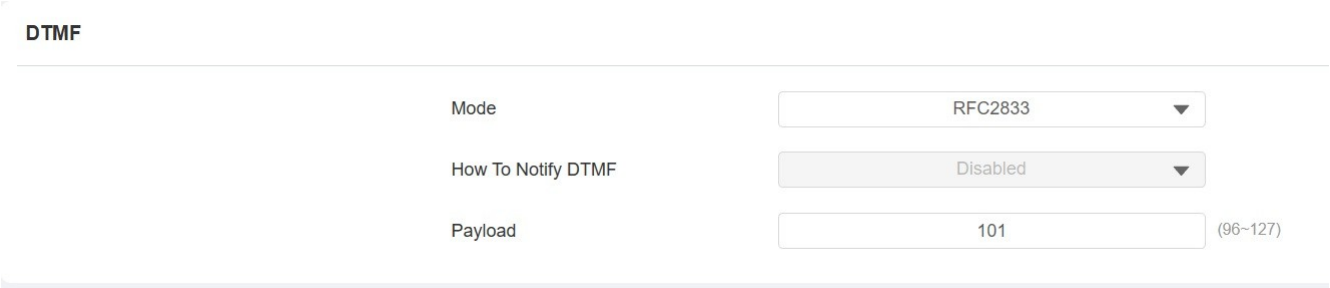
Uwaga

- Tylko zewnętrzne urządzenia podłączone do przełącznika przekaźnikowego muszą być zasilane z zewnętrznych adapterów, ponieważ przełącznik przekaźnikowy nie dostarcza zasilania.
- Jeśli tryb DTMF jest ustawiony na 1 Cyfrowy DTMF, nie możesz edytować kodu DTMF w polu DTMF 2-4 Cyfrowego. Natomiast, jeśli ustawisz tryb DTMF na 2-4 Cyfrowy w polu DTMF 2-4 Cyfrowego, nie będziesz mógł edytować kodu DTMF w polu 1 Cyfrowego DTMF.

Konfiguracja kodu DTMF

Dwutonowa sygnalizacja wieloczęstotliwościowa (**DTMF**) to sposób wysyłania sygnałów przez linie telefoniczne przy użyciu różnych pasm częstotliwości głosu. Użytkownicy mogą korzystać z funkcji DTMF, aby odblokować drzwi dla gości podczas połączenia, wpisując kod DTMF na klawiaturze programowej lub dotykając zakładki odblokowania z kodem DTMF na ekranie.

Ścieżka: **Konto > Zaawansowane > DTMF** .



Konfiguracja parametrów :

- **Tryb**: wybór typu DTMF spośród sześciu opcji: **Inband, RFC 2833, Info, Info+Inband, Info+RFC 2833** oraz **Info+Inband+RFC 2833** w zależności od potrzeb.
- **Format transportu kodu DTMF**: wybierz jedną z czterech opcji: **Disable, DTMF, DTMF- Relay, Telephone-Event w zależności od** potrzeb.
- **Payload (Ładunek)**: wybierz ładunek 96-127 do identyfikacji transmisji danych. Domyślnym ładunkiem jest 101.

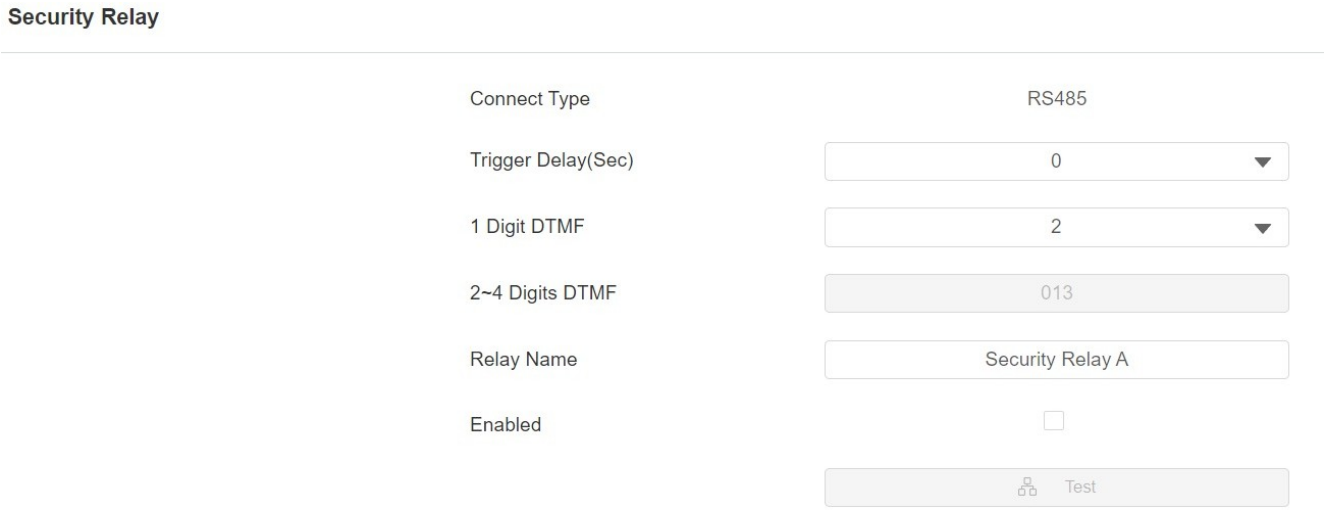
Uwaga

- Proszę odnieść się do sekcji **Konfigurowanie transmisji danych DTMF** w rozdziale **Konfiguracja połączeń interkomowych** w celu uzyskania szczegółowych informacji na temat ustawień kodu DTMF.
- Urządzenia interkomowe muszą być zgodne co do typu DTMF, w przeciwnym razie kod DTMF nie będzie działał.

Ustawienie przekaźnika bezpieczeństwa

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

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



Konfiguracja parametrów :

- **Typ połączenia**: wybierz typ połączenia między przekaźnikiem bezpieczeństwa a bramofonem. Można wybrać połączenie przez wyjście zasilania przekaźnika A bramofonu
- 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.
- **1 Digit DTMF**: ustawienie 1-cyfrowego kodu DTMF z zakresu (0-9 i *,#).

  2~4 Digits 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.

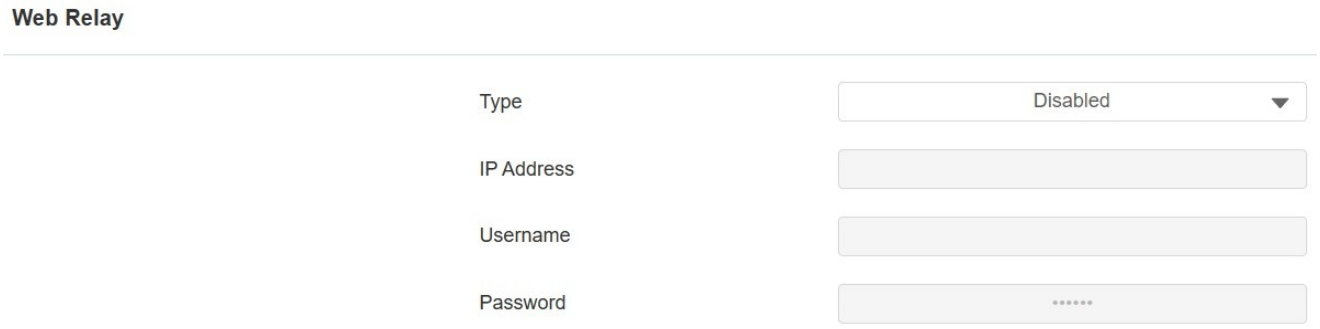
Ustawienia przekaźnika internetowego

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

Konfiguracja Web Relay w interfejsie sieciowym

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

Ścieżka: **Access Control > Web Relay**. Adres IP, nazwa użytkownika i hasło są dostarczane przez producenta przekaźnika internetowego.

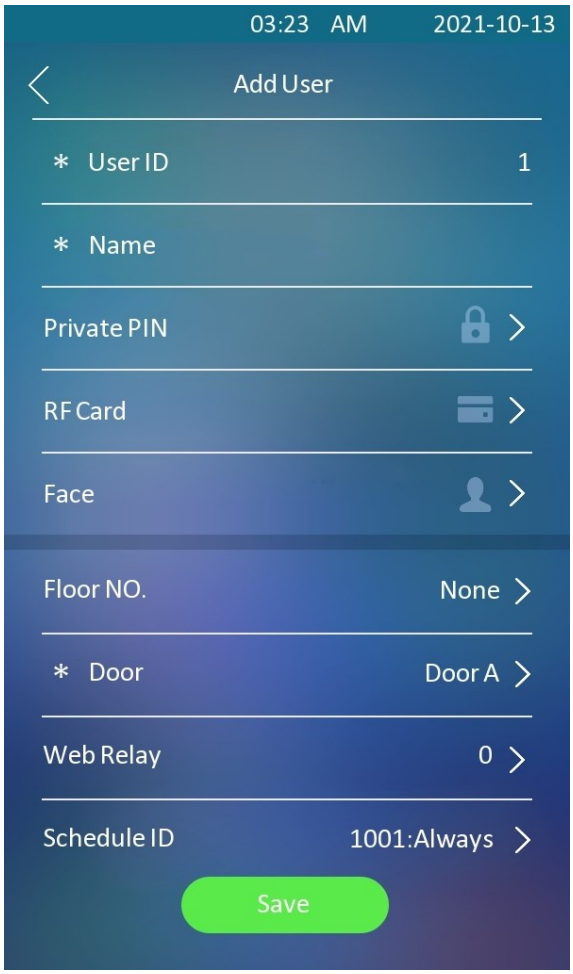


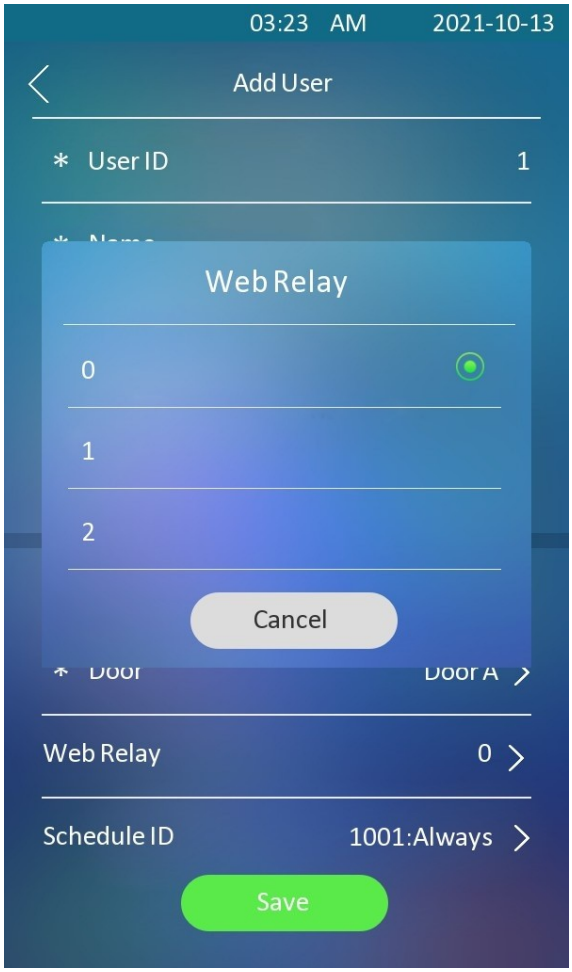
Konfiguracja parametrów :

- **Typ**: wybierz jedną z trzech opcji: **Wyłączone, Przekaźnik sieciowy** i **Oba.** Wybierz **Web Relay,** aby włączyć przekaźnik internetowy. Wybierz **Disable,** aby wyłączyć przekaźnik sieciowy. Wybierz opcję **Oba,** aby włączyć zarówno przekaźnik lokalny, jak i internetowy.
- **Hasło** : Hasła są 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** .

Konfiguracja funkcji Web Relay na urządzeniu

Po wprowadzeniu działań przekaźnika sieciowego w interfejsie sieciowym można teraz wybrać określoną liczbę działań przekaźnika sieciowego, które mają zostać wykonane dla określonego mieszkańca dodanego w celu odblokowania drzwi. Ścieżka: **Użytkownik > Lista**

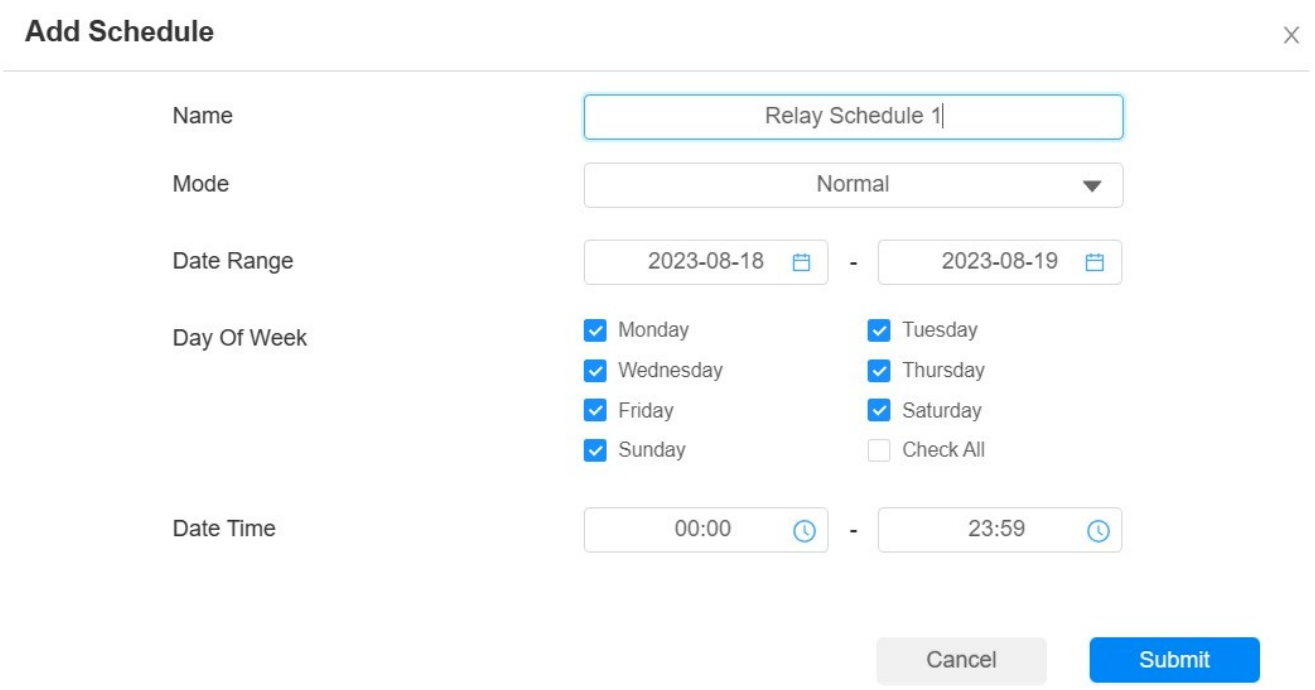




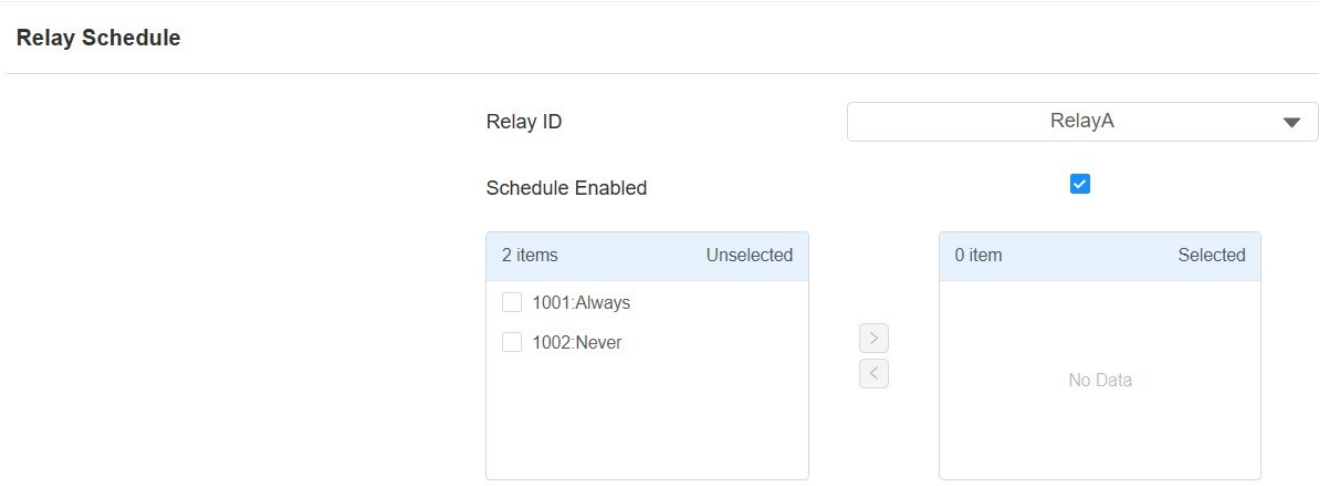
Harmonogram przekaźników

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

Przed zastosowaniem harmonogramu przekaźnika do konkretnego przekaźnika kontroli dostępu do drzwi należy najpierw ustawić harmonogram przekaźnika. Ścieżka: **Ustawienia > Harmonogram** .



Po utworzeniu harmonogramu przekaźnika można wybrać harmonogram przekaźnika i wybrać konkretny przekaźnik, do którego ma zostać zastosowany harmonogram. Ścieżka: **Kontrola**



Uwaga

- Informacje na temat ustawień harmonogramu przekaźnika można znaleźć w sekcji **Tworzenie harmonogramu dostępu do drzwi.**

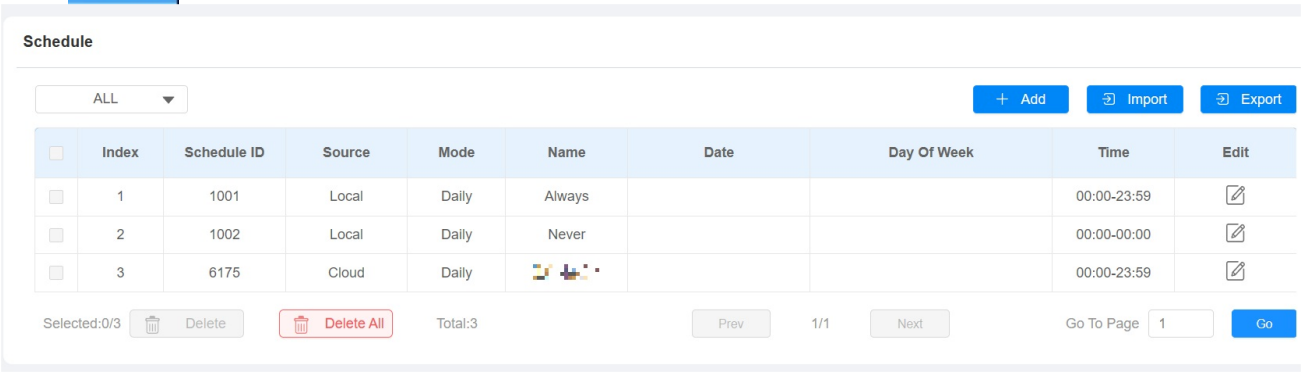
Zarządzanie harmonogramem dostępu do drzwi

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.

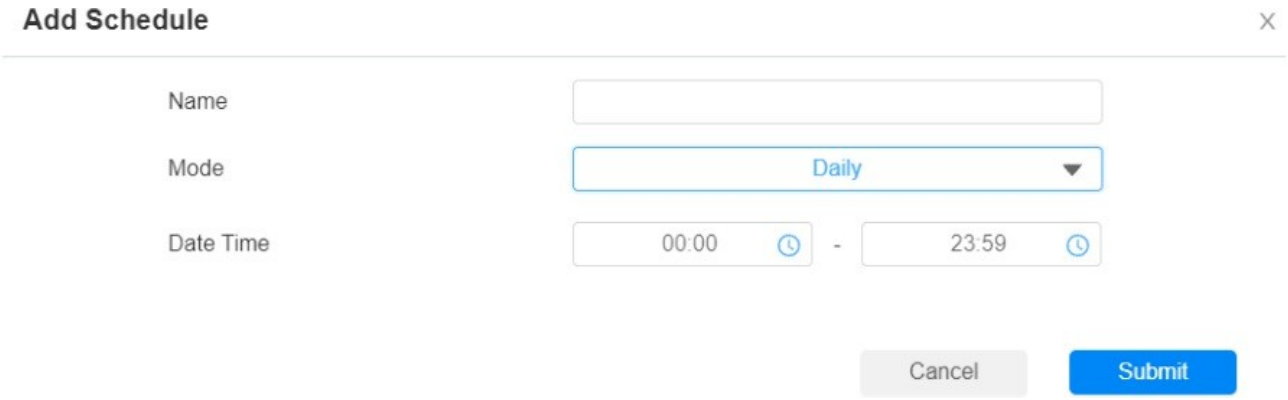
Tworzenie harmonogramu dostępu do drzwi w interfejsie internetowym

Harmonogram dostępu do drzwi można tworzyć codziennie lub co miesiąc, a oprócz codziennego lub comiesięcznego uruchamiania harmonogramu dostępu do drzwi można także utworzyć harmonogram umożliwiający planowanie na dłuższy okres. Aby skonfigurować klikn + Add .

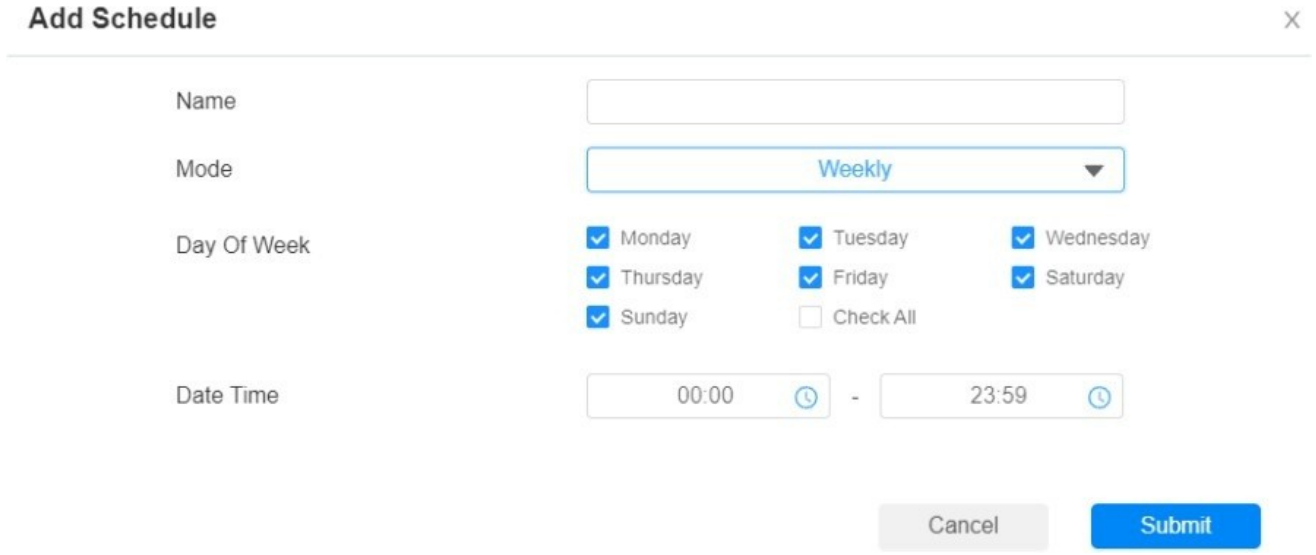


harmonogram, przejdź do opcji **Ustawienia > Harmonogram** , a następnie

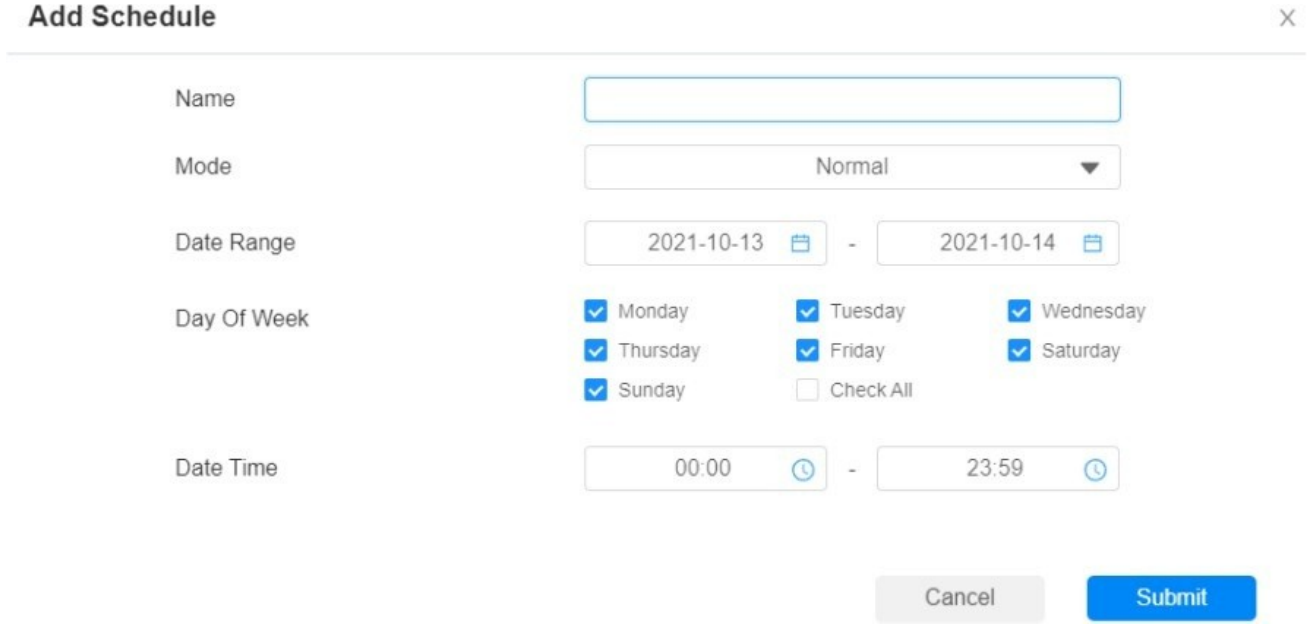
Aby utworzyć harmonogram dzienny:



Aby utworzyć harmonogram tygodniowy:

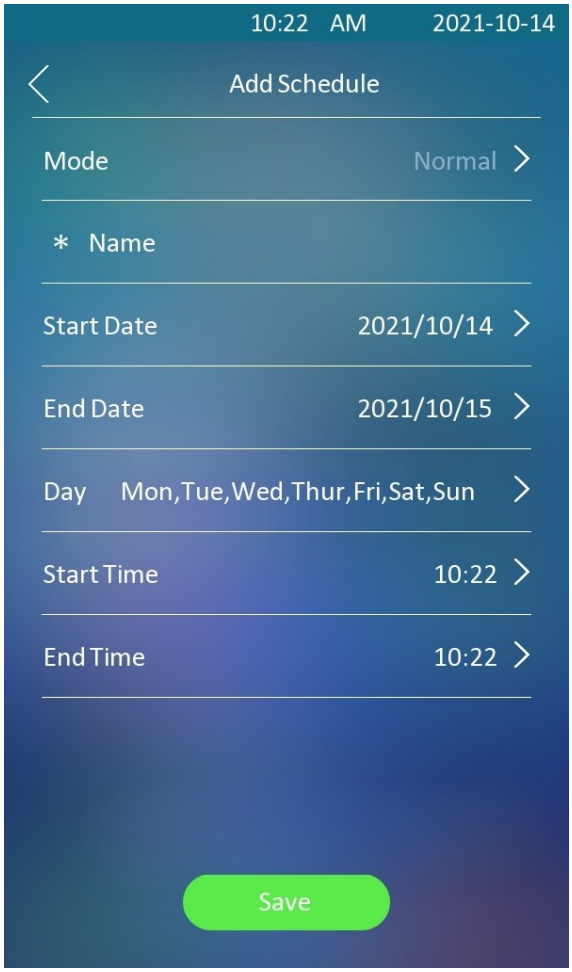


Aby utworzyć harmonogram na dłuższy okres:



Tworzenie harmonogramu dostępu do drzwi na urządzeniu

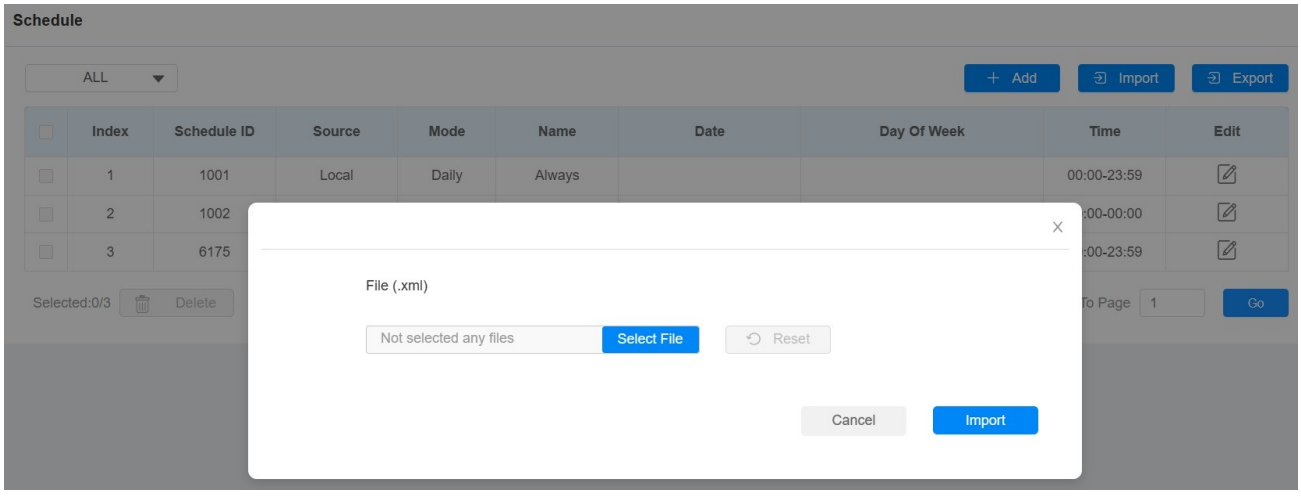
Można również utworzyć harmonogram dostępu do drzwi na urządzeniu. Ścieżka: **Harmonogram > Dodaj harmonogram** .



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.

Ścieżka: **Ustawienia > Harmonogram.**



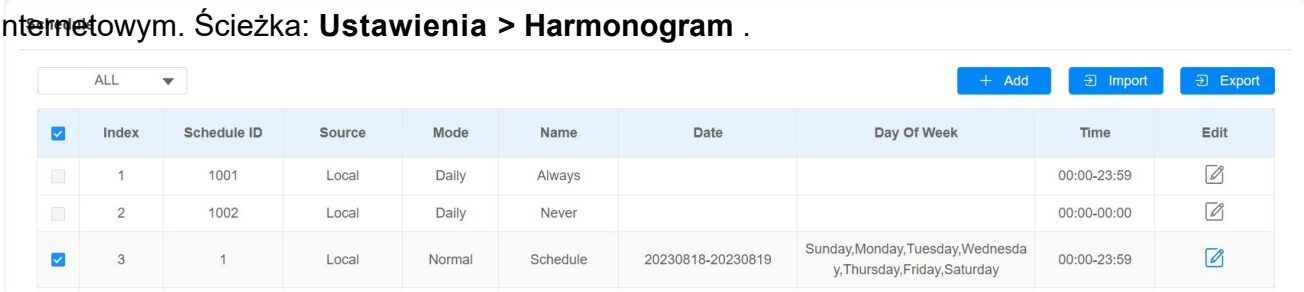
Uwaga

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

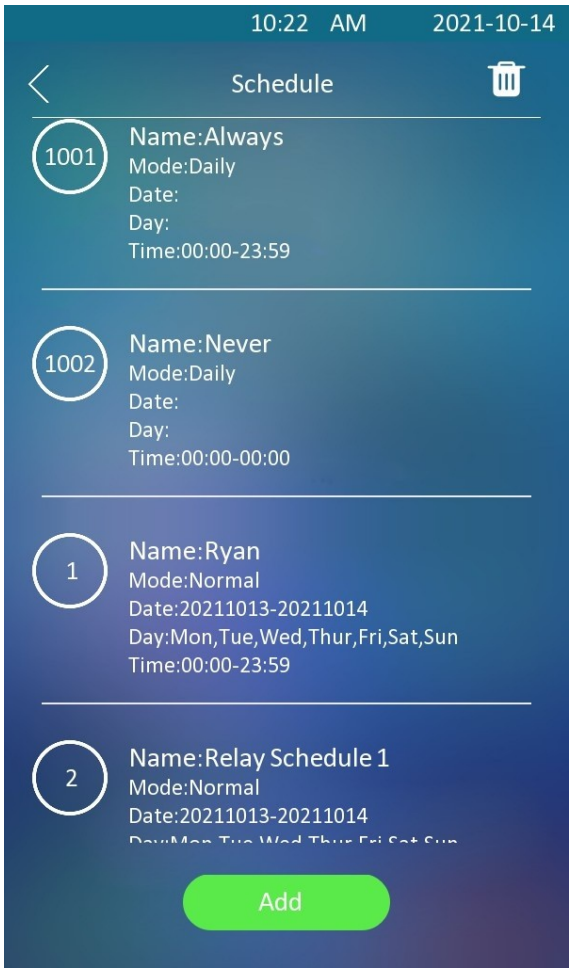
Edycja harmonogramu dostępu do drzwi

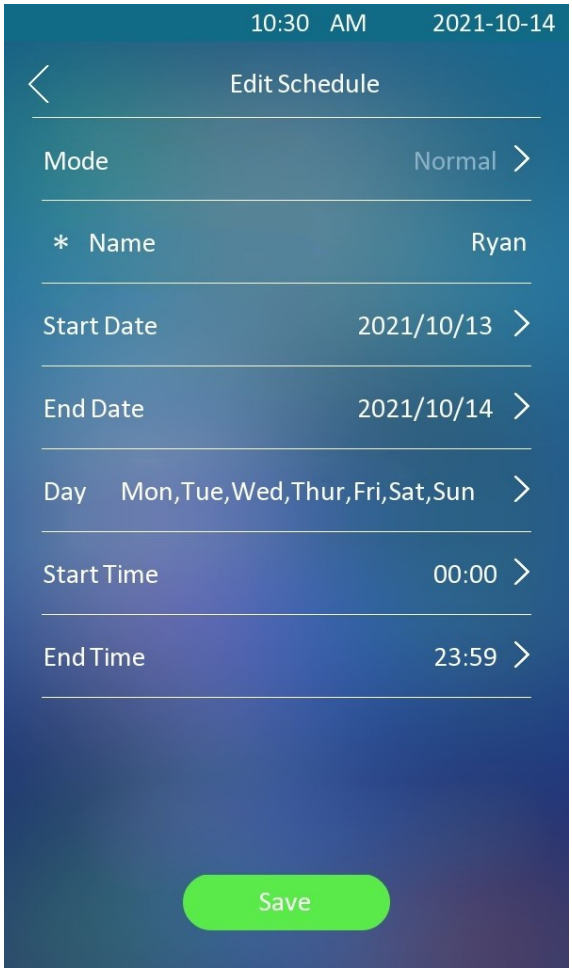
Edycja harmonogramu dostępu do drzwi w interfejsie internetowym

Jeśli chcesz edytować lub usunąć utworzony harmonogram dostępu do drzwi, możesz edytować lub usunąć skonfigurowany harmonogram osobno lub zbiorczo w interfejsie internetowym. Ścieżka: **Ustawienia > Harmonogram** .



Można również edytować lub usunąć harmonogram dostępu do drzwi na urządzeniu. Ścieżka: **Harmonogram > Harmonogram** .





Konfiguracja odblokowania drzwi

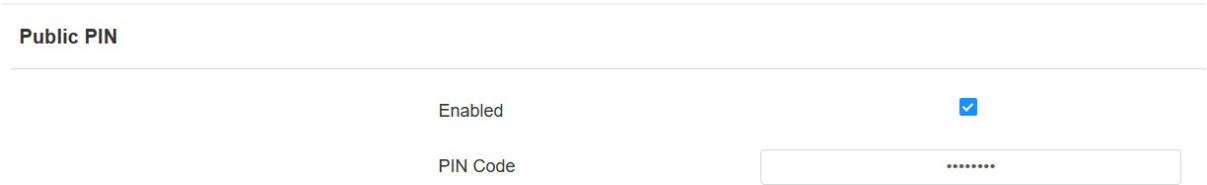
Konfiguracja kodu PIN do odblokowywania drzwi

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.

Konfiguracja publicznego kodu PIN

Publiczne kody PIN można konfigurować i modyfikować na urządzeniu oraz w interfejsie internetowym urządzenia.

- **Skonfiguruj publiczny kod PIN w interfejsie internetowym** Ścieżka: **Access Control > PIN**

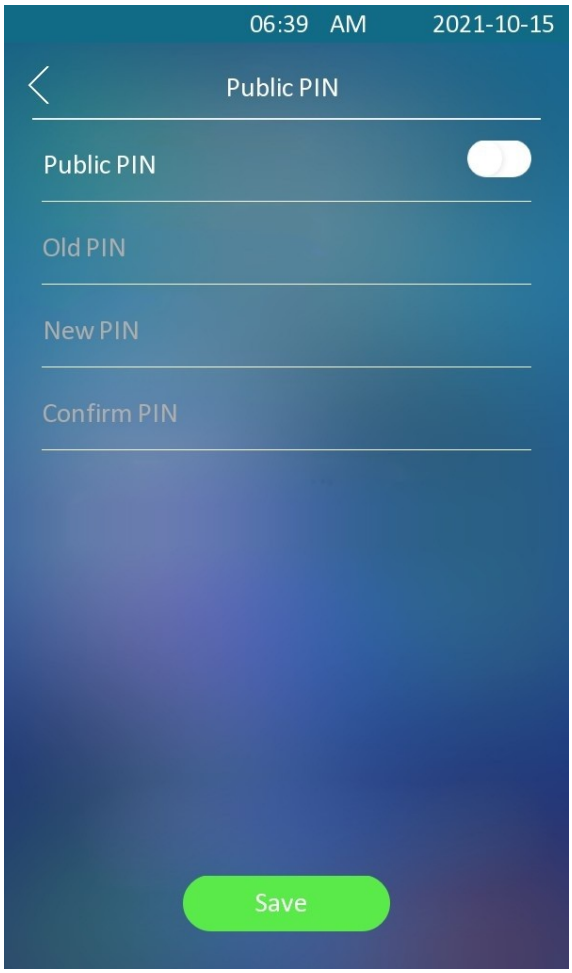


Konfiguracja parametrów :

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

- **Skonfiguruj publiczny kod PIN na urządzeniu**

Ścieżka: **Security > Public PIN.**



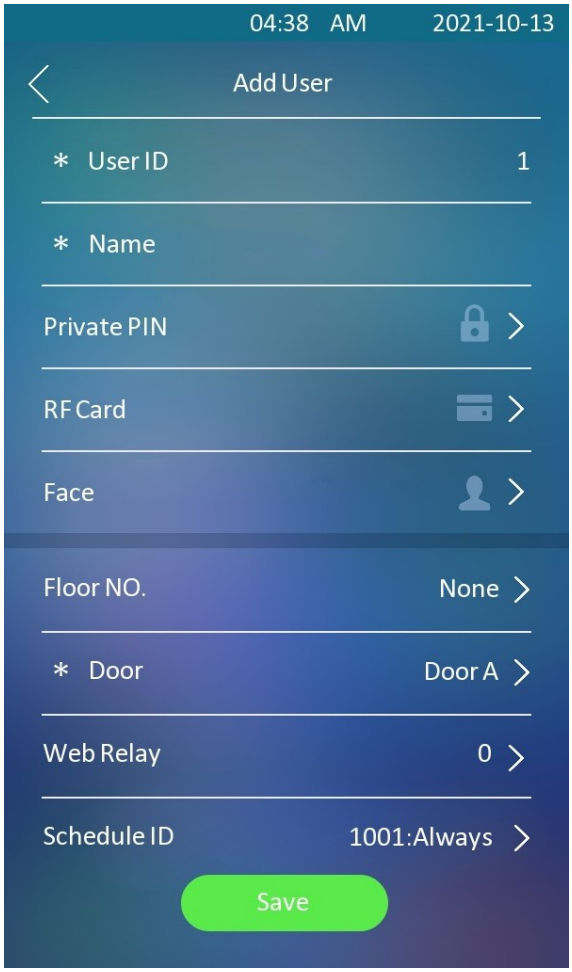
Uwaga

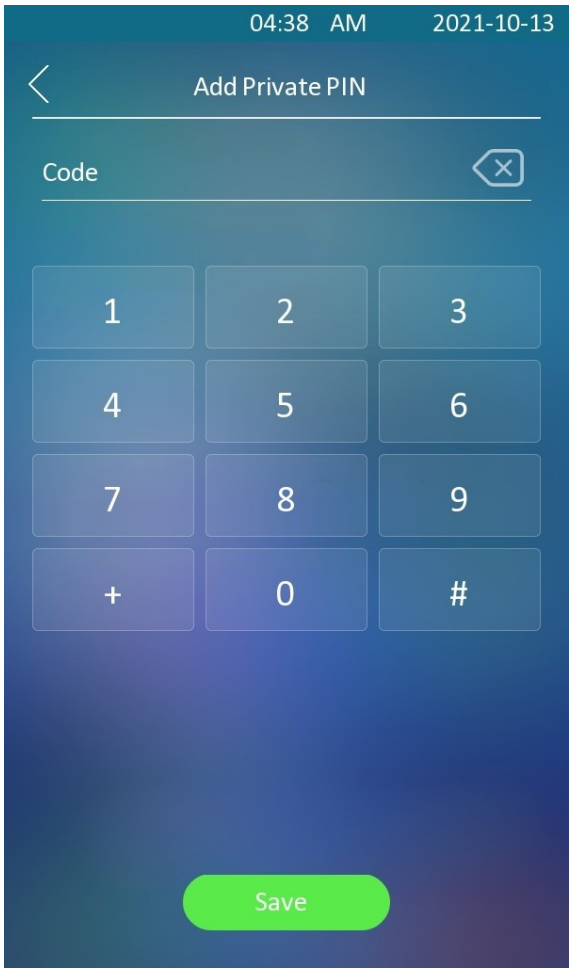
- Publiczny kod PIN będzie ważny dopiero po włączeniu tej funkcji.
- **APT+PIN** może mieć zastosowanie tylko wtedy, gdy urządzenie jest dodane do Akuvox SmartPlus.

Konfiguracja prywatnego kodu PIN na urządzeniu

Na urządzeniu można skonfigurować prywatny kod PIN dla określonego

użytkownika. Ścieżka: **Użytkownik > Lista użytkowników**

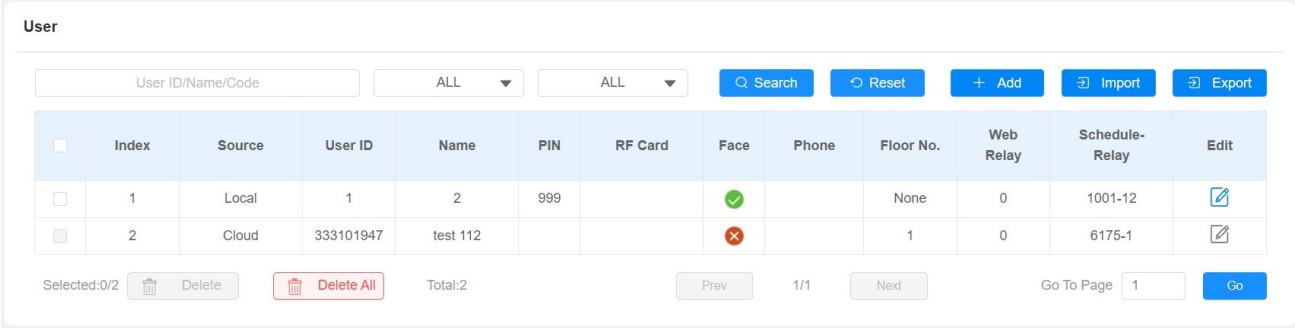

04:38 AM 2021-10-13
Add User
* User ID 1
* Name
Private PIN
RF Card
Face
Floor NO. None
* Door Door A
Web Relay 0
Schedule ID 1001:Always
Save

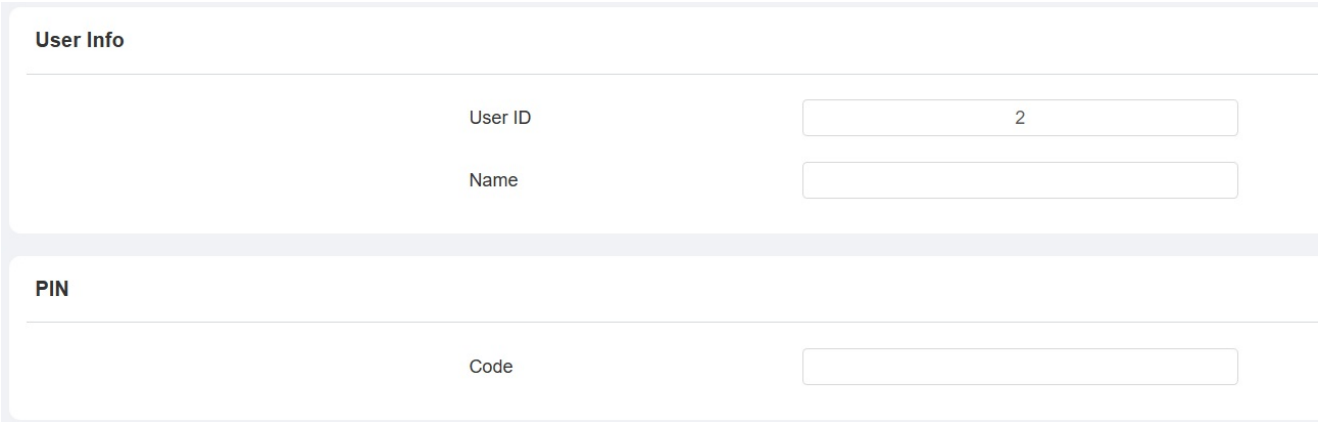

04:38 AM 2021-10-13
Add Private PIN
Code
1 2 3
4 5 6
7 8 9
+ 0 #
Save

Konfiguracja prywatnego kodu PIN w interfejsie internetowym

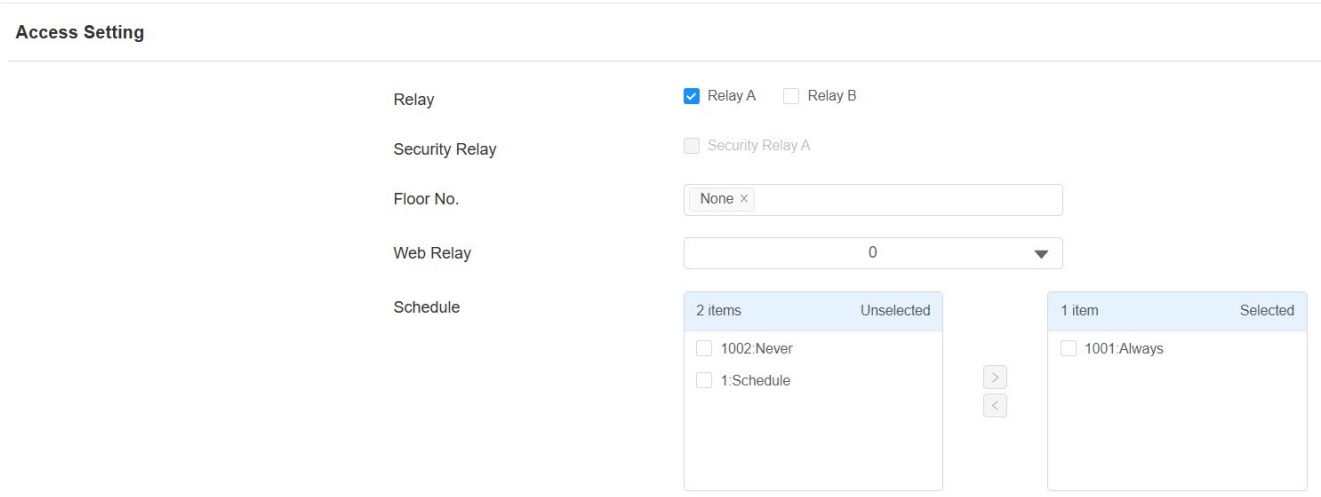
W interfejsie internetowym można utworzyć kod PIN i dostosować dodatkowe ustawienia, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenia, który przekaźnik ma zostać otwarty.

Ścieżka: **Katalog > Użytkownik**.





Po wprowadzeniu informacji o użytkowniku i kodu PIN można rozpocząć konfigurację prywatnego kodu PIN dostępu do drzwi.



Konfiguracja parametrów :

- **Przekaźnik sieciowy**: wybierz określoną liczbę poleceń akcji przekaźnika sieciowego skonfigurowanych w interfejsie sieciowym.

- **Harmonogram** : wybierz jeden z utworzonych harmonogramów dostępu do drzwi w prawym polu i przenieś ten, który ma zostać zastosowany do dostępu do drzwi z kodem PIN użytkownika(-ów), do pola po prawej stronie.

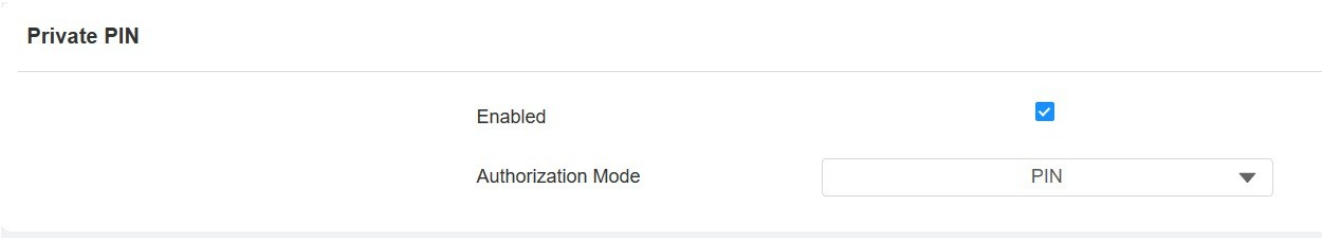
Uwaga

- Ten krok ma zastosowanie do dostępu do drzwi za pomocą karty RF i poświadczeń rozpoznawania twarzy

Konfiguracja prywatnego trybu dostępu PIN

Urządzenie 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.

Ścieżka: **Kontrola dostępu > Ustawienia PIN > Prywatny PIN**



Konfiguracja parametrów :

- **Tryb autoryzacji**: 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.

Konfiguracja karty RF do odblokowywania drzwi

Możesz dodać kartę RF dla konkretnego użytkownika w celu odblokowania drzwi w interfejsie internetowym i na urządzeniu.

Konfiguracja karty RF w interfejsie internetowym

Możesz dotknąć karty RF na czytniku i kliknąć Uzyskaj, aby dodać kartę RF dla użytkownika.
Ścieżka: **Katalog**

> Użytkownik > Karta RF .

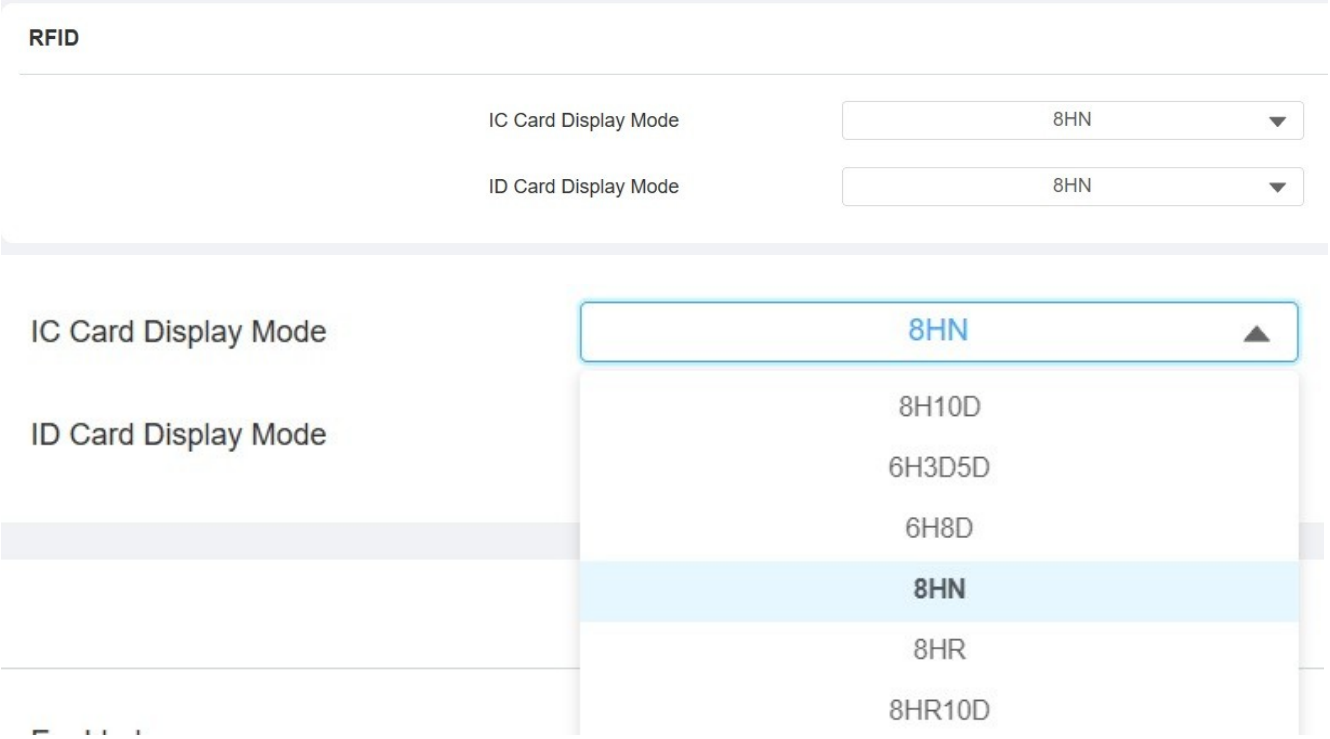
Uwaga

- Proszę odnieść się do sekcji wyboru harmonogramu dostępu za pomocą kodu PIN dla użytkowników kart RF w celu uzyskania szczegółowych informacji na temat dostępu do drzwi.
- Karty RF o częstotliwości 13,56 MHz i 125 kHz mogą być stosowane w telefonach drzwiowych do 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.

Ścieżka: **Kontrola dostępu > Ustawienia karty > RFID.**

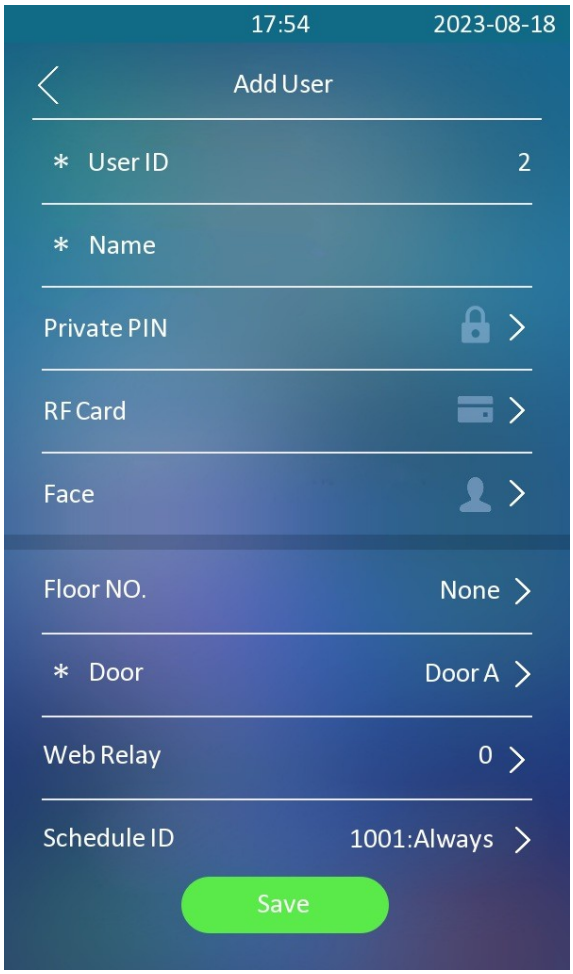


Konfiguracja parametrów:

- **Tryb wyświetlania karty IC/ID**: wybór formatu **karty ID/IC** dla dostępu do drzwi spośród sześciu opcji formatu: **8H10D; 6H3D 5D; 6H8D; 8HN; 8HR; 8HR10D** . Domyślny format kodu karty w bramofonie to **8HN.**

Konfiguracja rozpoznawania twarzy do odblokowywania drzwi
Konfiguracja funkcji rozpoznawania twarzy na urządzeniu

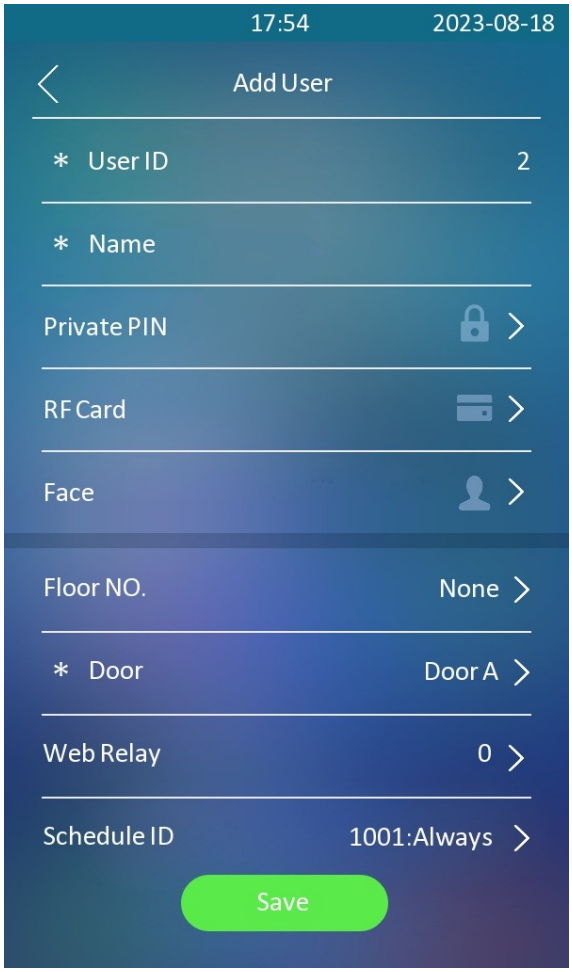
Można skonfigurować dostęp do drzwi poprzez rozpoznawanie twarzy na urządzeniu, wprowadzając nazwę użytkownika i rejestrując swój identyfikator twarzy na urządzeniu w celu uzyskania dostępu do drzwi. Ścieżka: **Użytkownik > Lista użytkowników > Dodaj użytkownika.**

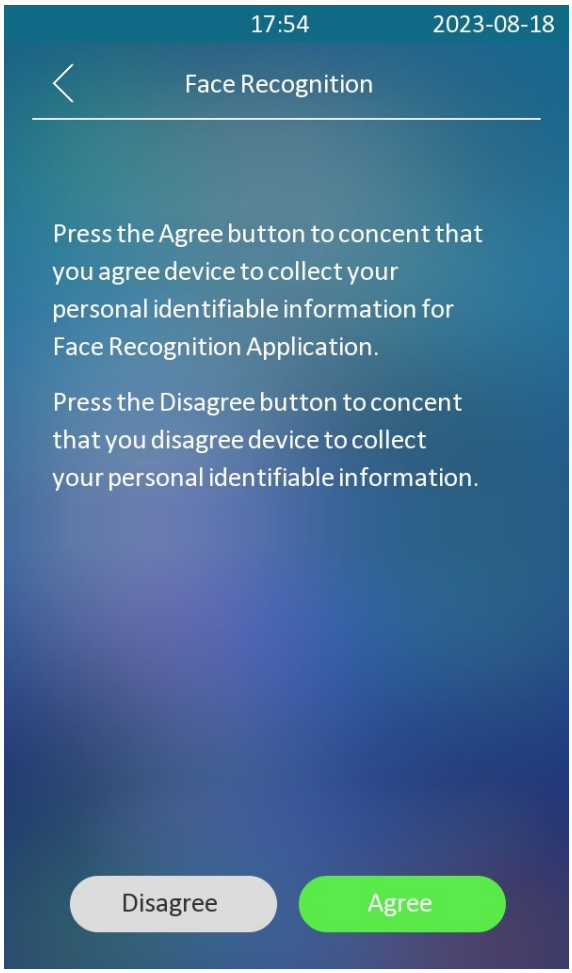


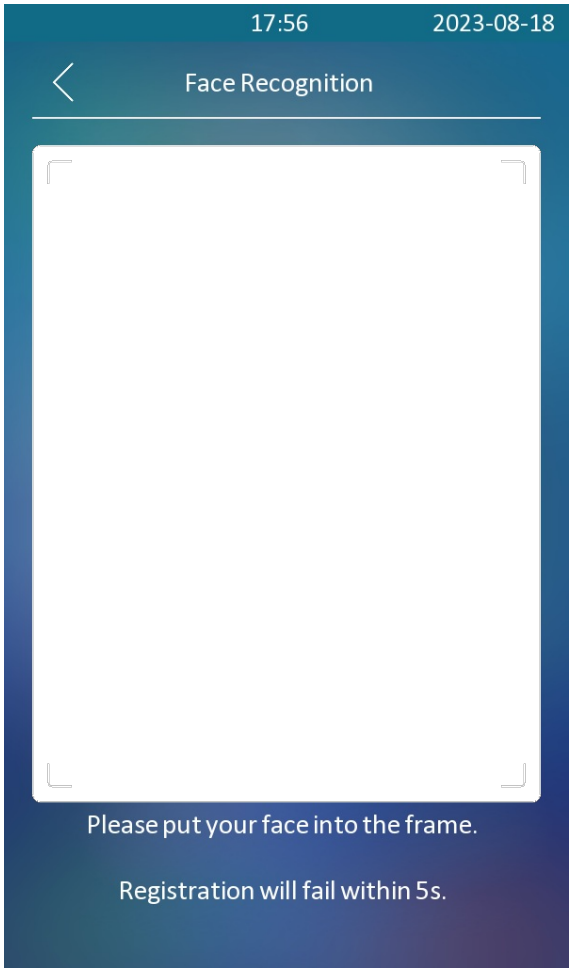
Przesyłanie danych twarzy na urządzenie

Dane twarzy można przesłać do urządzenia za pośrednictwem interfejsu internetowego.

Ścieżka: **Użytkownik > Lista użytkowników > Dodaj użytkownika.**



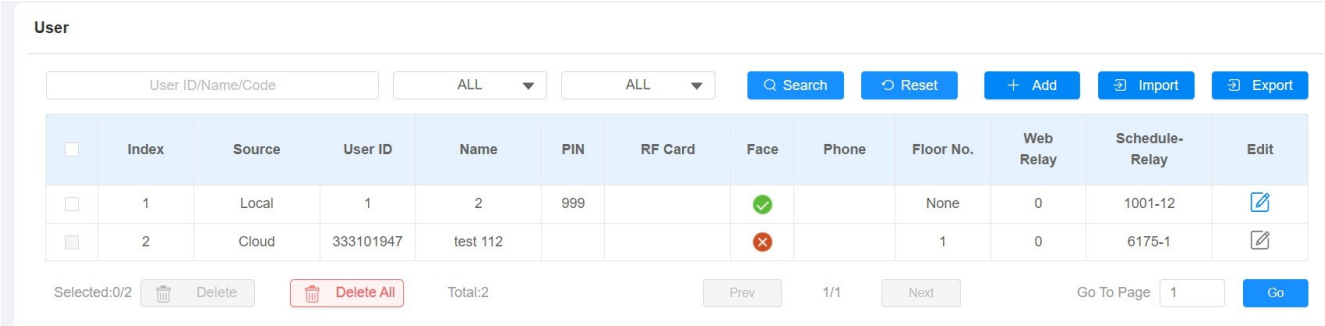

17:54
2023-08-18
Face Recognition
Press the Agree button to concent that you agree device to collect your personal identifiable information for Face Recognition Application.
Press the Disagree button to concent that you disagree device to collect your personal identifiable information.
Disagree
Agree

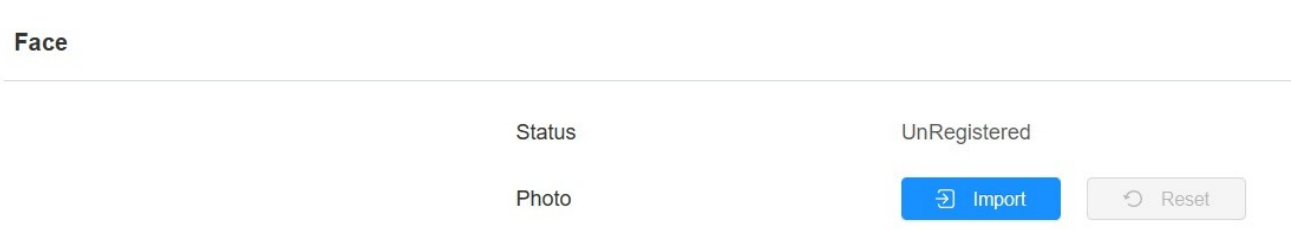


Przesyłanie danych twarzy w interfejsie internetowym

Dane twarzy można przesłać do urządzenia za pośrednictwem interfejsu internetowego.

Aby to zrobić, przejdź do **Katalog > Użytkownik**, a następnie kliknij **+Dodaj** . Następnie prześlij zdjęcie 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.**
  Photo(jpg/png): wybierz zdjęcie w formacie jpg lub png, które ma zostać przesłane do urządzenia i naciśnij, jeśli chcesz wyczyścić przesłane zdjęcie.

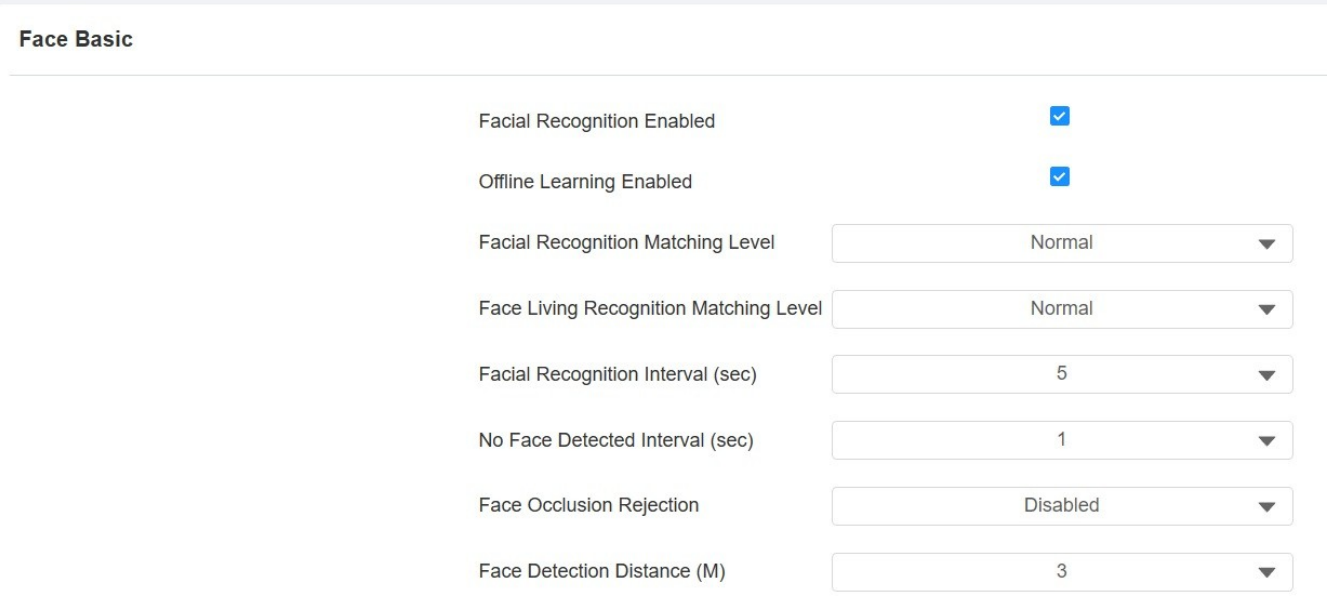
Uwaga

- Przesyłane zdjęcia powinny być w formacie jpg lub png.

Konfiguracja rozpoznawania twarzy

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

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



Konfiguracja parametrów :

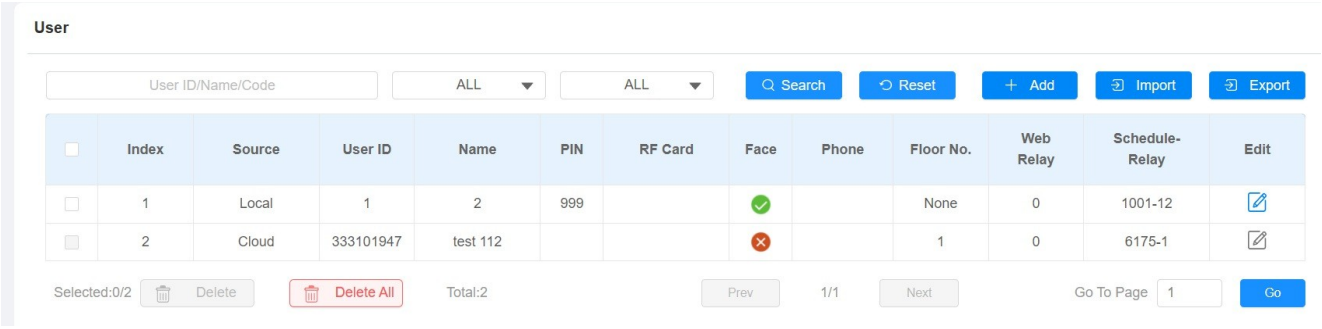
- **Offline Learning Enabled** : wybierz opcję **Enable,** jeśli chcesz poprawić zdolność rozpoznawania urządzenia, koncentrując się na głównych cechach twarzy, a pomijając drobne zmiany, które zaszły na twarzy. Dokładność rozpoznawania twarzy poprawia się wraz ze wzrostem liczby rozpoznań twarzy.

Face Recognition Matching Level: kliknij, aby wybrać poziom dokładności rozpoznawania twarzy spośród czterech opcji: **Low, Normal, High** i **Highest**. Na przykład, jeśli wybierzesz **Highest**, będzie najmniejsze prawdopodobieństwo, że ktoś inny zostanie pomylony z tobą lub w inny sposób w rozpoznawaniu twarzy.
Face Living Recognition Matching Level: wybierz poziom Anti-spoofing spośród czterech opcji: **Low, Normal, High i Highest**. Na przykład, jeśli wybierzesz **Highest**, będzie najmniejsze prawdopodobieństwo, że urządzenie zostanie oszukane przez obrazy cyfrowe lub zdjęcia dowolnego rodzaju.

- **Facial Recognition Interval(Sec)**: wybierz odstęp czasu między każdym rozpoznaniem twarzy od 1 do 8 sekund. Na przykład, jeśli wybierzesz **5**, musisz odczekać 5 sekund. Zanim będzie można ponownie wykonać rozpoznawanie twarzy.
- **No Face Detected Interval(Sec)**: ustawienie prawidłowego przedziału czasu dla uwierzytelniania po przekroczeniu temperatury ciała. Jeśli interwał czasowy jest zbyt długi, może to zostać wykorzystane przez inne osoby do uzyskania dostępu do drzwi tylko poprzez rozpoznawanie twarzy. Na przykład, jeśli pomyślnie przeszedłeś wykrywanie temperatury ciała, ale nie udało Ci się rozpoznać twarzy, odszedłeś, a ktoś za Tobą może spróbować użyć tylko rozpoznawania twarzy do wejścia do drzwi przed osiągnięciem prawidłowego przedziału czasu. Można więc skrócić interwał czasowy do dowolnego miejsca od 1 do 8 sekund, aby nikt nie mógł uzyskać dostępu do drzwi tylko za pomocą rozpoznawania twarzy. Pomoże to również przyspieszyć szybkie otwieranie drzwi, ponieważ bramofon szybko powróci do ekranu głównego w celu wykrycia temperatury, gdy komuś nie uda się rozpoznać twarzy.
- **Face Detection Distance(M)**: umożliwia ustawienie prawidłowej odległości wykrywania twarzy (1 metr, 2 metry i 3 metry). Na przykład, jeśli chcesz zmniejszyć liczbę niepotrzebnych rozpoznań twarzy osób, które przechodzą obok urządzenia. Domyślna odległość to 3 metry.

Konfiguracja dostępu do drzwi przy użyciu skonfigurowanych plików

E18 umożliwia szybką konfigurację dostępu do drzwi dla poszczególnych użytkowników w trybie wsadowym poprzez importowanie skonfigurowanych plików kontroli dostępu do drzwi typu "wszystko w jednym", zawierających informacje o użytkowniku, typie dostępu do drzwi, harmonogramie dostępu do drzwi itp. Ścieżka: **Directory > User > User**.

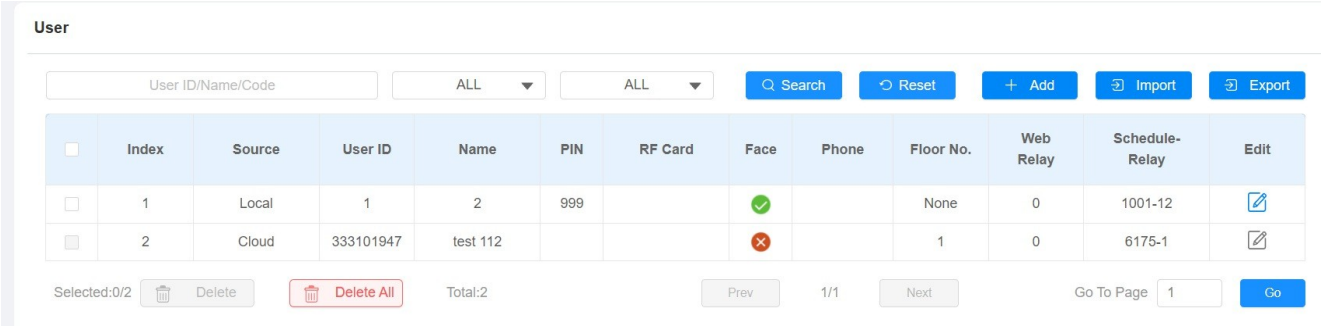


Uwaga

- Skonfigurowane pliki do rozpoznawania twarzy oraz inne typy skonfigurowanych plików dostępu do drzwi są rozdzielone różnymi formatami plików.

Edycja danych dostępu do drzwi dla poszczególnych użytkowników

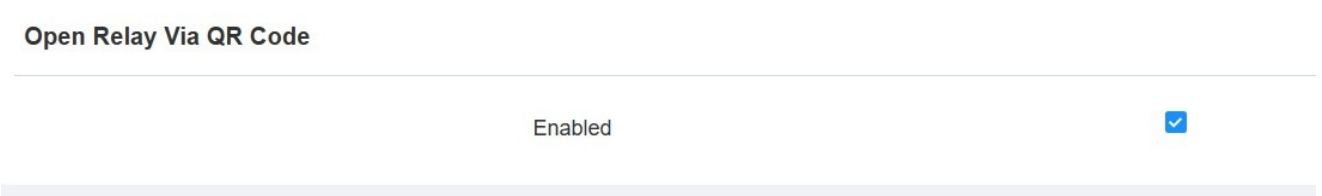
W interfejsie internetowym można wyszukiwać dostęp do drzwi dla poszczególnych użytkowników i edytować dane dostępu do drzwi. Ścieżka: **Directory > User > User**.



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.

Ścieżka: **Kontrola dostępu > Przekaźnik > Otwórz przekaźnik za pomocą kodu QR** .



Uwaga

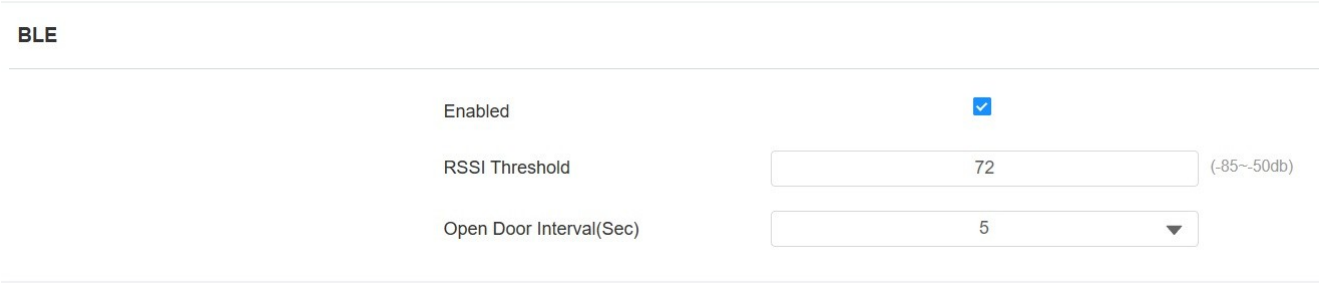
- Funkcja powinna działać z chmurą Akuvox. Aby uzyskać więcej informacji, prosimy o kontakt z Zespół techniczny Akuvox.

Odblokowanie przez Bluetooth

Aplikacja SmartPlus z obsługą Bluetooth umożliwia użytkownikom otwieranie drzwi bez użycia rąk.

Mogą oni otwierać drzwi z aplikacją w kieszeni lub machać telefonem w kierunku bramofonu, gdy zbliżają się do drzwi.

Ścieżka: **Kontrola dostępu > BLE > BLE** .



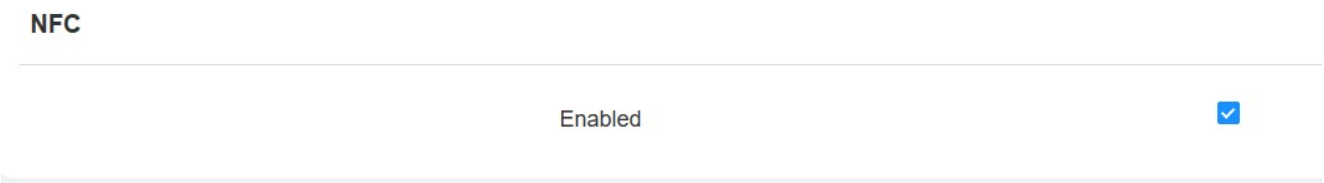
Konfiguracja parametrów :

- **Próg RSSI**: wybierz siłę odbieranego sygnału z zakresu -85~-50db w wartościach bezwzględnych. Im wyższa wartość, tym większa siła sygnału. Wartość domyślna to 72 dB w wartościach bezwzględnych.
- **Interwał otwierania drzwi (sek.)**: wybór odstępu czasu między kolejnymi dwoma otwarciami drzwi Bluetooth.

Odblokowanie przez NFC

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

Ścieżka: **Kontrola dostępu > Ustawienia karty > NFC**

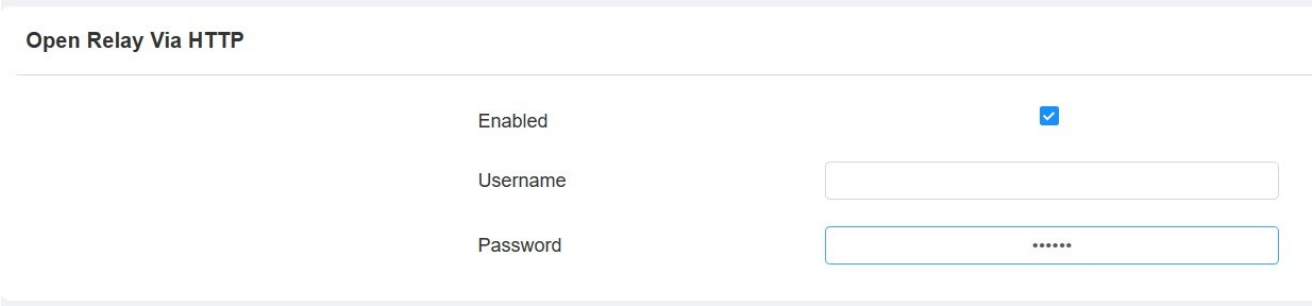


Odblokowanie za pomocą polecenia HTTP w przeglądarce internetowej

Bramofon obsługuje zdalne odblokowywanie drzwi za pomocą polecenia HTTP. Wystarczy włączyć tę funkcję i wprowadzić polecenie HTTP (URL) dla bramofonu. Spowoduje to uruchomienie przekaźnika i otwarcie drzwi, nawet jeśli użytkownicy znajdują się z dala od urządzenia.

Ścieżka: **Kontrola dostępu > Przekaźnik**

- **Otwarty przekaźnik przez HTTP**



Konfiguracja parametrów :

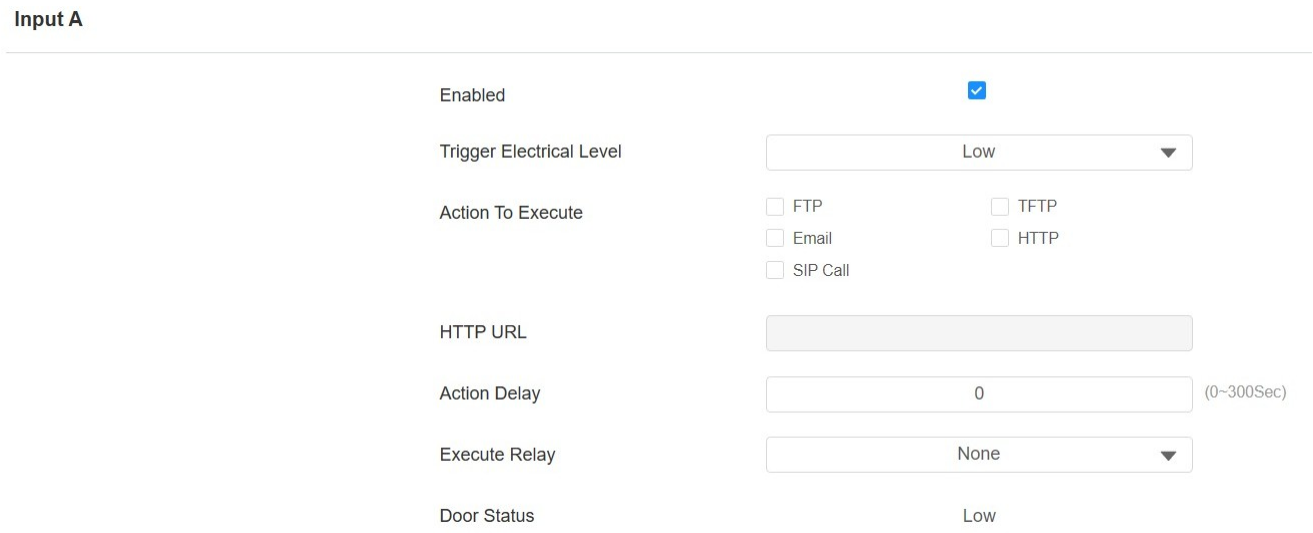
- **User Name** : wprowadź nazwę użytkownika interfejsu internetowego urządzenia, na przykład **admin**. • **Hasło** : wprowadź hasło dla polecenia HTTP. Na przykład **12345** .

Zapoznaj się z poniższym przykładem: http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Odblokowanie przyciskiem wyjścia przy drzwiach

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

Ścieżka: **Kontrola dostępu > Wejście > Wejście A**



Konfiguracja parametrów :

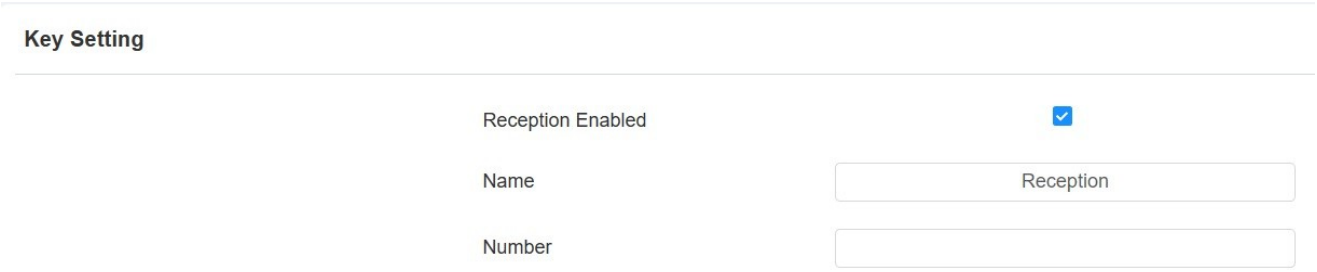
- **Poziom** wyzwalania elektrycznego: wybór opcji poziomu wyzwalania elektrycznego pomiędzy **wysokim** i **niskim** zgodnie z rzeczywistym działaniem przycisku wyjścia.
- **Action to Execute** : wybierz metodę wykonania akcji spośród pięciu opcji: **FTP, Email, TFTP, HTTP** i **SIP Call**.

- **Http URL** : wprowadź adres URL, jeśli wybierzesz HTTP do wykonania akcji.
- **Action Delay (Opóźnienie akcji)**: ustawienie czasu opóźnienia wykonania akcji. Na przykład, jeśli czas opóźnienia akcji zostanie ustawiony na 5 sekund, odpowiednie akcje zostaną wykonane 5 minut po naciśnięciu przycisku.

Odblokowanie przez kartę odbioru

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.

Ścieżka: **Interkom > Podstawowe > Ustawienia klawiszy**



Konfiguracja parametrów :

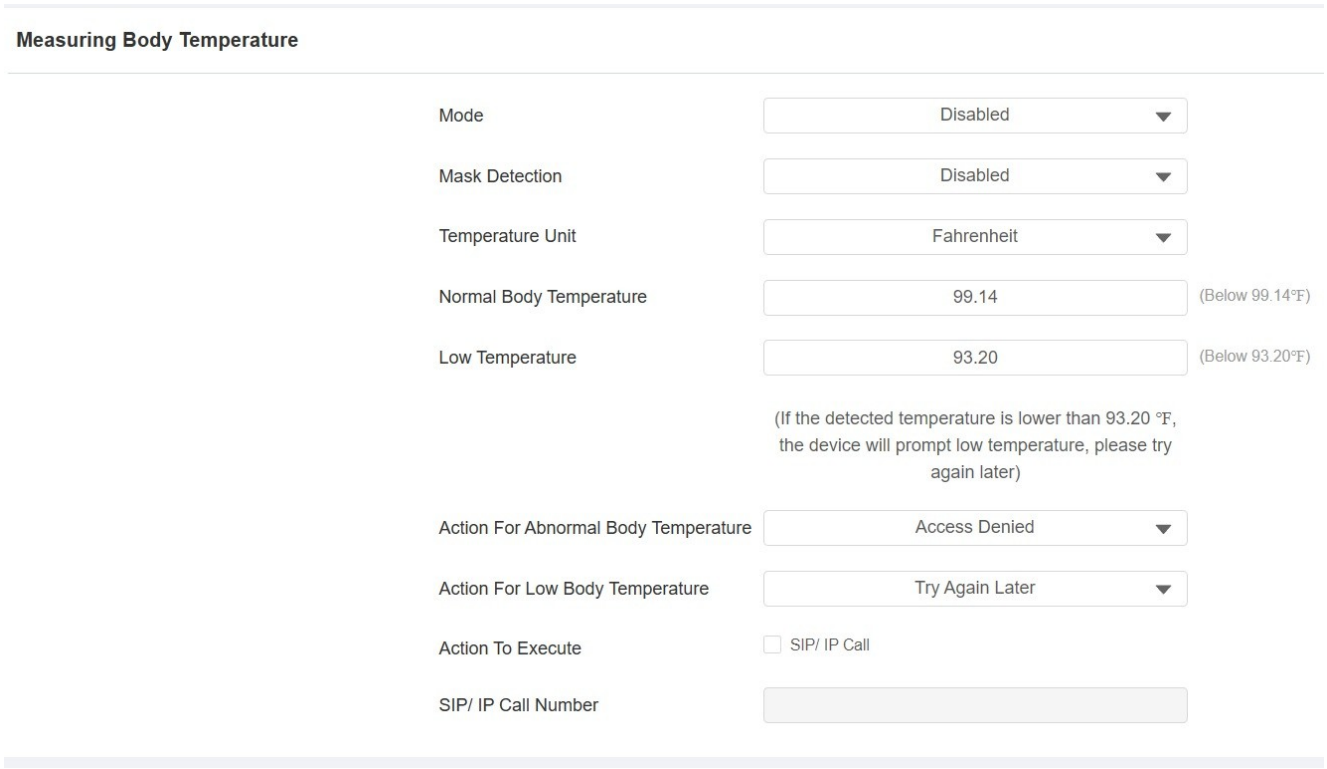
Numer: wprowadź numer SIP/IP, który ma zostać wybrany po naciśnięciu **ikony odbioru** w celu uzyskania dostępu do drzwi.

Pomiar temperatury ciała na potrzeby dostępu do drzwi

Funkcja pomiaru temperatury ciała pozwala bramofonowi mierzyć temperaturę ciała i sprawdzać maski pod kątem bezpieczeństwa. Po włączeniu tej funkcji bramofon otwiera drzwi tylko tym mieszkańcom lub gościom, którzy pomyślnie przejdą test.

Konfiguracja pomiaru temperatury ciała

Funkcję pomiaru temperatury ciała można skonfigurować w zakresie definiowania normalnej temperatury, a także tworzenia harmonogramu ważności funkcji itp. Ścieżka: **Kontrola dostępu > Temperatura ciała > Pomiar temperatury ciała** .



Konfiguracja parametrów :

- **Tryb**: wybierz **tryb wyłączenia, tryb nadgarstka** lub **tryb czoła** do pomiaru temperatury w zależności od potrzeb. Urządzenie można zainstalować z cyfrowym czujnikiem temperatury na czole, dlatego wymagane jest odpowiednie ustawienie trybu w zależności od zastosowania.
- **Wykrywanie maski**: wybierz opcję **Wyłącz**, jeśli chcesz wyłączyć wykrywanie maski. Wybierz opcję **Ustaw noszenie maski** jako obowiązkowe, a urządzenie sprawdzi, czy odwiedzający nosi maskę lub nie podczas przypominania odwiedzającemu za pomocą komunikatu "Proszę nosić maskę". Po wybraniu opcji **Wyświetlaj** monit o **noszenie maski** urządzenie będzie wyświetlać tylko monit o noszenie maski bez obowiązku jej noszenia.
- **Normalna temperatura ciała**: ustaw temperaturę ciała na wstępnie zdefiniowaną temperaturę ciała jako podstawę pomiaru w stopniach **Fahrenheita** lub **Celsjusza**. Na przykład, jeśli ustawisz temperaturę 37,3 stopni Celsjusza jako normalną temperaturę, wówczas każda temperatura ciała zmierzona powyżej 37,3 stopni Celsjusza zostanie uznana za nieprawidłową temperaturę, podczas gdy temperatura niższa niż 34 stopnie Celsjusza zostanie uznana za niską temperaturę ciała.
- **Action For Abnormal Body Temperature (Działanie w przypadku nieprawidłowej temperatury ciała)**: w przypadku wybrania opcji **Access Denied (Odmowa dostępu)** każdy, u kogo zostanie wykryta nieprawidłowa temperatura ciała, otrzyma odmowę dostępu do drzwi. W przypadku wybrania opcji **Tylko dla przypomnienia** każda osoba z nieprawidłową temperaturą ciała nadal będzie miała

dostęp do drzwi.

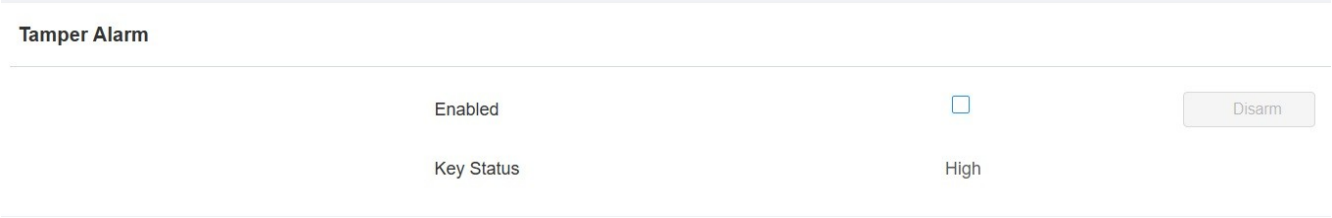
- **Działanie w przypadku niskiej temperatury ciała**: jeśli wybrano opcję **Spróbuj ponownie później**, odmówiony zostanie dostęp do drzwi z komunikatem "Spróbuj ponownie później ze względu na niską temperaturę ciała". W przypadku wybrania opcji **Tylko dla przypomnienia**, osoba z niską temperaturą ciała nadal będzie miała dostęp do drzwi.
- **Działanie do wykonania**: zaznacz pole, aby włączyć lub wyłączyć połączenie SIP/IP. Jeśli chcesz otrzymywać powiadomienia za pośrednictwem połączenia SIP/IP w przypadku wykrycia nieprawidłowej temperatury i niskiej temperatury.
- **Numer połączenia SIP/IP**: wprowadź numer połączenia SIP lub IP dla powiadomienia. Pole pojawi się, aby wypełnić numery SIP/IP po zaznaczeniu pola **Action to Execute.**

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 urządzenie wykryje zmianę wartości grawitacji w stosunku do pierwotnej.

Ścieżka: **System > Bezpieczeństwo > Alarm sabotażowy**



Konfiguracja parametrów :

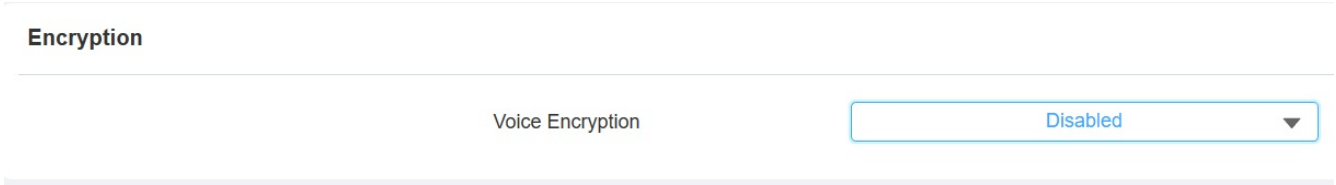
- **Enabled** : zaznacz pole wyboru, aby włączyć funkcję alarmu sabotażowego. Gdy włączy się alarm sabotażowy, można nacisnąć przycisk **Disarm** obok pola wyboru, aby skasować alarm.
- **Stan klucza**: alarm sabotażowy nie zostanie wyzwolony, jeśli stan klucza nie zostanie zmieniony z **niskiego** na **wysoki.**

Uwaga

- Po usunięciu alarmu sabotażowego zakładka **Rozbrój** zmieni kolor na szary.
- Okrągły gumowy przycisk z tyłu urządzenia musi być wciśnięty, w przeciwnym razie alarm nie zostanie uruchomiony.

Szyfrowanie głosu

Secure Real-time Transport Protocol (SRTP) to protokół wywodzący się z Real-time Transport Protocol (RTP). Zwiększa on bezpieczeństwo transmisji danych, zapewniając szyfrowanie, uwierzytelnianie wiadomości, zapewnienie integralności i ochronę przed powtórkami.
Ścieżka: **Konto > Zaawansowane >** Interfejs **szyfrowania.**



Konfiguracja parametrów :

- **Szyfrowanie głosu (SRTP)**: wybierz **Wyłączone, Opcjonalne** lub **Obowiązkowe** dla SRTP. Jeśli jest to **Opcjonalne** lub **Obowiązkowe**, głos podczas połączenia jest szyfrowany i można pobrać pakiet RTP, aby go wyświetlić.

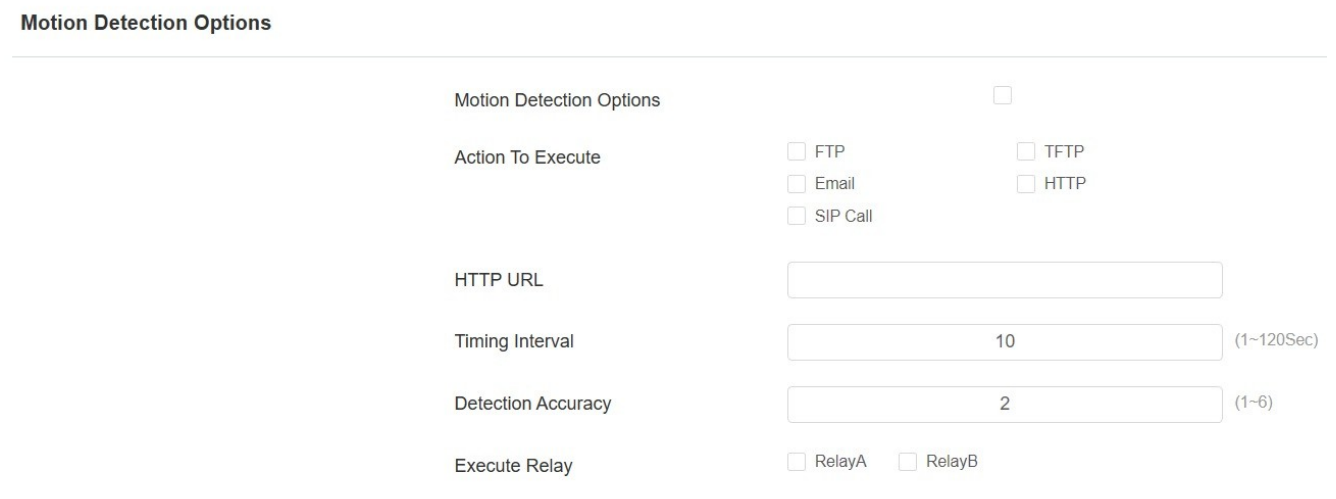
Wykrywanie ruchu

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.

Konfiguracja wykrywania ruchu w interfejsie internetowym

W interfejsie internetowym urządzenia można dostosować różne ustawienia wykrywania ruchu, takie jak interwał czasowy, poziom czułości, metoda powiadamiania o wykryciu ruchu i inne.

Ścieżka: **Surveillance > Motion > Motion Detection** Interfejs **opcji.**



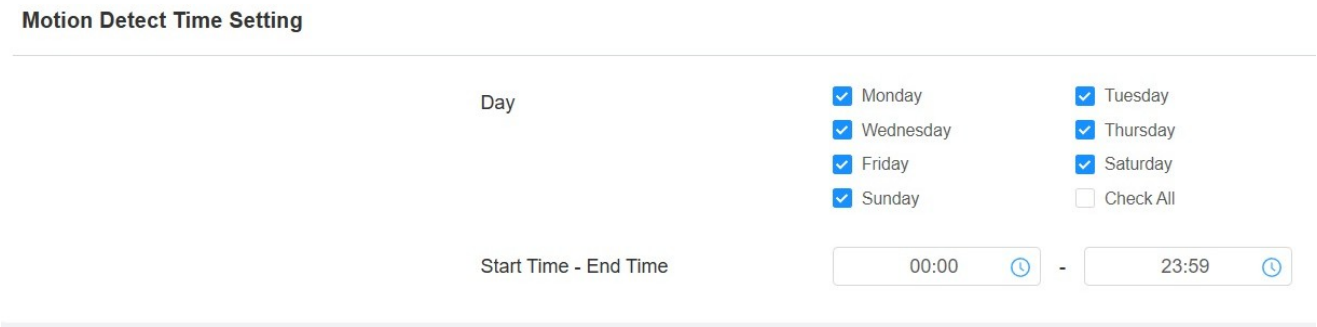
Konfiguracja parametrów :

- **Akcja do wykonania**: wybierz akcję do wykonania (FTP, TFTP, Email, HTTP i SIP).

Call) po wyzwoleniu detekcji ruchu.

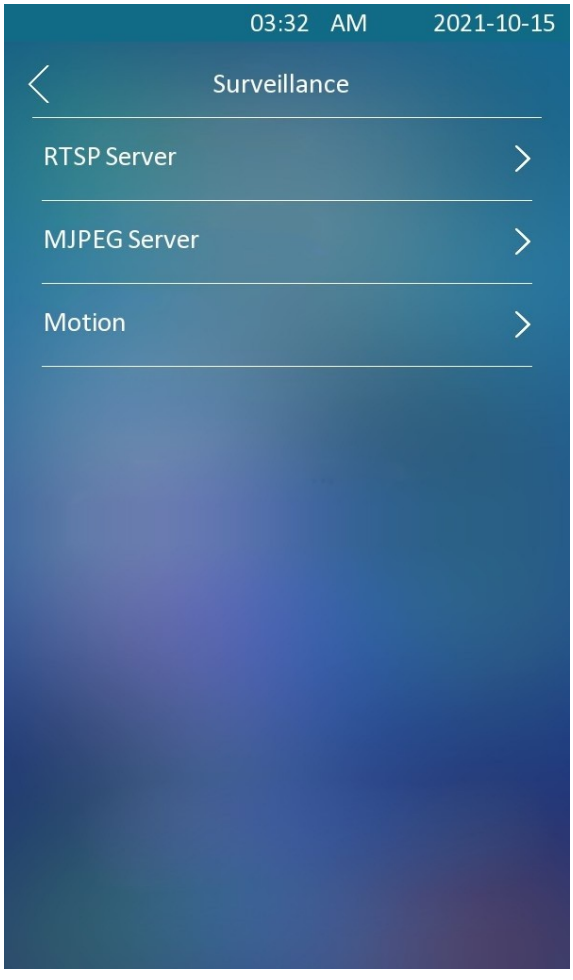
- **HTTP URL** : wprowadź polecenie HTTP URL, które zostanie wysłane do wyznaczonego serwera w celu wykonania określonej akcji.
- **Interwał** czasowy: ustaw interwał czasowy w taki sam sposób, jak na urządzeniu.
- **Dokładność wykrywania**: ustaw dokładność wykrywania dla czułości wykrywania. Im wyższa wartość, tym większa czułość. Domyślna wartość dokładności wykrywania to **2** .
  Execute Relay: wybór przekaźnika A lub przekaźnika B, który zostanie wyzwolony po wykryciu ruchu.

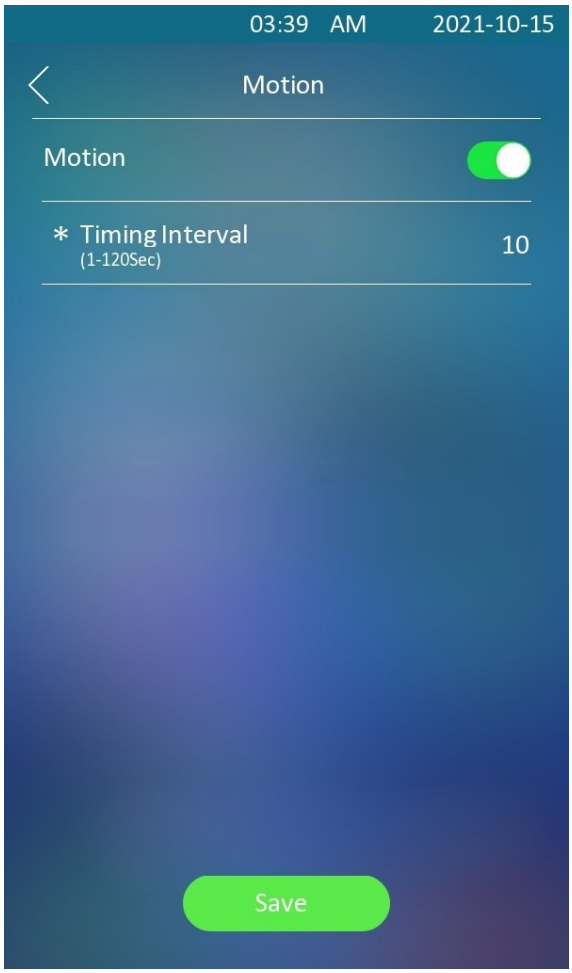
Można również ustawić harmonogram wykrywania ruchu.



Konfiguracja wykrywania ruchu na urządzeniu

Można włączyć wykrywanie ruchu i ustawić interwał wykrywania ruchu na urządzeniu. Ścieżka: **Advanced > Surveillance >Motion**.





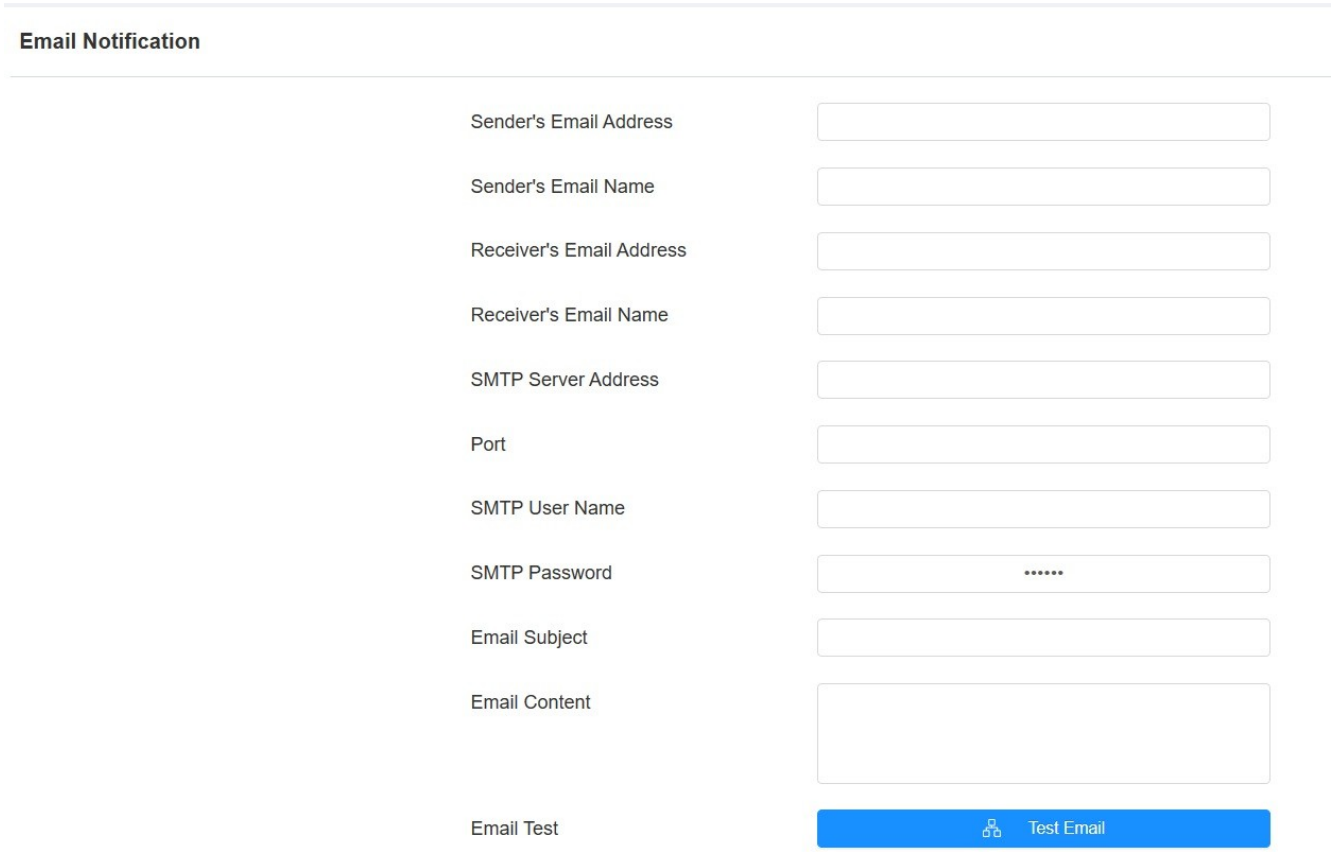
Ustawienia powiadomień bezpieczeństwa

Powiadomienie bezpieczeństwa może zostać zainicjowane jako akcja po wyzwoleniu detekcji ruchu. Powiadomienia bezpieczeństwa mogą być wysyłane za pośrednictwem poczty e-mail, serwera FTP, serwera TFTP i połączenia SIP.

Ustawienia powiadomień e-mail

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

Ścieżka: **Ustawienia > Działanie** .



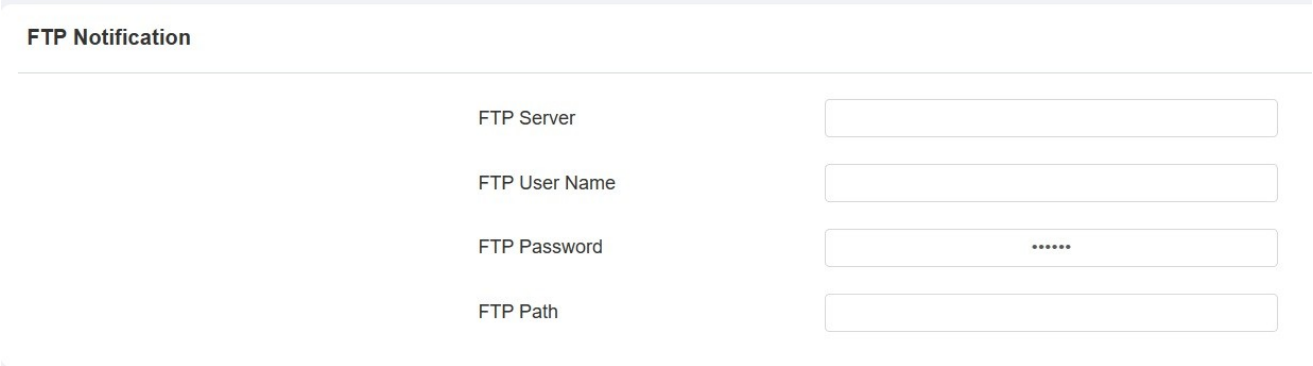
Konfiguracja parametrów :

- **Nazwa e-mail nadawcy**: wprowadź nazwę nadawcy wiadomości e-mail.
- **Adres e-mail nadawcy**: wprowadź adres e-mail nadawcy, z którego zostanie wysłane powiadomienie e-mail.
- **Adres e-mail odbiorcy**: wprowadź adres e-mail odbiorcy.
- **Receiver's Email Name** : wprowadź nazwę odbiorcy wiadomości e-mail.
- **Adres serwera SMTP**: wprowadź adres serwera SMTP nadawcy.
- **Port**: wprowadź numer portu, z którego wysyłana jest wiadomość e-mail.
- **Nazwa użytkownika SMTP** : wprowadź nazwę użytkownika SMTP, która jest zwykle taka sama jak adres e-mail nadawcy.
- **Hasło SMTP** : skonfiguruj hasło usługi SMTP, które jest takie samo jak adres e-mail nadawcy.

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.

Ścieżka: **Setting > Action > FTP Notification**.

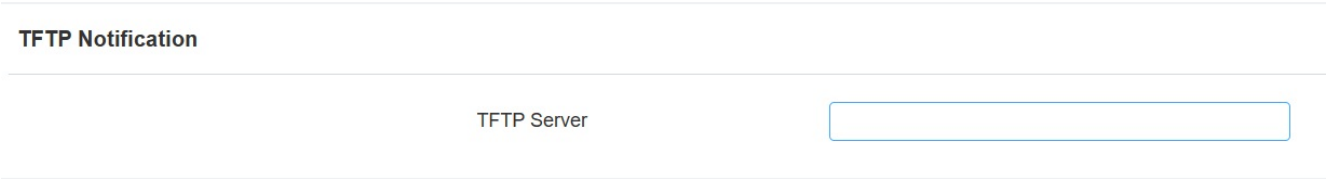


Konfiguracja parametrów :

- **FTP Server**: wprowadź adres (URL) serwera FTP dla powiadomienia FTP. • **FTP Path**: wprowadź nazwę folderu utworzonego na serwerze FTP.

Ustawienia powiadomień TFTP

Aby otrzymywać powiadomienia bezpieczeństwa za pośrednictwem serwera TFTP, należy wprowadzić adres serwera TFTP. Ścieżka: **Setting > Action > TFTP Notification**.

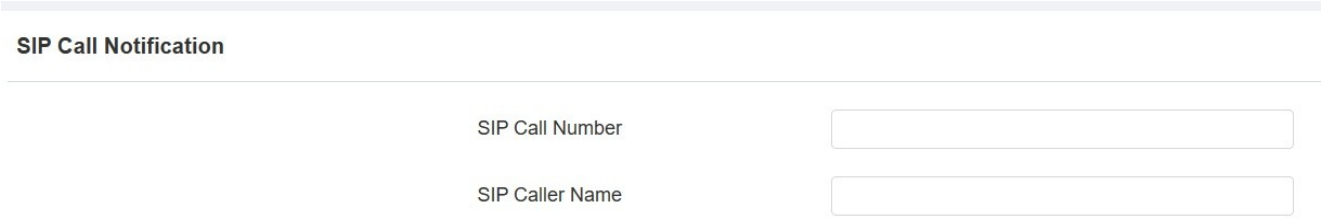


Konfiguracja parametrów :

- **TFTP Server**: wprowadź adres (URL) serwera TFTP dla powiadomienia TFTP.

Powiadomienie o połączeniu SIP

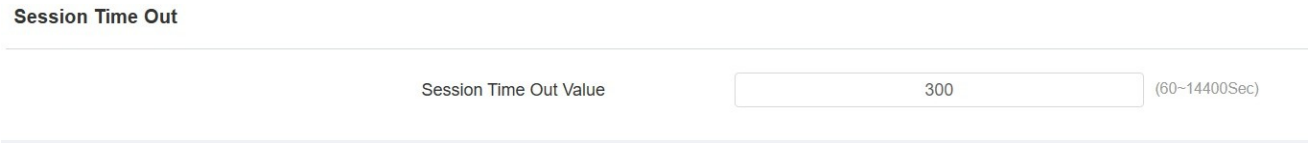
Jeśli chcesz otrzymywać powiadomienia o zabezpieczeniach za pośrednictwem połączenia SIP, możesz odpowiednio skonfigurować powiadomienie FTP w interfejsie internetowym. Ścieżka: **Setting > Action > SIP Call Notification**.



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 ją skonfigurować, przejdź do **System> Bezpieczeństwo > Limit czasu sesji.**



Konfiguracja parametrów :

- **Session Time Out Value**: ustawia czas automatycznego wylogowania interfejsu sieciowego w zakresie od 60 sekund do 14400 sekund. Wartość domyślna to 300.

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.

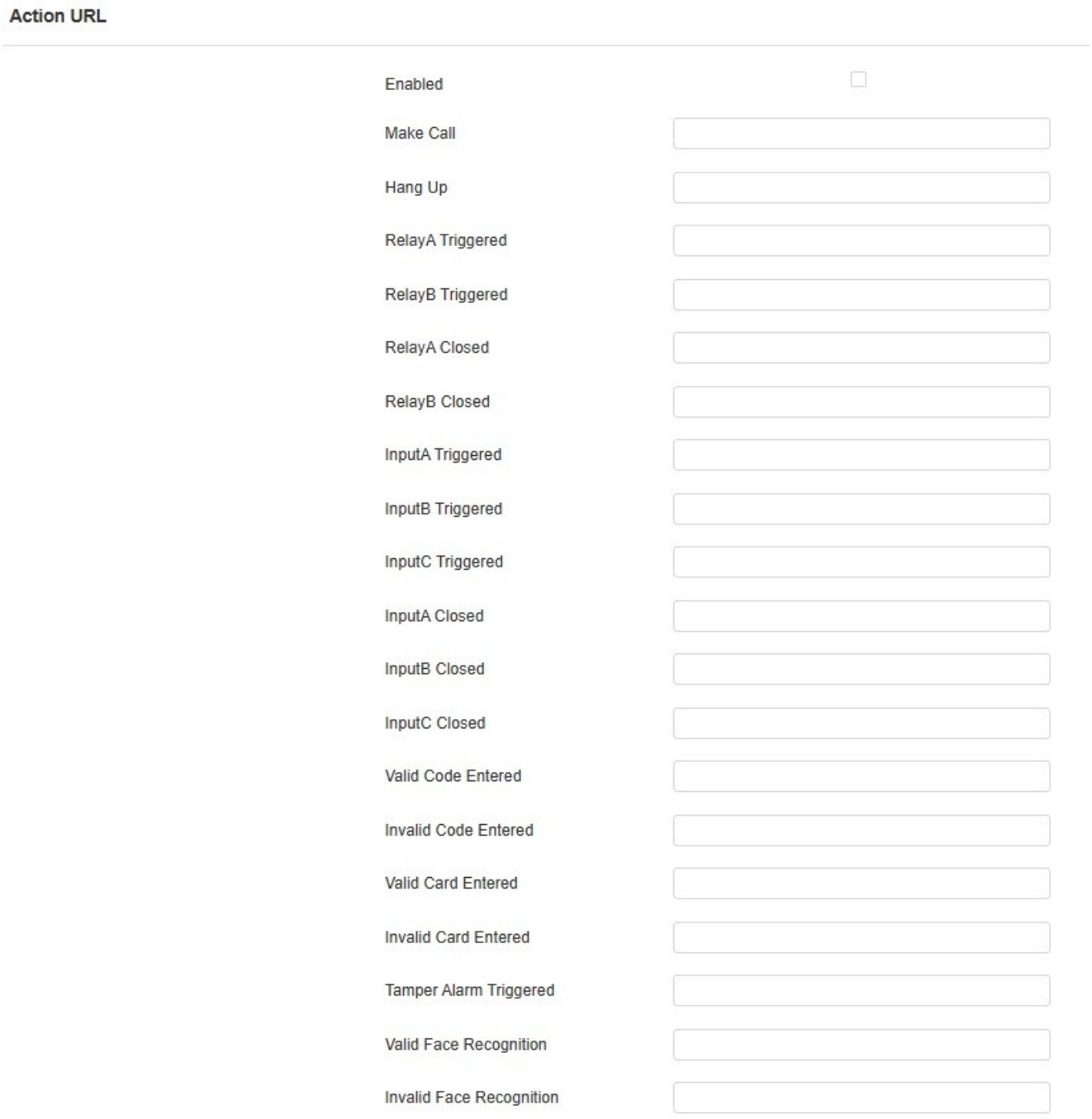
Akuvox Action URL:

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** .



Uwaga

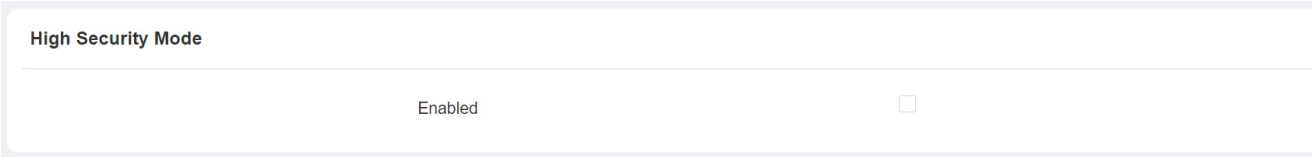
- Adres URL działania i format są dostarczane przez zewnętrznego producenta, firmę Akuvox telefon wysyła adres URL tylko do urządzeń innych firm.

Tryb wysokiego bezpieczeństwa

Tryb wysokiego bezpieczeństwa został zaprojektowany w celu zwiększenia bezpieczeństwa.

Wykorzystuje on szyfrowanie w różnych aspektach, w tym w procesie komunikacji, poleceniach otwierania drzwi, metodach przechowywania haseł i nie tylko.

Aby skonfigurować tę funkcję w Internecie: **System > Bezpieczeństwo > Tryb wysokiego bezpieczeństwa**



Ważne uwagi

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

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

-PC Manager: 1.2.0.0

-IP Scanner: 2.2.0.0

-Upgrade Tool: 4.1.0.0

-SDMC: 6.0.0.34

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

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

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

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

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

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

Monitor i obraz

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

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

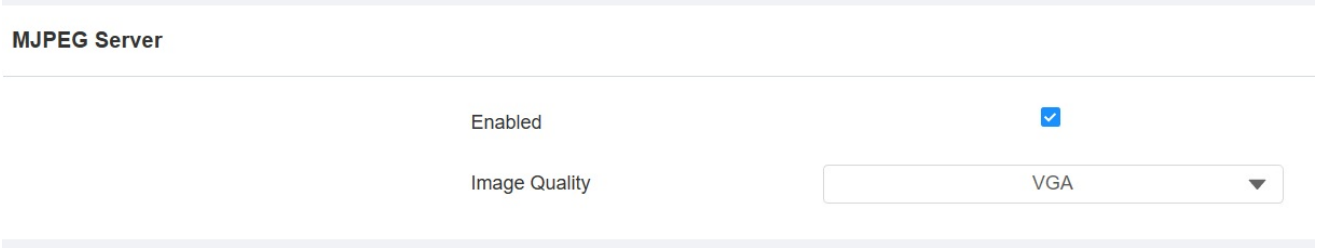
RTSP to skrót od Real Time Streaming Protocol. Może być używany do strumieniowego przesyłania obrazu i dźwięku z kamer innych firm do urządzenia. Możesz dodać strumień z kamery, dodając jej adres URL. Format adresu URL urządzeń Akuvox to rtsp://Device's IP/live/ch00_0

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

Przechwytywanie obrazu MJPEG

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

Ścieżka: **Surveillance > MJPEG > Mjpeg Server**



Konfiguracja parametrów :

- **Jakość obrazu**: wybór jakości przechwytywanego obrazu spośród siedmiu opcji: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P**

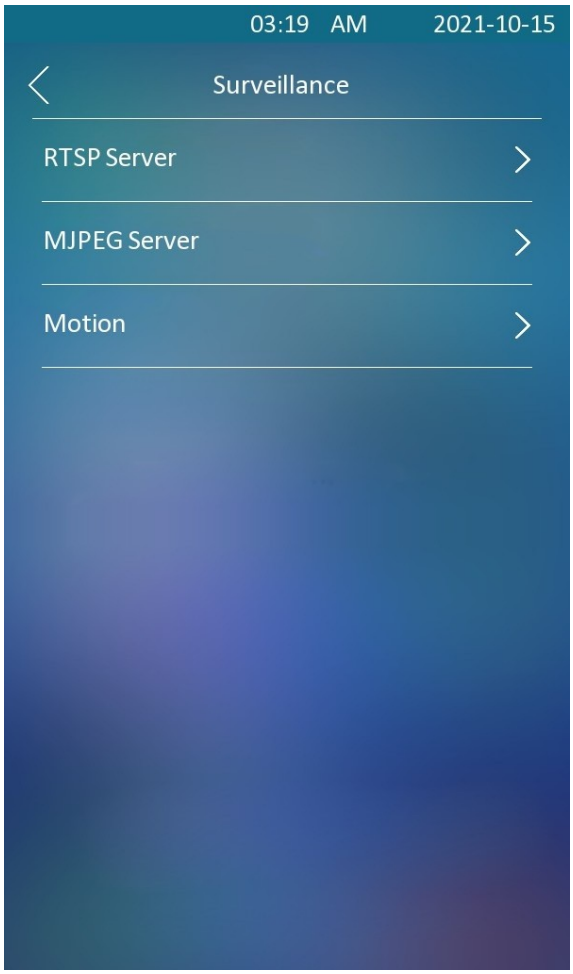
Po włączeniu usługi Mjpeg można przechwytywać obraz z telefonu przy użyciu następujących trzech typów formatu URL:

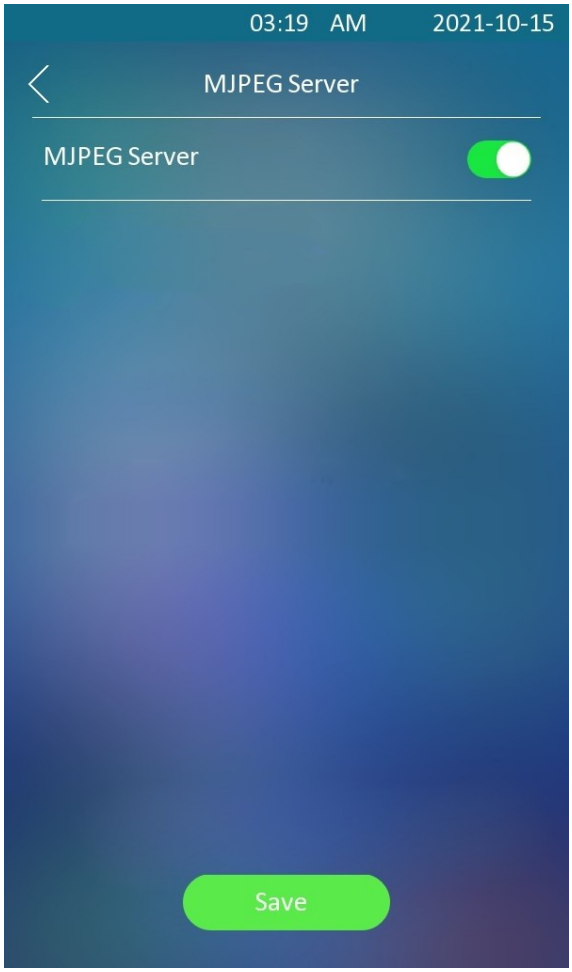
- http:// urządzenie ip:8080/picture.cgi
- http://device ip:8080/picture.jpg
- http://device ip:8080/jpeg.cgi

Na przykład, jeśli chcesz przechwycić obraz w formacie jpg z bramofonu o adresie IP: 192.168.1.104, możesz wykonać następujące czynności:

1. Wprowadź adres http://192.168.1.104:8080/picture.jpg w przeglądarce internetowej
2. Naciśnij klawisz **Enter** na klawiaturze, aby przechwycić obraz.

Serwer MJPEG można również włączyć bezpośrednio na urządzeniu. Ścieżka: **Advanced > Surveillance > MJPEG server**.

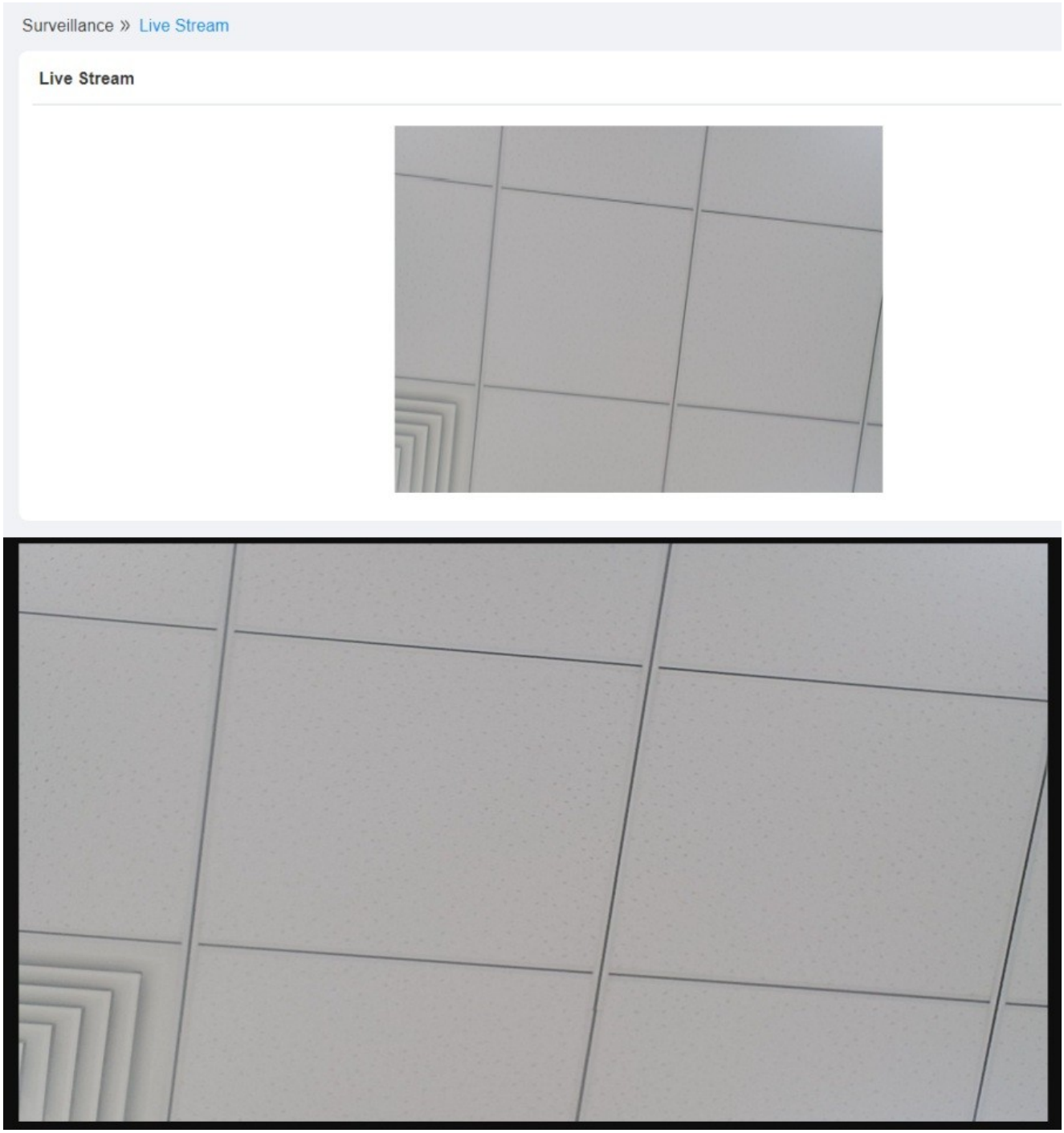




Transmisja na żywo

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

Ścieżka: **Monitoring > Transmisja na żywo**.



Uwaga

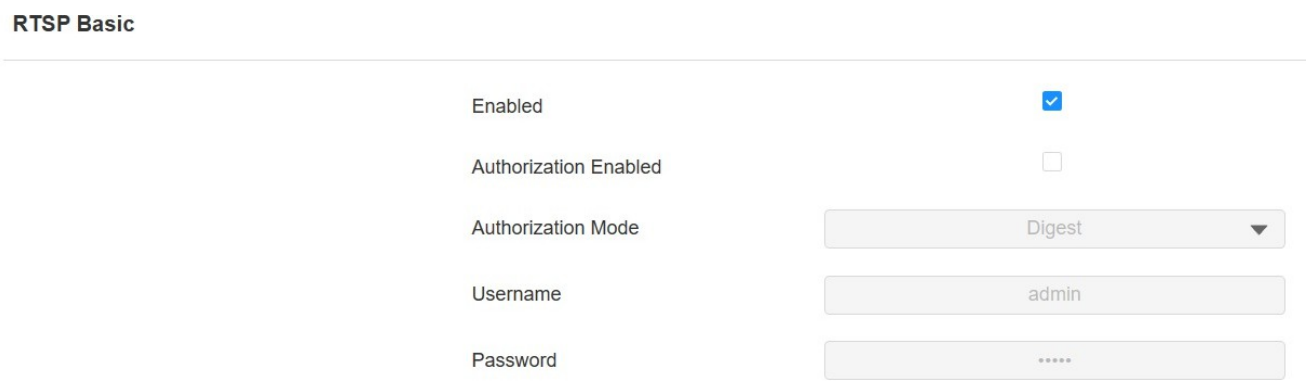
- Możesz również wpisać poprawny adres URL (http://IP_address:8080/video.cgi) w przeglądarce internetowej, jeśli chcesz uzyskać wideo w czasie rzeczywistym bez przechodzenia do interfejsu webowego.

Monitorowanie strumienia RTSP

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

Podstawowe ustawienia RTSP

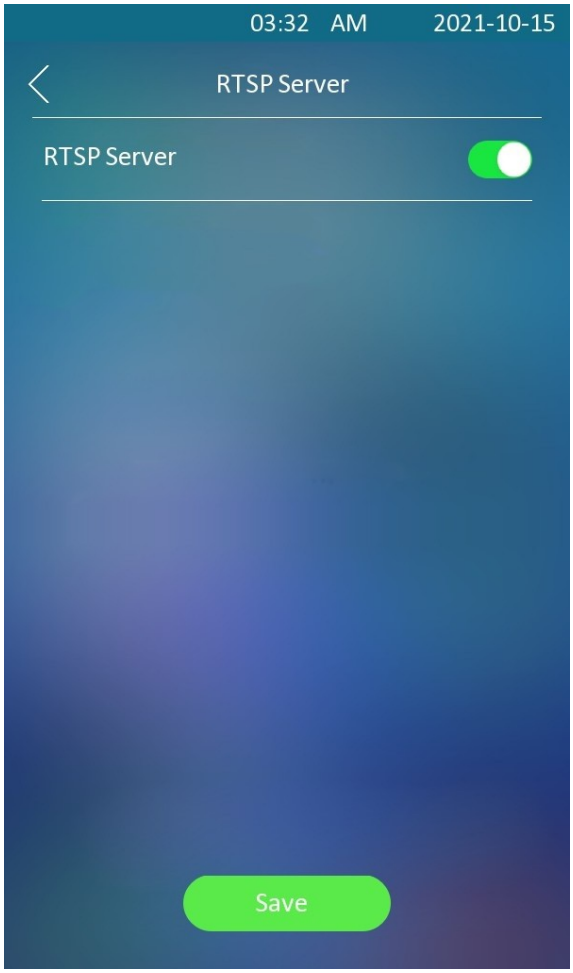
Przed rozpoczęciem korzystania z tej funkcji należy skonfigurować funkcję RTSP pod kątem autoryzacji RTSP, uwierzytelniania i hasła itp. Ścieżka: **Surveillance > RTSP > RTSP Basic**



Konfiguracja parametrów :

- **Authorization Enabled** : zaznacz pole wyboru, aby włączyć autoryzację RTSP. Po włączeniu autoryzacji RTSP wymagane jest wprowadzenie typu uwierzytelniania RTSP, nazwy użytkownika RTSP, hasła RTSP na urządzeniu interkomowym, takim jak monitor wewnętrzny, w celu autoryzacji.
- **Typ uwierzytelniania RTSP**: wybierz typ uwierzytelniania RTSP pomiędzy **Basic** i **Digest. Basic** jest domyślnym typem uwierzytelniania.

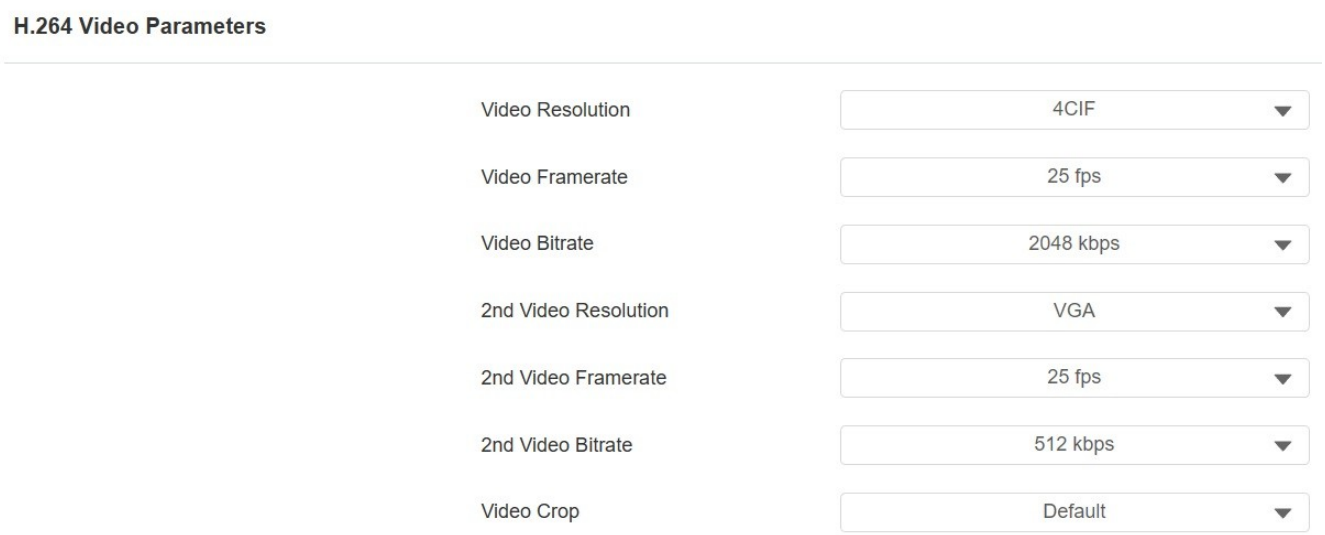
Funkcję RTSP można również włączyć bezpośrednio na urządzeniu. Ścieżka: **Advanced > Surveillance > RTSP Server**



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.

Ścieżka: **Monitoring > RTSP > Parametry wideo H.264**



Konfiguracja parametrów :

- **Rozdzielczość wideo**: wybór rozdzielczości wideo spośród siedmiu opcji: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P** . Domyślną rozdzielczością wideo jest **4CIF**. Jeśli rozdzielczość jest wyższa niż **4CIF**, 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 kbps w** zależności od środowiska sieciowego. Domyślna szybkość transmisji wideo to **2048 kb/s**.
- **2. rozdzielczość wideo**: wybór rozdzielczości wideo dla drugiego kanału strumienia wideo.

  Domyślnym rozwiązaniem wideo jest **VGA**.
- **2nd Video Framerate** : wybór szybkości klatek wideo dla drugiego kanału strumienia wideo.

  25 klatek na sekundę to domyślna liczba klatek na sekundę dla drugiego kanału strumienia wideo.
- **2nd Video Bitrate** : wybierz szybkość transmisji wideo spośród sześciu opcji dla drugiego kanału strumienia wideo. Drugi kanał strumienia wideo ma domyślnie szybkość **512 kb/s.**
- **Kadrowanie wideo** : wybierz **Domyślne,** jeśli chcesz uzyskać przycięty obraz wideo i wybierz Oryginalne, jeśli chcesz uzyskać oryginalny obraz wideo.

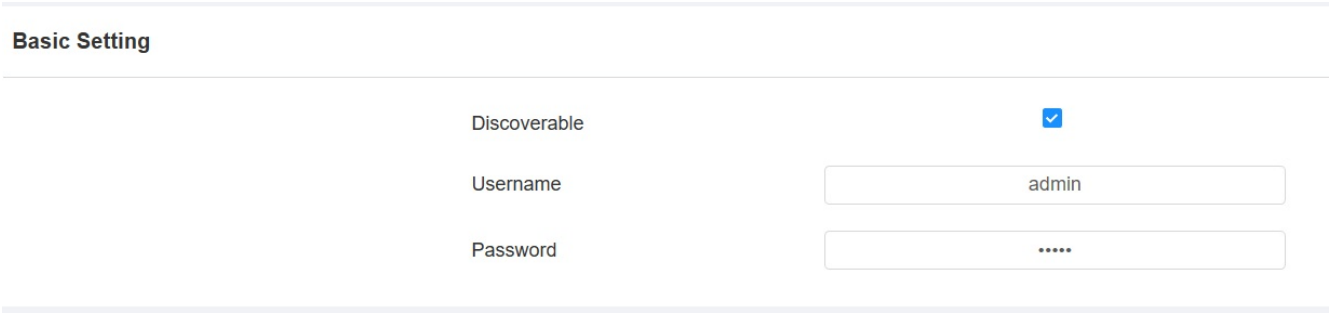
Uwaga

- Seria E18 obsługuje dwa kanały strumienia wideo dla kodeka H.264.

ONVIF

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

Ścieżka: **Monitoring > ONVIF > Ustawienia podstawowe**



Konfiguracja parametrów :

- **Discoverable** : zaznacz pole wyboru, aby włączyć tryb ONVIF. Po wybraniu tej opcji wideo z kamery telefonu może być wyszukiwane przez inne urządzenia. Tryb ONVIF jest domyślnie **włączony.**
- **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

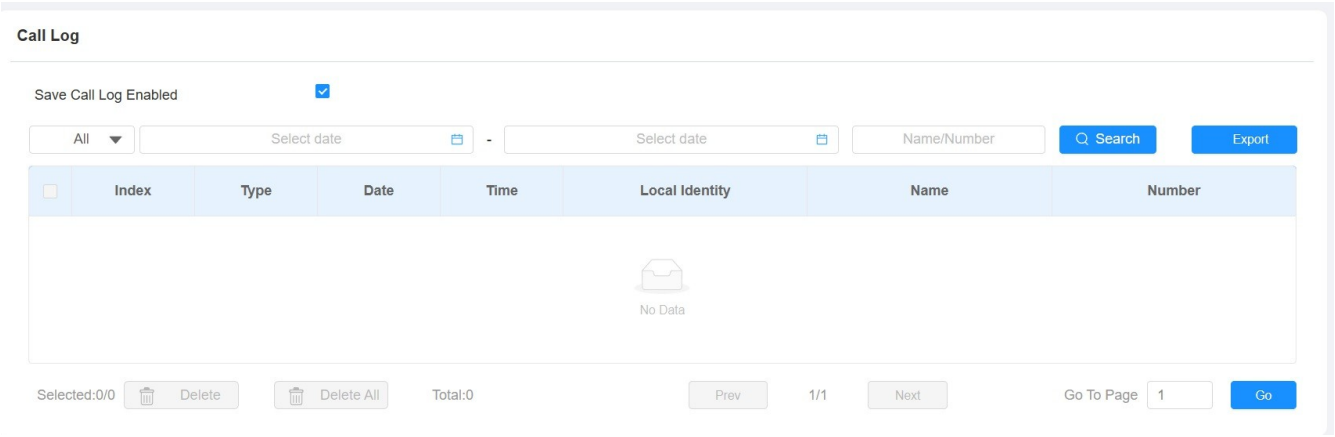
- Wpisz konkretny adres IP telefonu w adresie URL.

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.

Ścieżka: **Status > Rejestr połączeń**



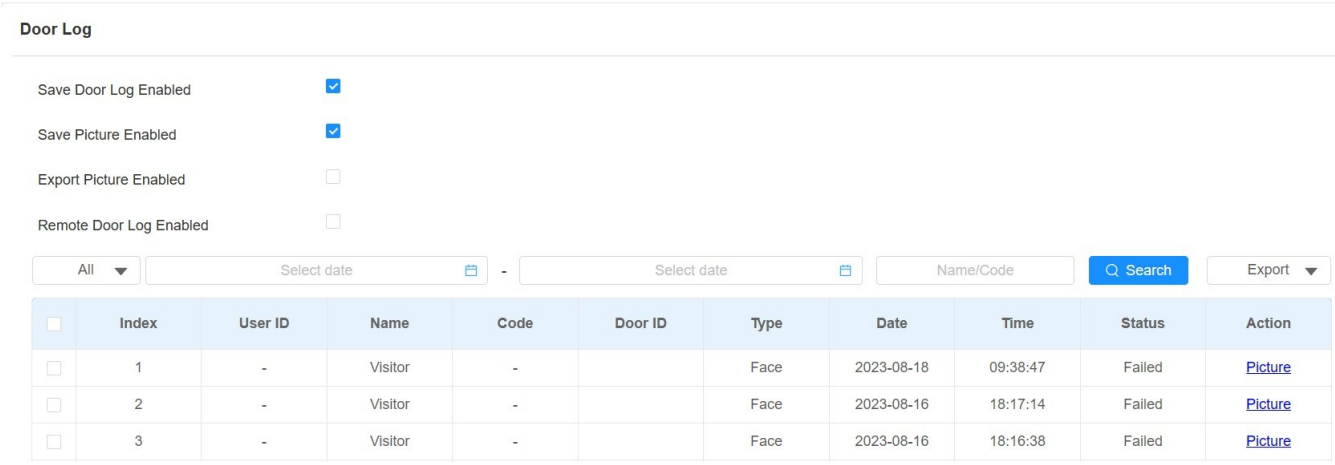
Konfiguracja parametrów :

- **Historia połączeń**: wybierz historię połączeń spośród czterech opcji: **Wszystkie, Wybrane, Odebrane, Nieodebrane** dla określonego typu rejestru połączeń, który ma być wyświetlany.

Dzienniki drzwi

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

Ścieżka: **Status > Access Log** .



Konfiguracja parametrów :

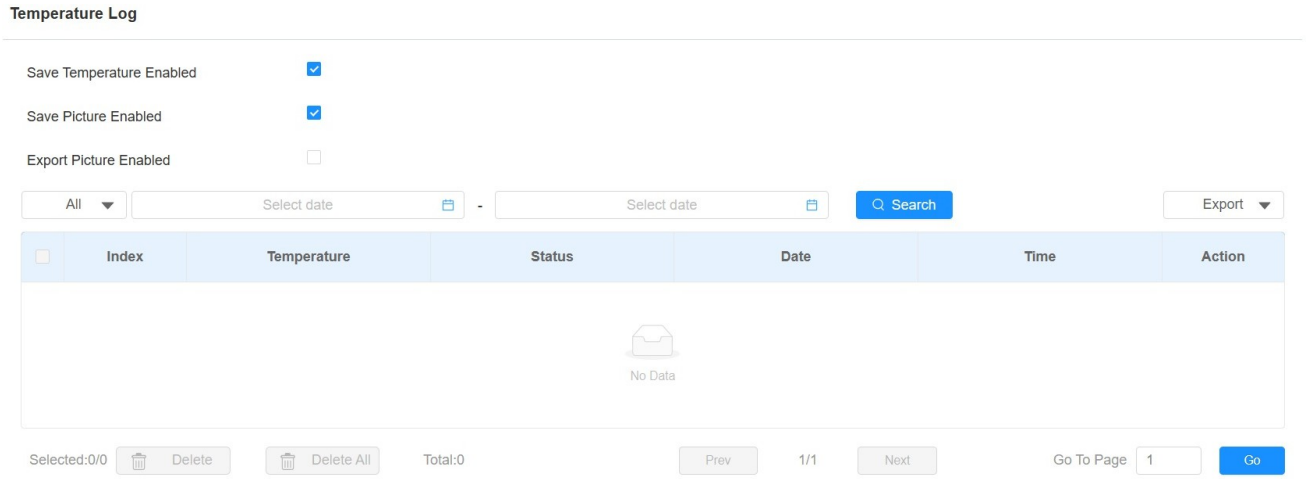
- **Save Picture Enabled**: włącz, jeśli chcesz zapisać przechwyconą migawkę otwartych

drzwi.

- **Export Picture Enabled**: włącz, jeśli chcesz wyeksportować dziennik drzwi z przechwyconym obrazem migawki.
- **Status** : wybierz pomiędzy opcjami **Sukces** i **Niepowodzenie**, aby wyszukać udane lub nieudane dostępy do drzwi.
- **Czas**: wybierz określony przedział czasowy dzienników drzwi, które chcesz wyszukać, sprawdzić lub wyeksportować.
- **Nazwa/Kod** : wybierz opcje **Nazwa** i **Kod,** aby przeszukać dziennik drzwi według nazwy lub kodu PIN.
- **Działanie**: kliknij, aby wyświetlić zrobione zdjęcie.

Dziennik temperatury

Jeśli chcesz wyszukać i sprawdzić dziennik temperatury, możesz wyszukać i sprawdzić dzienniki w interfejsie internetowym urządzenia. Ścieżka: **Status > Temperature Log**

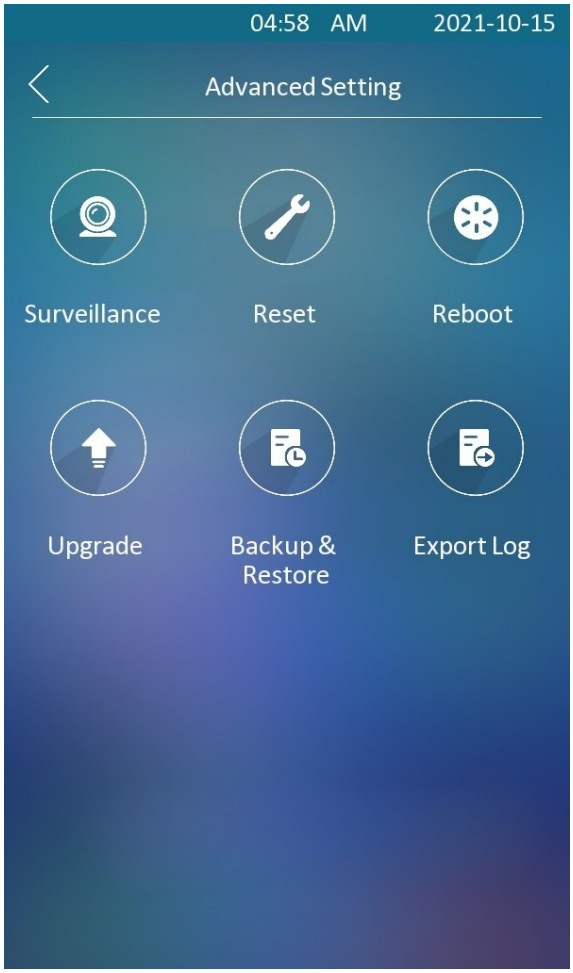


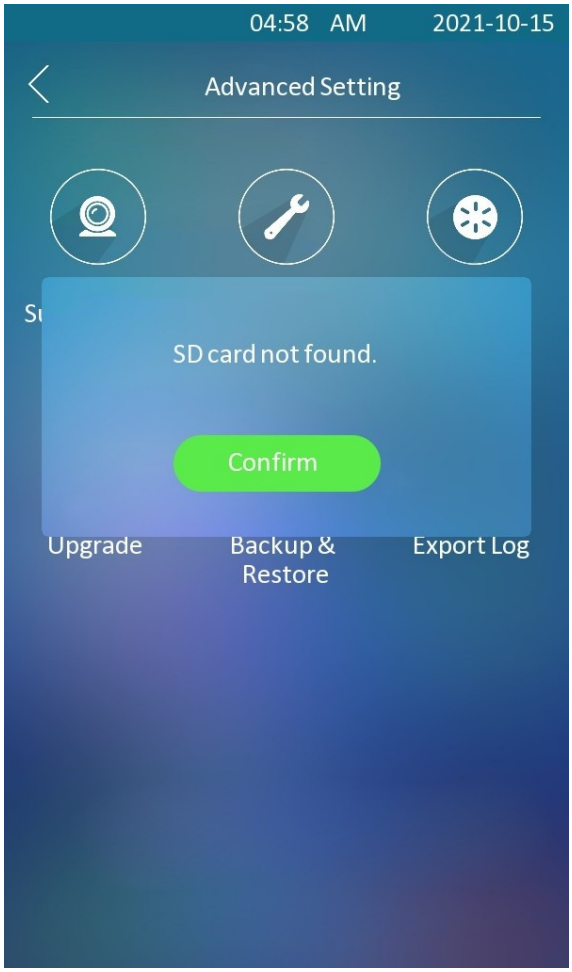
Konfiguracja parametrów :

- **Save Picture Enabled** : włącz, jeśli chcesz zapisać migawkę pomiaru temperatury.
- **Export Picture Enabled**: włącz, jeśli chcesz wyeksportować dziennik temperatury z przechwyconym obrazem migawki.
- **Czas**: wybierz określony przedział czasowy dziennika temperatury, który chcesz wyszukać, sprawdzić lub wyeksportować.
- **Działanie**: kliknij, aby wyświetlić zrobione zdjęcie.

Eksport dzienników

W razie potrzeby można eksportować dzienniki drzwi, dzienniki połączeń i dzienniki temperatury. Ścieżka: **Zaawansowane > Eksportuj dziennik.**





Uwaga

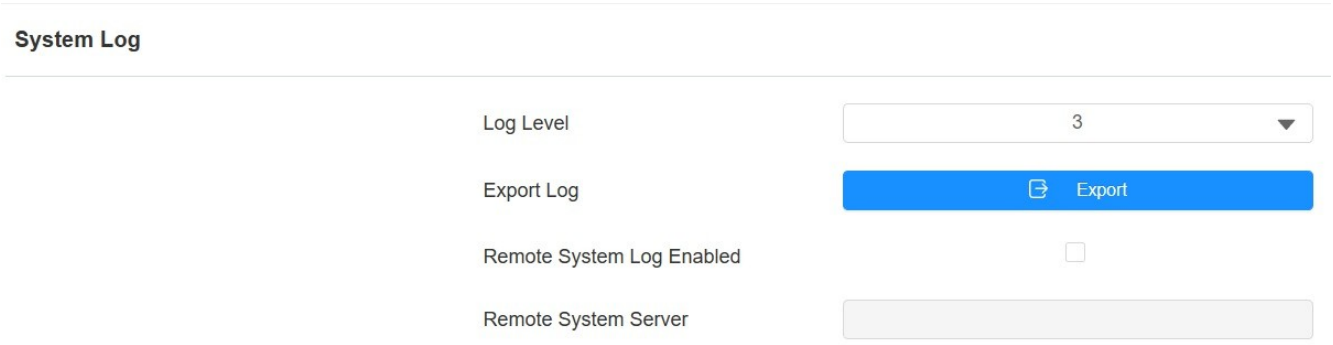
- Aby eksportować dzienniki na ekranie urządzenia, należy włożyć kartę SD.

Debugowanie

Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Ścieżka: **System >Maintenance > System Log**



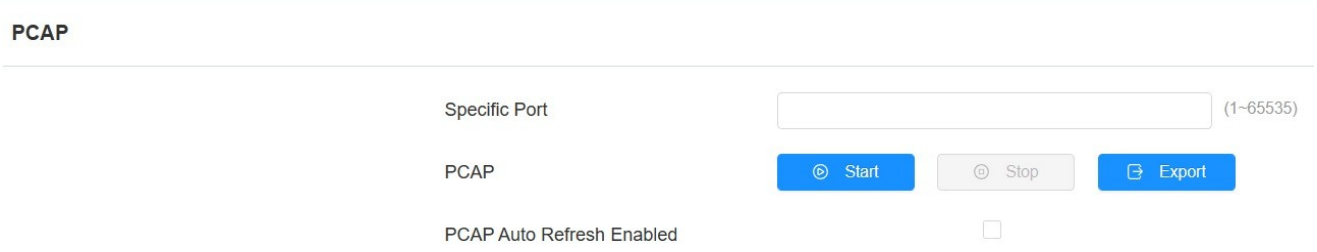
Konfiguracja parametrów :

- **Log Level (Poziom dziennika)**: wybierz poziom dziennika od 1 do 7. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić do celów debugowania. Domyślny poziom dziennika to **3**, im wyższy poziom to **5**, tym bardziej kompletny jest dziennik **7**.
- **Eksportuj dziennik**: kliknij kartę **Eksportuj**, aby wyeksportować tymczasowy plik dziennika debugowania do lokalnego komputera.
- **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.

Ścieżka: **System >Maintenance > PCAP.**



Konfiguracja parametrów :

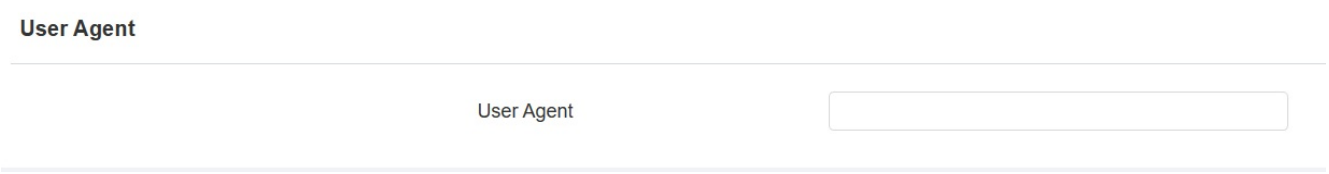
Określony port: wybierz określone porty z zakresu **1-65535**, aby można było przechwytywać tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.

- **PCAP**: kliknij zakładkę **Start** i zakładkę **Stop**, aby przechwycić określony zakres pakietów danych przed kliknięciem zakładki **Export**, aby wyeksportować pakiety danych do lokalnego komputera.
- **Automatyczne odświeżanie PCAP**: wybierz **Włącz** lub **Wyłącz**, 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 na Disable, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycony pakiet danych osiągnie maksymalną pojemność 1 MB.

Agent użytkownika

Agent użytkownika jest używany do celów identyfikacji podczas analizy pakietu danych SIP.

Ścieżka: **Konto > Zaawansowane > Agent użytkownika**



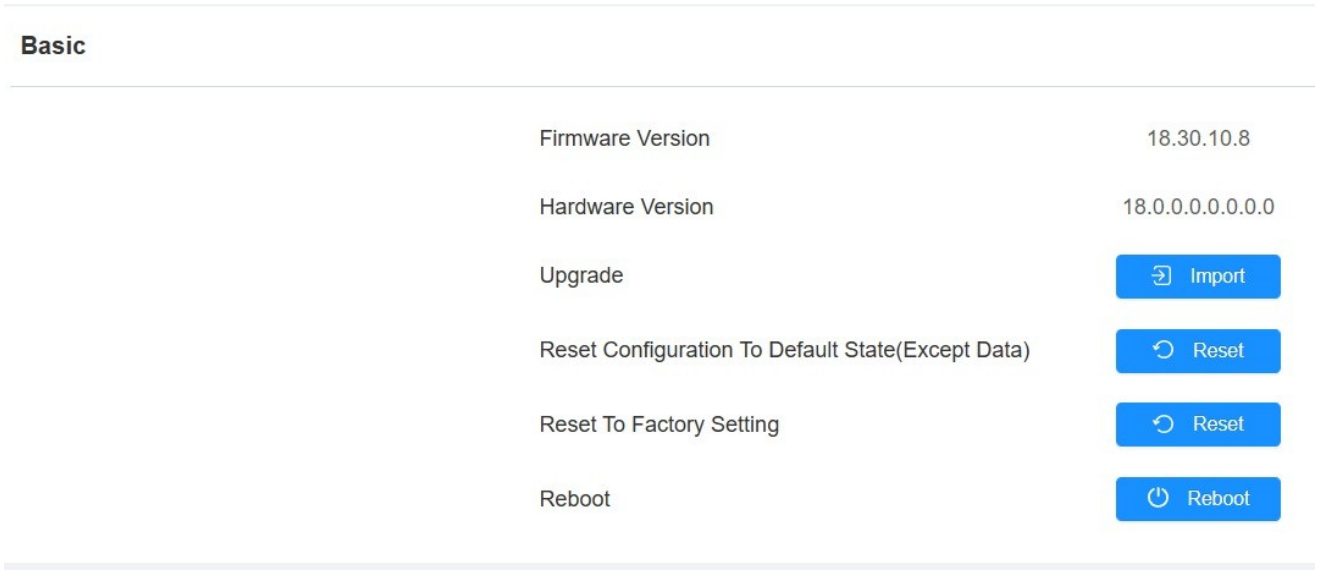
Konfiguracja parametrów :

- **User Agent** : obsługa wprowadzania innej określonej wartości, domyślnie jest to Akuvox.

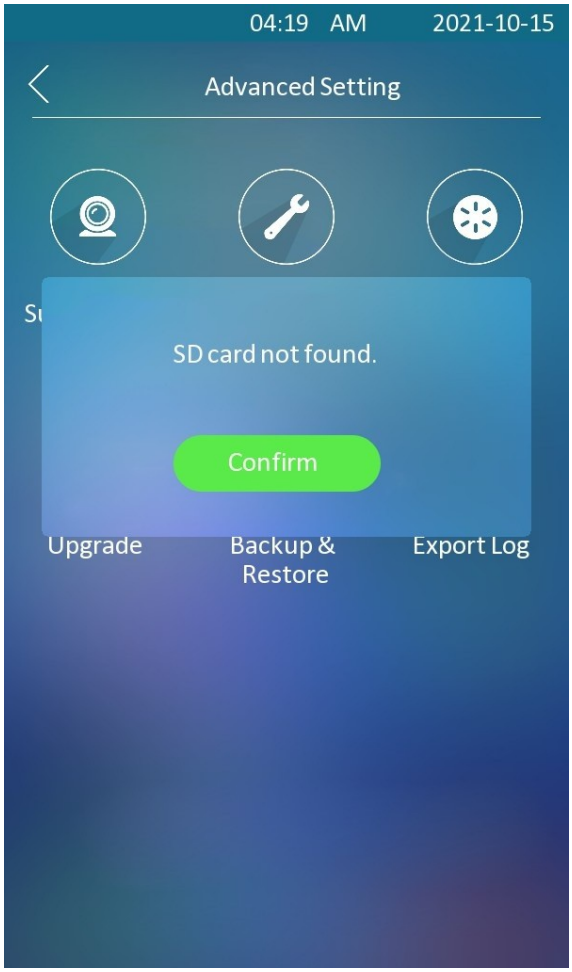
Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można aktualizować w interfejsie internetowym urządzenia.

Aktualizacja urządzenia w interfejsie internetowym Ścieżka: **System > Upgrade.**



- **Aktualizacja urządzenia na** ścieżce **urządzenia**: **Advanced > Upgrade.**



Uwaga

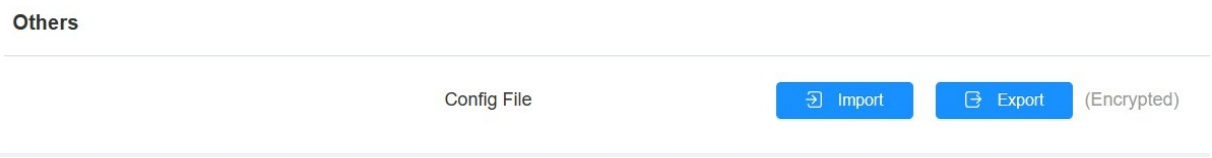
- Po włożeniu karty SD wymagane jest dodanie pliku .rom w katalogu głównym i zmień nazwę pliku na update.rom.

Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować do komputera lokalnego.

Tworzenie kopii zapasowej danych w interfejsie internetowym

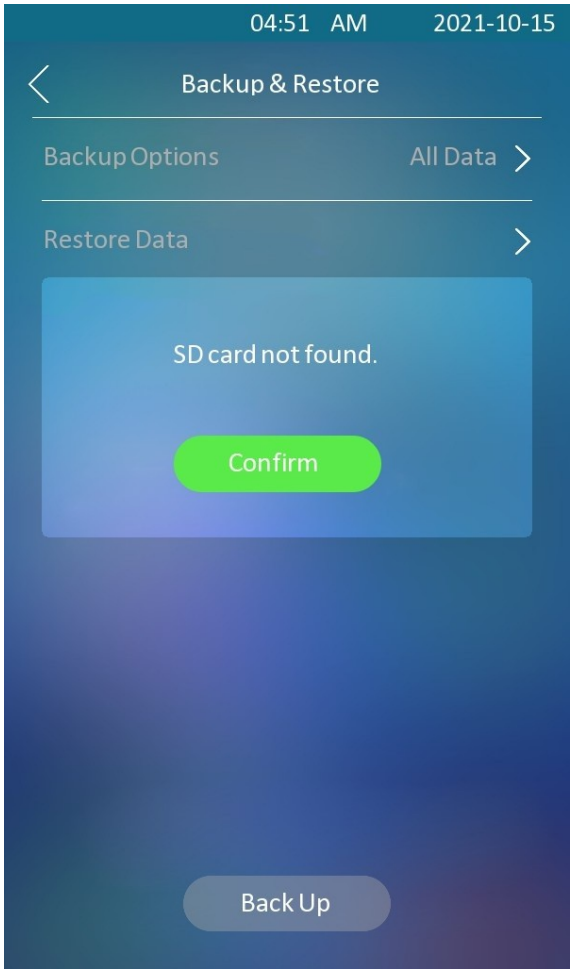
Ścieżka: **System > Konserwacja > Inne**



- **Tworzenie kopii zapasowych danych na urządzeniu**

  Aby wykonać kopię zapasową, należy włożyć kartę SD do urządzenia.

  Ścieżka: **Zaawansowane > Kopia zapasowa i przywracanie**



Konfiguracja parametrów :

- **Opcje kopii zapasowej** : wybierz **Tylko dane użytkownika** lub **Wszystkie dane**, co jest ustawieniem domyślnym. Wybierz opcję **Wszystkie dane**, jeśli chcesz utworzyć kopię zapasową danych użytkownika, harmonogramu grupy i danych konfiguracyjnych

z wyłączeniem wszystkich typów dzienników. Wybierz **Tylko dane użytkownika**, jeśli chcesz utworzyć kopię zapasową tylko danych użytkownika i harmonogramu.

Uwaga

- Obsługiwane są karty SDHC i SDXC w formacie FAT32.

Automatyczne dostarczanie

Konfigurację i aktualizację urządzenia można przeprowadzić w interfejsie internetowym za pomocą jednorazowego automatycznego udostępniania i zaplanowanego automatycznego udostępniania za pomocą plików konfiguracyjnych, oszczędzając w ten sposób konieczność ręcznego konfigurowania poszczególnych konfiguracji na terminalu kontroli dostępu.

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

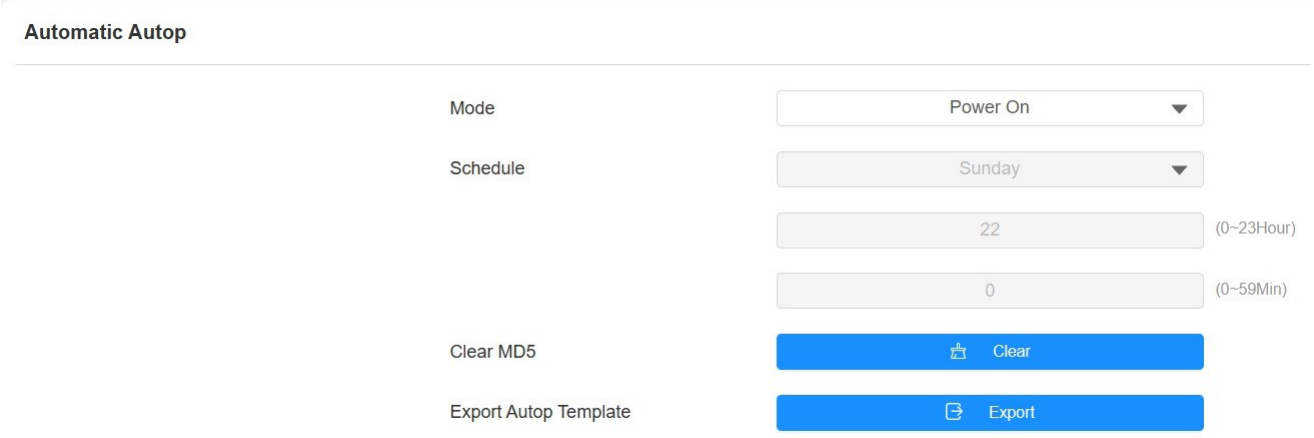
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny do konfiguracji grupowej różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC do specyficznej konfiguracji urządzenia jest nazwany według jego adresu MAC.
- Jeśli serwer ma oba typy plików konfiguracyjnych, urządzenia najpierw uzyskają dostęp do ogólnych plików konfiguracyjnych, zanim uzyskają dostęp do plików konfiguracyjnych opartych na adresie 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.

Ścieżka: **System > Auto Provisioning > Automatic Autop**



Konfiguracja parametrów :

- **Tryb** :
  - **Power On**: wybierz **Power on**, jeśli chcesz, aby urządzenie wykonywało Autop przy każdym uruchomieniu.
  - **Wielokrotnie**: wybierz opcję **Wielokrotnie**, jeśli chcesz, aby urządzenie wykonywało funkcję Autop zgodnie z ustawionym harmonogramem.
  - **Power On + Repeatedly**: wybierz **Power On + Repeatedly,** jeśli chcesz połączyć tryb **Power On** z trybem **Repeatedly**, który umożliwi urządzeniu wykonywanie Autop przy każdym uruchomieniu lub zgodnie z ustawionym harmonogramem.
  - **Hourly Repeat**: wybierz opcję **Hourly Repeat**, jeśli chcesz, aby urządzenie wykonywało funkcję Autop co godzinę.

Konfiguracja PNP

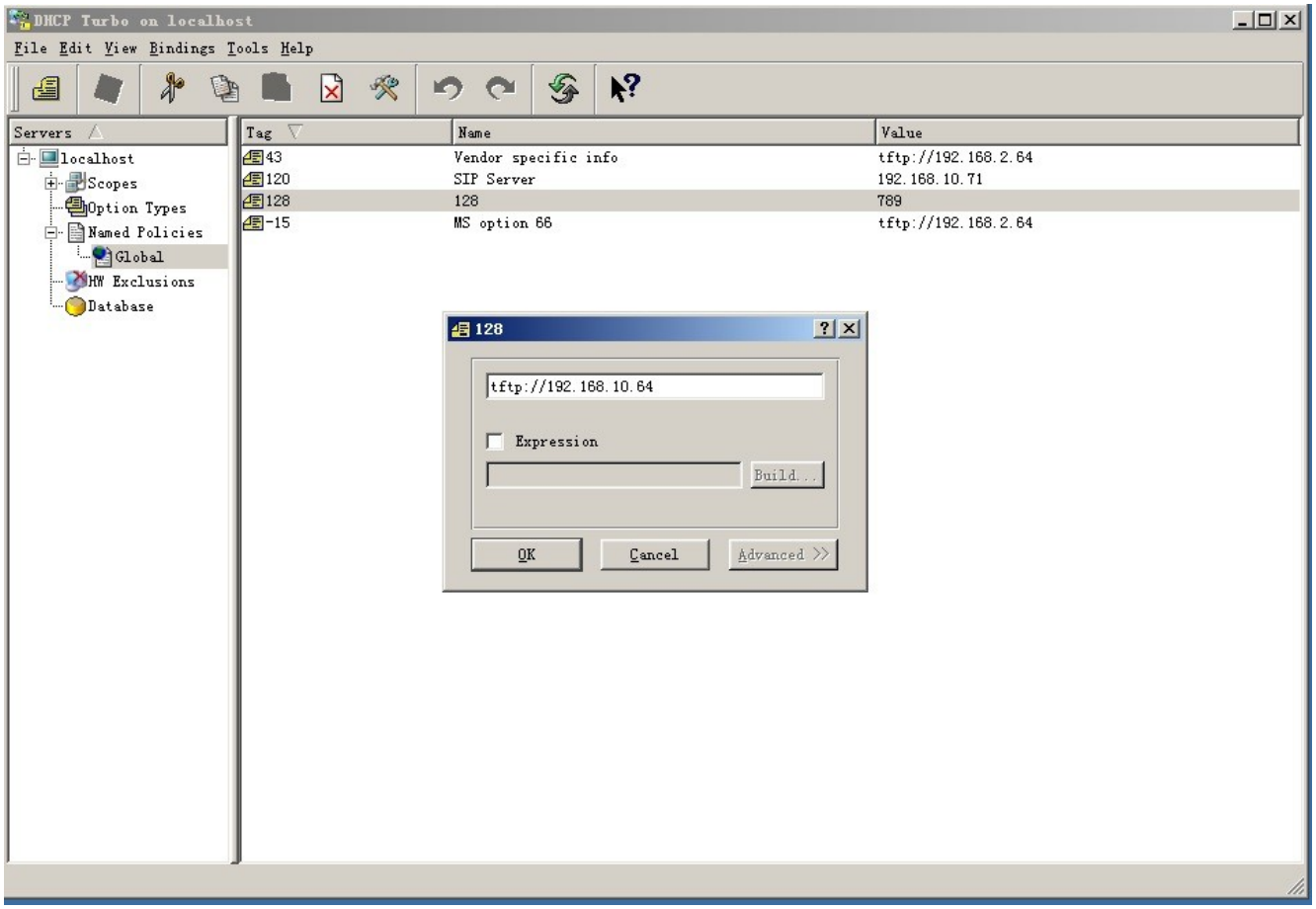
Plug and Play (PNP) to połączenie wsparcia sprzętowego i programowego, które umożliwia systemowi komputerowemu rozpoznawanie i dostosowywanie się do zmian konfiguracji sprzętowej przy niewielkiej lub żadnej interwencji użytkownika.

Ścieżka: **System > Automatyczne udostępnianie > Opcja PNP**

Konfiguracja udostępniania DHCP

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

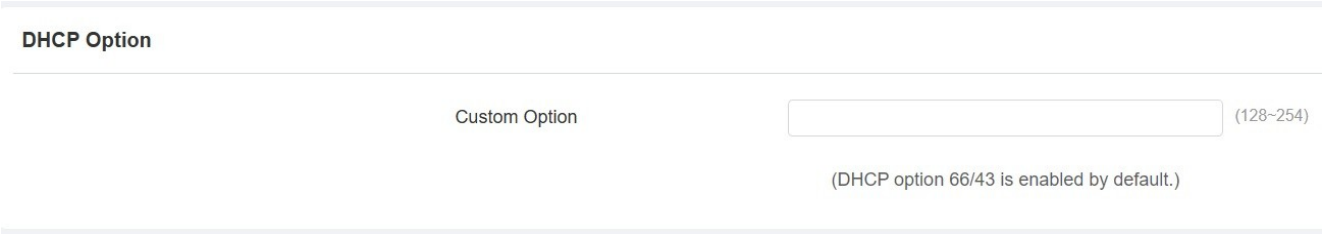
Opcja niestandardowa zdefiniowana przez użytkowników z kodami opcji w zakresie 128-255), należy skonfigurować opcję niestandardową DHCP w interfejsie internetowym.



Uwaga

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

Ścieżka: **System > Auto Provisioning > DHCP Option.**



Konfiguracja parametrów :

- **Opcja niestandardowa**: wprowadź kod DHCP dopasowany do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych w celu konfiguracji lub aktualizacji.

- **Opcja 66 DHCP**: jeśli żadna z powyższych opcji nie jest ustawiona, urządzenie automatycznie użyje Opcji 66 DHCP do uzyskania adresu URL serwera aktualizacji. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 66 z adresem URL serwera aktualizacji.
- **Opcja 43 DHCP**: jeśli urządzenie nie otrzyma adresu URL z Opcji 66 DHCP, automatycznie użyje Opcji 43 DHCP. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 43 z adresem URL serwera aktualizacji.

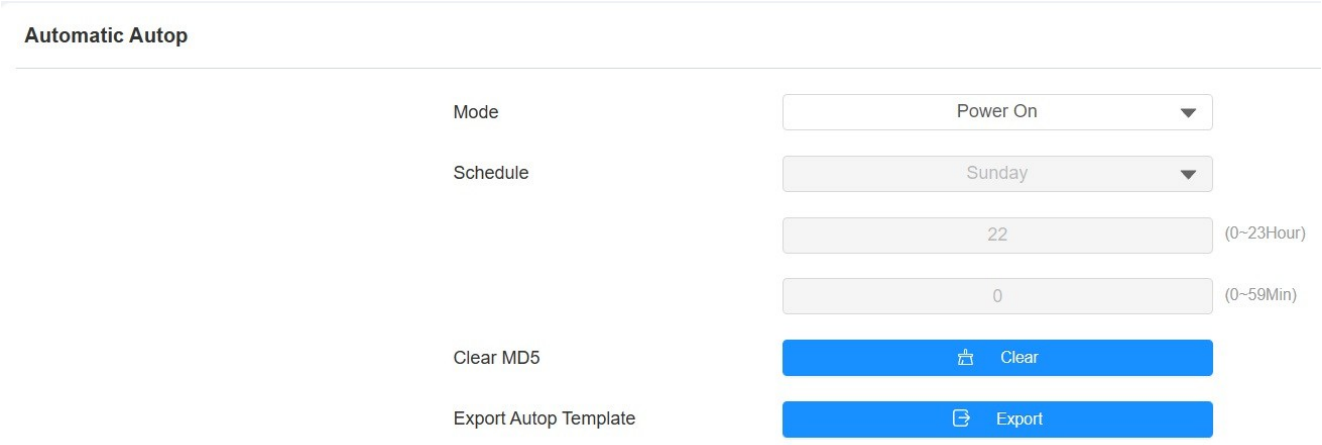
Uwaga

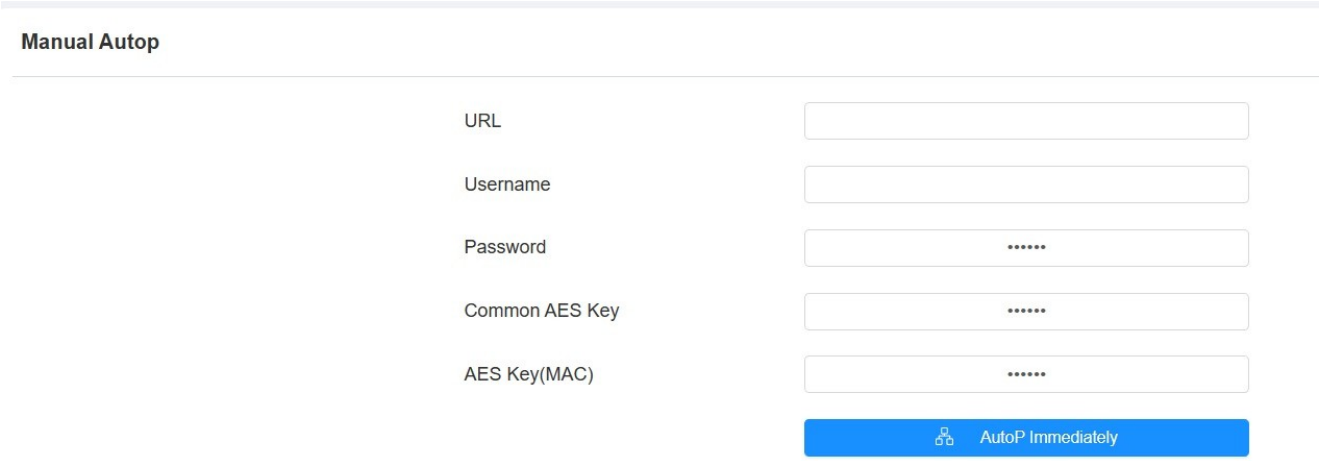
- Ogólny plik konfiguracyjny dla udostępniania wsadowego ma format "cfg". I Biorąc za przykład E18, "r000000000018.cfg (w sumie 10 zer), podczas gdy plik konfiguracyjny oparty na MAC dla konkretnego udostępniania urządzenia ma format MAC_Address urządzenia.cfg, na przykład "0C110504AE5B.cfg".

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** : skonfiguruj adres serwera TFTP, HTTP, HTTPS, FTP dla provisioningu.
- **Nazwa użytkownika**: ustaw nazwę użytkownika, jeśli serwer wymaga dostępu do nazwy użytkownika, w przeciwnym razie pozostaw to pole puste.
- **Hasło**: ustaw hasło, jeśli serwer wymaga hasła dostępu, w przeciwnym razie pozostaw to pole puste.
- **Common AES Key**: ustawienie kodu AES dla interkomu w celu odszyfrowania ogólnego pliku konfiguracyjnego Auto Provisioning.
- **Klucz AES (MAC)**: ustawienie kodu AES dla interkomu w celu odszyfrowania pliku konfiguracyjnego Auto Provisioning opartego na MAC.

Wskazówka

- AES, jako jeden z typów szyfrowania, powinien być skonfigurowany tylko wtedy, gdy plik konfiguracyjny jest szyfrowany za pomocą AES.

Uwaga

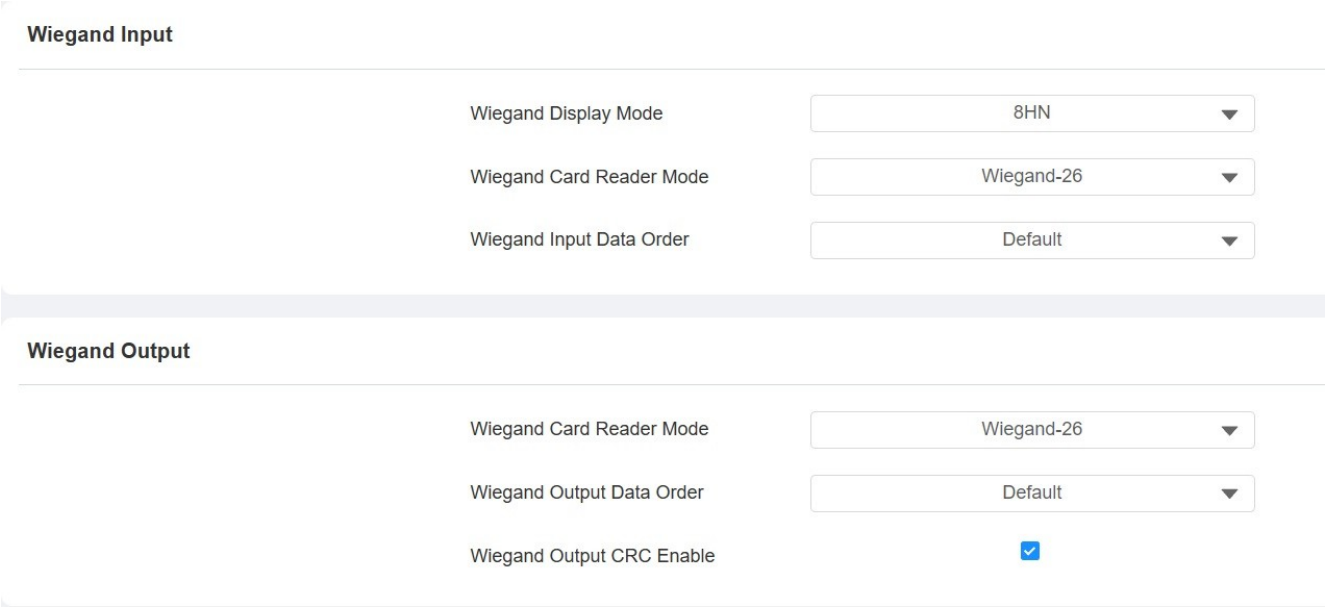
- Format adresu serwera:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/ (umożliwia logowanie anonimowe) ftp://username @192.168.0.19/ (wymaga nazwy użytkownika i hasła)
  - HTTP: http://192.168.0.19/ (używa domyślnego portu 80) http://192.168.0.19:8080/ (używa innych portów, takich jak 8080)
  - HTTPS: https://192.168.0.19/ (używa domyślnego portu 443)
- Akuvox nie dostarcza serwera określonego przez użytkownika. Proszę samodzielnie przygotować serwer TFTP/FTP/HTTP/HTTPS.

Integracja z urządzeniami innych firm

Integracja przez Wiegand

Jeśli chcesz zintegrować bramofon z urządzeniami innych firm za pośrednictwem Wiegand, możesz skonfigurować Wiegand w interfejsie internetowym.

Ścieżka: **Urządzenie > Wiegand**



Konfiguracja parametrów :

- **Tryb wyświetlania Wiegand**: wybór formatu kodu karty Wigand spośród **8H10D; 6H3D 5D; 6H8D; 8HN; 8HR; RAW; 8HR10D**.
- **Tryb czytnika kart Wiegand**: ustawienie formatu transmisji danych Wiegand spośród trzech opcji: **Wiegand 26, Wiegand 34** i **Wiegand 58** . Format transmisji powinien być identyczny między bramofonem a urządzeniem, które ma zostać zintegrowane.
- **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.
- Wiegand **Output Data Order (Kolejność danych wyjściowych** Wiegand): ustawienie kolejności danych wyjściowych Wiegand pomiędzy **Normal (Normalna)** i Reversed (**Odwrócona)**. W przypadku wybrania opcji Reversed numer karty wejściowej zostanie odwrócony i odwrotnie.
- **Wyjście Wiegand CRC**: zaznacz, aby włączyć funkcję sprawdzania parzystości w celu zapewnienia, że dane oparte na sygnale mogą być przesyłane poprawnie zgodnie z ustaloną transmisją danych.

Podczas integracji z urządzeniami innych firm należy skonfigurować wyjście kodu PIN Wiegand w oparciu o format wyjściowy Wiegand urządzenia innej firmy.

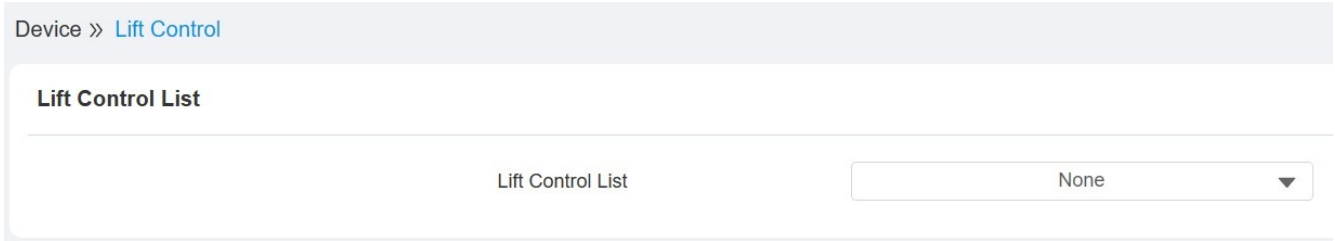
Konfiguracja parametrów :

- **8 bitów na cyfrę**: wybierz, jeśli urządzenie innej firmy przyjmuje format **8 bitów na cyfrę.** Kod PIN jest przesyłany oddzielnie za pomocą cyfry (jedna cyfra składa się z 8 bitów).
- **4 bity na cyfrę**: wybierz, jeśli urządzenie innej firmy przyjmuje format **4 bitów na cyfrę.** Kod PIN jest przesyłany oddzielnie za pomocą cyfry (jedna cyfra składa się z 4 bitów).
- **All at once** : wybierz tę opcję, jeśli urządzenie innej firmy obsługuje format **All at once.** Po wybraniu tej opcji kod PIN nie zostanie przesłany, dopóki nie zostanie wprowadzony cały kod PIN.

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 :

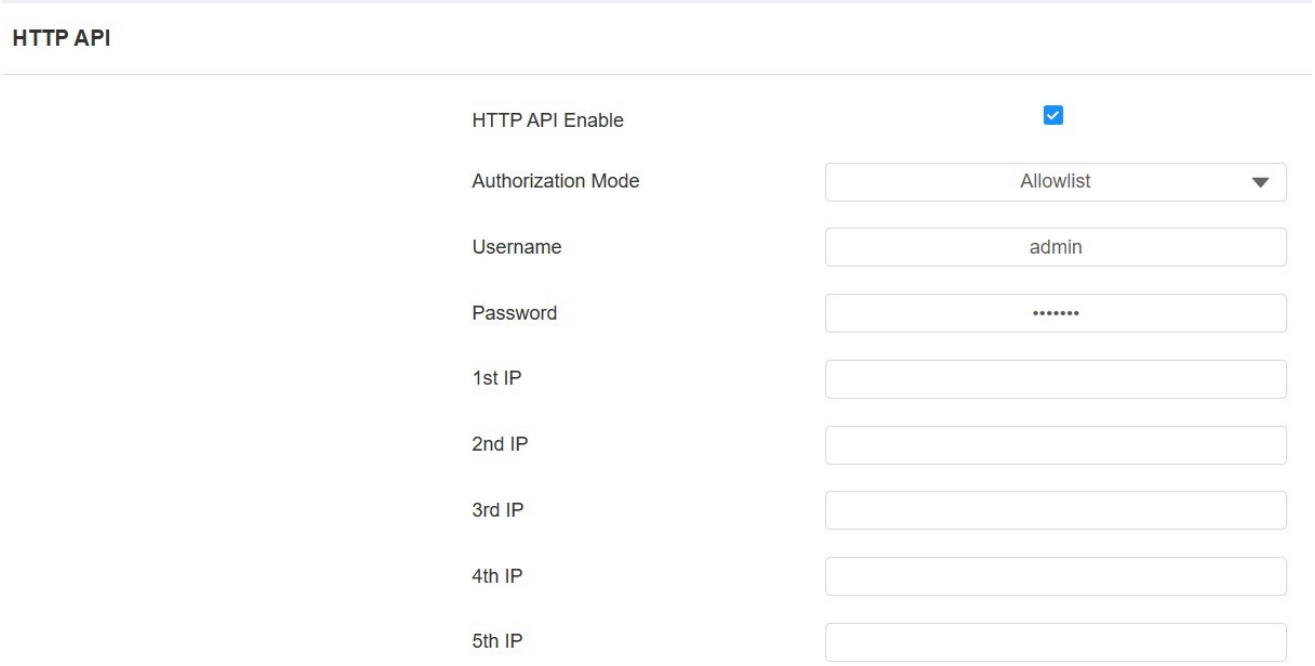
- **Lift Control List**: wybierz tryb integracji spośród **None, OSDP, Akuvox EC 32, KEYKING**. Szczegóły dotyczące opcji zostaną przedstawione w poniższej tabeli.

Nie.	Tryb integracji	Opis
1	Brak	W przypadku wybrania opcji **Brak** integracja RS485 zostanie wyłączona.
2	OSDP	W przypadku wybrania trybu **OSDP** komunikacja między bramofonem a urządzeniem innej firmy odbywa się za pośrednictwem protokołu OSDP. Należy sprawdzić protokół integracji urządzeń i upewnić się, że korzystają one z tego samego protokołu integracji.
3	Akuvox EC32	Wybierz **Akuvox EC 32**, jeśli chcesz połączyć urządzenie z kontrolerem windy Akuvox EC32.
4	KEYKING	Wybierz **KEYKING**, jeśli chcesz zintegrować się z kontrolerem windy KEYKING.

Integracja przez HTTP API

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

Ścieżka: **Ustawienia > HTTP API**



Konfiguracja parametrów :

- **HTTP API Enable** : włącz lub wyłącz funkcję HTTP API dla integracji z innymi firmami. Na przykład, jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status zabroniony HTTP 403.
- **Tryb autoryzacji**: wybierz jedną z czterech opcji: **None, Allowlist, Basic, Digest** i **Token** dla typu autoryzacji, które zostaną szczegółowo wyjaśnione w poniższej tabeli.
- **Nazwa użytkownika** : wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic** i **Digest.**
  Domyślną nazwą użytkownika jest admin.

  Hasło : wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic** i **Digest.** Domyślna

nazwa użytkownika to admin.

1st IP- 5th IP : wprowadź adres IP urządzeń innych firm, gdy dla integracji wybrano autoryzację WhiteList.

Zapoznaj się z poniższym opisem trybu uwierzytelniania:

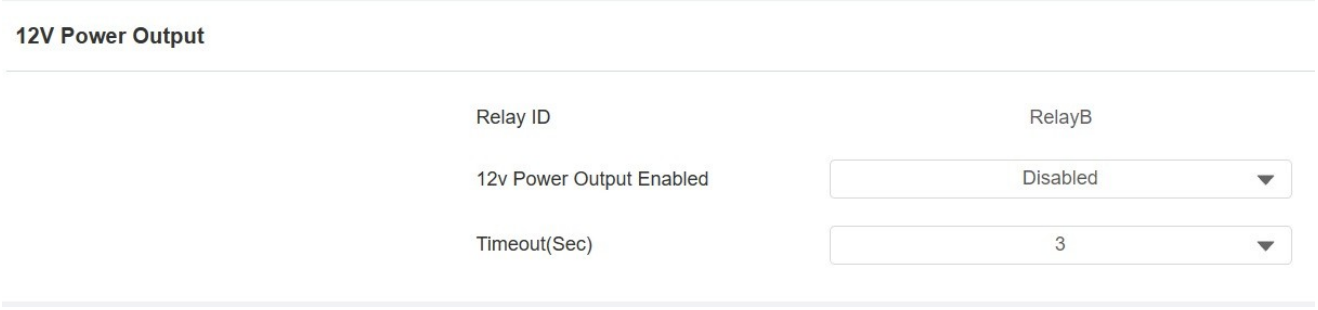
NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Allow List	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
3	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication.In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
4	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In Authorization field of Http request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
5	Token	This mode is used by Akuvox developer only.

Kontrola mocy wyjściowej

Urządzenie może służyć jako źródło zasilania dla

zewnętrznych przekaźników. Ścieżka: **Kontrola dostępu >**

Przekaźnik > Wyjście zasilania 12 V



Konfiguracja parametrów :

Identyfikator przekaźnika: wybierz przekaźnik, który ma być zasilany przez E18.
12V Power Output: wybierz **Disabled,** aby wyłączyć funkcję wyjścia zasilania; wybierz **Always**, aby umożliwić kontrolerowi dostępu ciągłe zasilanie urządzenia zewnętrznego. Wybierz **Triggered By Open Relay**, jeśli chcesz, aby E18 dostarczał zasilanie do urządzenia zewnętrznego za pośrednictwem wyjścia 12 i interfejsu GND podczas limitu czasu, gdy stan przekaźników zostanie zmieniony z niskiego na wysoki.

- **Time Out (Sec)**: wybór czasu zasilania po wyzwoleniu przekaźnika. Trzy opcje: **3, 5, 10** . Domyślnie są to 3 sekundy. Napięcie wyjściowe wynosi 12 V, a maksymalny prąd wyjściowy to 0,8 A.

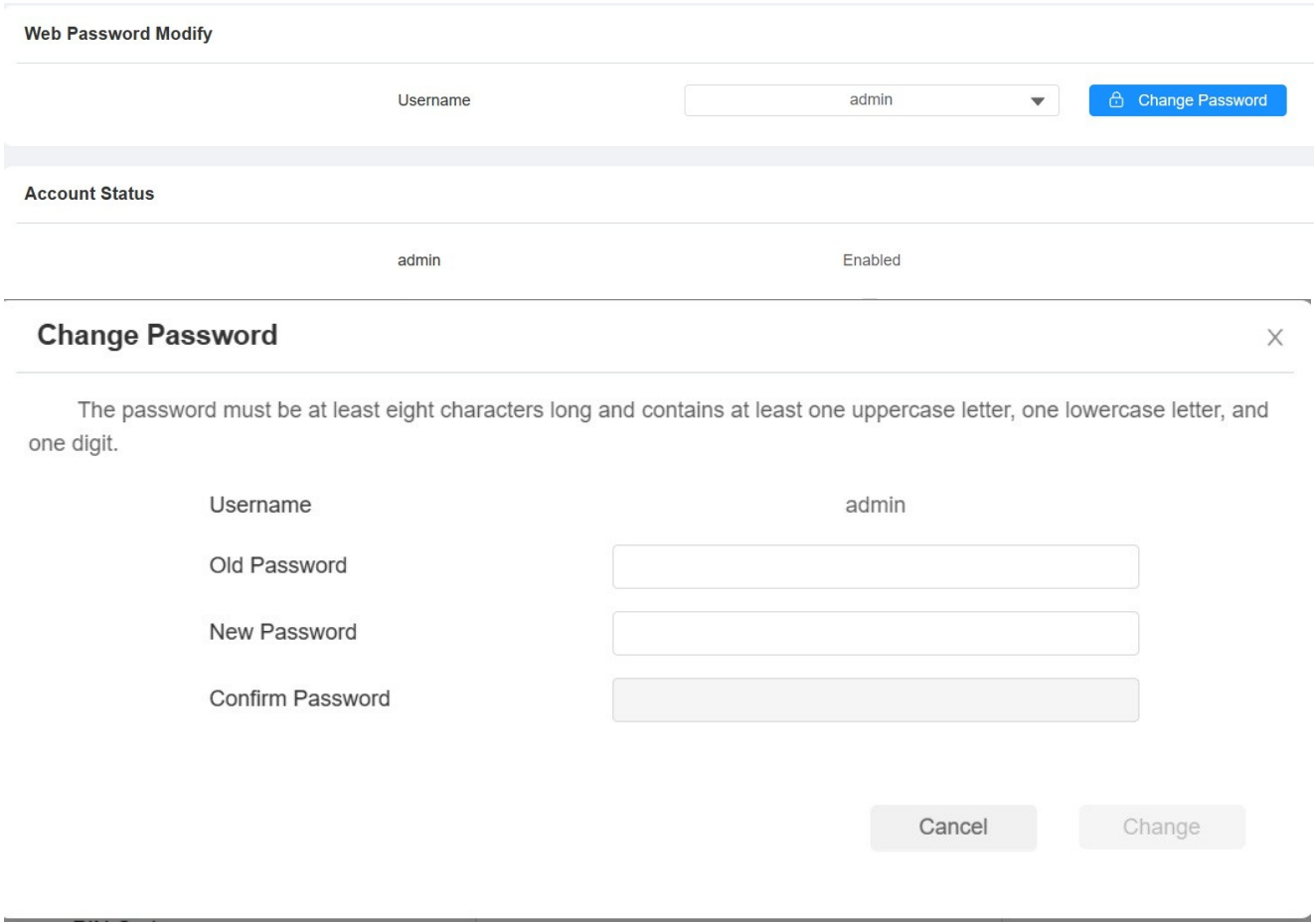
Modyfikacja hasła

W interfejsie internetowym urządzenia można ustawić i zmienić zarówno systemowy kod PIN umożliwiający dostęp do ustawień urządzenia, jak i hasło logowania umożliwiające dostęp do interfejsu internetowego. Ponadto podczas ustawiania haseł można również wybrać rolę użytkownika.

Modyfikacja hasła interfejsu sieciowego urządzenia

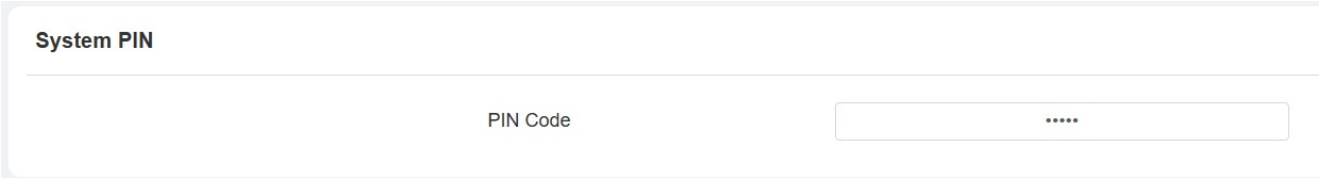
Aby zmodyfikować hasło interfejsu internetowego, można to zrobić w interfejsie internetowym urządzenia. Wybierz **Admin** dla konta administratora i **User** dla konta użytkownika. Kliknij kartę **Change Password**, aby zmienić hasło.

Ścieżka: **System > Bezpieczeństwo > Modyfikacja hasła sieciowego**



Modyfikacja hasła systemowego

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

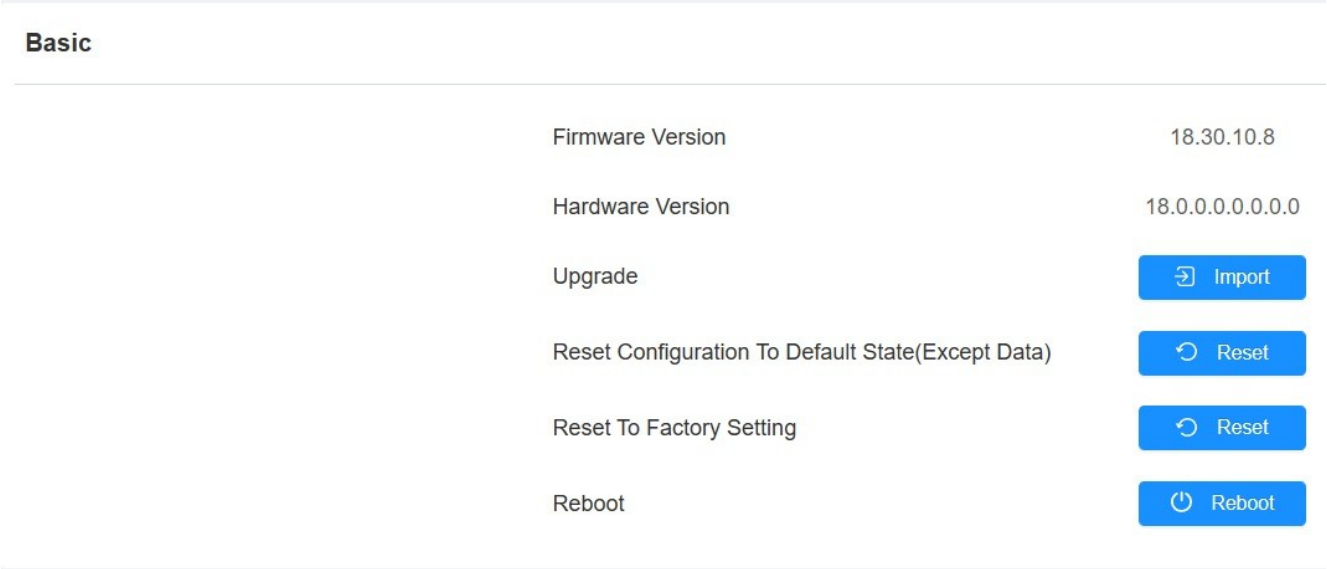


Ponowne uruchamianie i resetowanie systemu

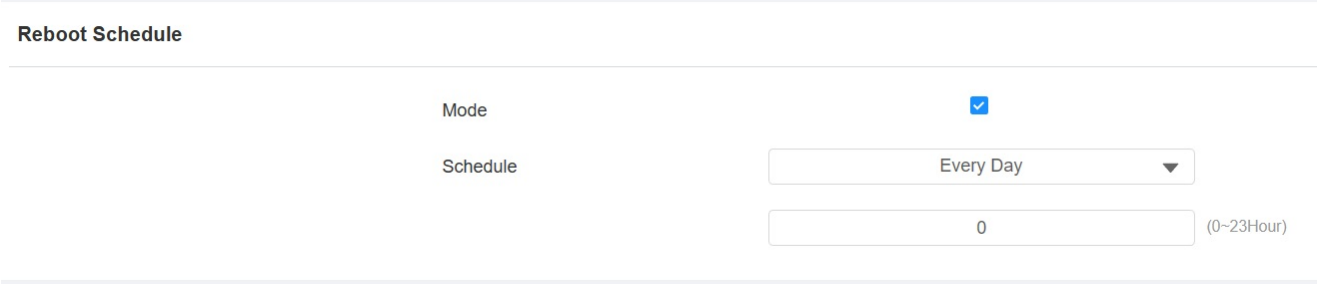
Reboot

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

Aby zrestartować ustawienia systemu w interfejsie sieci Web **System > Upgrade.**



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

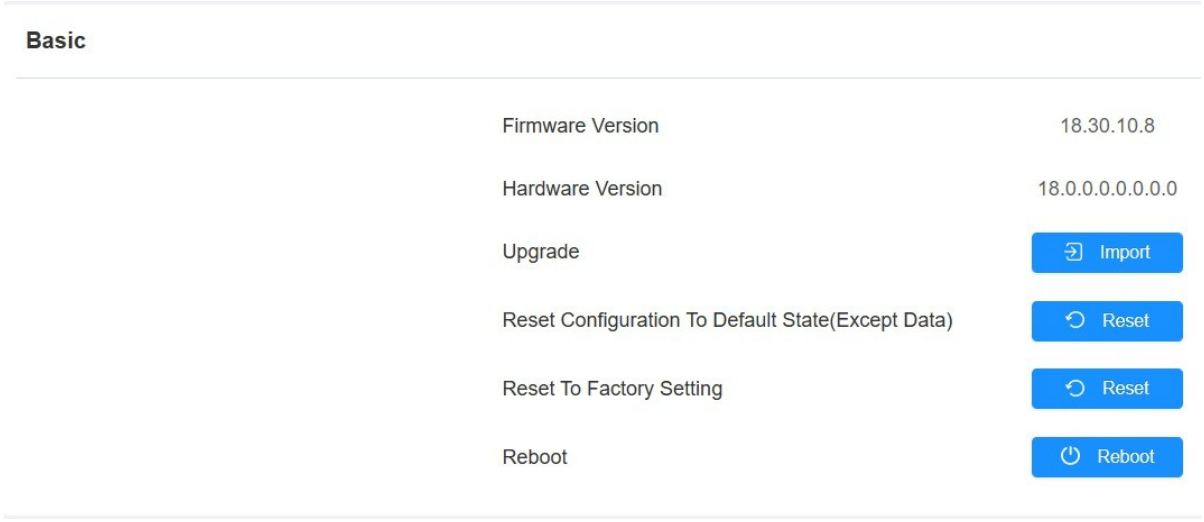


Reset

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

Ścieżka: **System > Aktualizacja > Podstawowa**

- **Aby zresetować urządzenie w interfejsie internetowym urządzenia**



- **Aby zresetować urządzenie na**
  Ścieżce **urządzenia: Zaawansowane**