Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

E16 SERIES DOOR PHONE

Administrator Guide

Dziękujemy za wybranie bramofonów Akuvox serii E16. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy wersji 216.30.0.67 i zawiera wszystkie konfiguracje funkcji bramofonów z serii E16. Odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe.

Przegląd produktów

Seria Akuvox E16 to wideodomofon IP z systemem Linux i ekranem dotykowym. Integruje komunikację audio i wideo, kontrolę dostępu i nadzór wideo. Seria E16 oferuje konfigurowalne funkcje dzięki zaawansowanemu systemowi SmartPlus i technologii komunikacji opartej na sztucznej inteligencji, dostosowując się do preferencji operacyjnych. Dzięki wielu portom, takim jak RS485 i Wiegand, umożliwia łatwą integrację z zewnętrznymi systemami cyfrowymi, takimi jak kontrolery wind i czujniki alarmu przeciwpożarowego. To kompleksowe rozwiązanie zapewnia całościową kontrolę nad wejściami do budynku i jego otoczeniem, zapewniając zwiększone bezpieczeństwo dzięki różnym metodom dostępu, takim jak dostęp za pomocą karty, NFC, Bluetooth, kod QR i dostęp do drzwi z pomiarem temperatury ciała, idealny do budynków mieszkalnych, biurowych i kompleksów.

Dziennik zmian

- Obsługa włączania i wyłączania prywatnego kodu
- PIN Ulepszone połączenie sekwencyjne
- Dodaj przekaźnik bezpieczeństwa
- Obsługa wyświetlania **najemców** na ekranie głównym urządzenia

Specyfikacja modelu

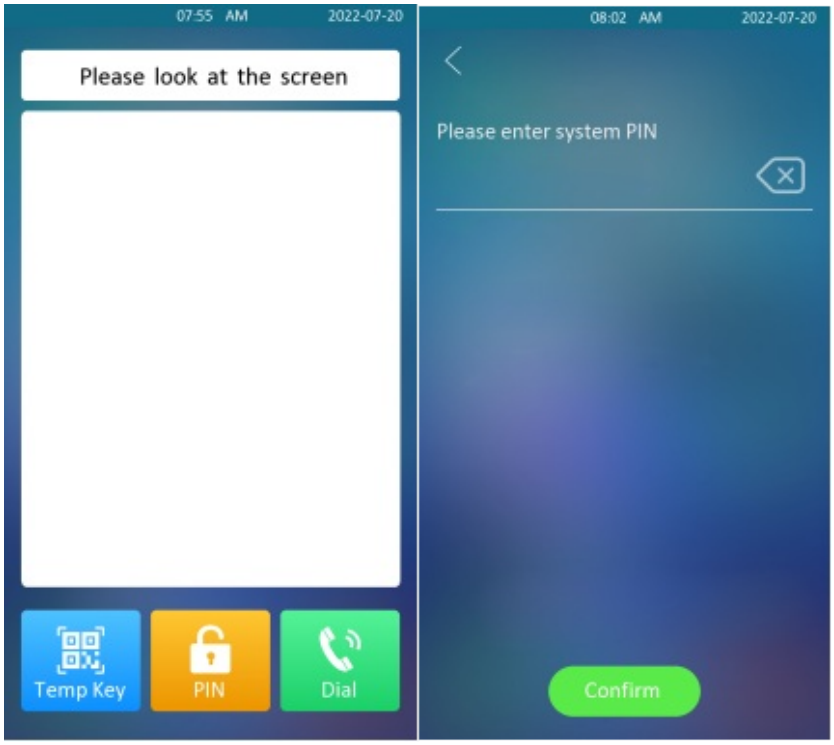
Ekran dotykowy	√
Wyjście przekaźnika	1
Alarm wł.	1
RS485	√
Czytnik kart	13,56 MHZ
Wi-Fi	X
Bluetooth	√
Wykrywanie temperatury	Opcjonalnie
Rozpoznawanie twarzy	√
LTE	X
USB	X
Zewnętrzna karta SD	X

Dostęp do urządzenia

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

Dostęp do ustawień urządzenia na urządzeniu

Aby uzyskać dostęp do ustawień urządzenia, można długo nacisnąć ekran początkowy przez około pięć sekund, a następnie wprowadzić domyślny kod PIN **administratora** i 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 można uzyskać za pomocą skanera IP.

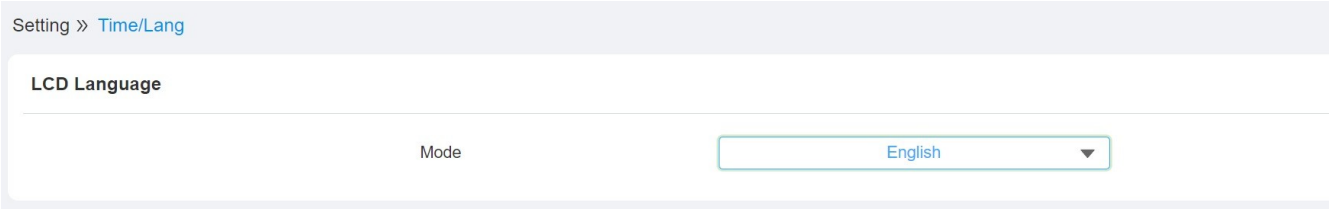
- Pobierz skaner IP: **https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP**
- Zobacz szczegółowy przewodnik: **https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner**
- Zdecydowanie zalecana jest przeglądarka Google Chrome.
- Początkowa nazwa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

Ustawienia czasu i języka

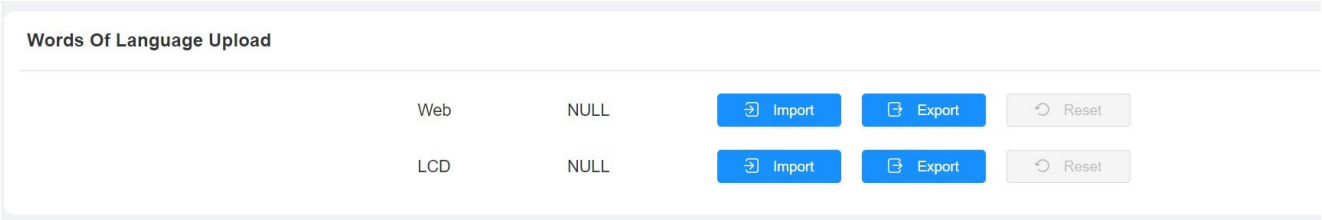
Ustawienia języka

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

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



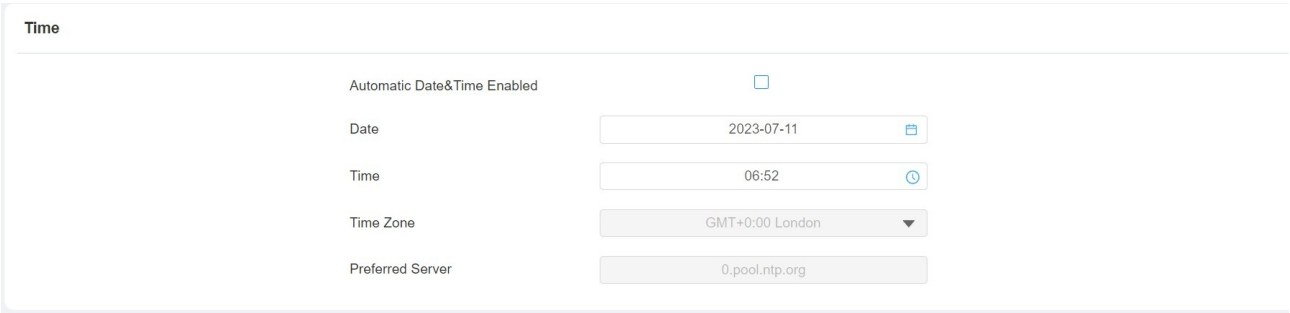
Aby dostosować nazwy konfiguracji i tekst monitu, należy wyeksportować i edytować plik .json przed przesłaniem go do urządzenia. Przejdź do **Ustawienia > Czas/Lang > Words Of Language Upload** .



Ustawienie czasu

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

Aby skonfigurować czas, przejdź do opcji **Ustawienia > Czas/język > Czas** .



Konfiguracja parametrów:

- **Automatic Date&Time Enabled** : włącz, jeśli chcesz, aby data i godzina urządzenia były automatycznie ustawiane i synchronizowane z domyślną strefą czasową i serwerem NTP (**Network Time Protocol**).
- **Primary Server**: wprowadź podstawowy serwer NTP uzyskany w **NTP Server.**

Uwaga

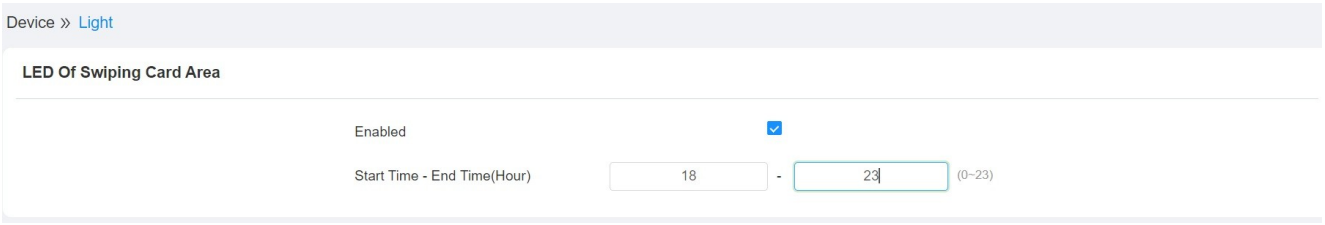
- Kiedy pole wyboru nie jest zaznaczone, parametry serwera NTP nie mogą być edytowane.

Ustawienie LED

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 czas, w którym światło LED może być wyłączone w celu zmniejszenia zużycia energii elektrycznej.

Aby skonfigurować konfigurację w interfejsie sieci Web **Device > Light > LED Of Swiping Card Area.**



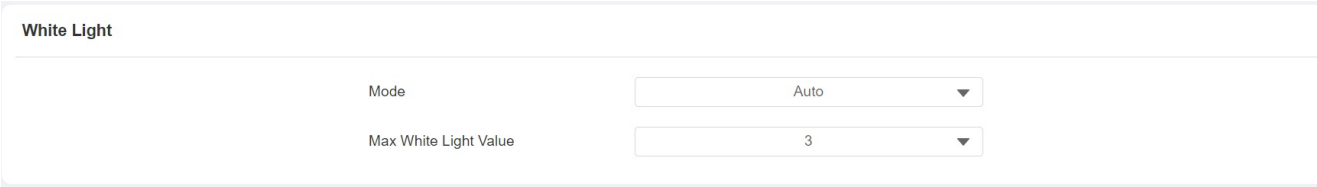
Konfiguracja parametrów:

- **Czas rozpoczęcia - czas zakończenia (H):** wprowadź zakres czasu, w którym oświetlenie LED ma obowiązywać, np. jeśli zakres czasu wynosi od **18-22** , oznacza to, że światło LED pozostanie włączone w przedziale czasowym od **18:00** do 22**:00** w ciągu jednego dnia (24 godziny).

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.

Aby skonfigurować tę funkcję, przejdź do opcji **Urządzenie > Światło >** Interfejs **światła białego.**



Konfiguracja parametrów:

- **Tryb** : po wybraniu opcji **Auto** białe światło będzie włączane automatycznie w celu rozpoznawania twarzy i skanowania kodu QR w celu otwarcia drzwi. W przypadku wybrania opcji **Off** (**Wył.)** białe światło będzie włączone automatycznie.

  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

- Światło podczerwone LED powinno zostać wyzwolone jako pierwsze, zanim białe światło będzie mogło być widoczne dla rozpoznania twarzy, jednak światło IR LED nie musi być wyzwalane dla funkcji białego światła podczas skanowania kodu QR.

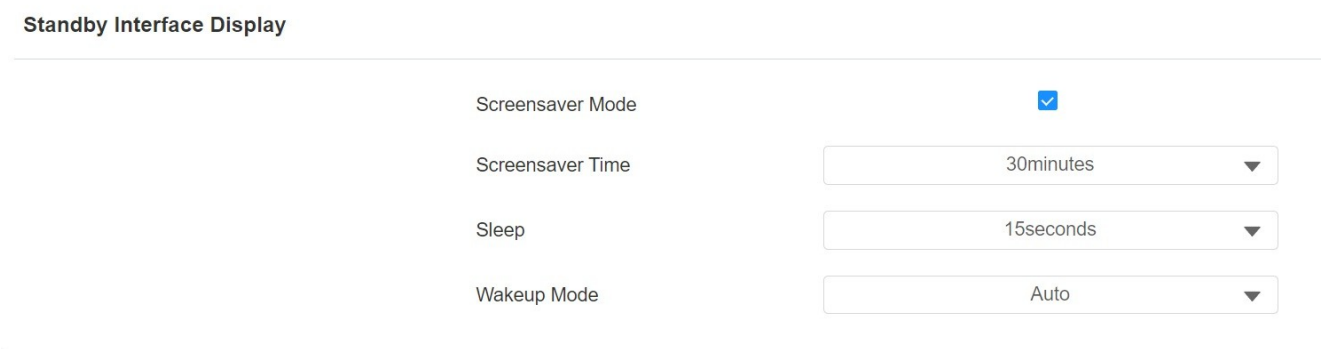
Konfiguracja ekranu

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

Konfiguracja wygaszacza ekranu

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

Aby skonfigurować konfigurację w sieci Web **Device > LCD > Standby Interface Display** interface.



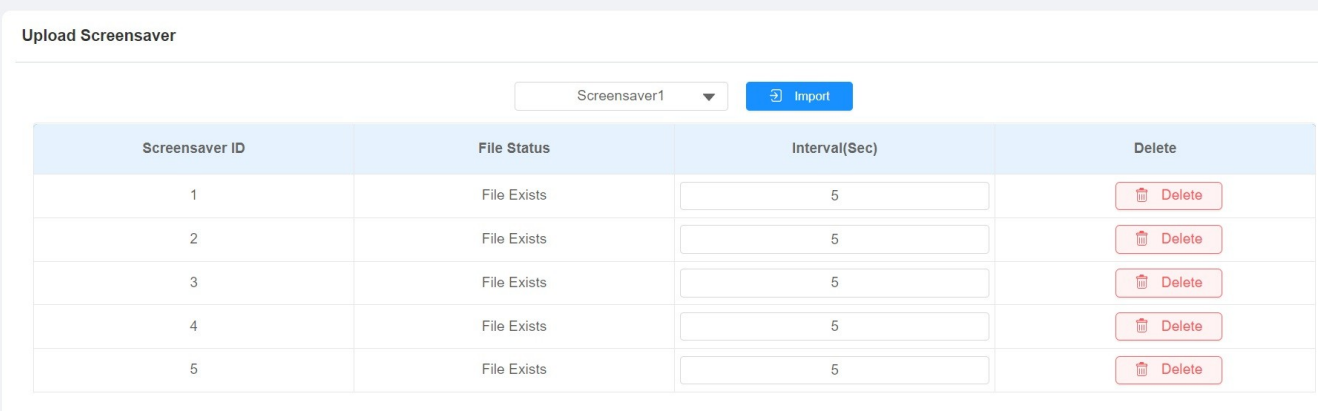
Konfiguracja parametrów:

- **Czas wygaszacza ekranu (sek.)**: ustawienie czasu rozpoczęcia wygaszacza ekranu w zakresie od 5 sekund do 2. Na przykład, jeśli ustawisz czas rozpoczęcia na 5 minut, wygaszacz ekranu uruchomi się, jeśli na urządzeniu nie będą wykonywane żadne operacje lub nikt nie zbliży się do urządzenia w ciągu pięciu minut.
- **Uśpienie** : ustawienie oczekiwanego czasu działania wygaszacza ekranu przed wyłączeniem ekranu urządzenia. Czas trwania wygaszacza ekranu można wybrać w zakresie od 2 sekund do 30 sekund.
- **Tryb wybudzania** : wybierz tryb wybudzania ekranu. Jeśli wybierzesz **tryb automatyczny**, ekran zostanie wybudzony, gdy ktoś się do niego zbliży bez dotykania go, a jeśli wybierzesz **tryb ręczny**, musisz dotknąć ekranu i go wybudzić.

Prześlij wygaszacz ekranu

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

Aby przeprowadzić konfigurację w interfejsie sieci Web **Urządzenie > LCD > Prześlij wygaszacz ekranu.**

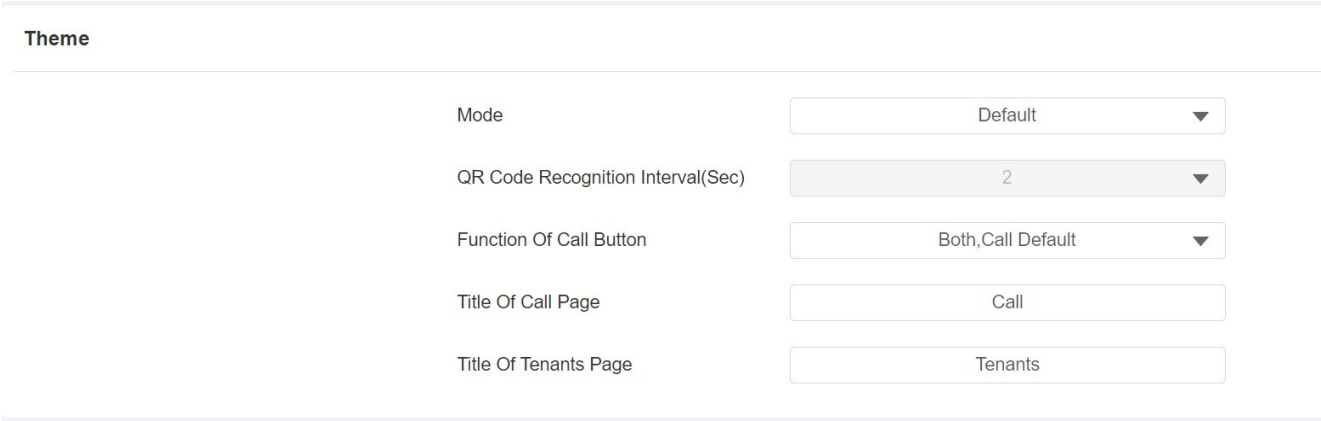


Uwaga

- Przesyłane zdjęcia powinny być w **formacie JPG** o maksymalnej rozdzielczości 2 mln pikseli.
- Poprzednie zdjęcia z określoną kolejnością ID zostaną nadpisane, gdy nastąpi powtarzające się przypisanie zdjęć do tej samej kolejności ID.

Konfiguracja trybu wyświetlania ekranu

Można wybrać dwa rodzaje trybu wyświetlania ekranu dostępu na ekranie głównym, a mianowicie tryb domyślny dla rozpoznawania twarzy i kodu QR. Aby przeprowadzić konfigurację w sieci Web, wybierz kolejno opcje **Device > LCD > Theme** interface.

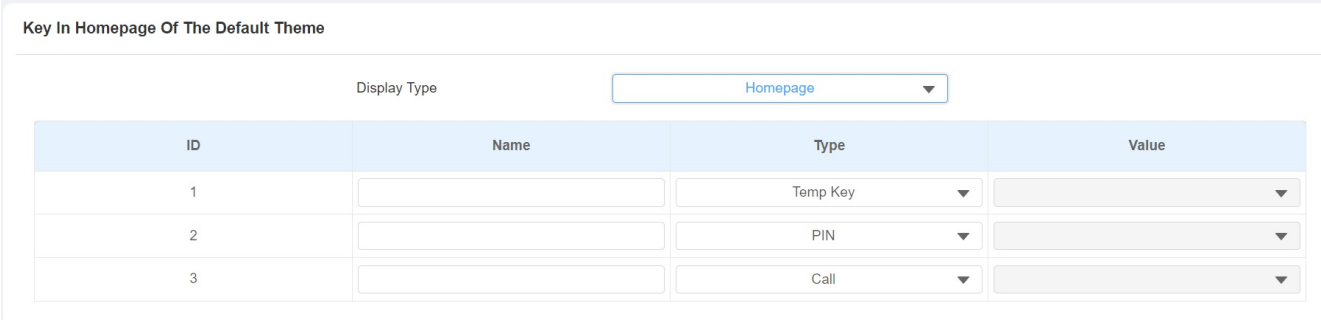


Konfiguracja parametrów:

- **Tryb:** W przypadku wybrania opcji **Kod QR**, na ekranie głównym domyślnie wyświetlany jest komunikat "Zeskanuj kod QR" przypominający o odblokowaniu za pomocą kodu QR. W przypadku wybrania opcji **Domyślny** na ekranie głównym domyślnie wyświetlany jest komunikat "Spójrz na ekran", przypominający o odblokowaniu za pomocą funkcji rozpoznawania twarzy.
- **QR Code Recognition Interval(Sec)**: ten interwał jest dostępny tylko po wybraniu trybu QR Code. Jest to rozpoznawanie odstępu czasu między dwoma kodami QR

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 Default Theme** .



Konfiguracja parametrów:

- **Typ wyświetlacza** : Wybierz jeden z pięciu typów wyświetlania: **Homepage, Call, Tenants, PIN** i **Temp Key**. W przypadku wybrania opcji Call (**Połączenie)** ekran będzie domyślnie wybudzany na stronie **Call (Połączenie).**
- **Nazwa:** wprowadź nową nazwę, aby zastąpić oryginalną nazwę typu, ale nie zmienia atrybutu typu.
- **Typ** : wybierz typ zakładki odpowiadający numerowi indeksu, który wskazuje pozycję

zakładki. Na przykład, jeśli chcesz, aby zakładka **szybkiego wybierania** była wyświetlana na pozycji pierwszej, możesz zmienić typ w indeksie numer 1 na **Szybkie wybieranie**. Można też odpowiednio zmienić inną pozycję zakładki.

- **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. Można wpisać maksymalnie pięć numerów szybkiego wybierania, a każde dwa numery muszą być oddzielone znakiem ";". Można również wybrać grupę kontaktów, z którą ma zostać nawiązane połączenie, naciskając ikonę **odbioru.**

Konfiguracja głośności i tonów

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

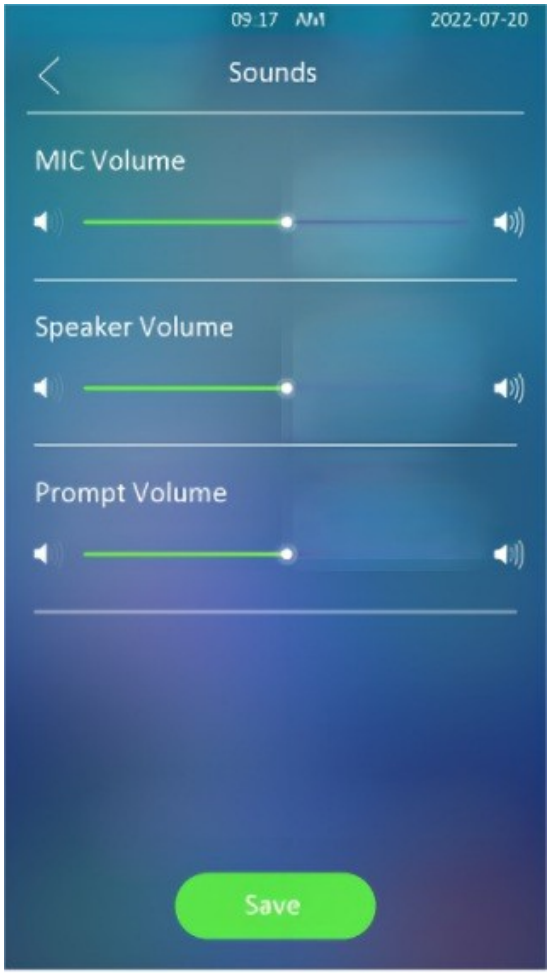
Konfiguracja głośności

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

Konfiguracja głośności na urządzeniu

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

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



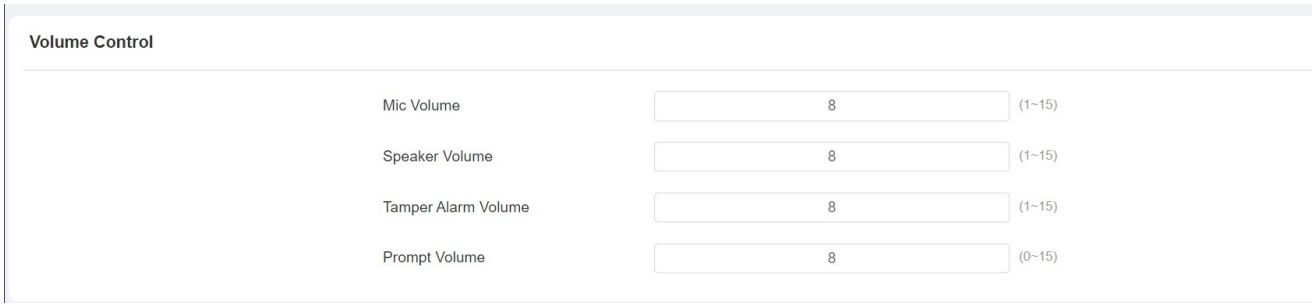
Konfiguracja parametrów:

- **Prompt Volume (Głośność komunikatów):** regulacja głośności komunikatów, w tym różnych rodzajów dźwięków informujących o powodzeniu lub niepowodzeniu otwarcia drzwi, dźwięku zwrotnego, dźwięku pomiaru temperatury itp.

Konfiguracja głośności w interfejsie internetowym

W interfejsie internetowym można ustawić głośność alarmu sabotażowego, głośność mikrofonu itp.

Ścieżka: **Urządzenie > Dźwięk > Regulacja głośności**



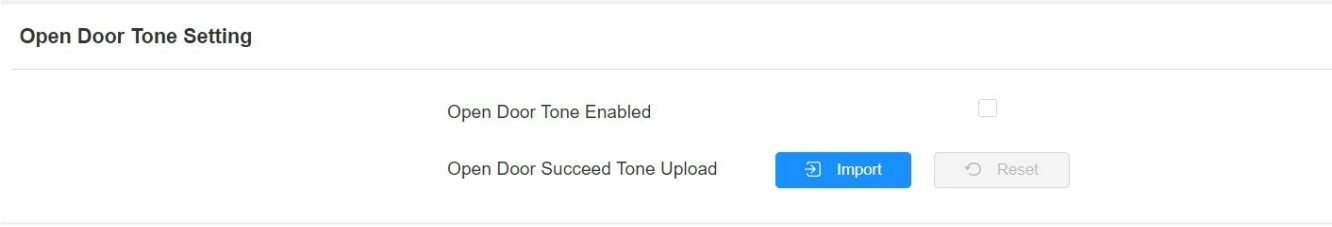
Konfiguracja parametrów:

- **Prompt Volume (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

Dźwięk informujący o niepowodzeniu i powodzeniu otwarcia drzwi można przesłać w interfejsie internetowym urządzenia. Aby skonfigurować konfigurację w sieci Web

Device > Audio > Open Door Tone Setting.



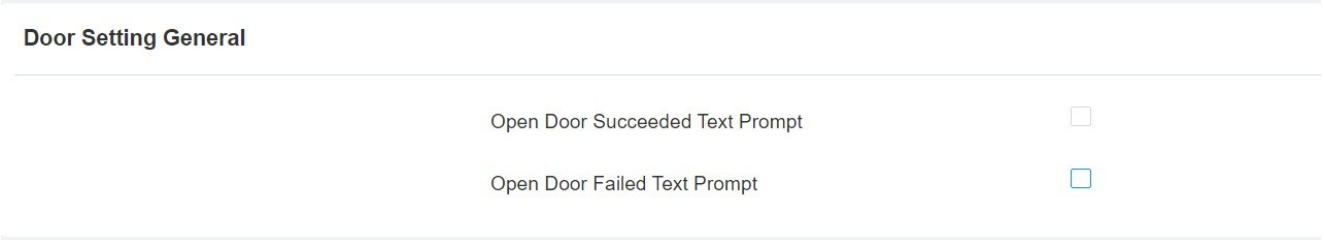
Uwaga

- Plik dźwiękowy otwartych drzwi powinien być w formacie .wav, a jego rozmiar powinien być mniejszy niż 200KB.

Konfiguracja tekstu monitu o dostęp do drzwi

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

Aby skonfigurować konfigurację w interfejsie Web **Access Control > Relay > Door Setting General.**



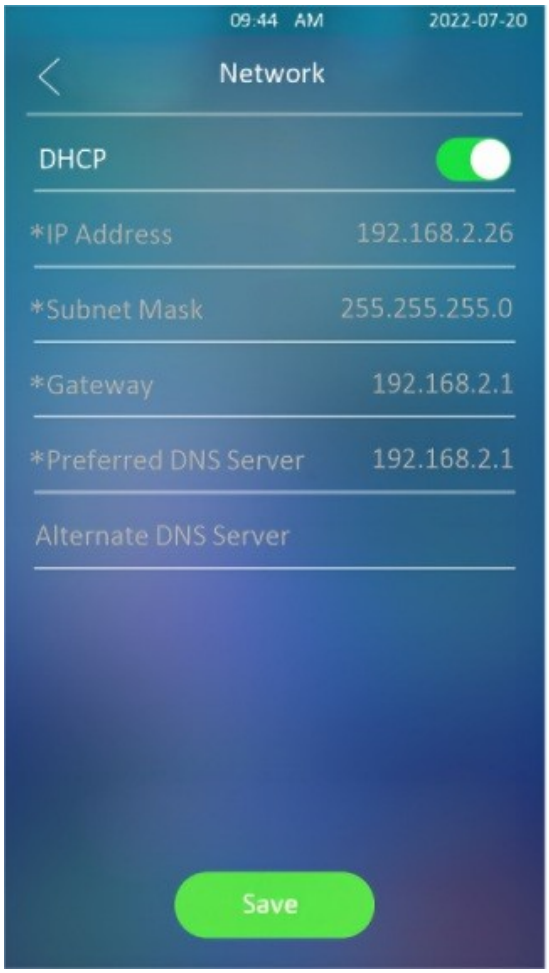
Konfiguracja parametrów:

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

Ustawienia sieciowe

Ustawienia połączenia sieciowego urządzenia

Można skonfigurować domyślny tryb DHCP (**Dynamic Host Configuration Protocol**) i statyczne połączenie IP. Ponadto można skonfigurować adres IP, maskę podsieci, bramę domyślną i serwery DNS.



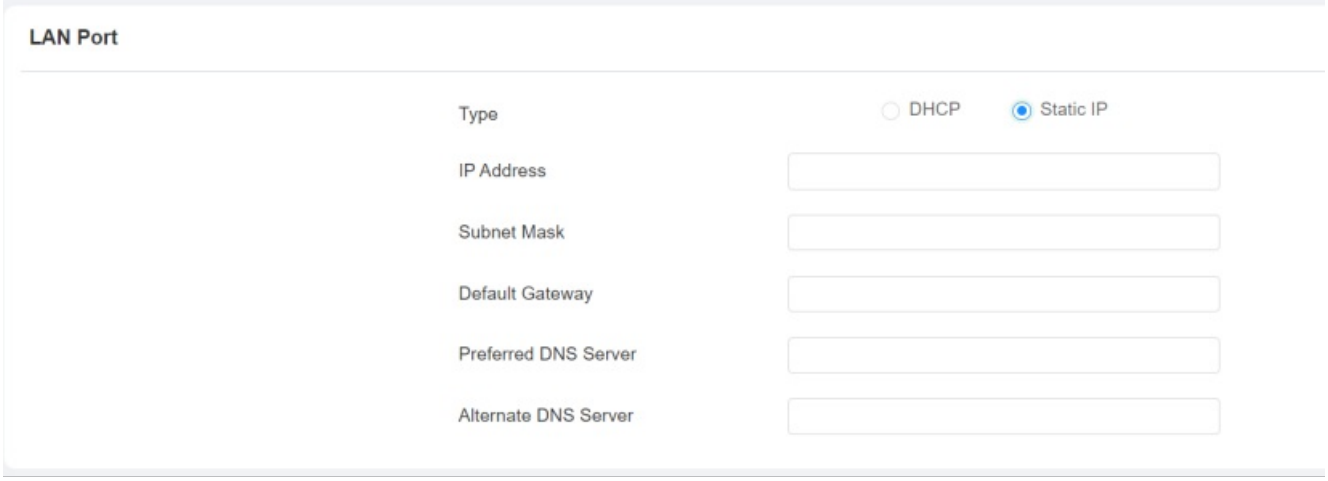
Konfiguracja parametrów :

- **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** : wybierz **tryb statycznego adresu IP**, odznaczając pole wyboru DHCP. Po wybraniu trybu statycznego IP, adres IP, maska podsieci, brama domyślna i serwer DNS

należy skonfigurować ręcznie zgodnie z rzeczywistym środowiskiem sieciowym.

- **Adres IP** : ustaw adres IP, jeśli wybrano tryb statycznego adresu IP.
- **Maska podsieci**: ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem
- sieciowym. **Brama**: ustaw prawidłową bramę domyślną zgodnie z adresem IP bramy domyślnej.
- **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.

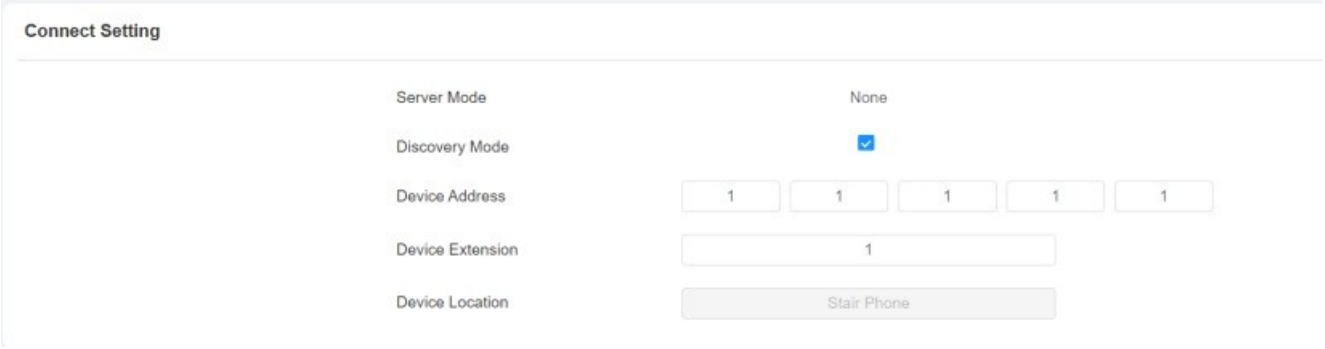
Aby skonfigurować sieć urządzenia w interfejsie internetowym, przejdź do opcji **Sieć > Podstawowe > Port LAN.**



Wdrażanie urządzeń w sieci

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

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



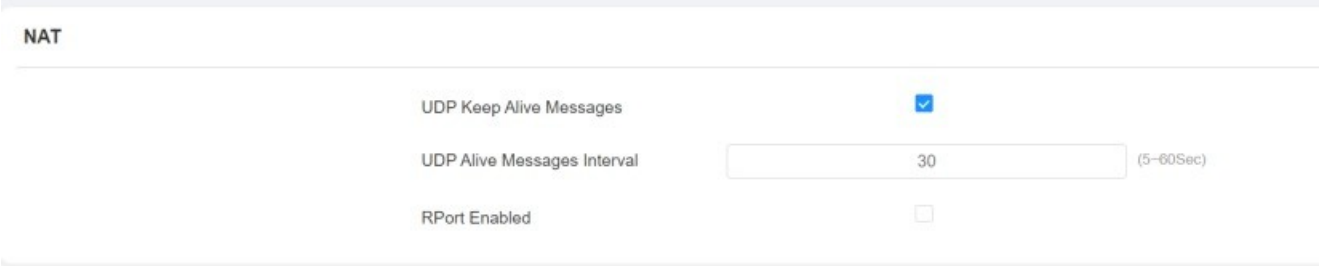
Konfiguracja parametrów:

- **Tryb** serwera: jest automatycznie konfigurowany zgodnie z rzeczywistym połączeniem
- urządzenia z określonym serwerem w sieci, takim jak **SDMC, ACMS Cloud** i **None. Brak**
- jest domyślnym ustawieniem fabrycznym wskazującym, że urządzenie nie jest w żadnym typie serwera, dlatego można wybrać Cloud, SMDC w trybie wykrywania.
  Discovery Mode (Tryb wykrywania): wybierz opcję **Enabled (Włączone)**, aby włączyć tryb wykrywania urządzenia, tak aby mogło być wykrywane przez inne urządzenia w sieci, lub wybierz opcję **Disabled (Wyłączone)**, jeśli chcesz ukryć urządzenie, aby nie było wykrywane przez inne urządzenia.
  Adres urządzenia : określ adres urządzenia, wprowadzając informacje o lokalizacji urządzenia od lewej do prawej: **Community (Wspólnota), Unit (Jednostka), Stair (Schody), Floor (Piętro), Room (Pokój)** w kolejności.
- **Device Extension**: wprowadź numer wewnętrzny zainstalowanego urządzenia. • **Device Location**: 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.

Możesz przejść do **Konto > Zaawansowane > NAT**.



Konfiguracja parametrów:

- **UDP Keep Alive Messages:** jeśli włączone, urządzenie wyśle wiadomość do serwera SIP, aby serwer SIP rozpoznał, czy 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**).

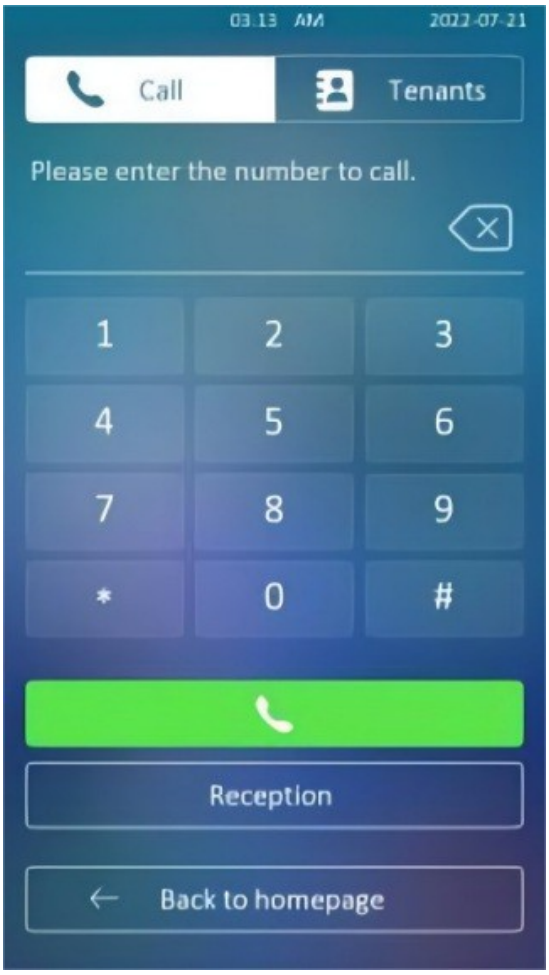
Konfiguracja połączeń interkomowych

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.

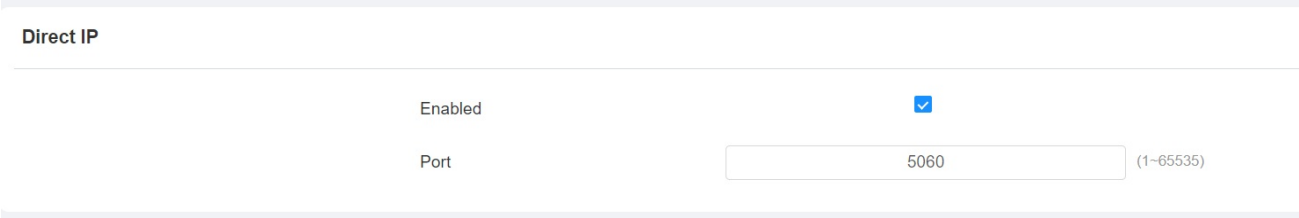
Nawiązywanie połączeń IP

Aby nawiązać bezpośrednie połączenie IP na urządzeniu, można nacisnąć ikonę Wybierz , a następnie wprowadzić numer IP lub SIP i nacisnąć ikonę , aby zadzwonić.



Konfiguracja połączeń IP

Aby skonfigurować połączenie IP na urządzeniu, przejdź do strony **Interkom > Podstawowe > Bezpośredni** interfejs **IP.**



Konfiguracja parametrów:

- **Bezpośredni port IP:** domyślny bezpośredni port IP to **5060** z zakresem portów od **1-65535**. W przypadku wprowadzenia wartości z zakresu innego niż 5060 należy sprawdzić, czy wprowadzona wartość jest zgodna z odpowiednią wartością na urządzeniu, z którym ma zostać nawiązana transmisja danych.

Konfiguracja połączeń SIP i połączeń SIP

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

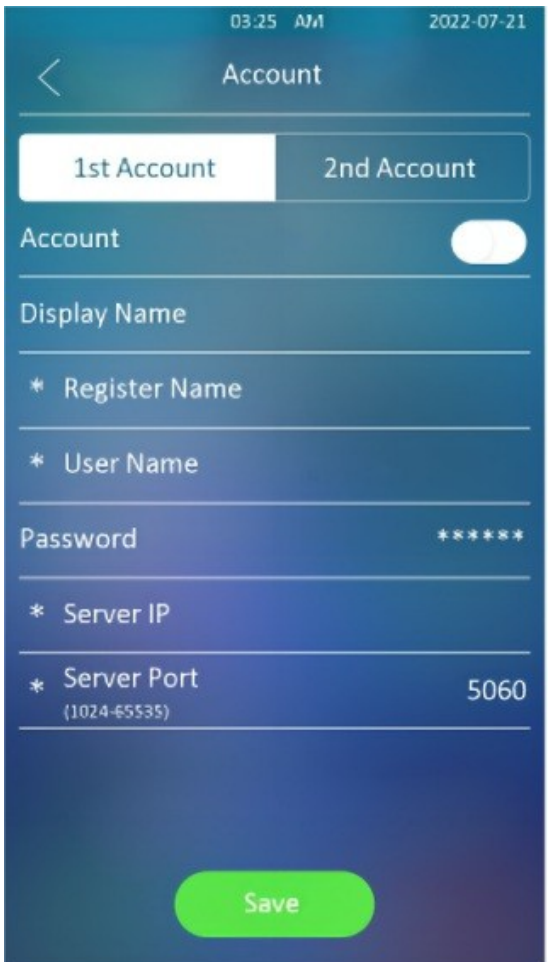
Połączenie SIP wykorzystuje protokół SIP do wysyłania i odbierania danych między urządzeniami SIP i może korzystać z Internetu lub sieci lokalnej w celu zapewnienia wysokiej jakości i bezpiecznej komunikacji. Inicjowanie połączenia SIP wymaga konta SIP, adresu SIP dla każdego urządzenia i skonfigurowania 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

Na ekranie **ustawień** urządzenia wybierz opcję **Konto**. **Nazwa rejestru, nazwa użytkownika** i **hasło są uzyskiwane** od administratora konta SIP.



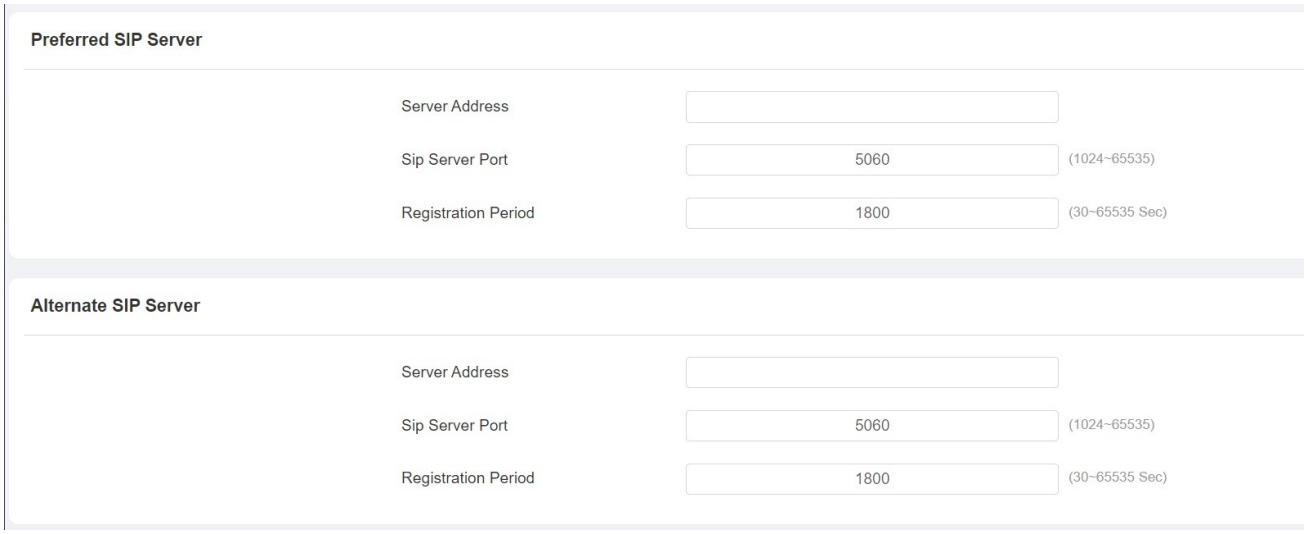
Konfiguracja parametrów:

- **Status**: sprawdza, czy konto SIP jest zarejestrowane, czy nie.
- **Display Name** : skonfiguruj nazwę, na przykład nazwę urządzenia, która będzie wyświetlana na urządzeniu, z którym nawiązywane jest połączenie.
- **Display Label**: skonfiguruj etykietę urządzenia, która będzie wyświetlana na ekranie urządzenia.

Konfiguracja serwera SIP

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

Aby skonfigurować serwer SIP, możesz przejść do **Konto > Podstawowy preferowany serwer SIP.**



Konfiguracja parametrów:

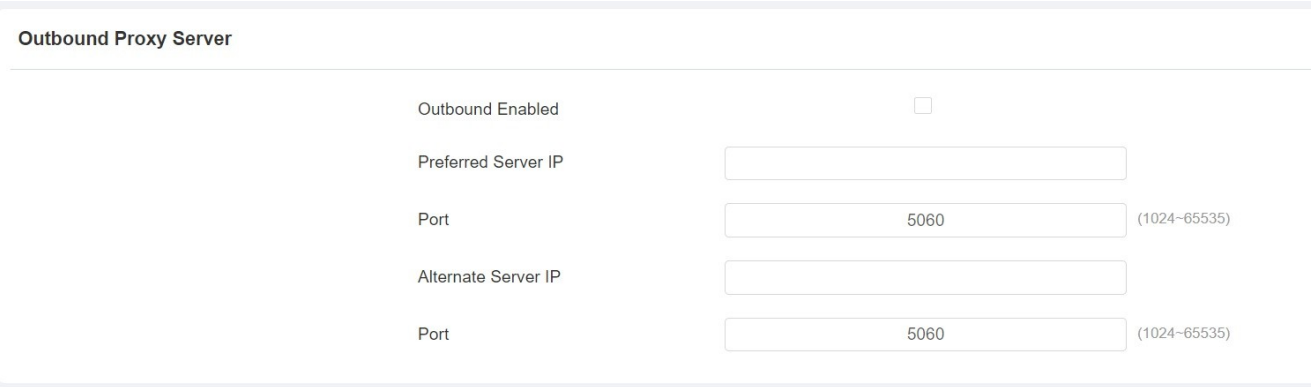
- **Preferowany serwer SIP**: wprowadź numer adresu IP serwera głównego, jego adres IP lub domenę.
- **Alternate SIP Server**: wprowadź adres IP lub domenę zapasowego serwera SIP. • **SIP Port**: ustawienie portu serwera SIP dla transmisji danych.
- **Registration Period** : ustawianie czasu rejestracji 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 serwera proxy połączeń wychodzących

Wychodzący serwer proxy służy do odbierania wszystkich inicjujących komunikatów żądań i

kierowania ich do wyznaczonego serwera SIP w celu ustanowienia sesji połączenia za pośrednictwem transmisji danych opartej na portach.

Aby skonfigurować serwer proxy, można przejść do opcji **Konto > Podstawowe > Serwer proxy** połączeń **wychodzących.**



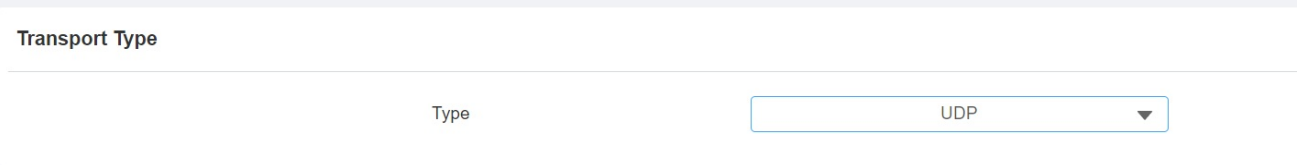
Konfiguracja parametrów:

- **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 serwera proxy połączeń wychodzących.
- **Port**: wprowadź numer portu w celu ustanowienia sesji połączenia za pośrednictwem zapasowego serwera proxy połączeń wychodzących.

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** .

Aby przeprowadzić konfigurację, można przejść do **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

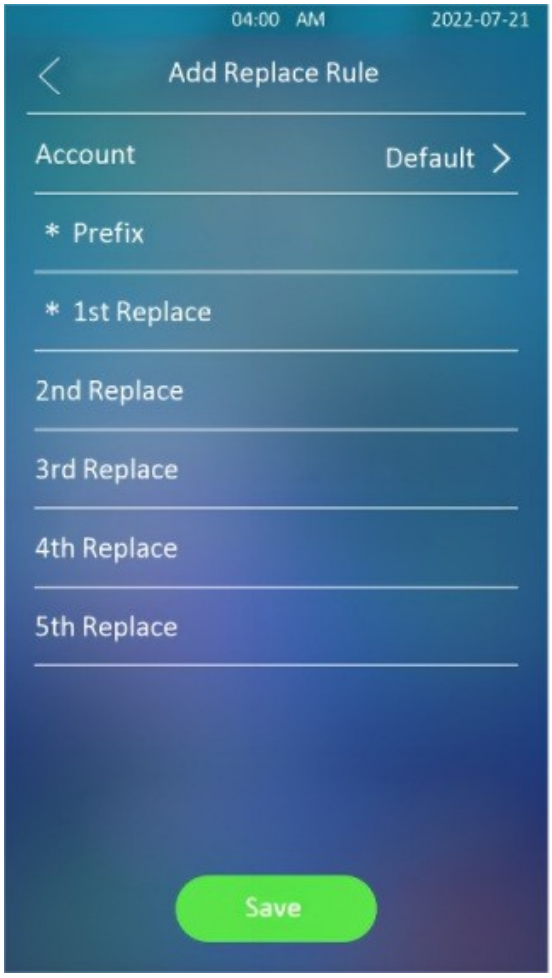
serwerów. **SRV** rejestruje nie tylko adres serwera, ale także port serwera. Ponadto SRV może być również używany do konfigurowania priorytetu i wagi adresu serwera.

Konfiguracja opcji wybierania numeru

Szybkie wybieranie według numeru na urządzeniu

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

Na ekranie **ustawień** urządzenia wybierz opcję **Zastąp regułę** , a następnie wybierz opcję **Dodaj** .



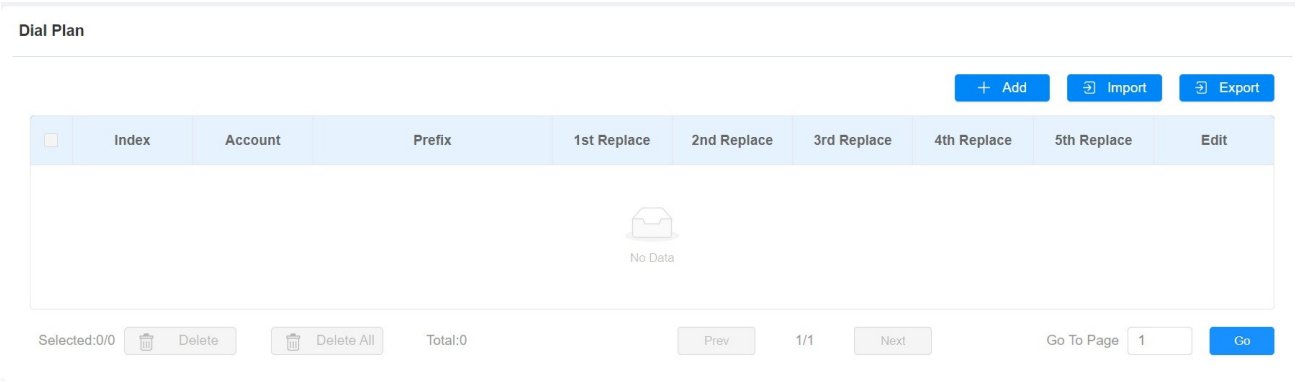
Konfiguracja parametrów:

- **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 w celu zastąpienia 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 interfejsie internetowym

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.

Aby go skonfigurować, możesz przejść do **Interkom > Plan wybierania.**

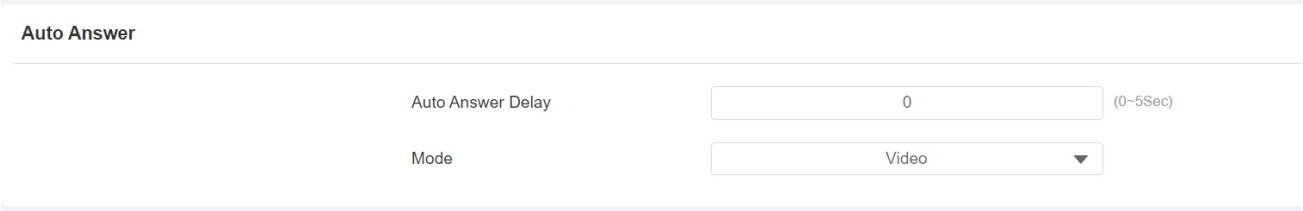


Konfiguracja automatycznej odpowiedzi

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.

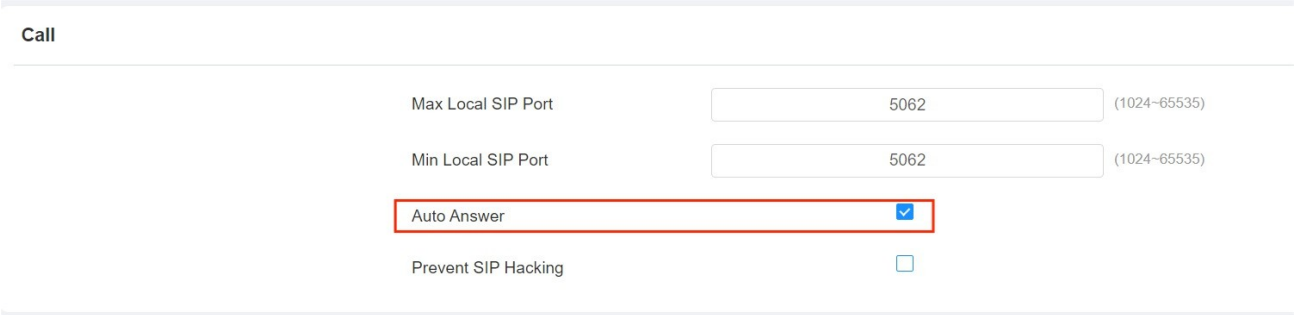
Aby skonfigurować funkcję automatycznej odpowiedzi:

Przejdź do **Interkom > Funkcja połączenia > Automatyczne odbieranie** .



Aby włączyć tryb automatycznej odpowiedzi:

Przejdź do opcji **Konto > Zaawansowane > Połącz**.



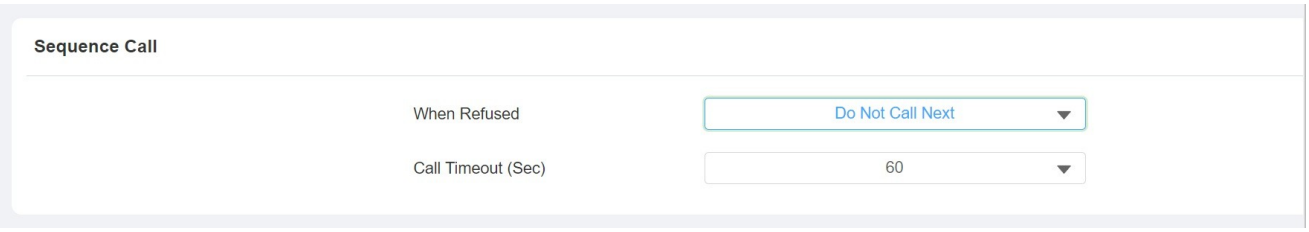
Konfiguracja parametrów:

- **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** : ustawienie preferowanego trybu **wideo** lub **audio** dla automatycznego odbierania połączeń.

Konfiguracja połączeń sekwencyjnych

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.

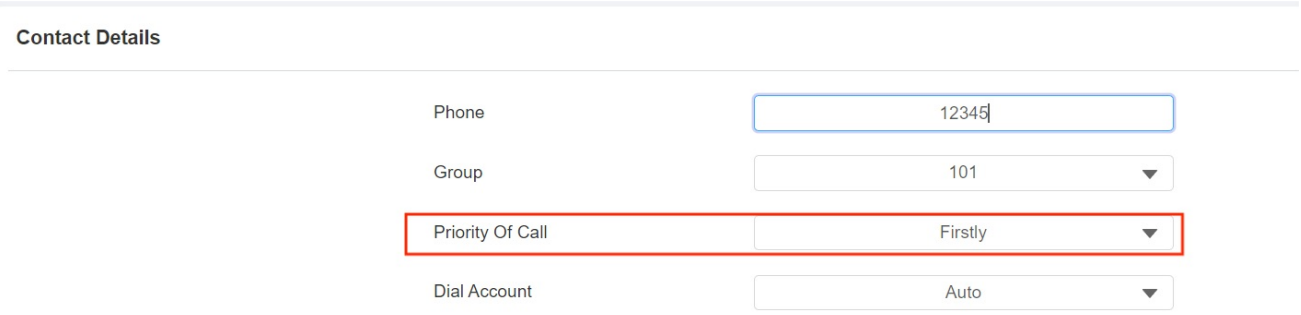
Aby przeprowadzić konfigurację w interfejsie web **Intercom > Basic > Sequence Call.**



Konfiguracja parametrów:

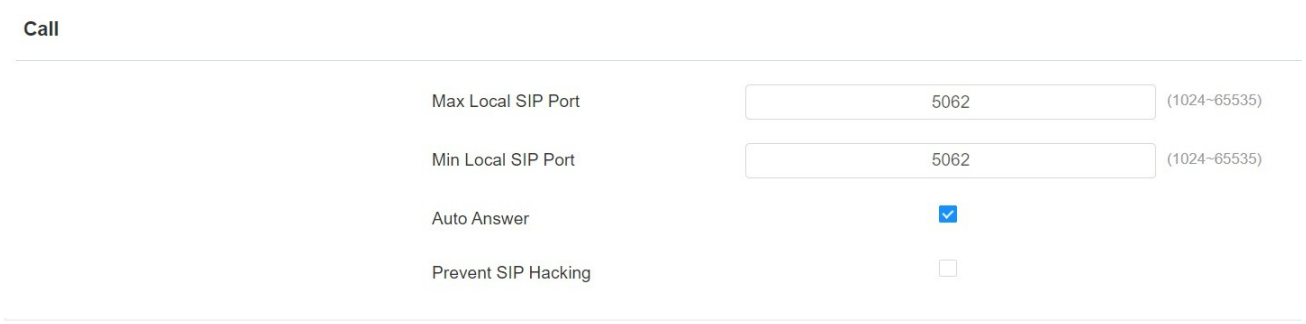
- **Gdy odrzucono**: Wybierz opcję **Nie dzwoń dalej,** gdy połączenie zostanie odrzucone, połączenie zostanie przerwane. Wybierz **Call Next**, połączenie zostanie przeniesione do następnego.
- **Timeout(Sec)**: aby sprawdzić interwał czasowy między kolejnymi numerami połączeń w docelowej grupie połączeń sekwencyjnych. Na przykład, jeśli ustawisz interwał czasowy na 10 sekund, połączenie (jeśli nie zostanie odebrane w ciągu 10 sekund) zostanie automatycznie zakończone i przeniesione sekwencyjnie do następnego numeru połączenia sekwencyjnego w docelowej grupie połączeń sekwencyjnych.

Aby określić kolejność połączeń, przejdź do opcji **Katalog > Użytkownik > Dodaj/Edytuj użytkownika > Dane kontaktowe** .



Włączenie funkcji zapobiegania włamaniom SIP

Podsłuch telefonu internetowego to atak sieciowy, który umożliwia nieautoryzowanym stronom przechwytywanie i uzyskiwanie dostępu do treści sesji komunikacyjnych między użytkownikami interkomu. Może to narazić atakujących na ujawnienie wrażliwych i poufnych informacji. Ochrona przed włamaniami SIP to technika, która zabezpiecza połączenia SIP przed naruszeniem w Internecie.



Uwaga

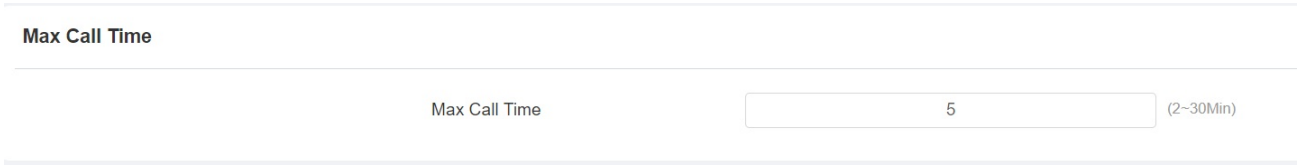
Bezpośrednie połączenia IP zostaną zablokowane, jeśli bezpośredni adres IP jest wyłączony.

Ustawienia połączeń

Ustawienie maksymalnego czasu trwania połączenia

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

Aby przeprowadzić konfigurację, możesz przejść do **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.

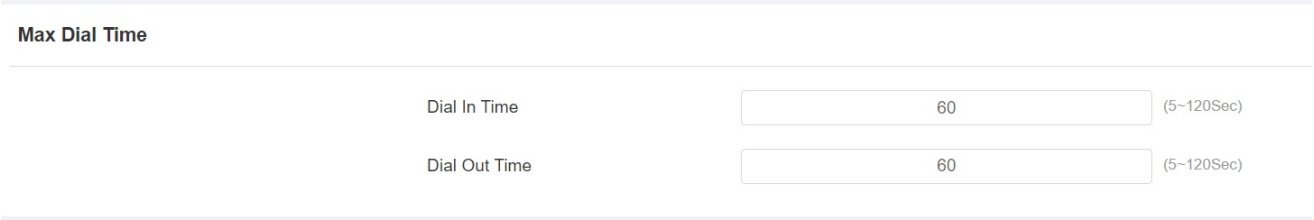
Uwaga

Maksymalny czas połączenia urządzenia jest również powiązany z maksymalnym czasem połączenia SIP. Jeśli używasz
SIP w celu nawiązania połączenia, należy zwrócić uwagę na maksymalny czas połączenia serwera SIP. Jeśli maksymalny czas połączenia serwera SIP jest krótszy niż maksymalny czas połączenia urządzenia, zastosowany zostanie maksymalny czas połączenia serwera SIP.

Ustawienie maksymalnego czasu wybierania numeru

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

Aby przeprowadzić konfigurację, możesz przejść do **Intercom > Call Feature > Max Dial Time.**



Konfiguracja parametrów:

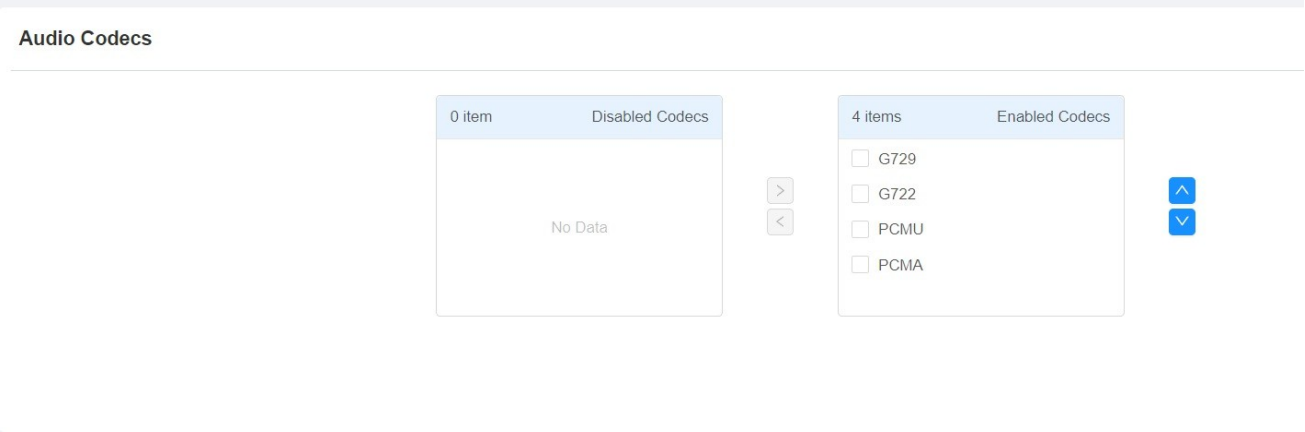
- **Dial In Time (Czas wybierania)**: wprowadź czas wybierania dla bramofonu (**w zakresie 5-120 sekund**). Na przykład, jeśli w bramofonie zostanie ustawiony czas wybierania 60 sekund, bramofon automatycznie rozłączy połączenie przychodzące, jeśli nie zostanie ono odebrane przez bramofon w ciągu 60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

Konfiguracja kodeka audio i wideo dla połączeń SIP

Konfiguracja kodeka audio

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

Aby przeprowadzić konfigurację, możesz przejść do **Konto > Zaawansowane > Kodeki audio** .



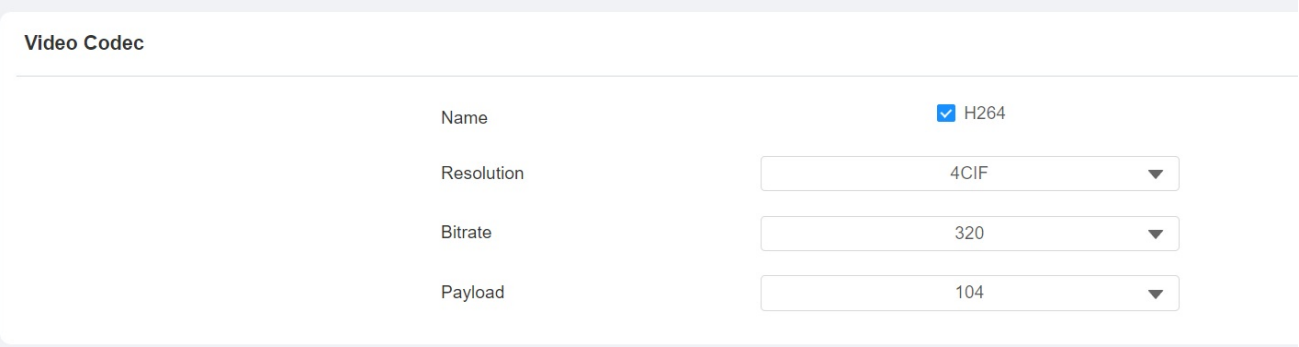
Poniżej znajdują się informacje na temat zużycia pasma i częstotliwości próbkowania dla czterech typów kodeków:

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

Konfiguracja kodeka wideo

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

Aby przeprowadzić konfigurację, można przejść do **Konto > Zaawansowane > Kodek wideo** .



Konfiguracja parametrów:

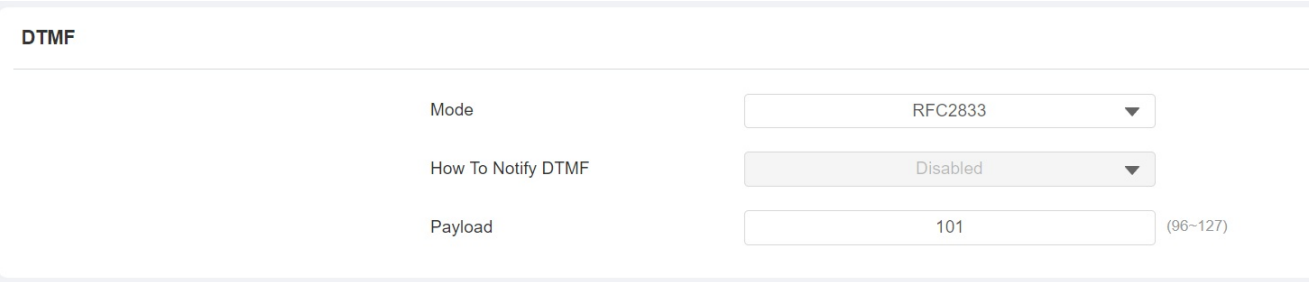
- **Nazwa:** zaznacz, aby wybrać format kodeka wideo H264 dla wideo z bramofonu. Domyślnym kodekiem wideo jest H264.
- **Rozdzielczość:** wybierz rozdzielczość kodu dla jakości wideo spośród czterech opcji: **QCIF, CIF, VGA, 4CIF i 720P** zgodnie z rzeczywistym środowiskiem sieciowym. Domyślną rozdzielczością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

- **Bitrate:** wybór szybkości transmisji strumienia wideo (w zakresie 320-2048). Im większa szybkość transmisji bitów, tym większa ilość danych przesyłanych w każdej sekundzie, dzięki czemu obraz wideo będzie wyraźniejszy. Domyślna szybkość transmisji kodu wynosi 2048.
- **Payload (Ładunek):** wybierz typ ładunku (w zakresie 90-118), 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.

Aby skonfigurować transmisję danych DTMF, można przejść do **Konto > Zaawansowane > DTMF**.



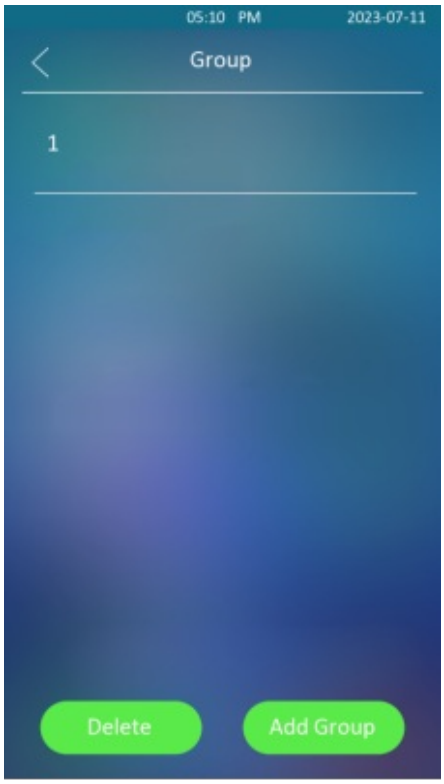
Konfiguracja parametrów:

- **Tryb:** wybór trybu DTMF spośród sześciu opcji: **Info, Inband, RFC 2833, 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.
- **Sposób powiadamiania DTMF:** wybierz jeden z czterech typów: **Disable, DTMF, DTMF-Relay** i **Telephone-Event** zgodnie z konkretnym typem przyjętym przez urządzenie innej firmy. Konfiguracja jest wymagana tylko wtedy, gdy urządzenie innej firmy, z którym ma zostać nawiązane połączenie, przyjmuje tryb **Info.**
  Payload: ustaw ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą a odbiorcą podczas transmisji danych.

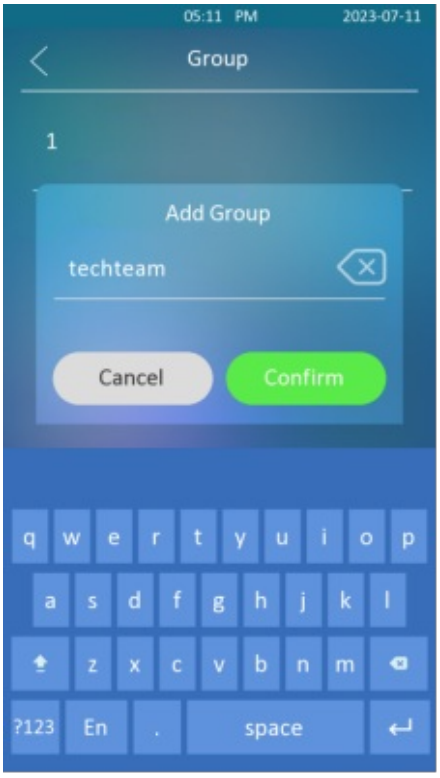
Konfiguracja listy kontaktów

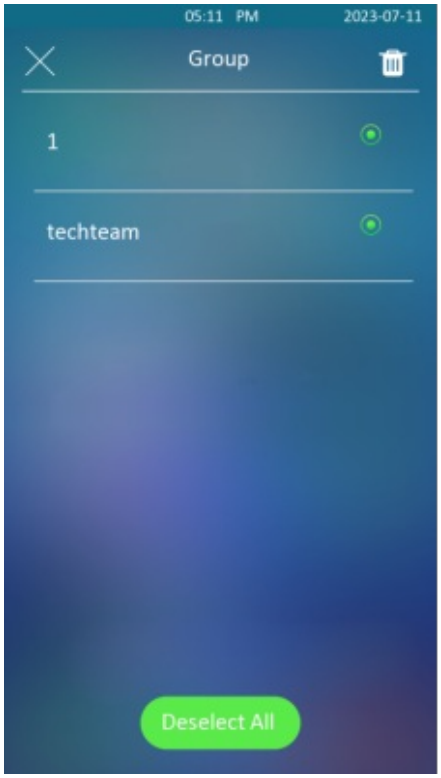
Konfiguracja listy kontaktów na urządzeniu

Listę kontaktów można skonfigurować pod kątem dodawania i modyfikowania grup kontaktów lub kontaktów bezpośrednio na urządzeniu. Aby skonfigurować książkę telefoniczną na urządzeniu **Użytkownik > Grupa.**



Konfiguracja listy kontaktów w interfejsie internetowym

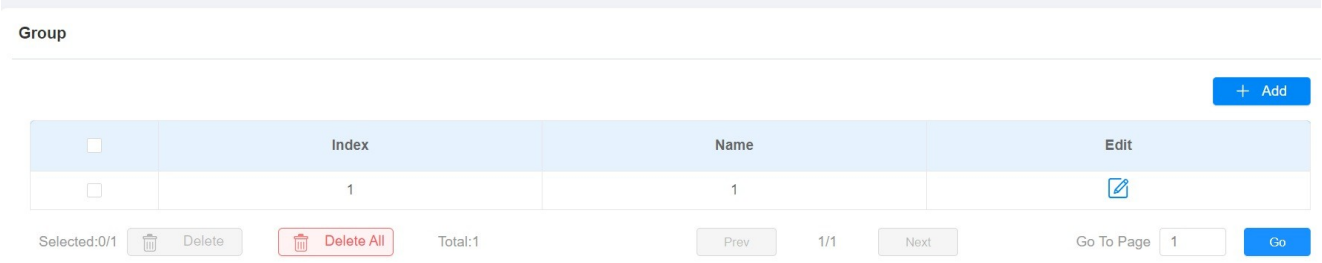




Zarządzanie grupami kontaktów w interfejsie internetowym

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

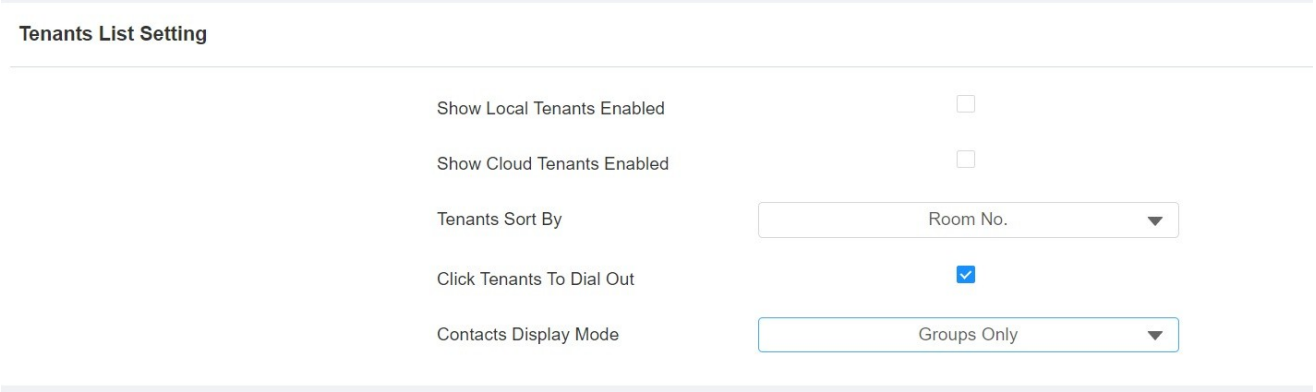
Ścieżka: **Katalog > Użytkownik > Grupa**



Zarządzanie ustawieniami 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 Ustawienie.**



Konfiguracja parametrów:

- **Show Tenants of Local Group Enabled** : zaznacz lub odznacz pole wyboru, aby kontrolować wyświetlanie etykiety grupy. Jeśli pole wyboru zostanie odznaczone, 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 dzierżawcy chmury zostaną ukryci.
- **Najemcy Sortuj według**: wybierz **Kod ASCII, Nr pokoju** lub **Importuj**. Po wybraniu opcji Kod ASC **I** najemcy zostaną wyświetleni według nazwisk w kolejności kodu ASC **I. Po** wybraniu opcji Room No. najemcy zostaną posortowani według numerów pokoi. Dotyczy to zarówno kontaktów lokalnych, jak i zsynchronizowanych z chmurą SmartPlus.

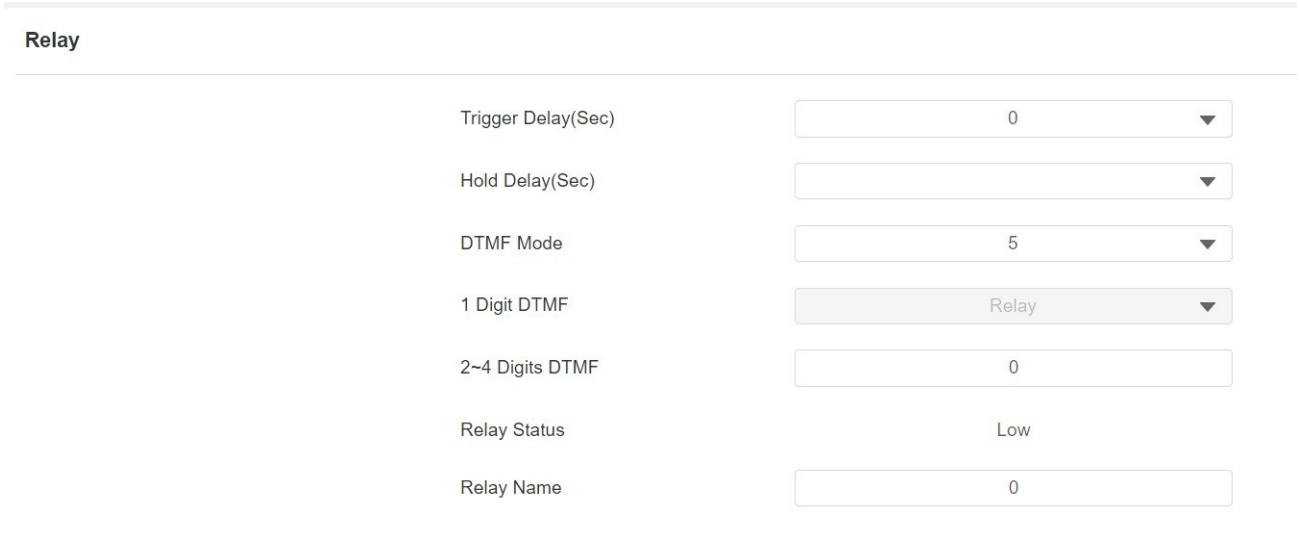
- **Kliknij Tenants to Dial Out**: zaznacz pole wyboru, aby włączyć funkcję wybierania numeru przez naciśnięcie karty kontaktu. Gdy ta funkcja jest włączona, można nacisnąć dowolne miejsce na karcie kontaktu, aby wybrać numer. Ta funkcja zostanie wyłączona po odznaczeniu pola wyboru, a gdy jest wyłączona, należy nacisnąć ikonę połączenia na środku karty, aby się połączyć.
- **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. Podczas nawiązywania połączenia wyświetlana jest nazwa grupy.

Ustawienie przekaźnika

Ustawienie przełącznika przekaźnika

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

> Przekaźnik > Interfejs **przekaźnika.**



Konfiguracja parametrów:

- **Trigger Delay (Sec)**: ustawienie 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 **Odblokuj.**
- **Hold Delay (Sec)**: ustaw czas opóźnienia zatrzymania przekaźnika (w zakresie od 1 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia podtrzymania na 5 sekund, przekaźnik pozostanie wyzwolony przez 5 sekund po otwarciu drzwi, co oznacza, że drzwi pozostaną otwarte przez 5 sekund.
- **Tryb DTMF**: wybór liczby cyfr DTMF dla kontroli dostępu do drzwi **(w zakresie od 1 do 4 cyfr**). Można na przykład wybrać 1-cyfrowy kod DTMF lub 2-cyfrowy kod DTMF itp. w zależności od potrzeb.
- **1 Digit DTMF:** ustawienie 1-cyfrowego kodu DTMF z zakresu (**0-9 i *, #**).

- **2~4 cyfry DTMF**: ustaw kod DTMF zgodnie z **opcją DMTP**. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli tryb DTMP jest ustawiony jako 3-cyfrowy.
- **Status przekaźnika:** status przekaźnika jest domyślnie niski, co oznacza stan normalnie zamknięty (NC). Jeśli stan przekaźnika jest wysoki, oznacza to, że jest on normalnie otwarty (NO).
- **Relay Name (Nazwa przekaźnika): nadaj** nazwę przełącznikowi przekaźnika zgodnie z potrzebami. Dla wygody można na przykład nazwać przełącznik przekaźnika zgodnie z jego lokalizacją.

Uwa

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

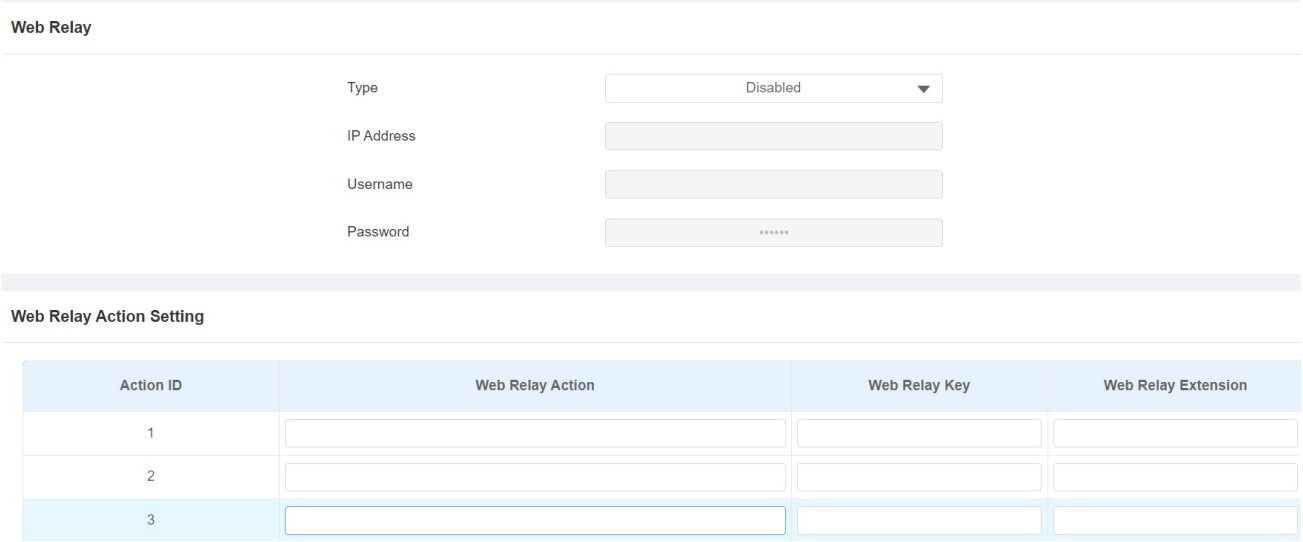
Ustawienia przekaźnika internetowego

Przekaźnik sieciowy ma wbudowany serwer sieciowy i może być sterowany przez Internet lub sieć lokalną. 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 sieciowym, w którym należy podać takie informacje, jak adres IP przekaźnika, hasło, działanie przekaźnika sieciowego itp. Przed

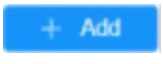
uzyskaniem dostępu do drzwi za pośrednictwem przekaźnika internetowego.
Ścieżka: **Access Control > Web Relay.** Adres IP, nazwa użytkownika i hasło są dostarczane przez producenta przekaźnika internetowego.



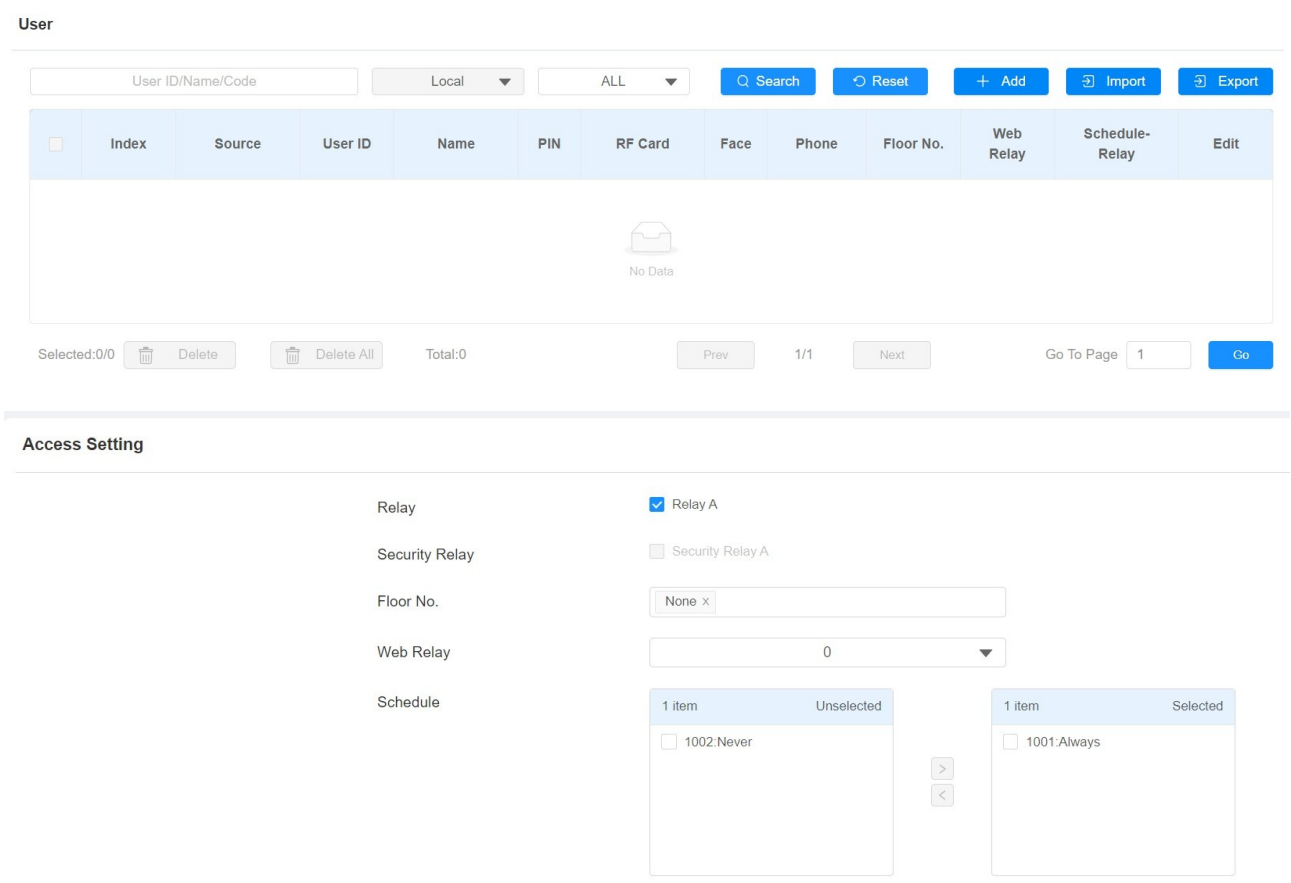
Konfiguracja parametrów :

- **Typ** : spośród trzech opcji: **Disabled (Wyłączone), Web Relay (Przekaźnik sieciowy) i Both (Oba).** Wybierz **Przekaźnik sieciowy**, aby włączyć przekaźnik sieciowy. Wybierz **Disable,** aby wyłączyć przekaźnik sieciowy. Wybierz **Both,** aby włączyć zarówno przekaźnik lokalny, jak i internetowy. Jeśli wybierzesz **Web Relay**, lokalny przekaźnik nie będzie ważny.
- **Hasło** : Hasła są uwierzytelniane przez HTTP i można je zdefiniować za pomocą **akcji http get.**
- **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.

Po skonfigurowaniu przekaźnika sieciowego można wybrać określone działanie przekaźnika sieciowego, które ma zostać wykonane.

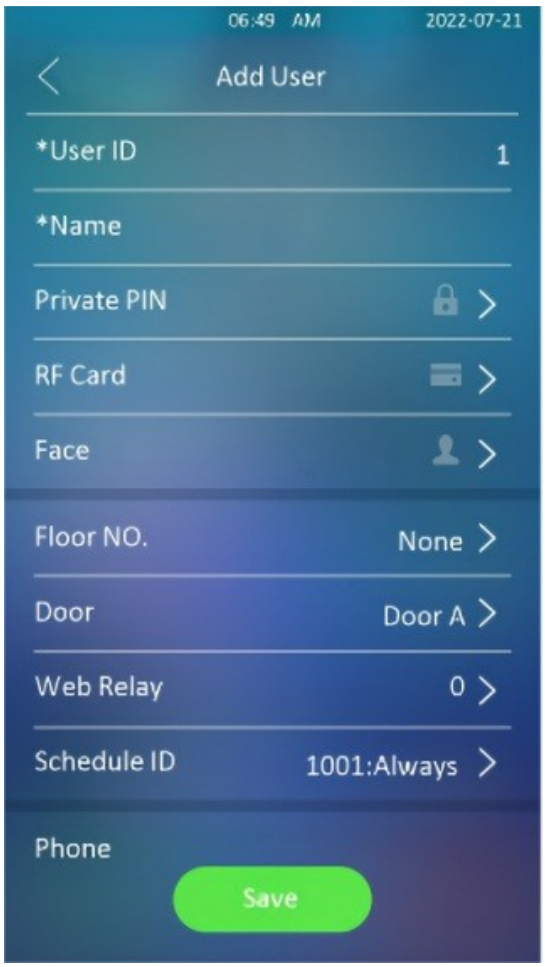
Możesz przejść do opcji **Katalog > Użytkownik**, a następnie kliknąć 

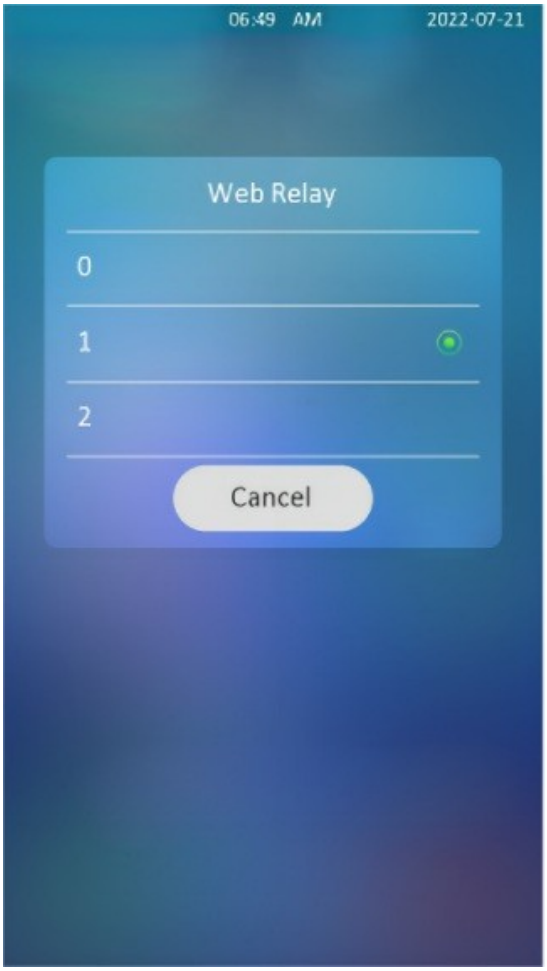
i przewinąć w dół do opcji **Ustawienia dostępu** .



Konfiguracja funkcji Web Relay na urządzeniu

Po wprowadzeniu działań przekaźnika internetowego w interfejsie internetowym można teraz wybrać określoną liczbę działań przekaźnika internetowego, które mają być wykonywane dla określonego mieszkańca dodanego w celu odblokowania drzwi. Aby to skonfigurować, przejdź do **User > User List (Użytkownik > Lista użytkowników)**.

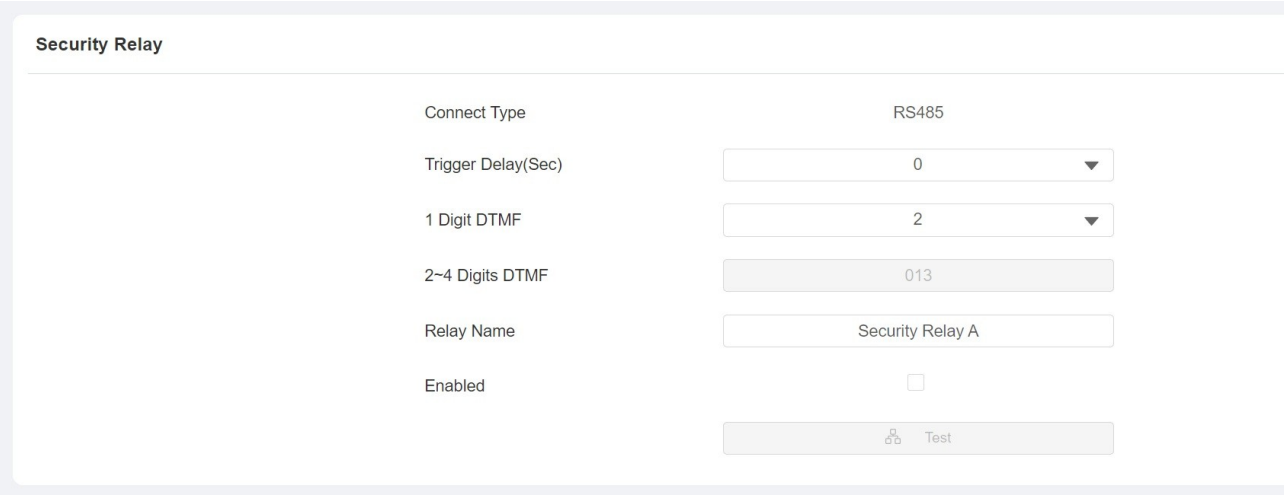




Przekaźnik bezpieczeństwa

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

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



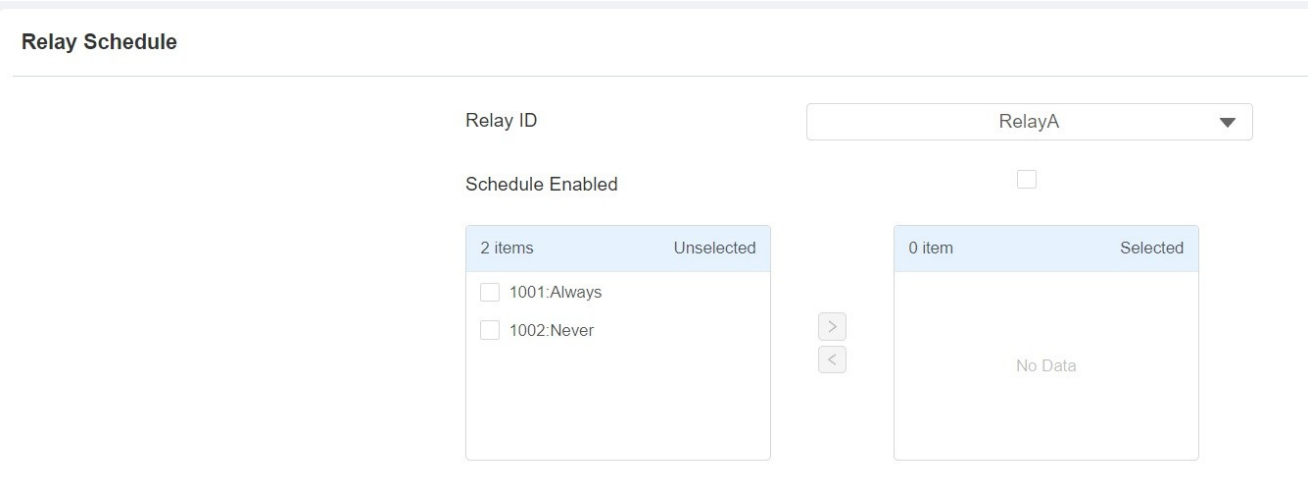
Konfiguracja parametrów:

- **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 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.

Harmonogram przekaźników

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

Aby przeprowadzić konfigurację, przejdź do interfejsu **Access Control > Relay > Relay Schedule.**



Konfiguracja parametrów:

- **Identyfikator przekaźnika**: wybierz przekaźnik, który chcesz skonfigurować.
- **Harmonogram włączony**: domyślnie jest wyłączony. Aby ją włączyć, wystarczy wybrać harmonogram.

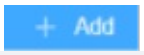
Uwaga

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

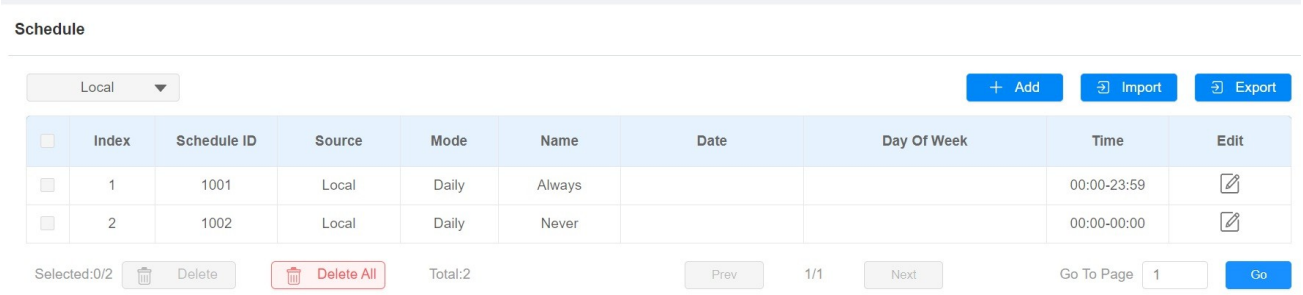
Zarządzanie harmonogramem dostępu do drzwi

Konfiguracja harmonogramu dostępu do drzwi

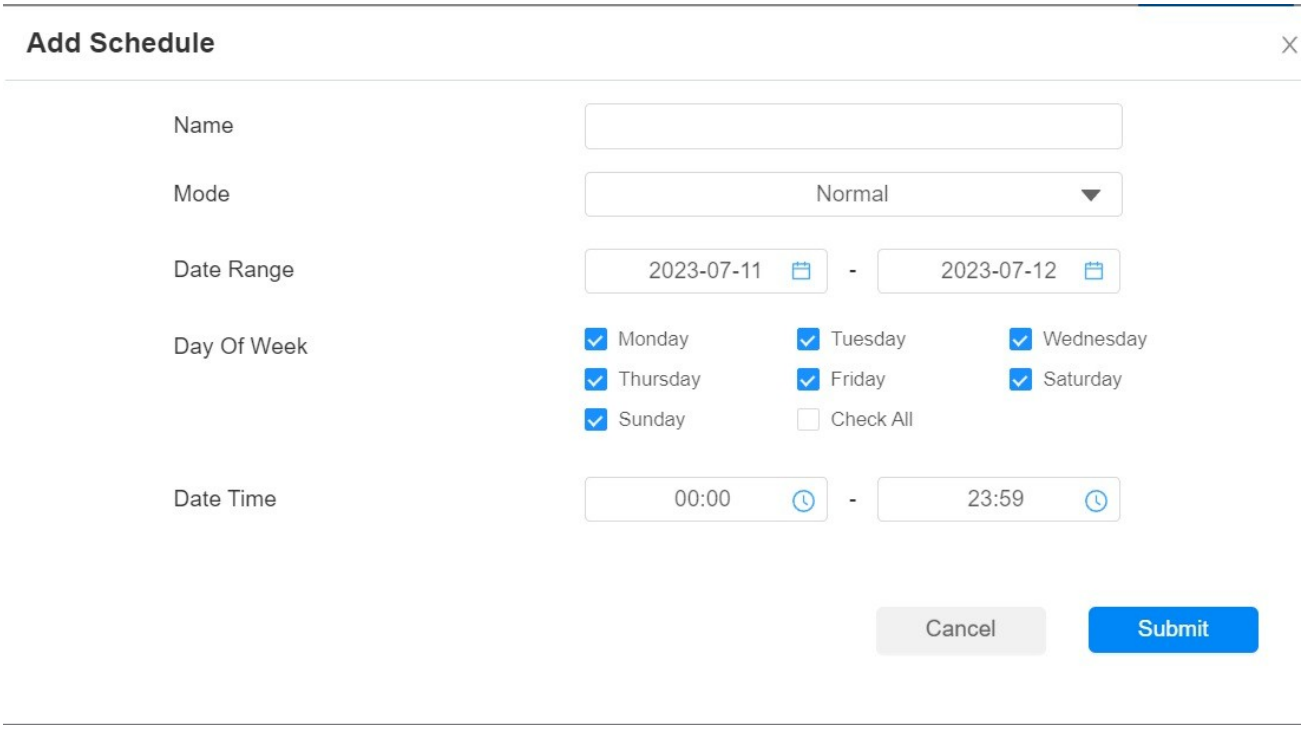
Harmonogram dostępu do drzwi pozwala zdecydować, kto i kiedy może otworzyć drzwi. Dotyczy to zarówno pojedynczych osób, jak i grup, zapewniając, że użytkownicy w ramach harmonogramu mogą otwierać drzwi przy użyciu autoryzowanej metody tylko w wyznaczonych okresach czasu.

Aby skonfigurować harmonogram, przejdź do opcji **Ustawienia** 

.



Aby utworzyć harmonogram dzienny, wybierz tryb **dzienny.**

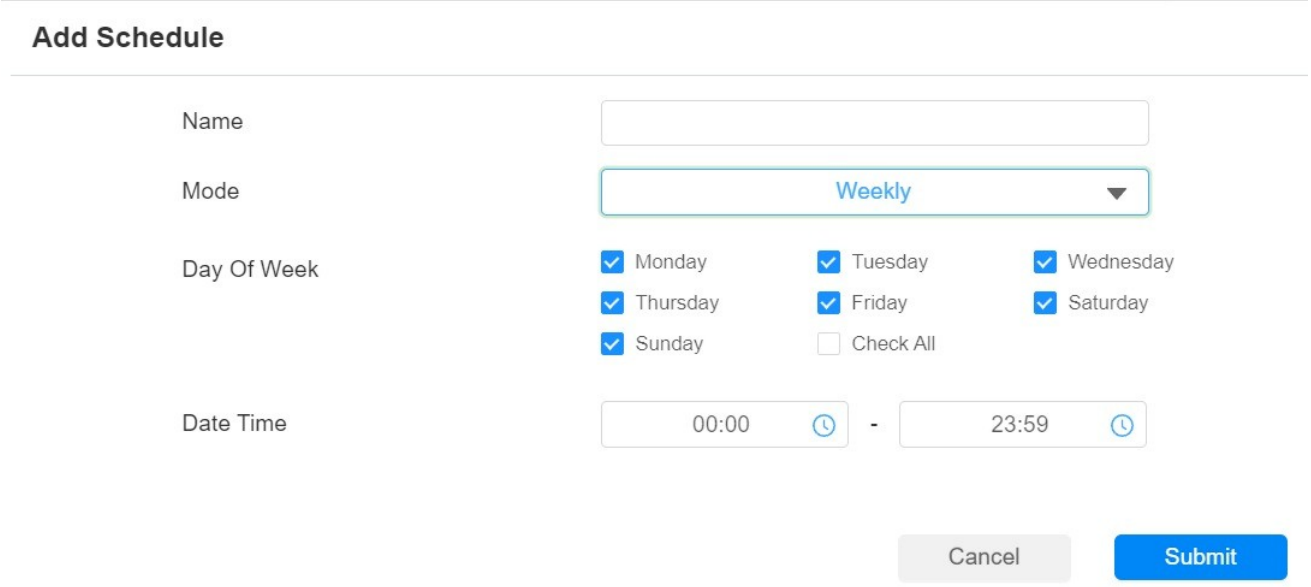


Konfiguracja parametrów :

- **Tryb** : wybór harmonogramu dziennego.

- **Nazwa**: wprowadź nazwę harmonogramu dziennego.
- **Date Time (Data i godzina)**: ustawienie harmonogramu ważności dostępu do drzwi w ciągu dnia.

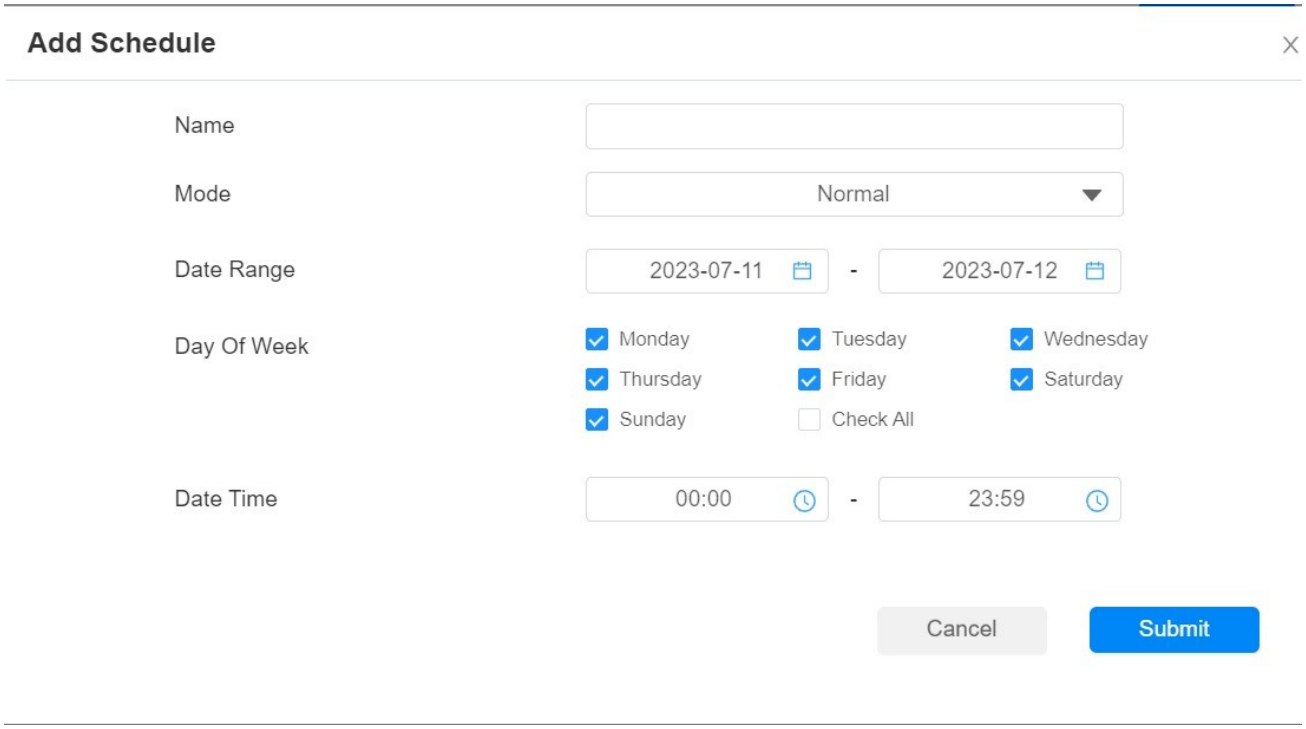
Aby utworzyć harmonogram dzienny, wybierz tryb **tygodniowy.**



Konfiguracja parametrów:

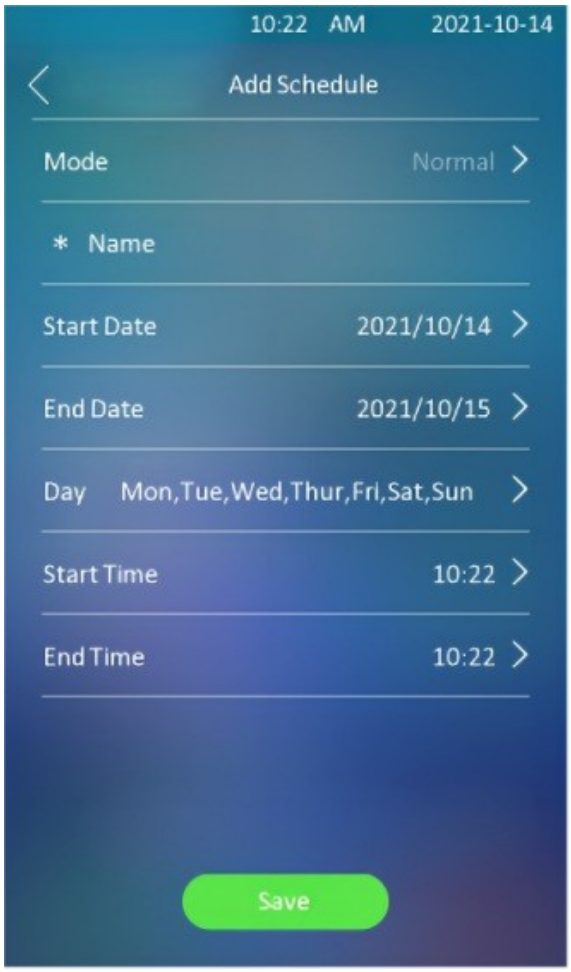
- **Dzień tygodnia**: wybierz dzień (dni), w których dostęp do drzwi może być ważny co tydzień.

Aby utworzyć harmonogram na dłuższy okres:



Tworzenie harmonogramu dostępu do drzwi na urządzeniu

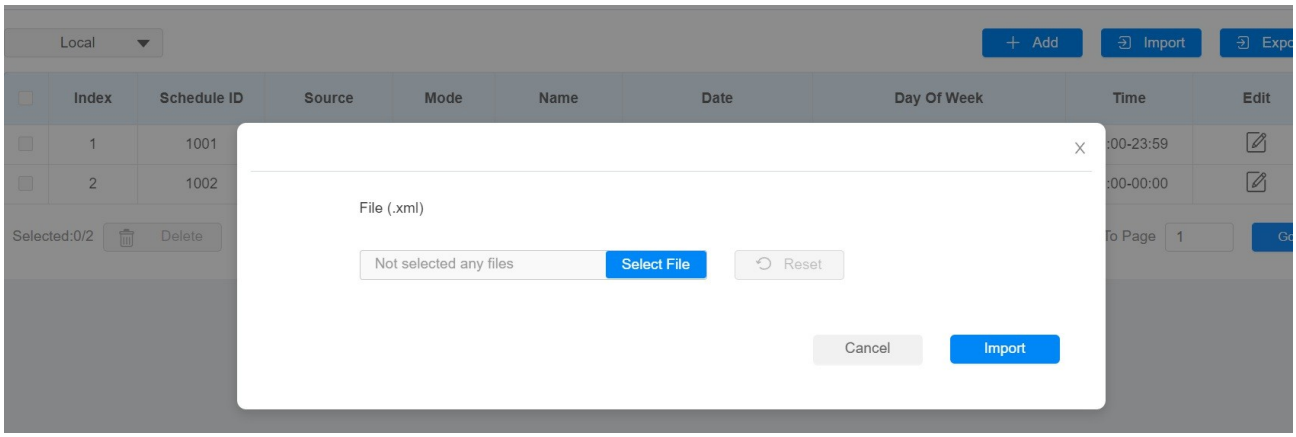
Na urządzeniu można również utworzyć harmonogram dostępu do drzwi. W tym celu należy przejść do opcji **Harmonogram > Dodaj harmonogram** .



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.

Możesz przejść do **Ustawienia > Harmonogram** , a następnie kliknąć **Importuj**.



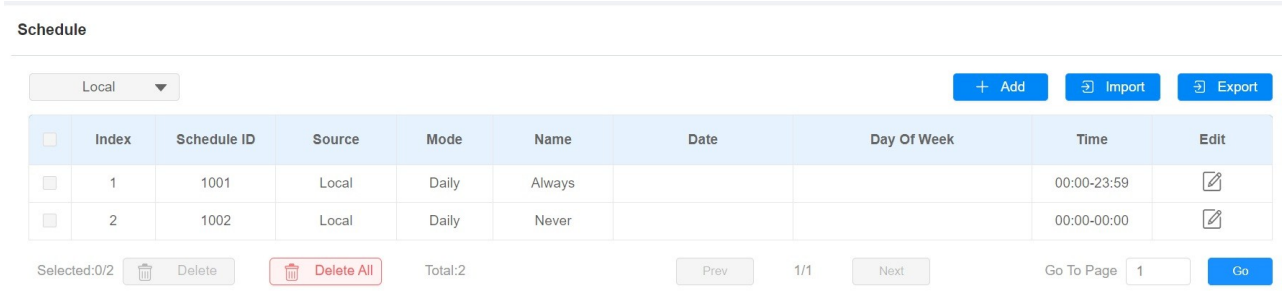
Uwaga

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

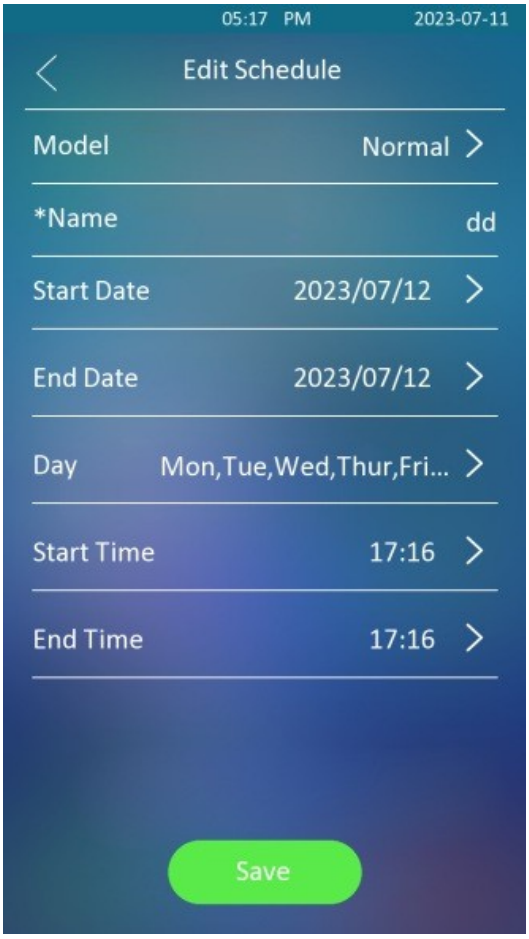
Edycja harmonogramu dostępu do drzwi

Jeśli chcesz edytować lub usunąć utworzony harmonogram dostępu do drzwi, możesz edytować lub usuwać skonfigurowany harmonogram oddzielnie lub zbiorczo.

Aby edytować harmonogram w interfejsie internetowym, przejdź do opcji **Ustawienia > Harmonogram** .



Aby edytować harmonogram na urządzeniu, kliknij opcję **Harmonogram** , a następnie wybierz harmonogram, który chcesz edytować.



Uwaga

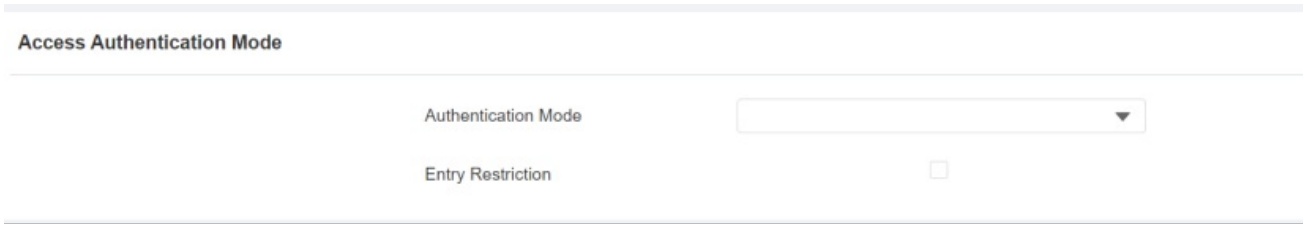
- Obsługuje tylko pliki w formacie .xml do importowania i eksportowania harmonogramu.

Konfiguracja odblokowania drzwi

Uwierzytelnianie dostępu

Można skonfigurować wiele trybów uwierzytelniania dostępu i skonfigurować zabezpieczenia uwierzytelniania zgodnie z potrzebami.

W sieci Web przejdź do **Kontrola dostępu > Przekaźnik > Tryb uwierzytelniania dostępu** .



Konfiguracja parametrów:

- **Authentication Mode (Tryb uwierzytelniania):** wybierz opcję **Any method (Dowolna metoda),** aby zezwolić na odblokowywanie drzwi wszystkimi metodami dostępu. Wybierz **Face + PIN,** jeśli chcesz zastosować podwójne metody dostępu (Face

+ PIN) do odblokowywania drzwi. Wybierz **Face + RF Card,** jeśli chcesz zastosować podwójne metody dostępu (Face + RF Card) do odblokowywania drzwi. Wybierz **RF Card+PIN,** jeśli chcesz zastosować podwójne metody dostępu (RF Card+PIN) do odblokowywania drzwi.

- **Ograniczenie wejścia**: włącz, aby ustawić interwał czasowy odblokowania drzwi.

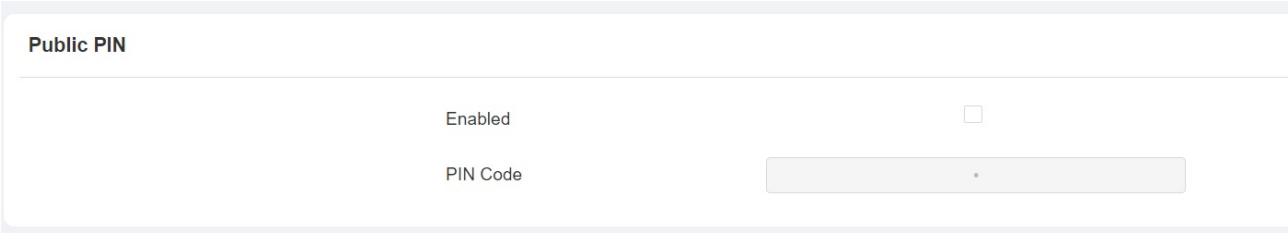
Konfiguracja kodu PIN do odblokowywania drzwi

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

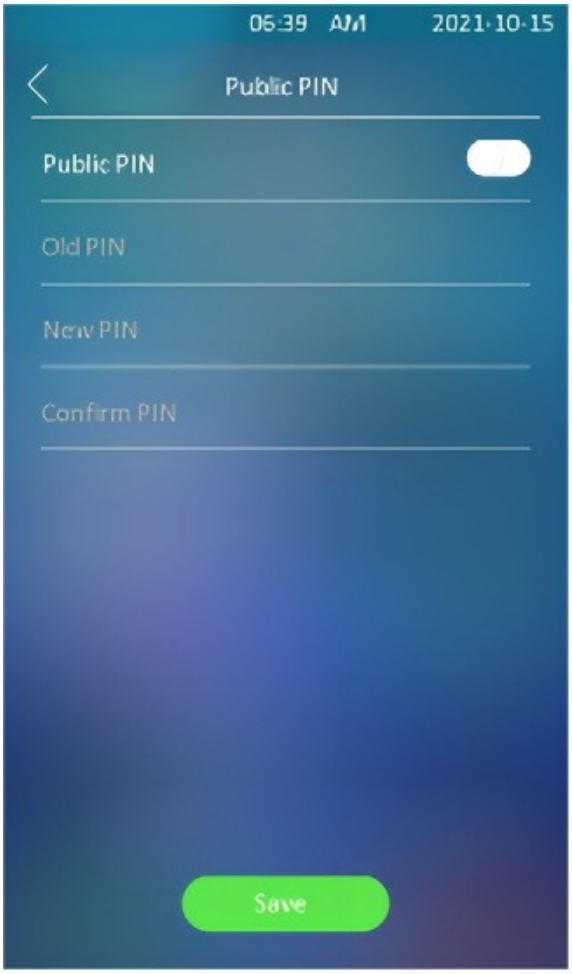
Można konfigurować i zmieniać publiczne kody PIN.

W interfejsie internetowym przejdź do opcji **Kontrola dostępu > Ustawienia kodu PIN > Publiczny kod PIN.**



Konfiguracja parametrów:

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



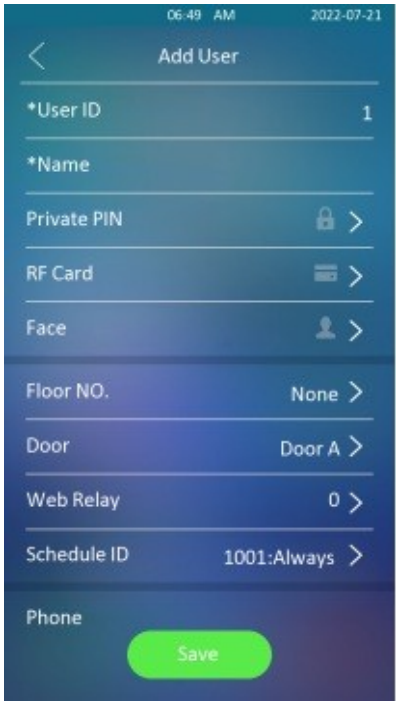
Uwaga

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

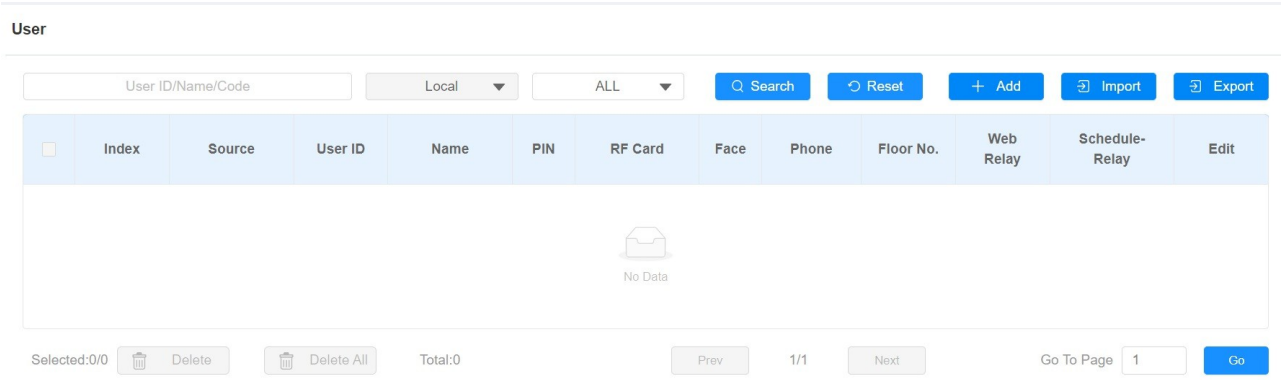
Ścieżka: **Użytkownik > Lista użytkowników**.

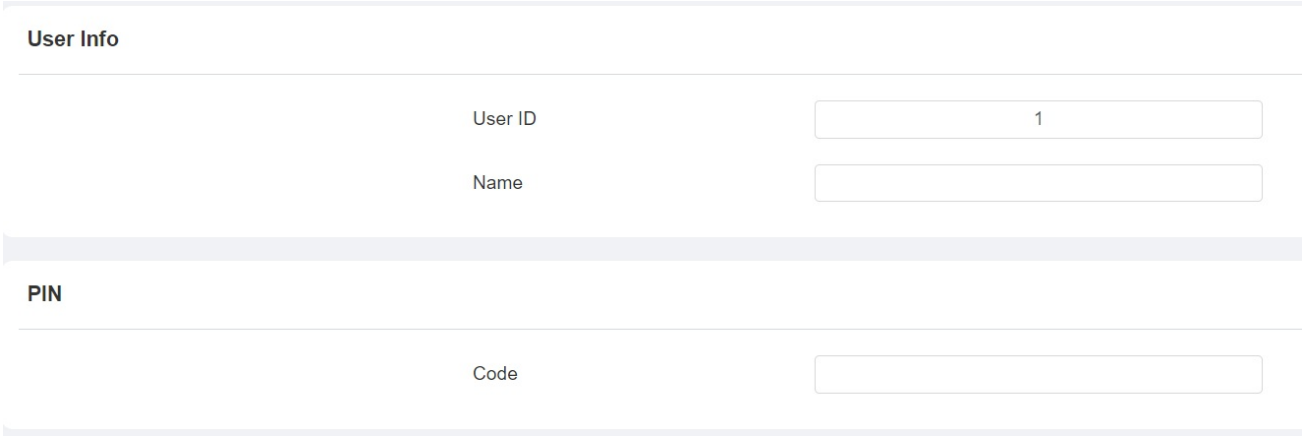


Konfiguracja prywatnego kodu PIN w interfejsie internetowym

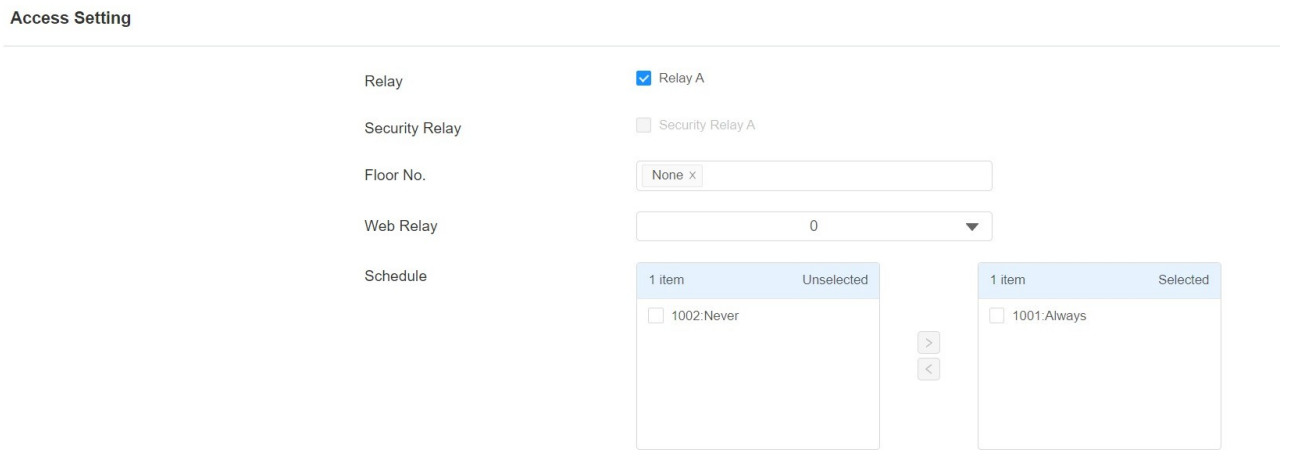
W interfejsie internetowym można utworzyć kod PIN i dostosować dodatkowe ustawienia, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenia, który przekaźnik ma zostać otwarty.

Aby skonfigurować kod PIN, przejdź do opcji **Katalog >** Interfejs **użytkownika.**





Po wprowadzeniu informacji o użytkowniku i kodu PIN można przewinąć w dół do **Ustawień dostępu** na tej samej stronie, aby ustawić harmonogram dostępu do drzwi dla prywatnego kodu PIN:



Konfiguracja parametrów:

- **Relay** (**Przekaźnik)**: wybór przekaźnika odblokowującego drzwi użytkownika. • **Floor NO**: wprowadź numer piętra mieszkańca.
- **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.

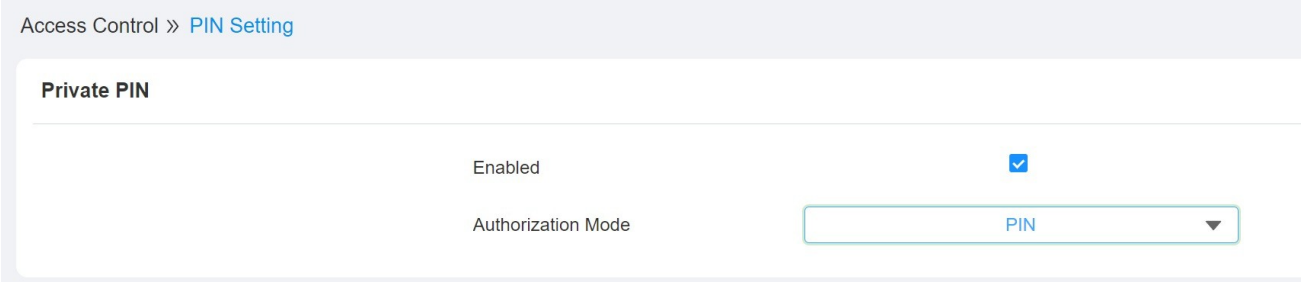
Uwaga

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

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: **Access Control > PIN Setting > Private PIN**. Na tej samej stronie można wyłączyć opcję Prywatny PIN.



Konfiguracja parametrów:

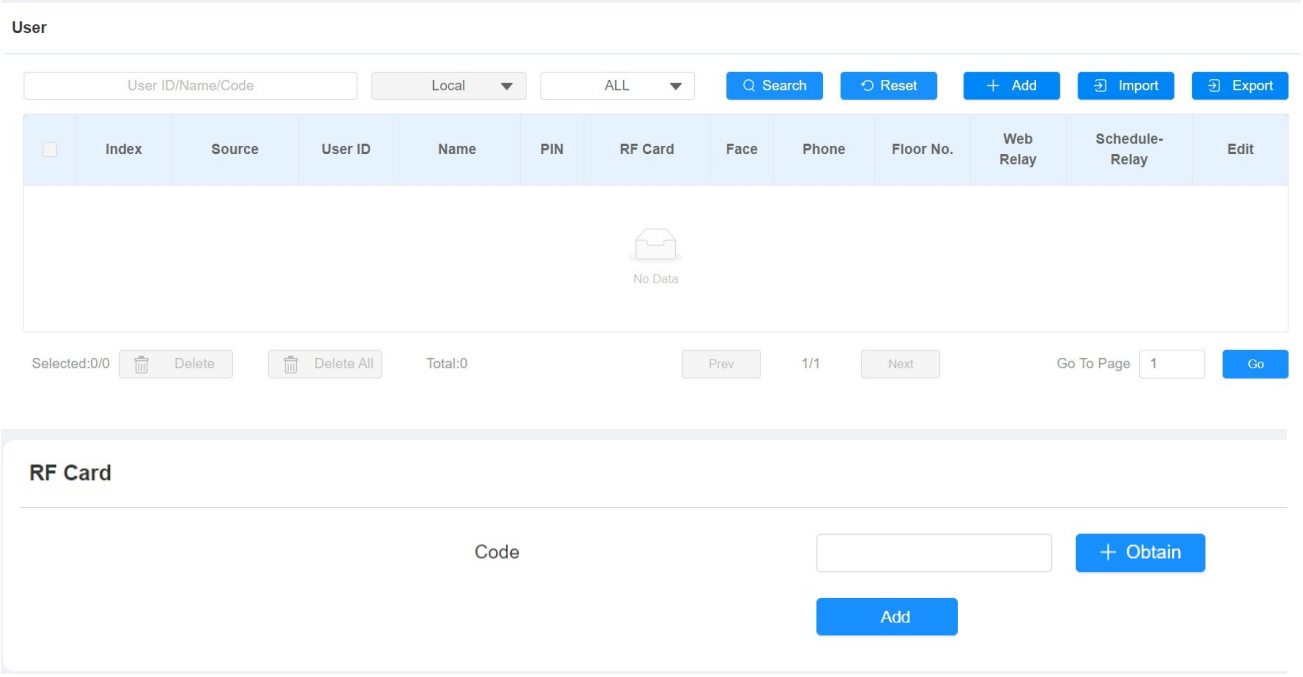
- **Tryb autoryzacji**: wybierz tryb dostępu pomiędzy **PIN** i **APT#+PIN**. W przypadku wybrania opcji **PIN** wymagane jest jedynie wprowadzenie kodu PIN bezpośrednio w celu uzyskania dostępu do drzwi, natomiast w przypadku wybrania opcji **APT#+PIN** wymagane jest wprowadzenie numeru apartamentu przed wprowadzeniem kodu PIN w celu uzyskania dostępu do drzwi.

Konfiguracja karty RF do odblokowywania drzwi

Dodawanie karty RF w interfejsie internetowym

Aby dodać karty RF, przejdź do opcji **Katalog >** 

.



Uwa

- Więcej informacji można znaleźć w rozdziale Wybór harmonogramu dostępu do kodu PIN dla użytkownika(-ów) karty RF.

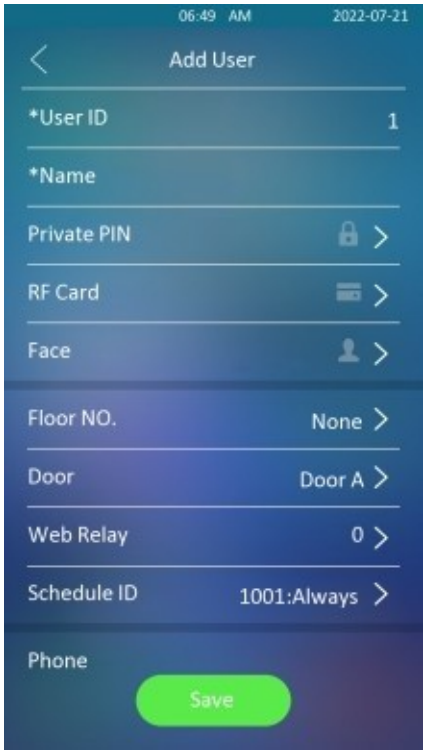
Uwaga

- Karta RF z częstotliwością 13,56 MHz i 125 KHz może być stosowana do kontroli dostępu do drzwi za pomocą domofonu.

Dodawanie karty RF do urządzenia

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

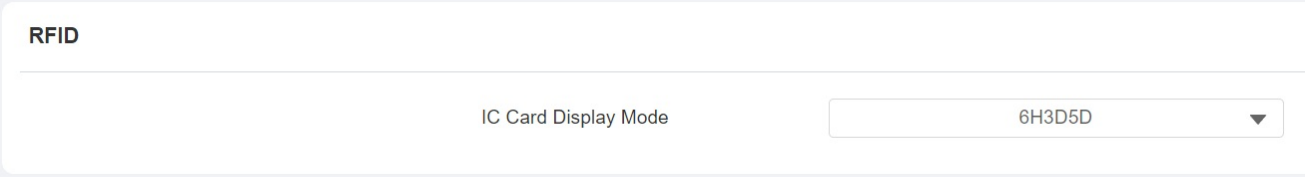
Aby dodać kartę RF, dotknij **Użytkownik**, następnie **Lista użytkowników**, a następnie **Dodaj** .



Konfiguracja formatu kodu karty RF

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

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



Konfiguracja parametrów:

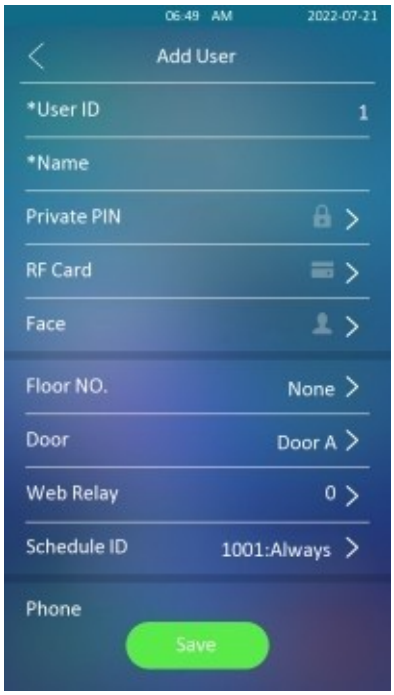
- **Tryb wyświetlania karty IC**: wybór formatu **karty IC** dla dostępu do drzwi spośród sześciu opcji formatu: **8H10D; 6H3D 5D(W26); 6H8D; 8HN; 8HR; 8HR10D** . Domyślny format kodu karty w bramofonie to 8HN.

Konfiguracja rozpoznawania twarzy do odblokowywania drzwi

Rejestrowanie danych twarzy na urządzeniu

Dane twarzy można zarejestrować na urządzeniu, wprowadzając nazwę użytkownika i rejestrując swój identyfikator twarzy na urządzeniu w celu uzyskania dostępu do drzwi.

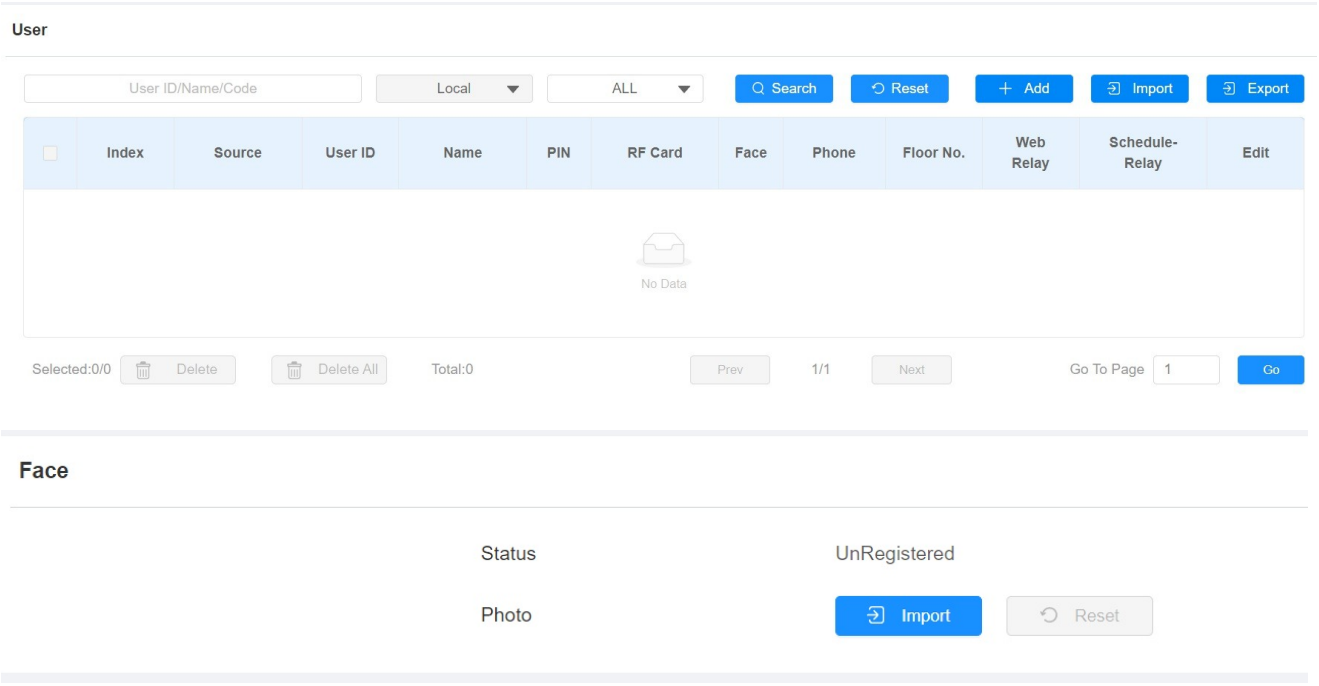
Stuknij **Użytkownik > Lista użytkowników**, a następnie stuknij **Dodaj** , i **Twarz** .



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**, gdy 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 usunięte po naciśnięciu przycisku **Reset**.
- **Photo(jpg/png)**: wybór zdjęcia w formacie jpg lub png, które ma zostać przesłane do urządzenia.

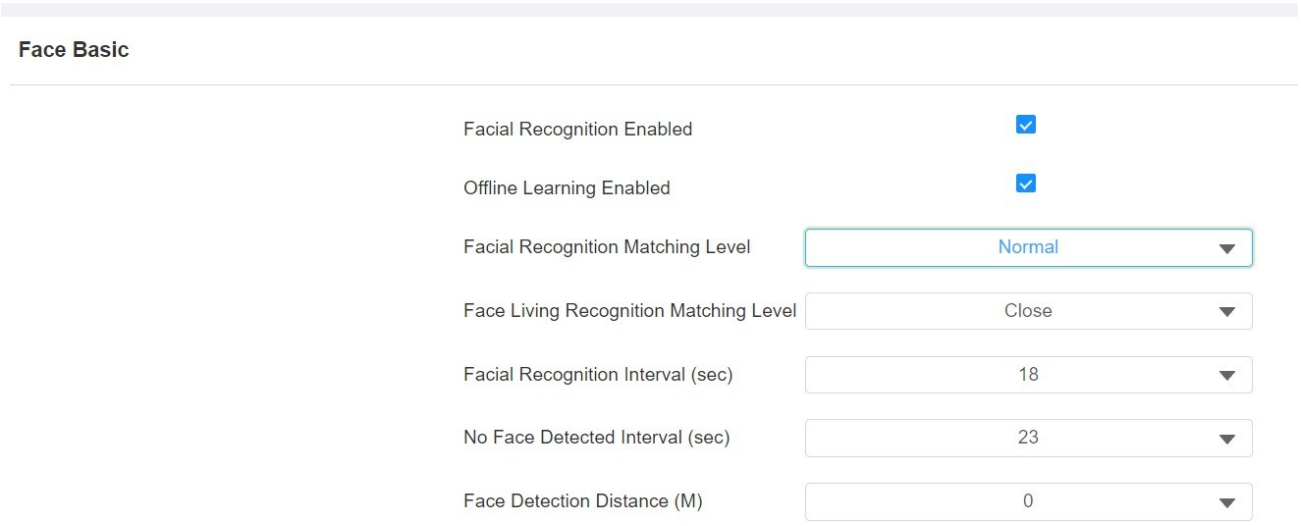
Uwaga

- 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.**

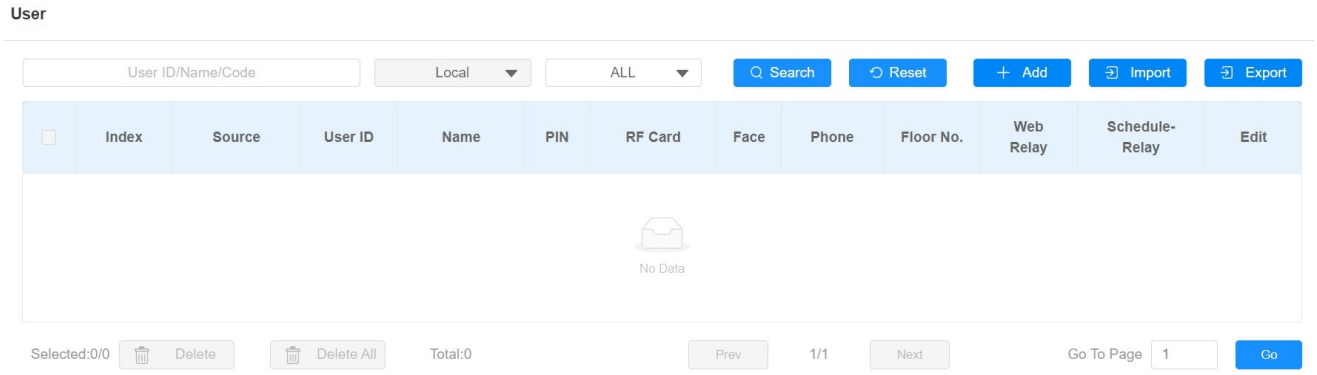


Konfiguracja parametrów:

- **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.
- **Poziom dopasowania rozpoznawania twarzy**: kliknij, aby wybrać poziom dokładności rozpoznawania twarzy spośród czterech opcji: **Niski, Normalny, Wysoki** i **Najwyższy**. Na przykład, jeśli wybierzesz **Najwyższy**, będzie najmniejsze prawdopodobieństwo, że ktoś inny zostanie pomylony z tobą przez pomyłkę lub w inny sposób podczas rozpoznawania twarzy.
- **Face Living Recognition Matching Level**: wybierz poziom Anti-spoofing spośród pięciu opcji: **Close,Low, Normal, High, Highest**. Na przykład, jeśli wybierzesz **Najwyższy**, będzie najmniejsze prawdopodobieństwo, że urządzenie zostanie oszukane przez obrazy cyfrowe lub zdjęcia dowolnego rodzaju.
- **Facial Recognition Interval(Sec) (Interwał rozpoznawania twarzy (sek.))**: wybierz odstęp czasu między każdymi dwoma rozpoznaniami twarzy w zakresie od 1 do 8 minut. Na przykład, jeśli wybierzesz **5**, musisz odczekać 5 minut, zanim będziesz mógł ponownie wykonać rozpoznawanie twarzy.

Konfiguracja dostępu do drzwi przy użyciu skonfigurowanych plików

Bramofony z serii E16 umożliwiają 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. Można przejść do **Katalog >** Interfejs **użytkownika.**



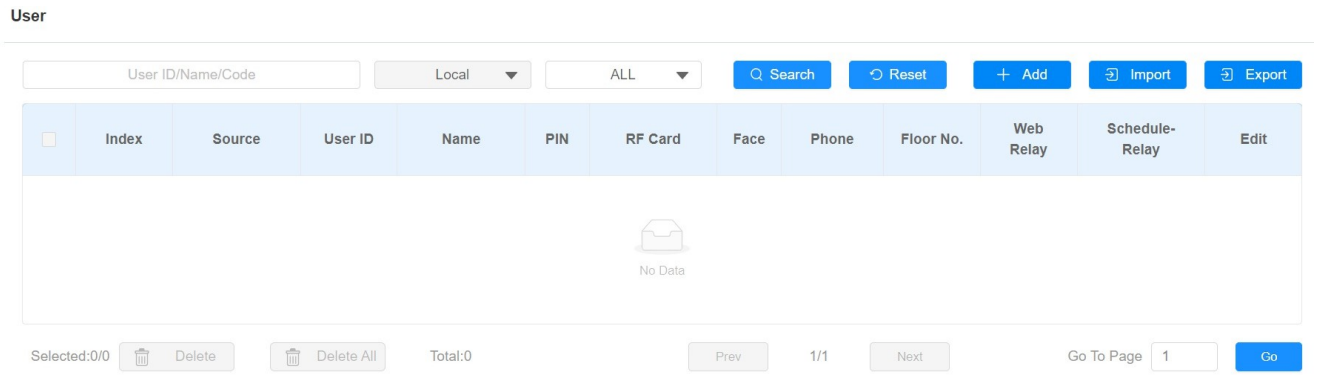
Uwaga

- Skonfigurowane pliki do rozpoznawania twarzy i innych typów skonfigurowanego dostępu do drzwi są oddzielone różnymi formami plików.

Edytowanie danych dostępu do drzwi dla poszczególnych użytkowników

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

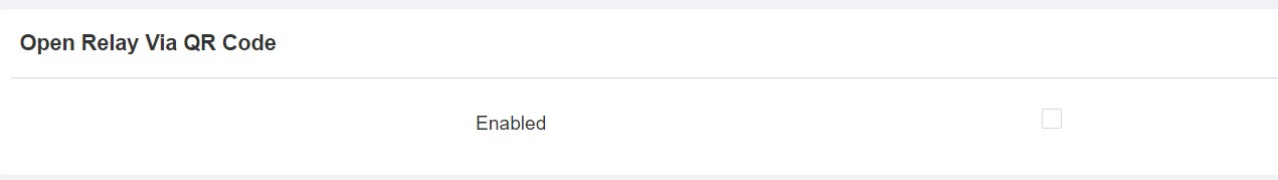
> Interfejs **użytkownika.**



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.

Możesz przejść do **Kontrola dostępu > Przekaźnik > Otwórz przekaźnik za pomocą kodu QR** .

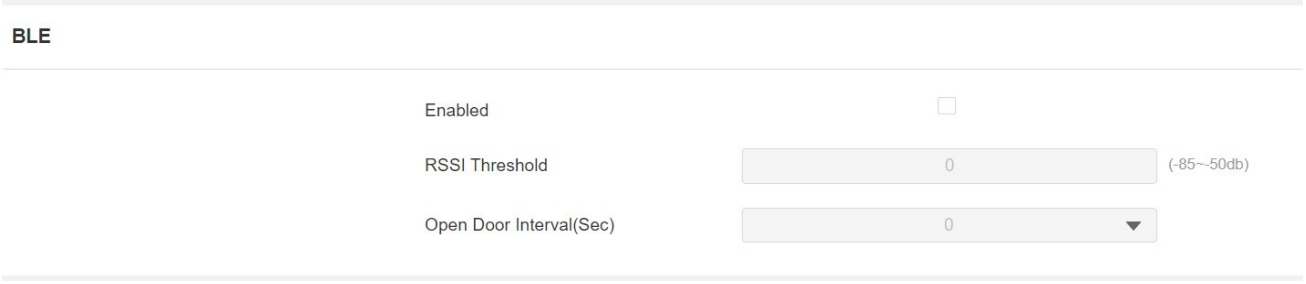


Uwa

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

Odblokowanie przez Bluetooth

Dostęp do drzwi można również uzyskać za pomocą telefonu komórkowego z Bluetooth, który jest używany z Akuvox SmartPlus. W celu uzyskania dostępu do drzwi można zbliżyć telefon komórkowy do terminala kontroli dostępu. Aby to skonfigurować na stronie internetowej **Kontrola dostępu > BLE >** Interfejs **BLE.**



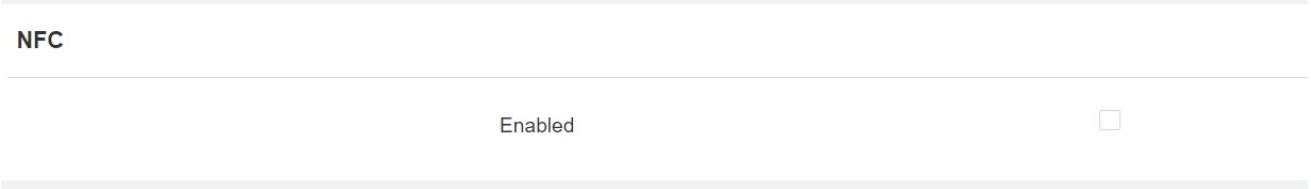
Konfiguracja parametrów:

- **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**: wybór interwału czasowego między 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.

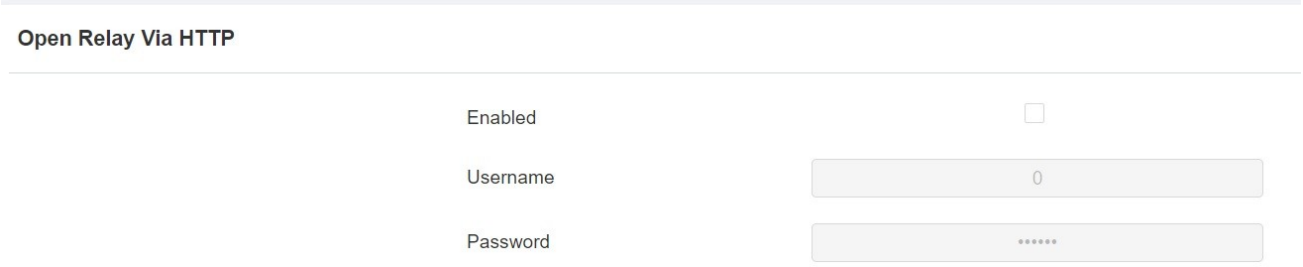
Ścieżka: **Kontrola dostępu > Ustawienia karty> NFC** .



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.

Aby skonfigurować konfigurację w sieci Web **Kontrola dostępu > Przekaźnik > Otwórz przekaźnik przez** interfejs **HTTP**



Konfiguracja parametrów:

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

Zapoznaj się z poniższym przykładem:

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

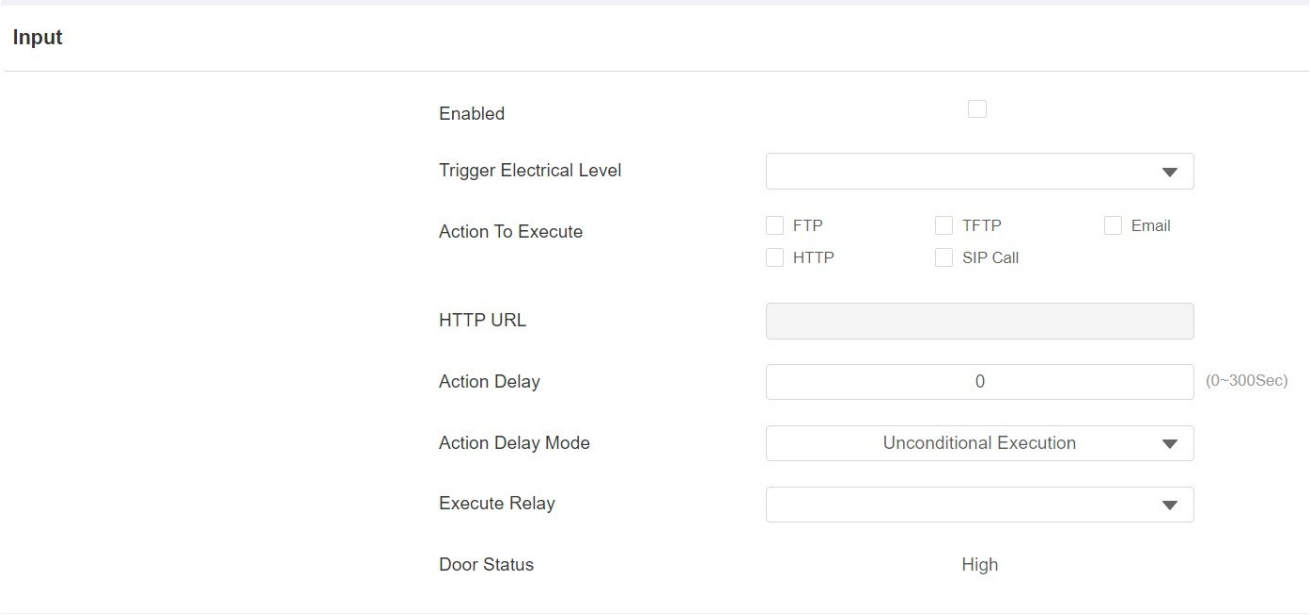
Uwaga

- **DoorNum** w powyższym poleceniu HTTP odnosi się do numeru przekaźnika #1, który ma być uruchomiony dla dostępu do drzwi.

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.

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



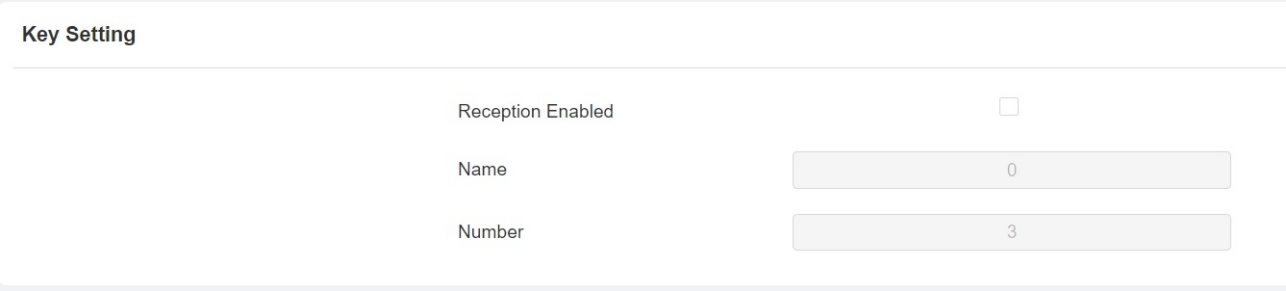
Konfiguracja parametrów:

- **Poziom wyzwalania** elektrycznego: wybierz opcje poziomu wyzwalania elektrycznego między **wysokim** i **niskim** zgodnie z rzeczywistym działaniem przycisku wyjścia.
- **Akcja do wykonania** : wybierz metodę wykonania akcji spośród pięciu opcji: **FTP, Email, SIP Call, HTTP i TFTP** .
- **HTTP URL** : wprowadź adres URL, jeśli wybierzesz HTTP do wykonania akcji.
- **Action Delay (Opóźnienie działania**): ustawienie czasu opóźnienia wykonania działania. Na przykład, jeśli ustawisz czas opóźnienia działania na 5 sekund, odpowiednie działania zostaną wykonane 5 minut po naciśnięciu przycisku (wejście zostanie wyzwolone).
- **Tryb opóźnienia akcji**: w przypadku wybrania opcji **Bezwarunkowe wykonanie**, akcja zostanie wykonana po wyzwoleniu wejścia. W przypadku wybrania opcji **Execute If Input Still Triggered** , akcja zostanie wykonana, jeśli wejście pozostanie wyzwolone. Na przykład, jeśli drzwi pozostaną otwarte po wyzwoleniu wejścia, zostanie wysłana akcja, taka jak wiadomość e-mail, aby powiadomić odbiorcę.
- **Execute Relay**: konfigurowanie przekaźników wyzwalanych przez wejście.

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.

Aby przeprowadzić konfigurację, możesz przejść do **Intercom > Basic > Key Setting** .



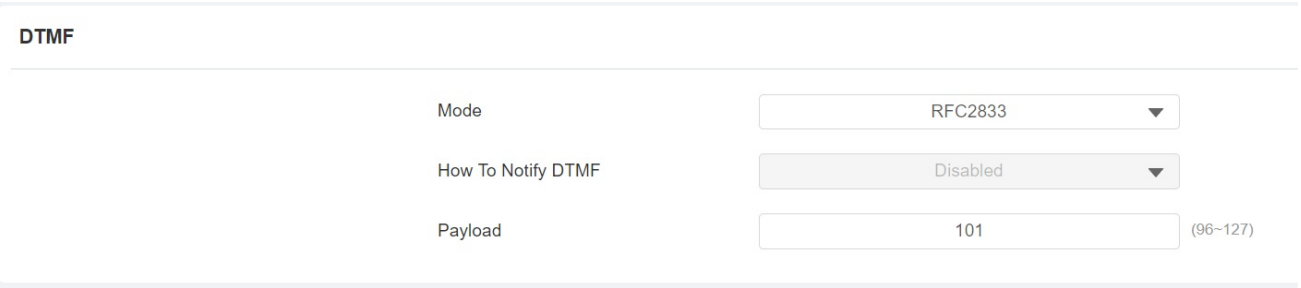
Konfiguracja parametrów:

- **Nazwa** : wprowadź nazwę ikony **recepcji** na ekranie głównym.
- **Numer**: wprowadź numer SIP/IP, który ma zostać wybrany po naciśnięciu ikony **odbioru** dostępu do drzwi.

Odblokowanie kodem 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.

Aby przeprowadzić dodatkową konfigurację DTMF w interfejsie internetowym, można przejść do **Konto > Zaawansowane**
Interfejs **>DTMF.**



Konfiguracja parametrów:

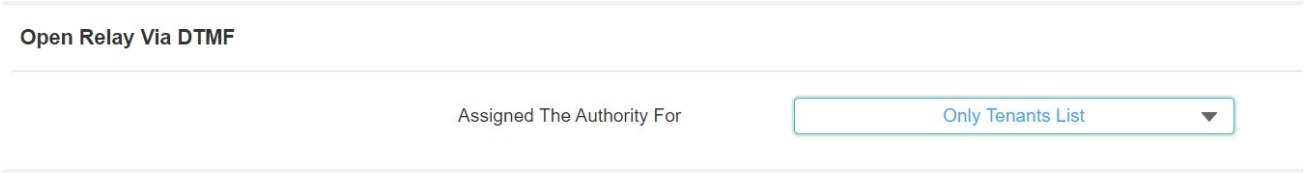
- **Typ**: wybierz typ DTMF spośród sześciu opcji: **Inband, RFC 2833, Info, Info+Inband, Info+RFC 2833** oraz **Info+Inband+RFC 2833 w** zależności od potrzeb. **Jak**
- **powiadamiać DTMF**: wybierz jedną z czterech opcji: **Disable, DTMF, DTMF-Relay** i **Telephone-Event w zależności od** potrzeb.
- **DTMF Payload** (**Ładunek DTMF)**: wybierz ładunek 96-127 do identyfikacji transmisji danych.

Uwa

- Szczegółowe informacje można znaleźć w rozdziale **Konfiguracja transmisji danych DTMF.**
  Ustawienie kodu DTMF.
- Zaangażowane urządzenia interkomowe muszą być zgodne pod względem typu DTMF, w przeciwnym razie nie można zastosować kodu DTMF.

Konfiguracja białej listy DTMF

Aby zabezpieczyć dostęp do drzwi za pomocą kodów DTMF, można skonfigurować białą listę DTMF w interfejsie sieci Web urządzenia **Access Control > Relay > Open Relay Via DTMF**, tak aby tylko numery dzwoniących wyznaczone w bramofonie mogły używać kodu DTMF w celu uzyskania dostępu do drzwi.

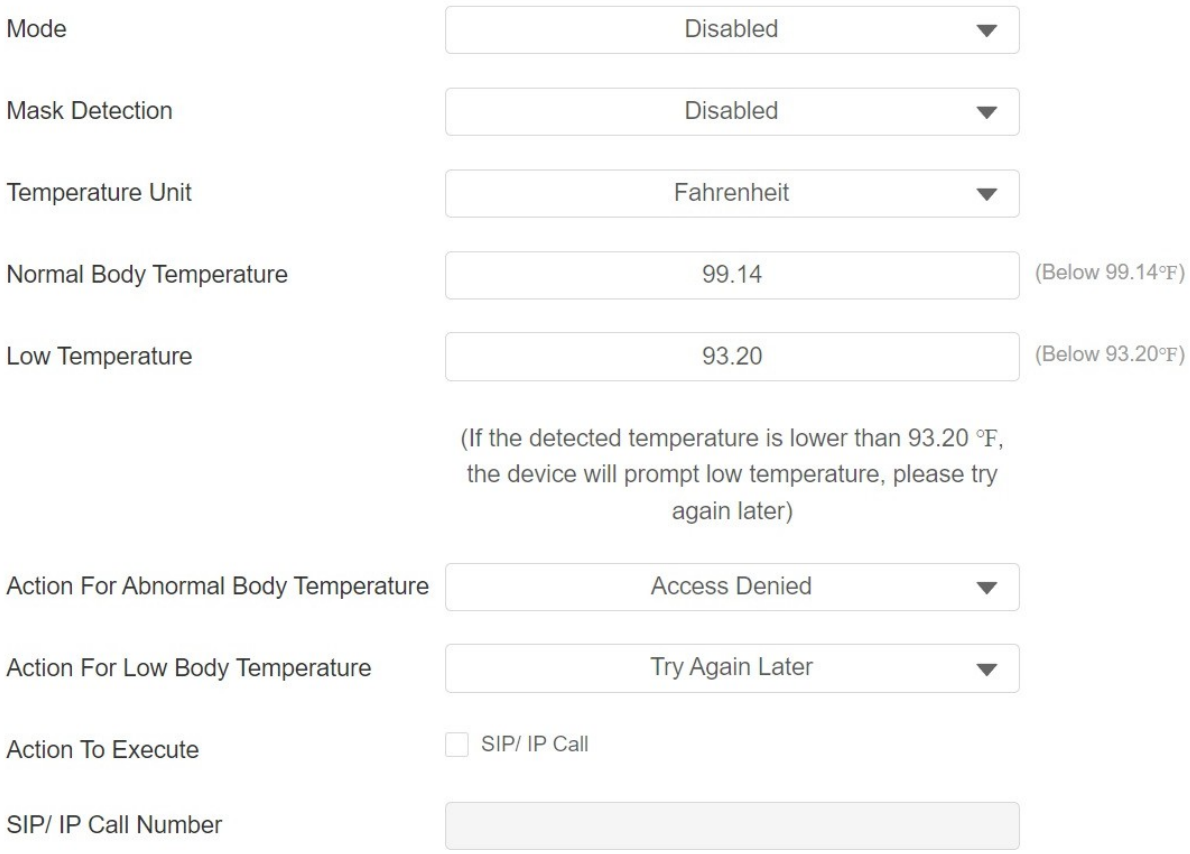


Pomiar temperatury ciała dla dostępu do drzwi (opcja)

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. Aby przeprowadzić konfigurację w interfejsie Web **Access Control > Body Temperature > Measuring Body Temperature.**



Konfiguracja parametrów:

- **Tryb**: wybierz tryb **wyłączenia**, tryb **czoła** lub tryb **nadgarstka** 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, czy nie, przypominając mu o tym komunikatem **Proszę nosić maskę** . Po wybraniu opcji **Wyświetl monit o noszenie maski** urządzenie będzie wyświetlać tylko monit o noszenie maski, nie wprowadzając obowiązku noszenia maski. Alarm ostrzegawczy zostanie uruchomiony, gdy zmierzona temperatura ciała będzie wyższa niż zdefiniowana normalna temperatura ciała.
- **Normalna temperatura ciała**: ustaw temperaturę ciała na wstępnie zdefiniowaną temperaturę ciała jako podstawę pomiaru w stopniach Fahrenheita lub Celsjusza. Na przykład, jeśli ustawiono

temperaturę 37,3 stopni Celsjusza jako temperaturę normalną, wówczas każda temperatura ciała zmierzona powyżej 37,3 stopni Celsjusza zostanie uznana za temperaturę nienormalną, podczas gdy temperatura niższa niż 34 stopnie Celsjusza zostanie uznana za niską temperaturę ciała.

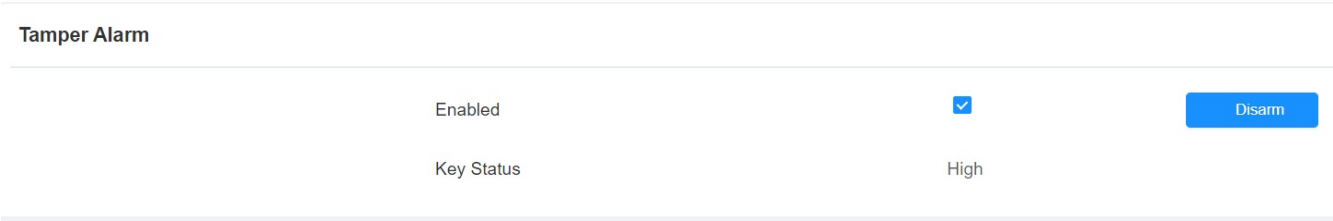
- **Niska temperatura**: ustawienie niskiej temperatury.
- **Action For Abnormal Body Temperature (Działanie w przypadku nieprawidłowej temperatury ciała)**: w przypadku wybrania opcji **Access Denied (Odmowa dostępu)** każdy, u kogo zostanie wykryta nieprawidłowa temperatura ciała, otrzyma odmowę dostępu do drzwi. W przypadku wybrania opcji **Just For Reminder (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**, użytkownikowi zostanie odmówiony dostęp do drzwi z komunikatem **Spróbuj ponownie później** ze względu na niską temperaturę ciała. W przypadku wybrania opcji **Tylko dla przypomnienia** każda 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 połączenie SIP lub IP dla powiadomienia. Pole pojawi się, aby wypełnić numery SIP/IP po zaznaczeniu pola w polu **Akcja do wykonania** .

Bezpieczeństwo

Ustawienie alarmu sabotażowego

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

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



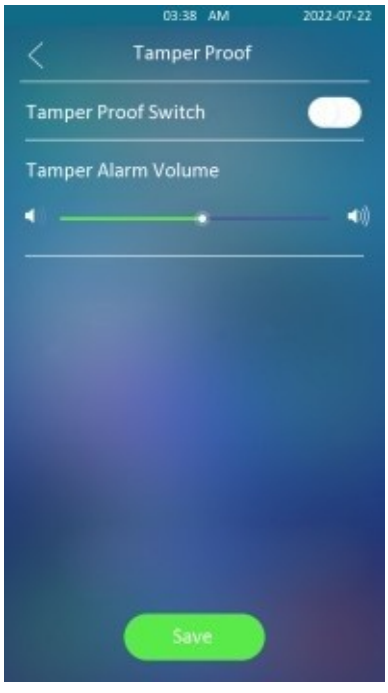
Konfiguracja parametrów:

- **Włącz** : zaznacz pole wyboru, aby włączyć funkcję alarmu sabotażowego. Gdy alarm sabotażowy wyłączy się, można nacisnąć przycisk **Disarm** obok pola wyboru, aby skasować alarm.
- **Stan klawisza**: po naciśnięciu przycisku alarmu sabotażowego stan zostanie zmieniony z niskiego na wysoki. Normalny stan to wysoki.

Uwaga

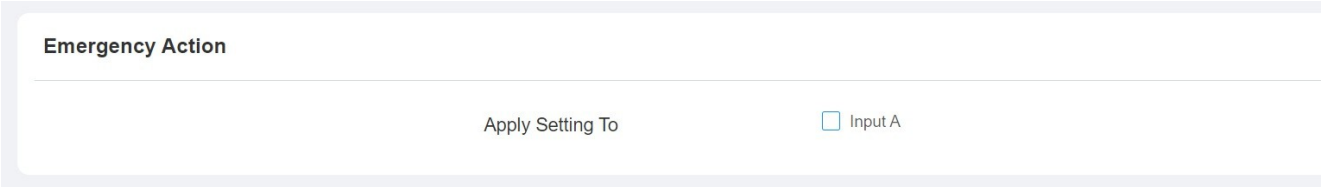
- Po usunięciu alarmu sabotażowego zakładka **Rozbrój** zmieni kolor na szary.
- Okrągły gumowy przycisk z tyłu urządzenia musi być wciśnięty, w przeciwnym razie alarm nie zostanie uruchomiony.

Aby włączyć funkcję zabezpieczenia antysabotażowego na urządzeniu, stuknij **Zabezpieczenia > Zabezpieczenie antysabotażowe**.



Akcja ratunkowa

W sytuacji awaryjnej drzwi mogą pozostać otwarte. Przejdź do opcji **System > Security > Emergency Action**.



Uwaga

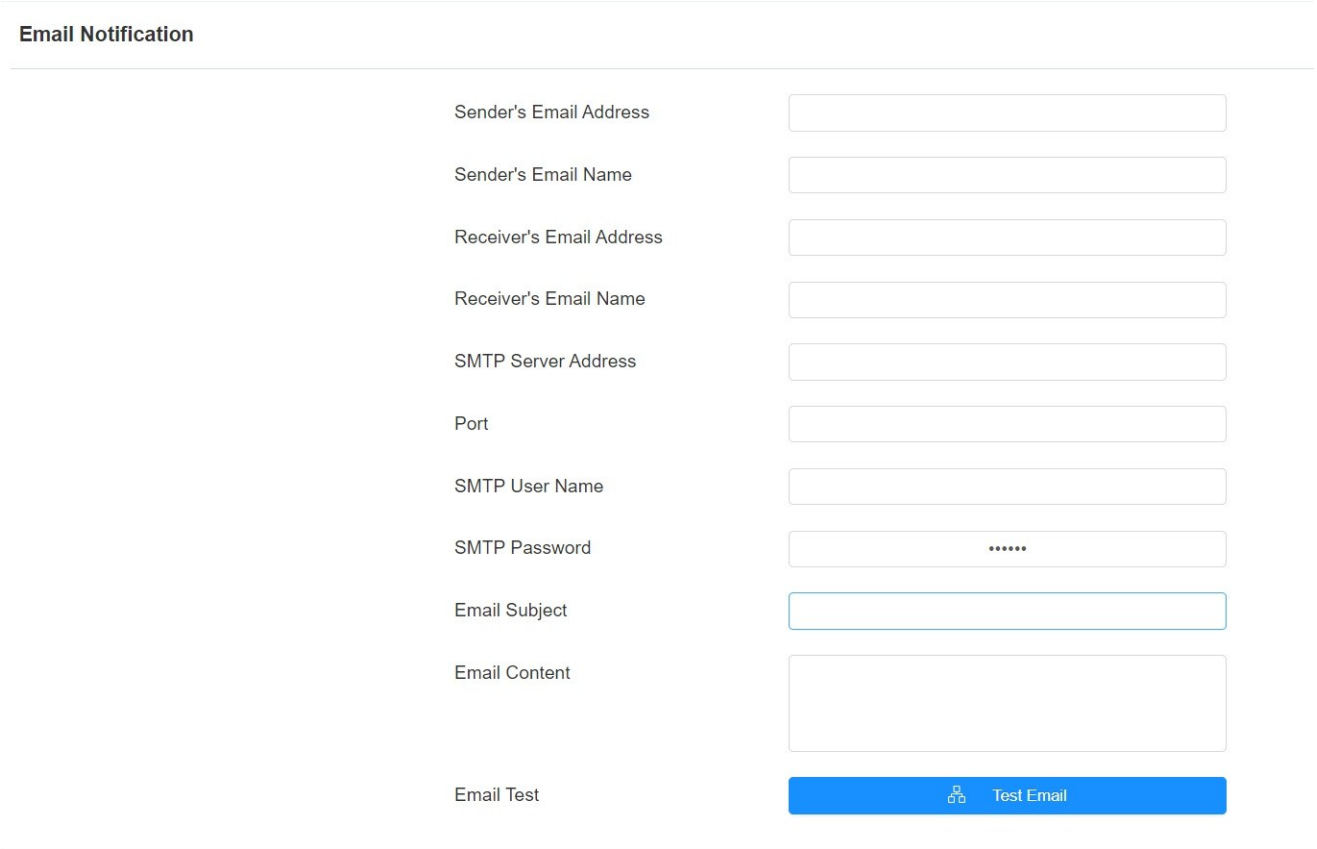
- Ta funkcja musi współpracować z Akuvox Cloud.

Ustawienia powiadomień bezpieczeństwa

Ustawienia powiadomień e-mail

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

Aby skonfigurować konfigurację w interfejsie sieci Web **Setting > Action > Email Notification.**



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. •

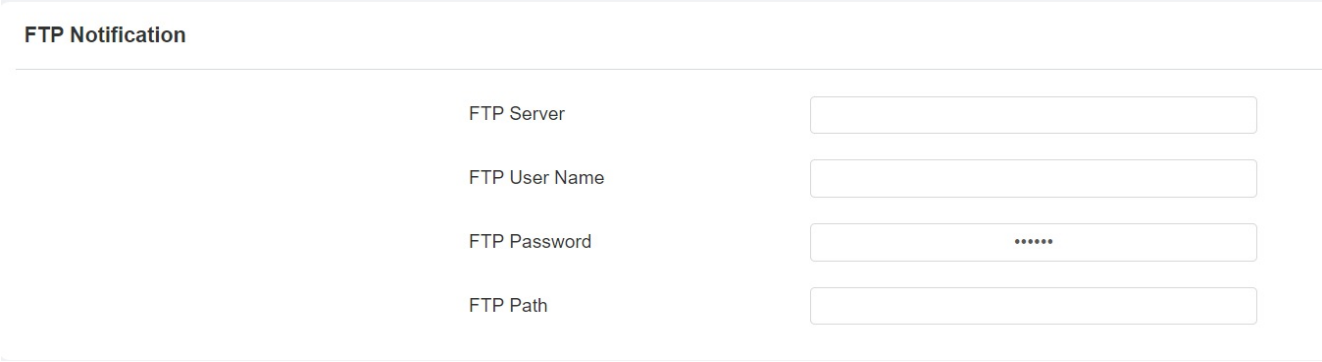
Nazwa e-mail odbiorcy: wprowadź nazwę odbiorcy wiadomości e-mail.

- **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 zazwyczaj jest taka sama jak adres e-mail nadawcy.
- **Hasło SMTP** : skonfiguruj hasło usługi SMTP, które jest takie samo jak adres e-mail nadawcy.
- **Temat wiadomości e-mail**: wprowadź temat wiadomości e-mail.
- **Treść wiadomości e-mail**: skompiluj treść wiadomości e-mail zgodnie ze swoimi potrzebami.

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.

Aby skonfigurować konfigurację w interfejsie sieci Web **Setting > Action > FTP Notification.**

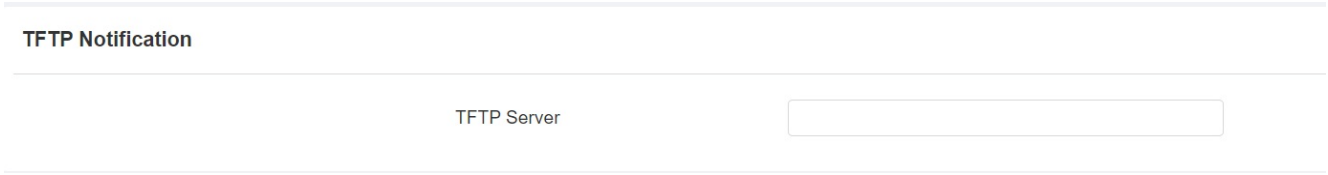


Konfiguracja parametrów:

- **FTP Server**: wprowadź adres (URL) serwera FTP dla powiadomienia FTP.
- **Nazwa użytkownika FTP**: wprowadź nazwę użytkownika serwera FTP.
- **Hasło FTP** : wprowadź hasło serwera 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. Aby dokonać konfiguracji w interfejsie **Ustawienia > Akcja > Powiadomienie TFTP.**

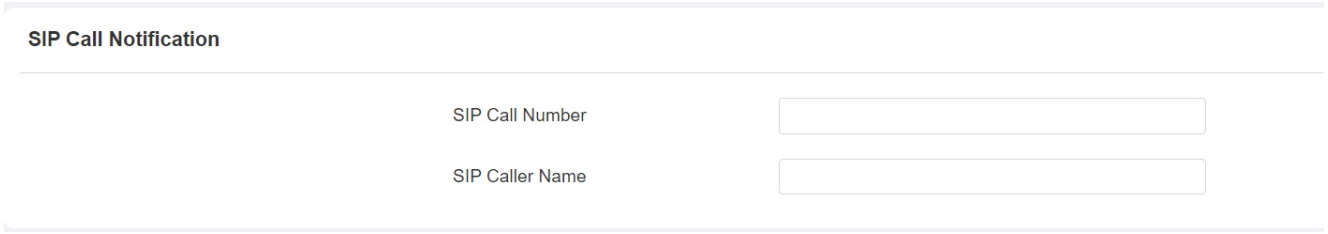


Konfiguracja parametrów:

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

Powiadomienie o połączeniu SIP

Jeśli chcesz otrzymywać powiadomienia o zabezpieczeniach za pośrednictwem połączenia SIP, możesz odpowiednio skonfigurować powiadomienie FTP w interfejsie internetowym. Ścieżka:



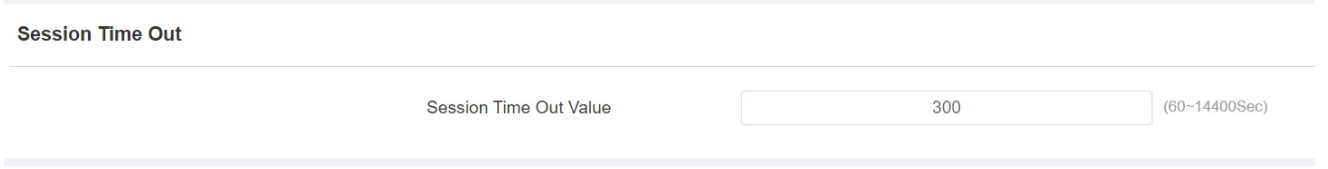
Konfiguracja parametrów :

- **SIP Call Number**: wprowadź numer IP połączenia SIP.
- **Nazwa dzwoniącego SIP**: wprowadź nazwę dzwoniącego.

Interfejs sieciowy Automatyczne wylogowanie

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

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



Konfiguracja parametrów:

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

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

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:

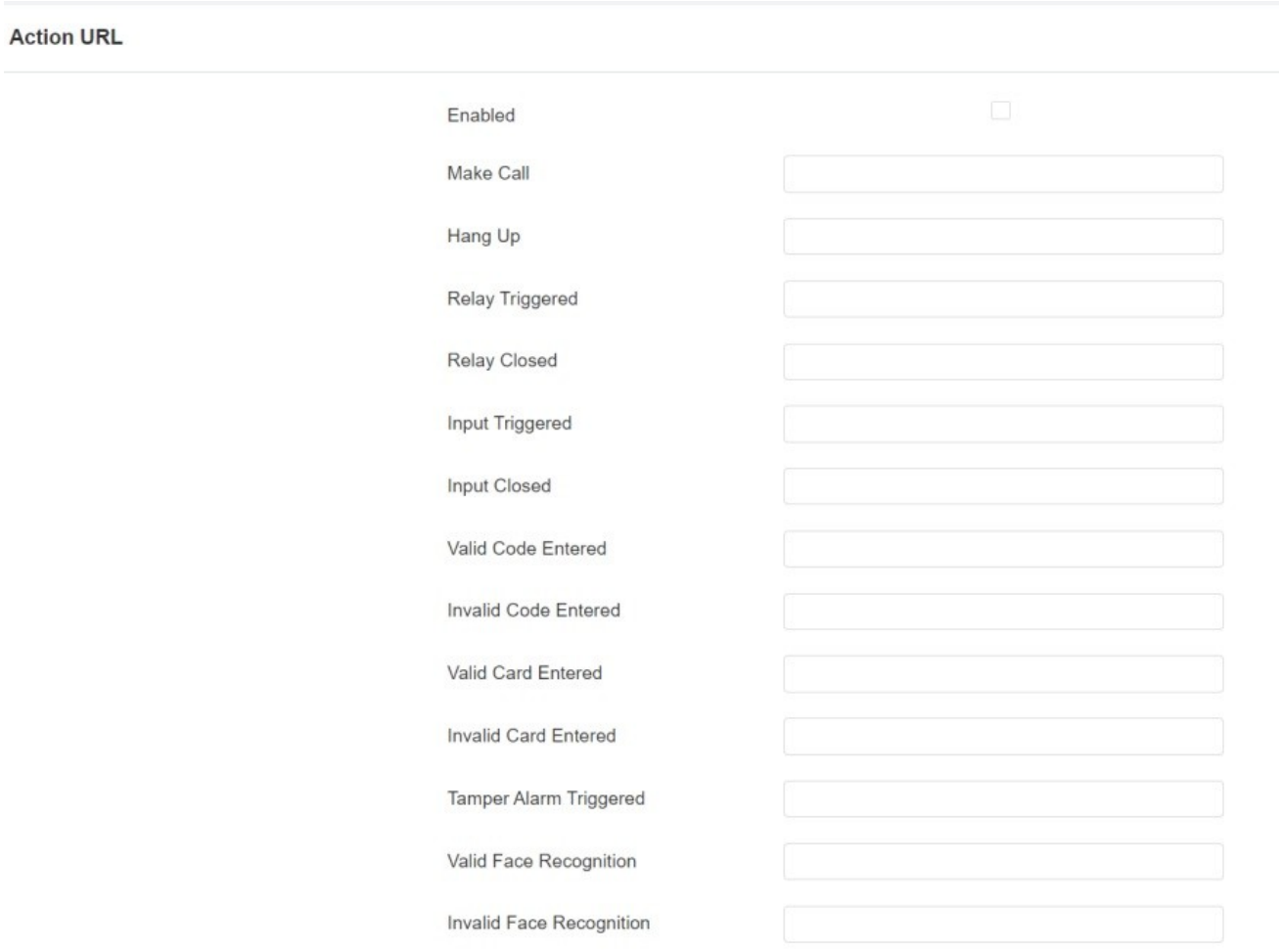
Nie	Wydarzenie	Format parametrów	Przykład
1	Wykonaj połączenie	$remote	Http://server ip/ Callnumber=$remote
2	Rozłącz się	$remote	Http://server ip/ Callnumber=$remote
3	Przekaźnik wyzwolony	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Przekaźnik zamknięty	$relay1status	Http://server ip/ relayclose=$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 **Ustawień > Adres URL akcji**

Uwa

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



Monitor i obraz

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

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

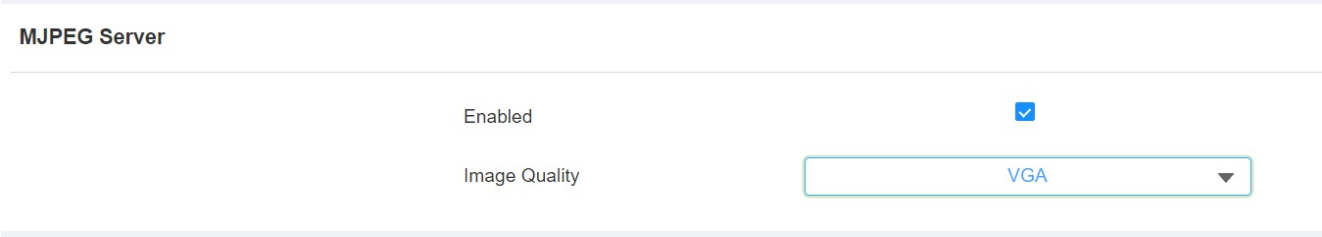
RTSP to skrót od Real Time Streaming Protocol. Może być używany do strumieniowego przesyłania obrazu i dźwięku z kamer innych firm do urządzenia. Możesz dodać strumień z kamery, dodając jej adres URL. Format adresu URL urządzeń Akuvox to rtsp://Device's IP/live/ch00_0

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

Przechwytywanie obrazu MJPEG

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

Aby skonfigurować konfigurację w interfejsie Web **Surveillance > MJPEG > MJPEG Server.**



Konfiguracja parametrów :

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

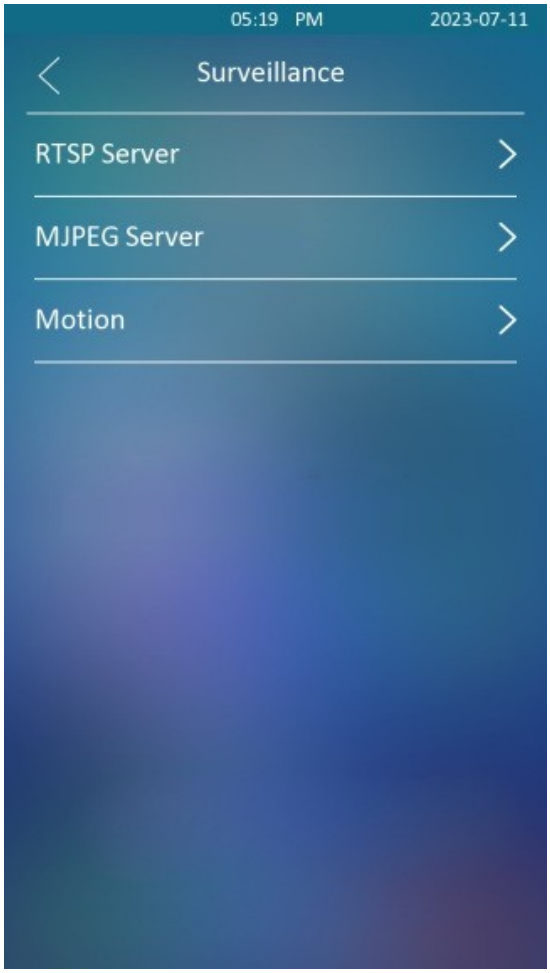
Po włączeniu usługi MJPEG można przechwytywać obraz z bramofonu przy użyciu następujących trzech typów formatu URL:

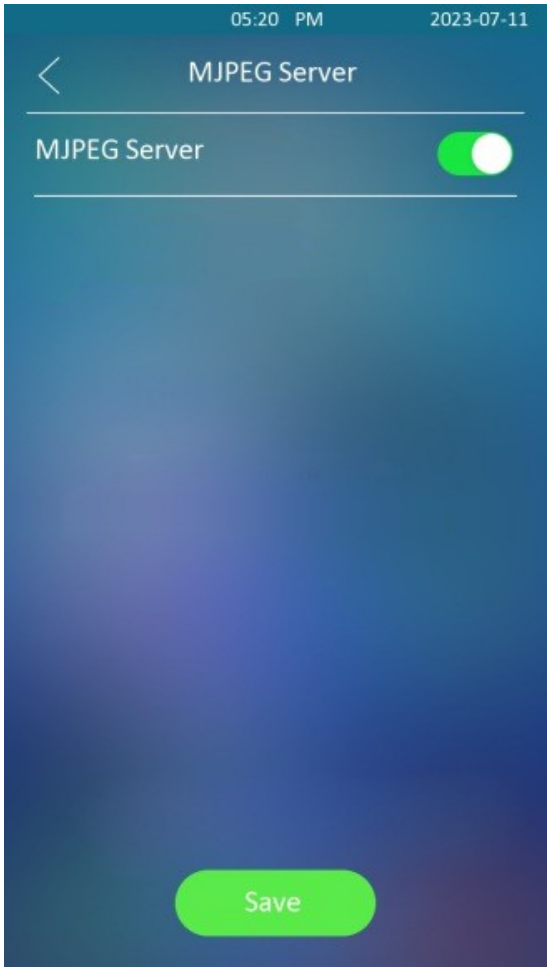
- http:// urządzenie ip:8080/picture.cgi

- http://deviceip:8080/picture.jpg
- http://deviceip:8080/jpeg.cgi

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

Serwer MJPEG można także włączyć bezpośrednio na urządzeniu. Stuknij kolejno opcje **Zaawansowane > Nadzór > Serwer MJPEG.**

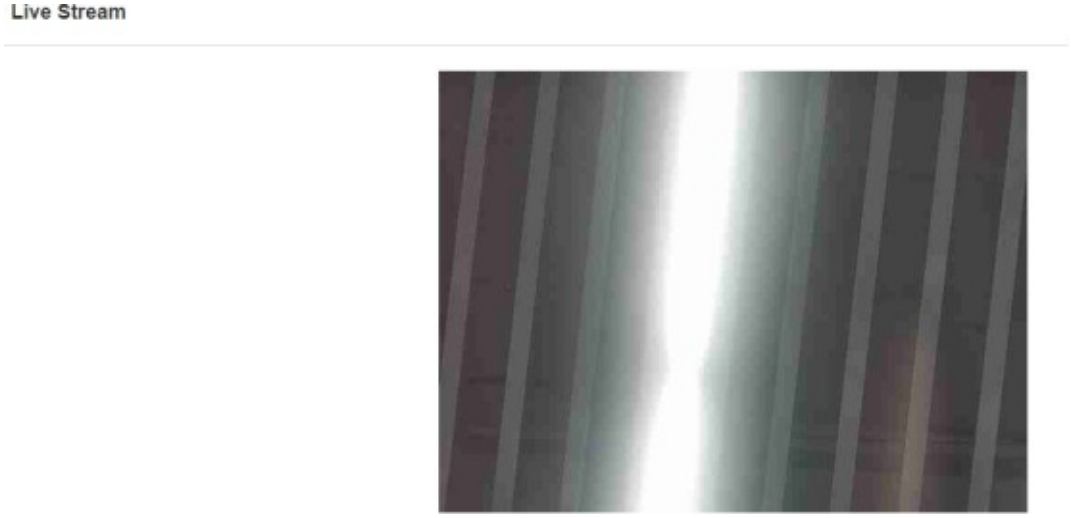




Transmisja na żywo

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.

Aby oglądać transmisję na żywo w interfejsie **Surveillance > Live Stream.**



Aby sprawdzić wideo w czasie rzeczywistym za pomocą adresu URL, można wprowadzić prawidłowy adres URL **(http:// IP_address:8080/video.cgi**).

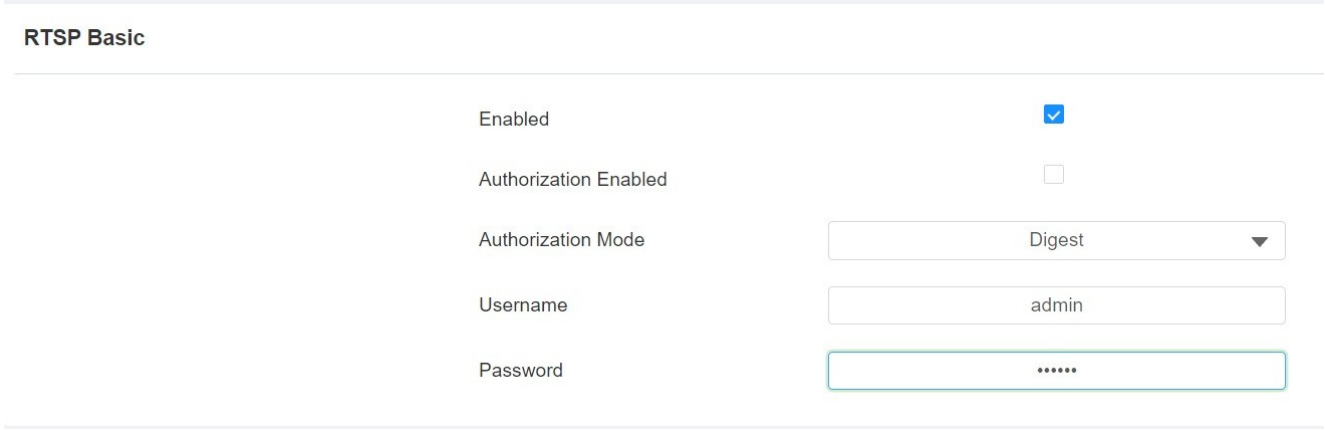
Na przykład http://192.168.2.5:8080/video.cgi

Monitorowanie strumienia RTSP

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

Podstawowe ustawienia RTSP

Przed użyciem funkcji RTSP należy ją skonfigurować pod kątem autoryzacji RTSP, uwierzytelniania, hasła itp. Aby przeprowadzić konfigurację w interfejsie Web **Surveillance > RTSP > RTSP Basic.**



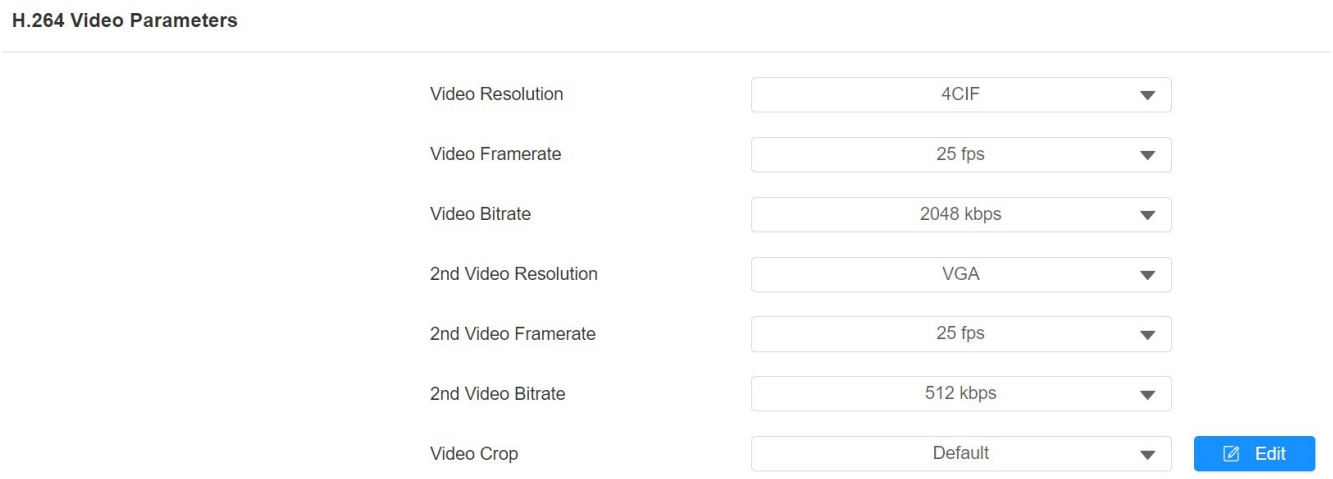
Konfiguracja parametrów:

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

Ustawienia strumienia RTSP

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

Aby skonfigurować konfigurację w interfejsie internetowym **Surveillance > RTSP > H.264 Video Parameters.**



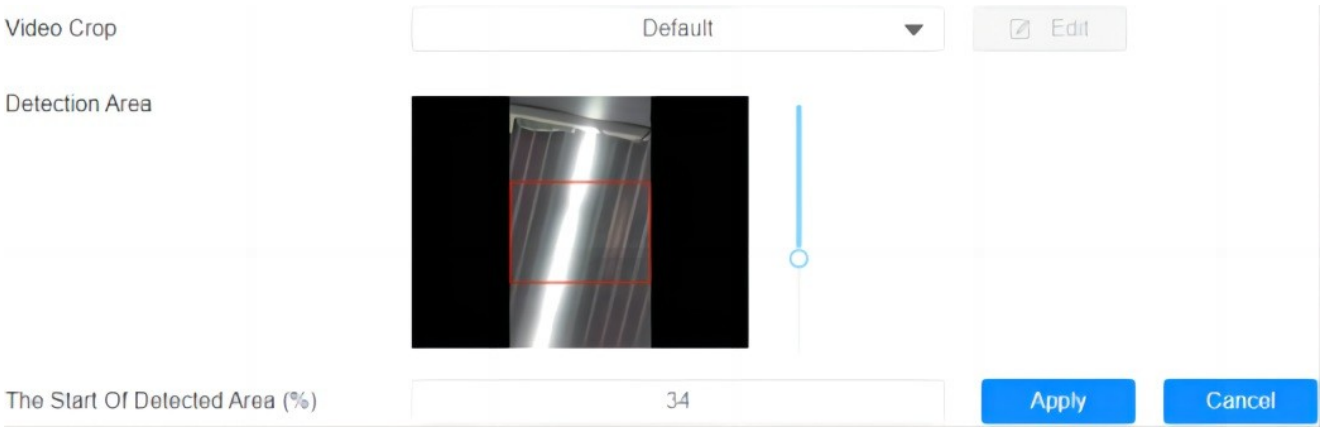
Konfiguracja parametrów:

- **Rozdzielczość wideo**: wybór rozdzielczości wideo spośród siedmiu opcji: **QCIF, QVGA, CIF, VGA, 4CIF, 720P i 1080P** . Domyślną rozdzielczością wideo jest **720P**, a wideo z bramofonu może nie być wyświetlane na monitorze wewnętrznym, jeśli rozdzielczość jest ustawiona na wyższą niż **720P**.
- **Częstotliwość klatek wideo: 25 klatek na sekundę** to domyślna częstotliwość klatek wideo.
- **Szybkość transmisji wideo** : wybór szybkości transmisji wideo spośród sześciu opcji: **128 kb/s, 256 kb/s, 512**

kb/s, 1024 kb/s, 2048 kb/s i 4096 kb/s w zależności od środowiska sieciowego.

Domyślna szybkość transmisji wideo wynosi **2048 kb/s.**

- **2nd Video Resolution2** : wybór rozdzielczości wideo dla drugiego kanału strumienia wideo. Domyślną rozdzielczością wideo jest **VGA**.
- **2nd Video Framerate** : wybierz liczbę klatek na sekundę 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 opcję **Oryginał,** aby wyświetlać wideo na pełnym ekranie. Wybierz **Default,** jeśli chcesz wybrać tylko określony obszar wideo do wyświetlenia. Możesz kliknąć **Edytuj,** aby rozpocząć przycinanie wideo.



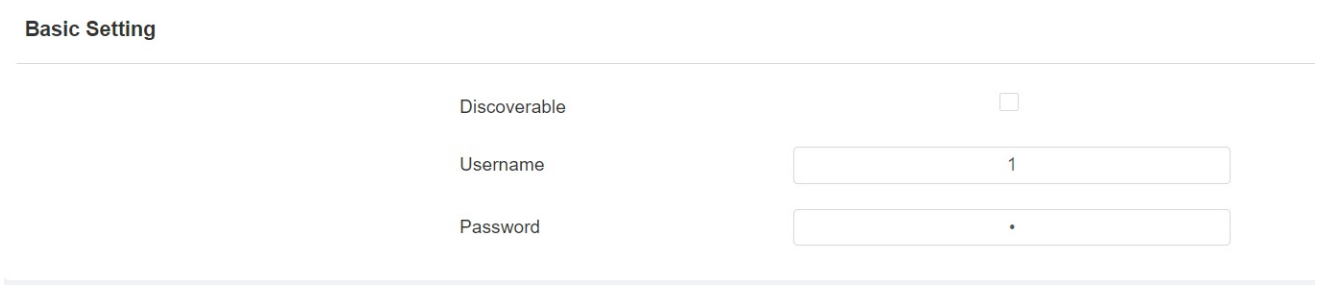
Uwaga

- Seria E16 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.

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



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.**
- **UserName** : wprowadź nazwę użytkownika. Domyślna nazwa użytkownika to **admin.**
- **Password** : wprowadź hasło. Domyślne hasło to **admin.**

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

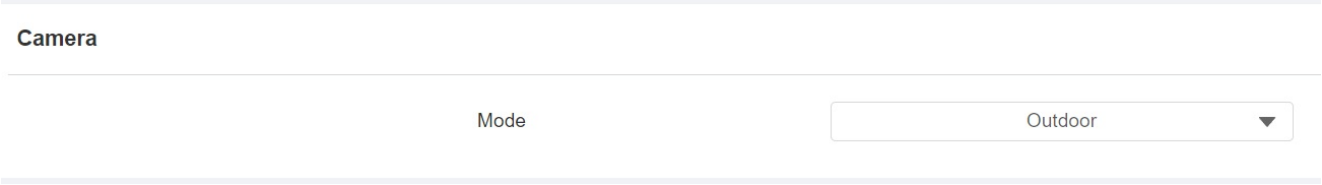
Na przykład: **http://IP address:80/onvif/device_service**

Uwaga

- Wpisz konkretny adres IP bramofonu w adresie URL.

Tryb kamery

W zależności od lokalizacji bramofonu można wybrać tryb kamery zapewniający lepszą jakość obrazu wideo. Można wybrać tryb wewnętrzny, aby uzyskać lepszy obraz wideo (RTSP, ONVIF i Mjpeg), jeśli bramofon znajduje się w pomieszczeniu. Tryb **zewnętrzny** można natomiast wybrać, jeśli bramofon znajduje się na zewnątrz.

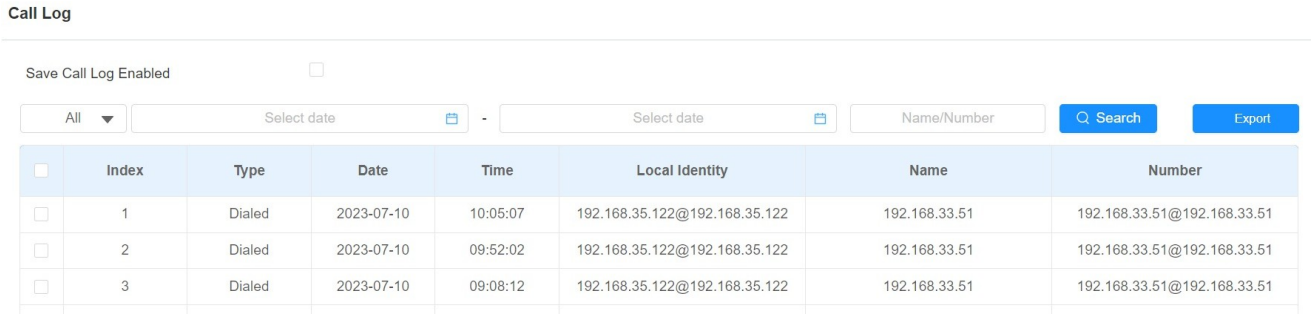


Dzienniki

Dzienniki połączeń

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

Aby sprawdzić rejestr połączeń, można przejść do opcji **Status > Rejestr połączeń** .



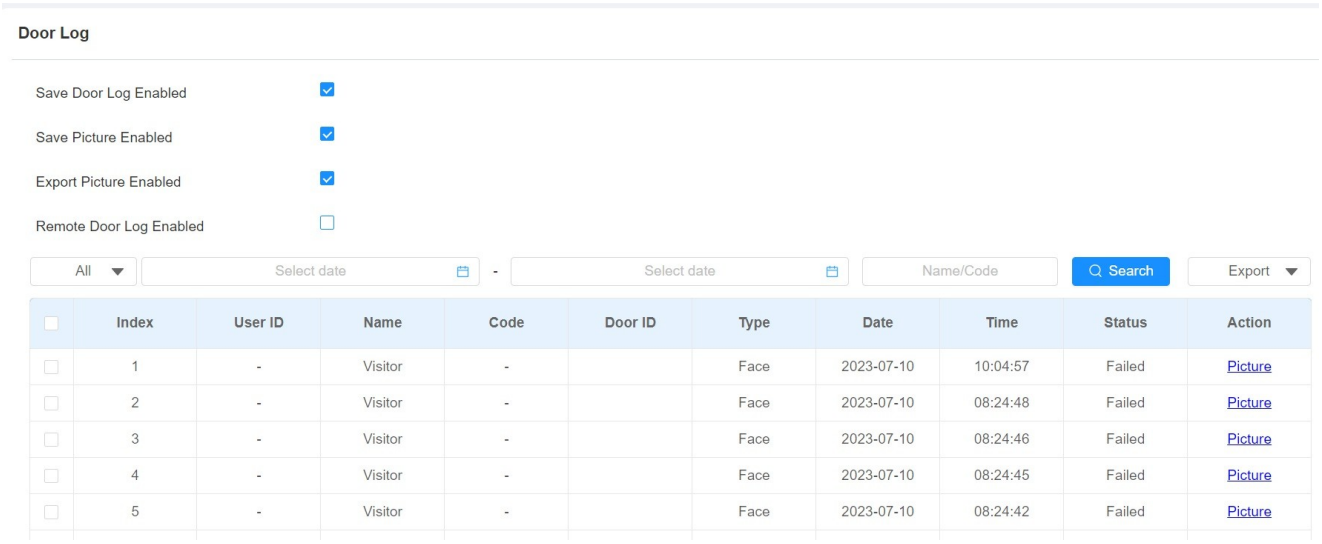
Konfiguracja parametrów :

- **Historia połączeń**: wybierz historię połączeń spośród czterech opcji: **All (Wszystkie), Dialed (Wybrane)**, **Received (Odebrane)** i **Missed (Nieodebrane)** dla określonego typu rejestru połączeń, który ma być wyświetlany.
- **Godzina rozpoczęcia ~ Godzina zakończenia** : wybierz określony przedział czasowy dzienników połączeń, które chcesz wyszukać, sprawdzić lub wyeksportować.
- **Tożsamość lokalna**: wyświetla konto SIP lub numer IP bramofonu, który odbiera połączenia przychodzące.
- **Nazwa/Numer**: wybierz opcje **Nazwa** i **Numer**, aby przeszukiwać rejestr połączeń według nazwy lub numeru SIP lub IP.

Dzienniki drzwi

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

Aby sprawdzić dzienniki drzwi, przejdź do **Status > Access Log** .

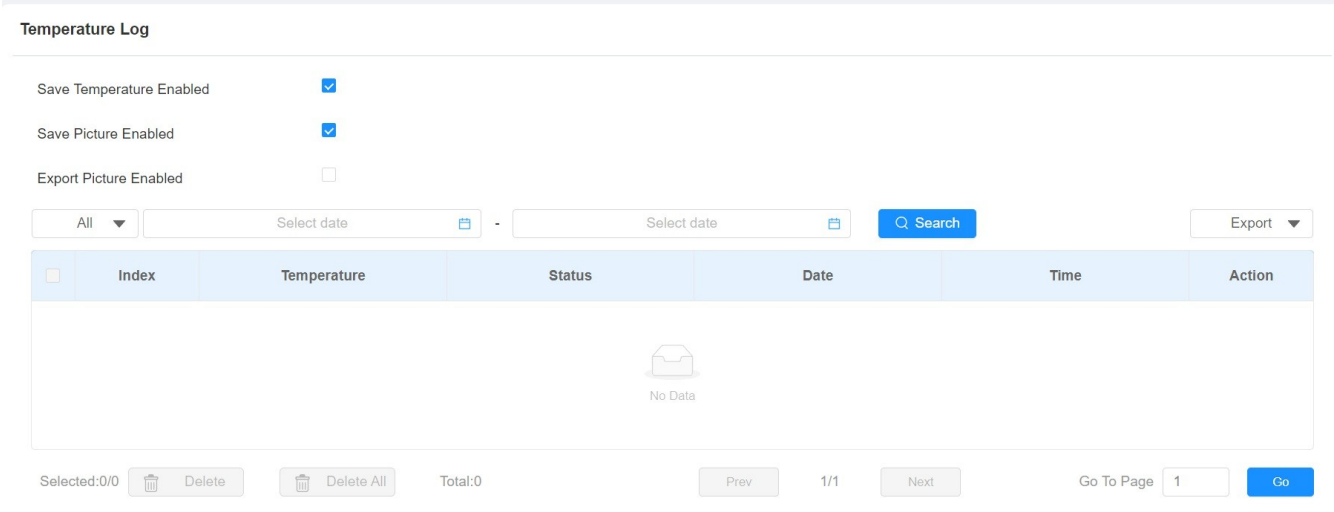


Konfiguracja parametrów:

- **Status** : wybierz pomiędzy opcjami **Udany i Nieudany**, 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

Aby sprawdzić dziennik temperatury, przejdź do **Status > Dziennik temperatury** .



Konfiguracja parametrów:

- **Save Picture Enabled**: włącz, jeśli chcesz zapisać pomiar temperatury.

migawka.

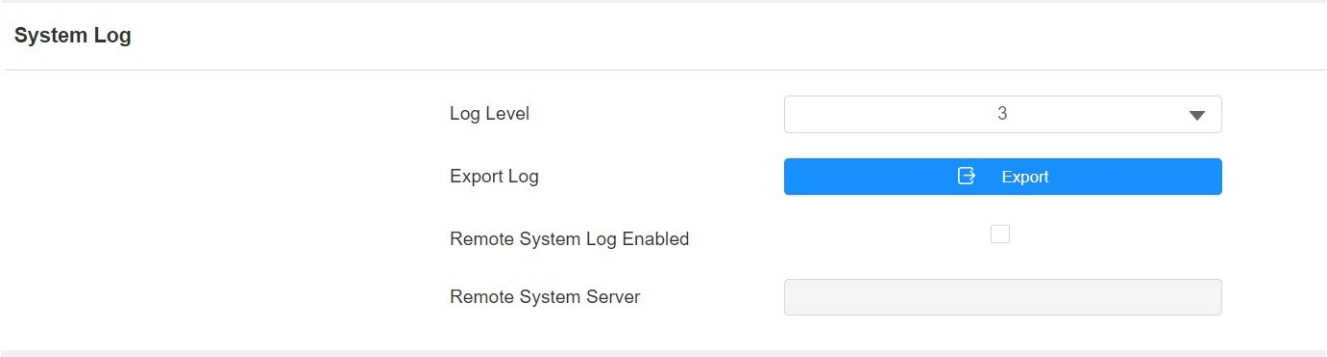
- **Export Picture Enabled**: włącz, jeśli chcesz wyeksportować dziennik temperatury z przechwyconym obrazem migawki.
- **Czas**: wybierz określony przedział czasowy dziennika temperatury, który chcesz wyszukać, sprawdzić lub wyeksportować.
- **Działanie**: kliknij, aby wyświetlić zrobione zdjęcie.

Debugowanie

Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

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



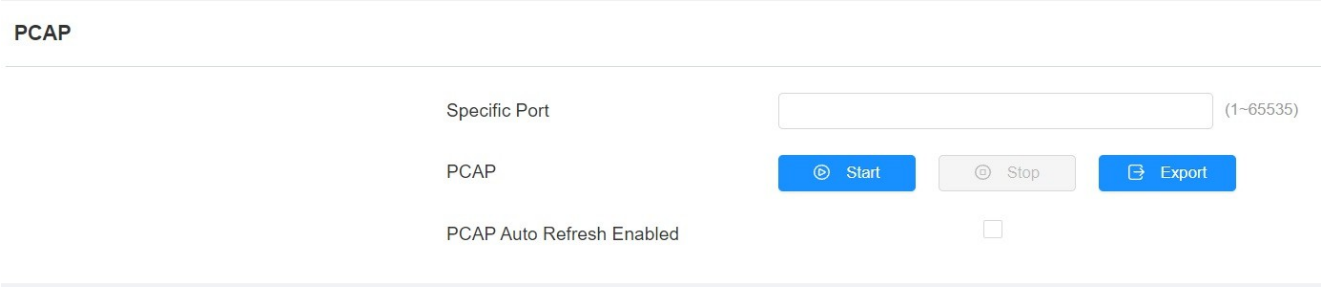
Konfiguracja parametrów:

- **Log Level (Poziom dziennika)**: wybierz poziom dziennika od 1 do 7. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić do celów debugowania. Domyślny poziom dziennika to 3, im wyższy poziom to 5, tym bardziej kompletny jest dziennik 7.
- **Eksportuj dziennik**: przejdź do zakładki **Eksportuj**, aby wyeksportować tymczasowy plik dziennika debugowania do lokalnego komputera.
- **Remote System Log Enabled** : wybierz **Enable** lub **Disable**, jeśli chcesz włączyć lub wyłączyć zdalny dziennik systemu.
- **Zdalny serwer systemu**: wprowadź adres zdalnego serwera, aby otrzymywać dziennik urządzenia.

PCAP do debugowania

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

PCAP można skonfigurować w witrynie internetowej urządzenia **System > Konserwacja > PCAP** przed jego użyciem.



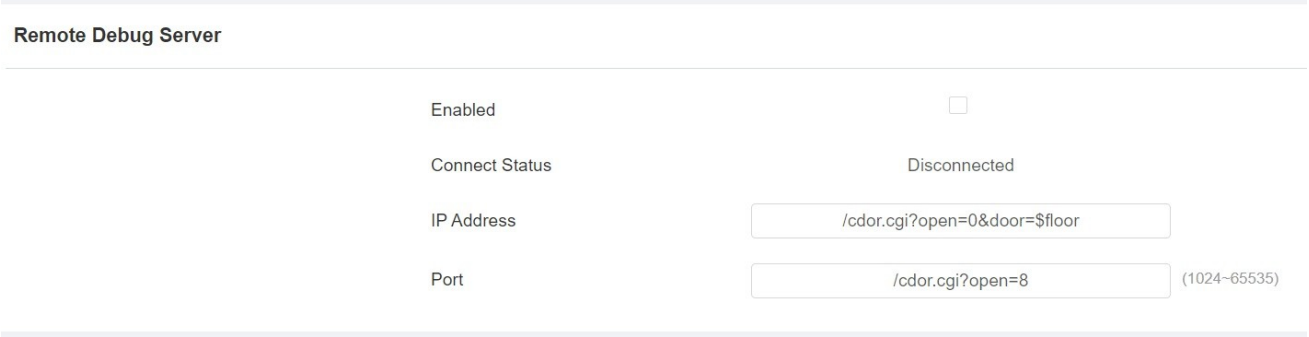
Konfiguracja parametrów:

- **Określony port**: wybierz określone porty z zakresu 1-65535, aby można było przechwytywać tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.
- **PCAP**: przejdź do zakładki Start i **Stop**, aby przechwycić określony zakres pakietów danych przed przejściem do 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. Jeśli opcja ta zostanie ustawiona jako **Disable**, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycony pakiet danych osiągnie maksymalną pojemność 1 MB.

Zdalny serwer debugowania

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

Aby skonfigurować serwer, przejdź do **System > Maintenance > Remote Debug Server**.



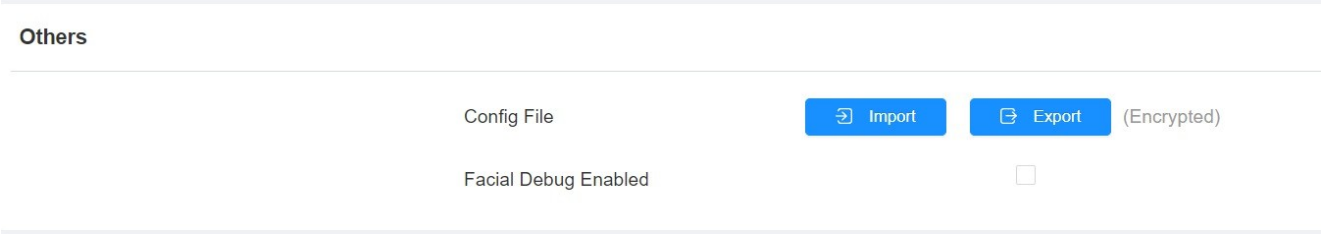
Konfiguracja parametrów:

- **Connect Status** : wyświetla stan połączenia ze zdalnym serwerem debugowania.
- **Adres IP** : wprowadź adres IP zdalnego serwera debugowania. Zapytaj zespół techniczny Akuvox dla adresu IP serwera.

  Port: wpisz port zdalnego serwera debugowania.

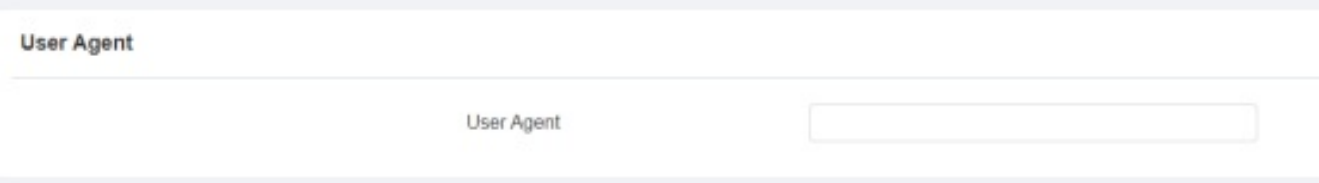
Debugowanie rozpoznawania twarzy

Włączenie funkcji rozpoznawania twarzy może być wymagane do debugowania w przypadku wystąpienia problemu z rozpoznawaniem twarzy. Aby je włączyć, przejdź do opcji **System > Konserwacja > Inne.**



Agent użytkownika

Agent użytkownika SIP (UA) to urządzenie końcowe obsługujące protokół SIP, które służy do nawiązywania połączeń i włączania sesji między dwoma urządzeniami końcowymi. UA składa się z UAC (klienta agenta użytkownika) i UAS (serwera agenta użytkownika), przy czym UAC służy do wydawania żądań, a UAS do wydawania odpowiedzi. UA działa jako dostawca usług SIP dla konkretnego użytkownika (urządzenia). Pole agenta użytkownika w wiadomości SIP można dostosować. Jeśli agent użytkownika jest ustawiony na określoną wartość, użytkownicy mogą zobaczyć informacje z PCAP. Jeśli agent użytkownika jest pusty, domyślnie użytkownicy mogą zobaczyć nazwę firmy "Akuvox", numer modelu i wersję oprogramowania układowego z PCAP. Ścieżka: **Konto > Zaawansowane >** Interfejs **agenta użytkownika.**



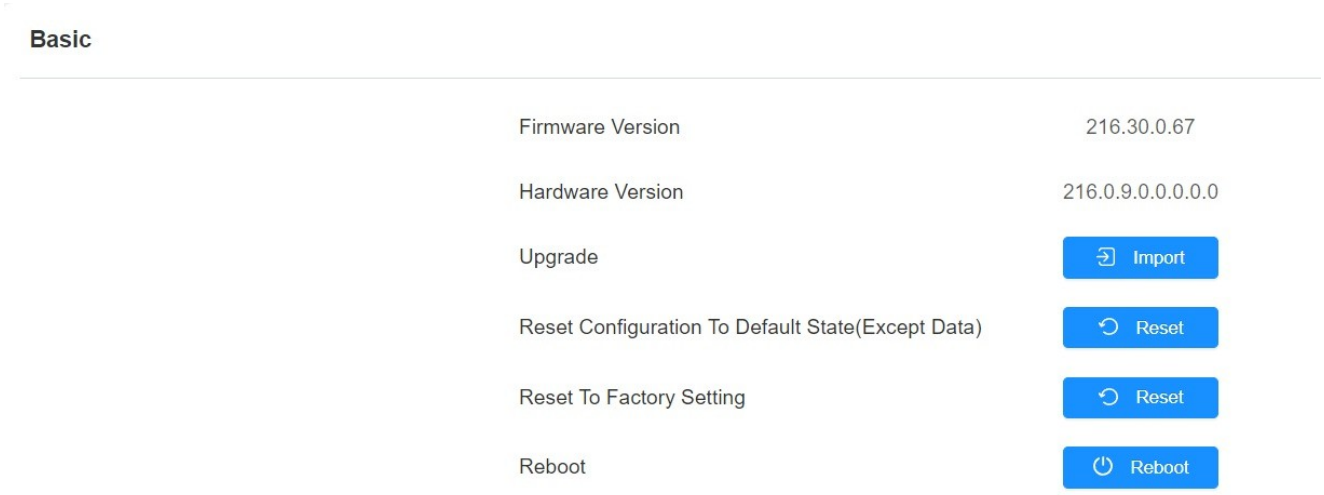
Konfiguracja parametrów :

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

Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można zaktualizować w interfejsie internetowym urządzenia.

Możesz przejść do **System > Aktualizacja** .



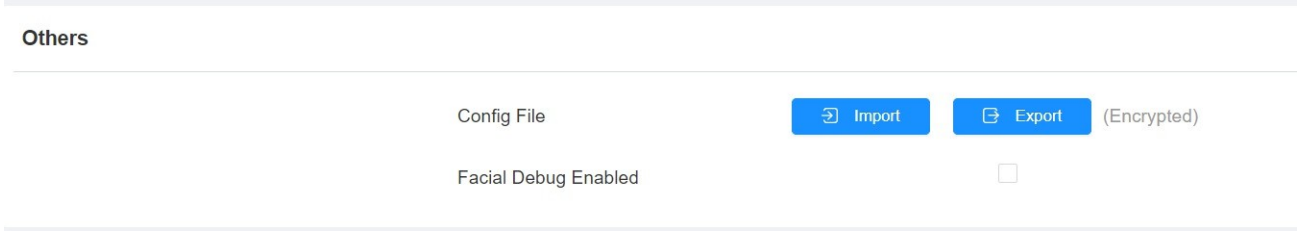
Uwaga

- Pliki oprogramowania układowego powinny być w formacie .zip do aktualizacji.

Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować

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



Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

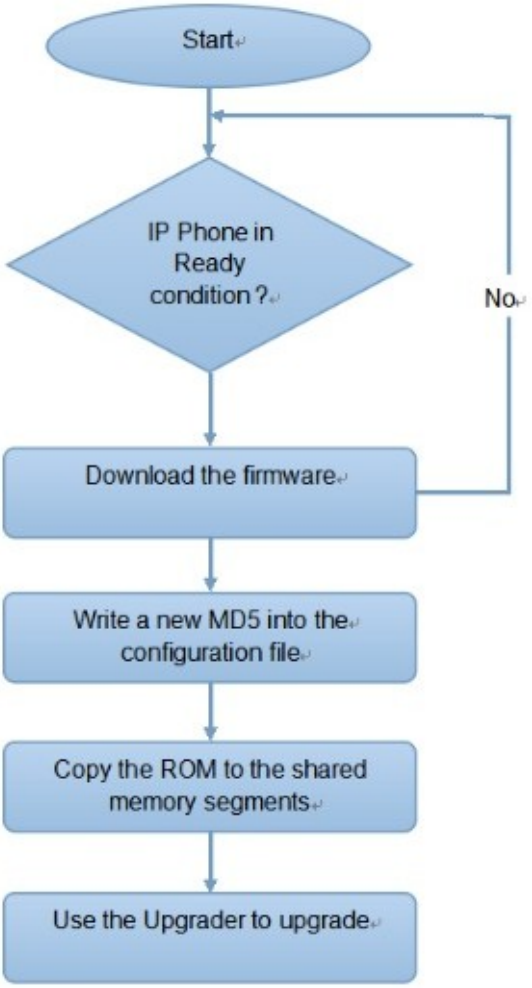
Bramofon można skonfigurować i zaktualizować w interfejsie internetowym za pomocą jednorazowego automatycznego udostępniania i zaplanowanego automatycznego udostępniania za pomocą plików konfiguracyjnych, co pozwala uniknąć konieczności ręcznego konfigurowania poszczególnych ustawień w bramofonie.

Zasada udostępniania

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

urządzeniu.

Zobacz poniższy schemat blokowy:



Pliki konfiguracyjne dla automatycznego przydzielania

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

Poniżej przedstawiono różnicę między tymi dwoma typami plików konfiguracyjnych:

- **Udostępnianie konfiguracji ogólnej**: plik ogólny jest przechowywany na serwerze, z którego wszystkie powiązane urządzenia będą mogły pobrać ten sam plik konfiguracyjny w celu aktualizacji parametrów na urządzeniach, takich jak cfg.

- **Udostępnianie konfiguracji opartej na MAC**: Pliki konfiguracyjne oparte na MAC są używane do automatycznego udostępniania na określonym urządzeniu, zgodnie z jego unikalnym numerem MAC. Pliki konfiguracyjne nazwane za pomocą numeru MAC urządzenia zostaną automatycznie dopasowane do numeru MAC urządzenia przed pobraniem w celu udostępnienia na określonym urządzeniu.

Uwaga

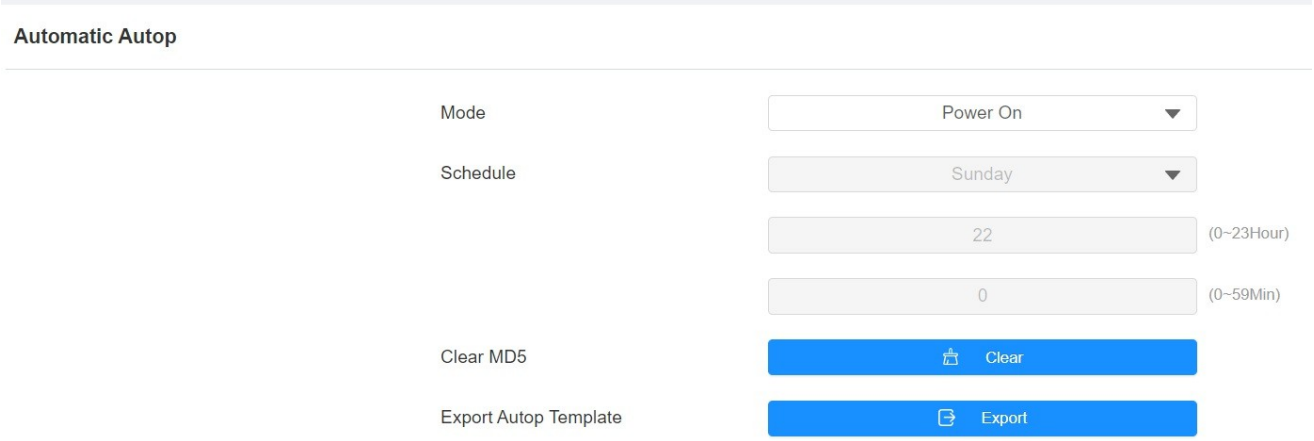
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny udostępniania wsadowego różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC dla określonego udostępniania urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer posiada te dwa typy plików konfiguracyjnych,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

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

Harmonogram AutoP

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

Możesz przejść do **System > Auto Provisioning > Automatic Autop** .



Konfiguracja parametrów:

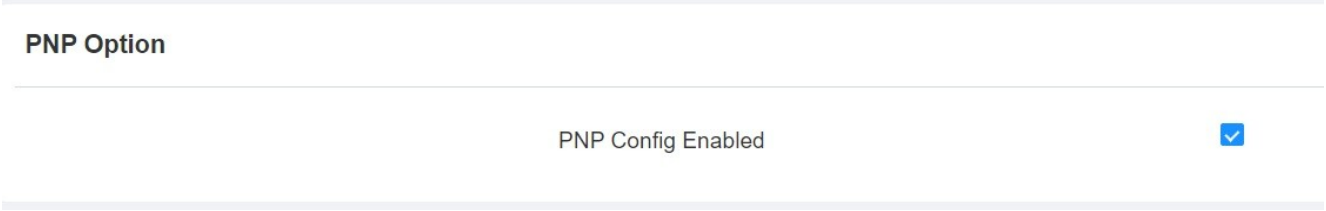
- **Power On**: wybierz **Power on**, jeśli chcesz, aby urządzenie wykonywało Autop przy każdym uruchomieniu.
- **Wielokrotnie**: wybierz opcję **Wielokrotnie**, jeśli chcesz, aby urządzenie wykonywało funkcję Autop zgodnie z ustawionym harmonogramem.
- **Power On + Repeatedly**: wybierz **Power On + 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

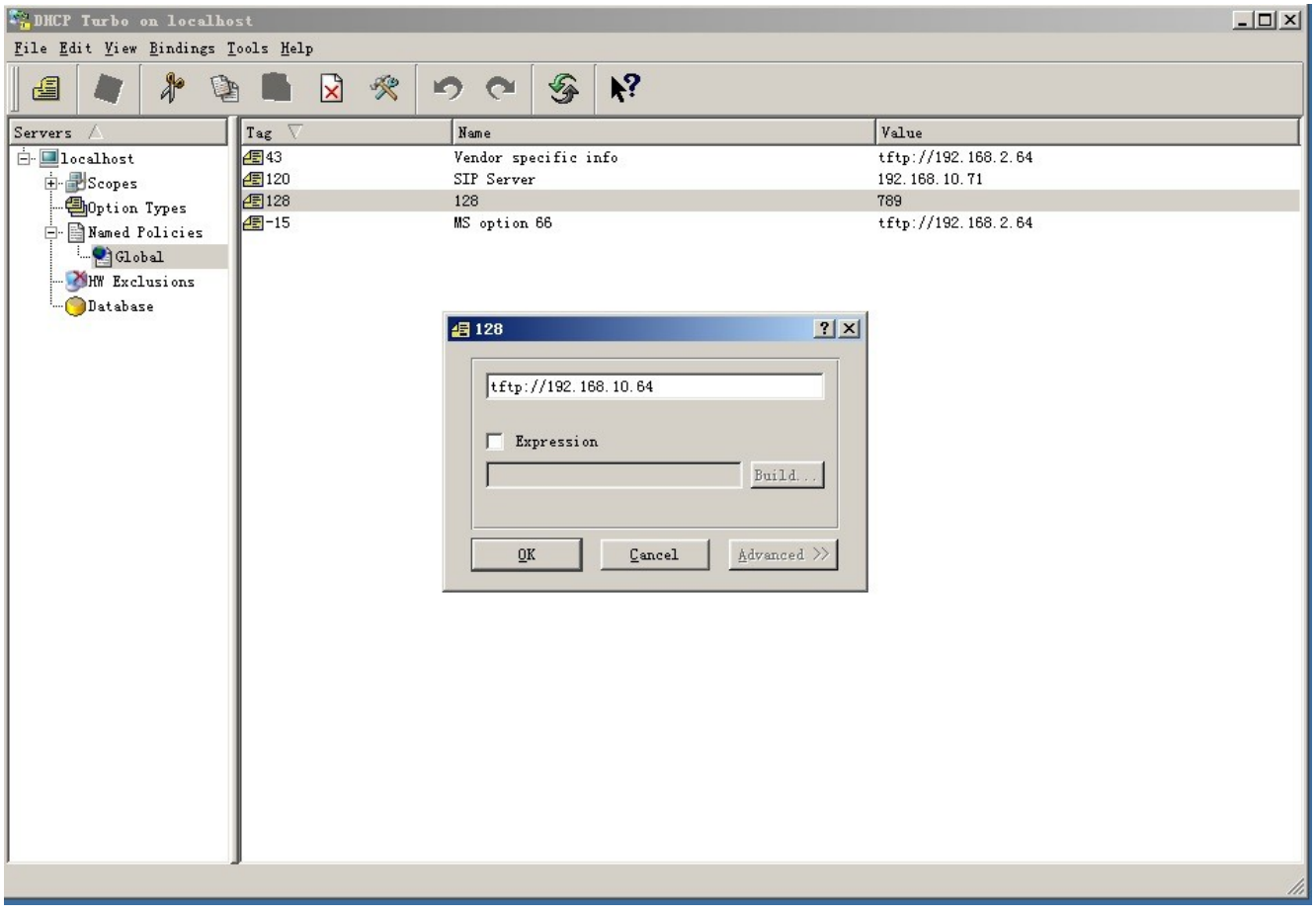
Plug and Play (PNP) to połączenie wsparcia sprzętowego i programowego, które umożliwia systemowi komputerowemu rozpoznawanie i dostosowywanie się do zmian konfiguracji sprzętowej przy niewielkiej lub żadnej interwencji użytkownika.

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

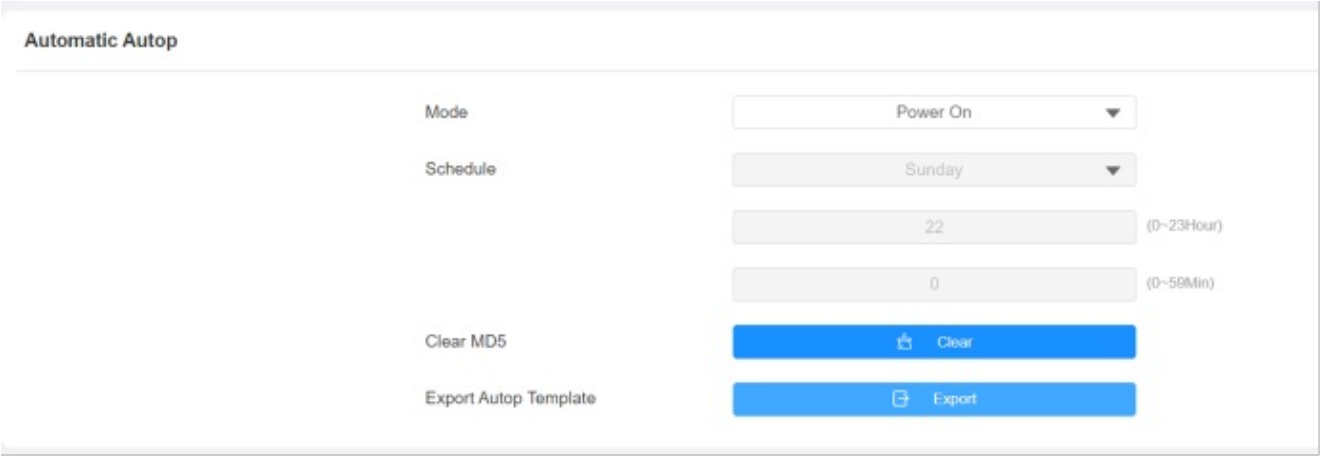


Konfiguracja udostępniania DHCP

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.



Aby skonfigurować DHCP AutoP z "opcją niestandardową" i trybem "Power on", w interfejsie **System > Auto Provisioning > Automatic Autop.** Kliknij zakładkę **Eksportuj** w **Eksportuj szablon Autop**, aby wyeksportować szablon Autop. Następnie skonfiguruj opcję DHCP na



Uwaga

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

Konfiguracja parametrów:

- **Opcja niestandardowa:** wprowadź kod DHCP pasujący do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych do 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 zaktualizowanym adresem URL serwera.
- **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 zaktualizowanym adresem URL serwera.

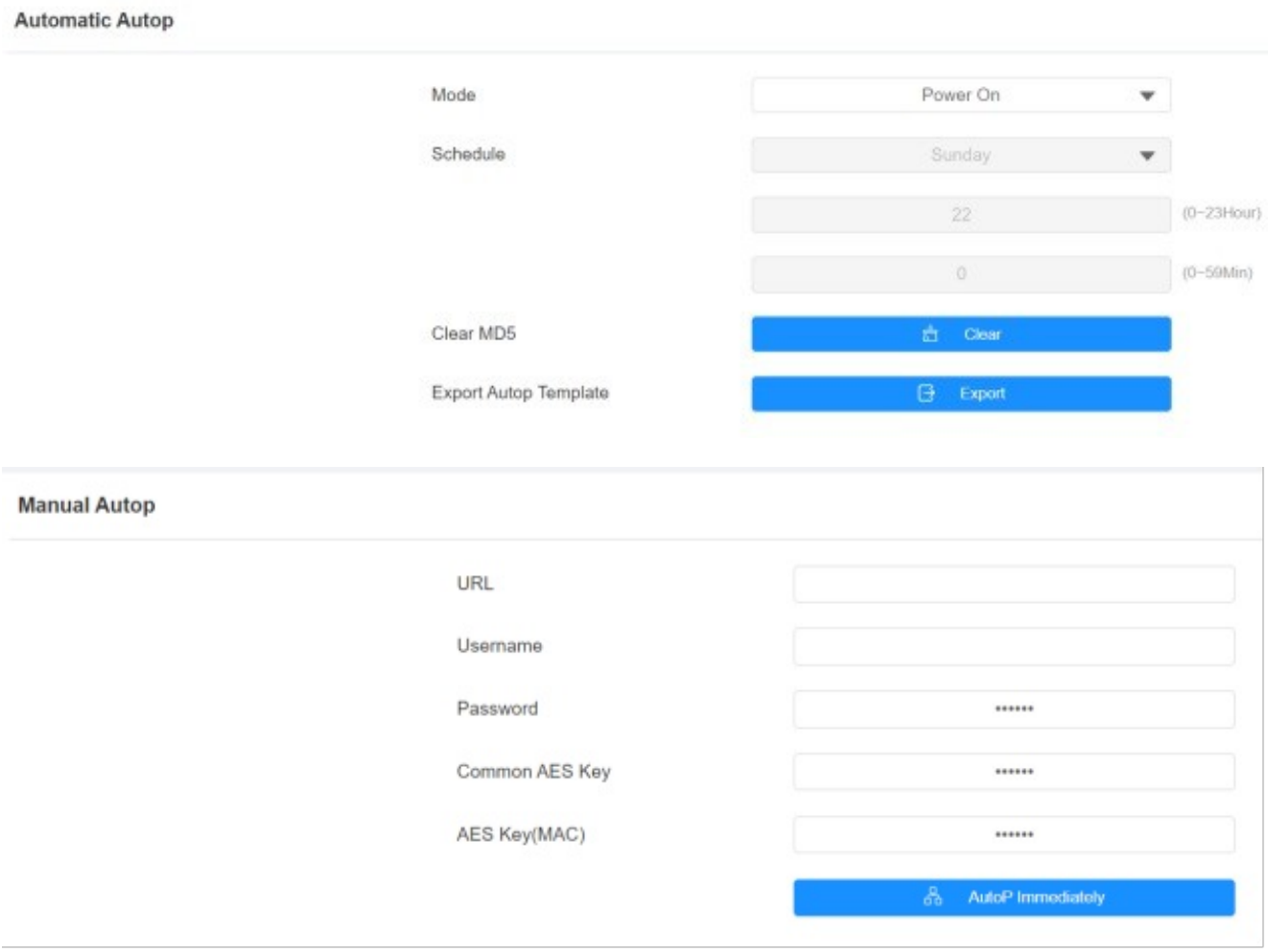
Uwaga

- Ogólny plik konfiguracyjny dla udostępniania wsadowego ma format **rcfg**
  Biorąc E16 jako przykład r000000000116.cfg (w sumie 9 zer, podczas gdy plik konfiguracyjny oparty na MAC dla konkretnego udostępniania urządzenia ma format MAC_Address urządzenia.cfg), na przykład **0C 110504AE5B.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 adresy serwerów TFTP, HTTP, HTTPS i FTP dla provisioningu.
- **User Name** : ustaw nazwę użytkownika, jeśli serwer wymaga nazwy użytkownika, aby uzyskać do niego dostęp.
  Hasło: ustaw hasło, jeśli serwer wymaga hasła dostępu, w przeciwnym razie pozostaw je.
- **Wspólny klucz AES**: ustawienie kodu AES dla interkomu w celu odszyfrowania ogólnego Auto

Udostępnianie plików konfiguracyjnych.

- **Klucz AES (MAC)**: ustawienie kodu AES dla interkomu w celu odszyfrowania pliku konfiguracyjnego automatycznego provisioningu opartego na MAC.

Wskazów

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

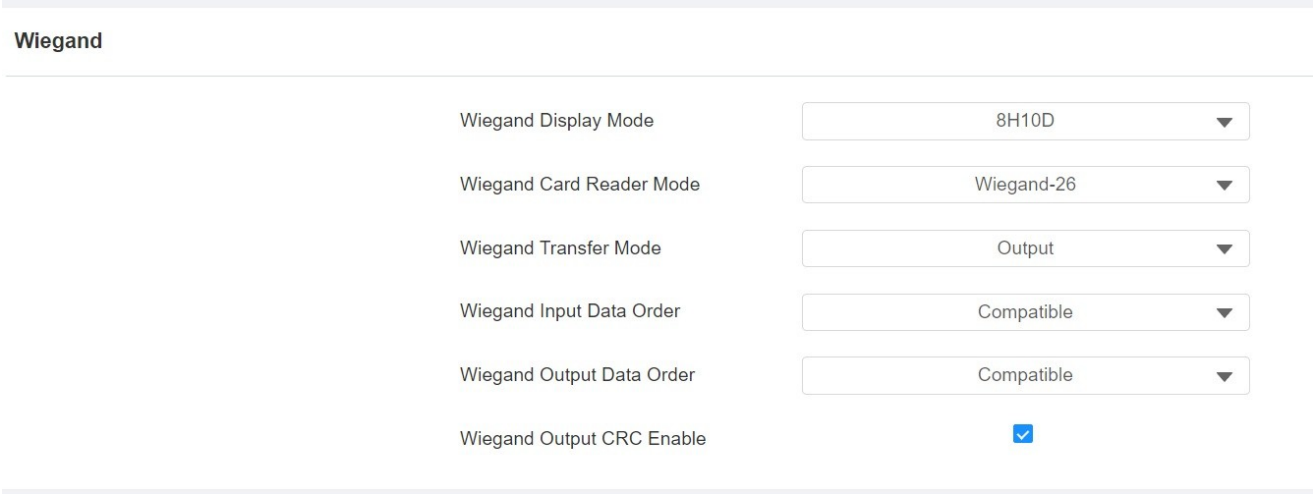
Uwaga

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

Integracja z urządzeniami innych firm

Integracja przez Wiegand

Funkcja Wiegand umożliwia bramofonowi Akuvox działanie jako kontroler lub czytnik kart. Aby ją skonfigurować, można przejść do interfejsu Web **Device > Wiegand.**



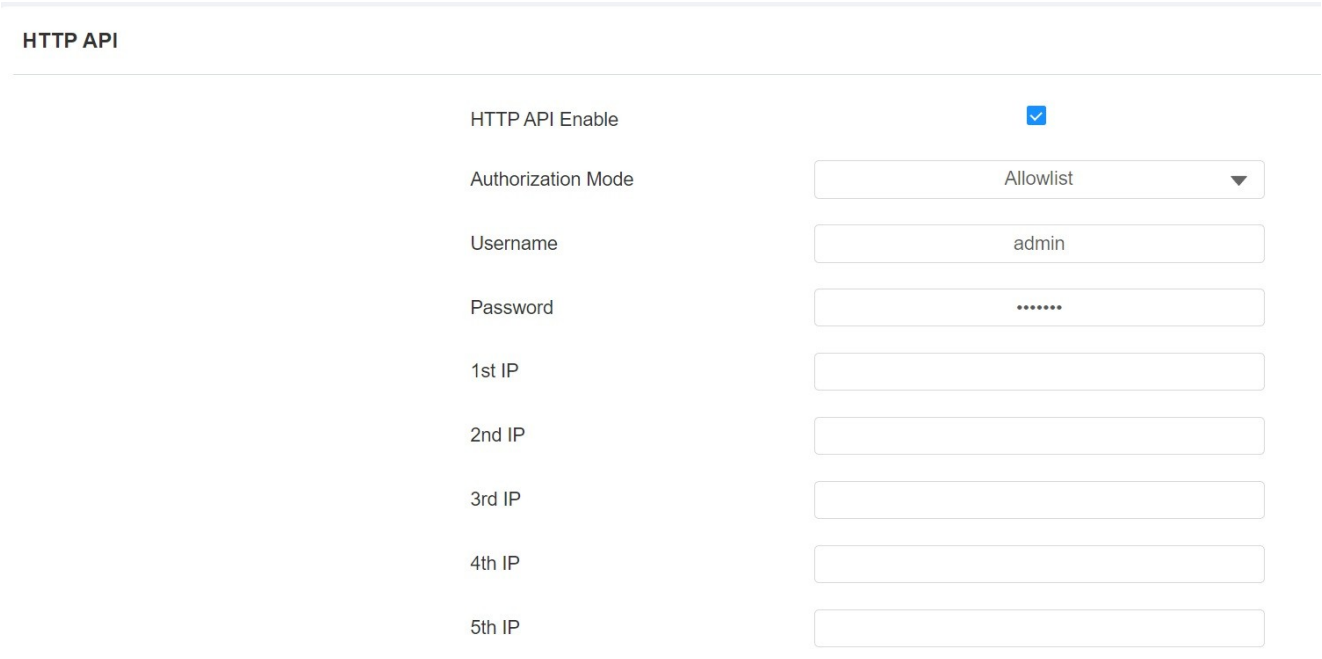
Konfiguracja parametrów:

- **Tryb wyświetlania** Wiegand: wybór formatu kodu karty Wiegand 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, Wiegand 58** . Format transmisji powinien być identyczny między bramofonem a urządzeniem, które ma zostać zintegrowane.
- **Tryb transferu Wiegand**: ustaw tryb transferu między **wejściem, wyjściem** lub **konwersją na kartę NO.Output,** jeśli bramofon jest używany jako odbiornik, ustaw go jako **wejście** dla bramofonu i odwrotnie.
- **Kolejność danych wejściowych** Wiegand: ustawia kolejność danych wejściowych Wiegand między **Domyślną** a **Zgodną**, jeśli wybierzesz **Zgodną**, numer karty wejściowej zostanie odwrócony i odwrotnie.
- **Kolejność danych wyjściowych** Wiegand: ustawienie kolejności danych wyjściowych Wiegand pomiędzy **Domyślna** i **Zgodna**. W przypadku wybrania opcji **Compatible** numer karty wejściowej zostanie odwrócony i odwrotnie.
- **Wiegand Output CRC**: ta funkcja służy do kontroli danych Wiegand. Jest ona domyślnie włączona. Jeśli nie jest włączona, integracja urządzenia z urządzeniami innych firm może być niemożliwa.

Integracja przez HTTP API

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

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



Konfiguracja parametrów:

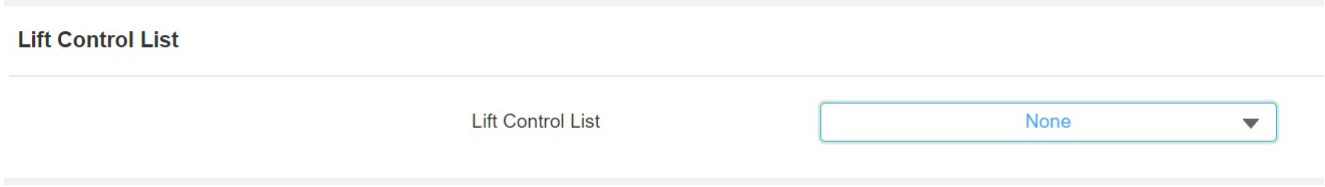
- **HTTP API Enable** : HTTP API Włącza lub wyłącza funkcję HTTP API dla integracji z innymi firmami. Na przykład, jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwrócony zostanie status HTTP 403 forbidden.
- **Tryb autoryzacji**: wybierz jedną z pięciu opcji: **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.** Domyślna nazwa użytkownika to Admin.
- **Hasło** : wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic** i **Digest.** Domyślna nazwa użytkownika to Admin.
- **1stIP- 5th IP** : wprowadź adres IP urządzeń innych firm, gdy dla integracji wybrano autoryzację WhiteList.

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 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**.



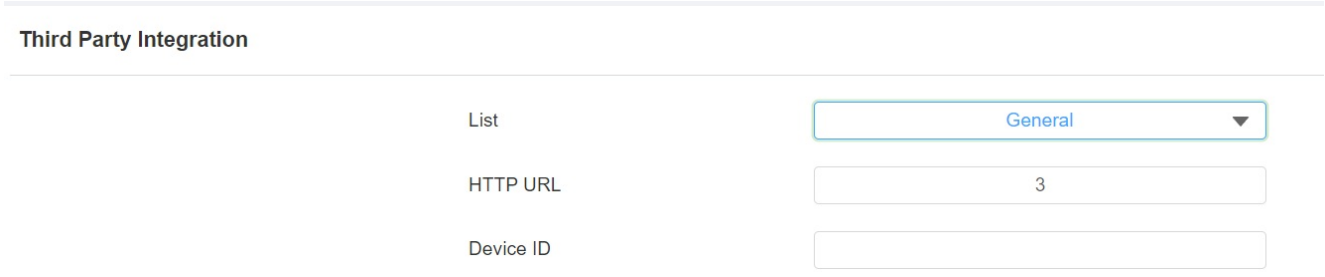
Konfiguracja parametrów :

- **Lift Control List**: wybór trybu integracji spośród siedmiu opcji: **Brak, 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 integracyjna między bramofonem serii E16 a urządzeniem innej firmy odbywa się za pośrednictwem protokołu OSDP. Jeśli chcesz zintegrować się z kontrolerem windy KEYKING, musisz sprawdzić protokół integracji urządzeń i upewnić się, że używają one tego samego protokołu integracji.
3	**Akuvox EC 32**	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 z zewnętrznym serwerem kontroli dostępu

Dostęp do bramofonu można uzyskać za pomocą kodu QR lub karty dostępu wygenerowanej przez serwer innej firmy. Na przykład, gdy użyjesz kodu QR na bramofonie, kod QR zostanie wysłany do serwera strony trzeciej w celu weryfikacji. Dostęp zostanie przyznany, jeśli kod QR pomyślnie przejdzie weryfikację. Aby to skonfigurować, można przejść do opcji **Access Control > Relay > Third Party Integration**.



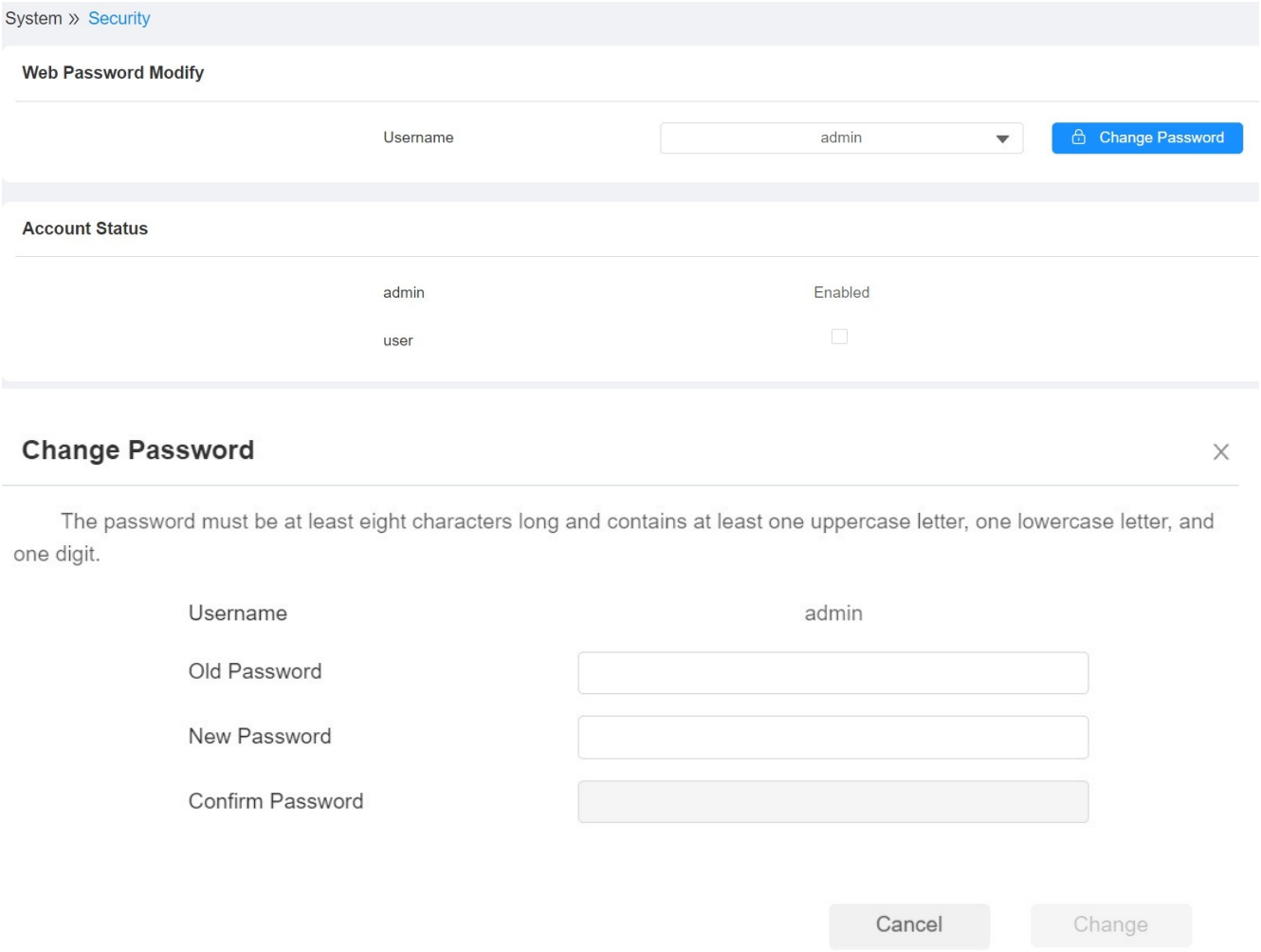
Konfiguracja parametrów:

- **Lista**: wybór trybów integracji.
    - Jeśli chcesz wyłączyć tę funkcję, wybierz
    - **None** . Jeśli chcesz używać tylko kodu QR, wybierz opcję **Ogólne.**
    - Jeśli chcesz wybrać między kodem QR a kartą dostępu z dostosowanymi funkcjami, wybierz opcję **Dostosuj** .
- **HTTP URL** :
    - W przypadku trybu ogólnego: wprowadź format polecenia HTTP dostarczony przez zewnętrznego dostawcę usług. Po zeskanowaniu kodu QR polecenie HTTP automatycznie przeniesie dynamiczne informacje o kodzie QR, zanim zostaną one wysłane do serwera kodów QR w celu weryfikacji. Zobacz poniższy przykład: http:// wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode} &deviceId= {DeviceID}
    - Tryb dostosowywania: wybierz kod QR lub weryfikację karty.
    - W celu weryfikacji kodu QR: wprowadź polecenie HTTP kodu QR dostarczone przez zewnętrznego dostawcę usług. Zobacz poniższy przykład: /hs/ACS/checking/QR">http://www.server.com//hs/ACS/checking/QRCode/{DeviceID}/{Card}
      W przypadku weryfikacji karty: wprowadź polecenie HTTP karty dostępu dostarczone przez zewnętrznego dostawcę usług. Zobacz przykład poniżej: http://www.server.com//hs/ACS/checking/{QRCode}/{DeviceID}/Card
- **Prompt On LCD (Monit na wyświetlaczu LCD)**: wybierz **Default (Domyślne)**, jeśli chcesz przyjąć monit bramofonu Akuvox dla dostępu do drzwi. Wybierz **Return** value (Wartość zwrotna), jeśli chcesz użyć wartości zwrotnej z serwera zewnętrznego jako monitu.
- **Weryfikacja zdalna**: wybierz **kod QR** lub weryfikację **kartą.**
- **Identyfikator urządzenia** : wprowadź identyfikator urządzenia, który zostanie automatycznie dodany do polecenia HTTP w przypadku użycia kodu QR lub karty dostępu.

Modyfikacja hasła

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.

Aby ustawić hasło, przejdź do opcji **System > Security > Web Password Modify**



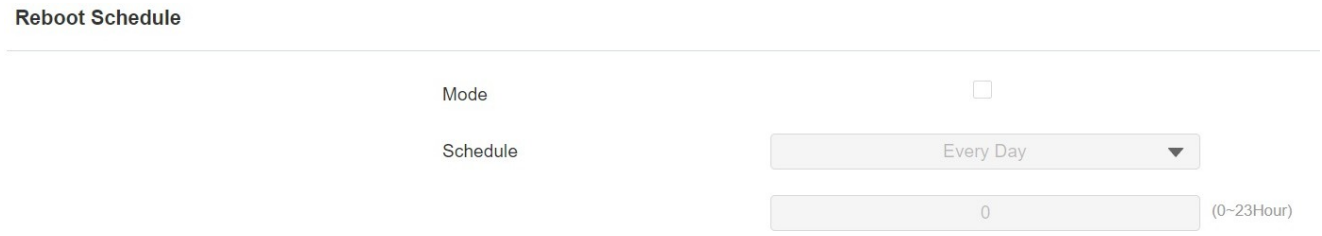
Aby skonfigurować systemowy kod PIN, można przejść do sekcji **systemowego kodu PIN.**

Ponowne uruchamianie i resetowanie systemu

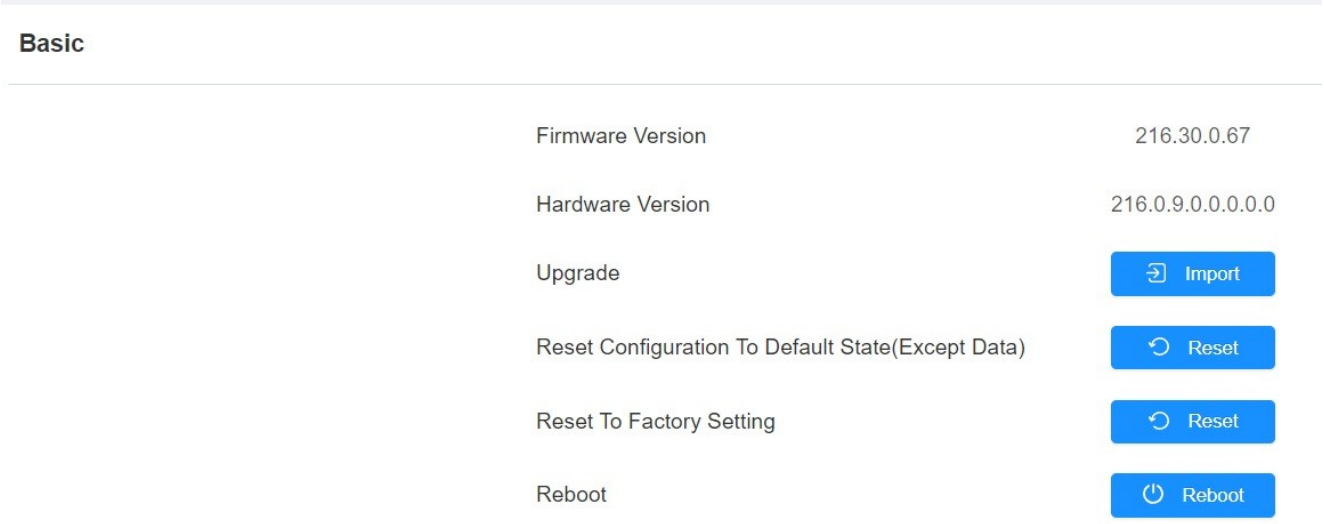
Reboot

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

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



Aby zrestartować urządzenie ręcznie, przejdź do **System > Aktualizacja > Podstawowe** .

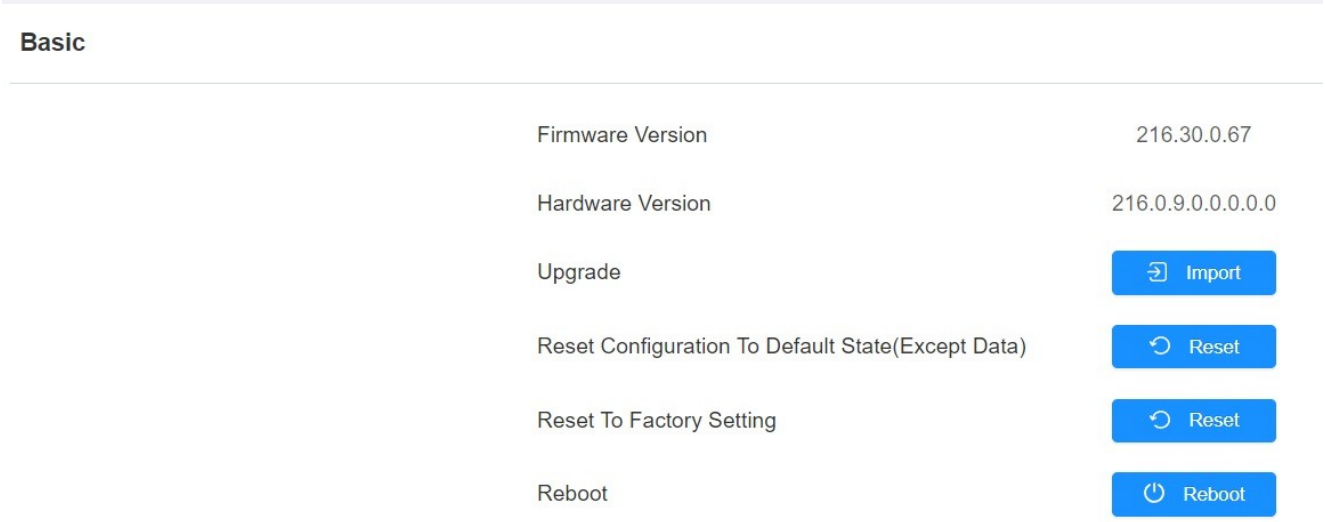


Aby ponownie uruchomić urządzenie, stuknij kolejno opcje **Zaawansowane > Uruchom ponownie.**

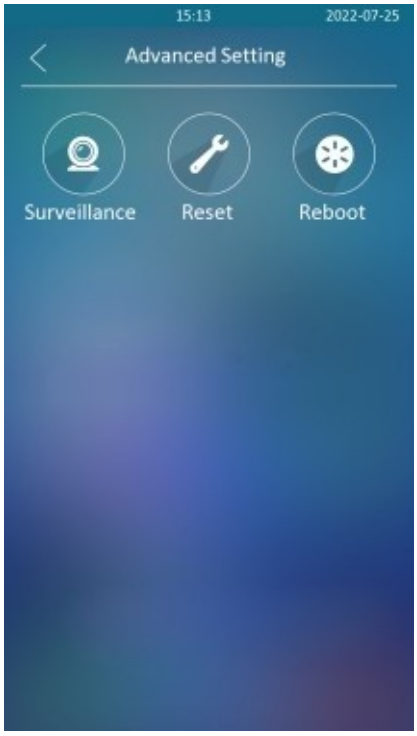
Reset

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).

Aby zresetować urządzenie, przejdź do **System > Aktualizacja** .



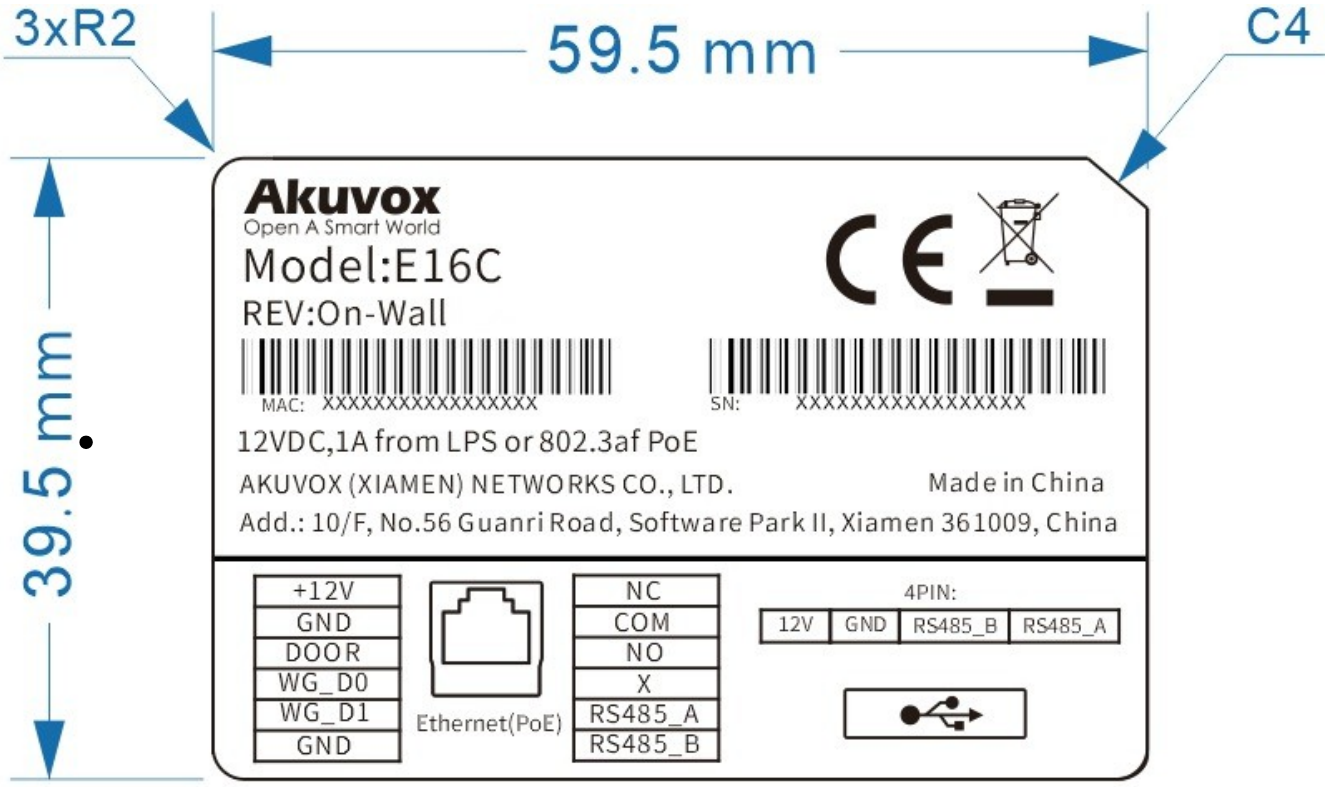
Aby zresetować urządzenie do ustawień fabrycznych, przejdź do opcji **Zaawansowane > Resetuj**.



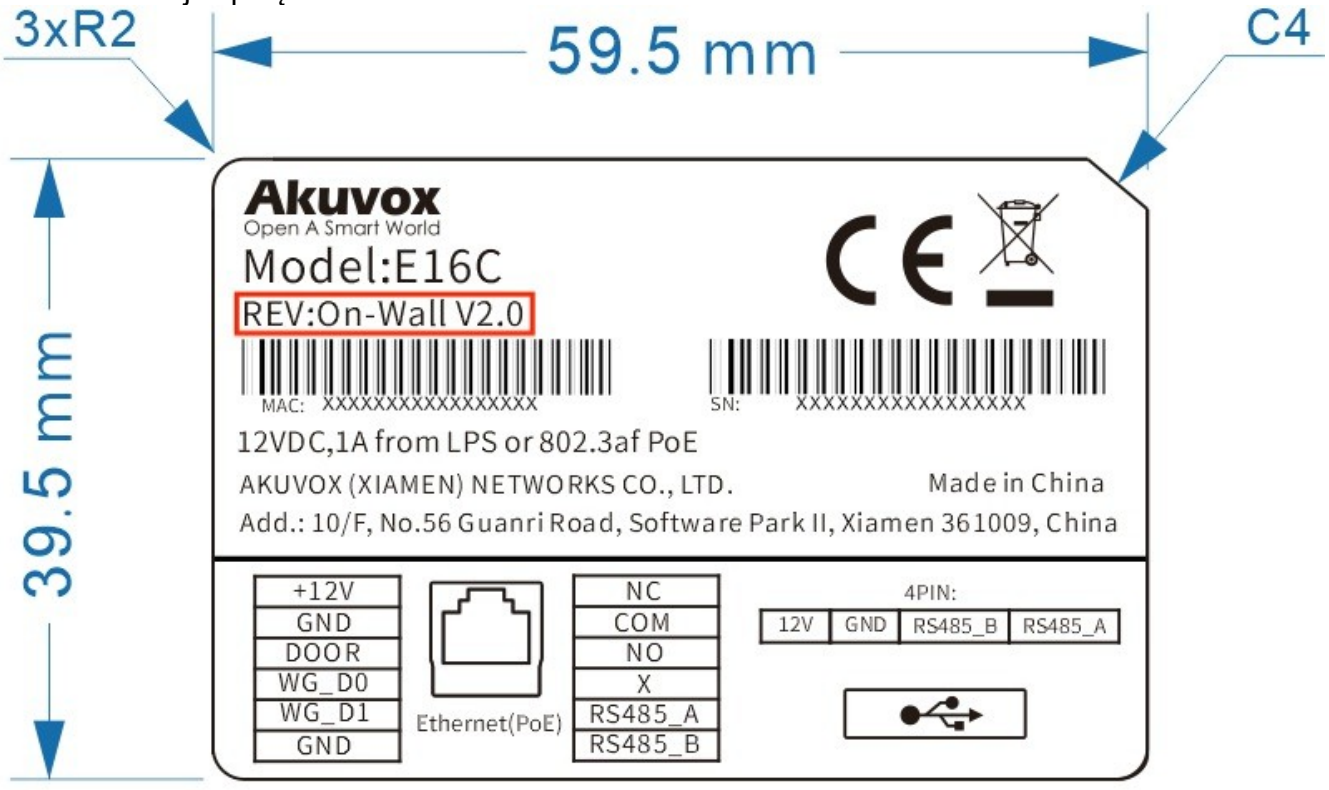
FAQ

P: Jak potwierdzić, czy moje urządzenie jest wersją sprzętową 1 czy wersją sprzętową 2? O: 1. Etykieta

- Wersja sprzętowa 1



Wersja sprzętowa 2



- Wersja oprogramowania sprzętowego

Oprogramowanie sprzętowe różni się między wersją sprzętu1 i wersją sprzętu2. Przejdź do **Web > Status > Firmware Version**
116.X.X.X to wersja sprzętu1.

216.X.X.X to wersja sprzętu2.

- Wersja sprzętowa

Oprogramowanie sprzętowe różni się między wersją sprzętu 1 i wersją

sprzętu 2. Przejdź do **Web > Status > Firmware Version**

Jeśli wersja sprzętowa to 216.X, urządzenie jest w wersji sprzętowej 2.