

## Informacje o niniejszej instrukcji



[WWW.AKUVOX.COM](http://WWW.AKUVOX.COM)



# S539 DOOR PHONE Admin Guide

Dziękujemy za wybranie bramofonu Akuvox z serii S539. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy wersji 539.30.10.6 i zawiera wszystkie konfiguracje funkcji i właściwości bramofonu serii S539. W celu uzyskania nowych informacji lub najnowszego oprogramowania sprzętowego należy odwiedzić forum Akuvox lub skontaktować się z pomocą techniczną.

## Przegląd produktów

Produkty z serii Akuvox S539 to oparte na systemie Android wideodomofony IP z ekranami dotykowymi. Obejmują one komunikację audio i wideo, kontrolę dostępu i nadzór wideo. Precyzyjnie dostrojony system operacyjny Android, chmura i technologia komunikacji oparta na sztucznej inteligencji pozwalają na lepsze dostosowanie do potrzeb użytkownika. Wiele portów serii S539, takich jak RS485 i Wiegand, można wykorzystać do łatwej integracji zewnętrznych systemów cyfrowych, takich jak kontrolery wind i czujniki alarmu przeciwpożarowego, pomagając w stworzeniu całościowej kontroli wejścia do budynku i jego otoczenia oraz dając duże poczucie bezpieczeństwa dzięki różnorodnym dostępom, takim jak dostęp kartą, NFC, Bluetooth, kod QR i nowo dodany dostęp do drzwi sterowany głosem w połączeniu z pomiarem temperatury ciała. Bramofony z serii S539 mają zastosowanie w budynkach mieszkalnych, biurowych i ich kompleksach.

## Specyfikacja modelu

Model	S539
Ekran dotykowy	✓
Wejście przekaźnika	3
Wyjście przekaźnika	3
Alarm wł.	X
RS485	✓
Czytnik kart	13,56 MHZ I 125 KHZ
Wi-Fi	X
Bluetooth	✓
Wykrywanie temperatury	Opcjonalnie
Rozpoznawanie twarzy	✓
LTE	X
USB	X
Zewnętrzna karta SD	X

# Wprowadzenie do menu konfiguracji

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

- HomePage
- Status
- Account
- Network
- Intercom
- Surveillance
- Access Control
- Directory
- Device
- Setting
- System

Status» [Info](#)

### Product Information

Model	S539
MAC Address	██████████
Firmware Version	539.30.10.6
Hardware Version	539.1.0.0
Server Mode	Cloud
Location	S539
Uptime	Up 0 Weeks, 0 Days, 0 Hours, 1 Minute

### Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.111
Subnet Mask	255.255.255.0

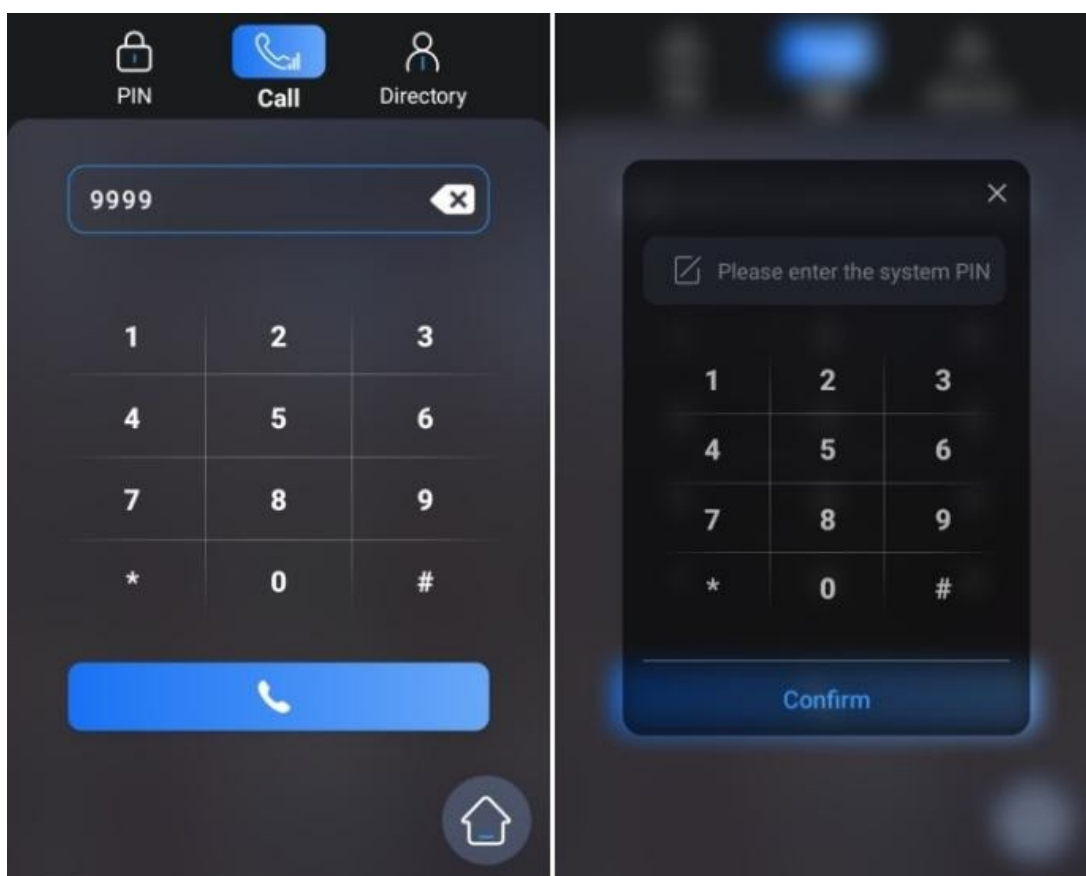
## Dostęp do urządzenia

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

### Dostęp do ustawień urządzenia na urządzeniu

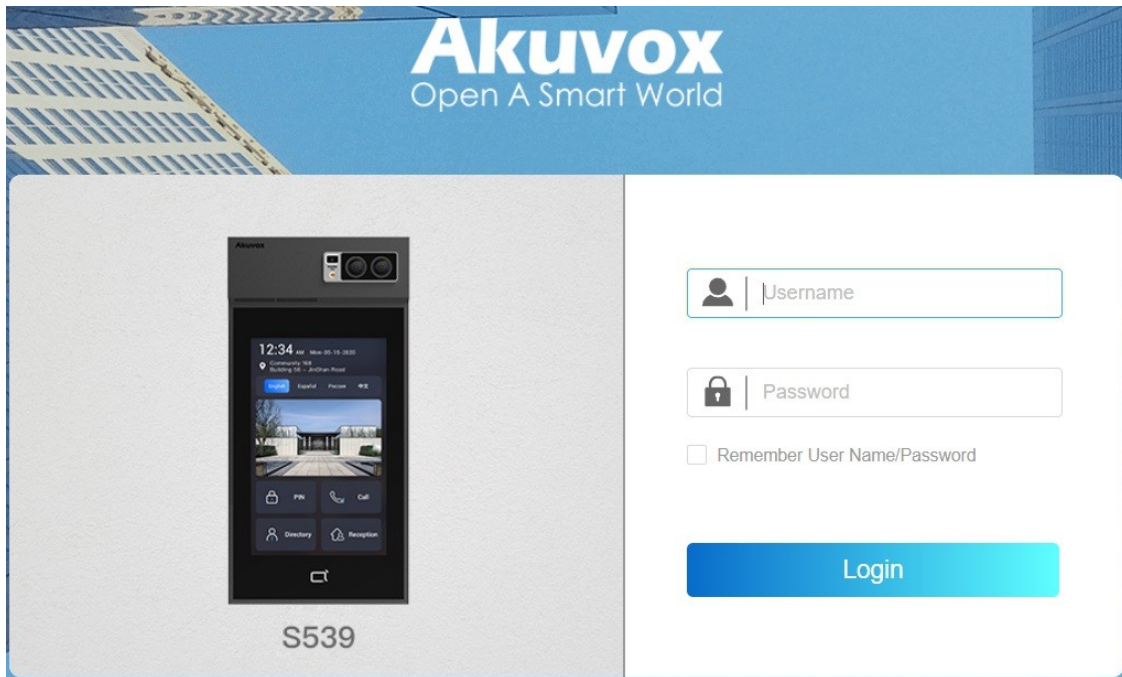
Przed konfiguracją bramofonu należy upewnić się, że urządzenie jest prawidłowo zainstalowane i podłączone do normalnej sieci.

Na ekranie urządzenia można skonfigurować podstawowe ustawienia, naciskając **9999** + **przycisk wybierania** + **3888** (hasło) na ekranie **wyberania**.



### Dostęp do ustawień urządzenia w interfejsie sieciowym

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



## Uwaga

- Adres IP urządzenia można uzyskać za pomocą skanera Akuvox IP w celu zalogowania się do urządzenia.
- Aby pobrać:  
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- Szczegółowy przewodnik:  
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Zdecydowanie zalecana jest przeglądarka Google Chrome.
- Początkowa nazwa użytkownika i hasło to **admin** i należy zwracać uwagę na wielkość liter we wprowadzanych nazwach użytkowników i hasłach.

# Ustawienia języka i czasu

## Ustawienia języka

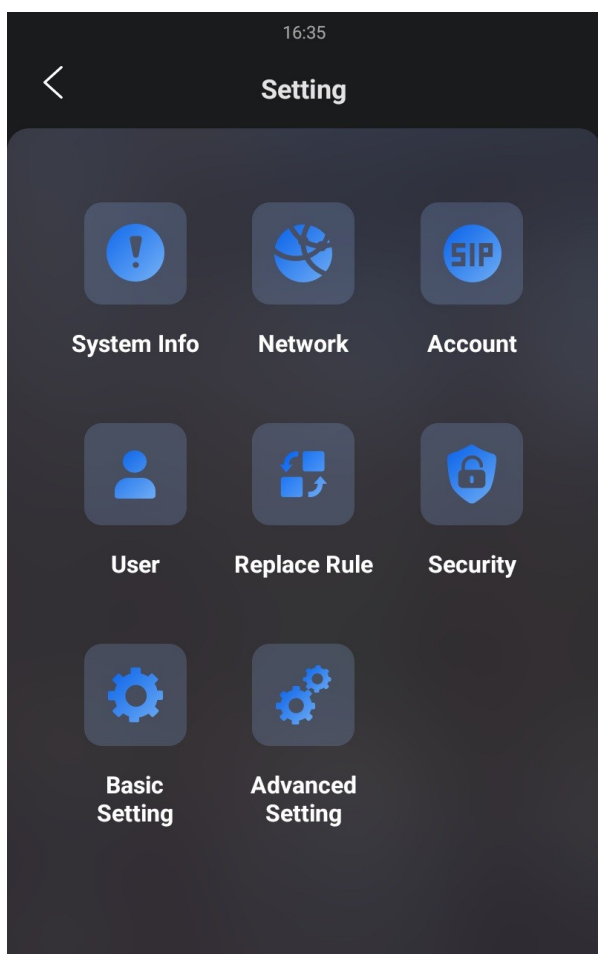
Ustaw język podczas początkowej konfiguracji urządzenia lub później za pomocą urządzenia lub interfejsu internetowego zgodnie z własnymi preferencjami.

## Ustawienia języka na urządzeniu

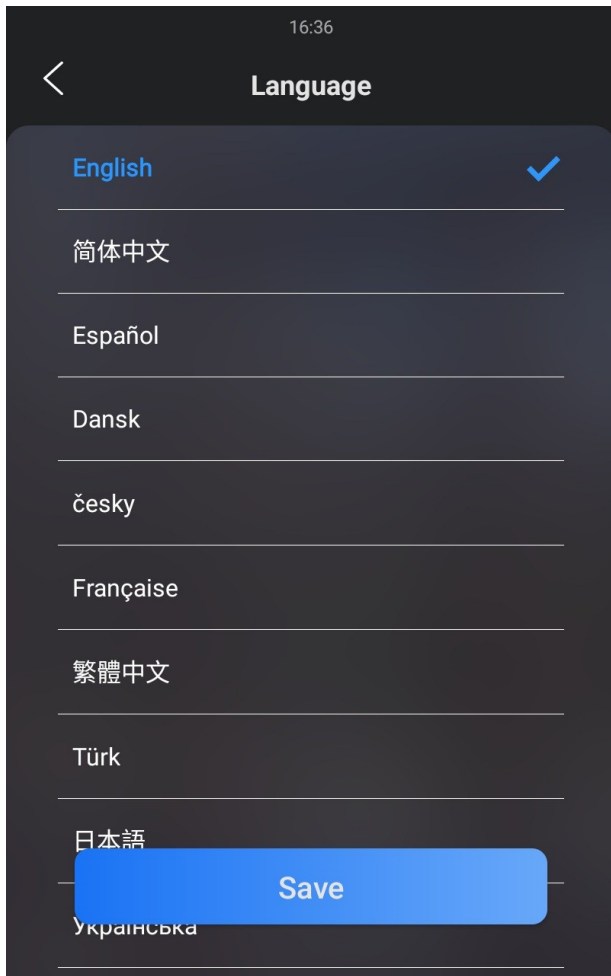
Aby skonfigurować język wyświetlany na urządzeniu, wybierz kolejno opcje

**Ustawienia podstawowe > Język** interfejsu. Urządzenie obsługuje następujące języki:

- Chiński uproszczony, angielski, hiszpański, duński, czeski, francuski, chiński tradycyjny, turecki, niemiecki, japoński, ukraiński, koreański, norweski, holenderski i rosyjski.



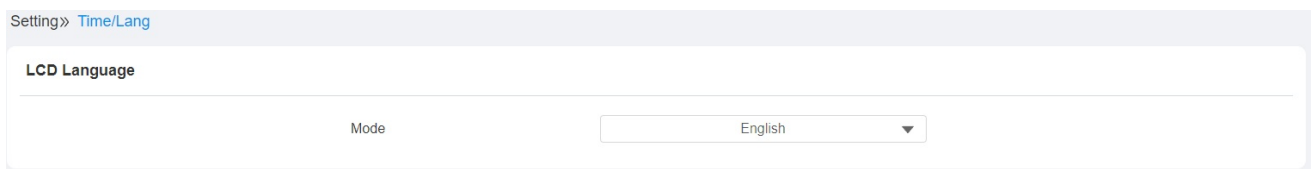




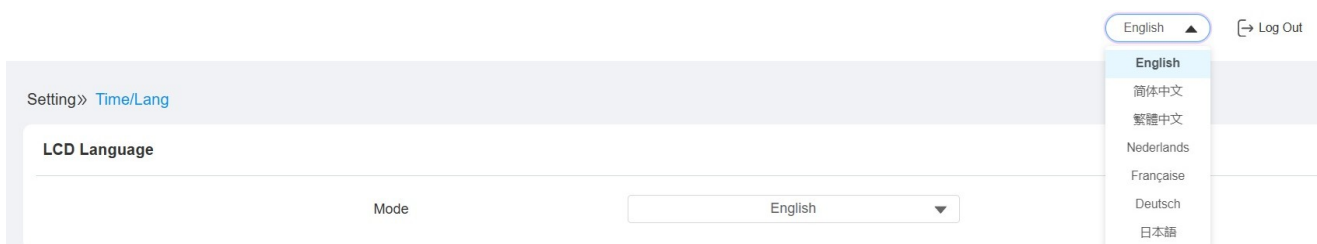
## Ustawienia języka w interfejsie internetowym urządzenia

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

Aby wybrać język urządzenia, przejdź do opcji **Setting > Time/Lang > LCD Language** interface.



Język internetowy można wybrać w prawym górnym rogu.



Aby dostosować język, należy wyeksportować i edytować plik .json przed przesłaniem pliku do urządzenia. Ścieżka: **Ustawienia > Czas/Język** .

Custom Language					
Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	Import	Export	Reset

Aby utworzyć ikony języka dla trybu **budynku**, przejdź do opcji **Ustawienia > Klawisze/Wyświetlacz > Ustawienia języka motywu budynku** .

Language Setting Of The Building Theme

Show

1st Language	2nd Language	3rd Language	4th Language
English ▼	Español ▼	Français ▼	简体中文 ▼

### Uwaga

- Należy najpierw wybrać tryb budowania lub tryb uwierzytelniania wieloskładnikowego, zanim można ustawić dla nich ikonę języka na ekranie głównym.

Aby utworzyć ikony językowe dla trybu uwierzytelniania **wieloskładnikowego**, przejdź do **Ustawienia > Klucz/Wyświetlacz > Ustawienia języka motywu uwierzytelniania wieloskładnikowego** .

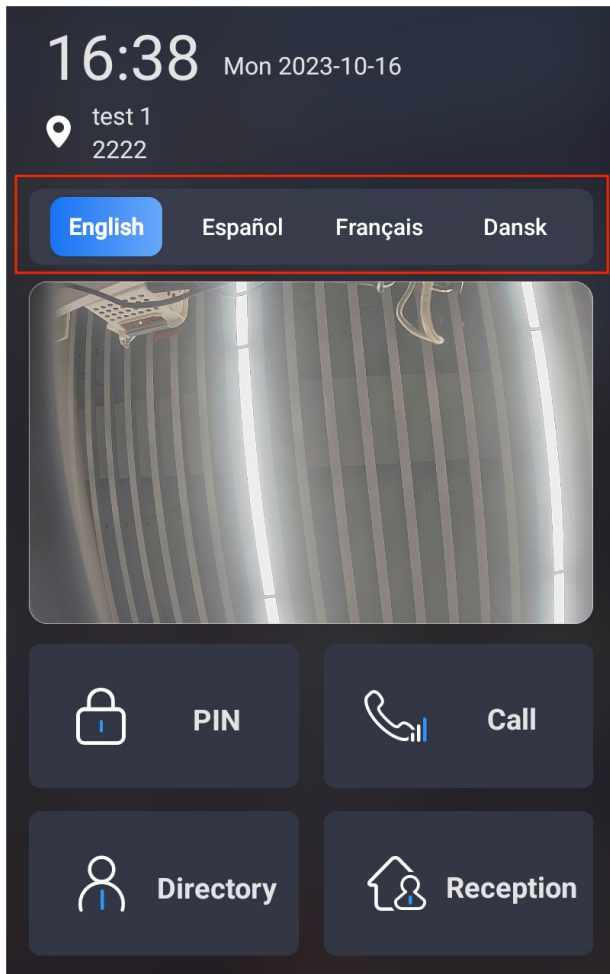
Language Setting of Multi-factor Authentication Theme

Show

1st Language	2nd Language	3rd Language	4th Language
English ▼	Español ▼	Français ▼	简体中文 ▼

### Konfiguracja parametrów :

- Widoczny** : włącz, jeśli chcesz, aby cztery ikony języka były wyświetlane na ekranie głównym w celu wyboru języka.
- Język 1/2/3/4** : wybór kolejności wyświetlania języka. Na przykład po ustawieniu pierwszego języka jako angielski, język angielski będzie wyświetlany jako pierwszy od lewej do prawej na ekranie.

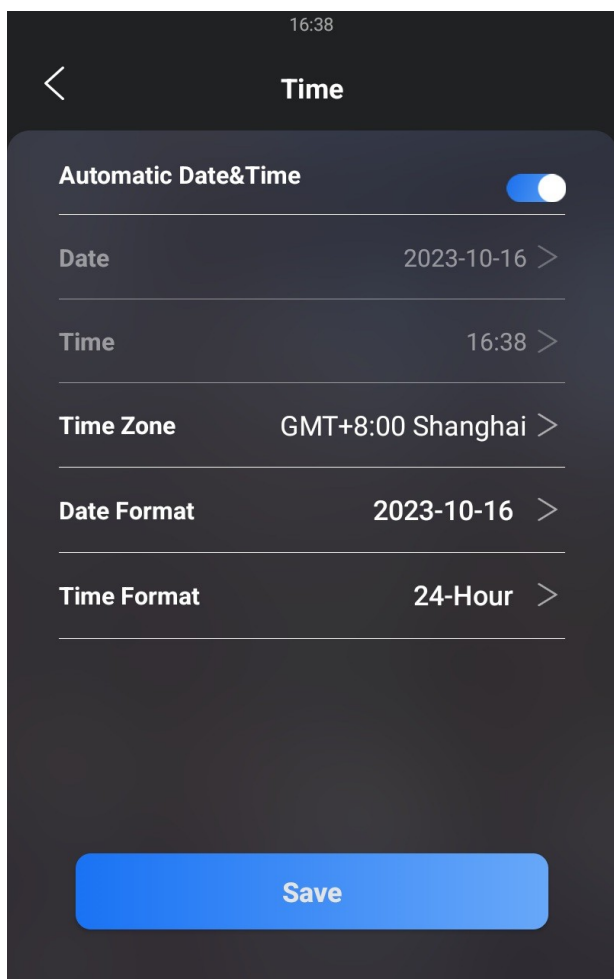


## Ustawienie czasu

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

## Ustawienie czasu na urządzeniu

Aby skonfigurować język wyświetlania na urządzeniu, wybierz kolejno opcje **Ustawienia podstawowe > Interfejs czasu**.



### Konfiguracja parametrów :

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

#### Uwaga

- Gdy przełącznik Automatic Date&Time jest wyłączony, parametry związane z serwerem NTP nie będą edytowalne. A gdy przełącznik jest włączony, edycja czasu i daty będzie zabroniona.

## Ustawienia czasu w interfejsie internetowym urządzenia

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

Aby skonfigurować konfigurację w interfejsie sieci Web **Setting >Time/Lang > Time**.

---

Time

---

Automatic Date&Time	<input checked="" type="checkbox"/>
Time Zone	GMT+8:00 Shanghai ▼
Date Format	2023-10-16 ▼
Time Format	24Hour ▼
NTP Server	pool.ntp.org

---

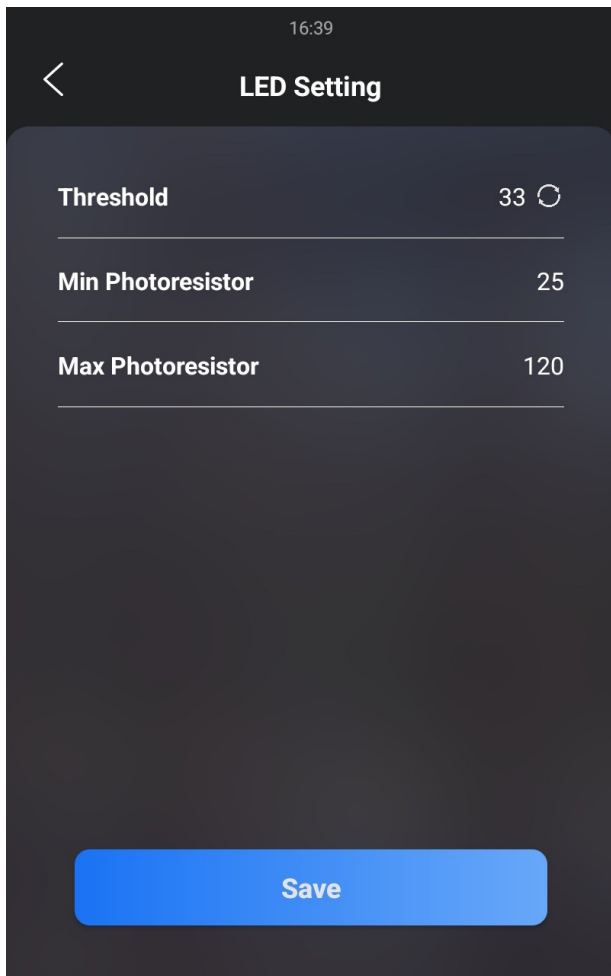
## Ustawienia LED i LCD

### Ustawienie diody LED podczerwieni

Dioda LED na podczerwień została zaprojektowana głównie w celu wzmocnienia światła do rozpoznawania twarzy w nocy lub w ciemnym otoczeniu, można skonfigurować diodę LED na podczerwień w urządzeniu i w interfejsie internetowym.


### Ustawienie diody LED podczerwieni na urządzeniu

Aby skonfigurować go w urządzeniu, należy wybrać interfejs **Ustawienia podstawowe > Wyświetlacz > Ustawienia LED**.



#### Konfiguracja parametrów :

- **Próg:** odnosi się do aktualnego natężenia światła wskazywanego przez wartość fotorezystora. Wyższe wartości fotorezystora odpowiadają niższemu natężeniu światła i odwrotnie. Domyślna wartość fotorezystora (**Threshold** ) wynosi 33, można jednak dotknąć ikony

 kilkakrotnie w celu uzyskania rzeczywistej wartości fotorezystora w określonym czasie.

(fluktuacja wartości wynosi około 5), a wartość jest oparta na konfiguracji minimalnej i maksymalnej wartości fotorezystora.

- **Min/Max Photoresistor:** ustawia minimalną i maksymalną wartość fotorezystora w oparciu o aktualnie wykrytą wartość fotorezystora w celu sterowania **włączaniem i wyłączeniem** diody LED. Można ustawić maksymalną wartość fotorezystora, aby włączyć diodę IR LED i minimalną wartość, aby ją wyłączyć. Domyślne minimalne i maksymalne wartości fotorezystora wynoszą od **0** minimum do **1000** maksimum.

## Ustawienie diody LED podczerwieni w interfejsie internetowym

Aby skonfigurować konfigurację w interfejsie sieci **Web Device > Light > LED**.



### Uwaga

- Należy zapoznać się z ustawieniami parametrów diody LED na podczerwień w urządzeniu.

## Ustawienie diody LED w obszarze czytnika kart

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

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



**Konfiguracja parametrów :**

- **Start Time- End Time(H):** wprowadź zakres czasu, w którym oświetlenie LED ma działać, np. jeśli zakres czasu jest ustawiony od **8-0 (czas rozpoczęcia-czas zakończenia)**, oznacza to, że światło LED pozostanie włączone w przedziale czasowym od **8:00** do **12:00** w ciągu jednego dnia (24 godziny).

## Ustawienie jasności ekranu LCD

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

## Ustawienie jasności ekranu LCD w interfejsie internetowym

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

Aby przeprowadzić konfigurację w interfejsie internetowym **Urządzenie > Światło > Jasność podświetlenia LCD**.

LCD Backlight Brightness

Mode	<input type="text" value="Auto"/>	
Backlight Brightness(Day)	<input type="text" value="60"/>	(1-255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="10"/>	(1-255)
Backlight Brightness(Night)	<input type="text" value="10"/>	(1-255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="3"/>	(1-255)

### Konfiguracja parametrów :

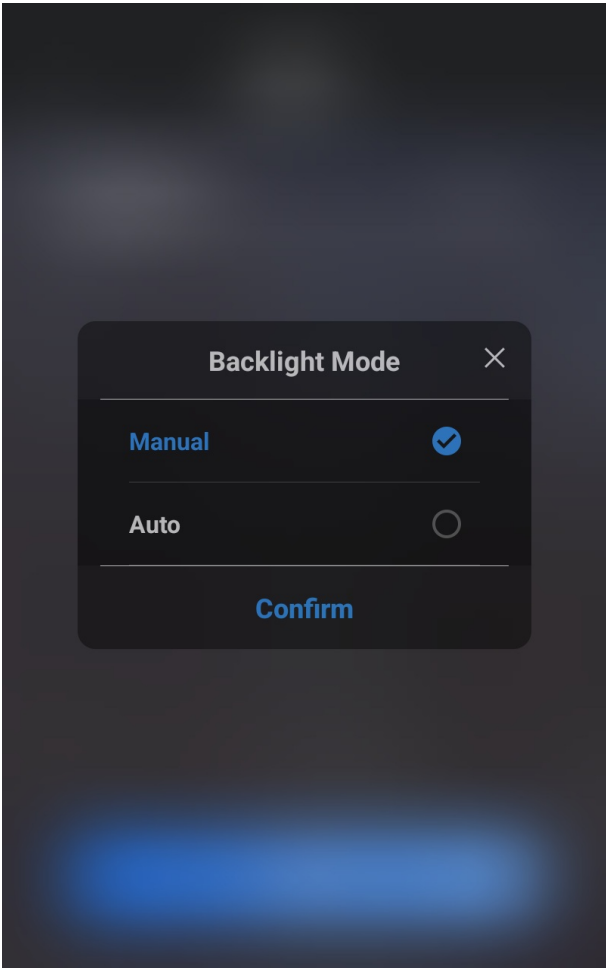
- **Tryb** : kliknij, aby wybrać tryb **ręczny** lub **automatyczny** podświetlenia. Po wybraniu opcji **Auto** podświetlenie zostanie automatycznie dostosowane do jasności ekranu i odwrotnie.
- **Jasność podświetlenia (dzień)**: ustawienie jasności podświetlenia ekranu w ciągu dnia przy użyciu wartości z zakresu **(0-255)** .
- **Backlight Brightness Of Screen Saver(day)**: ustawienie jasności podświetlenia ekranu dla wygaszacza ekranu w ciągu dnia w zakresie **(0-255)** .
- **Jasność podświetlenia (noc)**: ustawienie jasności podświetlenia ekranu w nocy przy użyciu wartości z zakresu **(0-255)** .
- **Backlight Brightness Of Screen Saver(night)**: ustawienie jasności podświetlenia ekranu dla wygaszacza ekranu w ciągu dnia z wartością w zakresie **(0-255)** .

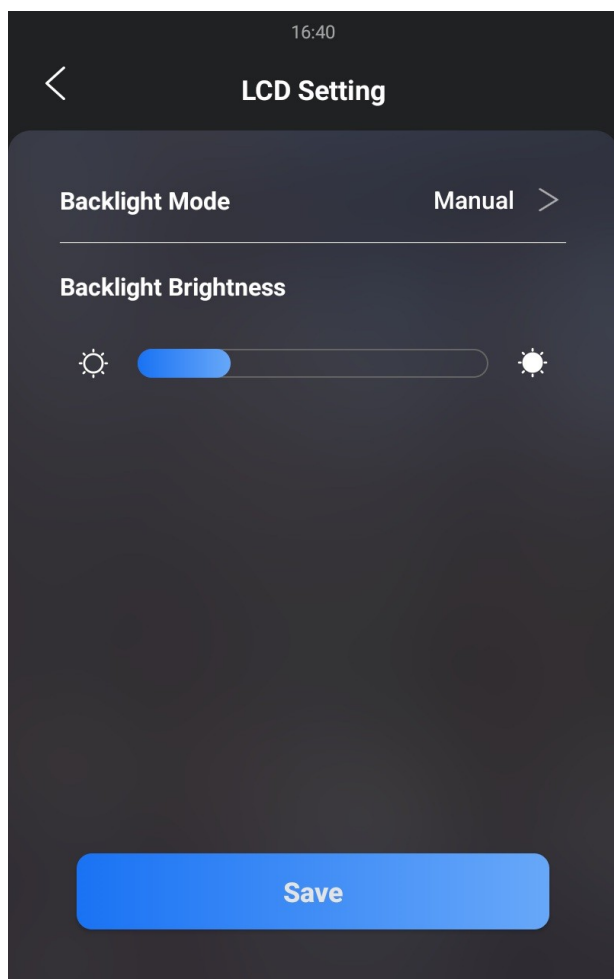
## Ustawienie jasności ekranu LCD na urządzeniu

W urządzeniu można ustawić i dostosować jasność podświetlenia ekranu.

Aby skonfigurować go w urządzeniu, należy wybrać interfejs **Ustawienia podstawowe > Wyświetlacz > Ustawienia LCD**.







## Ustawienie białego światła LED

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

Aby skonfigurować go w interfejsie internetowym **Urządzenie > Światło > Światło białe**.

White Light	
Mode	OFF
Limit Backlight Value	50 (1-255)
White Light PWM Value	80 (0-100)

### Konfiguracja parametrów :

- **Tryb:** wybierz **Auto** lub **OFF**. Jeśli wybierzesz **Auto**, białe światło włączy się na 5 minut w celu rozpoznania twarzy i zeskanowania kodu QR.

# Konfiguracja ekranu

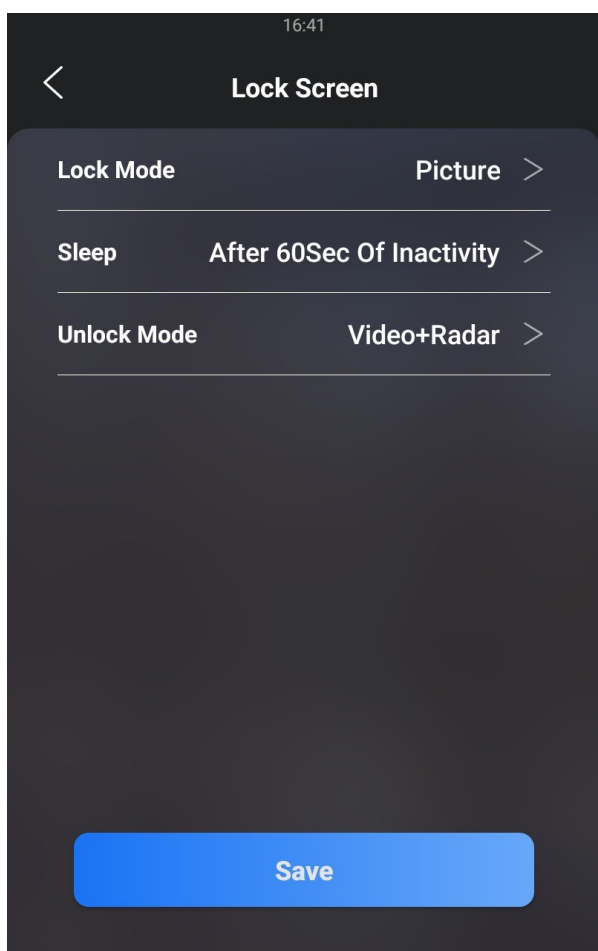
Możesz skonfigurować funkcje wyświetlania ekranu urządzenia, takie jak wygaszacz ekranu, aby zapewnić użytkownikom lepsze wrażenia wizualne i operacyjne.

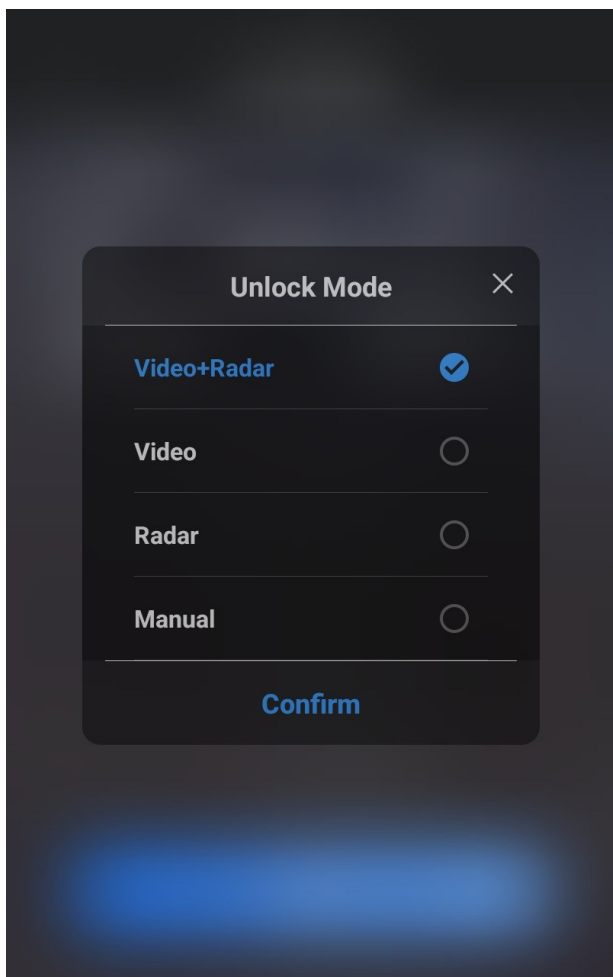
## Konfiguracja wygaszacza ekranu

### Konfiguracja wygaszacza ekranu na urządzeniu

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

Na ekranie urządzenia przejdź do opcji **Ustawienia podstawowe > Ekran blokady**.





#### Konfiguracja parametrów :

- **Tryb blokady** : wybór jednej z trzech opcji **NONE (Brak)**, **Blank Screen (Pusty ekran)** i **Picture (Obraz)**. Opcja **NONE** jest wybierana, gdy ekran ma pozostać włączony bez przechodzenia w tryb wygaszacza ekranu; jeśli wybrana zostanie opcja **Blank Screen**, ekran stanie się czarny. Jeśli wybrana zostanie opcja **Picture**, przesłane zdjęcie będzie wyświetlane jako wygaszcz ekranu.
- **Sleep (Uśpienie)**: ustawienie czasu uruchomienia wygaszacza ekranu w zakresie od 5 do 180 sekund. Wygaszcz ekranu uruchamia się, gdy urządzenie wykryje brak działania lub nikt się nie zbliża.
- **Tryb odblokowania** :
  - a. wybierz opcję **Ręcznie**, jeśli chcesz wybudzić ekran ręcznie, dotykając ekranu dotykowego.
  - b. wybierz **Wideo** , ekran urządzenia zostanie wybudzony po wykryciu obiektu na obrazie wideo.
  - c. Wybierz **Radar**, a ekran urządzenia zostanie wybudzony po wykryciu obiektu przez radar.
  - d. Po wybraniu opcji **Radar+Wideo** urządzenie zostanie wybudzone po wykryciu obiektu przez radar lub obraz wideo.

## Konfiguracja wygaszacza ekranu w interfejsie sieciowym

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

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

### Standby Interface Display

Screensaver Mode	Image ▼
Screensaver Time(Sec)	60 ▼
Wake Up Screensaver Mode	Video+Radar ▼
Deep Sleep Enabled	<input checked="" type="checkbox"/>
Deep Sleep Interval(Min)	30 ▼

### Konfiguracja parametrów :

- **Screensaver Mode (Tryb wygaszacza ekranu):** wybierz jedną z trzech opcji: **NONE (Brak)**, **Blank (Pusty)** i **Image (Obraz)**. Opcja **NONE** jest wybierana, gdy ekran ma pozostać włączony bez przechodzenia w tryb wygaszacza ekranu; jeśli wybrana zostanie opcja **Blank**, ekran stanie się czarny. Jeśli wybrana zostanie opcja **Obraz**, przesłane zdjęcie będzie wyświetlane jako wygaszcz ekranu.
- **Screensaver Time (Sec) (Czas wygaszacza ekranu (sek.)):** ustawienie czasu uruchomienia wygaszacza ekranu w zakresie od 5 do 180 sekund. Wygaszcz ekranu uruchamia się, gdy urządzenie nie wykryje żadnej operacji lub nikt się nie zbliża.
- **Tryb wybudzania wygaszacza ekranu:** wybór trybu wybudzania ekranu.
  - a. wybierz opcję Ręcznie, jeśli chcesz wybudzić ekran ręcznie, dotykając ekranu dotykowego.
  - b. Po wybraniu opcji Wideo ekran urządzenia zostanie wybudzony po wykryciu obiektu na obrazie wideo.
  - c. wybierz Radar, ekran urządzenia zostanie wybudzony po wykryciu obiektu przez radar.
  - d. wybierz Radar+Video, urządzenie zostanie wybudzone po wykryciu obiektu przez radar lub obraz wideo.

- **Deep Sleep Enabled** : zaznacz pole wyboru, jeśli chcesz, aby ekran był wyłączany po osiągnięciu przez wygaszacz ekranu zdefiniowanego czasu trwania.
- **Deep Sleep Interval (Min)**: ustawienie czasu wygaszacza ekranu przed jego wyłączeniem.

### Uwaga

- **Trybu wygaszacza ekranu nie** można zmienić z **automatycznego** na **ręczny**, gdy **Tryb wygaszacza ekranu** jest ustawiony jako **Pusty ekran**.

## Prześlij wygaszacz ekranu

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

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

### Upload Screensaver

Screensaver1

Screensaver ID	File Status	Interval(Sec)	Submit	Delete
1	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
2	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
3	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
4	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>
5	File Exists	<input type="text" value="5"/>	<input type="button" value="Submit"/>	<input type="button" value="Delete"/>

### Uwaga

- Przesyłane zdjęcia powinny być w **formacie JPG** o maksymalnej rozdzielczości 2 mln pikseli.
- Zalecana rozdzielczość to 1080x1920.
- Poprzednie zdjęcia o określonej kolejności ID zostaną nadpisane w przypadku powtarzającego się przypisywania zdjęć do tej samej kolejności ID.





## Prześlij obraz rozruchowy urządzenia

W razie potrzeby można przesłać obraz rozruchowy, który będzie wyświetlany podczas procesu uruchamiania urządzenia.

Aby skonfigurować konfigurację w interfejsie sieci Web **Setting > Key/Display > Picture/File Import**.

Picture/File Import

---

Boot Animation (.png / .zip)	 Import	 Reset
Background of Directory List(.png)	 Import	 Reset

### Uwaga

- Przesyłane zdjęcia powinny być w formacie **.png** lub **.zip**.
- Maksymalny rozmiar pliku zip to 20 MB; maksymalny rozmiar pliku png to 1 MB. Zalecana rozdzielczość to 800\*1280.





## Prześlij obraz tła listy kontaktów urządzenia

Można dostosować wyświetlanie tła listy kontaktów. Przed przesłaniem można wybrać zdjęcie.

W Internecie przejdź do **Ustawienia > Klawisze/Wyświetlacz > Interfejs importu zdjęć/plików**.

Picture/File Import

---

Boot Animation (.png / .zip)	 Import	 Reset
Background of Directory List(.png)	 Import	 Reset

## Uwaga

- Przesłane zdjęcia powinny być w formacie .png lub .zip.
- Maksymalny rozmiar pliku zip to 20 MB; maksymalny rozmiar pliku png to 1 MB.
- Zalecana rozdzielczość to 800x1280.

Key In Homepage Of The Building Theme

Index	Label	Type	Value
1	<input type="text"/>	PIN ▼	<input type="text"/>
2	<input type="text"/>	Call ▼	<input type="text"/>
3	<input type="text"/>	Directory ▼	<input type="text"/>
4	<input type="text"/>	Speed Dial ▼	0.0.0.0

## Konfiguracja trybu wyświetlania ekranu opartego na scenariuszu

Bramofony oferują dwa rodzaje trybów wyświetlania ekranu dla różnych zastosowań: Tryb budynku, Tryb willi i Tryb uwierzytelniania wieloskładnikowego.

Aby go skonfigurować, przejdź do **Ustawienia > Klawisze/Wyświetlacz > Motyw** .



11:30 Fri-2022-10-21

Community66666  
Config.Features.ACTIONURL.InputATriggered



PIN



Call



Directory



Reception

12:18

Fri 2022-10-21



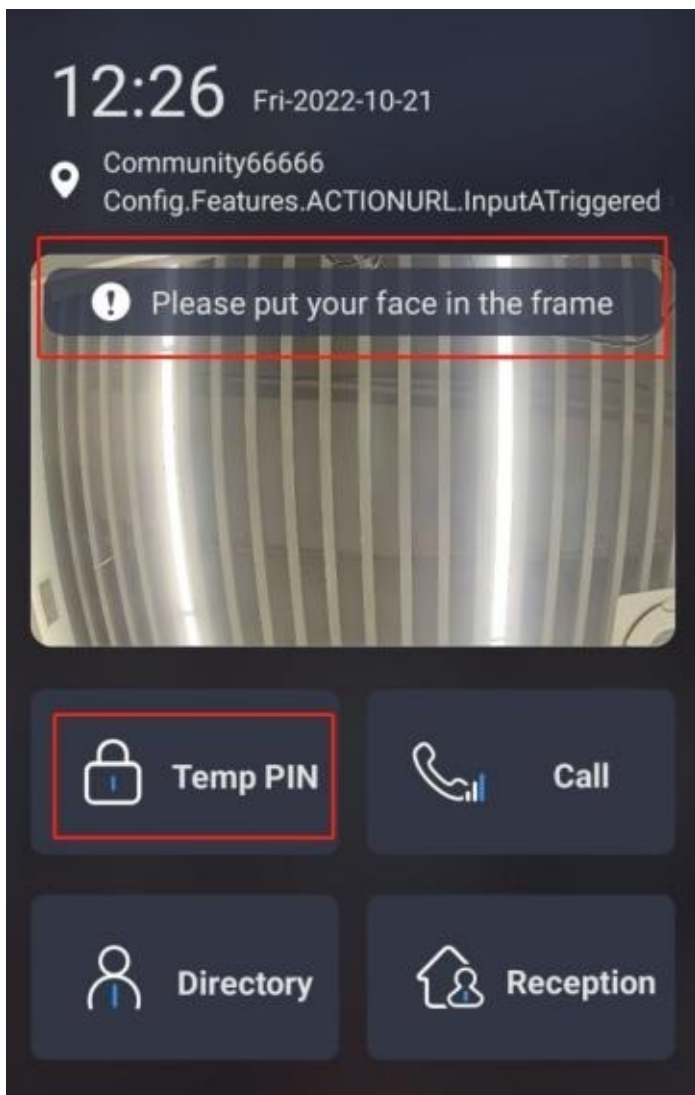
Directory



PIN



Call



## Wyświetlanie ekranu głównego trybu Villa

Można skonfigurować wyświetlanie na ekranie układu ikony lokatora, ikony PIN i ikony połączenia na ekranie głównym w trybie willi.

Możesz przejść do **Ustawienia > Klawisze/Wyświetlacz > Kontrola widoku** interfejsu motywu **Villa**.

View Control of The Villa Theme

Default Page

Index	Key	Label	Value
1	Directory	<input type="text"/>	Show
2	PIN	<input type="text"/>	Show
3	Call	<input type="text"/>	Show

**Konfiguracja parametrów :**

- **Default Page (Strona domyślna)** : wybierz opcję **Home Page (Strona główna)**, jeśli chcesz wyświetlać lokatorów, PIN i ikonę połączenia pionowo na ekranie głównym. Wybierz **Directory**, jeśli chcesz wyświetlać kontakty na ekranie głównym. Wybierz **PIN**, jeśli chcesz wyświetlać ikonę PIN z klawiaturą na ekranie głównym. Wybierz opcję **Call**, jeśli na ekranie głównym ma być wyświetlana ikona połączenia z klawiaturą numeryczną.
- **Klawisz**: ustawienie typu ikony, która ma być wyświetlana na ekranie głównym trybu willi.
- **Etykieta**: nadawanie nazw ikonom na ekranie głównym trybu willi.
- **Wartość**: jeśli ustawisz wartość jako pokazaną, ikona będzie widoczna na ekranie.

## Ekran główny trybu budynku

W razie potrzeby można dostosować wyświetlanie ikon na ekranie głównym trybu budowania.

Aby to zrobić, przejdź do **Ustawienia > Klucz/Wyświetlacz > Klucz na stronie głównej motywu budynku** .

Key In Homepage Of The Building Theme

Index	Label	Type	Value
1	<input type="text"/>	PIN ▼	<input type="text"/>
2	<input type="text"/>	Call ▼	<input type="text"/>
3	<input type="text"/>	Directory ▼	<input type="text"/>
4	<input type="text"/>	Speed Dial ▼	0.0.0.0

### Konfiguracja parametrów :

- **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.
- **Etykieta**: wprowadź nową nazwę, która zastąpi oryginalną nazwę zakładki, ale nie zmieni atrybutu typu.
- **Wartość** : wprowadź numer szybkiego wybierania.

## Ekran trybu uwierzytelniania wieloskładnikowego

W razie potrzeby można również dostosować wyświetlanie ikon na ekranie głównym dla trybu uwierzytelniania wieloskładnikowego.

Aby to zrobić, przejdź do **Ustawienia > Klucz/Wyświetlacz > Uwierzytelnianie wieloskładnikowe Interfejs tematyczny**.

Key In Homepage of Multi-factor Authentication Theme

Index	Label	Type	Value
1	<input type="text"/>	PIN ▼	<input type="text"/>
2	<input type="text"/>	Call ▼	<input type="text"/>
3	<input type="text"/>	Directory ▼	<input type="text"/>
4	<input type="text"/>	Speed Dial ▼	0.0.0.0.0

## Kolejność wybierania klawiszy

Bramofon oferuje dwie opcje wyświetlania przycisków klawiatury: Normalny i Nieuporządkowany. Wybranie ustawienia Disordered oznacza, że układ klawiszy jest za każdym razem losowy, co zwiększa bezpieczeństwo, zapobiegając szpiegowaniu haseł.

Można przejść do **opcji Ustawienia > Klawisze/Wyświetlacz > Tryb wyświetlania klawiatury interfejsu PIN**.

Keypad Display Mode Of PIN Interface

Mode

### Konfiguracja parametrów :

- **Tryb** : wybór wyświetlania kolejności klawiszy. Wybierz wyświetlanie klucza w kolejności, aby lepiej chronić swój kod PIN przed ujawnieniem go innym osobom podczas wprowadzania kodu PIN.

## Wyświetlanie monitu

Podpowiedzi wyświetlane na ekranie można dostosować do własnych potrzeb.

Aby to zrobić, przejdź do opcji **Ustawienia > Klawisze/Wyświetlacz > Monit tekstowy**. Wpisz monit dla różnych ekranów.

Text Prompt

Call Interface	Please enter the apartment number (e.g.101)
PIN Interface	Please enter your PIN
Directory Interface	Tap here to search

### Uwa

- Bramofon obsługuje tekst o maksymalnej długości 128 znaków podpowiedź.

## Wyświetlanie komunikatu tekstowego otwartych drzwi

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

Aby to zrobić, przejdź do **Kontrola dostępu > Przekaznik > Monit tekstowy**.

Text Prompt

Access Granted	<input checked="" type="checkbox"/>
Access Denied	<input checked="" type="checkbox"/>
Display User Info	<input checked="" type="checkbox"/>

## Konfiguracja głośności i tonów

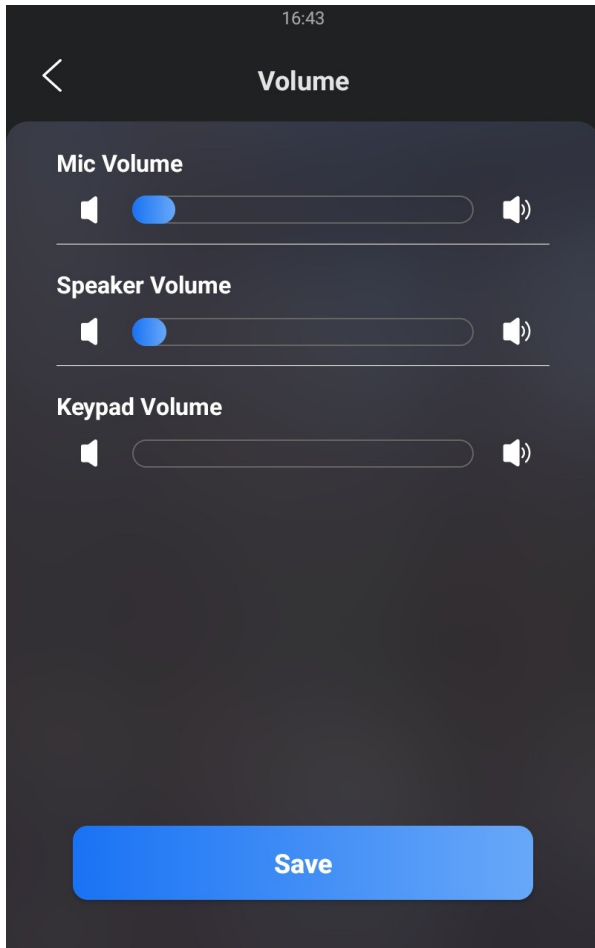
Konfiguracja głośności i tonów obejmuje głośność mikrofonu, głośność AD, głośność klawiatury, głośność głośnika, głośność alarmu sabotażowego i konfigurację dźwięku otwartych drzwi. Co więcej, możesz przesłać swój ulubiony dźwięk, aby wzbogacić spersonalizowane wrażenia użytkownika.

### Konfiguracja głośności

### Konfiguracja głośności na urządzeniu

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

Aby to zrobić, przejdź do opcji **Ustawienia podstawowe > Interfejs głośności**.



## Konfiguracja głośności w interfejsie internetowym

W interfejsie internetowym można ustawić głośność alarmu sabotażowego,

głośność mikrofonu itp. Aby skonfigurować je w interfejsie internetowym

**Urządzenie > Interfejs audio.**

**Volume Control**

Prompt Volume	<input type="text" value="4"/>	(0~10)
Mic Volume	<input type="text" value="1"/>	(1~8)
Speaker Volume	<input type="text" value="1"/>	(1~10)
Key Pressed Volume	<input type="text" value="0"/>	(0~7)
Tamper Alarm Volume	<input type="text" value="10"/>	(1~10)

---

**Volume Control On Talking Interface**









Enabled

### Konfiguracja parametrów:

- **Enabled** : zaznacz pole wyboru, jeśli zezwalasz na regulację głośności połączenia na ekranie rozmowy podczas połączenia.

## Prześlij dźwięk zachęty

Można przysyłać różne rodzaje komunikatów głosowych. Przejdź do interfejsu **Device > Audio > Voice Prompt Setting.**

Voice Prompt Setting					
ID	Tone	Import	Reset	Play	Enabled
1	Greetings	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
2	Access Granted	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
3	Access Denied	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
4	PIN Page	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
5	APT+PIN	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
6	Call Page	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
7	Calling	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>
8	Directory	<a href="#">Import</a>	<a href="#">Reset</a>		<input checked="" type="checkbox"/>



## Konfiguracja parametrów :

- **Powitanie** : import sygnału powitania po uruchomieniu
- urządzenia. **Access Granted** : zaimportuj sygnał zachęty po
- pomyślnym otwarciu drzwi. **Access Denied** : zaimportuj sygnał zachęty w przypadku niepowodzenia otwarcia drzwi.
- **PIN Page**: import sygnału zachęty dla ekranu PIN. **Apart+PIN**:
- import sygnału zachęty dla ekranu Apart+ PIN. **Strona**
- **połączenia**: zaimportuj dźwięk monitu dla ekranu połączenia.

### Uwaga

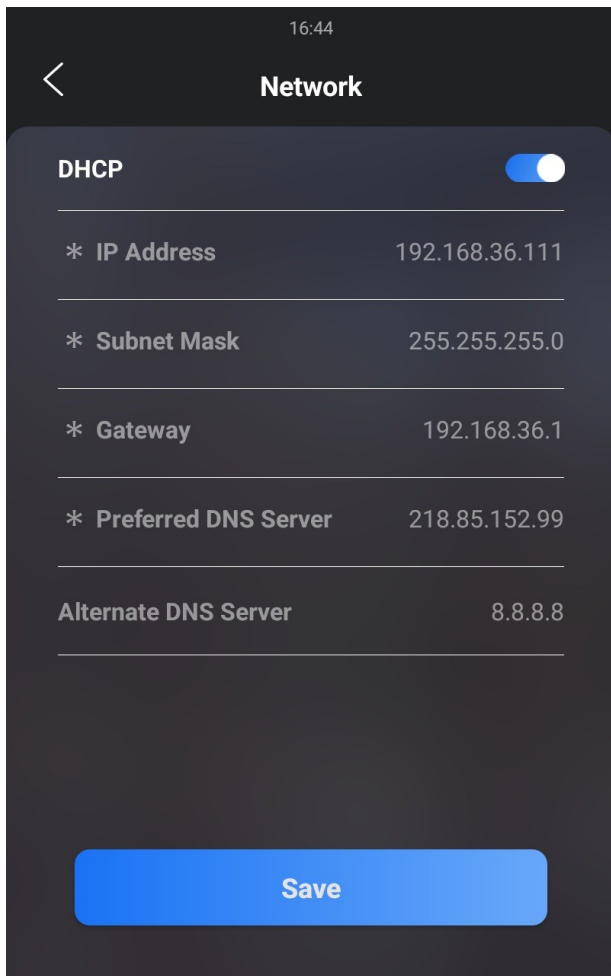
Plik dźwiękowy otwartych drzwi powinien być w formacie .wav, a jego rozmiar powinien być mniejszy niż 200KB.

## Ustawienia sieciowe

### Konfiguracja sieci urządzenia

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

Aby skonfigurować na urządzeniu **Ustawienia** > Interfejs sieciowy.



### Konfiguracja parametrów :

- **DHCP** : Wybierz tryb **DHCP** , przesuwając przełącznik w prawo. Tryb DHCP jest domyślnym połączeniem sieciowym. Jeśli tryb DHCP jest włączony, telefonowi zostanie automatycznie przypisany przez serwer DHCP adres IP, maska podsieci, brama domyślna i adres 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 ręcznie skonfigurować zgodnie z rzeczywistym środowiskiem sieciowym.

- **Adres IP** : ustawienie adresu IP w przypadku wybrania statycznego trybu IP.
- **Maska podsieci**: ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Default Gateway (Brama domyślna)**: ustawienie prawidłowej bramy zgodnie z adresem IP.
- **Preferowany i alternatywny serwer DNS**: skonfiguruj preferowany lub alternatywny serwer DNS (**Domain Name Server**) zgodnie z rzeczywistym środowiskiem sieciowym. Preferowany serwer DNS jest podstawowym adresem serwera DNS, podczas gdy alternatywny serwer DNS jest adresem serwera pomocniczego, a bramofon połączy się z serwerem alternatywnym, gdy podstawowy serwer DNS będzie niedostępny.

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

LAN Port

DHCP  Static IP

## Konfiguracja lokalnego protokołu RTP urządzenia

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

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

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

Local RTP

Starting RTP Port	<input type="text" value="11800"/>	(1024~65535)
Max RTP Port	<input type="text" value="12000"/>	(1024~65535)

### Konfiguracja parametrów :

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

## Wdrażanie urządzeń w sieci

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

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



Connect Setting

Server Mode	SDMC
Device Location	Door Phone

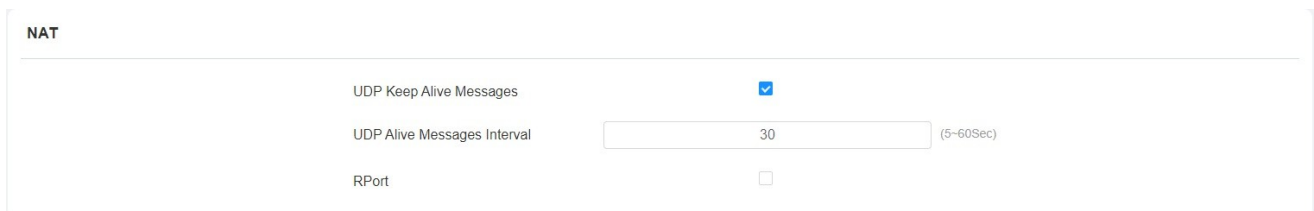
### Konfiguracja parametrów :

- **Typ serwera:** jest automatycznie konfigurowany zgodnie z rzeczywistym połączeniem urządzenia z określonym serwerem w sieci, takim jak **SDMC**, **Cloud** lub **None**. **Brak** jest domyślnym ustawieniem fabrycznym wskazującym, że urządzenie nie jest podłączone do żadnego typu serwera. Dlatego w trybie wykrywania można wybrać **Cloud** lub **SDMC**.
- **Device Location (Lokalizacja urządzenia):** wprowadź lokalizację, w której urządzenie jest zainstalowane, aby odróżnić je od innych urządzeń.

## 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.

Aby ją skonfigurować, przejdź do **Konto > Zaawansowane > Interfejs NAT**.



NAT

UDP Keep Alive Messages	<input checked="" type="checkbox"/>
UDP Alive Messages Interval	<input type="text" value="30"/> (5-60Sec)
RPort	<input type="checkbox"/>

### Konfiguracja parametrów :

- **UDP Keep Alive Messages** : Jeśli opcja ta jest włączona, urządzenie wyśle wiadomość do serwera SIP, aby serwer SIP rozpoznał, czy urządzenie jest w stanie online.
- **UDP Alive Messages Interval:** ustawienie interwału czasowego wysyłania wiadomości w zakresie 5-60

sekund, domyślnie 30 sekund.

- **RPort:** włącz Rport, gdy serwer SIP znajduje się w sieci WAN (**Wide Area Network**).

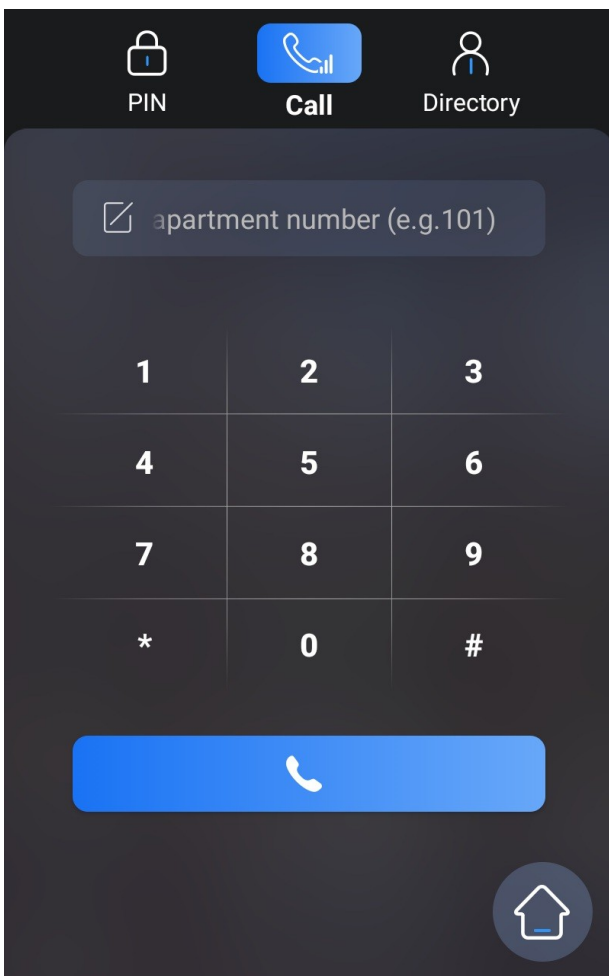
## Konfiguracja połączeń interkomowych

### 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 nawiązywać połączenia SIP lub IP na urządzeniu, należy kliknąć pokrętko na ekranie głównym.



### Konfiguracja połączeń IP

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

Direct IP

Enabled	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1024-65535)

### Konfiguracja parametrów :

- **Port:** bezpośredni port IP to domyślnie **5060** z zakresem portów od **1-65535**. Po wprowadzeniu jakichkolwiek wartości z zakresu innego niż 5060, należy sprawdzić, czy wprowadzona wartość jest zgodna z odpowiednią wartością na urządzeniu, które ma ustanowić transmisję 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

Aby skonfigurować konto SIP na urządzeniu, wybierz kolejno opcje **Ustawienia** > Interfejs **konta**.

16:45

< Account

1st Account 2nd Account

Account

Display Name

\* Register Name

\* Username

\* Password

\* Server IP

\* Server Port 5060  
(1024~65535)

Save

### Konfiguracja parametrów :

- **Konto**: zaznacz, aby aktywować zarejestrowane konto.
- **Display Name** : skonfiguruj nazwę, na przykład nazwę urządzenia, która będzie wyświetlana na urządzeniu, z którym nawiązywane jest połączenie.

a. Aby zarejestrować konto SIP dla monitorów wewnętrznych Akuvox, uzyskaj **nazwę rejestru, nazwę użytkownika, hasło, adres IP serwera i port serwera** na ekranie centrali PBX monitora wewnętrznego Akuvox.

b. Aby zarejestrować konto SIP dla urządzeń innych firm, uzyskaj **nazwę rejestru, nazwę użytkownika, hasło, adres IP serwera i port serwera** od zewnętrznego dostawcy usług.

### Konfiguracja konta SIP w interfejsie internetowym

Aby skonfigurować konfigurację w interfejsie Web **Account > Basic > SIP Account**.

SIP Account	
Status	UnRegistered
Account	Account1 ▼
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>

### Konfiguracja parametrów :

- **Konto aktywne:** kliknij Włącz lub Wyłącz, aby aktywować lub dezaktywować zarejestrowane konto SIP.
- **Wyświetlana nazwa:** skonfiguruj nazwę, która będzie wyświetlana na urządzeniu, z którym nawiązywane jest połączenie.
- **Konto:** wybierz dokładne konto (Konto 1 i 2), które ma zostać skonfigurowane.
- **Display Label:** skonfiguruj etykietę urządzenia, która będzie wyświetlana na ekranie urządzenia.

a. Aby zarejestrować konto SIP dla monitorów wewnętrznych Akuvox, uzyskaj **nazwę rejestru, nazwę użytkownika i hasło** na ekranie centrali PBX monitora wewnętrznego Akuvox.

b. Aby zarejestrować konto SIP dla urządzeń innych firm, należy uzyskać **nazwę rejestru, nazwę użytkownika i hasło** od zewnętrznego dostawcy usług.

## 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 konfigurację w interfejsie **Konto internetowe > Podstawowe > Preferowany serwer SIP**.



Preferred SIP Server		
Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024-65535)
Registration Period	<input type="text" value="1800"/>	(30-65535Sec)

Alternate SIP Server		
Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024-65535)
Registration Period	<input type="text" value="1800"/>	(30-65535Sec)

### Konfiguracja parametrów :

- **Preferred SIP Server:** wprowadź adres IP serwera podstawowego lub jego adres URL.
- **Alternate SIP Server:** wprowadź adres IP zapasowego serwera SIP lub jego adres URL.
- **Port:** ustawienie portu serwera SIP dla transmisji danych.
- **Registration Period :** 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** i mieści się w zakresie **30-65535** s.

### Konfiguracja połączenia SIP DND i kodu zwrotnego

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

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

DND	
Account	<input type="text" value="Account1"/>
Enabled	<input type="checkbox"/>
Return Code When DND	<input type="text" value="486(Busy Here)"/>
DND On Code	<input type="text"/>
DND Off Code	<input type="text"/>

### Konfiguracja parametrów :

- **Return Code When DND :** wybierz, jaki kod ma być wysyłany do urządzenia dzwoniącego za pośrednictwem serwera SIP. **404 dla Nie znaleziono; 480 dla Tymczasowo niedostępny; 486 dla Zajęty tutaj; 603 dla Odrzuć.**

## 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 w interfejsie **Konto internetowe > Podstawowe > Serwer proxy połączeń wychodzących**.

### Konfiguracja parametrów :

- **Preferred/Alternate Server IP** : wprowadź adres SIP podstawowego/zapasowego serwera proxy połączeń wychodzących.
- **Port**: wprowadź numer portu w celu nawiązania sesji połączenia za pośrednictwem głównego/zapasowego serwera proxy połączeń wychodzących.

## Konfiguracja typu transmisji danych

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

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

### Konfiguracja parametrów :

- **UDP** : wybierz **UDP** dla zawodnego, ale bardzo wydajnego protokołu warstwy transportowej. UDP jest domyślnym protokołem transportowym.
- **TCP** : wybierz **TCP** dla niezawodnego, ale mniej wydajnego protokołu warstwy transportowej.
- **TLS** : wybierz **TLS** dla bezpiecznego i niezawodnego protokołu warstwy transportowej.

# Konfiguracja opcji wybierania numeru

## Szybkie wybieranie numeryczne

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

## Szybkie wybieranie przez wymianę numeru na urządzeniu

Aby skonfigurować na urządzeniu interfejs **Ustawienia > Reguła zastępowania > Dodaj regułę zastępowania**.

16:45

< Add Replace Rule

Account Default >

\* Prefix

\* 1st Replace

2nd Replace

3rd Replace

4th Replace

5th Replace

Save

### 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). Możesz wybrać konto 1 lub konto 2, z którego numer może być wybierany. Jeśli numer wybierania został zarejestrowany zarówno na koncie 1, jak i na koncie 2, numer będzie domyślnie wybierany z konta 1.
- **Prefiks:** wprowadź krótki numer, który ma zastąpić wybierany numer.
- **Replace 1/2/3/4/5 :** wprowadź numery wybierania, które chcesz zastąpić. Zastąpienie może obejmować maksymalnie 5 numerów. Na przykład, jeśli zastąpisz pięć oryginalnych numerów wybierania wspólnym krótkim numerem, takim jak **101** , pięć urządzeń interkomowych z tym numerem wybierania zostanie wywołanych w tym samym czasie po wybraniu **101** .

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

Replace Rule

+ Add Import Export ▼

<input type="checkbox"/>	Index	Account	Prefix	1st Replace	2nd Replace	3rd Replace	4th Replace	5th Replace	Edit
No Data									

Delete Delete All Prev 1/1 Next 1 Go

### Uwaga

- Pole wyboru dla każdego wiersza Prefiksu powinno być zaznaczone, aby można było zobaczyć Zakładka **Edytuj**, którą należy kliknąć, aby dokonać modyfikacji.

## Szybkie wybieranie

### Szybkie wybieranie w trybie willi

Szybkie wybieranie to funkcja umożliwiająca utworzenie karty lub kombinacji zorganizowanych kart wyświetlanych na ekranie wybierania urządzenia. Można nawiązywać połączenia, naciskając określone karty, aby wykonywać szybkie połączenia bez wprowadzania numerów wybierania.

Aby skonfigurować szybkie wybieranie w Internecie **Ustawienia>Klucze/Wyświetlacz>Tryb wyświetlania interfejsu połączenia (szybkiego wybierania)** .

Display Mode of Call Interface (Speed Dial)

Mode Auto ▼

Keys

<input type="checkbox"/>	Index	Name	Number
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	3	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	4	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	5	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	6	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	7	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	8	<input type="text"/>	<input type="text"/>

Selected: 0/8 Clear Clear All Total: 64 Prev 1/8 Next Go To Page 1 Go

## Konfiguracja parametrów :

**Tryb** : wybierz układ kart szybkiego wybierania spośród 9 opcji zgodnie z własnymi preferencjami. Każda opcja oferuje inny układ kart wybierania wraz ze zmianami w układzie klawiatury programowej na ekranie wybierania. Poniżej objaśniono 9 opcji:

Opcje	Opisy
<b>Standard</b>	Wybierz <b>Standard</b> , jeśli chcesz wyświetlać tylko godzinę i klawiaturę, bez zakładki wybierania.
<b>Auto</b>	Wybierz opcję <b>Auto</b> , jeśli chcesz wybrać układ kart wybierania, który pasuje do dowolnej z pozostałych 8 opcji. Na przykład, jeśli chcesz utworzyć 3 zakładki wybierania, 5 zakładki wybierania lub 7 zakładki, które nie pasują do innych opcji.
<b>1 Klucz</b>	Wybierz opcję <b>1 Key</b> , jeśli wyświetlana jest tylko jedna karta wybierania bez klawiatury.
<b>1 Klawisz + Klawiatura</b>	Wybierz <b>1 Key+Keypad</b> , jeśli chcesz wyświetlić jedną kartę wybierania z klawiaturą.
<b>2 klawisze + klawiatura</b>	Wybierz opcję <b>2 Keys+Keypad</b> , jeśli chcesz wyświetlać dwie karty wybierania za pomocą klawiatury.
<b>4 klawisze + klawiatura</b>	Wybierz opcję <b>4 Keys+Keypad</b> , aby wyświetlić cztery karty wybierania za pomocą klawiatury.
<b>8 Klucze</b>	Wybierz opcję <b>8 klawiszy</b> , aby wyświetlić 8 kart wybierania bez klawiatury.
<b>16 Klucze</b>	Wybierz <b>16 przycisków</b> , jeśli chcesz wyświetlić 16 kart wybierania bez klawiatury.
<b>64 Klucze</b>	Wybierz <b>64 przyciski</b> , jeśli chcesz wyświetlić 64 karty wybierania bez klawiatury.

### Uwaga

- Funkcja ta nie może być stosowana w **trybie budynku**.
- Klawiatura nie zostanie wyświetlona, jeśli liczba kart wybierania przekroczy 4 karty.

## Szybkie wybieranie w trybie budynku

Bramofon umożliwia dzwonienie do grupy osób jednocześnie poprzez naciśnięcie przycisku

odbioru. W Internecie przejdź do interfejsu **Setting > Key/Display > Speed Dial Setting**.

Speed Dial Setting

---

Group Disabled ▼

Dial Out Forward

## Konfiguracja parametrów :

- **Grupa** : wybierz grupę kontaktów, do której chcesz zadzwonić, naciskając przycisk odbioru.

## Konfiguracja automatycznego odbierania połączeń

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

Aby włączyć tę funkcję w interfejsie internetowym **Konto > Zaawansowane > Połączenie** i skonfigurować ją w interfejsie internetowym **Interkom > Funkcja połączenia > Automatyczne odbieranie**.

Call

---

Max Local SIP Port	<input type="text" value="23923"/>	(1024-65535)
Min Local SIP Port	<input type="text" value="23913"/>	(1024-65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input checked="" type="checkbox"/>	

---

Auto Answer

Auto Answer Delay	<input type="text" value="0"/>	(0-5Sec)
Mode	<input type="text" value="Video"/>	

### 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 ją skonfigurować, przejdź do **Interkom > Podstawowe > Interfejs połączeń sekwencyjnych**.

Sequence Call

---

Enabled

Time Out (Sec)

When Refused

### Konfiguracja parametrów :

- **Timeout (Sec) (Limit czasu (sek.))**: kliknij, aby wybrać interwał czasowy między kolejnymi numerami połączeń w docelowej grupie połączeń sekwencyjnych. Na przykład, jeśli ustawisz interwał czasowy na 10 sekund, wówczas połączenie (jeśli nie zostanie odebrane w ciągu 10 sekund) zostanie automatycznie zakończone i przeniesione sekwencyjnie do następnego numeru połączenia sekwencyjnego w docelowej grupie połączeń sekwencyjnych.
- **Po odrzuceniu**: jeśli wybierzesz opcję **Nie dzwoń dalej**, połączenie sekwencyjne zostanie zakończone, jeśli połączenie zostanie odrzucone przez rozmówcę. Jeśli wybierzesz opcję **Call Next**, połączenie sekwencyjne będzie kontynuowane do następnego rozmówcy, jeśli zostanie odrzucone przez pierwszego rozmówcę.

### Uwaga

Funkcja Sequence Call powinna być obsługiwana przez SmartPlus, prosimy o kontakt z Akuvox.

## Połączenie internetowe

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

Możesz przejść do **System > Konserwacja > Interfejs połączeń internetowych**.

Web Call

---

Web Call(Ready)  Auto

### Konfiguracja parametrów :

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

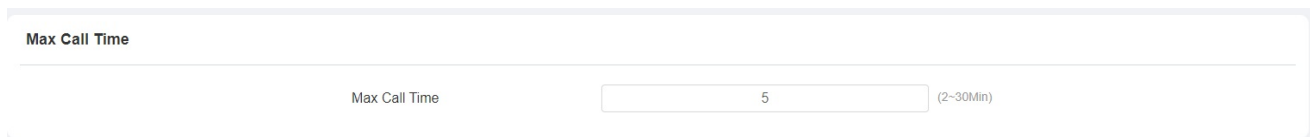


# Ustawienia połączeń

## Ustawienie maksymalnego czasu trwania połączenia

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

Aby ją skonfigurować, przejdź do interfejsu **Intercom > Call Feature > Max Call Time**.



Max Call Time	5	(2-30Min)
---------------	---	-----------

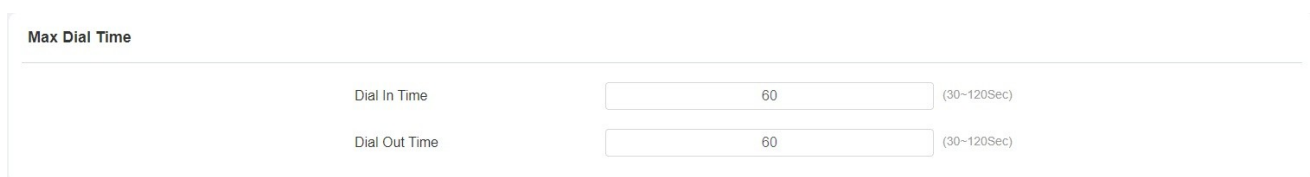
### Konfiguracja parametrów :

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

## Ustawienie maksymalnego czasu wybierania numeru

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

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



Dial In Time	60	(30-120Sec)
Dial Out Time	60	(30-120Sec)

### Konfiguracja parametrów :

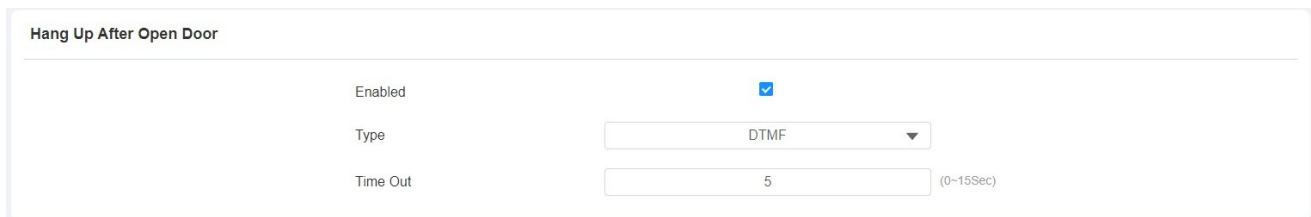
- **Dial In Time (Czas wybierania):** wprowadź czas wybierania dla bramofonu (w zakresie 30-120 sekund), na przykład, jeśli ustawisz czas wybierania na 60 sekund w bramofonie, wówczas bramofon automatycznie rozłączy połączenie przychodzące, jeśli połączenie nie zostanie odebrane przez bramofon w ciągu 60 sekund. Domyślnym czasem wybierania numeru jest 60 sekund.
- **Dial Out Time (Czas wybierania):** wprowadź czas wybierania dla swojego bramofonu (w zakresie 5-120 sekund).

Na przykład, jeśli w bramofonie ustawiono czas wybierania na 60 sekund, bramofon automatycznie rozłączy się z wybranym połączeniem, jeśli nie zostanie ono odebrane przez urządzenie, do którego dzwonił.

## Odłóż słuchawkę po otwarciu drzwi

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

Aby ustawić tę funkcję, przejdź do interfejsu **Intercom > Call Feature > Hang Up After Open Door**.



Hang Up After Open Door	
Enabled	<input checked="" type="checkbox"/>
Type	DTMF
Time Out	5 (0-15Sec)

### Konfiguracja parametrów :

- **Typ** : wybierz typ otwartych drzwi. Drzwi można odblokować za pomocą polecenia **DTMF, HTTP, DTMF lub HTTP** oraz **DTMF, HTTP lub wejścia**.
- **Limit czasu**: ustawienie od 1 sekundy do 15 sekund. Domyślnym ustawieniem jest 5 sekund. Jeśli ustawisz 5 sekund, połączenie zostanie rozłączone 5 sekund po otwarciu drzwi. Jeśli chcesz wyłączyć tę funkcję, ustaw limit czasu na 0.

## Konfiguracja kodeka audio i wideo dla połączeń SIP

### Konfiguracja kodeka audio

Bramofon obsługuje trzy typy kodeków (PCMU, PCMA 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 ją skonfigurować, przejdź do **Konto > Zaawansowane > Konto SIP** .

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

Typ kodeka	Zużycie przepustowości	Częstotliwość próbkowania
PCMA	64 kbit/s	8kHz
PCMU	64 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 go skonfigurować, przejdź do **Konto > Zaawansowane > Interfejs kodeka wideo**.

### Konfiguracja parametrów :

- **Nazwa** : zaznacz, aby wybrać format kodeka wideo H264 dla wideo z bramofonu. Jest on domyślnie włączony.
- **Rozdzielczość**: wybierz rozdzielczość kodu dla jakości wideo spośród pięciu opcji: **QCIF, CIF, VGA, 4CIF** , i **720P** zgodnie z rzeczywistym środowiskiem sieciowym. Domyślną rozdzielczością jest **VGA** .
- **Szybkość transmisji**: wybór szybkości transmisji strumienia wideo (w zakresie 320-2048). Im większa szybkość transmisji,

ilość danych przesyłanych w każdej sekundzie jest większa, dlatego obraz wideo będzie wyraźniejszy. Domyślna szybkość transmisji kodu wynosi 512 kb/s.

- **Payload (Ładunek):** wybierz typ ładunku (w zakresie 90-119), aby skonfigurować plik konfiguracyjny audio/wideo. Domyślny ładunek to 104.

## Konfiguracja kodeka wideo dla bezpośrednich połączeń IP

Jakość wideo połączenia IP można wybrać, wybierając odpowiednią rozdzielczość kodeka w zależności od stanu sieci.

Aby to zrobić, możesz przejść do **Interkom > Funkcja połączenia > Parametry wideo IP** .



IP Video Params	
Video Resolution	4CIF
Video Bitrate	2048 kbps
Payload	104

### Konfiguracja parametrów :

- **Rozdzielczość wideo:** wybierz rozdzielczość kodu dla jakości wideo spośród czterech opcji: **CIF, VGA, 4CIF i 720P** . Domyślną rozdzielczością kodu jest **720P** .
- **Szybkość transmisji 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 "**zgodnie ze środowiskiem sieciowym. Domyślna szybkość transmisji wideo wynosi **2048 kb/s**.
- **Video Payload (Ładunek wideo):** wybierz typ ładunku (w zakresie 90-119), aby skonfigurować plik konfiguracyjny audio/wideo. Domyślny ładunek to 104.

## Konfiguracja transmisji danych DTMF

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

Aby ją skonfigurować, przejdź do opcji **Konto > Zaawansowane > Interfejs DTMF**.

DTMF	
Type	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96-127)

### Konfiguracja parametrów :

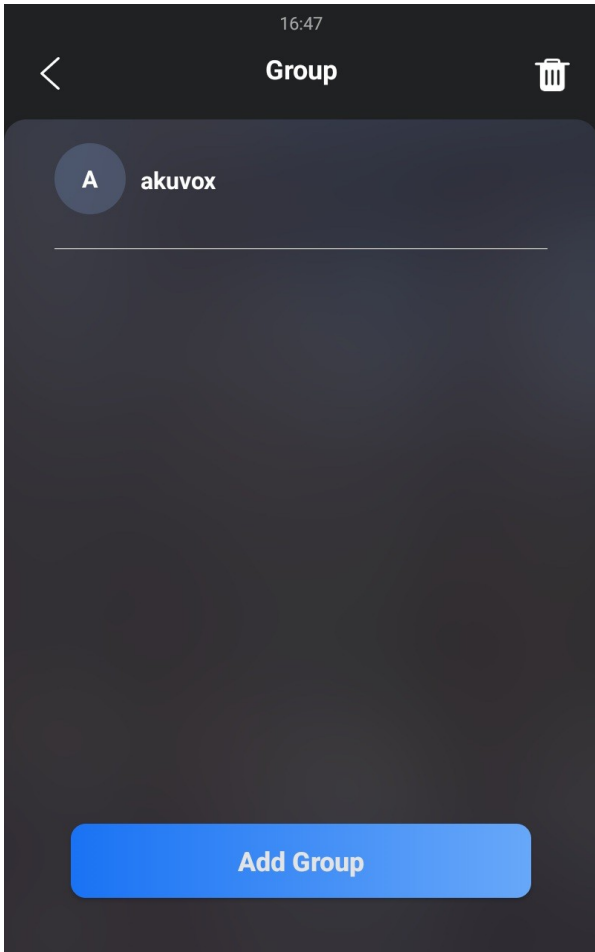
- **Tryb** : wybór trybu DTMF spośród sześciu opcji: **Inband**, **RFC 2833**, **Info+Inband**, **Info** , **Info+Inband+RFC 2833** oraz **Info+RFC 2833** w oparciu o określony typ transmisji DTMF urządzenia innej firmy, z którym ma zostać nawiązane połączenie jako strona odbierająca dane sygnału.
- **Jak powiadomić DTMF**: wybierz jeden z czterech typów: **Disable (Wyłącz)**, **DTMF**, **DTMF-Relay (Przekaznik DTMF)** i **Telephone-Event (Zdarzenie telefoniczne)** 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**: ustawia ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą i odbiorcą podczas transmisji danych.

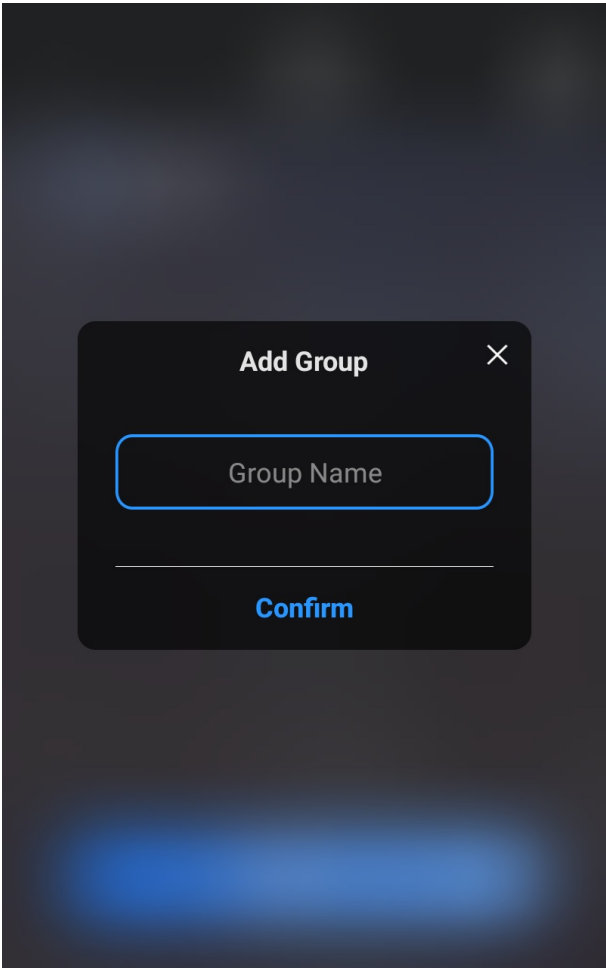
## Konfiguracja książki telefonicznej

### Konfiguracja książki telefonicznej na urządzeniu

Można tworzyć grupy kontaktów dla użytkowników.

Przejdź do **Ustawienia > Użytkownik > Grupa**, aby utworzyć grupę kontaktów, a następnie przejdź do **Lista użytkowników**, aby skonfigurować ustawienia kontaktów dla użytkowników.





16:53

< Add User

\* User ID : 1

\* Name

PIN >

RF Card >

Face >

Floor No. NULL >

\* Door ... >

Web Relay 0 >

Schedules ... >

Confirm

### Konfiguracja parametrów :

- **Telefon** : wpisz numer kontaktowy użytkownika.
- **Grupa** : wybór grupy kontaktów dla użytkownika.
  - a. Wybierz grupę **Domyślna**, jeśli nie utworzono grupy kontaktów dla użytkowników.
  - b. Wybierz opcję **Ukryte kontakty**, jeśli chcesz ukryć kontakt na ekranie katalogu.
  - c. Wybierz grupę kontaktów utworzoną dla użytkowników.
- **Konto wybierania** : wybierz konto wybierania, z którego chcesz zadzwonić do kontaktu na bramofonie.

### Uwaga

- Tylko numery SIP kontaktów mogą być wywoływane przez konto SIP. IP numery nie są ważne dla tej aplikacji.
- Przed wybraniem lub zmianą grupy należy ją najpierw utworzyć.

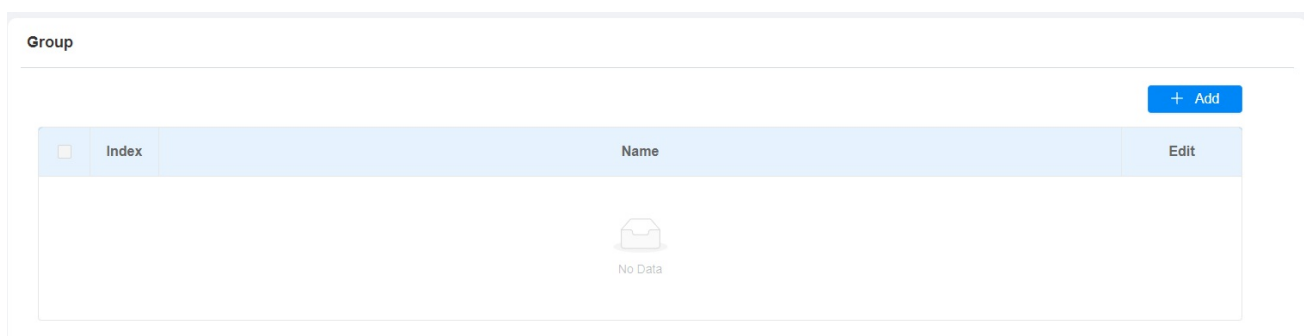


## Konfiguracja książki telefonicznej w interfejsie internetowym

### Zarządzanie grupami kontaktów w interfejsie internetowym

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

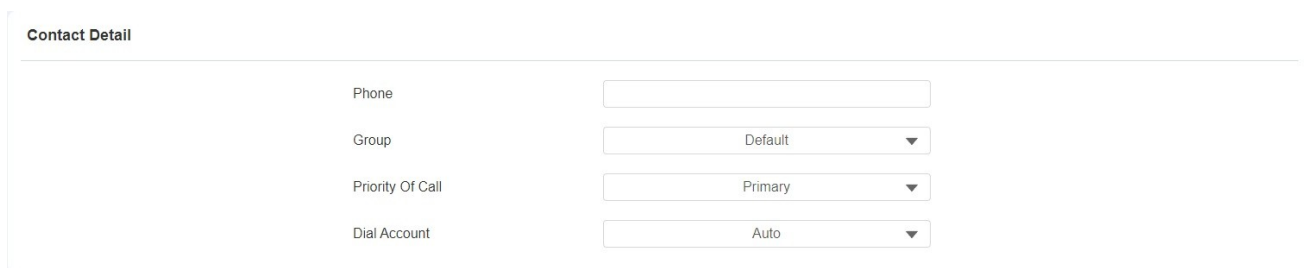
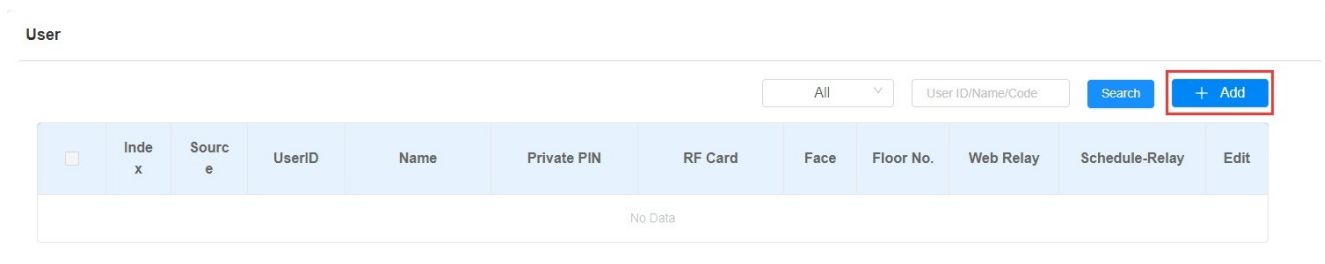
Aby utworzyć i edytować grupę kontaktów, przejdź do opcji **Katalog > Użytkownik > Interfejs grupy**.



### Konfiguracja kontaktu dla użytkownika

Ustawienia kontaktów użytkowników można skonfigurować podczas dodawania użytkownika.

Przejdź do **Katalog > Użytkownik**, kliknij **+Dodaj**, a następnie przewiń w dół do **Ustawienia szczegółów kontaktu**.



#### Konfiguracja parametrów :

- **Telefon** : wpisz numer kontaktowy użytkownika.

- **Grupa** : wybór grupy kontaktów dla użytkownika.
  - a. wybierz grupę **Domyślna**, jeśli nie utworzono grupy kontaktów dla użytkowników.
  - b. wybierz opcję **Ukryte kontakty**, jeśli chcesz ukryć kontakt na ekranie katalogu.
  - c. wybierz grupę kontaktów utworzoną dla użytkowników.
- **Priorytet połączenia**: ustawienie priorytetu połączenia dla użytkownika w grupie kontaktów (Pierwszorzędny, Drugorzędny i Trzeciorzędny) dla połączeń grupowych. Na przykład, jeśli ustawisz go jako pierwszorzędny dla użytkownika w wybranej grupie kontaktów, wówczas użytkownik będzie wywoływany jako pierwszy spośród wszystkich użytkowników w grupie kontaktów, gdy ktoś wykonuje połączenie grupowe.
- **Konto wybierania** : wybierz konto wybierania, z którego chcesz zadzwonić do kontaktu na bramofonie.

#### Uwaga

- Priorytet połączenia kontaktu nie może być ustawiony, gdy kontakt należy do jakiegokolwiek grupy kontaktowej.
- Format pliku kontaktu do importu powinien być w formacie .vcf, .csv lub .xml, podczas gdy format pliku kontaktu do eksportu powinien być tylko w formacie .vcf. Maksymalny rozmiar importowanego kontaktu to 3000.

## Ustawienia wyświetlania listy kontaktów

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

Aby ją skonfigurować, przejdź do interfejsu **Directory > Directory Setting**.

Show Cloud Contacts	<input checked="" type="checkbox"/>
Contacts Display Mode	Contact Display by Group
Sort By	ASCII Code
Click Contacts To Dial Out	<input checked="" type="checkbox"/>
Local Tenants Profile Display Mode	Enabled
Expand Tenants List View Mode	<input type="checkbox"/>
Search Function	<input checked="" type="checkbox"/>

**Konfiguracja parametrów :**

- **Pokaż kontakty w chmurze:** zaznacz pole wyboru, aby wyświetlić kontakty w chmurze na liście kontaktów. Po usunięciu zaznaczenia pola wyboru kontakt w chmurze zostanie ukryty.
- **Tryb wyświetlania kontaktów :** wybór trybu wyświetlania kontaktów.
  - Jeśli wybrano opcję Tylko **grupa**, wszystkie grupy kontaktów będą wyświetlane w kolejności według numeru pokoju.
  - Jeśli wybrano opcję **Wszystkie kontakty**, wszystkie kontakty zostaną wyświetlone w kolejności według numeru pokoju.
  - Jeśli wybrana jest opcja **Contact Display by Group**, po rozwinięciu grupy kontaktów wszystkie kontakty będą wyświetlane w kolejności ASC I.
- **Sortuj według:** wybierz **Kod ASCII, Nr pokoju lub Importuj**. Po wybraniu opcji Kod ASCII najemcy zostaną wyświetleni według nazwisk w kolejności kodu ASCII. Po wybraniu opcji Nr pokoju najemcy zostaną posortowani według numerów pokoi.
- **Click Contacts 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.
- **Local Tenants Profile Display Mode (Tryb wyświetlania profilu lokalnego najemcy):** wybierz **Enabled (Włączone)**, **Disabled (Wyłączone)** lub **Auto (Automatyczne)**. Gdy funkcja jest włączona, jeśli najemca ma przesłane zdjęcie profilowe kontaktu, zostanie ono wyświetlone obok nazwy; jeśli nie, obok nazwy zostanie wyświetlona domyślna ikona kontaktu. Jeśli funkcja jest wyłączona, zdjęcie lub ikona nie będą wyświetlane. Gdy funkcja jest ustawiona jako Auto, jeśli najemca ma przesłane zdjęcie profilu kontaktu, zdjęcie będzie wyświetlane obok nazwy; jeśli nie, obok nazwy nie będzie ikony.
- **Rozwiń tryb widoku listy kontaktów:** zaznacz pole wyboru, aby kontrolować rozmiar karty kontaktu. Na przykład, jeśli zaznaczysz to pole wyboru, karta kontaktu zostanie poszerzona. Po usunięciu zaznaczenia zakładka zmieni rozmiar na normalny.
- **Funkcja wyszukiwania:** zaznacz lub odznacz pole wyboru, aby kontrolować wyświetlanie pola **Dotknij tutaj, aby wyszukać** w górnej części ekranu. Jeśli nie zaznaczysz tego pola wyboru, pole **Dotknij tutaj, aby wyszukać** zostanie ukryte.

# Ustawienie przekaźnika

## Ustawienie przełącznika przekaźnika

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

> Interfejs przekaźnika.

Relay

Relay ID	<input type="text" value="RelayA"/>	<input type="text" value="RelayB"/>	<input type="text" value="RelayC"/>
Type	<input type="text" value="Default State"/>	<input type="text" value="Default State"/>	<input type="text" value="Default State"/>
Mode	<input type="text" value="Monostable"/>	<input type="text" value="Monostable"/>	<input type="text" value="Monostable"/>
Trigger Delay(Sec)	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>	<input type="text" value="5"/>	<input type="text" value="5"/>
DTMF Mode	<input type="text" value="1 Digit DTMF"/>		
1 Digit DTMF	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="2"/>
2~4 Digits DTMF	<input type="text" value="010"/>	<input type="text" value="012"/>	<input type="text" value="013"/>
Relay Status	<input type="text" value="RelayA: Low"/>	<input type="text" value="RelayB: Low"/>	<input type="text" value="RelayC: Low"/>
Relay Name	<input type="text" value="RelayA"/>	<input type="text" value="RelayB"/>	<input type="text" value="RelayC"/>

### Konfiguracja parametrów :

- **Trigger Delay (Sec):** ustaw czas opóźnienia wyzwolenia przekaźnika (w zakresie od 1 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia na 5 sekund, przekaźnik zostanie wyzwolony dopiero po **5** sekundach od naciśnięcia przycisku **odblokowania**.
- **Hold Delay (Sec):** ustaw czas opóźnienia zatrzymania przekaźnika (w zakresie od 1 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia na **5** sekund, przekaźnik będzie opóźniony o 5 sekund po odblokowaniu drzwi.
- **Tryb DTMF:** wybór liczby cyfr DTMF dla kontroli dostępu do drzwi (**w zakresie od 1 do 4 cyfr**). Można na przykład wybrać 1-cyfrowy kod DTMF lub 2-cyfrowy kod DTMF itp. w zależności od potrzeb.
- **1 Digit DTMF :** ustaw 1-cyfrowy kod DTMF z zakresu **(0-9, \* i #)**.
- **2~4 cyfry DTMF:** ustaw kod DTMF zgodnie z **opcją DMTP**. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli **tryb DTMF jest** ustawiony na 3 cyfry.
- **Status przekaźnika:** status przekaźnika jest domyślnie niski, co oznacza stan normalnie zamknięty (NC). Jeśli stan przekaźnika jest wysoki, oznacza to, że jest on normalnie otwarty (NO).
- **Nazwa przekaźnika:** nazwij przełącznik przekaźnika zgodnie z potrzebami. Dla wygody można na przykład nazwać przełącznik przekaźnika zgodnie z jego lokalizacją.

## Uwaga

- Tylko urządzenia zewnętrzne połączone do przełącznika przekaźnikowego muszą być zasilane przez zasilacze, ponieważ przełącznik przekaźnikowy nie dostarcza zasilania.
- Jeśli tryb DTMF jest ustawiony na **1-cyfrowy DTMF**, nie można edytować kodu DTMF w **2~4-cyfrowym DTMF**. A jeśli ustawisz tryb DTMF z 2-4 w polu **2~4-cyfrowym DTMF**, nie można edytować kodu DTMF w polu **1-cyfrowym 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 internetowym, w którym należy podać takie informacje, jak adres IP przekaźnika, hasło, akcja przekaźnika sieciowego itp. Przed uzyskaniem dostępu do drzwi za pośrednictwem przekaźnika internetowego.

**Adres IP, nazwa użytkownika i hasło** są dostarczane przez producenta sieci.

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

**Web Relay**

Type	<input type="text" value="Disabled"/>
IP Address	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password" value="*****"/>

---

**Web Relay Action Setting**

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
01	<input type="text"/>	<input type="text"/>	<input type="text"/>
02	<input type="text"/>	<input type="text"/>	<input type="text"/>
03	<input type="text"/>	<input type="text"/>	<input type="text"/>
04	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Konfiguracja parametrów :**

- **Typ:** wybierz jedną z trzech opcji: **Wyłączone**, **Przełącznik sieciowy** i **Oba**. Wybierz **Web Relay**, aby włączyć przełącznik internetowy. Wybierz **Disable**, aby wyłączyć przełącznik sieciowy. Wybierz opcję **Oba**, aby włączyć zarówno przełącznik lokalny, jak i internetowy.
- **Hasło :** Hasło jest uwierzytelniane przez HTTP i można je zdefiniować za pomocą **http get** in Action.
- **Web Relay Action (Akcja przełącznika sieciowego):** wprowadź określone polecenie akcji przełącznika sieciowego dostarczone przez producenta sieci w celu wykonania różnych akcji przez przełącznik sieciowy.
- **Klucz przełącznika internetowego:** wprowadź skonfigurowany kod DTMF, gdy drzwi zostaną odblokowane za pomocą kodu DTMF, polecenie akcji zostanie automatycznie wysłane do przełącznika internetowego.

Aby wybrać wstępną konfigurację w interfejsie sieci **Web Directory > User > Add > Access Setting**.

**Access Setting**

Allow To Open	<input checked="" type="checkbox"/> RelayA <input type="checkbox"/> RelayB <input type="checkbox"/> RelayC
Web Relay	<input type="text" value="0"/>
Buidling	<input type="text"/>
Floor No.	<input type="text" value="NULL x"/>
Room	<input type="text"/>

1 item    Unselected Schedules

1002:Never

1 item    Selected Schedules

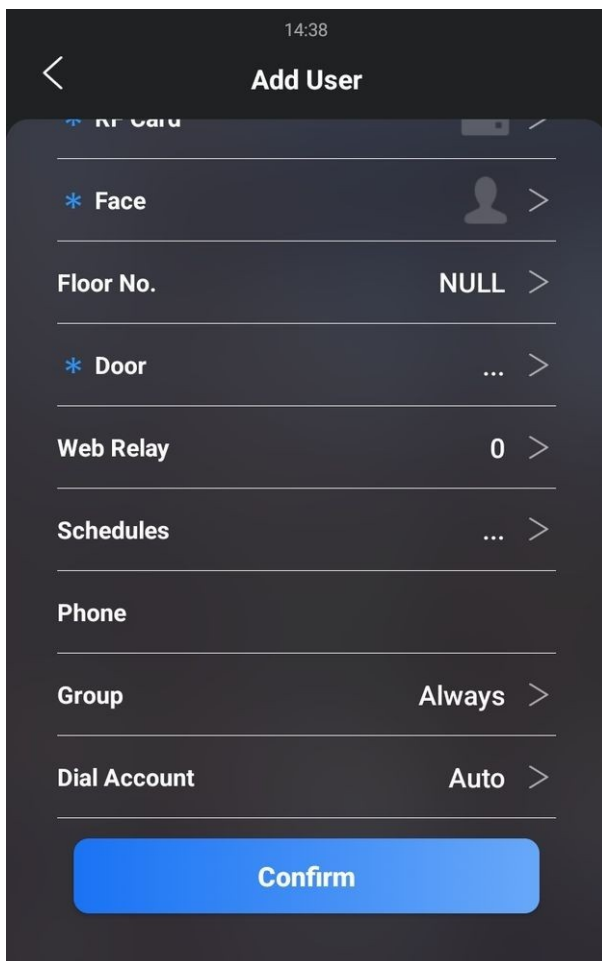
1001:Always

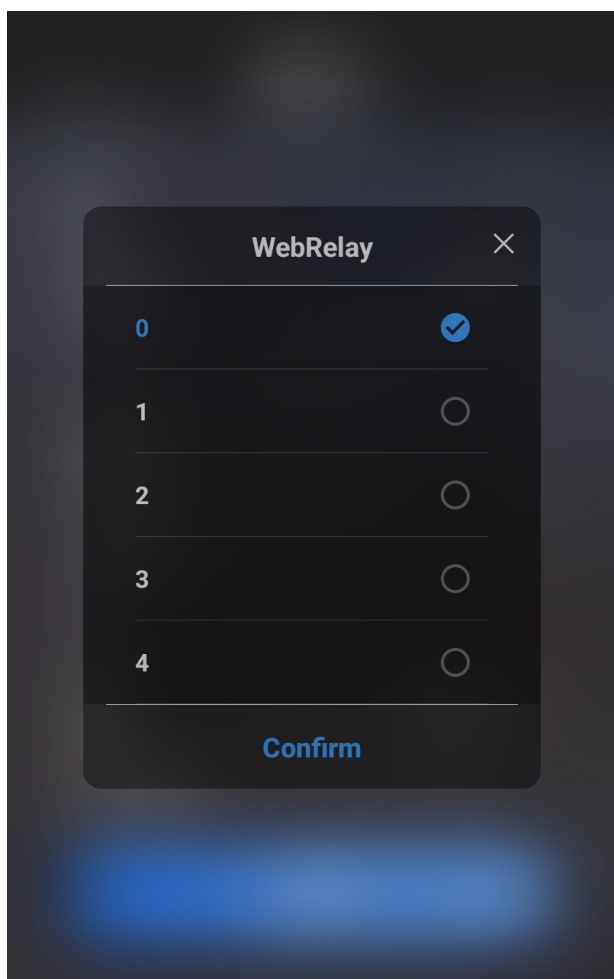
>
<

## Konfiguracja Web Relay na urządzeniu

Można wybrać identyfikator akcji przekaźnika sieciowego, aby wyzwoić określone akcje przekaźnika sieciowego, na przykład otwarcie drzwi.

Przejdź do **Ustawienia > Użytkownik > Lista użytkowników**, a następnie naciśnij **Dodaj**.





## Przełącznik bezpieczeństwa

Przełącznik 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 przełącznik zabezpieczeń, przejdź do interfejsu **Access Control > Relay > Security Relay**.



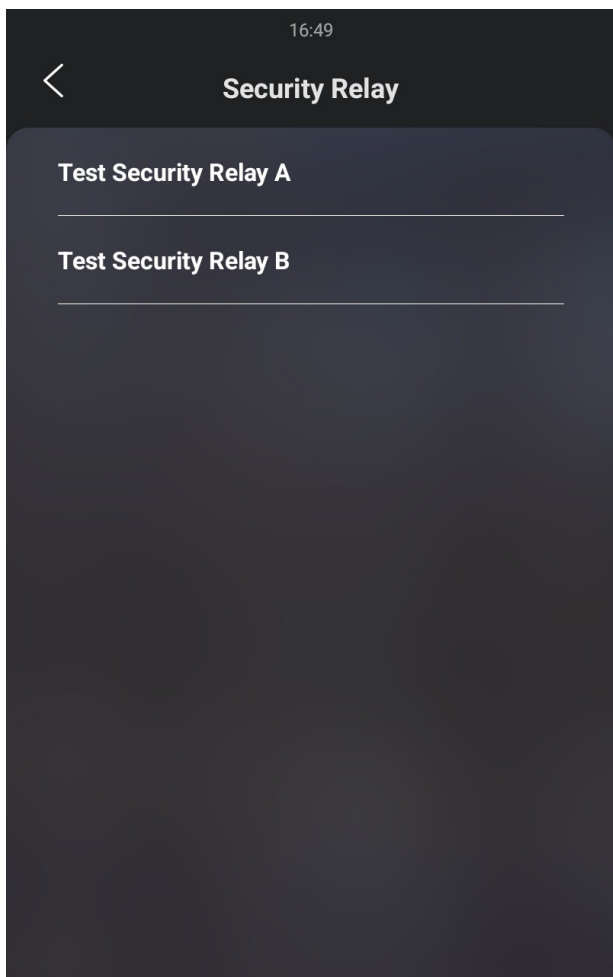
**Security Relay**

Relay ID	<input type="text" value="Security Re..."/>	<input type="text" value="Security Re..."/>
Enabled	<input type="checkbox"/>	<input type="checkbox"/>
Connect Type	<input type="text" value="Relay A Po..."/>	<input type="text" value="RS485"/>
Trigger Delay(Sec)	<input type="text" value="0"/>	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>	<input type="text" value="5"/>
1 Digit DTMF	<input type="text" value="3"/>	<input type="text" value="4"/>
2~4 Digits DTMF	<input type="text" value="013"/>	<input type="text" value="014"/>
Relay Name	<input type="text" value="Security Relay A"/>	<input type="text" value="Security Relay B"/>
	<input type="button" value="Test"/>	<input type="button" value="Test"/>

### Konfiguracja parametrów :

- **Typ połączenia:** wybierz typ połączenia między przekaźnikiem bezpieczeństwa a bramofonem.  
Można wybrać połączenie przez wyjście zasilania przekaźnika A bramofonu lub RS485.
- **Trigger Delay (Sec):** ustaw czas opóźnienia wyzwolenia przekaźnika (w zakresie od 1 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia na 5 sekund, przekaźnik zostanie wyzwolony dopiero 5 sekund po naciśnięciu zakładki Unlock. Domyślną wartością jest 0, co oznacza wyzwolenie przekaźnika zaraz po naciśnięciu przycisku odblokowania.
- **Opóźnienie wstrzymania (sek.):** ustaw czas opóźnienia wstrzymania przekaźnika (w zakresie od 1 do 10 sek.) Na przykład, jeśli ustawisz czas opóźnienia wstrzymania na 5 sekund, przekaźnik zostanie opóźniony o 5 sekund po odblokowaniu drzwi.
- **1 Digit DTMF :** ustaw 1-cyfrowy kod 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.

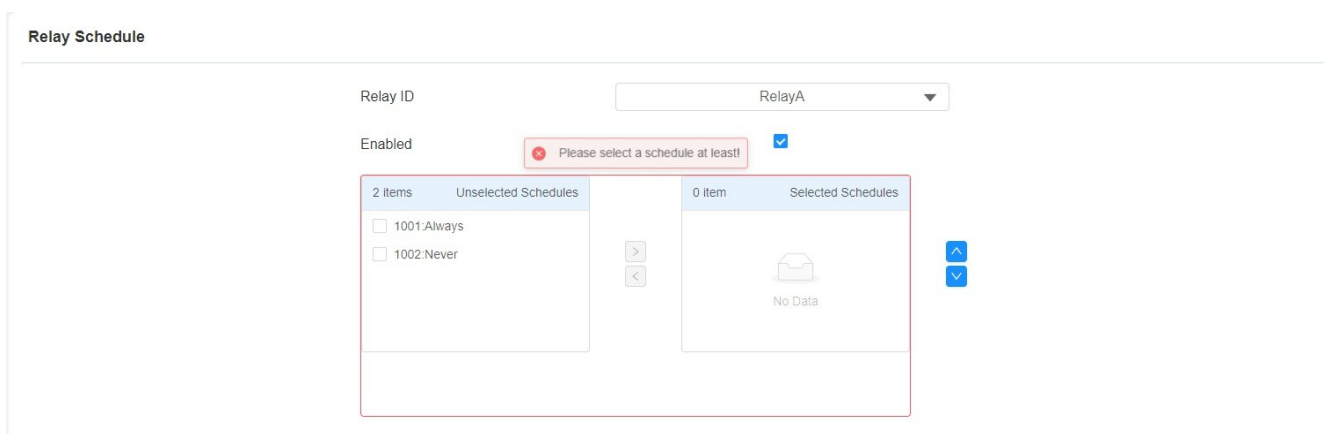
Możesz także przetestować przekaźnik bezpieczeństwa na urządzeniu, przejdź do **Security > Security Relay**.



## 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. Wystarczy ją włączyć i wybrać harmonogram. Aby utworzyć harmonogram, zapoznaj się z konfiguracją harmonogramu dostępu do drzwi.

#### Uwaga

Ustawienia harmonogramu przekaźnika można znaleźć w sekcji [\*\*Tworzenie harmonogramu dostępu do drzwi.\*\*](#)

Konfiguracja harmonogramu przekaźnika jest identyczna z harmonogramem dostępu do drzwi.

# Zarządzanie harmonogramem dostępu do drzwi

## Harmonogram dostępu

Można tworzyć harmonogramy dostępu do drzwi, aby później wygodnie zastosować je do kontroli dostępu do drzwi przeznaczonej dla poszczególnych użytkowników lub utworzonej grupy użytkowników. Ponadto w razie potrzeby można edytować harmonogram dostępu do drzwi.

## Tworzenie harmonogramu dostępu

Harmonogram dostępu do drzwi można tworzyć codziennie lub co miesiąc, a oprócz uruchamiania harmonogramu dostępu do drzwi codziennie lub co miesiąc można także utworzyć harmonogram umożliwiający planowanie na dłuższy okres czasu.

Aby ją skonfigurować, przejdź do opcji **Ustawienia > Harmonogram** interfejsu.

Schedule

All Search + Add Import Export

<input type="checkbox"/>	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
<input type="checkbox"/>	1	1002	Local	Daily	Never	--	--	-	
<input type="checkbox"/>	2	1001	Local	Daily	Always	--	--	00:00:00-23:59...	

Selected: 0/2 Delete Delete All Total: 2 Prev 1/1 Next Go To Page 1 Go

**Aby utworzyć harmonogram dzienny, można wykonać następujące czynności:**

### Add Schedule X

Mode Daily

Name

Start Time - End Time 00:00 - 00:00

Cancel Submit

**Aby utworzyć harmonogram tygodniowy:**

### Add Schedule ✕

Mode:

Name:

Day:  Mon  Tue  Wed  
 Thur  Fri  Sat  
 Sun  Check All

Start Time - End Time:  -

**Aby utworzyć harmonogram na dłuższy okres:**

### Add Schedule ✕

Mode:

Name:

Start Date - End Date:  ~

Day:  Mon  Tue  Wed  
 Thur  Fri  Sat  
 Sun  Check All

Start Time - End Time:  -

## Tworzenie harmonogramu dostępu na urządzeniu

Ścieżka: **Ustawienia podstawowe > Harmonogram > Dodaj .**

16:50

< **Add Schedule**

Mode Normal >

\* Name

Start Date 2023-10-16 >

End Date 2023-10-16 >

Day ... >

Start Time 00:00 >

End Time 00:00 >

**Confirm**

## Harmonogram dostępu do importu i eksportu

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

Aby skonfigurować go w interfejsie **Ustawienia > Harmonogram**.

Schedule									
Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit	
					All	Search	+ Add	Import	Export

### Import ✕

(Format: .xml)

Not selected any files
Select File
↻ Reset

Cancel
Upload

### Uwaga

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

## Edycja harmonogramu dostępu do drzwi

### Edycja harmonogramu dostępu do drzwi w interfejsie internetowym

Jeśli chcesz edytować lub usunąć utworzony harmonogram dostępu do drzwi, możesz edytować lub usunąć skonfigurowany harmonogram osobno lub zbiorczo w interfejsie Web **Setting** >

#### Schedule.

**Schedule**

All ▾
Search
+ Add
📄 Import
Export ▾

<input type="checkbox"/>	Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	Edit
<input type="checkbox"/>	1	1002	Local	Daily	Never	--	--	-	
<input type="checkbox"/>	2	1001	Local	Daily	Always	--	--	00:00:00-23:59...	

Selected: 0/2
🗑 Delete
🗑 Delete All
Total: 2
Prev
1/1
Next
Go To Page

Go

### Edycja harmonogramu dostępu do drzwi na urządzeniu

Ścieżka: **Ustawienia podstawowe** > **Harmonogram** > **Dodaj** .



### Add Schedule

Mode Normal >

\* Name

Start Date 2023-10-16 >

End Date 2023-10-16 >

Day ... >


Start Time 00:00 >

End Time 00:00 >

**Confirm**



16:51

< **Schedule** 

**1** **Name : schedule**

Mode: Normal

Date: 20231016 - 20231016

Day: Mon,Tues,Wed,Thur,Fri,Sat,Sun

Time: 00:00:00 - 01:00:00

---

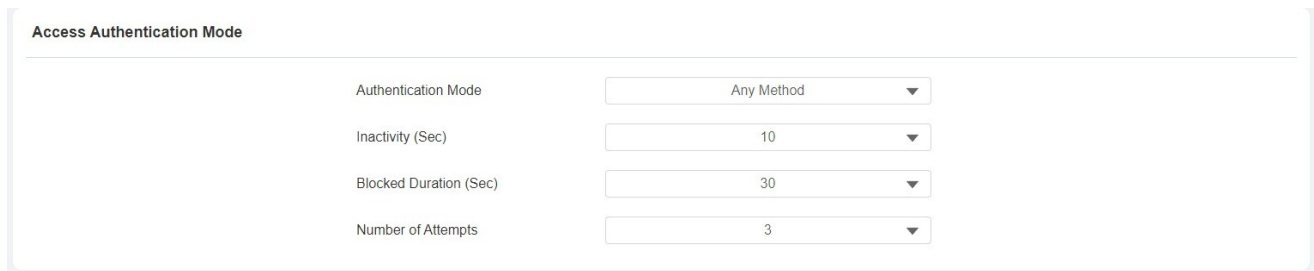
**Add**

# Konfiguracja odblokowania drzwi

## Uwierzytelnianie dostępu

Można skonfigurować wiele trybów uwierzytelniania dostępu i skonfigurować zabezpieczenia uwierzytelniania zgodnie z potrzebami. W Internecie przejdź do interfejsu **Ustawienia**>

### Klucz/Wyświetlacz > Tryb uwierzytelniania dostępu.

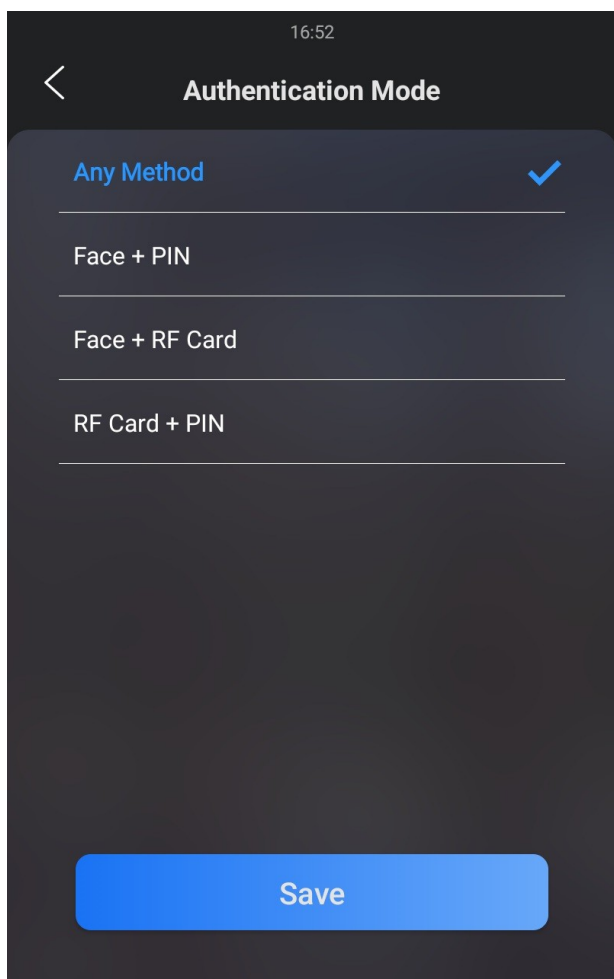


Access Authentication Mode	
Authentication Mode	Any Method
Inactivity (Sec)	10
Blocked Duration (Sec)	30
Number of Attempts	3

### 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 + Card**, jeśli chcesz zastosować podwójne metody dostępu (twarz + karta RF) do odblokowywania drzwi. Wybierz **Card + PIN**, jeśli chcesz zastosować podwójne metody dostępu (karta + PIN) do odblokowywania drzwi.
- **Inactivity (Sec):** ustawienie limitu czasu uwierzytelniania dla drugiego uwierzytelniania. Na przykład w przypadku uwierzytelniania **Face+PIN**, jeśli ustawisz limit czasu uwierzytelniania na 10 sekund, musisz wprowadzić kod PIN dziesięć sekund po pomyślnym rozpoznaniu twarzy, w przeciwnym razie ekran powróci do ekranu głównego.
- **Blocked Duration (Sec):** ustaw czas blokady dla pierwszego uwierzytelnienia. Na przykład, jeśli ustawisz liczbę prób na 3, a nie uda Ci się przejść drugiego uwierzytelnienia trzy razy, zostaniesz tymczasowo zablokowany przed pierwszym uwierzytelnieniem zgodnie z określonym czasem blokady.
- **Number of Attempts (Liczba prób):** umożliwia wysłanie dozwolonej liczby prób drugiego uwierzytelnienia.

Aby skonfigurować tryb uwierzytelniania na urządzeniu, przejdź do **Bezpieczeństwo > Tryb uwierzytelniania** .



## 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

Publiczny kod PIN można skonfigurować w interfejsie internetowym urządzenia **Kontrola dostępu > Ustawienia kodu PIN > Publiczny kod PIN**.

Public PIN

---

Enabled

PIN Code

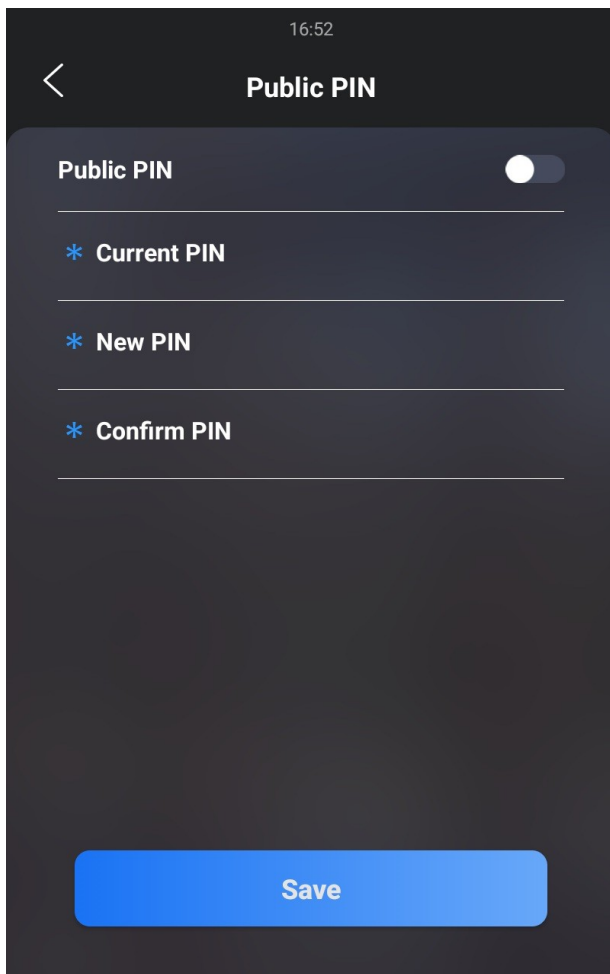
### Uwa

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

### Konfiguracja parametrów :

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

Aby skonfigurować go na urządzeniu, przejdź do opcji **Zabezpieczenia > Publiczny PIN**.



### Uwa

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

## Dodaj użytkownika

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

Przejdź do **Katalog > Użytkownik > + Dodaj > Podstawowy** interfejs użytkownika.

User Basic

---

UserID	<input type="text" value="1"/>
Name	<input type="text"/>

### Konfiguracja parametrów :

- **Identyfikator użytkownika:** Identyfikator użytkownika może zostać wygenerowany automatycznie przez system.

## 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 w sieci Web **Directory > User > +Add** interface.

User

---

All

<input type="checkbox"/>	Index	Source	UserID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											

---

**Private PIN**

Code

Przewiń w dół do opcji Ustawienia dostępu i wybierz harmonogram dostępu do drzwi dla prywatnego dostępu do drzwi z kodem PIN:

### Access Setting

Allow To Open

Web Relay

Buidling

Floor No.

Room

RelayA  RelayB  RelayC

0

NULL x

1 item Unselected Schedules

1002:Never

1 item Selected Schedules

1001:Always

### Konfiguracja parametrów :

- **Allow To Open:** wybór przekaźnika odblokowującego drzwi dla użytkownika.
- **Przekaźnik sieciowy:** wybierz określoną liczbę poleceń akcji przekaźnika sieciowego skonfigurowanych w interfejsie sieciowym.
- **Harmonogram :** wybierz jeden z utworzonych harmonogramów dostępu do drzwi w lewym 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 to identyczne w konfiguracji.

## Konfiguracja prywatnego kodu PIN na urządzeniu

Na urządzeniu można skonfigurować prywatny kod PIN dla określonego użytkownika.

Aby skonfigurować język wyświetlany na urządzeniu, wybierz kolejno opcje **Basic Setting (Ustawienia podstawowe) > User (Użytkownik) > User List (Lista użytkowników) > Add screen (Dodaj ekran)**.

16:53

< Add User

\* User ID : 1

\* Name

PIN

RF Card

Face

Floor No. NULL

\* Door ...

Web Relay 0

Schedules ...

Confirm

## 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.

Aby go skonfigurować, przejdź do opcji **Kontrola dostępu > Ustawienia kodu PIN > Interfejs prywatnego kodu PIN**.

Private PIN

PIN Mode PIN

### Konfiguracja parametrów :

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

**Uwaga**

Numer mieszkania można zastosować tylko wtedy, gdy urządzenie zostanie dodane do Akuvox SmartPlus.

## Konfiguracja karty RF do odblokowywania drzwi

### Konfiguracja karty RF w interfejsie internetowym

Aby skonfigurować go w interfejsie sieci **Web Directory > User > + Add > RF Card**.

The screenshot shows a web interface for configuring an RF Card. At the top left, it says 'RF Card'. Below this, there is a 'Code' label followed by an empty input field. To the right of the input field are two buttons: a blue 'Obtain' button and a red 'Delete' button with a trash icon. Below the input field and buttons is a large blue 'Add' button.

**Uwaga**

- Więcej informacji można znaleźć w rozdziale Wybór harmonogramu dostępu do kodu PIN dla użytkownika(-ów) karty RF.  
Karta RF o częstotliwości 13,56 MHz i 125 kHz może być stosowana do bramofonu w celu uzyskania dostępu do drzwi.

### Konfiguracja karty RF na urządzeniu

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

Aby skonfigurować na urządzeniu **Ustawienia>Użytkownik>Lista użytkowników>Dodaj** interfejs.





16:53


< **Add User**

\* User ID : 1

\* Name

PIN  >

**RF Card**  >

Face  >

Floor No. NULL >

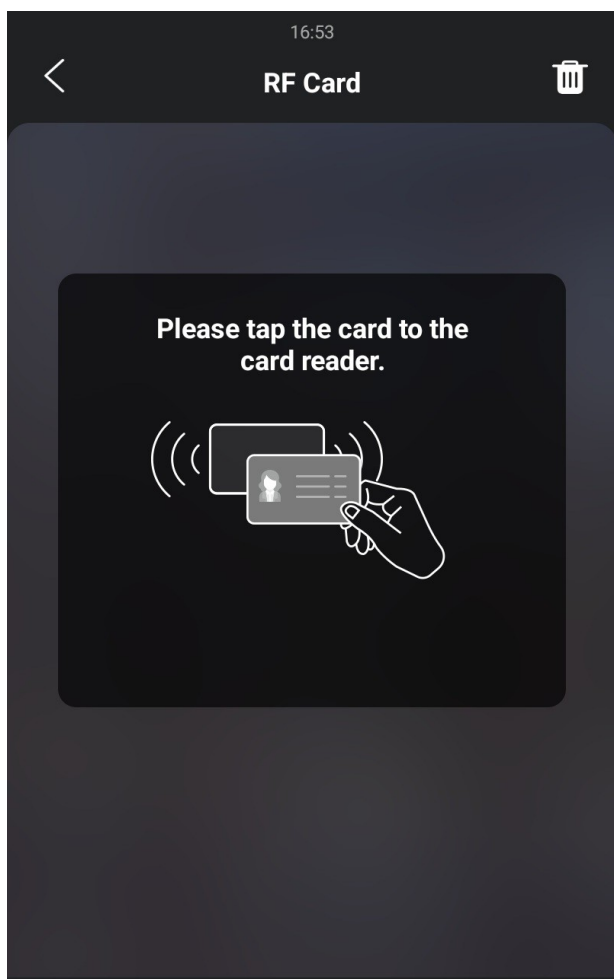
\* Door ... >

Web Relay 0 >

Schedules ... >

**Confirm**

P



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

RFID	
IC Card Display Mode	8HN ▼
ID Card Order	Normal ▼
ID Card Display Mode	8HN ▼

### Konfiguracja parametrów :

- **IC-Card Display Mode (Tryb wyświetlania karty IC):** wybór formatu karty ID dla dostępu do drzwi (**8H10D, 6H3D 5D(W26), 6H8D, 8HN, 6H3D 5D-R(W26), 8HR10D i 8HR**). Karta  
Format kodu karty to domyślnie 8HN.
- **Kolejność kart ID:** wybierz odczyt kart ID w normalnej lub odwróconej kolejności. Możesz potrzebować

aby wybrać zamówienia kart do integracji z innymi firmami (np. kontrola dostępu innych firm). można również odwrócić numer karty w celu ochrony karty.

- **Tryb wyświetlania karty ID** : Wybór formatu karty ID dla dostępu do drzwi: **8H10D**; **6H3D 5D(W26)**; **6H8D**; **8HN**; **8HR**, **6H3D 5D-R(W26)** i **8HR10D** . W przypadku Domyślny format kodu karty w bramofonie to 8HN.

## Bezstykowa karta inteligentna

W celu uzyskania dostępu zbliżeniowego można wybrać kartę NFC lub kartę Felica. Na przykład, jeśli włączysz zarówno karty NFC, jak i Felica, możesz uzyskać dostęp zbliżeniowy za pomocą obu typów kart.

Ścieżka: **Access Control > Card Setting > Contactless Smart Card** .

Contactless Smart Card	
Enabled	NFC

## Szyfrowanie kart Mifare/Desfire

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

W tym celu można przejść do opcji **Kontrola dostępu > Ustawienia karty > Szyfrowanie karty Mifare/Desfire**.

Mifare/Desfire Card Encryption	
Enabled	Classic
Sector/Block	0 / 0
Block Key	....

Mifare/Desfire Card Encryption	
Enabled	DesFire
App ID	(6 hex numbers)
File ID	(0-16)
Crypto	AES
Key	....
Key Index	(0-11)

**Konfiguracja parametrów :**

**Sector/Block** : wprowadź sektor i blok, w którym numer karty znajduje się na karcie Mifare/ Defire. Na przykład numer karty może znajdować się w sektorze 3 i bloku 3 na

- karcie.
- **Block Key**: wprowadź hasło bloku dostępu. •

**Crypto**: wybierz spośród AES i DES.

## Konfiguracja rozpoznawania twarzy do odblokowywania drzwi

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

## 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.

Aby to zrobić na urządzeniu, przejdź do **Ustawienia > Użytkownik > Lista użytkowników > Dodaj > Interfejs twarzy**.

17:44

< Add User

\* User ID : 1

\* Name

PIN >

RF Card >

Face >

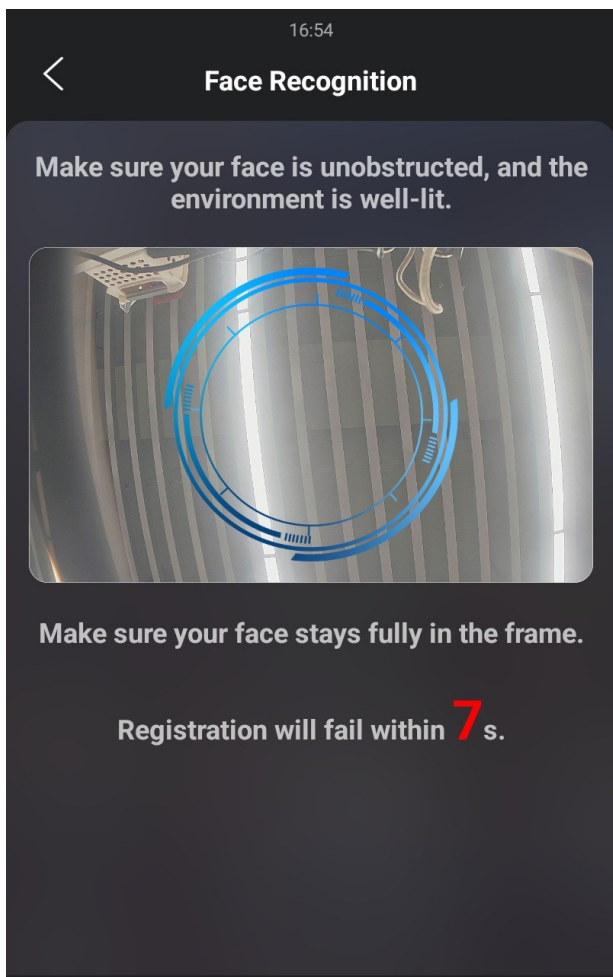
Floor No. NULL >

\* Door ... >

Web Relay 0 >

Schedules ... >

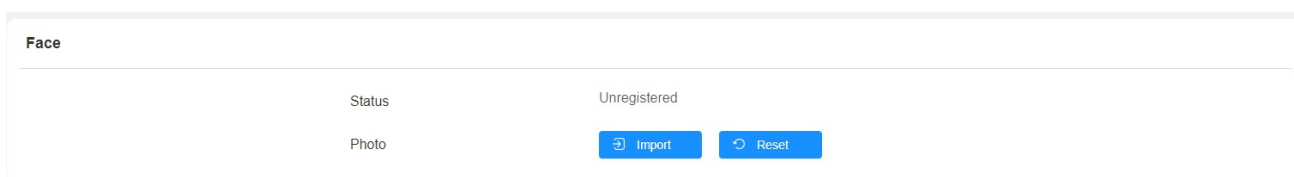
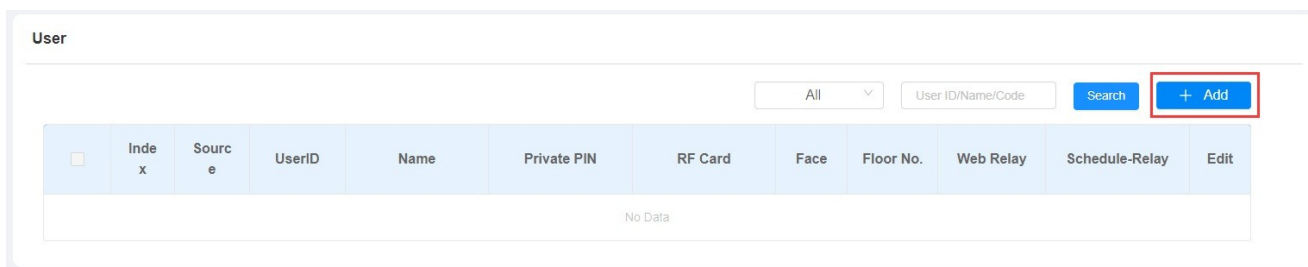
Confirm



## 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 możesz przesłać zdjęcie twarzy.

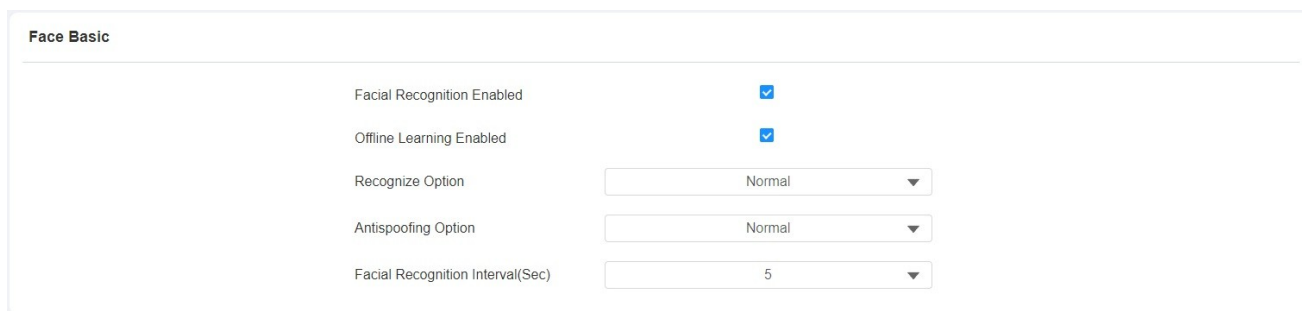


## Uwaga

Zdjęcia, które mają zostać przesłane, powinny być w formacie jpg lub png.

## Konfiguracja rozpoznawania twarzy w interfejsie internetowym

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



Face Basic	
Facial Recognition Enabled	<input checked="" type="checkbox"/>
Offline Learning Enabled	<input checked="" type="checkbox"/>
Recognize Option	Normal
Antispoofing Option	Normal
Facial Recognition Interval(Sec)	5

### Konfiguracja parametrów :

- **Offline Learning Enabled** : zaznacz to pole, 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.
- **Recognize Option**: 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 pomyłony z Tobą przez pomyłkę lub w inny sposób podczas rozpoznawania twarzy.
- **Opcja antyspoofingu**: wybierz poziom antyspoofingu spośród czterech opcji: **Niski**, **Normalny**, **Wysoki** i **Najwyższy**. Na przykład, jeśli wybierzesz **Najwyższy**, będzie najmniejsze prawdopodobieństwo, że urządzenie zostanie oszukane przez obrazy cyfrowe lub zdjęcia dowolnego rodzaju.
- **Facial Recognition Interval(Sec) (Interwał rozpoznawania twarzy(sek.))**: wybierz interwał czasowy między każdymi dwoma rozpoznaniem twarzy w zakresie od 1 do 8 minut. Na przykład, jeśli wybierzesz **5**, będziesz musiał odczekać 5 minut, zanim będziesz mógł ponownie wykonać rozpoznawanie twarzy.

## Edycja danych dostępu do drzwi specyficznych dla użytkownika

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

> Interfejs **użytkownika**.

User

All  Search

	Index	Source	UserID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											

## Import i eksport danych użytkownika kontroli dostępu

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

Aby ją skonfigurować, przejdź do menu **Directory>User>Import/Export User** interface.

Import/Export User

User Data

## Konfiguracja Bluetooth do odblokowywania drzwi

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

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

BLE Basic

Enabled

RSSI Threshold  (-85~-50db)

Open Door Interval(Sec)

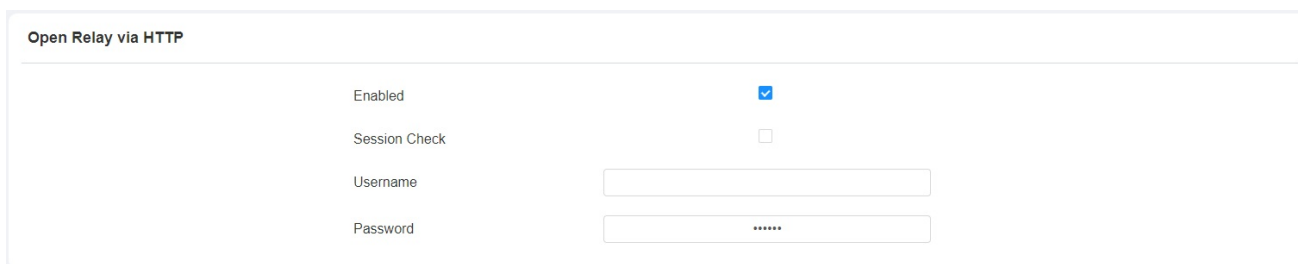
### Konfiguracja parametrów :

- **Próg RSSI:** wybierz siłę odbieranego sygnału w zakresie -85 ~ -50db w wartościach bezwzględnych, im wyższa wartość, tym większa siła. Wartość domyślna to 72 dB w wartościach bezwzględnych.
- **Interwał otwarcia drzwi (sek.):** wybór interwału czasowego między dwoma otwarciami drzwi Bluetooth.

## Konfiguracja Open Relay przez HTTP dla odblokowywania drzwi

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

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



Open Relay via HTTP	
Enabled	<input checked="" type="checkbox"/>
Session Check	<input type="checkbox"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>

### Konfiguracja parametrów :

- **Kontrola sesji**: włącz ją, aby chronić bezpieczeństwo transmisji danych.
- **User Name** : wprowadź nazwę użytkownika interfejsu internetowego urządzenia, na przykład **admin**.
- **Hasło** : wprowadź hasło dla polecenia HTTP. Na przykład **12345** .

### Zapoznaj się z poniższym przykładem:

`http://192.168.35.127/fcgi/do?`

`action=OpenDoor&UserName=admin&Password=12345&DoorNum=1`

#### Uwaga

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

## 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.

Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu > Przełącznik > Otwórz przekaźnik za pomocą interfejsu QR Code**.



Open Relay Via QR Code

Enabled

## Uwaga

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

## Konfiguracja przycisku wyjścia do odblokowywania drzwi

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

Aby go skonfigurować, przejdź do opcji **Access Control >Input >Input A** interface.

Input A

Enabled

Trigger Electrical Level

Action To Execute  FTP  Email  HTTP  
 TFTP  SIP Call

HTTP URL

Action Delay  (0-300Sec)

Action Delay Mode

Execute Relay

Break-in Intrusion

Door Status

Super Mode

### Konfiguracja parametrów :

- **Poziom** wyzwania elektrycznego: wybór opcji poziomu wyzwania elektrycznego pomiędzy **wysokim** i **niskim** zgodnie z rzeczywistym działaniem przycisku wyjścia.
- **Akcja do wykonania** : wybierz metodę wykonania akcji spośród czterech opcji: **FTP, Email, 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 **wykonania bezwarunkowego** akcja zostanie wykonana.

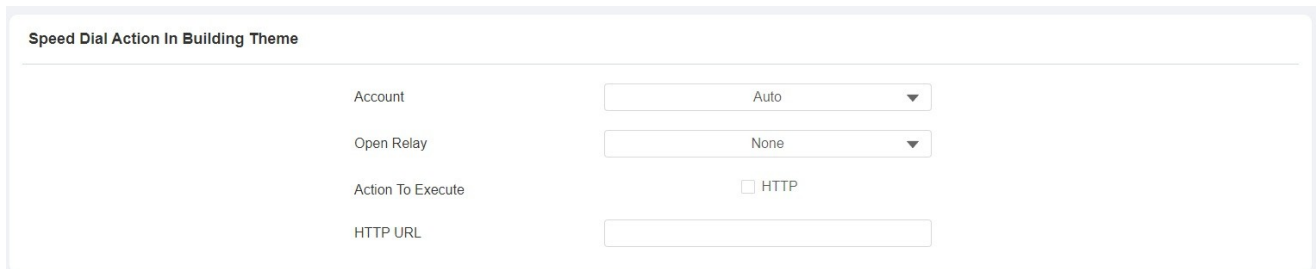
gdy wejście zostanie wyzwolone. W przypadku wybrania opcji **Wykonaj, jeśli wejście jest nadal wyzwolone**, akcja zostanie wykonana, jeśli wejście pozostanie wyzwolone. Na przykład, jeśli drzwi pozostaną otwarte po wyzwoleniu wejścia, akcja

- taka jak wiadomość e-mail zostanie wysłana w celu powiadomienia odbiorcy.
- **Execute Relay**: konfigurowanie przekaźników wyzwalanych przez wejście.
- **Włamanie**: włącza alarm, gdy drzwi zostaną odblokowane w nietypowy sposób. **Tryb super**: po włączeniu trybu super administrator będzie mógł otworzyć drzwi za pomocą karty RF, nawet jeśli bramofon ulegnie awarii lub usterce.

## Skonfiguruj kartę odbioru dla odblokowywania drzwi

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

Aby ją skonfigurować, przejdź do opcji **Ustawienia > Klawisze/Wyświetlacz > Akcja szybkiego wybierania w interfejsie motywu budynku**.



Account	Auto
Open Relay	None
Action To Execute	<input type="checkbox"/> HTTP
HTTP URL	

### Konfiguracja parametrów :

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

## 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 ją skonfigurować, przejdź do opcji **Kontrola dostępu > Interfejs przekaźnika**.

#### Relay

Relay ID	RelayA ▼	RelayB ▼	RelayC ▼
Type	Default State▼	Default State▼	Default State▼
Mode	Monostable ▼	Monostable ▼	Monostable ▼
Trigger Delay(Sec)	0 ▼	0 ▼	0 ▼
Hold Delay(Sec)	5 ▼	5 ▼	5 ▼
DTMF Mode	1 Digit DTMF▼		
1 Digit DTMF	# ▼	1 ▼	2 ▼
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	Relay1	RelayB	RelayC

#### Uwaga

Więcej informacji można znaleźć w sekcji **Konfiguracja transmisji danych DTMF** w [ustawieniach](#) połączeń, określone ustawienie kodu DTMF.

Zaangażowane urządzenia interkomowe muszą być zgodne pod względem typu DTMF, w przeciwnym razie nie można zastosować kodu DTMF.

## Bezpieczeństwo

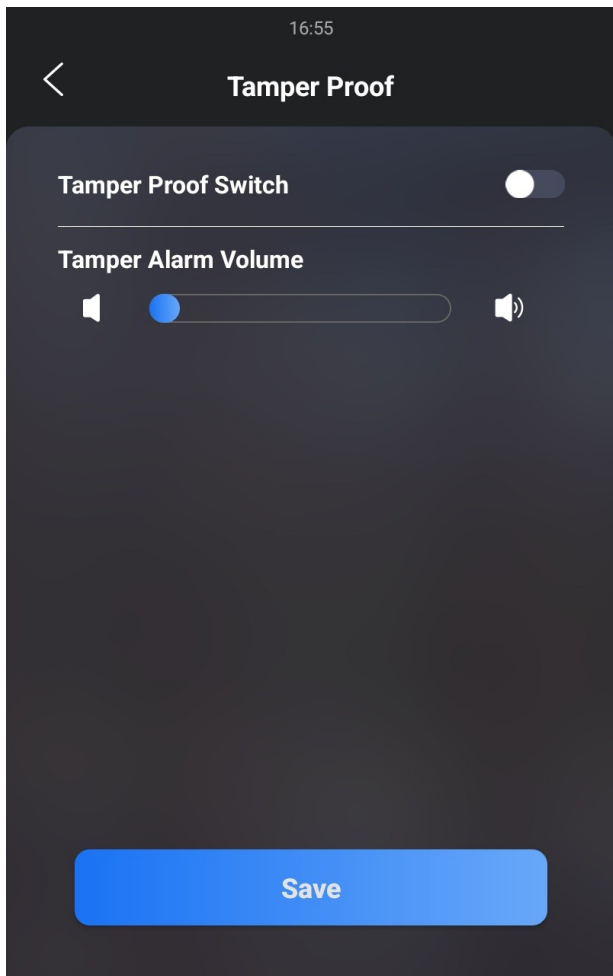
### Ustawienie alarmu sabotażowego

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

### Konfiguracja alarmu sabotażowego na urządzeniu

Alarm antysabotażowy i czujnik grawitacyjny można łatwo skonfigurować w bramofonie. Aby skonfigurować alarm antysabotażowy, przejdź do opcji

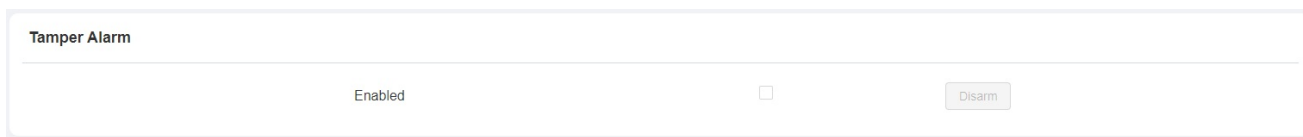
**Setting > Security > Tamper Proof.**



## Konfiguracja alarmu sabotażowego w interfejsie sieciowym

Funkcję alarmu sabotażowego można również włączyć w interfejsie internetowym.

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



## Bezpieczeństwo blokady

Bramofon może współpracować z innymi zamkami i czujnikami drzwi, aby zapewnić bezpieczeństwo zamka. Uruchomi alarm, aby powiadomić użytkowników, jeśli czujnik drzwi wykryje, że drzwi są otwarte lub nie są całkowicie zamknięte.

Na urządzeniu wybierz kolejno opcje **Zabezpieczenia > Blokada**.

16:55

< Lock

Lock Type  Positive  Negative

---

Lock Delay 0Sec >

---

Magnetism Type OFF >

---

Magnetism Delay 20Sec >

---

Save



### Konfiguracja parametrów :

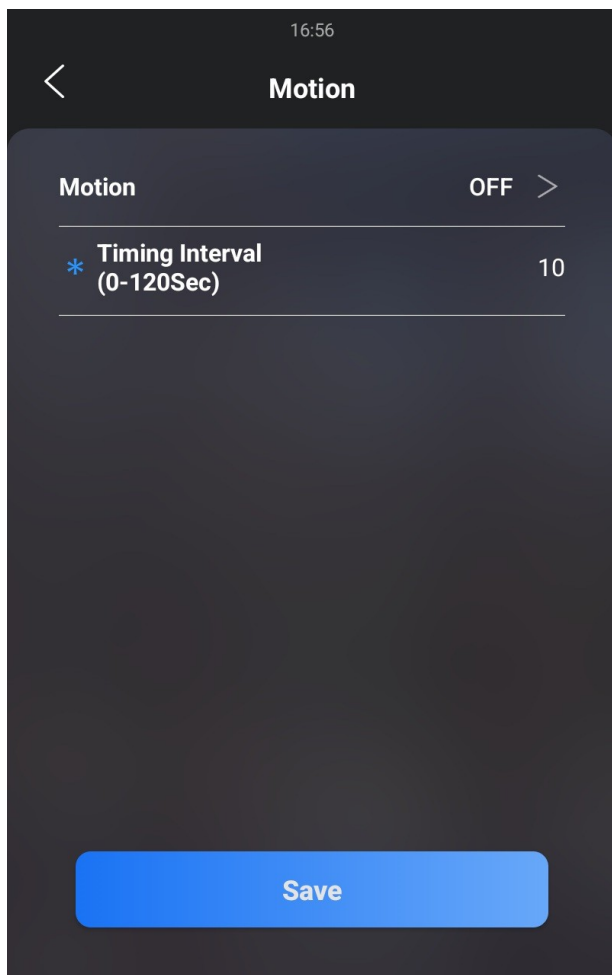
- **Typ blokady:** wybierz **Pozytywny** dla blokady, która odblokowuje się, gdy zasilanie jest włączone i wybierz **Negatywny** dla blokady, która odblokowuje się, gdy zasilanie jest wyłączone.
- **Opóźnienie blokady:** wybierz czas opóźnienia odblokowania drzwi po przyznaniu dostępu do drzwi. Zakres czasu opóźnienia wynosi od 0 do 10 sekund.
- **Magnetism Type :** wybierz **OFF**, jeśli chcesz wyłączyć czujnik drzwi i alarm. Aby ustawić typ wyzwalania alarmu, należy wybrać **ON-ALARM** i **OFF\_ALARM** zgodnie z zastosowanym typem blokady. Wybierz **ON\_ALARM** dla blokady dodatniej, a **OFF\_ALARM** dla blokady ujemnej.
- **Magnetism Delay:** wybór czasu opóźnienia alarmu po jego wyzwoleniu. Zakres opóźnienia wynosi od 10 do 120 sekund.

## Wykrywanie ruchu

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

## Konfiguracja wykrywania ruchu na urządzeniu

Możesz włączyć wykrywanie ruchu i skonfigurować interwał wykrywania ruchu na ekranie **Ustawienia zaawansowane urządzenia > Nadzór > Ruch**.



### Konfiguracja parametrów :

- **Interwał:** bezwzględny interwał wyzwalania wynosi 3 sekundy. W przypadku wybrania liczby większej niż 3 sekundy do wyzwolenia alarmu wymagany jest drugi interwał wyzwalania. Na przykład, jeśli wybierzesz 3 sekundy, alarm zostanie wyzwolony, gdy poruszający się obiekt zostanie wykryty jeden raz od 0 do 3 sekund (wyzwolony w dowolnym momencie od 0 do 3 sekund). Jeśli jednak na przykład wybrana zostanie opcja 5 sekund (więcej niż 3), alarm nie zostanie wyzwolony, dopóki poruszający się obiekt nie zostanie wykryty po raz drugi w przedziale od 3 do 5 sekund (wyzwolony w dowolnym momencie w przedziale od 3 do 5 sekund). Domyślny interwał wynosi 10 sekund.

## Konfiguracja wykrywania ruchu w interfejsie internetowym

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

Aby skonfigurować go w interfejsie internetowym **Surveillance > Motion > Motion Detection Options**.

**Motion Detection Options**

---


Suspicious Moving Object Detection Video + Radar ▼

Time Interval  (0-120Sec)

Detection Range  (m)

Detection Accuracy  (0-6)

Detection Area



Move the arrow to the start point, left click and hold down the mouse button, then drag the arrow to select an area. You can draw up to three detection area.

### Konfiguracja parametrów :

- **Wykrywanie podejrzanych ruchomych obiektów:** do wyboru są opcje **Wyłączone**, **Wykrywanie wideo**, **Wykrywanie radaru** i **Wideo + Radar**.
- **Interwał czasowy:** ustaw interwał czasowy w taki sam sposób, jak na urządzeniu.
- **Zasięg wykrywania:** ustawienie zasięgu wykrywania radaru (1-3 metry). Domyślny zasięg wykrywania wynosi 3 metry.
- **Dokładność wykrywania:** ustawienie dokładności wykrywania dla czułości wykrywania (0-6). Im wyższa wartość, tym większa czułość. Domyślna wartość dokładności wykrywania to 3.

Po skonfigurowaniu interwału można skonfigurować wymaganą akcję.

**Motion Action**

---

Action To Execute  FTP  Email  SIP Call  
 HTTP  TFTP

Execute Relay  ▼



## Konfiguracja parametrów :

- **Akcja do wykonania** : wybierz metodę wykonania akcji: FTP, Email, HTTP, TFTP, SIP Call. Na przykład, jeśli wybierzesz Email, wiadomość Email zostanie wysłana do Ciebie po wyzwoleniu alarmu detekcji ruchu.
- **Action HTTP URL** : wprowadź polecenie HTTP, które zostanie wysłane do serwera innej firmy w celu wykonania wstępnie zdefiniowanej akcji.
- **Action Relay (Przełącznik działania)**: wybór jednego z przełączników bramofonu, który będzie realizował wstępnie zdefiniowane działanie.

Przewiń w dół, aby ustawić harmonogram wykrywania ruchu.

Motion Detect Time Setting

Day	<input checked="" type="checkbox"/> Mon	<input checked="" type="checkbox"/> Tue	<input checked="" type="checkbox"/> Wed
	<input checked="" type="checkbox"/> Thur	<input checked="" type="checkbox"/> Fri	<input checked="" type="checkbox"/> Sat
	<input checked="" type="checkbox"/> Sun	<input type="checkbox"/> Check All	

Start Time - End Time      00:00 - 23:59

## Ustawienia powiadomień bezpieczeństwa

### Ustawienia powiadomień e-mail

Skonfiguruj powiadomienia e-mail, aby otrzymywać zrzuty ekranu nietypowych ruchów z

bramofonu. Przejdź do interfejsu **Setting > Action > Email Notification**.

Email Notification

Sender's Email Address	<input type="text"/>
Receiver's Email Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
Port	<input type="text"/> (1024-65535)
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>
EmailTest	<input type="button" value="Test"/>

## Konfiguracja parametrów :

- **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 hasło usługi SMTP.

## Ustawienia powiadomień FTP

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

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

FTP Notification	
FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password" value="*****"/>
FTP Path	<input type="text"/>

**Konfiguracja parametrów :**

- **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. Przejdź do **Ustawienia > Akcja > Interfejs**

**powiadomień TFTP**.

TFTP Notification	
TFTP Server	<input type="text"/>

## Powiadomienie o połączeniu SIP

Możesz wprowadzić numer SIP, aby otrzymywać powiadomienia.

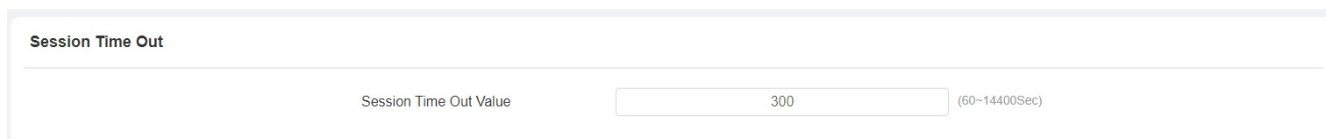
Przejdź do **Ustawienia > Akcja > Interfejs powiadomień o połączeniach SIP**.

SIP Call Notification	
SIP Call Number	<input type="text"/>
SIP Call Name	<input type="text"/>

## 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 w interfejsie sieci Web **System > Security > Session Time Out**.



The screenshot shows a configuration page titled "Session Time Out". It features a single input field labeled "Session Time Out Value" with the number "300" entered. To the right of the input field, the range "(60-14400Sec)" is displayed. The entire configuration area is enclosed in a light gray border.

### Konfiguracja parametrów :

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

## Adres URL akcji

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

### Akuvox Action URL:

Nie	Wydarzenie	Format parametrów	Przykład
1	Wykonaj połączenie	\$remote	Http://server ip/ Callnumber=\$remote
2	Rozłącz się	\$remote	Http://server ip/ Callnumber=\$remote
3	Przełącznik wyzwolony	\$relay1status	Http://server ip/ relaytrigger=\$relay1status
4	Przełącznik 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?](http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

[mac=\\$mac:ip=\\$ip:model=\\$model:firmware=\\$firmware:card\\_sn=\\$card\\_sn](http://192.168.16.118/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

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

## Action URL

Enabled	<input type="checkbox"/>
Type	<input type="text" value="GET"/>
Make Call	<input type="text"/>
Hang Up	<input type="text"/>
RelayA Triggered	<input type="text"/>
RelayB Triggered	<input type="text"/>
RelayC Triggered	<input type="text"/>
RelayA Closed	<input type="text"/>
RelayB Closed	<input type="text"/>
RelayC Closed	<input type="text"/>
InputA Triggered	<input type="text"/>
InputB Triggered	<input type="text"/>
InputC Triggered	<input type="text"/>
InputA Closed	<input type="text"/>

## Wirtualny kod PIN

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

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

Virtual PIN

---

Enabled

### Konfiguracja parametrów :

- Enabled (Włączone):** jeśli opcja ta jest włączona, użytkownik może umieszczać fałszywe cyfry na obu końcach kodu PIN w celu jego ochrony. Na przykład, jeśli twoje hasło to 1234567, możesz umieścić 99 i 88 na obu końcach (**99123456788**). Wirtualne hasło jest dopasowywane do użytkowników na podstawie liczby pasujących cyfr. Na przykład, jeśli użytkownik A ma większą liczbę cyfr pasujących do wprowadzonego hasła wirtualnego niż użytkownik B, zostanie ono uznane za hasło użytkownika A. Jednakże, gdy stosowane jest podwójne uwierzytelnianie, wówczas wirtualne hasło

hasło zostanie dopasowane do użytkowników, którzy przejdą pierwszy poziom uwierzytelniania, na przykład Face + PIN.

### Uwaga

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

## Ustawienia certyfikatu klienta

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

## Certyfikat serwera WWW

Jest to certyfikat wysyłany do klienta w celu uwierzytelnienia, gdy klient żąda połączenia SSL z bramofonem Akuvox. Prosimy o przesyłanie certyfikatów w akceptowanych formatach.

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

Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPhone	IPhone	Sun Oct 9 16:00:00 2034	Delete

Web Server Certificate Upload

## Certyfikat klienta

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

Aby przesłać i skonfigurować certyfikaty klienta na tej samej stronie.

**Client Certificate**

	Index	Issue To	Issuer	Expire Time
No Data				

Index

Client Certificate Upload

Only Accept Trusted Certificates

### Konfiguracja parametrów :

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

## Tryb wysokiego bezpieczeństwa

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

Aby skonfigurować ten tryb w interfejsie internetowym **System > Zabezpieczenia > Tryb wysokiego bezpieczeństwa**.

**High Security Mode**

Enabled

### Ważne uwagi

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

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

-PC Manager: 1.2.0.0

-IP Scanner: 2.2.0.0

-Upgrade Tool: 4.1.0.0

-SDMC: 6.0.0.34

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

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

- I <http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1>●  
I <http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1>

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

- I [http://deviceIP/fcgi/do?  
action=OpenDoor&UserName=username&Password=password&DoorNum=1](http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1)

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



# Monitor i obraz

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

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

RTSP to skrót od Real Time Streaming Protocol. Może być używany do strumieniowego przesyłania obrazu i dźwięku z kamer innych firm do urządzenia. Możesz dodać strumień z kamery, dodając jej adres URL. Format adresu URL urządzeń Akuvox to [rtsp://Device's IP/live/ch00\\_0](#)

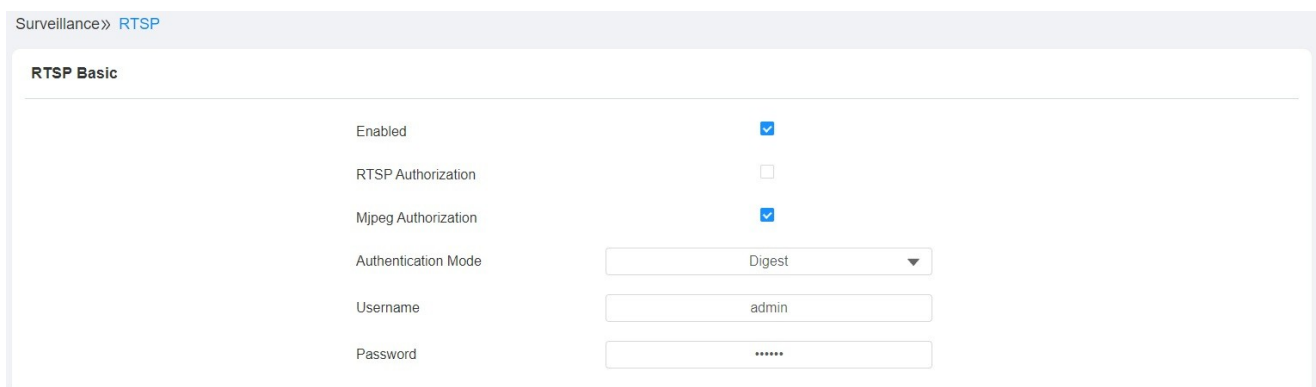
ONVIF to Otwarte Forum Sieciowego Interfejsu Wideo. Umożliwia urządzeniu skanowanie i wykrywanie kamer lub urządzeń domofonowych z aktywowanymi funkcjami ONVIF. Strumienie na żywo uzyskane za pośrednictwem ONVIF są zasadniczo w formacie RTSP.

## Monitorowanie strumienia RTSP

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

## Podstawowe ustawienia RTSP

Aby skonfigurować go w sieci Web, wybierz kolejno opcje **Surveillance > RTSP > RTSP Basic** .



Surveillance» RTSP

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
RTSP Authorization	<input type="checkbox"/>
Mjpeg Authorization	<input checked="" type="checkbox"/>
Authentication Mode	<input type="text" value="Digest"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

### Konfiguracja parametrów :

- **Autoryzacja RTSP** : włącz autoryzację RTSP. Jeśli włączysz autoryzację RTSP, musisz wprowadzić typ uwierzytelniania RTSP, nazwę użytkownika RTSP i nazwę użytkownika RTSP.

RTSP Hasło na urządzeniu interkomowym, takim jak monitor wewnętrzny, w celu autoryzacji.

- **Tryb uwierzytelniania:** wybór typu uwierzytelniania RTSP pomiędzy **Basic** i **Digest**. **Basic** jest domyślnym typem uwierzytelniania.

## Ustawienia strumienia RTSP

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

Przejdź do interfejsu **Surveillance > RTSP > RTSP Stream**.

RTSP Stream

Video Codec: H.264

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

H.264 Video Parameters

Video Resolution	720P
Video Framerate	25fps
Video Bitrate	2048kbps
2nd Video Resolution	VGA
2nd Video Framerate	25fps
2nd Video Bitrate	512kbps

### Konfiguracja parametrów :

- **Rozdzielczość wideo:** wybór rozdzielczości wideo spośród siedmiu opcji: **QCIF, QVGA, CIF, VGA, 4CIF, 720P** i **1080P**. Domyślna rozdzielczość wideo jest taka, że 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** : wybierz szybkość 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 to **2048 kb/s**.
- **2nd Video Resolution:** wybór rozdzielczości wideo dla drugiego kanału strumienia wideo. Domyślną rozdzielczością wideo jest **VGA**.

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

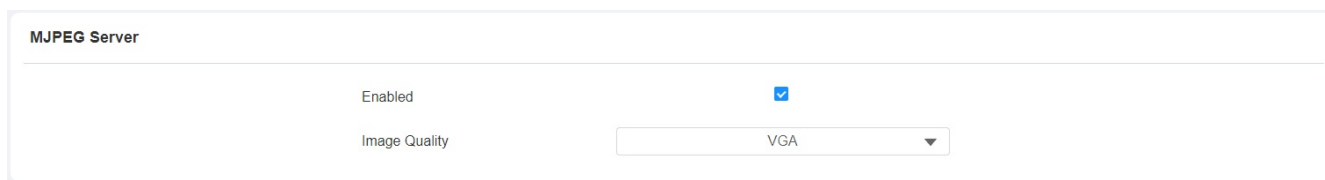
**25 klatek na sekundę** to domyślna liczba klatek na sekundę dla drugiego kanału strumienia wideo.

**2nd Video Bitrate** : wybierz szybkość transmisji wideo spośród sześciu opcji dla drugiego kanału strumienia wideo. Drugi kanał strumienia wideo ma domyślnie szybkość **512 kb/s**.

## 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.

Przejdź do interfejsu **Surveillance > MJPEG**.



**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:// device 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.

## 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 w interfejsie internetowym **Surveillance > ONVIF > Basic Setting**.

Basic Setting	
Discoverable	<input checked="" type="checkbox"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

### Konfiguracja parametrów :

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

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

Na przykład: **http://IP address:80/onvif/device\_service**

#### Uwaga

- Wpisz konkretny adres IP telefonu w adresie URL.

## Transmisja na żywo

Istnieją dwa sposoby 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.



## Dzienniki

### Dzienniki połączeń

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

Aby sprawdzić rejestr połączeń w sieci **Status > Rejestr połączeń** .

Call Log

Save Call Log Enabled

Call History All Start Time ~ End Time Name/Number Search Export

	Index	Type	Date	Time	Local Identity	Name	Number
<input type="checkbox"/>	1	Received	2023-07-19	22:43:47	192.168.2.9@192.168.2.9	Indoor Monitor	192.168.0.102@192.16...

Selected: 0/1 Delete Delete All Total: 1 Prev 1/1 Next Go To Page 1 Go

### 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.

- **Czas rozpoczęcia i czas zakończenia:** wybierz określony przedział czasowy dzienników połączeń, które chcesz wyszukać, sprawdzić lub wyeksportować.
- **Nazwa/Numer:** wybierz opcje **Nazwa** i **Numer**, aby przeszukiwać rejestr połączeń według nazwy lub numeru SIP lub IP.

## Dzienniki drzwi

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

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

**Access Log**

Save Access Log Enabled

~

<input type="checkbox"/>	Index	UserID	Name	Code	DoorID	Type	Date	Time	Status
<input type="checkbox"/>	1	--	Visitor	--	--	Face	2023-08-03	22:50:13	Failed
<input type="checkbox"/>	2	--	Visitor	--	--	Face	2023-07-31	04:06:58	Failed
<input type="checkbox"/>	3	--	Visitor	--	--	Face	2023-07-31	04:06:36	Failed
<input type="checkbox"/>	4	--	Visitor	--	--	Face	2023-07-31	04:02:16	Failed
<input type="checkbox"/>	5	--	Visitor	--	--	Face	2023-07-31	04:02:09	Failed
<input type="checkbox"/>	6	--	Visitor	--	--	Face	2023-08-02	06:19:30	Failed
<input type="checkbox"/>	7	--	Visitor	--	--	Face	2023-08-02	03:24:29	Failed
<input type="checkbox"/>	8	--	Visitor	--	--	Face	2023-08-02	03:24:21	Failed
<input type="checkbox"/>	9	--	Visitor	--	--	Face	2023-08-02	03:24:12	Failed
<input type="checkbox"/>	10	--	Visitor	--	--	Face	2023-07-31	23:58:49	Failed

Selected: 0/10  
Total: 124
 1/13 
Go To Page

### Konfiguracja parametrów :

- **Status:** Wybierz pomiędzy opcjami **Udane** i **Nieudane**, aby wyszukać udane lub nieudane dostępy do drzwi.
- **Godzina rozpoczęcia~ Godzina zakończenia:** 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.

# Debugowanie

## Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

System można wyeksportować do lokalnego komputera lub zdalnego serwera w celu debugowania.

Aby skonfigurować funkcję w interfejsie internetowym **System > Konserwacja > Dziennik systemowy**.

The screenshot shows the 'System Log' configuration page. It includes a dropdown menu for 'Log Level' set to '3', two 'Export' buttons for 'Export Log' and 'Export Debug Log', a checkbox for 'Remote System Log Enabled' which is unchecked, and an empty text input field for 'Remote System Server'.

### 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, tym bardziej kompletny jest dziennik.
- **Remote System Server (Zdalny serwer systemu):** wprowadź adres zdalnego serwera do odbioru urządzenia. Adres zdalnego serwera zostanie podany przez pomoc techniczną Akuvox.

## PCAP do debugowania

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

Przed rozpoczęciem korzystania z PCAP można go skonfigurować w interfejsie **System > Konserwacja > PCAP**.

The screenshot shows the 'PCAP' configuration page. It features a text input field for 'Specific Port' with a '(1~65535)' hint, three buttons ('Start', 'Stop', 'Export') for the 'PCAP' section, and a checkbox for 'PCAP Auto Refresh Enabled' which is unchecked.

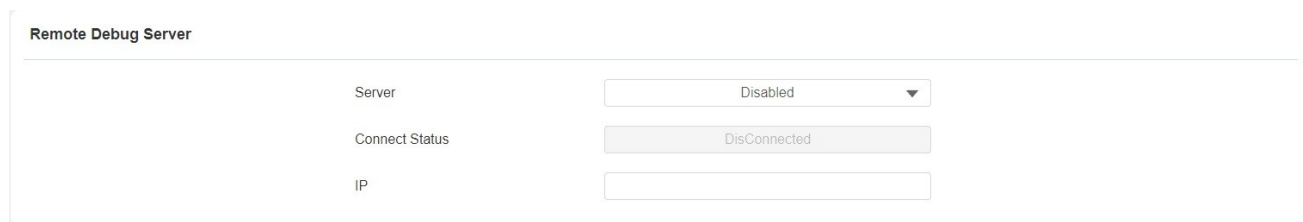
## Konfiguracja parametrów :

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

W Internecie przejdź do **System > Konserwacja > Interfejs serwera zdalnego debugowania**.



Remote Debug Server	
Server	Disabled
Connect Status	DisConnected
IP	

## Konfiguracja parametrów :

- **IP :** wprowadź adres IP zdalnego serwera debugowania. Zapytaj zespół techniczny Akuvox o adres IP serwera.

### Uwaga

Wymagane jest wysłanie adresu MAC bramofonu do działu technicznego Akuvox.



# Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można zaktualizować w interfejsie internetowym urządzenia. Możesz przejść do interfejsu

**System > Upgrade.**

**Basic**

---

Firmware Version	539.30.10.6
Hardware Version	539.1.0.0
Reset	<input type="checkbox"/>
Upgrade	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border-radius: 3px;">↻ Upgrade</a>
Reset To Factory Setting	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border-radius: 3px;">↻ Reset</a>
Reset Configuration to Default State(E...	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border-radius: 3px;">↻ Reset</a>
Reboot	<a href="#" style="background-color: #007bff; color: white; padding: 5px 10px; border-radius: 3px;">🔄 Reboot</a>

**Upgrade**
✕

---

(Format: .zip)

Not selected any files

Select File

↻ Reset

Cancel

Install

## Uwaga

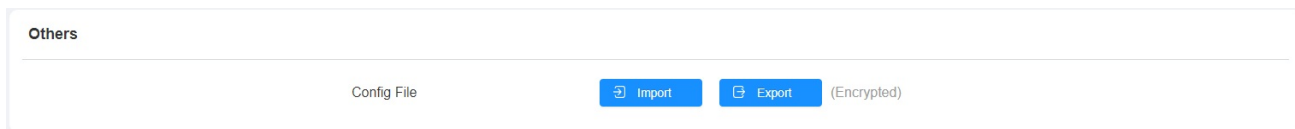
Pliki oprogramowania sprzętowego powinny być w formacie **.zip**.

# Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować

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

Inne.



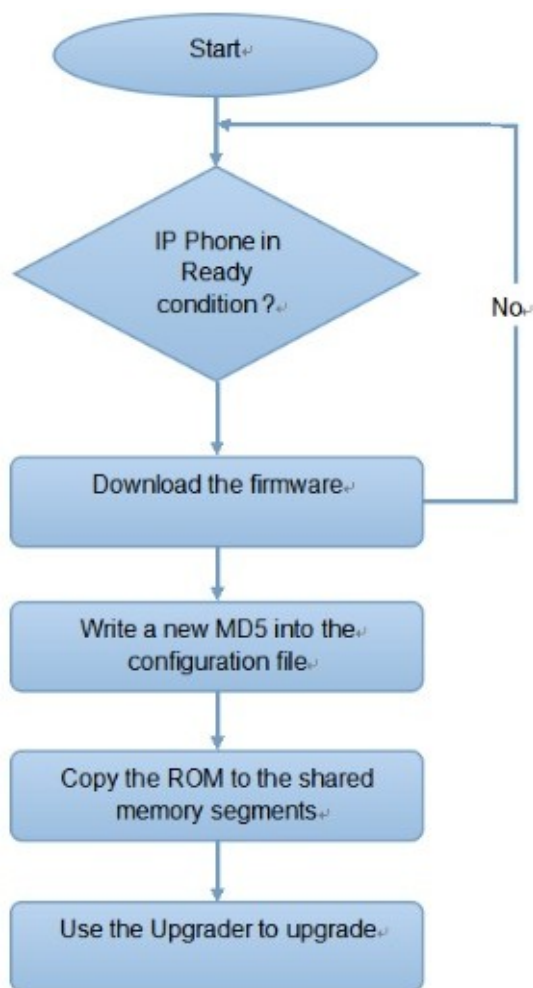
## Automatyczne dostarczanie Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

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 automatycznego udostępniania

Akuvox zapewnia różne metody AutoP, które umożliwiają telefonowi bramowemu samodzielne przeprowadzanie aprowizacji w określonym czasie zgodnie z harmonogramem użytkownika.

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

Automatic Autop

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0-23Hour)
	<input type="text" value="0"/> (0-59Min)
Clear MD5	<input type="button" value="Clear"/>
Export Autop Template	<input type="button" value="Export"/>

### Konfiguracja parametrów :

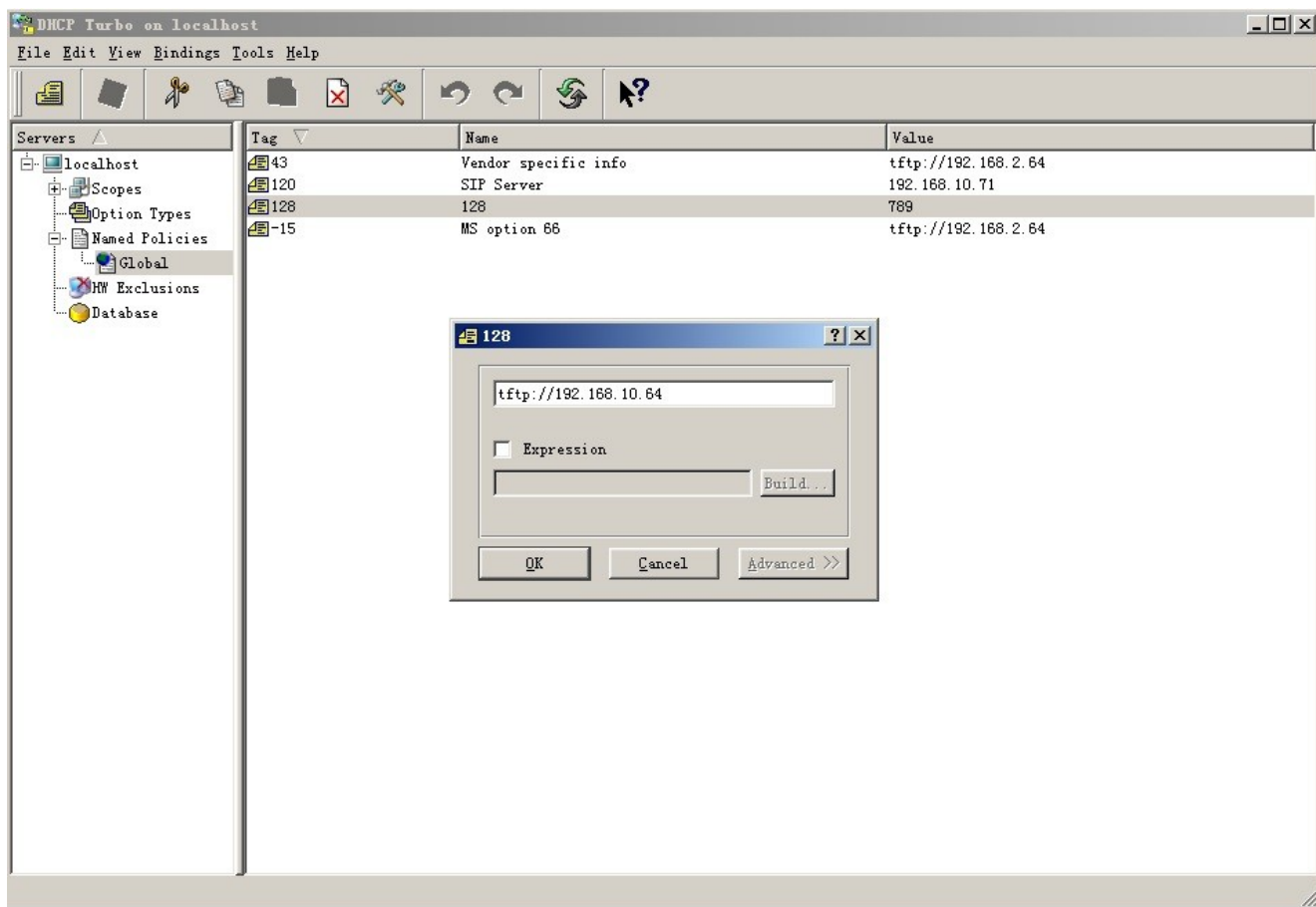
- **Tryb** : Wybierz **Włączanie, Powtarzanie, Włączanie + Powtarzanie i Powtarzanie godzinowe** jako harmonogram AutoP.
  - Wybierz opcję **Power on**, jeśli chcesz, aby urządzenie wykonywało AutoP przy każdym uruchomieniu. Wybierz opcję **Repeatedly**, jeśli chcesz, aby urządzenie wykonywało AutoP zgodnie z ustawionym harmonogramem.
  - Wybierz **Power On + Repeatedly**, jeśli chcesz połączyć tryb **Power On** z trybem **Repeatedly**, aby urządzenie wykonywało AutoP przy każdym uruchomieniu lub zgodnie z ustawionym harmonogramem.
  - Wybierz opcję **Hourly Repeat**, jeśli urządzenie ma wykonywać funkcję AutoP co godzinę.

## Konfiguracja udostępniania DHCP

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

Jeśli chcesz użyć

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



### Uwaga

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

Przejdź do interfejsu **System > Auto Provisioning**.

### DHCP Option

Custom Option

(128-254)

(DHCP option 66/43 is enabled by default)

## 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.

**DHCP Option 43:** Jeśli urządzenie nie otrzyma adresu URL z DHCP Option 66, automatycznie użyje DHCP Option 43. 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 udostępniania wsadowego ma format **r000000000xx.cfg**. Na przykładzie X915 r000000000915.cfg (w sumie **10 zer**, podczas gdy plik konfiguracyjny oparty na MAC dla konkretnego urządzenia ma format MAC Address of the device.cfg, na przykład **0C 110504AE5B.cfg**). Wygaszacz ekranu można przesłać za pomocą automatycznej konfiguracji.

## 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 Auto Provisioning w interfejsie **System > Auto Provisioning > Manual Autop**.

**Automatic Autop**

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0~23Hour)
	<input type="text" value="0"/> (0~59Min)
Clear MD5	<input type="button" value="Clear"/>
Export Autop Template	<input type="button" value="Export"/>

Manual Autop

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Common AES Key	<input type="password" value="*****"/>
AES Key(MAC)	<input type="password" value="*****"/>

### Konfiguracja parametrów :

- **URL** : skonfiguruj adresy serwerów TFTP, HTTP, HTTPS, FTP dla provisioningu.
- **User Name** : ustaw nazwę użytkownika, jeśli serwer wymaga nazwy użytkownika, aby uzyskać dostęp w razie potrzeby.
- **Hasło**: ustaw hasło, jeśli serwer potrzebuje hasła, aby uzyskać dostęp w razie potrzeby.
- **Wspólny klucz AES**: ustawienie kodu AES dla interkomu w celu odszyfrowania ogólnego klucza automatycznego.

Udostępnianie plików konfiguracyjnych.

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

### Uwaga

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

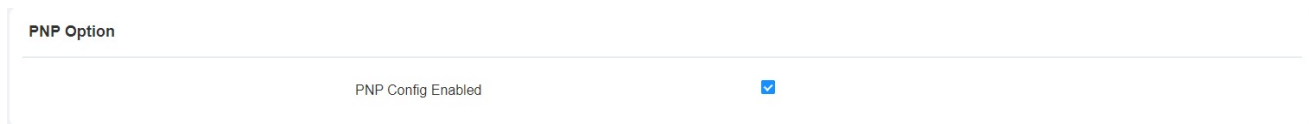
### Wskazówka

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

## Konfiguracja PNP

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

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

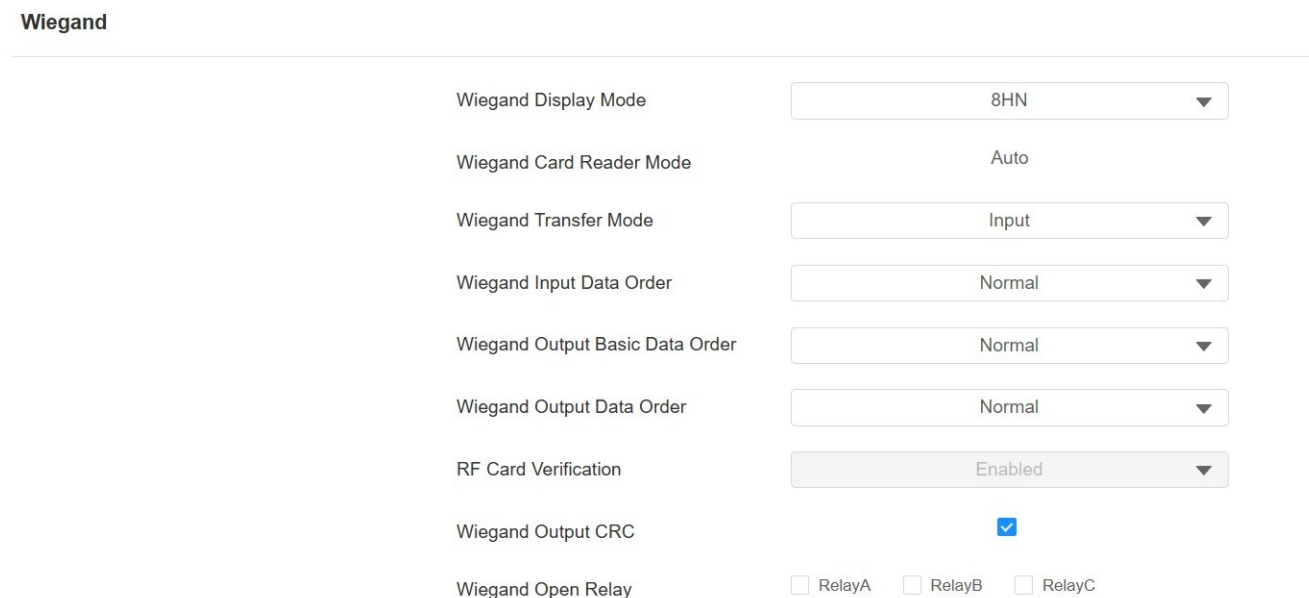


## Integracja z urządzeniami innych firm

### Integracja przez Wiegand

Funkcja **Wiegand** umożliwia bramofonowi Akuvox działanie jako kontroler lub czytnik

kart. można ją skonfigurować w interfejsie Web **Device > Wiegand**.



#### Konfiguracja parametrów :

- **Tryb wyświetlania Wiegand:** wybór formatu kodu karty Wiegand spośród **8H10D; 6H3D 5D; 6H8D; 8HN; 8HR; 6H3D 5D-R(W26); 8HR10D; RAW**.
- **Tryb czytnika kart Wiegand:** to pole jest przyciemnione i nie można go zmienić, ponieważ czytnik kart Wiegand może dostosować się do wszystkich typów wprowadzanych danych.
- **Tryb transferu Wiegand:** ustaw tryb transferu między **wejściem** a **wyjściem**, jeśli bramofon jest używany jako odbiornik, ustaw go jako wejście dla bramofonu i odwrotnie.
- **Kolejność danych wejściowych Wiegand:** ustawia kolejność danych wejściowych Wiegand pomiędzy **Normal** i **Reversed**, jeśli wybierzesz Reversed, numer karty wejściowej zostanie odwrócony i odwrotnie.
- Wiegand **Output Basic Data Order:** wybierz **Normal**, jeśli chcesz, aby dane



wyjściowe Wiegand były wyświetlane w normalnym stanie. Wybierz **Reversed**, jeśli chcesz odwrócić dane wyjściowe, na przykład z 0x110x220x330x44 na 0x440x330x220x11.

- **Kolejność danych wyjściowych Wiegand**: ustawia kolejność danych wyjściowych Wiegand pomiędzy **Normalna**

i **Reversed**, jeśli wybierzesz **Reversed**, 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.

Enabled	<input checked="" type="checkbox"/>
Authorization Mode	Allowlist
Username	admin
Password	*****
1st IP	
2nd IP	
3rd IP	
4th IP	
5th IP	

### Konfiguracja parametrów :

- **Enabled** : włącz lub wyłącz funkcję HPTT API dla integracji z innymi firmami. Na przykład, jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.
- **Tryb autoryzacji**: wybierz spośród **None**, **Normal**, **Allowlist**, **Basic**, **Digest** i **Token** dla typu autoryzacji, które zostaną szczegółowo wyjaśnione w poniższej tabeli.
- **Nazwa użytkownika**: wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic** i **Digest**. Domyślna nazwa użytkownika to **admin**.
- **Hasło** : wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic** i **Digest**. Domyślne hasło to admin.

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

Poniższy opis dotyczy trybu uwierzytelniania:

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

## Kontrola mocy wyjściowej

Urządzenie może służyć jako źródło zasilania dla zewnętrznych przekaźników.

Możesz przejść do interfejsu **Access Control > Relay > 12V Power Output**.

12V Power Output

12V Power Output	<input type="text" value="Disabled"/>
Time Out (Sec)	<input type="text" value="3"/>

**Konfiguracja parametrów :**

- **Wyjście zasilania 12V:** wybierz opcję **Wyłączone**, aby wyłączyć funkcję wyjścia zasilania; wybierz opcję **Zawsze**, aby włączyć kontroler dostępu do ciągłego zasilania urządzenia innej firmy.

Wybierz **Triggered By Open Relay**, jeśli chcesz, aby bramofon dostarczał zasilanie do urządzenia innej firmy za pośrednictwem wyjścia 12 i interfejsu GND podczas limitu czasu, gdy stan przekaźników zmieni się z niskiego na wysoki.

Wybierz **Security Relay A**, aby zasilać przekaźnik bezpieczeństwa.

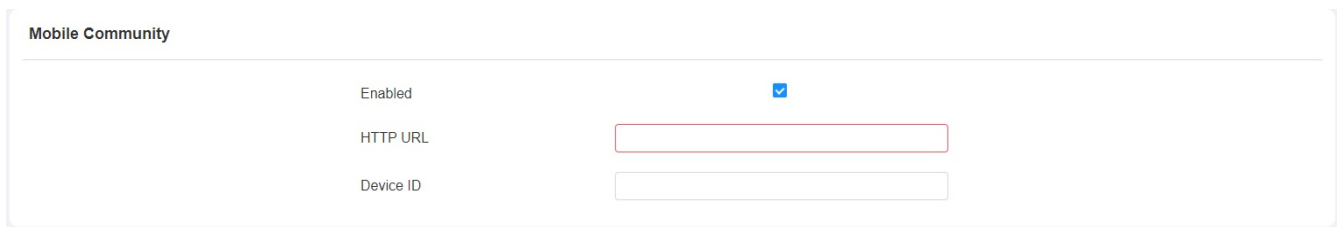
- **Time Out (Sec):** wybór czasu zasilania po wyzwoleniu przekaźnika. Trzy opcje: 3, 5, 10. Domyślnie jest to 3 sekundy. Wyjście zasilania wynosi 12 V, a maksymalne

natężenie prądu wyjściowego wynosi 0,8 A.

## Mobilna społeczność

Telefon z drzwiami można połączyć z serwerem kodów QR innej firmy w celu weryfikacji kodu QR. Po uzyskaniu dostępu do drzwi za pomocą kodu QR, kod QR zostanie wysłany do serwera kodów QR w celu weryfikacji przed przyznaniem uprawnień dostępu. Ta funkcja jest stosowana do urządzeń, które nie zostały wdrożone na platformie SmartPlus w celu uzyskania dostępu do drzwi za pomocą kodu QR.

Możesz przejść do opcji **Kontrola dostępu > Przekaznik > Interfejs społeczności mobilnej**.



Mobile Community	
Enabled	<input checked="" type="checkbox"/>
HTTP URL	<input type="text"/>
Device ID	<input type="text"/>

## Integracja z Milestone

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

Aby to zrobić, przejdź do interfejsu **Surveillance > ONVIF > Advanced Setting**.



Advanced Setting	
Milestone	<input type="checkbox"/>

# 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 interfejsu **Device > Lift Control**.

Lift Control List

Lift Control List

AK EC32 ▼

Akuvox EC32 Advanced Setting

Server IP

Port

Akuvox EC32 Action

Username

Password

Floor NO. Parameter

URL To Trigger Specific Floor

URL To Trigeer All Floors

URL To Close All Floors

## Konfiguracja parametrów :

- **Lift Control List:** wybierz **None**, aby wyłączyć funkcję i wybierz Akuvox E32, aby zintegrować bramofon z kontrolerem Akuvox EC32.
- **Server IP:** wprowadź adres IP serwera kontrolera Akuvox EC32. **Server**
- **Port:** wprowadź port Sever serwera kontrolera Akuvox EC32.
- **Floor NO. Parametr:** wprowadź parametr numeru piętra dostarczony przez Akuvox. Domyślny ciąg parametru to "\$floor". W razie potrzeby można zdefiniować własny ciąg parametrów. **URL To Trigger Specific Floor:** wprowadź adres URL Akuvox life control do wyzwalania określonego piętra. Adres URL to **"/cdor.cgi?open=0&door=\$floor"**, ale ciąg "\$floor" na końcu musi być identyczny z ciągiem parametrów zdefiniowanym przez użytkownika.
- **URL To Trigger All Floors :** wprowadź adres URL Akuvox do wyzwalania wszystkich pięter.
- **URL To Close All Floors :** wprowadź adres URL Akuvox używany do zamykania wszystkich pięter, co oznacza, że wszystkie przyciski uruchamiane dla odpowiednich pięter staną się nieważne.

# Modyfikacja hasła

## Modyfikacja hasła interfejsu sieciowego urządzenia

Aby zmienić domyślne hasło sieciowe w interfejsie **System > Bezpieczeństwo > Modyfikacja hasła sieciowego**.

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

Web Password Modify

---

Username  Change Password

---

**Account Status**

admin Enabled	<input checked="" type="checkbox"/>
user Enabled	<input type="checkbox"/>

---

**Change Password** ×

---

The password must be at least eight characters long containing at least one uppercase letter, one lowercase letter and one number.

Username	admin
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

Cancel
Change

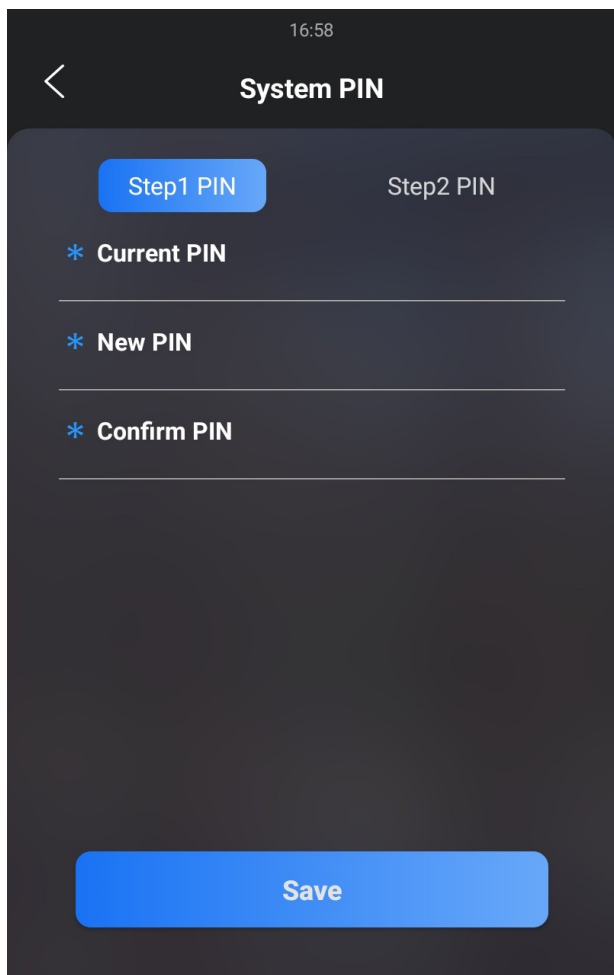
### Konfiguracja parametrów :

- **Nazwa użytkownika:** w razie potrzeby zmień hasło administratora lub użytkownika.
- **Użytkownik:** w razie potrzeby włącz konto użytkownika.

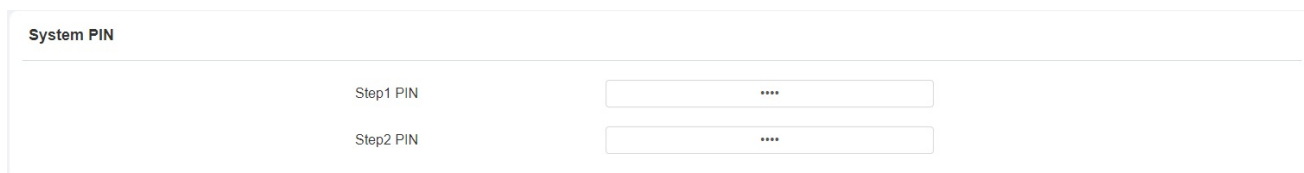
## Modyfikacja hasła systemowego

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

Aby ustawić systemowy kod PIN na urządzeniu, przejdź do **Security > System PIN**, a następnie wybierz **Step1 PIN**.



Aby skonfigurować systemowy kod PIN w interfejsie internetowym, przejdź do opcji **System > Security > System PIN**.



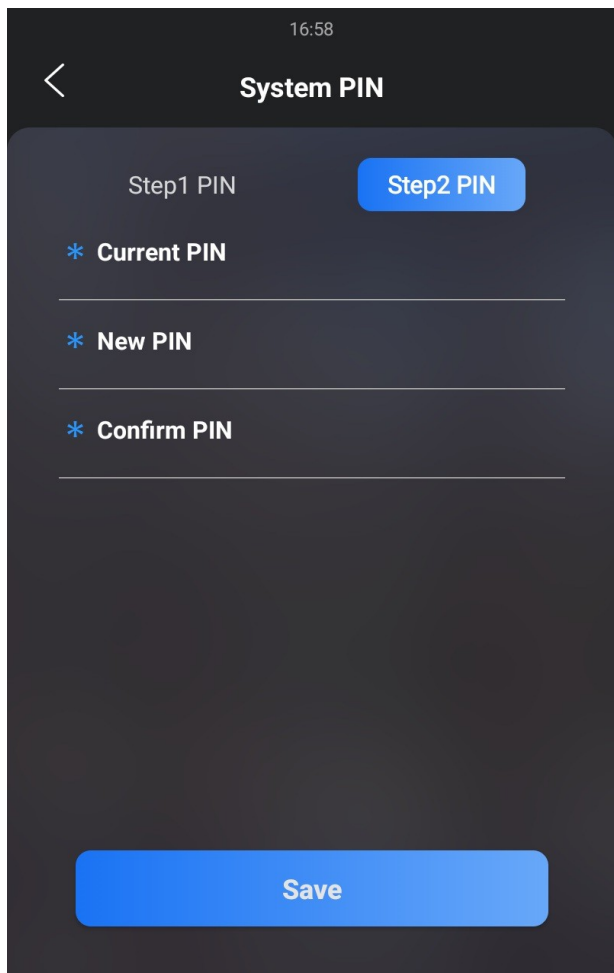
### Uwaga

- Domyślne hasło dostępu do systemu to 9999, a hasło ustawień systemowych to 3888.

## Modyfikacja hasła ustawień

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

Aby ustawić systemowy kod PIN na urządzeniu, przejdź do **Security > System PIN**, a następnie wybierz **Step2 PIN**.



Aby skonfigurować hasło ustawień w interfejsie internetowym, przejdź do **System > Security > System PIN**.

System PIN	
Step1 PIN	<input type="password"/>
Step2 PIN	<input type="password"/>

### Uwaga

- Domyślne hasło dostępu do systemu to 9999, a hasło ustawień systemowych to 3888.

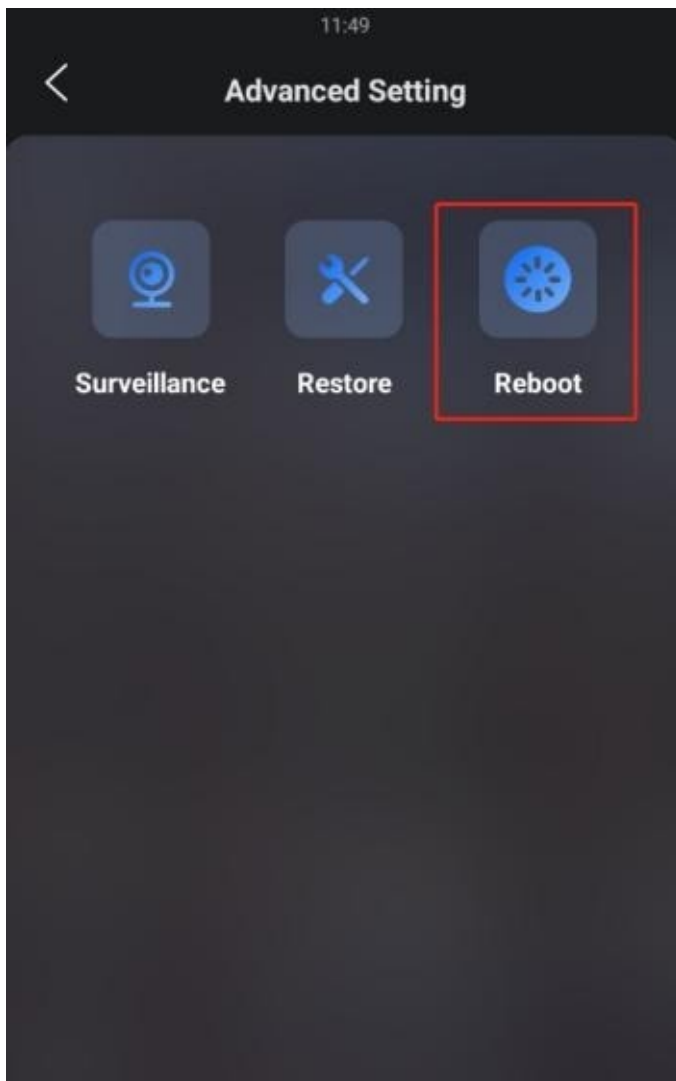
## Ponowne uruchamianie i resetowanie systemu Reboot

Aby ponownie uruchomić system, należy wybrać opcję **System > Upgrade**.

Reboot



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





## Reset

Możesz wybrać **Reset To Factory Setting**, jeśli chcesz zresetować urządzenie (usuając 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 opcji **System > Aktualizacja** .

### Basic

Firmware Version 539.30.10.6


Hardware Version 539.1.0.0

Reset

Upgrade  Upgrade

Reset To Factory Setting  Reset

Reset Configuration to Default State(E...  Reset

Reboot  Reboot

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

