

## Informacje o niniejszej instrukcji

**Akuvox**  
Open A Smart World

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



# X915 SERIES DOOR PHONE

## Administrator Guide

Dziękujemy za wybranie bramofonu z serii Akuvox X915. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy wersji 915.30.10.14 i zawiera wszystkie konfiguracje funkcji i właściwości bramofonu serii X915. W celu uzyskania nowych informacji lub najnowszego oprogramowania sprzętowego należy odwiedzić forum Akuvox lub skontaktować się z pomocą techniczną.

## Przegląd produktów

Seria Akuvox X915 to oparty na systemie Android wideodomofon IP z ekranem dotykowym. Łączy w sobie funkcje komunikacji audio i wideo, kontroli dostępu i nadzoru wideo. Dzięki zaawansowanemu systemowi operacyjnemu Android, chmurze i technologii komunikacji opartej na sztucznej inteligencji, oferuje konfigurowalne funkcje spełniające preferencje operacyjne. Seria X915 obsługuje wiele portów, takich jak RS485 i Wiegand, umożliwiając łatwą integrację z zewnętrznymi systemami, takimi jak kontrolery wind i czujniki alarmu przeciwpożarowego. To kompleksowe rozwiązanie zapewnia pełną kontrolę nad wejściami do budynku i jego otoczeniem, zapewniając zwiększone bezpieczeństwo dzięki różnym metodom dostępu, takim jak dostęp za pomocą karty, NFC, Bluetooth, kod QR, dostęp do drzwi sterowany głosem i pomiar temperatury ciała, idealny do budynków mieszkalnych i biurowych, a także kompleksów.

## Specyfikacja modelu












Model	X915S
Ekran dotykowy	✓
Wejście przekaźnika	3
Wyjście przekaźnika	3
Alarm wł.	X
RS485	✓
Czytnik kart	13.56MHZ&125KHZ
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, informacje o koncie itp.
- **Konto:** ta sekcja dotyczy konta SIP, serwera SIP, serwera proxy, typu protokołu transportowego, kodeka audio i wideo, DTMF, licznika sesji itp.
- **Sieć:** ta sekcja dotyczy głównie ustawień DHCP i statycznego adresu IP, ustawień portów RTP i wdrażania urządzeń itp.
- **Interkom:** ta sekcja obejmuje ustawienia interkomu, dzienniki połączeń 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, połączenie Wiegand itp.
- **Katalog:** ta sekcja obejmuje zarządzanie dzierżawcami.
- **Urządzenie:** ta sekcja zawiera ustawienia podświetlenia, wyświetlania przycisków i kart, ustawienia wyświetlacza LCD oraz ustawienia głosowe.
- **Ustawienia:** ta sekcja obejmuje czas i język, ustawienia akcji, ustawienia drzwi i zarządzanie harmonogramem kontroli dostępu.
- **System:** ta sekcja służy do modyfikacji hasła.

# Akuvox | X915S

Open A Smart World

-  [HomePage](#)
-  [Status](#) ▼
-  [Account](#) ▼
-  [Network](#) ▼
-  [Intercom](#) ▼
-  [Surveillance](#) ▼
-  [Access Control](#) ▼
-  [Directory](#) ▼
-  [Device](#) ▼
-  [Setting](#) ▼
-  [System](#) ▼

Status» [Info](#)

## Product Information

---

## Network Information

---

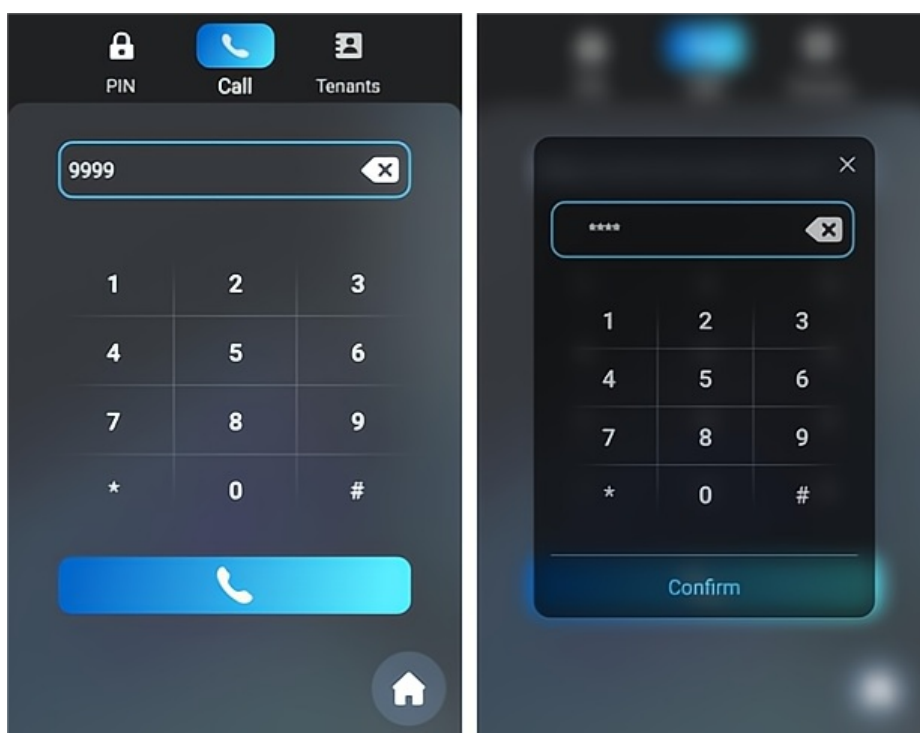
## Dostęp do urządzenia

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

### Dostęp do ustawień urządzenia na urządzeniu

Przed konfiguracją urządzenia należy upewnić się, że jest ono prawidłowo zainstalowane i podłączone do normalnej sieci. Użyj narzędzia skanera IP Akuvox, aby wyszukać adres IP urządzenia w tej samej sieci LAN. Następnie użyj adresu IP, aby załogować się do przeglądarki internetowej przy użyciu nazwy użytkownika i hasła **admin** i **admin**.

Można też skonfigurować podstawowe ustawienia na ekranie urządzenia, naciskając **9999** + przycisk **wybierania** + **3888** (hasło) na ekranie **wybierania**.



### Ustawienia sterowania gestami

Gdy urządzenie znajduje się w motywie Budynek lub Willa, dotknij obszaru czasu dziesięć razy na ekranie głównym urządzenia, aby uzyskać dostęp do ekranu ustawień. Domyślne hasło to 3888.

Aby włączyć tę funkcję, przejdź do interfejsu internetowego **System > Zabezpieczenia > Sterowanie gestami**.

#### Gesture Control

Enabled



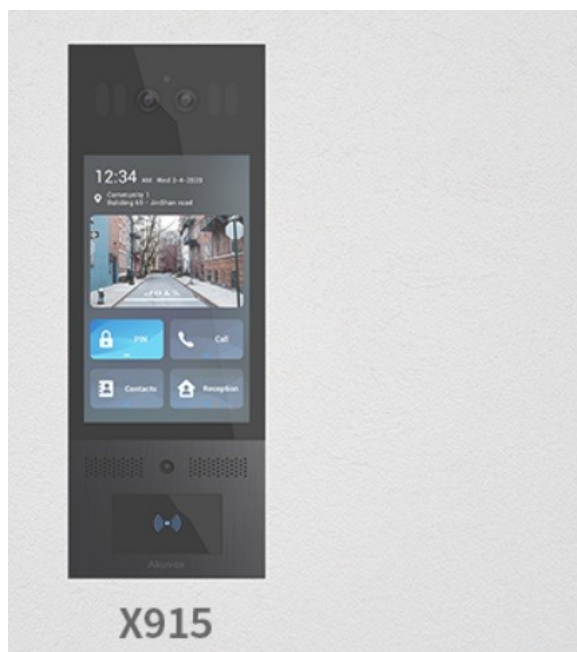
#### Uwaga

Patrz konfiguracja motywu w rozdziale [Konfiguracja ekranu](#).

## 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.

Początkowa nazwa użytkownika i hasło to **admin**.



admin

.....

Remember User Name/Password

Login

### Uwaga

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

- Pobierz skaner IP:  
<https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP>
- Zobacz szczegółowy przewodnik:  
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Zdecydowanie zalecana jest przeglądarka Google Chrome.
- 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 pośrednictwem urządzenia lub interfejsu internetowego zgodnie z własnymi preferencjami.

## Ustawienia języka w interfejsie internetowym urządzenia

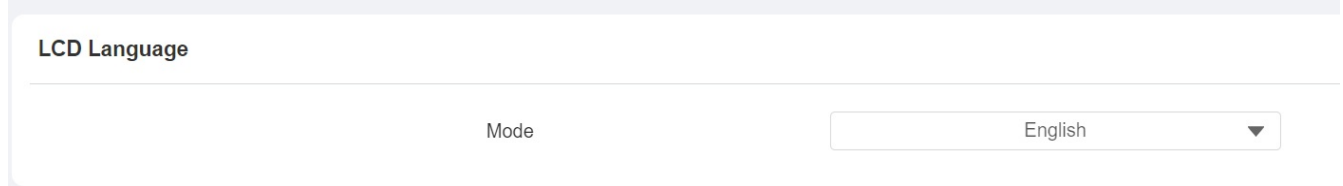
Można wybrać język urządzenia i ikony języka urządzenia, a także dostosować tekst interfejsu, w tym nazwy konfiguracji i tekst monitu.

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

interface. Wyświetlacz LCD urządzenia obsługuje następujące języki:

Angielski, chiński uproszczony, hiszpański, duński, francuski, czeski, chiński tradycyjny, turecki, japoński, norweski, koreański, rosyjski, holenderski, polski, szwedzki, niemiecki i ukraiński.

Setting» [Time/Lang](#)



LCD Language

Mode English

Aby przełączyć język internetowy urządzenia w prawym górnym rogu.



Aby dostosować nazwy konfiguracji i tekst monitu, należy wyeksportować i edytować plik .json przed przesłaniem go do urządzenia.

Przejdź do interfejsu **Ustawienia internetowe > Czas/język > Wgrywanie słów języka.**

Words Of Language Upload

Type	File Status	Import	Export	Reset
Web	NULL	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Reset</a>

## Ustawienia języka na urządzeniu

Aby skonfigurować język na urządzeniu, wybierz **Ustawienia podstawowe > Ekran języka.**

## Ustawienie czasu

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

## 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 czas w interfejsie internetowym **Setting > Time/Lang > Time**.

The screenshot shows the 'Time' settings page. At the top left, the word 'Time' is displayed. Below it, there are five settings:

- Automatic Date&Time:** A checkbox that is checked.
- Time Zone:** A dropdown menu showing 'GMT-5:00 New\_York'.
- Date Format:** A dropdown menu showing '07-21-2023'.
- Time Format:** A dropdown menu showing '24Hour'.
- NTP Server:** A text input field containing 'pool.ntp.org'.

- **Automatyczna data i czas:** umożliwia automatyczną konfigurację i synchronizację daty i czasu z domyślną strefą czasową i serwerem Network Time Protocol (NTP). Można również ustawić je ręcznie, wprowadzając godzinę i datę.
- **NTP Server:** adres serwera NTP.

## Ustawienie czasu na urządzeniu

Aby skonfigurować czas na urządzeniu, wybierz **Ustawienia podstawowe > Ekran czasu**.

## 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 w interfejsie internetowym

Przejdź do interfejsu internetowego **Urządzenie > Światło > LED**.

The screenshot shows the 'LED' settings page. At the top left, there is a breadcrumb 'Device >> Light'. Below it, the word 'LED' is displayed. The settings include:

- Mode:** A dropdown menu showing 'Always OFF'.
- Photoresistor Setting:** Two input fields showing '25' and '120', with a range '(0~1200)' indicated to the right.

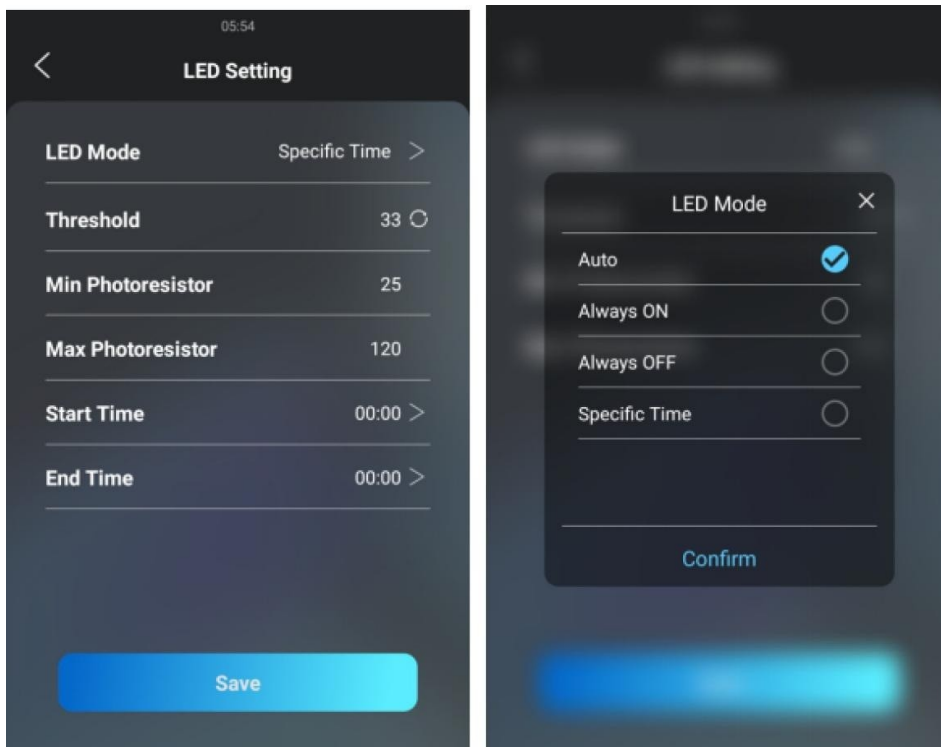
- **Tryb:**



- Auto: urządzenie automatycznie ustawi diodę LED.
  - Always On (Zawsze włączona): funkcja włączona przez cały czas.
  - Zawsze wyłączone: wyłączenie funkcji przez cały czas.
  - Określony czas: określa czas rozpoczęcia i zakończenia świecenia diody LED.
- **Ustawienie fotorezystora:** ustaw minimalną i maksymalną wartość fotorezystora na podstawie aktualnie wykrytej rzeczywistej wartości fotorezystora, aby kontrolować włączanie i wyłączenie światła LED. Można ustawić maksymalną wartość fotorezystora, aby włączyć diodę LED podczerwieni i minimalną wartość, aby ją wyłączyć. Domyślne minimalne i maksymalne wartości fotorezystora to odpowiednio 25 i 120.

## Ustawienie diody LED podczerwieni na urządzeniu

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



**Próg:** bieżące natężenie światła wskazywane przez wartość fotorezystora. Wyższe wartości fotorezystora odpowiadają niższemu natężeniu światła i odwrotnie. Domyślna wartość fotorezystora (**Threshold**) wynosi **33**. Można jednak stuknąć ikonę kilka razy, aby uzyskać rzeczywistą wartość fotorezystora w określonym środowisku (wahania wartości wynoszą około 5), a wartość ta jest podstawą do skonfigurowania minimalnej i maksymalnej wartości fotorezystora.

## 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.

Przejdź do interfejsu internetowego **Device > Light > LED of Swiping Card Area**.

### LED Of Swiping Card Area

Enabled	<input checked="" type="checkbox"/>
Start Time	<input type="text" value="18"/> (0~23Hour)
End Time	<input type="text" value="23"/> (0~23Hour)

**Start Time- End Time (H):** wprowadź okres, w którym oświetlenie LED ma obowiązywać, np. jeśli okres jest ustawiony od 8-0 (czas rozpoczęcia - czas zakończenia), oznacza to, że światło LED pozostanie włączone w okresie 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

Przejdź do interfejsu internetowego **Urządzenie > Światło > Jasność podświetlenia LCD**.

### LCD Backlight Brightness

Mode	<input type="text" value="Auto"/>
Backlight Brightness(Day)	<input type="text" value="60"/> (0~255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="10"/> (0~255)
Backlight Brightness(Night)	<input type="text" value="10"/> (0~255)
Backlight Brightness Of Screen Saver(...)	<input type="text" value="3"/> (0~255)

- **Tryb** : po wybraniu opcji **Auto** jasność podświetlenia ekranu zostanie dostosowana automatycznie.

Jasność podświetlenia ma dwa tryby, dzienny i nocny. Są one określane przez fotorezystor.

-Jeśli wartość prądu znajduje się pomiędzy minimalną i maksymalną wartością fotorezystora, urządzenie znajduje się w trybie Day.

-Jeśli wartość prądu jest wyższa niż maksymalna wartość fotorezystora, urządzenie znajduje się w trybie Night.

- **Jasność podświetlenia (dzień)**: ustawienie jasności podświetlenia ekranu w ciągu dnia w zakresie od **0** do **255** .
- **Jasność podświetlenia wygaszacza ekranu (dzień)**: ustawienie jasności podświetlenia ekranu dla wygaszacza ekranu w ciągu dnia w zakresie **0-255** .
- **Jasność podświetlenia (noc)**: ustawienie jasności podświetlenia ekranu w nocy w zakresie **0-255** .
- **Jasność podświetlenia wygaszacza ekranu (noc)**: ustawienie jasności podświetlenia ekranu dla wygaszacza ekranu w ciągu dnia z wartością w zakresie **0-255** .

## Ustawienie jasności ekranu LCD na urządzeniu

Aby skonfigurować jasność na urządzeniu, wybierz **Ustawienia podstawowe > Wyświetlacz > Ekran ustawień 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.

Przejdź do interfejsu internetowego **Urządzenie > Światło > Światło białe**.

White Light

Mode

OFF

OFF

Auto

Cancel

Submit

- **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 w interfejsie sieciowym

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

Przejdź do strony internetowej **Urządzenie > LCD > Interfejs wyświetlacza w trybie gotowości**.

Device» **LCD**

**Standby Interface Display**

Screensaver Mode: Image

Screensaver Time(Sec): 60

Wake Up Screensaver Mode: IR Detection

Deep Sleep Enabled:

Deep Sleep Interval(Min): 30

- **Tryb wygaszacza ekranu:**

- **Brak:** ekran pozostanie włączony bez przechodzenia w tryb wygaszacza ekranu.
- **Pusty:** ekran stanie się czarny.
- **Obraz :** przesłane zdjęcie będzie wyświetlane jako wygaszacz ekranu.
- **Screensaver Time (Sec) (Czas wygaszacza ekranu (sek.)):** ustawienie czasu uruchomienia wygaszacza ekranu w zakresie od 5 do 180 sekund. Wygaszacz ekranu uruchamia się, gdy urządzenie nie wykryje żadnej operacji lub nikt się nie zbliża.
- **Tryb wygaszacza ekranu budzenia :**
  - **Auto :** ekran zostanie wybudzony, gdy ktoś się do niego zbliży bez dotykania go.
  - **Ręcznie:** dotknięcie i wybudzenie ekranu.
- **Deep Sleep Enabled:** ekran wyłączy się po upływie zdefiniowanego czasu trwania wygaszacza ekranu.
- **Deep Sleep Interval (Min):** ustawienie czasu wygaszacza ekranu przed jego wyłączeniem.

#### Uwaga

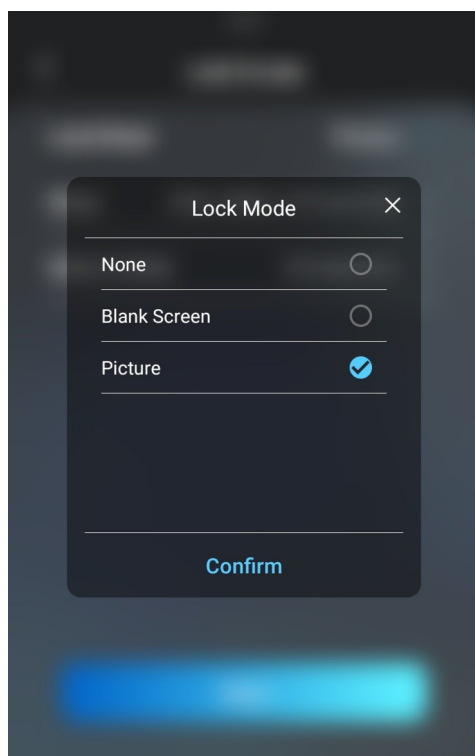
Trybu wygaszacza ekranu nie można zmienić z **automatycznego** na **ręczny**, gdy tryb wygaszacza ekranu jest ustawiony jako **pusty** ekran.

## Konfiguracja wygaszacza ekranu na urządzeniu

Można również skonfigurować wygaszacz ekranu na

urządzeniu. Przejdź do opcji **Ustawienia**

**podstawowe**> Ekran blokady.




## Prześlij wygaszacz ekranu

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

Przejdź do interfejsu internetowego **Urządzenie > LCD > Prześlij wygaszacz ekranu.**

Upload Screensaver

ScreenSaver1 ▾  Import

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

- Przesyłane zdjęcia powinny być w formacie JPG o maksymalnej rozdzielczości 2 mln pikseli.
- 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. Przejdź do interfejsu Web **Setting > Key/Display > Picture/File**

**Picture/File Import**

Boot Animation (.png / .zip)

 Import

 Reset

Background of Tenants List(.png)

 Import

 Reset

### Uwaga

- Przesyłane zdjęcia powinny być w formacie **.png lub .zip**.
- Maksymalny rozmiar pliku .zip: 20 MB; Maksymalny rozmiar obrazu: 1 MB; Maksymalna rozdzielczość: 800 \* 1280.

## Prześlij obraz tła listy kontaktów urządzenia

Można dostosować wyświetlanie tła listy kontaktów. Przed przesłaniem zdjęcia można je wybrać. Przejdź do interfejsu Web **Setting > Key/Display > Picture/File Import**.

### Picture/File Import

Boot Animation (.png / .zip)

Import

Reset

Background of Tenants List(.png)

Import

Reset

### Uwaga

- Przesyłane zdjęcia powinny być w formacie **.png**.
- Maksymalny rozmiar obrazu: 1 MB; Maksymalna rozdzielczość: 800\*1280.

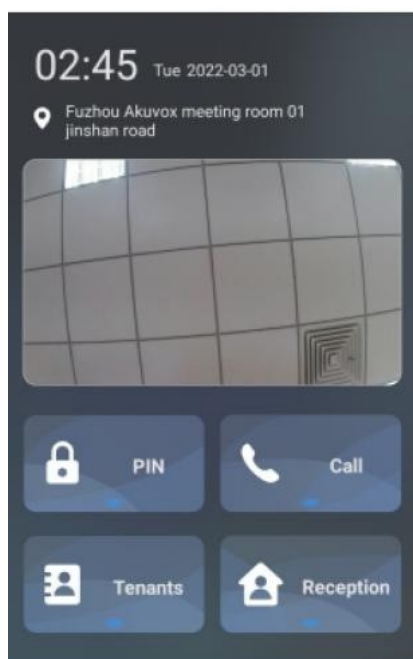
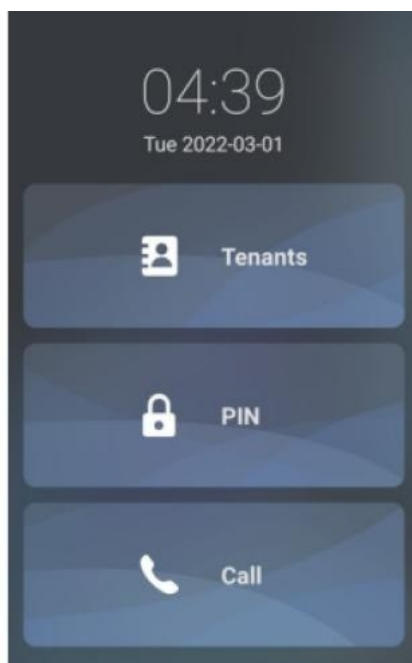
## Konfiguracja ekranu głównego

Wygląd ekranu głównego można zmienić poprzez konfigurację nazwy i układu kart w sieci Web urządzenia. Można przełączać się między motywami Building i Villa w interfejsie internetowym Setting > Key/Display > Theme.

### Theme

Mode

Villa

**Building Mode****Villa Mode**

## Wyświetlanie ekranu głównego trybu Villa

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

Przejdź do interfejsu web **Setting > Key/Display**. Wybierz **Villa** jako motyw.

**Theme**

Mode

Villa

**View Control of The Villa Theme**

Default Page

Home Page

Index	Key	Label	Value
1	Tenants		VISIBLE
2	PIN		VISIBLE
3	Call		VISIBLE

● **Strona domyślna :**

- **Strona główna :** wyświetlanie ikon lokatorów, PIN i połączeń pionowo na ekranie głównym.
- **Najemca:** wyświetlanie kontaktu na ekranie głównym.
- **PIN:** wyświetlenie ikony PIN za pomocą klawiatury na ekranie głównym.
- **Połączenie:** ikona połączenia z klawiaturą numeryczną na ekranie głównym.

● **Klawisz:** ustawienie typu ikony wyświetlanej na ekranie głównym trybu willi.

● **Etykieta:** nadawanie nazw ikonom na ekranie głównym trybu willi.

● **Widoczna :** jeśli ustawisz ikonę jako niewidoczną, nie będzie ona widoczna na ekranie.

## Ekran główny trybu budynku

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

Przejdź do interfejsu internetowego **Ustawienia > Klucz/Wyświetlanie > Klucz na stronie głównej motywu budynku**.

**Key In Homepage Of The Building Theme**

Index	Label	Type	Value
1		PIN	
2		Call	
3		Tenants	
4		Speed Dial	0.0.0.0

● **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.

## 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 hasła.

Przejdź do strony internetowej **Ustawienia > Klawisze/Wyświetlacz > Tryb wyświetlania klawiatury** interfejsu **PIN**.  
Keypad Display Mode Of PIN Interface

Mode

Normal

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

## Wyświetlanie monitu na ekranie wybierania

Przejdź do interfejsu internetowego **Ustawienia > Klawisze/Wyświetlacz > Monit strony połączenia**.

Prompt of The Call Page

Text Prompt

Please enter the apartment number (e.g. 101)

### Uwaga

X915 obsługuje monit tekstowy o maksymalnej długości 128 znaków.

## Wyświetlanie komunikatu tekstowego otwartych drzwi

Przejdź do interfejsu Web **Access Control > Relay > Open Door Text Prompt**.

### Open Door Text Prompt

Open Door Outside Succeeded Text P...



Open Door Inside Succeeded Text Pro...



Open Door Failed Text Prompt



Display User Info



- **Open Door Outside Succeeded Text Prompt**: po otwarciu drzwi na ekranie urządzenia pojawi się komunikat tekstowy. Domyślnie jest to "Access Granted".
- **Open Door Inside Succeeded Text Prompt**: po uruchomieniu wejścia pojawi się monit tekstowy.
- **Open Door Failed Text Prompt**: gdy otwarcie drzwi nie powiedzie się, pojawi się monit tekstowy.



- **Wyświetl informacje o użytkowniku:** wyświetla informacje o użytkowniku po rozpoznaniu twarzy. Jeśli rozpoznawanie twarzy powiedzie się, na ekranie urządzenia pojawi się komunikat tekstowy "Access Granted" z identyfikatorem i nazwą użytkownika. W przypadku niepowodzenia wyświetlony zostanie komunikat tekstowy "Access Denied" (Odmowa dostępu) z komunikatem "Stranger, Name: Nieznany".

## 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 personalizowane wrażenia użytkownika.

### Konfiguracja głośności

#### Konfiguracja głośności w interfejsie internetowym

Przejdź do strony internetowej **Urządzenie > Interfejs audio**.

Device» [Audio](#)

---

**Volume Control**

Tamper Alarm Volume	<input type="text" value="8"/>	(1~8)
Mic Volume	<input type="text" value="1"/>	(1~127)

---

**Volume Control On Talking Interface**

Enabled	<input checked="" type="checkbox"/>
---------	-------------------------------------

---

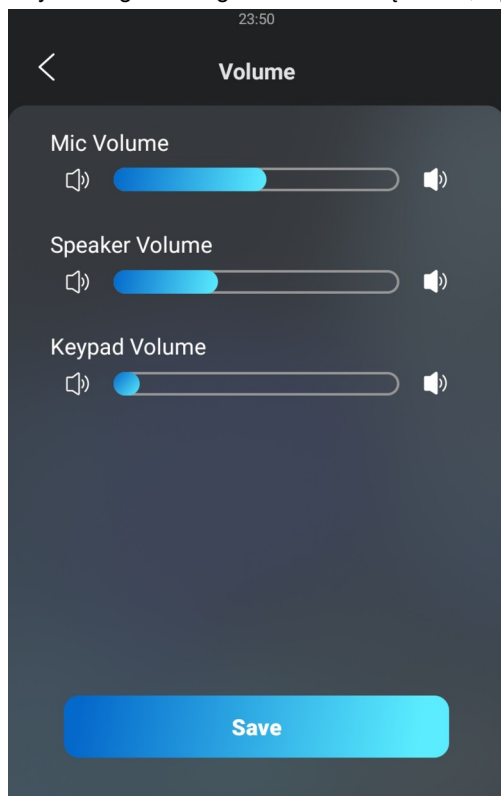
**Mic Mode**

Select On	<input type="text" value="Left Mic"/>	▼
-----------	---------------------------------------	---

- **Regulacja głośności w interfejsie rozmowy:** po włączeniu tej funkcji użytkownicy mogą regulować głośność połączenia podczas sesji rozmowy.
- **Select On:** wybór mikrofonu, który ma zostać zastosowany pomiędzy lewym i prawym mikrofonem.

## Konfiguracja głośności na urządzeniu

Aby skonfigurować głośność na urządzeniu, wybierz **Ustawienia podstawowe > Głośność**.



## Ustawienia komunikatów głosowych

Dźwięk dla różnych scenariuszy można przesłać w interfejsie internetowym urządzenia. Przejdź do interfejsu internetowego

**Device > Audio > Voice Prompt Setting.**

Voice Prompt Setting

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

## Uwaga

Format pliku: wav mp3, rozmiar: < 200KB, częstotliwość próbkowania: 16000, Bity: 16.

## Ustawienia sieciowe

### Ustawienia połączenia sieciowego urządzenia

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

Aby sprawdzić stan sieci w interfejsie internetowym **Status > Info > Network Information**.

#### Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.121
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	

Aby zmienić połączenie sieciowe w interfejsie **Sieć > Podstawowe**.

#### LAN Port

DHCP  Static IP

IP Address	192.168.1.104
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS Server	192.168.1.1
Alternate DNS Server	192.168.1.1

- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Jeśli wybrany zostanie tryb DHCP, bramofon zostanie automatycznie przypisany do adresu IP, maski podsieci, bramy domyślnej i adresu serwera DNS przez serwer DHCP.
- **Statyczne IP** : po wybraniu trybu statycznego IP, adres IP, maska podsieci, brama domyślna i adres serwera DNS muszą zostać skonfigurowane ręcznie zgodnie z rzeczywistym środowiskiem sieciowym.
- **Adres IP** : ustawienie adresu IP po wybraniu trybu statycznego adresu IP.
- **Maska podsieci**: ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Default Gateway (Brama domyślna)**: ustawienie prawidłowej bramy zgodnie z adresem IP.

- **Preferred/Alternate DNS Server:** skonfiguruj serwer nazw domen (DNS) zgodnie z rzeczywistym środowiskiem sieciowym. Preferowany serwer DNS jest podstawowym adresem serwera DNS, natomiast alternatywny serwer DNS jest serwerem dodatkowym. Bramofon łączy się z alternatywnym serwerem DNS, gdy podstawowy jest niedostępny.

## 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.

Przejdź do interfejsu **Sieć > Zaawansowane > Lokalny RTP**.

### Local RTP

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

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

Przejdź do interfejsu **Sieć > Zaawansowane > Ustawienia połączenia**.

### Connect Setting

Server Mode	Cloud
Discovery Mode	<input checked="" type="checkbox"/>
Device Address	<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="X915"/>

- **Tryb 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 w żadnym typie serwera.
- **Tryb wykrywania:** tryb wykrywania sprawia, że urządzenie jest wykrywane przez inne urządzenia w sieci. Wyłącz go, jeśli chcesz ukryć urządzenie, aby nie było wykrywane przez inne urządzenia. Po wyłączeniu trybu wykrywania należy ponownie uruchomić urządzenie.
- **Adres urządzenia :** określ adres urządzenia, wprowadzając informacje o lokalizacji urządzenia od lewej do prawej: **Community (Wspólnota)**, **Unit (Jednostka)**, **Stair (Schody)**, **Floor (Piętro)**, **Room (Pokój)** w kolejności.
- **Device Extension:** wprowadź numer wewnętrzny zainstalowanego urządzenia.

- **Lokalizacja urządzenia:** wprowadź lokalizację, w której urządzenie jest zainstalowane i używane.

## Ustawienie NAT

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

Przejdź do interfejsu **Konto internetowe > Zaawansowane > NAT**.

### NAT

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

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

## 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.

### Konfiguracja połączeń IP

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

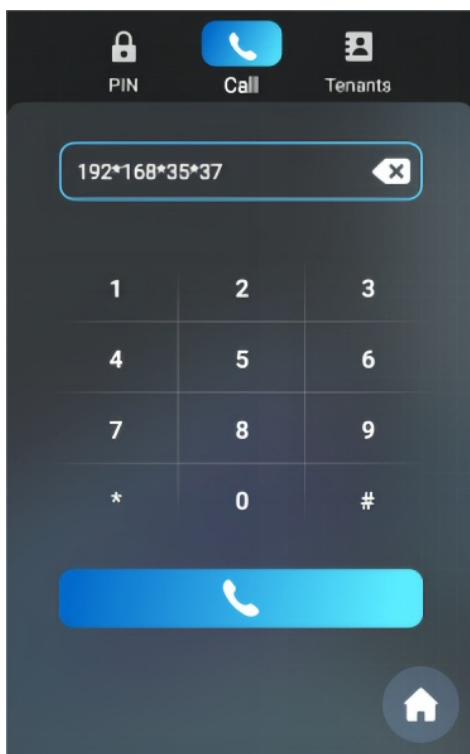
#### Direct IP

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

**Port:** ustawienie portu dla bezpośrednich połączeń IP. Domyślną wartością jest 5060, z zakresem od 1-65535. W przypadku wprowadzenia wartości z tego zakresu innej niż 5060, należy zapewnić spójność z odpowiednim urządzeniem do transmisji danych.

### Wykonywanie połączeń IP

Aby wykonywać połączenia SIP lub IP na urządzeniu, dotknij przycisku wybierania i wprowadź numer IP.



## Konfiguracja połączeń SIP i połączeń SIP

Session Initiation Protocol (**SIP**) to protokół transmisji sygnałów używany do inicjowania, utrzymywania i kończenia połączeń. Połączenie SIP wykorzystuje protokół SIP do wysyłania i odbierania danych między urządzeniami SIP i może wykorzystywać Internet lub sieć lokalną w celu zapewnienia wysokiej jakości i bezpiecznej komunikacji. Zainicjowanie 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 w interfejsie internetowym

Przejdź do interfejsu **Konto internetowe > Podstawowe > Konto SIP**.

**SIP Account**

Status	UnRegistered
Account	<input type="text" value="Account1"/>
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>

- **Konto 1/Konto 2:** bramofon obsługuje 2 konta SIP.

-Konto 1 jest domyślnym kontem do przetwarzania połączeń. Będzie ono również wykorzystywane po aktywacji usługi chmurowej Akuvox SmartPlus.

- System przełączy się na konto 2, jeśli konto 1 nie jest zarejestrowane.

- Aby wyznaczyć konto, które ma być używane do połączeń wychodzących, wybierz numer konta dla kontaktów lub prefiks planu wybierania w ich ustawieniach.

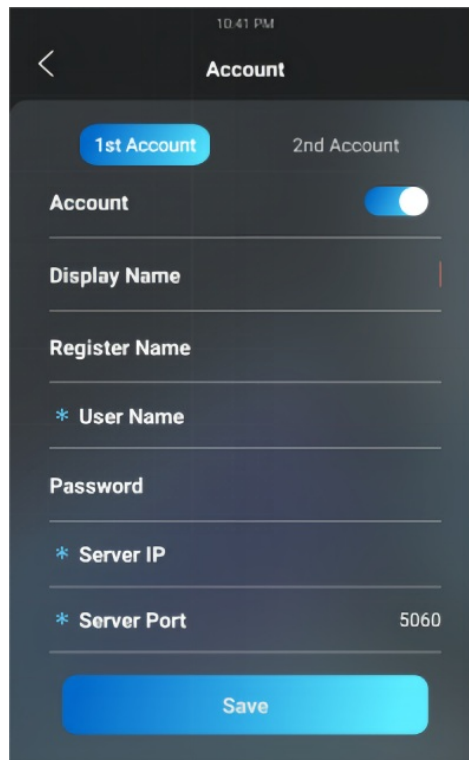
**Wskazówka**

Informacje na temat konfigurowania połączeń kontaktowych i planu wybierania numerów można znaleźć [tutaj](#).

- **Etykieta wyświetlacza:** etykieta urządzenia.
- **Wyświetlana nazwa:** oznaczenie konta 1 lub 2, które będzie wyświetlane na urządzeniu na ekranie wywoływania.
- **Nazwa rejestru:** taka sama jak nazwa użytkownika z serwera PBX.
- **Nazwa użytkownika:** taka sama jak nazwa użytkownika z serwera PBX do uwierzytelniania.
- **Hasło:** takie samo jak hasło z serwera PBX do uwierzytelniania.

## Konfiguracja konta SIP na urządzeniu

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



## 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.

Przejdź do interfejsu **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)

- **IP serwera:** wprowadź numer adresu IP serwera lub jego adres URL.
- **Port:** ustawienie portu serwera SIP dla transmisji danych.
- **Registration Period :** ustaw czas rejestracji konta SIP. Ponowna rejestracja SIP rozpocznie się automatycznie, jeśli rejestracja konta nie powiedzie się w czasie rejestracji. Domyślny okres rejestracji wynosi **1800**, w zakresie **30-65535s**.



## 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.

Przejdź do interfejsu web **Intercom > Call Feature > DND**.

### DND

Enabled

Return Code When DND

486(Busy Here) ▼

- **Return Code When DND** : określa kod wysyłany do dzwoniącego przez serwer SIP w przypadku odrzucenia połączenia przychodzącego w trybie DND.

## 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.

Przejdź do interfejsu Web **Account > Basic > Outbound Proxy Server**.

### Outbound Proxy Server

Outbound Enabled

Preferred Server IP

Port

5060

(1024-65535)

Alternate Server IP

Port

5060

(1024-65535)

- **Preferred Server IP**: wprowadź adres IP **serwera** proxy SIP.
- **Port**: ustawienie portu do nawiązywania sesji połączenia przez wychodzący serwer proxy.
- **Alternate Server IP**: wprowadź adres IP **serwera** proxy SIP, który będzie używany w przypadku awarii głównego serwera proxy.
- **Port**: ustawienie portu proxy do nawiązywania sesji połączeń za pośrednictwem zapasowego serwera proxy połączeń wychodzących.

## Konfiguracja typu transmisji danych

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

Przejdź do interfejsu **Konto internetowe > Podstawowe > Typ transportu**.

### Transport Type

Type

UDP ▼

- **UDP:** Niezawodny, ale bardzo wydajny protokół warstwy transportowej. Jest to domyślny protokół transportowy.
  - **TCP:** Mniej wydajny, ale niezawodny protokół warstwy transportowej.
  - **TLS:** Szyfrowany i zabezpieczony protokół warstwy transportowej. Wybierz tę opcję, jeśli chcesz szyfrować wiadomości SIP w celu zwiększenia bezpieczeństwa lub jeśli serwer drugiej strony korzysta z TLS. Aby z niej skorzystać, należy przesłać certyfikaty w celu uwierzytelnienia.
- DNS-SRV:** Rekord usługi DNS definiuje lokalizację serwerów. Rekord ten zawiera nazwę hosta i numer portu serwera, a także wartości priorytetu i wagi, które określają kolejność i częstotliwość korzystania z serwera.

## Konfiguracja opcji wybierania numeru

### Szybkie wybieranie numeryczne

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

### Szybkie wybieranie 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. Przejdź do interfejsu web **Intercom > Dial Plan > Replace Rule**. Kliknij +Add.

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

**Add Replace Rules** ✕

Account	Auto ▼
Prefix	
1st Replace	
2nd Replace	
3rd Replace	
4th Replace	
5th Replace	

Cancel
Submit

- **Konto:** wybór konta dial-out.

- **Auto:** wybieranie numeru przy użyciu zarejestrowanego konta. Jeśli zarejestrowane są 2 konta, konto 1 jest domyślne.

- **Konto 1/2:** wybieranie numeru przy użyciu wybranego konta.

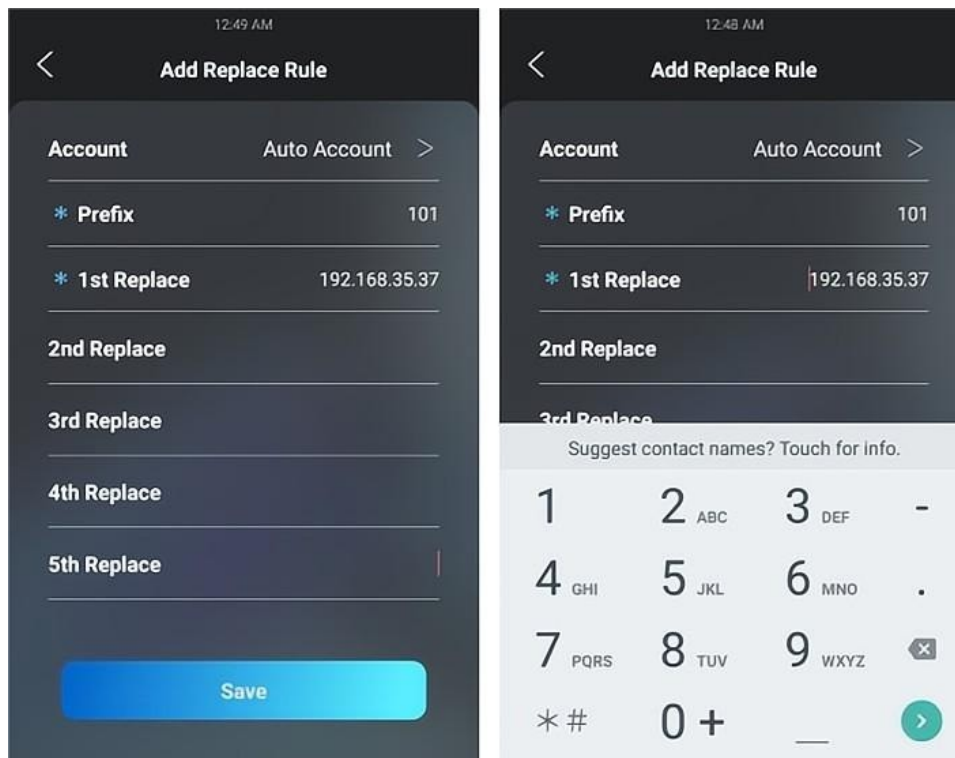
- **Prefiks:** określenie krótkiego numeru zastępującego określone wybierane numery.
- **Zastęp 1/2/3/4/5:** określa do 5 numerów, które mogą być numerami SIP lub adresami IP, które mają zostać zastąpione prefiksem. Wszystkie te numery będą wywoływane jednocześnie, gdy dzwoniący wybierze prefiks.

### Uwaga

Pole wyboru dla każdego wiersza **Prefiksu** powinno być zaznaczone, zanim pojawi się zakładka **Edytuj**, którą należy kliknąć, aby zmodyfikować.

## Szybkie wybieranie przez wymianę numeru na urządzeniu

Aby skonfigurować zastępowanie numerów na ekranie **Ustawienia** urządzenia > **Reguła zastępowania** > **Dodaj regułę zastępowania**.



## 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, wybierz kolejno opcje **Ustawienia** > **Klawisze/Wyświetlacz** > **Tryb wyświetlania interfejsu połączeń (Szybkie wybieranie)**.

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"/>

- **Tryb:** definiowanie układu przycisków szybkiego wybierania i klawiatury na ekranie wybierania. Poniżej objaśniono 9 opcji:

Opcje	Opisy
Standard	Wyświetlanie czasu i klawiatury.
Auto	Wyświetla wszystkie przyciski szybkiego wybierania ustawione przez użytkowników.
1 Klucz	Wyświetlanie pojedynczej umowy bez klawiatury.
1 Klawisz + Klawiatura	Wyświetlanie pojedynczego przycisku wybierania za pomocą klawiatury.
2 klawisze + klawiatura	Wyświetlanie do 2 przycisków wybierania za pomocą klawiatury.
4 klawisze + klawiatura	Wyświetlanie do 4 przycisków wybierania za pomocą klawiatury.
8 Klucze	Wyświetlanie do 8 przycisków wybierania bez klawiatury.
16 Klucze	Wyświetlanie do 16 przycisków wybierania bez klawiatury.
64 Klucze	Wyświetlanie do 64 przycisków 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**. Przejdź do interfejsu Web **Setting > Key/Display > Speed Dial Setting**.

## Speed Dial Setting

Group	<input type="text" value="Disabled"/>	
Dial Out Forward	<input checked="" type="checkbox"/>	
Mode	<input type="text" value="Schedule"/>	
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> <span>1 item</span> <span>All Schedules</span> </div> <div style="padding: 5px;"> <input type="checkbox"/> 1002:Never                 </div> </div>	<input type="button" value="&gt;"/> <input type="button" value="&lt;"/>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> <span>1 item</span> <span>Schedules Selected</span> </div> <div style="padding: 5px;"> <input type="checkbox"/> 1001:Always                 </div> </div> <div style="text-align: right; margin-top: 5px;"> <input type="button" value="↑"/>  <input type="button" value="↓"/> </div>

- **Grupa** : wybierz grupę kontaktów, do której chcesz zadzwonić, naciskając przycisk odbioru.
- **Dial Out Forward** : po włączeniu wszystkie połączenia będą wykonywane na ten sam numer docelowy po naciśnięciu przycisku odbioru.
- **Mode (Tryb)**: gdy funkcja Dial Out Forward jest włączona, należy skonfigurować harmonogram jej działania. Możesz także wybrać opcję **Auto Disable** i zdecydować, po ilu godzinach funkcja zostanie wyłączona.

## Ustawienia połączeń

### 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"/>	

- **Auto Answer Delay (Opóźnienie automatycznego odbierania)**: ustaw czas, po którym połączenie zostanie automatycznie odebrane po zadzwonieniu. Na przykład, jeśli ustawisz czas opóźnienia na 5 sekund, bramofon automatycznie odbierze połączenie po 5 sekundach.
- **Tryb**: określenie, czy połączenie ma być automatycznie odbierane jako połączenie wideo czy audio.

## 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.

Przejdź do interfejsu web **Intercom > Basic > Sequence Call**.

### Sequence Call

Enabled	<input type="checkbox"/>
Time Out (Sec)	60 ▼
When Refused	Do Not Call Next ▼

- **Time Out(Sec):** określa limit czasu dla połączenia między dwoma kolejnymi numerami połączeń. Na przykład, jeśli wartość czasu jest ustawiona na 10, połączenie, które nie zostanie odebrane w ciągu 10 sekund, zostanie automatycznie zakończone i przekazane do następnego numeru połączenia w kolejności.
- **When Refused:** określa, czy zadzwonić do następnego, jeśli połączenie zostało odrzucone przez poprzednio dzwoniącego.
  - **Do Not Call Next:** połączenie sekwencyjne zostanie zatrzymane, gdy połączenie zostanie odrzucone.
  - **Call Next:** urządzenie zadzwoni na następny numer w kolejności, gdy połączenie zostanie odrzucone.

#### Uwaga

Funkcja Sequence Call powinna być obsługiwana przez **SmartPlus**, aby uzyskać więcej informacji, skontaktuj się z pomocą techniczną Akuvox.

## Połączenie grupowe

Można skonfigurować akcję, gdy połączenie grupowe zostanie odrzucone.

Przejdź do interfejsu web **Intercom > Basic > Only Group Call Allowed**.

### Only Group Call Allowed

When Refused

End This Call Only ▼

**When Refused** : w przypadku wybrania opcji **End All Calls** , połączenie grupowe zostanie zakończone, jeśli zostanie odrzucone przez rozmówcę. Jeśli wybierzesz opcję **Zakończ tylko to połączenie**, połączenie grupowe będzie kontynuowane, gdy zostanie odrzucone przez jednego z rozmówców.

## Połączenie internetowe

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

Przejdź do interfejsu web **System > Maintenance > Web Call**. Wybierz zarejestrowane konto SIP, aby nawiązać połączenie internetowe.

---

**Web Call**

---

Web Call(Ready)  Auto ▼

## Nawiązywanie dwukierunkowych połączeń wideo

Dwukierunkowa funkcja wideo umożliwia wizualne połączenie zarówno z dzwoniącymi, jak i odbiorcami za pośrednictwem bramofonu, zapewniając bardziej interaktywną i bezpieczną rozmowę.

Przejdź do interfejsu web **Intercom > Basic > Two-way Video**.

---

**Two-Way Video**

---

Enabled

---

## 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.

Przejdź do interfejsu web **Intercom > Call Feature > Max Call Time**.

---

**Max Call Time**

---

Max Call Time  (2~30Min)

---

- **Max Call Time (Maksymalny czas połączenia):** określa maksymalny czas trwania wszystkich połączeń. Bramofon automatycznie zakończy połączenie po osiągnięciu limitu czasu.

## 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.

Przejdź do interfejsu Web **Intercom > Call Feature > Max Dial Time**.

---

**Max Dial Time**

---

Dial In Time  (3~120Sec)

Dial Out Time  (3~120Sec)

---

- **Dial In Time:** określenie maksymalnego czasu trwania połączenia przychodzącego. Bramofon automatycznie zakończy połączenie przychodzące, jeśli nie zostanie ono odebrane w ustawionym czasie.

- **Dial Out Time:** określa maksymalny czas trwania połączenia wychodzącego. Bramofon automatycznie zakończy wybrane połączenie, jeśli odbiorca nie odbierze go w ustawionym czasie.

## Odlóż słuchawkę po otwarciu drzwi

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

Przejdź do interfejsu web **Intercom > Call Feature > Hang Up After Open Door**.

### Hang Up After Open Door

Enabled	<input checked="" type="checkbox"/>
Type	DTMF Or HTTP
Time Out	5 (0~15Sec)

- **Typ:** określa metodę odblokowywania drzwi. Jeśli ta konkretna metoda jest używana do odblokowania drzwi podczas połączenia, bramofon zakończy połączenie po osiągnięciu ustawionego czasu rozłączenia.
- **Time Out:** określenie limitu czasu rozłączenia. Bramofon automatycznie zakończy połączenie po osiągnięciu określonego czasu po otwarciu drzwi.

## 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.

Przejdź do interfejsu **Konto internetowe > Zaawansowane > Konto SIP**.

### SIP Account

Account

Account1

Account1

Account2

### Audio Codecs

0 item Disabled Codecs



3 items Enabled Codecs

- PCMU
- PCMA
- G722



Poniżej znajdują się informacje na temat zużycia pasma i częstotliwości próbkowania dla poszczególnych 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.

Przejdź do interfejsu **Konto internetowe > Zaawansowane > Kodek wideo.**

### Video Codec

Name	<input checked="" type="checkbox"/> H.264
Resolution	<input type="text" value="4CIF"/>
Bitrate	<input type="text" value="320 kbps"/>
Payload	<input type="text" value="104"/>

- **Nazwa** : zaznacz, aby wybrać format kodeka wideo H264 dla obrazu wideo z bramofonu H264 jest domyślnym kodekiem wideo.
- **Rozdzielczość**: wybierz rozdzielczość kodu dla jakości wideo spośród **QCIF, CIF, VGA, 4CIF i 720P** zgodnie z rzeczywistym środowiskiem sieciowym. Domyślną rozdzielczością kodu jest VGA.
- **Bitrate** : wybór szybkości transmisji strumienia wideo (w zakresie 320-2048). Im większa szybkość transmisji bitów, tym większa ilość danych przesyłanych w każdej sekundzie i tym wyraźniejszy obraz wideo. 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.

Przejdź do interfejsu web **Intercom > Call Feature > IP Video Parameters.**

### IP Video Parameters

Video Resolution	<input type="text" value="4CIF"/>
Video Bitrate	<input type="text" value="2048 kbps"/>
Payload	<input type="text" value="104"/>

- **Rozdzielczość wideo**: wybierz rozdzielczość kodu dla jakości wideo spośród **CIF, VGA, 4CIF i 720P**. Domyślną rozdzielczością kodu jest 720P.

- **Szybkość transmisji wideo:** wybierz szybkość transmisji wideo spośród **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**.
- **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.

Przejdź do **Konto internetowe > Zaawansowane > Interfejs DTMF**.

### DTMF

Type	<input type="text" value="RFC2833"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
Payload	<input type="text" value="101"/> (96~127)

- **Tryb:** wybór trybu DTMF spośród **Inband, RFC 2833, Info, Info+Inband, Info+RFC 2833** i **Info+Inband+RFC 2833** w oparciu o określony typ transmisji DTMF urządzenia innej firmy, z którym ma zostać nawiązane połączenie jako strona odbierająca dane sygnału.
- **Jak powiadamiać DTMF:** wybierz jeden z czterech typów: **Disabled, DTMF, DTMF-Relay** i **Telephone-Event** zgodnie z określonym typem przyjętym przez urządzenie innej firmy. Konfiguracja jest wymagana tylko wtedy, gdy urządzenie innej firmy, z którym ma zostać nawiązane połączenie, przyjmuje tryb **Info**.
- **Payload:** ustaw ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą a odbiorcą podczas transmisji danych.

## Konfiguracja książki telefonicznej

### 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. Przejdź do interfejsu **Web Directory > Tenants List > Group**.

#### Group

<input type="checkbox"/>	Index	Name	Edit
No Data			

1/1

## Konfiguracja listy kontaktów w interfejsie internetowym

Przejdź do interfejsu Web **Directory > Tenants List > Local Tenants List**. Kliknij **+Add**, aby dodać kontakt.

Local Tenants List

Index	Name	Phone	Group	Dial Account	Email	Floor Num	Priority Of Call	Edit
No Data								

1/1

### Tenants Basic

Name	<input type="text" value="Judy"/>
Phone	<input type="text" value="123"/>
Email	<input type="text" value="123@akuvox.com"/>
Group	<input type="text" value="Default"/>
Dial Account	<input type="text" value="Auto"/>
Priority Of Call	<input type="text" value="NULL"/>
Floor No.	<input type="text" value="1"/>

**Priorytet połączenia:** ustaw priorytet połączenia spośród czterech opcji: **Null, Firstly, Secondary i Lastly**. Ta funkcja ma zastosowanie głównie do kontaktów w określonej grupie kontaktów. Na przykład, jeśli ustawisz priorytet połączenia dla jednego z kontaktów w określonej grupie kontaktów jako **Pierwszy**, wówczas kontakt ten będzie wywoływany jako pierwszy spośród wszystkich kontaktów w tej samej grupie kontaktów, gdy ktoś naciśnie grupę kontaktów w celu wykonania połączenia grupowego.

#### Uwaga

- Priorytetu połączenia kontaktu nie można ustawić, gdy kontakt należy do dowolnej grupy kontaktów.
- Format pliku kontaktu do importu powinien być w formacie CSV lub XML, natomiast format pliku kontaktu do eksportu powinien być w formacie XML, CSV i VCF. Maksymalna liczba importowanych kontaktów wynosi 3000.
- Tylko numery SIP kontaktów mogą być wywoływane przez konto SIP. Numery IP nie są ważne dla tej aplikacji.
- Zanim będzie można wybrać lub zmienić grupę, należy ją najpierw utworzyć.

## Konfiguracja książki telefonicznej na urządzeniu

Książkę telefoniczną można również skonfigurować na ekranie **Ustawienia urządzenia > Najemcy**.

### Ustawienia wyświetlania listy kontaktów

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

Przejdź do interfejsu Web **Directory > Tenants List > Tenants List Setting.**

### Tenants List Setting

Show Tenants Of Local Group Enabled	<input checked="" type="checkbox"/>
Show Cloud Tenants Enabled	<input checked="" type="checkbox"/>
Call Permission	Single Call & Group Call ▼
Tenants Sort By	ASCII Code ▼
Click Tenants To Dial Out	<input checked="" type="checkbox"/>
Local Tenants Profile Display Mode	Enabled ▼
Expand Tenants List View Mode	<input type="checkbox"/>
Hide Group Label For Local Tenants List	<input type="checkbox"/>
Tenant List Search Box Visibled	<input checked="" type="checkbox"/>

- **Show Tenants of Local Group Enabled** : zaznacz lub odznacz pole wyboru, aby kontrolować wyświetlanie etykiety grupy. Jeśli pole wyboru zostanie odznaczone, wyświetlana będzie tylko karta grupy, a karta kontaktu będzie ukryta i odwrotnie.
- **Show Cloud Tenants Enabled**: zaznacz pole wyboru, aby wyświetlić dzierżawców chmury na liście dzierżawców. Po usunięciu zaznaczenia pola wyboru dzierżawcy chmury zostaną ukryci.
- **Najemcy Sortuj według**:
  - Kod ASCII: najemcy będą wymieniani według nazw w kolejności kodu ASCII.
  - Numer pokoju: najemcy zostaną posortowani według numerów pokoi.
  - Import: najemcy zostaną posortowani według kolejności w importowanym pliku.

**Click Tenants to Dial Out**: po włączeniu tej opcji można nacisnąć dowolne miejsce na karcie kontaktu, aby wybrać numer. Gdy opcja ta jest wyłączona, użytkownicy muszą nacisnąć ikonę połączenia, aby wybrać numer.

#### Tryb wyświetlania profilu lokalnego najemcy :

Włączone: jeśli najemca ma przesłane zdjęcie profilowe kontaktu, zdjęcie będzie wyświetlane obok nazwy; jeśli nie, obok nazwy będzie wyświetlana domyślna ikona kontaktu.

Wyłączone: obraz lub ikona nie będą wyświetlane.

Automatycznie: jeśli najemca ma przesłane zdjęcie profilowe kontaktu, zdjęcie zostanie wyświetlone obok nazwy; jeśli nie, obok nazwy nie będzie ikony.

- **Rozwiń tryb widoku listy kontaktów**: zaznacz pole wyboru, aby kontrolować rozmiar karty kontaktu. Po włączeniu zakładka kontaktów zostanie poszerzona.
- **Hide Group Label for Local Tenants List (Ukryj etykietę grupy dla lokalnej listy najemców)**: kontroluje wyświetlanie etykiety grupy. Po włączeniu tej opcji wyświetlana będzie tylko karta kontaktu, a karta grupy będzie ukryta.

- **Pole wyszukiwania listy kontaktów widoczne** : kontroluj wyświetlanie pola **Dotknij tutaj, aby wyszukać** w górnej części ekranu. Po wyłączeniu pole **Dotknij tutaj, aby wyszukać** będzie ukryte.

## Konfiguracja kontroli dostępu do drzwi

### Ustawienie przełącznika przekaźnika

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

#### 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	0 ▼	1 ▼	2 ▼
2~4 Digits DTMF	010	012	013
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Relay Name	RelayA	RelayB	RelayC

- **Identyfikator przekaźnika**: można skonfigurować łącznie trzy przełączniki przekaźnikowe do kontroli dostępu do drzwi.
- **Typ**: jeśli wybrano stan Domyślny, stan przekaźnika pokazuje Niski, co oznacza, że drzwi są zamknięte, a jeśli stan przekaźnika pokazuje Wysoki, drzwi są otwarte. Jeśli wybrano opcję Invert State (Odwrócony stan), stan przekaźnika pokazuje High (Wysoki), co oznacza, że drzwi są zamknięte, a Low (Niski) oznacza, że drzwi są otwarte.
- **Tryb**: dostępne są dwa tryby: monostabilny i bistabilny. Jeśli wybrano tryb Monostabilny, stan przekaźnika zostanie automatycznie zresetowany po upływie czasu opóźnienia po wyzwoleniu przekaźnika. Jeśli wybrano opcję Bistable, stan przekaźnika zostanie zresetowany po ponownym wyzwoleniu przekaźnika.
- **Trigger Delay (Sec)**: ustaw czas opóźnienia wyzwolenia przekaźnika (w zakresie od 1 do 10 sekund). Na przykład, jeśli ustawisz czas opóźnienia na **5** sekund, przekaźnik zostanie wyzwolony dopiero po 5 sekundach od naciśnięcia przycisku **odblokowania**.
- **Opóźnienie wstrzymania (sek.)**: ustaw czas opóźnienia wstrzymania przekaźnika (w zakresie od 1 do 10 sek.) Na przykład, jeśli ustawisz czas opóźnienia wstrzymania na **5** sekund, przekaźnik powróci do stanu początkowego po utrzymaniu stanu wyzwolenia przez 5 sekund.
- **Opcja 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.
- **DTMF**: ustawienie 1-cyfrowego kodu DTMF w zakresie (**0-9 i \*,#**), jeśli opcja DTMF jest ustawiona jako **1-cyfrowa**.
- **Multiple DTMF** : ustaw kod DTMF zgodnie z ustawieniem **opcji DMTP**. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli **opcja DTMP jest ustawiona** 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. Na przykład, dla wygody można nazwać przełącznik przekaźnika zgodnie z jego lokalizacją.

#### Uwaga

- Tylko urządzenia zewnętrzne podłączone do przełącznika przekaźnikowego muszą być zasilane przez zasilane adaptory, ponieważ przekaźnik nie dostarcza zasilania.

## Ustawienie przekaźnika bezpieczeństwa

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



Przejdź do interfejsu Web **Access Control > Relay > Security Relay**.

#### Security Relay

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

- **Typ połączenia:** wybierz typ połączenia między przekaźnikiem bezpieczeństwa a bramofonem. Można wybrać połączenie przez wyjście zasilania przekaźnika A bramofonu lub RS485.
- **Trigger Delay (Sec):** ustawienie opóźnienia wyzwolenia przekaźnika (w zakresie od 1 do 10 sekund). Na przykład,

jeśli ustawisz czas opóźnienia na 5 sekund, przełącznik zostanie wyzwolony dopiero po 5 sekundach od naciśnięcia przycisku Odblokuj. Domyślną wartością jest 0, co oznacza wyzwolenie przełącznika zaraz po naciśnięciu przycisku odblokowania.

- **Opóźnienie wstrzymania (sek.):** ustawienie czasu opóźnienia wstrzymania przełącznika (w zakresie od 1 do 10 sek.) Na przykład, jeśli ustawisz czas opóźnienia wstrzymania na 5 sekund, przełącznik zostanie opóźniony o 5 sekund po odblokowaniu drzwi.

**1 Digit DTMF:** ustawienie 1-cyfrowego kodu DTMF z zakresu 0-9, \* i #.

**2-4 Digits DTMF :** ustaw kod DTMF zgodnie z ustawieniem opcji DMTP. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli tryb DTMP jest ustawiony na 3 cyfry.

**Nazwa przełącznika:** nadaj nazwę przełącznikowi, aby odróżnić go od innych.

## Ustawienia przełącznika internetowego

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



Aby skonfigurować WebRelay, przejdź do strony internetowej **Access Control > Web Relay**. **Adres IP, nazwa użytkownika i hasło są** dostarczane przez producenta sieci.

**Web Relay**

---

Type	<input style="width: 100%;" type="text" value="Disabled"/>
IP Address	<input style="width: 100%;" type="text"/>
User Name	<input style="width: 100%;" type="text"/>
Password	<input style="width: 100%;" type="password"/>

---

**Web Relay Action Setting**

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
Action ID 01	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 02	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Action ID 03	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

- **Typ:** wybierz jedną z trzech opcji: **Wyłączone**, **Przełącznik sieciowy** i **Oba**. Wybierz **Web Relay**, aby włączyć przełącznik internetowy. Wybierz **Disabled**, aby wyłączyć przełącznik sieciowy. Wybierz **Both**, 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.
- **Web Relay Extension:** wprowadź numer SIP/IP określonego urządzenia, aby uruchomić WebRelay za pomocą kodu DTMF.

Skonfigurowany moduł WebRelay można wybrać w interfejsie Web **Directory > User > Add/Edit**.

Allow To Open	<input checked="" type="checkbox"/> RelayA <input type="checkbox"/> RelayB <input type="checkbox"/> RelayC
Web Relay	<input type="text" value="0"/>
Building	<input type="text"/>
Floor No.	<input type="text" value="NULL x"/>
Room	<input type="text"/>
<div>1 item Unselected Schedules</div> <div><input type="checkbox"/> 1002:Never</div>	<div>1 item Selected Schedules</div> <div><input type="checkbox"/> 1001:Always</div>

## Harmonogram przełączników

Harmonogram przełącznika umożliwia ustawienie konkretnego przełącznika 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.

Przejdź do interfejsu Web **Access Control > Relay > Relay Schedule**.



## Relay Schedule

Relay ID RelayA ▼

Enabled

2 items Unselected Schedules

- 1001:Always
- 1002:Never

>

<

0 item Selected Schedules

No Data

- **Identyfikator przekaźnika:** wybierz przekaźnik, który chcesz skonfigurować.
- **Harmonogram włączony:** domyślnie jest wyłączony. Wystarczy ją włączyć i wybrać harmonogram. Aby utworzyć harmonogram, zapoznaj się z sekcją [Konfiguracja harmonogramu dostępu do drzwi](#).

Wymagane jest skonfigurowanie i utworzenie harmonogramu dostępu do drzwi opartego na użytkownikach za pomocą karty RF, prywatnego kodu PIN i rozpoznawania twarzy.

## Konfiguracja harmonogramu dostępu do drzwi

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

## Tworzenie harmonogramu dostępu do drzwi

Harmonogramy dostępu do drzwi można tworzyć dla okresów dziennych, tygodniowych lub niestandardowych. Przejdź do interfejsu 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	--	--	00:00:00-00:00:00...	
<input type="checkbox"/>	2	1001	Local	Daily	Always	--	--	00:00:00-23:59:59...	

Delete Delete All Prev 1/1 Next 1 Go

**Aby utworzyć harmonogram dzienny:**

The screenshot shows the 'Add Schedule' dialog box with the following fields and options:

- Mode:** A dropdown menu set to 'Daily'.
- Name:** An empty text input field.
- Start Time - End Time:** Two time pickers, both set to '00:00'.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom right.

- **Start Time-End Time** : ustawienie harmonogramu ważności dostępu do drzwi w ciągu dnia.

**Aby utworzyć harmonogram tygodniowy:**

The screenshot shows the 'Add Schedule' dialog box with the following fields and options:

- Mode:** A dropdown menu set to 'Weekly'.
- Name:** An empty text input field.
- Day:** A grid of checkboxes for days of the week: Mon, Tue, Wed, Thur, Fri, Sat, Sun. All are checked. There is also an unchecked 'Check All' option.
- Start Time - End Time:** Two time pickers, both set to '00:00'.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom right.

**Aby utworzyć harmonogram na dłuższy okres:**

The screenshot shows the 'Add Schedule' dialog box with the following fields and options:

- Mode:** A dropdown menu set to 'Normal'.
- Name:** An empty text input field.
- Start Date - End Date:** Two date pickers, both set to 'Start Date'.
- Day:** A grid of checkboxes for days of the week: Mon, Tue, Wed, Thur, Fri, Sat, Sun. All are checked. There is also an unchecked 'Check All' option.
- Start Time - End Time:** Two time pickers, both set to '00:00'.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom right.

## Tworzenie harmonogramu dostępu do drzwi na urządzeniu

Na urządzeniu można również utworzyć harmonogram dostępu do drzwi. Przejdź do ekranu **Harmonogram > Dodaj harmonogram**.

1:14 AM

< Add Schedule

Mode Normal >

\* Name

Start Date 20220316 >

End Date 20220316 >

Day ... >

Start Time 12:00 AM >

End Time 12:00 AM >

Confirm

## Harmonogram importu i eksportu dostępu do drzwi

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

Przejdź do interfejsu **Ustawienia** sieciowe > **Harmonogram**. Kliknij przycisk Importuj lub Eksportuj.

### Schedule

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

1/1

### Uwaga

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

# Konfiguracja odblokowania drzwi

## Uwierzytelnianie dostępu

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

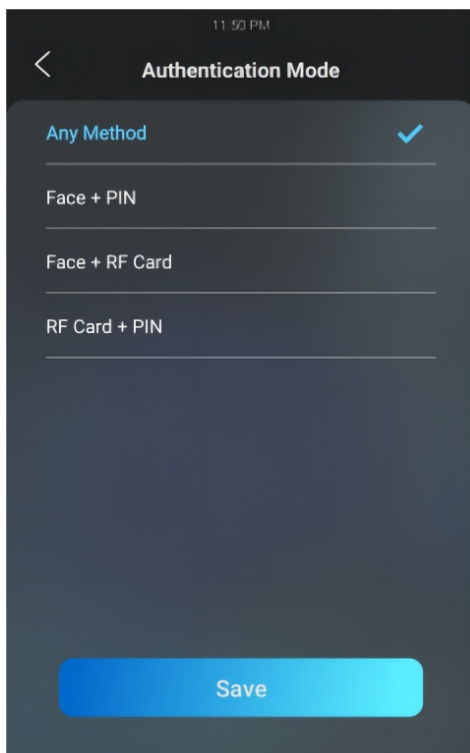
Przejdź do strony **Kontrola dostępu > Przekaznik > Tryb uwierzytelniania dostępu** w interfejsie **motywu budynku**.

### Access Authentication Mode Of The Building Theme

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

- **Tryb uwierzytelniania** : wybierz dowolną metodę, jeśli zezwalasz na wszystkie metody dostępu do odblokowania drzwi. Wybierz Face + PIN, jeśli chcesz zastosować podwójne metody dostępu (Face + PIN) do odblokowywania drzwi. Wybierz Face + RF Card, jeśli chcesz zastosować podwójne metody dostępu (Face + RF Card) do odblokowywania drzwi.
- **Inactivity (Sec)**: ustawienie limitu czasu uwierzytelniania dla drugiego uwierzytelnienia. Na przykład w Uwierzytelnianie **twarz + PIN**, jeśli ustawisz limit czasu uwierzytelniania na 10 sekund, użytkownicy będą musieli wprowadzić kod PIN dziesięć sekund po przejściu przez rozpoznawanie 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 użytkownicy nie przejdą drugiego uwierzytelnienia trzy razy, użytkownicy zostaną tymczasowo zablokowani przed pierwszym uwierzytelnieniem zgodnie z czasem blokady.
- **Number of Attempts (Liczba prób)**: liczba dozwolonych prób drugiego uwierzytelnienia.

Aby skonfigurować tryb uwierzytelniania na urządzeniu, przejdź do ekranu **Zabezpieczenia > 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.

Przejdź do interfejsu Web **Access Control > PIN Setting > Public PIN**.

### Public PIN

Enabled

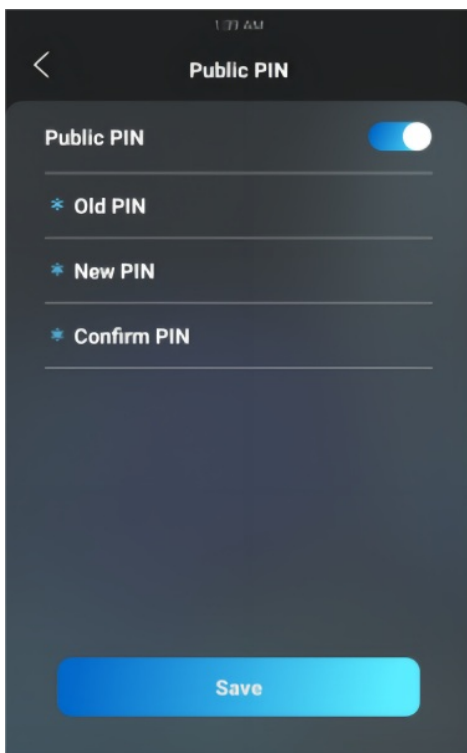


PIN Code

\*\*\*\*\*

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

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



## 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.

Przejdź do **Katalog** internetowy > Interfejs **użytkownika**. Kliknij +Add.

User

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

1/1

**Private PIN**

Code

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

## 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"/>
Building	<input type="text"/>
Floor No.	<input type="text" value="NULL x"/>
Room	<input type="text"/>

1 item	Unselected Schedules		1 item	Selected Schedules	
<input type="checkbox"/>	1002:Never		<input type="checkbox"/>	1001:Always	

- **Allow To Open Relay:** wybierz przekaźnik, który ma zostać wyzwolony.
- **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 prawego pola.

### Uwaga

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

## Konfiguracja prywatnego trybu dostępu PIN

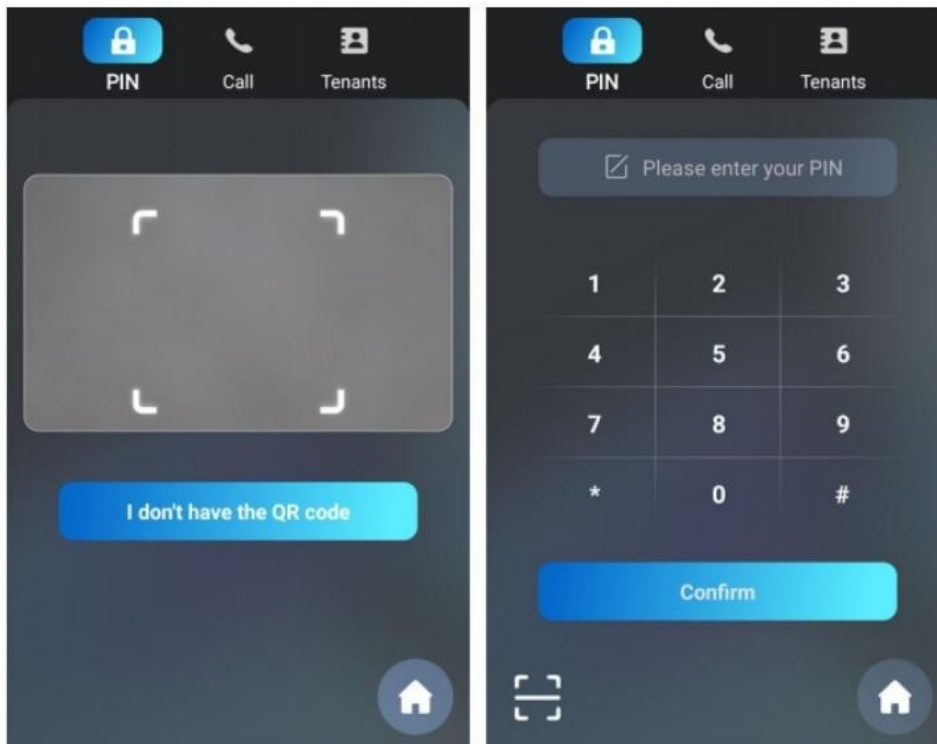
Urządzenie zapewnia dwie metody uwierzytelniania w celu uzyskania dostępu do prywatnego kodu PIN: PIN i APT# + PIN. Ta ostatnia wymaga od użytkowników wprowadzenia numeru mieszkania, a następnie prywatnego kodu PIN w celu odblokowania drzwi.

Przejdź do interfejsu Web **Access Control > PIN Setting > Private PIN.**

### Private PIN

Display Mode	<input type="text" value="Keyboard"/>
PIN Mode	<input type="text" value="PIN"/>

**Tryb wyświetlania:** wybór trybu dostępu między kodem QR a klawiaturą.



### Uwaga

Kod QR można zastosować tylko po dodaniu urządzenia do aplikacji Akuvox SmartPlus.

## Konfiguracja karty RF do odblokowywania drzwi

### Konfiguracja karty RF w interfejsie internetowym

Przejdź do interfejsu **Web Directory > User > +Add > RF Card**.

RF Card

1st Card Code

Obtain



Delete

2nd Card Code

Obtain



Delete

Add

### Uwaga

Karty RF o częstotliwości 13,56 MHz i 125 kHz mogą być stosowane do bramofonu w celu uzyskania dostępu do drzwi.

## Konfiguracja formatu kodu karty RF

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

Aby skonfigurować go w interfejsie internetowym **Access Control > Card Setting**.



**RFID**

IC Card Display Mode	<input type="text" value="8HN"/>
ID Card Order	<input type="text" value="Normal"/>
ID Card Display Mode	<input type="text" value="8HN"/>

- **Tryb wyświetlania karty IC/ID:** wybierz format karty IC/ID dla dostępu do drzwi spośród **8H10D**, **6H3D 5D(W26)**, **6H8D**, **8HN**, **8HR**, **6H3D 5D-R(W26)** i **8HR10D**. Domyślny format kodu karty to 8HN.

## Szyfrowanie kart Mifare

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

Przejdź do interfejsu Web **Access Control > Card setting > Mifare Card Encryption**.

**Mifare Card Encryption**

Enabled	<input type="checkbox"/>
Sector/Block	<input type="text" value="0"/> / <input type="text" value="0"/>
Block Key	<input type="text" value="*****"/>

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

## Konfiguracja rozpoznawania twarzy do odblokowywania drzwi

### Przesyłanie danych twarzy w interfejsie internetowym

Dane twarzy można przesłać do urządzenia za pośrednictwem interfejsu internetowego.

Przejdź do **Katalog internetowy > Użytkownik > +Dodaj > Interfejs twarzy**.

Face

---

Status Unregistered

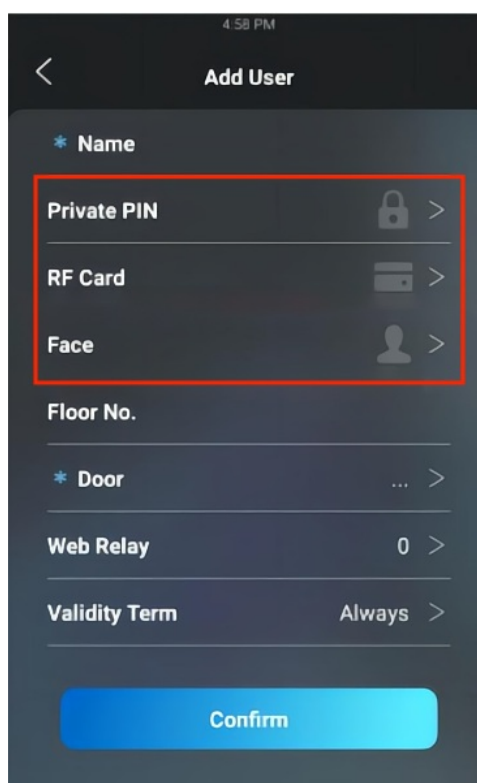
Photo

**Uwaga**

Maksymalny rozmiar pliku: 2M, Format: .jpg/.png/.bmp

## Dodawanie użytkowników na urządzeniu

Użytkowników można również dodawać na ekranie **użytkownika** urządzenia.



## Konfiguracja funkcji rozpoznawania twarzy w interfejsie internetowym

Bramofon umożliwi dostosowanie dokładności rozpoznawania twarzy, interwałów rozpoznawania i innych parametrów w celu poprawy komfortu użytkownika. Przejdź do interfejsu Web **Access Control > Face Setting**.

## Face Basic

Facial Recognition	Auto	▼
Offline Learning Enabled	<input checked="" type="checkbox"/>	
Recognize Option	Normal	▼
Antispoofing Option	Low	▼
Facial Recognition Interval(Sec)	5	▼
Face Occlusion Rejection	Enabled	▼
Visitor Friendly Mode	<input type="checkbox"/>	?

- **Offline Learning Enabled:** gdy funkcja ta jest włączona, poprawia zdolność rozpoznawania twarzy przez urządzenie, koncentrując się na głównych cechach twarzy i pomijając drobne zmiany, które na niej zachodzą. Dokładność rozpoznawania twarzy poprawia się wraz ze wzrostem liczby rozpoznań twarzy.

**Recognize Option:** wybierz poziom dokładności rozpoznawania twarzy spośród **Low, Normal, High i Highest**. Na przykład, jeśli wybierzesz Najwyższy, będzie najmniejsze prawdopodobieństwo, że ktoś inny zostanie pomyłony z Tobą przez pomyłkę lub w inny sposób podczas rozpoznawania twarzy.

**Antispoofing Option (Opcja antyspoofingu):** wybierz poziom antyspoofingu spośród **Low (Niski), Normal (Normalny), High (Wysoki) i Highest (Najwyższy)**. Na przykład, jeśli wybierzesz Najwyższy, będzie najmniejsza możliwość, że urządzenie zostanie oszukane przez obrazy cyfrowe lub zdjęcia dowolnego rodzaju.

**Facial Recognition Interval(Sec):** wybierz interwał czasowy między każdymi dwoma rozpoznaniem twarzy od 1 do 8 sekund. Na przykład, jeśli wybierzesz 5, użytkownicy będą musieli poczekać 5 sekund, zanim będą mogli ponownie wykonać rozpoznawanie twarzy.

- **Odrzucenie okluzji twarzy:** po włączeniu tej funkcji urządzenie wykryje, czy użytkownik nosi maskę.
- **Tryb przyjazny dla użytkownika:** po włączeniu nie będzie wyświetlany monit wizualny ani dźwiękowy, gdy rozpoznanie nie powiedzie się.

## Edycja danych dostępu do drzwi specyficznych dla użytkownika

Można wyszukiwać dostęp do drzwi dla poszczególnych użytkowników i edytować dane dostępu do drzwi w interfejsie **Web Directory > User**.

### User

											All	▼	User ID/Name	Search	+ Add
<input type="checkbox"/>	Index	Source	User ID	Name	Private PIN	RF Card	Face	Floor No.	Web Relay	Schedule-Relay	Edit	No Data			
											Prev	1/1	Next	1	Go

## 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.

Przejdź do interfejsu Web **Directory > User > Import/Export User**.

#### Import/Export User

User Data

Import

Export

### Uwaga

Importowany/eksportowany plik jest w formacie TGZ.

## 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.

Przejdź do interfejsu Web **Access Control > BLE**.

#### BLE Basic

Enabled	<input type="checkbox"/>
RSSI Threshold	<input type="text" value="72"/> (-85~-50db)
Open Door Interval(Sec)	<input type="text" value="5"/>

- **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 kolejnymi dwoma otwarciem drzwi Bluetooth.

## Konfiguracja Open Relay przez HTTP do odblokowywania drzwi

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

Przejdź do interfejsu Web **Access Control > Relay > Open Relay via HTTP**.

#### Open Relay via HTTP

Enabled	<input type="checkbox"/>
SessionCheck	<input type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>

- **Kontrola sesji**: ta funkcja służy do ograniczenia bezpieczeństwa sieci, jeśli ją włączysz, drzwi mogą nie zostać odblokowane w ten sposób.
- **Nazwa użytkownika** : wprowadź nazwę użytkownika interfejsu internetowego urządzenia, na przykład **admin**.
- **Hasło** : wprowadź hasło dla polecenia HTTP, na przykład **12345** .

Zapoznaj się z poniższym przykładem:

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

### Uwaga

**DoorNum** w powyższym poleceniu HTTP odnosi się do numeru przekaźnika #1, który ma zostać wyzwolony w celu uzyskania dostępu do drzwi. Urządzenie z włączonym trybem wysokiego bezpieczeństwa obsługuje tylko nowe formaty HTTP. Więcej informacji można znaleźć w sekcji [Bezpieczeństwo](#).

## 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.

Przejdź do interfejsu Web **Access Control > Relay > Open Relay via QR Code**.

### Open Relay Via QR Code

Enabled



### Uwaga

Funkcja powinna działać z Akuvox SmartPlus. Aby uzyskać więcej informacji, skontaktuj 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 przekaźnik dostępu do drzwi.

Przejdź do strony internetowej **Kontrola dostępu > Wejście > Interfejs wejścia**.

## Input A

Enabled	<input checked="" type="checkbox"/>
Trigger Electrical Level	Low ▼
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> Email <input type="checkbox"/> SIP Call <input type="checkbox"/> HTTP <input type="checkbox"/> TFTP
HTTP URL	<input type="text"/>
Action Delay	0 (0~300Sec)
Action Delay Mode	Unconditional Execution ▼
Execute Relay	RelayA ▼
Break-in Intrusion	<input type="checkbox"/>
Door Status	DoorA: High
Super Mode	Enabled ▼

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

**Stan drzwi**: wyświetlanie stanu sygnału wejściowego.

**Tryb super**: po włączeniu trybu super administrator będzie mógł otworzyć drzwi za pomocą karty RF nawet w przypadku awarii lub usterki bramofonu.

## Konfiguracja karty Odbiór dla funkcji odblokowywania drzwi

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

Przejdź do strony internetowej **Ustawienia > Klawisz/Wyświetlacz > Akcja szybkiego wybierania w interfejsie motywu budynku**.

**Speed Dial Action In Building Theme**

---

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

- **Otwórz przekaźnik:** wybierz przekaźnik (przekaźniki), który ma zostać wyzwolony, naciskając ikonę odbioru.
- **Akcja do wykonania:** zaznacz pole wyboru, aby włączyć opcję HTTP.
- **HTTP URL :** wprowadź polecenie URL, które ma zostać wysłane w celu uzyskania dostępu do drzwi. Na przykład `http://192.168.35.127/fcgi/do? action=OpenDoor&UserName=admin&Password=12345&DoorNum=1`

## 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.

Przejdź do interfejsu Web **Access Control > Relay**.

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

- Zapoznaj się z [Konfiguracją połączeń](#) transmisji danych DTMF, aby uzyskać informacje o konkretnych ustawieniach kodu DTMF.
- Urządzenia interkomowe muszą być spójne pod względem typu DTMF. W przeciwnym razie kod DTMF nie może zostać zastosowany.

## 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](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

Przejdź do interfejsu internetowego **Surveillance > RTSP > RTSP Basic**.

### RTSP Basic

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

- **RTSP Authorization Enabled** : włączenie autoryzacji RTSP. Po włączeniu autoryzacji RTSP wymagane jest wybranie trybu uwierzytelniania RTSP i wprowadzenie nazwy użytkownika RTSP oraz hasła RTSP na urządzeniu interkomowym, takim jak monitor wewnętrzny, w celu autoryzacji.
- **Tryb uwierzytelniania**: wybierz typ uwierzytelniania RTSP pomiędzy Basic i Digest. Basic jest domyślnym typem uwierzytelniania.

## Ustawienia strumienia RTSP

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

Przejdź do interfejsu Web **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

VGA

Video Framerate

25fps

Video Bitrate

1024kbps

2nd Video Resolution

VGA

2nd Video Framerate

25fps

2nd Video Bitrate

512kbps

- **Rozdzielczość wideo:** wybór rozdzielczości wideo spośród **QCIF, QVGA, CIF, VGA, 4CIF, 720P i 1080P**.  
Domyślną rozdzielczością wideo jest **VGA**, a wideo z bramofonu może nie być wyświetlane na monitorze wewnętrznym, jeśli rozdzielczość jest ustawiona na wyższą niż **VGA**.
- **Częstotliwość klatek wideo:** **25 klatek na sekundę** to domyślna częstotliwość klatek wideo.
- **Szybkość transmisji wideo:** wybierz szybkość transmisji wideo spośród **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 **1024 kb/s**.
- **2nd Video Resolution:** wybór rozdzielczości wideo dla drugiego kanału strumienia wideo. Domyślną rozdzielczością wideo jest **VGA**.
- **2nd Video Framerate :** wybierz liczbę klatek na sekundę dla drugiego kanału strumienia wideo. **25 klatek na sekundę** to domyślna liczba klatek na sekundę dla drugiego kanału strumienia wideo.
- **2nd Video Bitrate :** wybierz szybkość transmisji wideo dla drugiego kanału strumienia wideo. Drugi kanał strumienia wideo ma domyślnie **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 Web **Surveillance > MJPEG**.

### MJPEG Server

Enabled



Image Quality

VGA

- **Jakość obrazu:** wybór jakości przechwytywania obrazu spośród **QCIF, QVGA, CIF, VGA, 4CIF, 720P i 1080P**. Po włączeniu usługi MJPEG można przechwytywać obraz z telefonu przy użyciu następujących trzech typów formatu URL:

- [http:// urządzenie ip:8080/picture.cgi](http://urządzenie ip:8080/picture.cgi)

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

Na przykład, jeśli chcesz przechwycić obraz w formacie JPG z bramofonu o adresie IP: 192.168.1.104, można wpisać adres <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.

Przejdź do interfejsu internetowego **Surveillance > ONVIF**.

### Basic Setting

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

- **Discoverable** : po włączeniu tej funkcji wideo z kamery telefonu może być wyszukiwane przez inne urządzenia.
- **Nazwa użytkownika**: dostosuj nazwę użytkownika. Domyślna nazwa użytkownika to **admin**.
- **Hasło**: dostosuj hasło. Domyślne hasło to **admin**.

Po zakończeniu ustawień można wprowadzić adres URL ONVIF na urządzeniu innej firmy, aby wyświetlić strumień wideo. Na przykład: [http://doorphone Adres IP:80/onvif/device\\_service](http://doorphone Adres IP:80/onvif/device_service)

## Transmisja na żywo

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

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



## 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 w interfejsie sieciowym

W interfejsie internetowym można dostosować alarm sabotażowy i ustawienia czujnika.

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

#### Tamper Alarm

---

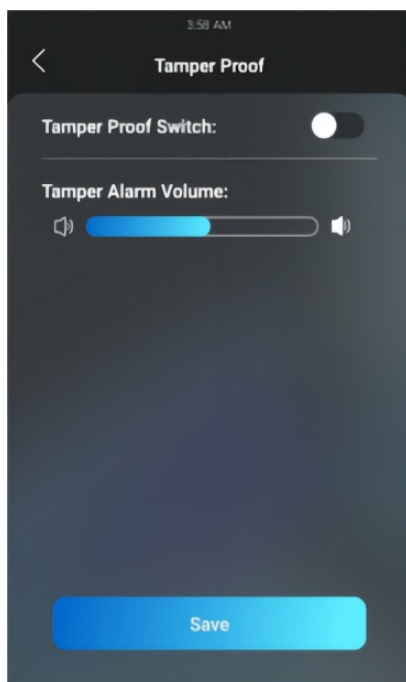
Enabled



### Konfiguracja alarmu sabotażowego na urządzeniu

Alarm sabotażowy i czujnik grawitacyjny można łatwo skonfigurować na bramofonie.

Przejdź do ekranu **Ustawienia urządzenia > Zabezpieczenia > Alarm sabotażowy**.



## Ustawienie rozbrojenia

Kod rozbrojenia można ustawić w interfejsie urządzenia **System > Security > Disarm Setting**.

### Disarm Setting

Enabled

PIN Code

(Enter \*# + PIN to disarm)

## Akcja ratunkowa

W sytuacji awaryjnej drzwi mogą pozostać otwarte.

Przejdź do interfejsu sieci Web **System > Security > Emergency Action**.

### Emergency Action

Apply Setting To

Input A

Input B

Input C

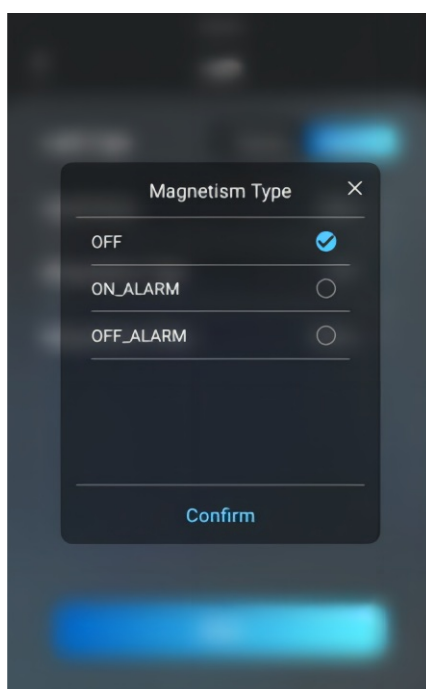
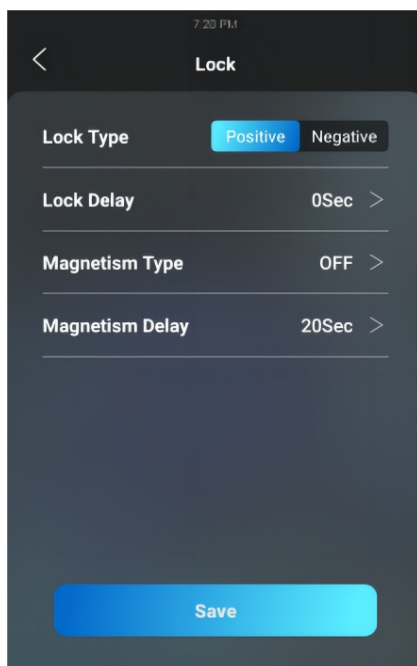
### Uwaga

Ta funkcja działa z usługą SmartPlus Cloud.

## 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**.



- **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 użytkownikom 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 wyzwania 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.
- **Typ magnetyzmu:** wybierz czas 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 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.

Przejdź do interfejsu internetowego **Surveillance > Motion > Motion Detection Options**.

### Motion Detection Options

Suspicious Moving Object Detection	<input type="text" value="Video Detection"/>	
Timing Interval	<input type="text" value="10"/>	(0~120 Sec)
Detection Accuracy	<input type="text" value="3"/>	(0~6)

- Wykrywanie podejrzanych ruchomych obiektów:** wybierz spośród opcji **Wykrywanie wideo**, **Wykrywanie podczerwieni** i **Wyłączone**. Wykrywanie podczerwieni opiera się na wykrywaniu promieniowania podczerwonego emitowanego lub odbijanego przez obiekty, podczas gdy wykrywanie wideo koncentruje się na analizie informacji wizualnych przechwyconych przez kamery.
- Time Interval (Interwał czasowy):** 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.
- Dokładność detekcji:** ustawienie dokładności detekcji dla czułości detekcji. Im wyższa wartość, tym większa czułość. Domyślna wartość dokładności wykrywania to **2**.

Po skonfigurowaniu interwału można skonfigurować wymaganą akcję.

### Motion Action



Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> TFTP <input type="checkbox"/> SIP Call
Action HTTP Url	<input type="text"/>
Action Relay	<input type="text" value="None"/>

- Akcja do wykonania:** wybierz metodę wykonania akcji: FTP, Email, HTTP, TFTP i 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.

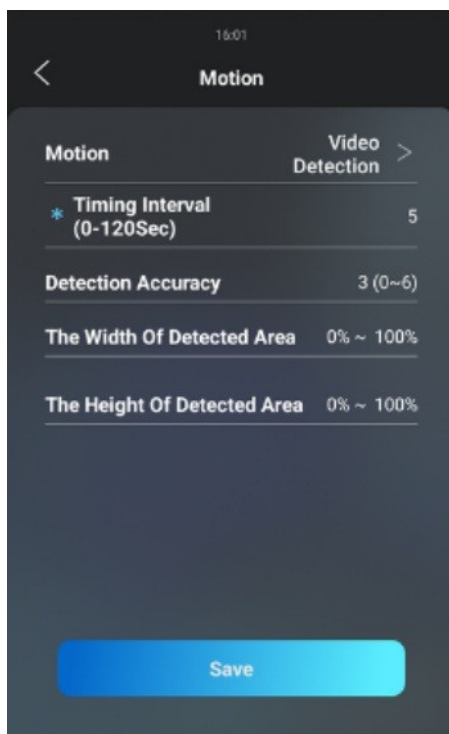
#### Motion Detect Time Setting

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 		

## Konfiguracja wykrywania ruchu na urządzeniu

Można włączyć wykrywanie ruchu i skonfigurować interwał wykrywania ruchu na urządzeniu **Ustawienia zaawansowane > Nadzór**

> Ekran **ruchu**.



## Ustawienia powiadomień bezpieczeństwa

### Ustawienia powiadomień e-mail

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

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



## Email Notification

---

Sender's Email Address	<input type="text"/>
Email Send Name	<input type="text"/>
Receiver's Email Address	<input type="text"/>
Receiver's Email Name	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password" value="*****"/>
Email Subject	<input type="text"/>
Email Content	<input type="text"/>

- **SMTP Server Address** : wprowadź adres serwera SMTP nadawcy.
- **Port** : wprowadź numer portu, z którego wysyłana jest wiadomość e-mail.
- **Nazwa użytkownika SMTP**: wprowadź nazwę użytkownika SMTP, która zazwyczaj jest taka sama jak adres e-mail nadawcy.
- **SMTP Password** : skonfiguruj hasło usługi SMTP, które jest takie samo jak adres e-mail nadawcy.

## Ustawienia powiadomień FTP

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

Przejdź do interfejsu web **Setting > Action > FTP Notification**.

### FTP Notification

---

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

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

## Ustawienia powiadomień TFTP

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

Przejdź do interfejsu web **Setting > Action > TFTP Notification**.

TFTP Notification

---

TFTP Server

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

## Adres URL akcji

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

**Akuvox Action URL:**

Nie	Wydarzenie	Format parametrów	Przykład
1	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? 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) Przejdź do interfejsu internetowego **Setting > Actions URL**.

**Uwaga:**

Adresy URL akcji i formaty są dostarczane przez producentów zewnętrznych. Bramofon Akuvox wysyła adres URL tylko do urządzeń innych producentów.

Setting» [Action URL](#)

### 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"/>

## Szyfrowanie głosu

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

Przejdź do interfejsu **Konto internetowe > Zaawansowane > Szyfrowanie**.

### Encryption

Voice Encryption(SRTP)

**Voice Encryption(SRTP):** wybór trybu szyfrowania. Jeśli wybierzesz opcję wyłączenia, połączenie nie będzie szyfrowane.

- **Obowiązkowe:** wszystkie sygnały audio (technicznie rzecz biorąc, są to strumienie RTP) będą szyfrowane w celu poprawy bezpieczeństwa.
- **Opcjonalnie:** szyfrowanie głosu od strony wywoływanej, jeśli strona wywoływana również włącza SRTP, sygnały głosowe będą również szyfrowane.

## Interfejs sieciowy Automatyczne wylogowanie

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

Przejdź do interfejsu internetowego **System > Security > Session Time Out**.

### Session Time Out

Session Time Out Value

300

(60~14400Sec)

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

## 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 w interfejsie **System WWW > 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

 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 w interfejsie **System WWW > Certyfikat > Certyfikat serwera WWW**.

### Client Certificate

<input type="checkbox"/>	Index	Issue To	Issuer	Expire Time
No Data				

 Delete

 Delete All

Index

Auto

Client Certificate Upload

 Upload

Only Accept Trusted Certificates

- **Index:** wybierz żadaną wartość z rozwijanej listy Index. 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).

- **Akceptuj tylko zaufane certyfikaty:** po włączeniu tej opcji telefon będzie weryfikował certyfikat serwera na podstawie listy certyfikatów klienta, o ile uwierzytelnianie przebiegnie pomyślnie. Po wyłączeniu tej opcji telefon nie będzie weryfikował certyfikatu serwera bez względu na to, czy certyfikat jest ważny, czy nie.

## Prześlij certyfikat TLS do rejestracji konta SIP

Przed złożeniem wniosku o konto SIP z serwera SIP lub DNS przy użyciu protokołu TLS należy przesłać certyfikat TLS. Certyfikat ten jest niezbędny do uwierzytelnienia serwera.

Aby przesłać certyfikat TLS, przejdź do **System > Certyfikat > Interfejs certyfikatu DNS**.

### DNS Certificate

DNS Certificate Upload

 Upload

DNS Certificate Reset

 Reset

## 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.

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

### High Security Mode

Enabled



### Ważne uwagi

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

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

-PC Manager: 1.2.0.0

-IP Scanner: 2.2.0.0

-Upgrade Tool: 4.1.0.0

-SDMC: 6.0.0.34

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

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

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

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

## Dzienniki

### Dzienniki połączeń

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

Aby sprawdzić rejestr połączeń w interfejsie internetowym **Status > Call Log**. Dzienniki połączeń można eksportować w formacie CSV.

#### Call Log

Save Call Log Enabled

Call History   ~

<input type="checkbox"/>	Index	Type	Date	Time	Local Identity	Name	Number
No Data							

1/1

- **Call History (Historia połączeń):** wybór historii połączeń spośród opcji **All (Wszystkie)**, **Dialed (Wybrane)**, **Received (Odebrane)** i **Missed (Nieodebrane)** w celu wyświetlenia określonego typu rejestru połączeń.
- **Czas rozpoczęcia ~ Czas zakończenia :** wybierz konkretny czas dzienników połączeń, które chcesz wyszukać, sprawdzić lub wyeksportować.
- **Nazwa/Numer:** wyszukiwanie w rejestrze połączeń według nazwy, adresu IP lub numeru SIP.

## 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 Web **Status > Access Log**. Dzienniki przejść można eksportować w formacie XML lub CSV.

#### Access Log

Save Door Log Enabled

~

<input type="checkbox"/>	Index	Name	Code	Type	Date	Time	Status
No Data							

1/1

- **Status** : wybierz pomiędzy **Success (Sukces)** i **Failed (Niepowodzenie)**, aby wyszukać udane lub nieudane dostępy do drzwi.
- **Nazwa/Kod** : wyszukiwanie dziennika drzwi według nazwy lub kodu PIN.

## Debugowanie

### Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Przejdź do interfejsu internetowego **System > Maintenance > System Log**.

#### System Log

Log Level	<input type="text" value="3"/>
Export Log	<input type="button" value="Export"/>
Export Debug Log	<input type="button" value="Export"/>
Remote System Log Enabled	<input type="checkbox"/>
Remote System Server	<input type="text"/>

- **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.
- **Eksportuj dziennik**: kliknij kartę **Eksportuj**, aby wyeksportować tymczasowy plik dziennika debugowania do lokalnego komputera.
- **Eksportuj dziennik debugowania**: kliknij kartę **Eksportuj**, aby wyeksportować plik dziennika debugowania do lokalnego komputera.
- **Zdalny serwer systemu**: wprowadź adres zdalnego serwera, aby otrzymywać dziennik urządzenia. Adres serwera zdalnego zostanie dostarczony przez pomoc techniczną Akuvox.

## PCAP do debugowania

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

Przejdź do interfejsu internetowego **System > Konserwacja > PCAP**.

#### PCAP

Specific Port	<input type="text" value=""/>	(1~65535)	
PCAP	<input type="button" value="Start"/>	<input type="button" value="Stop"/>	<input type="button" value="Export"/>
PCAP Auto Refresh Enabled	<input type="checkbox"/>		

- **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 opcji, PCAP będzie kontynuował przechwytywanie pakietów danych nawet po



- osiągnięciu przez nie maksymalnej pojemności 1M. Gdy opcja ta jest wyłączona, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycony pakiet danych osiągnie maksymalną pojemność przechwytywania wynoszącą 1 MB.

## Zdalny serwer debugowania

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

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

### Remote Debug Server

Server	<input type="text" value="Disabled"/>
Connect Status	<input type="text"/>
IP	<input type="text"/>

- **Connect Status** : wyświetla status połączenia ze zdalnym serwerem debugowania.
- **IP** : wprowadź adres IP zdalnego serwera debugowania. O adres IP serwera należy poprosić zespół techniczny Akuvox.

### Uwaga

Wymagane jest przesłanie adresu MAC bramofonu do zespołu technicznego Akuvox.

## Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można zaktualizować w interfejsie

internetowym urządzenia. Przejdź do interfejsu internetowego

System > **Upgrade > Basic**.

## Upgrade

Firmware Version	915.30.10.14
Hardware Version	915.1.0.0
Reset	<input type="checkbox"/>
Upgrade	<a href="#">Upgrade</a>
Reset To Factory Setting	<a href="#">Reset</a>
Reset Configuration to Default State(E...	<a href="#">Reset</a>
Reboot	<a href="#">Reboot</a>

### Upgrade

(Format: .zip)

Not selected any files [Select File](#) [Reset](#)

[Cancel](#) [Install](#)

### Uwaga

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

## Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować do komputera lokalnego. Przejdź do interfejsu internetowego **System** >

**Konserwacja** > **Inne**.

### Others

Config File [Import](#) [Export](#) (Encrypted)

## Ping

Urządzenie umożliwia sprawdzenie dostępności serwera docelowego. Przejdź do interfejsu internetowego **System** >

### Ping

Cloud Server

Verify the network address accessibility  [Ping](#) [Stop](#)

You can enter the domain name or IP you want to detect in the drop-down box.

## Konserwacja > Ping.

- **Client Server:** serwer, który ma zostać zweryfikowany.
- **Wykorzystanie przedsiębiorstwa pracy:** typ usługi.

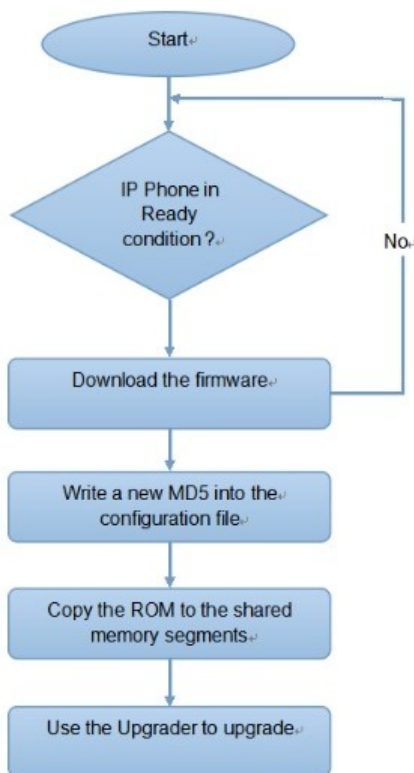
## Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

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.
- **Dostarczanie konfiguracji opartej na MAC:** Pliki konfiguracyjne oparte na MAC są używane do automatycznego dostarczania na określonym urządzeniu.

urządzenie, zgodnie z jego unikalnym numerem MAC. Pliki konfiguracyjne o nazwie z numerem 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 udostępnienia urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer posiada te dwa typy plików konfiguracyjnych, urządzenia będą najpierw uzyskiwać dostęp do ogólnych plików konfiguracyjnych przed uzyskaniem dostępu do plików konfiguracyjnych opartych na MAC.

Możesz kliknąć [tutaj](#), aby zobaczyć szczegółowy format i kroki.

## Harmonogram AutoP

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

Przejdź do interfejsu internetowego **System > Auto Provisioning > Automatic 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"/>

#### • Tryb :

- Po **włączeniu zasilania** urządzenie wykonuje funkcję Autop przy każdym uruchomieniu.
- **Wielokrotnie** umożliwia urządzeniu wykonanie automatycznego zatrzymania zgodnie z ustawionym harmonogramem.
- **Power On + Repeatedly** łączy w sobie tryb **Power On** i tryb **Repeatedly**, który umożliwia urządzeniu wykonywanie automatycznego zatrzymania przy każdym uruchomieniu lub zgodnie z harmonogramem.
- **Hourly Repeat (Powtarzanie co godzinę)** umożliwia urządzeniu wykonywanie automatycznego zatrzymania co godzinę.
- **Harmonogram**: po wybraniu opcji **Re p e a t e d l y** można skonfigurować harmonogram Autop.

## 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.

Przejdź do interfejsu internetowego **System > Auto Provisioning > PNP Option**.

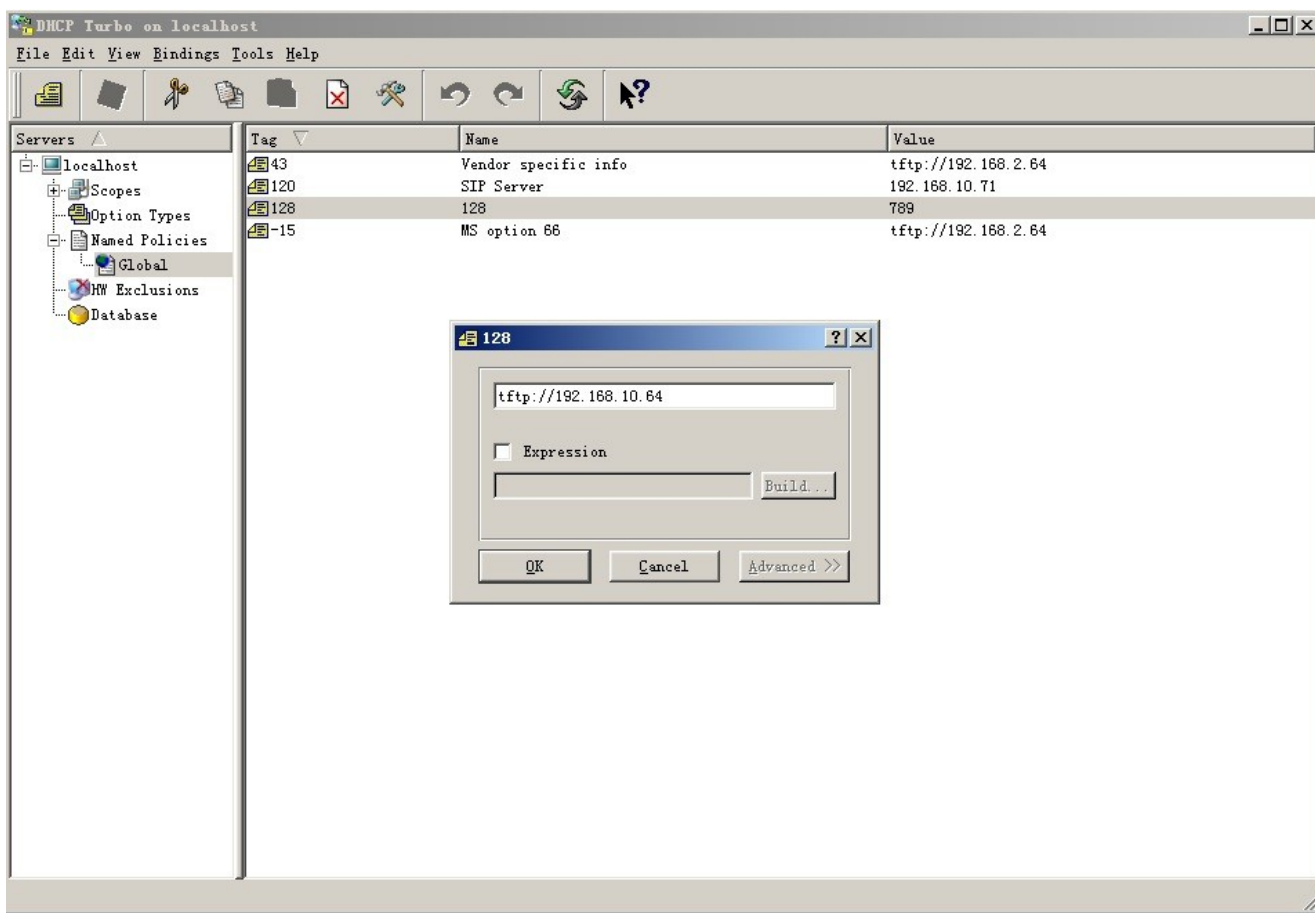
## PNP Option

PNP Config Enabled



## Konfiguracja udostępniania DHCP

Adres URL automatycznego dostarczania można również uzyskać za pomocą opcji DHCP, która umożliwia urządzeniu wysyłanie żądania do serwera DHCP dla określonego kodu opcji DHCP. Jeśli chcesz korzystać z **opcji niestandardowej** zdefiniowanej przez użytkowników z kodami opcji od 128 do 255, musisz skonfigurować opcję niestandardową DHCP w interfejsie internetowym.



### Uwa

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

Aby skonfigurować DHCP Autop z trybem Power On i wyeksportować Autop Template w celu edycji konfiguracji. Przejdź do interfejsu internetowego **System > Auto Provisioning > Automatic 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"/>

Następnie skonfiguruj opcję DHCP w interfejsie **System > Auto Provisioning > DHCP Option**.

## DHCP Option

Custom Option	<input type="text"/>	(128-254)
---------------	----------------------	-----------

(DHCP option 66/43 is enabled by default)

- **Opcja niestandardowa:** wprowadź kod DHCP odpowiadający odpowiedniemu adresowi 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, aby uzyskać adres URL serwera aktualizacji. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 66 z 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 dla udostępniania wsadowego ma format **r000000000xx.cfg**, przyjmując X915 jako przykład r0000000915.cfg, podczas gdy plik konfiguracyjny oparty na MAC dla udostępniania konkretnego urządzenia ma format Adres MAC urządzenia. cfg, na przykład **0C 110504AE5B.cfg**.

## Konfiguracja udostępniania statycznego

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

Aby pobrać szablon Autop w interfejsie **System > Auto Provisioning > Automatic Autop** i ustawić serwer Autop 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"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>
Common AES Key	<input type="password" value="....."/>
AES Key(MAC)	<input type="password" value="....."/>
	<input type="button" value="Autop Immediately"/>

- **URL** : skonfiguruj adresy serwerów TFTP, HTTP, HTTPS lub FTP dla provisioningu.
- **Nazwa użytkownika** : ustaw nazwę użytkownika, jeśli serwer wymaga nazwy użytkownika, aby uzyskać do niego dostęp.
- **Hasło** : ustaw hasło, jeśli serwer wymaga hasła dostępu.
- **Common AES Key**: ustawienie kodu AES dla interkomu w celu odszyfrowania ogólnego pliku konfiguracyjnego Auto Provisioning.
- **Klucz AES (MAC)**: ustawienie kodu AES dla interkomu w celu odszyfrowania pliku konfiguracyjnego automatycznego udostępniania opartego na MAC.

### Uwaga

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

### Wskazówka

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

## 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 Web **Device > Lift Control**.

#### Lift Control List

Lift Control List	<input type="text" value="None"/>	▼
Server IP	<input type="text"/>	
Port	<input type="text"/>	

#### Akuvox EC32 Action

User Name	<input type="text" value="admin"/>	
Password	<input type="password" value="*****"/>	
Floor NO. Parameter	<input type="text" value="\$floor"/>	
URL To Trigger Specific Floor	<input type="text" value="/cdor.cgi?open=0&amp;door=\$floor"/>	
URL To Trigeer All Floors	<input type="text" value="/cdor.cgi?open=8"/>	
URL To Close All Floors	<input type="text" value="/cdor.cgi?open=9"/>	

- **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.
- **Nazwa użytkownika:** wprowadź nazwę użytkownika kontrolera windy w celu uwierzytelnienia.
- **Hasło :** wprowadź hasło kontrolera windy w celu uwierzytelnienia.
- **Floor NO. Parametr:** wprowadź parametr numeru piętra dostarczony przez Akuvox. Domyślny ciąg parametru to \$floor. W razie potrzeby można zdefiniować własny ciąg parametrów.
- **URL To Trigger Specific Floor:** wprowadź adres URL sterowania Akuvox life, aby wyzwolić określone piętro. Adres URL to /cdor.cgi? open=0&door=\$floor, ale ciąg \$floor na końcu musi być identyczny z ciągiem parametrów zdefiniowanym przez użytkownika.



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

## Integracja z urządzeniami innych firm

### Integracja przez Wiegand

Funkcja Wiegand umożliwia bramafonowi Akuvox działanie jako kontroler lub czytnik kart.

Przejdź do interfejsu Web **Device > Wiegand**.

Device» [Wiegand](#)

#### Wiegand

Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Wiegand-26
IC Card Reading Order	Normal
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
RF Card Verification	Enabled
Wiegand Output CRC	<input checked="" type="checkbox"/>
Wiegand Open Relay	<input type="checkbox"/> RelayA <input type="checkbox"/> RelayB <input type="checkbox"/> RelayC

- **Tryb wyświetlania Wiegand**: wybór formatu kodu karty Wiegand spośród 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.
- **Tryb czytnika kart Wiegand**: ustawienie formatu transmisji danych Wiegand spośród trzech opcji: **Wiegand 26**, **Wiegand 34** i **Wiegand 58** . Format transmisji powinien być identyczny między bramafonem a urządzeniem, które ma zostać zintegrowane.
- **Kolejność odczytu kart IC**: ta opcja działa tylko po wybraniu Wiegand-26.
  - Normalny: urządzenie odczyta trzy ostatnie bajty karty IC. Na przykład, jeśli numer karty IC to 840C9F50, odczytane zostanie 0C9F50.
  - Odwrotnie: urządzenie odczyta pierwsze trzy bajty karty IC. Na przykład, jeśli numer karty IC to 840C9F50, odczytany zostanie numer 840C9F.
- **Tryb transferu Wiegand** :

- Wejście: bramofon jest używany jako odbiornik.
- Wyjście: bramofon jest używany jako nadajnik.
- Convert to Card No.Output Wiegand: wyjście Wiegand zostanie przekonwertowane na numer karty przed wysłaniem go z bramofonu do odbiornika.
- **Kolejność danych wejściowych** Wiegand: ustawienie kolejności danych wejściowych Wiegand pomiędzy **Normal** i **Reversed**. W przypadku wybrania opcji **Reversed** numer karty wejściowej zostanie odwrócony i odwrotnie.
- 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.
- Wiegand **Output Data Order (Kolejność danych wyjściowych)** Wiegand): ustawia kolejność danych wyjściowych Wiegand pomiędzy **Normal (Normalna)** i **Reversed (Odwrócona)**. 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.
- **Wiegand Open Relay**: przekaźnik, który ma zostać wyzwolony.

## 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.

Setting» [HTTP API](#)

### HTTP API

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

- **Enabled** : włączenie lub wyłączenie funkcji API HPTT dla integracji innej firmy. Na przykład, jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.

- **Tryb autoryzacji:** wybierz spośród **None, Normal, Allowlist, Basic, Digest i Token** dla typu autoryzacji, które zostały szczegółowo wyjaśnione w poniższej tabeli.
- **Nazwa użytkownika:** wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic i Digest**. Domyślna nazwa użytkownika to admin.
- **Hasło :** wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic i Digest**. Domyślna nazwa użytkownika to admin.

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

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 wyłącznie przez programistów Akuvox.
3	Lista dozwolonych	Po wybraniu tego trybu wymagane jest jedynie podanie adresu IP urządzenia innej firmy w celu uwierzytelnienia. Lista zezwoleń jest odpowiednia do pracy w sieci LAN.
4	Podstawowy	Po wybraniu tego trybu wymagane jest podanie nazwy użytkownika i hasła w celu uwierzytelnienia. W polu Authorization nagłówka żądania HTTP należy użyć metody kodowania Base64 do zakodowania nazwy użytkownika i hasła.
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 programistów Akuvox.

## Kontrola mocy wyjściowej

Urządzenie może służyć jako źródło zasilania dla zewnętrznych przełączników.

Przejdź do interfejsu Web **Access Control > Relay >12V Power Output**.

**12V Power Output**

---

Relay ID	RelayA
12V Power Output	<input type="text" value="Disabled"/> ▼

### • Wyjście zasilania 12V:

- **Wyłączone:** wyłączenie funkcji wyjścia zasilania;
- **Zawsze :** umożliwia kontrolerowi dostępu ciągle zasilanie urządzenia innej firmy.
- **Triggered By Open Relay:** dostarcza zasilanie do urządzenia zewnętrznego za pośrednictwem wyjścia 12 i interfejsu GND podczas limitu czasu, gdy stan przełączników zmienia się z niskiego na wysoki.

o **Przełącznik bezpieczeństwa A** : umożliwia współpracę bramofonu z przełącznikiem bezpieczeństwa.

- **Time Out (Sec)**: wybór czasu zasilania po wyzwoleniu przełącznika spośród 3, 5 i 10. Domyślnie są to 3 sekundy. Napięcie wyjściowe wynosi 12 V, a maksymalne natężenie prądu wyjściowego 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.

Przejdź do interfejsu Web **Access Control > Relay > Mobile Community**.

### Mobile Community

Enabled

HTTP URL

Device ID

## Integracja z Milestone

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

Przejdź do interfejsu internetowego **Surveillance > ONVIF > Advanced Setting**.

### Advanced Setting

Milestone

## Modyfikacja hasła

### Modyfikacja hasła interfejsu sieciowego urządzenia

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

Aby zmienić domyślne hasło sieciowe w interfejsie **System > Zabezpieczenia > Modyfikuj hasło sieciowe**. Można również włączyć konto użytkownika w interfejsie.

System» Security

---

**Web Password Modify**

Account	<input type="text" value="admin"/>	<input type="button" value="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 one uppercase letter, one lowercase letter and one digit at least.

User Name	<input type="text" value="admin"/>
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

### 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 skonfigurować systemowy kod PIN w interfejsie internetowym, przejdź do opcji

**System > Security > System PIN.**

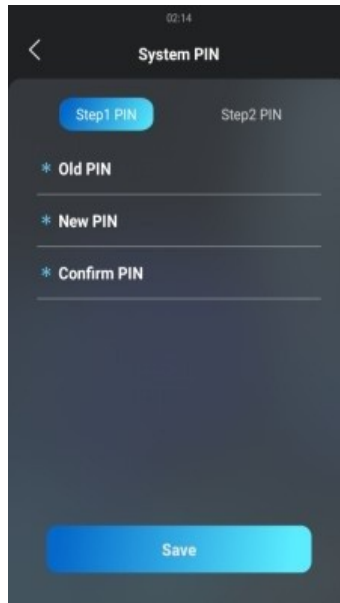
#### System PIN

Step1 PIN

Step2 PIN

- **Krok 1 PIN:** wprowadź czterocyfrowe nowe hasło projektu, aby zastąpić stare. Początkowe hasło projektu to **9999**.
- **Krok 2 PIN:** wprowadź czterocyfrowe hasło ustawień, aby zastąpić stare hasło. Początkowe hasło ustawień to **3888**.

Aby ustawić systemowy kod PIN na urządzeniu, przejdź do **Security > System PIN**, a następnie wybierz **Step1 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 skonfigurować hasło ustawień w interfejsie internetowym, przejdź do **System > Security > System PIN** interface.

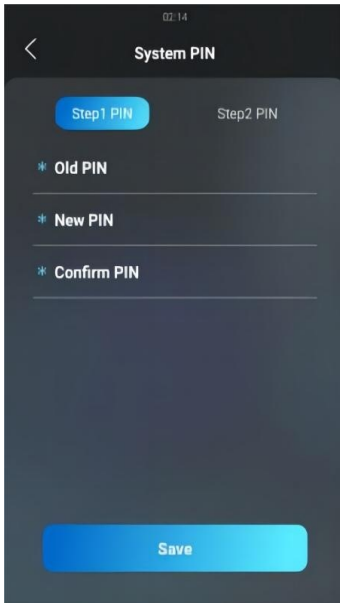
### System PIN

Step1 PIN

Step2 PIN

- **Krok 1 PIN:** wprowadź czterocyfrowe nowe hasło projektu, aby zastąpić stare. Początkowe hasło projektu to **9999**.
- **Krok 2 PIN:** wprowadź czterocyfrowe hasło ustawień, aby zastąpić stare hasło. Początkowe hasło ustawień to **3888**.

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



## Ponowne uruchamianie i resetowanie systemu

### Reboot

### Reboot w sieci

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

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

#### Upgrade

Firmware Version	915.30.10.14
Hardware Version	915.1.0.0
Reset	<input type="checkbox"/>
Upgrade	Upgrade
Reset To Factory Setting	Reset
Reset Configuration to Default State(E...	Reset
Reboot	Reboot

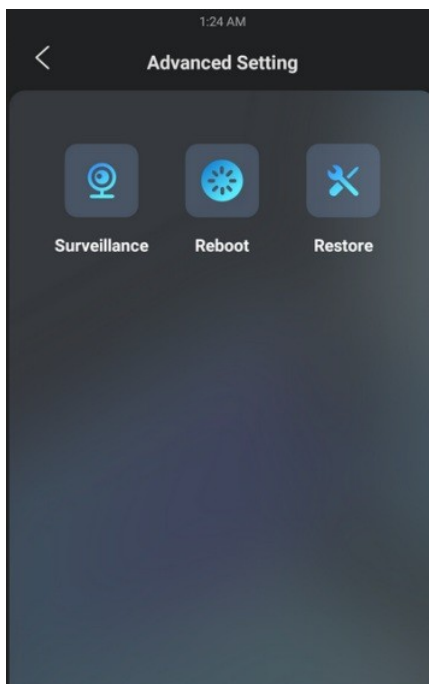
#### Reboot Schedule

Enabled

Schedule

(0~23Hour)

Aby ponownie uruchomić urządzenie, przejdź do ekranu **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** .

### Upgrade

Firmware Version	915.30.10.14
Hardware Version	915.1.0.0
Reset	<input type="checkbox"/>
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** .



