

## Informacje o niniejszej instrukcji

**Akuvox**  
Open A Smart World

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



# AKUVOX R20B DOOR PHONE Administrator Guide

Dziękujemy za wybranie bramofonu Akuvox z serii R20B. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy wersji 320.30.10.9 i zawiera wszystkie konfiguracje funkcji i cech bramofonu Akuvox. Odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie układowe.

## Przegląd produktów

Seria Akuvox R20B może być połączona z monitorami wewnętrznymi w celu zdalnej kontroli dostępu i komunikacji. Umożliwiają one rozmowy audio i wideo z odwiedzającymi, a także odblokowanie drzwi w razie potrzeby.

# Dziennik zmian

[Dodaj moduł rozszerzenia.](#)

## Specyfikacja modelu

R20B	
Wyjście przekaźnika	2
Wejścia	2
Głośnik	1
Mikrofon	1
PoE	✓
RS485	✓
Czytnik kart	✓

## Wprowadzenie do menu konfiguracji

- **Status** : ta sekcja zawiera podstawowe informacje, takie jak informacje o produkcie, informacje o sieci, informacje o koncie itp.
- **Interkom**: ta sekcja obejmuje ustawienia interkomu, rejestr połączeń itp.
- **Konto**: ta sekcja dotyczy konta SIP, serwera SIP, serwera proxy, typu protokołu transportowego, kodeka audio i wideo, DTMF, licznika sesji itp.
- **Sieć** : ta sekcja dotyczy głównie ustawień DHCP i statycznego adresu IP, ustawień portu RTP, wdrażania urządzeń itp.
- **Telefon** : ta sekcja zawiera ustawienia podświetlenia, wyświetlania kart i przycisków, ustawienia wyświetlacza LCD i ustawienia głosowe.
- **Kontakty** : ta sekcja zawiera ustawienia grup i kontaktów.
- **Aktualizacja**: ta sekcja obejmuje aktualizację oprogramowania układowego, resetowanie i ponowne uruchamianie urządzenia, automatyczne dostarczanie plików konfiguracyjnych i diagnostykę błędów.
- **Bezpieczeństwo**: ta sekcja służy do modyfikacji hasła.

▼ **Status**

**Basic**

▶ **Intercom**

▶ **Account**

▶ **Network**

▶ **Phone**

▶ **Contacts**

▶ **Upgrade**

▶ **Security**

## Dostęp do urządzenia

### Uzyskiwanie adresu IP urządzenia

Sprawdź adres IP urządzenia, przytrzymując przycisk przez 5 sekund. Można też wyszukać adres IP urządzenia za pomocą skanera IP w tej samej sieci LAN. Wystarczy kliknąć zakładkę **Scan** w skanerze IP, aby sprawdzić adres IP urządzenia.

Online Device : 7

Search Refresh

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C11050785A9	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A8102020128A		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C11050A5951	R29	1.1.1.1.1	29.30.2.16

### 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** i należy zwracać uwagę na wielkość liter we wprowadzonej nazwie użytkownika i hasle.

User Name: admin

Password: .....

Remember Username/Password

Login



## Uwa

- 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.

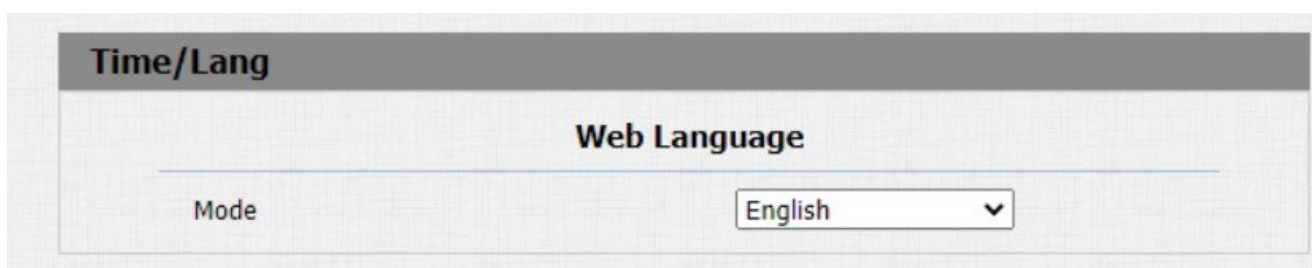
# Ustawienia języka i czasu

## Ustawienia języka

Urządzenie obsługuje następujące języki internetowe:

- Angielski, rosyjski, hiszpański, holenderski, francuski, niemiecki, polski, japoński i hebrajski.

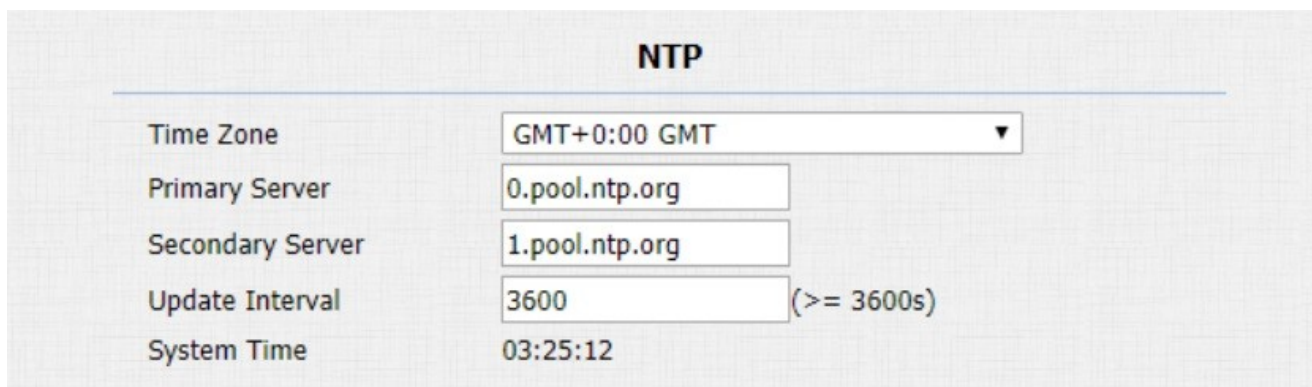
Przejdź do interfejsu **Web Phone > Time/Lang > Web Language**.



## Ustawienie czasu

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

Przejdź do interfejsu **Web Phone > Time/Lang > NTP**.



**Konfiguracja parametrów:**

- **Preferred/Alternate Server:** adres serwera NTP. Serwer alternatywny zacznie działać, gdy serwer podstawowy będzie nieprawidłowy.

**Update Interval:** odstęp czasu między dwoma kolejnymi żądaniami NTP.

Można również skonfigurować czas ręcznie, zaznaczając pole wyboru **Ręcznie** i

wprowadzając dane czasu.

### Type

---

Manual

Date                       Year    Mon    Day

Time                       Hour    Min    Sec

Auto

# Ustawienie LED

## Światło wypełniające LED

Oświetlenie wypełniające LED jest przeznaczone głównie do wzmocnienia światła w nocy lub w ciemnym otoczeniu.

Przejdź do interfejsu web **Intercom > LED Setting > LED Fill Light**.

LED Fill Light	
Mode	Auto <input type="button" value="v"/>
Min Photoresistor	1500 (0~1800)
Max Photoresistor	1600 (0~1800)

### Konfiguracja parametrów :

- **Tryb : Auto** umożliwia automatyczne włączanie światła LED. **Harmonogram** włącza diodę LED zgodnie z harmonogramem.
- **Min/Max Photoresistor**: ustawia minimalną i maksymalną wartość fotorezystora w oparciu o aktualnie wykrytą wartość fotorezystora w celu sterowania włączaniem i wyłączeniem diody LED. Można ustawić maksymalną wartość fotorezystora, aby włączyć diodę IR LED i minimalną wartość, aby ją wyłączyć. Minimalna i maksymalna wartość fotorezystora wynosi odpowiednio od 0 do 1800.

## Status wyświetlacza LED

Regulacja wyświetlacza LED służy do wskazywania zmian podświetlenia przycisku połączenia w 5 stanach: normalnym (bezczynności), offline, połączenia, rozmowy i odbierania połączenia. Stan diody LED pozwala użytkownikom zweryfikować aktualny tryb urządzenia.

Aby skonfigurować go w interfejsie internetowym **Intercom > LED Setting > LED Status**.

LED Status		
Device Status	LED Color	LED Display Mode
NORMAL ▾	Blue ▾	Always On ▾
OFFLINE ▾	Red ▾	2500/2500 Blink ▾
CALLING ▾	Blue ▾	2500/2500 Blink ▾
TALKING ▾	Green ▾	Always On ▾
RECEIVING ▾	Green ▾	2500/2500 Blink ▾

### Domyślny stan wyświetlacza LED:

Status LED		Opis	
Niebieski	Zawsze włączony	Status normalny	
	Miganie	Dzwonienie	
Czerwony	Miganie	Sieć jest niedostępna	
Zielony	Zawsze włączony	Rozmowa podczas połączenia	
	Miganie	Odbieranie połączeń	
Różowy	Miganie	Aktualizacja	

### Konfiguracja parametrów:

- **Stan:** istnieje pięć stanów: **Normalny, Offline, Połączenie, Rozmowa i Odbiór.**
- **Kolor LED:** może obsługiwać trzy kolory: **Czerwony, Zielony, Niebieski.**
- **Tryb wyświetlania LED:** różne częstotliwości migania.

#### Uwaga:

- Statusu i koloru elementu nie można zmienić.
- Dioda LED trybu aktualizacji nie może być regulowana.

## Konfiguracja wyświetlacza LED z adresu URL HTTP

Możesz wprowadzić adres URL HTTP w przeglądarce, aby zarządzać kolorem i częstotliwością LED. Przejdź do strony internetowej **Intercom > LED Setting > LED**

**Control**, aby włączyć tę funkcję.

### LED Control

---

Wake Mode	Auto <span style="float: right;">▼</span>
LED Control	<input checked="" type="checkbox"/>
Keypad LED Enabled	<input type="checkbox"/>
Card LED Enabled	<input type="checkbox"/>

Format URL HTTP to: **http://PhoneIP/fcgi/do?**

**action=LedAction&State=1&Color=1&Mode=2500**

- **Status:** 1=bezczylny; 2=wyłączony; 3=wywołujący; 4=rozmawiający; 5=odbierający; Kolor: 1=zielony; 2=niebieski; 3=czerwony; Tryb: 0=zawsze włączony; 1=zawsze wyłączony; 500/1000/1500/2000/25000/3000

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

Przejdź do interfejsu web **Intercom > LED Setting > LED Control**.

### LED Control

---

Wake Mode	Auto <span style="float: right;">▼</span>
LED Control	<input type="checkbox"/>
Keypad LED Enabled	<input type="checkbox"/>
Card LED Enabled	<input checked="" type="checkbox"/>
Time (H)	18 - 06 (0~23)

**Konfiguracja parametrów :**

- **Czas (H):** zakres czasu, w którym oświetlenie LED będzie działać. Jeśli zakres czasu jest ustawiony od **8 do 0 (czas rozpoczęcia-zakończenia)**, oznacza to, że światło LED pozostanie włączone w zakresie czasu od **8:00** rano. do **12:00** w ciągu jednego dnia (24 godziny).

## Ustawienie diody LED na klawiaturze

Podświetlenie LED w obszarze klawiatury można włączyć lub wyłączyć w interfejsie internetowym. Tymczasem, jeśli nie chcesz, aby dioda LED w obszarze czytnika kart pozostawała włączona, możesz również ustawić dokładny czas, w którym dioda LED może być wyłączona w celu zmniejszenia zużycia energii elektrycznej.

Przejdź do interfejsu web **Intercom > LED Setting > LED Control**.

### LED Control

---

Wake Mode	<input type="text" value="Auto"/> ▾
LED Control	<input type="checkbox"/>
Keypad LED Enabled	<input checked="" type="checkbox"/>
Time (H)	<input type="text" value="18"/> - <input type="text" value="06"/> (0~23)
Card LED Enabled	<input type="checkbox"/>

- **Czas (H)**: zakres czasu, w którym oświetlenie LED będzie działać. Jeśli zakres czasu jest ustawiony na **8-0 (czas rozpoczęcia-zakończenia)**, oznacza to, że światło LED pozostanie włączone w przedziale czasowym od **8:00** do **12:00** w ciągu jednego dnia (24 godziny).

# Konfiguracja głośności i tonów

## Konfiguracja głośności

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

Przejdź do interfejsu Web **Phone > Audio > Volume Control**.

Volume Control		
Mic Volume	<input type="text" value="8"/>	(1~15)
Volume Level	<input type="text" value="1"/> ▾	
Speaker Volume	<input type="text" value="15"/>	(1~15)
Keypad Volume	<input type="text" value="8"/>	(1~15)
Tamper Alarm Volume	<input type="text" value="15"/>	(1~15)
Prompt Volume	<input type="text" value="15"/>	(0~15)

### Konfiguracja parametrów:

- **Poziom głośności:** kontroluje głośność wszystkich głośników. Domyślnie jest to 1, pierwszy poziom głośności, zakres głośności wynosi około 80-95, a 2 to drugi poziom głośności, zakres głośności wynosi około 95-109.
- **Głośność komunikatów:** obejmuje różne rodzaje komunikatów dźwiękowych informujących o pomyślnym i nieudanym otwarciu drzwi, oddzwonieniu itp.

## Ogłoszenie IP

Przejdź do interfejsu Web **Phone > Audio > IP announcement**.

IP Announcement	
Active Time After Reboot	<input type="text" value="0"/> (0~180 sec)
Loop Times	<input type="text" value="1"/> (0~10)



### Konfiguracja parametrów :

- **Active Time After Reboot:** czas komunikatu IP po ponownym uruchomieniu urządzenia. Jeśli ustawiono 30 sekund, po ponownym uruchomieniu urządzenia należy nacisnąć przycisk połączenia w ciągu 30 sekund, aby wyświetlić komunikat IP, w przeciwnym razie komunikat IP wygaśnie. Jeśli ustawisz 0 sekund, możesz nacisnąć przycisk połączenia w dowolnym momencie po ponownym uruchomieniu urządzenia, aby wyświetlić komunikat IP.

## Konfiguracja sygnału dźwiękowego otwartych drzwi

Możesz kontrolować słowa zachęty towarzyszące sygnałowi w interfejsie internetowym **Telefon**  
> **Dźwięk** > **Ustawienia sygnału otwartych drzwi.**



Open Door Tone Setting	
Open Door Inside Tone	<input checked="" type="checkbox"/>
Open Door Outside Tone	<input checked="" type="checkbox"/>
Open Door Failed Tone	<input checked="" type="checkbox"/>

### Konfiguracja parametrów :

- **Open Door Inside Tone** : umożliwia użytkownikom usłyszenie sygnału dźwiękowego otwarcia drzwi po naciśnięciu przycisku wyjścia.
- **Open Door Outside Tone** : umożliwia użytkownikom usłyszenie sygnału dźwiękowego otwarcia drzwi przy użyciu metod dostępu obsługiwanych przez bramofon.

## Ustawienie tonu klawiatury



Keypad Tone Setting	
Keypad Tones	Beep ▾

### Konfiguracja parametrów :

- **Keypad Tones (Dźwięki klawiatury)** : wybierz opcję **Beep (Sygnał dźwiękowy)**, aby usłyszeć sygnał dźwiękowy po naciśnięciu klawiatury. W przypadku wybrania opcji **Digital Sounds (Dźwięki cyfrowe)** po naciśnięciu klawiatury można usłyszeć komunikat odpowiednich klawiszy numerycznych.

## Przesyłanie plików dźwiękowych

### Prześlij dźwięk dzwonka

Przejdź do interfejsu Web **Phone > Audio > Tone Upload**.

**Tone Upload**  
File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

---

Open Door Succeeded Outside Warning	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Succeeded Inside Warning	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Open Door Failed Warning	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Ringback	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>
Trigger Manager Dial Warning	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Delete"/> <input type="button" value="Export"/>

### Prześlij dźwięk otwartych drzwi

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

Dźwięk zewnętrzny jest słyszalny, gdy użytkownicy otwierają drzwi za pomocą karty lub DTMF. Dźwięk wewnętrzny jest słyszalny, gdy użytkownicy otwierają drzwi za pomocą wyzwalanego interfejsu wejściowego. Postępuj zgodnie z instrukcjami dotyczącymi rozmiaru i formatu pliku.

Przejdź do interfejsu Web **Phone > Audio > Tone Upload**.

### Tone Upload

File Format: wav, size: < 200KB, samplerate: 16000, Bits: 16

Open Door Succeeded Outside Warning	Choose File	No file chosen		
	Upload	Delete	Export	
Open Door Succeeded Inside Warning	Choose File	No file chosen		
	Upload	Delete	Export	
Open Door Failed Warning	Choose File	No file chosen		
	Upload	Delete	Export	
Ringback	Choose File	No file chosen		
	Upload	Delete	Export	
Trigger Manager Dial Warning	Choose File	No file chosen		
	Upload	Delete	Export	

#### Konfiguracja parametrów :

- **Open Door Succeeded Outside Warning**: sygnał ostrzegawczy, który włączy się, gdy użytkownicy otworzą drzwi, naciskając przycisk wyjścia.
- **Open Door Succeeded Inside Warning** : sygnał ostrzegawczy, który włączy się po otwarciu drzwi przy użyciu metod dostępu obsługiwanych przez bramofon.
- **Trigger Manager Dial Warning**: dźwięk ostrzegawczy, który włączy się, gdy użytkownik naciśnie przycisk w celu wykonania połączenia grupowego lub sekwencyjnego.

# Ustawienia sieciowe

## Status sieci

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

Network Information	
Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.103
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8

## Konfiguracja sieci urządzenia

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

Przejdź do interfejsu **Sieć > Podstawowy**

LAN Port	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static IP
IP Address	<input type="text" value="192.168.1.100"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Preferred DNS Server	<input type="text" value="8.8.8.8"/>
Alternate DNS Server	<input type="text"/>

**Konfiguracja parametrów :**

- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Jeśli tryb DHCP jest włączony, bramofon zostanie automatycznie przypisany przez serwer DHCP z adresem IP, maską podsieci, domyślną bramą i adresem serwera DNS.
- **Stacyjny adres IP**: po wybraniu trybu statycznego adresu IP adres IP, maska podsieci, brama domyślna i adres serwerów DNS muszą zostać skonfigurowane ręcznie zgodnie z rzeczywistym środowiskiem sieciowym.
- **Adres IP** : wprowadź adres IP, gdy wybrany jest tryb statycznego adresu IP.
- **Maska podsieci**: ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Default Gateway (Brama domyślna)**: ustawienie prawidłowej bramy zgodnie z adresem IP.
- **Preferowany/Alternatywny serwer DNS**: preferowany serwer DNS to podstawowy adres serwera DNS, podczas gdy alternatywny serwer DNS jest serwerem drugorzędym. Bramofon połączy się z alternatywnym serwerem, gdy podstawowy będzie niedostępny.

## 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	<input type="text" value="None"/>
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="Stair Phone"/>

### Konfiguracja parametrów :

- **Tryb** serwera: jest automatycznie konfigurowany zgodnie z rzeczywistym połączeniem urządzenia z określonym serwerem w sieci, takim jak **SDMC**, **Cloud** i **None**. **Brak** jest domyślnym ustawieniem fabrycznym wskazującym, że urządzenie nie jest w żadnym typie serwera, dlatego można wybrać Cloud lub SMDC w trybie wykrywania.

- **Tryb wykrywania:** umożliwia wykrywanie urządzenia przez inne urządzenia w sieci. Wyłączenie tej opcji spowoduje, że urządzenie zostanie ukryte i nie będzie wykrywane przez inne urządzenia.
- **Adres urządzenia :** określa 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:** numer wewnętrzny zainstalowanego urządzenia.

**Lokalizacja urządzenia:** lokalizacja, w której urządzenie jest zainstalowane i używane.

## Lokalna konfiguracja RTP urządzenia

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

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

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)

**Konfiguracja parametrów :**

- **Min. port RTP:** wartość portu służąca do ustalenia punktu początkowego dla wyłącznego zakresu transmisji danych.
- **Max RTP port:** wartość portu do ustalenia punktu końcowego dla wyłącznego zakresu transmisji danych.

## Ustawienie NAT

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

Aby skonfigurować NAT, przejdź do interfejsu **Konto internetowe > Podstawowe > NAT**.

### NAT

---

NAT	<input type="text" value="Disabled"/>	
Stun Server Address	<input type="text"/>	Port <input type="text" value="3478"/> (1024~65535)

#### Konfiguracja parametrów :

- **Stun Server Address**: adres serwera SIP w sieci rozległej (WAN).
- **Port**: port serwera SIP.

Następnie przejdź do **Konto internetowe > Zaawansowane > Interfejs NAT**.

### NAT

---

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

#### Konfiguracja parametrów :

- **UDP Keep Alive Messages**: jeśli włączone, urządzenie wyśle wiadomość do serwera SIP, aby serwer SIP rozpoznał, czy urządzenie jest w stanie online.
- **UDP Alive Msg Interval**: interwał czasowy wysyłania wiadomości wynosi od 5 do 60 sekund. Domyślnie jest to 30 sekund.
- **RPort**: włącz RPort, gdy serwer SIP znajduje się w sieci WAN.

## Ustawienie SNMP

Simple Network Management Protocol (**SNMP**) to protokół zarządzania urządzeniami sieciowymi IP. Umożliwia on administratorom sieci monitorowanie urządzeń i otrzymywanie alertów dotyczących warunków wymagających uwagi. SNMP zapewnia zmienne opisujące konfigurację systemu, zorganizowane w hierarchie i opisane przez bazy informacji zarządzania (MIB).

Przejdź do interfejsu **Sieć > Zaawansowane > SNMP**.

SNMP	
Enabled	<input type="checkbox"/>
Port	<input type="text" value=""/> (1024~65535)
Trusted IP	<input type="text" value=""/>

**Konfiguracja parametrów :**

- **Zaufany adres IP:** dozwolony adres serwera SNMP. Może to być adres IP lub dowolna prawidłowa nazwa domeny URL.

## Ustawienie VLAN

Wirtualna sieć lokalna (VLAN) to logiczna grupa węzłów z tej samej domeny IP, niezależnie od ich fizycznego segmentu sieci. Oddziela ona domenę rozgłoszeniową warstwy 2 za pośrednictwem przełączników lub routerów, wysyłając oznaczone pakiety tylko do portów o pasujących identyfikatorach VLAN. Korzystanie z sieci VLAN zwiększa bezpieczeństwo, ograniczając ataki ARP do określonych hostów i poprawia wydajność sieci, minimalizując niepotrzebne ramki rozgłoszeniowe, oszczędzając w ten sposób przepustowość w celu zwiększenia wydajności.

Przejdź do interfejsu **Sieć > Zaawansowane > VLAN**.

VLAN	
LAN Port	Enabled <input type="checkbox"/>
	VID <input type="text" value="1"/> (1~4094)
	Priority <input type="text" value="0"/> ▼

**Konfiguracja parametrów :**

- **VID:** identyfikator VLAN dla wyznaczonego portu.
- **Priorytet:** priorytet VLAN dla wyznaczonego portu.

## Ustawienie TR069



TR-069 (Technical Report 069) zapewnia komunikację między urządzeniami lokalnymi klienta (CPE) a serwerami autokonfiguracji (ACS). Obejmuje zarówno bezpieczną automatyczną konfigurację, jak i kontrolę innych funkcji zarządzania CPE w zintegrowanej strukturze. W przypadku bramofonów administratorzy mogą zarządzać wszystkimi urządzeniami na wspólnej platformie TR-069. Telefony IP można łatwo i bezpiecznie skonfigurować na platformie TR-069, aby usprawnić masowe wdrażanie.

Przejdź do interfejsu **Sieć > Zaawansowane > TR069**.

The screenshot shows the TR069 configuration page with the following settings:

TR069		
ACS	Enabled	<input type="checkbox"/>
	Version	1.0 <input type="button" value="v"/>
	URL	<input type="text"/>
	User Name	<input type="text"/>
Periodic Inform	Password	*****
	Enabled	<input type="checkbox"/>
	Periodic Interval	1800 (3~24x3600s)
CPE	URL	<input type="text"/>
	User Name	<input type="text"/>
	Password	*****

#### Konfiguracja parametrów :

- **Wersja:** wybór obsługiwanej wersji TR069 (wersja 1.0 lub 1.1).
- **ACS/CPE:** ACS to skrót od serwerów automatycznej konfiguracji po stronie serwera, a CPE to skrót od urządzeń klienta po stronie klienta.
- **URL :** adres URL dla ACS lub CPE.
- **Periodic Interval:** interwał dla okresowych informacji.

#### Uwaga

- TR-069 to specyfikacja techniczna zatytułowana CPE WAN Management Protocol (CWMP). Definiuje on protokół warstwy aplikacji do zdalnego zarządzania urządzeniami użytkowników końcowych.

## Ustawienia HTTP sieci Web urządzenia

Ta funkcja zarządza dostępem do strony internetowej urządzenia. Bramofon obsługuje dwie metody zdalnego dostępu: HTTP i HTTPS (szyfrowanie).

Przejdź do interfejsu **Sieć > Zaawansowane > Serwer WWW**.

Web Server	
HTTP Enabled	<input checked="" type="checkbox"/>
HTTPS Enabled	<input checked="" type="checkbox"/>
HTTP Port	<input type="text" value="80"/> (80,1024~65534)
HTTPS Port	<input type="text" value="443"/> (443,1024~65534)

# 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.

Przejdź do interfejsu Web **Phone > Call Feature > Direct IP**.



Direct IP	
Enabled	<input checked="" type="checkbox"/>
Auto Answer	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1~65535)

## Konfiguracja połączeń SIP i połączeń SIP

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

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

## Rejestracja konta SIP

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

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

Przejdź do strony internetowej **Konto > Podstawowe > Interfejs konta SIP**.

**Account-Basic**

**SIP Account**

---

Status	UnRegistered
Account	Account 1 ▼
Account Enabled	<input type="checkbox"/>
Display Label	204
Display Name	204
Register Name	204
User Name	204
Password	*****

### Konfiguracja parametrów :

- **Display Label:** etykieta urządzenia wyświetlana na ekranie urządzenia.
- **Wyświetlana nazwa:** nazwa urządzenia, która będzie wyświetlana na urządzeniu, z którym nawiązywane jest połączenie.

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

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

## Konfiguracja serwera SIP

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

Przejdź do interfejsu Web **Account > Basic > SIP Server**.

Preferred SIP Server		
Server IP	<input type="text" value="192.168.1.88"/>	Port <input type="text" value="5060"/> (1024~65535)
Registration Period	<input type="text" value="1800"/>	(30~65535s)

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

- Aby zarejestrować konto SIP dla monitorów wewnętrznych Akuvox, uzyskaj adres IP serwera i port serwera na ekranie centrali PBX monitora wewnętrznego Akuvox.
- Aby zarejestrować konto SIP dla urządzeń innych firm, należy uzyskać adres IP serwera i port serwera od zewnętrznego dostawcy usług.

#### Konfiguracja parametrów :

- **Preferowany serwer SIP:** adres IP głównego serwera lub jego adres URL.
- **Alternatywny serwer SIP:** adres IP zapasowego serwera SIP lub jego adres URL.
- **Port:** port serwera SIP do transmisji danych.
- **Registration Period:** okres rejestracji konta SIP. Ponowna rejestracja SIP rozpocznie się automatycznie, jeśli rejestracja konta nie powiedzie się w okresie rejestracji. Okres rejestracji wynosi **30-65535s** z domyślną wartością **1800**.

## 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 **Konto internetowe > Podstawowe > Interfejs serwera proxy połączeń wychodzących.**

Outbound Proxy Server		
Outbound Enabled	<input type="checkbox"/>	
Server IP	<input type="text"/>	Port <input type="text" value="5060"/> (1024~65535)
Backup Server IP	<input type="text"/>	Port <input type="text" value="5060"/> (1024~65535)

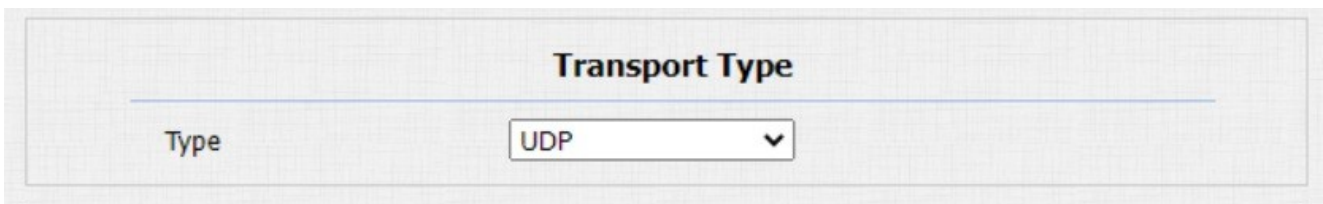
### Konfiguracja parametrów :

- **Adres IP serwera:** adres SIP serwera proxy połączeń wychodzących.
- **Port:** numer portu służący do nawiązywania sesji połączeń przez wychodzący serwer proxy.

## 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**.



### Konfiguracja parametrów :

- **UDP:** zawodny, ale bardzo wydajny protokół warstwy transportowej. UDP jest domyślnym protokołem transportowym.
- **TCP:** niezawodny, ale mniej wydajny protokół warstwy transportowej.
- **TLS:** bezpieczny i niezawodny protokół warstwy transportowej.
- **DNS-SRV** : uzyskuje rekord DNS w celu określenia lokalizacji serwerów. **SRV** rejestruje nie tylko adres serwera, ale także port serwera. Ponadto SRV może być również używany do konfigurowania priorytetu i wagi adresu serwera.

# Ustawienia połączeń

## DND

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

Przejdź do interfejsu Web **Phone > Call Feature**.

**Phone-Call Feature**

**DND**

Enabled

Return Code When DND 486(Busy Here) ▼

## Zapobieganie włamaniom SIP

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

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

**Call**

Max Local SIP Port 63531 (1024~65535)

Min Local SIP Port 63521 (1024~65535)

Auto Answer

Prevent SIP Hacking

## Wybieranie połączenia przez menedżera

Funkcja Manager Dial Call obejmuje dwa rodzaje połączeń: Połączenie sekwencyjne i połączenie

grupowe. Umożliwia szybkie inicjowanie wstępnie skonfigurowanych numerów poprzez naciśnięcie przycisków na bramofonie.



Przejdź do interfejsu web **Intercom > Basic > Manager Dial**.

### Manager Dial

---

Call Type Group Call ▼

Call Timeout (Sec) 20 ▼

(If the local group is not blank, then only the local numbers will be called.)

#### Group Call Number (Local)

Key	Number 1	Number 2	Number 3	Number 4	Number 5	Number 6
Push Button 1	192.168.33					
Push Button 2						
Push Button 3						
Push Button 4						
Push Button 5						

#### Group Call Number (Cloud)

011122334455/1	011122334455/1	333102922/1	192.168.1.4/1

#### Konfiguracja parametrów :

- **Typ połączenia:** wybierz połączenie grupowe lub połączenie sekwencyjne (połączenie Robin) dla połączenia wybierania menedżera.
- **Połączenie sekwencyjne:** połączenie sekwencyjne służy do inicjowania wielu numerów po naciśnięciu przycisku wybierania menedżera. Jeśli poprzedni rozmówca nie odbierze połączenia w ciągu limitu czasu połączenia sekwencyjnego, połączenie zostanie przeniesione do następnego. Jeśli połączenie zostanie odebrane przez jednego z rozmówców, połączenie nie zostanie przeniesione.
- **Po odrzuceniu :** w przypadku wybrania opcji **Zakończ wszystkie połączenia** , połączenie sekwencyjne zostanie zakończone, jeśli zostanie odrzucone przez stronę wywoływaną. Jeśli wybierzesz opcję **Zakończ tylko to połączenie** , połączenie sekwencyjne będzie kontynuowane do następnego rozmówcy, jeśli zostanie odrzucone przez pierwszego rozmówcę.
- **Połączenie grupowe:** połączenie grupowe służy do inicjowania połączeń z wieloma numerami jednocześnie po naciśnięciu przycisku wybierania menedżera.

### Uwaga

Połączenie sekwencyjne działa z SmartPlus Cloud.

## Szybkie wybieranie

Szybkie wybieranie to funkcja umożliwiająca szybkie nawiązywanie połączeń poprzez naciśnięcie przycisku wybierania na klawiaturze.

Przejdź do interfejsu web **Intercom > Basic > Speed Dial**. Wprowadź jeden numer SIP/IP w jednym polu.

### Speed Dial

---


Po skonfigurowaniu wybierania menedżera można skonfigurować przekaźniki, które będą wyzwalane przez naciśnięcie przycisków na bramofonie.

Przewiń w dół do sekcji **Trigger Relay By Manager Dial**.

### Trigger Relay By Manager Dial

---

Push Button 1	RelayA <input type="checkbox"/> RelayB <input type="checkbox"/>
Push Button 2	RelayA <input type="checkbox"/> RelayB <input type="checkbox"/>
Push Button 3	RelayA <input type="checkbox"/> RelayB <input type="checkbox"/>
Push Button 4	RelayA <input type="checkbox"/> RelayB <input type="checkbox"/>
Push Button 5	RelayA <input type="checkbox"/> RelayB <input type="checkbox"/>

## Szybkie wybieranie w module rozszerzającym

Urządzenie obsługuje połączenie z jednostką rozszerzającą, umożliwiając skonfigurowanie większej liczby numerów szybkiego wybierania. Użytkownicy mogą nacisnąć przycisk na urządzeniu, aby nawiązać połączenie.



Przejdź do interfejsu web **Intercom > Extension Unit**.

A screenshot of a web interface for 'Extension Unit 1'. The title 'Extension Unit' is at the top left, and 'Extension Unit 1' is centered. Below the title, it says 'Current Version : 6' and there is a 'Locate Module' button. A table with 6 rows and 3 columns is shown. The columns are 'Index', 'Label', and 'Number'. The rows are numbered 1 to 6, but the 'Label' and 'Number' cells are empty.

Index	Label	Number
1		
2		
3		
4		
5		
6		

**Konfiguracja parametrów:**

- **Locate Module (Zlokalizuj modul):** po kliknięciu przycisku dioda przycisku mignie
- trzy razy w odstępach 500 ms. **Etykieta:** nazwa klucza, zazwyczaj nazwa osoby dzwoniącej.
- **Numer:** numer IP/SIP wywoływanego urządzenia.

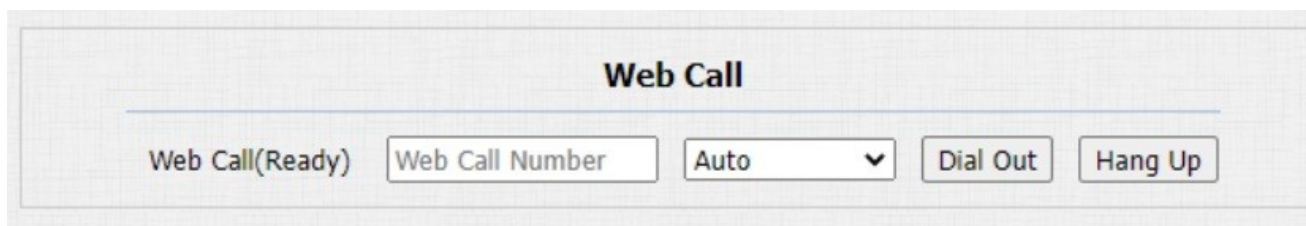
### Uwaga

- TYLKO urządzenia z oprogramowaniem sprzętowym w wersji 320.30.10.116 i wyższej obsługują tę funkcję. funkcja.  
Skonsultuj się z zespołem technicznym Akuvox, aby uzyskać najnowsze oprogramowanie sprzętowe.

## Połączenie internetowe

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

Przejdź do interfejsu Web **Intercom > Basic > Web Call**.



**Konfiguracja parametrów :**

**Web Call (Ready):** wywoływany numer IP/SIP.

## Automatyczna odpowiedź

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 **Konto internetowe > Zaawansowane > Połączenie**, można skonfigurować powiązane parametry w interfejsie **Telefon > Funkcja połączenia > Automatyczne odbieranie** .

## Call

Max Local SIP Port	<input type="text" value="5062"/>	(1024~65535)
Min Local SIP Port	<input type="text" value="5062"/>	(1024~65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input type="checkbox"/>	

### Auto Answer

---

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

#### Konfiguracja parametrów :

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

## Multicast

Funkcja Multicast umożliwia transmisję jeden-do-wielu do różnych celów. Na przykład umożliwia ona monitorowi wewnętrznemu ogłaszanie komunikatów z kuchni do innych pomieszczeń lub nadawanie powiadomień z biura zarządu do wielu lokalizacji. W tych scenariuszach monitory wewnętrzne mogą słuchać lub wysyłać transmisje audio.

Przejdź do interfejsu Web **Phone > Multicast**.

**Multicast**

**Multicast Setting**

---

Multicast Priority Paging Barge  ▼

Paging Priority Enabled

**Priority List**

---

IP Address	Listening Address	Label	Priority
1st IP Address	<input style="width: 90%;" type="text" value="224.1.6.21:51230"/>	<input style="width: 90%;" type="text" value="AKUVOX"/>	1
2nd IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	2
3rd IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	3
4th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	4
5th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	5
6th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	6
7th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	7
8th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	8
9th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	9
10th IP Address	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	10

**Konfiguracja parametrów :**

- **Multicast Priority Paging Barge:** multicast lub ile połączeń multicast ma wyższy priorytet niż połączenie SIP, jeśli wyłączysz Paging Priority Active, połączenie SIP będzie miało wysoki priorytet.
- **Priorytet przywoływania włączony:** połączenia multiemisji są wywoływane w kolejności według priorytetu lub nie.
- **Listening Address:** adres IP multiemisji, który ma być nasłuchiwany. Adres IP multiemisji musi być taki sam jak część nasłuchiwana, a port multiemisji nie może być taki sam dla każdego adresu IP. Adres IP multiemisji mieści się w zakresie od 224.0.0.0 do 239.255.255.255.

**Konfiguracja 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 > Basic > Max Call Time**.

<b>Max Call Time</b>		
Max Call Time	<input type="text" value="5"/>	(2~30 Min)

#### Uwaga

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

## Maksymalny czas 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 > Basic > Max Dial Time**.

<b>Max Dial Time</b>		
Dial In Time	<input type="text" value="60"/>	(5~120 Sec)
Dial Out Time	<input type="text" value="60"/>	(5~120 Sec)

#### Uwaga

- Maksymalny czas wybierania urządzenia jest również powiązany z maksymalnym czasem wybierania serwera SIP. W przypadku korzystania z SIP aby nawiązać połączenie, należy zwrócić uwagę na maksymalny czas wybierania serwera SIP. Jeśli maksymalny czas wybierania serwera SIP jest krótszy niż maksymalny czas wybierania urządzenia, dostępny jest krótszy czas.



## Odlóż słuchawkę po otwarciu drzwi

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

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

### Hang Up After Open Door

---

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

### Konfiguracja parametrów :

- **Typ:** drzwi można otworzyć za pomocą **DTMF, polecenia HTTP, DTMF lub HTTP** oraz **wejścia, DTMF lub HTTP**.
- **Limit czasu:** połączenie zostanie automatycznie rozłączone po otwarciu drzwi.

# Konfiguracja kontaktów

Lista kontaktów służy do przyznawania uprawnień dostępu lub wywoływania monitora wewnętrznego lub innych urządzeń. Można ją skonfigurować w interfejsie internetowym

**Contacts > Access Allowlist.**

## Zarządzanie kontaktami

W Internecie można wyszukiwać, wyświetlać, edytować i usuwać kontakty z listy kontaktów. Przejdź do strony internetowej **Contacts > Access Allowlist** .

**Access Allowlist**

**Contacts** All Contacts ▾

**Search**  Search Reset

Index	Name	Phone Number	Account	Floor	<input type="checkbox"/>
1					<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Page 1 ▾
Prev
Next
Delete
Delete All

**Contact Setting**

Name

Account Auto ▾

Phone Number

Floor None

Add
Edit
Cancel

**Konfiguracja parametrów :**

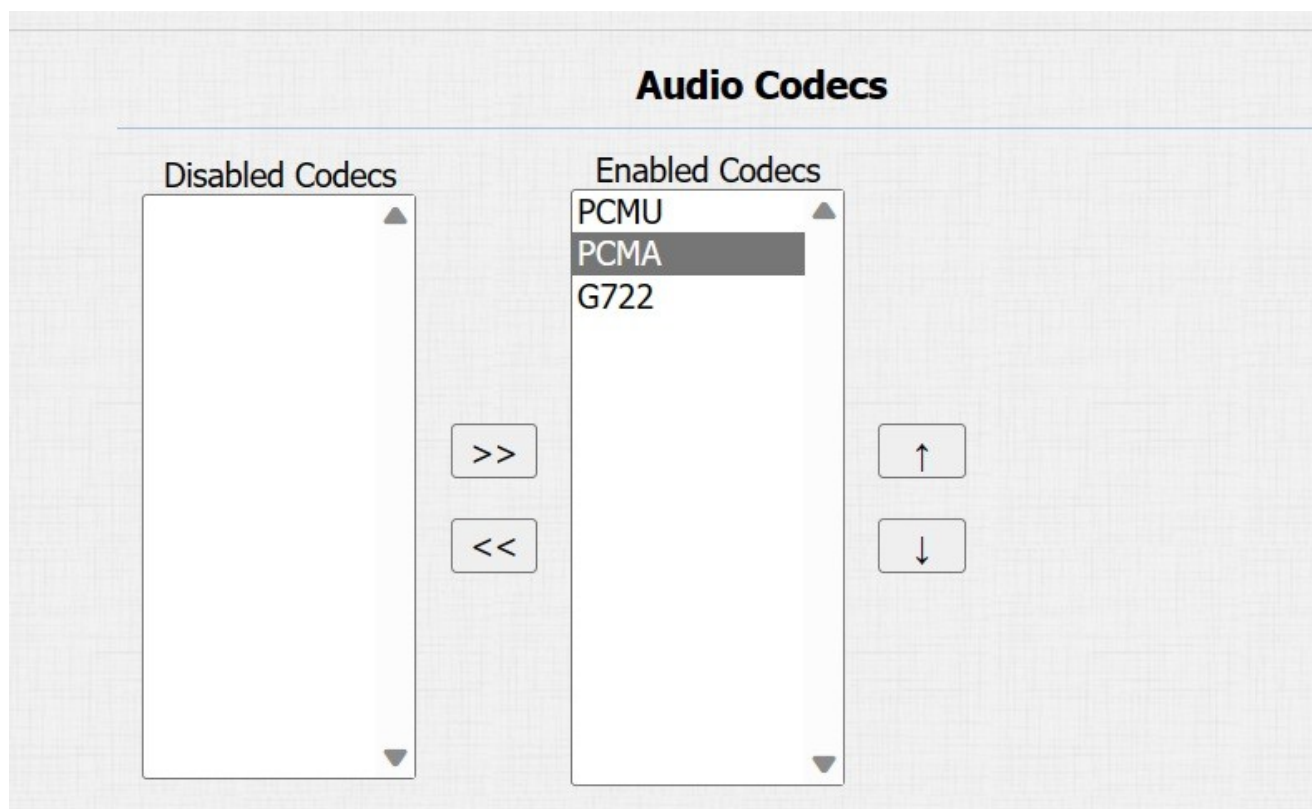
- **Account:** zarejestrowane konto SIP do wykonywania połączeń. W przypadku korzystania z bezpośredniego połączenia IP jest ono niedostępne.
- **Piętro:** numer piętra, do którego kontakt ma dostęp.

# 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 kodek 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**.



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

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

## Konfiguracja kodeka wideo

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

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

Video Codec	
Name	<input checked="" type="checkbox"/> H264
Resolution	4CIF ▼
Bitrate	2048 ▼
Payload	104 ▼

#### Konfiguracja parametrów :

- **Name** : zaznacz, aby wybrać format kodeka wideo H264 dla strumienia wideo z bramofonu. Domyślnym kodekiem wideo jest H264.
- **Rozdzielczość**: rozdzielczość wideo ma cztery opcje, **CIF**, **VGA**, **4CIF** i **720P**, w zależności od rzeczywistego środowiska sieciowego. Domyślną rozdzielczością jest **4CIF**.
- **Bitrate**: bitrate strumienia wideo waha się od 128 do 2048. Im większa szybkość transmisji bitów, tym większa ilość danych przesyłanych w każdej sekundzie, a tym samym wyraźniejszy obraz wideo.  
Domyślna szybkość transmisji kodu wynosi 2048.
- **Ładunek**: ładunek mieści się w zakresie od 90 do 119 dla konfiguracji pliku konfiguracyjnego audio/wideo. Domyślny ładunek wynosi 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 Phone > Call Feature > IP Video Parameters**.

IP Video Parameters	
Video Resolution	4CIF ▼
Video Bitrate	2048 kbps ▼
Video Payload	104 ▼

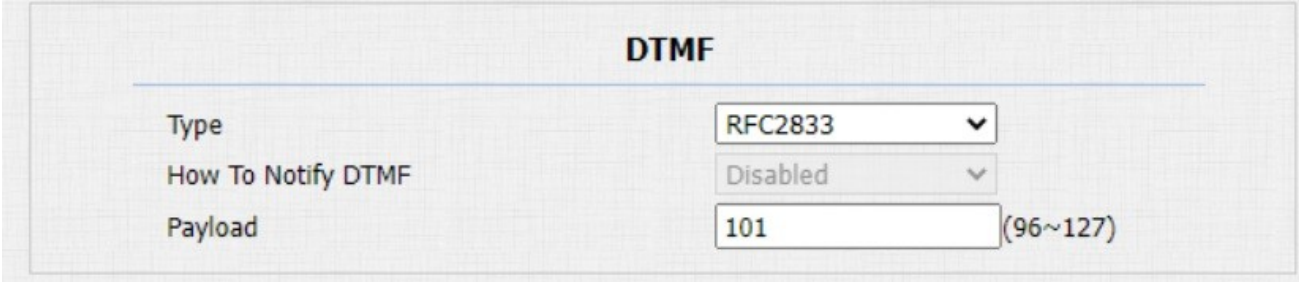
## Konfiguracja parametrów :

- **Rozdzielczość wideo:** rozdzielczość wideo ma cztery opcje, **CIF, VGA, 4CIF i 720P**, w zależności od rzeczywistego środowiska sieciowego. Domyślną rozdzielczością jest **4CIF**.
- **Szybkość transmisji wideo:** szybkość transmisji strumienia wideo wynosi od 64 do 2048 kb/s. Im większa szybkość transmisji, tym większa ilość danych przesyłanych w każdej sekundzie, a tym samym wyraźniejszy obraz wideo. Domyślna szybkość transmisji kodu wynosi 2048.
- **Ładunek wideo:** ładunek mieści się w zakresie od 90 do 119 dla konfiguracji pliku konfiguracyjnego audio/wideo. Domyślny ładunek wynosi 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	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)

## Konfiguracja parametrów :

- **Typ:** wybór trybu DTMF spośród pięciu opcji: **Inband, RFC 2833, Info, Info+Inband i Info+RFC 2833** w oparciu o określony typ transmisji DTMF urządzenia innej firmy, z którym ma zostać nawiązane połączenie jako strona odbierająca dane sygnału.
- **Jak powiadomić DTMF:** wybierz jeden z czterech typów: **Disable, DTMF, DTMF-Relay i Telephone-Event** zgodnie z konkretnym typem przyjętym przez urządzenie innej firmy. Należy to skonfigurować tylko wtedy, gdy urządzenie innej firmy, z którym ma zostać nawiązane połączenie, przyjmuje tryb **Info**.
- **Payload:** ustawia ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą i odbiorcą podczas transmisji danych.

# Ustawienie przekaźnika

## Ustawienie przełącznika przekaźnika

Przełącznik(i) przekaźnika i DTMF dla dostępu do drzwi można skonfigurować w interfejsie Web Intercom > Relay.

Relay		
Relay ID	RelayA ▼	RelayB ▼
Type	Default state ▼	Default state ▼
Mode	Monostable ▼	Monostable ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	3 ▼	3 ▼
DTMF Mode	1 Digit DTMF ▼	
1 Digit DTMF	0 ▼	1 ▼
2~4 Digits DTMF	010	012
Relay Status	RelayA: Low	RelayB: Low
Relay Name	RelayA	RelayB

### Konfiguracja parametrów :

- **Typ:** gdy wybrany jest stan domyślny, stan przekaźnika pokazuje wartość niską, co oznacza, że drzwi są zamknięte, a stan przekaźnika pokazuje wartość wysoką, co oznacza, że drzwi są otwarte. W przypadku wybrania opcji Invert State (Stan odwrócony) stan przekaźnika będzie wskazywał wartość High (Wysoki), co oznacza, że drzwi są zamknięte, a Low (Niski), 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)**: czas opóźnienia wyzwolenia przekaźnika wynosi od 1 do 10 sekund. Jeśli ustawisz czas opóźnienia na **5** sekund, przekaźnik zostanie wyzwolony dopiero po 5 sekundach od naciśnięcia przycisku odblokowania.
- **Hold Delay (Sec)**: czas opóźnienia zatrzymania przekaźnika wynosi od 1 do 10 sekund. Jeśli ustawisz czas opóźnienia na **5** sekund, przekaźnik powróci do stanu początkowego po utrzymaniu stanu wyzwolenia przez 5 sekund.
- **Tryb DTMF**: liczba cyfr DTMF dla kontroli dostępu do drzwi (w zakresie od 1 do 4 cyfr).
- **1 Digit DTMF** : wybierz kod z zakresu \*0-9 i #, jeśli opcja DTMF jest ustawiona jako 1-cyfrowa.
- **2~4 Digits DTMF** : ustaw kod DTMF zgodnie z ustawieniem **opcji DMTP**. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli **opcja DMTP** jest ustawiona jako 3-cyfrowa.
- **Status przekaźnika**: status przekaźnika jest domyślnie niski, co oznacza stan normalnie zamknięty (NC). Jeśli stan przekaźnika jest wysoki, oznacza to, że jest on normalnie otwarty (NO).
- **Nazwa przekaźnika**: nadaj nazwę przełącznikowi przekaźnika, aby odróżnić go od innych. Dla wygody można nazwać przełącznik przekaźnika zgodnie z jego lokalizacją.

#### Wskazówka

- Tylko urządzenia zewnętrzne podłączone do przełącznika przekaźnika muszą być zasilane przez zasilanie ponieważ przełącznik przekaźnika nie dostarcza zasilania.
- Zaleca się podłączenie blokady drzwi do **przekaźnika B**.

## 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 **Intercom > Relay > Security Relay**.

### Security Relay

Relay ID	Security Relay A
Connect Type	RS485
Trigger Delay(Sec)	<input style="width: 80px;" type="text" value="0"/> ▼
Hold Delay(Sec)	<input style="width: 80px;" type="text" value="5"/> ▼
1 Digit DTMF	<input style="width: 80px;" type="text" value="2"/> ▼
2~4 Digits DTMF	<input style="width: 120px;" type="text" value="013"/>
Relay Name	<input style="width: 120px;" type="text" value="Security Relay A"/>
Enabled	<input type="checkbox"/>
<input style="width: 80px;" type="button" value="Test"/>	

#### Konfiguracja parametrów :

- **Connect Type**: typ połączenia między przekaźnikiem bezpieczeństwa a bramofonem.
- **Trigger Delay(Sec)**: czas opóźnienia wyzwolenia przekaźnika wynosi od 0 do 10 sekund. Jeśli ustawisz czas opóźnienia na 5 sekund, przekaźnik zostanie wyzwolony dopiero po 5 sekundach od naciśnięcia przycisku odblokowania. Domyślnym ustawieniem jest 0, co oznacza wyzwolenie przekaźnika zaraz po naciśnięciu przycisku odblokowania.
- **Hold Delay(Sec)**: czas opóźnienia zatrzymania przekaźnika wynosi od 1 do 60 sekund. Jeśli ustawisz czas opóźnienia na 5 sekund, przekaźnik zostanie opóźniony o 5 sekund po otwarciu drzwi.
- **1 Digit DTMF** : ustawienie 1-cyfrowego kodu DTMF od 0-9 i \*, #.
- **2~4 Digits DTMF** : ustaw kod DTMF zgodnie z ustawieniem opcji DMTP. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli tryb DTMP jest ustawiony jako 3-cyfrowy.

- **Nazwa przekaźnika:** nadaj nazwę przekaźnikowi, aby odróżnić go od innych. Można ją edytować w chmurze SmartPlus i SDMC.

## Ustawienia przekaźnika internetowego

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



Przejdź do interfejsu Web **Phone > Web Relay**. **Adres IP, nazwa użytkownika i hasło są** dostarczane przez producenta przekaźnika internetowego.

**Web Relay**

**Web Relay**

---

Type

IP Address

User Name

Password

Disabled ▾

**Web Relay Action Setting**

---

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

### Konfiguracja parametrów :

- **Typ** : **Web Relay** włącza tę funkcję. **Both** włącza zarówno przekaźnik lokalny, jak i internetowy. Przekaźnik lokalny ma wyższy priorytet.
- **Hasło**: hasło jest uwierzytelniane przez HTTP i można je zdefiniować za pomocą **http get** in Action.
- **Web Relay Action**: wprowadź określone polecenie akcji przekaźnika sieciowego dostarczone przez producenta sieci w celu wykonania różnych działań przez przekaźnik sieciowy. Bez dodawania adresu IP, nazwy użytkownika i hasła można wprowadzić wiele poleceń HTTP w polu akcji przekaźnika internetowego. Zobacz poniższy przykład polecenia HTTP:

a. Jeśli adres IP nie został wprowadzony w polu Adres IP powyżej, należy wpisać pełne polecenie HTTP.

Na przykład **http://admin:admin@192.168.1.2/state.xml?relayState=2** . ( HTTP://@adresIP>/state.xml?relayState=2)

b. Jeśli adres IP został już wprowadzony powyżej, należy wpisać pominięte polecenie HTTP, na przykład **state.xml?relayState=2** .

- **Web Relay Key**: ustawienie opcjonalne. Po wprowadzeniu skonfigurowanego kodu DTMF drzwi można otworzyć tylko za pomocą kodu DTMF i kart RF.

- **Web Relay Extension:** ustawienie opcjonalne. Po wprowadzeniu numeru SIP lub IP urządzenia interkomowego, takiego jak monitor wewnętrzny, tylko to urządzenie może odebrać polecenie akcji przekaźnika internetowego i wyzwolić przekaźnik internetowy za pomocą kodu DTMF.

# Zarządzanie harmonogramem dostępu do drzwi

## Harmonogram przekaźników

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

Przejdź do interfejsu web **Intercom > Relay > Relay Schedule**.

### Konfiguracja parametrów :

- **Identyfikator przekaźnika:** przekaźnik, który ma zostać skonfigurowany.

## 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 **Intercom > Harmonogram**.

### Schedule Setting

---

Schedule Type

Schedule Name

Date Range  -

Day of Week  
 Mon  Tue  Wed  Thur   
 Fri  Sat  Sun  Check All

Date Time  :  -  :

### Schedules Management

---

Index	Schedule ID	Source	Mode	Name	Date	Day of Week	Time	<input type="checkbox"/>
1	1002	Local	Daily	Never	-	-	-	<input type="checkbox"/>
2	1001	Local	Daily	Always	-	-	00:00:00-23:59:59	<input type="checkbox"/>
3								<input type="checkbox"/>
4								<input type="checkbox"/>
5								<input type="checkbox"/>
6								<input type="checkbox"/>
7								<input type="checkbox"/>
8								<input type="checkbox"/>
9								<input type="checkbox"/>
10								<input type="checkbox"/>

Page

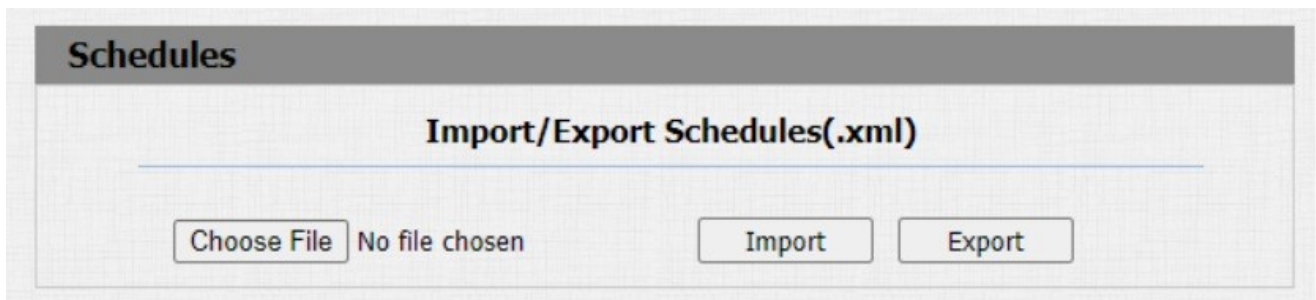
**Konfiguracja parametrów :**

- **Typ harmonogramu:** do wyboru są trzy typy harmonogramów: **dzienny, tygodniowy i normalny**.
- **Zakres dat:** to pole będzie wyświetlane tylko po wybraniu typu **Normalny**.

## 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 **Intercom > Harmonogram > Import/Eksport harmonogramu(.xml)**.



# Konfiguracja odblokowania drzwi

## Konfiguracja karty RF do odblokowywania drzwi

Użytkownicy mogą przesuwając karty RF, aby otwierać drzwi. Zanim będą mogli to zrobić, należy skonfigurować odpowiednie parametry.

## Przypisywanie kart RF do użytkowników

Przejdź do interfejsu **Interkom > Użytkownik**. Kliknij przycisk **Dodaj**.

The screenshot shows the 'User' management interface. At the top, there is a search bar with 'Name/User ID', a dropdown menu set to 'All', and buttons for 'Search', 'Reset', and 'Add'. Below this is a table with the following columns: Index, Source, User ID, Name, RF Card, Floor No., Web Relay, Schedule-Relay, and Edit. The table contains three rows, each with an 'Index' value (1, 2, 3) and an 'Edit' icon.

Index	Source	User ID	Name	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
1								
2								
3								

The screenshot shows the 'User Basic' configuration form. It includes fields for 'User ID' (value: 1), 'Name', and 'Role' (dropdown menu: General User). Below this is the 'RF Card' section, which includes a 'Code' field, an 'Obtain' button, and a '+Add' button.

**Konfiguracja parametrów :**



- **Identyfikator użytkownika:** identyfikator użytkownika składa się maksymalnie z 11 cyfr i nie może być ponownie użyty przez innych użytkowników. Identyfikator użytkownika może zostać wygenerowany automatycznie lub ręcznie.
- **Rola:** wybierz opcję Użytkownik ogólny dla mieszkańców i Administrator dla administratora.
- **Kod:** umieść kartę w obszarze czytnika kart urządzenia i kliknij przycisk **Uzyskaj**, aby uzyskać kod karty.

### Uwaga

- Karta RF o częstotliwości 13,56 MHz i 125 kHz może być stosowana do bramofonu do drzwi dostęp.

Po skonfigurowaniu informacji o użytkowniku i karty RF można skonfigurować kontrolę dostępu w sekcji **Ustawienia dostępu**.

**Access Setting**

Relay  Relay A  Relay B

Web Relay

Floor No.

All Schedules

- 1001:Always
- 1002:Never

Enabled Schedules

- 1001:Always

>>

<<

### Konfiguracja parametrów :

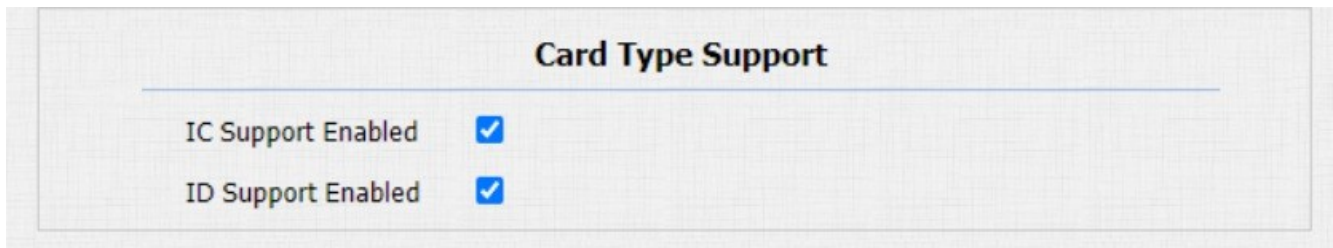
- **Relay (Przełącznik):** wybierz przełącznik lub przełączniki, do których ma zostać
- zastosowany prywatny kod PIN w celu odblokowania drzwi. **Przełącznik internetowy:** wybierz określoną liczbę poleceń akcji przełącznika internetowego skonfigurowanych w interfejsie internetowym.
- **Harmonogram :** wybierz jeden z utworzonych harmonogramów dostępu do drzwi w

prawym polu i przenieś ten, który ma zostać zastosowany do dostępu do drzwi z kodem PIN użytkownika(-ów), do pola po prawej stronie.

## Kontrola kart IC/ID

Włączenie lub wyłączenie typu karty obsługującej urządzenie.

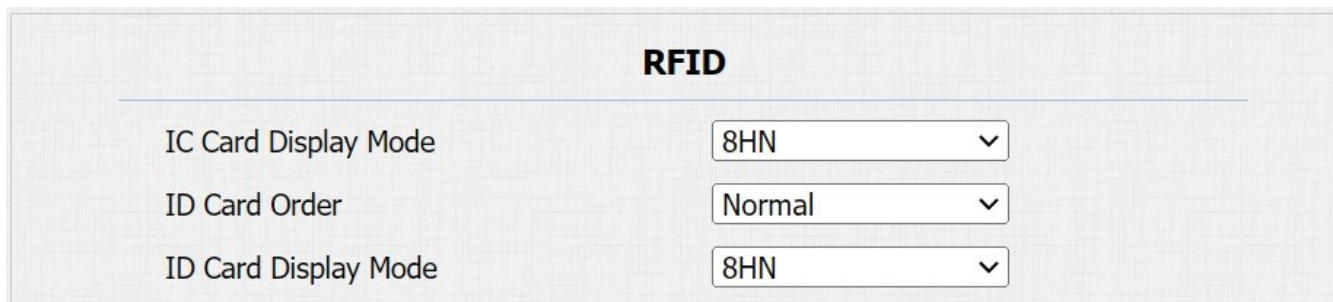
Przejdź do interfejsu web **Intercom > Card Setting > Card Type Support**.



## 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.

Przejdź do interfejsu web **Intercom > Card Setting > RFID**.



### Konfiguracja parametrów :

- **Tryb wyświetlania karty IC:** wybierz format kodu **karty IC** dla dostępu do drzwi spośród siedmiu opcji formatu: **8H10D; 6H3D 5D(W26); 6H8D; 8HN; 8HR; 6H3D 5D-R(W26); 8HR10D** . Domyślnym formatem kodu karty w bramofonie jest 8HN.
- **Kolejność kart ID:** wybór odczytu kart ID w normalnej lub odwróconej kolejności. Konieczne może być wybranie kolejności kart w celu integracji z innymi firmami (np. kontrola dostępu innych firm). można również odwrócić numer karty w celu jej ochrony.
- **Tryb wyświetlania karty ID:** wybór formatu **karty ID** dla dostępu do drzwi spośród siedmiu opcji formatu: **8H10D; 6H3D 5D(W26); 6H8D; 8HN; 8HR; 6H3D 5D- R(W26); 8HR10D** . Domyślnym formatem kodu karty w bramofonie jest 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 **Intercom > Card Setting > Mifare Card Encryption**.



The screenshot shows a web interface for configuring Mifare Card Encryption. The title is "Card Setting" and the sub-section is "Mifare Card Encryption". There are three main settings:

- Enabled:** A checkbox that is currently unchecked.
- Sector / Block:** Two input fields, both containing the number "0", separated by a slash.
- Block Key:** A text input field containing ten asterisks, representing a masked key.

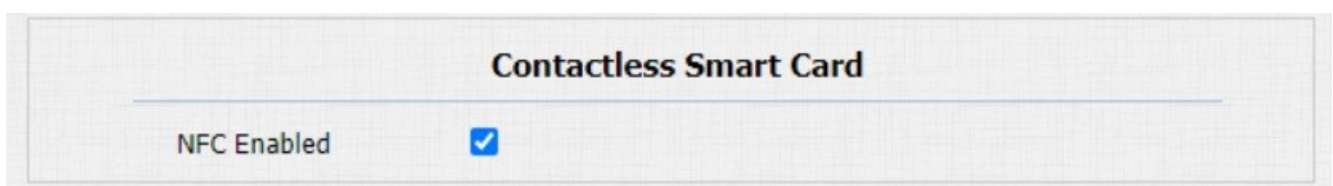
**Konfiguracja parametrów :**

- **Sector/Block :** sektor i blok, w którym numer karty ma zostać zapisany na karcie Mifare. Na przykład numer karty można zapisać w sektorze 3 i bloku 3 na karcie.
- **Block Key:** hasło dostępu do bloku.

## Ustawienia karty NFC

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

Aby włączyć tę funkcję w interfejsie internetowym **Intercom > Card Setting > Contactless Smart Card**.



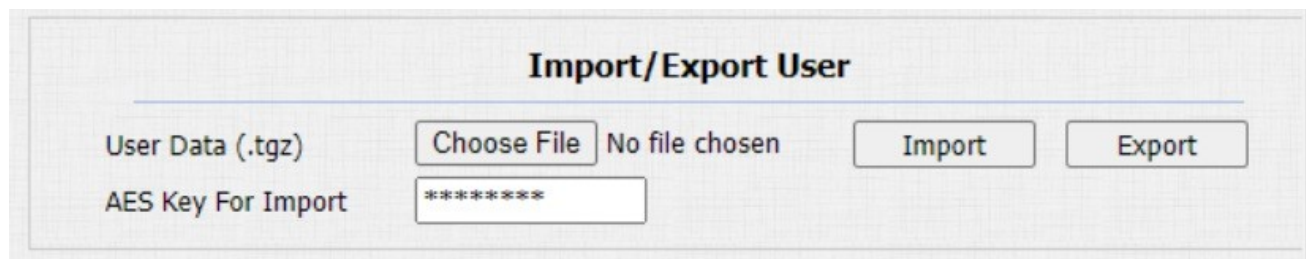
The screenshot shows a web interface for configuring Contactless Smart Card. The title is "Contactless Smart Card". There is one main setting:

- NFC Enabled:** A checkbox that is checked, indicated by a blue checkmark.

## Import i eksport danych użytkownika

Dane użytkowników można eksportować wsadowo, aby zmodyfikować takie informacje, jak kody kart RF. Następnie można je zaimportować do innych urządzeń w celu efektywnego zarządzania użytkownikami.

Przejdź do strony internetowej **Intercom > Interfejs użytkownika**.



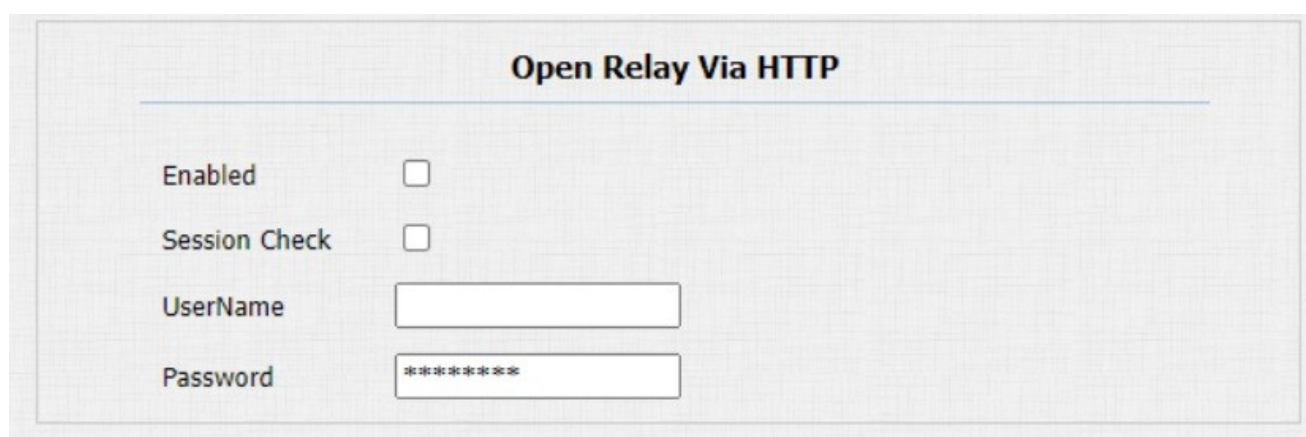
**Konfiguracja parametrów :**

- **AES Key For Import:** wprowadź kod AES przed zaimportowaniem zaszyfowanego AES pliku .tgz do bramofonu.

## Konfiguracja Open Relay przez HTTP dla odblokowywania drzwi

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

Przejdź do interfejsu Web **Intercom > Relay > Open Relay Via HTTP**.



**Konfiguracja parametrów :**

- **Kontrola sesji:** włącz ją, aby chronić bezpieczeństwo transmisji danych.
- **Nazwa użytkownika:** dostosuj nazwę użytkownika jako część polecenia HTTP, na przykład **admin**.
- **Hasło:** dostosuj hasło jako część 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
- dla dostępu do drzwi.  
Urządzenie z włączonym trybem wysokiego bezpieczeństwa obsługuje tylko nowe formaty HTTP. Więcej informacji można znaleźć w sekcji [Bezpieczeństwo](#).

## 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 interfejsu web **Intercom > Input**.

Enabled	<input type="checkbox"/>
Trigger Electrical Level	Low ▾
Action To Execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call <input type="checkbox"/>
HTTP URL	<input type="text"/>
Action Delay	0 (0~300 Sec)
Action Delay Mode	Unconditiona ▾
Execute Relay	None ▾
Door Status	DoorA: High

### Konfiguracja parametrów :

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

- **HTTP URL** : wprowadź adres URL, jeśli wybierzesz HTTP do wykonania akcji.
- **Action Delay (Opóźnienie akcji)**: ustawienie czasu opóźnienia wykonania akcji. Na przykład, jeśli ustawisz czas opóźnienia akcji na 5 sekund, odpowiednie akcje zostaną wykonane 5 sekund po naciśnięciu przycisku.
- **Action Delay Mode (Tryb opóźnienia akcji)**: w przypadku wybrania opcji **Unconditional Execution (Wykonanie bezwarunkowe)** akcja zostanie wykonana po wyzwoleniu wejścia. W przypadku wybrania opcji **Execute If Input Still Triggered**, akcja zostanie wykonana, gdy 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**: skonfiguruj przekaźniki, które będą wyzwalane przez akcje.

## Konfiguracja DTMF do odblokowywania drzwi

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 **Intercom > Relay > Open Relay Via DTMF**.

Relay		
Relay ID	RelayA ▼	RelayB ▼
Type	Default state ▼	Default state ▼
Mode	Monostable ▼	Monostable ▼
Trigger Delay(Sec)	0 ▼	0 ▼
Hold Delay(Sec)	3 ▼	3 ▼
DTMF Mode	1 Digit DTMF ▼	
1 Digit DTMF	0 ▼	1 ▼
2~4 Digits DTMF	010	012
Relay Status	RelayA: Low	RelayB: Low
Relay Name	RelayA	RelayB

## Konfiguracja parametrów :

- **Tryb DTMF:** liczba cyfr DTMF dla kontroli dostępu do drzwi (od 1 do 4 cyfr).  
**1 Digit DTMF :** wybierz kod z zakresu \*0-9 i #, jeśli opcja DTMF jest ustawiona jako 1-cyfrowa.
- **2~4 Digits DTMF :** ustaw kod DTMF zgodnie z ustawieniem **opcji DMTP**. Na przykład, wymagane jest ustawienie 3-cyfrowego kodu DTMF, jeśli **opcja DTMP** jest ustawiona jako 3-cyfrowa.

### Uwaga

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

## Biała lista DTMF

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



## Konfiguracja parametrów :

- **Przypisane uprawnienia dla: All Numbers** zezwala na wszystkie numery dla odblokowania drzwi DTMF; **None** blokuje wszystkie numery dla odblokowania drzwi DTMF; **Only Contacts List** zezwala na numery kontaktowe w telefonie z drzwiami.

## 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 Web Intercom > RTSP > RTSP Basic.



**RTSP**

**RTSP Basic**

---

Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input type="checkbox"/>
Authentication Mode	Basic <span style="font-size: 0.8em;">▼</span>
User Name	admin
Password	*****

### Konfiguracja parametrów :

- **RTSP Authorization Enabled:** po włączeniu wymagane jest wybranie trybu uwierzytelniania RTSP i wprowadzenie nazwy użytkownika i hasła RTSP w celu uwierzytelnienia.
- **Tryb uwierzytelniania RTSP:** wybierz typ uwierzytelniania RTSP pomiędzy **Basic** i **Digest**.

## 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 **Intercom > RTSP > RTSP Stream**.

**RTSP Stream**

---

Audio Enabled	<input checked="" type="checkbox"/>
Video Enabled	<input checked="" type="checkbox"/>
2nd Video Enabled	<input checked="" type="checkbox"/>
Audio Codec	PCMU <span style="font-size: 0.8em;">▼</span>
Video Codec	H.264 <span style="font-size: 0.8em;">▼</span>
2nd Video Codec	H.264 <span style="font-size: 0.8em;">▼</span>

## Konfiguracja parametrów :

- **Video Enabled** : Po włączeniu funkcji RTSP, wideo RTSP jest domyślnie włączone i nie można go modyfikować.
- **2nd Video Enabled** : Bramofony Akuvox obsługują 2 strumienie RTSP, można włączyć drugi.

H.264 And H.265 Video Parameters	
Video Resolution	720P ▼
Video Framerate	30 fps ▼
Video Bitrate	2048 kbps ▼
2nd Video Resolution	VGA ▼
2nd Video Framerate	30 fps ▼
2nd Video Bitrate	512 kbps ▼

## Konfiguracja parametrów :

- **Rozdzielczość wideo**: wybór rozdzielczości wideo spośród pięciu opcji: **CIF, VGA, 4CIF, 720P, 1080P** . Domyślną rozdzielczością wideo jest **720P**, a wideo z bramofonu może nie być wyświetlane na monitorze wewnętrznym, jeśli rozdzielczość jest ustawiona na wyższą niż **720P**.
- **Częstotliwość klatek wideo**: **30 klatek na sekundę** to domyślna częstotliwość klatek wideo.
- **Szybkość transmisji wideo**: wybierz szybkość transmisji wideo spośród sześciu opcji: **64 kbps , 128kbps , 256kbps , 512 kbps , 1024 kbps , 2048 kbps** w zależności od środowiska sieciowego. Domyślna szybkość transmisji wideo to **2048 kb/s**.
- **2. rozdzielczość wideo**: wybór rozdzielczości wideo dla drugiego kanału strumienia wideo. Domyślnie jest to **VGA** .
- **2nd Video Framerate** : wybierz liczbę klatek na sekundę dla drugiego kanału strumienia wideo. Domyślnie jest to **30 kl**.
- **2nd Video Bitrate** : wybierz szybkość transmisji wideo spośród sześciu opcji: **64 kbps , 128kbps , 256kbps , 512 kbps , 1024 kbps , 2048 kbps** w zależności od środowiska sieciowego. Domyślna szybkość transmisji wideo to **512 kb/s**.

## NACK

Potwierdzenie **negatywne ( NACK )** Wskazuje awarię lub błąd w transmisji lub przetwarzaniu danych. Służy do żądania retransmisji lub sygnalizowania niepowodzenia nadawcy w celu zapewnienia integralności danych.

Aby włączyć funkcję NACK, przejdź do interfejsu Web **Phone > Call Feature > Others**.



Others	
Return Code When Refuse	486(Busy Here) ▾
NACK Enabled	<input type="checkbox"/>

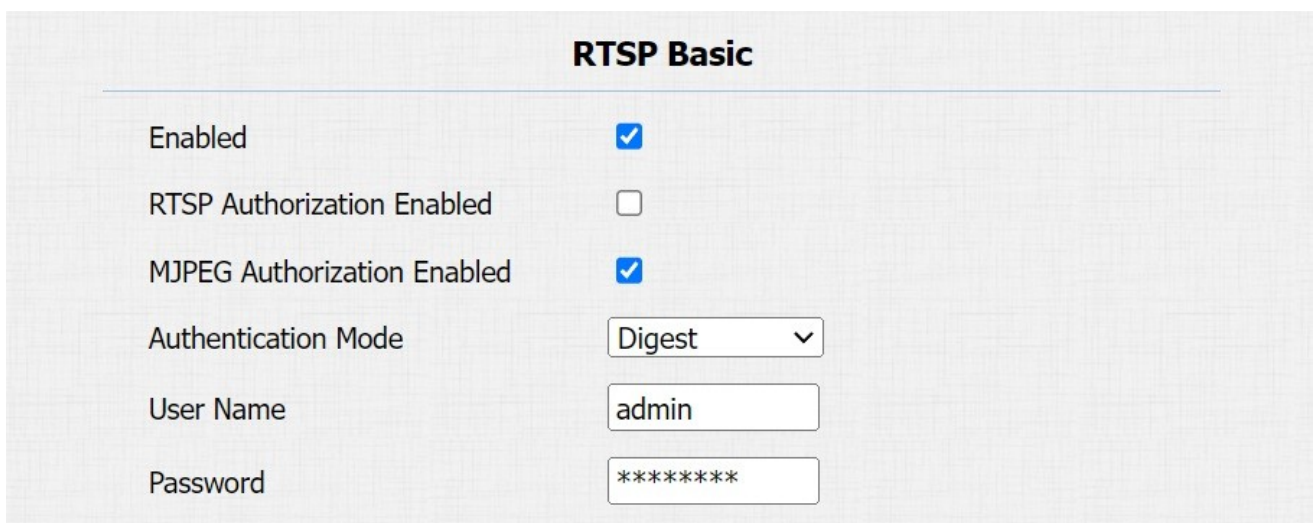
### Konfiguracja parametrów :

- **NACK Enabled:** Może być używany do zapobiegania utracie pakietów danych w słabym środowisku sieciowym, gdy nastąpiło przerwanie i mozaika obrazu wideo.

## 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.

Funkcję Mjpeg można włączyć w interfejsie **Intercom > RTSP > RTSP Basic** i ustawić jakość obrazu w interfejsie **Intercom > RTSP > MJPEG Video Parameters**.



RTSP Basic	
Enabled	<input checked="" type="checkbox"/>
RTSP Authorization Enabled	<input type="checkbox"/>
MJPEG Authorization Enabled	<input checked="" type="checkbox"/>
Authentication Mode	Digest ▾
User Name	admin
Password	*****

<b>MJPEG Video Parameters</b>	
Enabled	<input checked="" type="checkbox"/>
Video Resolution	VGA <input type="button" value="v"/>
Video Framerate	30 fps <input type="button" value="v"/>
Video Quality	90 <input type="button" value="v"/>

#### Konfiguracja parametrów :

- **Rozdzielczość wideo**: wybór rozdzielczości wideo spośród pięciu opcji: **CIF**, **VGA**, **4CIF**, **720P**, **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**.

## 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 web **Intercom > ONVIF**.

<b>Basic Setting</b>	
Discoverable	<input checked="" type="checkbox"/>
User Name	admin <input type="button" value="v"/>
Password	***** <input type="button" value="v"/>

#### Konfiguracja parametrów :

- **Discoverable** : po włączeniu tej funkcji wideo z kamery telefonu może być wyszukiwane przez inne urządzenia.
- **Hasło**: dostosuj hasło do uwierzytelniania. Domyślnie jest to **admin**.

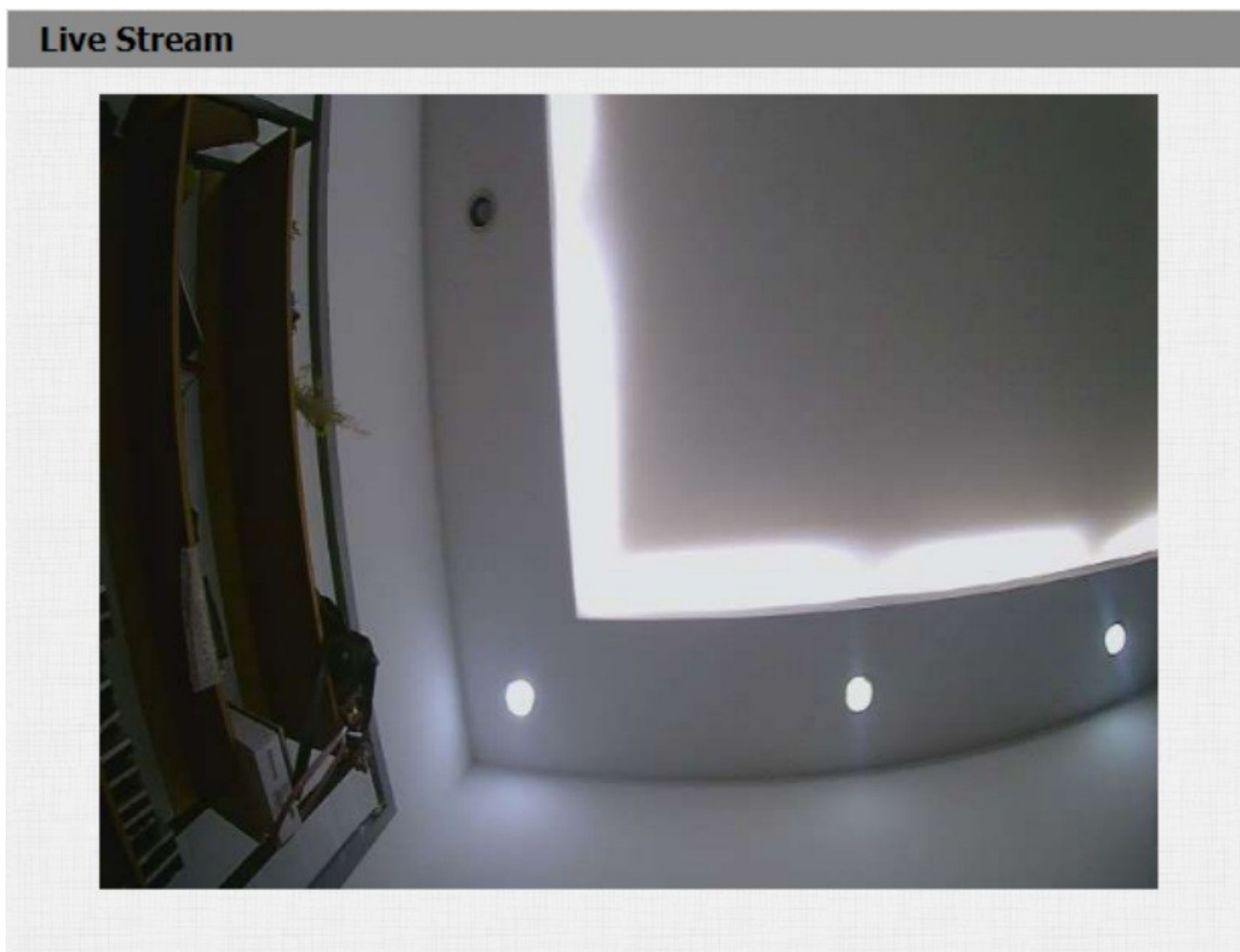
Po zakończeniu ustawień można wprowadzić adres URL ONVIF na urządzeniu zewnętrznym, aby wyświetlić strumień wideo.

Przykładowy format to: **http://IP address: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.

Przejdź do interfejsu web **Intercom > Live Stream**.



# Bezpieczeństwo

## Ustawienie alarmu sabotażowego

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

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

**Tamper Alarm**

---

Enabled	<input type="checkbox"/>
Gravity Sensor Threshold	<input style="width: 150px;" type="text" value="32"/> (0~127)
Trigger Options	<input style="width: 100px;" type="text" value="Only Alarm"/> ▼

**Konfiguracja parametrów :**

- **Próg czujnika** grawitacyjnego: próg czułości czujnika grawitacyjnego. Im niższa wartość, tym łatwiej zostanie uruchomiony alarm sabotażowy. Domyślnie jest to 32.
- **Opcje wyzwalań:** decyduje o tym, co może zostać wyzwolone po uruchomieniu czujnika grawitacyjnego.

## 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.

Przejdź do interfejsu Web **Security > Advanced > Web Server Certificate**.

### Web Server Certificate

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

### Web Server Certificate Upload(.PEM/.DER/.CER)

Choose File No file chosen Submit Cancel

## 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.

Przejdź do interfejsu Web **Security > Advanced > Web Server Certificate**.

### Client Certificate

Index	Issue To	Issuer	Expire Time	<input type="checkbox"/>
1				<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

### Client Certificate Upload(.PEM/.DER/.CER/.CRT)

Index

 No file chosen

Auto ▾

Only Accept Trusted Certificates

Disabled ▾

#### Konfiguracja parametrów :

- **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.
- **Wybierz Plik :** kliknij Wybierz plik przeglądaj dysk lokalny i znajdź żądany certyfikat. (Tylko \*.pem)
- **Tylko akceptuj zaufane certyfikaty:** jeśli wybrano opcję Włączone, dopóki uwierzytelnianie się powiedzie, telefon będzie weryfikował certyfikat serwera na podstawie listy certyfikatów klienta. W przypadku wybrania opcji Disabled (Wyłączone) 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.

Przejdź do interfejsu Web **Security > Advanced > Web Server Certificate**.

### SIP Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	akpbx	cloud.akuvox.com	Sun Sep 10 03:21:52 2049	Delete

### SIP Server Certificate Upload(.PEM/.DER/.CER)

No file chosen

## 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

Przejdź do interfejsu web **Intercom > Motion > Motion Detection Options**.

### Motion Detection Options

Suspicious Moving Object Detection

Disabled ▾

Timing Interval

10 (0~120 Sec)

---

### Motion Detect Time Setting

Day

Mon
  Tue
  Wed
  Thur
   
 Fri
  Sat
  Sun
  Check All

Start Time - End Time

00 ▾ : 00 ▾ - 23 ▾ : 59 ▾

**Konfiguracja parametrów :**

- **Suspicious Moving Object Detection**: wybierz **Disable**, aby wyłączyć wykrywanie ruchu. Wybierz **IR Detection**, aby włączyć detekcję ruchu opartą na czujniku podczerwieni. Wybierz **Video Detection**, aby włączyć detekcję ruchu opartą na wideo podczas monitorowania podejrzanego poruszającego się obiektu.
- **Time Interval**: interwał czasowy wykrywania ruchu. Jeśli ustawisz domyślny interwał czasowy na **10** sekund, wówczas czas wykrywania ruchu będzie wynosił 10 sekund. Zakładając, że ustawimy interwał czasowy na **10** sekund, a pierwszy uchwycony ruch może być postrzegany jako punkt początkowy detekcji ruchu, a jeśli ruch będzie kontynuowany przez 7 sekund w 10-sekundowym interwale, wówczas alarm zostanie wyzwolony po 7 sekundach (pierwszy punkt wyzwolenia), a akcja detekcji ruchu może zostać wyzwolona (wysłanie powiadomienia) w dowolnym miejscu między **7 a 10** sekundami po wykryciu ruchu. Interwał "10" sekund to pełny cykl detekcji ruchu przed rozpoczęciem kolejnego cyklu w tym samym interwale czasowym. Mówiąc dokładniej, pierwszy punkt wyzwolenia można obliczyć jako **interwał czasowy minus trzy**.

W tym samym interfejsie można skonfigurować działania wyzwolane przez detekcję ruchu.

**Action To Execute**

---

Action To Execute    FTP     Email     SIP Call     HTTP

HTTP URL

## Ustawienia powiadomień bezpieczeństwa

### Ustawienia powiadomień e-mail

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

Przejdź do interfejsu web **Intercom > Action > Email Notification**. Powiadomienie e-mail wyświetli przechwycony obraz.

### Email Notification

---

Sender's Email Address	<input type="text"/>
Receiver's Email Address	<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"/>
Email Test	<input type="button" value="Email Test"/>

#### Konfiguracja parametrów :

- **Nazwa użytkownika SMTP:** nazwa użytkownika SMTP jest zwykle taka sama jak adres e-mail nadawcy.
- **Hasło SMTP:** hasło serwera SMTP jest zwykle takie samo jak adres e-mail nadawcy.
- **Email Test:** kliknij Email Test, aby sprawdzić, czy funkcja działa normalnie.

## 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 **Intercom > Action > FTP Notification**.

### FTP Notification

---

FTP Server	<input style="width: 90%;" type="text"/>
FTP User Name	<input style="width: 90%;" type="text"/>
FTP Password	<input style="width: 90%;" type="password" value="*****"/>
FTP Test	<input type="button" value="FTP Test"/>

#### Konfiguracja parametrów :

- **Serwer FTP:** adres (URL) serwera FTP.
- **Test FTP:** uruchom test, aby sprawdzić, czy powiadomienia FTP mogą być wysyłane i odbierane przez serwer FTP.

## Ustawienia powiadomień o połączeniach SIP

Przejdź do interfejsu **Intercom > Action > SIP Call Notification**.

### SIP Call Notification

---

SIP Call Number	<input style="width: 90%;" type="text"/>
SIP Caller Name	<input style="width: 90%;" type="text"/>

## Konfiguracja działań zabezpieczających

### Konfiguracja akcji ruchu

Można skonfigurować działanie wyzwalane przez detekcję ruchu.

Przejdź do interfejsu Web **Intercom > Motion**.

### Action To Execute

---

Action To Execute	FTP <input type="checkbox"/>	Email <input type="checkbox"/>	SIP Call <input type="checkbox"/>	HTTP <input type="checkbox"/>
HTTP URL	<input style="width: 90%;" type="text"/>			

## Konfiguracja akcji wejściowej

Gdy interfejs wejściowy działa, może również wyzwać akcję.

Przejdź do interfejsu web **Intercom > Input**.

Trigger Electrical Level	Low ▾
Action To Execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call <input type="checkbox"/>
HTTP URL	<input type="text"/>

## Powiadomienie o zdarzeniu połączenia

Jeśli chcesz otrzymywać powiadomienia o zdarzeniach związanych z połączeniami (odbieranie połączeń, odbieranie połączeń itp.), przejdź do interfejsu web **Intercom > Basic > Call Event**.

<b>Call Event</b>	
Action To Execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/>
HTTP URL	<input type="text"/>

## 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

Na przykład: <http://192.168.16.118/help.xml?>

mac=\$mac:ip=\$ip:model=\$model:firmware=\$firmware:card\_sn=\$card\_sn

Przejdź do interfejsu Web **Phone > Action URL.**

Action URL	
Active	<input type="checkbox"/>
Make Call	<input type="text"/>
Hang Up	<input type="text"/>
RelayA Triggered	<input type="text"/>
RelayB Triggered	<input type="text"/>
RelayA Closed	<input type="text"/>
RelayB Closed	<input type="text"/>
InputA Triggered	<input type="text"/>
InputB Triggered	<input type="text"/>
InputA Closed	<input type="text"/>
InputB Closed	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<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)	<input type="text" value="Disabled"/>

**Konfiguracja parametrów :**

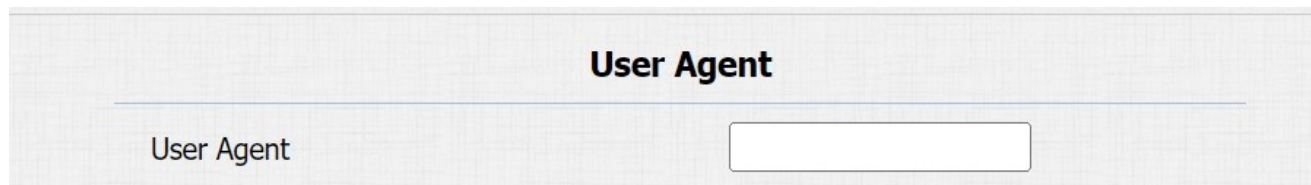
- **Szyfrowanie głosu (SRTP):** wybierz **Wyłączone**, **Opcjonalne** lub **Obowiązkowe** dla SRTP. Jeśli jest to **Opcjonalne** lub **Obowiązkowe**, głos podczas połączenia jest szyfrowany i można pobrać pakiet RTP, aby go wyświetlić.

## Agent użytkownika

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

Jeśli agent użytkownika jest ustawiony na określoną wartość, użytkownicy mogą zobaczyć informacje z PCAP. Jeśli agent użytkownika jest pusty, domyślnie użytkownicy mogą zobaczyć nazwę firmy Akuvox, numer modelu i wersję oprogramowania układowego z PCAP.

Przejdź do interfejsu **Konto internetowe > Zaawansowane > Agent użytkownika.**



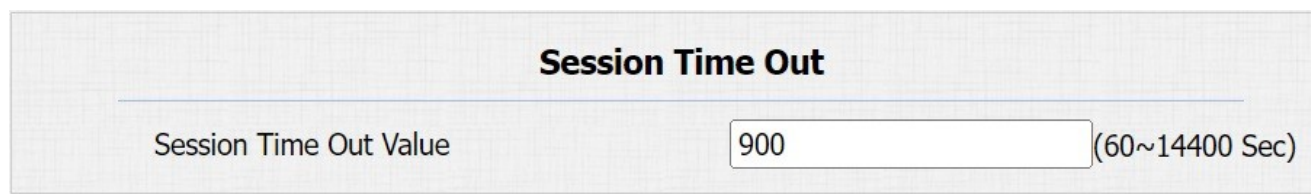
**Konfiguracja parametrów :**

- **Agent użytkownika** : Domyślnie Akuvox.

## 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.

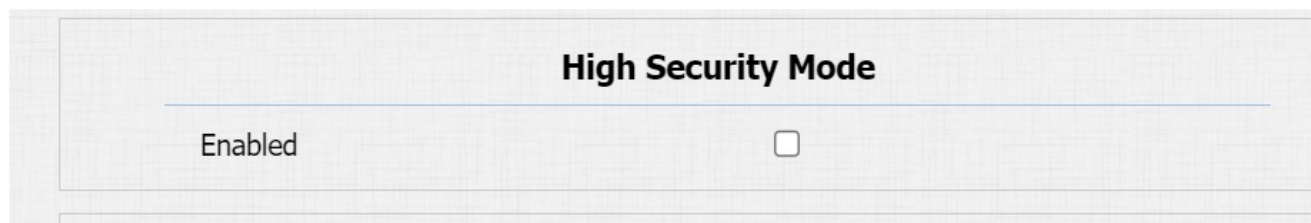
Przejdź do interfejsu sieci **Web Security > Basic > Session Time Out.**



## 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 **Web Security>Basic >High Security Mode.**



**Ważne uwagi**



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

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

-PC Manager: 1.2.0.0

-IP Scanner: 2.2.0.0

-Upgrade Tool: 4.1.0.0

-SDMC: 6.0.0.34

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

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

- I `http://username:password@deviceIP/cgi/OpenDoor?action=OpenDoor&DoorNum=1`
- I `http://deviceIP/cgi/OpenDoor?action=OpenDoor&DoorNum=1`

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

- I `http://deviceIP/cgi/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.

Przejdź do interfejsu Web **Phone > Call Log**.

Index	Type	Date	Time	Local Identity	Name	Number
1	Dialed	2022-02-11	08:37:43	192.168.31.6 @192.168.31.6	192.168.0.4	<a href="#">192.168.0.4@192.168.0.4</a>
2	Dialed	2022-01-19	07:34:06	192.168.31.6 @192.168.31.6	192.168.1.119	<a href="#">192.168.1.119@192.168.1.119</a>
3	Dialed	2022-01-19	07:34:06	192.168.31.6 @192.168.31.6	192.168.1.119:5060	<a href="#">192.168.1.119:5060@192.168.1.119:5060</a>

### Konfiguracja parametrów :

- **Nazwa/Numer:** przeszukiwanie rejestru połączeń według nazwy lub numeru SIP lub IP.

## Dzienniki drzwi

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

Przejdź do interfejsu Web **Phone > Door Log**.

### Door Log

Save Door Log Enabled

Status

Time  -

Name/Code

Index	Name	Code	Type	Date	Time	Status	<input type="checkbox"/>
1	Security..	1	DTMF	2022-02-11	08:38:50	Success	<input type="checkbox"/>
2	Security..	1	DTMF	2022-02-11	08:38:50	Success	<input type="checkbox"/>
3	Security..	1	DTMF	2022-02-11	08:38:50	Success	<input type="checkbox"/>
4	Security..	1	DTMF	2022-02-11	08:38:49	Success	<input type="checkbox"/>
5	Security..	1	DTMF	2022-02-11	08:38:49	Success	<input type="checkbox"/>
6	Security..	1	DTMF	2022-02-11	08:38:49	Success	<input type="checkbox"/>
7	Security..	1	DTMF	2022-02-11	08:38:49	Success	<input type="checkbox"/>
8	Security..	1	DTMF	2022-02-11	08:38:48	Success	<input type="checkbox"/>
9	Security..	1	DTMF	2022-02-11	08:38:48	Success	<input type="checkbox"/>
10	Security..	1	DTMF	2022-02-11	08:38:48	Success	<input type="checkbox"/>
11	Security..	1	DTMF	2022-02-11	08:38:48	Success	<input type="checkbox"/>
12	Security..	1	DTMF	2022-02-11	08:38:48	Success	<input type="checkbox"/>
13	Security..	1	DTMF	2022-02-11	08:38:47	Success	<input type="checkbox"/>
14	Security..	1	DTMF	2022-02-11	08:38:47	Success	<input type="checkbox"/>
15	Security..	1	DTMF	2022-02-11	08:38:47	Success	<input type="checkbox"/>

Page 1

#### Konfiguracja parametrów :

- **Nazwa:** jeśli jest to lokalnie dodany klucz lub karta, zostanie wyświetlona odpowiednia dodana nazwa. Jeśli jest to nieznany klucz lub karta, zostanie wyświetlony komunikat Nieznany.
- **Kod :** w przypadku otwierania drzwi za pomocą kodu PIN wyświetlony zostanie odpowiedni kod PIN. W przypadku otwierania drzwi za pomocą kart RF wyświetlony zostanie odpowiedni numer karty. Jeśli drzwi zostaną otwarte za pomocą polecenia HTTP, będą puste.
- **Eksport:** można wyeksportować dzienniki drzwi w formacie .xml lub .csv.

# Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można zaktualizować w interfejsie internetowym

urządzenia. Przejdź do interfejsu internetowego **Upgrade > Basic**.

Firmware Version	320.30.10.9
Hardware Version	320.0
Upgrade	<input type="button" value="Choose File"/> No file chosen
	Reset: <input type="checkbox"/>
	<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>
Reset To Factory Setting	<input type="button" value="Reset"/>
Reboot	<input type="button" value="Reboot"/>

## Uwaga

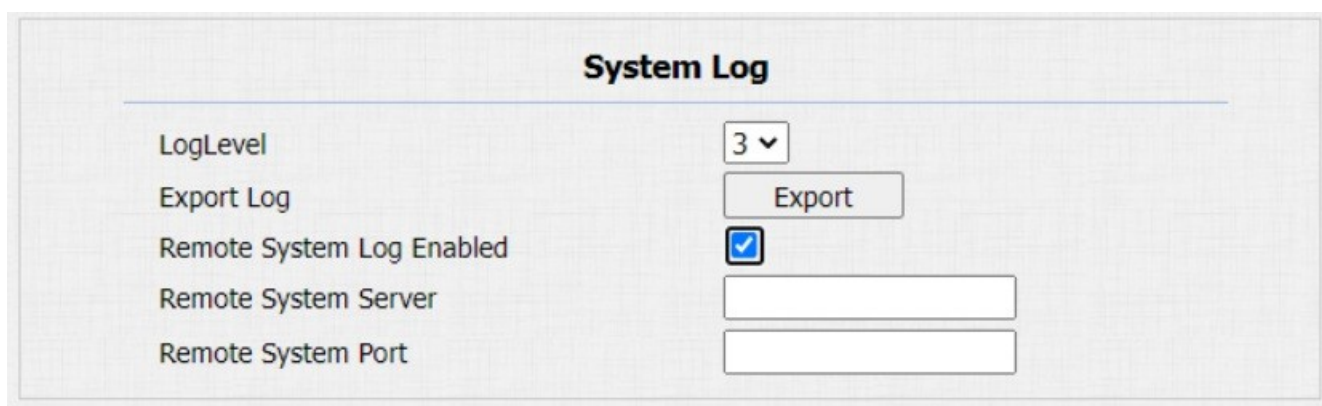
- Plik aktualizacji ma format .rom.
- Nie odłączaj urządzenia od Internetu i zasilania, gdy trwa aktualizacja oprogramowania sprzętowego, w przeciwnym razie może to spowodować awarię aktualizacji lub awarię systemu.

# Debugowanie

## Dziennik systemowy

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Przejdź do interfejsu Web **Upgrade > Advanced > System Log**.



The screenshot shows the 'System Log' configuration page. It features a title 'System Log' at the top. Below the title, there are five configuration items: 'LogLevel' with a dropdown menu set to '3', 'Export Log' with an 'Export' button, 'Remote System Log Enabled' with a checked checkbox, 'Remote System Server' with an empty text input field, and 'Remote System Port' with an empty text input field.

### Konfiguracja parametrów :

- **Log Level (Poziom dziennika):** wybierz poziom dziennika od 1 do 7. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić w celu debugowania. Domyślny poziom dziennika to **3** . Im wyższy poziom, tym bardziej kompletny jest dziennik.
- **Zdalny serwer systemu:** adres zdalnego serwera do odbierania dziennika urządzenia. Adres serwera zdalnego zostanie dostarczony przez pomoc techniczną Akuvox.

## 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 Web **Upgrade > Advanced > Remote Debug Server**.

### Remote Debug Server

Enabled	<input type="checkbox"/>
Connect Status	DisConnected
IP	<input style="width: 150px;" type="text"/>
Port	<input style="width: 150px;" type="text"/> (1024~65535)

## PCAP

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

Przejdź do interfejsu Web **Upgrade > Advanced > PCAP**.

### PCAP

Specific Port	<input style="width: 150px;" type="text"/> (1~65535)
PCAP	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Export"/>
PCAP Auto Refresh	<input type="checkbox"/>
New PCAP	<input type="button" value="Start"/>

### Konfiguracja parametrów :

- **Określony port:** wybierz określony port z zakresu 1-65535, aby przechwytywane były tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.
- **PCAP:** kliknij zakładkę **Start** i zakładkę **Stop**, aby przechwycić określony zakres pakietów danych przed kliknięciem zakładki **Export**, aby wyeksportować pakiety danych do lokalnego komputera.
- **PCAP Auto Refresh:** 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 1 MB.
- **Nowy PCAP:** kliknij **Start**, aby przechwycić większy pakiet danych.

# Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować

do komputera lokalnego. Przejdź do interfejsu **Upgrade > Advanced**

**> Others.**



# Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

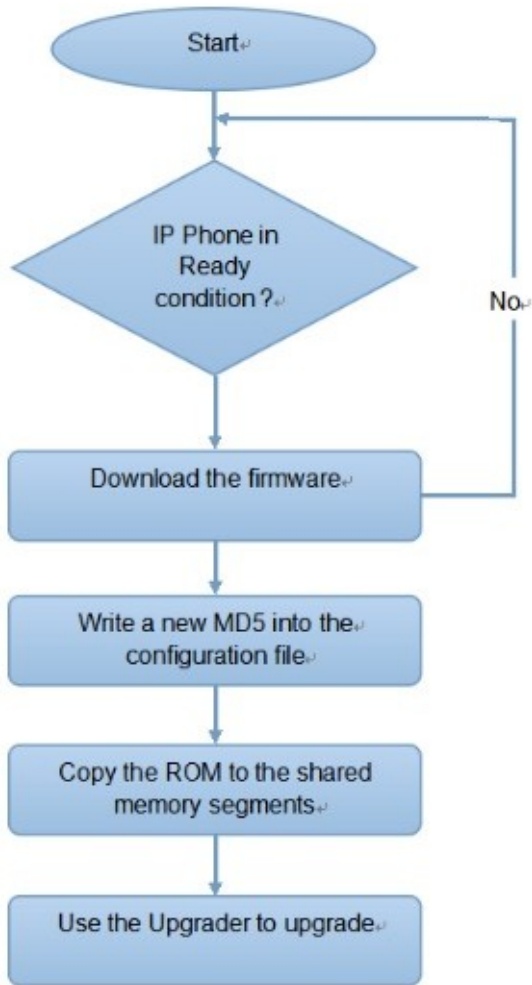
Bramofon można skonfigurować i zaktualizować w interfejsie internetowym za pomocą jednorazowego automatycznego udostępniania i zaplanowanego automatycznego udostępniania za pomocą plików konfiguracyjnych, co pozwala uniknąć konieczności ręcznego konfigurowania poszczególnych ustawień w bramofonie.

## Zasada udostępniania

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

**Zobacz poniższy schemat blokowy:**





## Pliki konfiguracyjne dla automatycznego przydzielania

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

**Poniżej przedstawiono różnicę między tymi dwoma typami plików konfiguracyjnych:**

- **Udostępnianie konfiguracji ogólnej:** plik ogólny jest przechowywany na serwerze, z którego wszystkie powiązane urządzenia będą mogły pobrać ten sam plik konfiguracyjny w celu aktualizacji parametrów na urządzeniach, takich jak cfg.
- **Udostępnianie konfiguracji opartej na MAC:** Pliki konfiguracyjne oparte na MAC są używane do automatycznego udostępniania na określonym urządzeniu, zgodnie z jego unikalnym numerem MAC. Pliki konfiguracyjne 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 udostępniania urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer posiada te dwa typy plików konfiguracyjnych, urządzenia będą najpierw uzyskiwać dostęp do ogólnych plików konfiguracyjnych przed uzyskaniem dostępu do plików konfiguracyjnych opartych na MAC.

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

Aby uzyskać szablon pliku konfiguracji Autop w interfejsie **Upgrade > Advanced > Automatic Autop**.

### Automatic Autop

---

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

## Harmonogram AutoP

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

Przejdź do interfejsu Web **Upgrade > Advanced > Automatic Autop**.

**Konfiguracja parametrów :**

- **Tryb :**

- **Power on (Włącz)** umożliwia urządzeniu wykonywanie automatycznego zatrzymania przy każdym uruchomieniu. **Wielokrotnie** umożliwia urządzeniu wykonywanie 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.

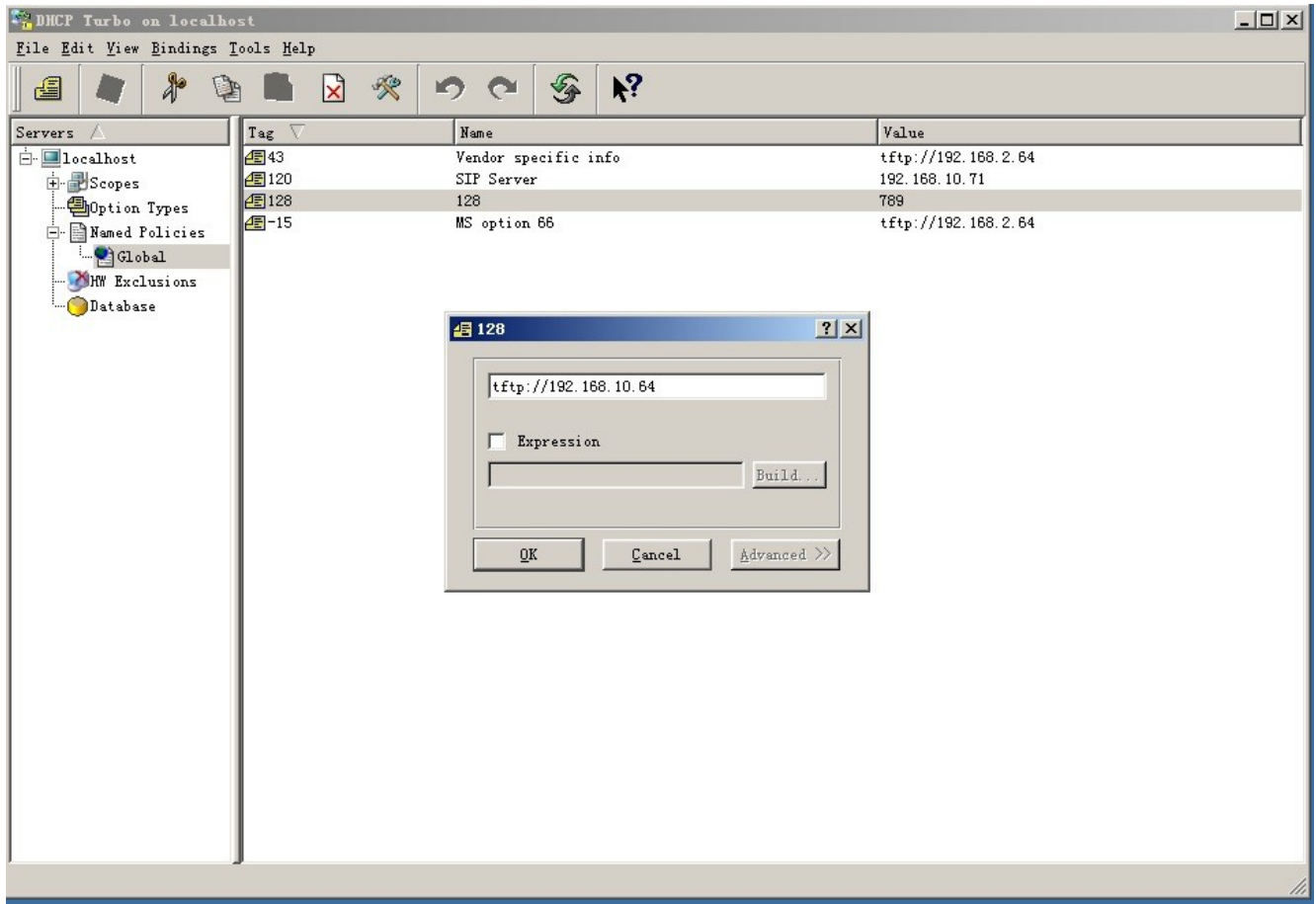
- **Harmonogram:** po wybraniu opcji **Powtarzaj** można skonfigurować harmonogram automatycznego działania.

## Konfiguracja udostępniania DHCP

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

Jeśli chcesz użyć

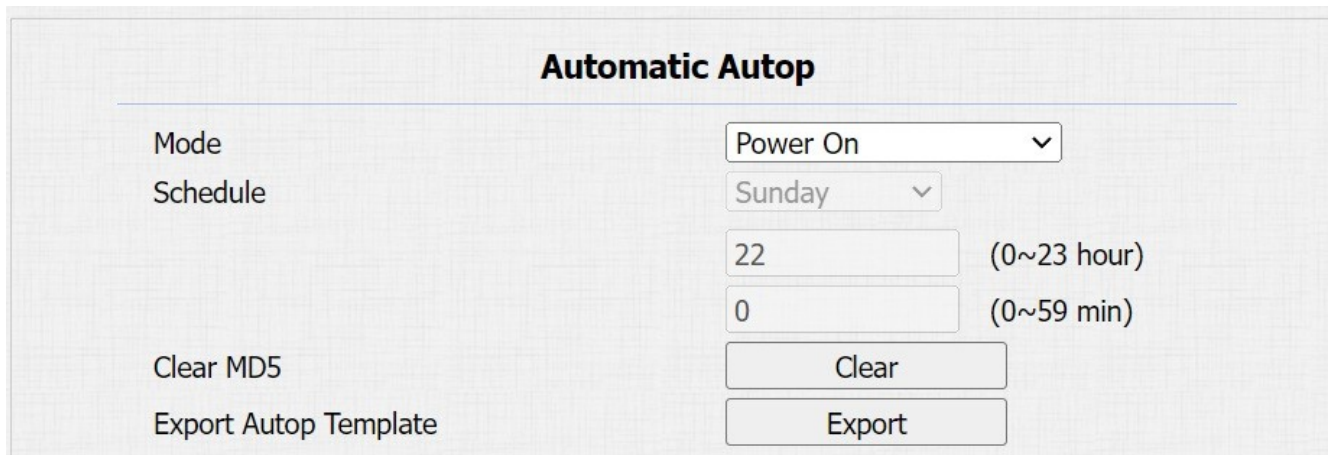
**Opcja niestandardowa** zdefiniowana przez użytkowników z kodami opcji w zakresie 128-255), należy skonfigurować opcję niestandardową DHCP w interfejsie internetowym.



### Uwaga

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

Aby skonfigurować DHCP Autop z trybem Power On i wyeksportować Autop Template w celu edycji konfiguracji. Przejdź do interfejsu Web **Upgrade > Advanced > Automatic Autop**.



Następnie skonfiguruj opcję DHCP w interfejsie **Upgrade > Advanced > DHCP Option**.

## DHCP Option

Custom Option  (128~254)  
(DHCP Option 66/43 is Enabled by Default)

### Konfiguracja parametrów:

- **Opcja niestandardowa:** wprowadź kod DHCP pasujący do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych do konfiguracji lub aktualizacji.
- **Opcja 66 DHCP:** jeśli żadna z powyższych opcji nie jest ustawiona, urządzenie automatycznie użyje Opcji 66 DHCP do uzyskania adresu URL serwera aktualizacji. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 66 z zaktualizowanym adresem URL serwera.
- **Opcja 43 DHCP:** jeśli urządzenie nie otrzyma adresu URL z Opcji 66 DHCP, automatycznie użyje Opcji 43 DHCP. Odbywa się to w ramach oprogramowania i użytkownik nie musi tego określać. Aby to działało, należy skonfigurować serwer DHCP dla opcji 43 z zaktualizowanym adresem URL serwera.

### Uwaga

- Ogólny plik konfiguracyjny udostępniania wsadowego ma format **r000000000xx.cfg** . Na przykładzie X915 r000000000915.cfg (w sumie **10 zer**, podczas gdy plik konfiguracyjny oparty na MAC dla konkretnego urządzenia ma format MAC Address of the device.cfg, na przykład **0C 110504AE5B.cfg** ).
- Wygaszacz ekranu można przesłać za pomocą automatycznej konfiguracji.

## Konfiguracja udostępniania statycznego

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

### Manual Autop

---

URL	<input style="width: 90%;" type="text"/>
User Name	<input style="width: 90%;" type="text"/>
Password	<input style="width: 90%;" type="password" value="*****"/>
Common AES Key	<input style="width: 90%;" type="password" value="*****"/>
AES Key(MAC)	<input style="width: 90%;" type="password" value="*****"/>

#### Konfiguracja parametrów :

- **URL** : skonfiguruj adres serwera TFTP, HTTP, HTTPS, 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 provisioningu opartego na MAC.

#### Uwaga

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

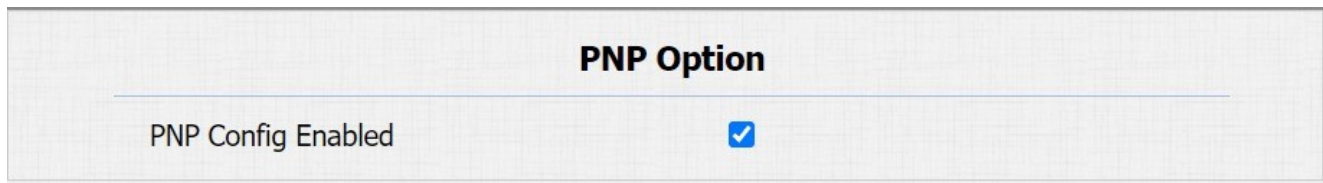
#### Wskazówka

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

## Konfiguracja PNP

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

Przejdź do interfejsu **Upgrade > Advanced > PNP Option**.



# Integracja z urządzeniami innych firm

## Integracja przez Wiegand

Funkcja Wiegand umożliwia bramofonowi Akuvox działanie jako kontroler lub czytnik

kart. Przejdź do interfejsu web **Intercom > Wiegand**.

Wiegand	
Wiegand Display Mode	8HN ▾
Wiegand Card Reader Mode	Wiegand-26 ▾
Wiegand Transfer Mode	Input ▾
Wiegand Input Data Order	Normal ▾
Wiegand Output Basic Data Order	Normal ▾
Wiegand Output Data Order	Normal ▾
Wiegand Output CRC	Enabled ▾

### Konfiguracja parametrów :

- **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 bramofonem a urządzeniem, które ma zostać zintegrowane.
- **Tryb transferu Wiegand :**
  - **Wejście:** gdy bramofon działa jako kontroler, użytkownicy mogą przesunąć kartę RF na czytniku kart innej firmy, aby otworzyć drzwi.
  - **Wyjście:** użytkownicy mogą otworzyć drzwi tylko po wprowadzeniu kodu PIN lub przeciągnięciu karty RF.
  - **Convert To Card No. Output:** gdy użytkownicy są przypisywani za pomocą wielu metod otwierania drzwi, dane muszą zostać przekonwertowane na numer



karty, który jest przypisany do użytkownika trzeciego.  
urządzenie zewnętrzne może zweryfikować.

- **Kolejność danych wejściowych Wiegand**: po wybraniu opcji **Normal** numer karty jest wyświetlany w takiej kolejności, w jakiej został odebrany. Po wybraniu opcji **Reversed** kolejność numerów kart zostanie odwrócona.
- **Kolejność danych wyjściowych Wiegand**: określa kolejność danych wyjściowych Wiegand. Po wybraniu opcji **Normal** dane są wyświetlane w takiej kolejności, w jakiej zostały odebrane. Po wybraniu opcji **Reversed** kolejność bitów danych zostanie odwrócona.
- **Wiegand Output CRC** : jest domyślnie włączony dla kontroli danych Wiegand.  
Wyłączenie go może prowadzić do niepowodzenia integracji z urządzeniami innych firm.

Gdy bramofon działa w trybie wyjścia Wiegand, można skonfigurować format wyjścia kodu PIN Wiegand, który określa sposób przesyłania danych. Format powinien być taki sam, jak format urządzenia zewnętrznego.

### Convert To Wiegand Output

---

PIN

#### Konfiguracja parametrów :

- **PIN**:
  - **8 bitów na cyfrę**: gdy użytkownik naciśnie "1" na klawiaturze, dane binarne zostaną przesłane w 8 bitach "11100001".
  - **4 bity na cyfrę**: gdy użytkownik naciśnie "1" na klawiaturze, dane binarne zostaną przesłane w 4 bitach "0001".
  - **Wszystko na raz**: po wprowadzeniu przez użytkownika całego kodu PIN dane zostaną przesłane zgodnie z trybem czytnika kart Wiegand.

## Integracja przez HTTP API

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

Przejdź do interfejsu Web **Intercom > HTTP API**.

## HTTP API

### HTTP API

---

Enabled	<input checked="" type="checkbox"/>
Authorization Mode	Digest <span style="font-size: 0.8em;">▼</span>
User Name	admin
Password	*****
1st IP	<input type="text"/>
2nd IP	<input type="text"/>
3rd IP	<input type="text"/>
4th IP	<input type="text"/>
5th IP	<input type="text"/>

#### Konfiguracja parametrów :

- **Enabled** : 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, który zostanie wyjaśniony w poniższej tabeli.
- **Nazwa użytkownika**: wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic** i **Digest**. Domyślnie jest to **admin**.
- **Hasło** : wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic** i **Digest**. Domyślnie jest to **admin**.
- **1st IP-5th IP** : wprowadź adres IP urządzeń innych firm, gdy dla integracji wybrano autoryzację **Allowlist**.

Poniższy opis dotyczy trybu uwierzytelniania:

NIE.	Tryb autoryzacji	Opis
1	Brak	Uwierzytelnianie nie jest wymagane dla HTTP API, ponieważ jest ono używane tylko do testów demonstracyjnych.
2	Normalny	Ten tryb jest używany wyłącznie przez programistów Akuvox.
3	Lista dozwolonych	Po wybraniu tego trybu wymagane jest jedynie podanie adresu IP urządzenia zewnętrznego w celu uwierzytelnienia. Biała lista jest odpowiednia do pracy w sieci LAN.
4	Podstawowy	Jeśli wybrano ten tryb, wymagane jest podanie nazwy użytkownika i hasła w celu uwierzytelnienia. W polu Authorization nagłówek 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 nagłówek 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.

## Konfiguracja sterowania windą

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.

Przejdź do interfejsu web **Intercom > Lift Control**.

### Lift Control

---

Lift Control List

### Akuvox EC32 & ZKT Advance Setting

---

Server IP

Port  (1~65535)

Timeout(Sec)  (1~60)

### Akuvox EC32 Action

---

User Name

Password

Floor No. Parameter

URL To Trigger Specific Floor

URL To Trigger All Floors

URL To Close All Floors

#### Konfiguracja parametrów :

- **Life Control List:** wybierz markę sterownika windy.

NIE.	nagłówek	nagłówek
1	Brak	W przypadku wybrania opcji <b>Brak</b> integracja RS485 zostanie wyłączona.
2	Akuvox EC32	Wybierz <b>Akuvox EC 32</b> , jeśli chcesz połączyć urządzenie z kontrolerem windy Akuvox EC33.
3	KEKING	Wybierz <b>KEYKING</b> , jeśli chcesz zintegrować się z kontrolerem windy KEYKING.
4	ZKT	Wybierz <b>ZKT</b> , jeśli chcesz zintegrować się z kontrolerem windy <b>ZKTeco</b> .
5	Chiyu	Wybierz <b>Chiyu</b> , jeśli chcesz zintegrować się z kontrolerem windy <b>Chiyu</b>

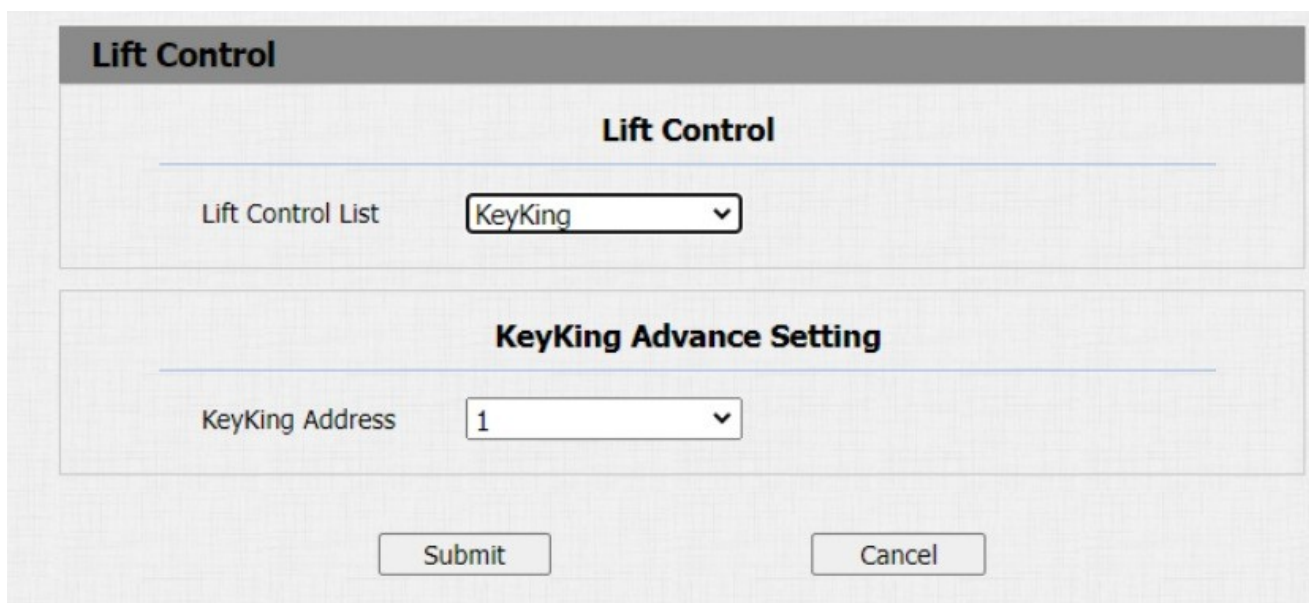
#### Uwaga

- Skontaktuj się z pomocą techniczną Akuvox, jeśli masz jakiegokolwiek pytania dotyczące tryb integracji dowolnego projektu integracji sterownika windy OEM.

## Ustawienia KeyKing

Aby zintegrować kontroler windy KeyKing, należy skonfigurować adres KeyKing uzyskany od dostawcy rozwiązania.

Przejdź do interfejsu web **Intercom > Lift Control** i wybierz KeyKing.



The screenshot displays a web interface for configuring lift control. It features two main sections: 'Lift Control' and 'KeyKing Advance Setting'. In the 'Lift Control' section, there is a dropdown menu labeled 'Lift Control List' with 'KeyKing' selected. The 'KeyKing Advance Setting' section contains a dropdown menu labeled 'KeyKing Address' with the value '1' selected. At the bottom of the interface, there are two buttons: 'Submit' and 'Cancel'.

**Konfiguracja parametrów :**

- **KeyKing Address** : wprowadź adres KeyKing dostarczony przez dostawcę rozwiązania.  
Numer adresu musi być identyczny z numerem adresu na karcie sterownika windy.

## Sterownik windy Akuvox EC32

Przejdź do interfejsu web **Intercom > Lift Control** i wybierz **Akuvox EC 32** .

### Lift Control

Lift Control List Akuvox EC32 ▾

### Akuvox EC32 & ZKT Advance Setting

Server IP

Port  (1~65535)

Timeout(Sec)  (1~60)

### Akuvox EC32 Action

User Name

Password

Floor No. Parameter

URL To Trigger Specific Floor

URL To Trigger All Floors

URL To Close All Floors

#### Konfiguracja parametrów :

- **Timeout (Sec):** wprowadź limit czasu sterownika windy. Na przykład, jeśli ustawisz limit czasu na 30 sekund, użytkownicy muszą nacisnąć przycisk windy odpowiadający piętru, na które jadą, w ciągu 30 sekund, w przeciwnym razie przycisk zostanie ponownie zablokowany, a użytkownicy będą musieli wyjść z windy i zrobić wszystko od nowa.
- **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 Akuvox life control w celu wyzwolenia określonego piętra.

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

## Kontroler windy ZKT

Przejdź do interfejsu web **Intercom > Lift Control** i wybierz **ZKT**.

**Lift Control**

---

Lift Control List

---

**Akuvox EC32 & ZKT Advance Setting**

---

Server IP	<input type="text"/>
Port	<input type="text" value="80"/> (1~65535)
Timeout(Sec)	<input type="text" value="60"/> (1~60)

**Konfiguracja parametrów :**

- **Timeout (Sec):** wprowadź limit czasu sterownika windy. Na przykład, jeśli ustawisz limit czasu na 30 sekund, użytkownicy muszą nacisnąć przycisk windy odpowiadający piętru, na które jadą, w ciągu 30 sekund, w przeciwnym razie przycisk zostanie ponownie zablokowany, a użytkownicy będą musieli wyjść z windy i zrobić wszystko od nowa.

## Kontroler windy Chiyu

Przejdź do **Interkom > Sterowanie windą** i wybierz **Chiyu**.

**Lift Control**

---

Lift Control List

---

## Kontrola mocy wyjściowej

Urządzenie może służyć jako źródło zasilania dla zewnętrznych przekaźników.

Przejdź do interfejsu web **Intercom > Relay > 12V Power Output**.

### 12V Power Output

---

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

Note: '12V Power Output' is disabled under POE mode.

Konfiguracja parametrów:

- **12V Power Output:** wybierz Disabled, aby wyłączyć funkcję wyjścia zasilania; wybierz Always, aby umożliwić kontrolerowi dostępu ciągle zasilanie urządzenia innej firmy. Wybierz Triggered By Open Relay, jeśli chcesz, aby bramofon dostarczał zasilanie do urządzenia innej firmy za pośrednictwem wyjścia 12 i interfejsu GND podczas limitu czasu, gdy stan przekaźników zmieni się z niskiego na wysoki. Wybierz Security Relay A, aby zasilać przekaźnik bezpieczeństwa.



# Modyfikacja hasła

## Modyfikacja hasła interfejsu sieciowego urządzenia

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

Przejdź do interfejsu Web **Security > Basic**.

The image shows two screenshots from a web interface. The top screenshot is titled "Security-Basic" and "Web Password Modify". It features a "User Name" dropdown menu with "admin" selected and a "Change Password" button. Below this is an "Account Status" section with a table:

Account Status	
admin	<input checked="" type="checkbox"/>
user	<input type="checkbox"/>

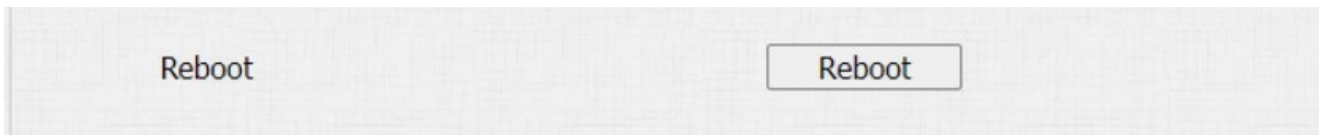
The bottom screenshot is a "Change Password" dialog box. It contains a warning: "The password must be at least eight characters long containing one uppercase letter, one lowercase letter and one digit at least". Below the warning, there are three input fields: "User Name" (with "user" entered), "Old Password", "New Password", and "Confirm Password". At the bottom, there are "Ignore" and "Change" buttons.

# Ponowne uruchamianie i resetowanie systemu

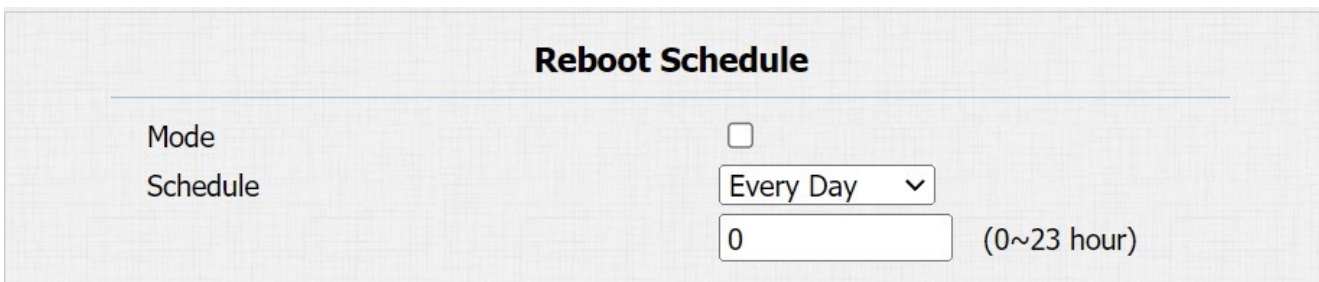
## Reboot

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

Przejdź do interfejsu internetowego **Upgrade > Basic**.



Aby skonfigurować harmonogram, przejdź do interfejsu **Upgrade > Advanced > Reboot Schedule**.



## Reset

Możesz wybrać **Reset To Factory Setting**, jeśli chcesz zresetować urządzenie (usuwając zarówno dane konfiguracyjne, jak i dane użytkownika, takie jak karty RF, dane twarzy itp.)

Można też wybrać **Reset Configuration to Default State (Except Data) Reset**, aby zresetować urządzenie (zachowując dane użytkownika).

Przejdź do interfejsu internetowego **Upgrade > Basic**.

