Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

E12 SERIES DOOR PHONE

Administrator Guide

Dziękujemy za wybranie bramofonu Akuvox z serii E12. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy oprogramowania sprzętowego w wersji 312.30.10.18 i zawiera wszystkie konfiguracje funkcji i właściwości bramofonów E12 i E12S-2. Odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe.

Przegląd produktów

Bezpieczeństwo zapewniane przez kontrolowanie dostępu do budynku i weryfikowanie tożsamości werbalnie i wizualnie jest nieocenione. Bramofony Akuvox z serii E12, zgodne ze standardem SIP, mogą łączyć się z monitorami wewnętrznymi Akuvox w celu zdalnej kontroli dostępu i monitorowania. Użytkownicy mogą wchodzić w interakcje z odwiedzającymi poprzez połączenia audio i wideo, przyznając dostęp. Ten bramofon umożliwia łatwe monitorowanie punktów wejścia, zapewniając większe bezpieczeństwo obiektu i spokój ducha.

Specyfikacja modelu i różnice

Model	E12W	E12S
Kamera	2M pikseli, automatyczne oświetlenie	2M pikseli, automatyczne oświetlenie
Wejście przekaźnika	2	2
Wyjście przekaźnika	1	1
RS485	X	X
Wi Fi	✓	X
Czytnik kart	✓	✓
Mikrofon	1	1
Głośnik	1	1
Bluetooth	✓	✓
Gniazdo kart TF	1	1
Port Wiegand	✓	✓
Alarm sabotażowy	✓	✓
Zasilanie	802.3af Power-over-Ethernet Złącze 12 V DC (jeśli nie jest używane PoE)	802.3af Power-over-Ethernet Złącze 12 V DC (jeśli nie jest używane PoE)

Wprowadzenie do menu konfiguracji

- **Status:** Ta sekcja zawiera podstawowe informacje, takie jak informacje o produkcie, informacje o sieci, informacje o koncie itp.

  Konto: Ta sekcja dotyczy konta SIP, serwera SIP, serwera proxy, typu protokołu transportowego, kodeka audio i wideo, DTMF, licznika sesji itp.

- **Sieć:** Ta sekcja dotyczy głównie ustawień DHCP i statycznego IP, ustawień portów RTP, wdrażania urządzeń itp.

  Interkom: Ta sekcja obejmuje ustawienia interkomu, dzienniki połączeń itp.

- **Nadzór:** Ta sekcja obejmuje wykrywanie ruchu, RTSP, MJPEG, ONVIF i przesyłanie strumieniowe na żywo.
- **Kontrola dostępu:** Ta sekcja obejmuje kontrolę wejścia, przekaźnik, ustawienia karty, prywatny kod PIN, połączenie Wiegand itp.
- **Urządzenie:** Ta sekcja zawiera ustawienia LED, audio i karty SD.

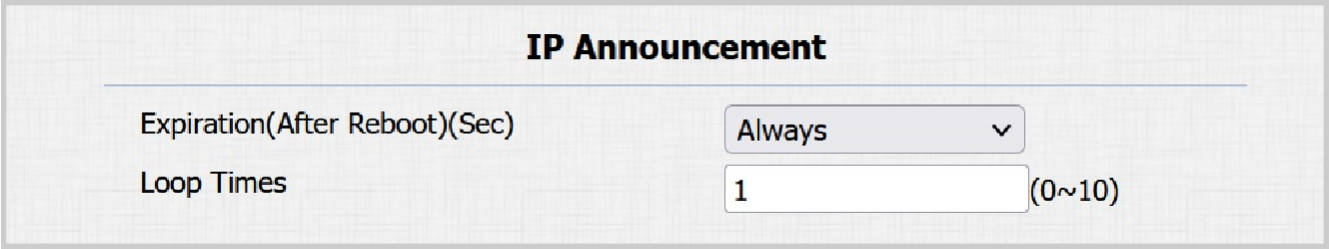
- **Ustawienia:** Ta sekcja zawiera czas i język, ustawienia akcji, ustawienia drzwi i harmonogram kontroli dostępu.
- **Aktualizacja:** Ta sekcja obejmuje aktualizację oprogramowania układowego, resetowanie i ponowne uruchamianie urządzenia, automatyczne dostarczanie plików konfiguracyjnych i diagnostykę błędów.
- **Bezpieczeństwo:** Ta sekcja obejmuje konfigurację trybu wysokiego bezpieczeństwa, modyfikację hasła, alarm sabotażowy, ustawienia HTTP API itp.


Status
Account
Network
Intercom
Surveillance
Access Control
Device
Setting
Upgrade
Security

Dostęp do urządzenia

Uzyskiwanie adresu IP urządzenia

Sprawdź adres IP urządzenia, przytrzymując przycisk. Czasy pętli komunikatów IP można ustawić w interfejsie **Urządzenie > Audio.**

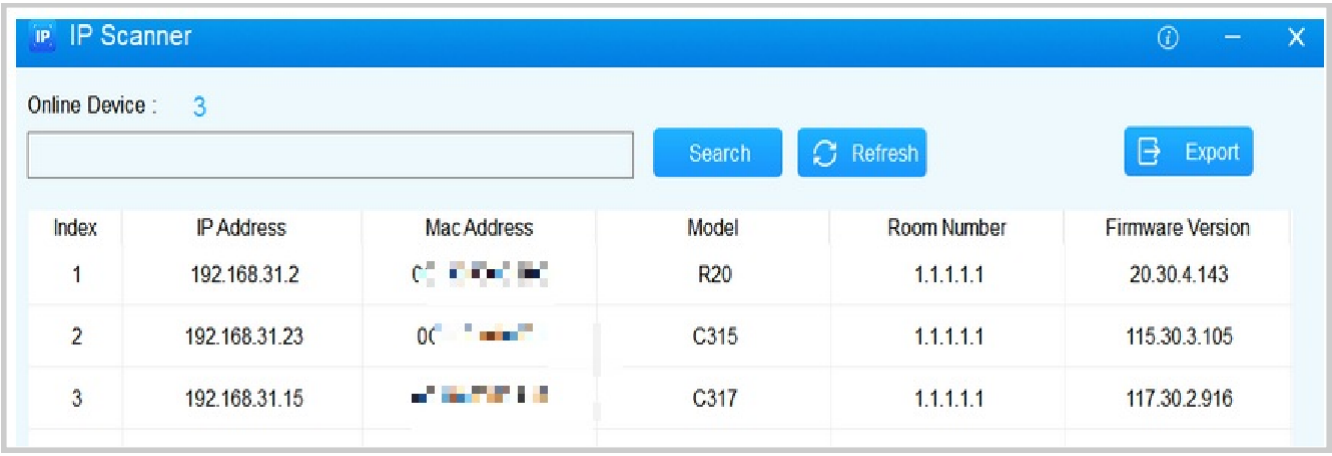


- **Wygaśnięcie (po ponownym uruchomieniu)**

  (Sec): Ustaw limit czasu, w którym użytkownicy powinni przytrzymać przycisk połączenia, aby włączyć komunikat IP po uruchomieniu urządzenia.
  restart. W przypadku wybrania opcji Zawsze, użytkownicy mogą przytrzymać przycisk połączenia w dowolnym momencie, aby wyświetlić komunikat IP po ponownym uruchomieniu urządzenia.

- **Czasy pętli:** Ustaw czas pętli komunikatów IP.

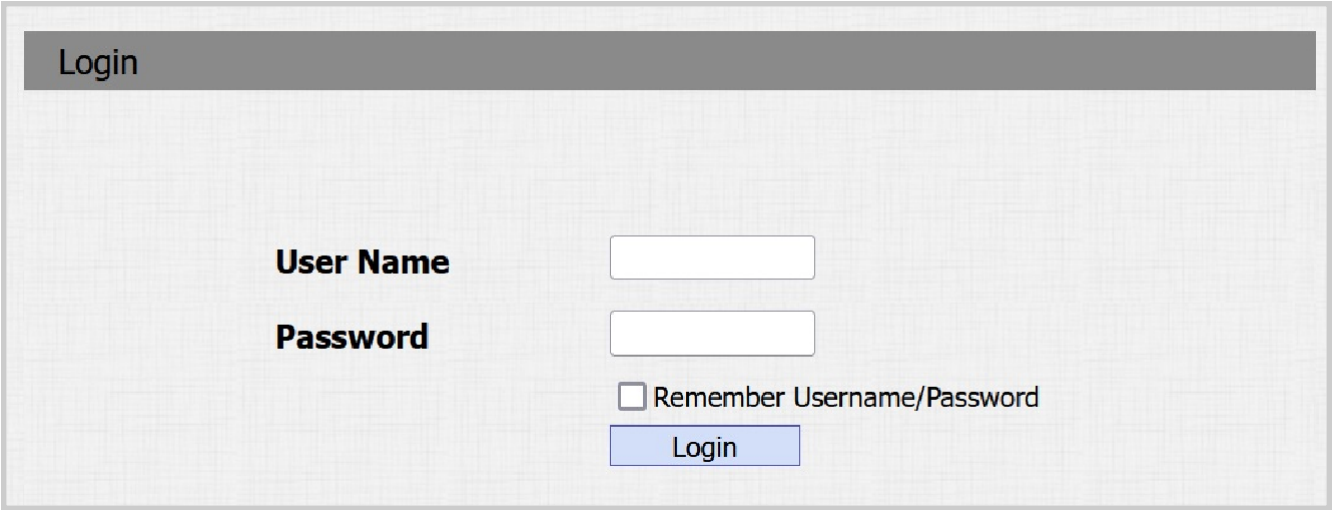
Można też wyszukać adres IP urządzenia za pomocą skanera IP w tej samej sieci LAN. Kliknij przycisk **Odśwież**, aby zaktualizować listę.



Dostęp do ustawień urządzenia

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 wprowadzanych nazwach użytkownika i hasłach.



Ustawienia języka i czasu

Ustawienia języka

Język sieciowy urządzenia można skonfigurować w interfejsie **Ustawienia** sieciowe urządzenia **> Czas/język > Język sieciowy.**

Urządzenie obsługuje następujące języki internetowe:

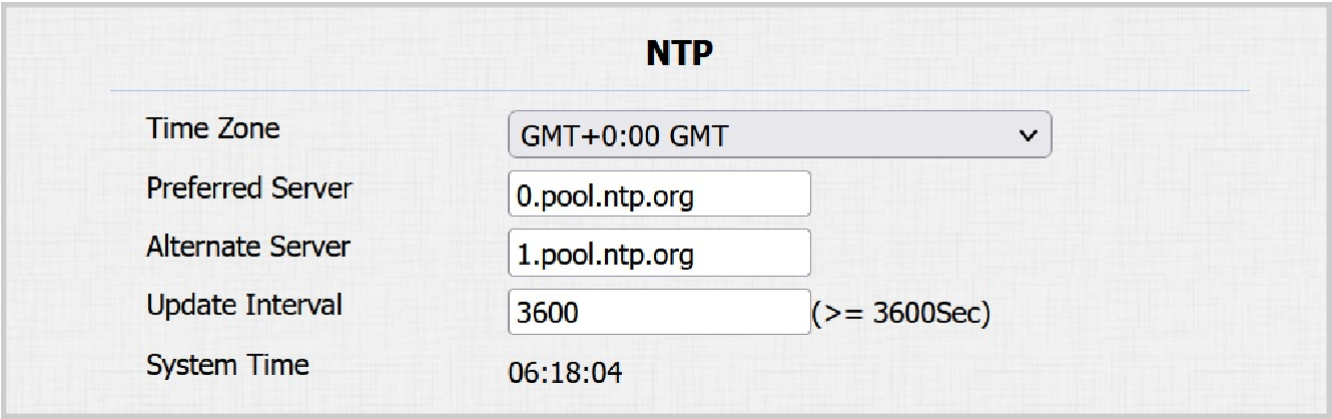
Angielski, rosyjski, portugalski, hiszpański, włoski, holenderski, francuski, niemiecki i turecki.

- **Tryb:** Domyślnym językiem strony jest angielski.

Ustawienie czasu

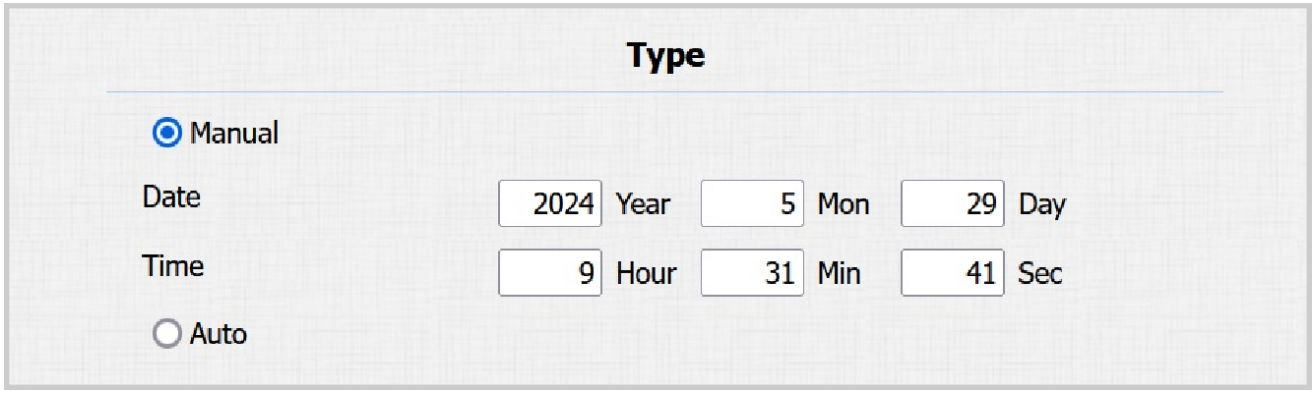
Ustawienia czasu w interfejsie internetowym umożliwiają skonfigurowanie adresu serwera NTP uzyskanego w celu automatycznej synchronizacji czasu i daty. Po wybraniu strefy czasowej urządzenie automatycznie powiadomi serwer NTP o strefie czasowej, aby serwer NTP mógł zsynchronizować ustawienia strefy czasowej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

Skonfiguruj go w interfejsie **Setting > Time/Lang > NTP.**



- **Strefa czasowa**: Wybierz określoną strefę czasową w zależności od tego, gdzie urządzenie jest używane. Domyślną strefą czasową jest GMT+0:00.
- **Preferred Server (Preferowany serwer)**: Wprowadź adres głównego serwera NTP do aktualizacji czasu. Domyślny adres serwera NTP to 0.pool.ntp.org.
- **Alternate Server**: Wprowadź adres zapasowego serwera NPT, gdy podstawowy ulegnie awarii.
- **Interwał aktualizacji**: Ustawienie interwału aktualizacji czasu. Na przykład, jeśli ustawisz 3600s, urządzenie będzie wysyłać żądanie do serwera NPT w celu aktualizacji czasu co 3600 sekund.
- **Czas** systemowy: wyświetla bieżący czas urządzenia.

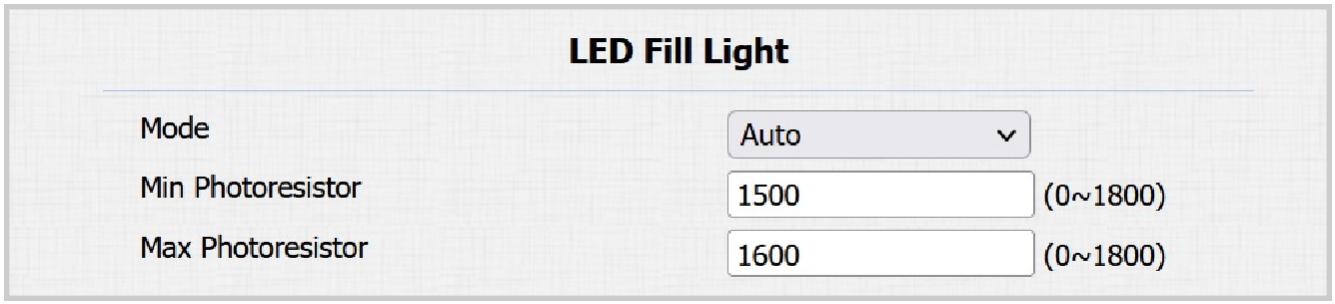
Godzinę można również ustawić ręcznie. Wybierz opcję **Ręcznie i** wprowadź datę i godzinę.



Ustawienie LED

Ustawienie światła LED

Oświetlenie wypełniające LED jest przeznaczone głównie do wzmocnienia światła w nocy lub w ciemnym otoczeniu.
Skonfiguruj go w interfejsie **Device > LED Setting > LED Fill Light.**

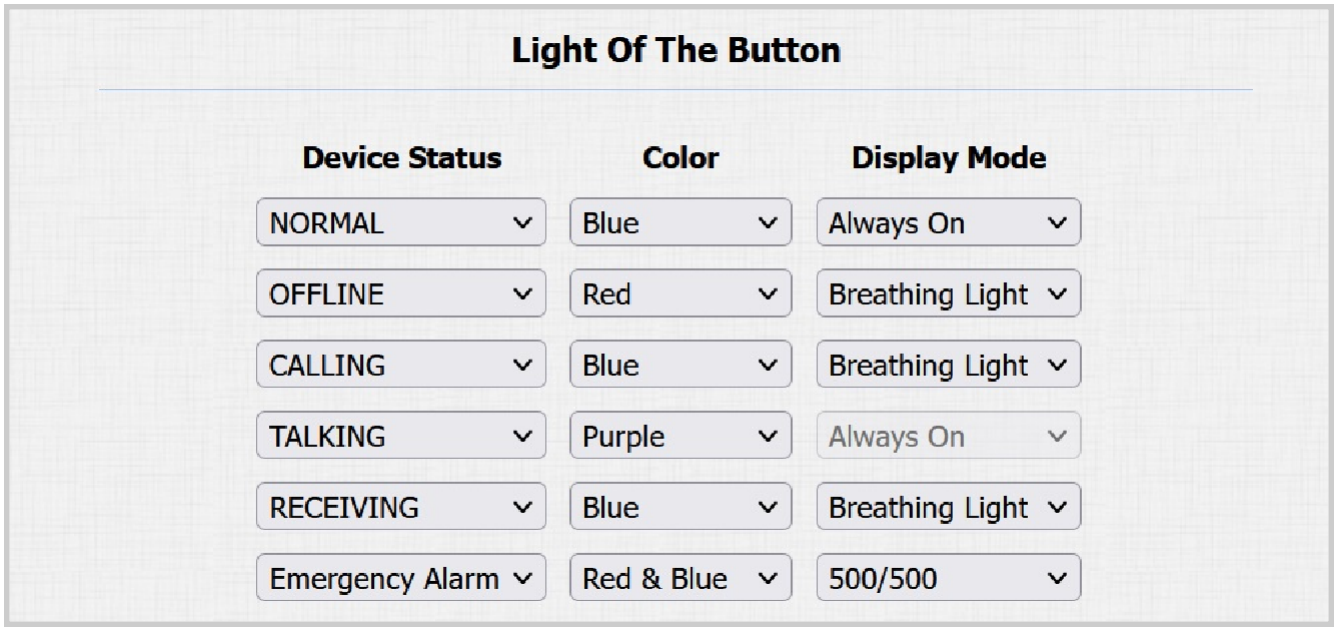


- **Tryb:**
  - Automatycznie włącza światło LED.
  - **Aways OFF** wyłącza światło LED.
  - **Określony czas** włącza diodę LED zgodnie z harmonogramem.
- **Min/Max Photoresistor:** Ustawienie minimalnej i maksymalnej wartości fotorezystora na podstawie aktualnie wykrytej rzeczywistej wartości fotorezystora w celu sterowania włączaniem i wyłączaniem diody LED. Można ustawić maksymalną wartość fotorezystora, aby włączyć diodę LED i minimalną wartość, aby ją wyłączyć.

Stan podświetlenia LED

Regulacja wyświetlacza LED służy do wskazywania zmian podświetlenia przycisku połączenia w różnych stanach. Stan diody LED pozwala użytkownikom zweryfikować aktualny tryb urządzenia.

Skonfiguruj go w interfejsie internetowym **Urządzenie > Ustawienia LED > Światło przycisku.**

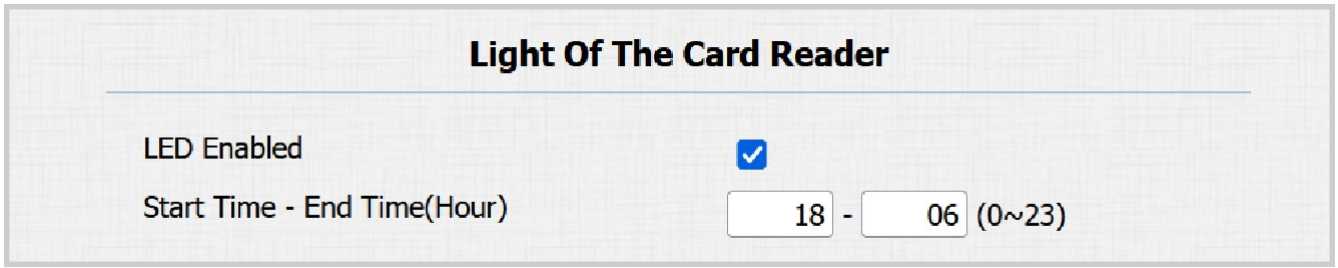


- **Status urządzenia:** Dostępnych jest sześć statusów: Normalny, Offline, Połączenie, Rozmowa, Odbiór i Alarm. Statusu nie można zmienić.
- **Kolor: do** wyboru niebieski, czerwony i fioletowy. Można wybrać czerwony i niebieski (migający na przemian czerwony i niebieski) dla stanu alarmu awaryjnego.
- **Tryb wyświetlania:** Ustaw różne częstotliwości migania.

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.

Skonfiguruj go w menu **Device > LED Setting > Light** interfejsu **czytnika kart.**



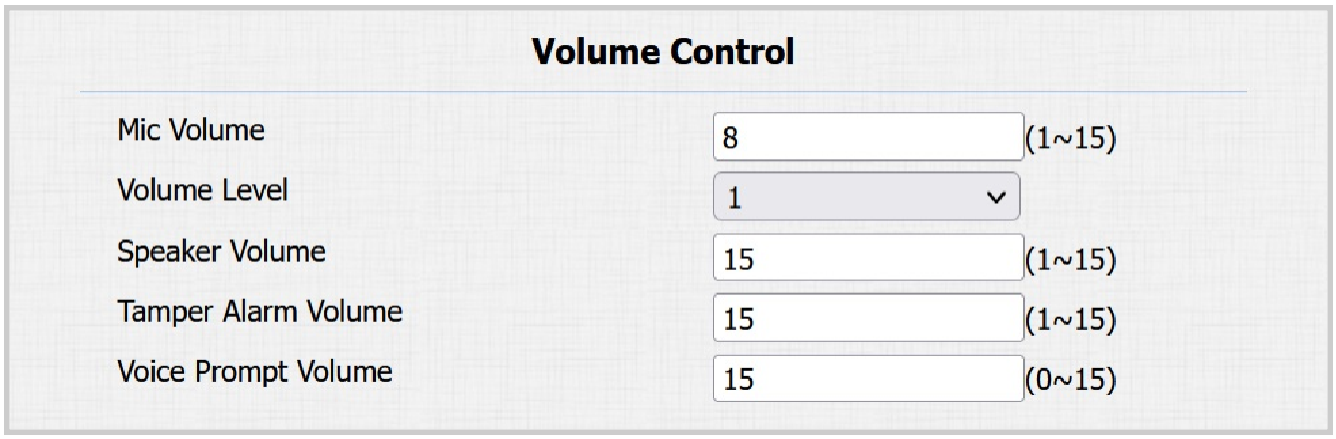
- **Czas rozpoczęcia - Czas zakończenia (godzina):** Ustawianie czasu ważności światła LED. Jeśli czas jest ustawiony w zakresie od 8 do 0 (czas rozpoczęcia - czas zakończenia), światło LED pozostanie włączone od 8:00 do 12:00 przez jeden dzień (24 godziny).

Konfiguracja głośności i tonów

Konfiguracja głośności i tonów obejmuje różne regulatory głośności. Ponadto można przesyłać dźwięki, aby wzbogacić wrażenia użytkownika.

Tony

Aby skonfigurować głośność, przejdź do interfejsu internetowego **Urządzenie > Audio.**

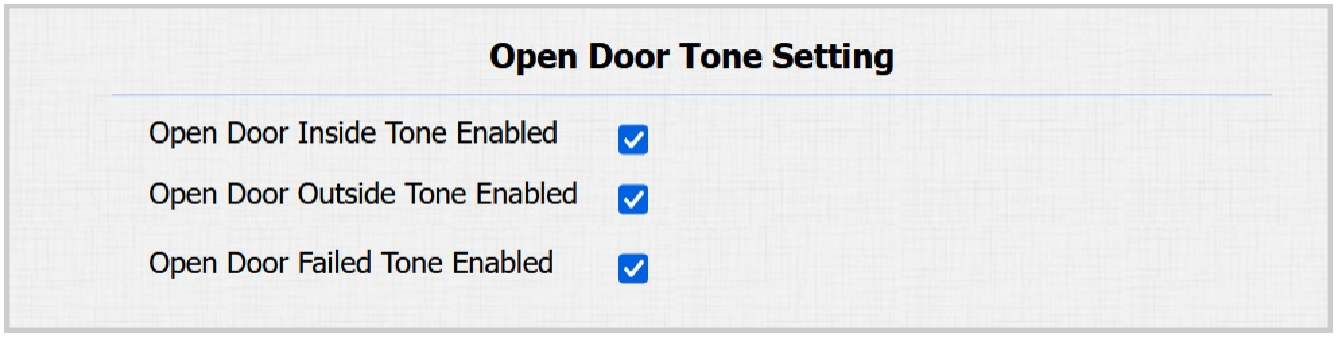


- **Głośność alarmu** sabotażowego: Ustaw głośność, gdy alarm sabotażowy jest wyzwalany.

- **Głośność komunikatów głosowych**: ustawienie głośności komunikatów głosowych.

Dźwięki otwartych drzwi

Dźwięki otwierania drzwi można włączyć lub wyłączyć w interfejsie internetowym **Device > Audio > Open Door Tone Setting.**



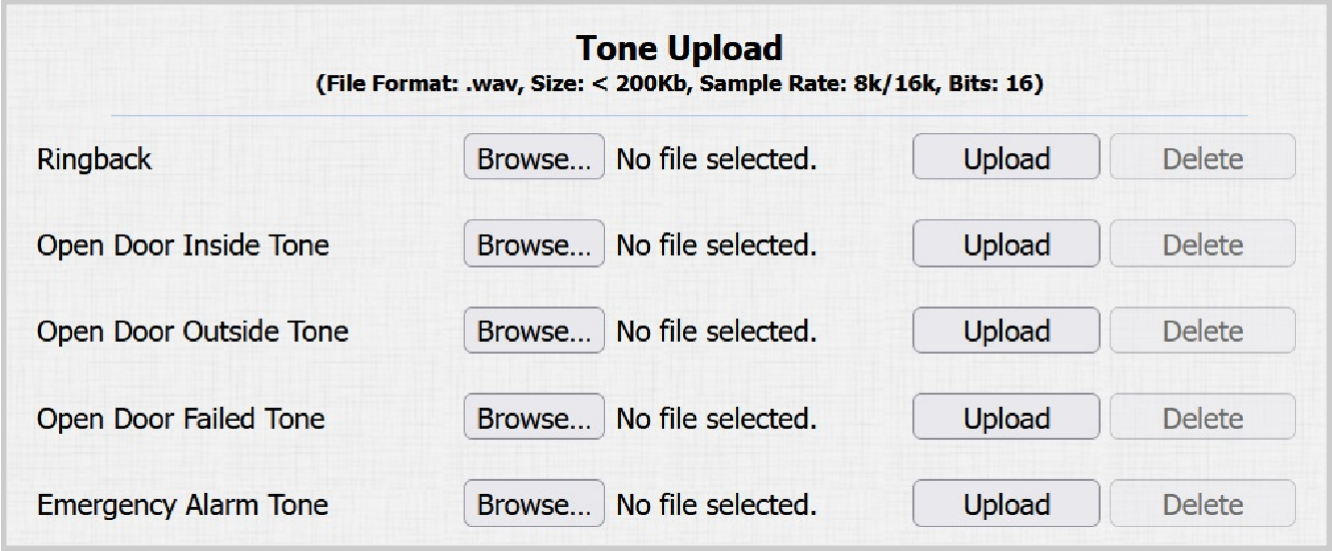
- **Open Door Inside Tone Enabled:** Dźwięk rozlega się, gdy użytkownicy otwierają drzwi, naciskając przycisk wyjścia.

- **Open Door Outside Tone Enabled:** Dźwięk rozlega się, gdy użytkownicy otwierają drzwi za pomocą różnych metod dostępu obsługiwanych przez urządzenie.

- **Open Door Failed Tone Enabled**: Dźwięk rozlega się, gdy otwarcie drzwi nie powiedzie się.

Przesyłanie plików dźwiękowych

Można dostosować dźwięki dzwonka, otwierania drzwi i alarmu awaryjnego.
Prześlij pliki w interfejsie **Device > Audio > Tone Upload.**



- **Ringback:** Dźwięk jest słyszany przez użytkowników dzwoniących na urządzenie.

- **Open Door Inside Tone:** Dźwięk rozlega się, gdy użytkownicy otwierają drzwi, naciskając przycisk wyjścia.
- **Open Door Outside Tone:** Dźwięk rozlega się, gdy użytkownicy otwierają drzwi za pomocą różnych metod dostępu obsługiwanych przez urządzenie.
- **Sygnał dźwiękowy nieudanego otwarcia drzwi:** Sygnał dźwiękowy nieudanego otwarcia drzwi.

- **Dźwięk alarmu awaryjnego:** Dźwięk rozbrzmiewa po uruchomieniu alarmu awaryjnego.

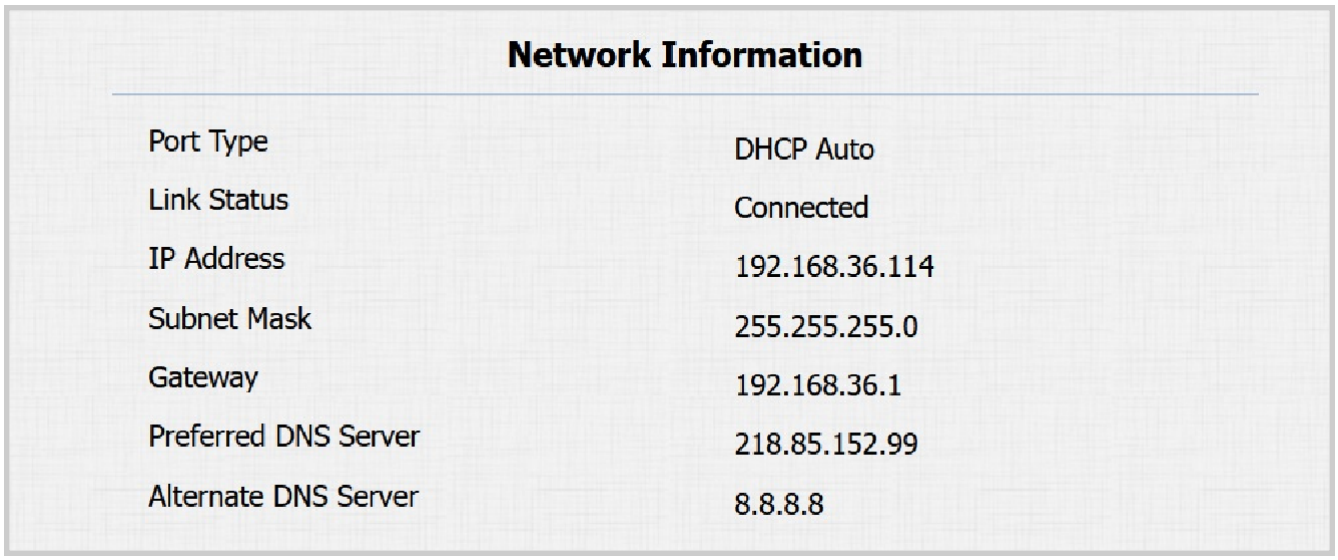
Uwaga

Format pliku: .wav, Rozmiar: < 200Kb, Częstotliwość próbkowania: 8k/16k, Bity: 16.

Ustawienia sieciowe

Status sieci

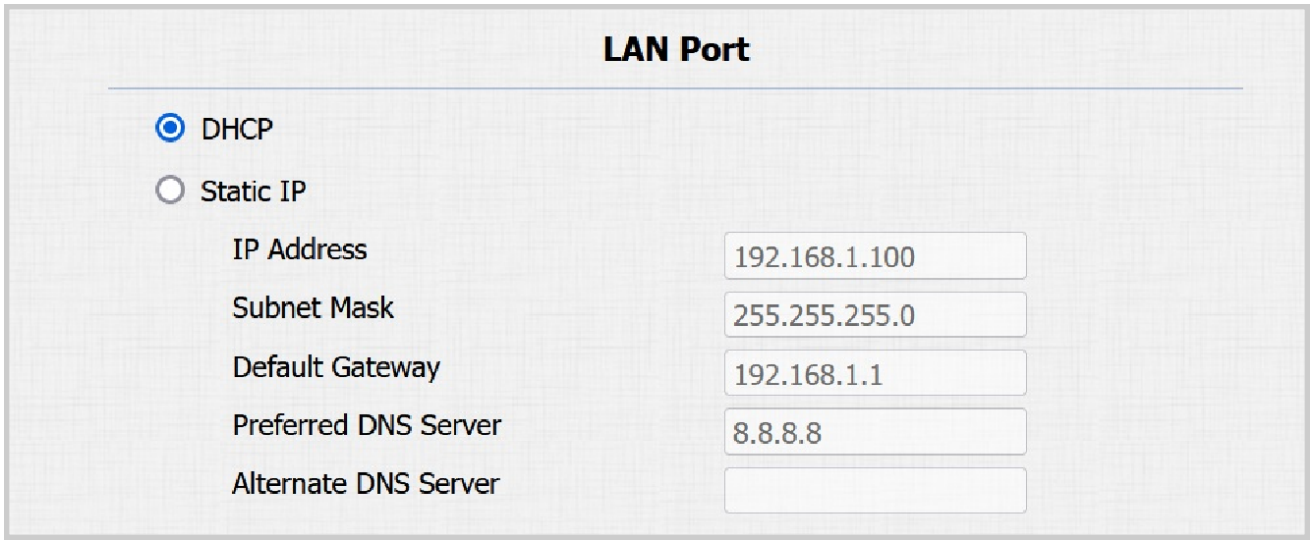
Sprawdź stan sieci w interfejsie Web **Status > Network Information.**



Konfiguracja sieci urządzenia

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

Aby go skonfigurować, przejdź do opcji **Sieć >** Interfejs **podstawowy.**



- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Po wybraniu trybu DHCP urządzenie zostanie automatycznie przypisane przez serwer DHCP z adresem IP, maską podsieci, domyślną bramą i adresem serwera DNS.
- **Statyczne IP**: Po wybraniu trybu statycznego IP, adres IP, maska podsieci, brama domyślna i adres serwera DNS powinny być skonfigurowane zgodnie ze środowiskiem sieciowym.
- **Adres IP**: Ustawienie adresu IP w przypadku wybrania statycznego trybu IP.
- **Maska podsieci**: Ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Brama domyślna**: Ustaw prawidłową bramę zgodnie z adresem IP.
- **Preferowany/alternatywny serwer DNS**: Skonfiguruj preferowany lub alternatywny serwer DNS (Domain Name Server) zgodnie z rzeczywistym środowiskiem sieciowym. Preferowany serwer DNS jest serwerem podstawowym, podczas gdy alternatywny serwer DNS jest serwerem dodatkowym. Serwer dodatkowy służy do tworzenia kopii zapasowych.

Wdrażanie urządzeń w sieci

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

Aby ją skonfigurować, przejdź do interfejsu **Sieć > Zaawansowane > Ustawienia połączenia.**

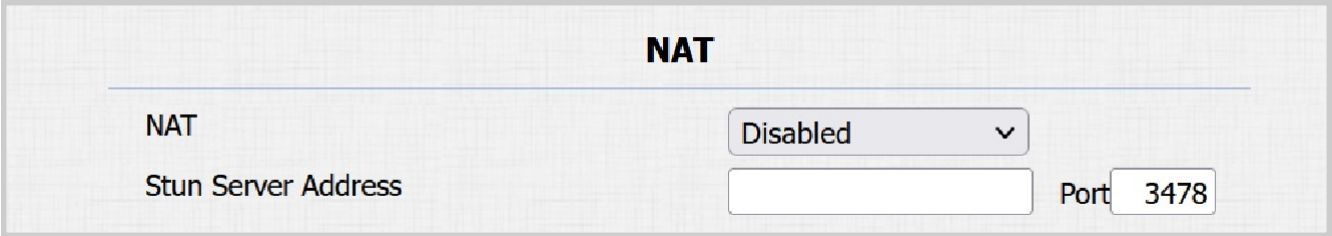
- **Tryb serwera** : Jest ustawiany automatycznie w zależności od połączenia urządzenia z określonym serwerem w sieci, takim jak SDMC, Cloud lub None. **Brak** jest domyślnym ustawieniem fabrycznym wskazującym, że urządzenie nie jest w żadnym typie serwera.

- **Discovery Mode Enabled**: Po włączeniu urządzenie może być wykrywane przez inne urządzenia w sieci. Po wyłączeniu urządzenie będzie ukryte i nie będzie wykrywane przez inne urządzenia.
- **Adres urządzenia** : Określ adres urządzenia, wprowadzając informacje o lokalizacji urządzenia od lewej do prawej: Community (Społeczność), Unit (Jednostka), Stair (Schody), Floor (Piętro) i Room (Pokój) w kolejności.
- **Rozszerzenie urządzenia**: Numer wewnętrzny urządzenia.
- **Lokalizacja urządzenia**: Lokalizacja, w której urządzenie jest zainstalowane i używane.

Ustawienie NAT

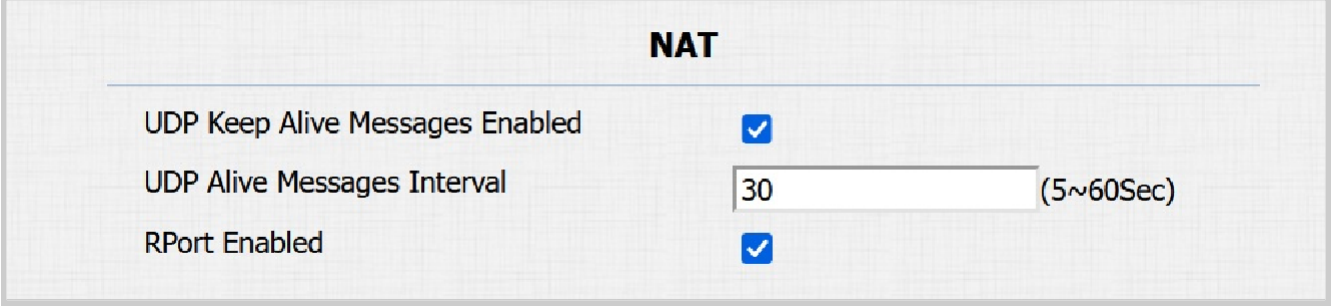
Translacja adresów sieciowych (**NAT**) umożliwia urządzeniom w sieci prywatnej korzystanie z jednego publicznego adresu IP w celu uzyskania dostępu do Internetu lub innych sieci publicznych. NAT zapisuje ograniczone publiczne adresy IP i ukrywa wewnętrzne adresy IP i porty przed światem zewnętrznym.

Aby włączyć NAT, przejdź do **Konto > Podstawowe >** Interfejs **NAT.**



- **Stun Server Address**: Wprowadź adres serwera, gdy urządzenie znajduje się w sieci rozległej (WAN).
- **Port**: port serwera.

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



- **UDP Keep Alive Messages Enabled:** Jeśli opcja ta jest włączona, urządzenie wyśle

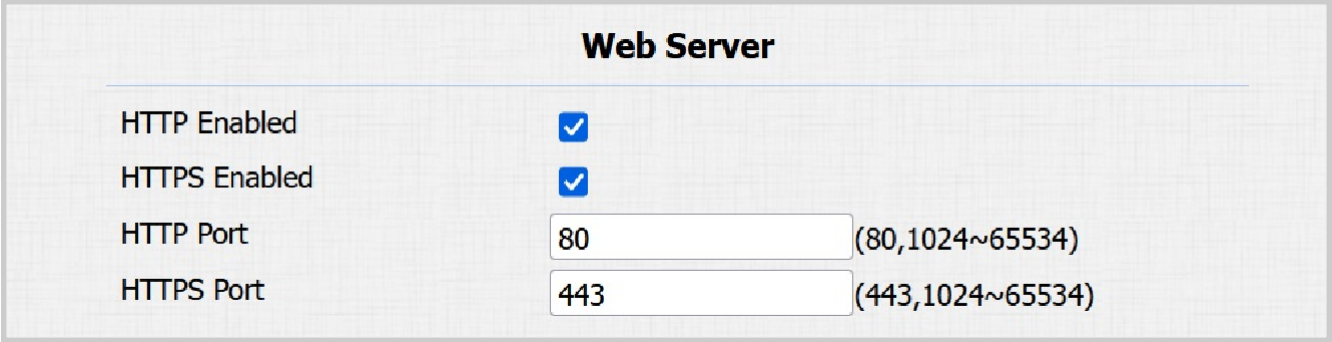
wiadomość do serwera SIP, który rozpozna, czy urządzenie jest w trybie online.

- **UDP Alive Messages Interval:** Ustawienie interwału wysyłania wiadomości w zakresie 5-60 sekund. Domyślnie jest to 30 sekund.
- **RPort**: Włącz RPort, gdy serwer SIP znajduje się w sieci WAN.

Ustawienia HTTP sieci Web urządzenia

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

Skonfiguruj go w interfejsie **Sieć > Zaawansowane > Serwer WWW.**



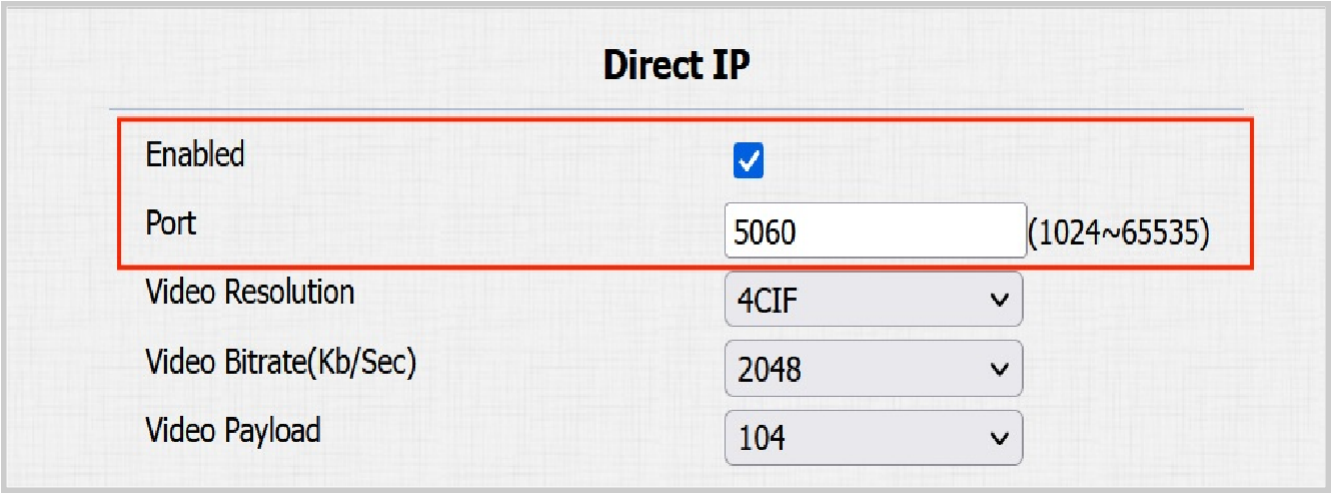
- **HTTP/HTTPS Enabled**: Protokoły HTTP i HTTPS są domyślnie włączone.
- **Port HTTP/HTTPS**: Określa port serwera WWW umożliwiający dostęp do interfejsu WWW urządzenia za pośrednictwem protokołu HTTP/HTTPS.

Konfiguracja połączeń interkomowych

Konfiguracja połączeń IP

Połączenie IP to bezpośrednie połączenie między dwoma urządzeniami interkomowymi przy użyciu ich adresów IP, bez serwera lub centrali PBX. Połączenia IP działają, gdy urządzenia znajdują się w tej samej sieci.

Włącz Direct IP w interfejsie **Intercom > Basic > Direct IP.**



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

Konfiguracja połączeń SIP

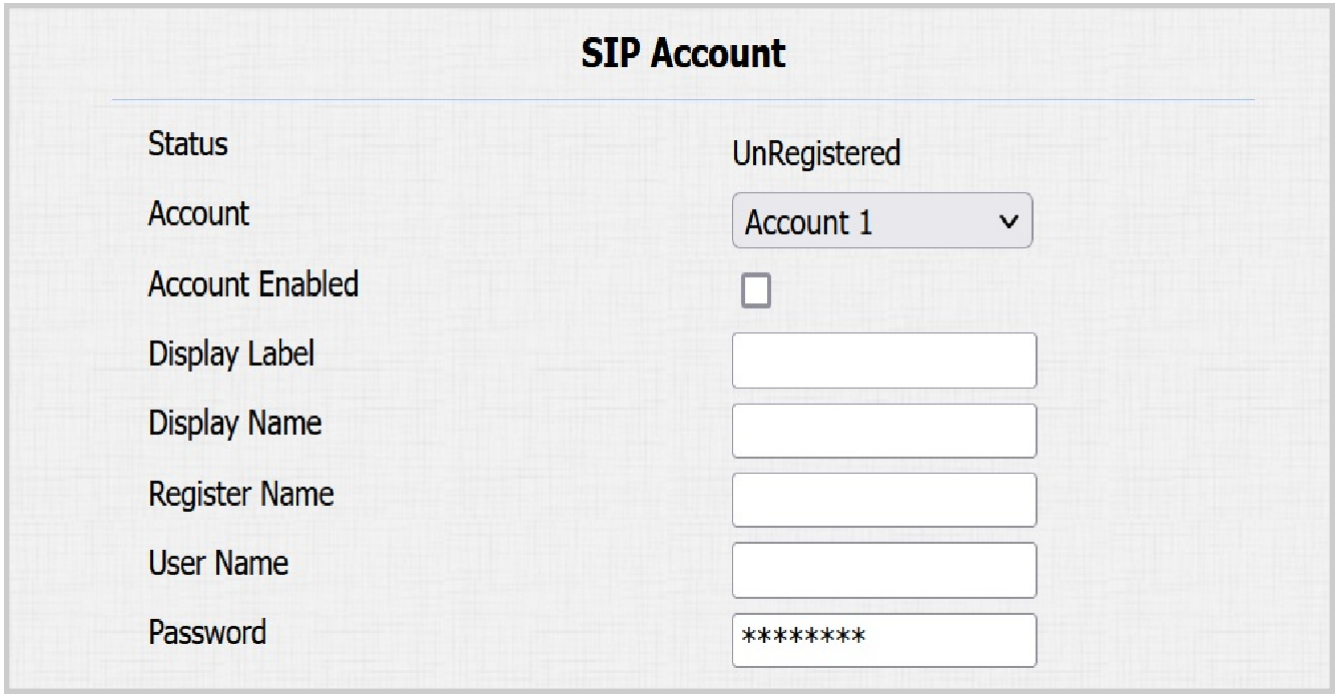
Session Initiation Protocol (**SIP**) to protokół transmisji sygnałów używany do inicjowania, utrzymywania i kończenia połączeń.

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.

Aby ją skonfigurować, przejdź do strony internetowej **Konto > Podstawowe >** Interfejs **konta SIP.**



- **Status:** Wskazuje, czy konto SIP jest zarejestrowane, czy nie.

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

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

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

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

> Wskazówka
>
> Informacje na temat konfigurowania połączeń kontaktowych i planu wybierania numerów można znaleźć tutaj.

- **Etykieta wyświetlacza:** Etykieta urządzenia.

- **Wyświetlana nazwa:** Oznaczenie konta 1 lub 2 ma być wyświetlane na samym urządzeniu na ekranie wywoływania.

- **Nazwa rejestru:** Taka sama jak nazwa użytkownika z serwera PBX.

- **Nazwa użytkownika:** Taka sama jak nazwa użytkownika z serwera PBX do

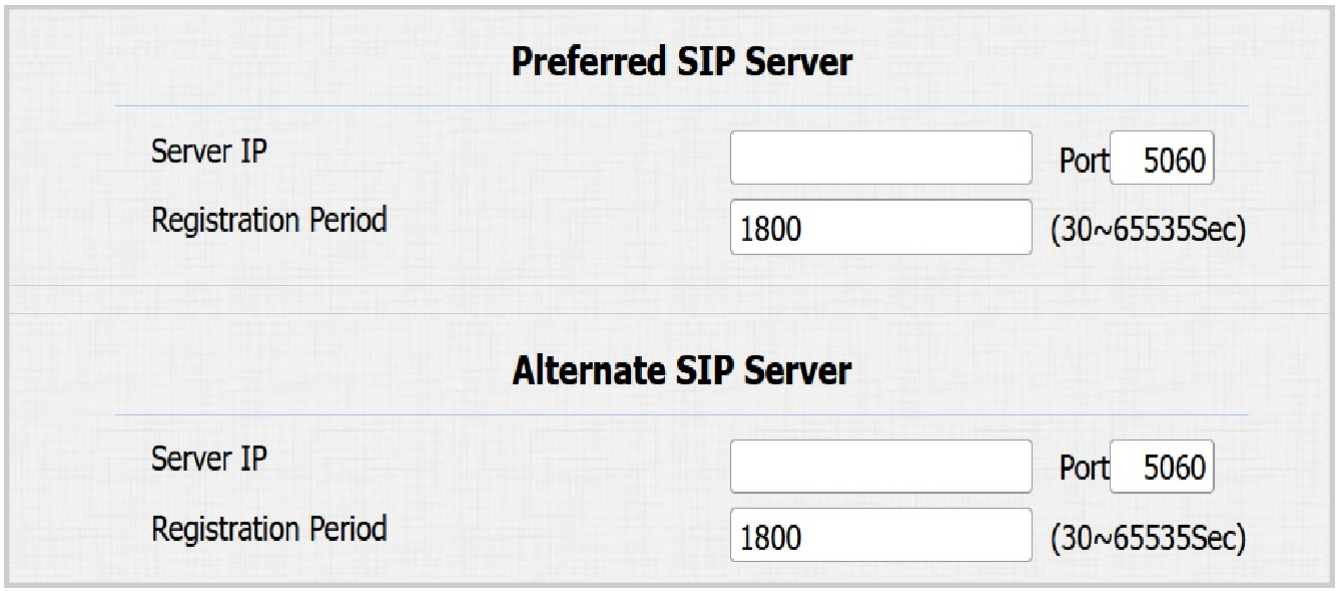
uwierzytelniania.

- **Hasło:** takie samo jak hasło z serwera PBX do uwierzytelniania.

Konfiguracja serwera SIP

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

Aby ją skonfigurować, przejdź do sekcji **Konto** internetowe **>** Interfejs **podstawowy.**



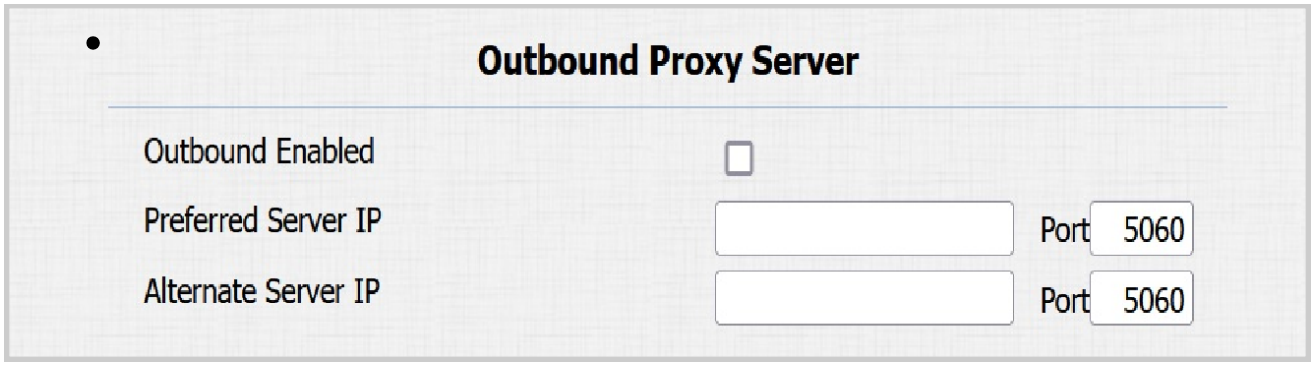
- **IP serwera**: Wprowadź adres IP serwera lub jego nazwę domeny.
- **Port**: Określa port serwera SIP do transmisji danych.
- **Okres rejestracji** : Określa limit czasu dla rejestracji konta SIP. Automatyczna ponowna rejestracja rozpocznie się, jeśli rejestracja konta nie powiedzie się w określonym czasie.

Serwer proxy połączeń wychodzących

Wychodzący serwer proxy służy do odbierania wszystkich inicjujących komunikatów żądań i kierowania ich do wyznaczonego serwera SIP w celu ustanowienia sesji połączenia za pośrednictwem transmisji danych opartej na portach.

Aby ją skonfigurować, przejdź do **Konto** internetowe **> Podstawowe >** Interfejs **serwera proxy**

połączeń wychodzących.

- 

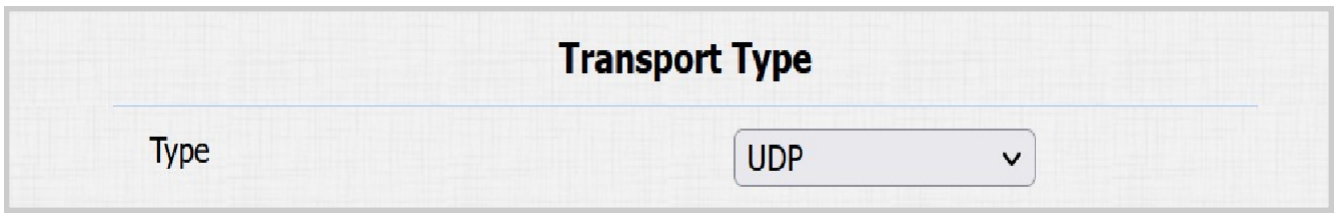
Preferred Server IP: Wprowadź adres IP serwera proxy SIP.

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

Typ transmisji danych

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

Aby ją skonfigurować, przejdź do interfejsu **Konto** internetowe **> Podstawowe > Typ transportu.**



- **UDP:** Niezawodny, ale bardzo wydajny protokół warstwy transportowej. Jest to domyślny protokół transportowy.
- **TCP:** Mniej wydajny, ale niezawodny protokół warstwy transportowej.
- **TLS**: Szyfrowany i zabezpieczony protokół warstwy transportowej. Wybierz tę opcję, jeśli chcesz szyfrować wiadomości SIP w celu zwiększenia bezpieczeństwa lub jeśli serwer

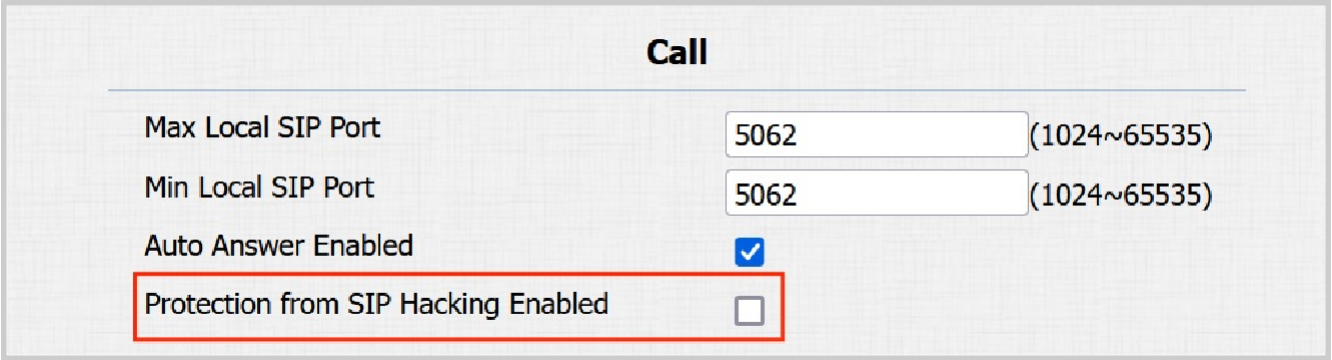
drugiej strony korzysta z TLS. Aby z niej skorzystać, należy przesłać certyfikaty w celu uwierzytelnienia.

- **DNS-SRV:** Rekord usługi DNS definiuje lokalizację serwerów. Rekord ten zawiera nazwę hosta i numer portu serwera, a także wartości priorytetu i wagi, które określają kolejność i częstotliwość korzystania z serwera.

Ochrona przed włamaniami SIP

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

Aby ją włączyć, przejdź do opcji **Konto > Zaawansowane >** Interfejs **połączeń.**

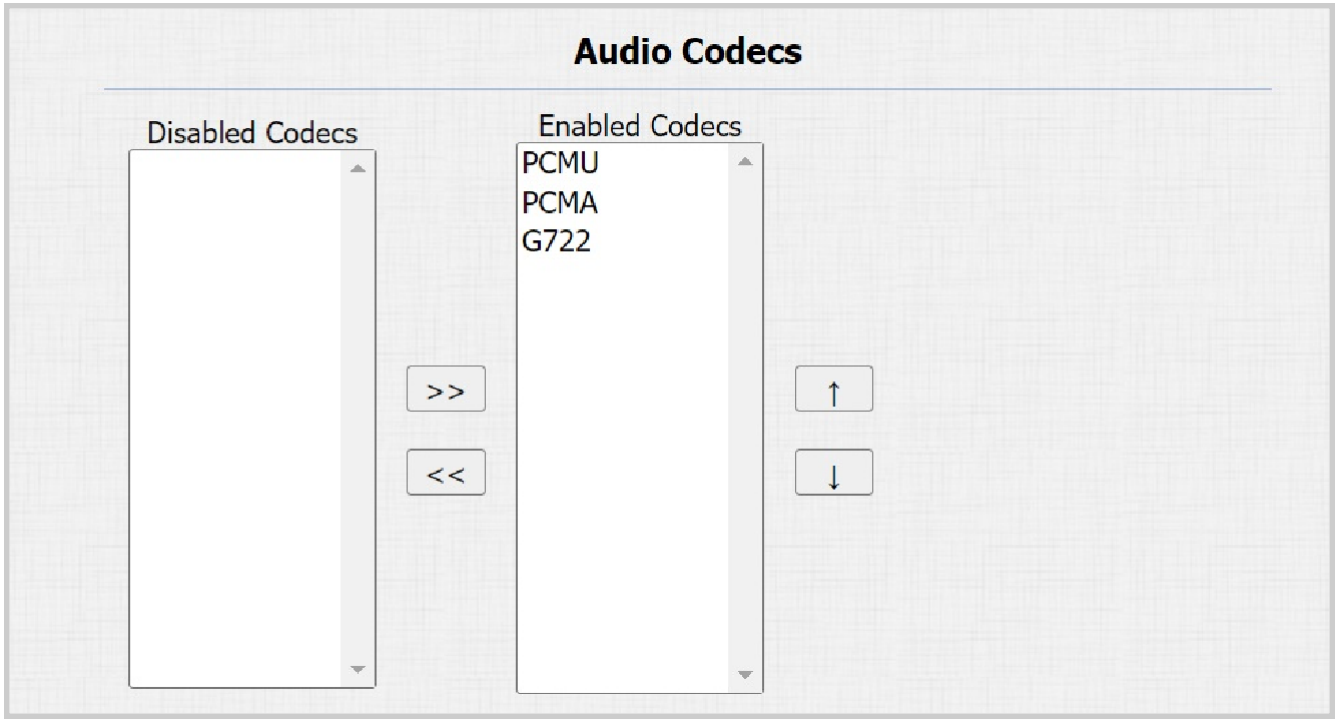


Konfiguracja kodeka audio i wideo

Kodek audio

Bramofon obsługuje trzy rodzaje 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.

Skonfiguruj go w interfejsie **Konto > Zaawansowane** > **Audio Co decs.**



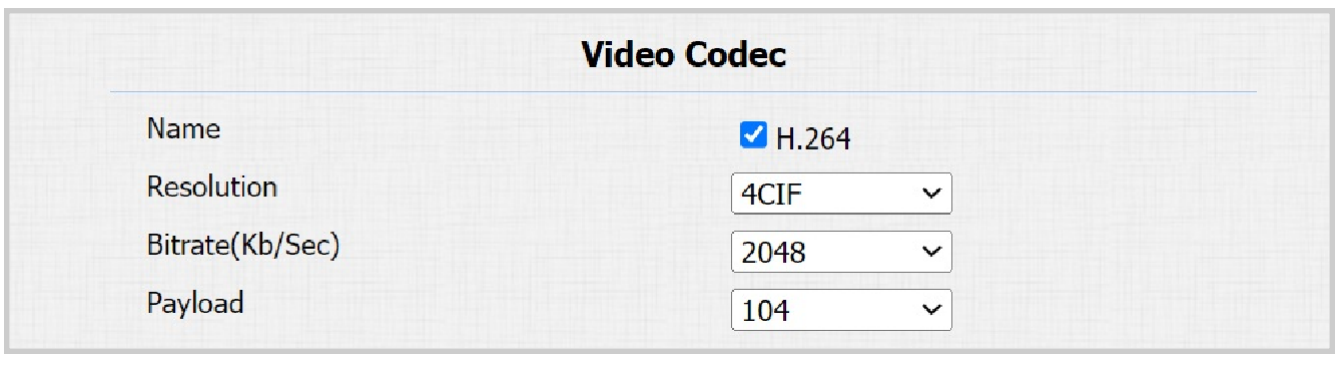
Poniżej znajdują się informacje na temat zużycia pasma i częstotliwości próbkowania dla trzech typów kodeków:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Kodek wideo

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

Aby ją skonfigurować, przejdź do **Konto** internetowe **> Zaawansowane >** Interfejs **Video Co dec.**



- **Nazwa**: Zaznacz, aby włączyć format kodeka wideo H264 dla strumienia wideo z bramofonu.

- **Rozdzielczość**: Wybierz rozdzielczość z dostępnych opcji. Domyślna rozdzielczość kodu to 4CIF.

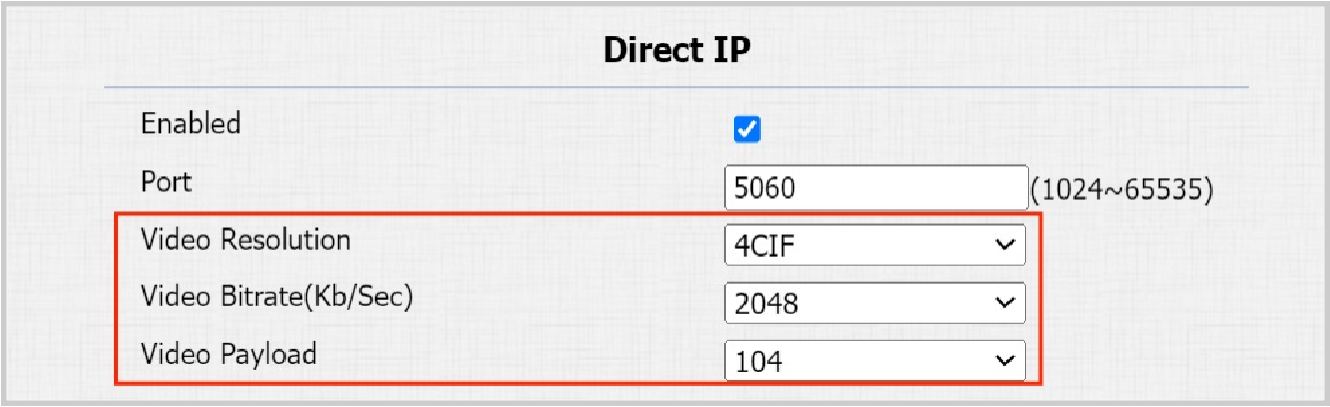
- **Szybkość transmisji** : Szybkość transmisji strumienia wideo wynosi od 128 do 2048 kb/s. Im większa szybkość transmisji, tym więcej danych jest przesyłanych w każdej sekundzie i tym wyraźniejszy jest obraz wideo. Domyślna szybkość transmisji kodu wynosi 2048.

- **Payload**: Ładunek mieści się w zakresie od 90 do 119 dla konfigurowania plików konfiguracyjnych audio/wideo. Domyślną wartością jest 104.

Kodek wideo dla bezpośrednich połączeń IP

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

Aby ją skonfigurować, przejdź do interfejsu **Intercom > Basic > Direct IP.**



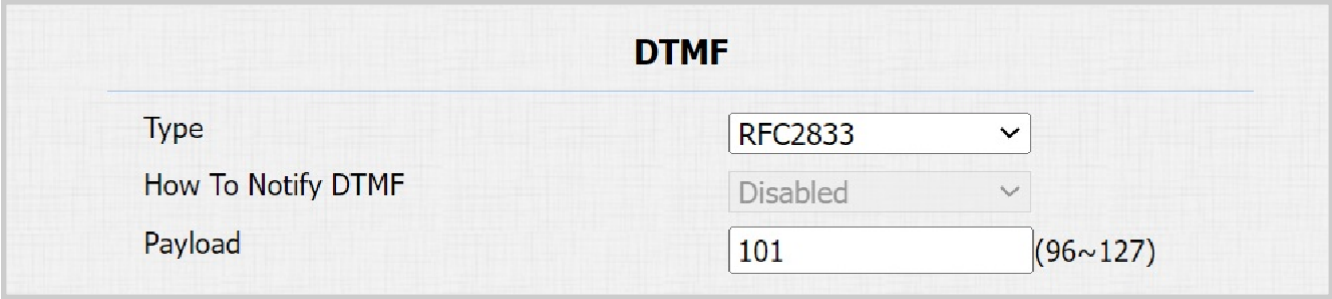
- **Rozdzielczość wideo**: Wybierz rozdzielczość spośród dostępnych opcji.
- **Szybkość transmisji wideo** : Szybkość transmisji strumienia wideo wynosi od 128 do 2048 kb/s. Domyślna szybkość transmisji to 2048.

- **Video Payload**: Ładunek mieści się w zakresie od 90 do 119 dla konfigurowania plików konfiguracyjnych audio/wideo. Domyślną wartością jest 104.

Konfiguracja transmisji danych DTMF

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

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



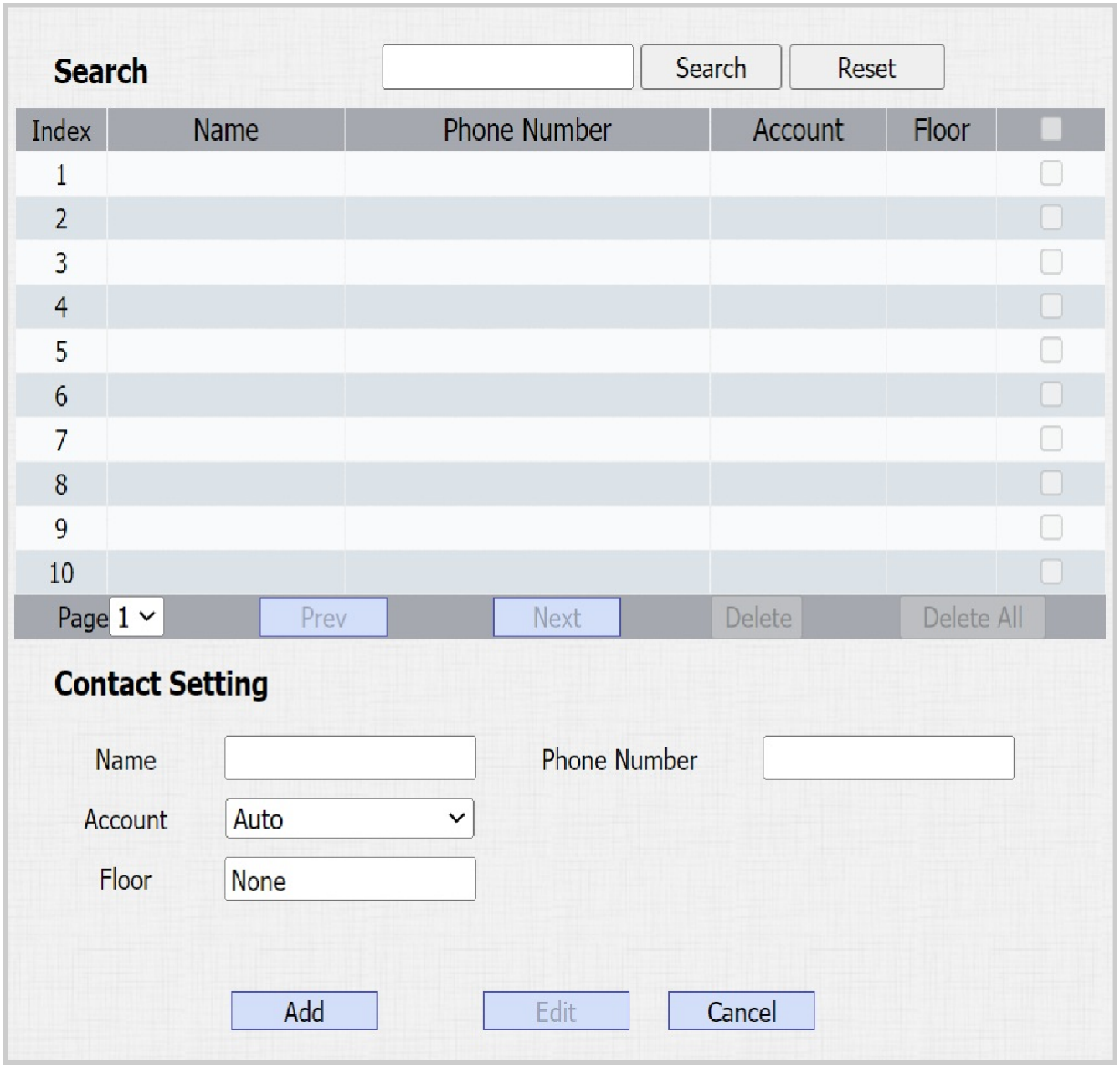
- **Typ:** Wybierz spośród następujących opcji: **Inband, RFC 2833, Info, Info+Inband, Info+RFC 2833 w** oparciu o określony typ transmisji DTMF urządzenia strony trzeciej, z którym ma być dopasowane jako strona odbierająca dane sygnału.
- **Jak powiadamiać DTMF**: Wybierz **Disabled (Wyłączone), DTMF**, **DTMF-Relay (Przekaźnik DTMF)** lub **Telephone-Event (Zdarzenie telefoniczne)** zgodnie z określonym typem przyjętym przez urządzenie innej firmy. Konfiguracja jest wymagana tylko wtedy, gdy urządzenie innej firmy, z którym ma zostać nawiązane połączenie, przyjmuje tryb **Info.**
- **Payload (Ładunek**): Ustaw ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą i odbiorcą podczas transmisji danych.

Konfiguracja listy dozwolonego dostępu

Bramofon może przechowywać do 500 kontaktów, dając uprawnienia dostępu monitorom wewnętrznym lub innym urządzeniom.

Kontakty na liście dozwolonych kontaktów można wyszukiwać, tworzyć, edytować i usuwać.

Skonfiguruj ją w interfejsie **Access Control > Access Allowlist.**



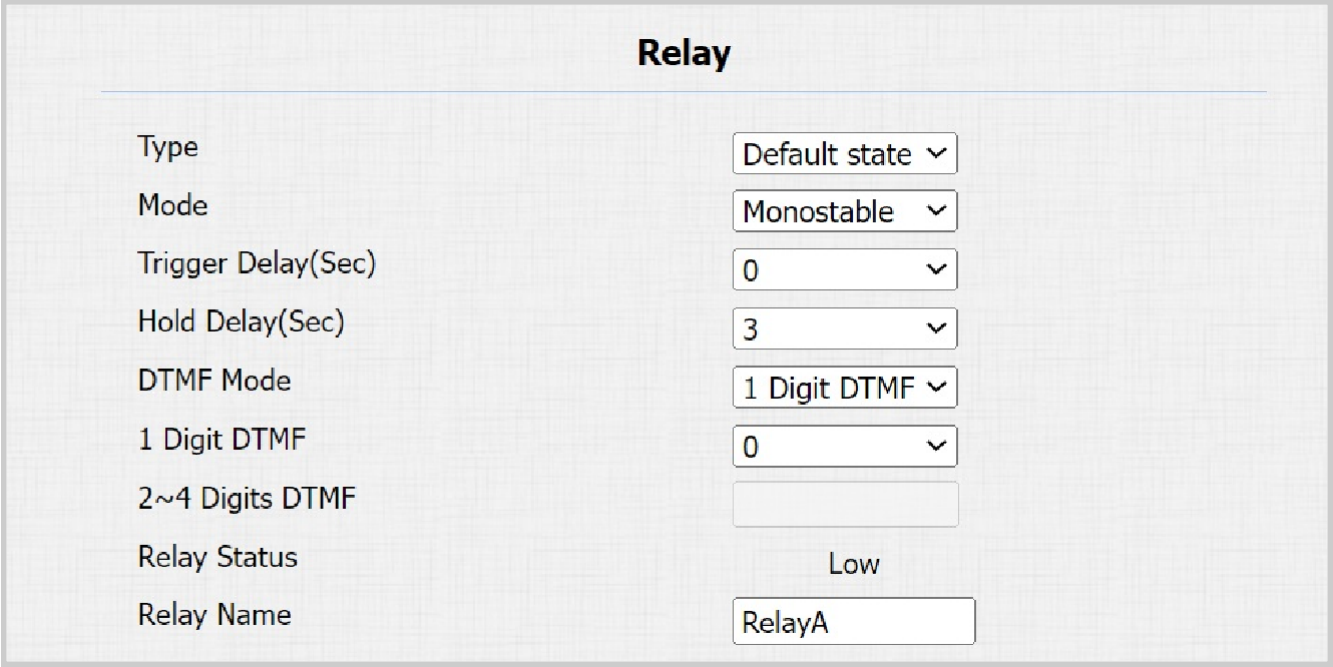
- **Nazwa:** Nazwa kontaktu.
- **Numer telefonu:** Numer telefonu kontaktu. Obsługuje adresy IP i numery SIP.
- **Konto:** Wybierz konto, z którego chcesz wykonać połączenie.
- **Piętro:** Określ piętro (piętra) dostępne dla kontaktu za pośrednictwem windy.

Ustawienie przekaźnika

Ustawienie przełącznika przekaźnika

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

> Interfejs **przekaźnika.**



- **Typ**: Określa interpretację statusu przekaźnika w odniesieniu do stanu drzwi:
    - **Status domyślny**: Stan "Niski" w polu Status przekaźnika oznacza, że drzwi są zamknięte, natomiast stan "Wysoki" oznacza, że są otwarte.
    - **Odwrócony stan**: Stan "Niski" w polu stanu przekaźnika oznacza otwarte drzwi, podczas gdy stan "Wysoki" oznacza drzwi zamknięte.
- **Tryb** : Określa warunki automatycznego resetowania stanu przekaźnika.
    - **Monostabilny**: Status przekaźnika resetuje się automatycznie w czasie opóźnienia przekaźnika po aktywacji.
    - **Bistabilny:** Stan przekaźnika resetuje się po ponownym wyzwoleniu przekaźnika.
- **Trigger Delay(Sec)**: Ustaw czas opóźnienia przed wyzwoleniem przekaźnika. Na przykład, jeśli ustawiono 5 sekund, przekaźnik aktywuje się 5 sekund po naciśnięciu przycisku odblokowania.

- **Hold Delay(Sec)**: Określa, jak długo przekaźnik pozostaje aktywny. Na przykład, jeśli ustawione na 5 sekund, przekaźnik pozostanie otwarty przez 5 sekund przed zamknięciem.
- **Tryb DTMF** : Ustaw cyfry kodu DTMF.
- **1 Digit DTMF**: Zdefiniuj 1-cyfrowy kod DTMF w zakresie (0-9 i *,#), gdy tryb DTMF jest ustawiony na 1-cyfrowy.
- **2~4 cyfry DTMF**: Ustaw kod DTMF na podstawie liczby cyfr wybranych w trybie DTMF.
- **Status** przekaźnika: Wskazuje stany przekaźnika, które są normalnie otwarte i zamknięte. Domyślnie pokazuje stan niski dla normalnie zamkniętego (NC) i wysoki dla normalnie otwartego (NO).
- **Nazwa przekaźnika**: Przypisz odrębną nazwę w celu identyfikacji.

> **Uwaga**
>
> Urządzenia zewnętrzne podłączone do przekaźnika wymagają osobnego zasilacza.

Ustawienie przekaźnika bezpieczeństwa

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

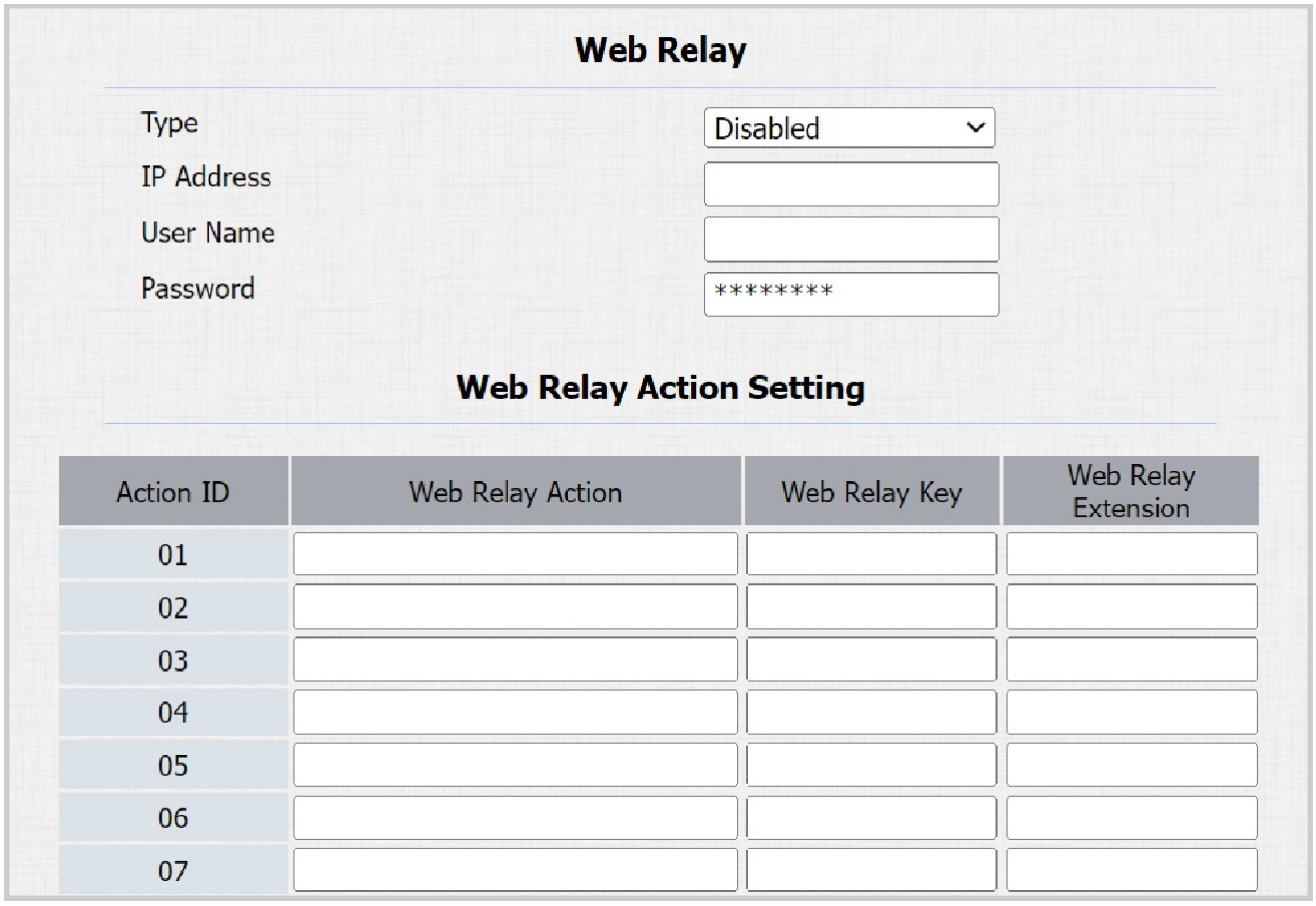
Aby skonfigurować przekaźnik zabezpieczeń, przejdź do interfejsu **Access Control > Relay > Security Relay.**

- **Typ połączenia** : Wskazuje typ połączenia między przekaźnikiem bezpieczeństwa a bramofonem.
- **Trigger Delay(Sec)**: Ustaw czas opóźnienia przed wyzwoleniem przekaźnika. Na przykład, jeśli ustawiono 5 sekund, przekaźnik aktywuje się 5 sekund po naciśnięciu przycisku odblokowania.
- **Hold Delay(Sec)**: Określa, jak długo przekaźnik pozostaje aktywny. Na przykład, jeśli ustawione na 5 sekund, przekaźnik pozostanie otwarty przez 5 sekund przed zamknięciem.
- **1 Digit DTMF**: Zdefiniuj 1-cyfrowy kod DTMF w zakresie (0-9 i *,#), gdy tryb DTMF w sekcji Przekaźnik powyżej jest ustawiony na 1-cyfrowy.
- **2~4 cyfry DTMF**: Ustaw kod DTMF na podstawie liczby cyfr wybranych w trybie DTMF.
- **Nazwa przekaźnika** : Nazwa przekaźnika bezpieczeństwa. Nazwa może być wyświetlana w dziennikach otwarcia drzwi. Podczas łączenia z chmurą SmartPlus Cloud serwer chmury automatycznie przypisze nazwę przekaźnika.
- **Test**: Kliknij, aby wysłać sygnał do SR01. Po sparowaniu bramofonu i SR01 kliknij Test, aby zakończyć dopasowywanie.

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.

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



- **Typ** : Określa typ przekaźnika aktywowanego podczas korzystania z metod dostępu do drzwi.

- **Wyłączone**: Aktywuje tylko lokalny przekaźnik.
- **WebRelay**: Aktywuj tylko przekaźnik sieciowy.
- **Oba**: aktywuje zarówno przekaźnik lokalny, jak i internetowy. Zazwyczaj najpierw uruchamiany jest przekaźnik lokalny, a następnie przekaźnik sieciowy w celu wykonania wstępnie skonfigurowanych działań.

- **Adres IP**: Adres IP przekaźnika sieciowego dostarczony przez producenta przekaźnika sieciowego.
- **Nazwa użytkownika**: Nazwa użytkownika podana przez producenta przekaźnika sieciowego.
- **Hasło** : Klucz uwierzytelniania dostarczony przez producenta dla przekaźnika internetowego. Uwierzytelnianie odbywa się za pośrednictwem protokołu HTTP. Pozostawienie pustego pola Hasło oznacza nieużywanie uwierzytelniania HTTP. Hasło można zdefiniować za pomocą HTTP GET w polu Web Relay Action.
- **Web Relay Action**: Skonfiguruj akcje, które mają być wykonywane przez przekaźnik sieciowy po wyzwoleniu. Wprowadź dostarczone przez producenta adresy URL dla różnych działań, zawierające do 50 poleceń.

UWAGA

Jeśli adres URL zawiera pełną zawartość HTTP (np. http://admin:admin@192.168.1.2/state.xml? relayState=2), nie opiera się na adresie IP wprowadzonym powyżej. Jeśli jednak adres URL jest prostszy (np. state.xml?relayState=2), przekaźnik używa wprowadzonego adresu IP.

- **Klucz przekaźnika internetowego**: Określa metody aktywacji przekaźnika internetowego na podstawie tego, czy kod DTMF jest wypełniony.

- Wypełnienie skonfigurowanym kodem DTMF ogranicza aktywację do przeciągnięcia karty i DTMF.

- Pozostawienie pustego pola umożliwia korzystanie ze wszystkich metod otwierania drzwi.

- **Web Relay Extension**: Określa urządzenie interkomowe i metody, których może ono używać do aktywacji przekaźnika internetowego podczas połączeń.

- Po określeniu adresu IP/SIP urządzenia interkomowego, tylko to urządzenie może wyzwalać przekaźnik sieciowy (z wyjątkiem przeciągnięcia karty lub DTMF) podczas połączeń.

- Jeśli pozostanie puste, wszystkie urządzenia mogą wyzwalać przekaźnik podczas połączeń.

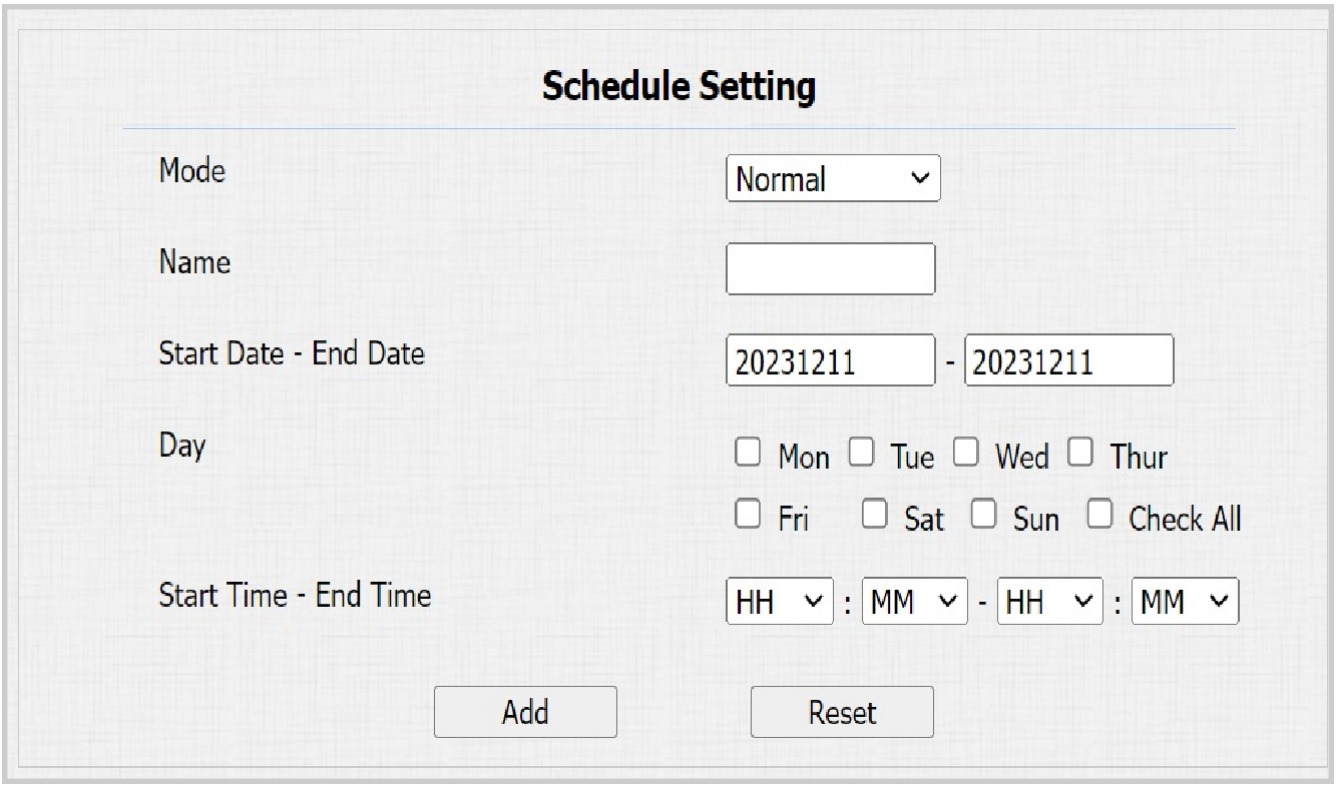
Zarządzanie harmonogramem dostępu do drzwi

Konfiguracja harmonogramu dostępu do drzwi

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

Tworzenie harmonogramu dostępu do drzwi

Harmonogramy dostępu do drzwi można tworzyć dla okresów dziennych, tygodniowych lub niestandardowych.
Aby ją skonfigurować, przejdź do interfejsu **Ustawienia** sieciowe **> Harmonogram.**



- **Tryb**:
    - **Normalny**: Ustaw harmonogram na podstawie miesiąca, tygodnia i dnia. Służy do tworzenia harmonogramów na długie okresy.
    - **Tygodniowy**: Ustaw harmonogram na podstawie tygodnia.

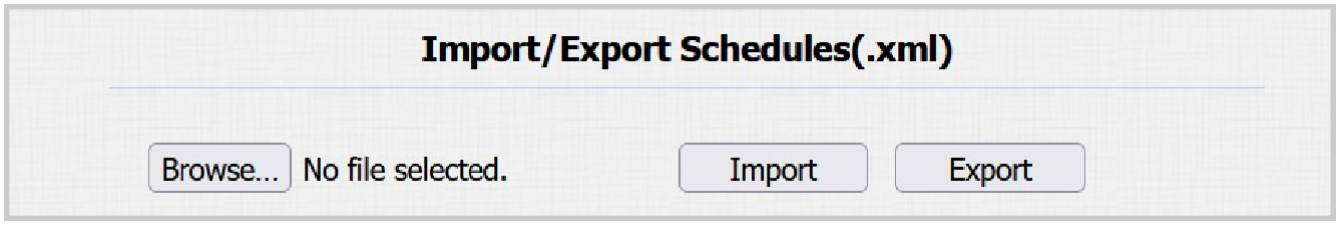
- **Codziennie**: Ustaw harmonogram w oparciu o 24 godziny na dobę.

- **Nazwa**: Nazwa harmonogramu.

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.

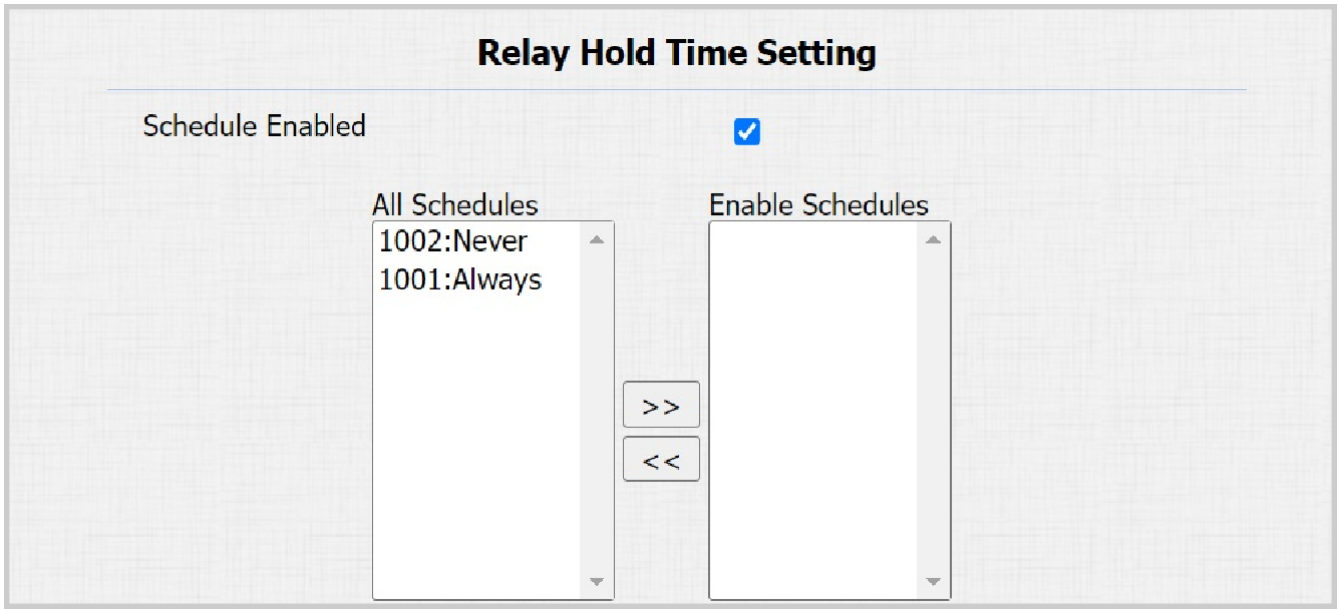
Aby go skonfigurować, przejdź do interfejsu **Ustawienia > Harmonogram.** Plik eksportu jest w formacie **TGZ. Plik** importu powinien być w formacie **XML.**



Harmonogram przekaźników

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

Aby skonfigurować harmonogram przekaźnika, przejdź do interfejsu **Access Control > Relay > Relay Hold Time Setting.**



- **Schedule Enabled**: Przypisz określone harmonogramy dostępu do drzwi do wybranego przekaźnika. Wystarczy przenieść je do pola Selected Schedules (Wybrane harmonogramy).

Instrukcje dotyczące tworzenia harmonogramów można znaleźć w sekcji Tworzenie harmonogramu dostępu do drzwi.

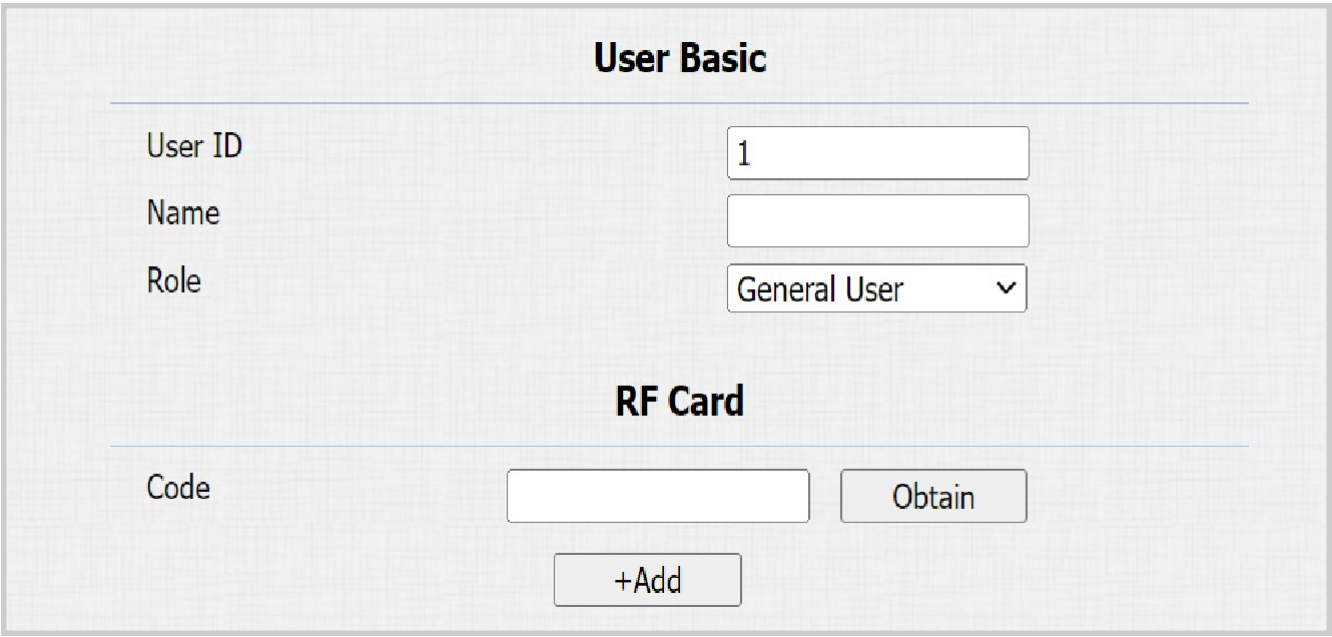
Konfiguracja odblokowania drzwi

Odblokowanie za pomocą kart RF

Karta RF powinna być przypisana do konkretnego użytkownika w celu otwierania drzwi.

Podczas dodawania użytkownika można również dostosować ustawienia, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenie, który przekaźnik ma zostać otwarty.

Aby dodać użytkownika, przejdź do opcji **Kontrola dostępu >** Interfejs **użytkownika** i kliknij przycisk **Dodaj** .



- **Identyfikator użytkownika**: unikalny numer identyfikacyjny przypisany do użytkownika.

- **Nazwa**: nazwa tego użytkownika.

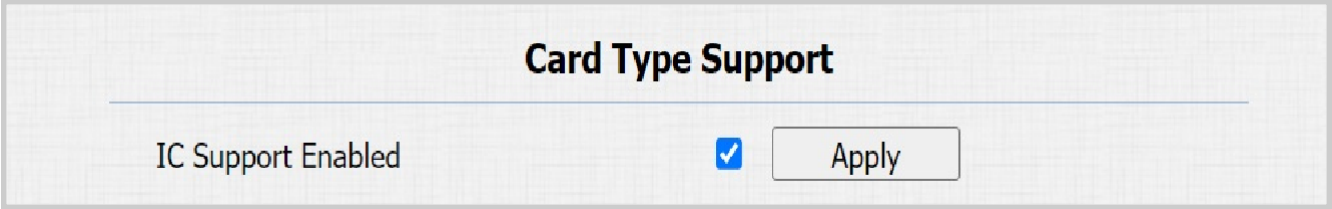
- **Rola**: Zdefiniuj użytkownika jako użytkownika ogólnego lub administratora. Karta administratora może być użyta do dodania karty użytkownika. Szczegółowa konfiguracja znajduje się w sekcji Konfiguracja kart administratora i użytkownika.

- **Kod** : Numer karty odczytywany przez czytnik kart.

Uwaga:

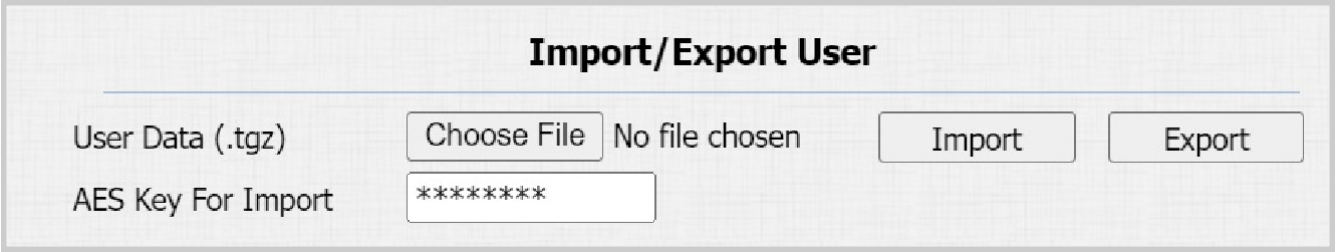
- Każdy użytkownik może dodać maksymalnie 5 kart.
- Urządzenie pozwala na dodanie 5000 użytkowników.
- Karty RF działające na częstotliwości 125 KHz są kompatybilne z bramofonem.

Aby włączyć funkcję karty IC, przejdź do interfejsu **Access Control > Card Setting > Card Type Support.**



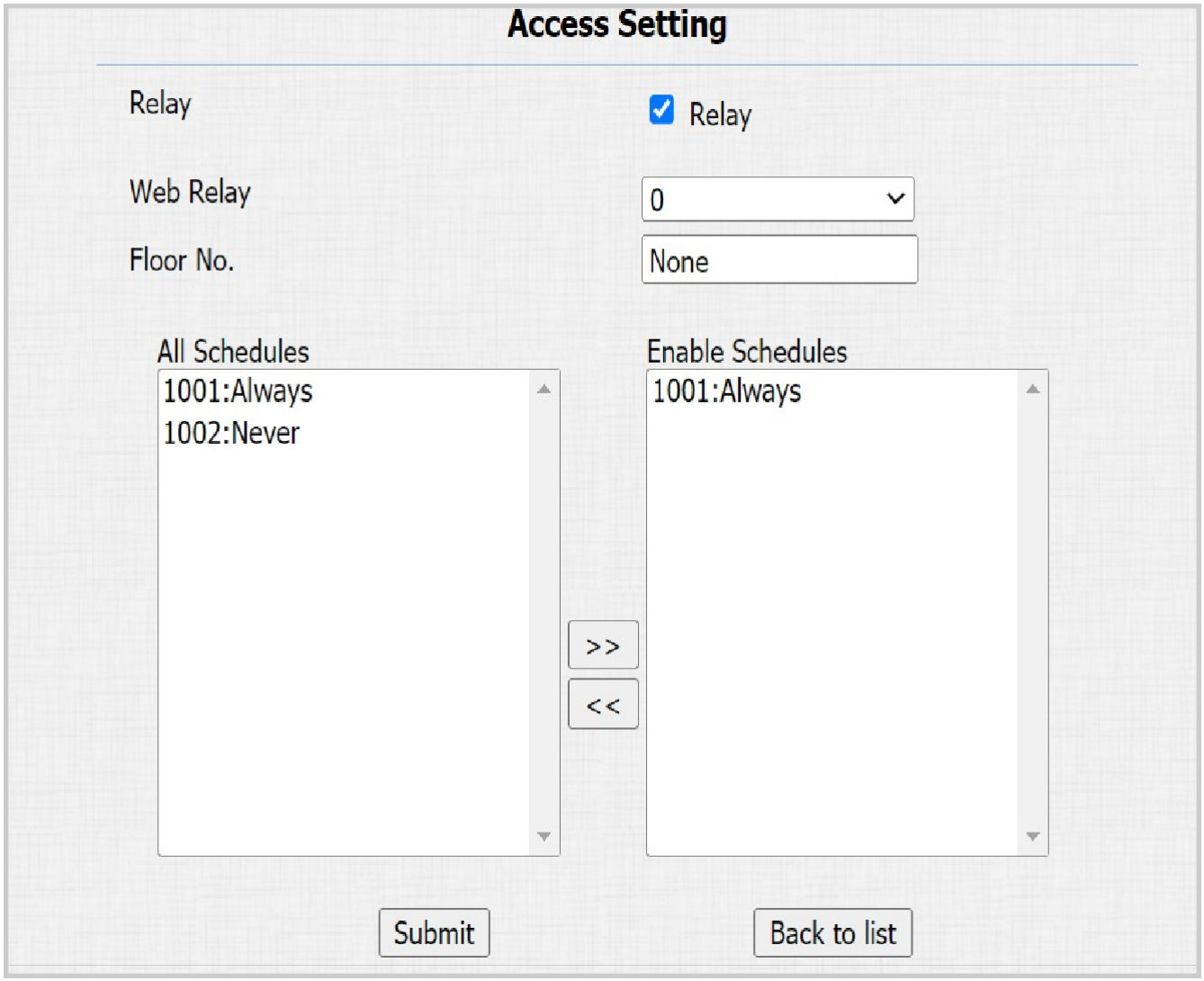
Po dodaniu użytkowników można wyeksportować dane użytkownika i zaimportować je do innego urządzenia interkomowego w celu szybkiego zarządzania.

W interfejsie **Access Control > User** przewiń do sekcji **Import/Export User.**



Ustawienia dostępu

Po wprowadzeniu informacji o użytkowniku i kodu karty RF można przewinąć w dół do opcji **Access Setting (Ustawienia dostępu)** i skonfigurować kontrolę dostępu za pomocą karty RF.

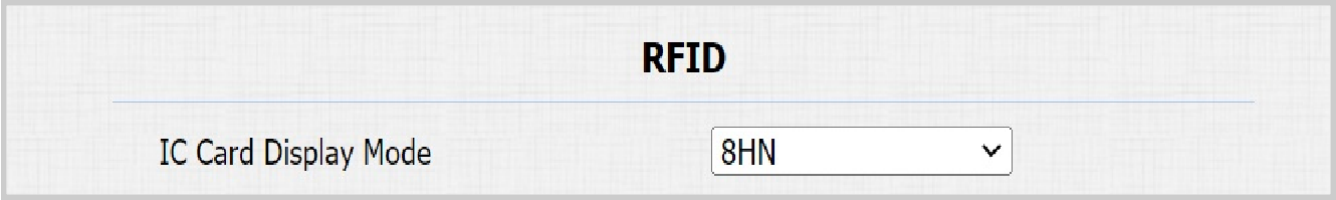


- **Przekaźnik**: Przekaźnik, który ma zostać odblokowany przy użyciu metod otwierania drzwi, powinien zostać przypisany do użytkownika.
- **Web Relay**: Określa identyfikator poleceń akcji web relay skonfigurowanych w interfejsie Web Relay. Domyślna wartość 0 oznacza, że przekaźnik sieciowy nie będzie uruchamiany.
- **Nr piętra**: Określ piętro (piętra) dostępne dla użytkownika za pośrednictwem windy.
- **Harmonogram** : Przyznaj użytkownikowi dostęp do otwierania wyznaczonych drzwi w ustalonych okresach, przenosząc żądany harmonogram (harmonogramy) z lewego pola do prawego. Oprócz niestandardowych harmonogramów dostępne są 2 opcje domyślne:
    - Zawsze: Zezwala na otwieranie drzwi bez ograniczeń liczby otwarć drzwi w ważnym okresie.
    - Nigdy: Zabrania otwierania drzwi.

Format kodu karty RF

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

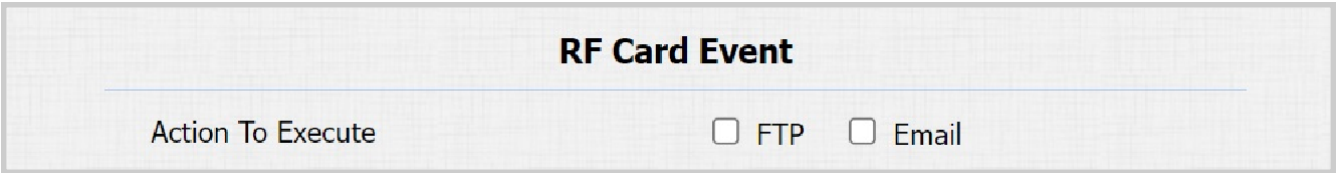
Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu > Ustawienia karty >** Interfejs **RFID.**



- **Tryb wyświetlania karty IC** : Ustaw format numeru karty spośród dostępnych opcji. Domyślnym formatem w urządzeniu jest 8HN.

Zdarzenia wyzwalane przez użycie kart RF

Zdarzenia wyzwalane przez przeciągnięcie karty RF można skonfigurować w interfejsie **Access Control > Card Setting > RF Card Event.**

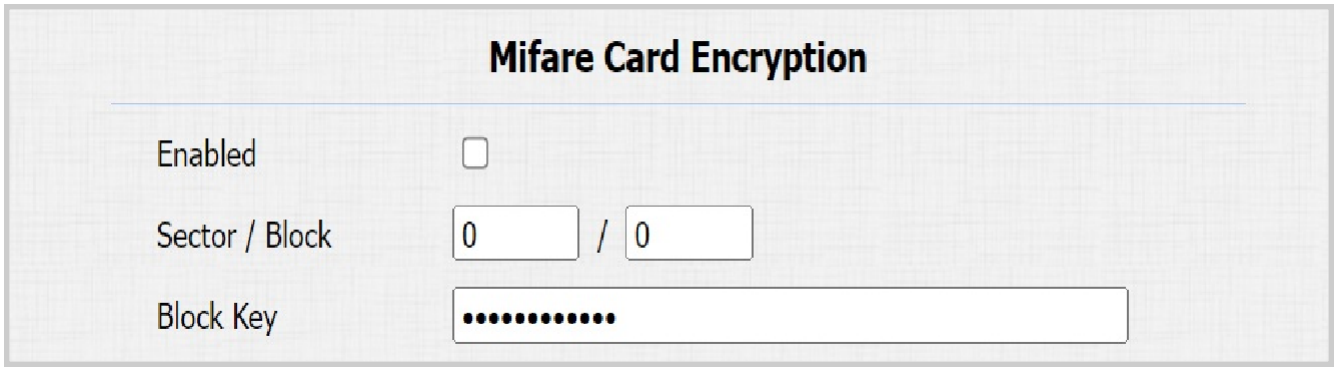


- **Action to Execute (Działanie do wykonania)**: Ustaw żądane działania, które mają być wykonywane po otwarciu drzwi przez przeciągnięcie karty RF.
    - **E-mail**: Wyślij wiadomość na wstępnie skonfigurowany adres e-mail.
    - **FTP**: wysłanie wiadomości na wstępnie skonfigurowany adres FTP.

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.

Aby zaszyfrować kartę, przejdź do interfejsu **Access Control > Card Setting > Mifare Card Encryption.**



- **Sector/Block**: Określa lokalizację, w której przechowywane są zaszyfrowane dane karty. Karta Mifare ma 16 sektorów (ponumerowanych od 0 do 15), a każdy sektor ma 4 bloki (ponumerowane od 0 do 3).

- **Block Key (Klucz bloku)**: Ustawienie hasła dostępu do danych zapisanych we wstępnie zdefiniowanym sektorze/bloku.

Karta 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 użyć konkretnej karty, przejdź do opcji **Kontrola dostępu > Ustawienia karty >** Interfejs **zbliżeniowej karty inteligentnej**

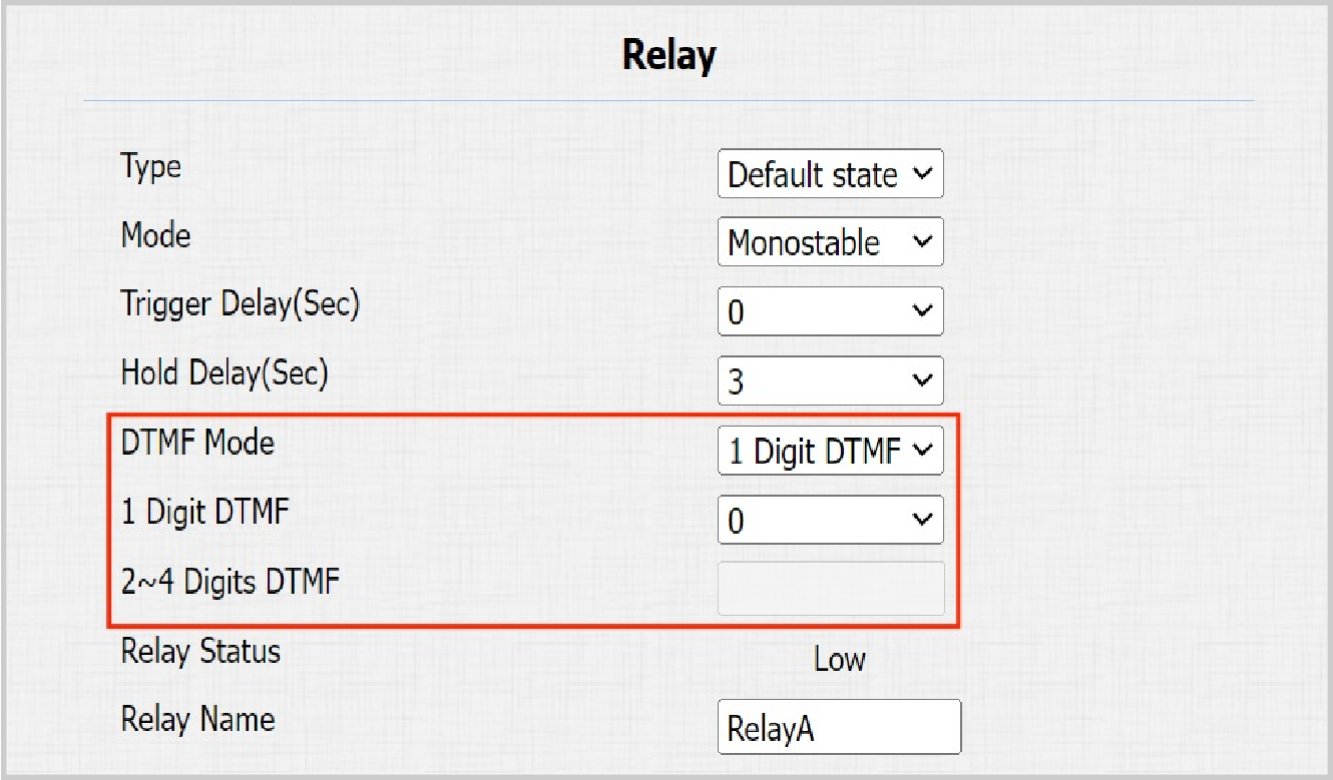
Funkcja NFC nie jest dostępna na iPhone'ach.

Aby uzyskać szczegółową konfigurację, zapoznaj się z tematem **Otwieranie drzwi za pomocą NFC**.

Odblokowanie kodem DTMF

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

Aby skonfigurować kody DTMF, przejdź do opcji **Kontrola dostępu >** Interfejs **przekaźnika.**



- **Tryb DTMF** : Ustaw liczbę cyfr dla kodu DTMF.

- **1 Digit DTMF**: Zdefiniuj 1-cyfrowy kod DTMF w zakresie (0-9 i *,#), gdy tryb DTMF jest ustawiony na 1-cyfrowy.

- **2-4 Digit DTMF**: Ustaw kod DTMF na podstawie liczby cyfr wybranych w trybie DTMF.

Biała lista DTMF

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

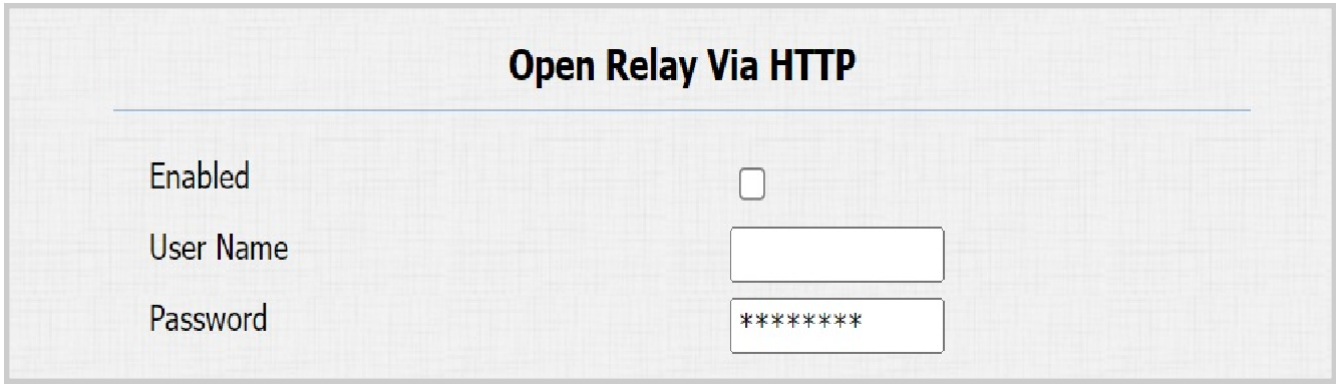
- **Przypisane uprawnienia dla**: Określ kontakty upoważnione do otwierania drzwi za pomocą DTMF:
    - Wyłączone: Żaden numer nie może odblokować drzwi za pomocą DTMF.
    - Lista kontaktów i przycisk: Drzwi mogą być otwierane przez numery dodane do listy kontaktów bramofonu i naciśnięcie przycisku.
    - Wszystkie numery: Wszystkie numery można odblokować za pomocą DTMF.

> **Uwaga**
>
> Po wybraniu tej opcji wywołujący monitor wewnętrzny powinien zostać dodany do listy kontaktów bramofonu.

Odblokowanie za pomocą polecenia HTTP

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

Skonfiguruj go w interfejsie Web **Access Control > Relay > Open Relay Via HTTP.**



- **Kontrola sesji**: Włącz, aby zwiększyć bezpieczeństwo transmisji danych.

- **Nazwa użytkownika**: Ustaw nazwę użytkownika do uwierzytelniania w adresach URL poleceń HTTP.

- **Hasło**: ustawienie hasła do uwierzytelniania w adresach URL poleceń HTTP.

Wskazówka:

Oto przykład adresu URL polecenia HTTP dla wyzwalania przekaźnika.

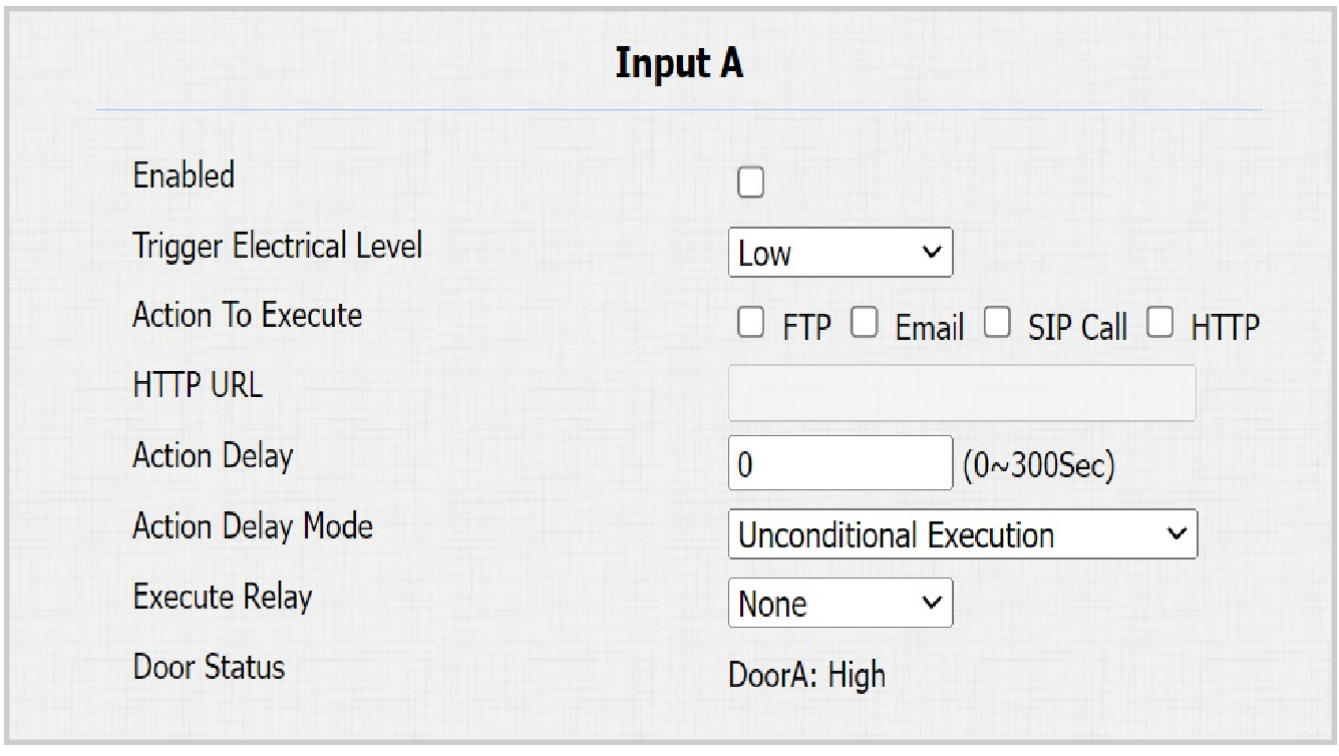
Uwaga

Format HTTP dla wyzwalania przekaźnika różni się w zależności od tego, czy włączony jest tryb wysokiego bezpieczeństwa bramofonu. **Więcej informacji można znaleźć w poradniku Otwieranie drzwi za pomocą polecenia HTTP.**

Odblokowanie przyciskiem wyjścia

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

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



- **Enabled**: Aby użyć określonego interfejsu wejściowego.

- **Poziom wyzwalania elektrycznego**: Ustawienie wyzwalania interfejsu wejściowego na niskim lub wysokim poziomie elektrycznym.

  Action To Execute: Ustaw żądane działania, które wystąpią po wyzwoleniu określonego interfejsu wejściowego.

  ° FTP: wysłanie zrzutu ekranu na wstępnie skonfigurowany serwer FTP.

  ° E-mail: Wyślij zrzut ekranu na wstępnie skonfigurowany adres e-mail.

  ° Połączenie SIP: Połączenie z ustawionym numerem po wyzwoleniu.

  ° HTTP: Po uruchomieniu komunikat HTTP może zostać przechwycony i wyświetlony w odpowiednich pakietach. Aby skorzystać z tej funkcji, należy włączyć serwer HTTP i wprowadzić treść wiadomości w wyznaczonym polu poniżej.

- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/Treść wiadomości.

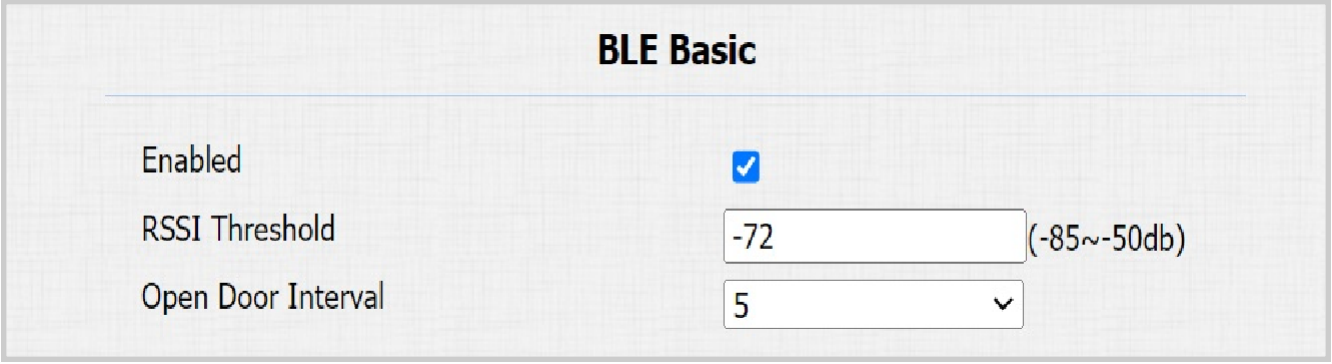
- **Opóźnienie akcji**: Określa, o ile sekund ma zostać opóźnione wykonanie wstępnie skonfigurowanych działań.
- **Tryb opóźnienia działania** :
  - Bezwarunkowe wykonanie: Akcja zostanie wykonana, gdy wejście zostanie wyzwolone.
  - Wykonaj, jeśli wejście jest nadal wyzwolone: Akcja zostanie wykonana, gdy wejście pozostanie wyzwolone. Na przykład, jeśli drzwi pozostaną otwarte po wyzwoleniu wejścia, zostanie wysłana akcja, taka jak wiadomość e-mail, aby powiadomić odbiorcę.

- **Wykonaj przekaźnik**: Określa przekaźnik, który ma być wyzwalany przez akcje.
- **Stan drzwi**: Wyświetlanie stanu sygnału wejściowego.

Odblokowanie przez Bluetooth

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

Aby skonfigurować Bluetooth, przejdź do opcji **Kontrola dostępu >** Interfejs **BLE.**



- **Próg RSSI**: Ustawienie siły odbieranego sygnału. Wyższe wartości oznaczają większą siłę sygnału, co ułatwia odbieranie sygnału Bluetooth.
- **Interwał otwarcia drzwi**: Ustawienie interwału (w sekundach) między kolejnymi próbami dostępu do drzwi Bluetooth.

Monitor i obraz

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

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

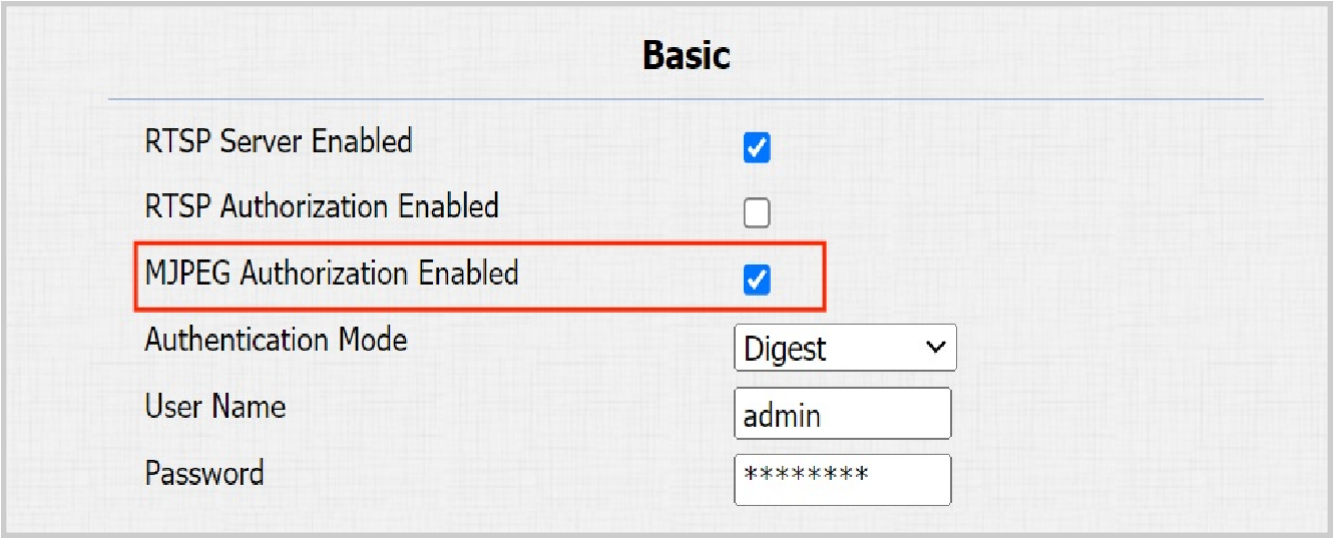
RTSP to skrót od Real Time Streaming Protocol. Może być używany do strumieniowego przesyłania obrazu i dźwięku z kamer innych firm do urządzenia. Możesz dodać strumień z kamery, dodając jej adres URL. Format adresu URL urządzeń Akuvox to rtsp://Device's IP/live/ch00_0

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

Przechwytywanie obrazu MJPEG

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

Aby ją skonfigurować, przejdź do **Surveillance > RTSP > Basic** interface.



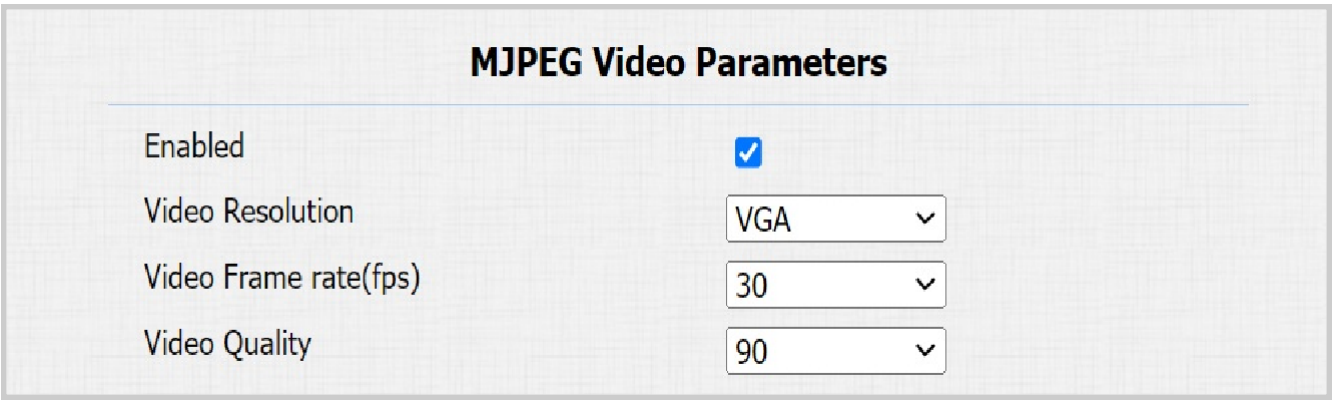
- **MJPEG Authorization Enabled**: Po włączeniu tej opcji dostęp do obrazu lub wideo w czasie rzeczywistym z bramofonu poprzez wprowadzenie adresu URL w przeglądarce wymaga weryfikacji trybu uwierzytelniania, nazwy użytkownika RTSP i hasła RTSP.

Ws

- Aby wyświetlić dynamiczny strumień, użyj adresu URL http://device_IP:8080/video.cgi.
- Aby przechwycić zrzut ekranu, użyj następujących adresów URL, przy czym formaty obrazu różnią się odpowiednio:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi

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

Parametry wideo MJPEG można skonfigurować w sekcji **Parametry wideo MJPEG.**



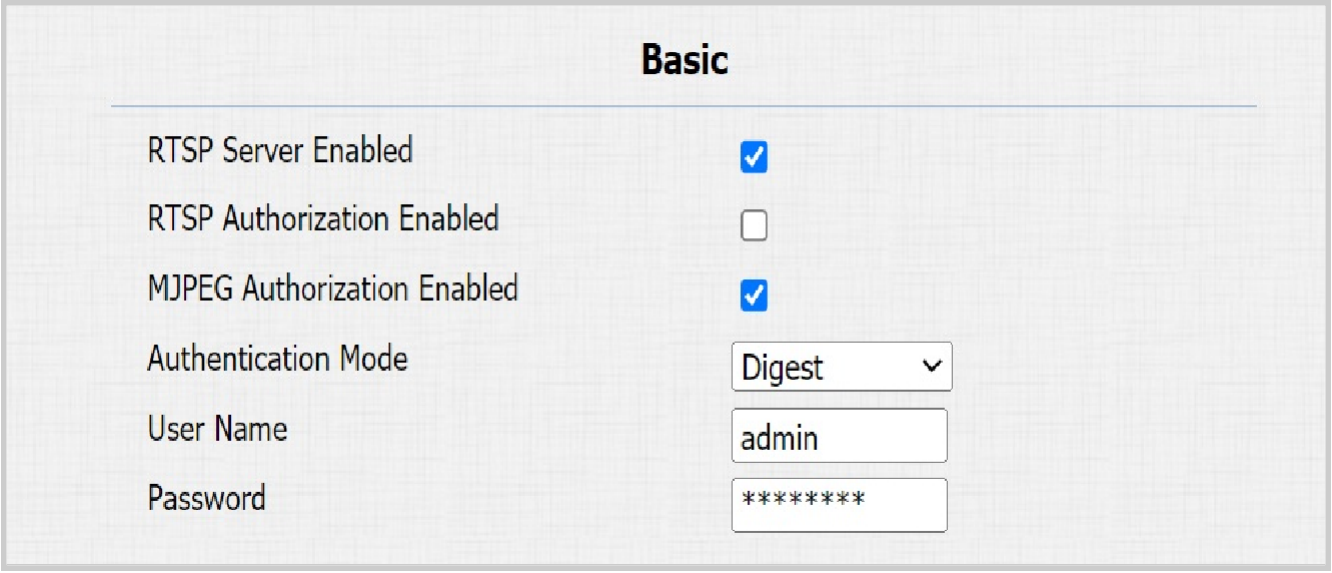
- **Rozdzielczość wideo**: Określa rozdzielczość obrazu, od najniższej CIF (352×288 pikseli) do najwyższej 1080P (1920×1080 pikseli).
- **Szybkość klatek wideo (fps)**: Liczba klatek na sekundę odnosi się do liczby klatek wyświetlanych w jednej sekundzie wideo. Domyślna liczba klatek na sekundę wynosi 30 kl.
- **Jakość wideo**: Szybkość transmisji wideo wynosi od 50 do 90.

Monitorowanie strumienia RTSP

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

Podstawowe ustawienia RTSP

Przed rozpoczęciem korzystania z tej funkcji należy skonfigurować funkcję RTSP w interfejsie internetowym urządzenia **Surveillance > RTSP > Basic** w zakresie autoryzacji RTSP, uwierzytelniania, hasła itp.



- **RTSP Authorization Enabled**: Po włączeniu skonfiguruj tryb uwierzytelniania RTSP, nazwę użytkownika RTSP i hasło RTSP. Te dane uwierzytelniające są wymagane do uzyskania dostępu do strumienia RTSP bramofonu z innych urządzeń interkomowych, takich jak monitory wewnętrzne.
- **Tryb uwierzytelniania** : Wybierz pomiędzy Basic i Digest. Basic jest domyślnym typem uwierzytelniania.
    - Podstawowy: Nazwa użytkownika i hasło są łączone w formie "nazwa użytkownika: hasło", po czym następuje kodowanie Base64 przed wysłaniem do

serwera. Następnie serwer odszyfrowuje ciąg, aby pobrać nazwę użytkownika i hasło do weryfikacji.

- Digest: Użycie haszowania zamiast łatwo odwracalnego kodowania Base64. Do weryfikacji używany jest token.

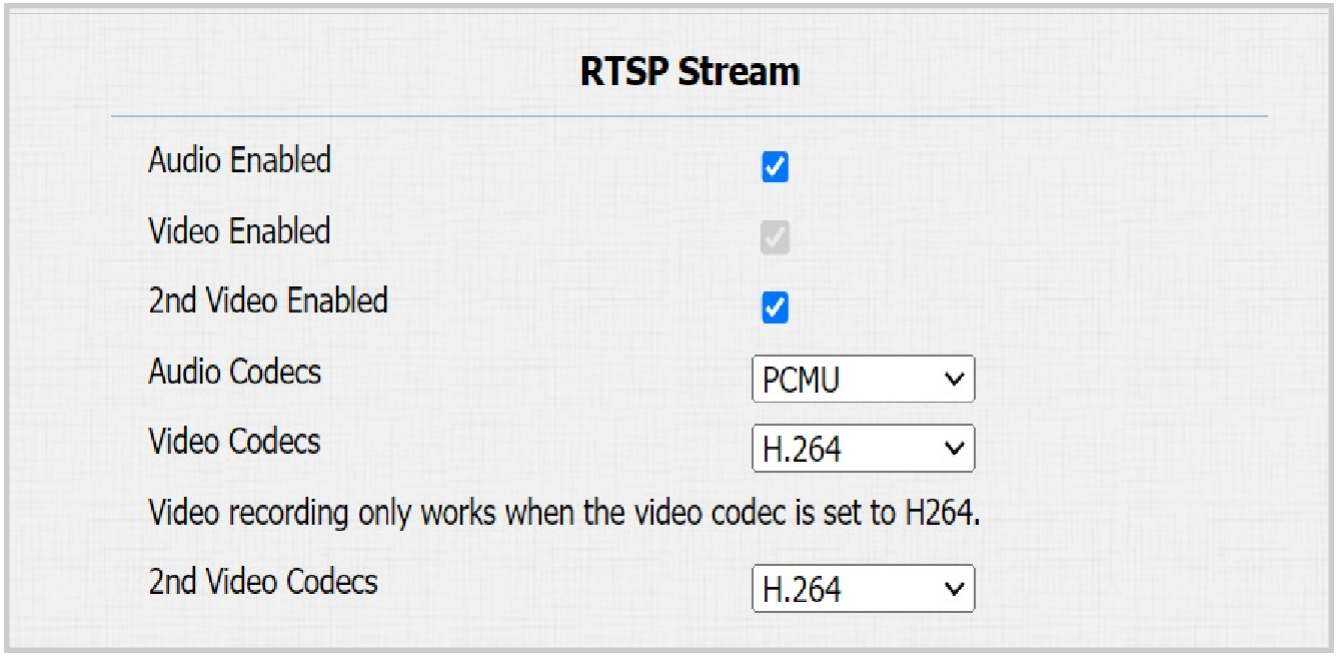
- **Nazwa użytkownika**: Ustaw nazwę użytkownika do autoryzacji.

- **Hasło**: ustawienie hasła autoryzacji.

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 **Surveillance > RTSP > RTSP Stream** interface.



- **Audio Enabled:** Określa, czy strumień RTSP ma dźwięk.

- **Video Enabled:** Określa, czy strumień RTSP zawiera wideo. Po włączeniu funkcji RTSP wideo RTSP jest domyślnie włączone i nie można go modyfikować.

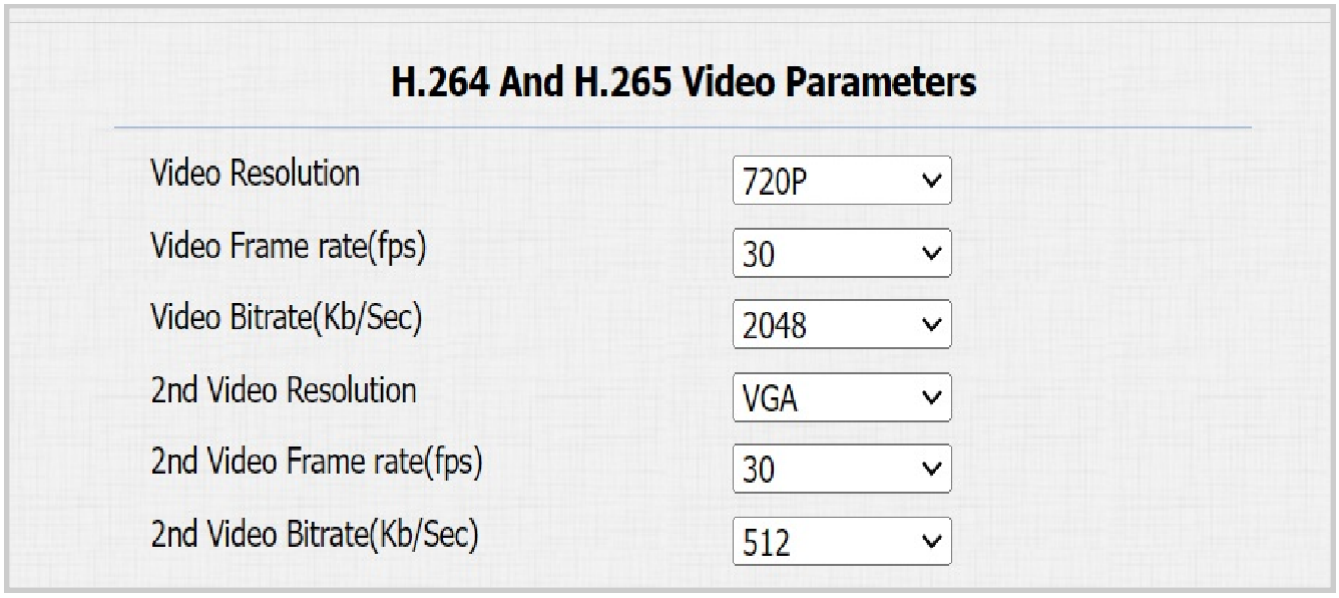
- **2nd Video Enabled:** E12 obsługuje dwa strumienie RTSP.

- **Kodeki audio:** Wybierz odpowiedni kodek audio dla dźwięku RTSP.

- **Kodeki wideo:** Określa formaty kompresji wideo.

- H.264: Oferuje wysoce wydajną kompresję, ale kosztem wyższych opóźnień i obciążenia obliczeniowego.
- H.265: Oferuje wyższą wydajność kompresji i obsługę wyższych rozdzielczości, ale wiąże się z wyższymi wymaganiami obliczeniowymi i potencjalnymi problemami z kompatybilnością.
- MJEPG: Oferuje lepszą jakość, ale nieefektywną kompresję.

Parametry wideo dla H.264 i H.265 można skonfigurować w sekcji **Parametry wideo H.264 i H.265.**



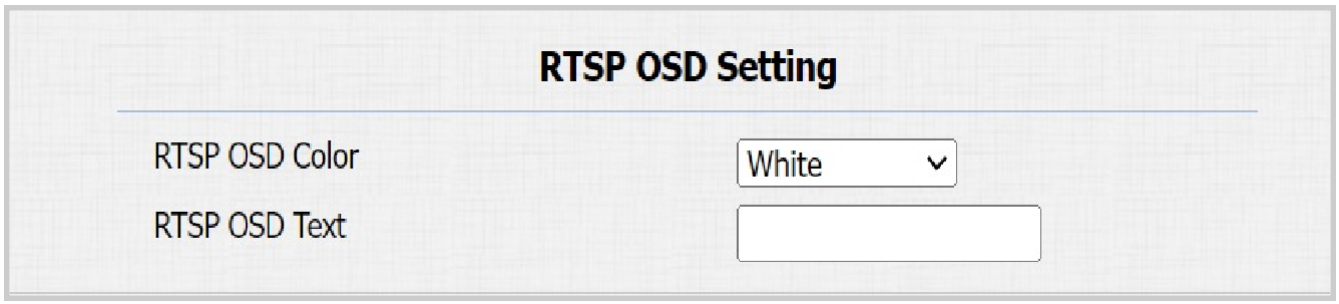
- **Rozdzielczość wideo**: Określa rozdzielczość obrazu, od najniższej CIF (352×288 pikseli) do najwyższej 1080P (1920x1080 pikseli).
- **Szybkość klatek wideo (fps)**: Liczba klatek na sekundę odnosi się do liczby klatek wyświetlanych w jednej sekundzie wideo. Domyślna liczba klatek na sekundę wynosi 30 kl.
- **Video Bitrate(Kb/Sec)**: Ilość danych wideo przesyłanych w określonym czasie. Wyższy bitrate wideo oznacza wyższą możliwą jakość, ale także większe rozmiary plików i większą przepustowość. Domyślną wartością jest 2048 kb/s.
- **2. rozdzielczość wideo**: Określa rozdzielczość obrazu dla drugiego kanału strumienia wideo.
- **2nd Frame rate(fps)**: Ustawia liczbę klatek na sekundę dla drugiego kanału strumienia wideo.

- **2nd Video Bitrate(Kb/Sec)**: Ustawienie szybkości transmisji dla drugiego kanału strumienia wideo. Domyślnie jest to 512 kb/s.

Ustawienia OSD RTSP

Ta funkcja służy do dodawania znaku wodnego do wideo lub obrazu RTSP.

Skonfiguruj go w interfejsie internetowym **Surveillance > RTSP > RTSP OSD Setting.**

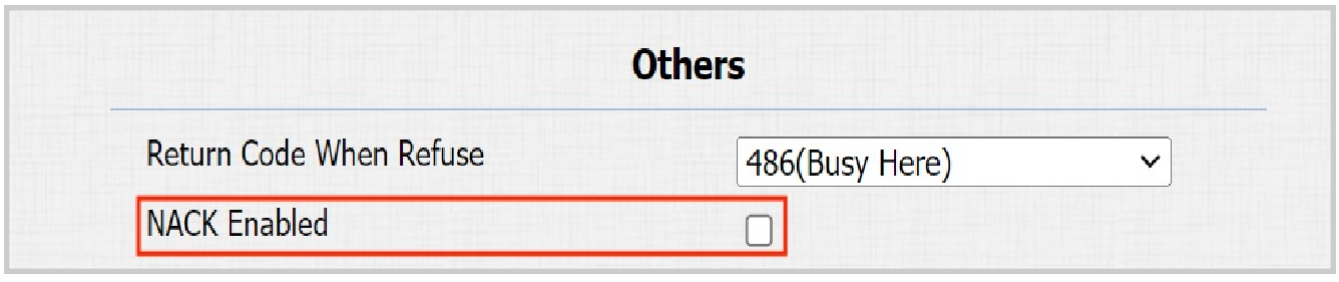


- **Kolor OSD RTSP**: Dostępnych jest pięć kolorów: biały, czarny, czerwony, zielony i niebieski dla tekstu znaku wodnego RTSP.
- **Tekst OSD RTSP**: Dostosuj tekst znaku wodnego.

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 NACK, przejdź do interfejsu **Intercom > Call Feature > Others.**

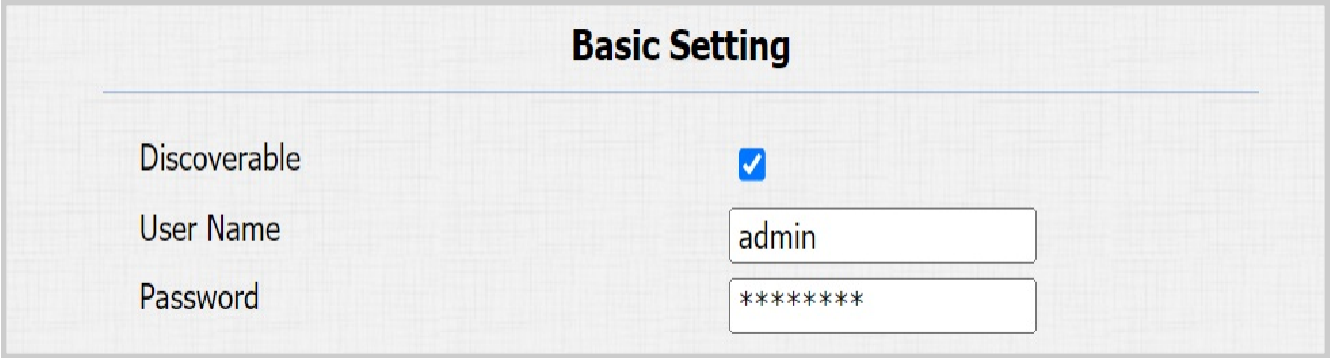


- **NACK Enabled:** Może być używana do zapobiegania utracie pakietów danych w słabym środowisku sieciowym w przypadku przerwania i mozaiki obrazów wideo.

ONVIF

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

Aby ją skonfigurować, przejdź do interfejsu **Surveillance > ONVIF.**



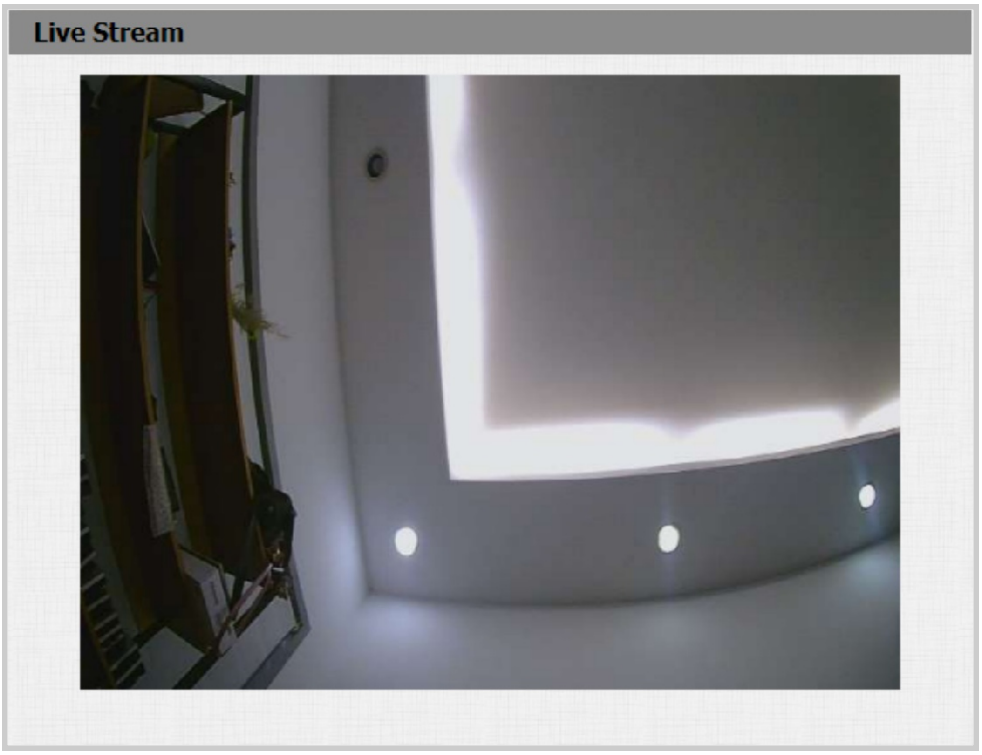
- **Discoverable**: Po włączeniu tej opcji obraz wideo z kamery telefonu może być wyszukiwany przez inne urządzenia.
- **Nazwa użytkownika**: Ustaw nazwę użytkownika wymaganą do uzyskania dostępu do strumienia wideo z bramofonu na innych urządzeniach. Domyślnie jest to admin.
- **Hasło** : Ustaw hasło wymagane do uzyskania dostępu do strumienia wideo z bramofonu na innych urządzeniach. Domyślnie jest to admin.

> **Wskazówka**
>
> Po skonfigurowaniu ustawień, aby uzyskać dostęp do strumienia wideo na urządzeniu innej firmy, wystarczy wprowadzić adres URL ONVIF: http://Device's IP:80/onvif/device_service.

Transmisja na żywo

Istnieją dwa sposoby sprawdzania 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.

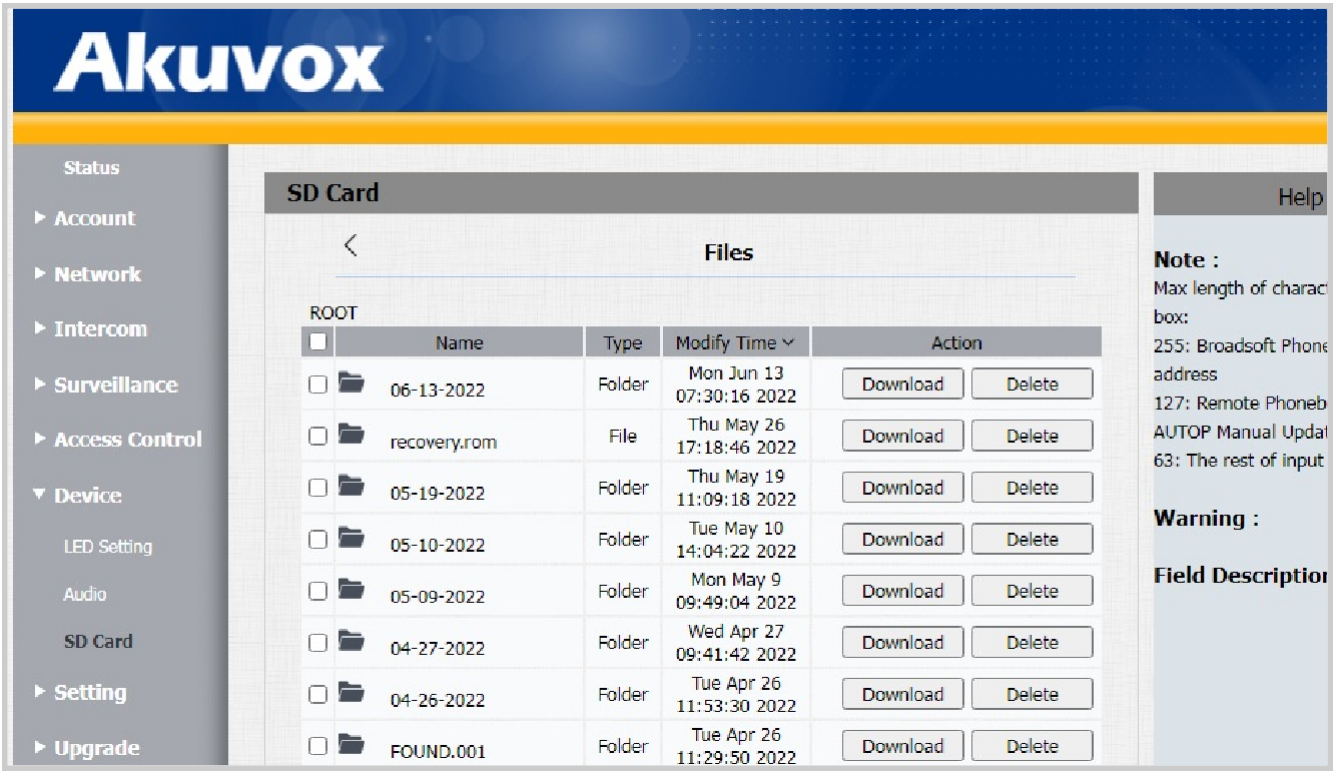
Zobacz transmisję na żywo w interfejsie urządzenia **Monitoring > Transmisja na żywo.**



Karta SD do przechowywania filmów

Do urządzenia można włożyć kartę SD, na której można zapisywać ruch i filmy z rozmów.

Aby sprawdzić filmy, przejdź do opcji **Urządzenie >** Interfejs **karty SD.** Jeśli na karcie SD nie ma wystarczającej ilości miejsca, aby nagrać kolejny film, system automatycznie usunie najstarszy film.

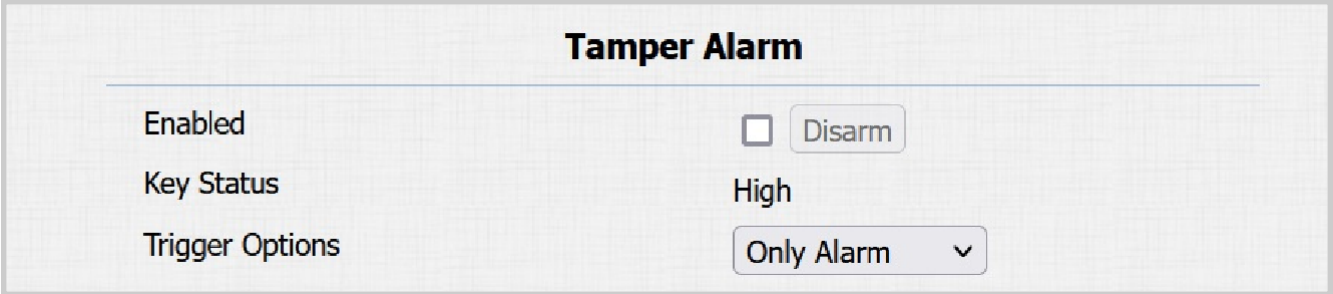


Bezpieczeństwo

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.

Skonfiguruj go w interfejsie **Security > Basic > Tamper Alarm.** Kliknij Rozbrój, aby skasować alarm.



- **Opcje wyzwalania:** Wybierz, co może zostać wyzwolone po uruchomieniu czujnika grawitacyjnego.

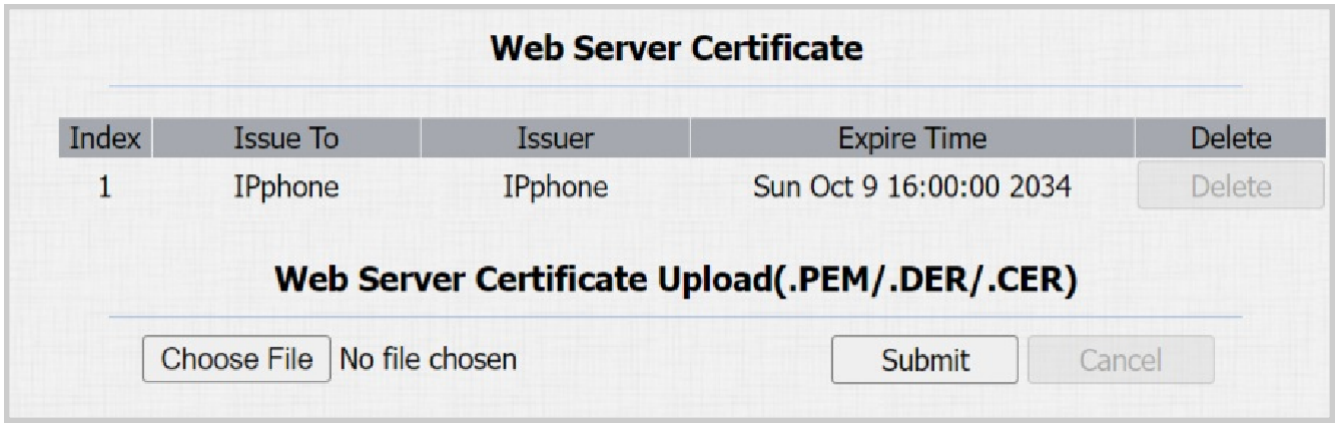
Ustawienia certyfikatu klienta

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.

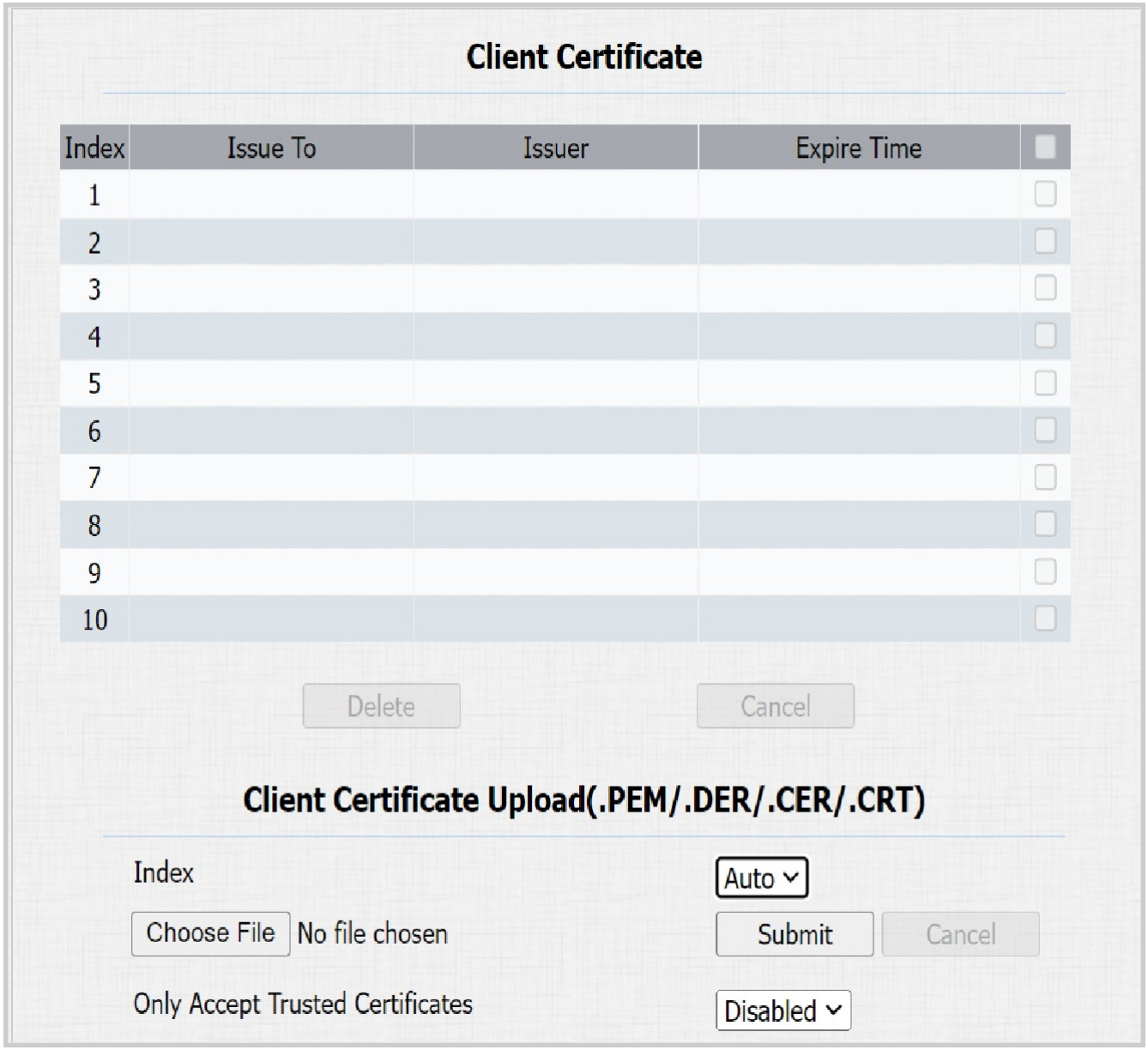
Prześlij certyfikat serwera WWW w interfejsie **Zabezpieczenia WWW > Zaawansowane > Certyfikat serwera WWW.**



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.

Prześlij i skonfiguruj certyfikat klienta w interfejsie **Security > Advanced > Web Server Certificate.**



- **Indeks:**
    - Auto: Przesłany certyfikat zostanie wyświetlony w kolejności numerycznej.
    - 1 do 10: przesłany certyfikat zostanie wyświetlony zgodnie z wybraną wartością.

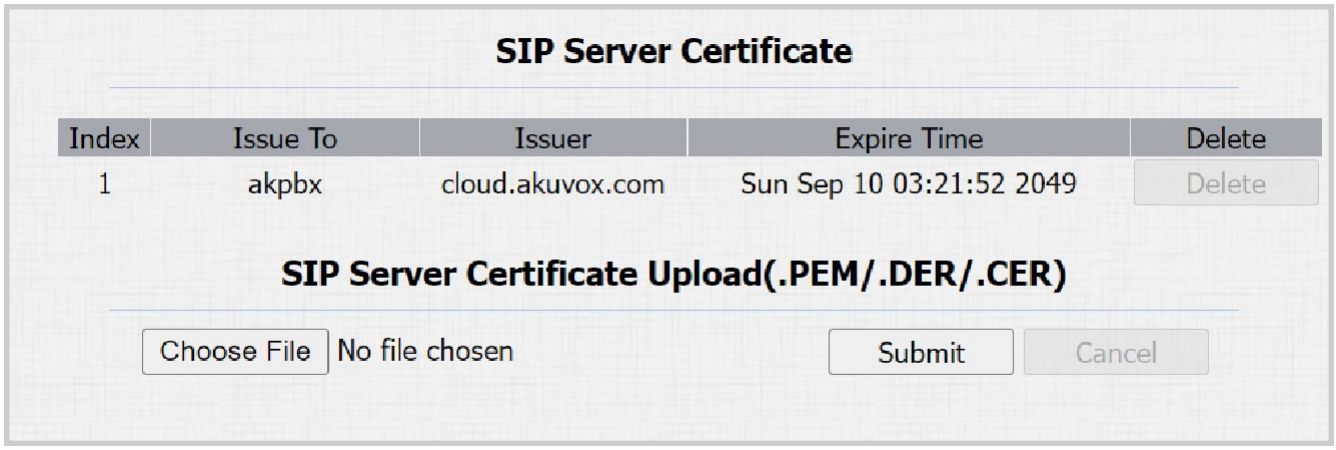
- **Wybierz plik:** Kliknij Wybierz plik, aby przesłać certyfikat.

- **Akceptuj tylko zaufane certyfikaty:** Po włączeniu tej opcji, o ile uwierzytelnianie się powiedzie, bramofon zweryfikuje certyfikat serwera na podstawie listy certyfikatów klienta. Po wybraniu opcji Disabled (Wyłączone) bramofon nie będzie weryfikował certyfikatu serwera bez względu na to, czy certyfikat jest ważny, czy nie.

Prześlij certyfikat TLS do rejestracji konta SIP

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

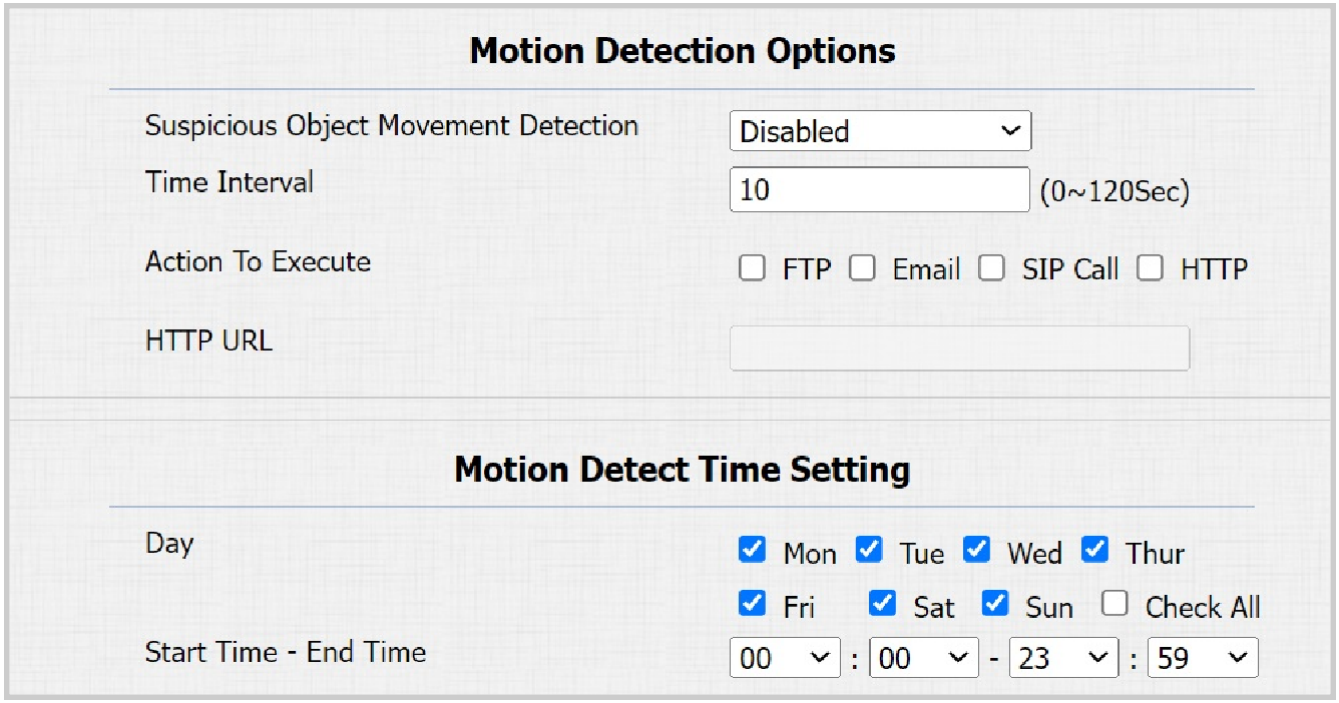
Aby ją skonfigurować, przejdź do opcji **Zabezpieczenia > Zaawansowany** interfejs.



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.

Skonfiguruj wykrywanie ruchu w interfejsie **Surveillance > Motion.**



- **Wykrywanie ruchu podejrzanego obiektu:** Wybierz Video Detection, aby włączyć wykrywanie ruchu w oparciu o wideo podczas monitorowania podejrzanego poruszającego się obiektu.
- **Interwał czasowy:** Jeśli ustawisz domyślny interwał czasowy na 10 sekund, okres wykrywania ruchu będzie wynosił 10 sekund. Zakładając, że ustawiliśmy interwał czasowy na 10, a pierwszy uchwycony ruch może być postrzegany jako punkt początkowy wykrywania ruchu, a jeśli ruch będzie kontynuowany przez 7 sekund z 10-sekundowego interwału, alarm zostanie wyzwolony po 7 sekundach (pierwszy punkt wyzwalania), a akcja wykrywania ruchu może zostać wyzwolona (wysłanie powiadomienia) w dowolnym miejscu między 7-10 sekundami po wykryciu ruchu. 10-sekundowy interwał to pełny cykl wykrywania ruchu przed rozpoczęciem kolejnego cyklu o tym samym interwale czasowym. Aby być bardziej szczegółowym, pierwszy punkt wyzwalania można obliczyć jako **interwał czasowy minus trzy**.
- **Action To Execute (Działanie do wykonania)**: Ustaw żądane działania, które mają być wykonywane po wykryciu podejrzanego ruchu.
    - FTP: wysłanie zrzutu ekranu na wstępnie skonfigurowany serwer FTP.
    - E-mail: Wyślij zrzut ekranu na wstępnie skonfigurowany adres e-mail.
    - Połączenie SIP: Połączenie z ustawionym numerem po wyzwoleniu.
    - HTTP: Po uruchomieniu komunikat HTTP może zostać przechwycony i

wyświetlony w odpowiednich pakietach. Aby skorzystać z tej funkcji, należy włączyć serwer HTTP i wprowadzić treść wiadomości w wyznaczonym polu poniżej.

- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/treść wiadomości.

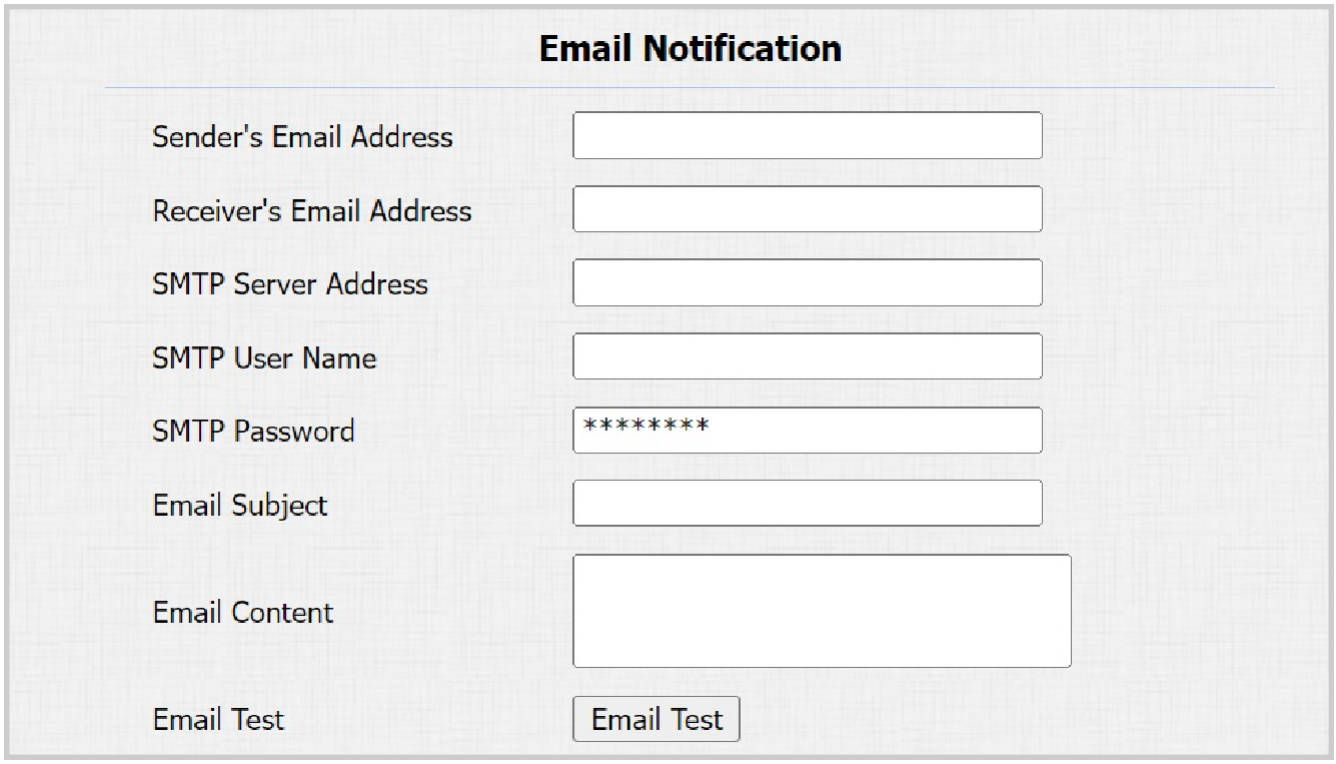
Powiadomienie o zabezpieczeniach

Powiadomienie bezpieczeństwa informuje użytkowników lub pracowników ochrony o wszelkich naruszeniach lub zagrożeniach wykrytych przez bramofon. Na przykład, jeśli bramofon wykryje coś nietypowego, system wysyła powiadomienie do użytkowników lub ochrony za pośrednictwem wiadomości e-mail, połączenia telefonicznego lub innych metod.

Aby skonfigurować powiadomienia bezpieczeństwa, przejdź do opcji **Ustawienia >** Interfejs **akcji.**

Powiadomienie e-mail

Skonfiguruj powiadomienia e-mail, aby otrzymywać zrzuty ekranu nietypowego ruchu z bramofonu. Skonfiguruj to w sekcji **Powiadomienia e-mail.**



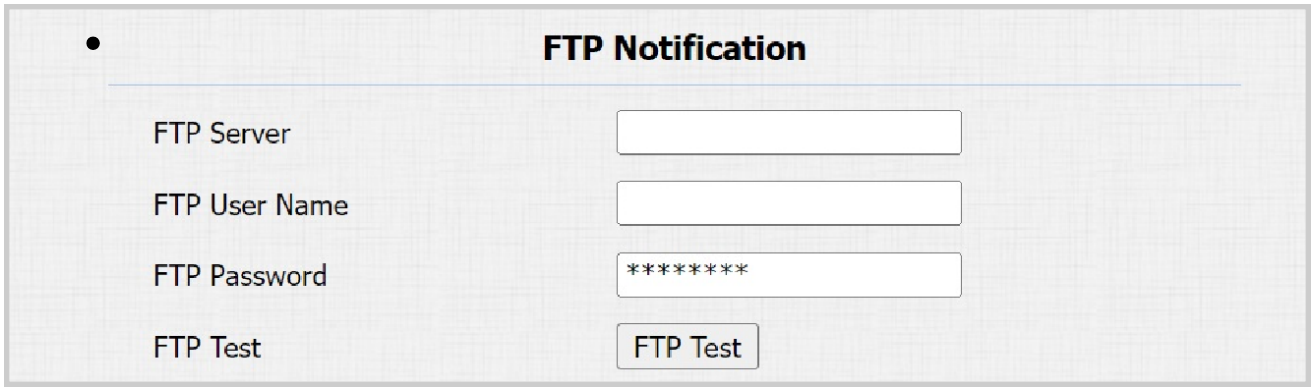
- **Adres serwera** SMTP: Adres serwera SMTP nadawcy.

- **Nazwa użytkownika SMTP**: Nazwa użytkownika SMTP jest zwykle taka sama jak adres e-mail nadawcy.
- **Hasło SMTP** : Hasło usługi SMTP jest takie samo jak adres e-mail nadawcy.
- **Test wiadomości e-mail**: Służy do testowania możliwości wysyłania i odbierania wiadomości e-mail.

Powiadomienie 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.

Skonfiguruj ją w sekcji **Powiadomienia FTP.**



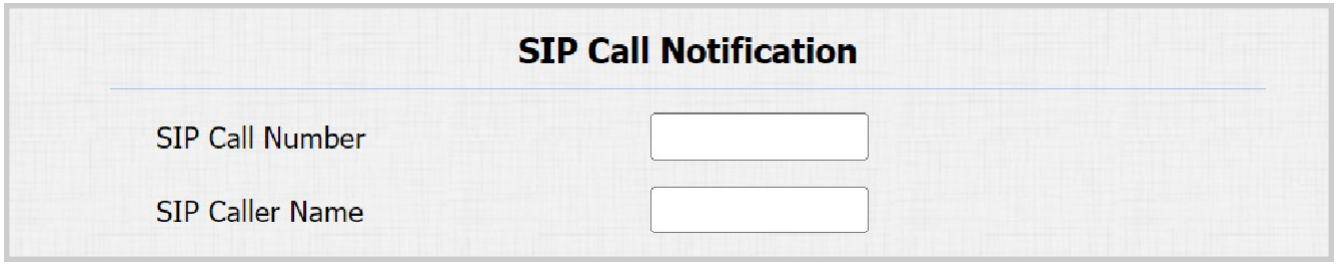
Serwer FTP: Ustaw adres (URL) serwera FTP.

- **Nazwa użytkownika FTP**: Wprowadź nazwę użytkownika, aby uzyskać dostęp do serwera FTP.
- **Hasło FTP** : Wprowadź hasło dostępu do serwera FTP.
- **Test FTP:** Służy do testowania, czy powiadomienie FTP może być wysyłane i odbierane przez serwer FTP.

Powiadomienie o połączeniu SIP

Oprócz powiadomień FTP i e-mail, bramofon może również wykonać połączenie SIP po uruchomieniu określonej funkcji.

Skonfiguruj ją w sekcji **Powiadomienie o połączeniu SIP.**



Powiadomienie HTTP

Można również skonfigurować komunikat HTTP wysyłany do serwera HTTP.

Ustaw adres URL HTTP podczas konfigurowania żądanych działań. Format adresu URL to http://HTTP IP serwera/Treść wiadomości.

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 lub dostęp do karty RF.

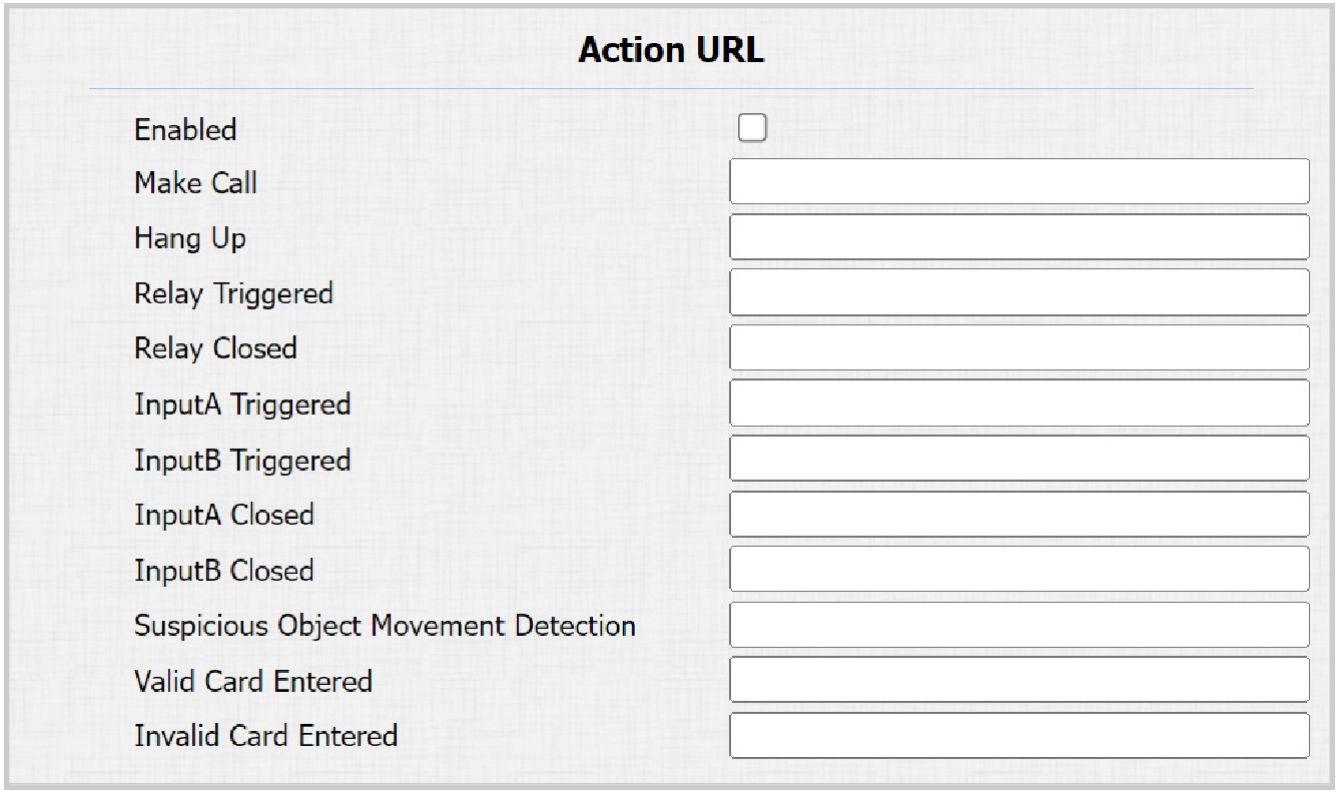
Akuvox Action URL:

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

5	Wejście wyzwalane	$input1status	Http://server ip/inputtrigger=$input1status
6	Wejście zamknięte	$input1status	Http://server ip/inputclose=$input1status
7	Wykrywanie ruchu podejrzanych obiektów	$active_user	Http://server ip/active_user=$active_user
8	Wprowadzona ważna karta	$card_sn	Http://server ip/validcard=$card_sn
9	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

Aby ją skonfigurować, przejdź do interfejsu **Ustawienia > Action URL.**



Szyfrowanie głosu

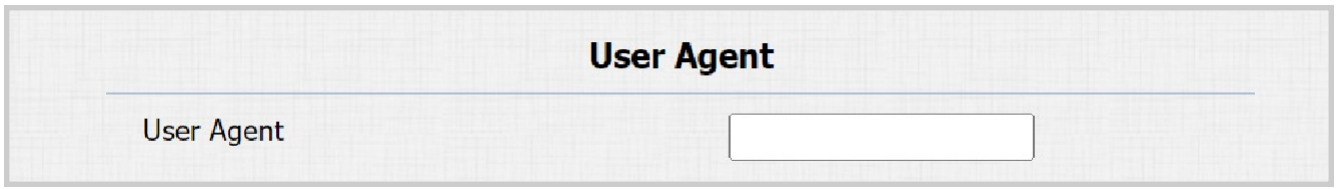
Secure Real-time Transport Protocol (SRTP) to protokół wywodzący się z Real-time Transport Protocol (RTP). Zwiększa on bezpieczeństwo transmisji danych, zapewniając szyfrowanie, uwierzytelnianie wiadomości, zapewnienie integralności i ochronę przed powtórkami.

Skonfiguruj go w interfejsie **Konto** internetowe **> Zaawansowane > Szyfrowanie.**

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

Agent użytkownika

Agent użytkownika służy do identyfikacji podczas analizy pakietu danych SIP. Aby go skonfigurować, przejdź do interfejsu **Account > Advanced > User Agent.**



- **Agent użytkownika:** Akuvox jest domyślnie.

Akcja ratunkowa

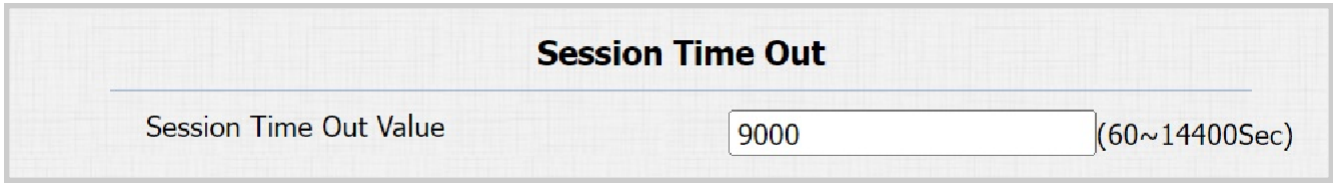
Ta funkcja działa z Akuvox SmartPlus Cloud. Utrzymuje drzwi otwarte w sytuacji awaryjnej.

Aby ją skonfigurować, przejdź do **Security > Basic > Emergency Action** interface. Wybierz wejścia, które mają zostać wyzwolone.

Interfejs sieciowy Automatyczne wylogowanie

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

Aby ją skonfigurować, przejdź do opcji **Zabezpieczenia > Podstawowe >** Interfejs **limitu czasu sesji.**



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.

Włącz ją w interfejsie **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 tym trybem. Jeśli jednak zresetujesz urządzenie do ustawień fabrycznych, tryb ten będzie domyślnie włączony.

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

-PC Manager: 1.2.0.0

-IP Scanner: 2.2.0.0

-Upgrade Tool: 4.1.0.0

-SDMC: 6.0.0.34

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

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

otwierania drzwi.

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

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

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

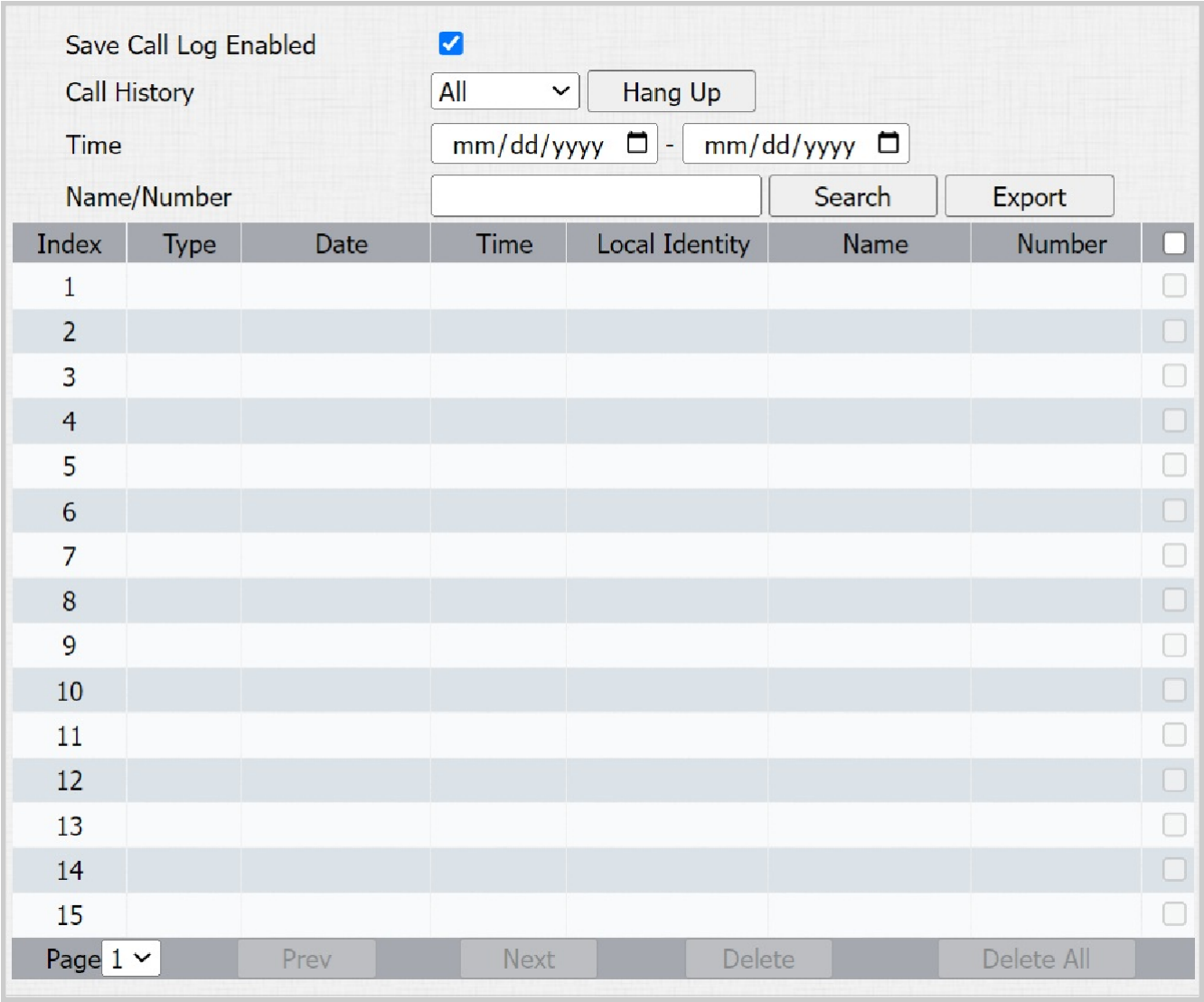
4. Niedozwolone jest importowanie/eksportowanie plików konfiguracyjnych w formacie tgz. między urządzeniem z trybem wysokiego bezpieczeństwa a innym bez niego. Aby uzyskać pomoc dotyczącą przesyłania plików, skontaktuj się z pomocą techniczną Akuvox.

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 **Interkom > Rejestr połączeń.**



- **Historia połączeń: Istnieją** cztery rodzaje dzienników połączeń: Wszystkie, Wybrane, Odebrane i Nieodebrane.

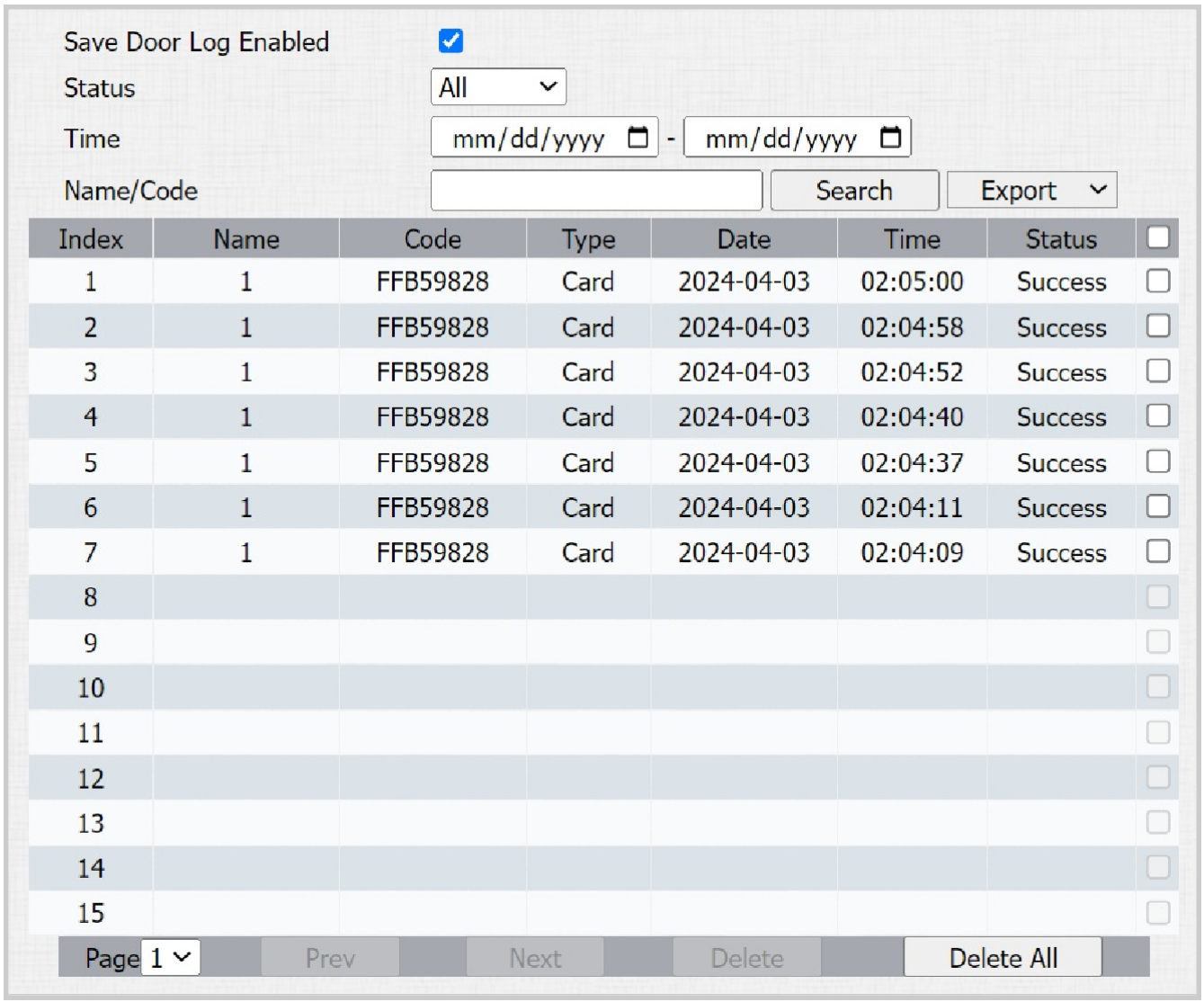
- **Czas:** wyszukiwanie żądanego rejestru połączeń poprzez wprowadzenie określonego okresu.

- **Nazwa/Numer:** Wyszukiwanie żądanego rejestru połączeń poprzez wprowadzenie nazwy i numeru.

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 **Kontrola dostępu > Dziennik drzwi.**



- **Status:** Wyświetla wszystkie, udane i nieudane otwarcia drzwi.

- **Czas:** wyszukiwanie żądanego rejestru połączeń poprzez wprowadzenie określonego okresu.

- **Nazwa:** Wyświetla nazwę użytkownika. Jeśli jest to nieznany klucz lub karta, wyświetli się Nieznany.

- **Kod:** Jeśli drzwi są otwierane za pomocą kart RF, wyświetlony zostanie kod karty. Jeśli drzwi są otwierane za pomocą polecenia HTTP, będzie ono puste.

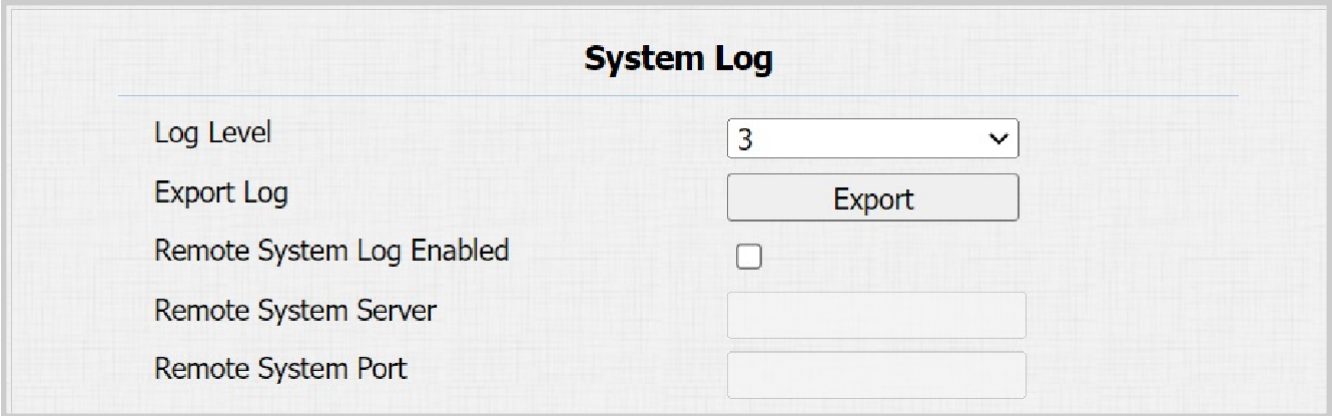
- **Typ:** Wyświetla metody dostępu.

Debugowanie

Dziennik systemowy

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Aby ją skonfigurować, przejdź do interfejsu internetowego **Upgrade > Diagnose > System Log.**

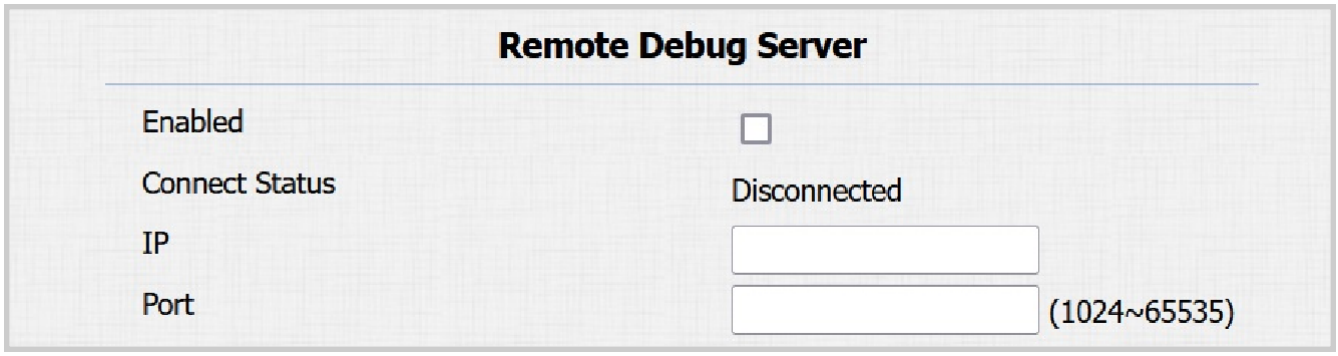


- **Poziom dziennika:** Wybierz poziom dziennika od 1 do 7 poziomów. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić do celów debugowania. Domyślny poziom dziennika to 3. Im wyższy poziom, tym bardziej kompletny jest dziennik.
- **Eksportuj dziennik:** Kliknij kartę Eksportuj, aby wyeksportować tymczasowy plik dziennika debugowania do lokalnego komputera.
- **Zdalny serwer systemu:** Ustaw adres zdalnego serwera, na który ma być przesyłany dziennik urządzenia. Adres serwera zdalnego zostanie dostarczony przez pomoc techniczną Akuvox.
- **Port systemu zdalnego**: Ustaw port serwera systemu zdalnego.

Zdalny serwer debugowania

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

Aby go skonfigurować, przejdź do interfejsu **Upgrade > Diagnose > Remote Debug Server.**

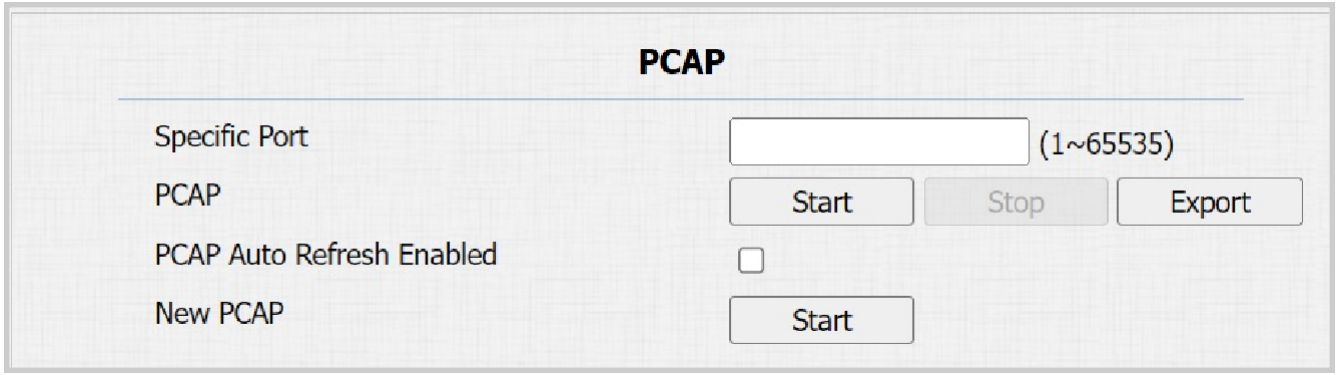


- **Stan połączenia**: wyświetla stan połączenia między urządzeniem a serwerem.
- **IP** : Wprowadź adres IP serwera.
- **Port**: Wprowadź port serwera.

PCAP

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

Skonfiguruj PCAP w interfejsie internetowym **Upgrade > Diagnose > PCAP.**



- **Określony port:** Wybierz określone porty z zakresu 1-65535, aby można było przechwytywać tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.
- **PCAP:** Kliknij kartę Start i Stop, aby przechwycić określony zakres pakietów danych przed kliknięciem karty Eksport, aby wyeksportować pakiety danych do lokalnego komputera.
- **Automatyczne odświeżanie PCAP:** Jeśli ta opcja jest włączona, PCAP będzie kontynuował przechwytywanie pakietów danych nawet po osiągnięciu przez nie maksymalnej pojemności 1 MB. Jeśli jest wyłączona, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycony pakiet danych osiągnie maksymalną pojemność

przechwytywania 1 MB.

- **Nowy PCAP:** Kliknij Start, aby przechwycić większy pakiet danych.

Kopia zapasowa

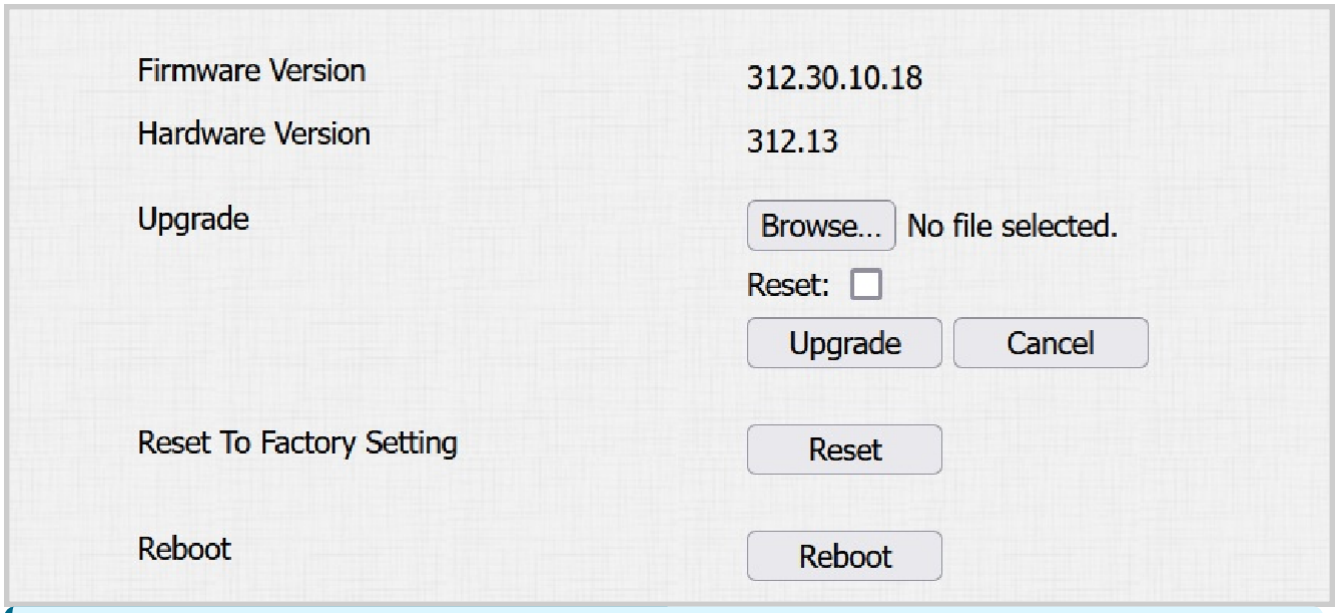
Zaszyfrowane pliki konfiguracyjne można importować lub eksportować do komputera lokalnego.

Wyeksportuj plik w interfejsie **Upgrade > Diagnose > Others.**

Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można aktualizować w interfejsie internetowym

urządzenia. Zaktualizuj urządzenie w interfejsie **Upgrade > Basic.**



Uwaga

Pliki aktualizacji powinny być w formacie .rom.

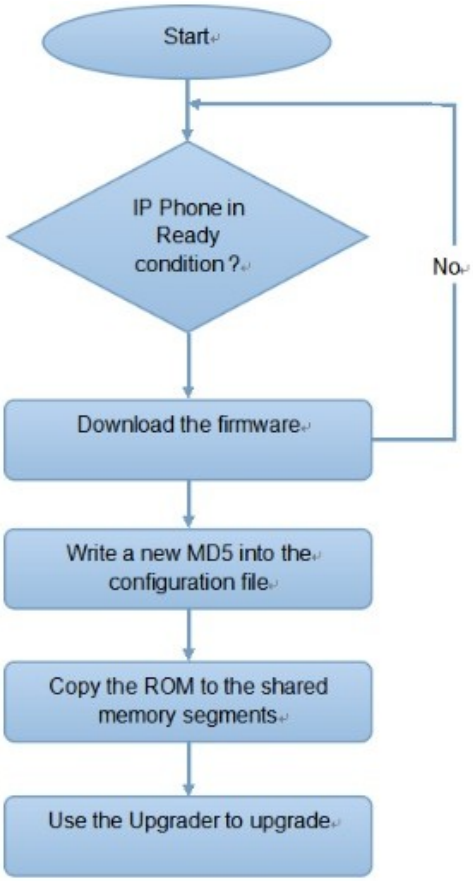
Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

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

Zasada udostępniania

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

Zobacz poniższy schemat blokowy:



Pliki konfiguracyjne dla automatycznego przydzielania

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

Poniżej przedstawiono różnicę między tymi dwoma typami plików konfiguracyjnych:

- **Udostępnianie konfiguracji ogólnej**: plik ogólny jest przechowywany na serwerze, z którego wszystkie powiązane urządzenia będą mogły pobrać ten sam plik konfiguracyjny w celu aktualizacji parametrów na urządzeniach, takich jak cfg.
- **Udostępnianie konfiguracji opartej na MAC**: Pliki konfiguracyjne oparte na MAC są używane do automatycznego udostępniania na określonym urządzeniu, zgodnie z jego unikalnym numerem MAC. Pliki konfiguracyjne nazwane za pomocą numeru MAC urządzenia zostaną automatycznie dopasowane do numeru MAC urządzenia przed pobraniem w celu udostępnienia na określonym urządzeniu.

Uwaga

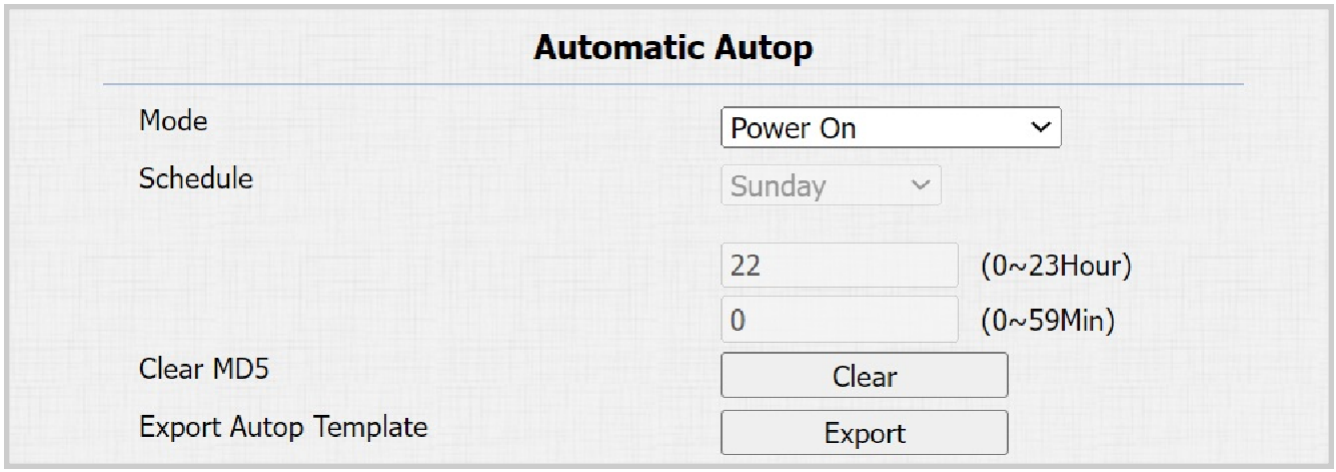
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny dla provisioningu wsadowego różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC dla konkretnego provisioningu urządzenia jest nazywany według jego adresu MAC.
- Jeśli serwer ma te dwa typy plików konfiguracyjnych, urządzenia najpierw uzyskają dostęp do ogólnych plików konfiguracyjnych przed uzyskaniem dostępu do plików konfiguracyjnych opartych na adresie MAC.

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

Harmonogram AutoP

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

Aby ją skonfigurować, przejdź do **Upgrade > Advanced > Automatic Autop** interface.

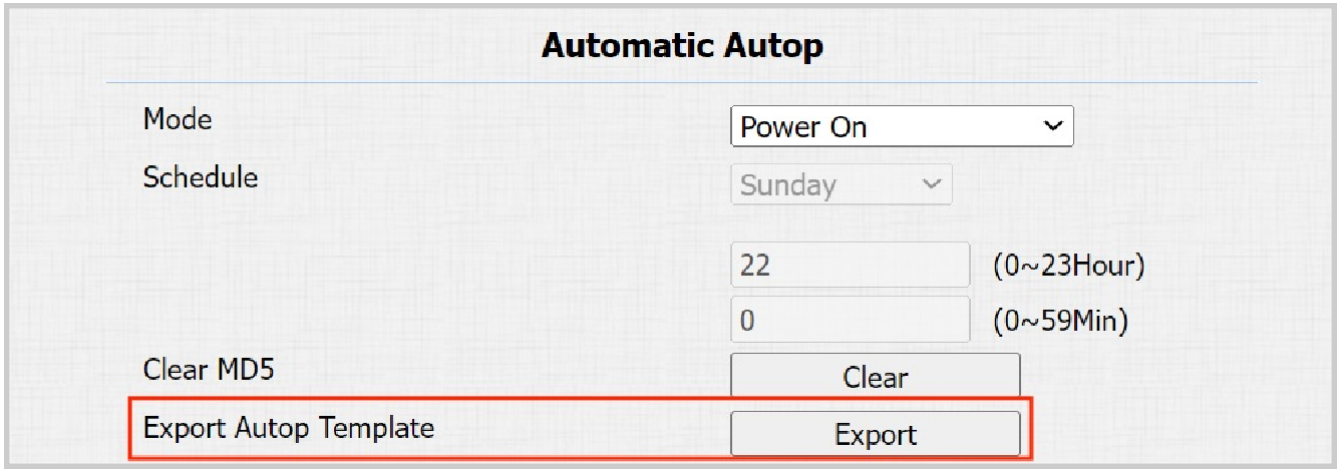


- **Tryb** :
  - **Power On**: Urządzenie wykona Autop przy każdym uruchomieniu.
  - **Wielokrotnie**: Urządzenie wykona funkcję Autop zgodnie z ustawionym harmonogramem.
  - **Power On + Repeatedly**: Połączenie trybów **Power On** i **Repeatedly**, które umożliwią urządzeniu wykonywanie funkcji Autop przy każdym uruchomieniu lub zgodnie z ustawionym harmonogramem.
  - **Hourly Repeat (Powtarzanie co godzinę):** Urządzenie będzie wykonywać funkcję Autop co godzinę.

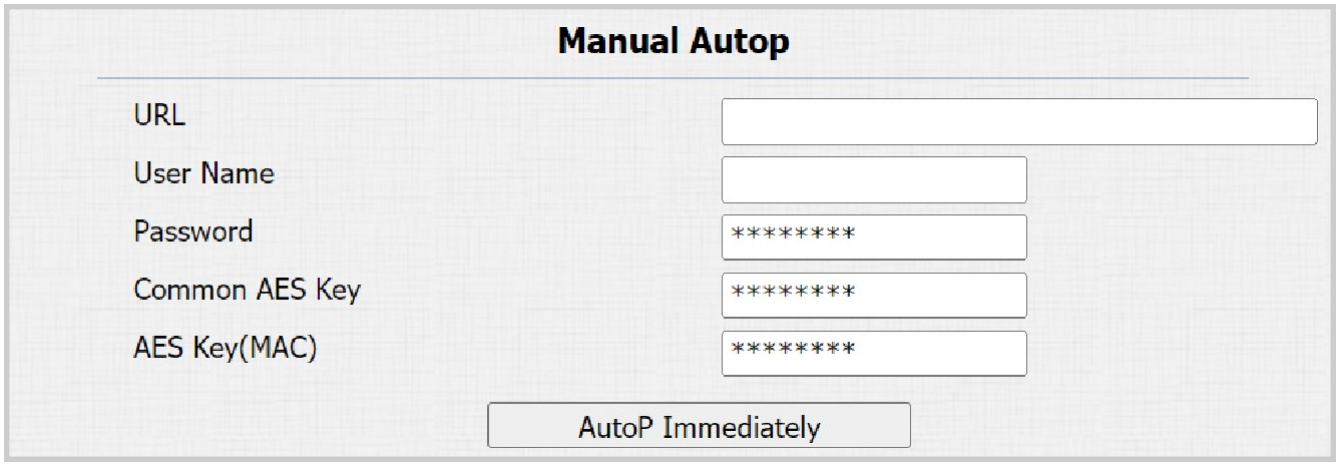
Udostępnianie statyczne

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

Aby ją skonfigurować, należy najpierw pobrać szablon w interfejsie **Upgrade > Advanced > Automatic Autop.**



Skonfiguruj serwer Autop w sekcji **Ręczny Autop.**



- **URL** : Określa adres serwera TFTP, HTTP, HTTPS lub FTP dla provisioningu.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika, jeśli serwer wymaga nazwy użytkownika, aby uzyskać do niego dostęp.
- **Hasło** : Wprowadź hasło, jeśli dostęp do serwera wymaga podania hasła.
- **Wspólny klucz AES**: Jest używany przez interkom do odszyfrowania ogólnych plików konfiguracyjnych Autop.
- **Klucz AES (MAC)**: Służy do odszyfrowania przez interkom pliku konfiguracyjnego Autop opartego na MAC.

Uwaga

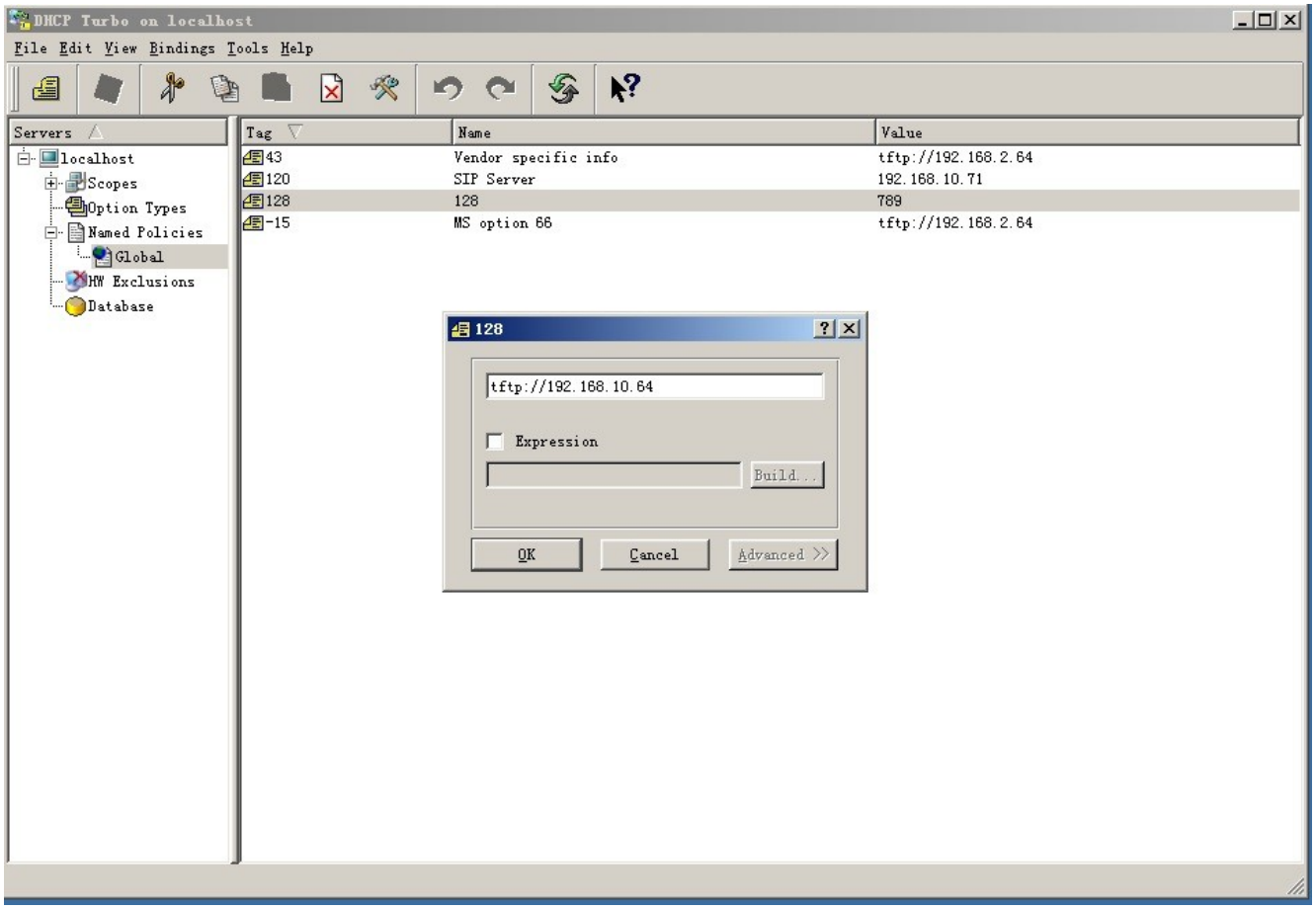
- AES jako jeden z typów szyfrowania powinien być skonfigurowany tylko wtedy, gdy plik konfiguracyjny jest zaszyfrowany za pomocą AES.
- Format adresu serwera:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(umożliwia anonimowe logowanie) ftp://username:password@192.168.0.19/(wymaga nazwy 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. Należy samodzielnie przygotować serwer TFTP/FTP/HTTP/HTTPS.

Konfiguracja udostępniania DHCP

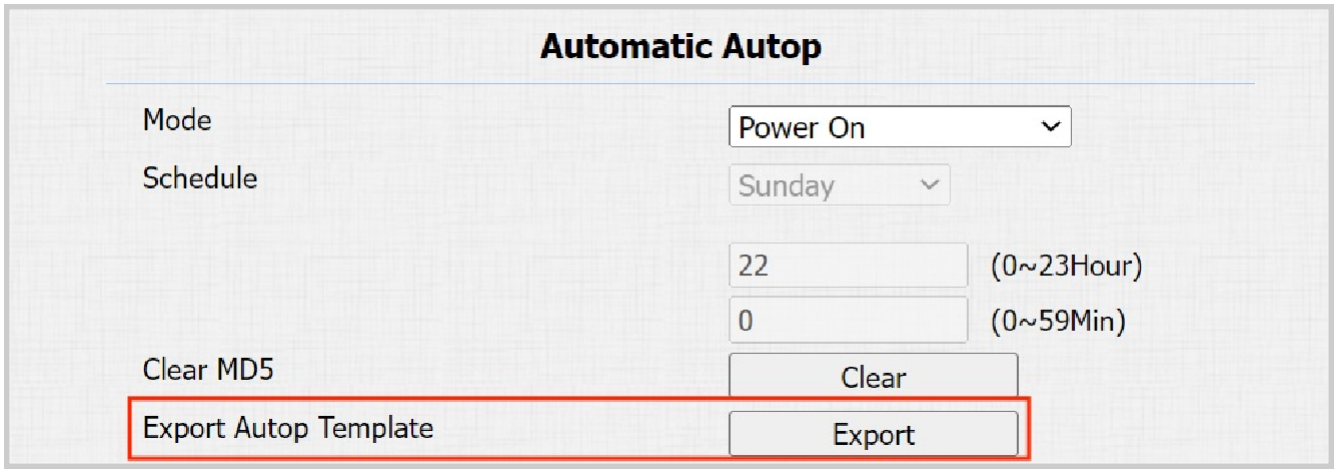
Adres URL automatycznego dostarczania można również uzyskać za pomocą opcji DHCP, która umożliwia urządzeniu wysłanie żądania do serwera DHCP dla określonego kodu opcji DHCP. Jeśli chcesz użyć
Opcja niestandardowa zdefiniowana przez użytkowników z kodami opcji w zakresie 128-255), należy skonfigurować opcję niestandardową DHCP w interfejsie internetowym.



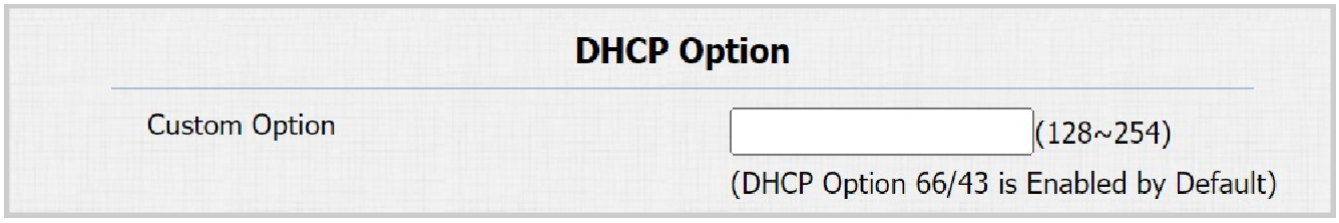
Uwaga

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

Skonfiguruj DHCP Autop z trybem Power On i wyeksportuj Autop Template, aby edytować konfigurację. Przejdź do **Upgrade > Advanced > Automatic Autop** interface.



Aby skonfigurować opcję DHCP, przewiń do sekcji **Opcja DHCP.**

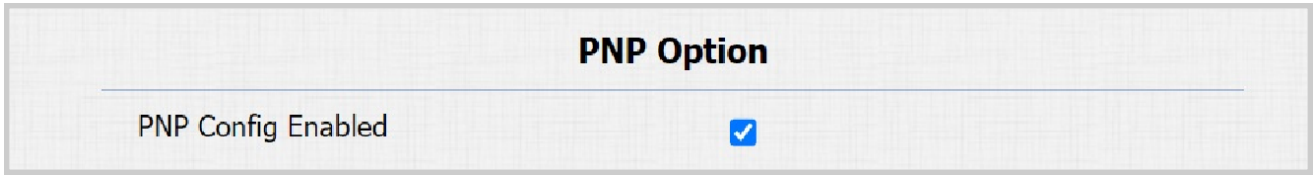


- **Opcja niestandardowa**: Wprowadź kod DHCP pasujący do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych do konfiguracji lub aktualizacji.
- **Opcja 43 DHCP**: Jeśli urządzenie nie otrzyma adresu URL z Opcji 66 DHCP, automatycznie użyje Opcji 43 DHCP. Odbywa się to w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

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.

Skonfiguruj ją w interfejsie **Upgrade > Advanced > PNP Option.**

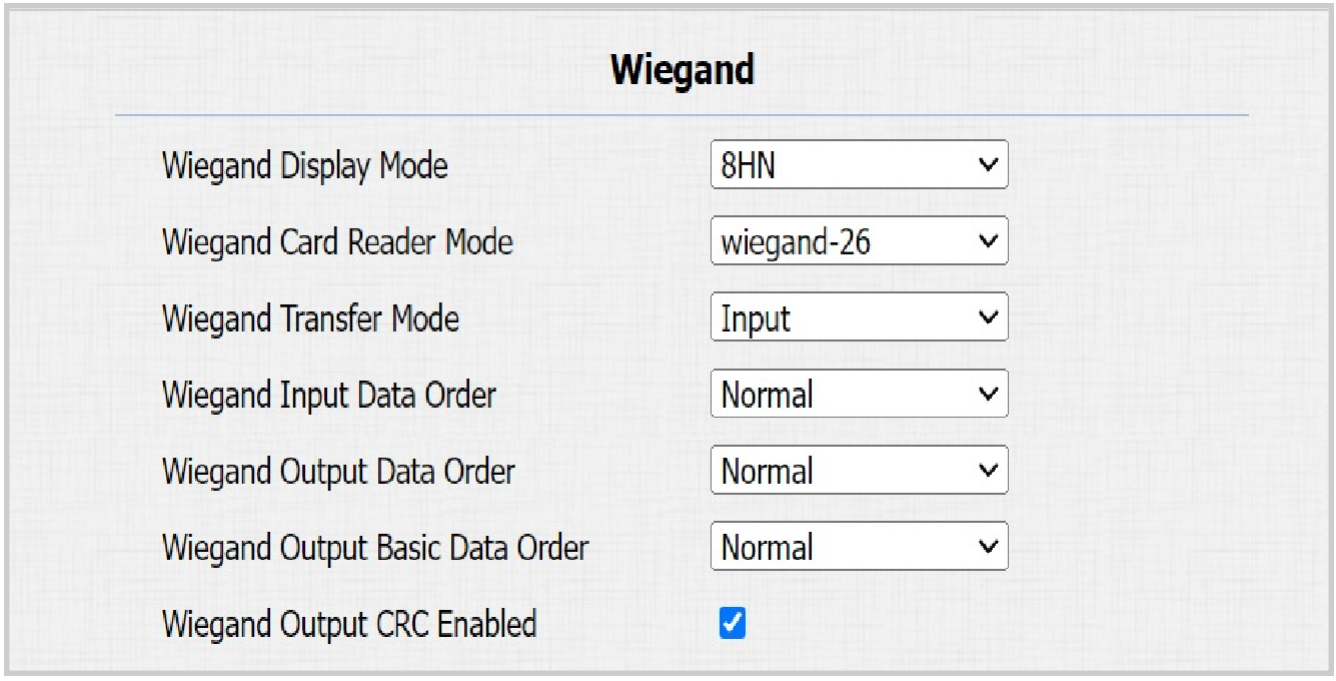


Integracja z urządzeniami innych firm

Integracja przez Wiegand

Urządzenie można zintegrować z urządzeniami innych firm za pośrednictwem Wiegand.

Skonfiguruj go w interfejsie **Access Control > Card Setting > Wiegand.**



- **Tryb wyświetlania Wiegand** : Wybierz format kodu karty Wiegand spośród dostępnych opcji.
- **Tryb czytnika kart Wiegand**: Format transmisji powinien być identyczny między terminalem kontroli dostępu a urządzeniem innej firmy. Jest on konfigurowany automatycznie.
- **Tryb transferu Wiegand** :
    - **Wejście**: Urządzenie służy jako odbiornik.

- **Wyjście**: Urządzenie służy jako nadajnik. Jeśli użytkownicy mogą otwierać drzwi tylko poprzez przeciągnięcie karty RF, wybierz tryb transferu Wiegand jako Wyjście.
- **Konwertuj na kartę nr Wyjście**: Urządzenie służy jako nadajnik. Jeśli użytkownikom przypisano wiele metod otwierania drzwi, wybierz tryb transferu Wiegand jako Convert To Card No. Output.

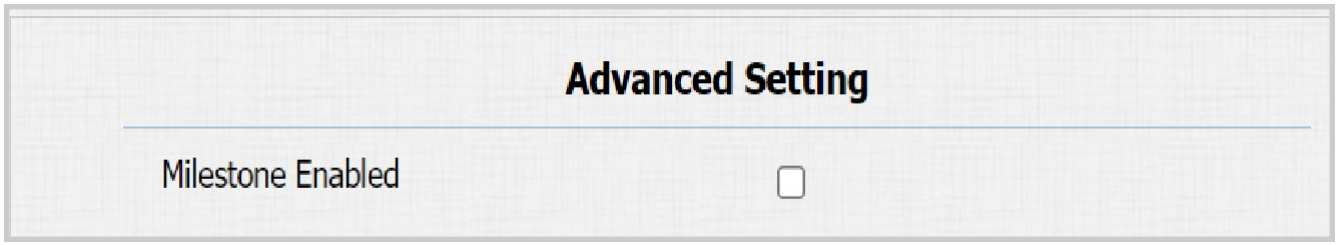
- **Kolejność danych wejściowych Wiegand**: Ustawienie kolejności danych wejściowych Wiegand pomiędzy Normal i Reversed. W przypadku wybrania opcji Reversed numer karty wejściowej zostanie odwrócony.
- **Kolejność danych wyjściowych Wiegand:** Określa kolejność numeru karty.
  - **Normalnie**: Numer karty jest wyświetlany w takiej postaci, w jakiej został odebrany.
  - **Odwrócona**: Kolejność numerów kart jest odwrócona.
- **Kolejność podstawowych danych wyjściowych Wiegand**: Ustawia kolejność danych wyjściowych Wiegand.
  - **Normalnie**: Dane są wyświetlane w takiej postaci, w jakiej zostały odebrane.
  - **Reversed**: Kolejność bitów danych jest odwrócona.
- **Wiegand Output CRC Enabled**: Jest domyślnie włączona dla kontroli danych Wiegand. Wyłączenie go może prowadzić do niepowodzenia integracji z urządzeniami innych firm.

> **Uwaga**
>
> Kliknij **tutaj**, aby zobaczyć szczegółowe kroki konfiguracji.

Integracja z Milestone

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

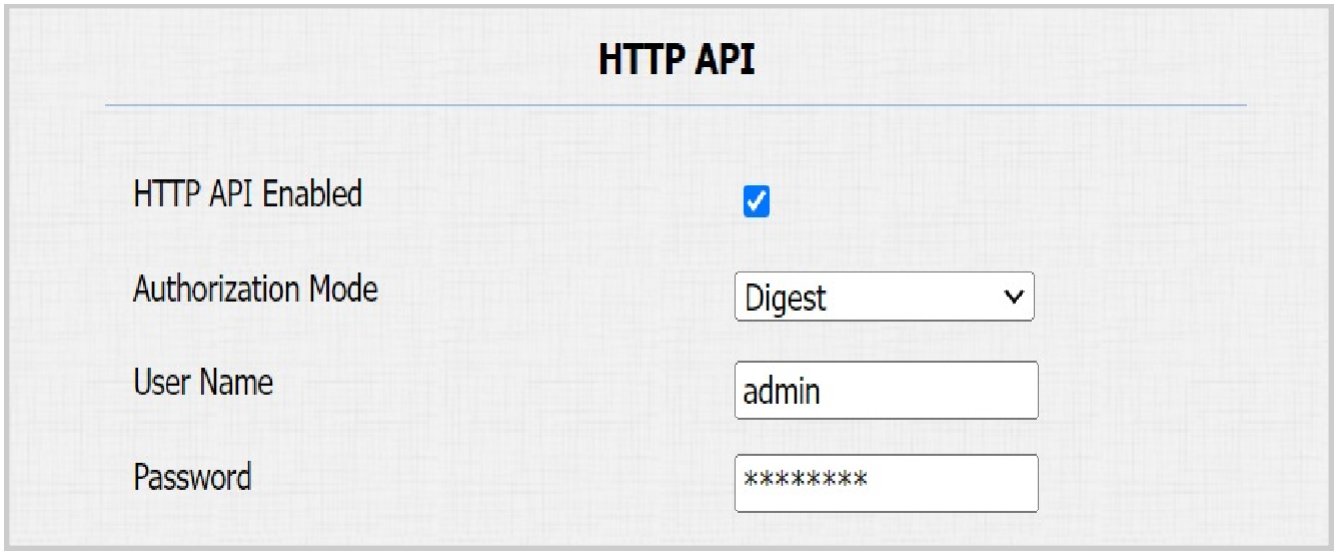
Włącz ją w interfejsie **Surveillance > ONVIF > Advanced Setting.**



Integracja przez HTTP API

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

Skonfiguruj go w interfejsie Web **Security > HTTP API.**



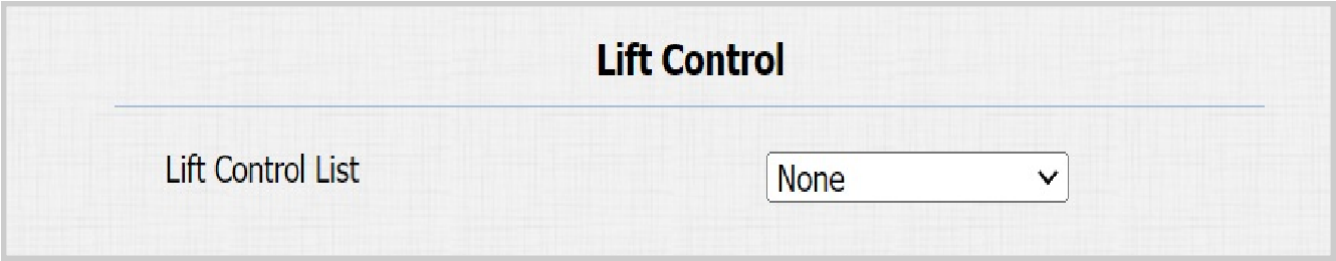
- **Enabled** : Włącz lub wyłącz funkcję HTTP API dla integracji z innymi firmami. Jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.
- **Tryb autoryzacji** : Domyślnie jest to Digest. Wymagane jest podanie nazwy użytkownika i hasła w celu uwierzytelnienia. W polu Authorization nagłówka żądania HTTP użyj metody kodowania Base64, aby zakodować nazwę użytkownika i hasło.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika do uwierzytelniania. Domyślnie jest to admin.

- **Hasło**: Wprowadź hasło uwierzytelniania. Domyślnie jest to admin.

Kontrola podnoszenia

Bramofony można podłączyć do sterownika windy Akuvox w celu sterowania windą. Użytkownicy mogą wezwać windę, aby zjechała na parter, gdy uzyskają dostęp za pomocą różnych metod dostępu na bramofonie.

Skonfiguruj go w interfejsie **Access Control > Lift Control.**



- **Life Control List:** Wybierz markę sterownika windy.
    - Brak: Integracja RS485 zostanie wyłączona.

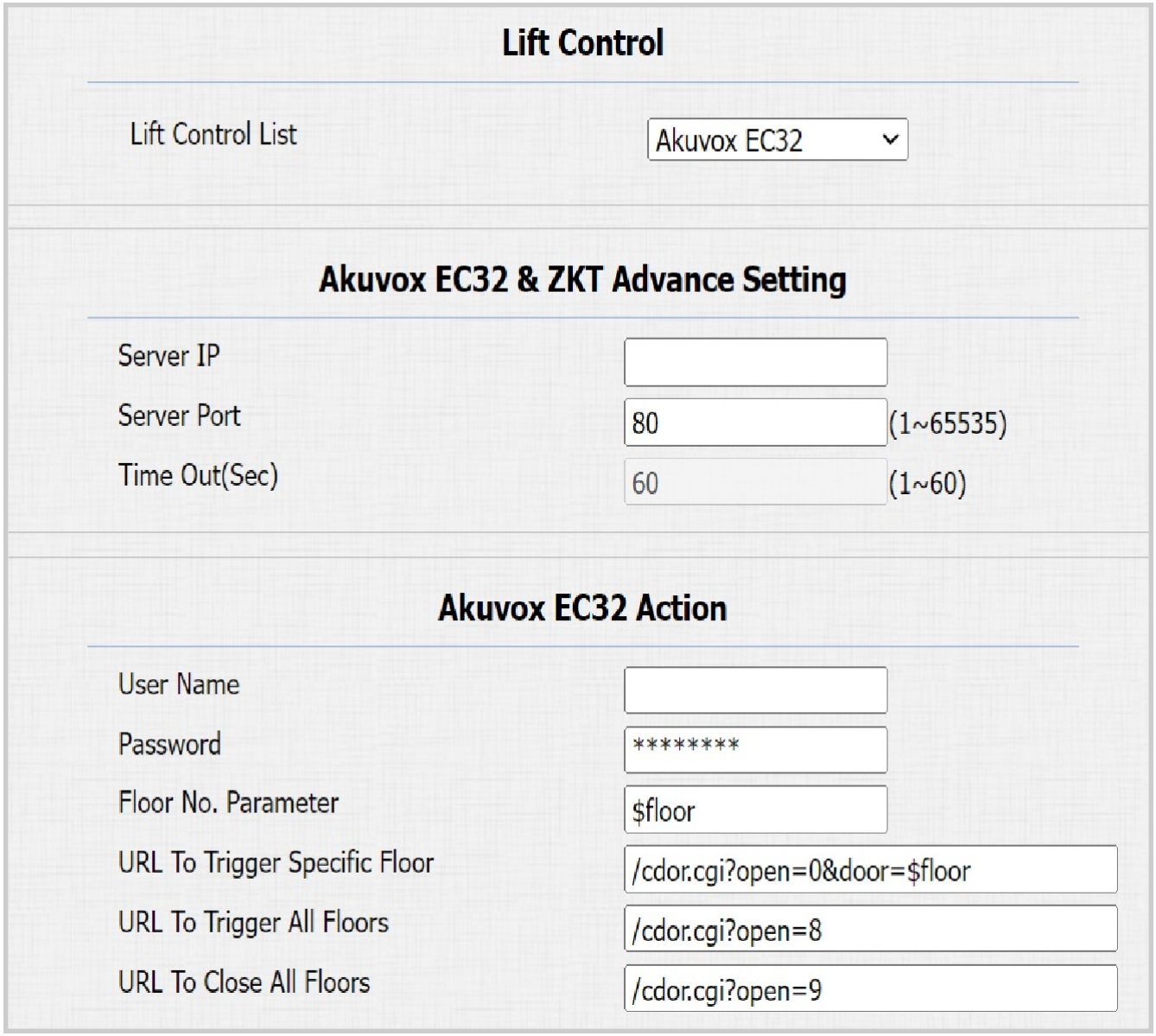
      Akuvox EC32: Podłącz urządzenie do kontrolera windy Akuvox EC33.

    ZKT: Integracja z kontrolerem windy ZKTeco.

> **Uwaga**
>
> W przypadku jakichkolwiek pytań dotyczących trybu integracji dowolnego projektu integracji sterownika windy OEM należy skonsultować się z pomocą techniczną Akuvox. Kliknij **tutaj**, aby wyświetlić przykładową konfigurację Lift Control.

Kontroler windy Akuvox

Po wybraniu Akuvox EC32 na liście Lift Control List, należy skonfigurować odpowiednie parametry.



- **IP serwera:** Wprowadź adres IP kontrolera windy Akuvox.

  Port serwera: Wprowadź port kontrolera windy Akuvox.

  Time Out(Sec): Określa limit czasu, w którym użytkownicy powinni nacisnąć przycisk windy na wybranym piętrze.

  Nazwa użytkownika: Wprowadź nazwę użytkownika ustawioną w sterowniku windy.

  Hasło: Wprowadź hasło ustawione w sterowniku windy.

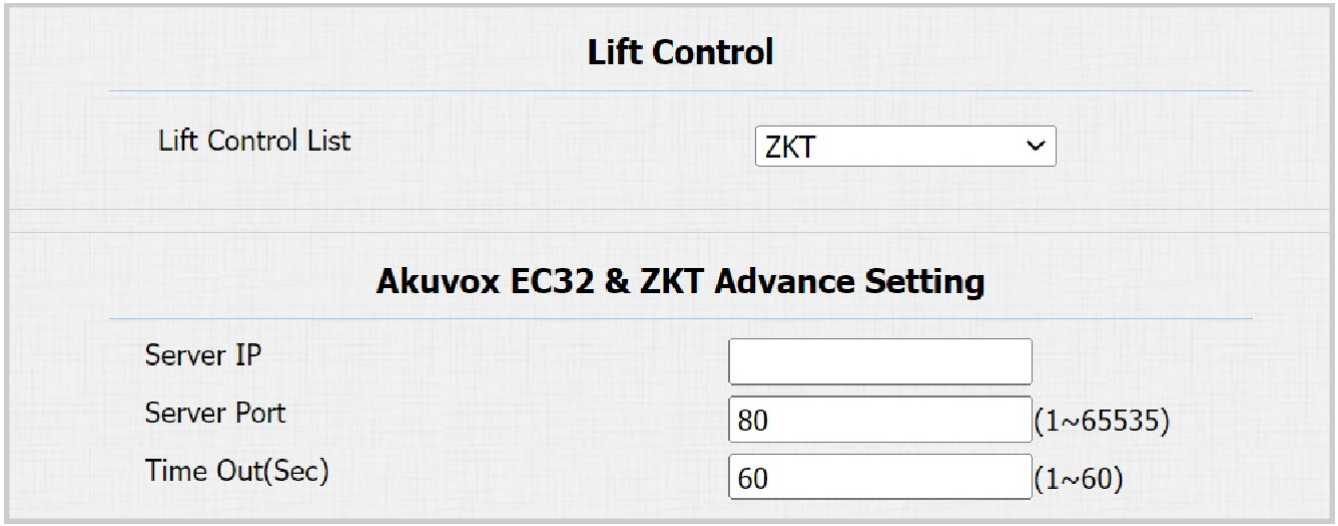
  Floor NO. Parametr: Parametr numeru piętra jest dostarczany przez Akuvox. Domyślnie jest to

  $floor. Można zdefiniować własny ciąg parametrów.

- **Adres URL do wyzwalania określonego piętra:** Adres URL sterowania windą Akuvox do wyzwalania określonego piętra. Adres URL to /cdor.cgi?open=0&door=$ floor, ale ciąg $floor na końcu musi być identyczny z ciągiem parametrów zdefiniowanym przez użytkownika.
- **Adres URL do wyzwalania wszystkich pięter:** Adres URL Akuvox do wyzwalania wszystkich pięter.
- **Adres URL do zamykania wszystkich pięter:** Adres URL Akuvox do zamykania wszystkich pięter.

Kontroler windy ZKT

Po wybraniu ZKT należy skonfigurować odpowiednie parametry.

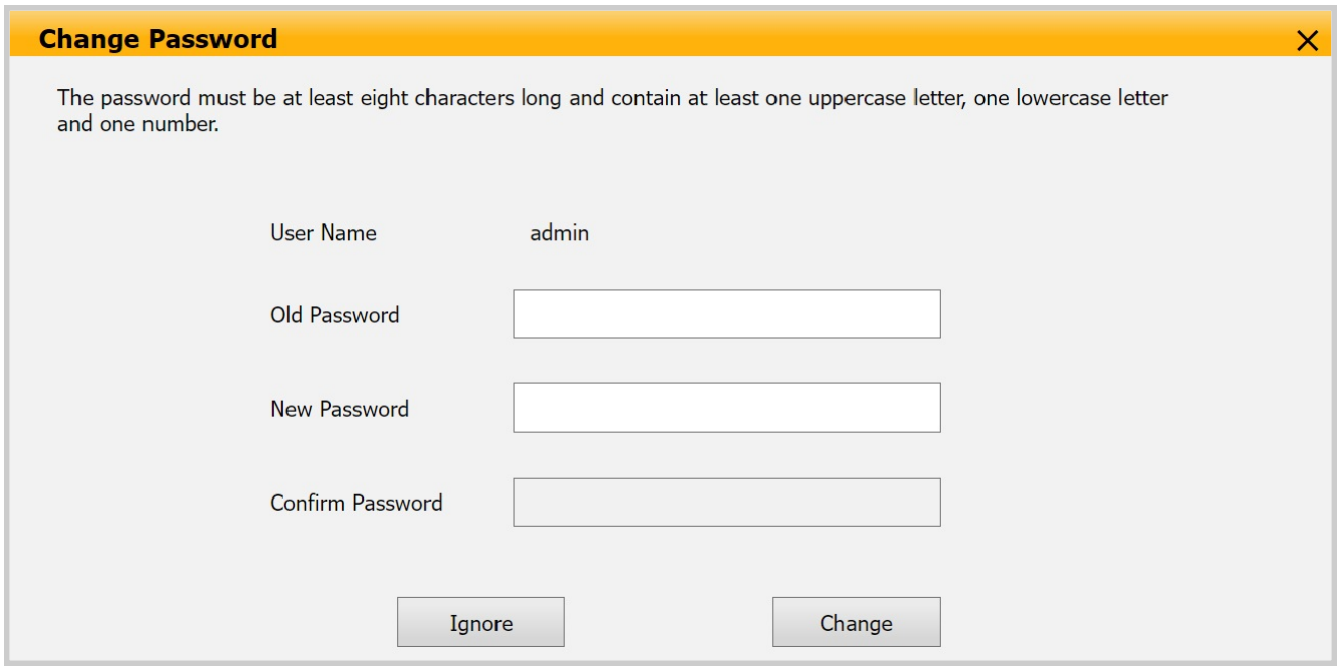


- **Server IP:** Wprowadź adres IP serwera kontrolera.
- **Port:** Wprowadź port serwera kontrolera.
- **Time Out(Sec):** Określa limit czasu, w którym użytkownicy powinni nacisnąć przycisk windy na wybranym piętrze.

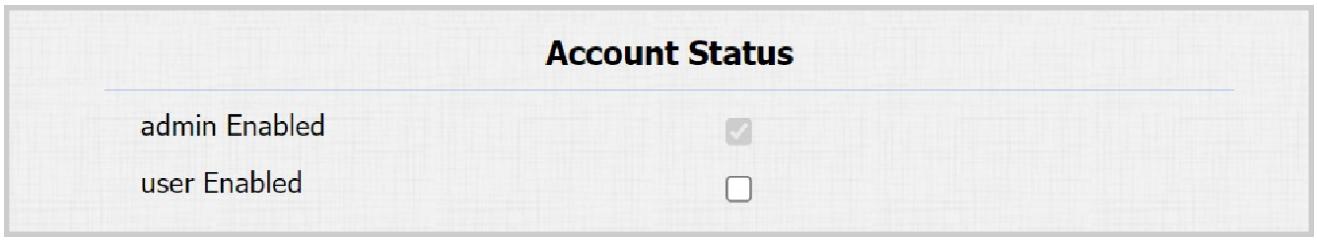
Modyfikacja hasła

Hasło internetowe urządzenia można modyfikować zarówno dla konta administratora, jak i konta użytkownika. Aby to zrobić, przejdź do interfejsu **Security > Basic > Web Password Modify.**

Kliknij przycisk **Zmień hasło**, aby zmodyfikować hasło.



Aby włączyć lub wyłączyć konto użytkownika, przewiń do sekcji **Stan konta.**

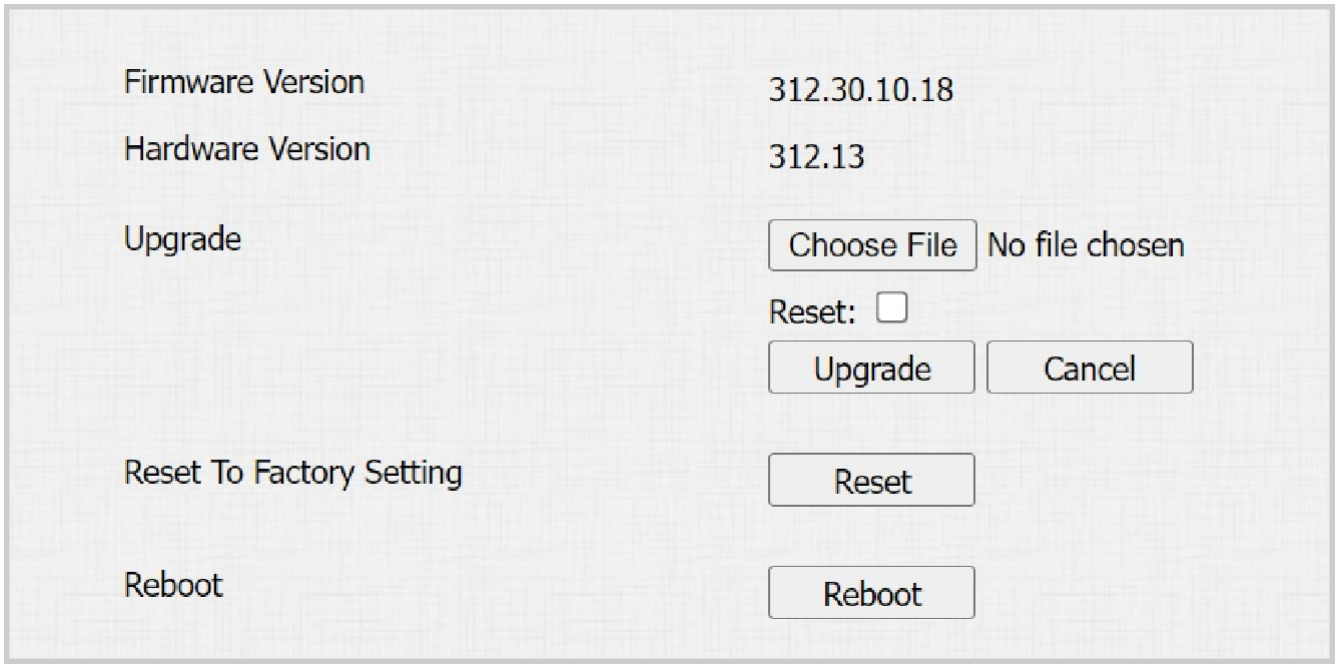


Ponowne uruchamianie i resetowanie systemu

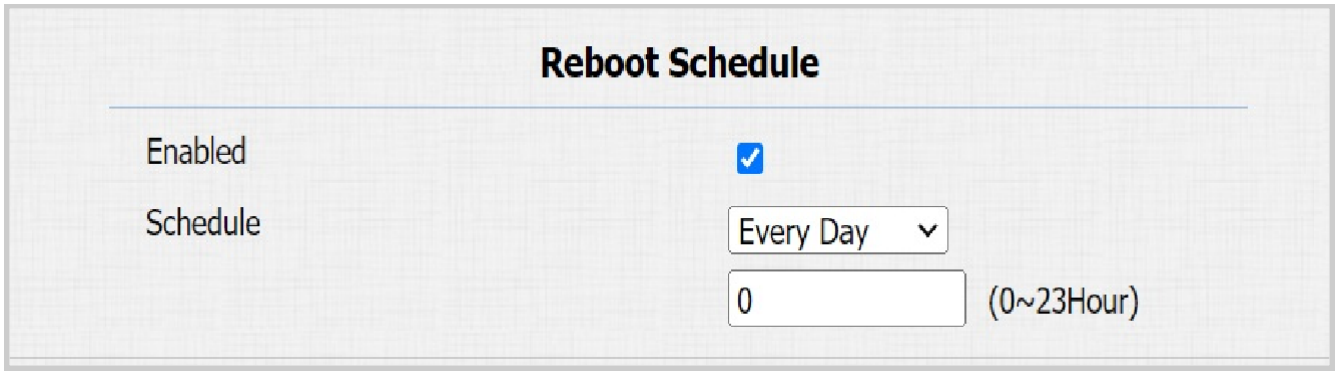
Reboot

Jeśli chcesz ponownie uruchomić system urządzenia, możesz to zrobić na stronie internetowej urządzenia. Ponadto można skonfigurować harmonogram ponownego uruchamiania urządzenia.

Przejdź do interfejsu **Upgrade > Basic.**



Aby skonfigurować harmonogram, przejdź do interfejsu **Aktualizacja > Zaawansowane.**



Reset

Zresetuj urządzenie w interfejsie internetowym **Upgrade > Basic.**