Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX S532
DOOR PHONE
Administrator Guide

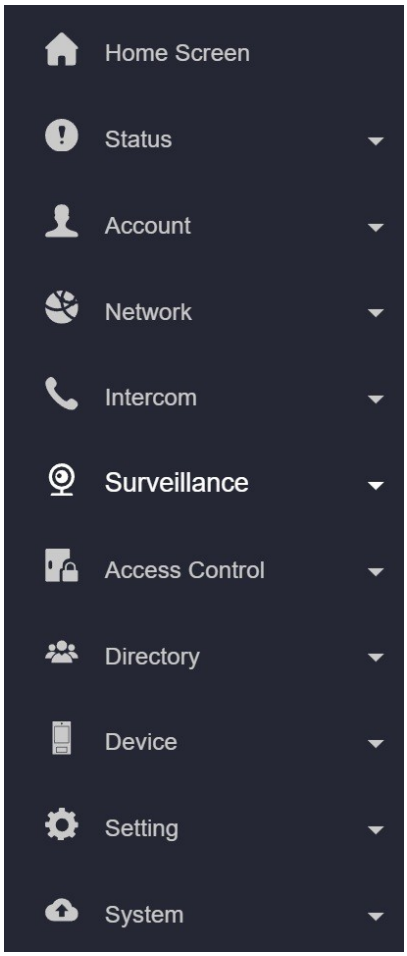
Dziękujemy za wybranie bramofonów Akuvox serii S532. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować bramofon. Niniejsza instrukcja dotyczy wersji 532.30.1.19 i zawiera wszystkie konfiguracje funkcji i właściwości bramofonu Akuvox. Odwiedź stronę internetową Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe.

Przegląd produktów

- 2.8" LCD
- Aluminum Body
- **Linux OS**
- Numeric keypad
- Multiple access control (RFID, NFC, Bluetooth)
- **IP to Analog audio/video output (optional)**
- **IK08** & **IP66**

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 itp.
- **Sieć:** ta sekcja dotyczy głównie ustawień DHCP i statycznego adresu IP, ustawień portu RTP, wdrażania urządzeń itp.
- **Interkom**: ta sekcja obejmuje ustawienia LCD, funkcje połączeń, multiemisję itp.
- **Nadzór**: sekcja obejmuje wykrywanie ruchu, ustawienia RTSP, ustawienia ONVIF itp.
- **Kontrola dostępu**: ta sekcja obejmuje ustawienie przekaźnika, ustawienie karty, ustawienie kodu PIN itp.
- **Katalog**: ta sekcja służy do zarządzania użytkownikami.
- **Urządzenie : ta sekcja** obejmuje ustawienia LCD, oświetlenia, wiegand, audio i
- sterowania windą. **Ustawienia**: ta sekcja obejmuje ustawienia czasu i języka, akcji,
- harmonogramu i HTTP API. **System**: ta sekcja służy do aktualizacji, konserwacji, automatycznego dostarczania itp.



Dostęp do urządzenia

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

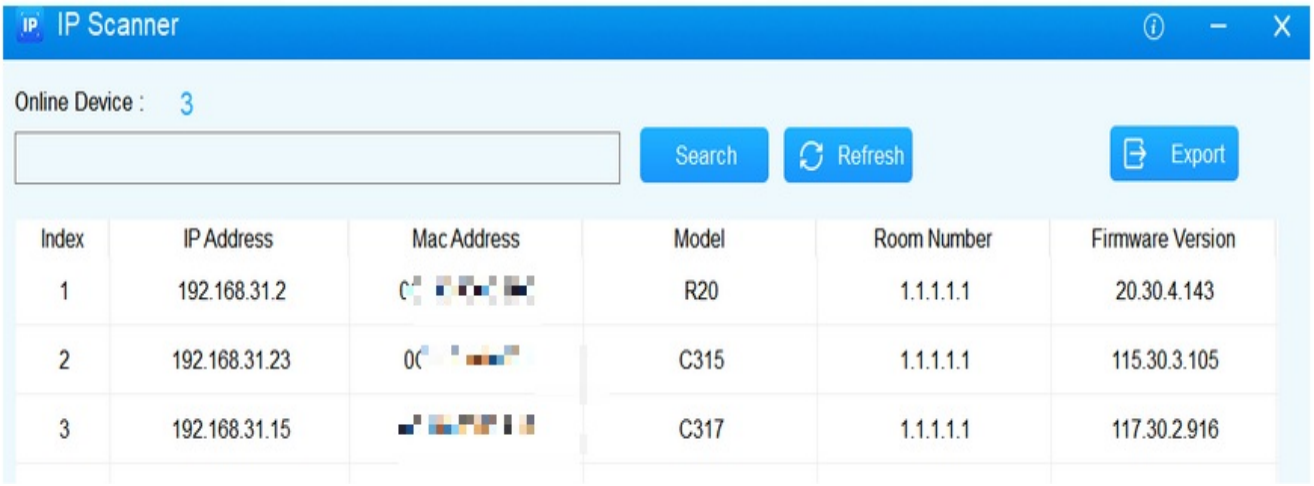
Dostęp do ustawień urządzenia na urządzeniu

Aby uzyskać dostęp do ustawień urządzenia, naciśnij *2396#, aby przejść do ekranu ustawień zaawansowanych. Zapewnia on pewne zaawansowane uprawnienia, takie jak edycja sieci, resetowanie i modyfikacja hasła administratora dla administratorów, w tym **Informacje o systemie, Ustawienia administratora** i **Ustawienia systemu**.

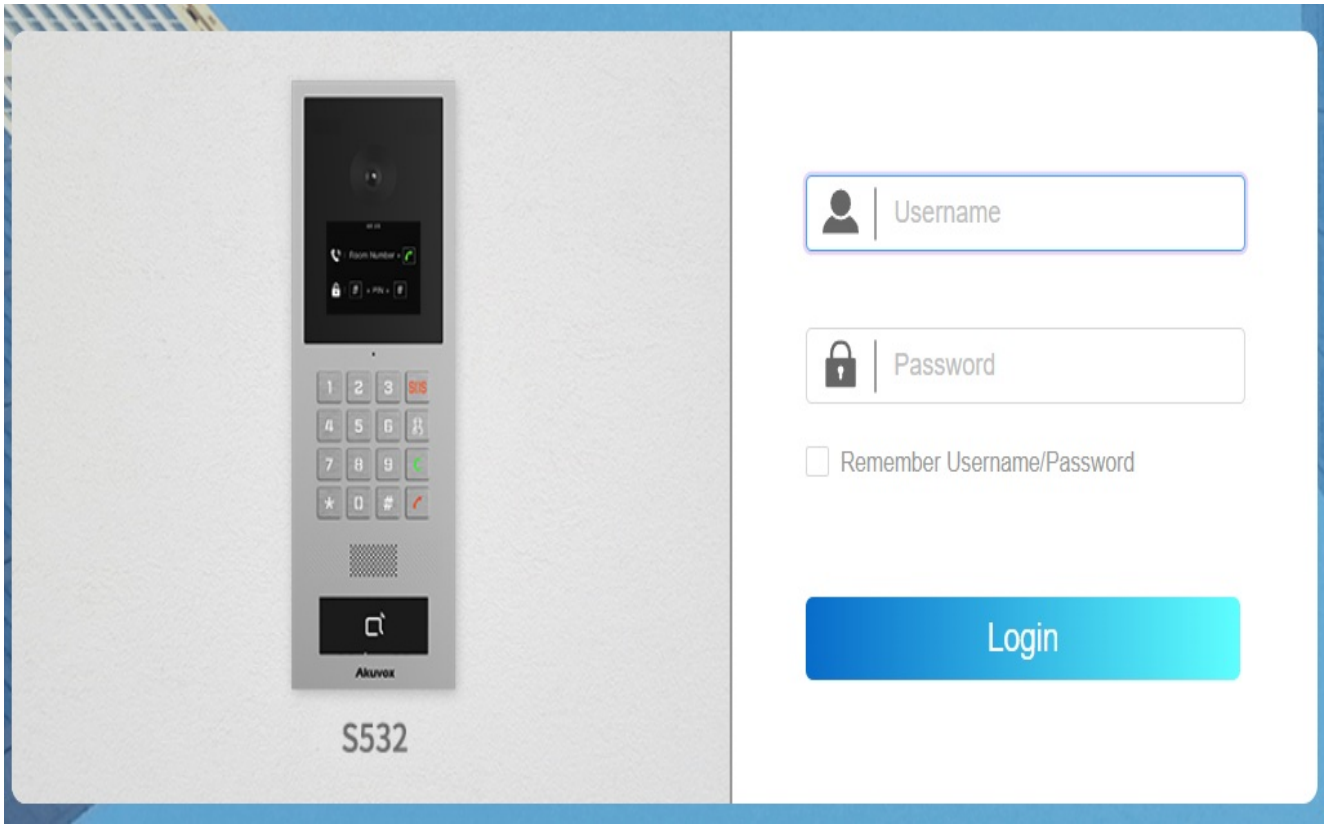
Dostęp do ustawień urządzenia w interfejsie sieciowym

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

Adres IP można sprawdzić na ekranie **informacji systemowych** urządzenia lub wyszukać adres IP urządzenia za pomocą skanera IP w tej samej sieci LAN.



Początkowa nazwa użytkownika i hasło to **admin** i należy zwracać uwagę na wielkość liter we wprowadzanych nazwach użytkowników i hasłach.



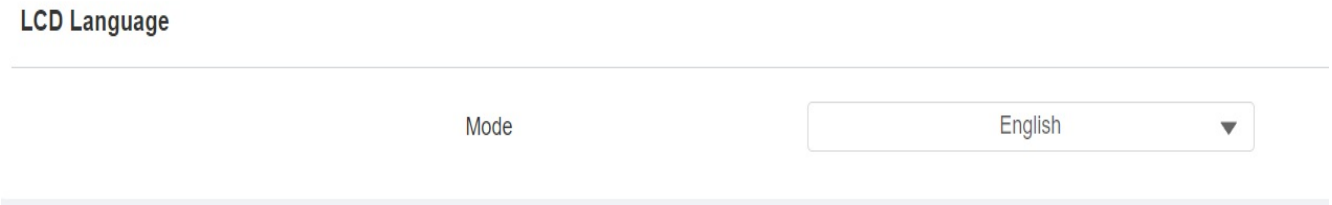
Uwaga

- Pobierz skaner IP: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Zobacz szczegółowy przewodnik: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IPScanner
- Gorąco zalecamy przeglądarkę Google Chrome.

Ustawienia języka i czasu

Ustawienia języka

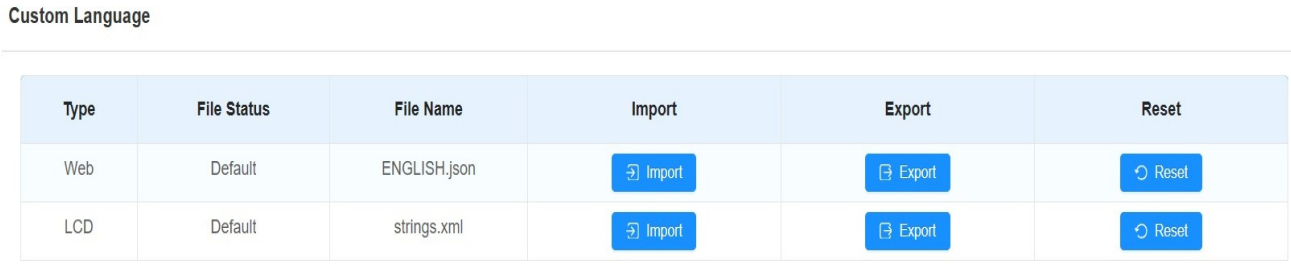
Aby skonfigurować język, przejdź do interfejsu Web **Setting > Time/Lang.** Obecnie obsługiwany jest tylko język angielski.



Język internetowy można wybrać w prawym górnym rogu.

Język strony internetowej i urządzenia można dostosować, eksportując plik i importując go po modyfikacji.

Aby dostosować język, przejdź do interfejsu Web **Setting > Time/Lang.**



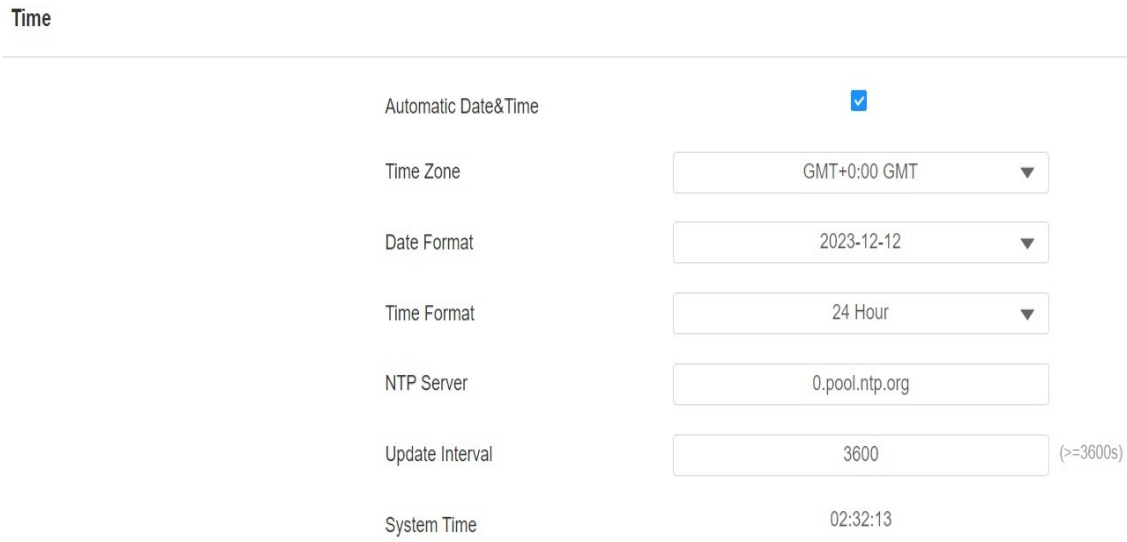
Uwaga

- Wczytany plik do dostosowania języka internetowego powinien być w formacie .json.
- Wczytany plik do dostosowania języka LCD powinien być w formacie .xml.

Ustawienie czasu

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

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



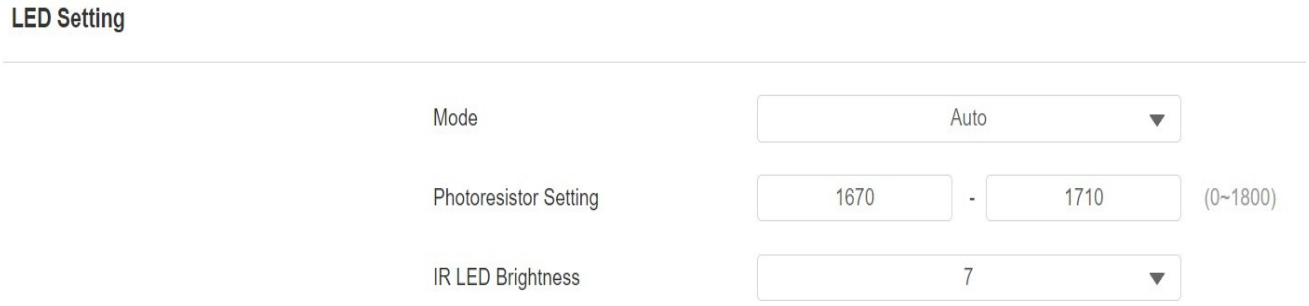
- **Automatyczna data i godzina**: Po włączeniu, data i godzina urządzenia są automatycznie ustawiane i synchronizowane z domyślną strefą czasową i serwerem NTP (Network Time Protocol).
- **Serwer NTP**: Adres serwera NTP.
- **Interwał aktualizacji**: Interwał między dwoma kolejnymi żądaniami NTP.

Ustawienia LED i LCD

Ustawienie diody LED podczerwieni

Dioda LED na podczerwień została zaprojektowana głównie w celu wzmocnienia światła do rozpoznawania twarzy w nocy lub w ciemnym otoczeniu.

Aby skonfigurować diodę LED, przejdź do interfejsu internetowego **Device > Light > LED Setting.**



- **Tryb** : Do wyboru są: **Automatyczny, Zawsze włączony**, **Zawsze wyłączony** i **Harmonogram**.
- **Ustawienie fotorezystora**: Ustaw minimalną i maksymalną wartość fotorezystora w oparciu o aktualnie wykrytą rzeczywistą wartość fotorezystora, aby sterować włączaniem

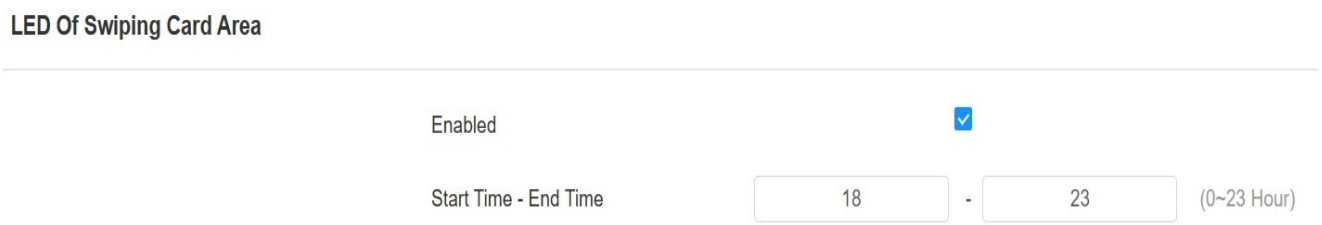
i wyłączaniem diody LED. Można ustawić maksymalną wartość fotorezystora, aby włączyć diodę LED podczerwieni i minimalną wartość, aby ją wyłączyć.

- **Jasność diody IR LED**: Regulacja jasności diody IR LED w zakresie od 0 do 10.

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.

Aby ją skonfigurować, przejdź do interfejsu internetowego **Urządzenie > Światło > LED obszaru karty przesuwanej.**

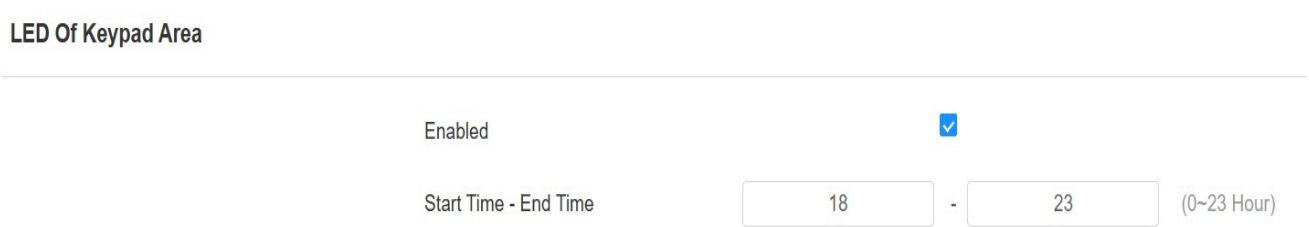


- **Czas rozpoczęcia - czas zakończenia (H)**: Wprowadź czas, przez jaki oświetlenie LED ma być włączone, np. jeśli czas jest ustawiony na 8-0 (czas rozpoczęcia-zakończenia), oznacza to, że oświetlenie LED będzie włączone w godzinach od 8:00 do 12:00 w ciągu jednego dnia (24 godziny).

Ustawienie diody LED na klawiaturze

W interfejsie internetowym można włączyć lub wyłączyć podświetlenie LED w obszarze klawiatury. Można również ustawić dokładny czas, w którym podświetlenie LED może być wyłączone, aby zmniejszyć zużycie energii elektrycznej.

Aby ją skonfigurować, przejdź do interfejsu internetowego **Device > Light > LED Of Keypad Area.**



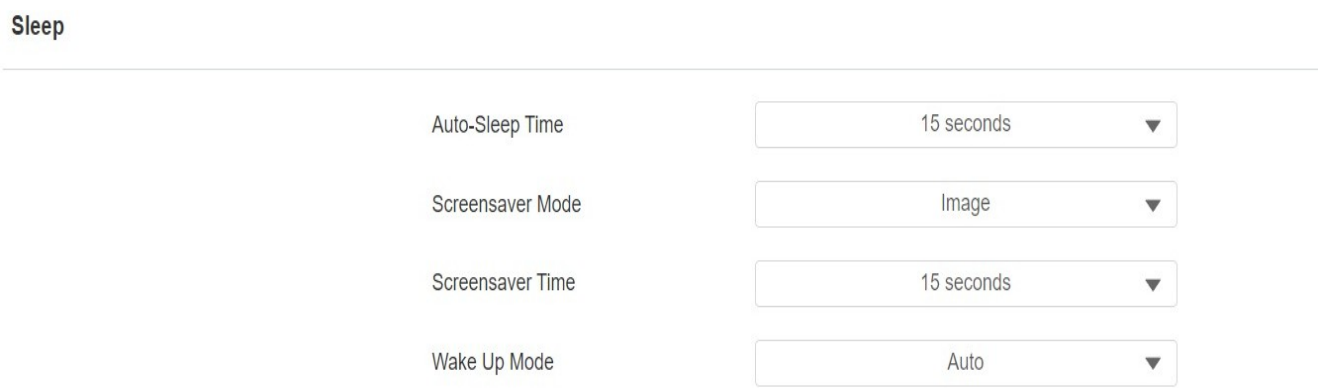
- **Czas rozpoczęcia - czas zakończenia (H)**: Wprowadź czas, przez jaki oświetlenie LED ma być włączone, np. jeśli czas jest ustawiony na 8-0 (czas rozpoczęcia-zakończenia), oznacza to, że oświetlenie LED będzie włączone w godzinach od 8:00 do

12:00 w ciągu jednego dnia (24 godziny).

Konfiguracja wygaszacza ekranu

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

Przejdź do interfejsu internetowego **Urządzenie > LCD.**

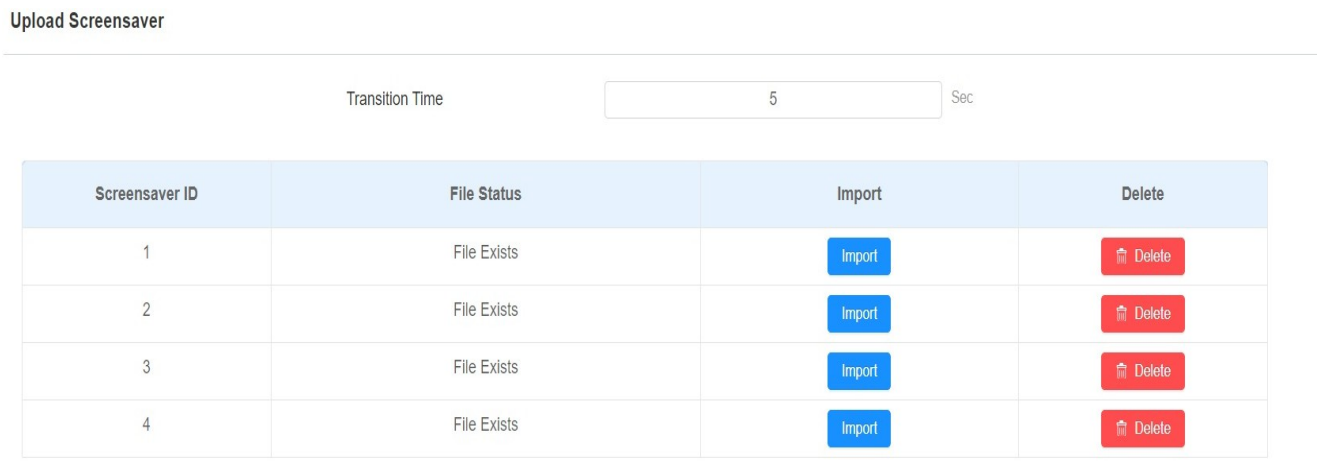


- **Czas automatycznego uśpienia**: Zakres od 5 sekund do 30 minut. Jeśli ustawisz go na 10 sekund, urządzenie przejdzie w tryb wygaszacza ekranu po 10 sekundach, gdy na urządzeniu nie będą wykonywane żadne operacje lub nikt nie wykryje zbliżania się urządzenia.
- **Tryb wygaszacza ekranu** : **Obraz** wyświetla domyślny obraz lub przesłany obraz.
- **Czas wygaszacza ekranu**: Czas trwania wygaszacza ekranu po przejściu urządzenia w tryb uśpienia. Czas trwania wygaszacza ekranu wynosi od 5 sekund do 30 minut. Domyślnie jest to 15 sekund.
- **Tryb wybudzania** : Po wybraniu opcji **Auto** ekran zostanie wybudzony, gdy ktoś się do niego zbliży bez dotykania go. Gdy wybrana jest opcja **Manual**, dotknięcie ekranu spowoduje jego wybudzenie.

Prześlij wygaszacz ekranu

Do urządzenia można przesłać obrazy wygaszacza ekranu w celach reklamowych lub dla lepszych wrażeń wizualnych.

Przejdź do interfejsu internetowego **Urządzenie > LCD.**



- **Czas przejścia**: czas przełączania między dwoma obrazami.

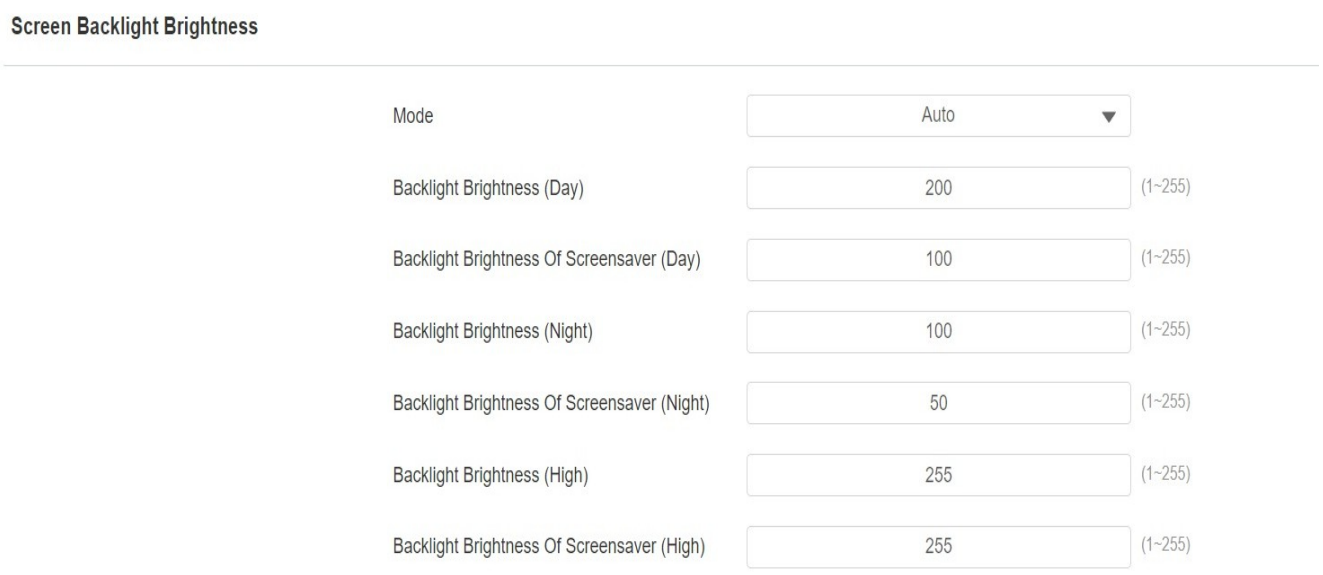
Uwaga

Plik powinien być w formacie .jpg o maksymalnym rozmiarze 1 MB.

Jasność podświetlenia ekranu

Można dostosować jasność podświetlenia ekranu i wygaszacza

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



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

Jasność podświetlenia ma trzy tryby: dzienny, nocny i wysoki. Są one określane przez fotorezystor.
-Jeśli bieżący fotorezystor jest niższy niż ustawiony minimalny fotorezystor, urządzenie znajduje się w trybie **High.**
-Jeśli wartość prądu znajduje się pomiędzy minimalną i maksymalną wartością fotorezystora,

urządzenie znajduje się w trybie **dziennym.**

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

- **Jasność podświetlenia (dzień)**: Wartość jasności mieści się w zakresie 1-255. Wartość domyślna to
  200. Im większa wartość, tym jaśniejszy ekran.

- **Jasność podświetlenia wygaszacza ekranu (dzień)**: Podświetlenie wygaszacza ekranu w ciągu dnia o wartości z zakresu 1-255.

  Jasność podświetlenia (noc): Podświetlenie w nocy o wartości z zakresu 1-255.

  Jasność podświetlenia wygaszacza ekranu (noc): Podświetlenie wygaszacza ekranu w nocy o wartości z zakresu 1-255.

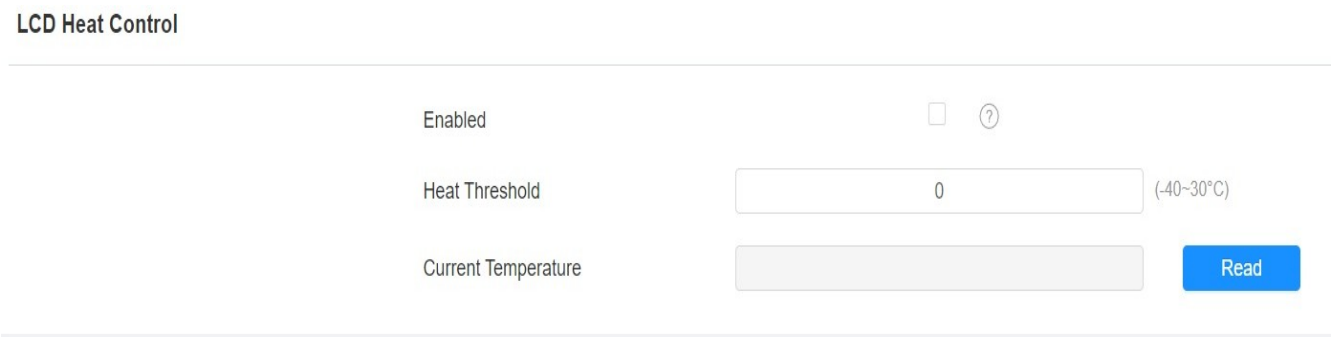
  Jasność podświetlenia (wysoka): Podświetlenie o wartości z zakresu 1-255.

  Jasność podświetlenia wygaszacza ekranu (wysoka): Podświetlenie wygaszacza ekranu o wartości z zakresu 1-255.

Grzałka LCD

Aby zapewnić normalne działanie bramofonu w środowiskach o niskiej temperaturze, można podgrzać ekran LCD urządzenia zgodnie z ustawieniem kontroli ciepła.

Przejdź do **Interkom >** Interfejs **podstawowy.**



- **Enabled** : Ta funkcja nie może być używana w trybie niskiego zużycia energii. Aby zapewnić wystarczające zasilanie, należy użyć POE+.

- **Próg**: Gdy temperatura urządzenia osiągnie wartość progową, urządzenie zacznie się nagrzewać.

- **Bieżąca temperatura**: Kliknij przycisk **Odczytaj**, aby odczytać bieżącą temperaturę urządzenia.

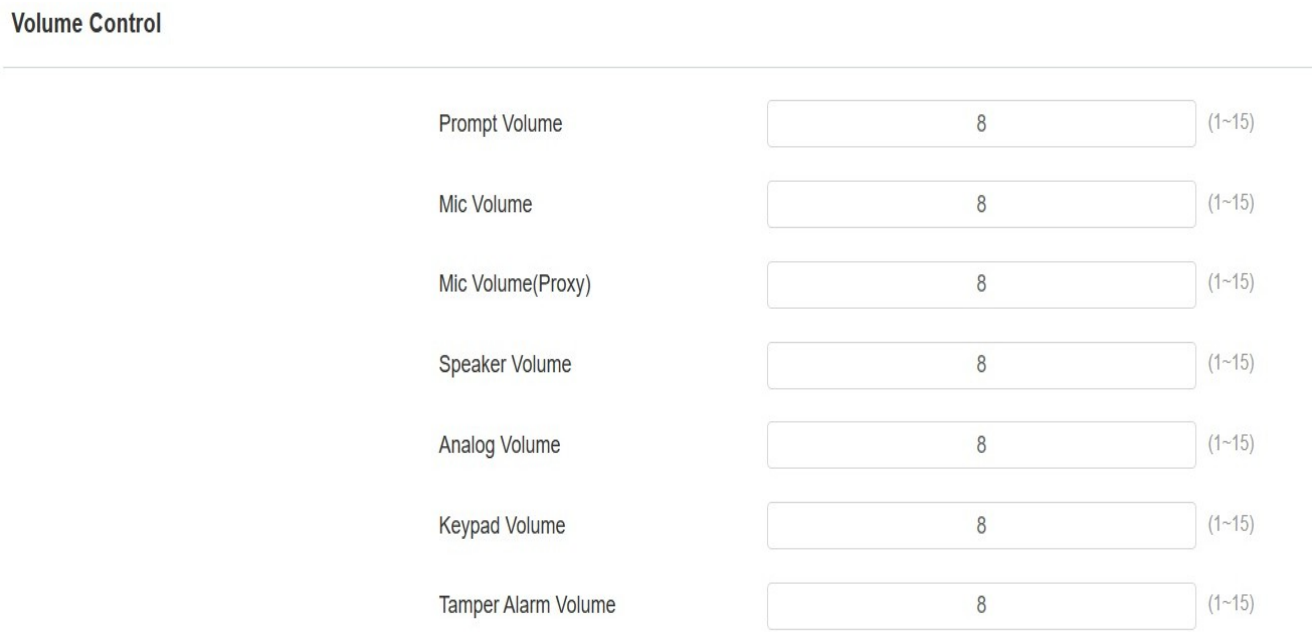
Konfiguracja głośności i tonów

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

Konfiguracja głośności

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

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



- **Mic Volume(Proxy)**: Głośność mikrofonu przełącznika analogowego.
- **Głośność** analogowa: Głośność przełącznika analogowego podczas połączenia.

Przesyłanie plików dźwiękowych

Dźwięk informujący o niepowodzeniu i powodzeniu otwarcia drzwi można przesłać w interfejsie internetowym urządzenia. Przejdź do interfejsu internetowego **Urządzenie > Audio.**

Akuvox
Open A Smart World

Tone Upload

ID	Tone	Import	Reset	Play	Enabled
1	Access Granted	Import	Reset		
2	Access Granted(Input)	Import	Reset		
3	Access Denied	Import	Reset		

Ustawienia sieciowe

Status sieci

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

Network Information

Port Type	DHCP Auto
Link Status	Connected
IP Address	192.168.36.100
Subnet Mask	255.255.255.0
Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternative DNS Server	8.8.8.8

Konfiguracja sieci urządzenia

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

Aby skonfigurować sieć, przejdź do interfejsu internetowego **Network > Basic.**

LAN Port

Network Mode	DHCP / Static IP
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Preferred DNS Server	8.8.8.8
Alternative DNS Server	

- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Jeśli tryb DHCP jest włączony, bramofon zostanie automatycznie przypisany przez serwer DHCP z adresem IP, maską podsieci, domyślną bramą i adresem serwera DNS.

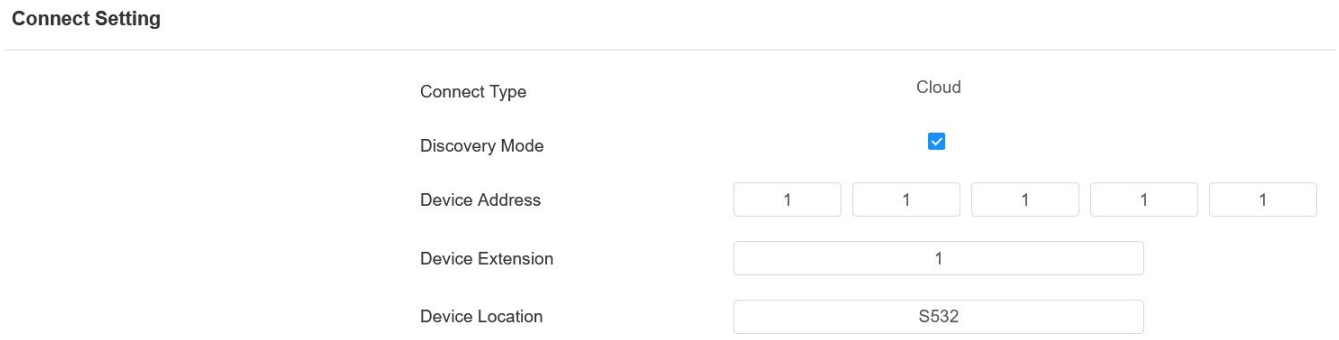
- **Statyczny adres IP**: Po wybraniu trybu statycznego adresu IP adres IP, maska podsieci, brama domyślna i adresy serwerów DNS muszą zostać skonfigurowane ręcznie zgodnie z rzeczywistym środowiskiem sieciowym.
- **Adres IP**: Adres IP po wybraniu statycznego trybu IP.
- **Maska podsieci:** Maska podsieci zgodna z rzeczywistym środowiskiem sieciowym.
- **Brama domyślna**: Prawidłowa brama zgodnie z adresem IP.
- **Preferowany/Alternatywny DNS** : Preferowany serwer DNS to podstawowy adres serwera DNS, natomiast alternatywny serwer DNS to serwer dodatkowy. Jeśli serwer podstawowy jest niedostępny, bramofon połączy się z serwerem alternatywnym.

Można również skonfigurować sieć na urządzeniu. Naciśnij *2396# na klawiaturze urządzenia i dotknij 3 i 1, aby przejść do ekranu ustawień sieci.

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.**



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

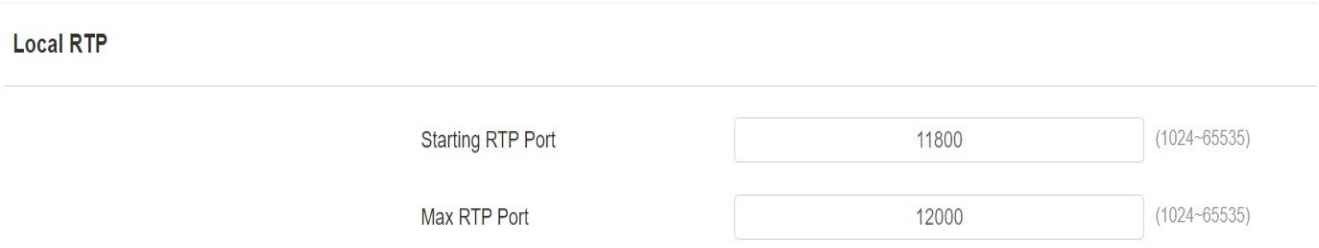
- **Rozszerzenie urządzenia**: Numer wewnętrzny urządzenia.
- **Lokalizacja urządzenia**: Lokalizacja, w której urządzenie jest zainstalowane i używane.

Konfiguracja lokalnego protokołu RTP urządzenia

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

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

Aby skonfigurować protokół RTP, przejdź do interfejsu **Sieć > Zaawansowane.**

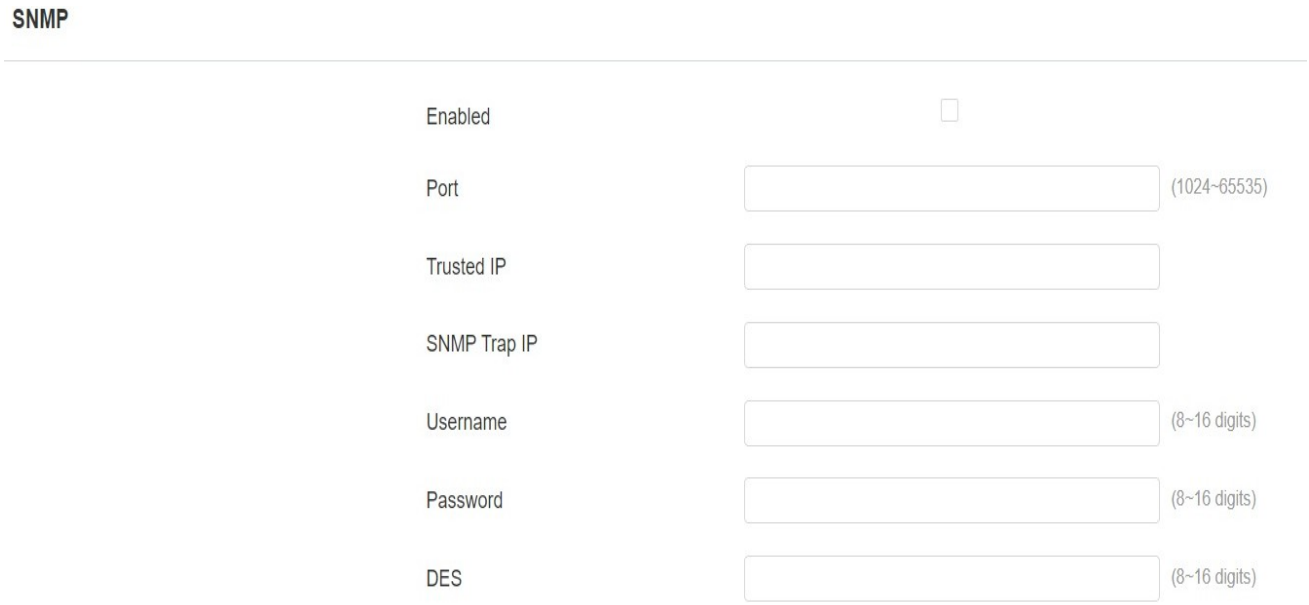


- **Startowy port RTP**: Wartość portu służąca do ustalenia punktu początkowego dla wyłącznego zakresu transmisji danych.
- **Max RTP Port**: Wartość portu do ustanowienia punktu końcowego dla wyłącznego zakresu transmisji danych.

Ustawienie SNMP

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

Aby skonfigurować SNMP, przejdź do interfejsu **Sieć > Zaawansowane.**

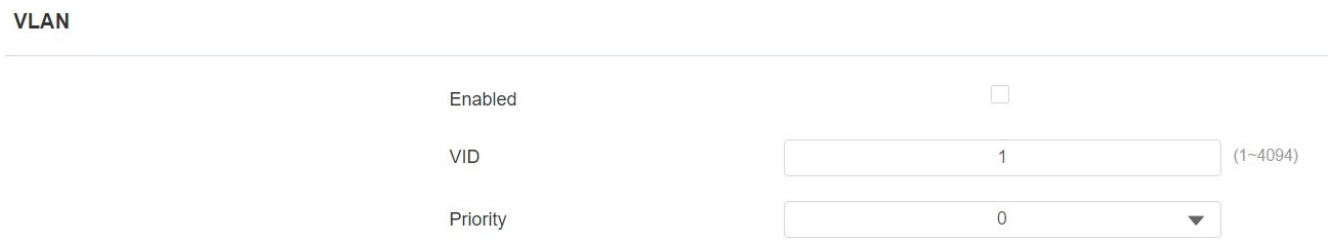


- **Port**: port serwera SNMP.
- **Zaufany adres IP**: dozwolony adres serwera SNMP. Może to być adres IP lub dowolna prawidłowa nazwa domeny URL.

Ustawienie VLAN

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

Aby skonfigurować sieć VLAN, przejdź do interfejsu **Sieć > Zaawansowane.**

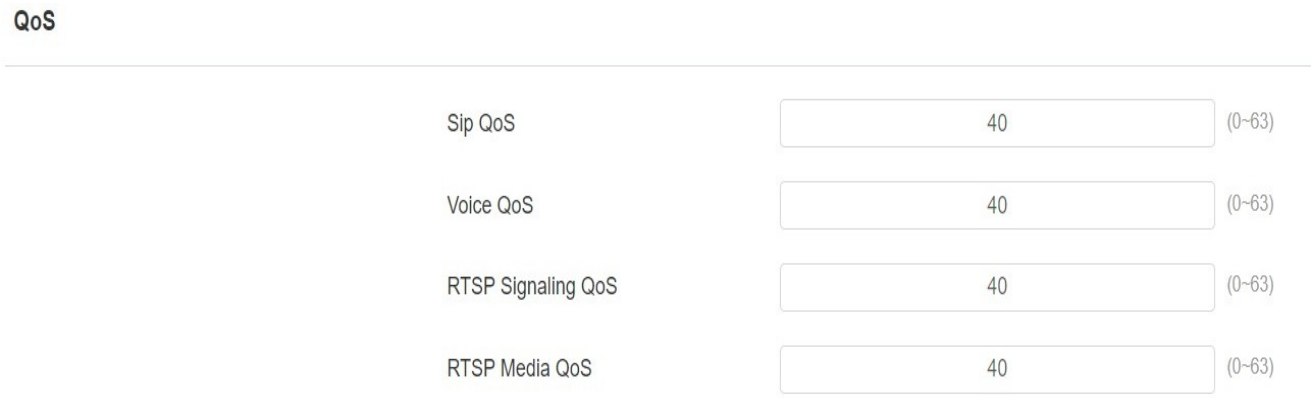


- **VID**: Identyfikator VLAN dla wyznaczonego portu.
- **Priorytet**: Priorytet VLAN dla wyznaczonego portu.

Ustawienia QoS

Quality of Service (**QoS**) to zdolność sieci do zapewnienia lepszych usług dla określonej komunikacji sieciowej poprzez wykorzystanie różnych technologii. Służy ona jako mechanizm bezpieczeństwa w sieciach, rozwiązując kwestie takie jak opóźnienia i przeciążenia sieci. Zapewnienie QoS ma kluczowe znaczenie dla sieci o ograniczonej przepustowości, szczególnie dla aplikacji multimedialnych, takich jak VoIP i IPTV. Aplikacje te często wymagają stałej szybkości transmisji i są wrażliwe na opóźnienia.

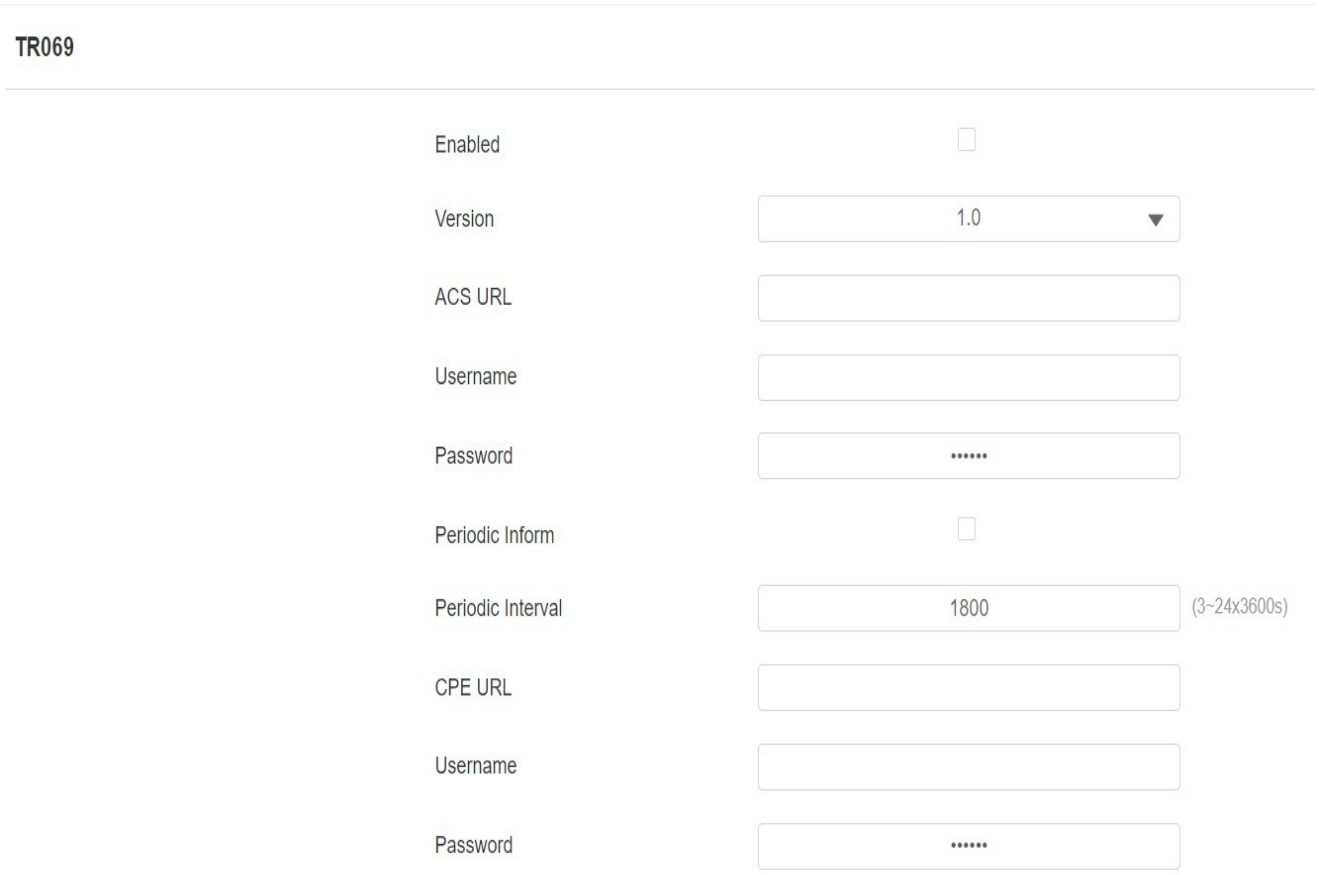
Aby skonfigurować QoS, przejdź do interfejsu **Sieć > Zaawansowane.**



Ustawienie TR069

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

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

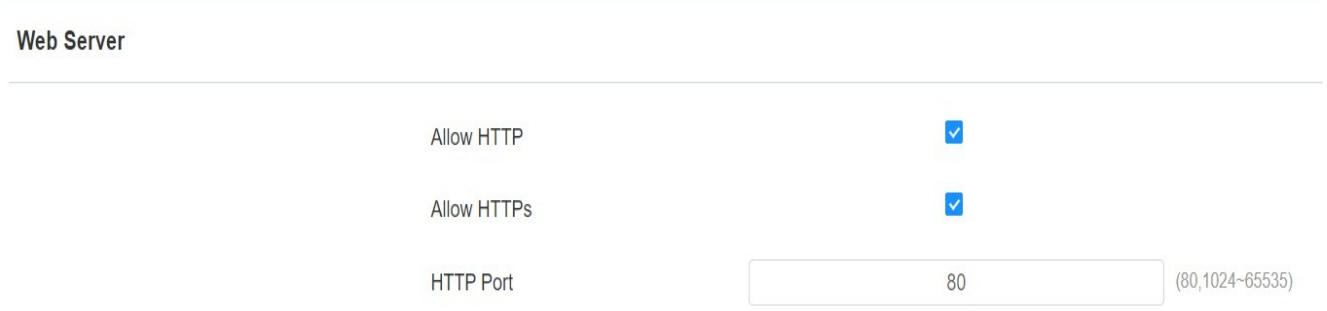


- **Wersja**: Wybierz obsługiwaną wersję TR069 (wersja 1.0 lub 1.1).
- **ACS/CPE URL**: Adres URL dla ACS lub CPE. ACS jest skrótem od serwerów automatycznej konfiguracji po stronie serwera, a CPE jest skrótem od sprzętu lokalnego klienta jako urządzeń po stronie klienta.
- **Interwał okresowy**: Interwał dla powiadomień okresowych.

Ustawienia HTTP sieci Web urządzenia

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

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

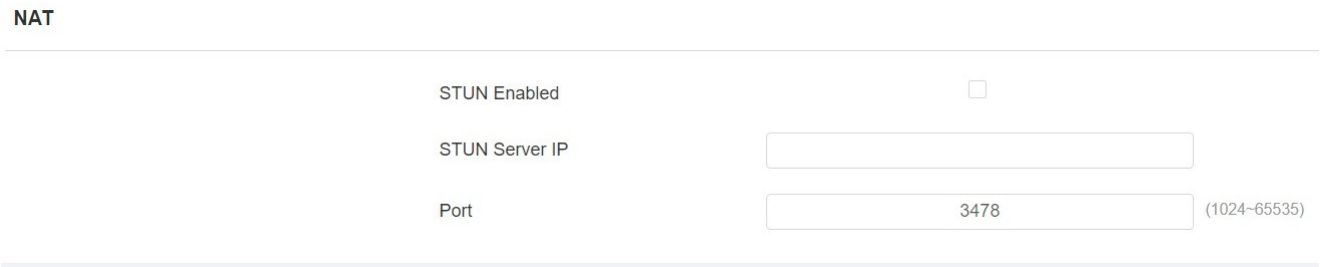


- **Port HTTP**: Port dla metody dostępu HTTP. Domyślnym portem jest 80.

Ustawienie NAT

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

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



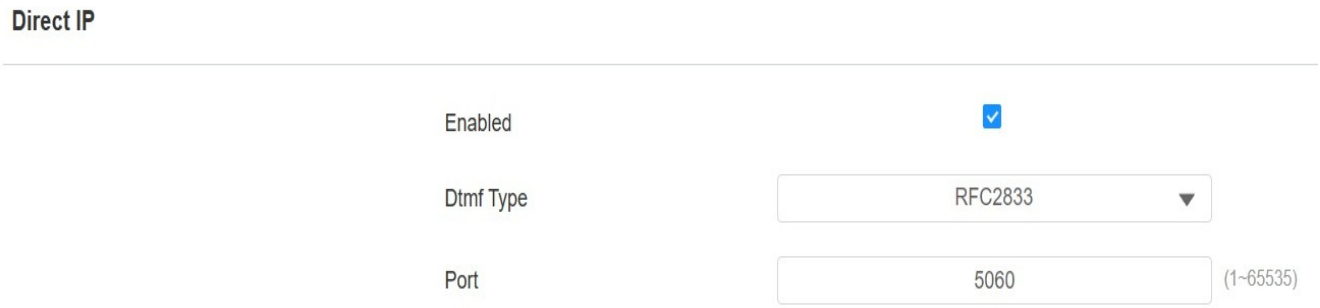
- **Port**: Domyślnie jest to 3478.

Konfiguracja połączeń interkomowych

Konfiguracja połączeń IP i połączeń IP

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

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



- **Port**: Ustaw port dla bezpośrednich połączeń IP. Domyślnie jest to 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 i połączeń SIP

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

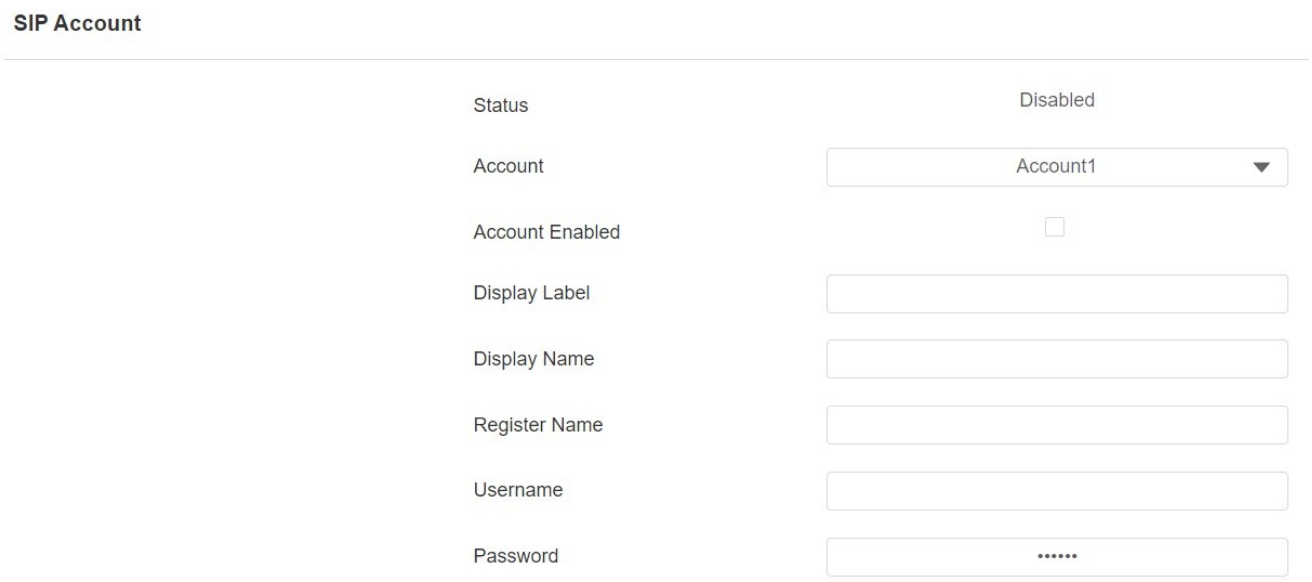
Połączenie SIP wykorzystuje protokół SIP do wysyłania i odbierania danych między urządzeniami SIP i może wykorzystywać Internet lub sieć lokalną w celu zapewnienia wysokiej jakości i bezpiecznej komunikacji. Inicjowanie połączenia SIP wymaga konta SIP, adresu SIP dla każdego urządzenia i skonfigurowania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

Rejestracja konta SIP

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

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

Aby skonfigurować konto SIP, przejdź do interfejsu Web **Account > Basic.**



- **Status**: Wyświetla, 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 wykorzystywane po aktywacji usługi chmurowej Akuvox SmartPlus.

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

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

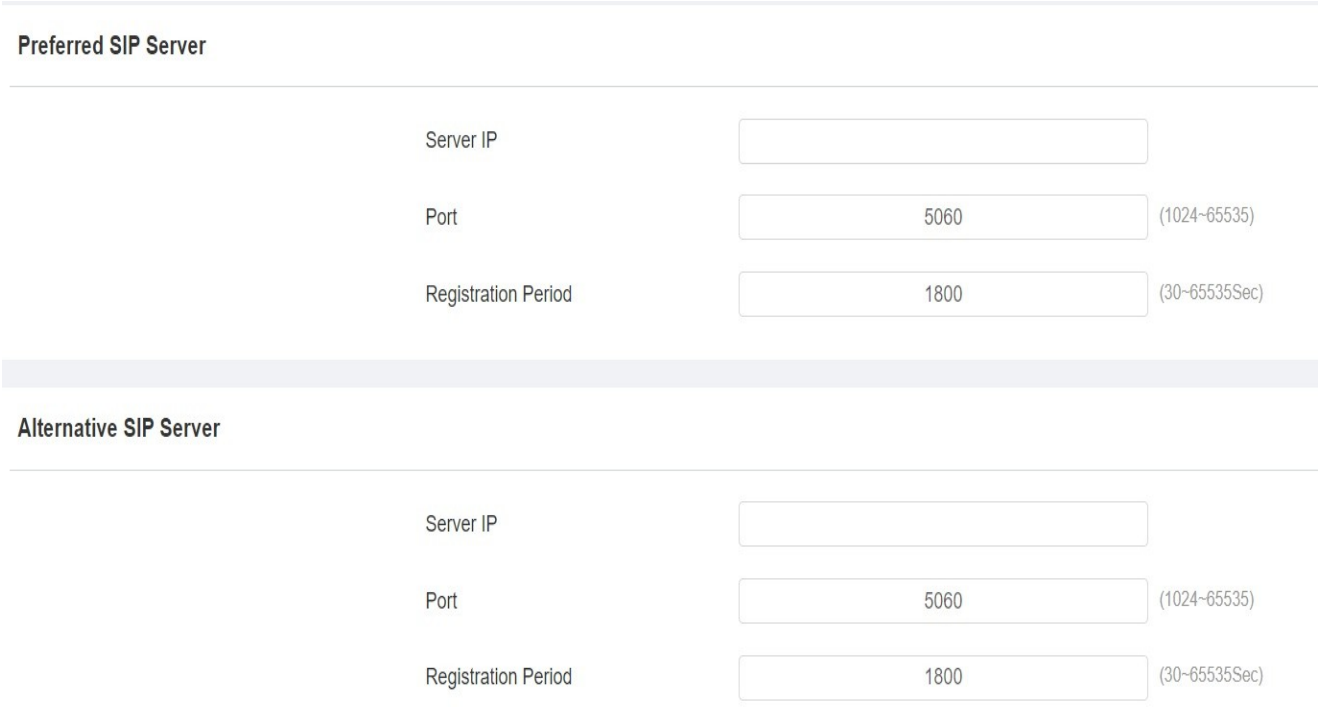
> Wskazówka
>
> Informacje na temat konfigurowania połączeń kontaktowych i planu wybierania numerów można znaleźć tutaj.

- **Account Enabled** : Zaznacz, aby aktywować zarejestrowane konto SIP.
- **Wyświetlana etykieta**: Etykieta urządzenia wyświetlana na ekranie urządzenia.
- **Wyświetlana nazwa**: nazwa urządzenia, która będzie wyświetlana na urządzeniu, z którym nawiązywane jest połączenie.
- **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 skonfigurować serwer SIP, przejdź do strony **Konto > Interfejs podstawowy.**

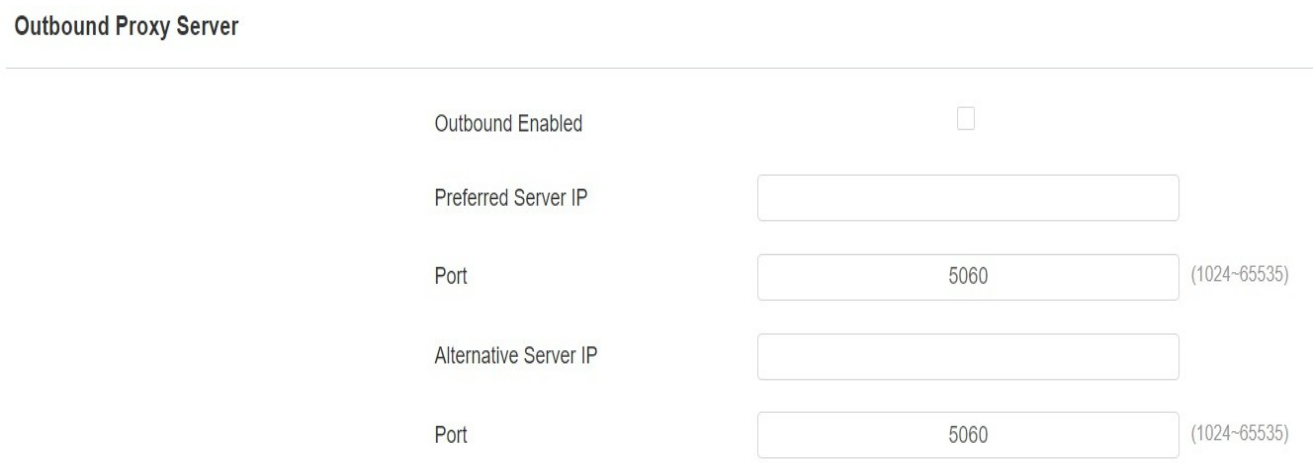


- **IP serwera**: Wprowadź adres IP serwera lub jego nazwę domeny.
- **Port**: Określa port serwera SIP do transmisji danych.
- **Okres rejestracji** : Określa limit czasu dla rejestracji konta SIP. Automatyczna ponowna rejestracja zostanie zainicjowana, jeśli rejestracja konta nie powiedzie się w określonym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

Konfiguracja serwera proxy połączeń wychodzących

Wychodzący serwer proxy odbiera i przekazuje wszystkie żądania do wyznaczonego serwera. Jest to opcjonalna konfiguracja, ale jeśli zostanie skonfigurowana, wszystkie przyszłe żądania SIP będą tam wysyłane w pierwszej kolejności.

Aby skonfigurować wychodzący serwer proxy, przejdź do interfejsu internetowego urządzenia **Konto > Podstawowe > Wychodzący serwer proxy.**



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

Konfiguracja typu transmisji danych

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

Aby skonfigurować typ transmisji danych, przejdź do interfejsu Web **Account > Basic.**

- **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.

Ustawienie analogowe

Użytkownicy mogą używać przełącznika analogowego do odbierania połączeń przychodzących na bramofon po jego podłączeniu do bramofonu.

Przejdź do interfejsu internetowego **Intercom > Basic > Analog Setting.**

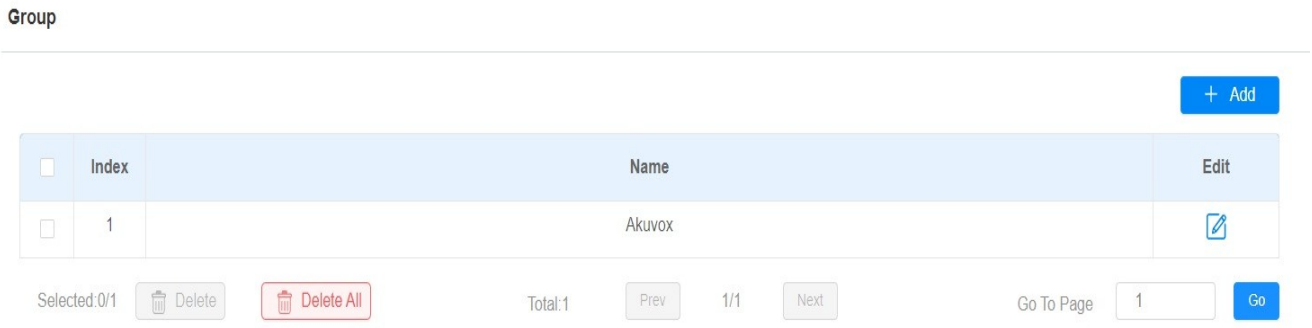
- **Adapter**: Marka przełącznika analogowego, do którego podłączony jest bramofon. Można wybrać spośród **Vizit, Cyfral, Eltis**, **Metakom** i **Lascomex**.

Konfiguracja kontaktów

Zarządzanie grupami kontaktów

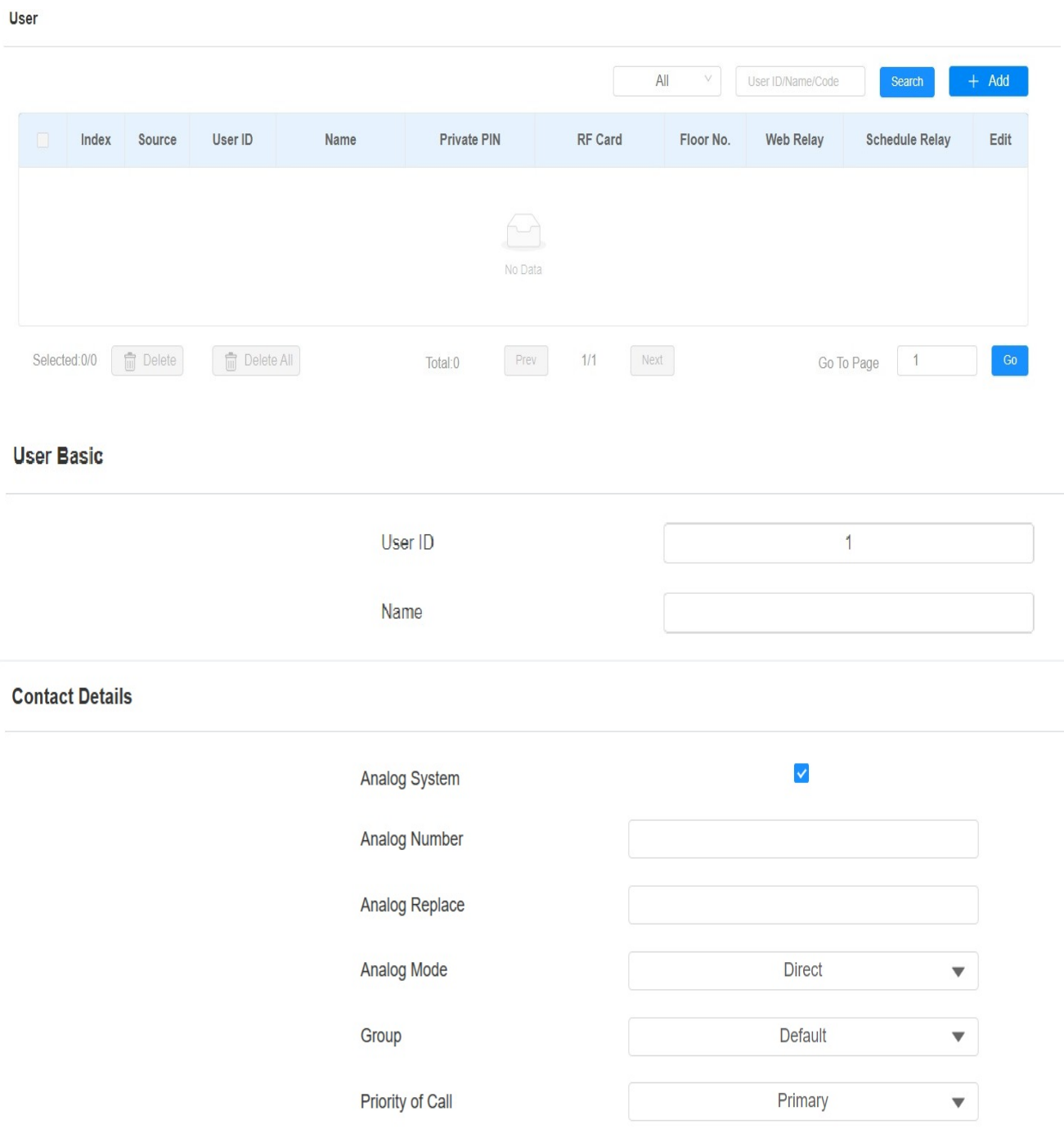
Można utworzyć i edytować grupę kontaktów dla kontaktów. Grupa kontaktów będzie używana podczas dodawania użytkownika.

Przejdź do interfejsu Web **Directory > User > Group.** Kliknij +Add, aby dodać grupę. Urządzenie obsługuje dodawanie do 1000 grup.



Dodaj kontakty

Przejdź do interfejsu Web **Directory > User.** Urządzenie obsługuje dodawanie do 10000 użytkowników. Kliknij +Add, aby dodać użytkownika. Następnie przejdź do **User Basic** i **Contact Details** .



- **System analogowy**: Po włączeniu tej opcji należy skonfigurować numer analogowy, aby użytkownicy mogli nawiązywać połączenia z przełącznikiem analogowym.
- **Numer analogowy**: Numer przełącznika analogowego.
- **Analog Replace** : Opcjonalna konfiguracja. Numer skrócony zastępuje numer analogowy. Użytkownicy mogą połączyć się z przełącznikiem analogowym, wprowadzając numer skrócony na klawiaturze bramofonu.

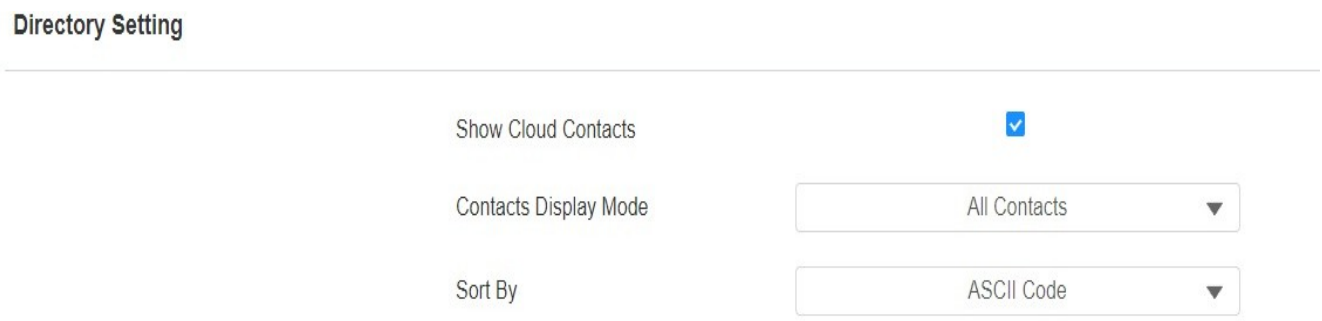
- **Tryb analogowy** : **Bezpośredni** oznacza, że przełącznik analogowy jest podłączony do bramofonu za pomocą przewodów. **Proxy** oznacza, że przełącznik analogowy nie jest połączony przewodowo z bramofonem, a po wybraniu tej opcji należy wpisać analogowy adres proxy.
- **Analog Proxy Address**: Adres IP serwera proxy.
- **Grupa** : Umieść użytkownika w wybranej grupie kontaktów.
- **Priorytet połączenia**: Ustawienie priorytetu połączenia spośród trzech opcji: Primary, Secondary i Tertiary. Na przykład, jeśli ustawisz priorytet połączenia dla jednego z kontaktów w określonej grupie kontaktów jako Podstawowy, wówczas kontakt ten będzie wywoływany jako pierwszy spośród wszystkich kontaktów w tej samej grupie kontaktów, gdy ktoś naciśnie grupę kontaktów w celu wykonania połączenia grupowego.
- **Wybierz konto** : Konto, z którego ma zostać wykonane połączenie.

> **Wskazówka**
>
> Aby zobaczyć szczegółowe kroki konfiguracji funkcji analogowej, zapoznaj się z **Integracja między S532 i słuchawkami analogowymi** .

Ustawienia wyświetlania listy kontaktów

Można dostosować sposób wyświetlania listy kontaktów na ekranie

urządzenia. Przejdź do interfejsu **Directory > Directory Setting.**



- **Pokaż kontakty z chmury** : Można wyświetlić kontakty zsynchronizowane z chmurą SmartPlus.
- **Tryb wyświetlania kontaktów** :
    - **Wszystkie** kontakty wyświetla wszystkie kontakty.

- **Grupy** Wyświetlane są **tylko** grupy kontaktów. Naciśnij żądaną grupę na ekranie urządzenia, aby nawiązać połączenie grupowe.
- **Wyświetlanie kontaktów według grup** wyświetla kontakty według grup. Po naciśnięciu grupy użytkownicy mogą zobaczyć należące do niej kontakty.

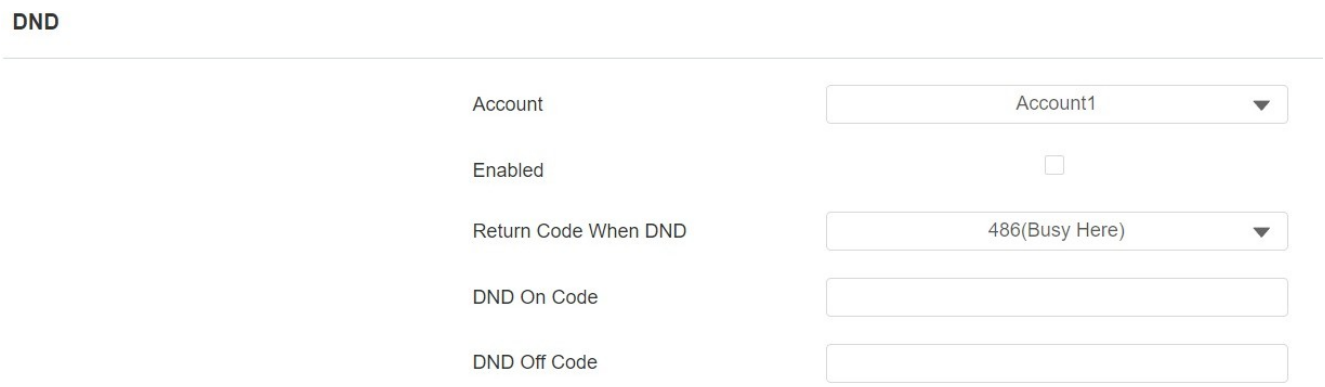
- **Sortuj według**:
  - **Kod** ASCII wymienia najemców według ich nazw w kolejności kodu ASC**I.**
  - **Numer pokoju** zawiera listę najemców według numerów ich pokoi.
  - **Import** wyświetla listę najemców zgodnie z ich kolejnością w importowanym pliku.

Ustawienie połączenia

Konfiguracja DND

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

Aby skonfigurować DND, przejdź do interfejsu web **Intercom > Call Feature.**

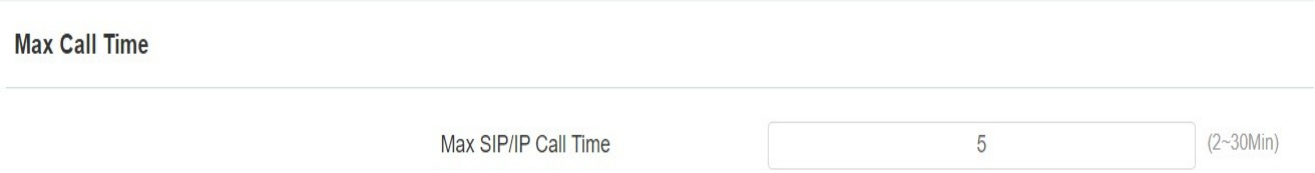


- **Konto**: Konto do zastosowania funkcji DND.
- **Return Code When** DND : Określa kod wysyłany do dzwoniącego przez serwer SIP w przypadku odrzucenia połączenia przychodzącego w trybie DND.
- **Kod włączenia DND** : Kod używany do włączania DND na serwerze SIP.
- **Kod wyłączenia DND** : Kod używany do wyłączenia DND na serwerze SIP.

Maksymalny czas trwania połączenia

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

Aby skonfigurować czas trwania połączenia, przejdź do interfejsu web **Intercom > Call Feature.**

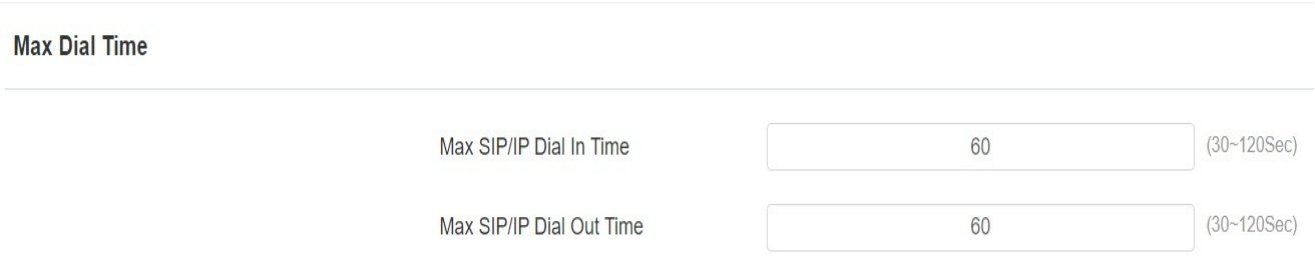


- **Max SIP/IP Call Time** : Określ maksymalny czas trwania wszystkich połączeń. Bramofon automatycznie zakończy połączenie po osiągnięciu limitu czasu.

Maksymalny czas wybierania numeru

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

Aby skonfigurować maksymalny czas wybierania, przejdź do interfejsu web **Intercom > Call Feature.**



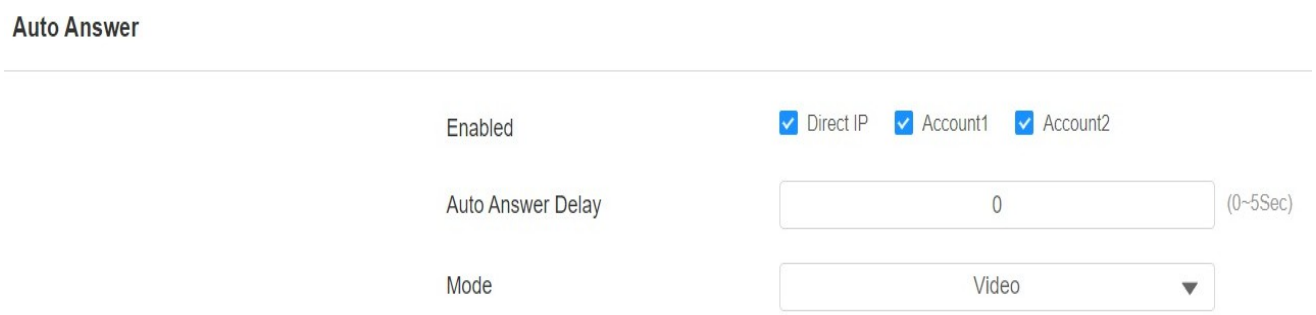
- **Max SIP/IP Dial In Time** : Określ maksymalny czas trwania połączenia przychodzącego. Bramofon automatycznie zakończy połączenie przychodzące, jeśli nie zostanie ono odebrane w ustawionym czasie.
- **Max SIP/IP Dial Out Time** : Określ maksymalny czas trwania połączenia wychodzącego. Bramofon automatycznie zakończy wybrane połączenie, jeśli odbiorca nie odbierze go w ustawionym czasie.

Konfiguracja automatycznej odpowiedzi

Funkcja automatycznego odbierania pozwala urządzeniu na automatyczne odbieranie połączeń

przychodzących bez konieczności ręcznej interwencji. Można również dostosować tę funkcję, ustawiając czas trwania automatycznego odbierania i wybierając tryb komunikacji między audio i wideo.

Aby skonfigurować automatyczne odbieranie, przejdź do interfejsu internetowego **Intercom > Call Feature.**



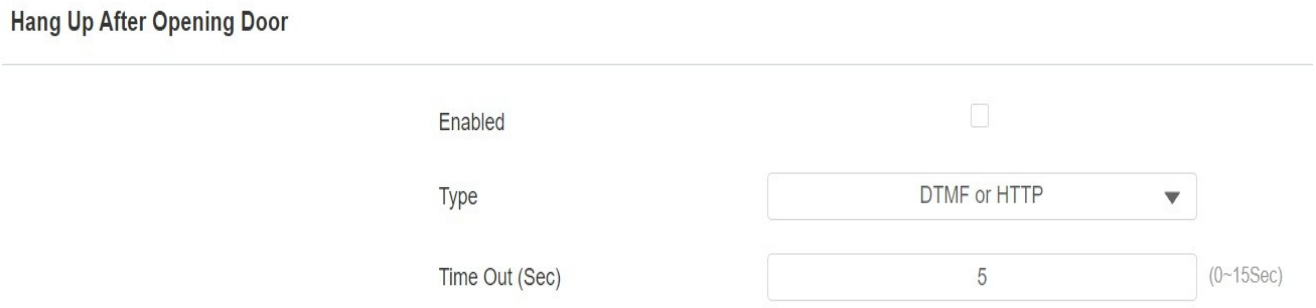
Opóźnienie automatycznego odbierania: Ustaw czas, po którym połączenie zostanie automatycznie odebrane po dzwonku. Na przykład, jeśli ustawisz czas opóźnienia na 5 sekund, bramofon automatycznie odbierze połączenie po 5 sekundach.

Tryb : Określenie, czy połączenie ma być automatycznie odbierane jako połączenie wideo czy audio.

Odłóż słuchawkę po otwarciu drzwi

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

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



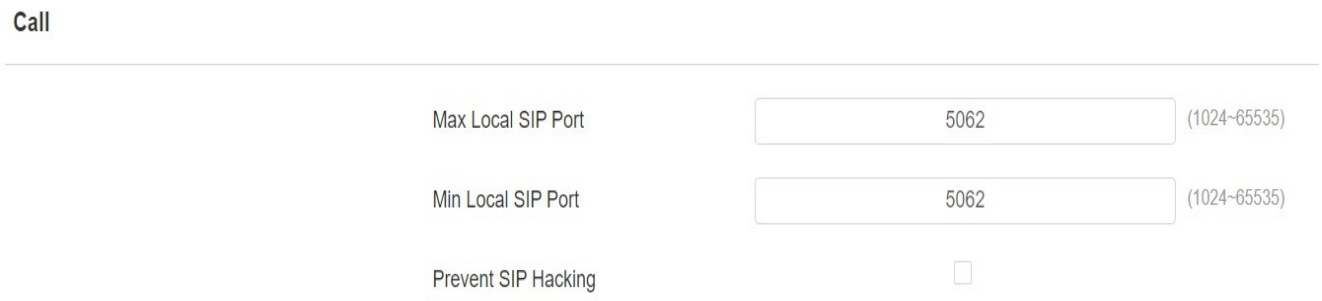
- **Typ** : Określa metodę odblokowywania drzwi. Jeśli ta konkretna metoda jest używana do odblokowania drzwi podczas połączenia, bramofon zakończy połączenie po osiągnięciu ustawionego czasu rozłączenia.
- **Time Out(Sec)**: Określa limit czasu rozłączenia. Bramofon automatycznie zakończy połączenie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

Zapobieganie włamaniom SIP

Podsłuch telefonu internetowego to atak sieciowy, który umożliwia nieautoryzowanym stronom

przechwytywanie i uzyskiwanie dostępu do treści sesji komunikacyjnych między użytkownikami interkomu. Może to narazić atakujących na ujawnienie wrażliwych i poufnych informacji. Ochrona przed włamaniami SIP to technika, która zabezpiecza połączenia SIP przed naruszeniem w Internecie.

Aby skonfigurować hakowanie SIP, przejdź do interfejsu **Konto** internetowe **> Zaawansowane.**

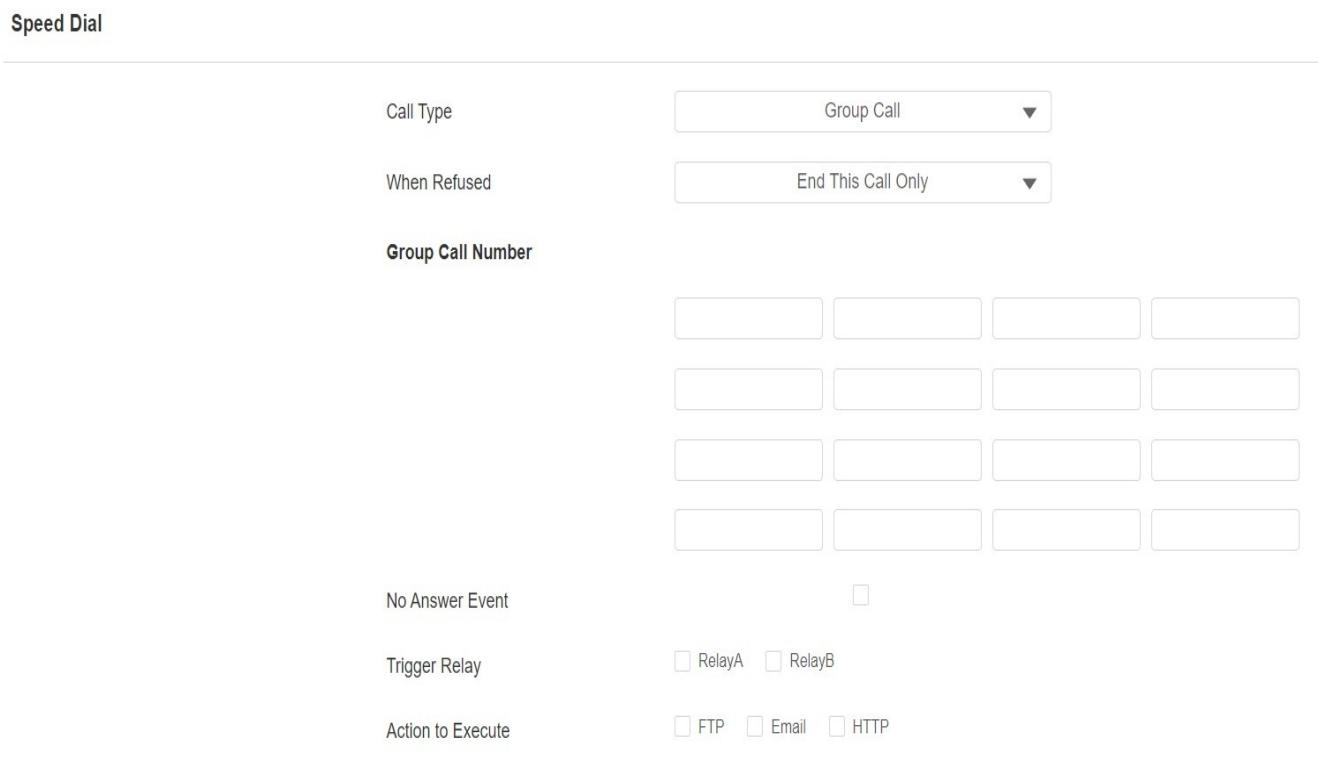


- **Prevent SIP Hacking** : Aktywuj tę funkcję, aby odbierać połączenia tylko od kontaktów znajdujących się na białej liście. Chroni to prywatne i tajne informacje użytkowników przed potencjalnymi hakerami podczas połączeń SIP.

Szybkie wybieranie
Połączenie grupowe

Połączenie grupowe służy do szybkiego inicjowania wstępnie skonfigurowanych numerów poprzez naciśnięcie przycisku Dial. Można utworzyć do 16 numerów połączeń grupowych.

Aby skonfigurować połączenie grupowe, przejdź do interfejsu web **Intercom > Basic.**



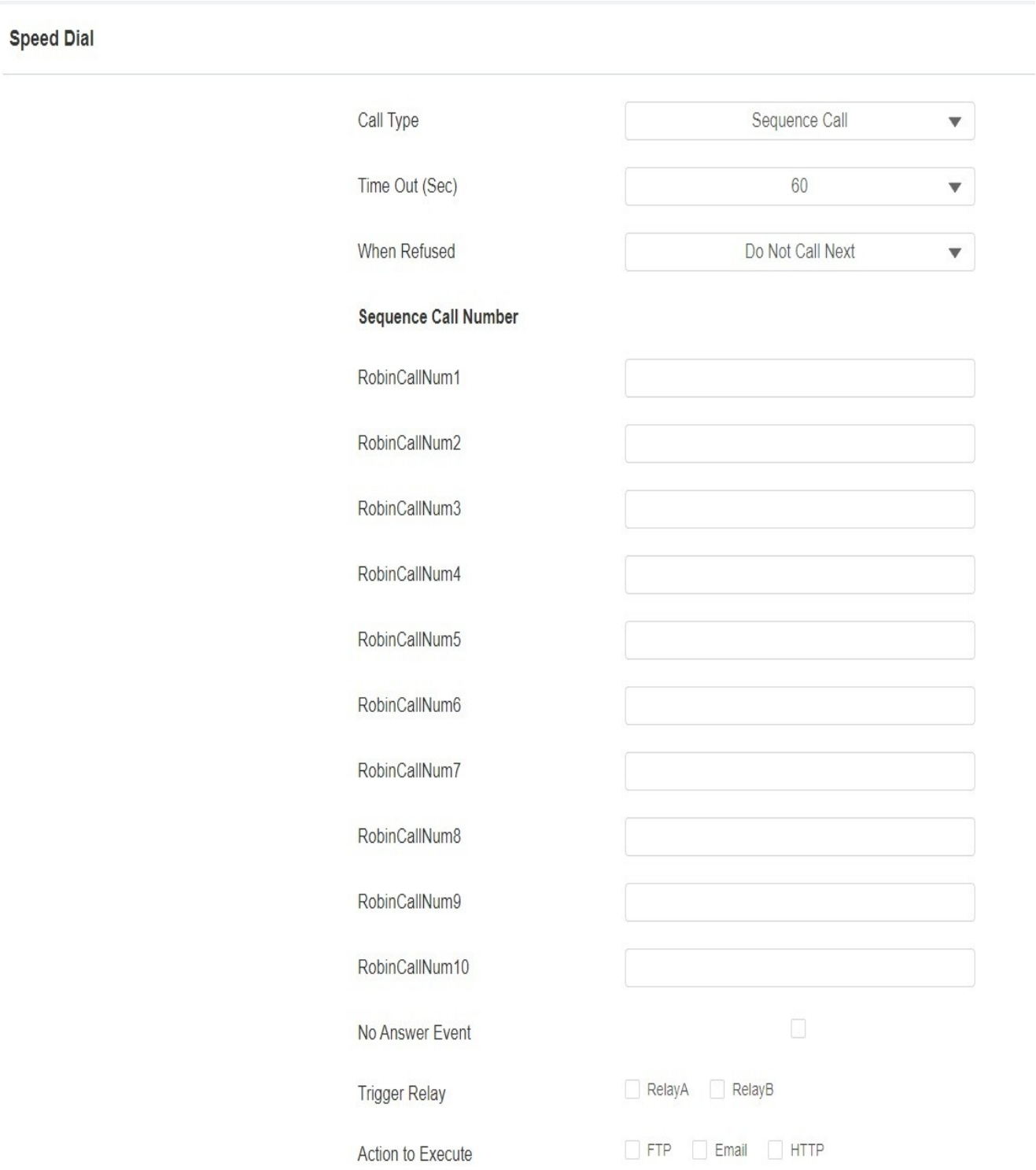
- **Typ połączenia** : Połączenie grupowe lub Połączenie sekwencyjne.

- **W przypadku odmowy** :
    - **End This Call Only**: Połączenie wykonane do strony odmawiającej zostanie zakończone.
    - **Zakończ wszystkie połączenia** : wszystkie połączenia zostaną zakończone.
- **Numer połączenia grupowego**: Jeśli wpiszesz lokalny numer połączenia grupowego, zamiast numeru połączenia grupowego SmartPlus zostanie wybrany numer grupy lokalnej.
- **Zdarzenie braku odpowiedzi**: Gdy połączenie nie zostanie odebrane, uruchomione zostaną odpowiednie działania.
- **Przekaźnik wyzwalający**: Przekaźnik wyzwalany, gdy połączenie nie zostanie odebrane.
- **Akcja do wykonania**: Akcja, która ma zostać uruchomiona, gdy połączenie nie zostanie odebrane.

Wywołanie sekwencji

Połączenie sekwencyjne to funkcja, która umożliwia wybieranie grupy numerów w określonej kolejności, aż jeden z nich odbierze połączenie. Funkcja ta jest obsługiwana przez aplikację Akuvox SmartPlus, która zapewnia zestaw numerów połączeń sekwencyjnych dla aplikacji.

Aby skonfigurować połączenie sekwencyjne, przejdź do interfejsu web **Intercom > Basic.**



- **Typ połączenia** : Połączenie grupowe lub Połączenie sekwencyjne.
- **Time Out(Sec)**: Ustawienie limitu czasu połączenia przed nawiązaniem połączenia z następnym rozmówcą, gdy pierwszy rozmówca nie odbierze połączenia przed upływem limitu czasu.
- **W przypadku odmowy** :
    - **Do Not Call Next**: połączenie sekwencyjne zostanie zakończone, jeśli połączenie zostanie odrzucone przez rozmówcę.

- **Call Next**: połączenie sekwencyjne będzie kontynuowane do następnego rozmówcy, jeśli zostanie odrzucone przez rozmówcę.

- **Zdarzenie nieodebrania połączenia**: gdy połączenie nie zostanie odebrane, uruchomione zostaną odpowiednie działania.

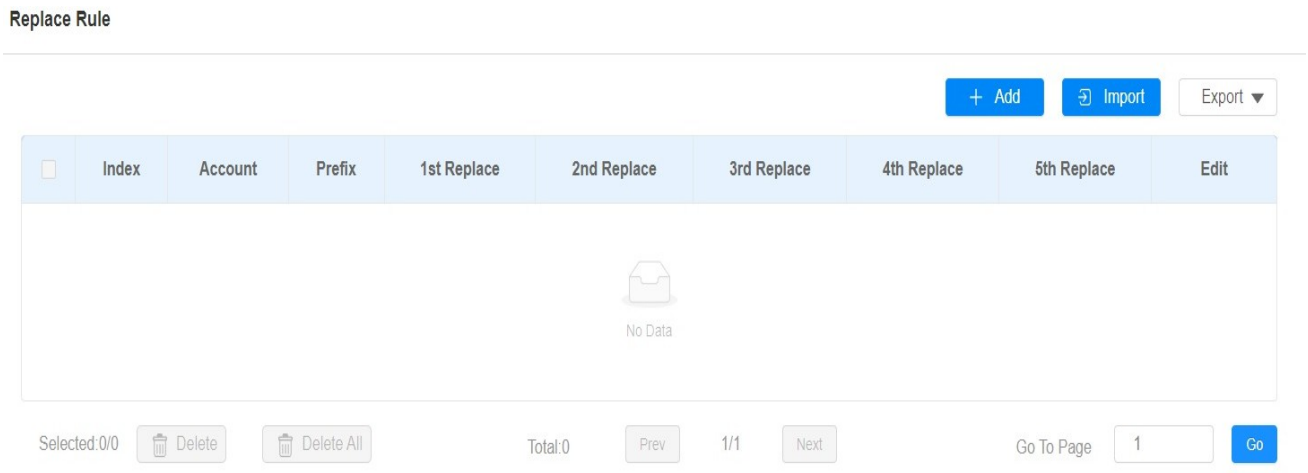
- **Trigger Relay (Przekaźnik wyzwalający)**: przekaźnik(i) wyzwalany(e), gdy połączenie nie zostanie odebrane.

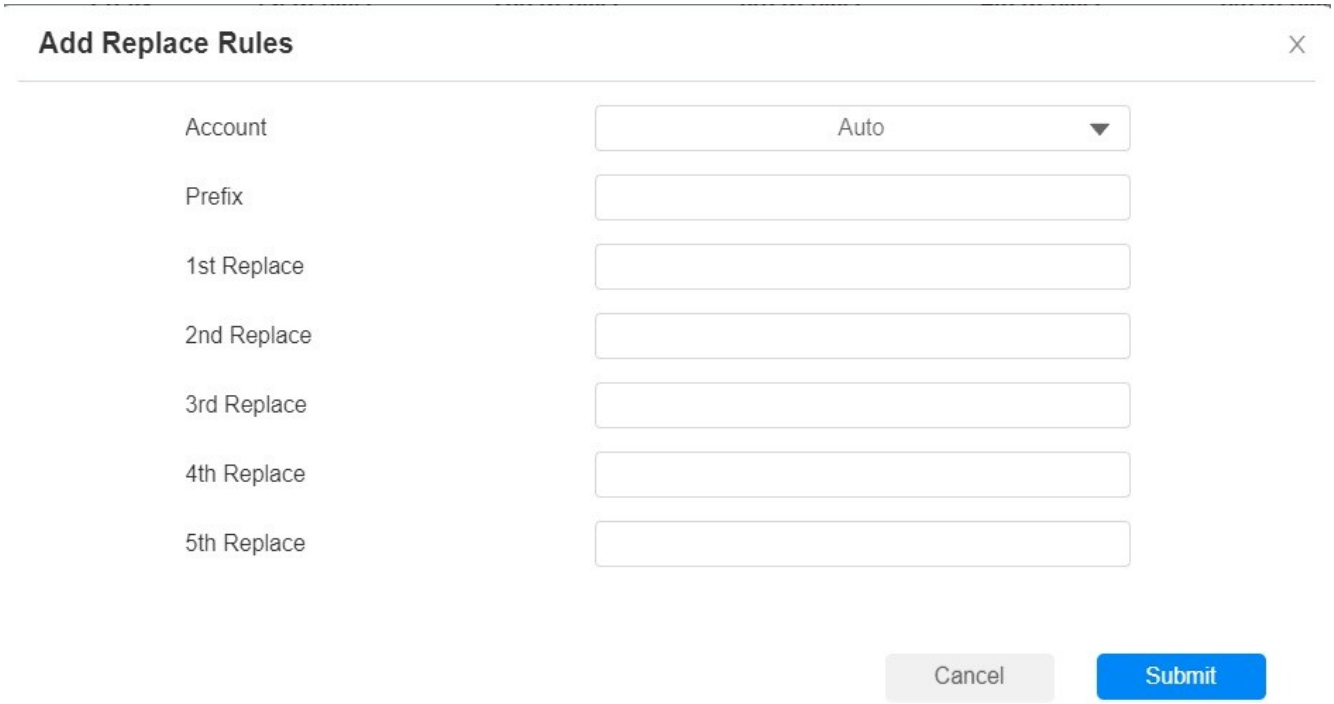
- **Action to Execute** : akcja (akcje), która ma zostać uruchomiona, gdy połączenie nie zostanie odebrane.

Plan wybierania numerów

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

Aby skonfigurować plan wybierania, przejdź do interfejsu web **Intercom > Dial Plan.** Kliknij przycisk **Dodaj** .





- **Konto:** Wybierz konto dial-out.

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

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

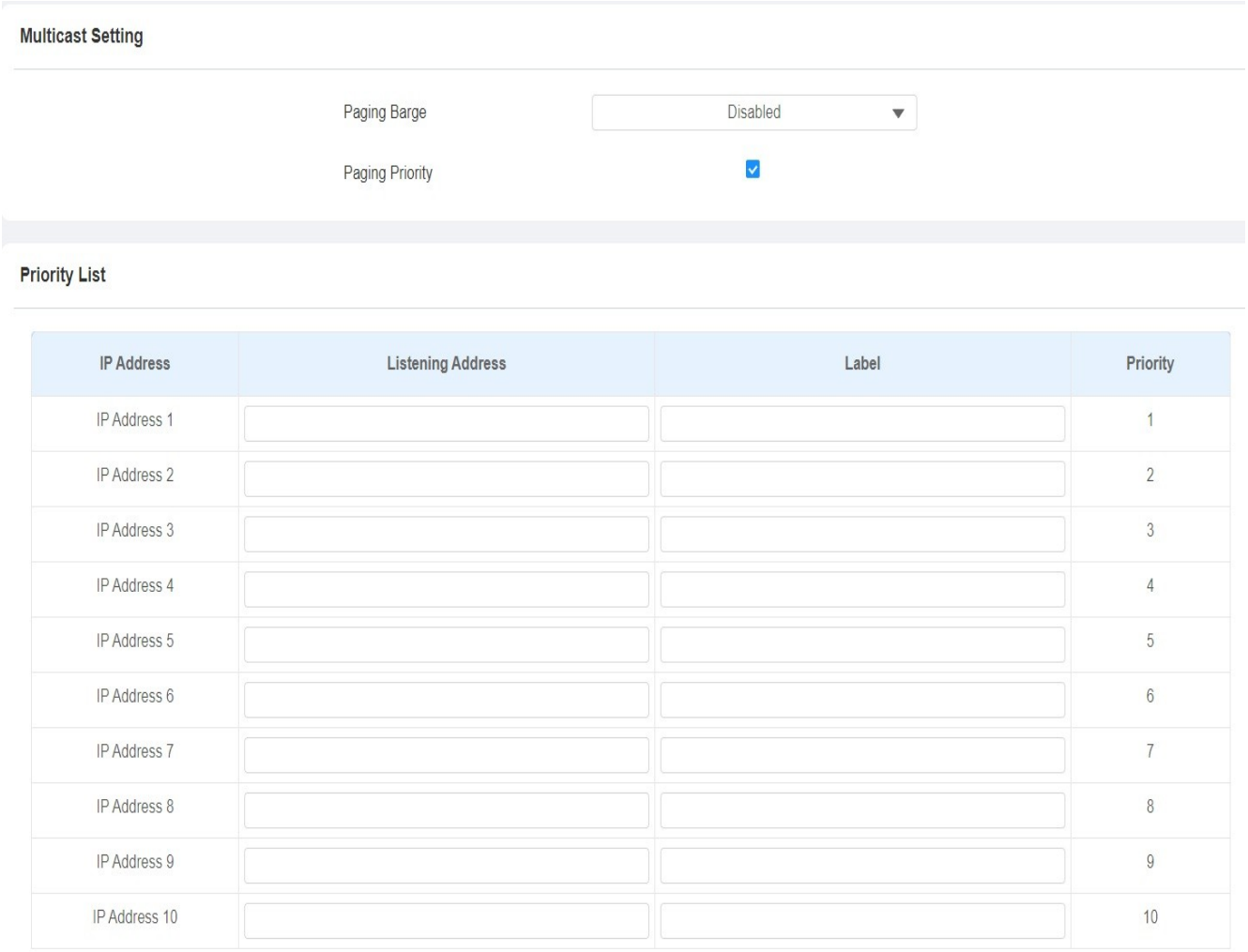
- **Prefiks:** Określenie krótkiego numeru zastępującego wybrane numery.

- **Replace 1/2/3/4/5:** Określ do 5 numerów, które mogą być numerami SIP lub adresami IP, które zostaną zastąpione prefiksem. Wszystkie te numery będą wywoływane jednocześnie, gdy dzwoniący wybierze prefiks.

Multicast

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

Aby skonfigurować multiemisję, przejdź do **Interkom >** Interfejs **multiemisji.**

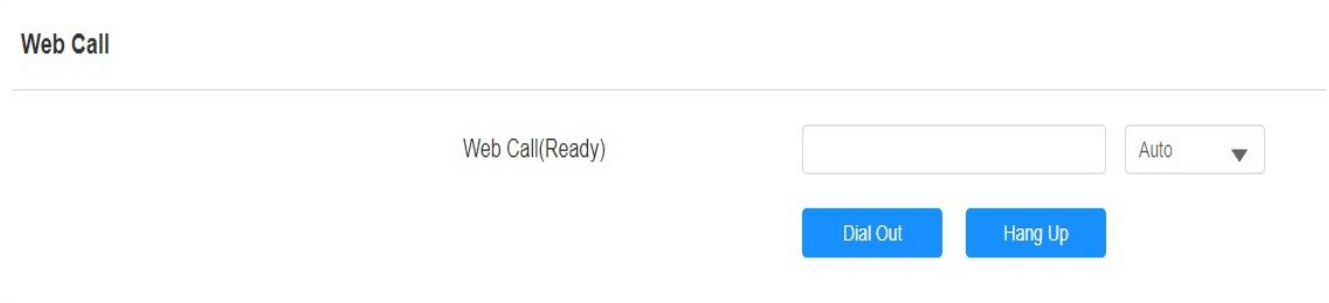


- **Paging Barge**: Multicast lub ile połączeń multicast ma wyższy priorytet niż połączenie SIP, jeśli wyłączysz Paging Priority, połączenie SIP będzie miało wyższy priorytet.
- **Priorytet przywoływania**: Połączenia multiemisji są wywoływane w kolejności według priorytetu lub nie.
- **Adres nasłuchiwania**: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

Połączenie internetowe

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

Aby skonfigurować połączenie internetowe, przejdź do interfejsu **System > Konserwacja > Połączenie internetowe. Wybierz** zarejestrowane konto SIP, aby nawiązać połączenie internetowe.



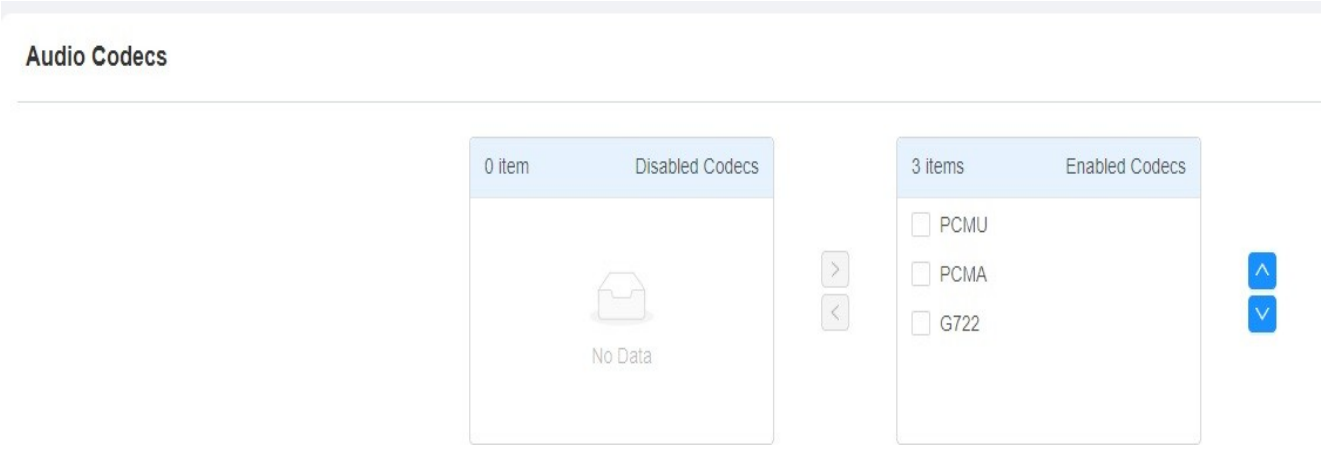
- **Web Call(Ready)**: Docelowy numer SIP/IP.

Konfiguracja kodeka audio i wideo dla połączeń SIP

Konfiguracja kodeka 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.

Aby skonfigurować kodek audio, przejdź do interfejsu **Konto** internetowe **> Zaawansowane.**



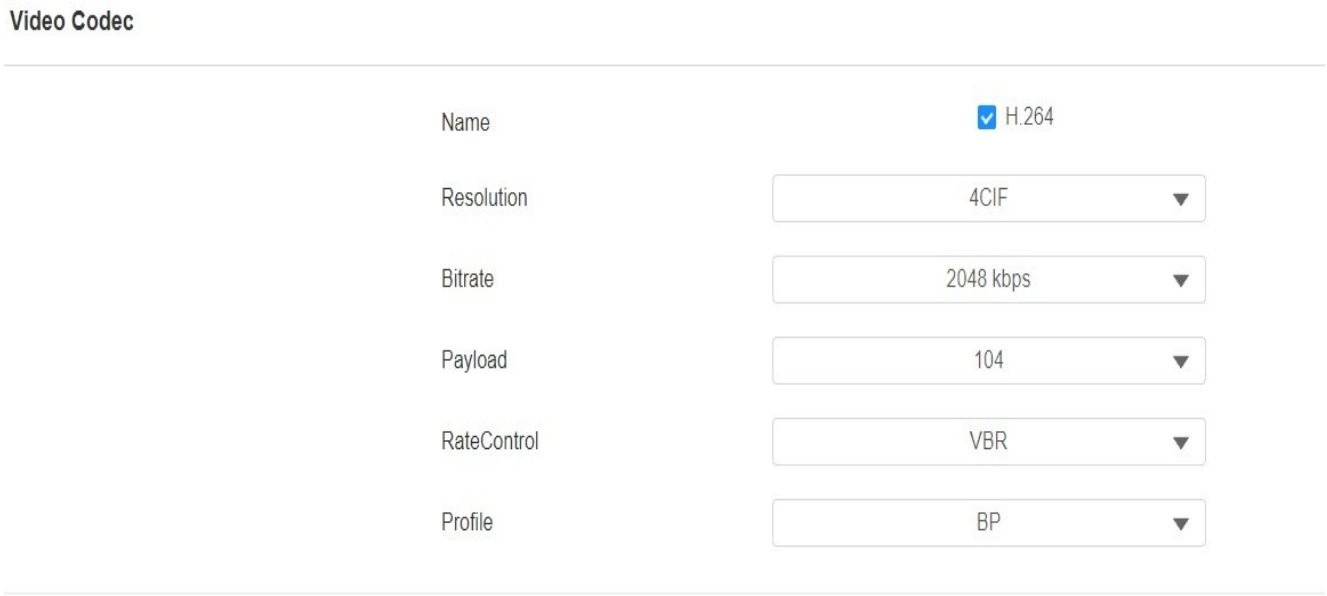
Poniżej znajdują się informacje na temat zużycia pasma i częstotliwości próbkowania dla trzech typów kodeków:

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

Konfiguracja kodeka wideo

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

Aby skonfigurować kodek wideo, przejdź do interfejsu **Konto** internetowe **> Zaawansowane.**

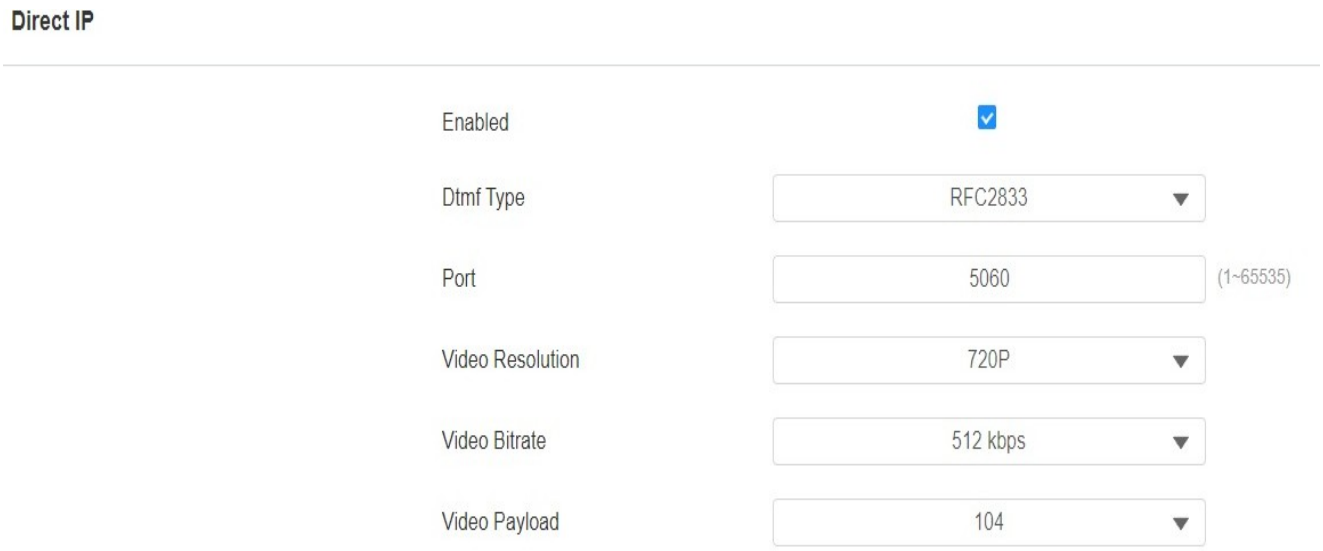


- **Nazwa** : Zaznacz, aby włączyć format kodeka wideo H264 dla strumienia wideo z bramofonu.
- **Rozdzielczość**: Rozdzielczość kodu dla jakości wideo ma następujące opcje: **CIF, VGA, 4CIF** i **720P** . Domyślną rozdzielczością kodu jest 4CIF.
- **Szybkość transmisji** : Szybkość transmisji strumienia wideo wynosi od 128 do 2048 kb/s. Im większa szybkość transmisji bitów, tym większa ilość danych przesyłanych w każdej sekundzie, a tym samym wyraźniejszy obraz wideo. Domyślna szybkość transmisji kodu wynosi 2048.
- **Payload**: Ładunek mieści się w zakresie od 90 do 119 dla konfigurowania plików konfiguracyjnych audio/wideo. Domyślną wartością jest 104.

Konfiguracja kodeka wideo dla bezpośrednich połączeń IP

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

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

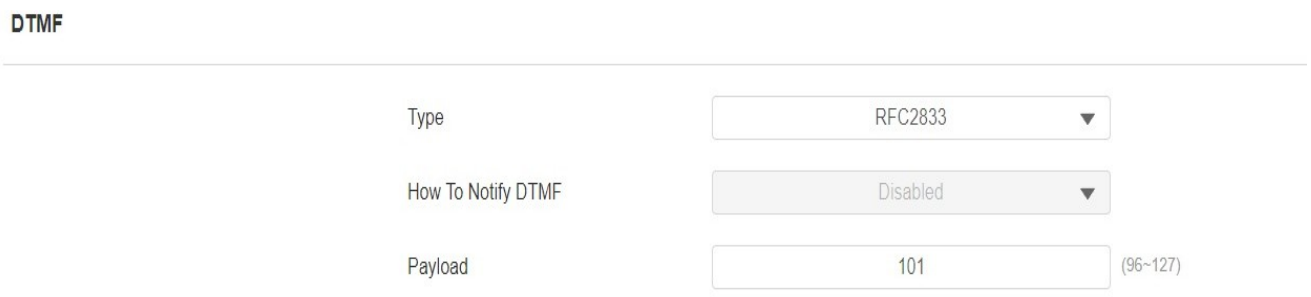


- **Rozdzielczość wideo**: Rozdzielczość kodu dla jakości wideo ma następujące opcje: **CIF, VGA, 4CIF, 720P** i **1080P** . Domyślną rozdzielczością jest 720P.
- **Szybkość transmisji wideo** : Szybkość transmisji strumienia wideo wynosi od 128 do 2048 kb/s. Domyślna szybkość transmisji kodu wynosi 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 skonfigurować transmisję danych DTMF, przejdź do **Konto** internetowe **> Zaawansowane >** Interfejs **DTMF.**



- **Typ** : Wybierz jedną z następujących opcji: **Inband, RFC 2833, Info, Info+Inband, Info+RFC 2833, Info+Inband+RFC 2833 w** oparciu o konkretny typ transmisji DTMF urządzenia strony trzeciej, z którym ma zostać dopasowane jako strona odbierająca dane sygnału.

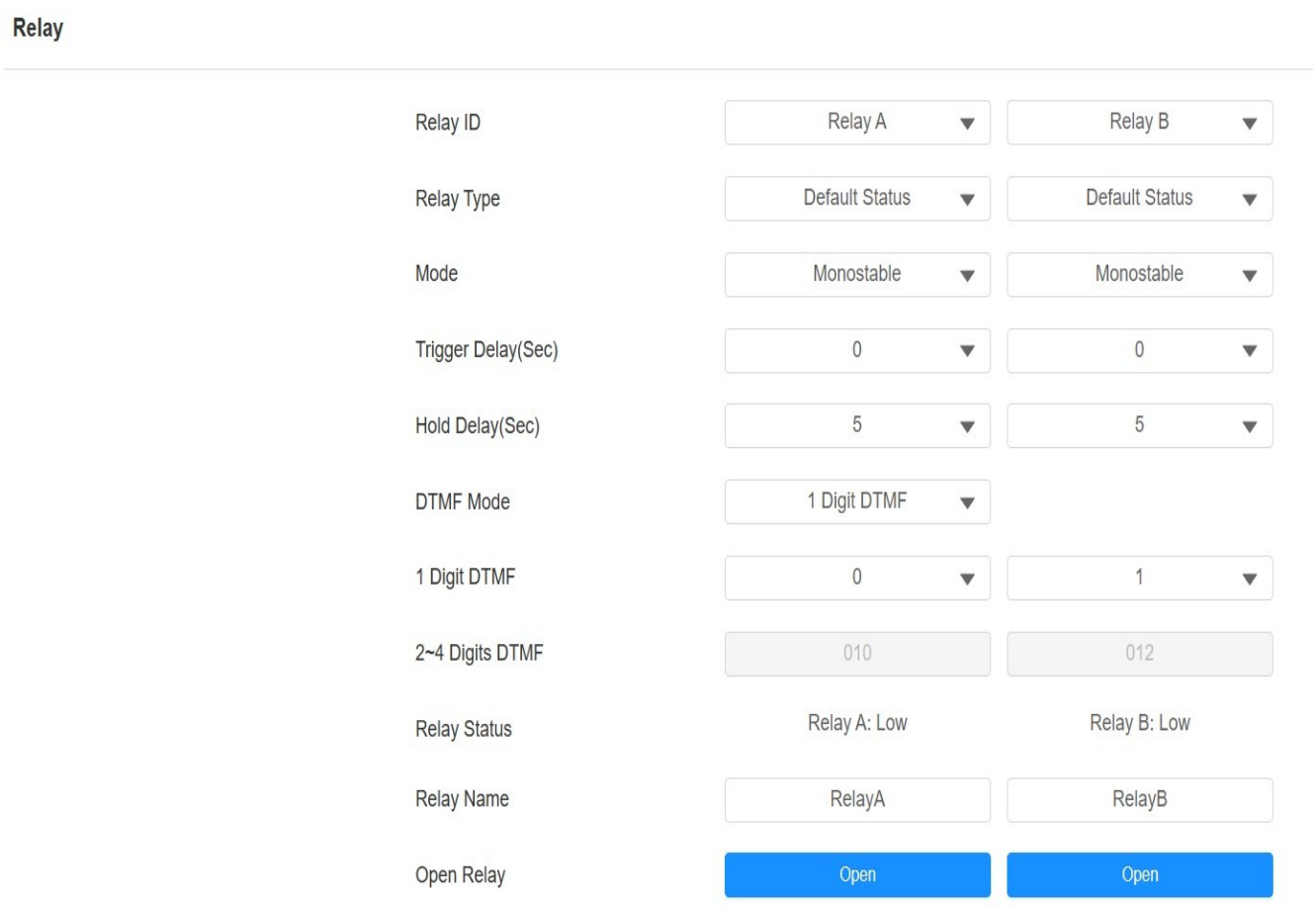
- **Jak powiadamiać DTMF**: Wybierz **Disabled (Wyłączone), DTMF**, **DTMF-Relay (Przekaźnik DTMF)** lub **Telephone-Event (Zdarzenie telefoniczne)** zgodnie z określonym typem przyjętym przez urządzenie innej firmy. Konfiguracja jest wymagana tylko wtedy, gdy urządzenie innej firmy, z którym ma zostać nawiązane połączenie, przyjmuje tryb **Info.**
- **Payload (Ładunek**): Ustaw ładunek zgodnie z określonym ładunkiem transmisji danych uzgodnionym między nadawcą i odbiorcą podczas transmisji danych.

Ustawienie przekaźnika

Ustawienie przełącznika przekaźnika

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

> Interfejs **przekaźnika.**



- Identyfikator **przekaźnika**: określony przekaźnik dostępu do drzwi.
- **Typ przekaźnika** : 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.

- **Opóźnienie wyzwalania (sek.)**: 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.

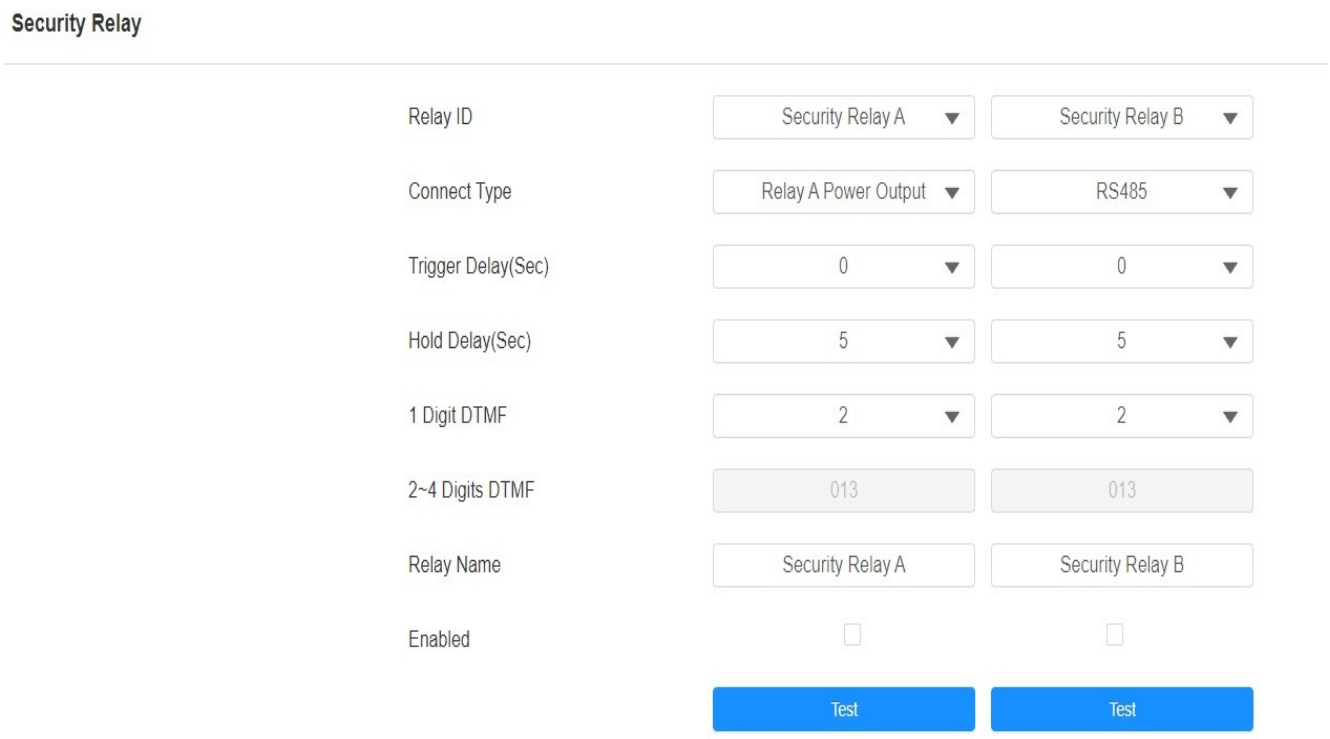
> **Uwaga**
>
> Urządzenia zewnętrzne podłączone do przekaźnika wymagają osobnego zasilacza.

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 Web **Access Control > Relay.**



- **Typ połączenia** : Wybierz typ połączenia między przekaźnikiem bezpieczeństwa a bramofonem. Można wybrać połączenie przez wyjście zasilania przekaźnika A bramofonu lub RS485.
- **Opóźnienie wyzwalania (sek.)**: 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.

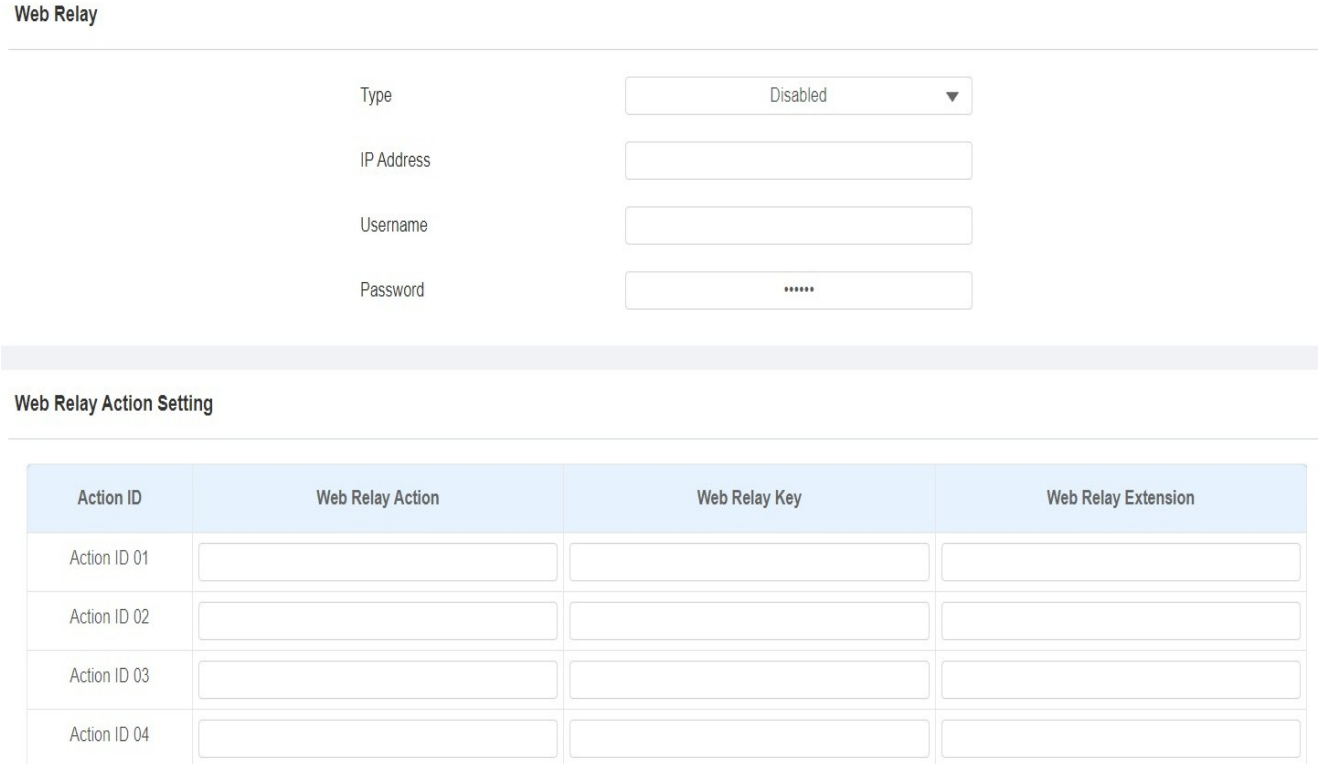
- **Nazwa przekaźnika** : Nazwa przekaźnika bezpieczeństwa. Nazwa może być wyświetlana w dziennikach otwarcia drzwi.

  Podczas łączenia się z chmurą SmartPlus Cloud serwer chmury automatycznie przypisze nazwę przekaźnika.

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 skonfigurować przekaźnik sieciowy, przejdź do opcji **Kontrola dostępu >** Interfejs **przekaźnika sieciowego.**



- **Typ** : Dostępne są trzy opcje: **Disabled (Wyłączone**), **Only WebRelay (Tylko przekaźnik internetowy)** i **Both Local Relay and Web Relay (Zarówno przekaźnik lokalny, jak i internetowy).**
- **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**: 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 skonfigurowanego kodu 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

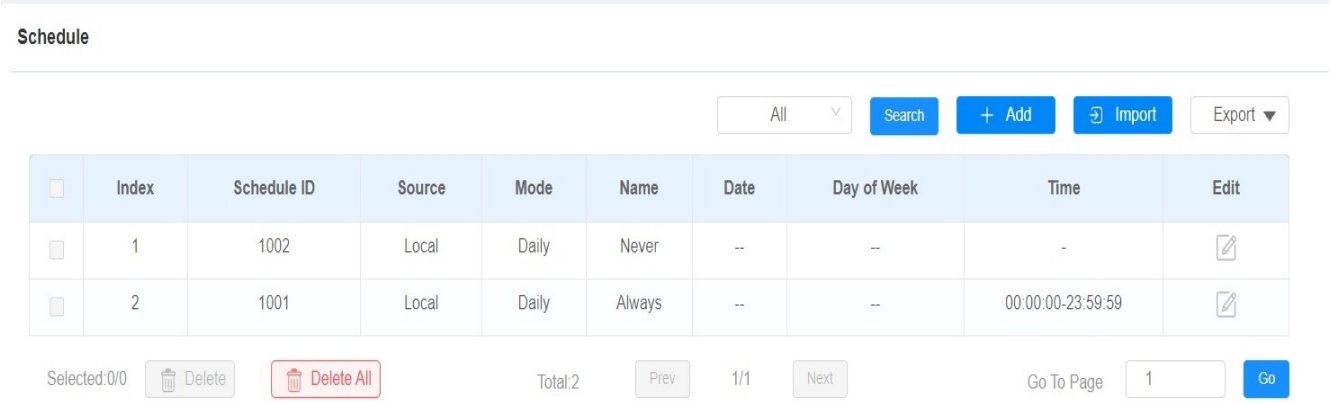
Konfiguracja harmonogramu dostępu do drzwi

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.

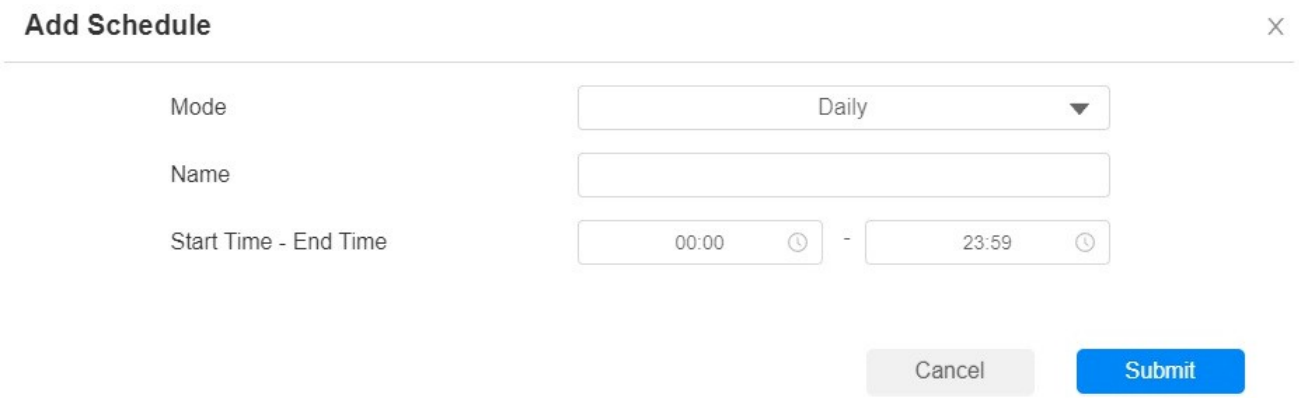
Tworzenie harmonogramu dostępu do drzwi

Harmonogramy dostępu do drzwi można tworzyć dla okresów dziennych, tygodniowych lub niestandardowych.

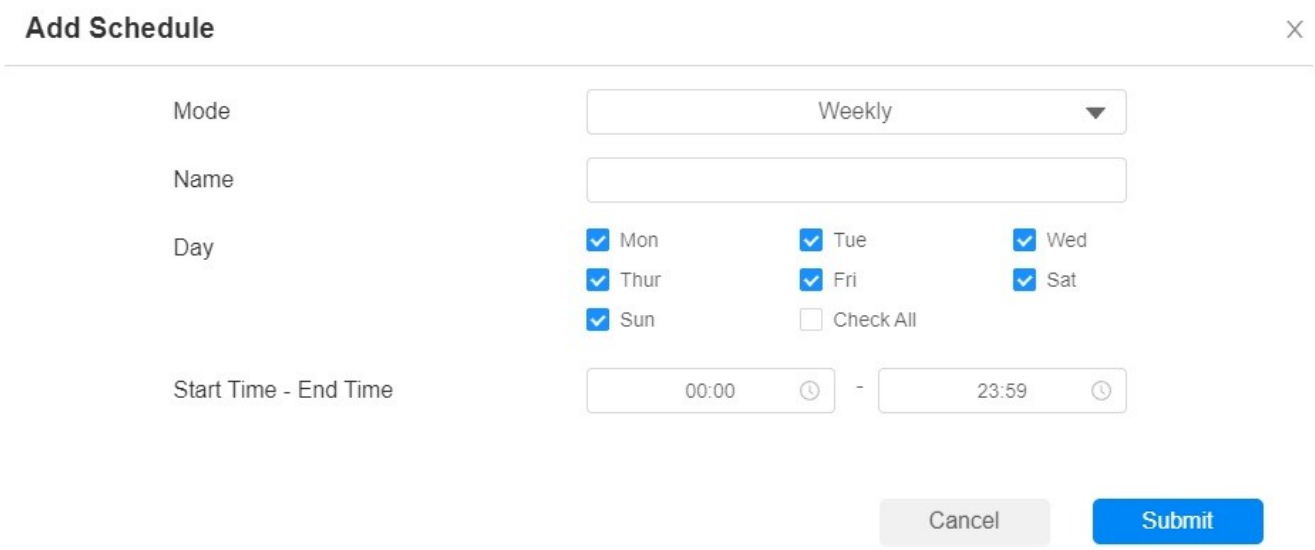
Aby skonfigurować harmonogram, przejdź do interfejsu Web **Setting > Schedule.** Kliknij **+Add**, aby utworzyć harmonogram.



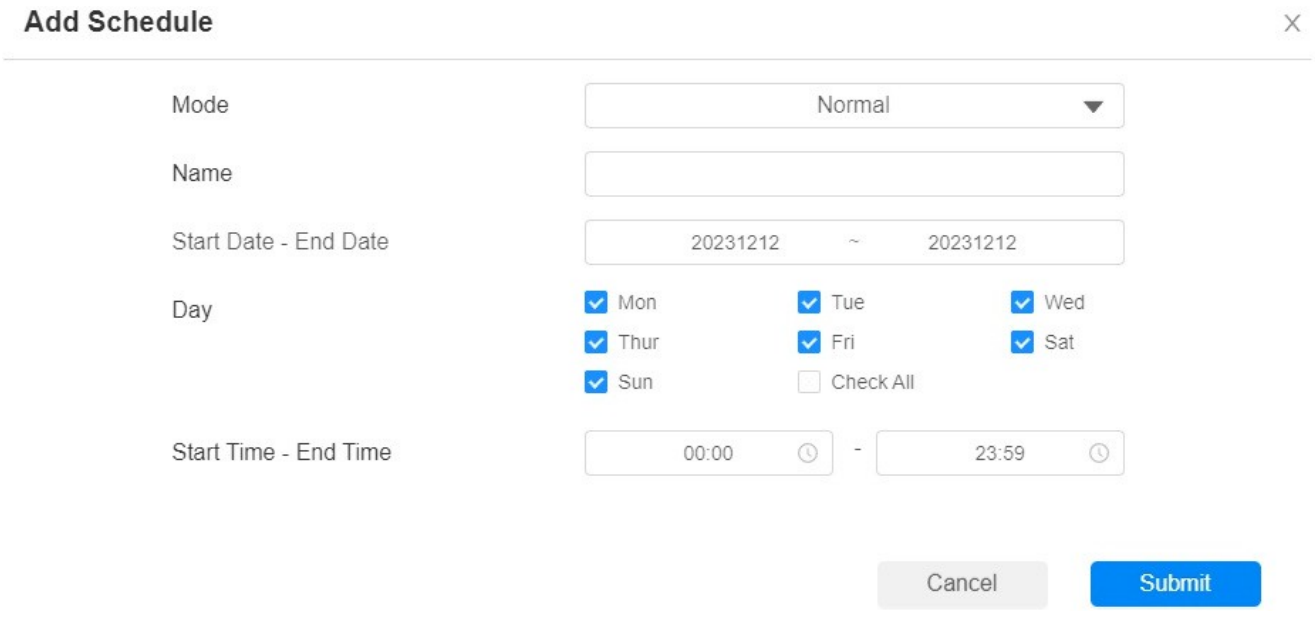
Aby utworzyć harmonogram dzienny:



Aby utworzyć harmonogram tygodniowy:



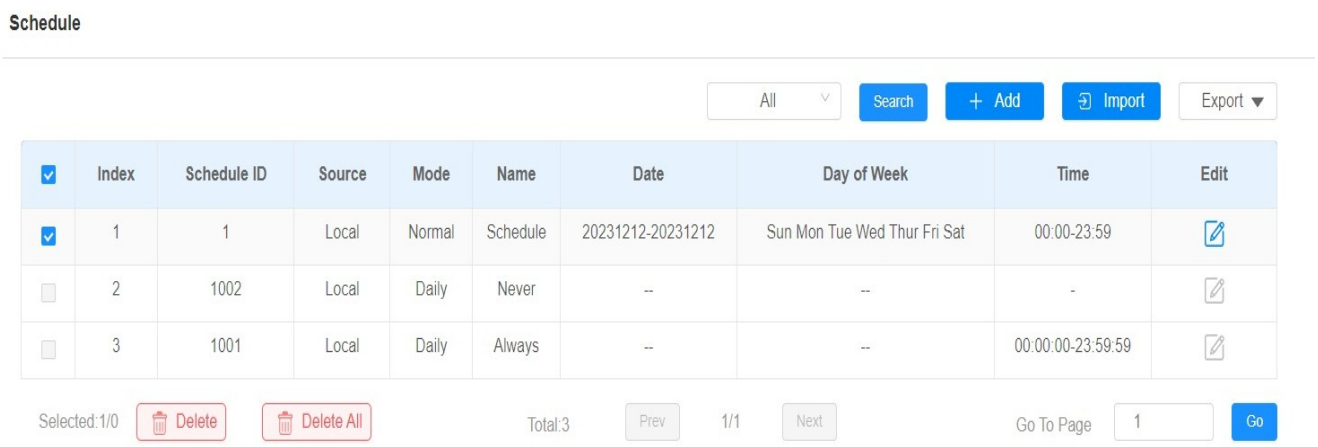
Aby utworzyć harmonogram na dłuższy okres:



Edycja harmonogramu dostępu do drzwi

Przejdź do interfejsu **Ustawienia** sieciowe **> Harmonogram.**

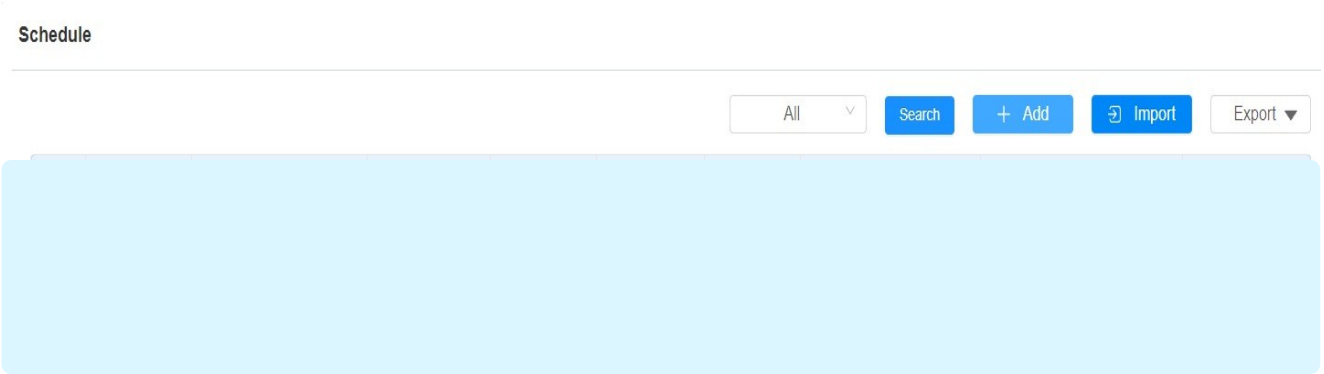
Zaznacz pole harmonogramu lokalnego, który chcesz edytować lub usunąć. Harmonogramu kontroli dostępu zsynchronizowanego z aplikacją SmartPlus nie można edytować ani usunąć.



Harmonogram importu i eksportu dostępu do drzwi

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

Przejdź do interfejsu **Ustawienia** sieciowe **> Harmonogram.**



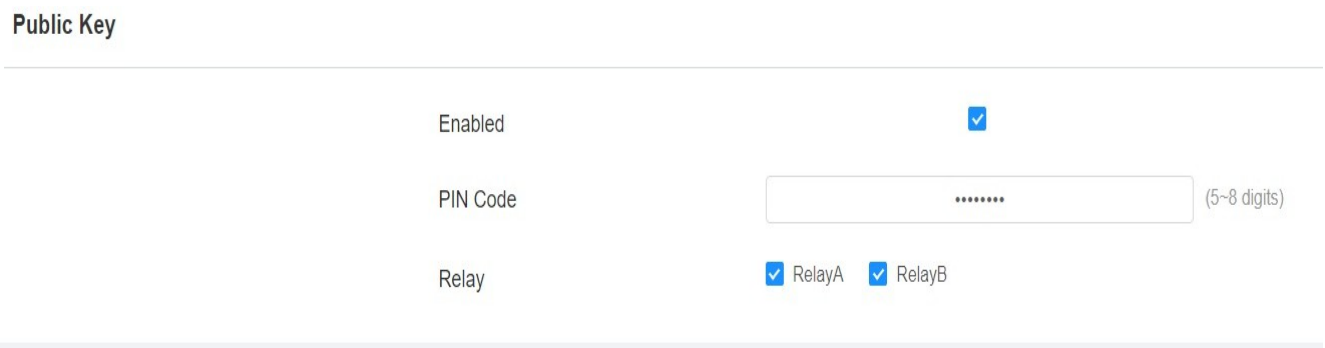
Konfiguracja odblokowania drzwi

Konfiguracja kodu PIN do odblokowywania drzwi

Istnieją dwa rodzaje kodów PIN dostępu do drzwi: publiczny i prywatny. Prywatny kod PIN jest unikalny dla każdego użytkownika, podczas gdy publiczny jest współdzielony przez mieszkańców tego samego budynku lub kompleksu. Można tworzyć i modyfikować zarówno publiczne, jak i prywatne kody PIN.

Konfiguracja publicznego kodu PIN

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

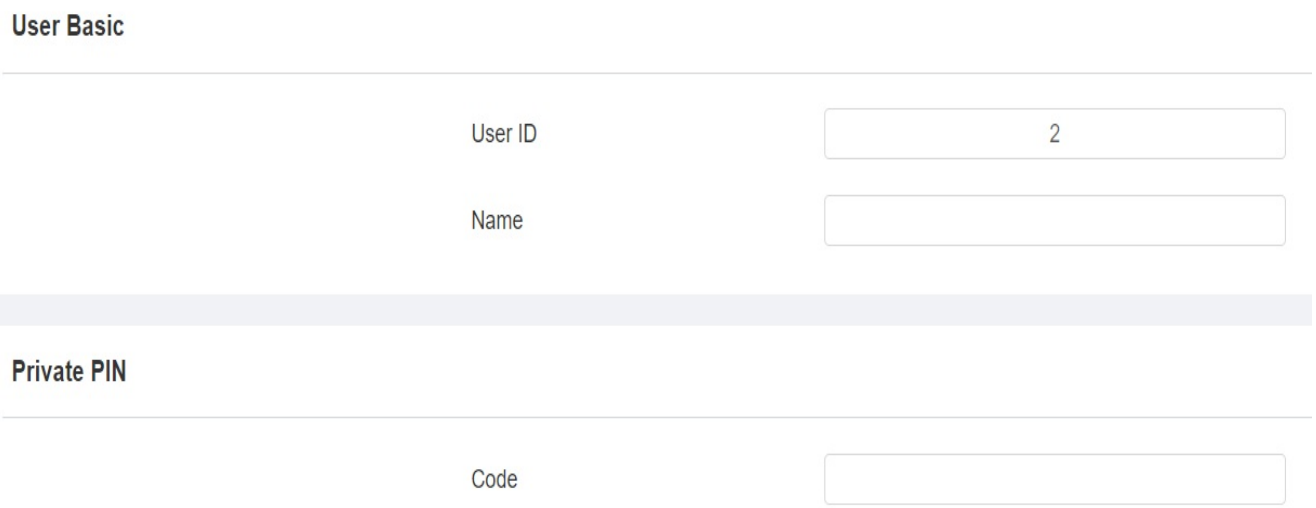


- **Kod PIN** : Ustawienie 3-8-cyfrowego kodu PIN dostępnego do uniwersalnego użytku.
- **Przekaźnik**: Przekaźnik, który ma zostać wyzwolony.

Konfiguracja prywatnego kodu PIN

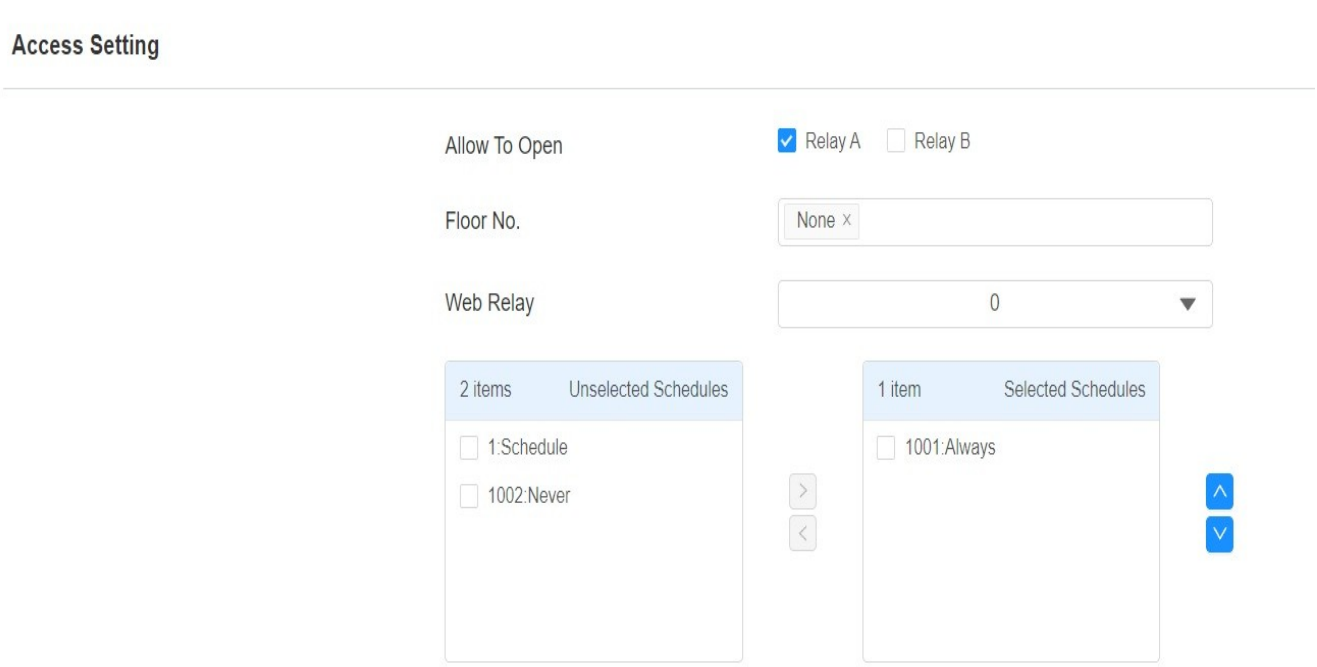
W interfejsie internetowym można utworzyć kod PIN i dostosować dodatkowe ustawienia, takie jak zdefiniowanie harmonogramu dostępu do drzwi w celu określenia, kiedy kod jest ważny i określenia, który przekaźnik ma zostać otwarty.

Przejdź do interfejsu Web **Directory > User.** Kliknij przycisk Add, aby skonfigurować prywatny kod PIN.



- **Identyfikator użytkownika**: unikalny numer identyfikacyjny przypisany do użytkownika.
- **Nazwa**: nazwa tego użytkownika.
- **Kod** : Ustawienie 2-8-cyfrowego kodu PIN wyłącznie do użytku tego użytkownika. Każdemu użytkownikowi można przypisać tylko jeden kod PIN.

Przewiń w dół i wybierz harmonogram dostępu do prywatnych drzwi z kodem PIN.



- **Allow To Open (Zezwalaj na otwieranie)**: umożliwia określenie przekaźników, które mają być odblokowywane przy użyciu metod otwierania drzwi przypisanych do użytkownika.
- **Floor NO.**: Określ piętra dostępne dla użytkownika za pośrednictwem windy.
- **Web Relay**: Określa identyfikator poleceń akcji web relay skonfigurowanych w interfejsie Web Relay. Domyślna wartość 0 oznacza, że przekaźnik sieciowy nie będzie uruchamiany.
- **Harmonogram** : Przyznaj użytkownikowi dostęp do otwierania wyznaczonych drzwi w ustalonych okresach, przenosząc żądany harmonogram (harmonogramy) z prawego pola do lewego. 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.

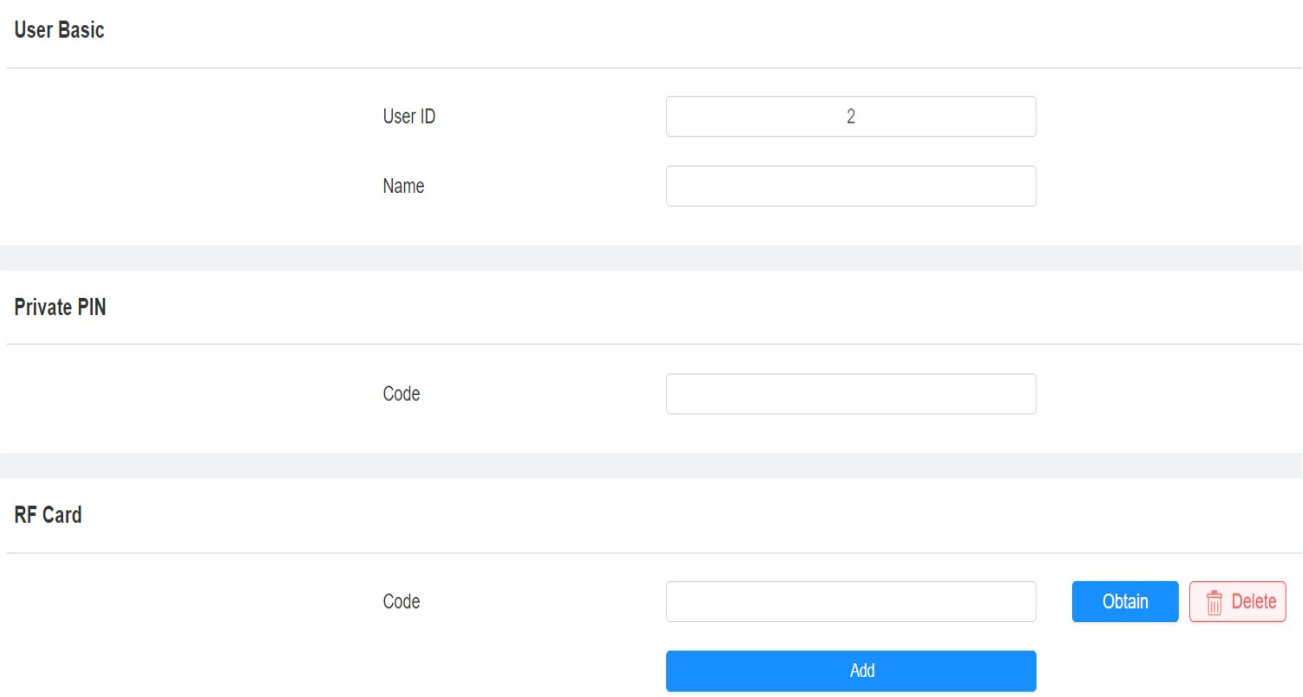
Uwaga

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

Konfiguracja karty RF do odblokowywania drzwi

Konfiguracja karty RF

Przejdź do **Katalog** internetowy **>** Interfejs **użytkownika.** Kliknij Add, aby skonfigurować kartę RF. Umieść kartę w obszarze czytnika kart i kliknij Obtain, aby dodać kartę.



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

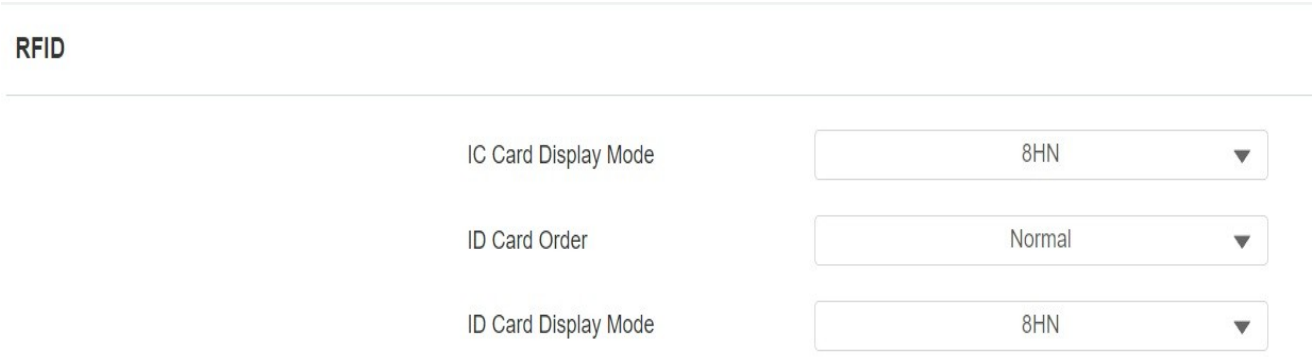
Uwaga

- Karty RF o częstotliwości 13,56 MHz i 125 KHz mogą być stosowane w bramofonie do drzwi.
- Każdy użytkownik może mieć dodanych maksymalnie 5 kart.
- Urządzenie pozwala na dodanie 10000 użytkowników.
- Karty RF działające na częstotliwościach 13,56 MHz i 125 KHz są kompatybilne z bramofonem.
- Na urządzeniu można również dodawać karty administratora. Naciśnij *2396# na klawiaturze. Następnie dotknij 2 i 1, aby przejść do ekranu ustawień karty, na którym można dodać lub usunąć kartę RF.

Konfiguracja formatu kodu karty RF

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

Aby skonfigurować kod karty RF, przejdź do interfejsu Web **Access Control > Card Setting.**

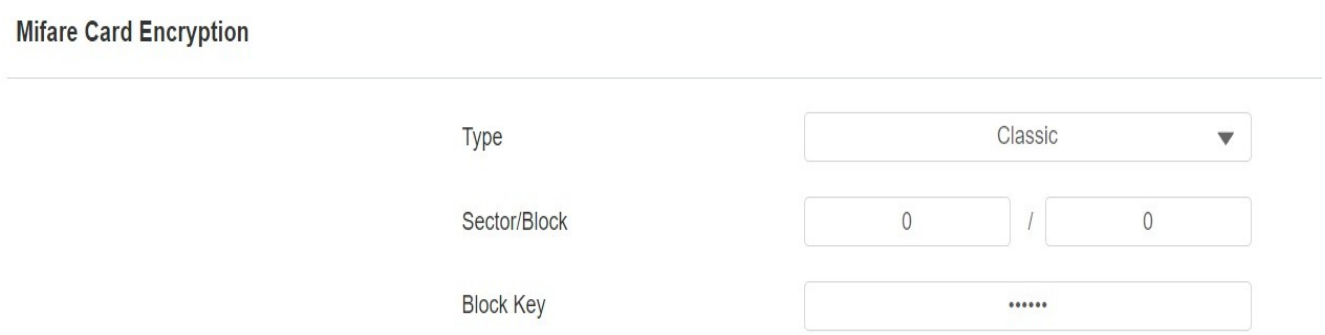


- **Tryb wyświetlania karty IC/ID** : Ustaw format numeru karty spośród dostępnych opcji. Domyślnym formatem w bramofonie jest 8HN.
- **Kolejność kart ID**: Wybór normalnego lub odwróconego wyświetlania numeru karty ID.

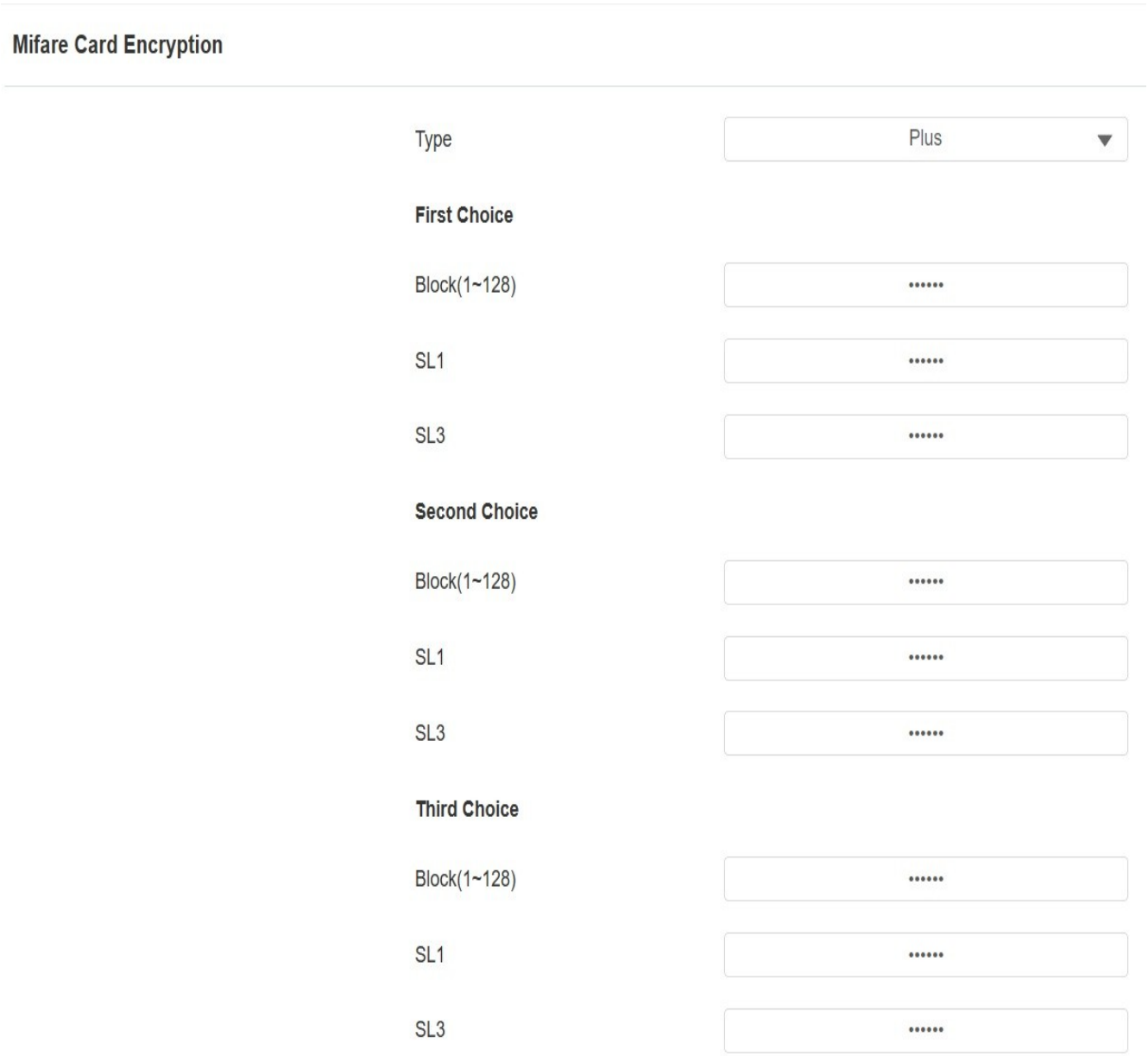
Szyfrowanie kart Mifare

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 skonfigurować kartę Mifare, przejdź do interfejsu Web **Access Control > Card Setting.**



- **Typ** : Dostępne są trzy opcje: **Brak, Klasyczny** i **Plus**.
- **Classic** :
    - **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.

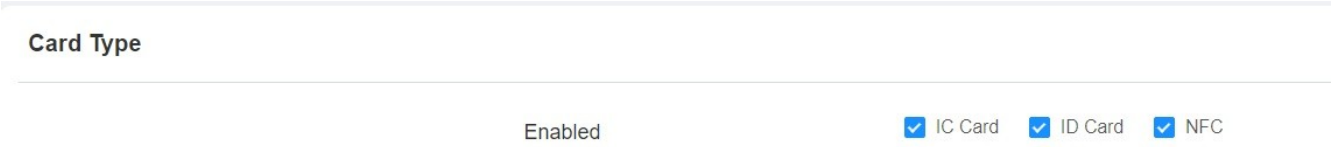


- **Plus**: Dostępne są trzy opcje bloków. Urządzenie może odczytać zaszyfrowane dane w SL1 i SL3.
    - **Blok**: numer bloku, w którym znajdują się zaszyfrowane dane.
    - **SL1**: numer klucza w zakresie 24 bitów.
    - **SL3**: numer klucza w zakresie 32 bitów.

Ustawienia karty NFC

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

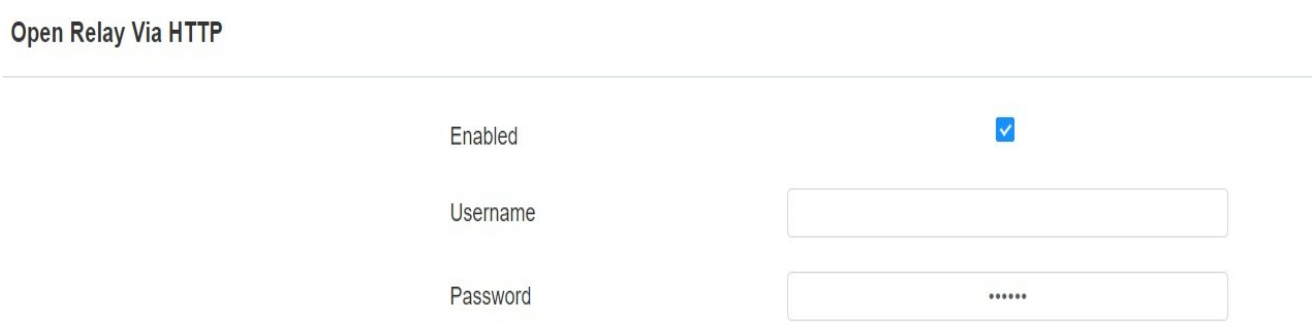
Aby skonfigurować NFC, przejdź do interfejsu Web **Access Control > Card Setting.** Włącz typ karty przed użyciem karty do otwarcia drzwi.



Konfiguracja Open Relay przez HTTP dla odblokowywania drzwi

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

Aby ją skonfigurować, przejdź do interfejsu Web **Access Control > Relay > Open Relay Via HTTP.**



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

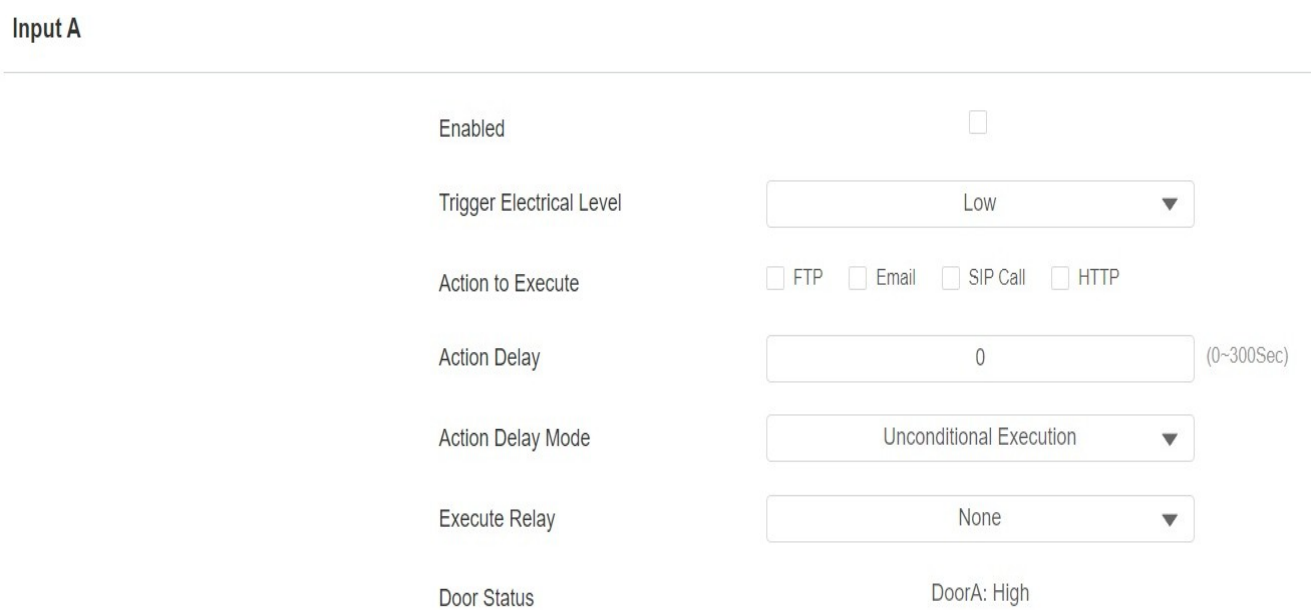
Wskazówka

Oto przykład adresu URL polecenia HTTP:

Konfiguracja przycisku wyjścia do odblokowywania drzwi

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

Przejdź do interfejsu Web **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, włącz HTTP i wprowadź adres URL.

- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/Treść wiadomości.
- **Opóźnienie działania**: Określa, czy przekaźnik może zostać wyzwolony w dowolnym momencie, czy tylko w zaplanowanym okresie.
- **Tryb opóźnienia działania** :
  - **Bezwarunkowe wykonanie**: akcja zostanie wykonana po wyzwoleniu wejścia.

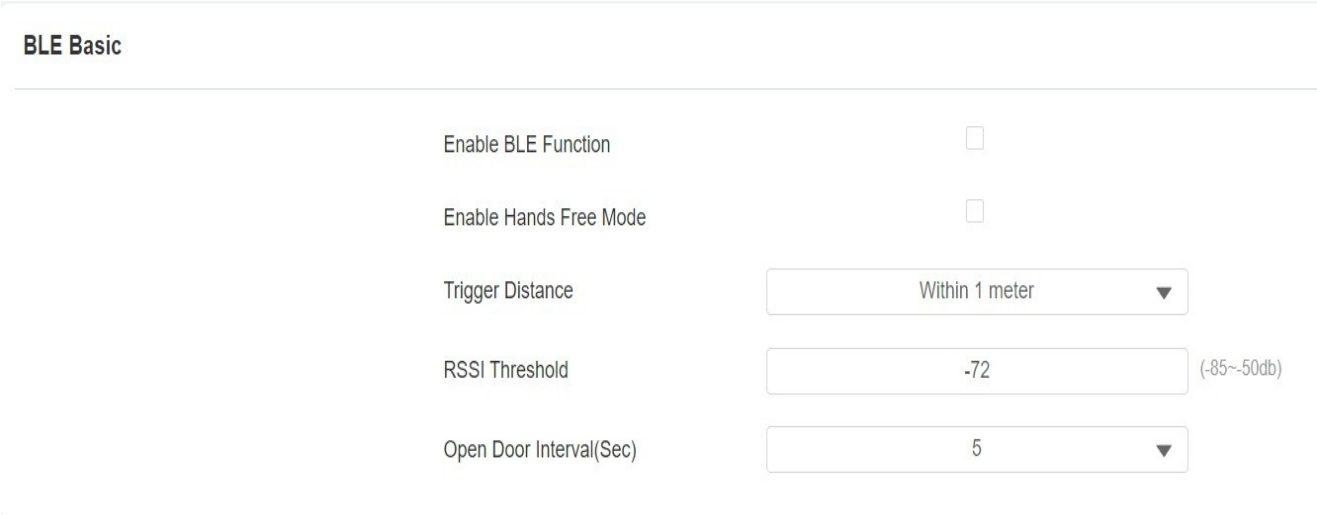
- **Execute If Input Still Triggered**: akcja zostanie wykonana, gdy wejście pozostanie wyzwolone. Na przykład, jeśli drzwi pozostaną otwarte po wyzwoleniu wejścia, zostanie wysłana akcja, taka jak wiadomość e-mail, aby powiadomić odbiorcę.

- **Wykonaj przekaźnik**: Określa przekaźnik, który ma być wyzwalany przez akcje.

Konfiguracja Bluetooth do odblokowywania drzwi

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

Aby skonfigurować odblokowanie Bluetooth, przejdź do interfejsu Web **Access Control > BLE.**



- **Włącz tryb głośnomówiący** : Jeśli jest włączony, użytkownicy mogą uzyskać dostęp do drzwi bez użycia rąk. Jeśli jest wyłączony, użytkownicy muszą machać rękami przed bramofonem, aby otworzyć drzwi.

- **Odległość wyzwalania**: Ustaw odległość wyzwalania Bluetooth dla dostępu do drzwi. Do wyboru są opcje Około 1 metra, W promieniu 1 metra i Ponad 2 metry. Odległość wyzwalania wynosi maksymalnie 3 metry.

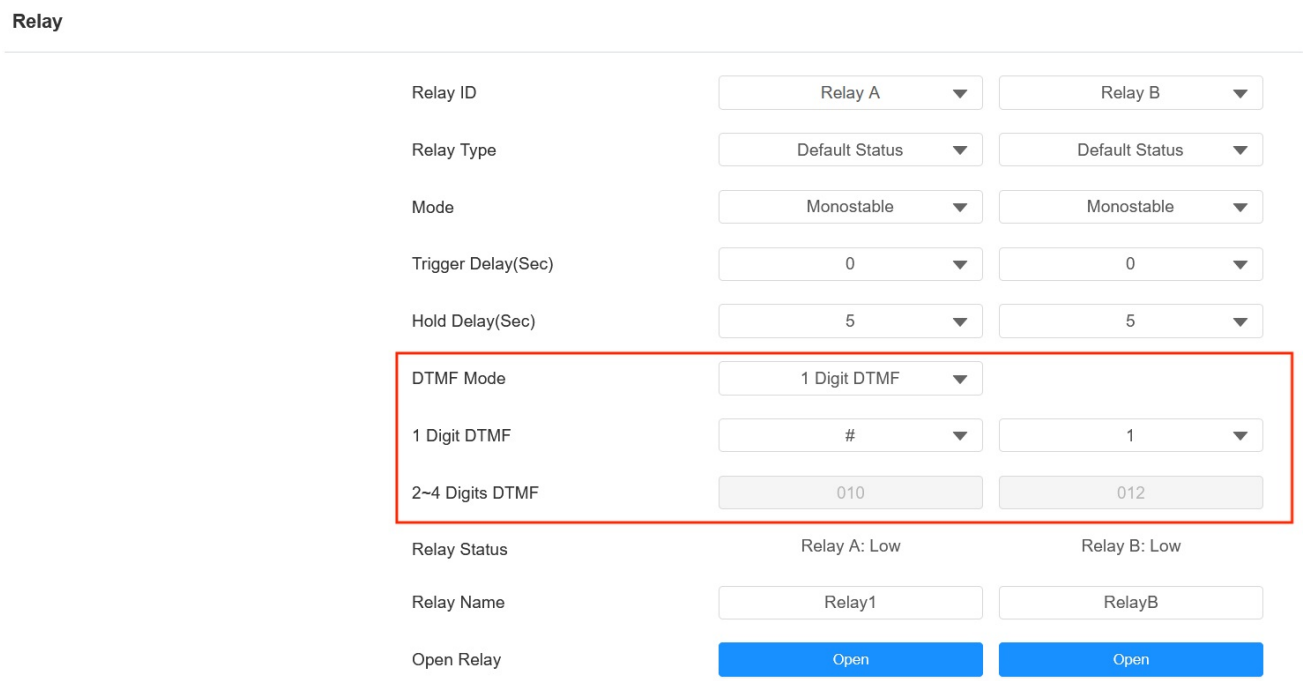
- **Próg RSSI**: Ustawienie siły odbieranego sygnału. Wyższe wartości oznaczają większą siłę sygnału, co ułatwia odbieranie sygnału Bluetooth.

- **Interwał otwarcia drzwi**: Ustawienie odstępu czasu między kolejnymi próbami uzyskania dostępu do drzwi przez Bluetooth.

Konfiguracja przekaźnika otwarcia poprzez DTMF dla odblokowania drzwi

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

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



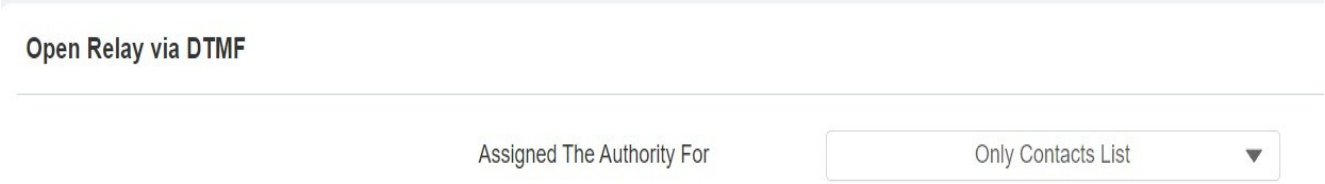
- **Tryb DTMF** : Ustaw liczbę cyfr dla kodu DTMF.
- **1 Digit DTMF**: Zdefiniuj 1-cyfrowy kod DTMF w zakresie (0-9 i *,#), gdy tryb DTMF jest ustawiony na 1-cyfrowy.
- **2-4 Digit DTMF** : Ustaw kod DTMF na podstawie liczby cyfr wybranych w trybie DTMF.

Uwaga

Aby otworzyć drzwi za pomocą DTMF, urządzenia interkomowe, które wysyłają i odbierają polecenie odblokowania, muszą używać tego samego trybu i kodu. W przeciwnym razie odblokowanie DTMF może się nie powieść. Szczegółowe kroki konfiguracji DTMF można znaleźć **tutaj.**

Biała lista DTMF

Aby skonfigurować białą listę DTMF, przejdź do strony internetowej **Access Control > Relay > Open Relay via DTMF** interface.



- **Przypisane uprawnienia dla**: Określ kontakty upoważnione do otwierania drzwi za pomocą DTMF:

  - **Brak** : Żaden numer nie może odblokować drzwi za pomocą DTMF.

  - **Tylko lista kontaktów**: Tylko numery dodane do listy kontaktów bramofonu mogą być odblokowywane za pomocą DTMF.

  - **Wszystkie numery**: Każdy numer można odblokować za pomocą DTMF.

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

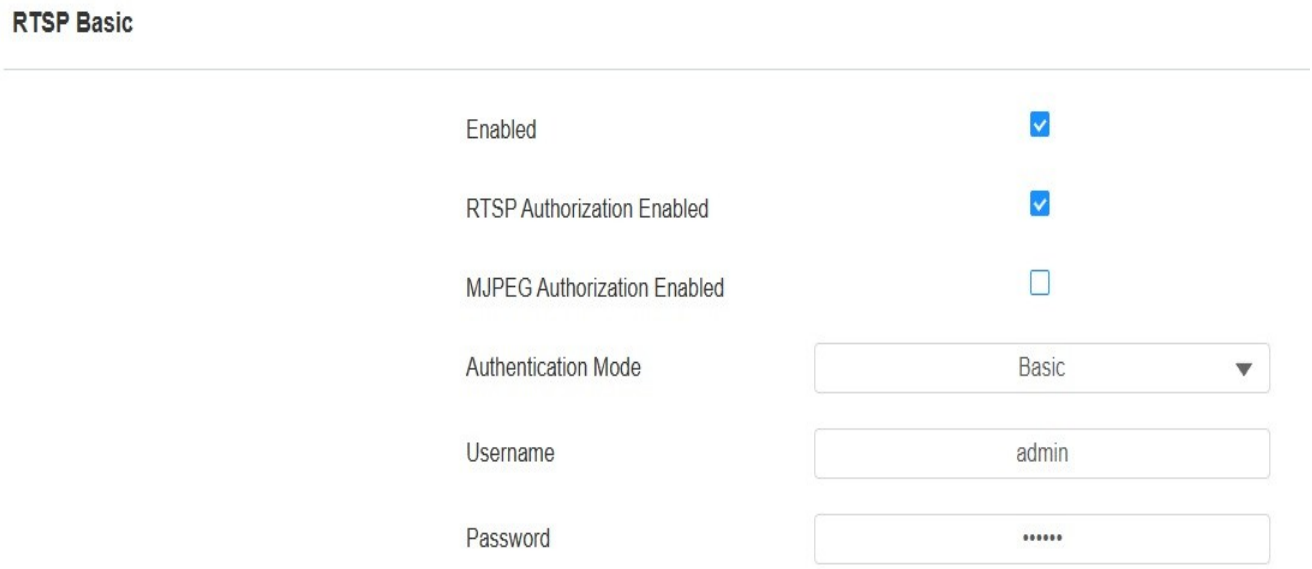
ONVIF to Otwarte Forum Sieciowego Interfejsu Wideo. Umożliwia urządzeniu skanowanie i wykrywanie kamer lub urządzeń domofonowych z aktywowanymi funkcjami ONVIF. Strumienie na żywo uzyskiwane za pośrednictwem ONVIF są zasadniczo w formacie RTSP.

Monitorowanie strumienia RTSP

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

Podstawowe ustawienia RTSP

Aby skonfigurować RTSP, przejdź do interfejsu Web **Surveillance > RTSP.**

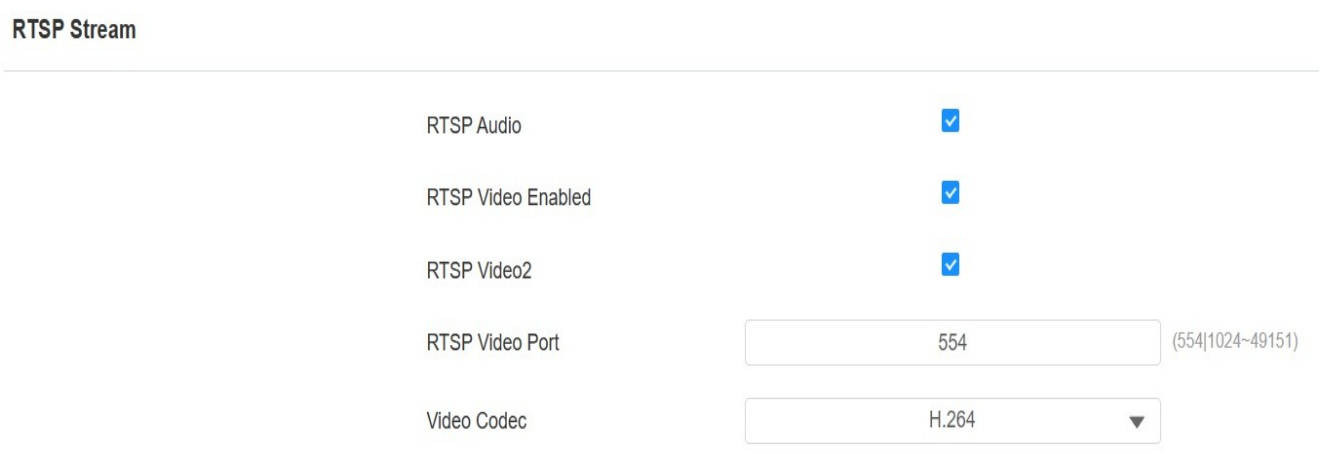


- **Włączona autoryzacja RTSP**: Po włączeniu autoryzacji RTSP wymagane jest skonfigurowanie trybu uwierzytelniania RTSP, nazwy użytkownika RTSP i hasła do autoryzacji.
- **Tryb uwierzytelniania** : Dostępne są dwie opcje: Basic i Digest. **Basic** jest domyślnym typem uwierzytelniania.
- **Nazwa użytkownika**: Ustaw nazwę użytkownika do uwierzytelniania.
- **Hasło**: ustawienie hasła uwierzytelniania.

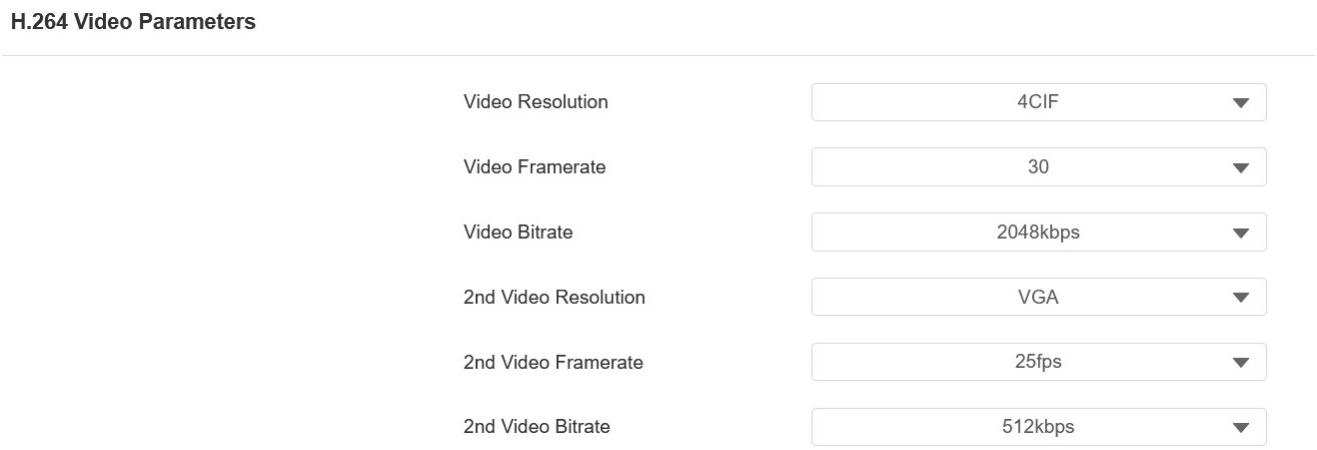
Ustawienia strumienia RTSP

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

Aby skonfigurować strumień RTSP, przejdź do interfejsu Web **Surveillance > RTSP.**



- **RTSP Audio**: Zezwala bramofonowi na wysyłanie informacji audio do monitora przez RTSP.
- **RTSP Video Enabled**: Bramofon może wysyłać informacje wideo do monitora. Po włączeniu funkcji RTSP wideo RTSP jest domyślnie włączone i nie można go modyfikować.
- **RTSP Video 2** : Bramofony Akuvox obsługują 2 strumienie RTSP, można włączyć drugi z nich.
- **Port wideo RTSP**: Wybierz odpowiedni kodek audio dla dźwięku RTSP.
- **Kodek wideo** : Wybierz odpowiedni kodek wideo dla wideo RTSP.

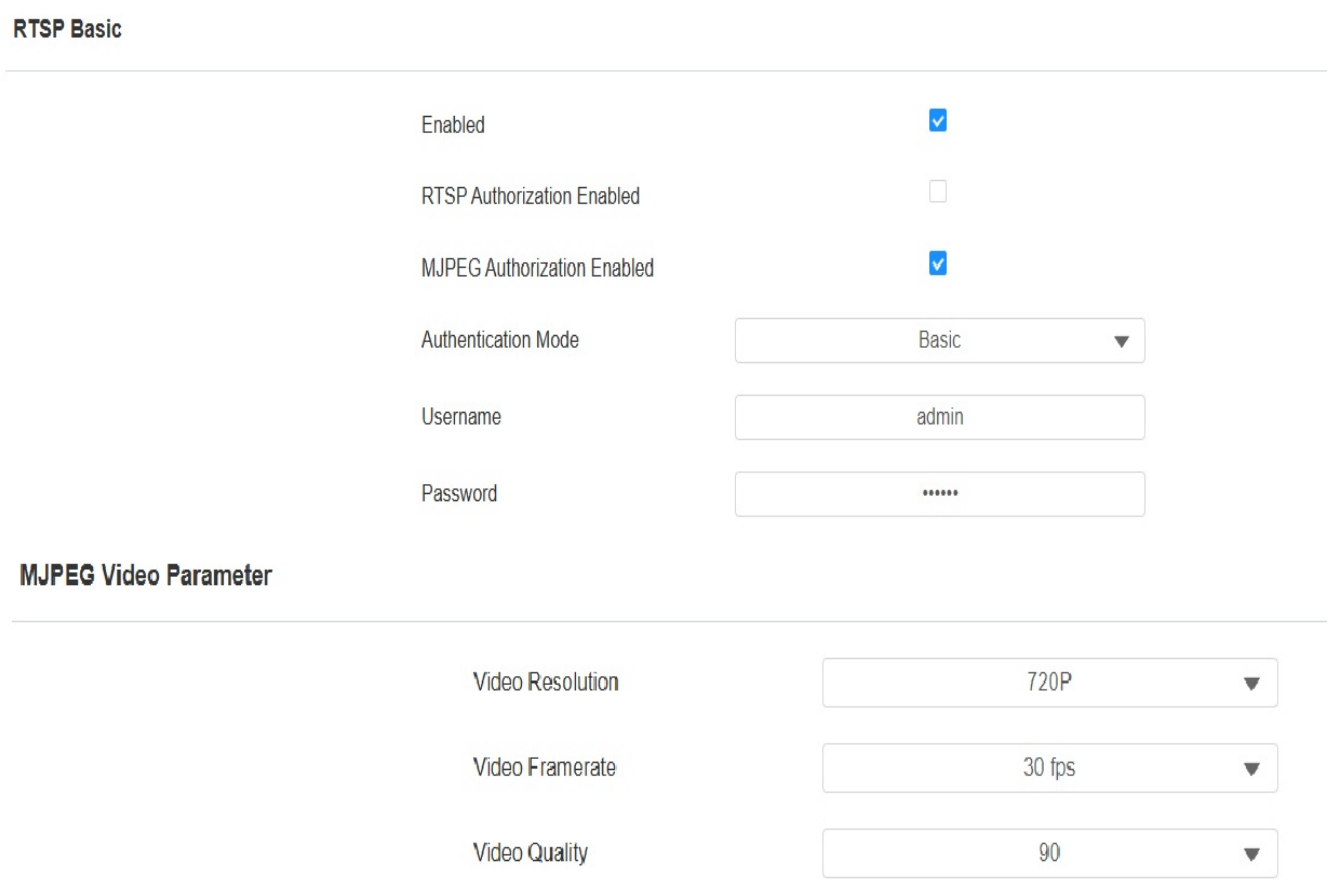


- **Rozdzielczość wideo**: Dostępne są następujące opcje: QVGA, CIF, VGA, 4CIF, 720P i 1080P. Domyślną rozdzielczością wideo jest **720P**. Wideo z bramofonu może nie być wyświetlane na monitorze wewnętrznym, jeśli rozdzielczość jest ustawiona na wyższą niż 720P.
- **Częstotliwość klatek wideo**: Domyślną częstotliwością klatek wideo jest 30 kl.
- **Szybkość transmisji wideo** : Dostępne są następujące opcje: 128 kb/s, 256 kb/s, 512 kb/s, 1024 kb/s, 2048 kb/s i 4096 kb/s. Wybierz ją w zależności od środowiska sieciowego. Domyślna szybkość transmisji wideo to 2048 kb/s.
- **2. rozdzielczość wideo**: Rozdzielczość wideo dla drugiego kanału strumienia wideo. Domyślną rozdzielczością wideo jest VGA.
- **2nd Video Framerate** : Liczba klatek na sekundę dla drugiego kanału strumienia wideo. Domyślnie dla drugiego kanału strumienia wideo ustawione jest 25 kl.
- **2. szybkość transmisji wideo** : Dostępne są następujące opcje: 128 kb/s, 256 kb/s, 512 kb/s, 1024 kb/s, 2048 kb/s i 4096 kb/s dla drugiego kanału strumienia wideo. Domyślnie drugi kanał strumienia wideo ma szybkość 512 kb/s.

Przechwytywanie obrazu MJPEG

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

Przejdź do interfejsu internetowego **Surveillance > RTSP**, aby włączyć tę funkcję i skonfigurować parametry.



- **MJPEG Authorization Enabled**: Po włączeniu wymagane jest skonfigurowanie trybu uwierzytelniania, nazwy użytkownika RTSP i hasła do autoryzacji.
- **Nazwa użytkownika**: Ustaw nazwę użytkownika do uwierzytelniania.
- **Hasło**: ustawienie hasła uwierzytelniania.

Obraz z telefonu można przechwycić przy użyciu następujących trzech typów formatów URL:

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

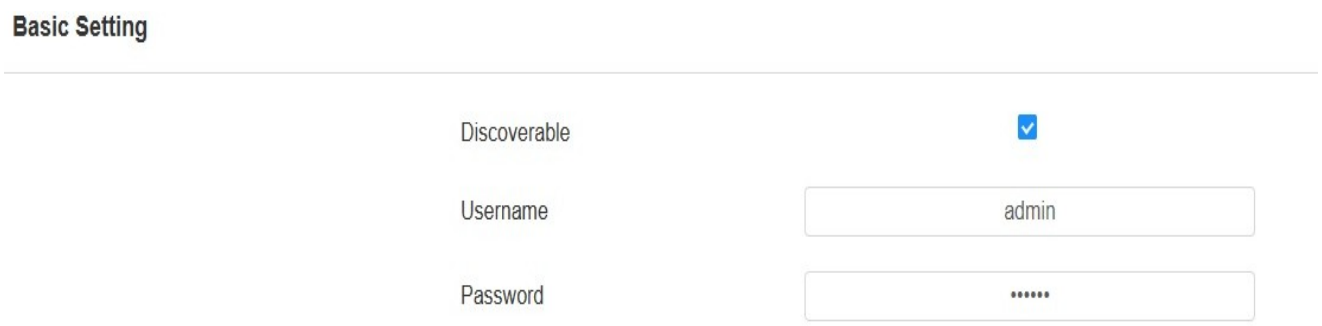
- **Tryb uwierzytelniania** : Dostępne są dwie opcje: Basic i Digest. **Basic** jest domyślnym typem uwierzytelniania.

- **Rozdzielczość wideo**: Dostępne są następujące opcje: QVGA, CIF, VGA, 4CIF, 720P i 1080P. Domyślną rozdzielczością wideo jest **720P**. Wideo z bramofonu może nie być wyświetlane na monitorze wewnętrznym, jeśli rozdzielczość jest ustawiona na wyższą niż 720P.
- **Szybkość klatek wideo** : Dostępne są trzy opcje: 10 fps, 15 fps i 30 fps. Domyślną szybkością klatek wideo jest 30 kl.
- **Jakość wideo**: Waha się od 50 do 90.

ONVIF

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

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



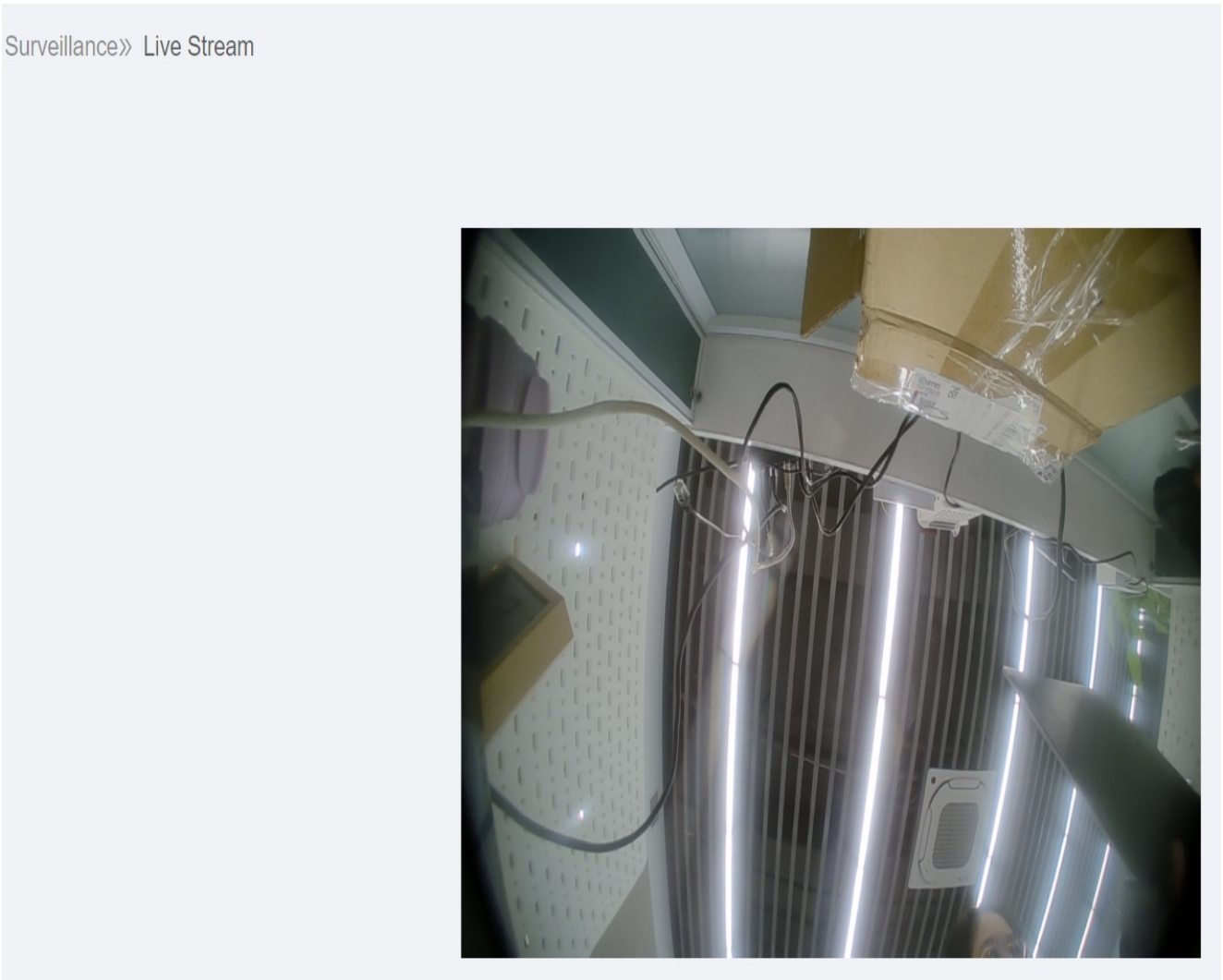
- **Discoverable**: Po włączeniu tej opcji obraz wideo z kamery telefonu może być wyszukiwany przez inne urządzenia.
- **Nazwa użytkownika** : Dostosuj nazwę użytkownika do uwierzytelniania. Domyślnie jest to admin.
- **Hasło** : Dostosuj hasło do uwierzytelniania. Domyślnie jest to admin.

Po zakończeniu ustawień można wprowadzić adres URL ONVIF na urządzeniu innej firmy, aby wyświetlić strumień wideo. Na przykład: http://IP address:80/onvif/device_service

Transmisja na żywo

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

Aby wyświetlić wideo w czasie rzeczywistym, przejdź do interfejsu internetowego **Surveillance > Live Stream.**

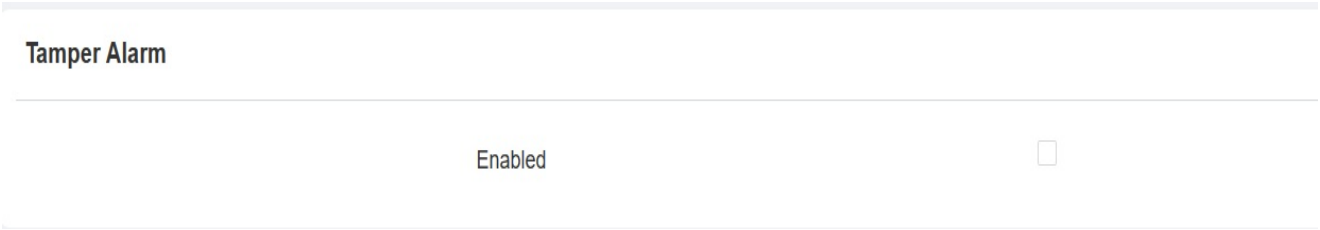


Bezpieczeństwo

Ustawienie alarmu sabotażowego

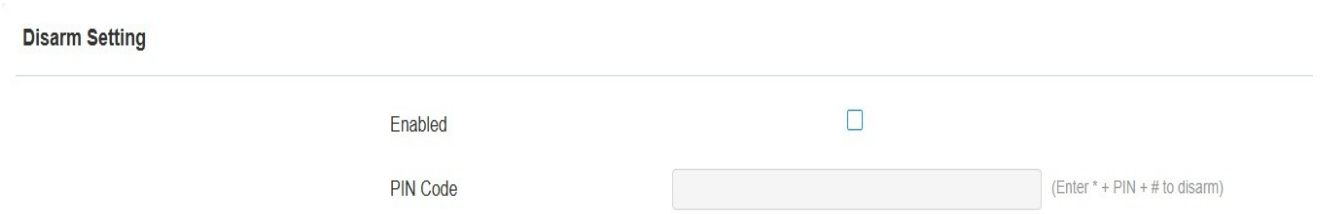
Funkcja alarmu sabotażowego zapobiega usuwaniu urządzeń przez osoby niepowołane. Odbywa się to poprzez uruchomienie alarmu sabotażowego i wykonanie połączenia do wyznaczonej lokalizacji, gdy urządzenie wykryje zmianę wartości grawitacji w stosunku do pierwotnej.

Aby skonfigurować alarm sabotażowy, przejdź do interfejsu internetowego **System > Security > Tamper Alarm.**



Ustawienie rozbrojenia

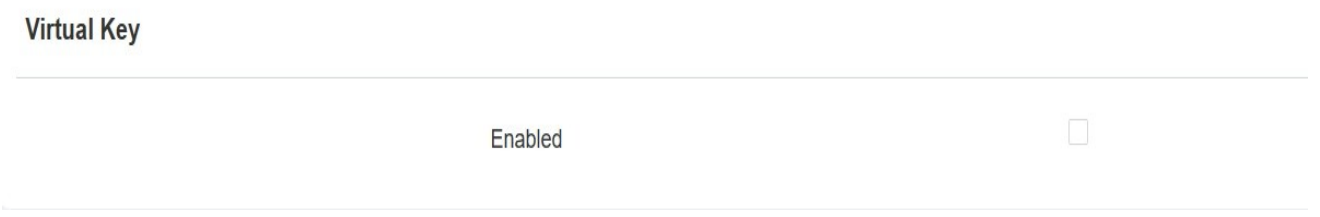
Kod rozbrojenia można ustawić w internetowym interfejsie **System > Security.**



Wirtualny kod PIN

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

Aby skonfigurować wirtualny kod PIN, przejdź do interfejsu Web **Access Control > PIN Setting.**



- **Enabled (Włączone)**: Jeśli opcja ta jest włączona, możesz umieścić fałszywe cyfry po obu stronach kodu PIN w celu jego ochrony. Na przykład, jeśli twoje hasło to 1234567, możesz umieścić 99 i 88 po obu stronach (99123456788). Wirtualne hasło jest dopasowywane do użytkowników na podstawie liczby pasujących cyfr. Na przykład, jeśli użytkownik A ma większą liczbę cyfr pasujących do wprowadzonego hasła wirtualnego niż użytkownik B, zostanie ono uznane za hasło użytkownika A. Jednak w przypadku zastosowania podwójnego uwierzytelniania, wirtualne hasło zostanie dopasowane do użytkowników, którzy przejdą pierwszy poziom uwierzytelniania, na przykład Face + PIN.

> **Uwaga**
>
> Ta funkcja nie jest używana w przypadku publicznych kodów PIN i Apartment+PIN.

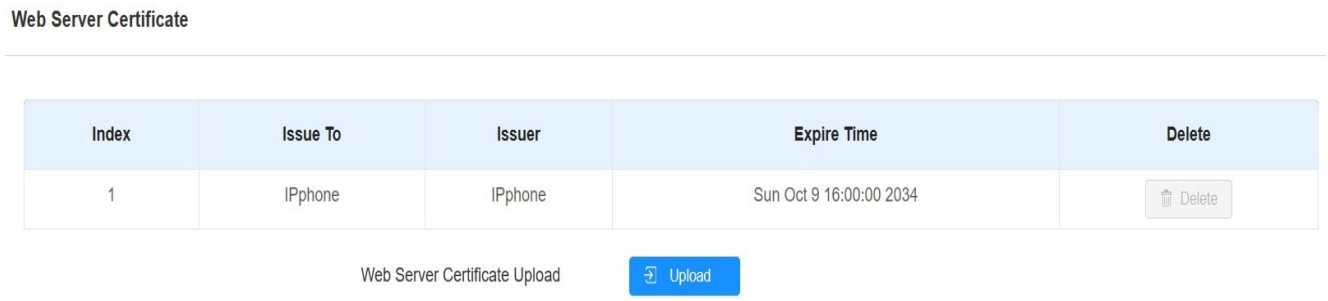
Ustawienia certyfikatu klienta

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

Certyfikat serwera WWW

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

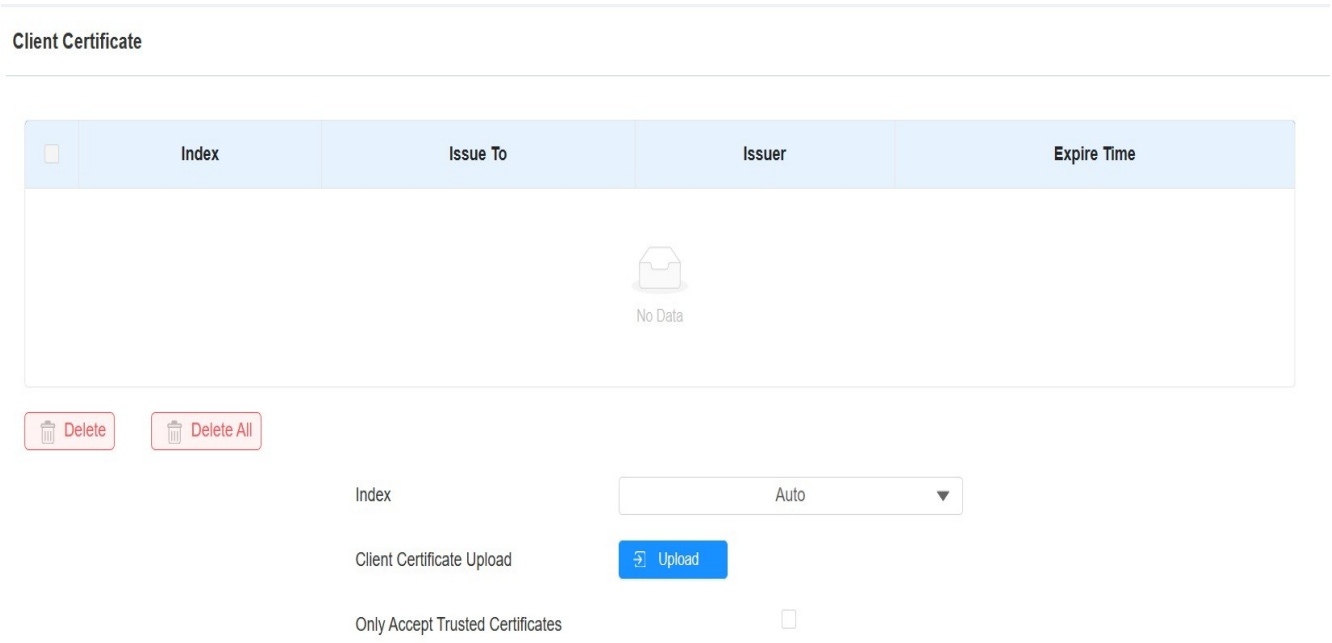
Aby przesłać certyfikat, przejdź do interfejsu internetowego **System > Certificate.**



Certyfikat klienta

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

Aby przesłać certyfikat, przejdź do interfejsu internetowego **System > Certificate.**

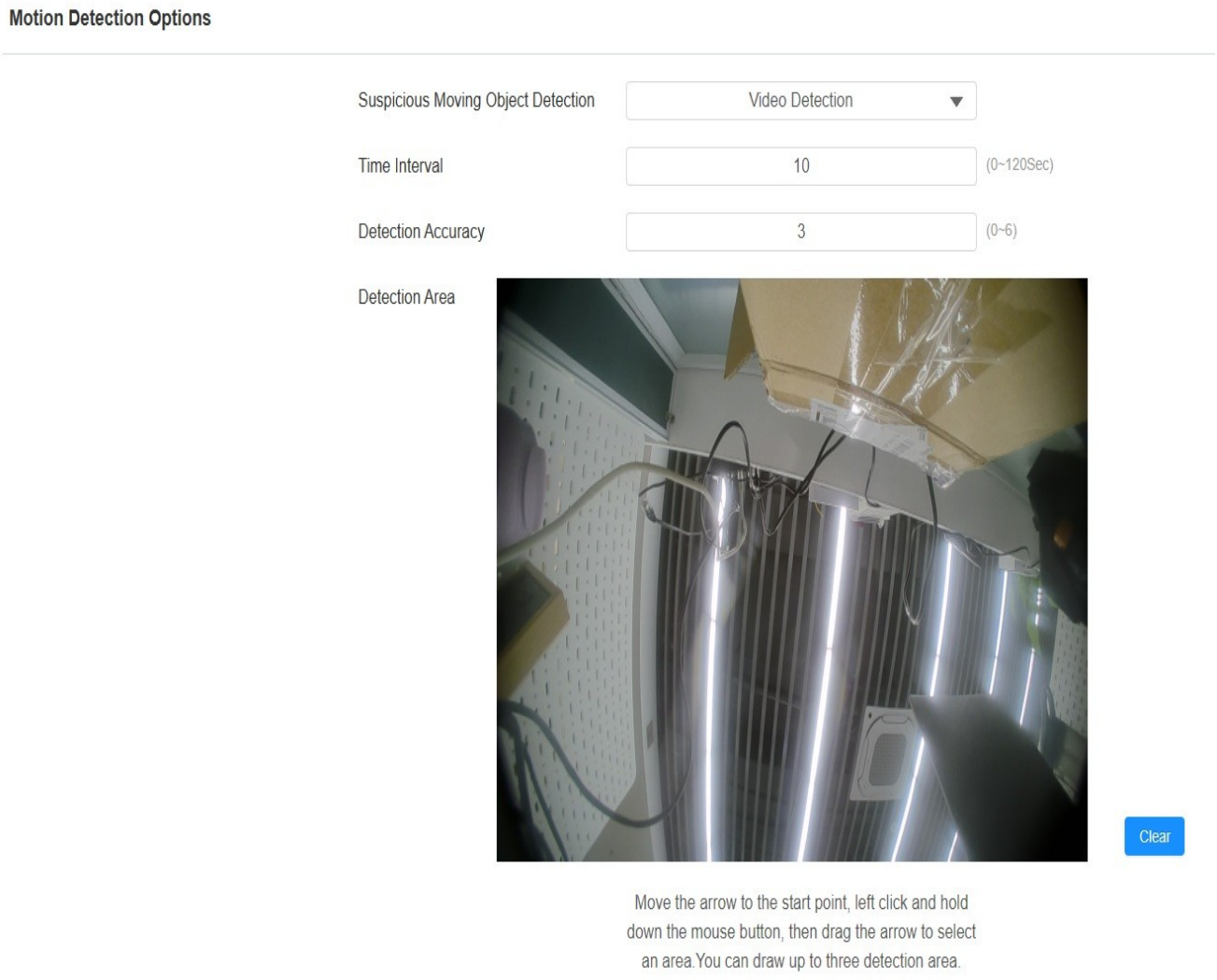


- **Indeks**: Wybierz żądaną wartość z listy rozwijanej Indeks. W przypadku wybrania opcji Auto przesłany certyfikat zostanie wyświetlony w kolejności numerycznej. W przypadku wybrania wartości od 1 do 10 przesłane certyfikaty będą wyświetlane zgodnie z numerami.
- **Przesyłanie certyfikatu klienta** : Zlokalizuj i prześlij żądany certyfikat (tylko *.pem).
- **Akceptuj tylko zaufane certyfikaty** : Po włączeniu tej opcji telefon będzie weryfikował certyfikat serwera na podstawie listy certyfikatów klienta, o ile uwierzytelnianie przebiegnie pomyślnie. Po wyłączeniu tej opcji telefon nie będzie weryfikował certyfikatu serwera bez względu na to, czy certyfikat jest ważny, czy nie.

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.

Aby skonfigurować wykrywanie ruchu, przejdź do interfejsu internetowego **Surveillance > Motion.**



- **Wykrywanie podejrzanych ruchomych obiektów**: Dostępne są cztery opcje: Wyłączone, Wykrywanie wideo, Wykrywanie radaru i Wideo + Radar. **Wykrywanie wideo** koncentruje się na analizie informacji wizualnych przechwyconych przez kamery. **Wykrywanie radarowe** oferuje większy zasięg i lepsze wykrywanie w warunkach słabej widoczności.

- **Zasięg wykrywania**: Po włączeniu wykrywania radaru można wybrać zasięg wykrywania spośród 1, 2 i 3 metrów.

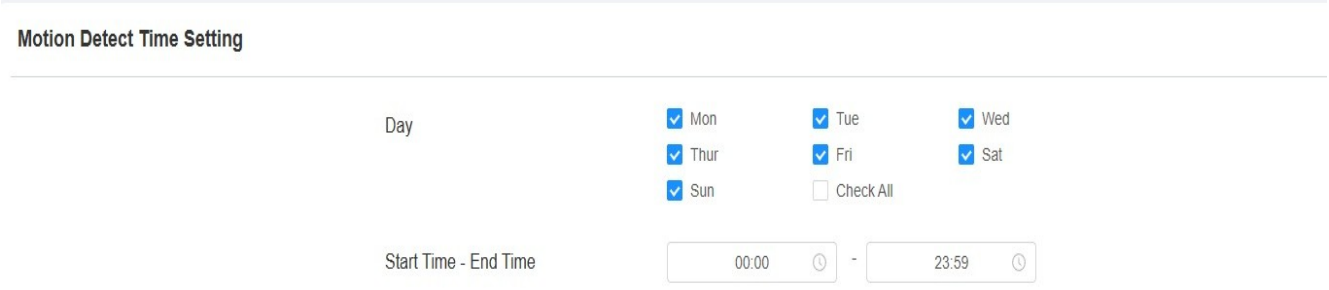
- **Interwał czasowy**: Bezwzględny interwał wyzwalania wynosi 3 sekundy. W przypadku wybrania liczby większej niż 3 sekundy do wyzwolenia alarmu wymagany jest drugi interwał wyzwalania. Na przykład, jeśli wybierzesz 3 sekundy, alarm zostanie wyzwolony, gdy poruszający się obiekt zostanie wykryty jeden raz od 0 do 3 sekund (wyzwolony w dowolnym momencie od 0 do 3 sekund). Jeśli jednak na przykład wybrana zostanie opcja 5 sekund (więcej niż 3), alarm nie zostanie wyzwolony, dopóki poruszający się obiekt nie zostanie wykryty po raz drugi w przedziale od 3 do 5 sekund (wyzwolony w dowolnym momencie w przedziale od 3 do 5 sekund). Domyślny interwał wynosi 10 sekund.
- **Zasięg wykrywania**: Ta opcja pojawia się po wybraniu wykrywania radaru. Wynosi on od 1 do 3 metrów.
- **Dokładność wykrywania**: Dokładność wykrywania dla czułości wykrywania. Im wyższa wartość, tym większa czułość. Domyślna wartość dokładności wykrywania to 3.
- **Obszar** detekcji: Kliknij i przytrzymaj przycisk myszy, aby wybrać maksymalnie trzy obszary detekcji.
- **Akcja do wykonania**: Typ powiadomienia obejmuje FTP, e-mail, połączenie SIP i HTTP.
    - FTP: powiadomienie zostanie wysłane na wskazany serwer.

E-mail: wiadomość e-mail zostanie wysłana na wstępnie skonfigurowany adres e-mail.

- SIP Call: połączenie zostanie wykonane na wstępnie skonfigurowany numer.
- HTTP: powiadomienie zostanie wysłane na wskazany serwer.

- **Wykonaj przekaźnik**: Przekaźnik, który ma zostać wyzwolony.

Przewiń w dół, aby ustawić harmonogram wykrywania ruchu.

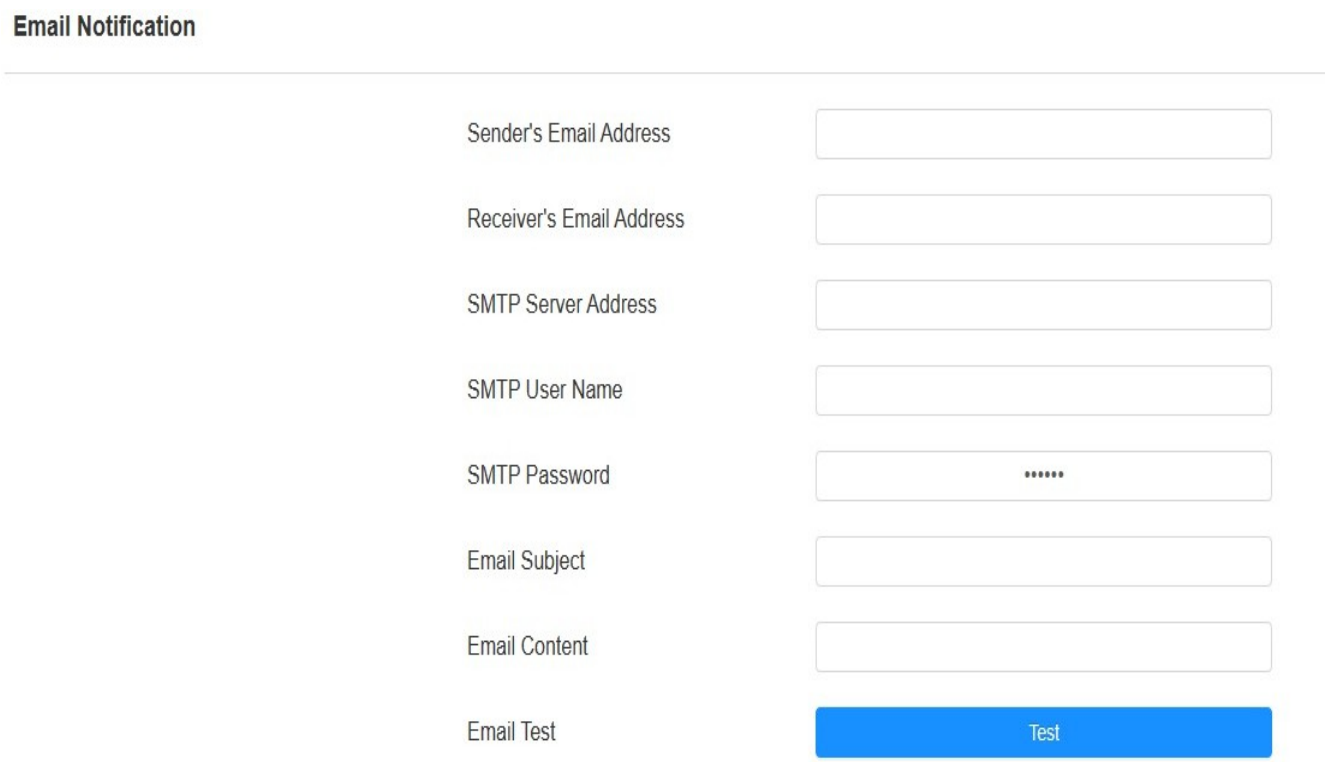


Ustawienia powiadomień bezpieczeństwa

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.

Ustawienia powiadomień e-mail

Skonfiguruj powiadomienia e-mail, aby otrzymywać zrzuty ekranu nietypowego ruchu z bramofonu. Przejdź do interfejsu web **Setting > Action.**

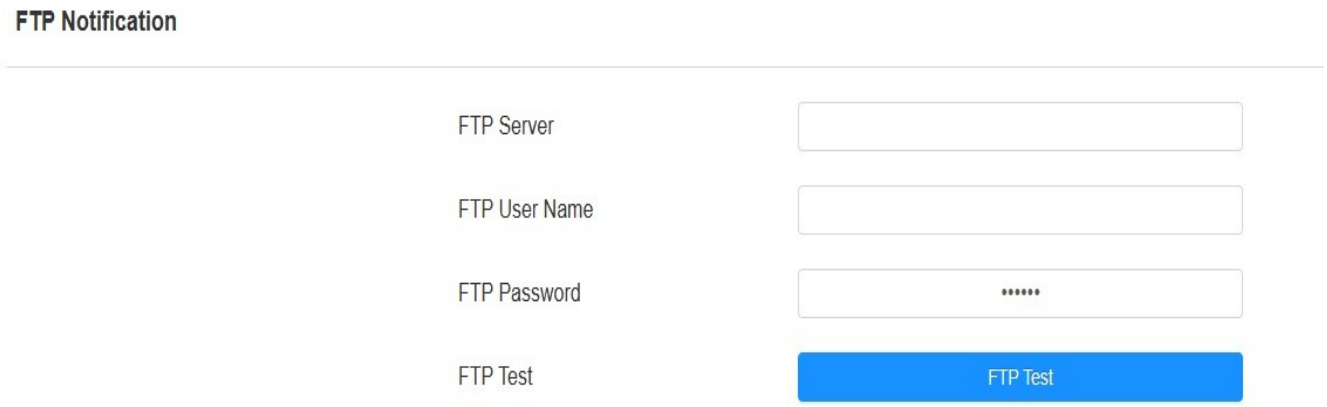


- **Nazwa użytkownika SMTP**: Nazwa użytkownika SMTP jest zwykle taka sama jak adres e-mail nadawcy.
- **Hasło SMTP** : Hasło serwera SMTP, które jest takie samo jak adres e-mail nadawcy.

Ustawienia powiadomień FTP

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

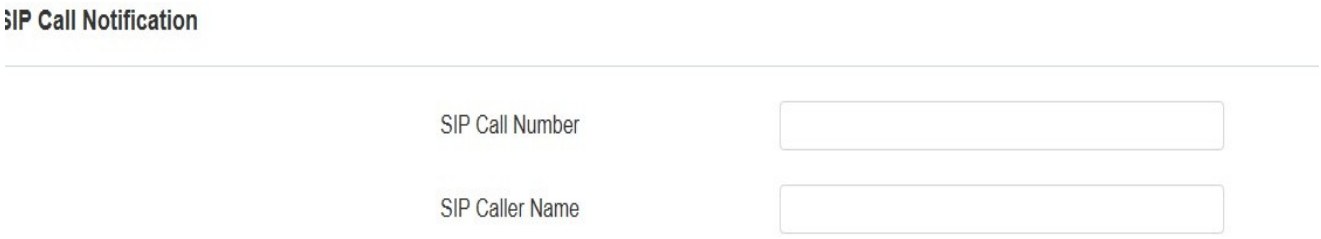
Przejdź do interfejsu web **Setting > Action.**



- **Ścieżka FTP**: Nazwa folderu utworzonego na serwerze FTP.

Powiadomienie o połączeniu SIP

Możesz wprowadzić numer SIP, aby otrzymywać powiadomienia.



Adres URL akcji

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

Akuvox Action URL:

Nie	Wydarzenie	Format parametrów	Przykład
1	Wykonaj połączenie	$remote	Http://server ip/ Callnumber=$remote
2	Rozłącz się	$remote	Http://server ip/ Callnumber=$remote
3	Przekaźnik wyzwolony	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Przekaźnik zamknięty	$relay1status	Http://server ip/ relayclose=$relay1status
5	Wejście wyzwalane	$input1status	Http://server ip/ inputtrigger=$input1status
6	Wejście zamknięte	$input1status	Http://server ip/ inputclose=$input1status
7	Wprowadzony prawidłowy kod	$code	Http://server ip/ validcode=$code
8	Wprowadzono nieprawidłowy kod	$code	Http://server ip/ invalidcode=$code
9	Wprowadzona ważna karta	$card_sn	Http://server ip/ validcard=$card_sn
10	Wprowadzono nieprawidłową kartę	$card_sn	Http://server ip/ invalidcard=$card_sn
11	Wyzwolenie alarmu sabotażowego	status alarmu	Http://server ip/tampertrigger=$alarm status

Na przykład: http://192.168.16.118/help.xml?
mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

Przejdź do interfejsu **Ustawienia** sieciowe **> Action URL.**

Action URL

Enabled	☐
Make Call	
Hang Up	
RelayA Triggered	
RelayB Triggered	
RelayA Closed	
RelayB Closed	
InputA Triggered	
InputB Triggered	
InputC Triggered	
InputD Triggered	
InputA Closed	
InputB Closed	
InputC Closed	
InputD Closed	
Valid Code Entered	
Invalid Code Entered	
Valid Card Entered	
Invalid Card Entered	

Interfejs sieciowy Automatyczne wylogowanie

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

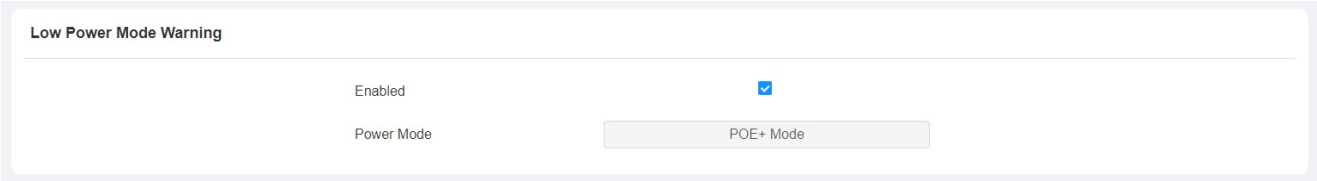
Przejdź do interfejsu internetowego **System > Security.**

- **Session Time Out Value**: Czas automatycznego wylogowania interfejsu sieciowego wynosi od 60 sekund do 14400 sekund. Wartością domyślną jest 300.

Tryb niskiego zużycia energii

Wyświetla tryb zasilania urządzenia. Gdy urządzenie jest zasilane przez POE, wyświetla POE+Mode. Gdy urządzenie jest zasilane napięciem 12 V, wyświetlany jest tryb niskiego poboru mocy.

Aby wyświetlić tryb zasilania w interfejsie **System > Security > Low Power Mode Warning.**

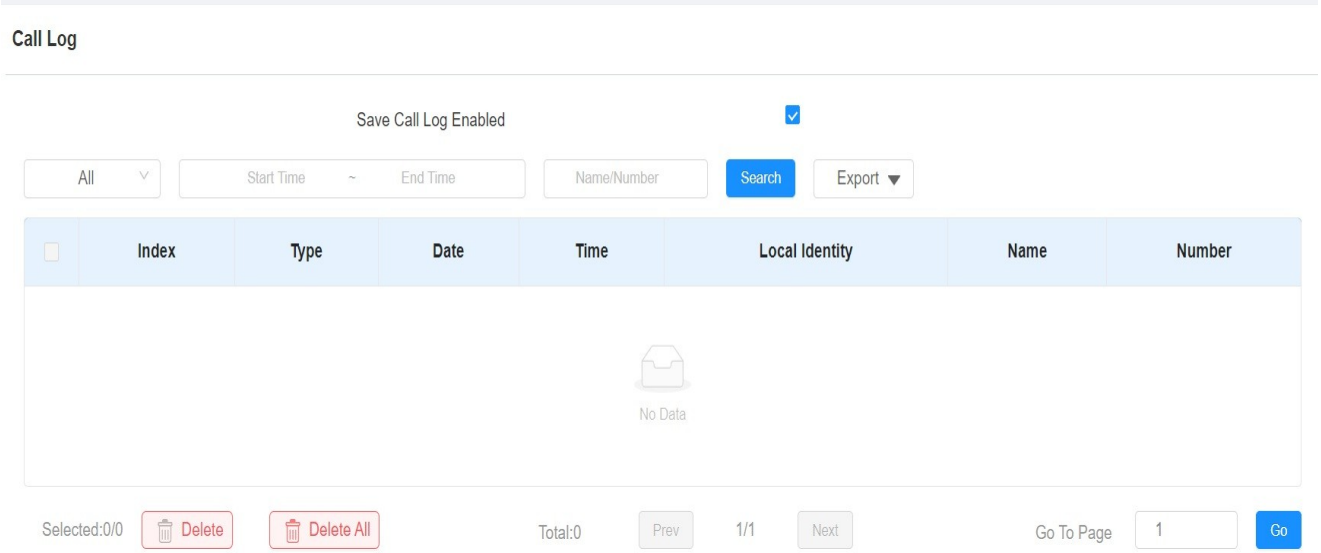


Dzienniki

Dzienniki połączeń

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

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



- **Wszystkie**: Dostępne są cztery typy historii połączeń: Wszystkie, Wybrane, Odebrane i Nieodebrane.

- **Czas rozpoczęcia i czas zakończenia**: Określony czas dzienników połączeń, które chcesz wyszukać, sprawdzić lub wyeksportować.

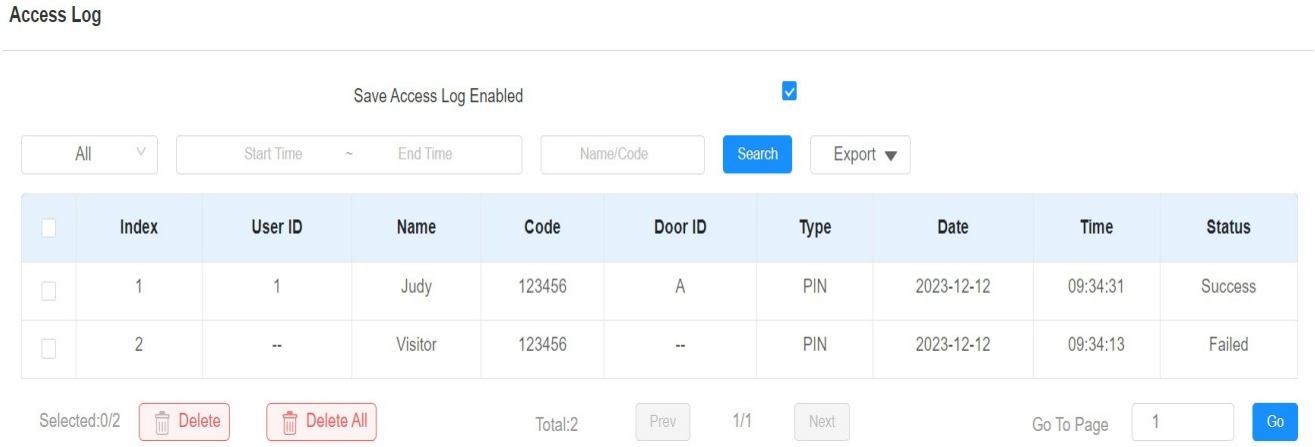
Nazwa/Numer: Przeszukiwanie rejestru połączeń według nazwy lub numeru SIP lub IP.

- **Eksport**: Dzienniki połączeń można eksportować w formacie .csv.

Dzienniki drzwi

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

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



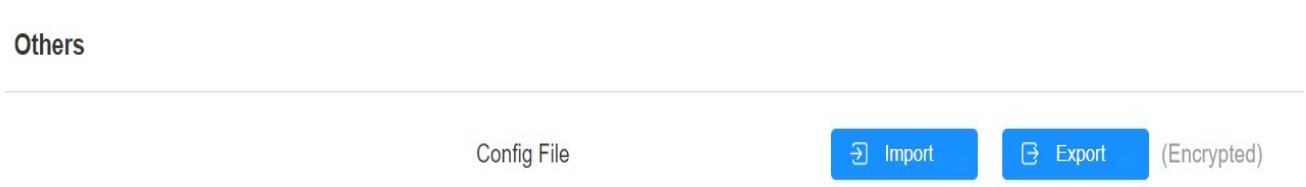
- **Wszystkie**: dostępne są trzy rodzaje dzienników dostępu: Wszystkie, Udane i Nieudane.
- **Czas rozpoczęcia i czas zakończenia**: Określony czas dzienników połączeń, które chcesz wyszukać, sprawdzić lub wyeksportować.
- **Nazwa/Kod** : Wyszukiwanie dziennika drzwi według nazwy lub kodu PIN.
- **Eksport**: Logi drzwi mogą być eksportowane w formacie .csv lub .xml.

Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować

do komputera lokalnego. Przejdź do interfejsu web **System >**

Maintenance.

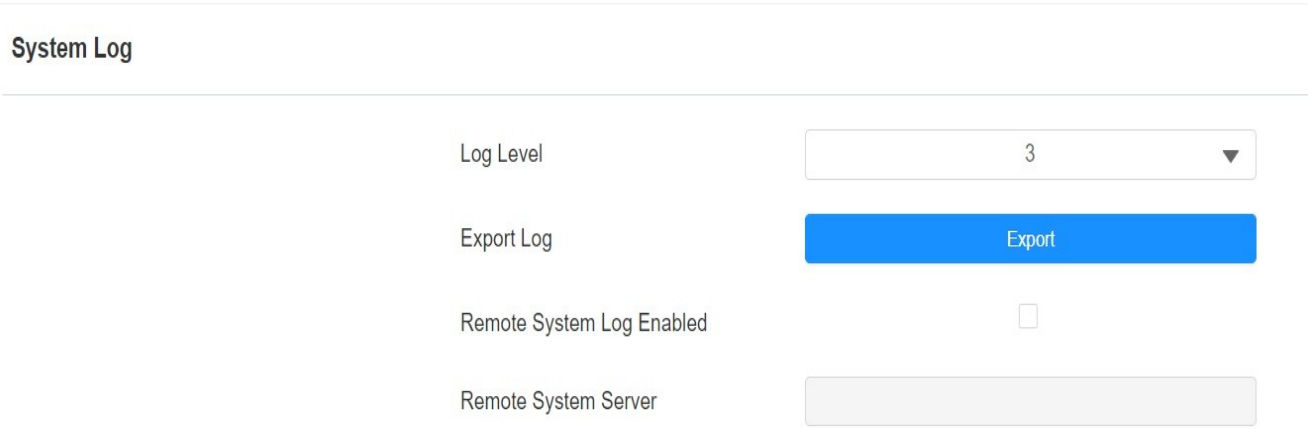


Debugowanie

Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

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



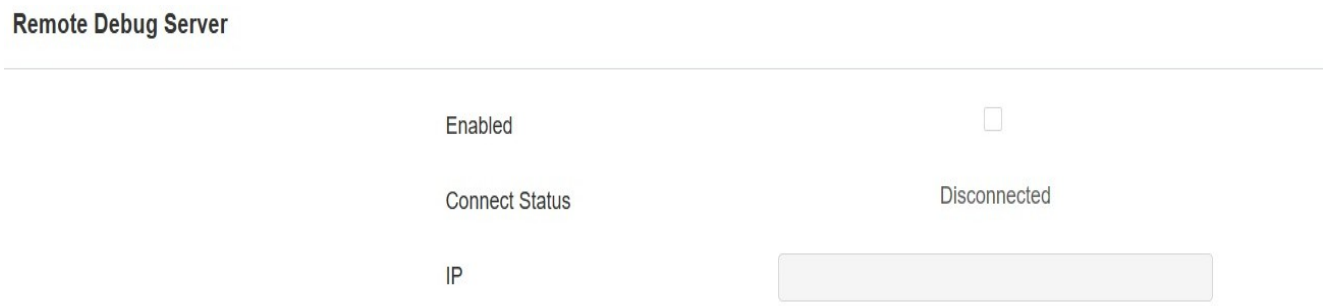
- **Poziom dziennika**: Poziom dziennika wynosi od 1 do 7 poziomów. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić do celów debugowania. Domyślny poziom dziennika to 3. Im wyższy poziom, tym bardziej kompletny jest dziennik.
- **Eksportuj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

Zdalny serwer debugowania

Gdy urządzenie ma problem, można użyć zdalnego serwera debugowania, aby uzyskać

zdalny dostęp do dziennika urządzenia w celu debugowania.

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

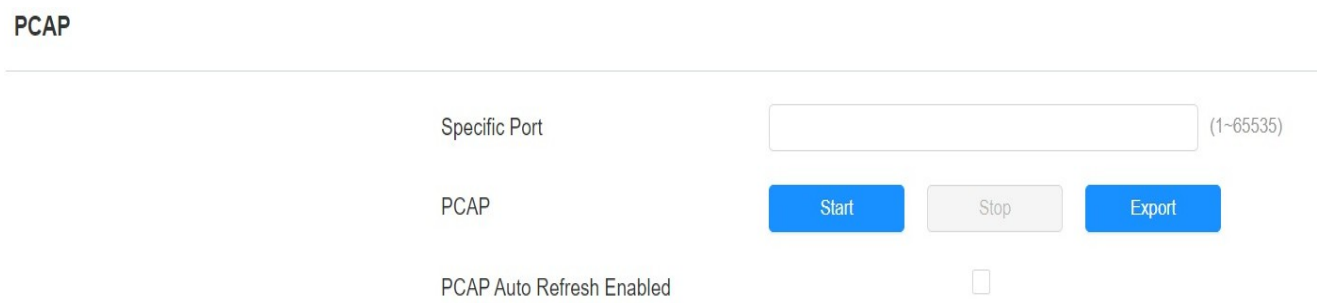


- **IP**: adres IP zdalnego serwera debugowania.

PCAP do debugowania

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

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

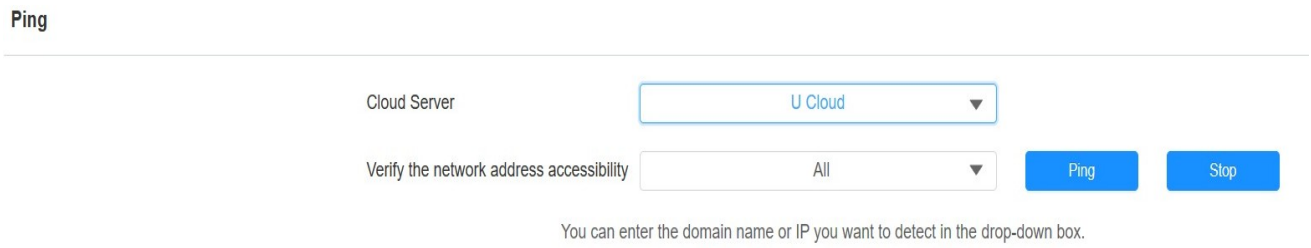


- **Określony port**: Wybierz określone porty z zakresu 1-65535, aby można było przechwytywać tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.
- **PCAP**: Kliknij kartę Start i Stop, aby przechwycić określony zakres pakietów danych przed kliknięciem karty Eksport, aby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

Ping

Urządzenie umożliwia sprawdzenie dostępności serwera docelowego.

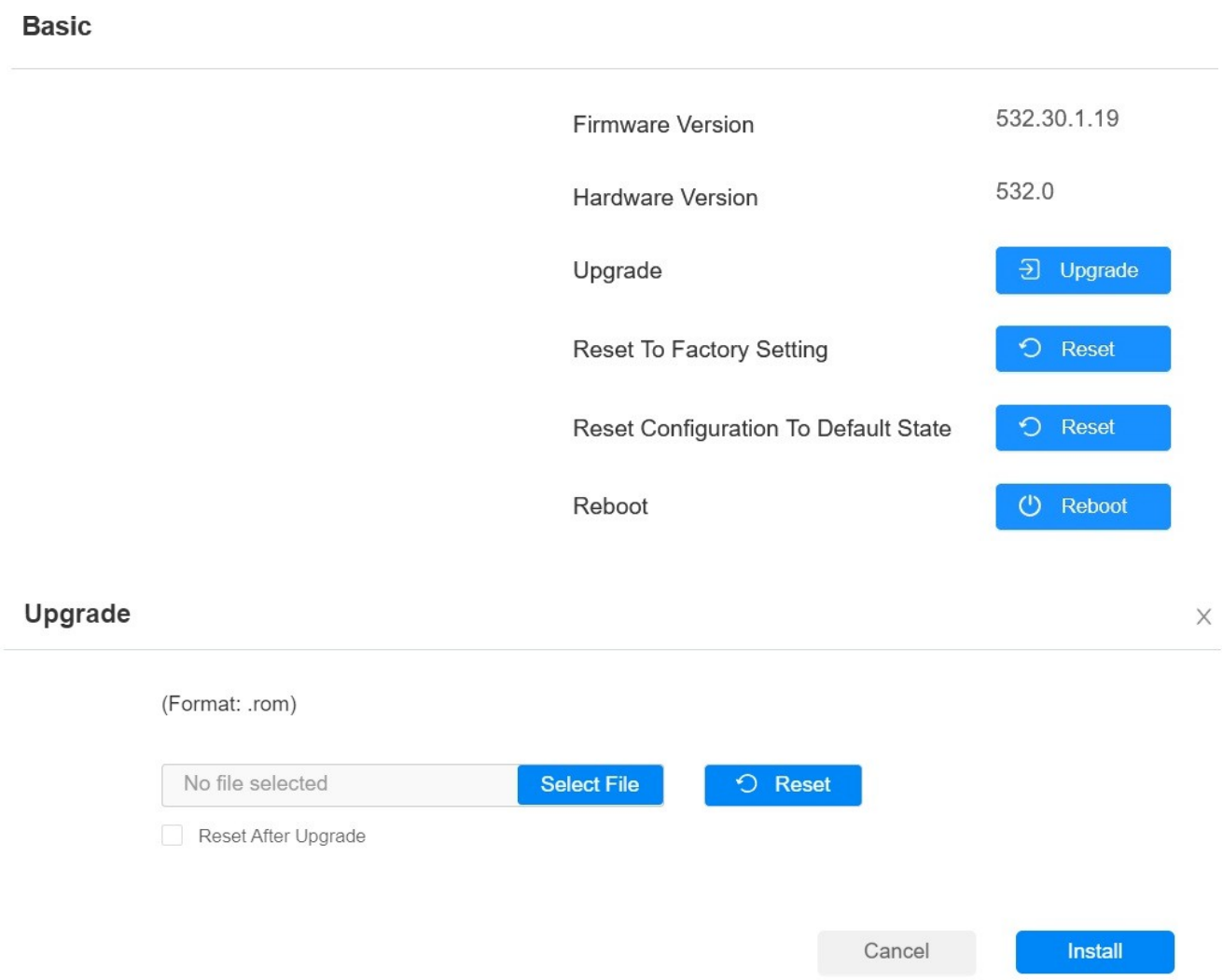
Przejdź do interfejsu internetowego **System > Konserwacja > Ping.**



- **Cloud Server**: Serwer, który ma zostać zweryfikowany.
- **Sprawdź dostępność adresu sieciowego**: Typ usługi.

Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można zaktualizować w interfejsie internetowym urządzenia. Przejdź do interfejsu internetowego **System > Upgrade.**



Uwaga

Pliki oprogramowania sprzętowego powinny być w formacie .rom.

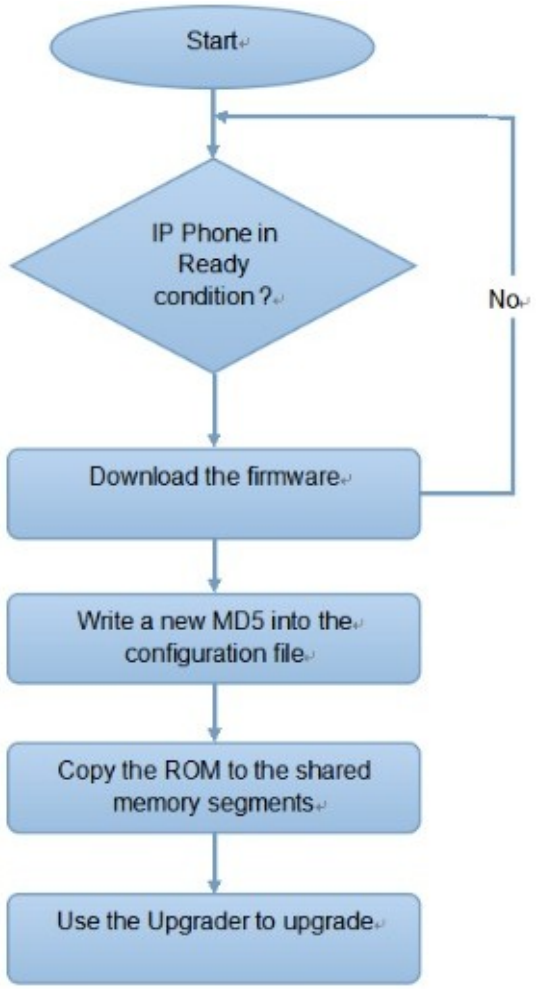
Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

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

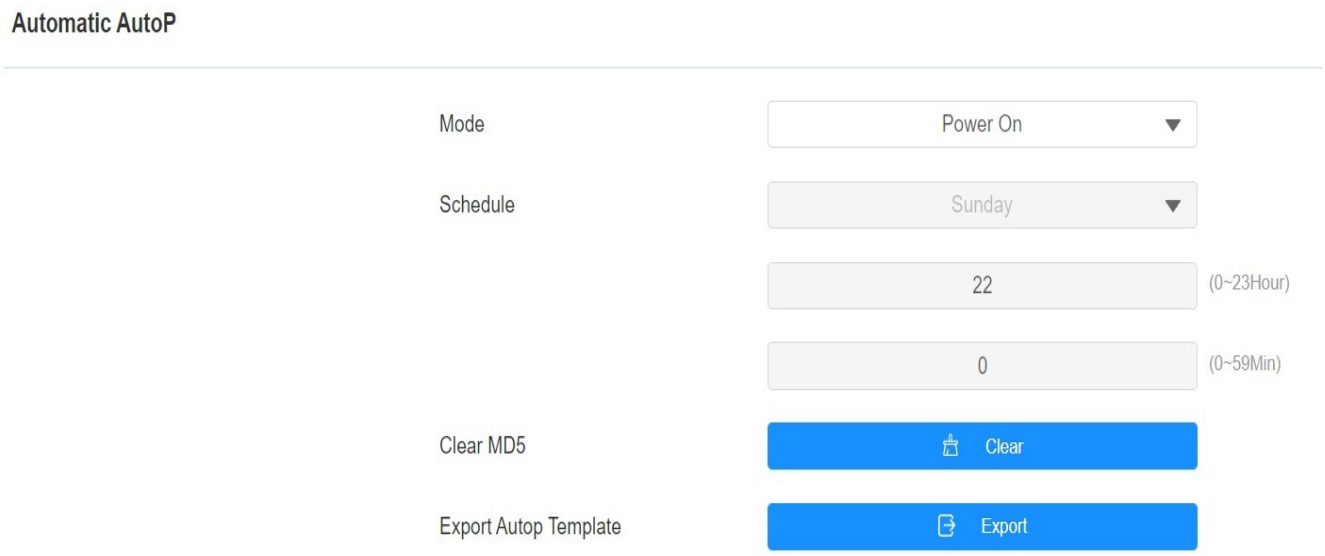
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny udostępniania wsadowego różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC dla określonego udostępniania urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer ma te dwa typy plików konfiguracyjnych,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

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

Harmonogram AutoP

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

Aby ją skonfigurować, przejdź do interfejsu internetowego **System > Auto Provisioning > Automatic AutoP.**



- **Tryb** :
    - **Power On**: Zezwól urządzeniu na automatyczne uruchamianie po każdym uruchomieniu.
    - **Wielokrotnie**: Zezwól urządzeniu na wykonywanie Autop zgodnie z harmonogramem.
    - **Power On + Repeatedly**: Łączy tryby **Power On** i **Repeatedly**, umożliwiając urządzeniu wykonywanie funkcji Autop przy każdym uruchomieniu lub zgodnie z harmonogramem.

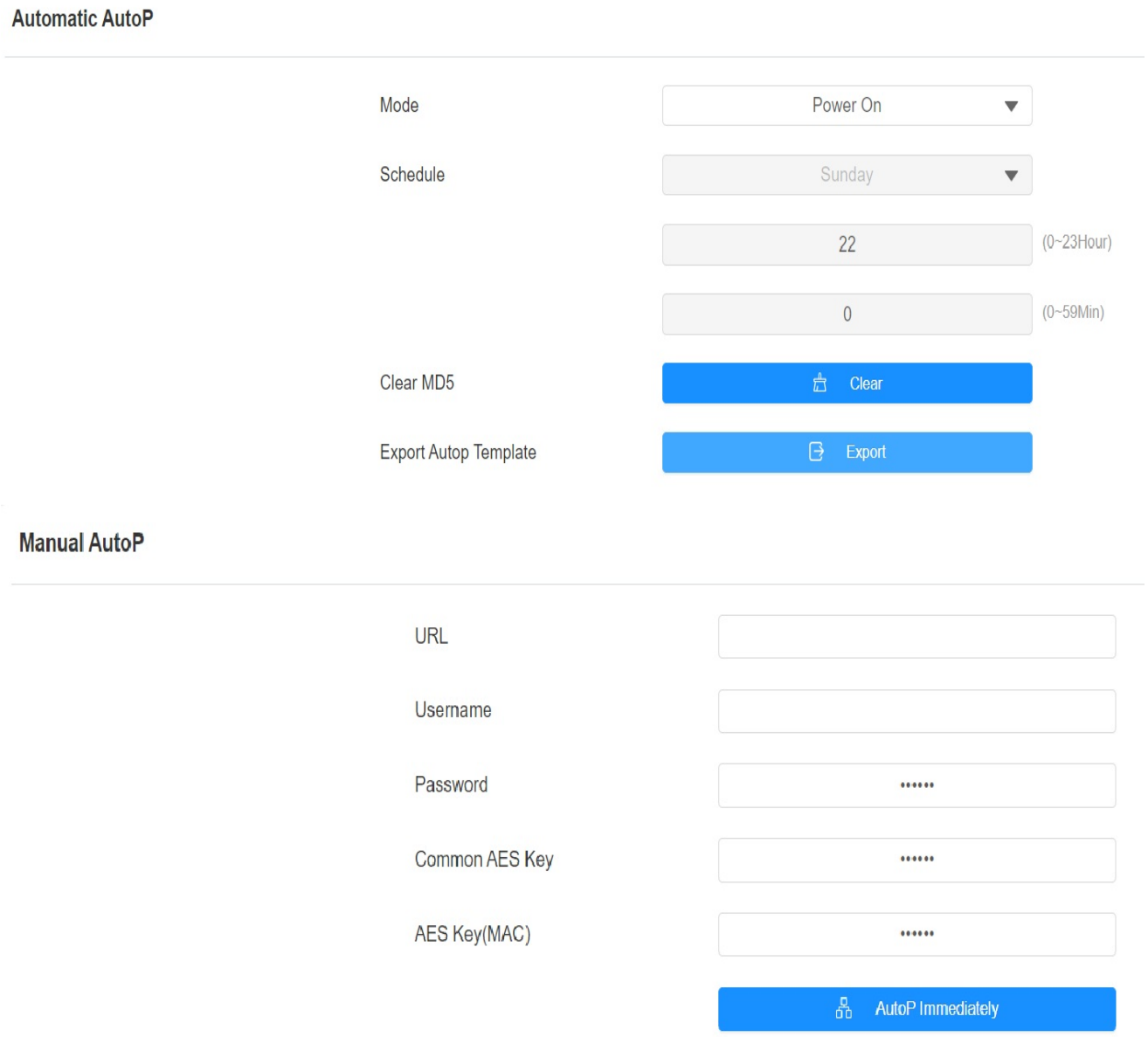
Hourly Repeat (Powtarzanie co godzinę): Umożliwia urządzeniu wykonywanie automatycznego zatrzymania co godzinę.

- **Harmonogram**: Po wybraniu trybu **Power On** + **Repeatedly** można wybrać konkretny dzień i godzinę automatycznego włączenia.
- **Clear MD 5**: Służy do porównywania istniejącego pliku autop z plikiem autop na serwerze, jeśli pliki są takie same, provisioning zostanie zatrzymany, co pozwoli uniknąć niepotrzebnego automatycznego provisioningu.

Konfiguracja udostępniania statycznego

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

Pobierz szablon Autop w interfejsie **System > Auto Provisioning > Automatic Autop** i skonfiguruj serwer Autop w interfejsie **System > Auto Provisioning > Manual Autop**.



- **Adres URL**: adres serwera TFTP, HTTP, HTTPS lub FTP dla provisioningu.
- **Nazwa użytkownika**: Ustaw nazwę użytkownika, jeśli serwer wymaga nazwy użytkownika, aby uzyskać do niego dostęp.
- **Hasło**: Ustaw hasło, jeśli dostęp do serwera wymaga podania hasła.
- **Wspólny klucz AES**: Konfiguracja kodu AES dla interkomu w celu odszyfrowania ogólnego pliku konfiguracyjnego Auto Provisioning.
- **AES Key(MAC)**: Ustawienie kodu AES dla interkomu w celu odszyfrowania pliku konfiguracyjnego automatycznego udostępniania opartego na MAC.

Uwaga

• AES jako jeden z rodzajów 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/ (pozwala na logowanie anonimowe) ftp://username:password@192.168.0.19/ (wymaga podania nazwy użytkownika i hasła)
- HTTP: http://192.168.0.19/ (używa domyślnego portu 80) http://192.168.0.19:8080/ (używa innych portów, np. 8080)
- HTTPS: https://192.168.0.19/ (używa domyślnego portu 443)

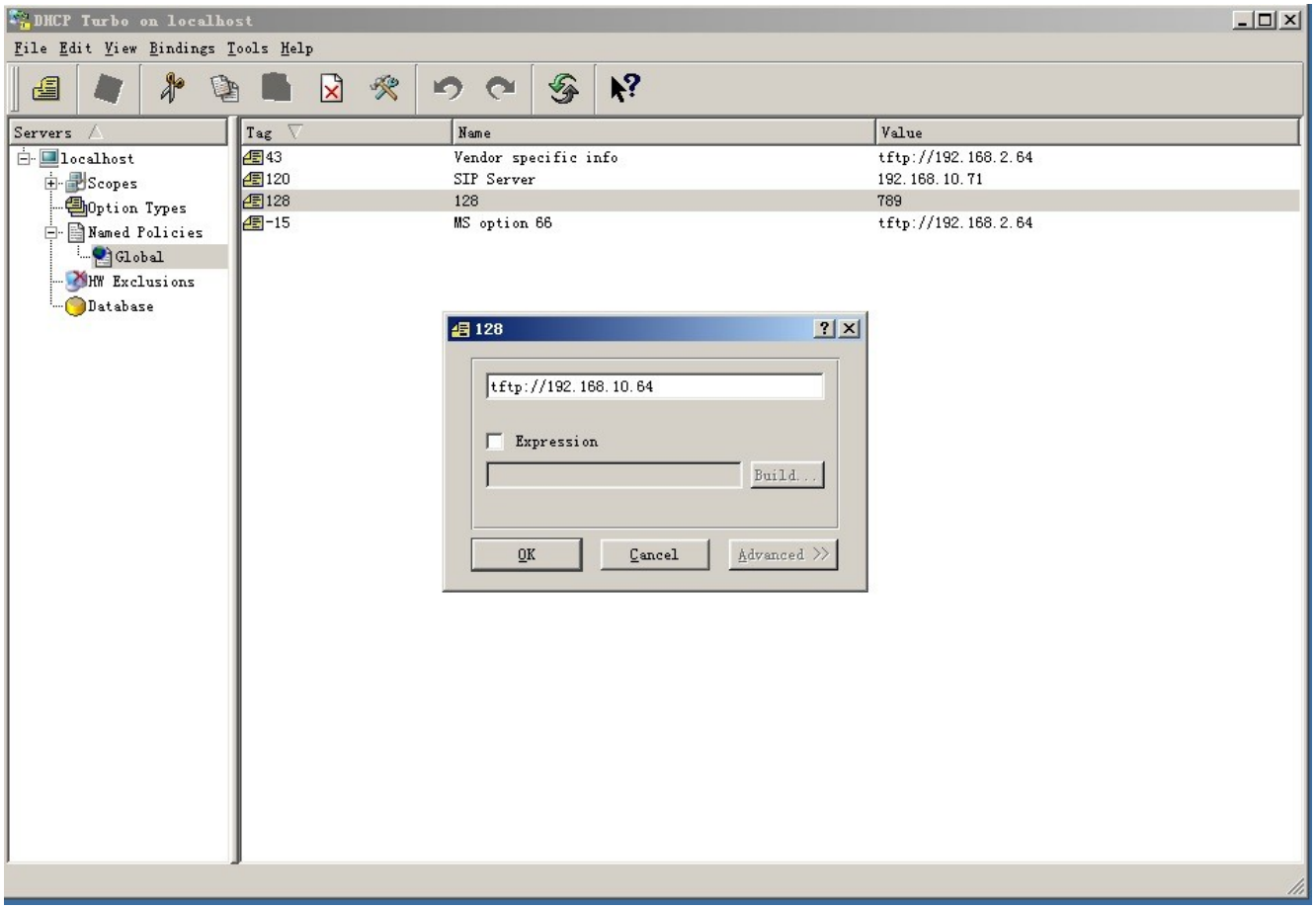
Wskazówka

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

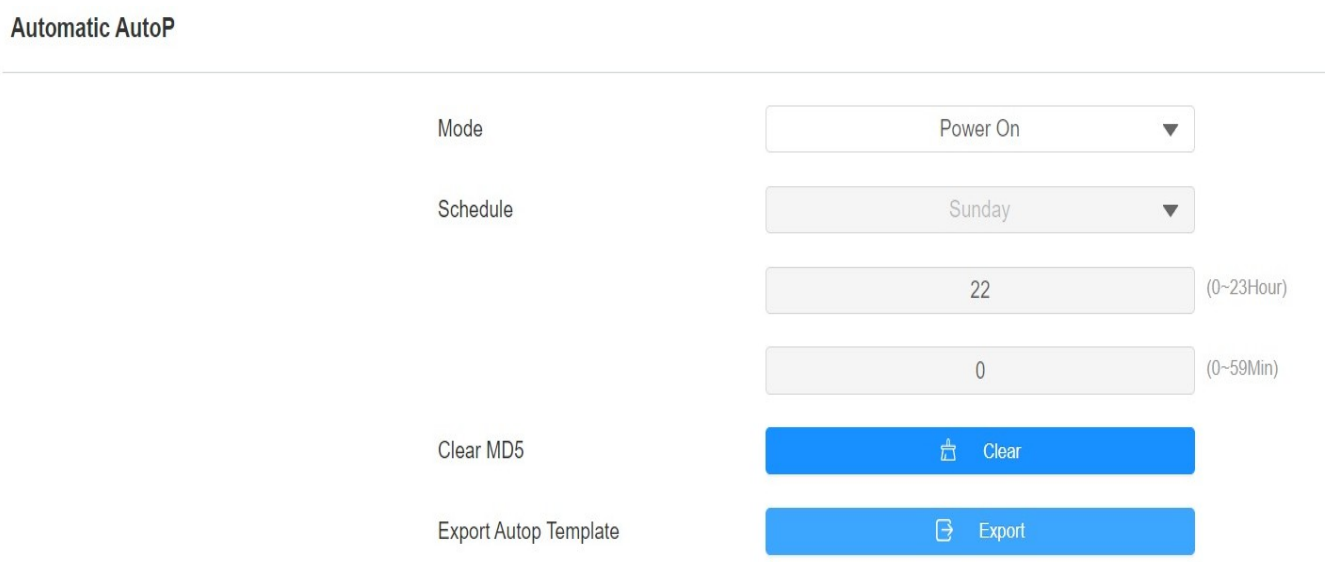
Opcja niestandardowa zdefiniowana przez użytkowników z kodami opcji w zakresie 128-255), należy skonfigurować opcję niestandardową DHCP w interfejsie internetowym.



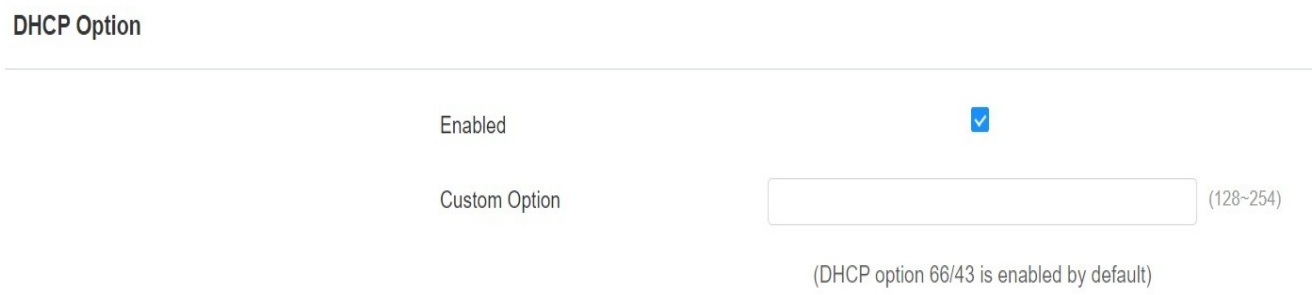
Uwaga

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

Aby skonfigurować DHCP Autop z trybem Power On i wyeksportować Autop Template w celu edycji konfiguracji na tym samym interfejsie, przejdź do interfejsu internetowego **System > Auto Provisioning.**



Następnie skonfiguruj opcję DHCP.



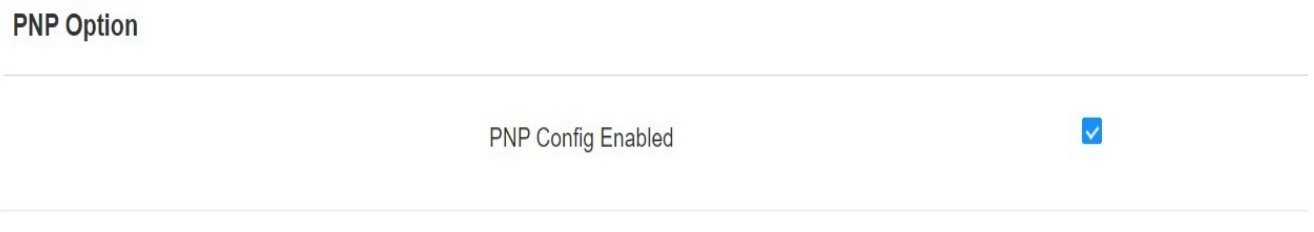
- **Opcja niestandardowa**: Wprowadź kod DHCP pasujący do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych do konfiguracji lub aktualizacji.
- **Opcja 66 DHCP**: Jeśli żadna z powyższych opcji nie jest ustawiona, urządzenie automatycznie użyje Opcji 66 DHCP, aby uzyskać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

> **Uwaga**
>
> Ogólny plik konfiguracyjny dla udostępniania wsadowego ma format cfg, biorąc R29 jako przykład, r000000000029.cfg (łącznie 10 zer), podczas gdy plik konfiguracyjny oparty na MAC dla udostępniania konkretnego urządzenia ma format MAC_Address urządzenia. cfg, na przykład 0C110504AE5B.cfg.

Konfiguracja PNP

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

Aby skonfigurować PNP, przejdź do interfejsu internetowego **System > Auto Provisioning > PNP Option.**

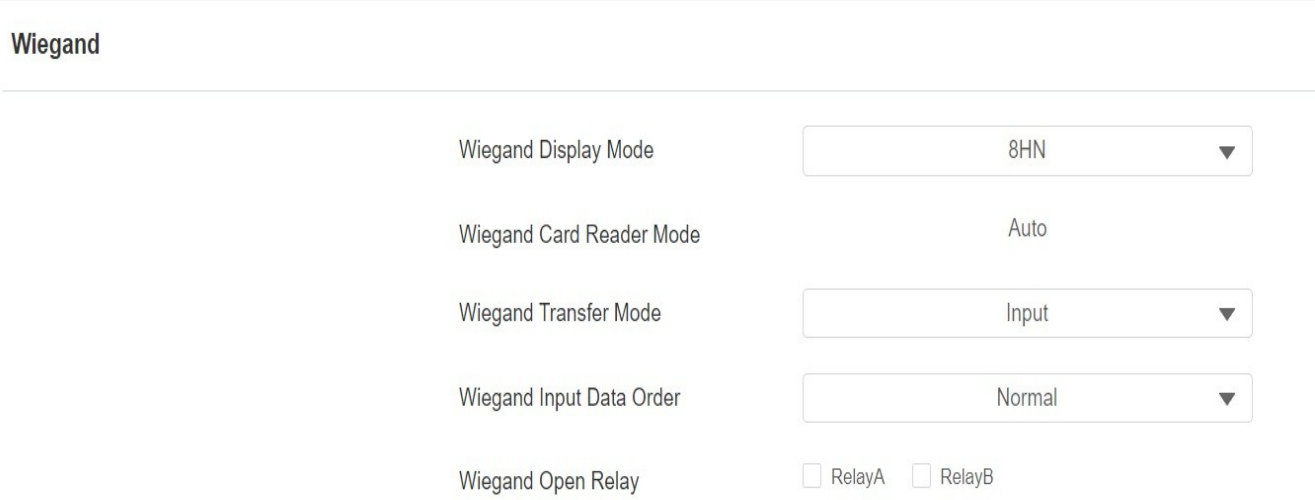


Integracja z urządzeniami innych firm

Integracja przez Wiegand

Urządzenie można zintegrować z Wiegand.

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

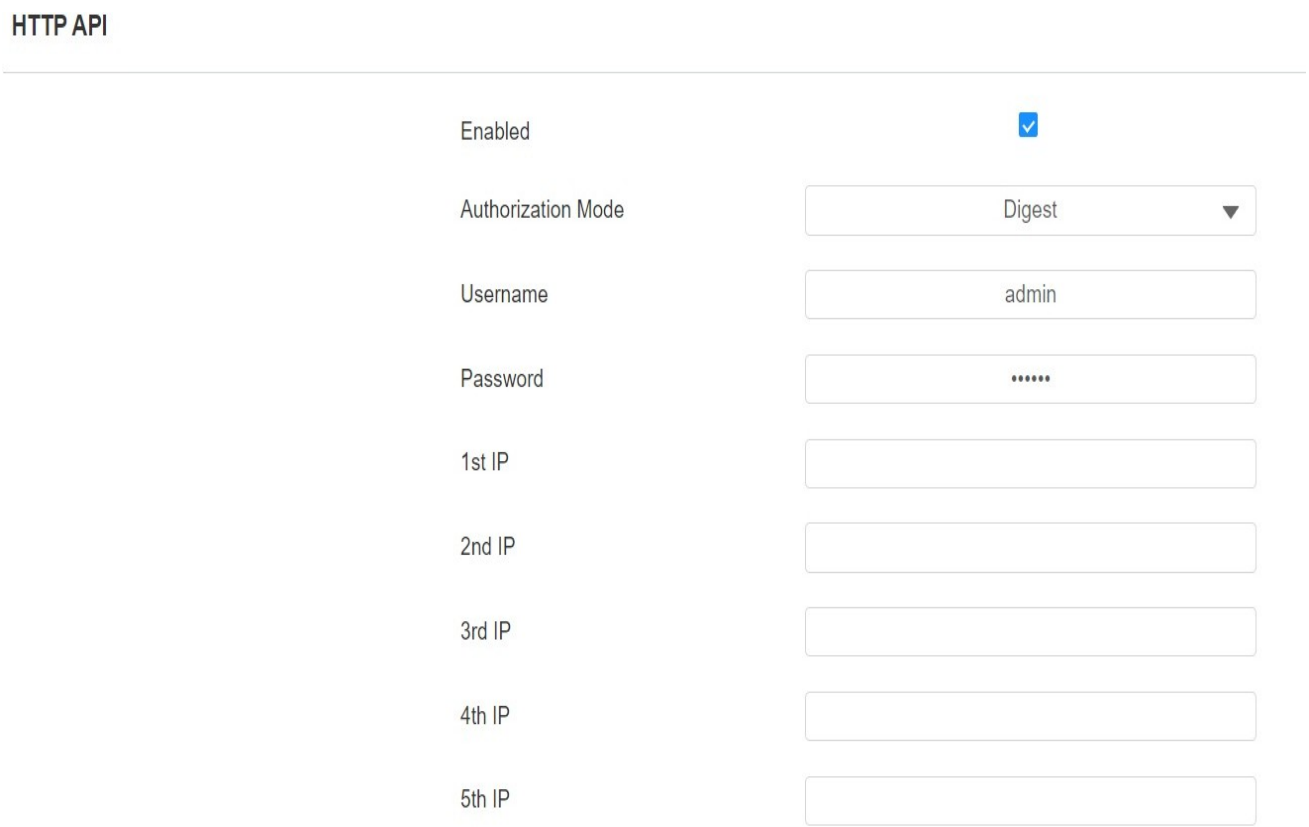


- **Tryb wyświetlania Wiegand** : Wybór formatu kodu karty Wiegand spośród 8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR; 6H3D5D-R(W26); 8HR10D; RAW.
- **Tryb czytnika kart Wiegand**: Format transmisji powinien być identyczny między bramofonem a urządzeniem, które ma zostać zintegrowane. Jest on konfigurowany automatycznie.
- **Tryb transferu Wiegand**: Dostępne są trzy opcje: Wejście, Wyjście i Konwertuj na kartę nr wyjścia Wiegand. Jeśli bramofon jest używany jako odbiornik, ustaw go jako **Wejście**. Wybierz **Output (Wyjście),** jeśli bramofon ma być nadawcą. Wybierz **Convert to Card No.Output Wiegand,** jeśli chcesz, aby dane wyjściowe Wiegand zostały przekonwertowane na numer karty przed wysłaniem ich z bramofonu do odbiornika.
- **Kolejność danych wejściowych Wiegand**: Ustawienie kolejności danych wejściowych Wiegand pomiędzy **Normal** i **Reversed**. W przypadku wybrania opcji Reversed numer karty wejściowej zostanie odwrócony i odwrotnie.
- **Wiegand Open Relay**: Przekaźnik, który ma zostać wyzwolony.

Integracja przez HTTP API

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

Aby skonfigurować HTTP API, przejdź do interfejsu Web **Setting > HTTP API.**



- **Enabled** : Włącz lub wyłącz funkcję HPTT API dla integracji z innymi firmami. Jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.
- **Tryb autoryzacji** : Wybierz jedną z następujących opcji: None, Normal, Allowlist, Basic, Digest i Token dla typu autoryzacji, które zostaną szczegółowo wyjaśnione w poniższej tabeli.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic** lub **Digest.** Domyślna nazwa użytkownika to admin.
- **Hasło** : Wprowadź hasło, gdy wybrany jest tryb autoryzacji **Basic** lub **Digest.** Domyślne hasło to admin.
- **1st IP-5th IP** : wprowadź adres IP urządzeń innych firm, gdy dla integracji wybrano autoryzację **Allowlist.**

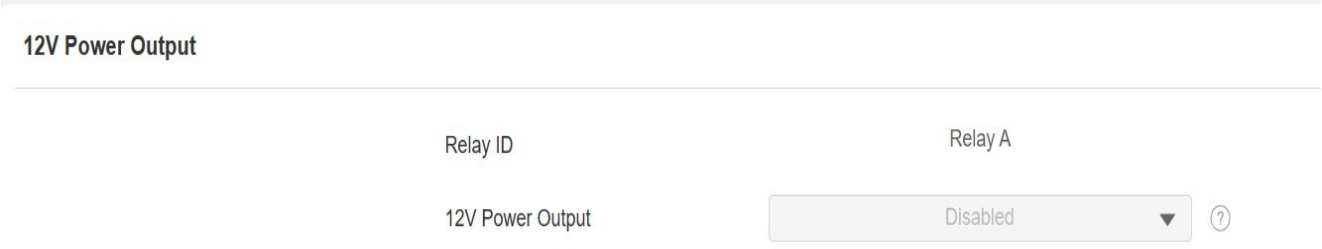
Poniższy opis dotyczy trybu uwierzytelniania:

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

Kontrola mocy wyjściowej

Urządzenie może służyć jako źródło zasilania dla zewnętrznych przekaźników.

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

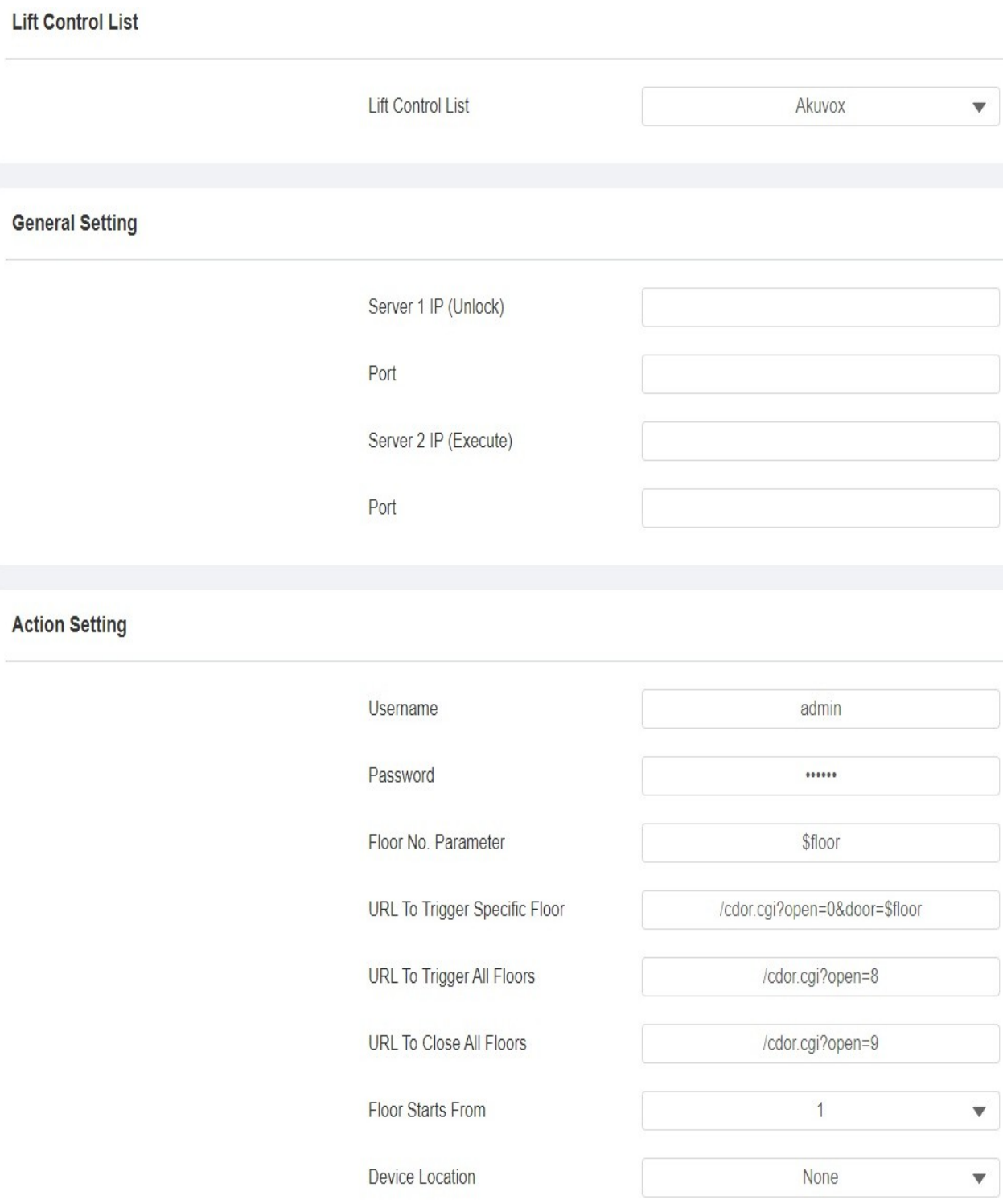


- **Wyjście zasilania 12V**: gdy wybrana jest opcja **Zawsze**, urządzenie może dostarczać ciągłe zasilanie do urządzenia innego producenta. Gdy wybrana jest opcja **Triggered By Open Relay**, urządzenie może dostarczać zasilanie do urządzenia innej firmy za pośrednictwem wyjścia 12 i interfejsu GND podczas limitu czasu, gdy stan przekaźników zostanie zmieniony z niskiego na wysoki. Po wybraniu opcji **Security Relay A urządzenie** może współpracować z przekaźnikiem bezpieczeństwa.

Kontrola podnoszenia

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

Aby ją skonfigurować, przejdź do interfejsu internetowego **Device > Lift Control.**



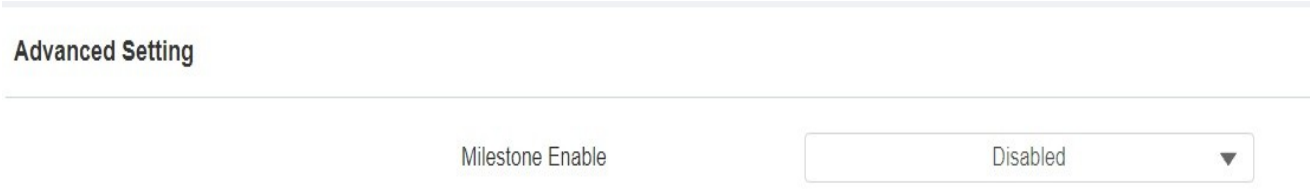
- **Lista sterowania windą**: Wybierz None, aby wyłączyć funkcję, i wybierz Akuvox, aby zintegrować bramofon z kontrolerem Akuvox.
- **Server 1 IP(Unlock)**: Adres IP serwera sterowania windą Akuvox. Obsługuje do 10 adresów serwerów oddzielonych znakiem ";".
- **Server 2 IP(Execute)**: Adres IP serwera, który uruchamia kontrolę podnoszenia.
- **Port**: port serwera kontrolera windy.

- **Nazwa użytkownika**: Nazwa użytkownika kontrolera windy do uwierzytelniania.
- **Hasło** : Hasło kontrolera windy do uwierzytelniania.
- **Floor NO. Parametr**: Wprowadź parametr numeru piętra dostarczony przez Akuvox. Domyślny ciąg parametru to "$floor". W razie potrzeby można zdefiniować własny ciąg parametrów.
- **URL To Trigger Specific Floor**: Wprowadź adres URL sterowania windą Akuvox w celu wyzwolenia określonego piętra. Adres URL to /cdor.cgi?open=0&door= $ floor, ale ciąg "$floor" na końcu musi być identyczny z ciągiem parametrów zdefiniowanym przez użytkownika.
- **URL do wyzwalania wszystkich pięter** : Wprowadź adres URL Akuvox, aby wyzwolić wszystkie piętra.
- **URL do zamknięcia wszystkich pięter** : Wprowadź adres URL Akuvox używany do zamykania wszystkich pięter, co oznacza, że wszystkie przyciski uruchamiane dla odpowiednich pięter staną się nieważne.
- **Floor Starts From**: Ustaw piętro, od którego rozpoczyna się zliczanie pięter. Na przykład, jeśli wybierzesz -3, 3 piętro w piwnicy zostanie uznane za pierwsze piętro dopasowane do przekaźnika#1 (pierwsze piętro).

Integracja z Milestone

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

Aby włączyć tę funkcję w interfejsie internetowym **Surveillance > ONVIF > Advanced Setting.**

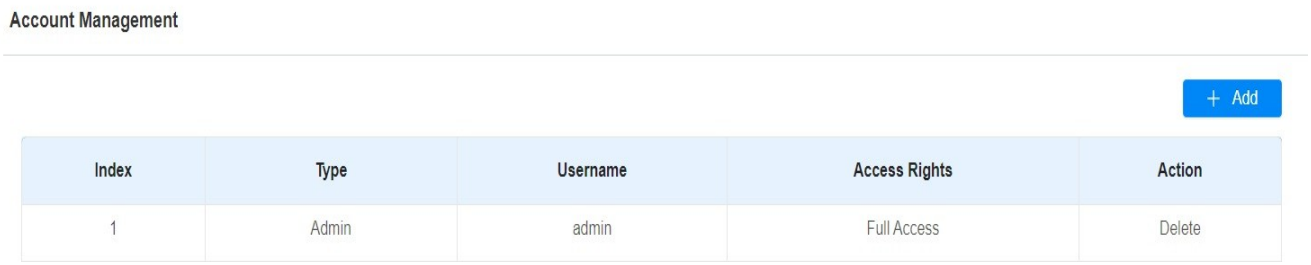


Modyfikacja hasła

Zarządzanie kontami

Można dodać konta administratora i użytkownika oraz skonfigurować ich hasła do logowania się do interfejsu internetowego urządzenia.

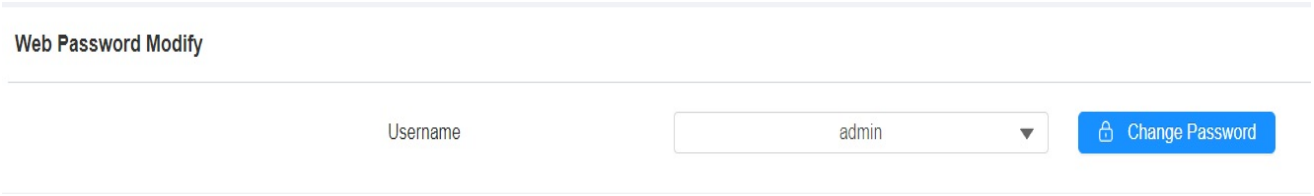
Przejdź do interfejsu internetowego **System > Security > Account Management.** Kliknij +Add, aby utworzyć konto.

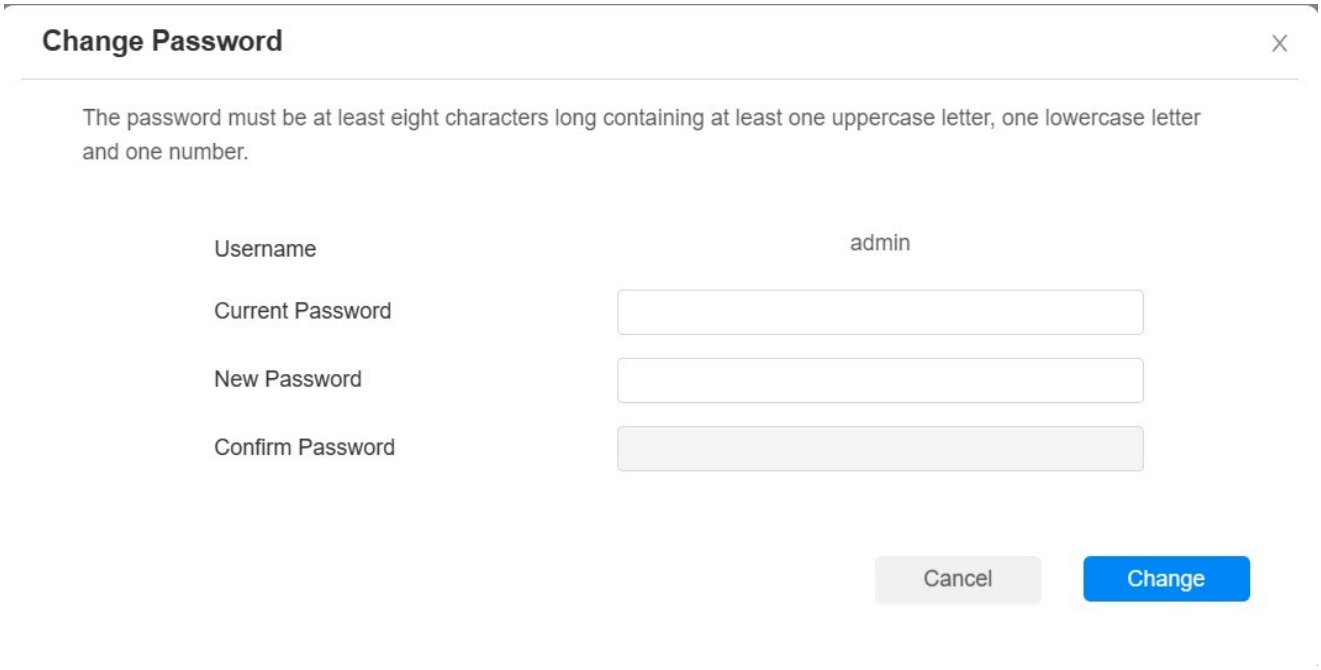


Modyfikacja hasła interfejsu sieciowego urządzenia

Przejdź do interfejsu internetowego **System > Security > Web Password Modify.**

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





Modyfikacja hasła systemowego

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

Naciśnij *2396# na klawiaturze urządzenia i naciśnij 2, aby przejść do ekranu **ustawień kodu administratora**.

Przejdź do interfejsu internetowego **System > Security > Admin Code Setting.**

Modyfikacja hasła ustawień

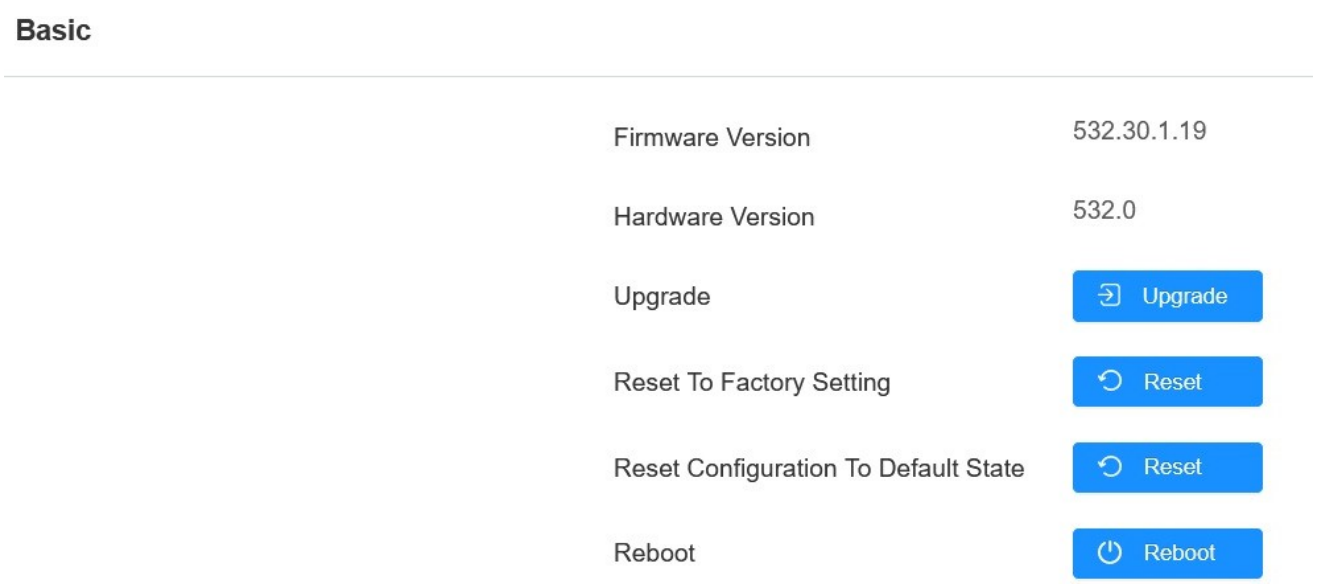
Kod PIN ustawień służy do uzyskiwania dostępu do ustawień obejmujących publiczny kod PIN, prywatny kod PIN i modyfikację kodu karty użytkownika. Kod PIN ustawień można zmodyfikować na urządzeniu.

Naciśnij *2396# na klawiaturze urządzenia i naciśnij 2, a następnie 3, aby przejść do ekranu **ustawień kodu serwisowego.**

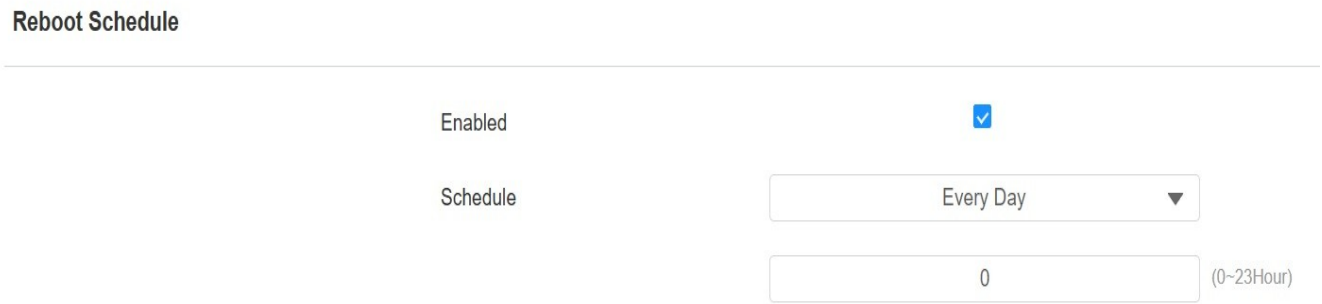
Ponowne uruchamianie i resetowanie systemu

Reboot

Aby zrestartować urządzenie w interfejsie sieci Web **System > Upgrade.**



Harmonogram restartów można skonfigurować w interfejsie **System > Auto Provisioning > Reboot Schedule.**

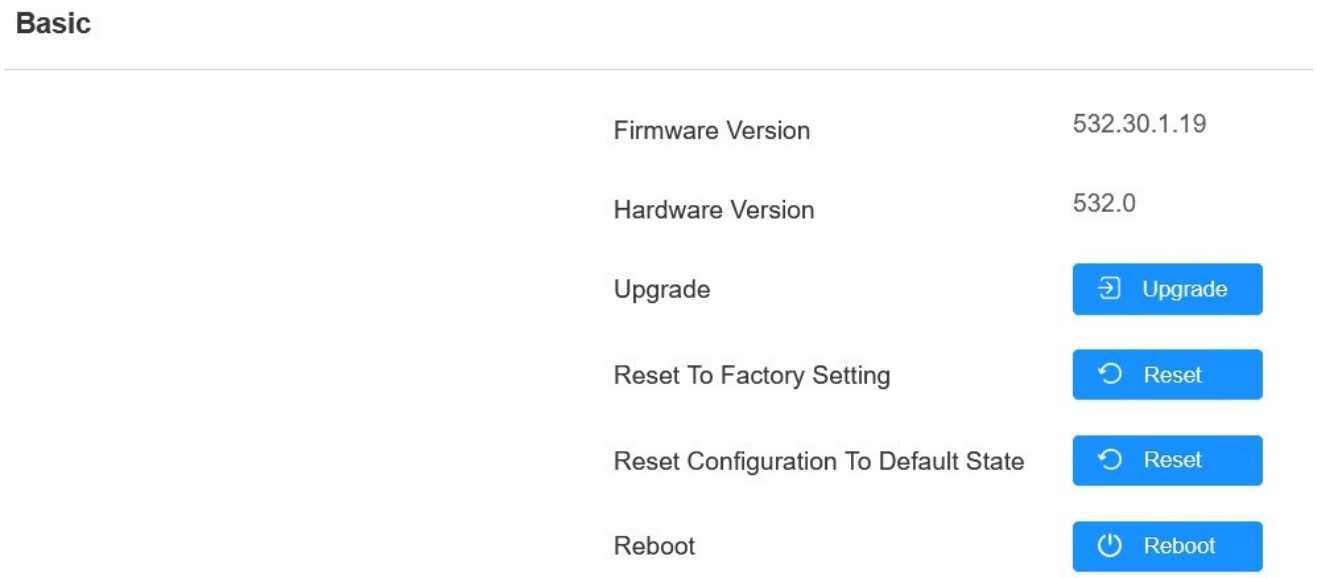


Reset

Resetowanie w interfejsie internetowym

Możesz wybrać **Reset To Factory Setting,** jeśli chcesz zresetować urządzenie (usuwając zarówno dane konfiguracyjne, jak i dane użytkownika, takie jak karty RF, dane twarzy itp.) Można też wybrać **Reset Configuration to Default State (Except Data) Reset**, aby zresetować urządzenie (zachowując dane użytkownika).

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



Resetowanie urządzenia

Naciśnij *2396# na klawiaturze urządzenia i naciśnij 3 i 2, aby przejść do ekranu przywracania. Następnie przesuń kartę administratora lub wprowadź kod administratora, aby zresetować urządzenie. Domyślny kod to 2396.