Informacje o niniejszej instrukcji

Akuvox
Open A Smart World

WWW.AKUVOX.COM

Akuvox Access Control Administrator Guide

Akuvox
Open A Smart World

Dziękujemy za wybranie terminala kontroli dostępu Akuvox A01. Niniejsza instrukcja jest przeznaczona dla administratorów, którzy muszą prawidłowo skonfigurować terminal kontroli dostępu. Niniejsza instrukcja została napisana w oparciu o wersję oprogramowania sprzętowego: 103.30.10.29 i zawiera wszystkie konfiguracje funkcji i cech terminala kontroli dostępu A03. Odwiedź forum Akuvox lub skonsultuj się z pomocą techniczną, aby uzyskać nowe informacje lub najnowsze oprogramowanie sprzętowe.

Przegląd produktów

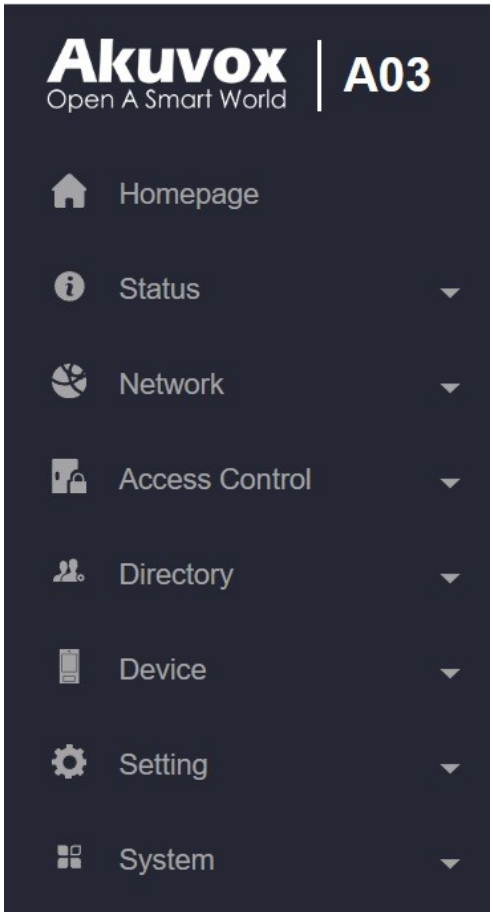
Terminal kontroli dostępu Akuvox A03 zawiera kontroler drzwi i czytnik RIFD w jednym samodzielnym urządzeniu, oszczędzając w ten sposób koszty rozwiązania. Jest wyposażony w czytnik kart (125 kHz i 13,5 MHz), który jest obecnie w stanie obsłużyć większość powszechnie używanych kart. Został zaprojektowany, aby zapewnić większą elastyczność i bezpieczeństwo niż tradycyjne systemy kontroli dostępu. Terminal kontroli dostępu A03 ma zastosowanie w budynkach mieszkalnych, biurowych i ich kompleksach.

Specyfikacja modelu

Model	**A03**
Czytnik kart RFID	13,56 MHz i 125 kHz
Przekaźnik wyłączony	1
Wejścia	2
Wiegand	✓
Głośnik	1
Alarm odporny na manipulacje	✓
Port Ethernet	RJ45, 10/100Mbps adaptacyjne złącze 802.3af power-over-Ethernet/12v DC (jeśli nie korzysta z PoE)
Wi-Fi	X
Bluetooth	✓

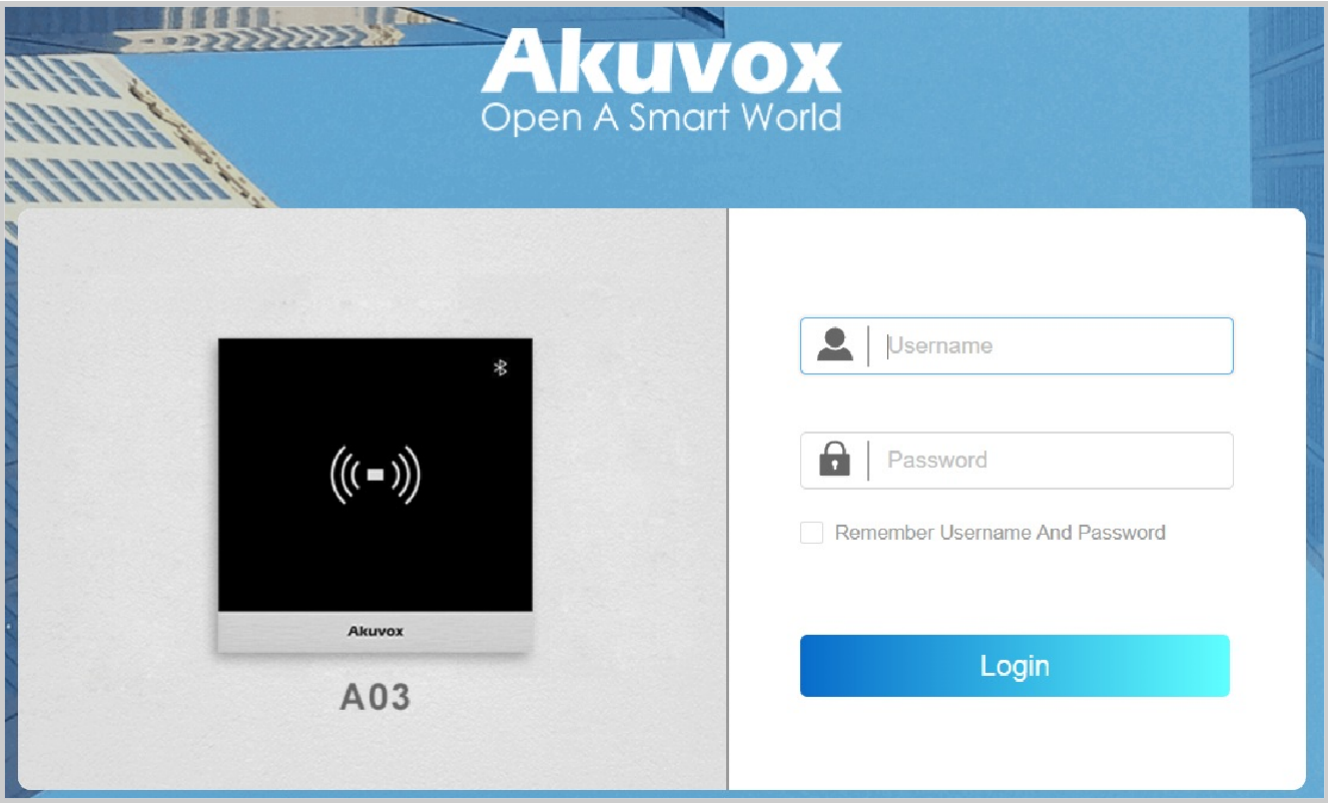
Wprowadzenie do menu konfiguracji

- **Status** : Ta sekcja zawiera podstawowe informacje, takie jak informacje o produkcie, informacje o sieci i zarządzanie dziennikiem dostępu.
- **Sieć** : Ta sekcja obejmuje ustawienia portu LAN.
- **Kontrola dostępu**: Ta sekcja obejmuje przekaźnik, wejście, przekaźnik sieciowy, ustawienia karty, ustawienia klawiatury itp.
- **Katalog**: Ta sekcja obejmuje zarządzanie harmonogramem dostępu i zarządzanie użytkownikami.
- **Urządzenie** : Ta sekcja zawiera ustawienia oświetlenia, Wiegand, sterowania windą i dźwięku.
- **Ustawienia**: Ta sekcja dotyczy harmonogramu przekaźnika, ustawień powiadomień bezpieczeństwa, przekaźnika internetowego, czasu, akcji i ustawień HTTP API.
- **System**: Ta sekcja obejmuje aktualizację oprogramowania układowego, resetowanie urządzenia, ponowne uruchamianie, automatyczne dostarczanie pliku konfiguracyjnego, dziennik systemowy i PCAP, modyfikację hasła, a także tworzenie kopii zapasowych urządzenia.



Dostęp do urządzenia

Przed konfiguracją Akuvox A03 należy upewnić się, że urządzenie jest prawidłowo zainstalowane i łączy się z normalną siecią. Za pomocą narzędzia skanera IP Akuvox wyszukaj adres IP urządzenia w tej samej sieci LAN. Następnie użyj adresu IP, aby zalogować się do przeglądarki internetowej przy użyciu nazwy użytkownika i hasła **admin** i **admin**.

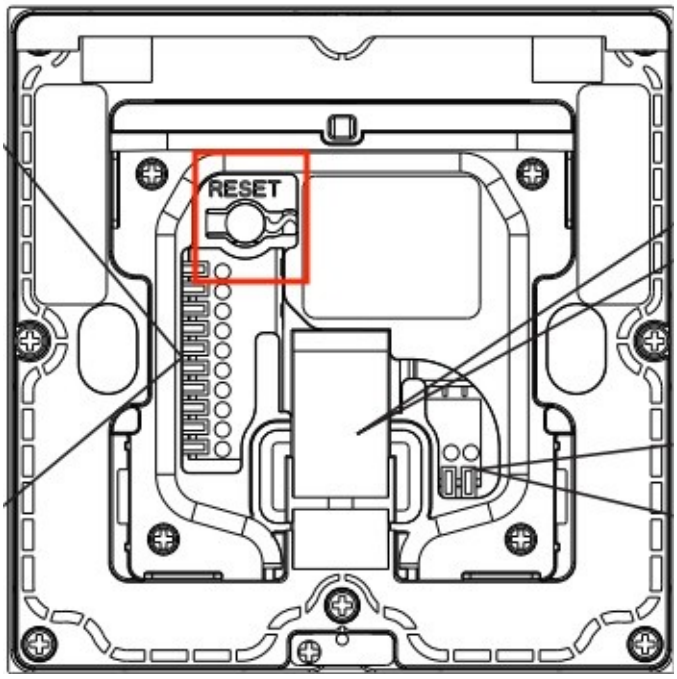


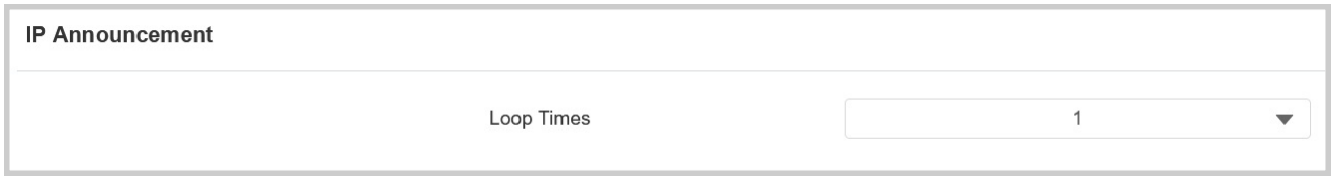
Uwa

- Pobierz skaner IP: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Zobacz szczegółowy przewodnik: **https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via- ip-scanner?highlight=IP%20Scanner**
- Zdecydowanie zalecana jest przeglądarka Google Chrome.
- Należy zwracać uwagę na wielkość liter we wprowadzanych nazwach użytkowników i hasłach.

Adres IP można również uzyskać, naciskając przycisk **Reset** z tyłu urządzenia. Urządzenie zgłosi adres IP.

Czasy pętli komunikatów IP można skonfigurować w interfejsie **Urządzenie > Audio**.



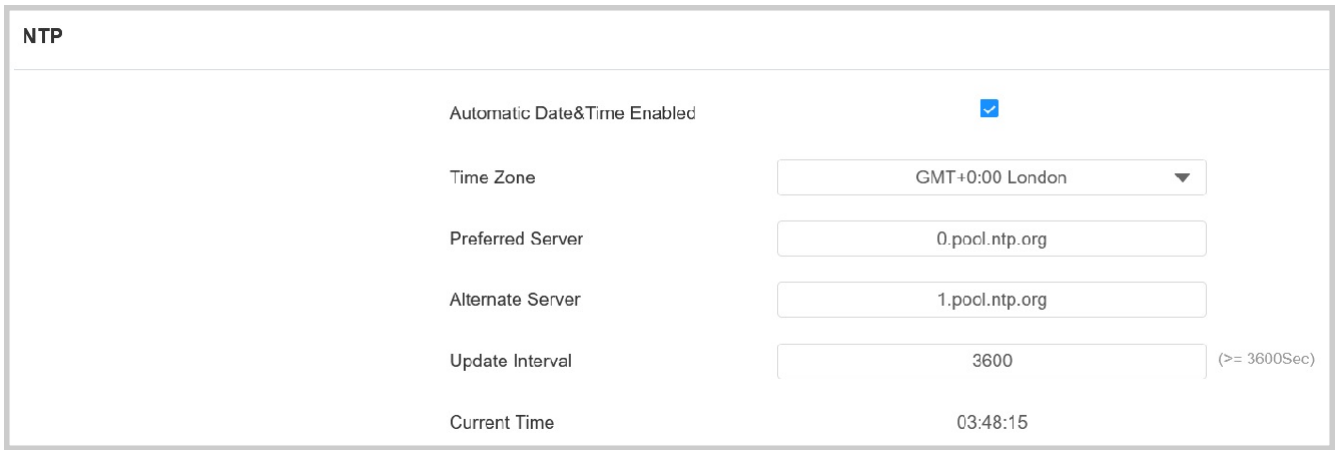


Czas i język

Czas

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.

Ustaw czas w interfejsie **Ustawienia > Czas**.



- **Automatic Date&Time Enabled**: Jeśli ta opcja jest włączona, urządzenie będzie automatycznie aktualizować czas za pośrednictwem serwera NTP (**Network Time**

Protocol). Wyłącz tę opcję, jeśli chcesz ustawić czas ręcznie.

- **Data/godzina**: ręczne ustawienie daty i godziny dla urządzenia po wyłączeniu usługi automatycznej daty i godziny.
- **Strefa czasowa**: Wybierz określoną strefę czasową w zależności od tego, gdzie urządzenie jest używane. Domyślną strefą czasową jest GMT+0:00.
- **Preferred Server** (**Preferowany serwer**): Wprowadź adres głównego serwera NTP, za pomocą którego chcesz aktualizować czas. Domyślny adres serwera NPT to 0.pool.ntp.org
- **Alternate Server**: Wprowadź adres serwera NPT dla kopii zapasowej.
- **Interwał aktualizacji**: Ustawienie interwału aktualizacji czasu. Na przykład, jeśli ustawisz 3600s, urządzenie będzie wysyłać żądanie do serwera NPT w celu aktualizacji czasu raz na 3600 sekund.
- **Bieżący** czas: wyświetla bieżący czas urządzenia.

Język

Język strony internetowej można zmienić, wybierając język w prawym górnym rogu.

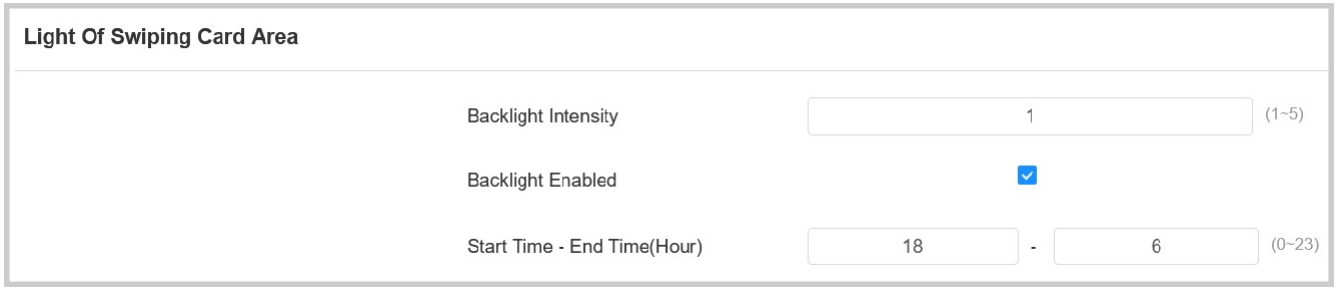
Obsługiwane są następujące języki: Angielski, chiński uproszczony, holenderski, francuski i niemiecki.

Ustawienie LED

Ustawienie diody LED w obszarze czytnika kart

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

Aby ją skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **Light**.

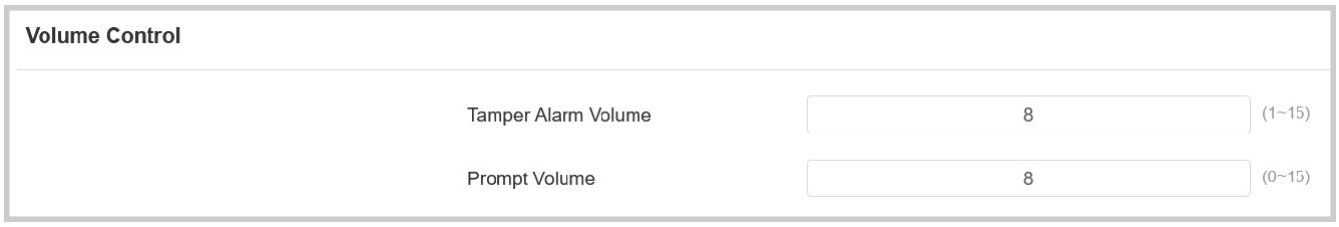


- **Intensywność podświetlenia**: Regulacja intensywności podświetlenia, im większa wartość, tym jaśniejsze podświetlenie.
- **Czas rozpoczęcia - Czas zakończenia (godzina)**: Wybierz zakres czasu, w którym oświetlenie LED ma obowiązywać, np. jeśli zakres czasu wynosi od 18-22, oznacza to, że światło LED pozostanie włączone w przedziale czasowym od 18:00 do 22:00 w ciągu jednego dnia (24 godziny).

Konfiguracja głośności i tonów

Konfiguracja głośności i tonów obejmuje alarm sabotażowy i głośność monitu. Poza tym można wgrać dźwięki dzwonka otwierania drzwi.

Aby go skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **audio**.



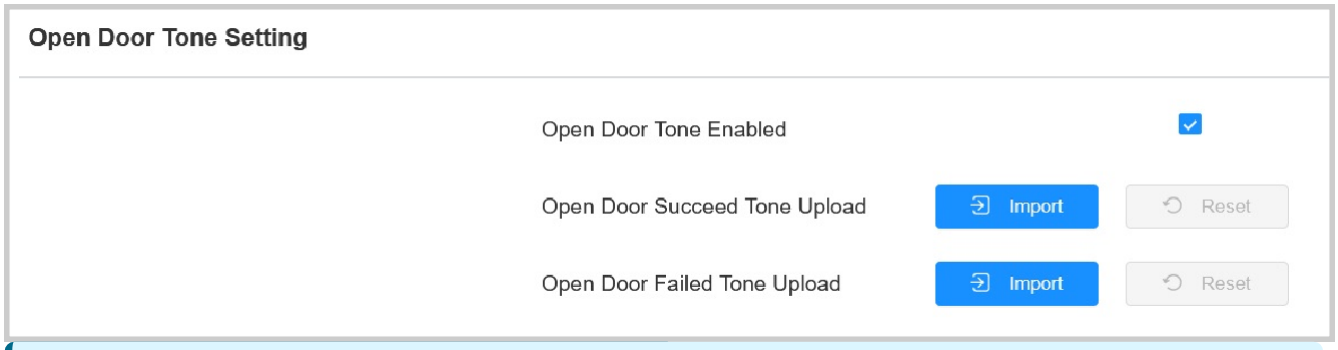
- **Alarm** antysabotażowy: Ustaw głośność po wyzwoleniu alarmu antysabotażowego. Domyślna głośność to 8.
- **Głośność komunikatów**: Ustaw głośność komunikatów głosowych. Domyślna głośność to 8.

Prześlij dźwięk otwartych drzwi

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

Aby przesłać dźwięki, przejdź do interfejsu **Device > Audio > Open Door Tone Setting**.

Włącz dźwięk otwartych drzwi przed przesłaniem pliku.



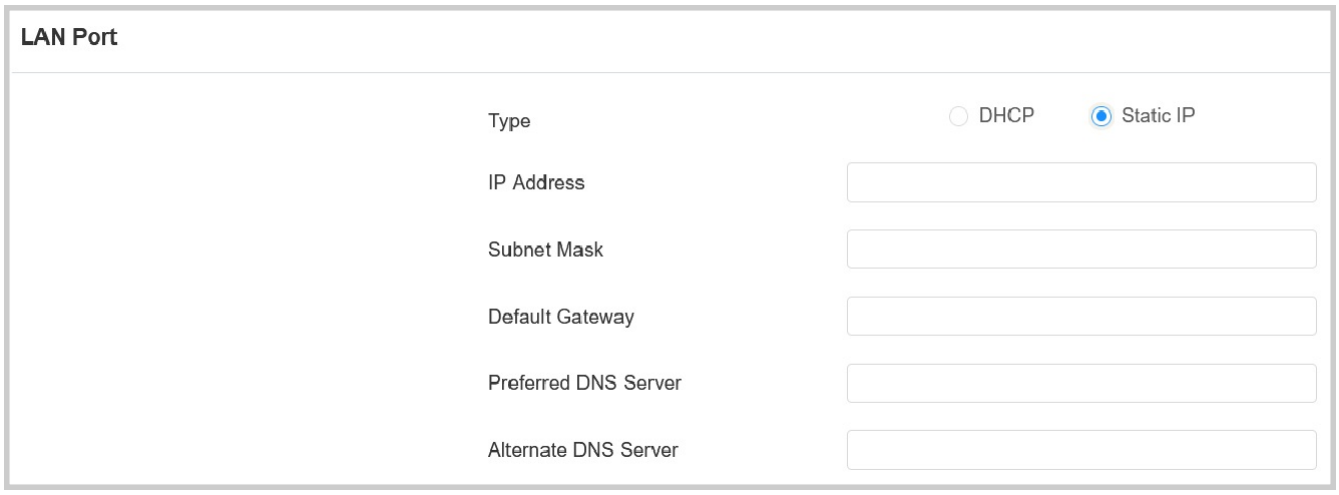
Uwaga

Format pliku: wav, rozmiar: < 200KB, pcm(częstotliwość próbkowania: 16000, bity: 16, mono)/pcma/pcmu

Ustawienia sieciowe

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

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



- **DHCP** : Tryb DHCP jest domyślnym połączeniem sieciowym. Po wybraniu trybu DHCP terminal kontroli dostępu zostanie automatycznie przypisany przez serwer DHCP z adresem IP, maską podsieci, bramą domyślną i adresem serwera DNS.
- **Statyczne IP**: Po wybraniu trybu statycznego IP, adres IP, maska podsieci, brama domyślna i adres serwera DNS powinny być skonfigurowane zgodnie ze środowiskiem sieciowym.
- **Adres IP**: Ustawienie adresu IP w przypadku wybrania statycznego trybu IP.
- **Maska podsieci**: Ustaw maskę podsieci zgodnie z rzeczywistym środowiskiem sieciowym.
- **Brama domyślna**: Ustaw prawidłową bramę zgodnie z adresem IP.

- **Preferowany/alternatywny serwer DNS**: Skonfiguruj preferowany lub alternatywny serwer DNS (Domain Name Server) zgodnie z rzeczywistym środowiskiem sieciowym. Preferowany serwer DNS jest serwerem podstawowym, podczas gdy alternatywny serwer DNS jest serwerem dodatkowym. Serwer dodatkowy służy do tworzenia kopii zapasowych.

Ustawienie SNMP

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

Aby ją skonfigurować, przejdź do opcji **Sieć >** Interfejs **zaawansowany**.

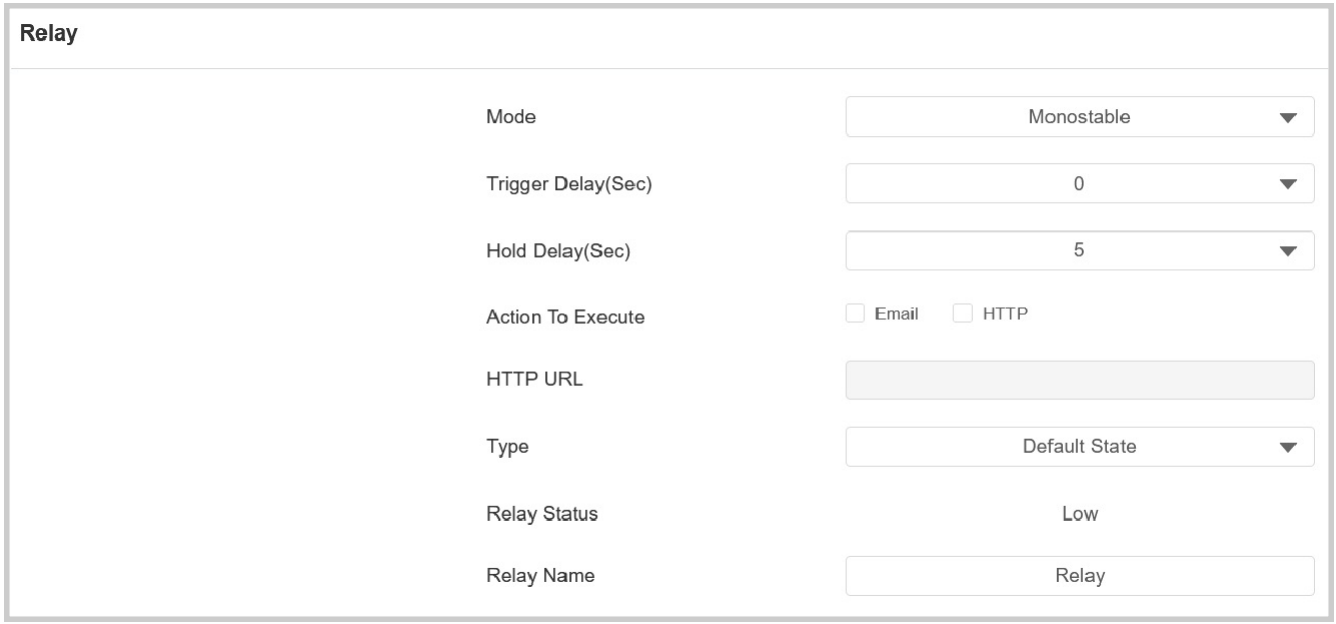
- **Port**: Ustaw określony port dla transmisji danych z zakresu 1024-65535.
- **Zaufany adres IP**: Wprowadź adres IP innej firmy.

Ustawienia przekaźnika

Przełączniki przekaźnikowe dostępu do drzwi można skonfigurować w interfejsie internetowym.

Przełącznik przekaźnika

Aby skonfigurować przekaźnik, przejdź do opcji **Kontrola dostępu > Przekaźnik >** Interfejs **przekaźnika**.



- **Tryb** : Określa warunki automatycznego resetowania stanu przekaźnika.
    - **Monostabilny**: Status przekaźnika resetuje się automatycznie w czasie opóźnienia przekaźnika po aktywacji.

    Bistabilny: Stan przekaźnika resetuje się po ponownym wyzwoleniu przekaźnika.

- **Trigger Delay(Sec)**: Ustaw czas opóźnienia przed wyzwoleniem przekaźnika. Na przykład, jeśli ustawiono 5 sekund, przekaźnik aktywuje się 5 sekund po naciśnięciu przycisku odblokowania.

- **Hold Delay(Sec)**: Określa, jak długo przekaźnik pozostaje aktywny. Na przykład, jeśli ustawione na 5 sekund, przekaźnik pozostanie otwarty przez 5 sekund przed zamknięciem.

- **Akcja do wykonania**: Sprawdź akcję, która ma zostać wykonana po wyzwoleniu przekaźnika.
    - **HTTP**: Po uruchomieniu, komunikat HTTP może zostać przechwycony i wyświetlony w odpowiednich pakietach. Aby skorzystać z tej funkcji, należy włączyć serwer HTTP i wprowadzić treść wiadomości w wyznaczonym polu poniżej.

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

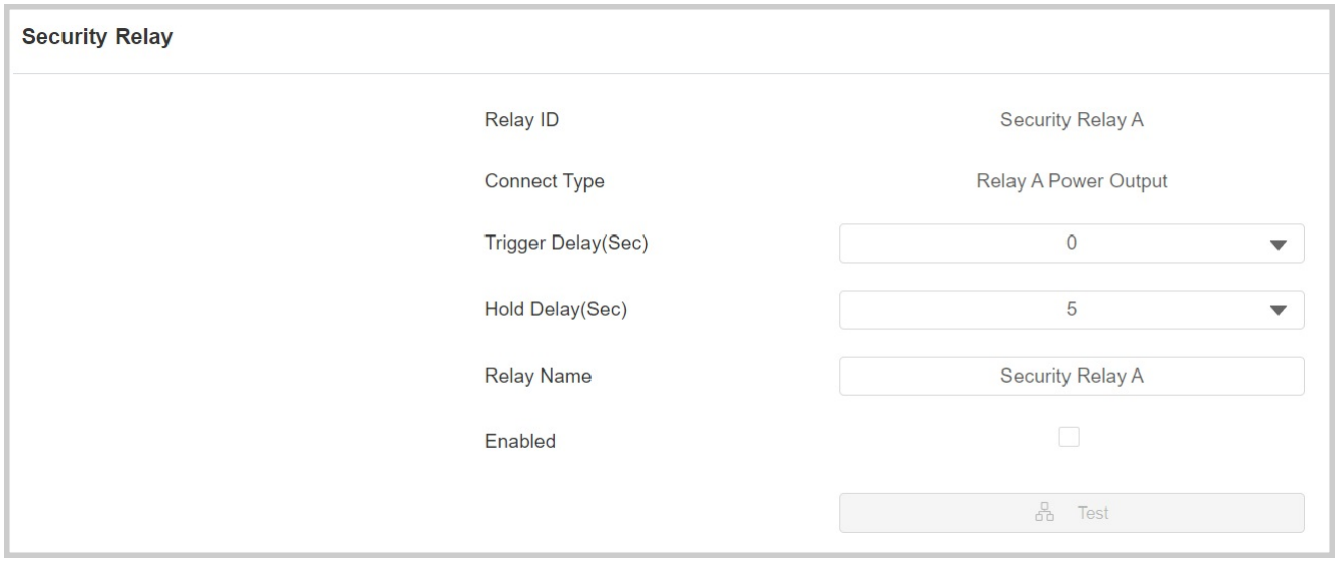
- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/treść wiadomości.
- **Typ** : Określa interpretację statusu przekaźnika w odniesieniu do stanu drzwi:
  - **Stan domyślny** : Stan "Niski" w polu Status przekaźnika oznacza, że drzwi są zamknięte, natomiast stan "Wysoki" oznacza, że są otwarte.
  - **Stan odwrócony** : Stan "Niski" w polu Status przekaźnika oznacza otwarte drzwi, natomiast stan "Wysoki" oznacza drzwi zamknięte.
- **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 osobnych zasilaczy.

Przekaźnik 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 go skonfigurować, przejdź do opcji **Kontrola dostępu > Przekaźnik >** Interfejs **przekaźnika zabezpieczeń**.



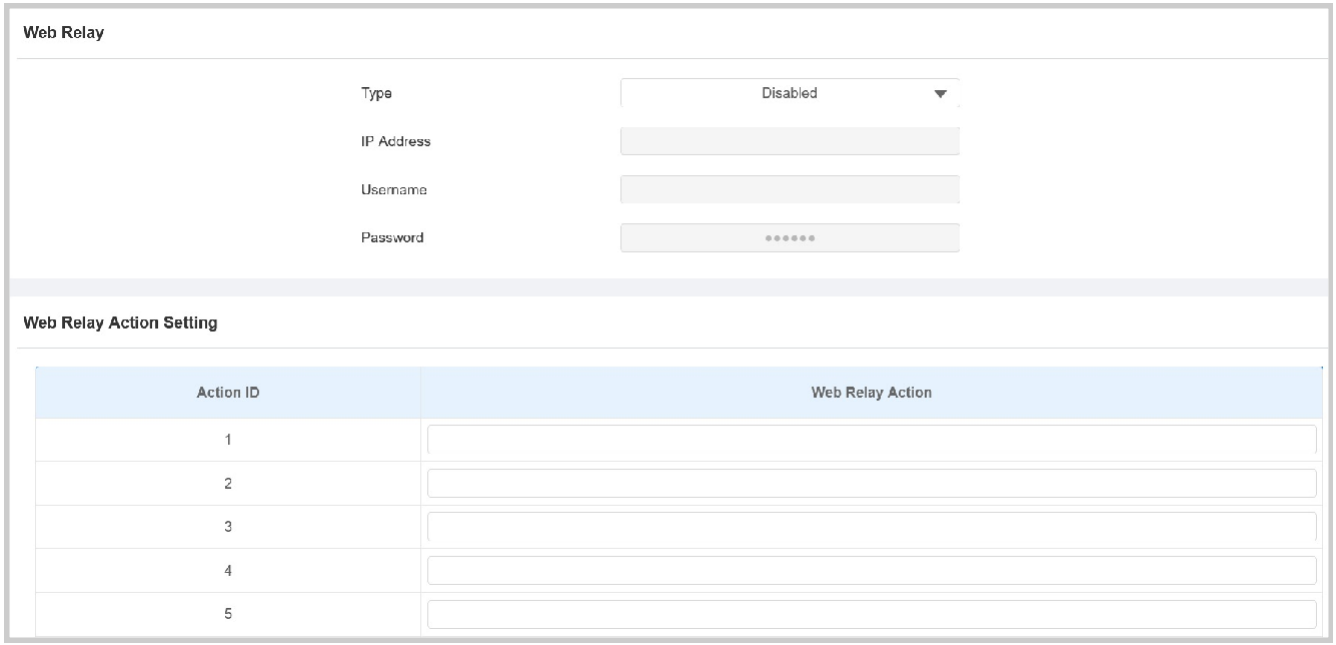
- Identyfikator **przekaźnika**: określony przekaźnik dostępu do drzwi.
- **Typ połączenia** : Przekaźnik bezpieczeństwa domyślnie łączy się z urządzeniem za pomocą wyjścia zasilania.
- **Trigger Delay(Sec)**: Ustaw czas opóźnienia przed wyzwoleniem przekaźnika. Na przykład, jeśli ustawiono 5 sekund, przekaźnik aktywuje się 5 sekund po naciśnięciu przycisku odblokowania.
- **Hold Delay(Sec)**: Określa, jak długo przekaźnik pozostaje aktywny. Na przykład, jeśli ustawione na 5 sekund, przekaźnik pozostanie otwarty przez 5 sekund przed zamknięciem.
- **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.

Przekaźnik internetowy

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

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



- **Typ** : Określa typ przekaźnika aktywowanego podczas korzystania z metod dostępu do drzwi.
    - **Wyłączone**: Aktywuje tylko lokalny przekaźnik.
    - **Przekaźnik sieciowy**: Aktywuj tylko przekaźnik sieciowy.
    - **Przekaźnik lokalny+przekaźnik sieciowy**: Aktywuje zarówno przekaźnik lokalny, jak i internetowy. Zazwyczaj najpierw uruchamiany jest przekaźnik lokalny, a następnie przekaźnik sieciowy w celu wykonania wcześniej skonfigurowanych działań.
- **Adres IP**: Adres IP przekaźnika sieciowego dostarczony przez producenta przekaźnika sieciowego.

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

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

Zarządzanie harmonogramem dostępu do drzwi

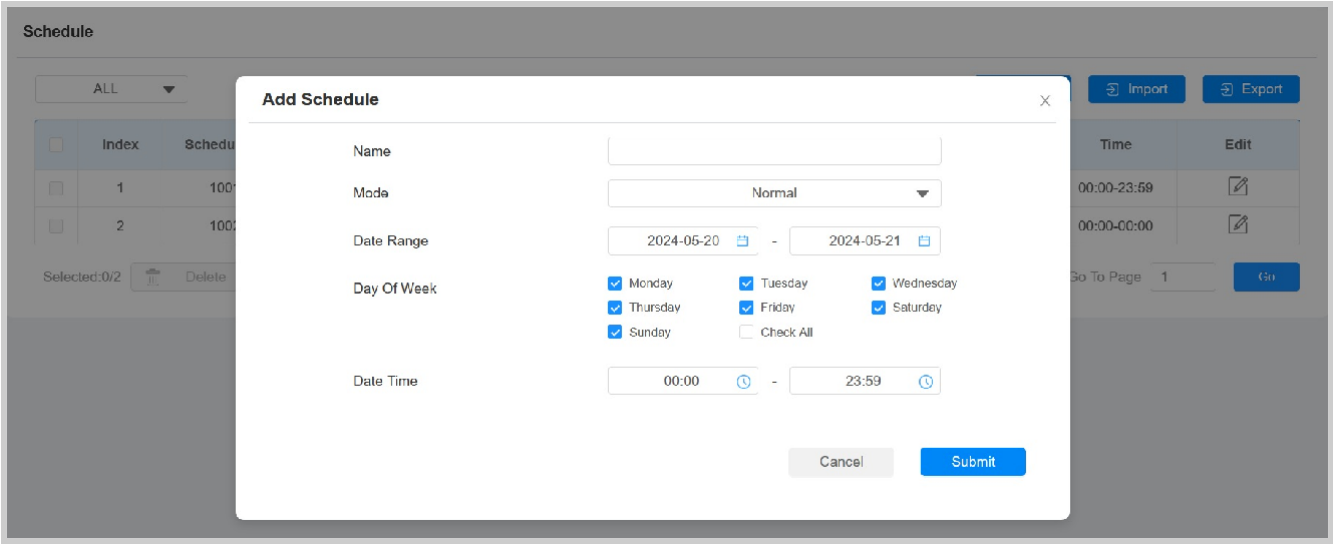
Harmonogram dostępu do drzwi

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

Aby utworzyć harmonogram dostępu do drzwi, przejdź do interfejsu **Setting > Schedule**.

Kliknij **+Dodaj**, aby utworzyć harmonogram.



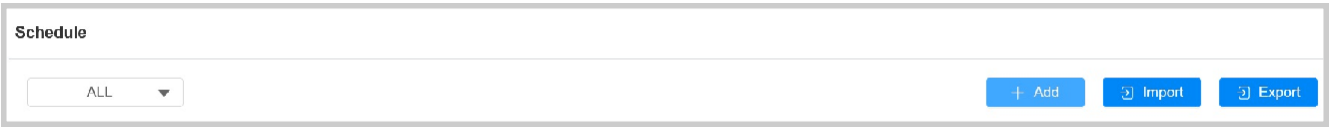
- **Nazwa**: Nazwa harmonogramu.
- **Tryb** :
  - **Normalny**: Ustaw harmonogram na podstawie miesiąca, tygodnia i dnia. Służy do tworzenia harmonogramów na długie okresy.

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

Harmonogram importu i eksportu dostępu do drzwi

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

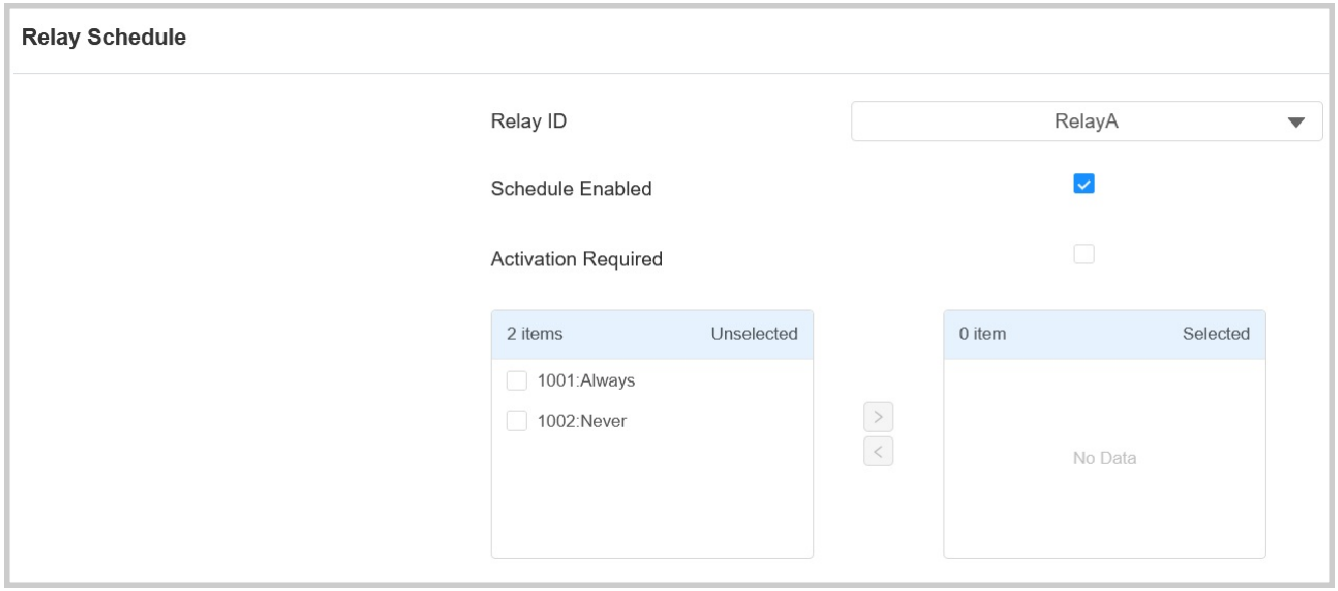
Aby go skonfigurować, przejdź do interfejsu **Ustawienia > Harmonogram**. Plik eksportu jest w formacie **TGZ**. Plik importu powinien być w formacie **XML**.



Harmonogram przekaźników

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

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



- **Identyfikator przekaźnika**: Określ przekaźnik, który chcesz skonfigurować.
- **Wymagana aktywacja**: Oznacza to, że dopiero po pomyślnym uruchomieniu przekaźnika po raz pierwszy, może on zostać uruchomiony później za pomocą metod dostępu obsługiwanych przez urządzenie.

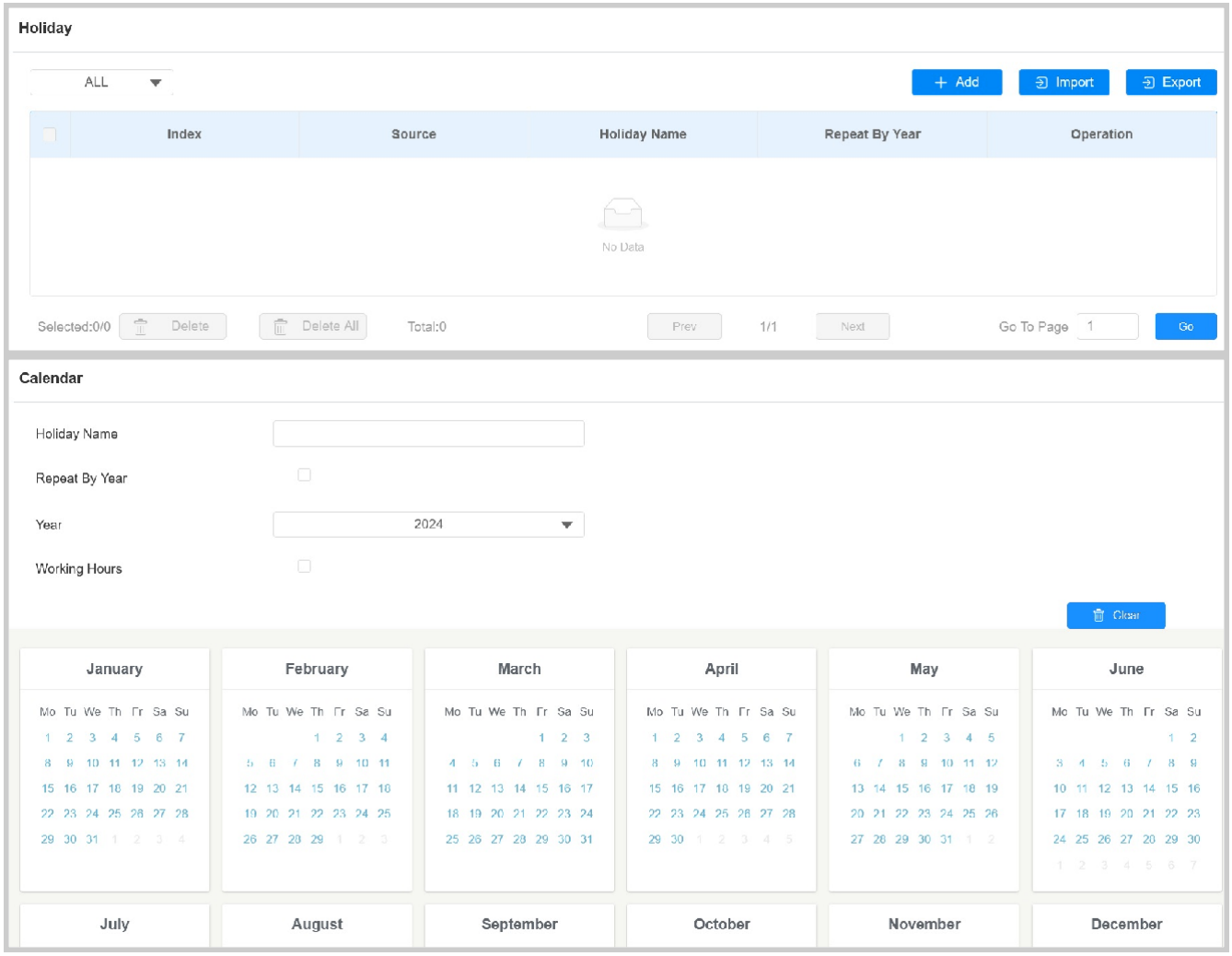
  Harmonogram: Przypisz określone harmonogramy dostępu do drzwi do wybranego przekaźnika. Wystarczy przenieść je do pola Selected Schedules.

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

Konfiguracja harmonogramu dostępu do drzwi w dni świąteczne

Można utworzyć harmonogram dostępu do drzwi w dni wolne od pracy. W te dni użytkownicy nie mogą otwierać drzwi.

Skonfiguruj go w interfejsie **Ustawienia > Urlop**. Kliknij **+Add**, aby dodać święto i kliknij **+Wyczyść**, aby usunąć zaznaczenie wszystkich dat.



W tym samym interfejsie można również importować i eksportować pliki harmonogramów. Eksportowany plik jest w formacie TGZ. Importowany plik powinien być w formacie XML.

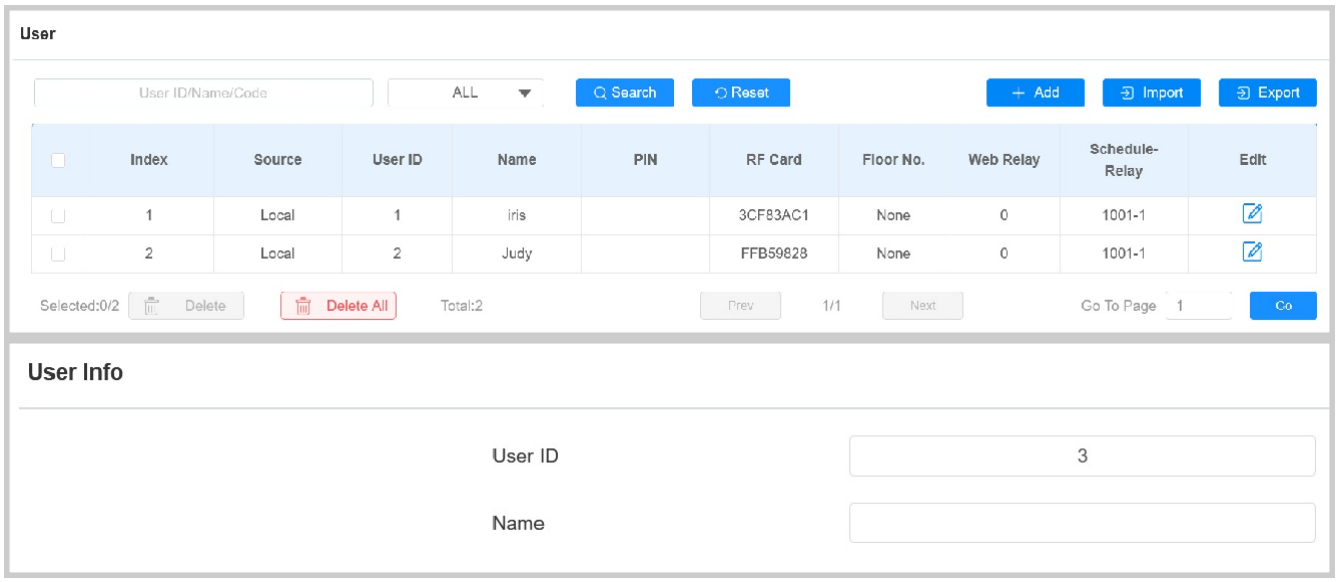
Konfiguracja odblokowania drzwi

Metody dostępu specyficzne dla użytkownika

Prywatny kod PIN, karta RF i ustawienia Bluetooth powinny być przypisane do konkretnego użytkownika w celu otwierania drzwi.

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

Aby dodać użytkownika, przejdź do **Katalog >** Interfejs **użytkownika** i kliknij **+Dodaj** .



- **Identyfikator użytkownika**: unikalny numer identyfikacyjny przypisany do użytkownika.
- **Nazwa**: nazwa tego użytkownika.

Odblokowanie za pomocą prywatnego kodu PIN

Urządzenie można podłączyć do zewnętrznej klawiatury. Użytkownicy mogą otwierać drzwi, wprowadzając swoje prywatne kody PIN na klawiaturze.

W interfejsie **Directory > User > +Add** przewiń do sekcji **PIN**.

- **Kod** : Ustawienie 2-8-cyfrowego kodu PIN wyłącznie do użytku tego użytkownika. Każdemu użytkownikowi można przypisać tylko jeden kod PIN.

Odblokowanie za pomocą karty RF

W interfejsie **Directory > User > +Add** przewiń do sekcji **RF Card**.

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

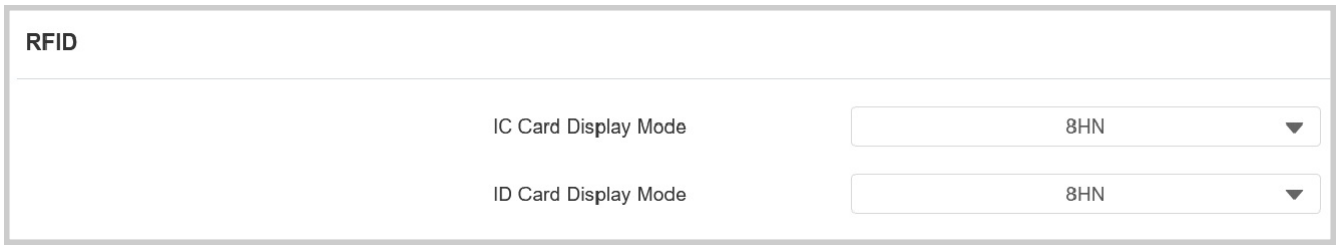
Uwaga:

- Każdy użytkownik może dodać maksymalnie 5 kart.
- Urządzenie pozwala na dodanie 20 000 użytkowników.
- Karty RF działające na częstotliwościach 13,56 MHz i 125 KHz są kompatybilne z urządzeniem.

Format kodu karty RF

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

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



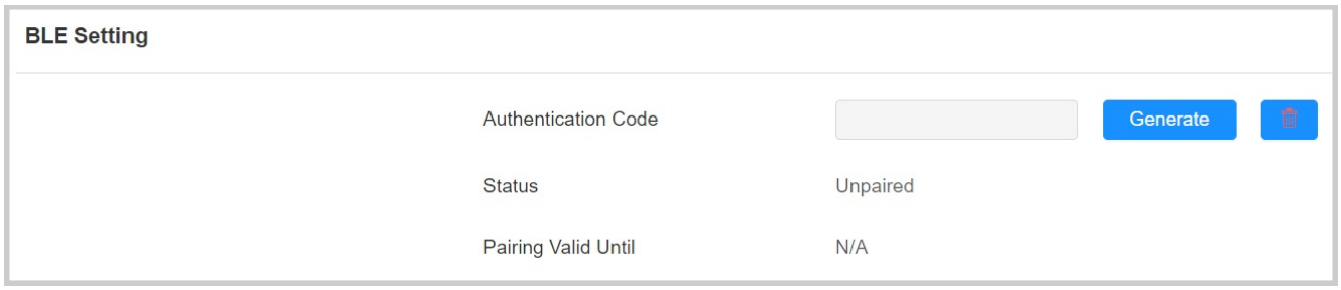
- **Tryb wyświetlania karty IC/ID** : Ustaw format numeru karty spośród dostępnych opcji. Domyślnym formatem w urządzeniu jest 8HN.

Odblokowanie przez Bluetooth

A03 obsługuje otwieranie drzwi za pomocą My MobileKey z obsługą Bluetooth lub aplikacji SmartPlus. Użytkownicy mogą otwierać drzwi za pomocą aplikacji w kieszeniach lub machać telefonem w kierunku urządzenia, gdy zbliżają się do drzwi.

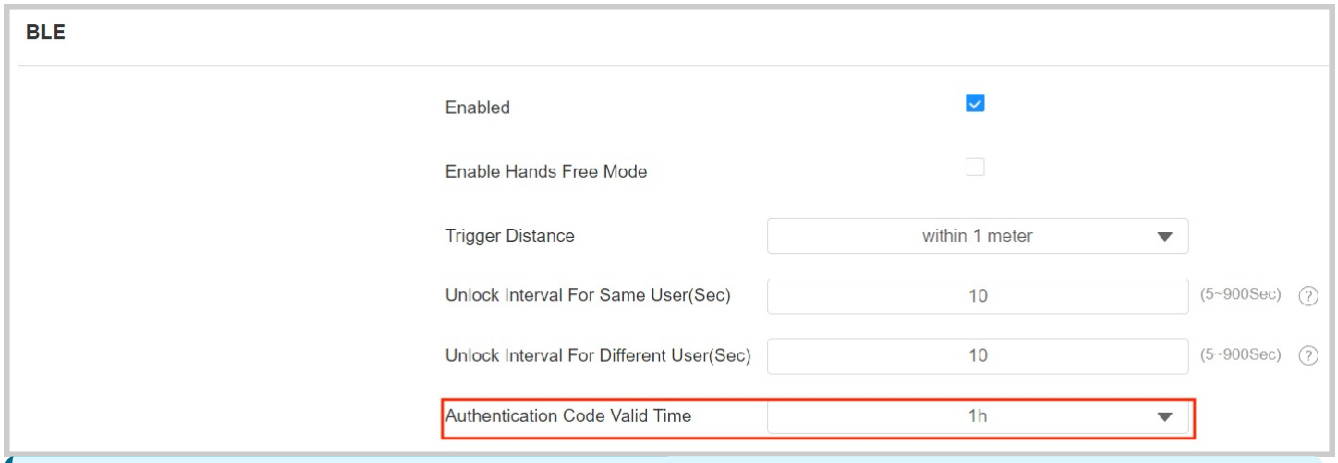
Odblokowanie za pomocą My MobileKey

W interfejsie **Directory > User > +Add** przewiń do sekcji **BLE Setting**.



- **Kod uwierzytelniający** : Kliknij **Generuj**, aby wygenerować 6-cyfrowy kod weryfikacyjny.

Można ustawić czas ważności parowania, w którym użytkownicy muszą zakończyć parowanie. Aby to zrobić, przejdź do opcji **Kontrola dostępu > BLE > Interfejs BLE**.

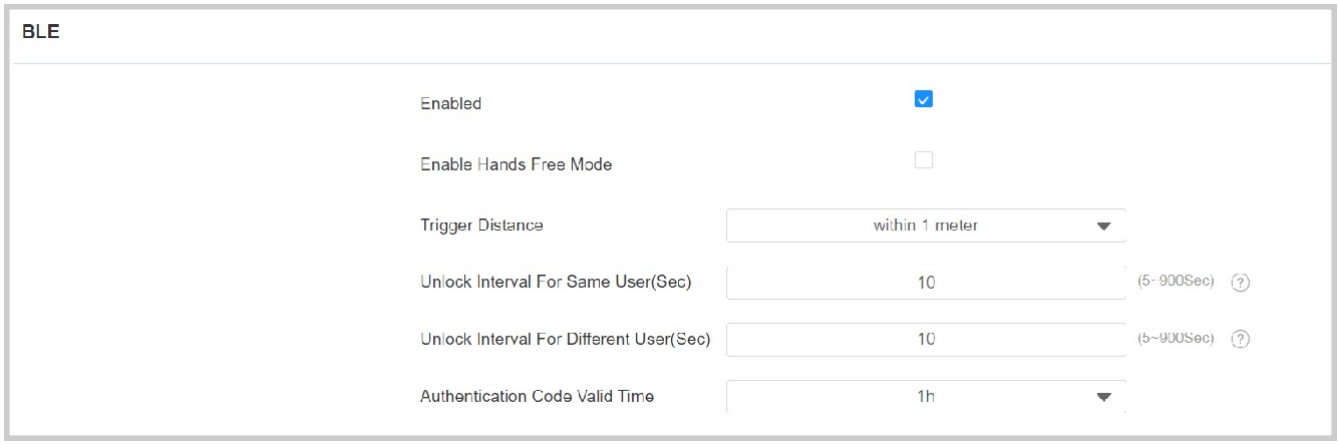


Uwaga

Kliknij **tutaj**, aby zobaczyć kroki konfiguracji.

Odblokowanie za pomocą aplikacji SmartPlus

Aby otworzyć drzwi za pomocą aplikacji SmartPlus, urządzenie powinno być połączone z chmurą SmartPlus. Aby skonfigurować odblokowanie Bluetooth, przejdź do opcji **Kontrola dostępu > BLE > Interfejs BLE**.



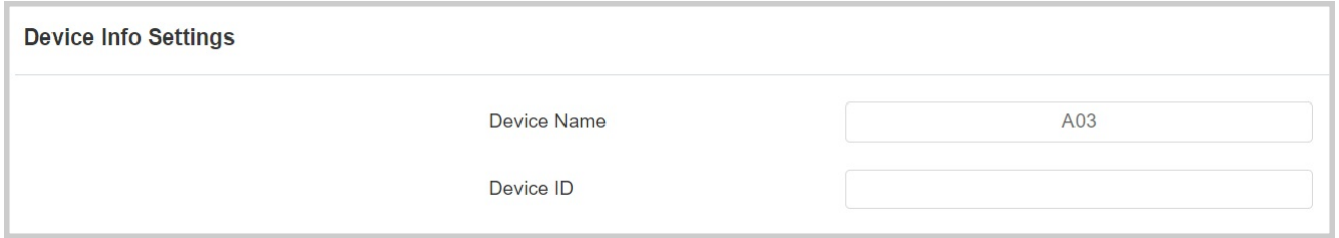
- **Włącz tryb głośnomówiący** : Jeśli jest włączony, użytkownicy mogą uzyskać dostęp do drzwi bez użycia rąk. Jeśli jest wyłączony, użytkownicy muszą machać rękami w pobliżu urządzenia, aby otworzyć drzwi.
- **Odległość wyzwalania**: Ustaw odległość wyzwalania Bluetooth dla dostępu do drzwi. Do wyboru są opcje W promieniu 1 metra, W promieniu 2 metrów i W promieniu 3 metrów. Odległość wyzwalania wynosi maksymalnie 3 metry.
- **Unlock Interval For Same User(Sec)**: Ustawienie odstępu czasu między kolejnymi próbami dostępu do drzwi Bluetooth dla tego samego użytkownika.
- **Unlock Interval For Different User(Sec)**: Ustawienie odstępu czasu między kolejnymi próbami dostępu do drzwi Bluetooth dla różnych użytkowników.

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

Ustawienie informacji o urządzeniu

Nazwę i identyfikator urządzenia można dostosować w celu wygodnego parowania Bluetooth.

Aby ją skonfigurować, przejdź do interfejsu **Access Control > BLE > Device Info Settings**.

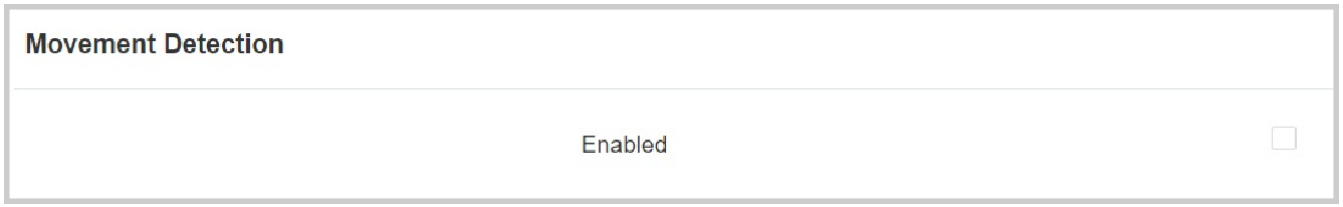


- **Nazwa urządzenia**: ograniczona do 1-63 cyfr lub znaków.
- **Identyfikator urządzenia**: Ograniczony do 1-12 cyfr lub znaków.

Ustawienie wykrywania ruchu

Ta funkcja działa tylko w przypadku otwierania drzwi przez Bluetooth za pomocą aplikacji My Mobilekey. Po włączeniu tej funkcji użytkownicy nie mogą otworzyć drzwi bez potrząśnięcia telefonem komórkowym.

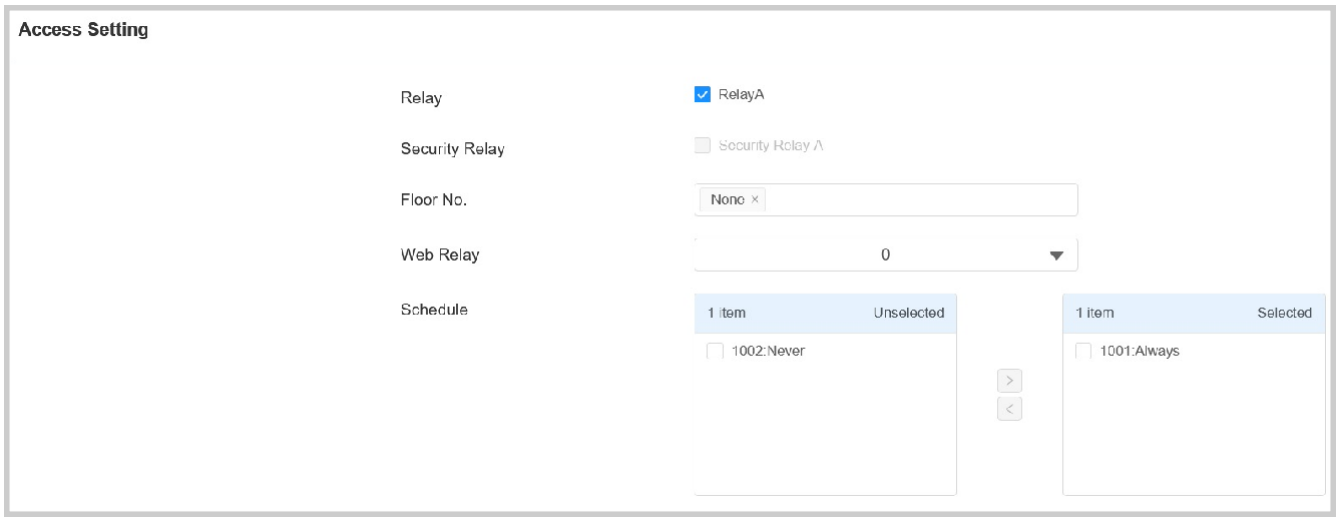
Włącz funkcję w interfejsie **Access Control > BLE > Movement Detection**.



Ustawienia dostępu

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

W interfejsie **Directory > User > +Add** przewiń do sekcji **Access Setting**.



- **Przekaźnik**: Określenie przekaźników, które mają zostać odblokowane przy użyciu metod otwierania drzwi przypisanych do użytkownika.
- **Przekaźnik zabezpieczeń**: Wybierz przekaźnik zabezpieczeń skonfigurowany w interfejsie Security Relay.
- **Nr piętra**: Określ piętro (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 lewego pola do prawego. Oprócz niestandardowych harmonogramów dostępne są 2 opcje domyślne:
    - **Zawsze** : Zezwala na otwieranie drzwi bez ograniczeń liczby otwarć drzwi w ważnym okresie.
    - **Nigdy**: Zabrania otwierania drzwi.

Ustawienia NFC i karty Felica

Ustaw urządzenie na obsługę kart NFC i Felica na urządzeniu, zanim będzie można z nich korzystać.

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

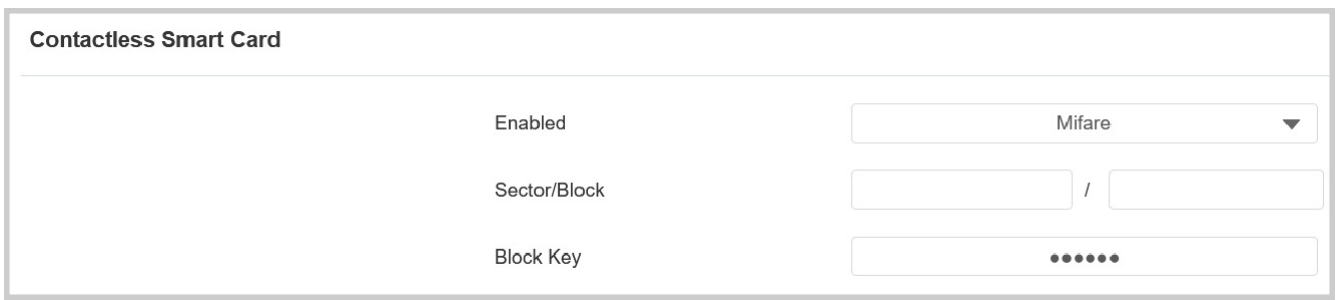
- **Enabled** : Wybierz NFC lub Felica z listy.

> **Uwaga**
>
> Funkcja NFC nie jest dostępna na iPhone'ach.

Karta Mifare

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

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



- **Sector/Block**: Określa lokalizację, w której przechowywane są zaszyfrowane dane

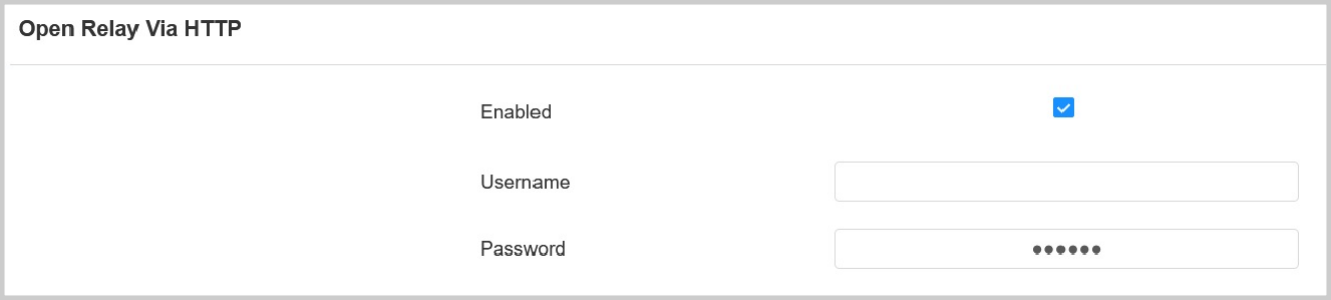
karty. Karta Mifare ma 16 sektorów (ponumerowanych od 0 do 15), a każdy sektor ma 4 bloki (ponumerowane od 0 do 3).

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

Odblokowanie za pomocą polecenia HTTP

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 opcji **Kontrola dostępu > Przekaźnik > Otwórz przekaźnik przez** interfejs **HTTP**.

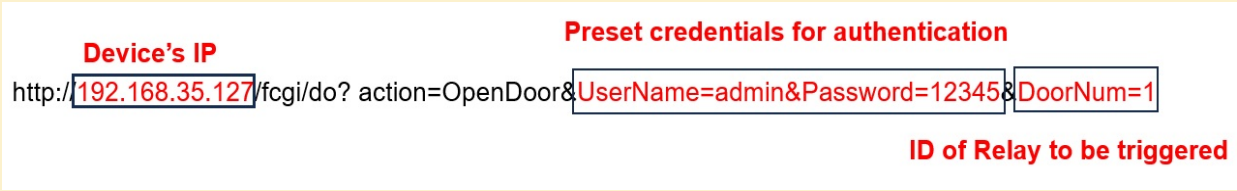


- **Nazwa użytkownika** : Ustaw nazwę użytkownika do uwierzytelniania w adresach URL poleceń HTTP.

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

Wskazówka:

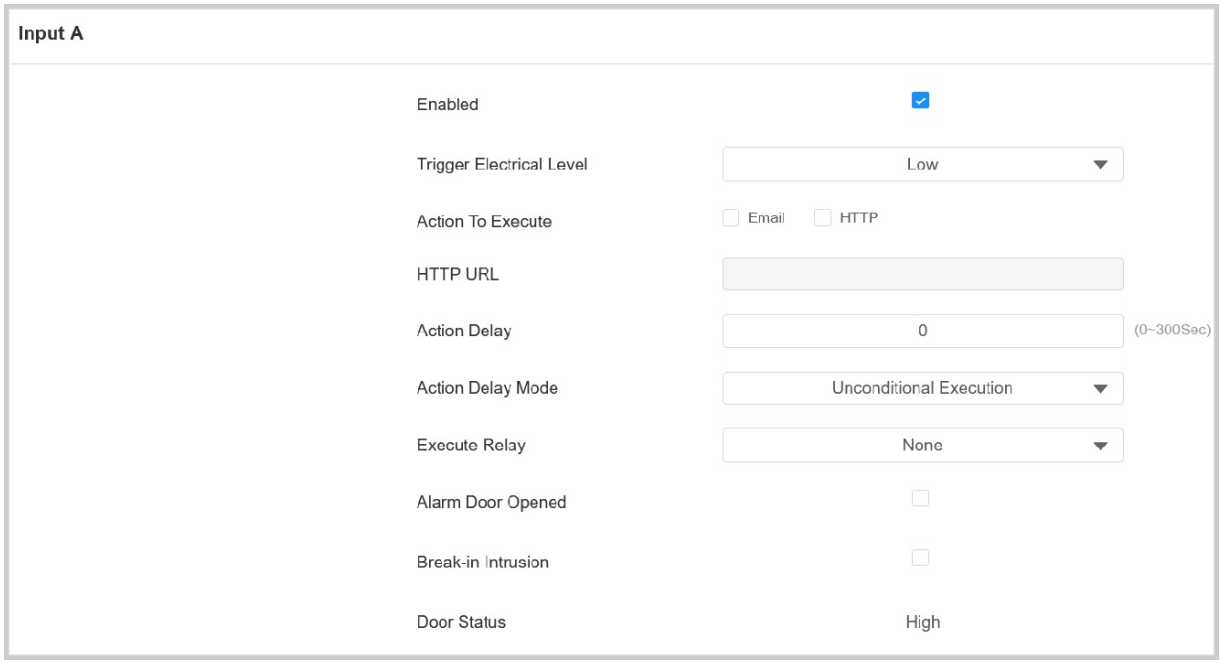
Oto przykład adresu URL polecenia HTTP dla wyzwalania przekaźnika.



Odblokowanie przyciskiem wyjścia

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

Aby ją skonfigurować, przejdź do opcji **Kontrola dostępu >** Interfejs wejści**owy**.



- **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.
    - **E-mail**: Wyślij zrzut ekranu na wstępnie skonfigurowany adres e-mail.
    - **HTTP**: Po uruchomieniu, komunikat HTTP może zostać przechwycony i wyświetlony w odpowiednich pakietach. Aby skorzystać z tej funkcji, należy włączyć serwer HTTP i wprowadzić treść wiadomości w wyznaczonym polu poniżej.
- **HTTP URL**: Wprowadź komunikat HTTP, jeśli jako akcję do wykonania wybrano HTTP. Format to http://HTTP IP serwera/treść wiadomości.
- **Opóźnienie akcji**: Określa, o ile sekund ma zostać opóźnione wykonanie wstępnie skonfigurowanych działań.
- **Tryb opóźnienia działania** :
    - **Bezwarunkowe wykonanie**: Akcja zostanie wykonana, gdy wejście zostanie wyzwolone.
    - **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.

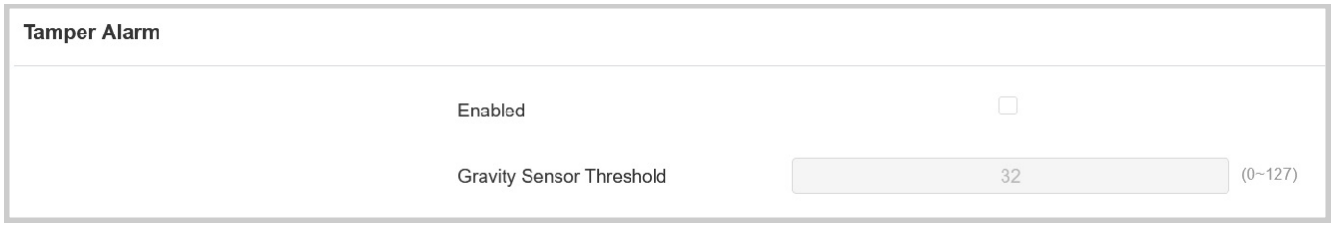
- **Wykonaj przekaźnik**: Określa przekaźnik, który ma być wyzwalany przez akcje.
- **Alarm Door Opened**: Określenie, czy ma być włączony limit czasu otwarcia drzwi.
- **Limit czasu otwarcia drzwi**: Ustawienie limitu czasu, przez jaki drzwi mają pozostać otwarte.
- **Włamanie**: Aktywacja alarmu w przypadku siłowego lub nielegalnego otwarcia drzwi. Wyłączenie tej opcji umożliwia wyłączenie alarmu po jego uruchomieniu.
- **Stan drzwi**: Wyświetla stan sygnału wejściowego.

Bezpieczeństwo

Alarm sabotażowy

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 ją skonfigurować, przejdź do **System > Bezpieczeństwo >** Interfejs **alarmu sabotażowego**.



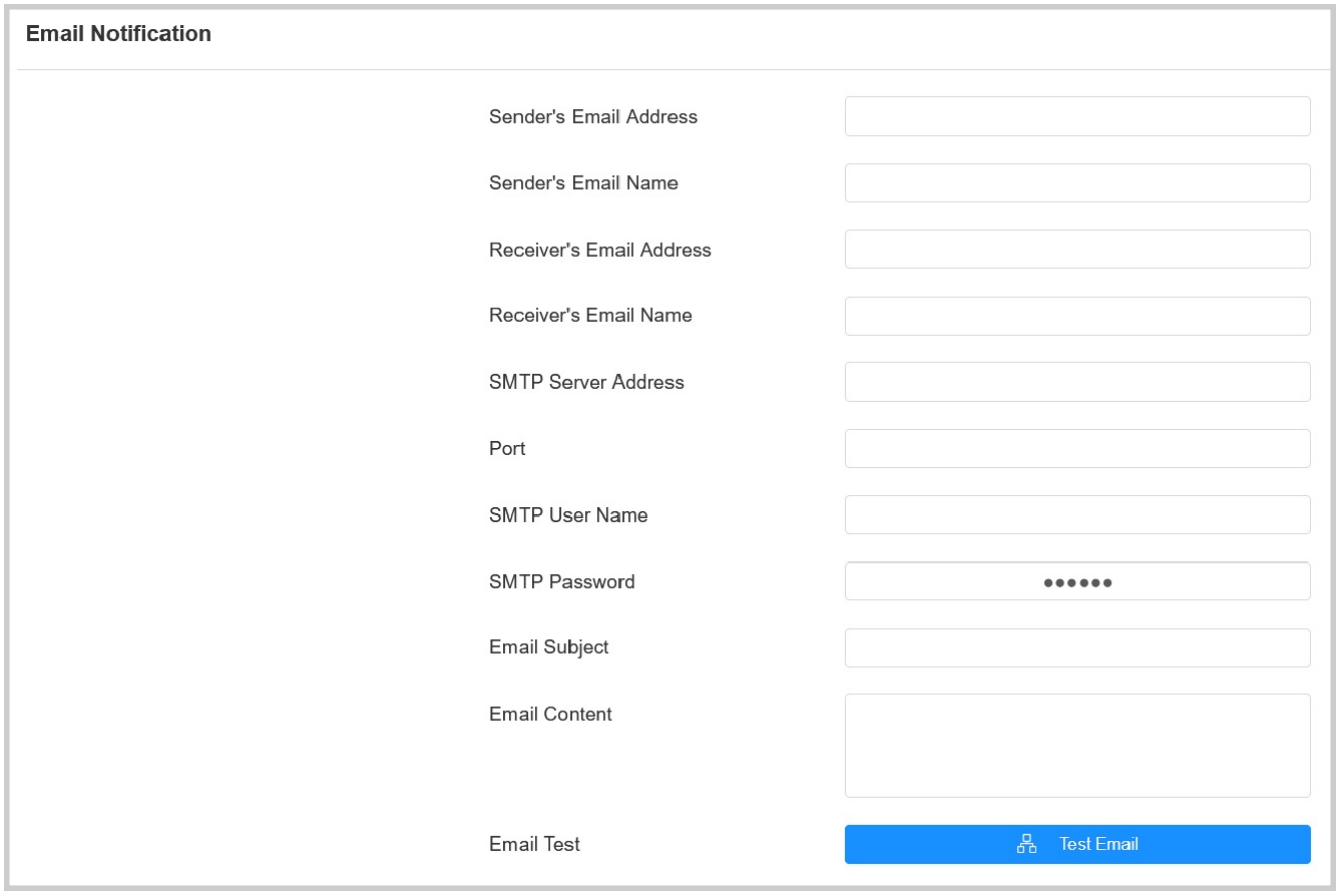
- **Próg czujnika grawitacji**: Próg czułości czujnika grawitacji. Im niższa wartość, tym bardziej czuły będzie czujnik. Domyślnie jest to 32.

Powiadomienie o zabezpieczeniach

Powiadomienie e-mail

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

z urządzenia. Przejdź do **Ustawienia > Akcja >** Interfejs **powiadomień e-mail**.



Adres URL akcji

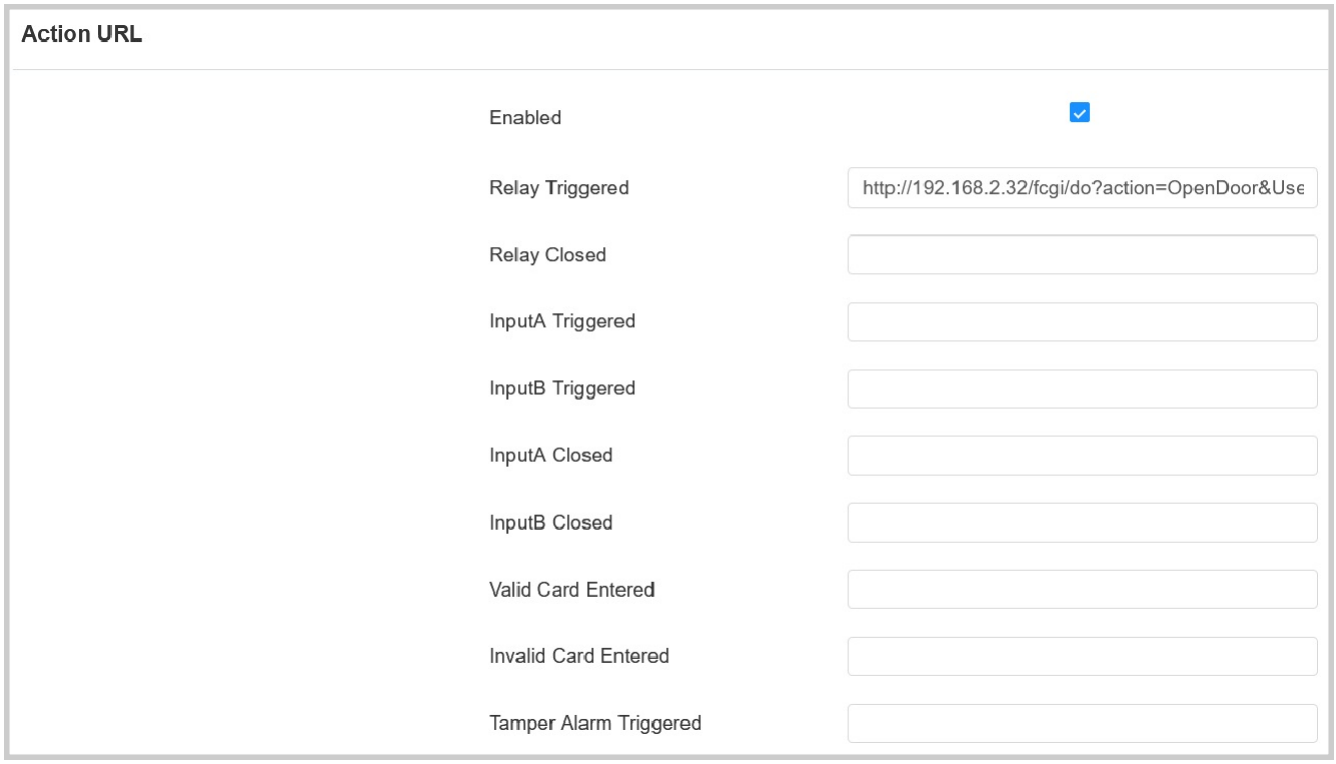
Za pomocą urządzenia można wysyłać określone polecenia HTTP URL do serwera HTTP w celu wykonania określonych działań. Działania te będą wyzwalane, gdy zmieni się stan przekaźnika, stan wejścia, kod PIN lub dostęp do karty RF.

Akuvox Action URL:

Nie	Wydarzenie	Format parametrów	Przykład
1	Przekaźnik wyzwolony	$relay1status	Http://server ip/ relaytrigger=$relay1status
2	Przekaźnik zamknięty	$relay1status	Http://server ip/ relayclose=$relay1status
3	Wejście wyzwalane	$input1status	Http://server ip/ inputtrigger=$input1status
4	Wejście zamknięte	$input1status	Http://server ip/ inputclose=$input1status
5	Wprowadzona ważna karta	$card_sn	Http://server ip/ validcard=$card_sn
6	Wprowadzono nieprawidłową kartę	$card_sn	Http://server ip/ invalidcard=$card_sn
7	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

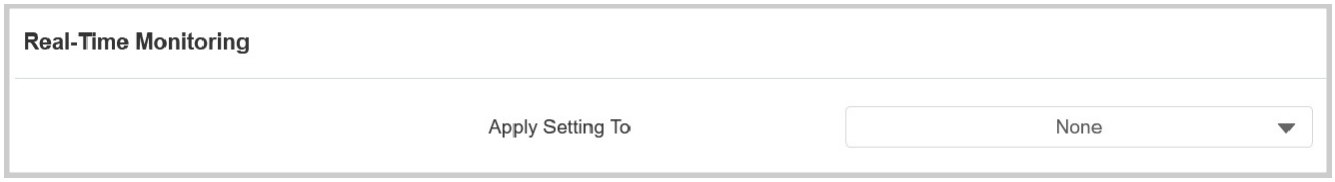
Aby ją skonfigurować, przejdź do opcji **Ustawienia >** Interfejs **Action URL**.



Monitorowanie w czasie rzeczywistym

Gdy urządzenie jest podłączone do SmartPlus Cloud lub ACMS, status drzwi może być wyświetlany na platformie SmartPlus lub ACMS.

Aby ją skonfigurować, przejdź do **System > Bezpieczeństwo >** Interfejs **monitorowania w czasie rzeczywistym**.



- **Zastosuj ustawienia do** :
  - **Brak** : Nie wyświetla stanu drzwi.
  - **Wejście**: drzwi są otwierane przez wejście wyzwalające.
  - **Przekaźnik**: drzwi są otwierane przez wyzwolenie przekaźnika.

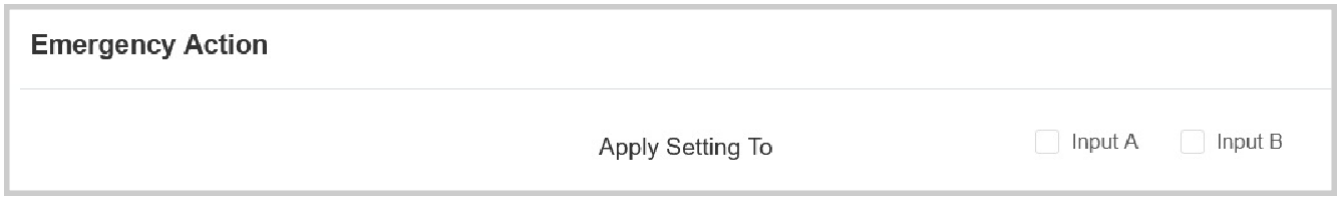
Uwaga

Kliknij tutaj, aby zobaczyć szczegółowe kroki konfiguracji.

Akcja ratunkowa

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

Aby ją skonfigurować, przejdź do opcji **System > Bezpieczeństwo >** Interfejs **akcji ratunkowych**.



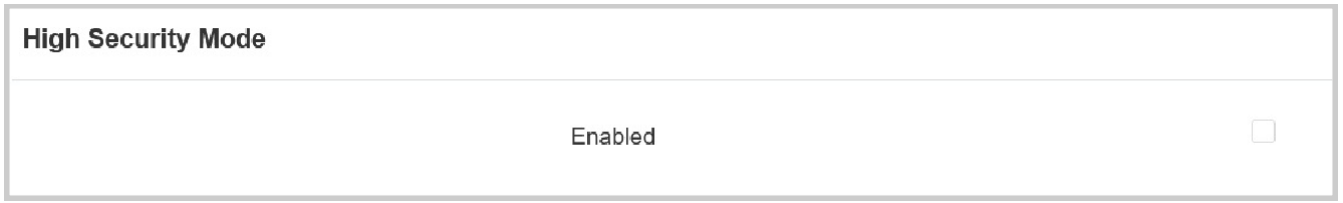
Interfejs sieciowy Automatyczne wylogowanie

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

Aby ją skonfigurować, przejdź do **System > Bezpieczeństwo >** Interfejs **limitu czasu sesji**.

Tryb wysokiego bezpieczeństwa

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

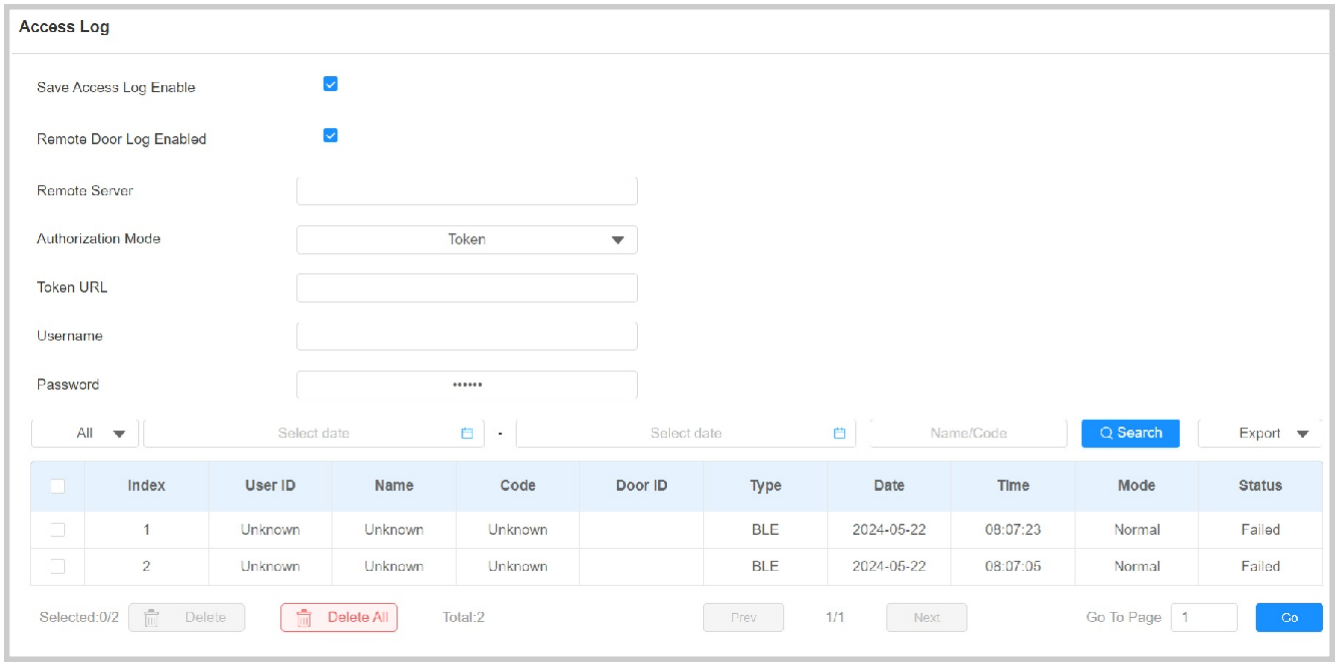


Tryb wysokiego bezpieczeństwa został zaprojektowany w celu zwiększenia bezpieczeństwa. Wykorzystuje on szyfrowanie w różnych aspektach, w tym w procesie komunikacji, poleceniach otwierania drzwi, metodach przechowywania haseł i nie tylko.

Dzienniki

Dziennik dostępu

Dzienniki drzwi można przeszukiwać i sprawdzać w interfejsie internetowym urządzenia **Status > Access Log.**



- **Save Access Log Enable (Włącz zapisywanie dziennika dostępu**): Określa, czy zapisywane mają być rekordy otwarcia drzwi.

- **Remote Door Log Enabled (Włączony zdalny dziennik** drzwi): Określa, czy dziennik drzwi ma być wysyłany do serwera innej firmy.

- **Serwer zdalny**: Wprowadź adres serwera zdalnego.

- **Tryb autoryzacji** : Wybierz spośród **None, Basic, Digest** i **Token**.

    - **Podstawowe**: wymagane jest wprowadzenie nazwy użytkownika i hasła w celu uwierzytelnienia.

    - **Token**: Wymagane jest wprowadzenie adresu URL tokena, nazwy użytkownika i hasła w celu uwierzytelnienia.

- **Status**: opcje **Success (sukces**) i **Failed (niepowodzenie**) oznaczają odpowiednio udany dostęp do drzwi i nieudany dostęp do drzwi.

- **Czas**: Wybierz konkretny okres dzienników drzwi, który chcesz przeszukać, sprawdzić lub wyeksportować.

- **Nazwa/Kod** : Przeszukuj dziennik według nazwy użytkownika lub kodu PIN.

- **ID drzwi**: Wyświetla nazwę drzwi.

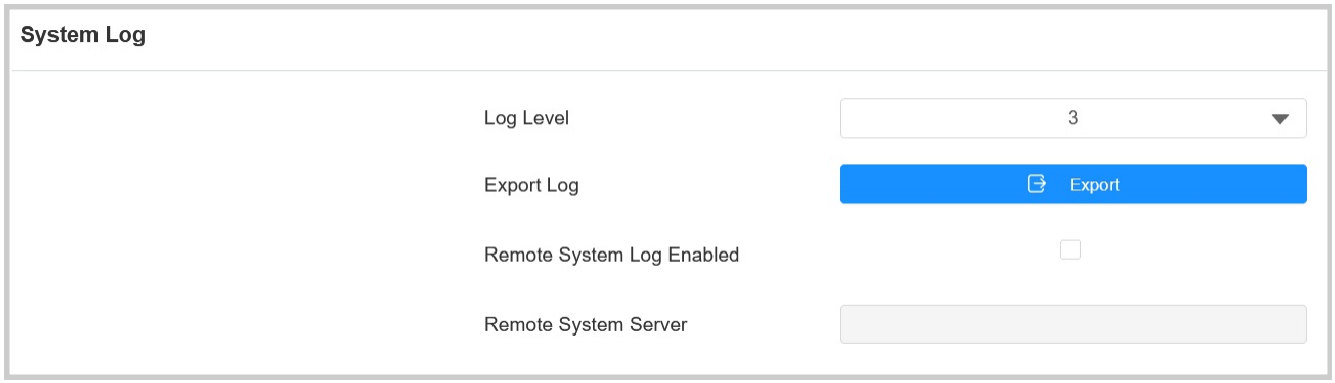
- **Typ** : Wyświetla typ dostępu, np. karta.

Debugowanie

Dziennik systemowy do debugowania

Dzienniki systemowe mogą być wykorzystywane do celów debugowania.

Aby ją skonfigurować, przejdź do opcji **System > Konserwacja >** Interfejs **dziennika systemowego**.

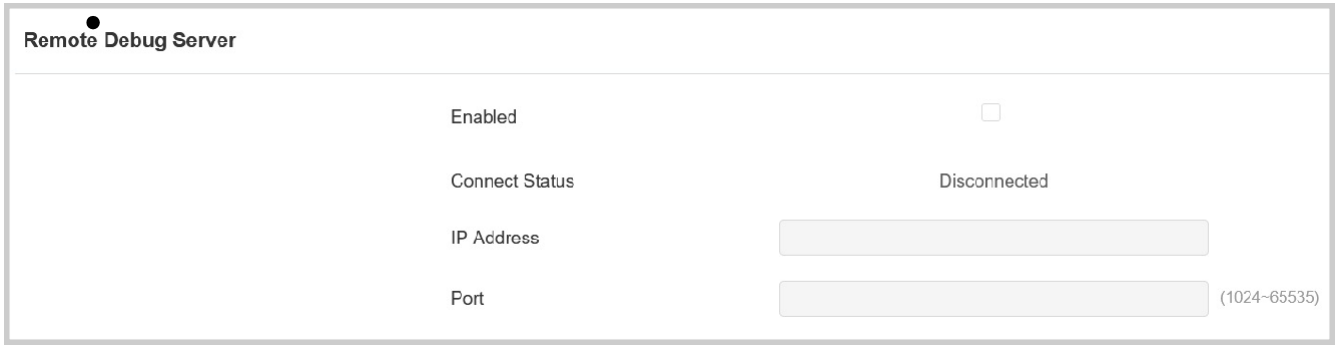


- **Poziom dziennika**: Poziomy dziennika wahają się od 1 do 7. Zostaniesz poinstruowany przez personel techniczny Akuvox o konkretnym poziomie dziennika, który należy wprowadzić do celów debugowania. Domyślny poziom dziennika to 3. Im wyższy poziom, tym bardziej kompletny jest dziennik.
- **Eksportuj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

Aby ją skonfigurować, przejdź do **System > Konserwacja >** Interfejs **serwera zdalnego debugowania**.



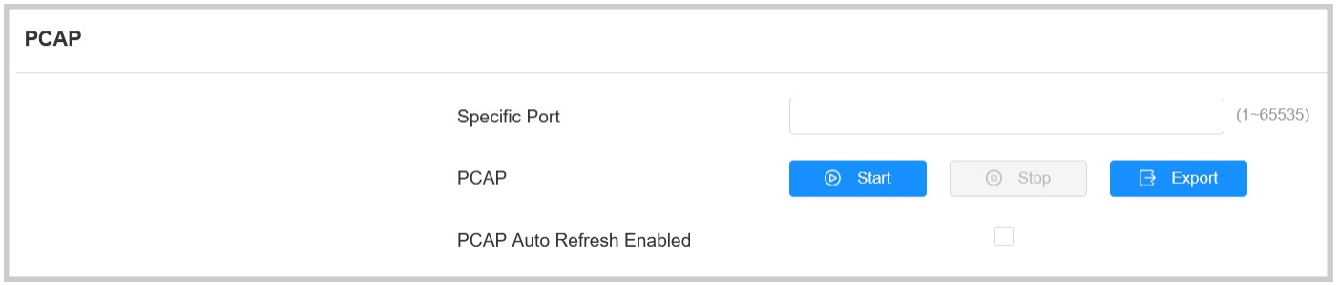
Connect Status: Wyświetla stan połączenia ze zdalnym serwerem debugowania.

- **Adres IP**: Ustaw adres IP zdalnego serwera debugowania. Zapytaj zespół techniczny Akuvox o adres IP serwera.
- **Port**: Ustawia port zdalnego serwera debugowania.

PCAP do debugowania

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

Aby ją skonfigurować, przejdź do **System > Konserwacja >** Interfejs **PCAP**.



- **Określony port**: Wybierz określone porty z zakresu 1-65535, aby można było przechwytywać tylko pakiety danych z określonego portu. Domyślnie pole to może pozostać puste.
- **PCAP**: Kliknij kartę **Start** i **Stop**, aby przechwycić określony zakres pakietów danych przed kliknięciem karty **Eksport**, aby wyeksportować pakiety danych do lokalnego komputera.
- **PCAP Auto Refresh Enabled**: Po włączeniu tej opcji, PCAP będzie kontynuował przechwytywanie pakietów danych nawet po osiągnięciu przez nie maksymalnej pojemności 50M. Po wyłączeniu, PCAP zatrzyma przechwytywanie pakietów danych, gdy przechwycone pakiety danych osiągną maksymalną pojemność 1 MB.

Kopia zapasowa

Zaszyfrowane pliki konfiguracyjne można importować lub eksportować do lokalnego komputera w celu utworzenia kopii zapasowej. Przejdź do interfejsu **System > Maintenance > Others**.

Aktualizacja oprogramowania sprzętowego

Urządzenia Akuvox można aktualizować w interfejsie internetowym urządzenia. Aby zaktualizować urządzenie, przejdź do opcji **System >** Interfejs **aktualizacji**.

Uwaga

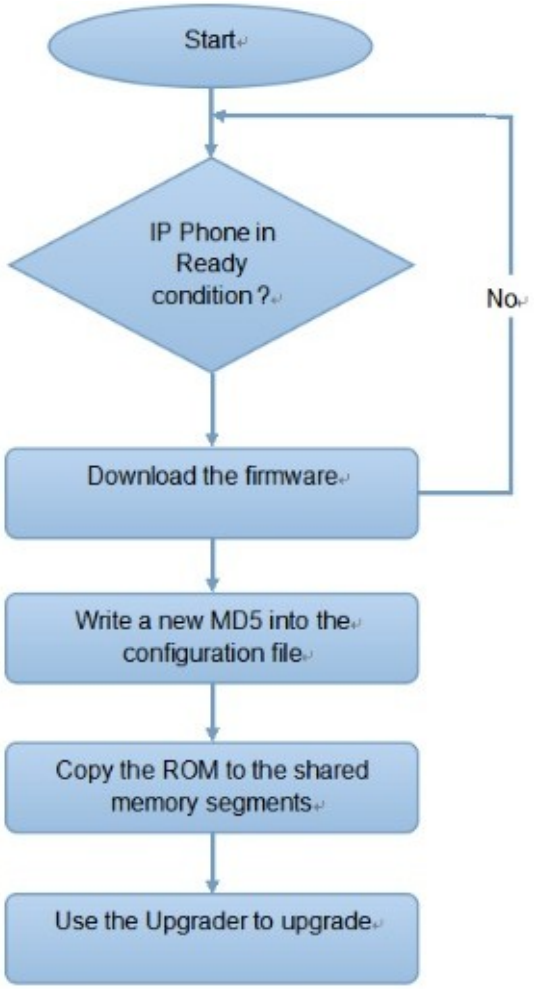
Plik powinien być w formacie .rom.

Automatyczne przydzielanie za pomocą pliku konfiguracyjnego

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:



Wprowadzenie do plików konfiguracyjnych automatycznego przydzielania uprawnień

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

Różnica między tymi dwoma typami konfiguracji jest niewielka:

- **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. Na przykład cfg.
- **Udostępnianie konfiguracji opartej na MAC**: Pliki konfiguracyjne oparte na MAC są używane do automatycznego udostępniania na określonym urządzeniu, zgodnie z jego unikalnym numerem MAC. Pliki konfiguracyjne nazwane za pomocą numeru MAC urządzenia zostaną automatycznie dopasowane do numeru MAC urządzenia przed pobraniem w celu udostępnienia na określonym urządzeniu.

Uwaga

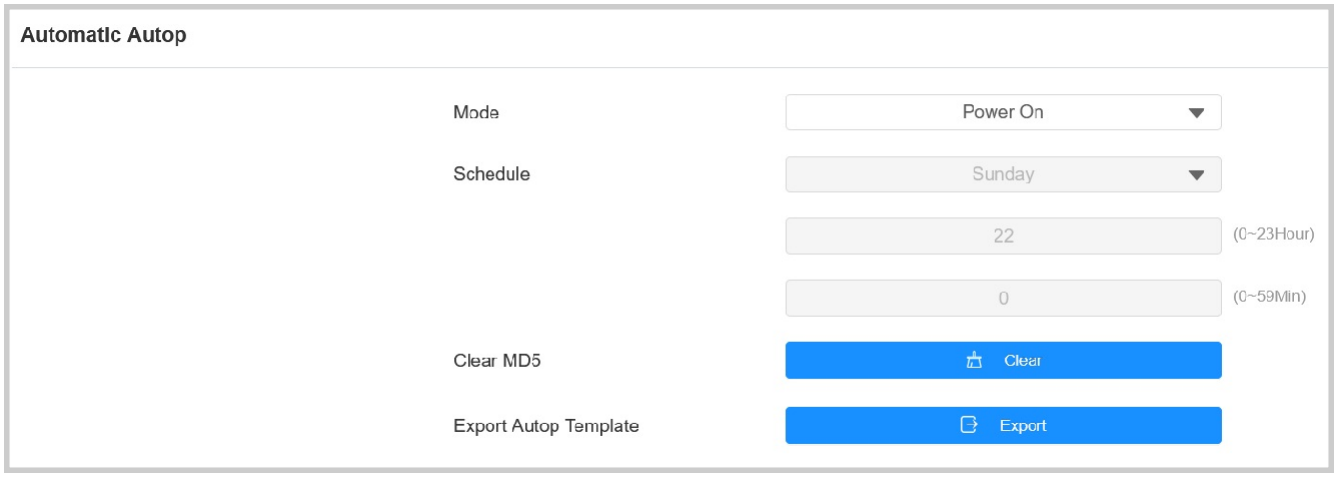
- Plik konfiguracyjny powinien być w formacie CFG.
- Ogólny plik konfiguracyjny udostępniania wsadowego różni się w zależności od modelu.
- Plik konfiguracyjny oparty na adresie MAC dla określonego udostępniania urządzenia jest nazywany jego adresem MAC.
- Jeśli serwer posiada te dwa typy plików konfiguracyjnych,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

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

Harmonogram Autop

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

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



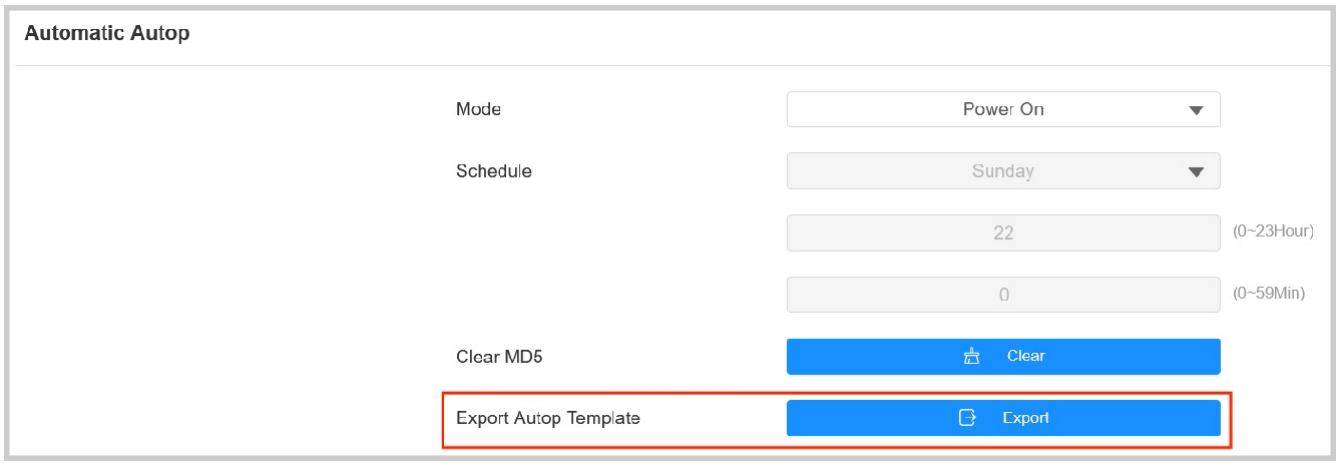
- **Tryb** :
  - **Power On**: Urządzenie wykona Autop przy każdym uruchomieniu.
  - **Wielokrotnie**: Urządzenie wykona funkcję Autop zgodnie z ustawionym harmonogramem.
  - **Power On + Repeatedly**: Połączenie trybu **Power On** i trybu **Repeatedly**, które umożliwi urządzeniu wykonywanie funkcji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

Udostępnianie statyczne

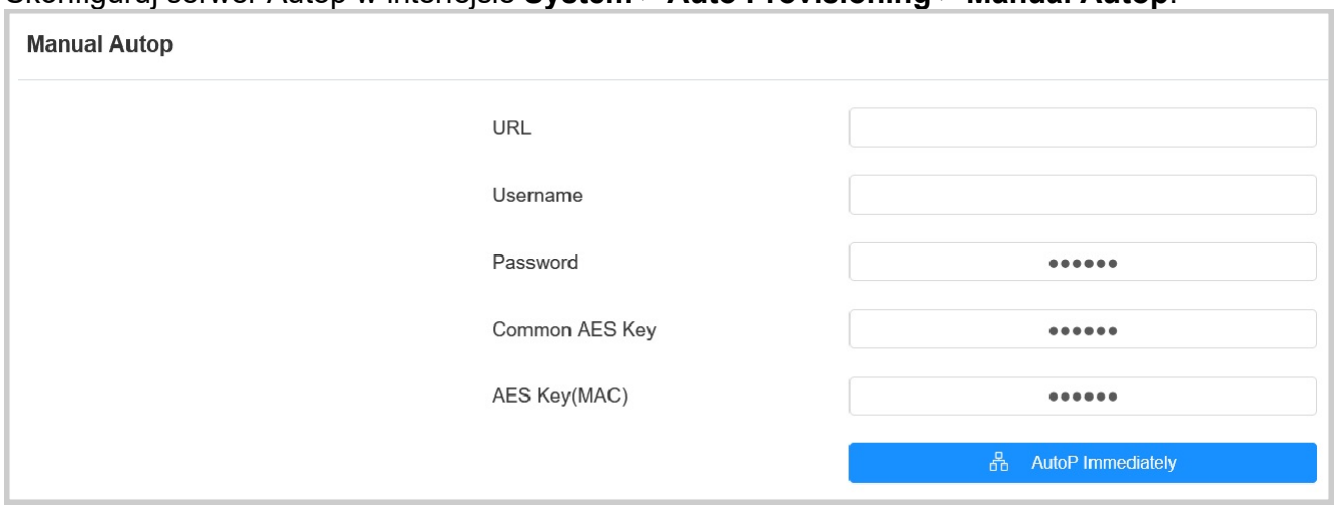
Można ręcznie skonfigurować określony adres URL serwera w celu pobrania oprogramowania sprzętowego lub pliku konfiguracyjnego. Jeśli skonfigurowano harmonogram automatycznego dostarczania, urządzenie wykona automatyczne dostarczanie w określonym czasie zgodnie z ustawionym harmonogramem automatycznego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

Aby ją skonfigurować, należy najpierw pobrać szablon w menu **System > Auto Provisioning >**

Automatic Autop.



Skonfiguruj serwer Autop w interfejsie **System > Auto Provisioning > Manual Autop**.



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

Uwaga

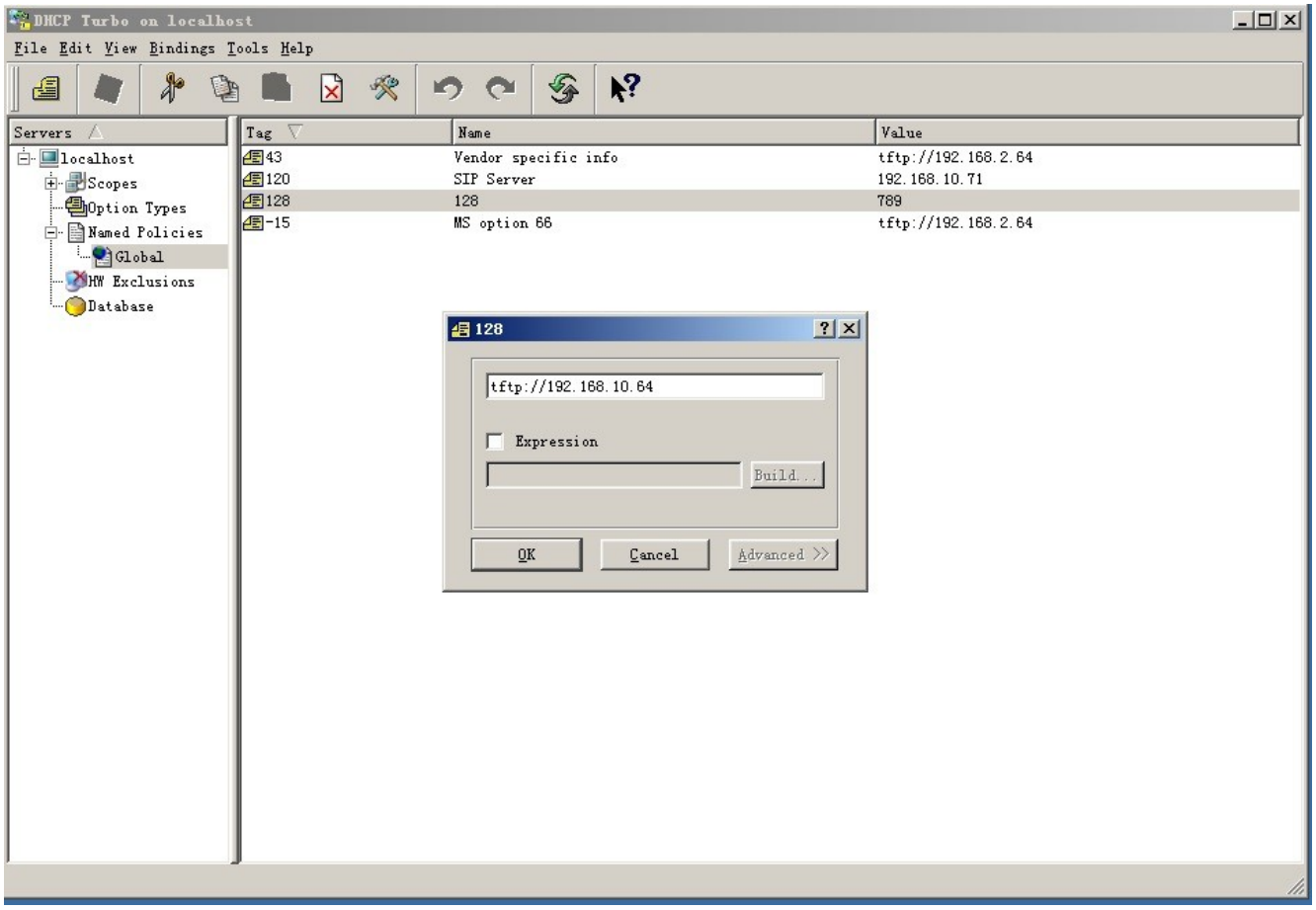
- AES jako jeden z typów szyfrowania powinien być skonfigurowany tylko wtedy, gdy plik konfiguracyjny jest zaszyfrowany za pomocą AES.Format adresu serwera:
- TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(umożliwia anonimowe logowanie)
  - ftp://username:password@192.168.0.19/(wymaga nazwy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

Wskazówka

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

Udostępnianie DHCP

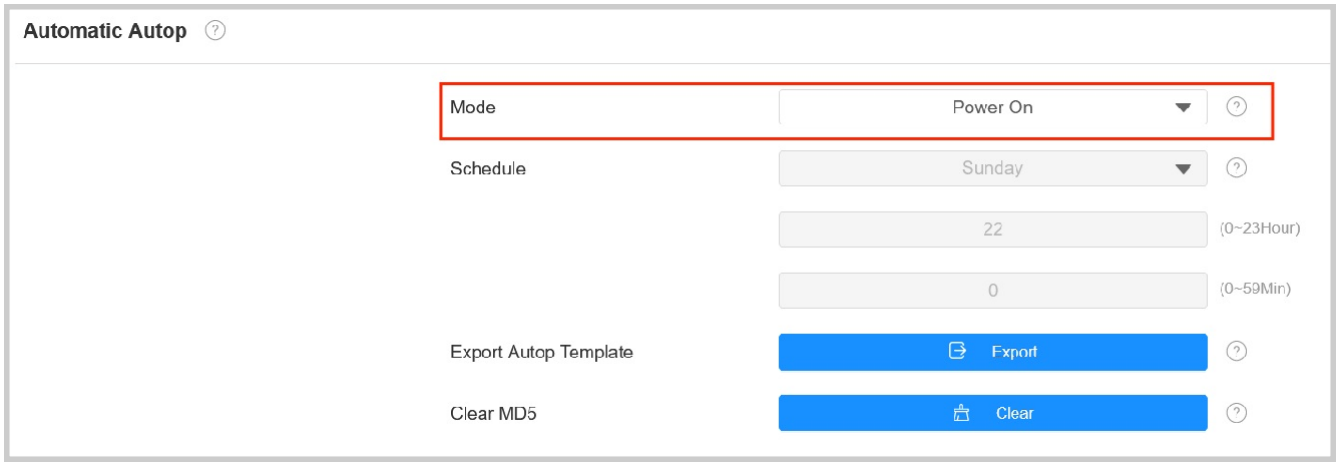
Adres URL automatycznego dostarczania można również uzyskać za pomocą opcji DHCP, która umożliwia urządzeniu wysłanie żądania do serwera DHCP dla określonego kodu opcji DHCP. Jeśli chcesz użyć
Opcja nie**standardowa** zdefiniowana przez użytkowników z kodami opcji w zakresie 128-255), należy skonfigurować 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**, przejdź do interfejsu **System > Auto Provisioning > Automatic Autop**.



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

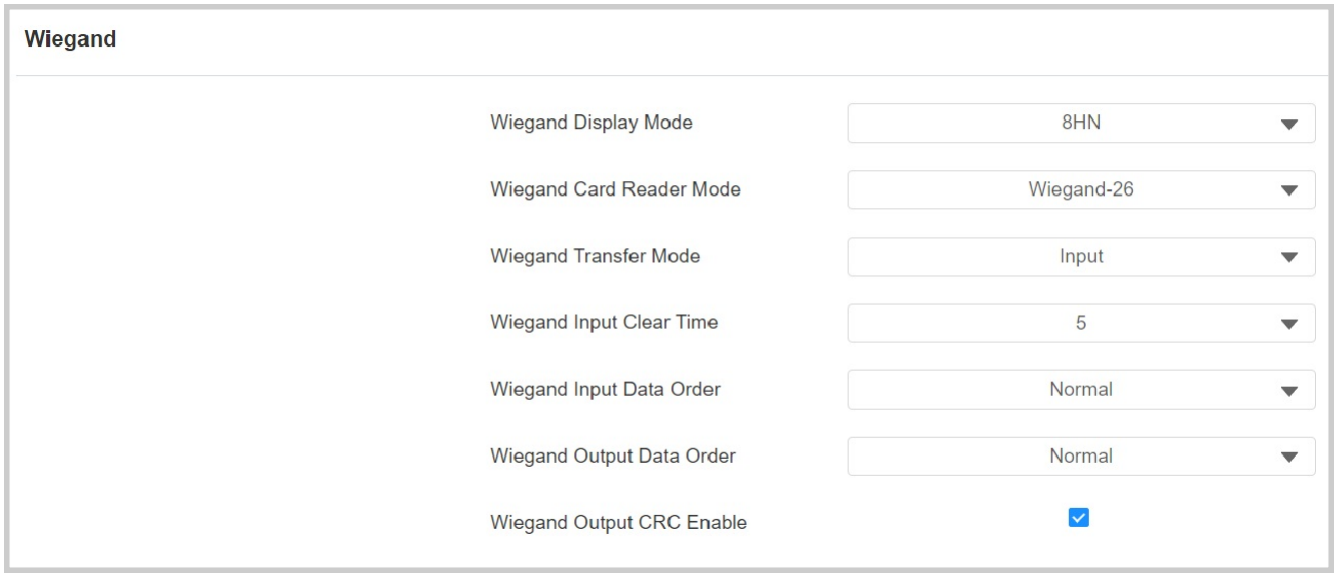
- **Opcja niestandardowa**: Wprowadź kod DHCP pasujący do odpowiedniego adresu URL, aby urządzenie znalazło serwer plików konfiguracyjnych w celu konfiguracji lub aktualizacji.
- **Opcja 43 DHCP**: Jeśli urządzenie nie otrzyma adresu URL z Opcji 66 DHCP, automatycznie użyje Opcji 43 DHCP. Odbywa się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

Integracja z urządzeniami innych firm

Integracja przez Wiegand

Terminal kontroli dostępu można zintegrować z urządzeniami innych firm za pośrednictwem Wiegand.

Aby go skonfigurować, przejdź do opcji **Urządzenie >** Interfejs **Wiegand**.



- **Tryb wyświetlania Wiegand** : Wybierz format kodu karty Wiegand spośród dostępnych opcji.
- **Tryb czytnika kart Wiegand**: Format transmisji powinien być identyczny między terminalem kontroli dostępu a urządzeniem innej firmy. Jest on konfigurowany automatycznie.
- **Tryb transferu Wiegand** :
    - **Wejście**: Urządzenie służy jako odbiornik.
    - **Wyjście**: Urządzenie służy jako nadajnik.
- **Wiegand Input Clear Time**: Gdy interwał wprowadzania haseł przekroczy ten czas. Wszystkie wprowadzone hasła zostaną usunięte.
- **Kolejność danych wejściowych Wiegand**: Ustawienie kolejności danych wejściowych Wiegand pomiędzy Normal i Reversed. W przypadku wybrania opcji Reversed numer karty wejściowej zostanie odwrócony.
- **Kolejność danych wyjściowych Wiegand:** Określa kolejność numeru karty.

  Normalnie: Numer karty jest wyświetlany w takiej postaci, w jakiej został odebrany.

Odwrócona: Kolejność numerów kart jest odwrócona.

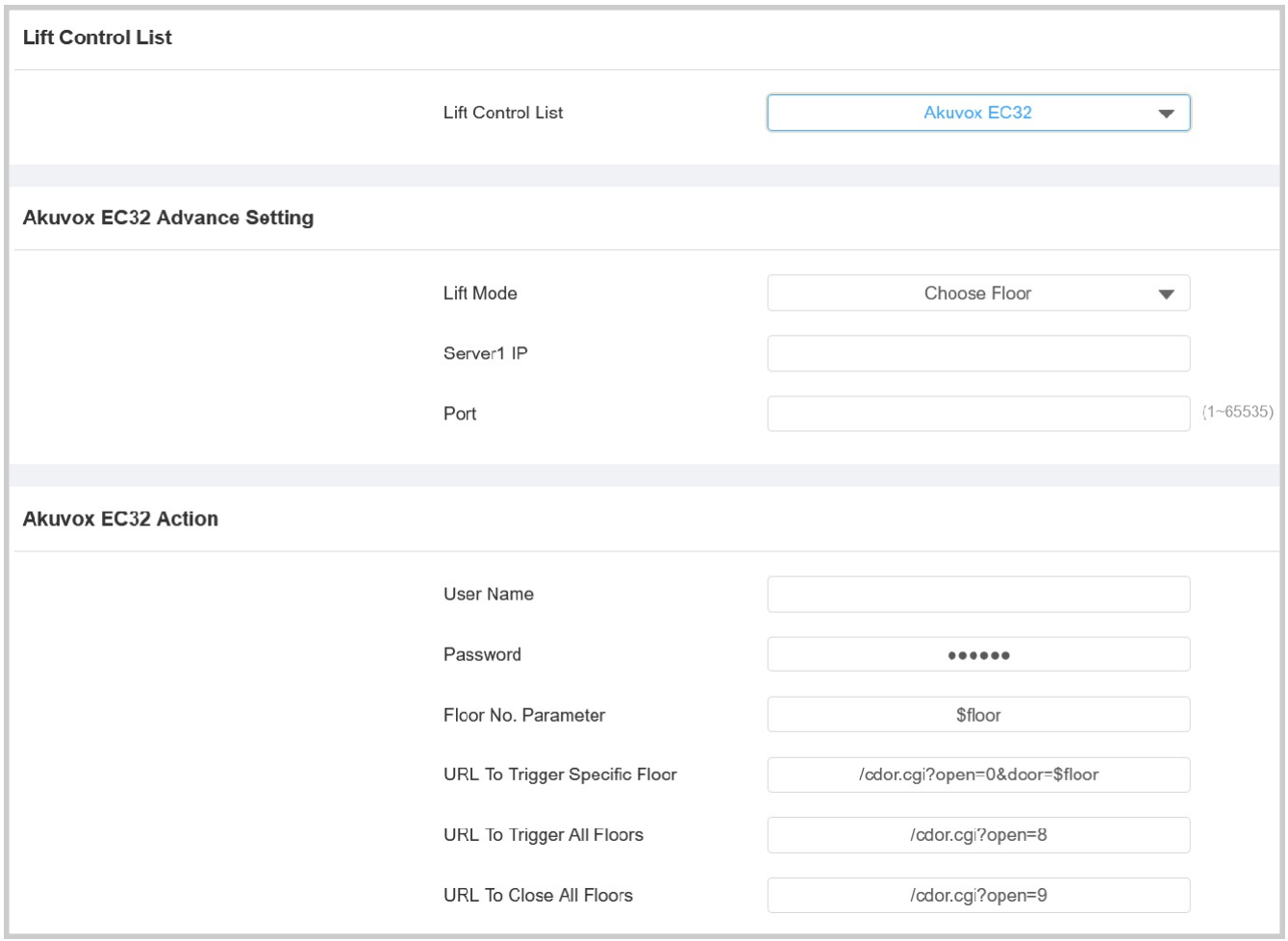
- Wiegand **Output CRC Enable**: Jest domyślnie włączona dla kontroli danych Wiegand. Wyłączenie go może prowadzić do niepowodzenia integracji z urządzeniami innych firm.

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

Kontrola podnoszenia

Urządzenie można podłączyć do sterownika windy Akuvox w celu sterowania windą. Możesz wezwać windę, aby zjechała na parter, gdy uzyskasz dostęp za pomocą różnych metod dostępu.

Aby skonfigurować sterowanie windą, przejdź do interfejsu **Device > Lift Control**.



- **Lista sterowania windą**: Wybierz Akuvox w celu integracji z kontrolerem windy Akuvox.

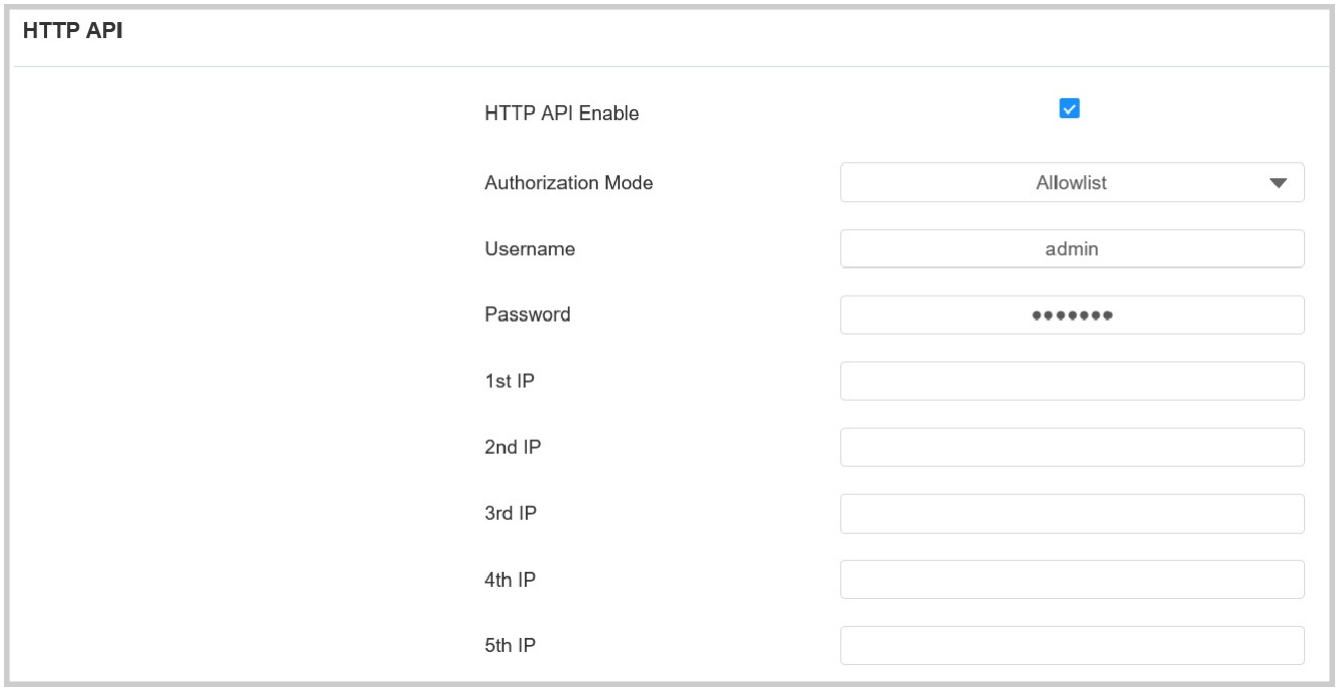
- **IP serwera**: Wprowadź adres IP serwera kontrolera windy Akuvox.
- **Port**: Wprowadź port serwera kontrolera windy Akuvox.

- **Nazwa użytkownika**: Wprowadź nazwę użytkownika kontrolera windy w celu uwierzytelnienia.
- **Hasło** : Wprowadź hasło kontrolera windy w celu uwierzytelnienia.
- **Floor NO. Parametr**: Wprowadź parametr Floor number dostarczony przez Akuvox.
- **URL To Trigger Specific Floor**: Wprowadź adres URL, aby wyzwolić określone piętro.
- **URL do wyzwalania wszystkich pięter** : Wprowadź adres URL do wyzwalania wszystkich pięter.
- **URL do zamknięcia wszystkich pięter** : Wprowadź adres URL używany do zamykania wszystkich pięter.

Integracja przez HTTP API

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

Aby go skonfigurować, przejdź do **Ustawienia >** Interfejs **API HTTP**.



- **HTTP API Enable** : Włącz lub wyłącz funkcję HTTP API dla integracji z innymi firmami. Jeśli funkcja jest wyłączona, każde żądanie zainicjowania integracji zostanie odrzucone i zwróci status HTTP 403 forbidden.

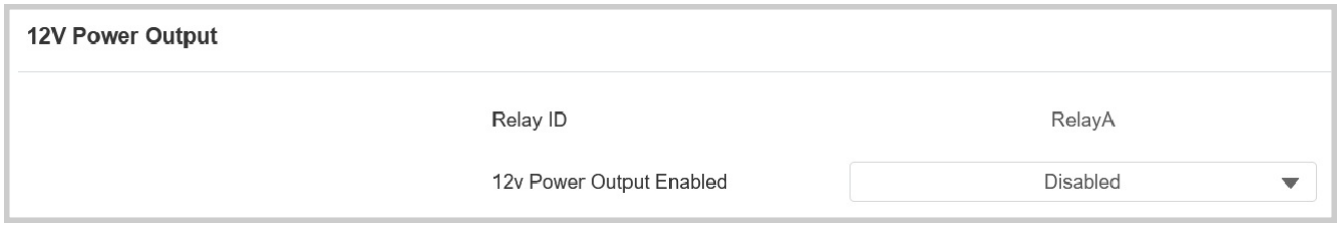
- **Tryb autoryzacji** : Wybierz jedną z następujących opcji: None, Allowlist, Basic, Digest i Token dla typu autoryzacji, które zostaną szczegółowo wyjaśnione w poniższej tabeli.
- **Nazwa użytkownika**: Wprowadź nazwę użytkownika, gdy wybrany jest tryb autoryzacji **Basic** lub **Digest**. Domyślna 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	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.
3	Podstawowy	W przypadku wybrania 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.
4	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".
5	Token	Ten tryb jest używany wyłącznie przez programistów Akuvox.

Kontrola mocy wyjściowej

Urządzenie może służyć jako źródło zasilania dla zewnętrznych przekaźników. Aby je skonfigurować, przejdź do opcji **Kontrola dostępu >** Interfejs **przekaźnika**.



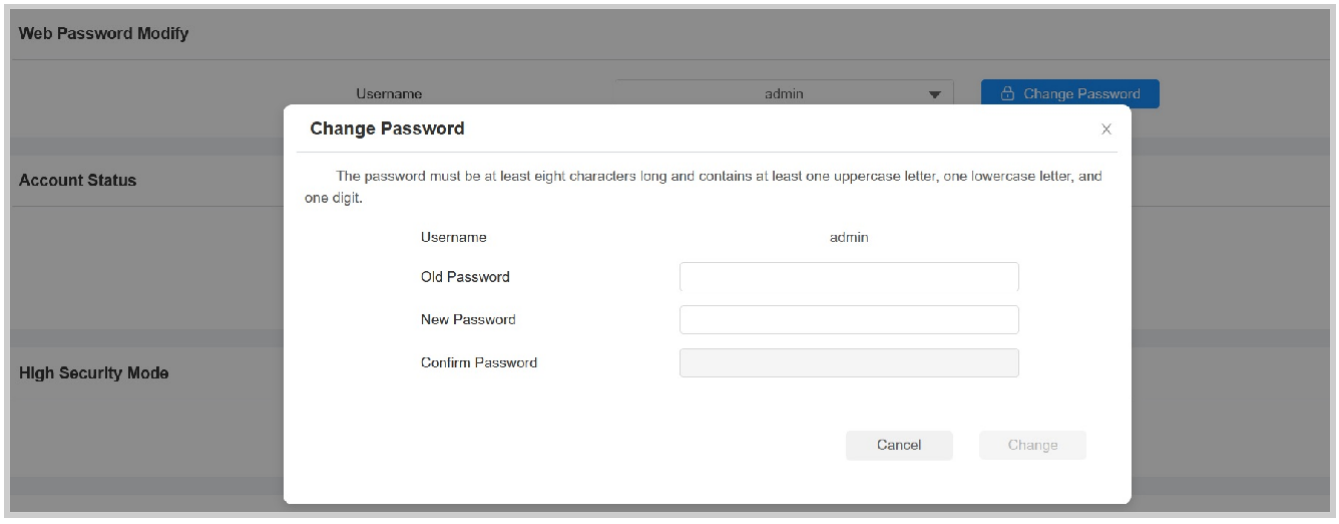
- **Włączone wyjście zasilania 12 V** :
    - **Zawsze** : Urządzenie może dostarczać ciągłe zasilanie do urządzenia innego producenta.

Przekaźnik bezpieczeństwa A: Urządzenie może współpracować z przekaźnikiem bezpieczeństwa.

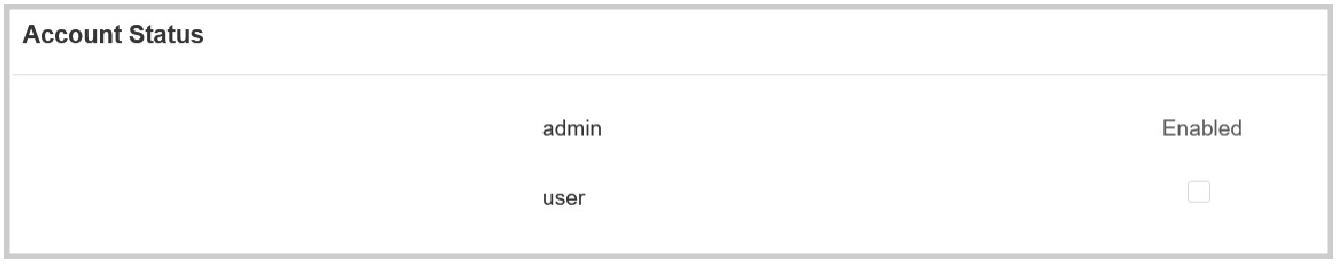
Modyfikacja hasła

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

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



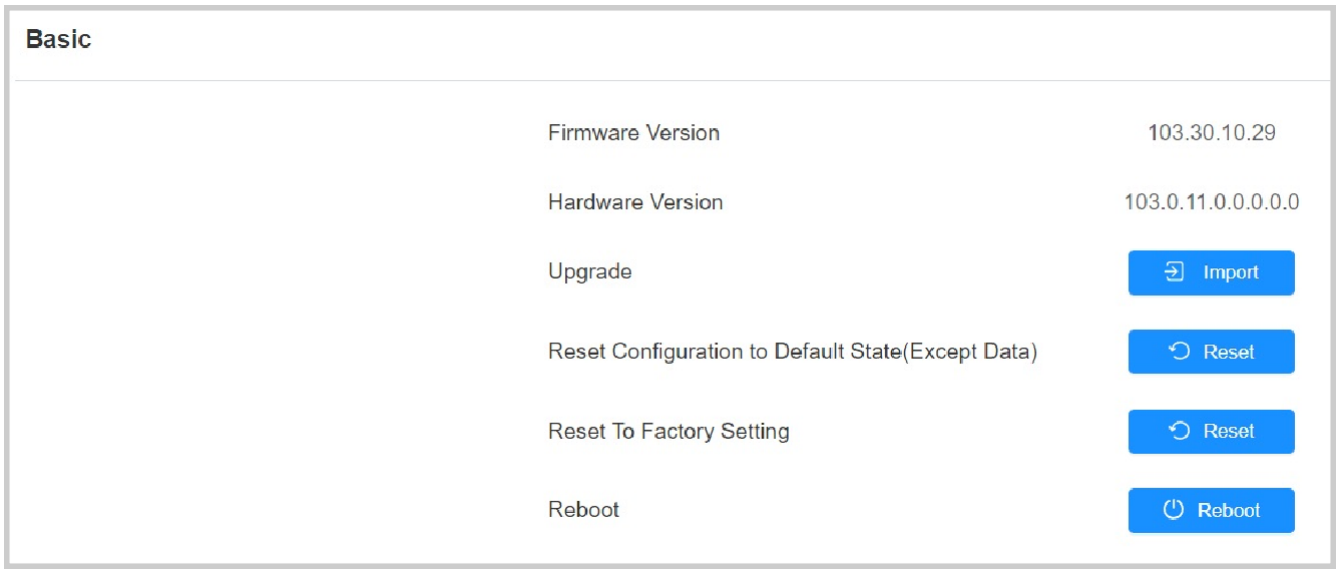
Aby włączyć lub wyłączyć konto użytkownika, przewiń do sekcji **Stan konta**.



Ponowne uruchamianie i resetowanie systemu

Reboot

Uruchom ponownie urządzenie w interfejsie **System > Aktualizacja.**

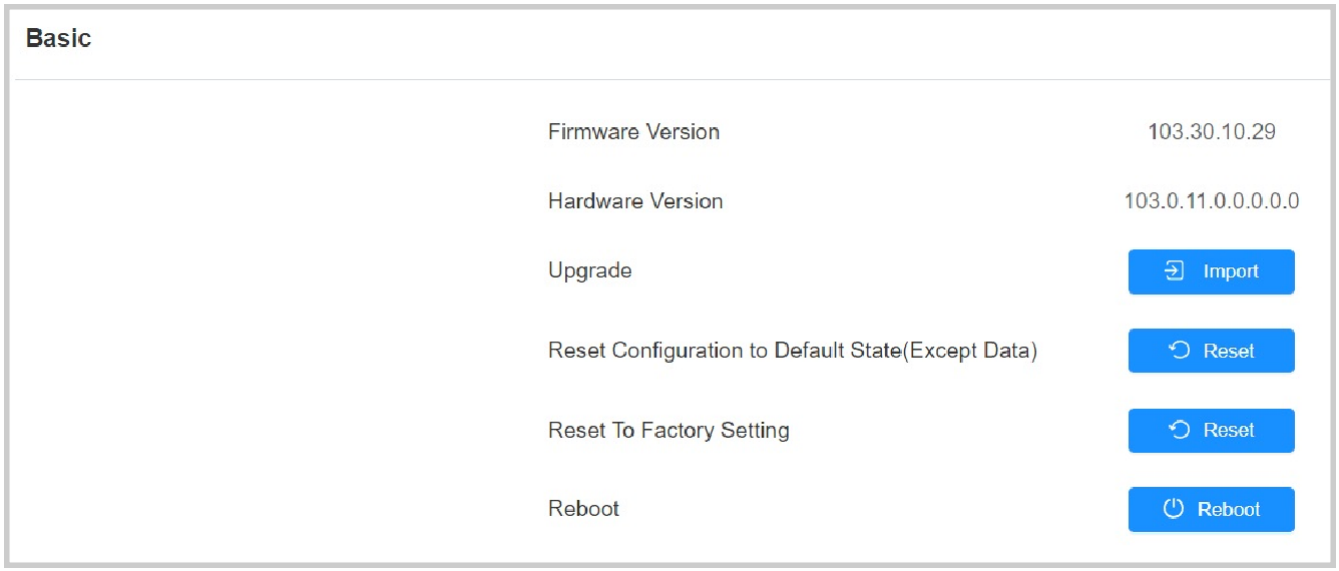


Aby skonfigurować harmonogram ponownego uruchamiania urządzenia, przejdź do interfejsu **System > Auto Provisioning > Reboot Schedule**.

Reset

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

Zresetuj urządzenie w interfejsie **System > Aktualizacja**.



Urządzenie można również zresetować, naciskając i przytrzymując przycisk **Reset** z tyłu urządzenia.