Stacja drzwiowa willi

Instrukcja obsługi

Wersja 1.0.1

Przedmowa

Ogólny

Niniejsza instrukcja przedstawia na stronie internetowej sposób konfiguracji domofonu willowego (zwanego dalej „VTO”).

Instrukcje bezpieczeństwa

W Podręczniku mogą pojawić się następujące skategoryzowane słowa sygnalizacyjne o określonym znaczeniu.

Hasła ostrzegawcze	Oznaczający
 **NIEBEZPIECZEŃSTWO**	Wskazuje na wysokie potencjalne zagrożenie, które, jeśli się nie uniknie, spowoduje śmierć lub poważne obrażenia.
 **OSTRZEŻENIE**	Wskazuje na średnie lub niskie potencjalne zagrożenie, które, jeśli się go nie uniknie, może spowodować lekkie lub umiarkowane obrażenia.
 **OSTROŻNOŚĆ**	Wskazuje potencjalne ryzyko, które, jeśli się go nie uniknie, może spowodować uszkodzenie mienia, utratę danych, zmniejszenie wydajności lub nieprzewidywalne skutki.
 **PORADY**	Zawiera metody, które pomogą Ci rozwiązać problem lub zaoszczędzić czas.
 **NOTATKA**	Zawiera dodatkowe informacje jako uzupełnienie tekstu.

Historia zmian

Wersja	Treść wersji	Data wydania
Wersja 1.0.1	Zmieniono „Ważne zabezpieczenia i ostrzeżenia”.	Grudzień 2022
V1.0.0	Pierwsze wydanie.	Styczeń 2021

Informacja o ochronie prywatności

Jako użytkownik urządzenia lub administrator danych możesz zbierać dane osobowe innych osób, takie jak ich twarz, odciski palców i numery rejestracyjne. Musisz przestrzegać lokalnych przepisów i regulacji dotyczących ochrony prywatności, aby chronić uzasadnione prawa i interesy innych osób, wdrażając środki, które obejmują między innymi: Zapewnienie jasnej i widocznej identyfikacji w celu poinformowania ludzi o istnieniu obszaru nadzoru oraz podać wymagane dane kontaktowe.

O Podręczniku

- Instrukcja ma wyłącznie charakter informacyjny. W przypadku rozbieżności pomiędzy instrukcją a rzeczywistym produktem, rozstrzygający będzie rzeczywisty produkt.
- Nie ponosimy odpowiedzialności za jakiekolwiek straty spowodowane obsługą niezgodną z instrukcją. Podręcznik zostanie
- zaktualizowany zgodnie z najnowszymi przepisami i regulacjami obowiązującymi w powiązanych jurysdykcjach. Szczegółowe informacje można znaleźć w instrukcji papierowej, płycie CD-ROM, kodzie QR lub w naszej instrukcji

oficjalna strona internetowa. W przypadku rozbieżności pomiędzy instrukcją papierową a wersją elektroniczną, rozstrzygająca będzie wersja elektroniczna.

- Wszystkie projekty i oprogramowanie mogą ulec zmianie bez uprzedniego pisemnego powiadomienia. Aktualizacje produktu mogą powodować pewne różnice pomiędzy rzeczywistym produktem a instrukcją. Aby uzyskać najnowszy program i dodatkową dokumentację, prosimy o kontakt z obsługą klienta.
- Nadal mogą występować odchylenia w danych technicznych, opisach funkcji i operacji lub błędy w druku. W przypadku jakichkolwiek wątpliwości lub sporów zastrzegamy sobie prawo do ostatecznych wyjaśnień.
- Zaktualizuj oprogramowanie czytnika lub wypróbuj inne popularne oprogramowanie czytnika, jeśli nie można otworzyć instrukcji (w formacie PDF).
- Wszystkie znaki towarowe, zastrzeżone znaki towarowe i nazwy firm zawarte w instrukcji są własnością odpowiednich właścicieli.
- Odwiedź naszą stronę internetową, skontaktuj się z dostawcą lub obsługą klienta, jeśli wystąpią jakiekolwiek problemy podczas korzystania z urządzenia.
- W przypadku jakichkolwiek wątpliwości lub kontrowersji zastrzegamy sobie prawo do ostatecznych wyjaśnień.

Ważne zabezpieczenia i ostrzeżenia

W tej sekcji przedstawiono treści dotyczące prawidłowego obchodzenia się z urządzeniem, zapobiegania zagrożeniom i zapobiegania uszkodzeniom mienia. Przeczytaj uważnie przed użyciem urządzenia i postępuj zgodnie z wytycznymi podczas jego użytkowania.

Wymagania operacyjne

- Przed użyciem sprawdź, czy zasilanie jest prawidłowe.
- Nie odłączaj przewodu zasilającego z boku urządzenia, gdy zasilacz jest włączony.
- Używaj urządzenia w znamionowym zakresie mocy wejściowej i wyjściowej.
- Transportuj, używaj i przechowuj urządzenie w dopuszczalnych warunkach wilgotności i temperatury.
- Jeżeli urządzenie nie było zasilane dłużej niż miesiąc, należy je umieścić w oryginalnym opakowaniu i uszczelnione. Trzymaj go z dala od wilgoci i przechowuj w pomieszczeniu o dopuszczalnej wilgotności warunki temperaturowe.
- Nie upuszczaj ani nie rozpryskuj płynu na urządzenie i upewnij się, że na urządzeniu nie znajduje się żaden przedmiot wypełniony płynem, aby zapobiec przedostaniu się płynu do środka.
- Nie demontuj urządzenia bez fachowego poinstruowania.

Wymagania instalacyjne

- Nie podłączaj zasilacza do urządzenia, gdy zasilacz jest włączony.
- Należy ściśle przestrzegać lokalnych przepisów i norm dotyczących bezpieczeństwa elektrycznego. Upewnij się, że napięcie otoczenia jest stabilne i spełnia wymagania zasilania urządzenia.
- Nie podłączaj urządzenia do dwóch lub więcej rodzajów źródeł zasilania, aby uniknąć uszkodzenia urządzenia.
- Niewłaściwe użycie akumulatora może spowodować pożar lub eksplozję.

- Personel pracujący na wysokościach musi podjąć wszelkie niezbędne środki w celu zapewnienia bezpieczeństwa osobistego, w tym nosić kask i pasy bezpieczeństwa.
- Nie należy umieszczać urządzenia w miejscu narażonym na działanie promieni słonecznych lub w pobliżu źródeł ciepła.
- Trzymaj urządzenie z dala od wilgoci, kurzu i sadzy.
- Zamontuj urządzenie na stabilnej powierzchni, aby zapobiec jego upadkowi.
- Urządzenie należy instalować w dobrze wentylowanym miejscu i nie blokować jego wentylacji.
- Użyj zasilacza lub zasilacza szafkowego dostarczonego przez producenta.
- Należy używać przewodów zasilających zalecanych dla danego regionu i zgodnych ze specyfikacją mocy znamionowej.
- Zasilanie musi spełniać wymagania ES1 w normie IEC 62368-1 i nie być wyższe niż PS2. Należy pamiętać, że wymagania dotyczące zasilania są podane na etykiecie urządzenia.
- Urządzenie jest urządzeniem elektrycznym klasy I. Należy upewnić się, że zasilanie urządzenia jest podłączone do gniazdka elektrycznego z uziemieniem ochronnym.

Spis treści

1 Inicjowanie VTO

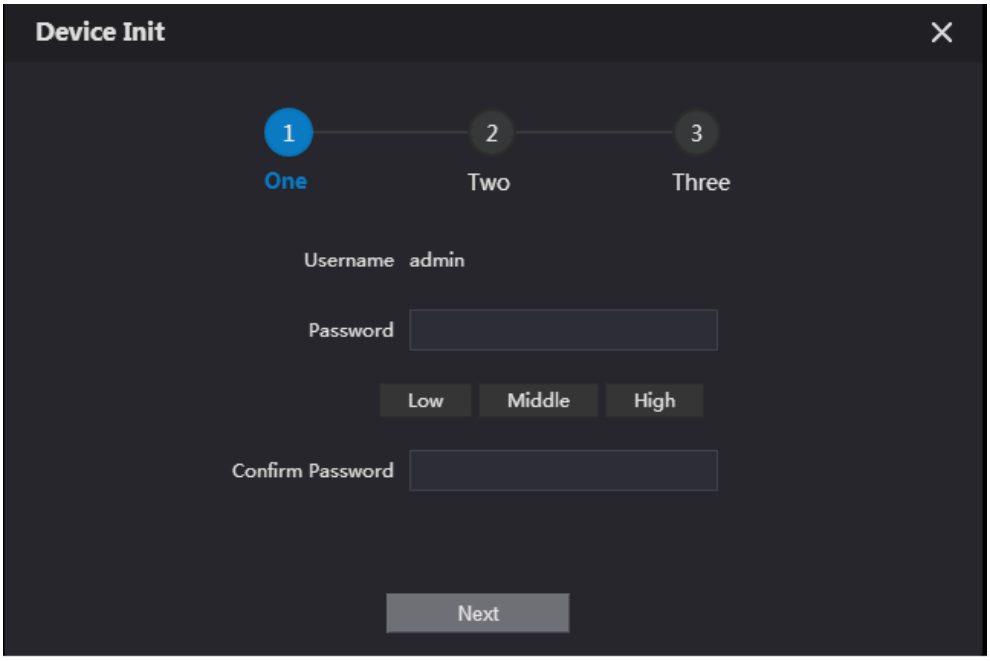
Przy pierwszym logowaniu lub po zresetowaniu VTO należy je zainicjować na stronie internetowej.

Step 1 Włącz VTO.

Step 2 Przejdź do domyślnego adresu IP (192.168.1.108) VTO.

Upewnij się, że adres IP Twojego komputera znajduje się w tym samym segmencie sieci, co VTO.

Figure 1-1 Inicjalizacja urządzenia



Step 3 Wprowadź i potwierdź hasło, a następnie kliknij**Następny**.

Step 4 Wprowadź adres e-mail, aby zresetować hasło.

Step 5 Kliknij**Następny**, a następnie kliknij**OK**.

2 Logowanie i resetowanie hasła

2.1 Zaloguj sie

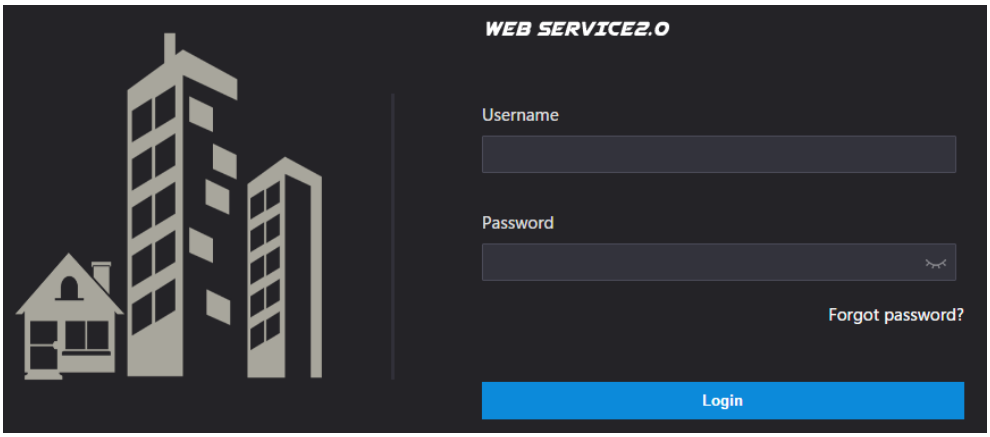
Przed zalogowaniem upewnij się, że komputer PC znajduje się w tym samym segmencie sieci co VTO.

Step 1 Przejdź do adresu IP VTO w przeglądarce.

Przy pierwszym logowaniu wprowadź domyślny adres IP (192.168.1.108). Jeśli masz wiele VTO, my zalecamy zmianę domyślnego adresu IP (**Sieć > Podstawowe**), aby uniknąć konfliktu.

Step 2 Wpisz „admin” jako nazwę użytkownika i hasło ustawione podczas inicjalizacji, a następnie kliknij **Zaloguj sie**.

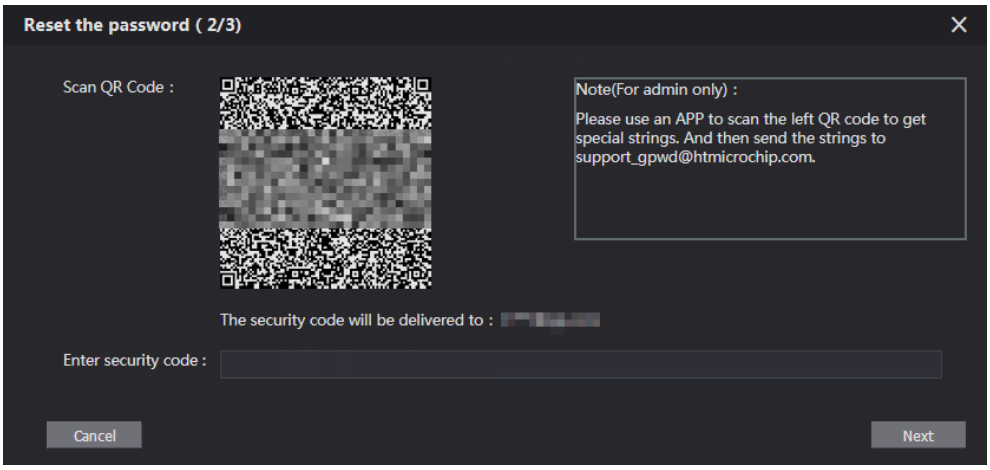
Figure 2-1 Zaloguj sie



2.2 Resetowanie hasła

Step 1 Na stronie logowania kliknij**Zapomniałeś hasła?**, a następnie kliknij**Następny**.

Figure 2-2 Zresetuj hasło



Step 2 Zeskanuj kod QR, a otrzymasz ciąg cyfr i liter.

Step 3 Wyślij ciąg znaków na adres e-mail: support_gpwd@htmicrochip.com , a następnie kod zabezpieczający zostanie wysłany na adres e-mail skonfigurowany podczas inicjalizacji.

Step 4 Wprowadź kod zabezpieczający w polu wejściowym, a następnie kliknij**Następny**.

- Jeśli podczas inicjalizacji nie ustawiłeś adresu e-mail, skontaktuj się ze swoim dostawcą lub obsługi klienta w celu uzyskania pomocy.
- Kod zabezpieczający będzie ważny tylko przez 24 godziny od otrzymania.
- Jeśli wpiszesz błędny kod zabezpieczający 5 razy z rzędu, Twoje konto zostanie zablokowane zablokowany na 5 minut.

Step 5 Wprowadź i potwierdź nowe hasło, a następnie kliknij**OK**.

3 Główny interfejs

Figure 3-1 Główny interfejs

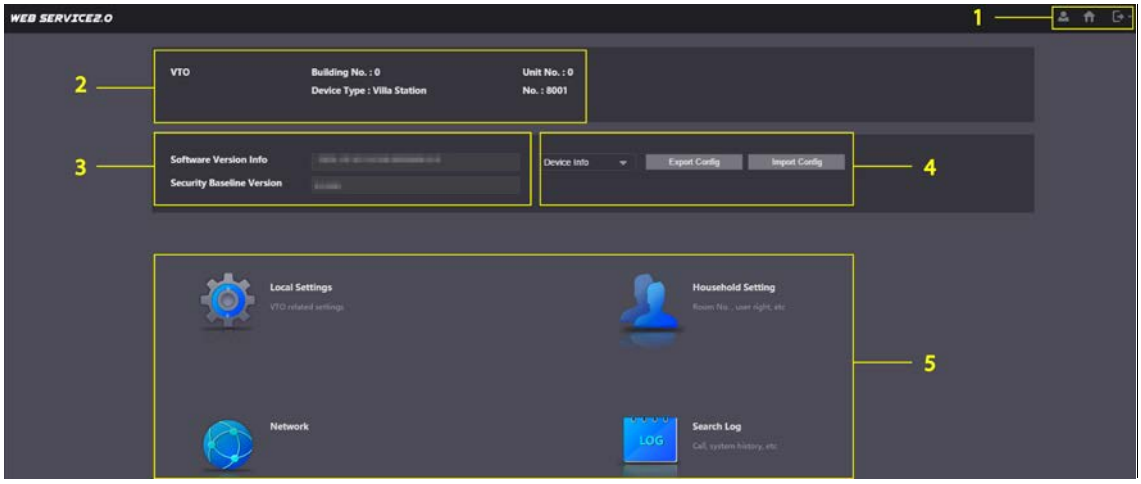


Tabela 3-1 Wprowadzenie do głównego interfejsu

NIE.	Funkcjonować	Opis
1	Funkcja ogólna	• : Zmień hasło i swój adres e-mail. • : Przejdź do głównego interfejsu. • : Wyloguj się, zrestartuj VTO lub przywróć VTO do ustawień fabrycznych. Jeśli przywrócisz VTO do ustawień fabrycznych, wszystkie dane z wyjątkiem pamięci zewnętrznej zostaną usunięte. Możesz sformatować kartę SD, aby usunąć zapisane na niej dane.
2	Informacje VTO	Wyświetl informacje o VTO i systemie.
3	Informacje o systemie	
4	Konfiguracja menedżer	Eksportuj lub importuj konfigurację VTO lub informacje o użytkowniku.
5	Funkcjonować	Skonfiguruj parametry dla różnych funkcji. Interfejs i funkcje mogą się różnić w zależności od modelu. Rzeczywisty produkt ma pierwszeństwo.

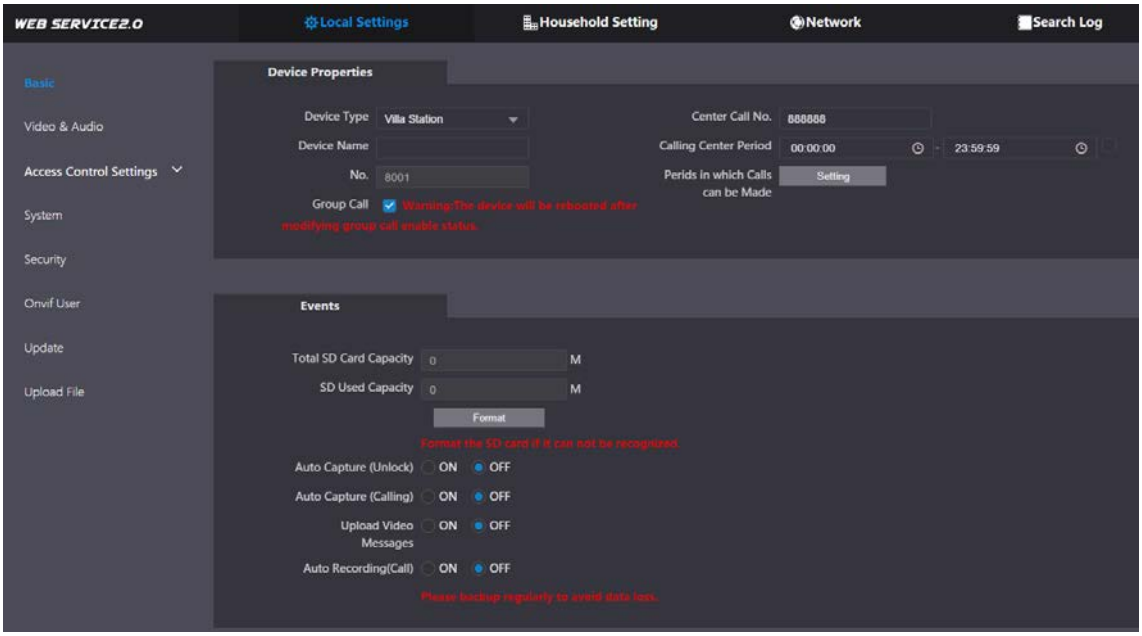
4 Ustawienia lokalne

W tym rozdziale przedstawiono szczegółową konfigurację VTO.

4.1 Podstawowy

Step 1 Wybierać**Ustawienia lokalne > Podstawowe**.

Figure 4-1 Podstawowy



Step 2 Skonfiguruj parametry.

Tabela 4-1 Podstawowy opis parametrów

Parametr	Opis
Rodzaj urządzenia	Wybierać**Stacja Willa**Lub**Mały apartament**w razie potrzeby.
Nr tel. centrum	Domyślny numer telefonu do centrum zarządzania to 888888, ale możesz go ustawić na dowolny numer składający się z maksymalnie 9 cyfr.
Nazwa urządzenia	Gdy inne urządzenia monitorują to VTO, nazwa urządzenia pojawi się na obrazie monitorowania.
Okres call center	Okres, w którym można zadzwonić do centrum zarządzania.
NIE.	Służy do rozróżnienia każdego VTO i zalecamy ustawienie go według numeru jednostki lub budynku, a następnie można dodać VTO do serwera SIP za pomocą ich numerów. Możesz zmienić numer VTO, gdy nie działa ono jako serwer SIP.
Okresy, w których można wykonywać połączenia	Skonfiguruj godzinę, jeśli chcesz odbierać połączenia tylko w określonym przedziale czasu.
Połączenie grupowe	Włącz tę opcję na VTO, które działa jako serwer SIP, a kiedy główny VTH odbierze połączenie, wszystkie VTH numery wewnętrzne również odbiorą połączenie.

Parametr	Opis
Całkowita karta SD Pojemność	Wyświetla całkowitą i wykorzystaną pojemność karty SD. Możesz kliknąć**Format** aby usunąć wszystkie dane z karty SD.
SD Używana pojemność	
Format	
Automatyczne przechwytywanie (Odblokować)	Po odblokowaniu drzwi VTO wykona dwa zdjęcia i zapisze je na karcie SD.
Automatyczne przechwytywanie (połączenia)	Zrób migawkę i zapisz ją na karcie SD VTO, gdy VTO dzwoni.
Prześlij wideo Wiadomości	Po włączeniu: ● Jeśli karta SD zostanie włożona zarówno do VTH, jak i VTO, wiadomość wideo zostanie zapisana zarówno na kartach SD VTH, jak i VTO. ● Jeśli karta SD zostanie włożona tylko do VTH lub VTO, wiadomość wideo zostanie zapisana tylko na karcie SD VTH lub VTO. ● Jeśli do VTH lub VTO nie zostanie włożona żadna karta SD, żadna wiadomość wideo nie zostanie zapisana.
Automatyczne nagrywanie (połączenie)	Nagrywaj, gdy VTO jest w trakcie rozmowy i zapisz nagranie na karcie SD VTO.

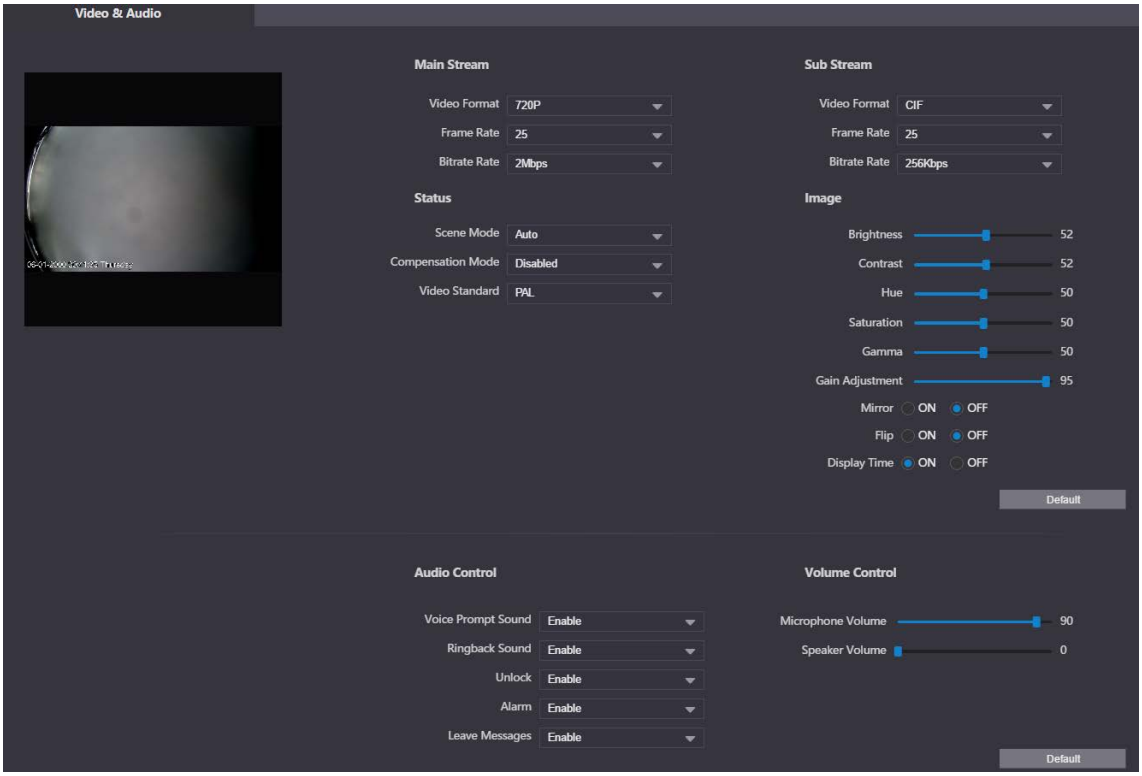
Step 3 Kliknij**Ratować**.

4.2 Wideo i dźwięk

Skonfiguruj format i jakość wideo oraz dźwięk VTO.

Step 1 Wybierać**Ustawienia lokalne > Wideo i audio**.

Figure 4-2 Wideo i dźwięk



Step 2 Skonfiguruj parametry, które zaczną obowiązywać po zmianie.

Tabela 4-2 Opis parametrów wideo

Parametr		Opis
Główny/podrzędny Strumień	Wideo Format	W razie potrzeby wybierz inną rozdzielczość: ● **1080p**: 1920 × 1080. ● **720P**: 1280 × 720. ● **WVGA**: 800 × 480. ● **QVGA**: 320 × 240. **D1**: ● 720 × 480. ● **CIF**: 352 × 288.
	Częstotliwość wyświetlania klatek	Im większa wartość, tym płynniejszy obraz wideo, ale wymaga to większej przepustowości.
	Szybkość transmisji	Im większa wartość, tym lepsza jakość wideo, ale wymaga to większej przepustowości.
Status	Tryb sceny	Wybierz w razie potrzeby, w zależności od warunków oświetlenia.**Automatyczny**jest zaznaczone domyślnie.
	Kompensacja w trybie	● **BLC**: Kompensacja światła tylnego. Popraw klarowność celu na obrazie. ● **WDR**: Szeroki zakres dynamiki. Zwiększ jasność ciemnych obszarów i zmniejsz jasność jasnych obszarów, aby poprawić ● obraz. **HLC**: Wysoka kompensacja światła. Zmniejsz jasność mocnych punktów, aby poprawić ogólny obraz.
	Wideo Standard	Wybierać**KUMPEL**Lub**NTSC**według Twojego obszaru. **KUMPEL**jest najczęściej używany w Chinach i Europie, oraz**NTSC**głównie w Stanach Zjednoczonych i Japonii.
Obraz	Jasność	Im większa wartość, tym jaśniejszy obraz.
	Kontrast	Większa wartość zapewnia większy kontrast pomiędzy jasnymi i ciemnymi obszarami.
	Odcień	Zmień kolor na jaśniejszy lub ciemniejszy. Wartość domyślna ustalana jest przez czujnik światła i zalecamy pozostawienie tej wartości domyślnej.
	Nasycenie	Im większa wartość, tym grubszy kolor.
	Gamma	Zmienia jasność obrazu i poprawia zakres dynamiki obrazu w sposób nieliniowy. Im większa wartość, tym jaśniejszy obraz.
	Osiągać Modyfikacja	Wzmocnij sygnał wideo, aby zwiększyć jasność obrazu. Jeśli wartość jest zbyt duża, na obrazie będzie więcej szumów.
	Lustro	Wyświetl obraz z odwróconą lewą i prawą stroną.
	Trzepnięcie	Wyświetl obraz do góry nogami.
	Czas wyświetlania	Wyświetla aktualną godzinę i datę na obrazie wideo.
Audio Kontrola	—	Włącz lub wyłącz każdy rodzaj dźwięku.
Tom Kontrola	Mikrofon Tom	Dostosuj głośność według potrzeb.
	Głośnik Tom	

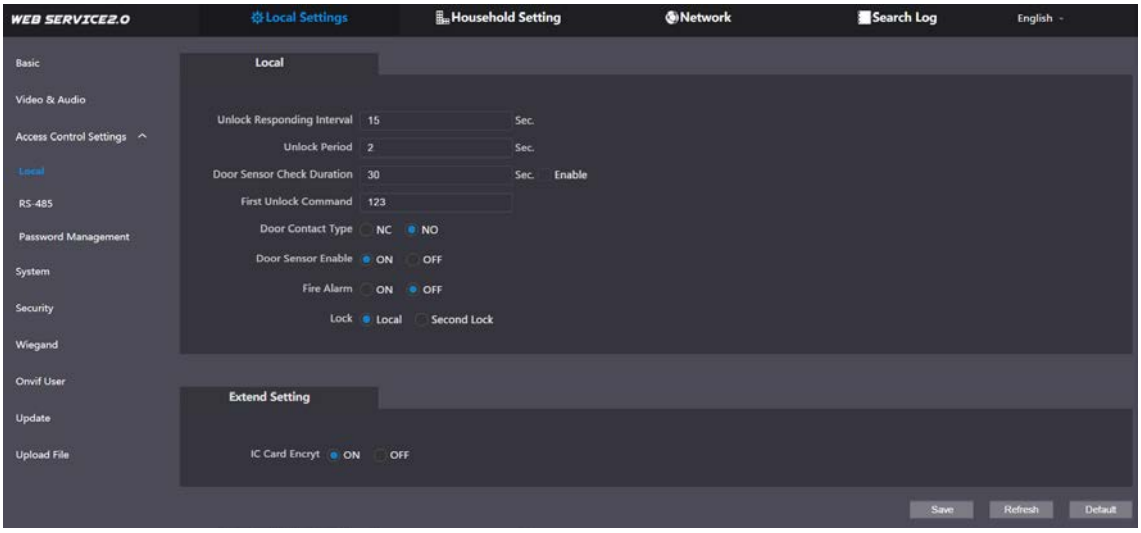
4.3 Ustawienia kontroli dostępu

W tej sekcji opisano sposób konfiguracji dwóch zamków podłączonych do portu zamka lub portu RS-485 VTO.

4.3.1 Lokalne

Step 1 Wybierać**Ustawienia lokalne > Ustawienia kontroli dostępu**.

Figure 4-3 Lokalny



Step 2 Skonfiguruj parametry.

Tabela 4-3 Opis parametrów lokalnej kontroli dostępu

Parametr	Opis
Odblokować Odpowiadanie Interwał	Drzwi można ponownie otworzyć dopiero po przerwie.
Okres odblokowania	Czas, przez który zamek pozostaje otwarty.
Czujnik drzwi Sprawdź czas trwania	● Włącz tę opcję, a drzwi nie zostaną zablokowane, dopóki czujniki drzwi nie zetkną się ze sobą. Jeśli drzwi będą otwarte dłużej niż**Czas sprawdzania czujnika drzwi**, zostanie uruchomiony alarm czujnika drzwi, a alarm zostanie wysłany do centrum zarządzania. ● Wyłącz ją, a wtedy drzwi zostaną zamknięte po**Okres odblokowania**. Aby skonfigurować ten parametr, należy zainstalować czujnik drzwiowy.
Pierwsza sekunda Odblokuj polecenie	Do VTO można podłączyć telefon innej firmy, np. telefon SIP, i za pomocą polecenia zdalnie otworzyć drzwi.
Kontakt drzwiowy Typ	● **NC**: Zwykle zamknięte. ● **NIE**: Normalnie otwarte.
Czujnik drzwi Włączać	Synchronizuj stan czujnika drzwi z monitorami wewnętrznymi (VTH).
Alarm przeciwpożarowy	Jeśli jest włączone, można podłączyć urządzenie alarmowe do portu, który pierwotnie był przeznaczony dla czujnika drzwiowego, ale nie można korzystać z funkcji czujnika drzwiowego.
Zamek	Metody inne niż zdalne, takie jak hasło lub karta, odblokują zamek

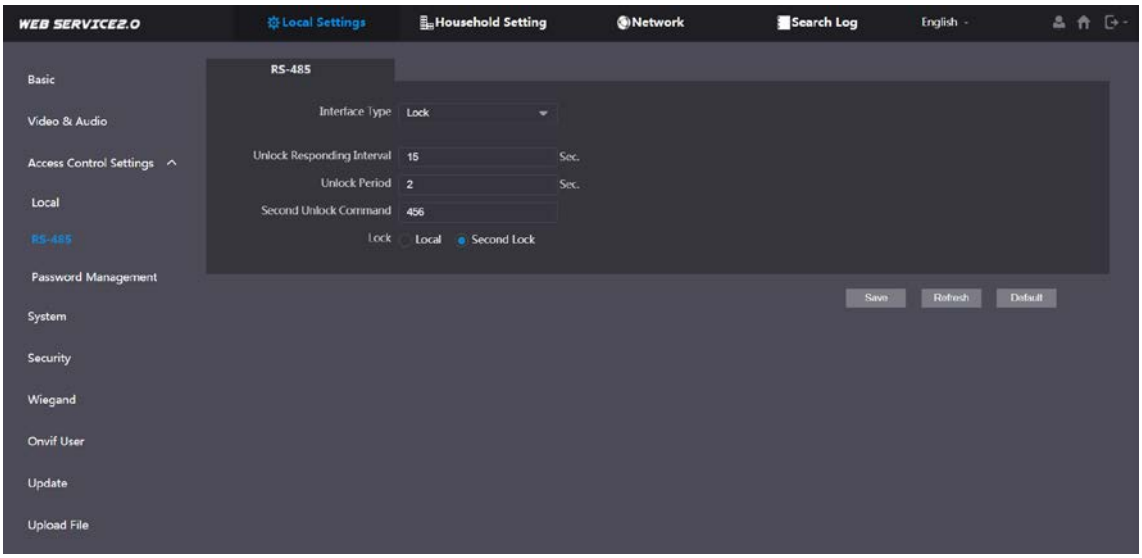
Parametr	Opis
	wybierać.
Szyfrowanie karty IC	Karty dostępu wydawane przez VTO będą szyfrowane i niemożliwe do sklonowania.

Step 3 Kliknij**Ratować**.

4.3.2 RS-485

Wybierać**Ustawienia lokalne > Ustawienia kontroli dostępu**, a następnie skonfiguruj parametry zamka podłączonego przez port RS-485. Opis parametrów można znaleźć w Tabeli 4-3.

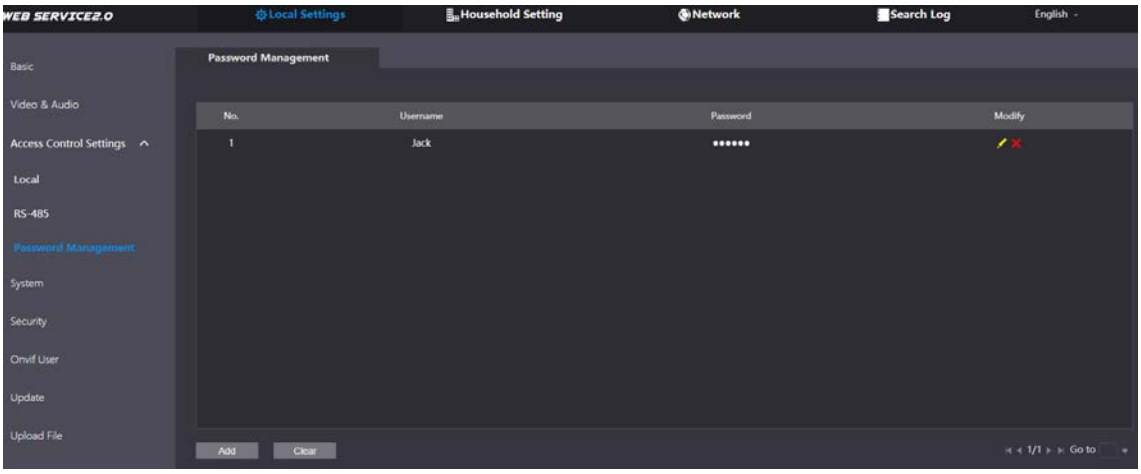
Figure 4-4 Zamek podłączany poprzez port RS-485



4.3.3 Zarządzanie hasłami

Dodaj nazwę użytkownika i hasło używane do odblokowania drzwi.

Figure 4-5 Zarządzanie hasłami

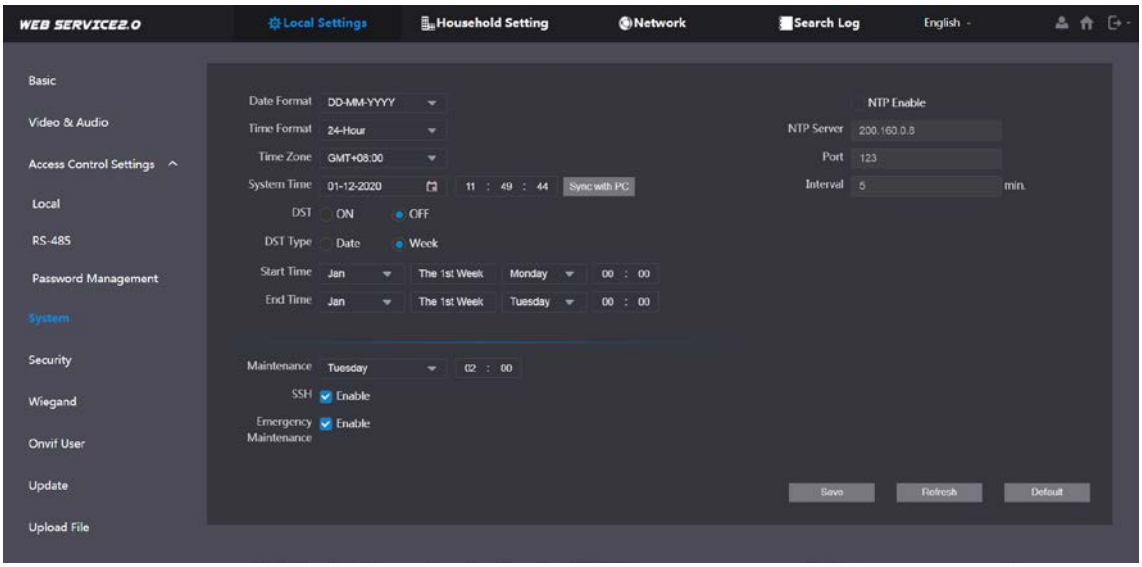


4.4 System

Skonfiguruj parametry czasu, serwer NTP i nie tylko.

Step 1 Wybierać**Ustawienia lokalne > System**.

Figure 4-6 System



Step 2 Skonfiguruj parametry.

Tabela 4-4 Opis parametrów systemu

Parametr	Opis
Format daty	Wybierz format według potrzeb.
Format czasu	
Czas systemu	⚠ Zmiana czasu systemowego może powodować problemy z wyszukiwaniem plików wideo i publikowaniem informacji. Przed zmianą wyłącz nagrywanie wideo i automatyczną migawkę.
Strefa czasowa	Skonfiguruj strefę czasową według potrzeb.
Synchronizuj z komputerem	Zsynchronizuj czas systemowy VTO z komputerem.
Czas letni	Czas letni. Jeśli dotyczy to Twojego obszaru, musisz je włączyć, a następnie skonfigurować typ czasu letniego, godzinę rozpoczęcia i godzinę zakończenia.
Typ czasu letniego	Wybierać**Data**Lub**Tydzień**w razie potrzeby, a następnie skonfiguruj konkretny okres.
Czas rozpoczęcia	Skonfiguruj godzinę rozpoczęcia i zakończenia czasu letniego.
Koniec czasu	
Włącz NTP	Włącz NTP i wprowadź adres IP serwera NTP, a następnie VTO automatycznie zsynchronizuje czas z serwerem NTP.
Serwer NTP	
Port	Numer portu serwera NTP.
Interwał	Cykl aktualizacji czasu VTO. Maksymalnie 30 minut.
Konserwacja	Określ godzinę, o której VTO automatycznie uruchomi się ponownie.
SSH	Możesz podłączyć urządzenia debugujące do VTO poprzez protokół SSH. ⚠ Zalecamy wyłączenie tej opcji, a następnie włączenie trybu bezpieczeństwa i ochrony informacji o usługach wychodzących. Patrz „4.5 Bezpieczeństwo”. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Nagły wypadek Konserwacja	Włącz tę opcję, aby móc analizować i naprawiać błędy.

Parametr	Opis
	Ta funkcja zajmie porty 8088 i 8087.

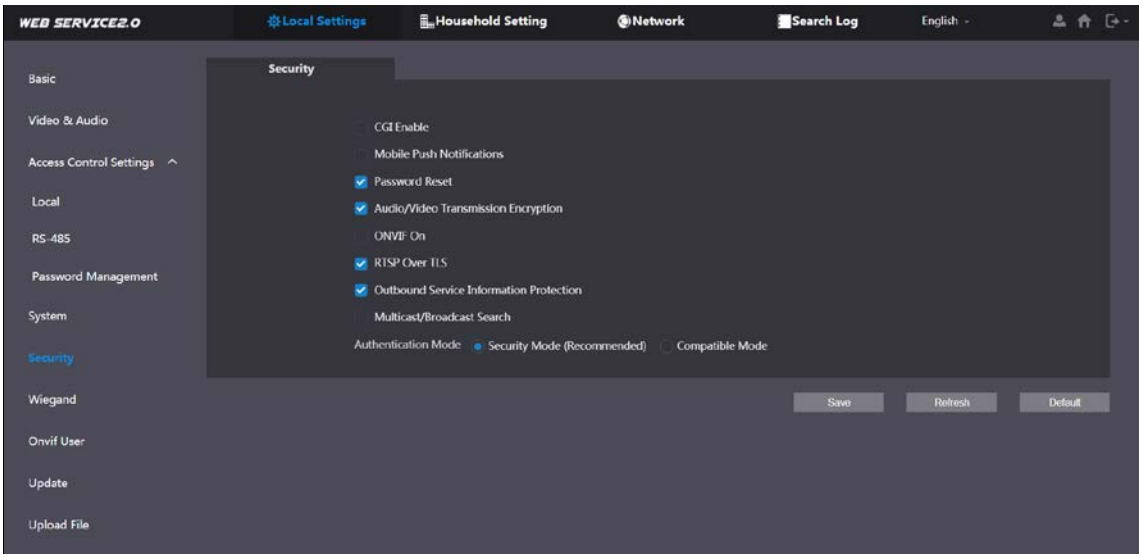
Step 3 Kliknij**Ratować**.

4.5 Bezpieczeństwo

Skonfiguruj funkcje związane z bezpieczeństwem urządzenia.

Step 1 Wybierać**Ustawienia lokalne > Bezpieczeństwo**.

Figure 4-7 Bezpieczeństwo



Step 2 Skonfiguruj parametry.

Tabela 4-5 Opis parametrów zabezpieczeń

Parametr	Opis
Włącz CGI	Włącz użycie polecenia CGI. ⚠ Zalecamy jego wyłączenie. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Wypychanie mobilne Powiadomienie	Wyślij informację do aplikacji na smartfonie. ⚠ Zalecamy wyłączenie tej funkcji, jeśli nie potrzebujesz tej funkcji. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Resetowania hasła	Jeśli opcja jest wyłączona, nie będzie możliwości zresetowania hasła.
Audio Video Przenoszenie Szyfrowanie	Szyfruj wszystkie dane podczas połączeń głosowych lub wideo. ⚠ Zalecamy jego włączenie. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Włączony ONVIF	Zezwalaj stronom trzecim na pobieranie strumienia wideo VTO za pośrednictwem protokołu ONVIF.

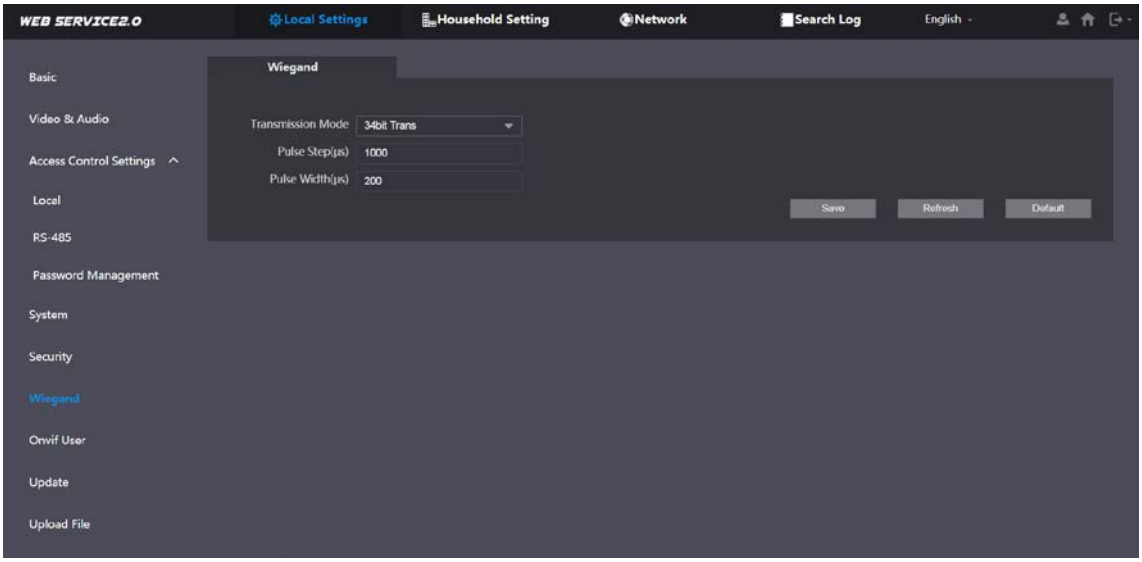
Parametr	Opis
	 Zalecamy jego wyłączenie. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
RTSP zamiast TSL	Wyprowadź zaszyfrowany strumień bitów przez RTSP.  Zalecamy jego włączenie. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Usługa wychodząca Informacja Ochrona	Chroń swoje hasła.  Zalecamy jego włączenie. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Multicast/transmisja Szukaj	Włącz tę opcję, a VTO zostanie znalezione przez inne urządzenia.  Zalecamy jego wyłączenie. W przeciwnym razie VTO może być narażony na ryzyko bezpieczeństwa i wyciek danych.
Uwierzytelnianie Tryb	• **Tryb Bezpieczny**(zalecane): Obsługa logowania przy użyciu uwierzytelniania Digest. • **Tryb zgodny**: Użyj starej metody logowania.  Zalecamy tryb bezpieczeństwa. Tryb zgodny może narazić VTO na zagrożenia bezpieczeństwa i wyciek danych.

Step 3 Kliknij**Ratować**.

4.6 Wieganda

Skonfiguruj parametry według potrzeb po podłączeniu do innych urządzeń, takich jak czytnik kart z portem Wiegand.

Figure 4-8 Wieganda



4.7 Użytkownik Onvif

Dodaj konta dla urządzeń do monitorowania VTO poprzez protokół ONVIF.

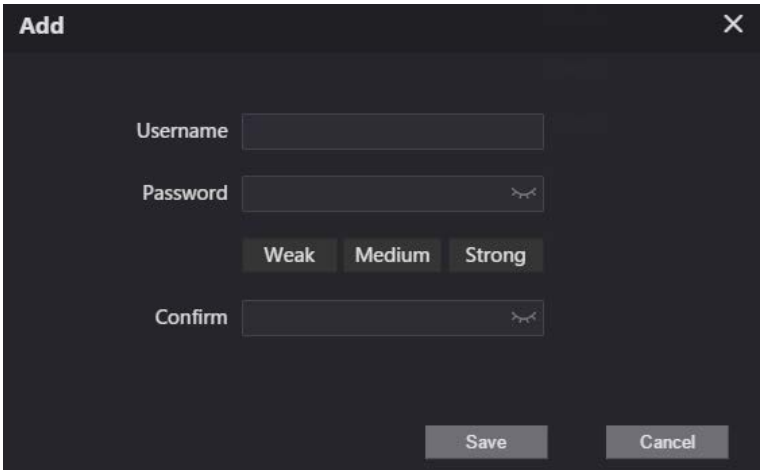
⚠

Jeżeli usuniesz konto, nie będzie można tego cofnąć.

Step 1 Wybierać**Ustawienia lokalne > Użytkownik Onvif**.

Step 2 Kliknij**Dodać**.

Figure 4-9 Dodaj użytkownika ONVIF



Step 3 Wprowadź informacje, a następnie kliknij**Ratować**.

Urządzenia ONVIF mogą teraz monitorować VTO za pomocą konta. Szczegółowe informacje można znaleźć w instrukcji obsługi urządzenia ONVIF.

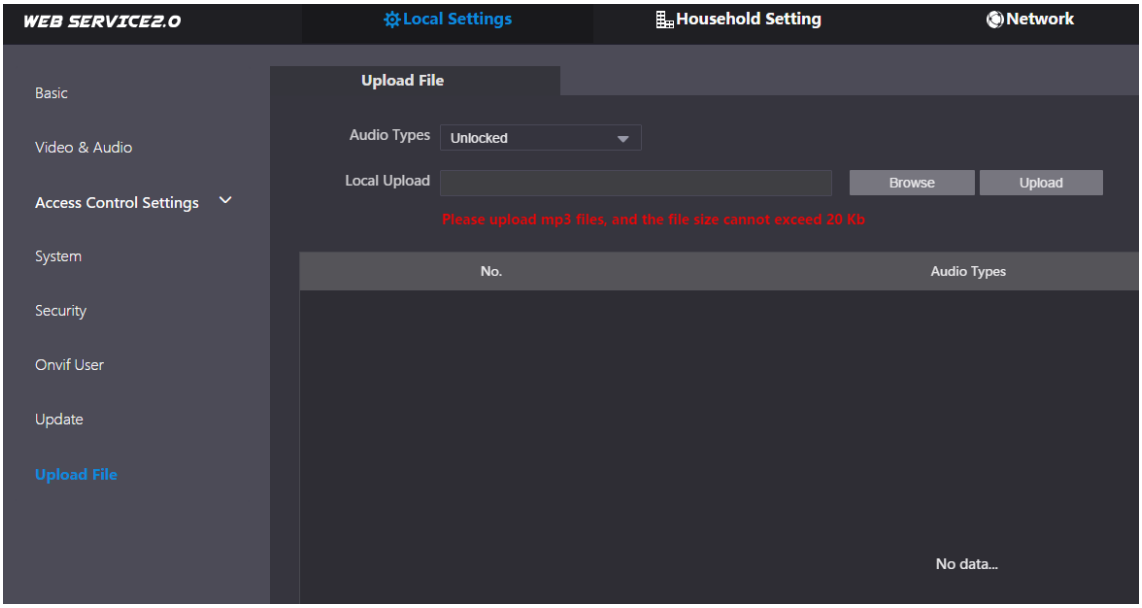
4.8 Przesyłanie pliku

Prześlij plik audio, aby zmienić dźwięk podczas dzwonienia, otwierania drzwi i nie tylko.

Step 1 Wybierać**Ustawienia lokalne > Prześlij plik**.

Step 2 Wybierz typ dźwięku, a następnie kliknij**Przeglądać**, aby wybrać plik audio według potrzeb.

Figure 4-10 Zmień monit dźwiękowy



Step 3 Kliknij**Wgrywać**.

5 Ustawienia domowe

W tym rozdziale opisano, jak dodawać, modyfikować i usuwać VTO, VTH, VTS i IPC oraz jak wysyłać komunikaty z serwera SIP do VTO i VTH, gdy VTO działa jako serwer SIP. Jeżeli używasz innych serwerów jako serwera SIP, szczegółowe informacje znajdziesz w odpowiedniej instrukcji.

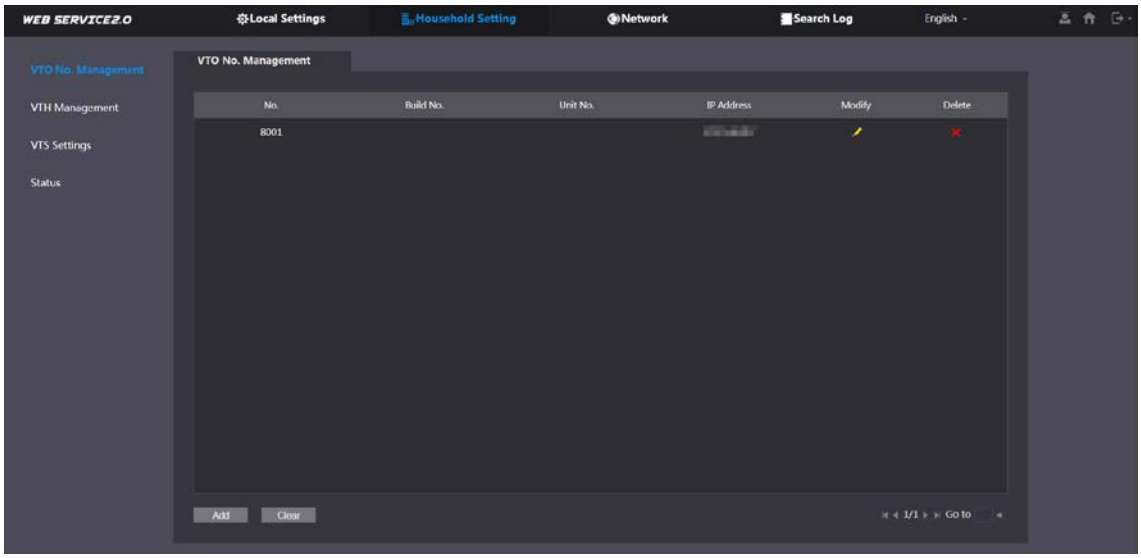
Aby skonfigurować parametry serwera SIP, zobacz szczegółowe informacje w rozdziale „6.3 Serwer SIP”.

5.1 Zarządzanie nr VTO

Możesz dodać VTO do serwera SIP, a wszystkie VTO podłączone do tego samego serwera SIP będą mogły się ze sobą kontaktować.

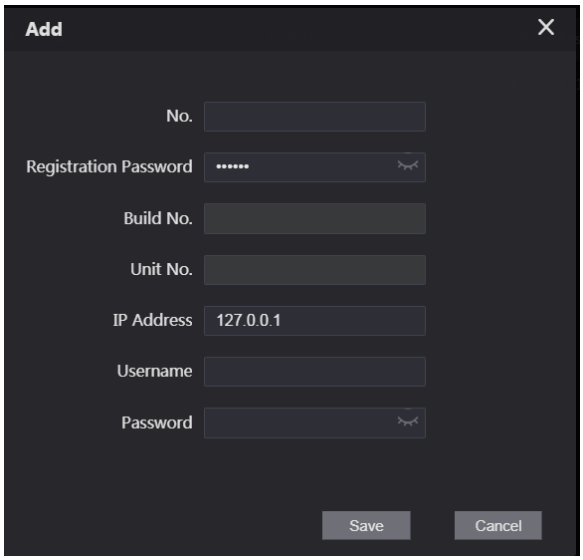
Step 1 Zaloguj się na stronę internetową VTO pracującego jako serwer SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Zarządzanie numerami VTO**.

Figure 5-1 Zarządzanie VTO



Step 2 Kliknij**Dodać**.

Figure 5-2 Dodaj VTO



Step 3 Skonfiguruj parametry.

Należy dodać serwer SIP.

Tabela 5-1 Dodawanie konfiguracji VTO

Parametr	Opis
NIE.	Skonfigurowany numer VTO. Aby uzyskać szczegółowe informacje, zobacz Tabela 4-1.
Rejestracja Hasło	Zostaw to jako domyślne.
Numer kompilacji Nr jednostki	Dostępne tylko wtedy, gdy inne serwery działają jako serwer SIP.
Adres IP	Adres IP VTO.
Nazwa użytkownika Hasło	Nazwa użytkownika i hasło VTO.

Step 4 Kliknij**Ratować**.

Kliknij Lub zmodyfikować lub usunąć VTO, lub**Jasne**, aby usunąć wszystkie dodane VTO, ale jedno do którego się zalogowałeś, nie można modyfikować ani usuwać.

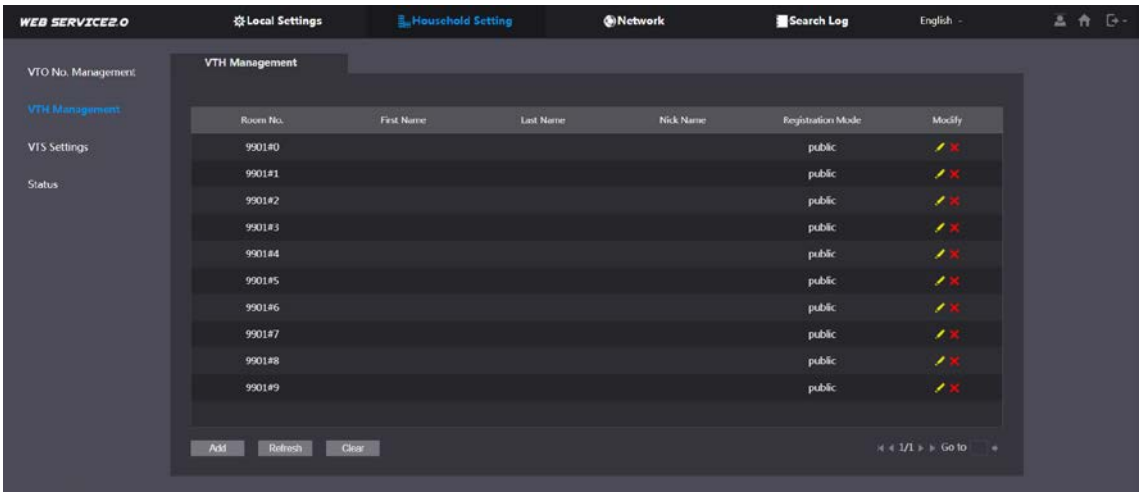
5.2 Zarząd VTH

5.2.1 Dodawanie numeru pokoju

Możesz dodać numery pokoi do serwera SIP, a następnie skonfigurować numer pokoju na VTH, aby połączyć je z siecią.

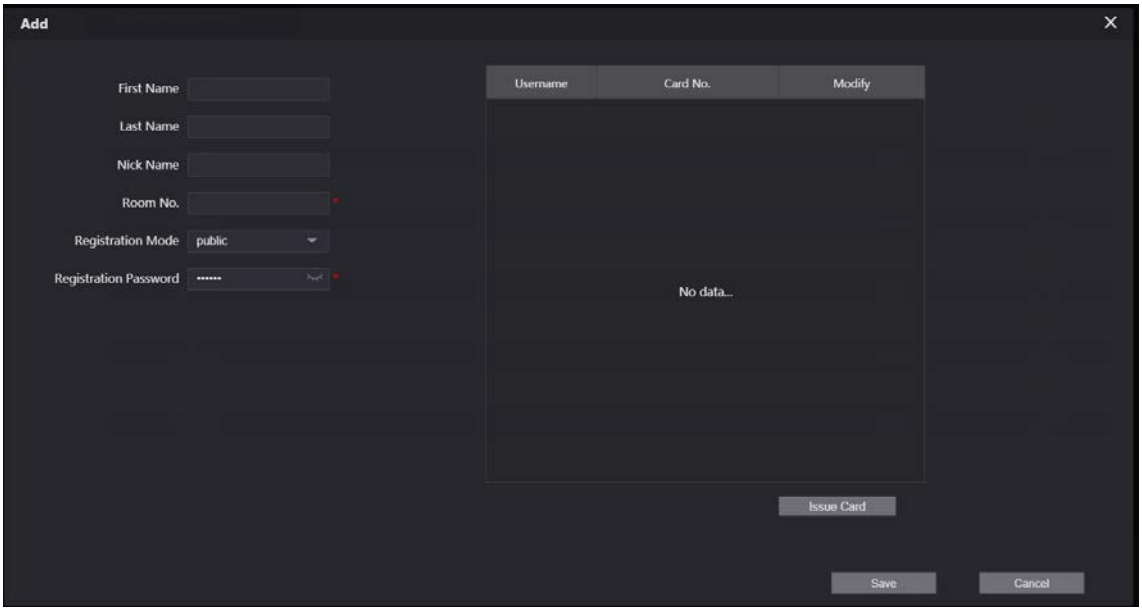
Step 1 Zaloguj się na stronę internetową serwera SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Zarządzanie VTH**.

Figure 5-3 Zarządzanie numerami pokoi



Step 2 Kliknij**Dodać**.

Figure 5-4 Dodaj numer pokoju



Step 3 Skonfiguruj parametry.

Tabela 5-2 Informacje o pokojach

Parametr	Opis
Imię	Wprowadź informacje potrzebne do wyróżnienia każdego pokoju.
Nazwisko	
Przezwisko	
Pokój numer.	Wprowadź numer pokoju, a następnie skonfiguruj numer na VTH, aby się połączyć aby podłączyć go do sieci.
Typ rejestracji	Wybierać**publiczny**.
Rejestracja Hasło	Zostaw to jako domyślne.

Step 4 Kliknij**Ratować**.

Kliknij Lub aby zmienić lub usunąć numer pokoju.

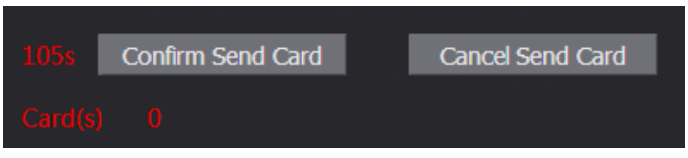
5.2.2 Wydanie Karty Dostępu

Wydaj kartę dostępu, aby otworzyć drzwi do pokoju.

Aby skorzystać z tej funkcji, VTO musi posiadać czytnik kart.

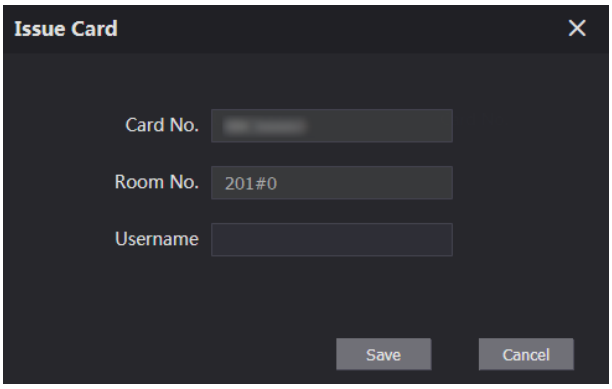
Step 1 Wybierać**Ustawienia gospodarstwa domowego > Zarządzanie VTH**, Kliknij**Dodać**, a następnie kliknij**Wydanie karty**.

Figure 5-5 Zawiadomienie o odliczaniu



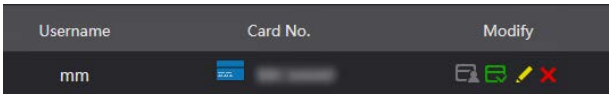
Step 2 Przesuń kartę na VTO.

Figure 5-6 Wydanie karty



Step 3 Wprowadź nazwę użytkownika, kliknij**Ratować**, a następnie kliknij**Potwierdź wysłanie karty**.

Figure 5-7 Wydana karta dostępu



Inne operacje

- Kliknij aby ustawić ją jako kartę główną, a następnie ikona zmieni się na . Karta główna może być używany do wydawania kart dostępu do tego pomieszczenia w VTO.
- Kliknij aby ustawić go na stratę, a następnie ikona zmieni się na . Zgubionej karty nie można wykorzystać Otwórz drzwi.
- Kliknij Lub zmienić nazwę użytkownika lub usunąć kartę.

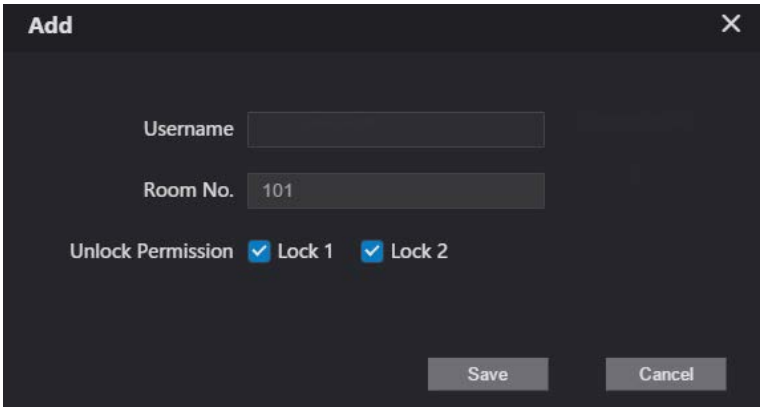
5.2.3 Wystawianie odcisku palca

Wystaw odciski palców, aby otworzyć drzwi do pokoju.

Aby skorzystać z tej funkcji, VTO musi posiadać skaner linii papilarnych.

Step 1 Wybierać**Ustawienia gospodarstwa domowego > Zarządzanie VTH**, Kliknij**Dodać**, a następnie kliknij**Wydaj odcisk palca**.

Figure 5-8 Wystaw odcisk palca



Step 2 Wprowadź nazwę użytkownika, w razie potrzeby przypisz uprawnienia do odblokowania, a następnie kliknij**Ratować**.

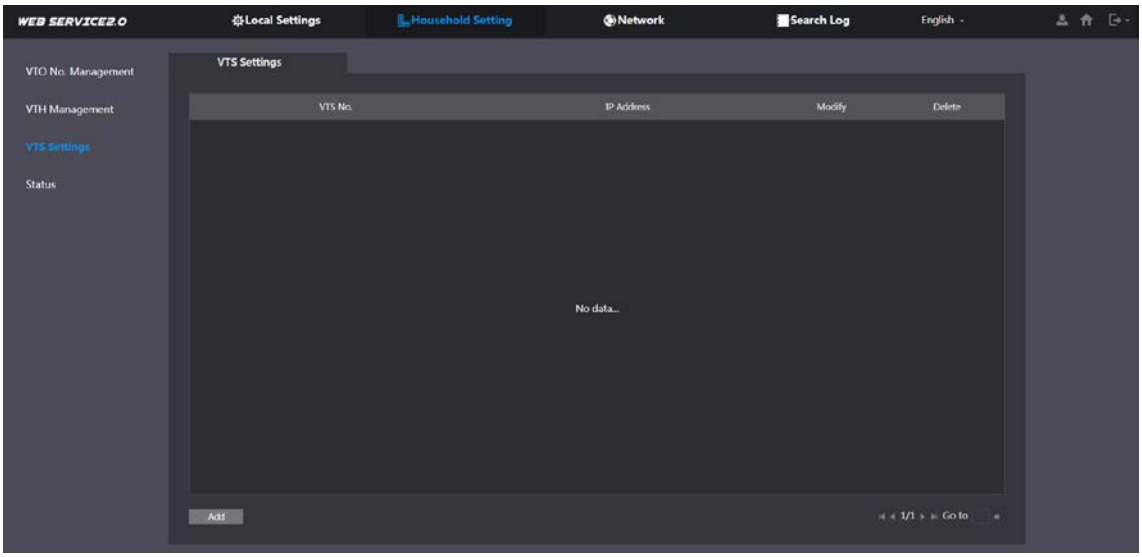
Step 3 Naciśnij odcisk palca na skanerze.

5.3 Zarządzanie VTSem

Możesz dodać VTS do serwera SIP i wtedy może służyć jako centrum zarządzania. Może także zarządzać, dzwonić i odbierać połączenia ze wszystkich VTO i VTH w sieci. Szczegółowe informacje można znaleźć w odpowiedniej instrukcji obsługi.

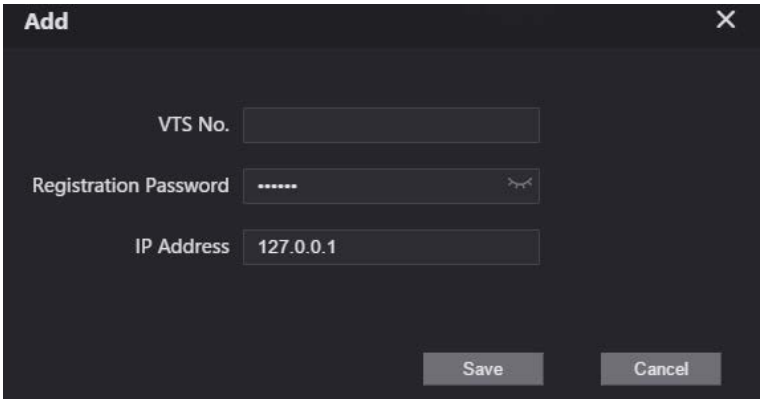
Step 1 Zaloguj się na stronę internetową VTO pracującego jako serwer SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Ustawienia VTS**.

Figure 5-9 Zarządzanie VTSem



Step 2 Kliknij**Dodać**.

Figure 5-10 Dodaj VTS



Step 3 Skonfiguruj parametry.

Tabela 5-3 Dodawanie konfiguracji VTS

Parametr	Opis
Nr VTS	Numer VTS.
Rejestracja Hasło	Zostaw to jako domyślne.
Adres IP	Adres IP VTS.

Step 4 Kliknij**Ratować**.

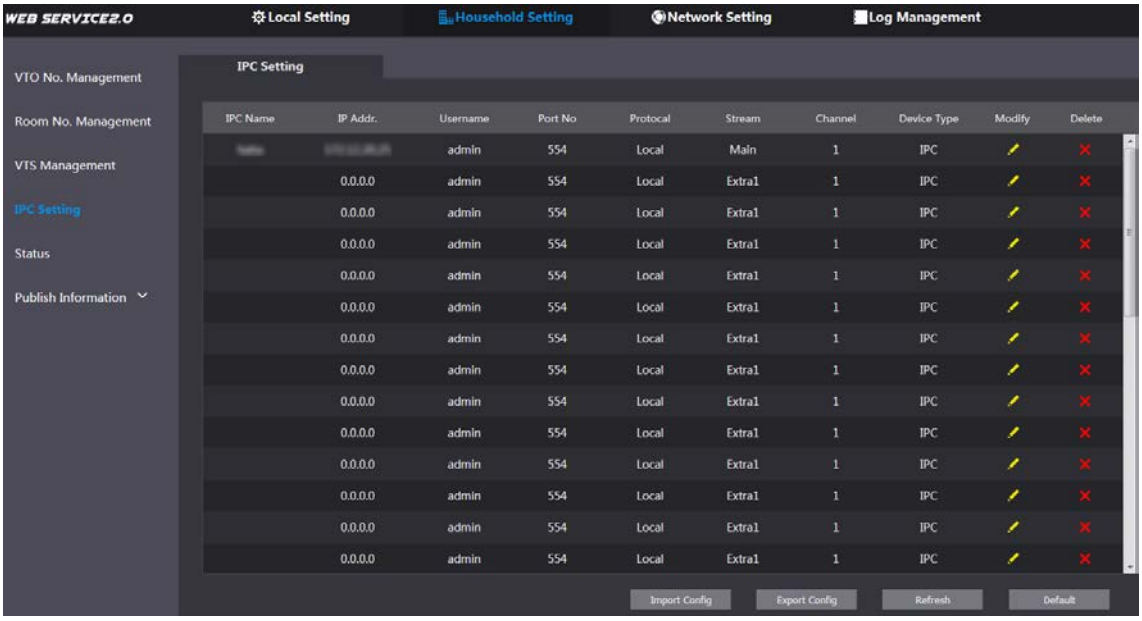
5.4 Ustawienie IPC

Możesz dodać IPC i NVR do VTO działającego jako serwer SIP, a następnie wszystkie podłączone VTH będą mogły je monitorować.

Interfejsy mogą się różnić w zależności od produktów. Obowiązujący będzie rzeczywisty interfejs.

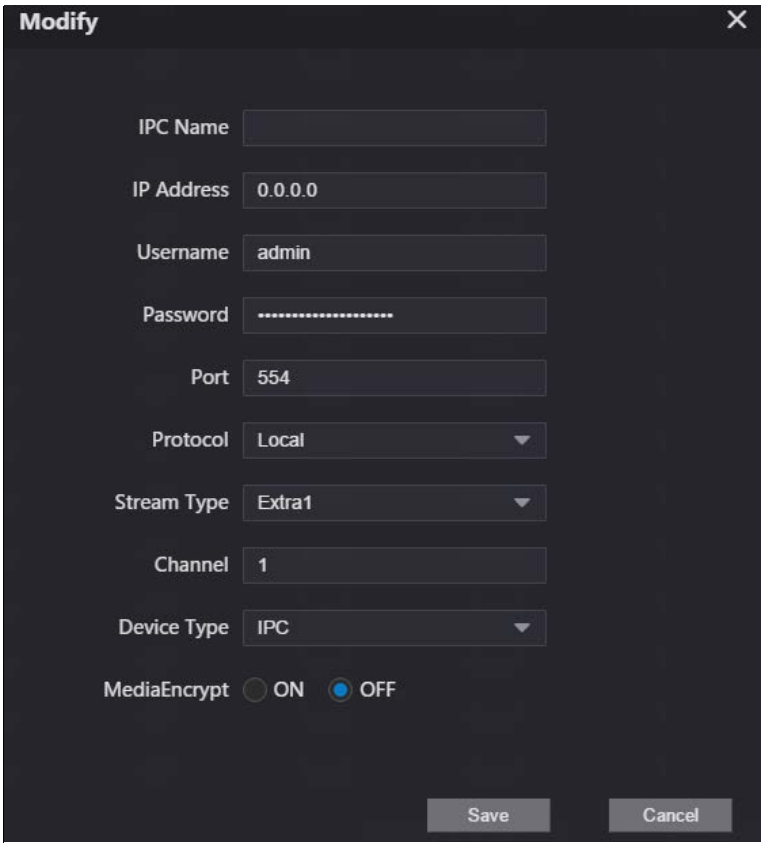
Step 1 Zaloguj się na stronę internetową VTO pracującego jako serwer SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Ustawienia IPC**.

Figure 5-11 Ustawienie IPC



Step 2 Kliknij .

Figure 5-12 Dodaj IPC



Step 3 Skonfiguruj parametry.

Tabela 5-4 Dodawanie konfiguracji IPC

Parametr	Opis
Nazwa IPC	Wprowadź nazwę identyfikującą IPC.
Adres IP	Adres IP IPC.
Nazwa użytkownika	Nazwa użytkownika i hasło urządzenia.
Hasło	
Port	Zostaw to jako domyślne.
Protokół	Wybierać**Lokalny**Lub**Onvif**.
Typ strumienia	• **Główny**: Lepsza jakość wideo, ale wymaga większej przepustowości. • **Ekstra1**: Płynniejszy obraz wideo o gorszej jakości, ale wymaga mniejszej przepustowości.
Kanał	Liczba kanałów obsługiwanych przez urządzenie.
Rodzaj urządzenia	Wybierz ten, który jest potrzebny.
Szyfrowanie multimediów	Wybierać**NA**czy dodawany IPC jest zaszyfrowany.

Step 4 Kliknij**Ratować**.

Inne operacje

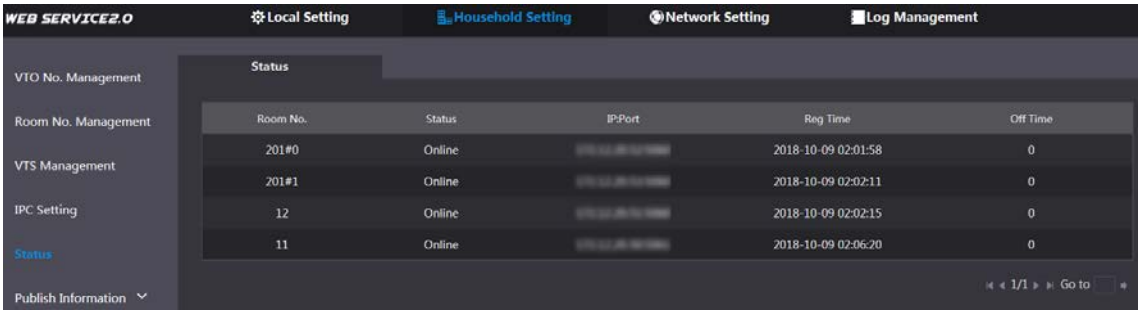
- **Eksportuj konfigurację**: Eksportuj informacje o urządzeniu do komputera.
- **Importuj konfigurację**: importowanie informacji o urządzeniu.

5.5 Status

Możesz przeglądać status online i adresy IP wszystkich podłączonych urządzeń.

Zaloguj się na stronę internetową serwera SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Stan**.

Figure 5-13 Status



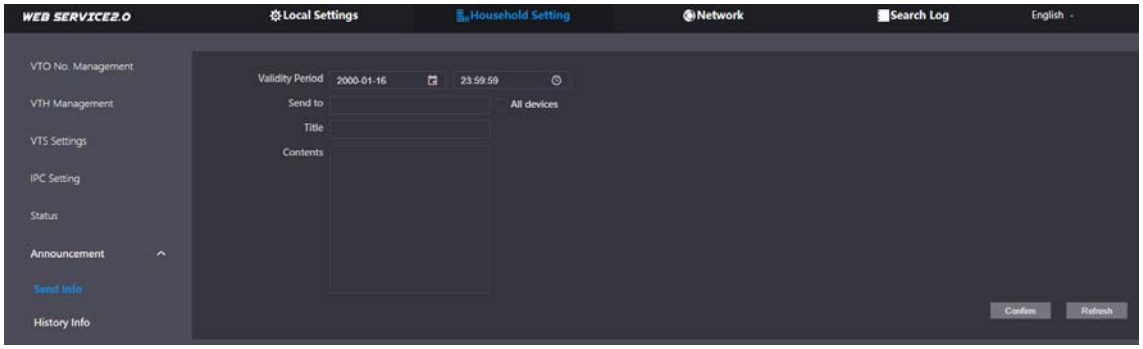
5.6 Publikuj informacje

Możesz wysyłać wiadomości z serwera SIP do urządzeń VTH i przeglądać historię wiadomości.

5.6.1 Wyślij informacje

Step 1 Zaloguj się na stronę internetową serwera SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Publikuj informacje > Wyślij informacje**.

Figure 5-14 Wyślij informację



Step 2 Określić**Termin ważności**że wiadomość będzie aktualna.

Step 3 Wprowadź numer VTO lub numer VTH lub wybierz**Wszystkie urządzenia**, aby wysłać wiadomość do wszystkich urządzeń w sieci, a następnie wprowadź tytuł i treść wiadomości.

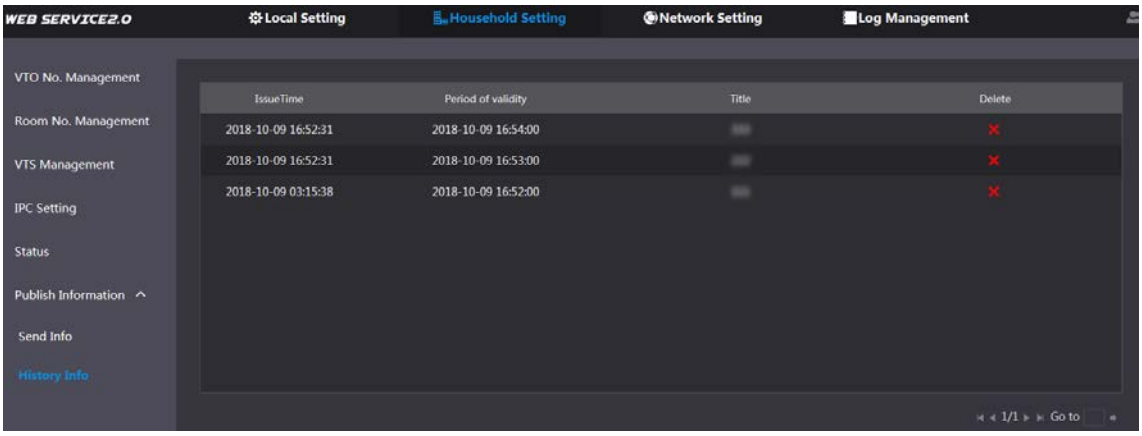
Step 4 Kliknij**Potwierdzać**.

5.6.2 Informacje o historii

Możesz przeglądać informacje o wysłanych wiadomościach.

Zaloguj się na stronę internetową serwera SIP, wybierz**Ustawienia gospodarstwa domowego > Publikuj informacje > Informacje o historii**.

Figure 5-15 Informacje historyczne



6 Sieć

W tym rozdziale opisano sposób konfiguracji parametrów sieciowych.

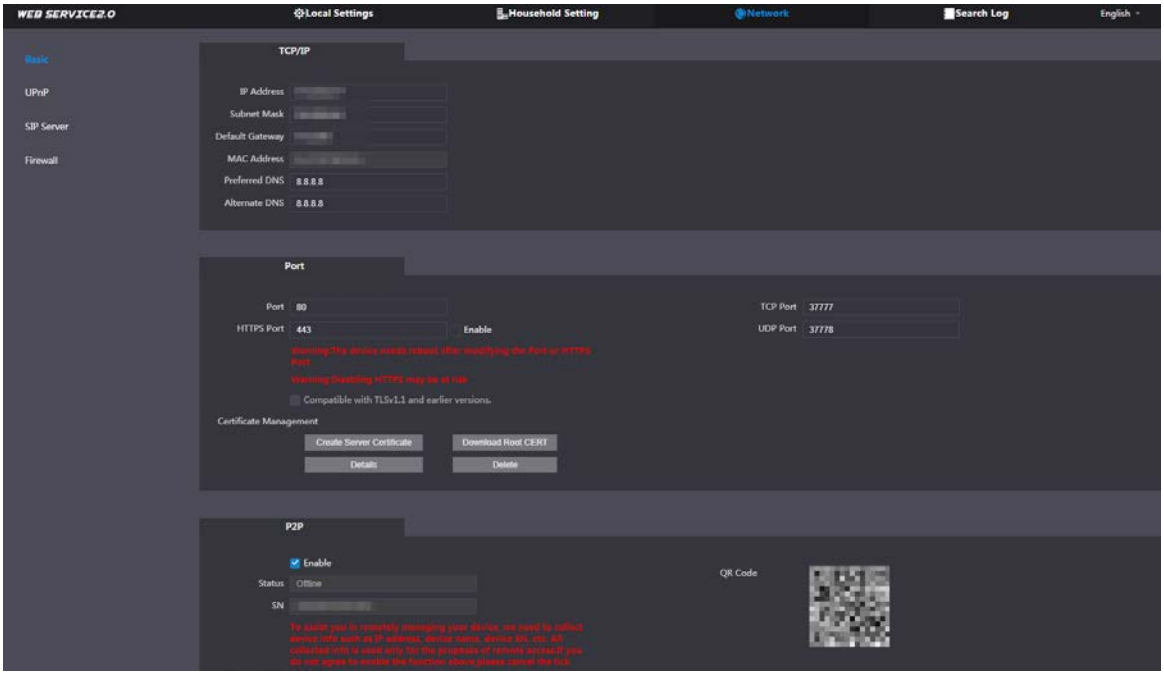
6.1 Podstawowy

6.1.1 TCP/IP

Możesz modyfikować adres IP, maskę podsieci, bramę domyślną i DNS VTO.

Step 1 Wybierać**Sieć > Podstawowe**.

Figure 6-1 TCP/IP i port



Step 2 Skonfiguruj parametry, a następnie kliknij**Ratować**.

VTO uruchomi się ponownie i aby zalogować się ponownie, należy zmienić adres IP komputera na ten sam segment sieci, co VTO.

6.1.2 Port

Tabela 6-1 Opis parametrów

Parametr	Opis
Port	domyślnie 80. Jeśli jest już używany, wybierz w razie potrzeby dowolny numer od 1025 do 65535. Możesz wejść*http://VTO Adres IP:Port*zalogować się do VTO.
Port HTTPS	Włącz i kliknij**Ratować**. Możesz teraz wejść*https://VTO Adres IP:Port HTTPS*zalogować się do VTO.
Port TCP/UDP	Służy do uzyskiwania dostępu do VTO za pomocą urządzeń w innych sieciach. Aby uzyskać szczegółowe informacje, zobacz „6.2 UPnP”.

Parametr	Opis
Tworzyć serwer Certyfikat	Unikalna cyfrowa identyfikacja VTO dla protokołu SSL. Przy pierwszym użyciu lub po zmianie adresu IP VTO należy przejść przez ten proces. ⚠ Jeśli usuniesz utworzony certyfikat, nie będzie można tego cofnąć.
Pobierz roota CERT	Jeśli korzystasz z komputera PC, który nigdy nie logował się do VTO, musisz pobrać certyfikat główny, kliknąć dwukrotnie, aby go zainstalować, a następnie możesz skorzystać z opisanej powyżej funkcji HTTPS. ⚠ Jeśli usuniesz zainstalowany certyfikat, nie będzie można tego cofnąć.

6.1.3 P2P

Włącz**P2P**funkcję, a następnie zeskanuj telefonem kod QR, aby dodać VTO do aplikacji na swoim smartfonie. Szczegółowe informacje można znaleźć w skróconej instrukcji obsługi.

6.2 UPnP

Gdy VTO pracuje jako serwer SIP, można skonfigurować funkcję UPnP, aby umożliwić urządzeniom WAN logowanie się do VTO.

Przygotowanie

- Włącz funkcję UPnP na routerze, a następnie skonfiguruj adres IP sieci WAN dla
- routera. Podłącz VTO do portu LAN routera.

6.2.1 Włączanie usług UPnP

Step 1 Wybierać**Sieć > UPnP**.

Step 2 W razie potrzeby włącz wymienione usługi.

Step 3 Wybierać**Włączać**.

Step 4 Kliknij**Ratować**.

6.2.2 Dodawanie usług UPnP

Step 1 Wybierać**Sieć > UPnP**.

Step 2 Kliknij**Dodać**.

Step 3 Skonfiguruj parametry według potrzeb.

Figure 6-2 Dodaj usługę UPnP

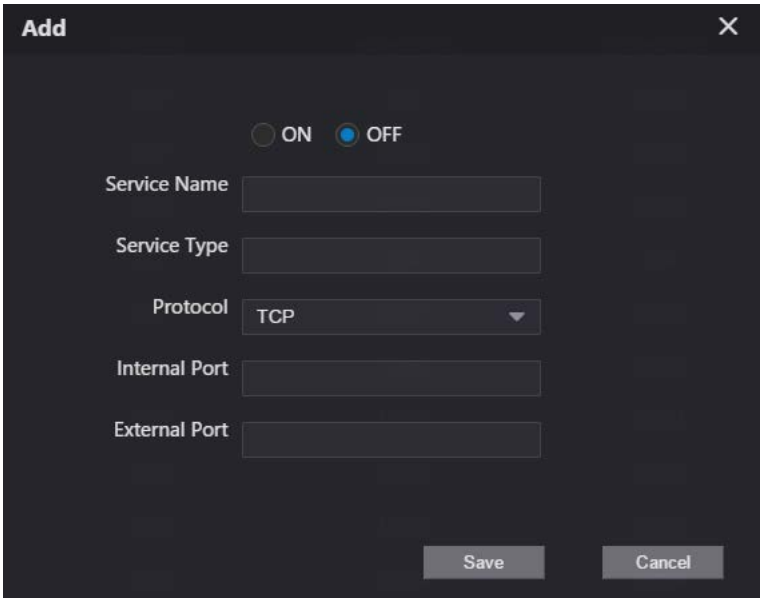


Tabela 6-2 Opis parametrów

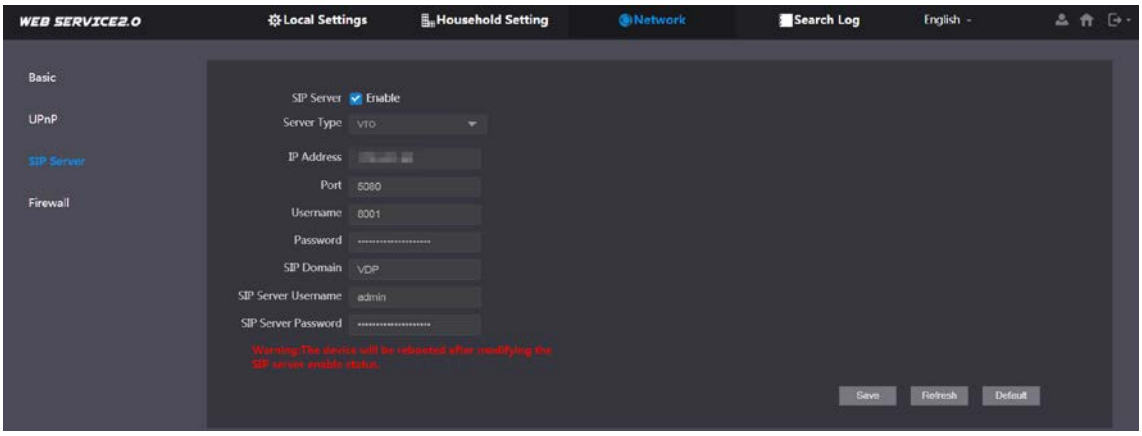
Parametr	Opis
Nazwa serwisu	Wprowadź potrzebne informacje.
Rodzaj usługi	
Protokół	Wybierać**TCP**Lub**UDP**w razie potrzeby.
Port wewnętrzny	Użyj numeru portu od 1024 do 5000. - Aby uniknąć konfliktu, nie używaj portów o numerach 1–1023. - Jeśli chcesz skonfigurować tę funkcję dla wielu urządzeń, upewnij się, że porty nie są takie same. - Numer portu, którego używasz, nie może być zajęty. - Numer portu wewnętrznego i zewnętrznego musi być taki sam.
Port zewnętrzny	

6.3 Serwer SIP

W sieci musi znajdować się serwer SIP, aby wszystkie podłączone VTO i VTH mogły się ze sobą łączyć. Jako serwera SIP możesz użyć VTO lub innego serwera.

Step 1 Wybierać**Sieć > Serwer SIP**.

Figure 6-3 Serwer SIP



Step 2 W razie potrzeby wybierz typ serwera.

- VTO, na którym zalogowałeś się jako serwer SIP:

  Włączać**Serwer SIP**i kliknij**Ratować**, a następnie VTO uruchomi się ponownie. Do tego VTO możesz dodać VTO i VTH.

  Zobacz szczegóły w „5 Ustawienia gospodarstwa domowego”.

  Jeśli VTO, do którego się zalogowałeś, nie obsługuje serwera SIP, nie włączaj go**Serwer SIP**; W przeciwnym razie połączenie nie powiedzie się.

- Jeżeli inny VTO pracuje jako serwer SIP:

  Nie włączaj**Serwer SIP**. Ustawić**Rodzaj serwera**Do**WTO**, skonfiguruj parametry, a następnie kliknij **Ratować**.

Tabela 6-3 Konfiguracja serwera SIP

Parametr	Opis
Adres IP	Adres IP VTO.
Port	• Domyślnie 5060, gdy VTO działa jako serwer SIP. Domyślnie • 5080, gdy platforma działa jako serwer SIP.
Nazwa użytkownika	Zostaw to jako domyślne.
Hasło	
Domena SIP	VDP.
Nazwa użytkownika serwera SIP	Nazwa użytkownika i hasło VTO.
Hasło serwera SIP	

- Jeśli inne serwery działają jako serwer SIP:

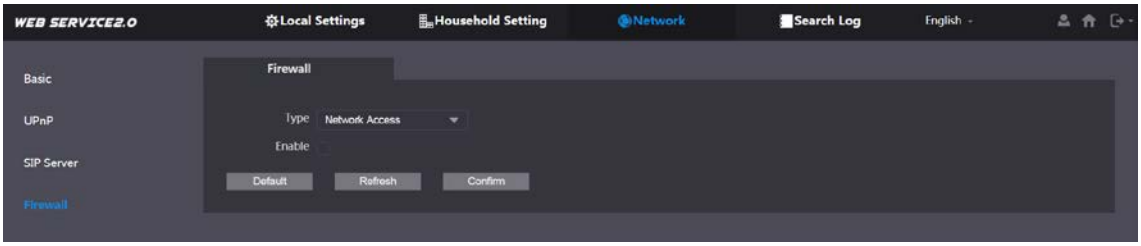
  Wybierz**Rodzaj serwera**w razie potrzeby, a następnie zapoznaj się ze szczegółami w odpowiedniej instrukcji.

6.4 Zapora sieciowa

Można włączyć różne typy zapór sieciowych, aby kontrolować dostęp sieciowy do VTO.

Step 1 Wybierać**Sieć > Zapora sieciowa**.

Figure 6-4 Zapora sieciowa



Step 2 Wybierz jeden lub więcej typów zapór sieciowych, a następnie włącz je.

Step 3 Skonfiguruj parametry.

Tabela 6-4 Opis typu zapory

Typ	Opis
Dostęp do sieci	Wybierz albo**Lista dozwolonych**Lub**Lista zablokowanych**, a następnie dodaj adres IP lub segment, który może lub nie może uzyskać dostępu do VTO.
PING zabroniony	Aby uniknąć ataków ping, VTO nie będzie reagować na polecenia ping.
Anty-semijoin	Chroni wydajność VTO poprzez blokowanie nadmiernych pakietów SYN.

7 Zarządzanie logami

Wybierać**Przeszukaj dziennik**. Możesz wyszukiwać różne dzienniki i w razie potrzeby eksportować je do komputera.

Jeśli pamięć jest pełna, najstarsze zapisy zostaną nadpisane. W razie potrzeby wykonaj kopię zapasową zapisów.

Appendix 1 Zalecenia dotyczące cyberbezpieczeństwa

Cyberbezpieczeństwo to coś więcej niż tylko modne hasło: to coś, co dotyczy każdego urządzenia podłączonego do Internetu. Nadzór wideo IP nie jest odporny na zagrożenia cybernetyczne, ale podjęcie podstawowych kroków w kierunku ochrony i wzmocnienia sieci i urządzeń sieciowych sprawi, że będą one mniej podatne na ataki. Poniżej znajduje się kilka wskazówek i zaleceń, jak stworzyć bezpieczniejszy system bezpieczeństwa.

Obowiązkowe działania, które należy podjąć w celu zapewnienia podstawowego bezpieczeństwa

sieci urządzenia: 1. Używaj silnych haseł

Aby ustawić hasła, zapoznaj się z poniższymi sugestiami:

- Długość nie powinna być mniejsza niż 8 znaków;
- Uwzględnij co najmniej dwa rodzaje znaków; typy znaków obejmują wielkie i małe litery, cyfry i symbole;
- Nie podawaj nazwy konta lub nazwy konta w odwrotnej kolejności; Nie
- używaj znaków ciągłych, takich jak 123, abc itp.;
- Nie używaj nakładających się znaków, takich jak 111, aaa itp.;

2. Zaktualizuj oprogramowanie sprzętowe i oprogramowanie klienckie na czas

- Zgodnie ze standardową procedurą obowiązującą w branży technologicznej, zalecamy aktualizowanie oprogramowania sprzętowego urządzenia (takiego jak NVR, DVR, kamera IP itp.), aby mieć pewność, że system jest wyposażony w najnowsze poprawki i poprawki zabezpieczeń. Gdy urządzenie jest podłączone do sieci publicznej, zalecamy włączenie funkcji „automatycznego sprawdzania dostępności aktualizacji", aby na bieżąco otrzymywać informacje o aktualizacjach oprogramowania sprzętowego wydanych przez producenta.
- Sugerujemy pobranie i używanie najnowszej wersji oprogramowania klienckiego.

„Miło jest mieć" zalecenia mające na celu poprawę bezpieczeństwa sieci

urządzenia: 1. Ochrona fizyczna

Sugerujemy wykonanie fizycznej ochrony urządzenia, zwłaszcza urządzeń pamięci masowej. Na przykład umieść urządzenie w specjalnej sali komputerowej i szafce oraz wdroż dobrze wykonaną kontrolę dostępu i zarządzanie kluczami, aby uniemożliwić nieuprawnionemu personelowi dokonywanie kontaktów fizycznych, takich jak uszkodzenie sprzętu, nieautoryzowane podłączenie urządzenia wymiennego (takiego jak dysk flash USB , port szeregowy) itp.

2. Regularnie zmieniaj hasła

Sugerujemy regularną zmianę haseł, aby zmniejszyć ryzyko odgadnięcia lub złamania hasła.

3. Ustaw i zaktualizuj hasła. Resetuj informacje w odpowiednim czasie

Urządzenie obsługuje funkcję resetowania hasła. Skonfiguruj powiązane informacje umożliwiające terminowe zresetowanie hasła, w tym skrzynkę pocztową użytkownika końcowego i pytania dotyczące ochrony hasła. Jeśli informacje ulegną zmianie, prosimy o ich modyfikację w odpowiednim czasie. Przy ustawianiu pytań zabezpieczających hasłem sugeruje się, aby nie używać tych, które można łatwo odgadnąć.

4. Włącz blokadę konta

Funkcja blokady konta jest domyślnie włączona i zalecamy pozostawienie jej włączonej, aby zagwarantować bezpieczeństwo konta. Jeśli atakujący spróbuje kilka razy zalogować się przy użyciu nieprawidłowego hasła, odpowiednie konto i źródłowy adres IP zostaną zablokowane.

5. Zmień domyślny port HTTP i inne porty usług

Sugerujemy zmianę domyślnych portów HTTP i innych usług na dowolny zestaw liczb z zakresu 1024–65535, co zmniejszy ryzyko, że osoby postronne będą w stanie odgadnąć, których portów używasz.

6. Włącz HTTPS

Sugerujemy włączenie protokołu HTTPS, aby móc odwiedzać serwis WWW poprzez bezpieczny kanał komunikacji.

7. Powiązanie adresu MAC

Zalecamy powiązanie adresu IP i MAC bramy z urządzeniem, co zmniejszy ryzyko fałszowania protokołu ARP.

8. Przydzielaj konta i uprawnienia w rozsądny sposób

Zgodnie z wymaganiami biznesowymi i zarządczymi rozsądnie dodawaj użytkowników i przypisuj im minimalny zestaw uprawnień.

9. Wyłącz niepotrzebne usługi i wybierz tryby bezpieczne

Jeśli nie jest to potrzebne, zalecamy wyłączenie niektórych usług, takich jak SNMP, SMTP, UPnP itp., aby zmniejszyć ryzyko.

W razie potrzeby zdecydowanie zaleca się korzystanie z trybów awaryjnych, obejmujących między innymi następujące usługi:

- SNMP: Wybierz SNMP v3 i skonfiguruj silne hasła szyfrujące i uwierzytelniające.
- SMTP: Wybierz TLS, aby uzyskać dostęp do serwera skrzynek
- pocztowych. FTP: Wybierz SFTP i skonfiguruj silne hasła.
- Hotspot AP: wybierz tryb szyfrowania WPA2-PSK i skonfiguruj silne hasła.

10. Szyfrowana transmisja audio i wideo

Jeśli zawartość danych audio i wideo jest bardzo ważna lub wrażliwa, zalecamy skorzystanie z funkcji szyfrowanej transmisji, aby zmniejszyć ryzyko kradzieży danych audio i wideo podczas transmisji.

Przypomnienie: szyfrowana transmisja spowoduje pewną utratę wydajności transmisji.

11. Bezpieczny audyt

- Sprawdzaj użytkowników online: sugerujemy regularne sprawdzanie użytkowników online, aby sprawdzić, czy urządzenie jest zalogowane bez autoryzacji.
- Sprawdź dziennik urządzenia: Przeglądając logi, możesz poznać adresy IP, które były używane do logowania się do Twoich urządzeń i ich kluczowych operacji.

12. Dziennik sieciowy

Ze względu na ograniczoną pojemność urządzenia, przechowywany dziennik jest ograniczony. Jeśli chcesz zapisać dziennik przez dłuższy czas, zaleca się włączenie funkcji dziennika sieciowego, aby zapewnić synchronizację krytycznych dzienników z serwerem dzienników sieciowych w celu śledzenia.

13. Zbuduj bezpieczne środowisko sieciowe

Aby lepiej zapewnić bezpieczeństwo urządzenia i ograniczyć potencjalne zagrożenia cybernetyczne, zalecamy:

- Wyłącz funkcję mapowania portów routera, aby uniknąć bezpośredniego dostępu do urządzeń intranetowych z sieci zewnętrznej.
- Sieć powinna być podzielona i izolowana zgodnie z rzeczywistymi potrzebami sieci. Jeśli nie ma wymagań komunikacyjnych pomiędzy dwiema podsieciami, sugeruje się użycie VLAN, GAP sieciowy i innych technologii w celu podziału sieci, aby uzyskać efekt izolacji sieci.
- Wprowadź system uwierzytelniania dostępu 802.1x, aby zmniejszyć ryzyko nieautoryzowanego dostępu do sieci prywatnych.
- Włącz funkcję filtrowania adresów IP/MAC, aby ograniczyć zakres hostów, które mogą uzyskać dostęp do urządzenia.