Stacja domofonowa do willi (wersja 4.5)

Skrócona instrukcja obsługi

Wersja 1.0.1

Przedmowa

Ogólny

Niniejsza instrukcja przedstawia budowę, proces montażu i podstawową konfigurację domofonu willowego (zwanego dalej „VTO”).

Instrukcje bezpieczeństwa

W instrukcji mogą pojawić się następujące skategoryzowane słowa ostrzegawcze 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 skutkować uszkodzeniem mienia, utratą danych, gorszą wydajnością lub nieprzewidywalnymi rezultatami.
 PORADY	Zawiera metody, które pomogą Ci rozwiązać problem lub zaoszczędzić czas.
 NOTATKA	Podaje dodatkowe informacje jako podkreślenie i 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.	Grudzień 2020

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 regionach. Szczegółowe informacje można znaleźć w instrukcji papierowej, płycie CD-ROM, kodzie QR lub na naszej oficjalnej stronie internetowej. 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 prosimy o zapoznanie się z naszymi ostatecznymi wyjaśnieniami.

- 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 prosimy o zapoznanie się z naszym ostatecznym wyjaśnieniem.

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

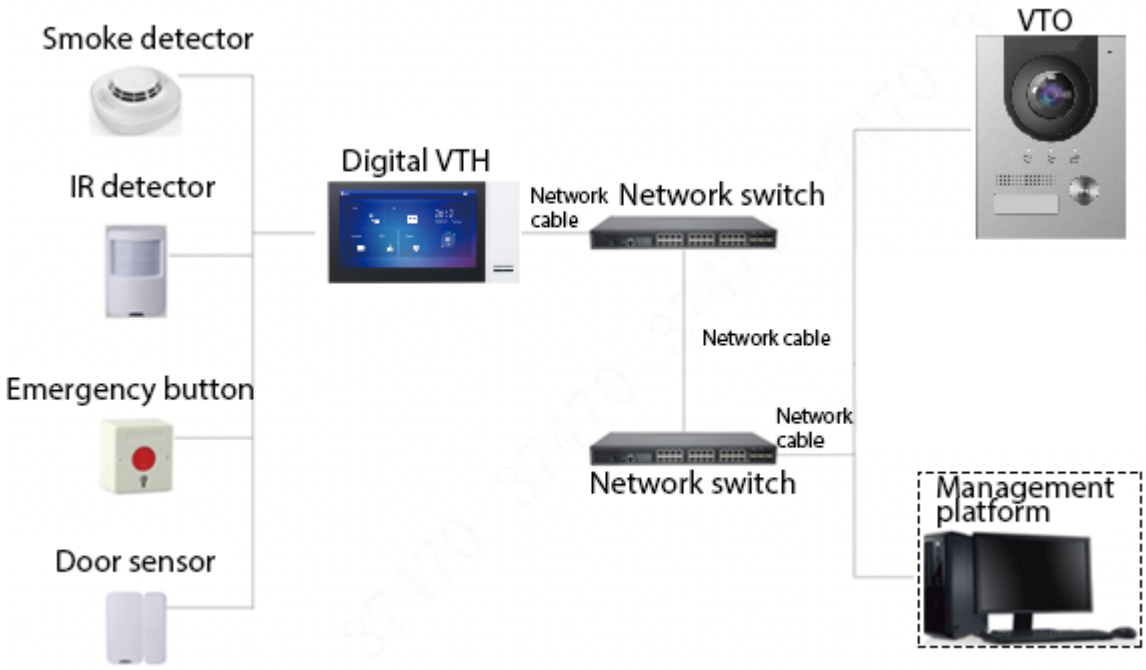
- Nie podłączaj zasilacza do urządzenia, gdy zasilacz jest włączony.
- Należy ściśle przestrzegać lokalnych przepisów i norm dotyczących bezpieczeństwa elektrycznego. Upewnij się, że napięcie otoczenia jest stabilne i spełnia wymagania zasilania urządzenia.
- Nie podłączaj urządzenia do dwóch lub więcej 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 Schemat sieci

Figure 1-1 Internetowy diagram



W niektórych aplikacjach, takich jak willa, Centrum/Platforma Zarządzania jest zwykle niepotrzebna.

2 Wygląd

2.1 VTO2101E-P

2.1.1 Panel przedni

Figure 2-1 VTO2101E-P

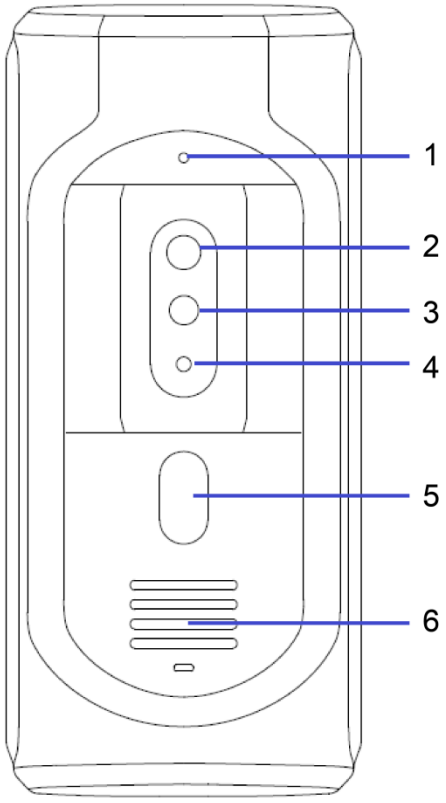


Tabela 2-1 Opis panelu przedniego

NIE.	Nazwa	Opis
1	Mikrofon	—
2	Kamera	—
3	Światło oświetlające IR	Zapewnia dodatkowe światło podczerwone dla kamery, gdy jest ciemno.
4	Czujnik światła	Wykrywa warunki oświetlenia otoczenia.
5	Przycisk dzwonienia	Zadzwoń do VTH lub centrum zarządzania.
6	Głośnik	—

2.1.2 Panel tylny

Figure 2-2 VTO2101E-P

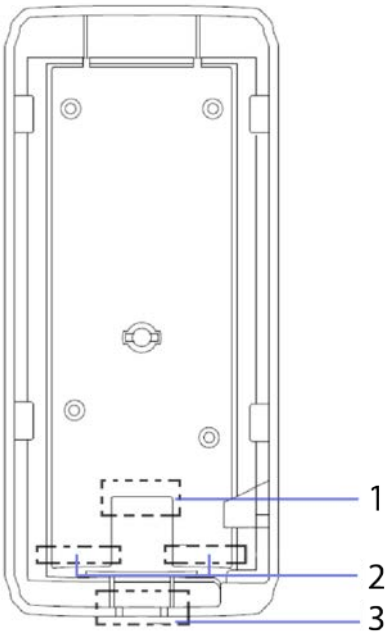


Tabela 2-2 Opis panelu tylnego

NIE.	Nazwa	Opis
1	Port sieciowy	Łączy się z kablem sieciowym.
2	Porty RS-485	Patrz rysunek i tabela poniżej.
3	Wyjście kablowe	Tutaj przeciągnij kable.

Figure 2-3 Połączenie kablowe

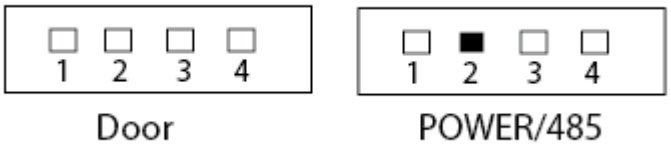


Tabela 2-3 Opis portu

DRZWI		MOC/485	
NIE.	Nazwa	NIE.	Nazwa
1	NIE	1	+ 12 V
2	NC	2	GND
3	KOM	3	RS-485A
4	ALARM IN lub Odblokuj (domyślnie)	4	RS-485B

2.2 VTO2202F-P-S2/VTO2202F-P/VTO2202F/VTO2201F-P

2.2.1 Panel przedni

Figure 2-4 Przedni panel

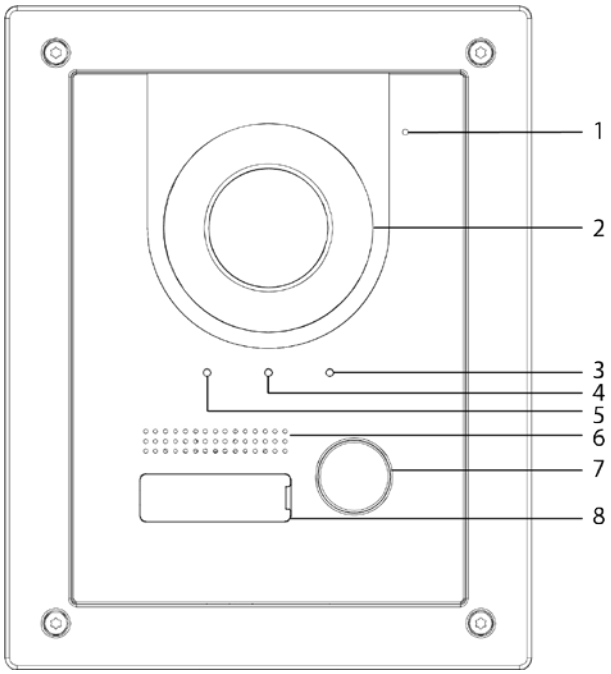


Tabela 2-4 Opis panelu przedniego

NIE.	Nazwa	Opis
1	Mikrofon	—
2	Kamera	—
3	Wskaźnik	Świeci: Drzwi odblokowane.
4		Wł.: podczas połączenia.
5		Włączone: dzwonię.
6	Głośnik	—
7	Przycisk dzwonienia	Zadzwoń do innego VTH lub centrum zarządzania.
8	Etykieta z nazwą	Nazwa hosta.

2.2.2 Panel tylny

Figure 2-5 Tylny panel

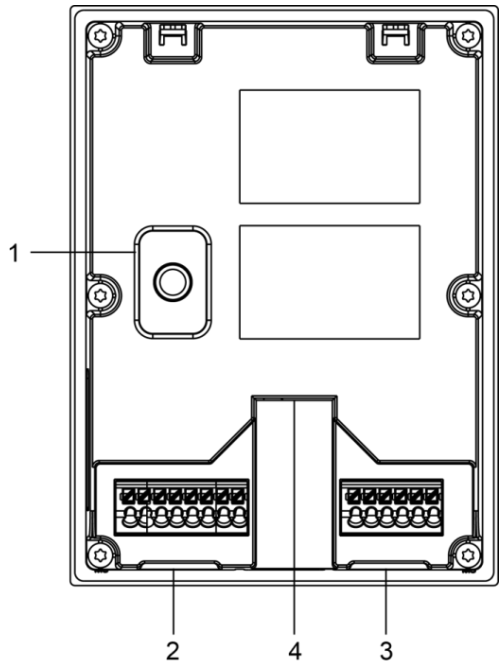


Tabela 2-5 Opis panelu tylnego

NIE	Nazwa	Opis
1	Ochrona przed manipulacją przełącznik	Kiedy VTO zostanie na siłę usunięte ze ściany, zostanie uruchomiony alarm, a informacja o alarmie zostanie wysłana do centrum zarządzania.
2	Port	Od lewej do prawej: GND + 12V_WYJ RS485_B RS485_A ALARM_NIE ALARM_COM VTO2202F-P-S2: 2-przewodowe + (48 V); VTO2202F-P i VTO2202F: EOC1 (+12V); VTO2201F: +24 V. VTO2202F-P-S2: 2-przewodowe - (GND); VTO2202F-P i VTO2202F: EOC2 (GND); VTO2201F: GND.
3		Od lewej do prawej: DOOR_BUTTON DOOR_FB GND DRZWI_NC DOOR_COM DRZWI_NR
4	Port Ethernet	Łączy się z siecią za pomocą kabla Ethernet. Tylko modele z literą „P” obsługują PoE.

2.3 VTO2111D-P-S2/VTO1101D-P

2.3.1 Panel przedni

Figure 2-6 Przedni panel

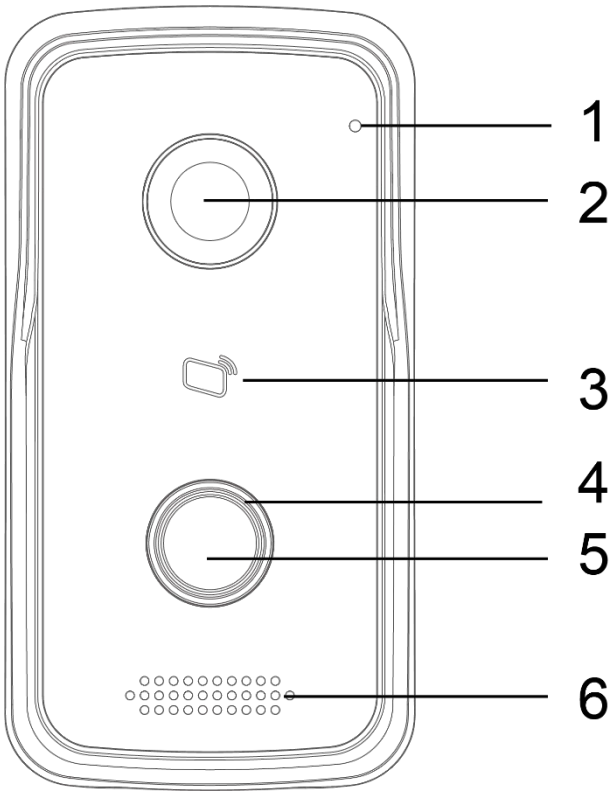


Tabela 2-6 Opis panelu przedniego

NIE.	Nazwa	Opis
1	Mikrofon	—
2	Kamera	—
3	Strefa odczytu kart	Przesuń, aby odblokować lub wydać kartę.
4	Wskaźnik	• Stałe niebieskie: tryb gotowości. • Miga na niebiesko: Trwa połączenie lub brak sieci.
5	Przycisk dzwonienia	Zadzwoń do VTH lub centrum zarządzania.
6	Głośnik	—

2.3.2 Panel tylny

Figure 2-7 Tylny panel

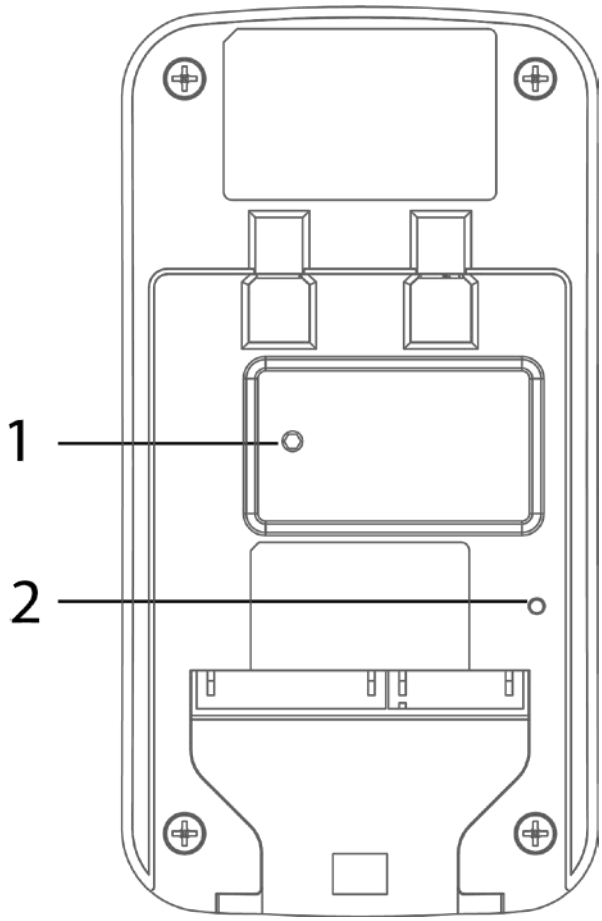


Tabela 2-7 Opis panelu tylnego

NIE.	Nazwa	Opis
1	Ochrona przed manipulacją przełącznik	Kiedy VTO zostanie na siłę usunięte ze ściany, zostanie uruchomiony alarm, a informacja o alarmie zostanie wysłana do centrum zarządzania.
2	RESETOWANIE	Naciśnij i przytrzymaj przez 10 sekund, aby zresetować wszystkie ustawienia.

Figure 2-8 Połączenie kablowe

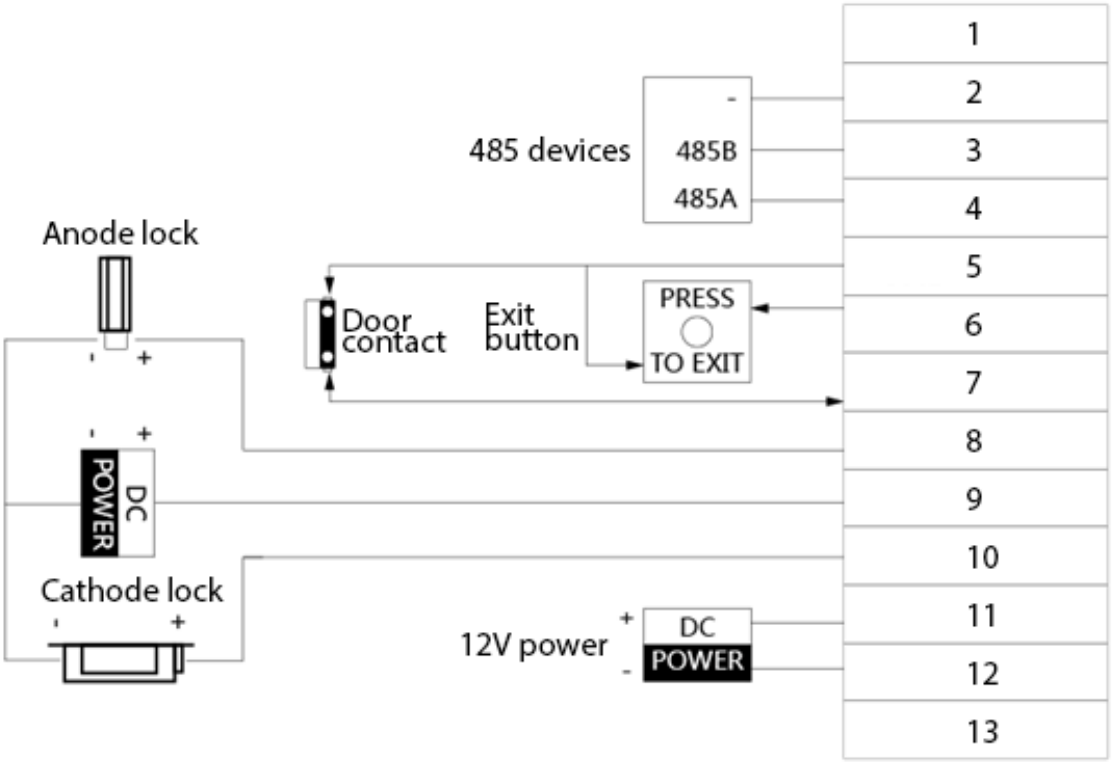


Tabela 2-8 Opis portu

NIE.	Opis	NIE.	Opis
1	Nie dotyczy	8	NC
2	GND	9	KOM
3	485_B	10	NIE
4	485_A	11	GND
5	GND	12	12 V
6	ODBLOKOWAĆ	13	INTERNET
7	INFORMACJA ZWROTNA	—	—

2.4 VTO3211D-P-S2

2.4.1 Panel przedni

Liczba przycisków na panelu przednim różni się w zależności od modelu. VTO3211D-P-S2 ma jeden przycisk, VTO3211D-P2-S2 ma dwa przyciski, a VTO3211D-P4-S2 ma cztery przyciski. Tutaj bierzemy jako przykład VTO3211D-P4-S2.

Figure 2-9 VTO3211D-P4-S2

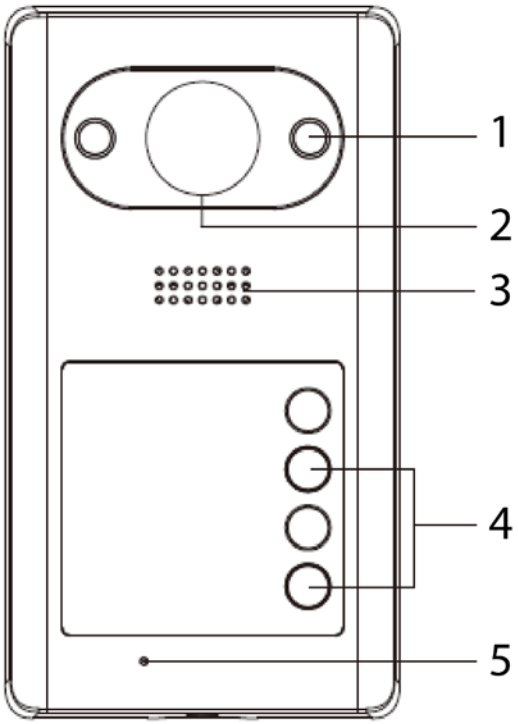


Tabela 2-9 Opis panelu przedniego

NIE.	Nazwa	Opis
1	Oświetlacz podczerwieni	Zapewnia dodatkowe światło podczerwone dla kamery, gdy jest ciemno.
2	Kamera	—
3	Głośnik	—
4	Przycisk dzwonienia	Zadzwoń do VTH lub centrum zarządzania.
5	Mikrofon	—

2.4.2 Panel tylny

Figure 2-10 VTO3211D-P4

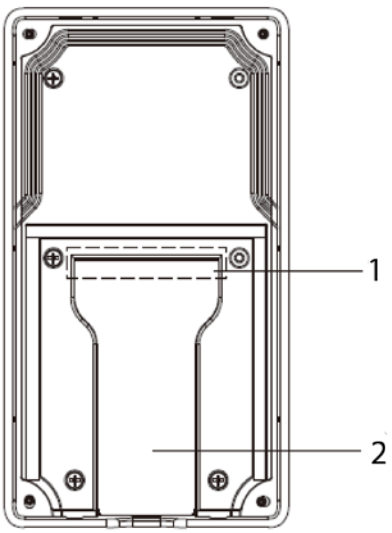


Tabela 2-10 Opis panelu tylnego

NIE.	Nazwa	Opis
1	Porty kablowe	Patrz rysunek i tabela poniżej.
2	Wyjście kablowe	Tutaj przeciągnij kable.

Figure 2-11 Połączenie kablowe

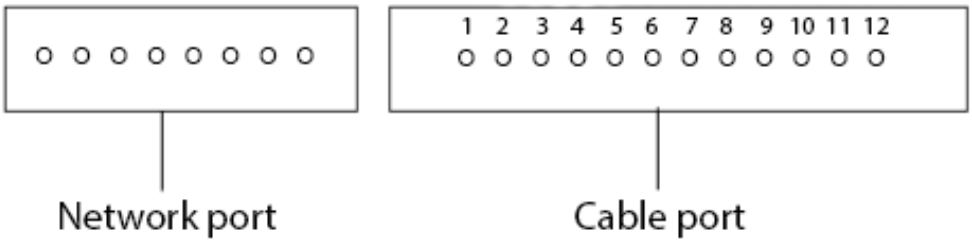


Tabela 2-11 Opis portu kablowego

NIE.	Nazwa	NIE.	Nazwa
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DRZWI_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DRZWI_NR
5	RS485A	11	GND
6	DRZWI OTWARTE	12	prąd stały 12 V

2.5 VTO3221E-P

2.5.1 Panel przedni

Figure 2-12 Przedni panel

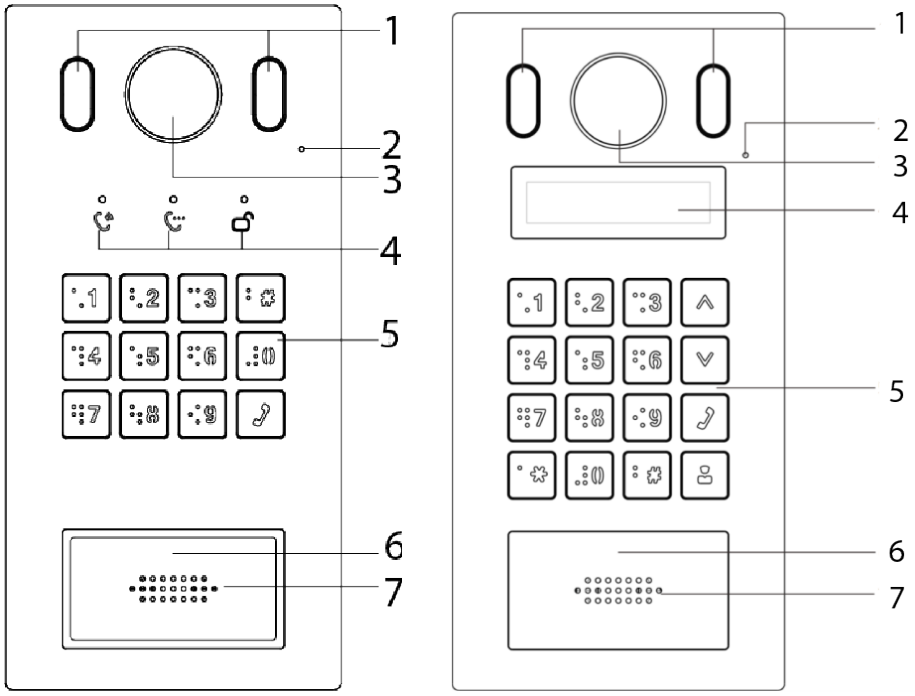


Tabela 2-12 Opis panelu przedniego

NIE.	Nazwa	Opis
1	Iluminator	Zapewnia dodatkowe światło dla aparatu, gdy jest ciemno.
2	Mikrofon	—
3	Kamera	—
4	Wskaźniki	Wyświetla status połączenia, rozmowy i odblokowania.
5	Klawiatura	—
6	Strefa odczytu kart	Przesuń kartę tutaj, aby odblokować drzwi.
7	Głośnik	—

2.5.2 Panel tylny

Figure 2-13 VTO3221E-P

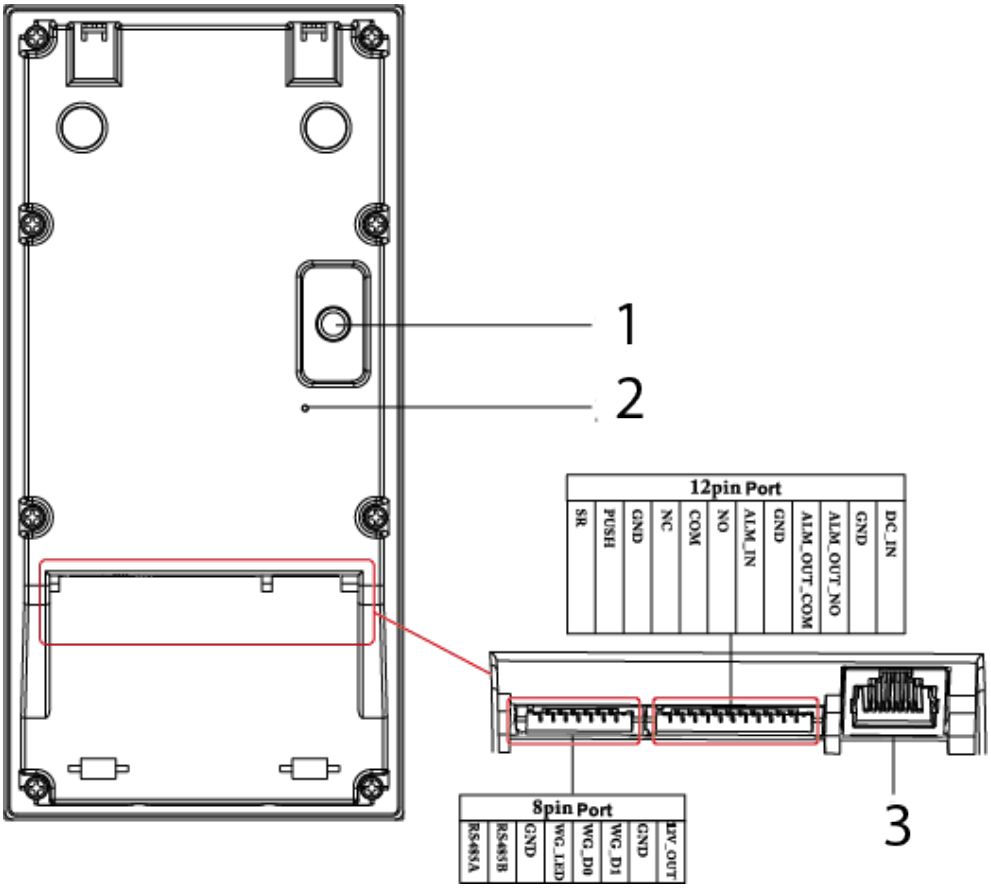


Tabela 2-13 Opis panelu tylnego

NIE.	Nazwa	Opis
1	Ochrona przed manipulacją przełącznik	Kiedy VTO zostanie na siłę usunięte ze ściany, zostanie uruchomiony alarm, a informacja o alarmie zostanie wysłana do centrum zarządzania.
2	Przycisk reset	Naciśnij i przytrzymaj przez 10 s, aby zresetować wszystkie ustawienia.
3	Port Ethernet	Umożliwia podłączenie kabla Ethernet.

2.6 VTO2211G-P/VTO1201G-P

2.6.1 Panel przedni

Figure 2-14 Panel przedni VTO2211G/VTO1201G

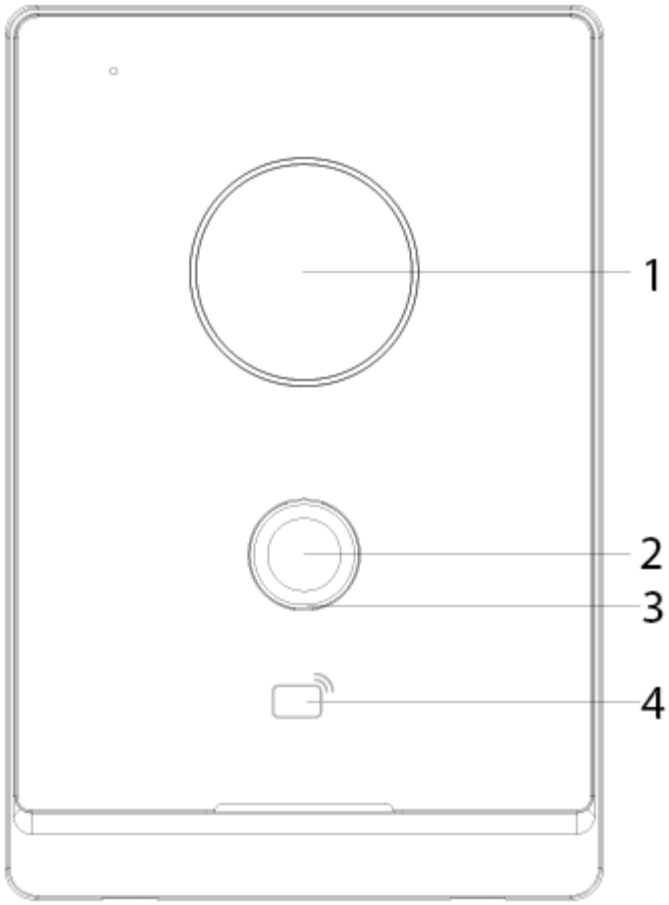


Tabela 2-14 Opis panelu przedniego

NIE.	Nazwa	Opis
1	Kamera	—
2	Przycisk dzwonienia	Zadzwoń do VTH lub centrum zarządzania.
3	Wskaźnik	• Wyłączona: urządzenie znajduje się w trybie gotowości. • Świeci na zielono: wykonywanie połączenia. • Świeci na niebiesko: trwa połączenie. • Żółto-zielony: Drzwi otwarte przez VTH podczas wykonywania połączenia przez VTO. Czerwono- • niebieski: Drzwi odblokowane przez VTH, gdy VTO jest w trakcie połączenia. • Niebieski oddech: Sieć rozłączona.
4	Czytnik kart obszar	Przesuń kartę w tym miejscu, aby odblokować drzwi (tylko dla VTO2211G-P).

2.6.2 Panel tylny

Figure 2-15 Panel tylny VTO2211G-P/VTO1201G-P

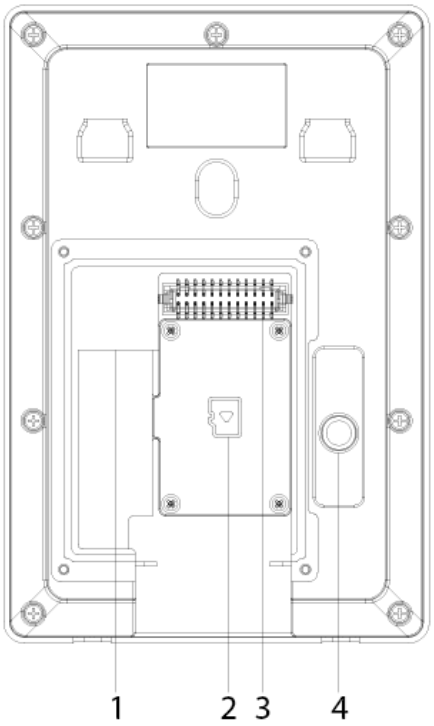
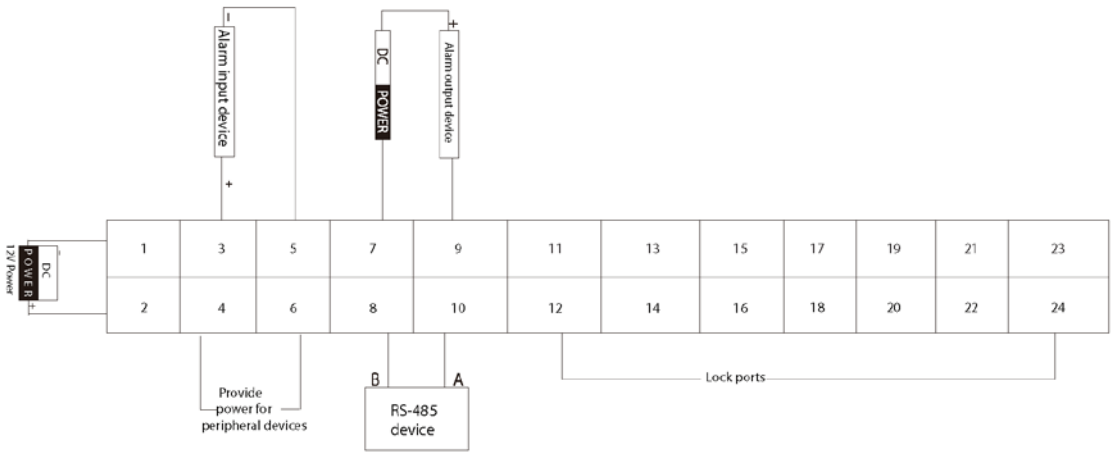


Tabela 2-15 Opis panelu tylnego

NIE.	Opis	NIE.	Opis
1	Port sieciowy	3	Porty
2	Osłona karty SD	4	Przełącznik antysabotażowy

Figure 2-16 Połączenie kablowe VTO2211G-P



Porty 12, 14, 16, 18, 20, 22 i 24 służą do podłączenia zamków.

Tabela 2-16 Opis portu

NIE.	Nazwa	NIE.	Nazwa
1	DC_IN-	13	Niedostępne
2	DC_IN+	14	DOOR1_COM

NIE.	Nazwa	NIE.	Nazwa
3	ALARM_IN	15	Niedostępne
4	+ 12V_WYJ	16	DRZWI1_NIE
5	GND	17	Niedostępne
6	GND	18	GND
7	ALARM_NIE	19	Niedostępne
8	RS485B	20	DOOR1_FB
9	ALARM_COM	21	Niedostępne
10	RS485A	22	GND
11	Niedostępne	23	Niedostępne
12	DRZWI1_NC	24	DRZWI1_PUSH

Figure 2-17 Połączenie kablowe VTO1201G-P

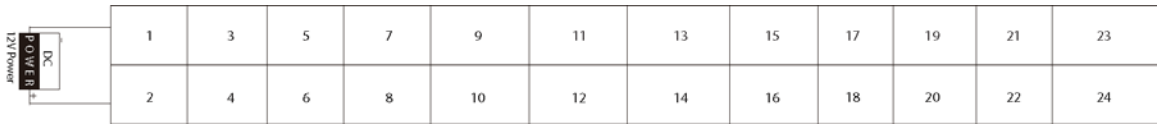
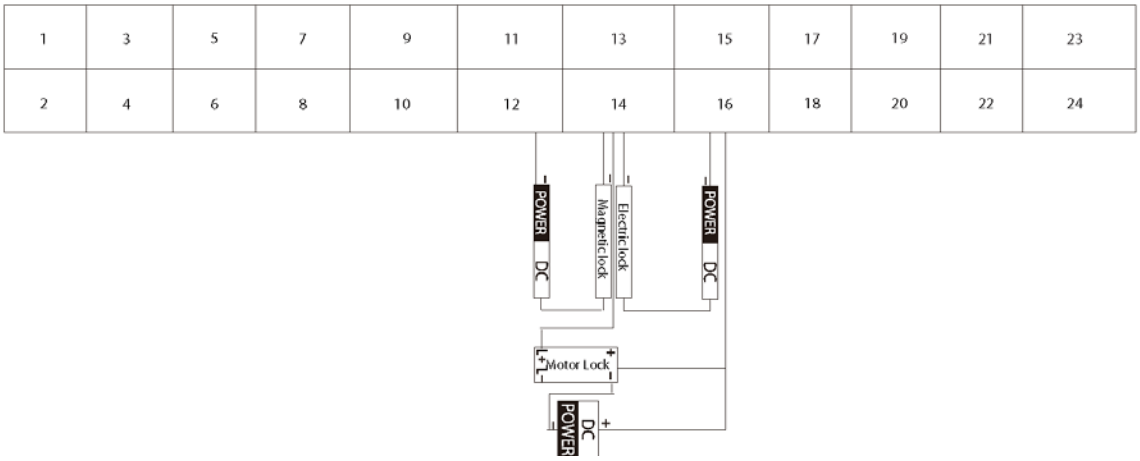


Tabela 2-17 Opis portu

NIE.	Nazwa
1	DC_IN-
2	DC_IN+
3-24	Zarezerwowana funkcja

Figure 2-18 Zablokuj połączenie kablowe

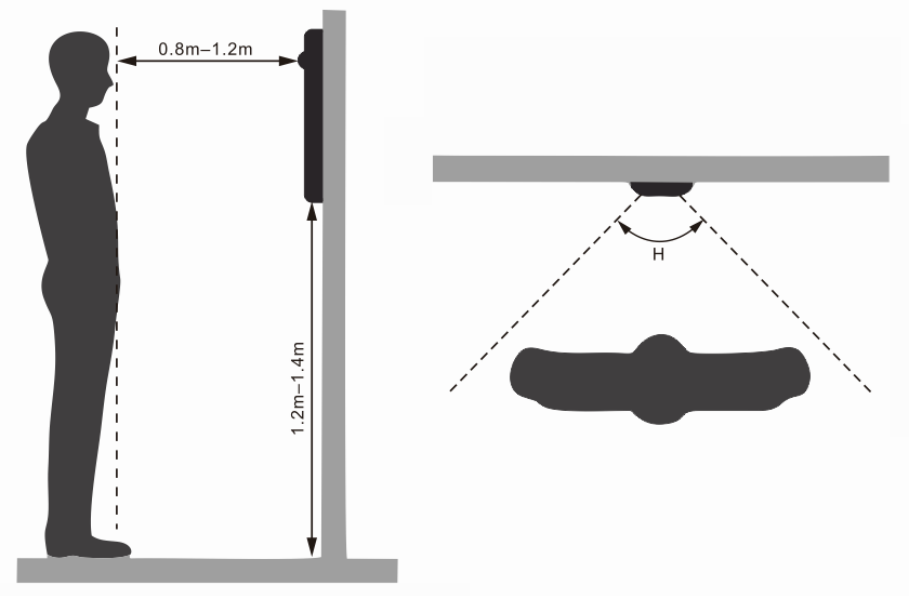


W razie potrzeby można podłączyć zamek magnetyczny lub zamek elektryczny. Zobacz powyższy rysunek, aby zapoznać się z zasadami połączenia z portem.

3 Instalacja

- Instalacja i konfiguracja muszą być wykonane przez profesjonalne zespoły. Jeśli chcesz naprawić urządzenie, skontaktuj się z pomocą techniczną.
- Patrz rysunek poniżej, aby zapoznać się z pozycją montażową. Poziomy kąt widzenia urządzenia różni się w zależności od modelu, a ludzka twarz powinna być skierowana na środek urządzenia.

Figure 3-1 Pozycja montażowa



4 Konfiguracja

W tym rozdziale przedstawiono podstawowe konfiguracje urządzeń VTO i VTH. Szczegółowe informacje można znaleźć w instrukcji obsługi.

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

4.1 Procedura

Przed konfiguracją sprawdź każde urządzenie i upewnij się, że nie ma zwarcia lub przerwy w obwodzie.

Step 1 Zaplanuj adres IP i numer (działa jako numer telefonu) dla każdego urządzenia.

Step 2 Skonfiguruj VTO. Patrz „4.3 Konfigurowanie VTO”.

Step 3 Skonfiguruj VTH. Zobacz instrukcję obsługi VTH. Sprawdź, czy

Step 4 wszystkie ustawienia są prawidłowe. Patrz „4.4 Uruchomienie”.

4.2 Narzędzie konfiguracyjne

Możesz pobrać narzędzie konfiguracyjne „VDPConfig” i używać go do konfiguracji i aktualizacji wielu urządzeń. Więcej szczegółów można znaleźć w odpowiedniej instrukcji obsługi.

4.3 Konfiguracja VTO

Podłącz VTO do komputera za pomocą kabla sieciowego i przy pierwszym użyciu musisz utworzyć nowe hasło logowania do interfejsu internetowego.

4.3.1 Inicjalizacja

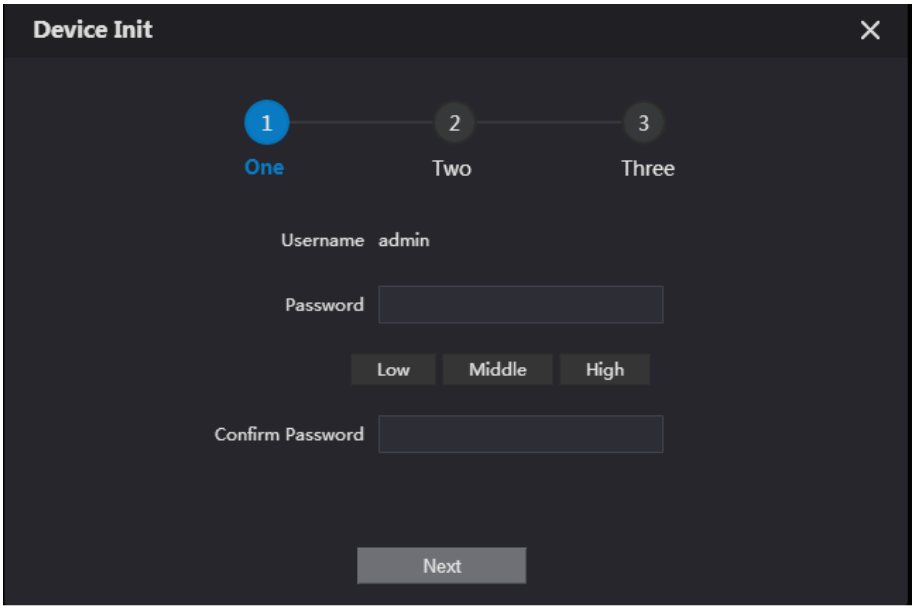
Upewnij się, że komputer znajduje się w tym samym segmencie sieci.

Step 1 Włącz VTO.

Step 2 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.

Figure 4-1 Inicjalizacja urządzenia

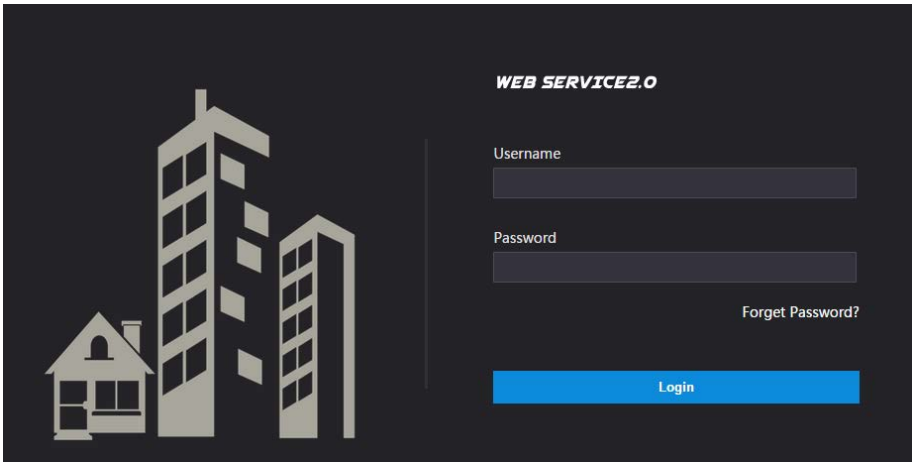


Step 3 Wprowadź i potwierdź nowe hasło, a następnie kliknij**Następny**. Wybierać

Step 4 **E-mail**i wprowadź adres e-mail, aby zresetować hasło. Kliknij**Następny**, a

Step 5 następnie kliknij**OK**aby przejść do interfejsu logowania.

Figure 4-2 Interfejs logowania



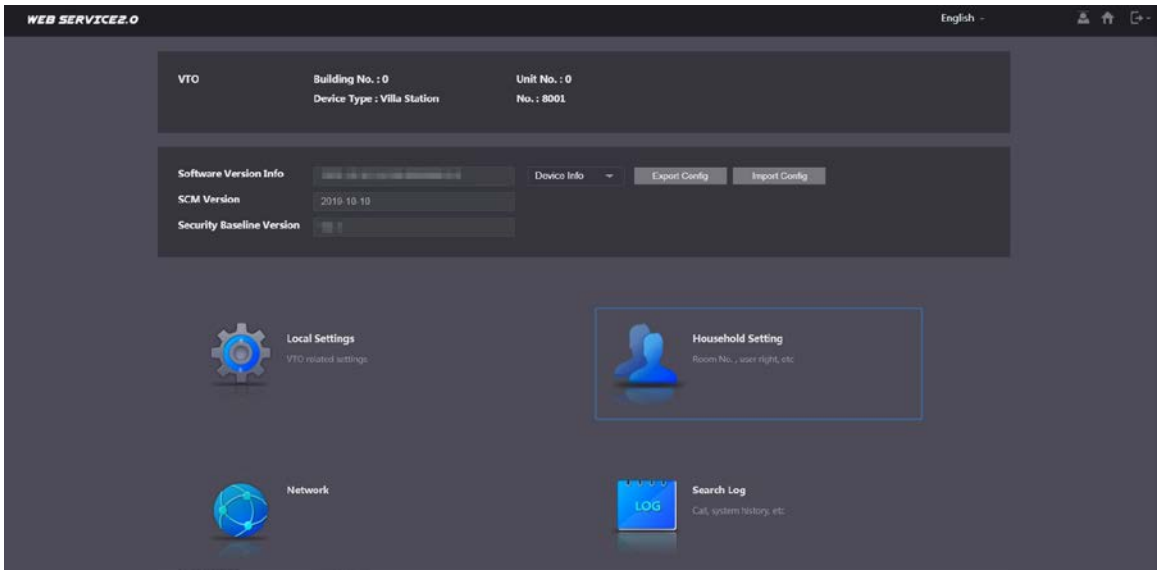
4.3.2 Konfiguracja numeru VTO

Do rozróżnienia każdego VTO można wykorzystać liczby, dlatego zalecamy ustawienie ich zgodnie z numerem jednostki lub budynku.

- Możesz zmienić numer VTO, gdy nie działa ono jako serwer SIP.
- Numer VTO może zawierać maksymalnie 5 cyfr i nie może być taki sam jak numer dowolnego pokoju.

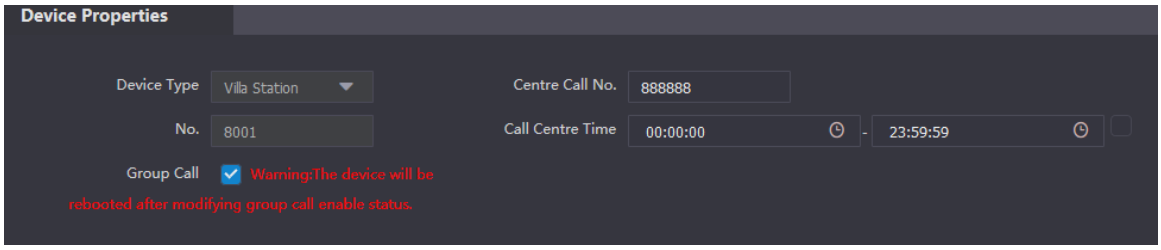
Step 1 Zaloguj się do interfejsu internetowego VTO.

Figure 4-3 Główny interfejs



Step 2 Wybierać**Ustawienia lokalne > Podstawowe**.

Figure 4-4 Właściwości urządzenia

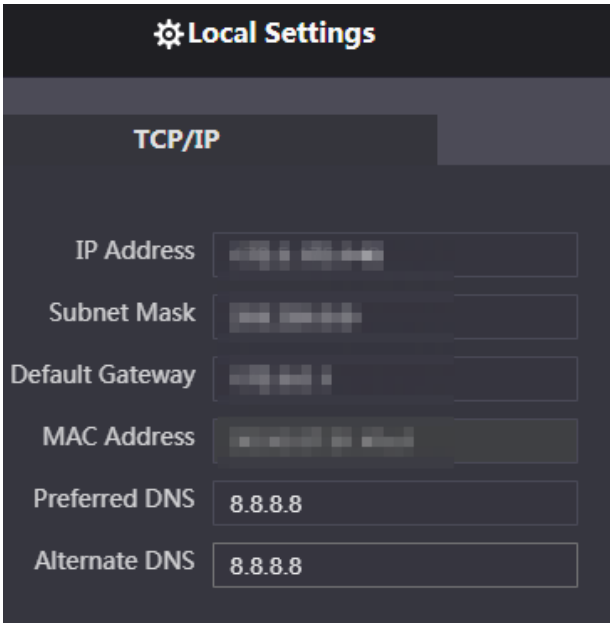


Step 3 Wpisz numer w**NIE.**, a następnie kliknij**Potwierdzać**.

4.3.3 Konfiguracja parametrów sieciowych

Step 1 Wybierać**Sieć > Podstawowe**.

Figure 4-5 Informacje o protokole TCP/IP



Step 2 Wprowadź każdy parametr, a następnie kliknij**Ratować**.

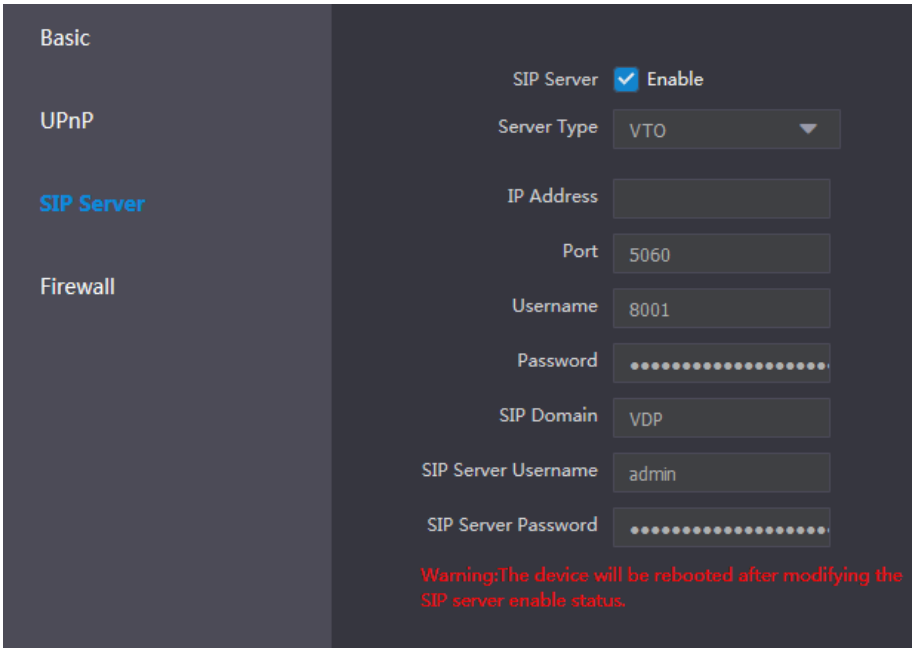
VTO zostanie automatycznie ponownie uruchomiony. Aby zalogować się ponownie, musisz dodać adres IP swojego komputera do tego samego segmentu sieci, co VTO.

4.3.4 Konfiguracja serwera SIP

Po podłączeniu do tego samego serwera SIP wszystkie VTO i VTH mogą się ze sobą łączyć. Jako serwera SIP możesz użyć VTO lub innego serwera.

Step 1 Wybierać**Sieć > Serwer SIP**.

Figure 4-6 Serwer SIP



Step 2 Wybierz typ serwera według potrzeb.

- Jeśli bieżący VTO działa jako serwer SIP, włącz**Serwer SIP**, a następnie kliknij**Ratować**. VTO zostanie automatycznie zrestartowane, a następnie będziesz mógł dodać inne VTO i VTH do tego VTO. Patrz „4.3.6 Dodawanie VTO i 4.3.7 Dodawanie numeru pokoju”.

  Jeśli bieżący VTO nie działa jako serwer SIP, nie włączaj**Serwer SIP**. W przeciwnym razie połączenie z tym VTO nie powiedzie się.

- Jeśli inne VTO pracują jako serwer SIP, ustaw**Rodzaj serwera**jako VTO, a następnie skonfiguruj parametry.

Tabela 4-1 Konfiguracja serwera SIP

Parametr	Opis
Adres IP	Adres IP VTO, który działa jako serwer SIP.
Port	● Domyślnie 5060, gdy VTO działa jako serwer SIP. Domyślnie ● 5080, gdy platforma działa jako serwer SIP.
Nazwa użytkownika	Zachowaj wartość domyślną.
Hasło	
Domena SIP	VDP.
Nazwa użytkownika serwera SIP	Nazwa użytkownika i hasło logowania do interfejsu sieciowego serwera SIP.
Hasło serwera SIP	

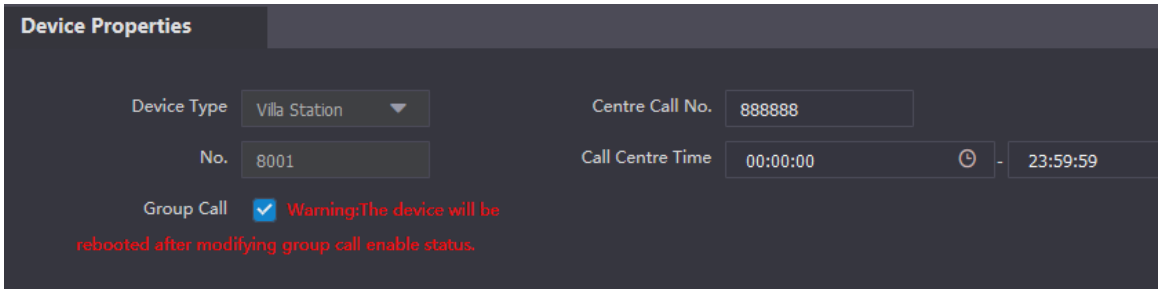
- Jeśli inne serwery działają jako serwer SIP, ustaw**Rodzaj serwera**w razie potrzeby, a następnie zapoznaj się ze szczegółami w odpowiedniej instrukcji.

4.3.5 Konfiguracja numeru połączenia i połączenia grupowego

Aby wybrać i zadzwonić do VTO, musisz skonfigurować numer połączenia na każdym VTO, który działa jako numer telefonu.

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

Figure 4-7 Właściwości urządzenia



Step 2 w**NIE.**wprowadź numer pokoju, do którego chcesz zadzwonić, a następnie kliknij**Potwierdzać**zapisać. Powtórz tę operację na każdym interfejsie internetowym stacji bramowej (VTO).

Na serwerze SIP możesz włączyć funkcję połączeń grupowych. Podczas wywoływania głównego VTH, wszystkie numery wewnętrzne VTH również odbiorą połączenie.

VTO uruchomi się ponownie po włączeniu lub wyłączeniu funkcji wywołania grupowego.

Step 3 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz**Ustawienia lokalne > Podstawowe**. Włączać

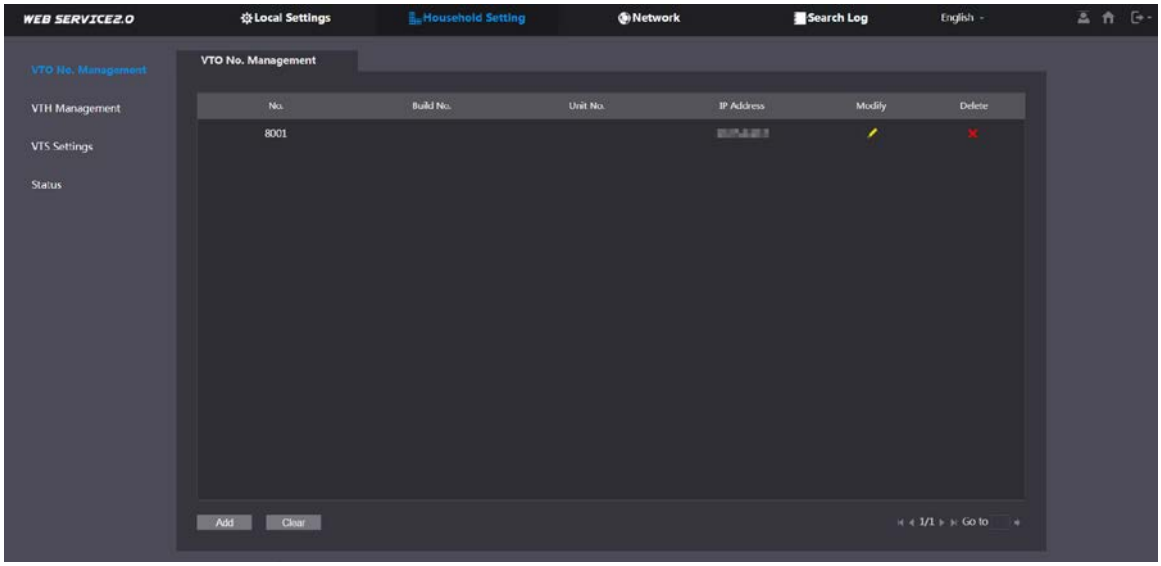
Step 4 **Połączenie grupowe**, Kliknij**Potwierdzać**, a następnie VTO uruchomi się ponownie.

4.3.6 Dodawanie VTO

Możesz dodać VTO do serwera SIP, a wszystkie VTO podłączone do tego samego serwera SIP będą mogły nawiązywać między sobą połączenia wideo. Ta sekcja ma zastosowanie, gdy VTO działa jako serwer SIP i jeśli używasz innych serwerów jako serwera SIP, zapoznaj się z odpowiednią instrukcją, aby uzyskać szczegółową konfigurację.

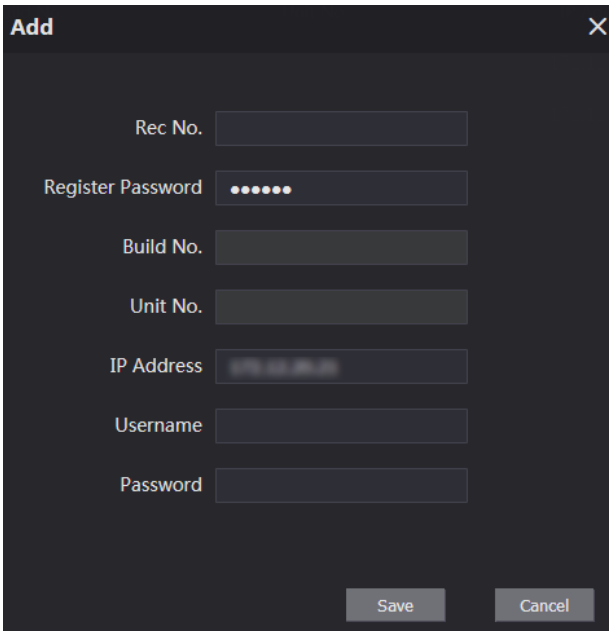
Step 1 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Zarządzanie numerami VTO**.

Figure 4-8 Zarządzanie numerem VTO



Step 2 Kliknij**Dodać**.

Figure 4-9 Dodaj VTO



Step 3 Skonfiguruj parametry.

Należy dodać serwer SIP.

Tabela 4-2 Dodawanie stacji zewnętrznych (VTO)

Parametr	Opis
Nr ref.	numer VTO. Patrz „4.3.2 Konfigurowanie numeru VTO”.
Zarejestruj hasło	Zachowaj wartość domyślną.
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 logowania do interfejsu internetowego VTO.

Step 4 Kliknij**Ratować**.

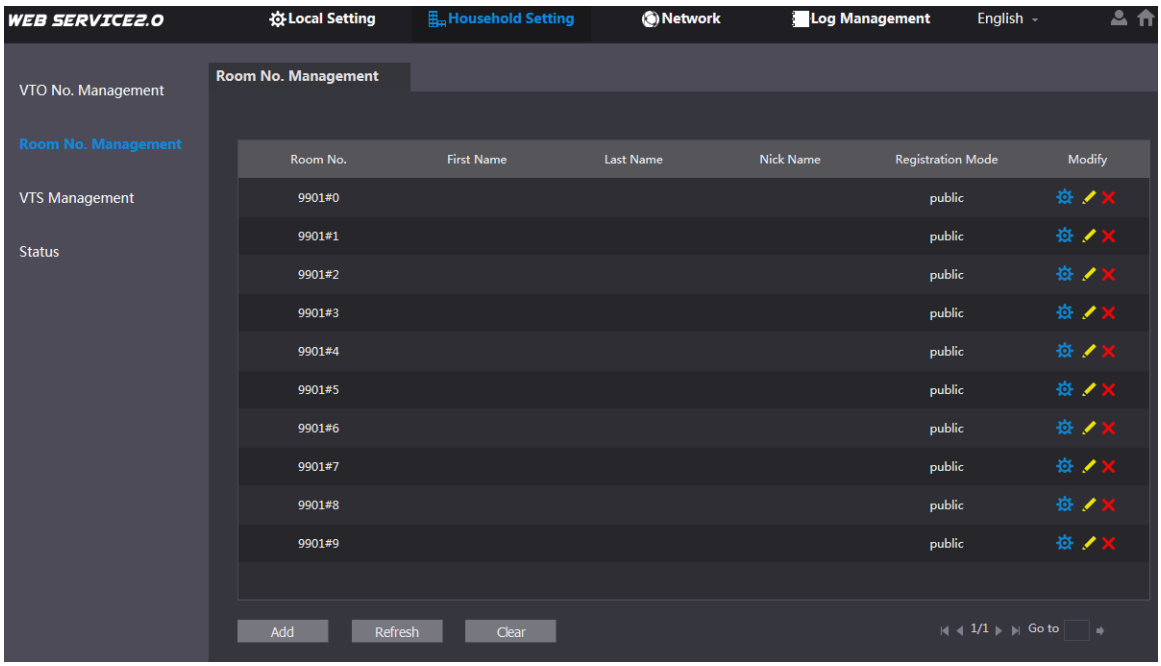
4.3.7 Dodawanie numeru pokoju

Możesz dodać numery pokoi do serwera SIP, a następnie skonfigurować numer pokoju na VTH, aby połączyć je z siecią. Ta sekcja ma zastosowanie, gdy VTO działa jako serwer SIP i jeśli używasz innych serwerów jako serwera SIP, zapoznaj się z odpowiednią instrukcją, aby uzyskać szczegółową konfigurację.

Numer pokoju może składać się maksymalnie z 6 cyfr lub liter lub ich kombinacji nie może być taki sam jak dowolny numer VTO.

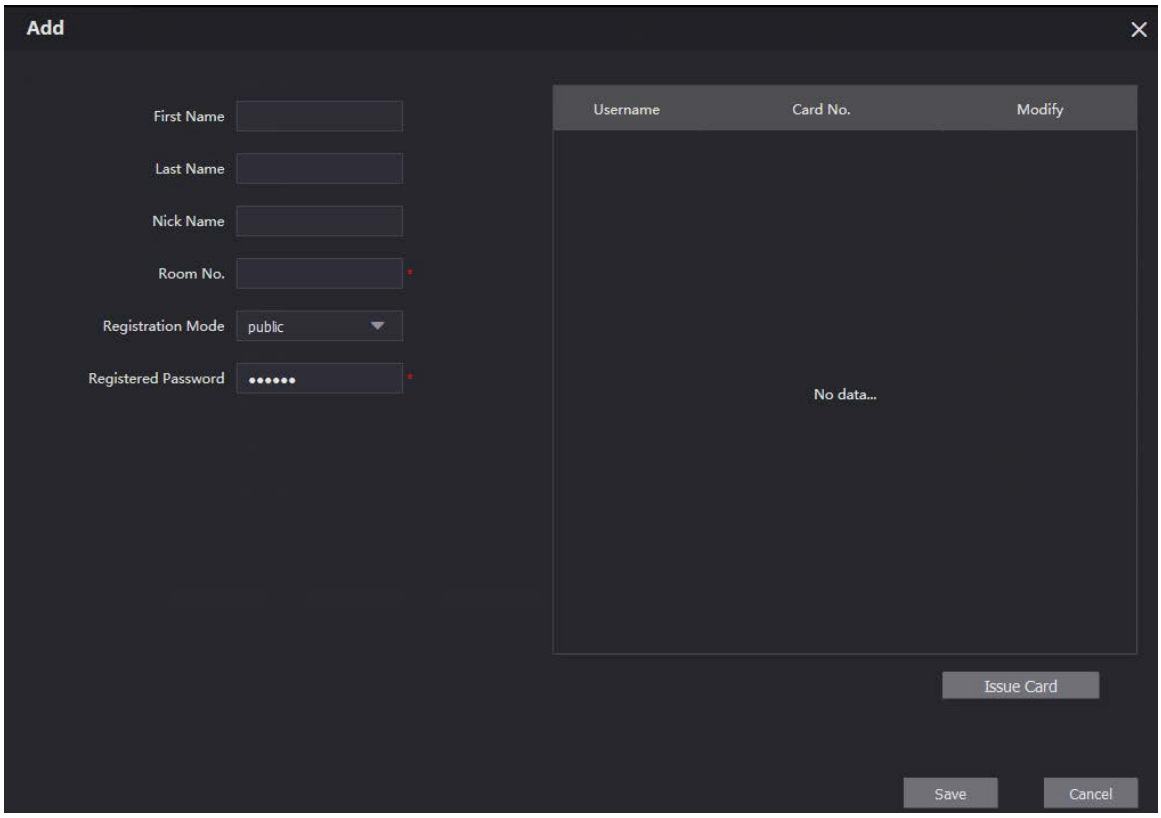
Step 1 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz**Ustawienia gospodarstwa domowego > Zarządzanie numerami pokoi**.

Figure 4-10 Zarządzanie numerami pokoi



Step 2 Kliknij**Dodać**.

Figure 4-11 Dodaj pojedynczy numer pokoju



Step 3 Skonfiguruj informacje o pokoju.

Tabela 4-3 Informacje o pokojach

Parametr	Opis
Imię	Informacje wykorzystywane do odróżnienia każdego pokoju.
Nazwisko	
Przezwisko	
Pokój numer.	Numer pokoju.

Parametr	Opis
	- Jeżeli istnieje wiele VTH, numer pokoju głównego VTH powinien kończyć się na #0, a numer pokoju dla dodatkowego VTH powinien kończyć się na #0. #1, #2... - Można skonfigurować do 9 rozszerzeń VTH dla jednego głównego VTH.
Tryb rejestracji	Wybierać**publiczny**.
Zarejestrowane hasło	Zachowaj wartość domyślną.

Step 4 Kliknij**Ratować**.

Kliknij , aby zmodyfikować informacje o pokoju i kliknij aby usunąć pokój.

4.4 Uruchomienie

4.4.1 VTO Wywołanie VTH

Step 1 Wybierz numer pokoju na VTO.

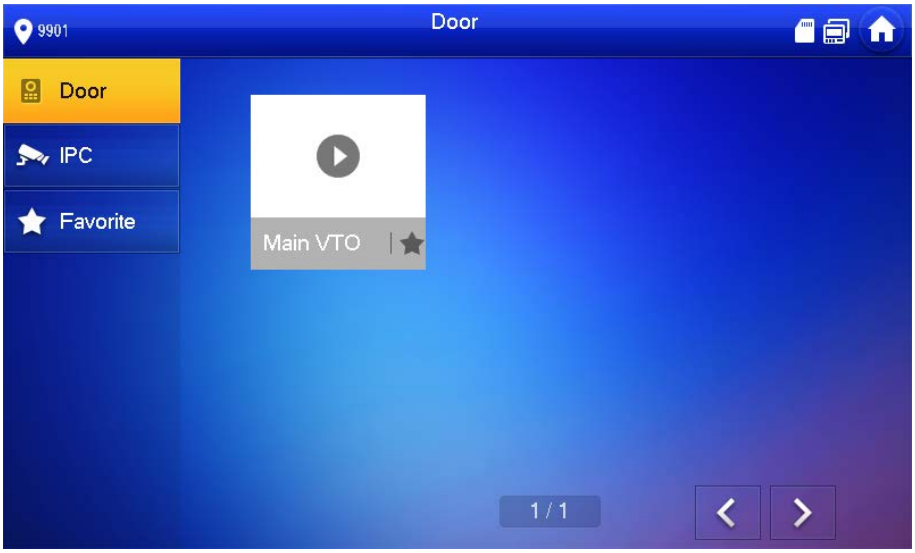
Step 2 Uzyskiwać na VTH, aby odebrać połączenie.

Figure 4-12 Ekran połączenia

4.4.2 Monitorowanie VTH VTO

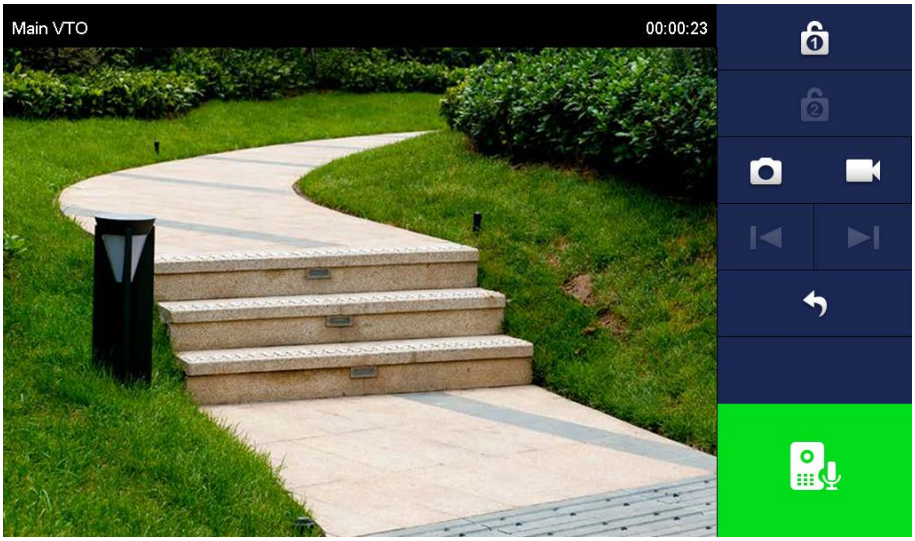
Step 1 W głównym interfejsie VTH wybierz**Monitor > Drzwi**.

Figure 4-13 Drzwi



Step 2 Wybierz VTO.

Figure 4-14 Monitorowanie wideo



5 EasyViewer Plus

EasyViewer Plus (zwana dalej „aplikacją”) umożliwia zarządzanie urządzeniami, odtwarzanie filmów, otwieranie drzwi i nie tylko.

Przed dodaniem VTO do aplikacji należy połączyć VTO z routerem poprzez Wi-Fi lub podłączyć VTO do routera za pomocą przełącznika, a następnie ręcznie zmienić adres IP VTO na tę samą sieć, w której znajduje się VTO router, jeśli protokół DHCP nie jest obsługiwany.

Pobierz aplikację ze sklepu z aplikacjami na swoim smartfonie. W aplikacji wybierz**Ustawienia > Pomoc i opinie**aby wyświetlić instrukcje dotyczące każdej funkcji.

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, zaleca się 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, zaleca się 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.