Cyfrowy VTH

Skrócona instrukcja obsługi

Wersja 1.0.1

Przedmowa

Ogólny

Dokument ten przedstawia głównie strukturę, proces instalacji i konfigurację produktu.

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.	sierpień 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.

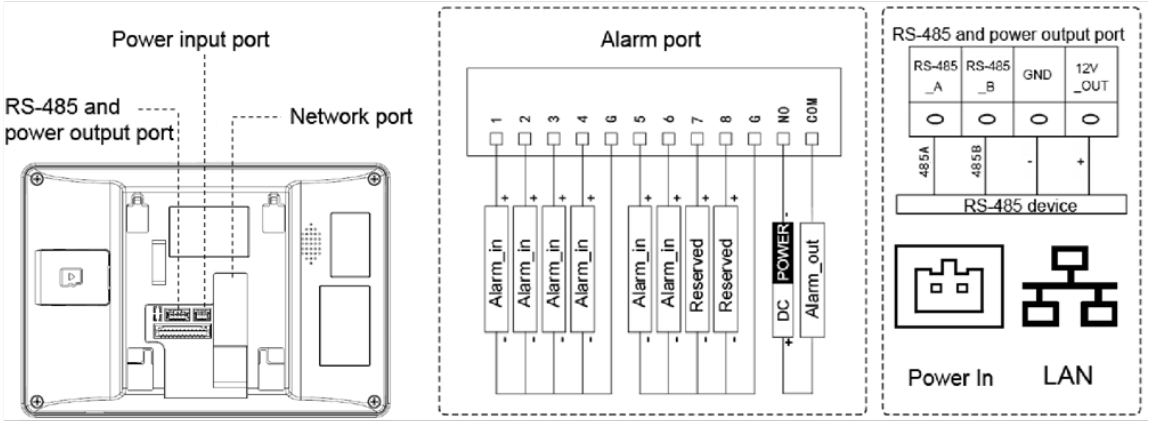
- Personel pracujący na wysokościach musi podjąć wszelkie niezbędne środki w celu zapewnienia bezpieczeństwa osobistego, w tym nosić kask i pasy bezpieczeństwa.
- Nie należy umieszczać urządzenia w miejscu narażonym na działanie promieni słonecznych lub w pobliżu źródeł ciepła.
- Trzymaj urządzenie z 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 port na panelu tylnym

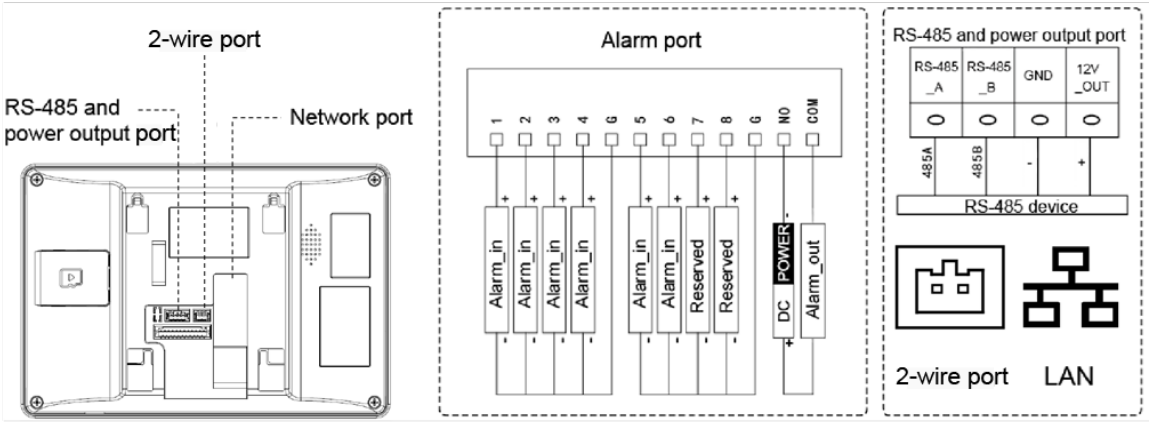
1.1 VTH5421H

Figure 1-1 Panel tylny VTH5421H



1.2 VTH5422H

Figure 1-2 Panel tylny VTH5422H



2 Instalacja i uruchomienie

2.1 Instalacja

⚠

- Nie instaluj VTH w trudnych warunkach z kondensacją, wysoką temperaturą, kurzem i korozją substancji i bezpośredniego światła słonecznego.
- W przypadku wystąpienia nieprawidłowości po włączeniu zasilania należy odłączyć kabel sieciowy i odciąć zasilanie o godz raz. Włącz zasilanie po rozwiązaniu problemu.
- Instalacja i debugowanie powinny być wykonywane przez profesjonalne zespoły. Nie demontuj ani nie naprawiaj siebie w przypadku awarii urządzenia. Skontaktuj się z obsługą posprzedażną.
- Wysokość centralnego punktu urządzenia powinna wynosić 1,4 m–1,6 m nad podłożem (to urządzenie jest dostępne wyłącznie na nadaje się do montażu na wysokości ≤ 2 m).

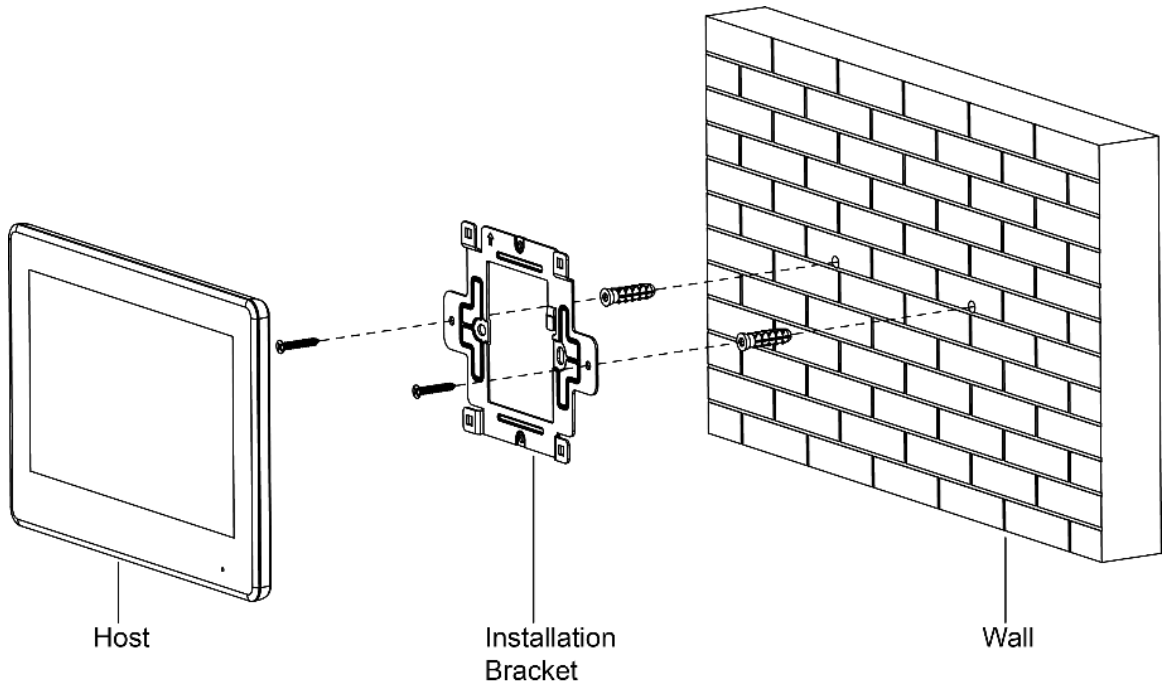
Zamontuj urządzenie bezpośrednio na ścianie za pomocą uchwytu, który jest odpowiedni dla wszystkich typów urządzeń.

Step 1 Wywierć otwory w ścianie zgodnie z położeniem otworów wspornika montażowego.

Step 2 Przymocuj wspornik montażowy do ściany za pomocą śrub.

Step 3 Umieścić urządzenie w uchwycie montażowym od góry do dołu.

Figure 2-1 Instalacja powierzchniowa



2.2 Przygotowania

Przed uruchomieniem należy sprawdzić, czy wykonano poniższe prace.

- Włącz urządzenie dopiero wtedy, gdy nie ma zwarcia lub przerwy w obwodzie.
- Zaplanuj adres IP i numer (działa jako numer telefonu) dla każdego VTO i VTH.
- Potwierdź lokalizację serwera SIP.
- Zeskanuj kod QR na okładce, aby uzyskać szczegółowe informacje.
- Ustaw informacje o VTO i informacje o VTH w interfejsie internetowym dla każdego VTO oraz ustaw informacje o VTH, informacje o sieci i informacje o VTO dla każdego VTH.

Przy pierwszym użyciu skonfiguruj hasło i powiąż e-mail. Hasło służy do wejścia do interfejsu ustawień projektu, natomiast adres e-mail służy do odzyskania hasła, gdy je zapomnisz.

Step 1 Włącz urządzenie, wybierz region i język, a następnie dotknij**OK**.

Figure 2-2 Wybierz region i język

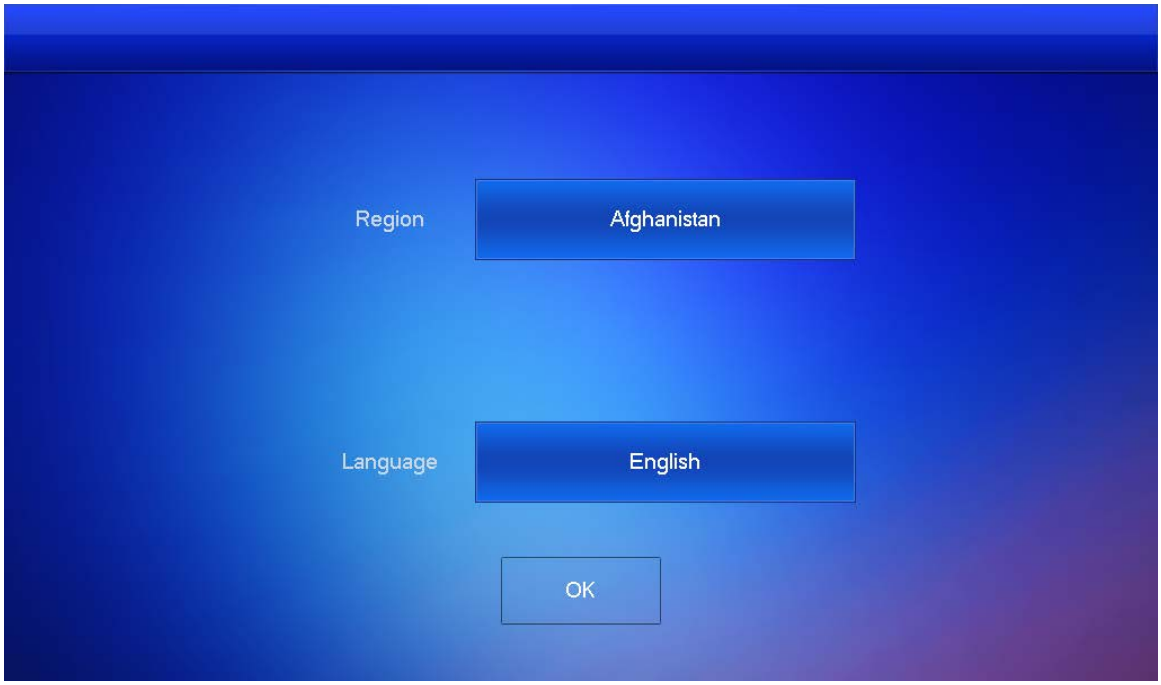


Figure 2-3 Ustaw hasło dla VTH

Step 2 Wprowadź hasło i potwierdź je, wpisz adres e-mail i dotknij**Następny**.

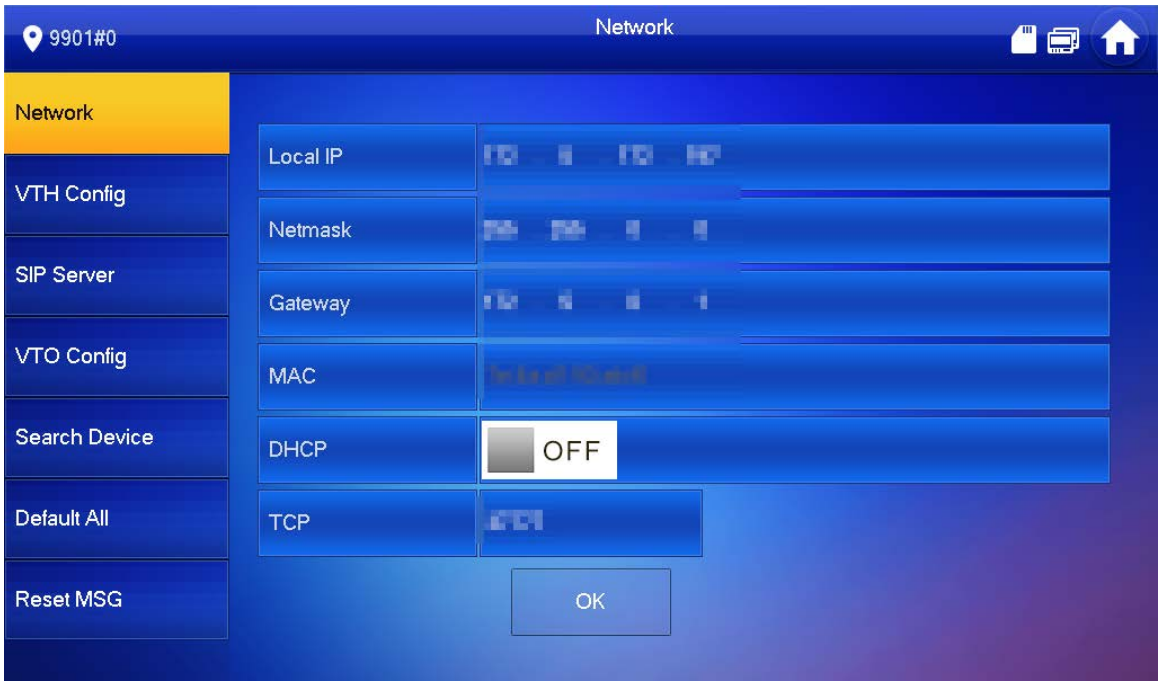
Step 3 Uzyskiwać**Ustawienie**przez ponad 6 sekund, wprowadź ustawione przed chwilą hasło, a następnie dotknij**OK**.

Step 4 Uzyskiwać**Sieć**. Wprowadź lokalny adres IP, maskę sieci i bramę, a następnie dotknij**OK**, Lub dotknij opcji Włącz 

Do funkcję DHCP, aby automatycznie uzyskać informacje o adresie IP.

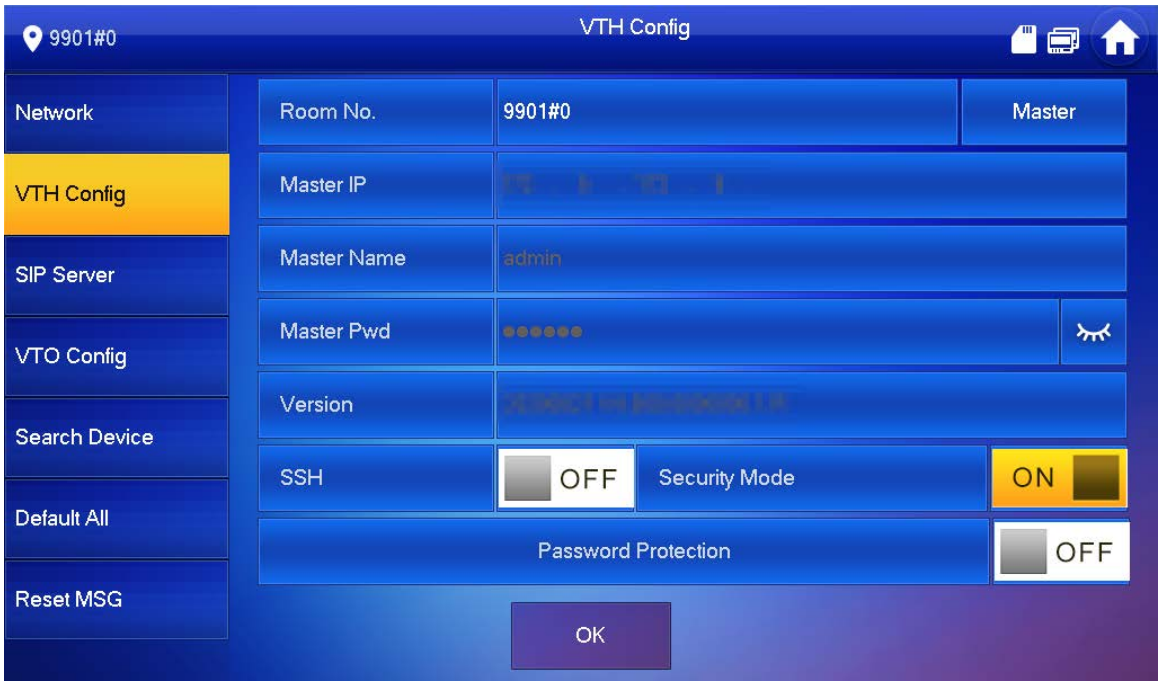
Adresy IP VTH i VTO powinny znajdować się w tym samym segmencie sieci. W przeciwnym razie VTH nie można uzyskać informacji o VTO po konfiguracji.

Figure 2-4 Sieć



Step 5 Uzyskiwać**Konfiguracja VTH**.

Figure 2-5 Konfiguracja VTH



- Użyj jako głównego VTH.

Wprowadź numer pokoju (np. 9901 lub 101#0) i dotknij**OK**.

Numer pokoju powinien być taki sam jak krótki numer VTH, który jest ustawiany podczas dodawania VTH w Internecie interfejs. W przeciwnym razie nie uda się połączyć z VTO.

Jeśli istnieje rozszerzenie VTH, numer pokoju powinien kończyć się na #0. W przeciwnym razie nie uda się nawiązać połączenia WTO.

- Użyj jako rozszerzenia VTH.

1) Stuknij**Gospodarz**i ikona zmienia się na**Rozszerzenie**.

2) Wprowadź numer pokoju (np. 101#1) i adres IP głównego VTH.

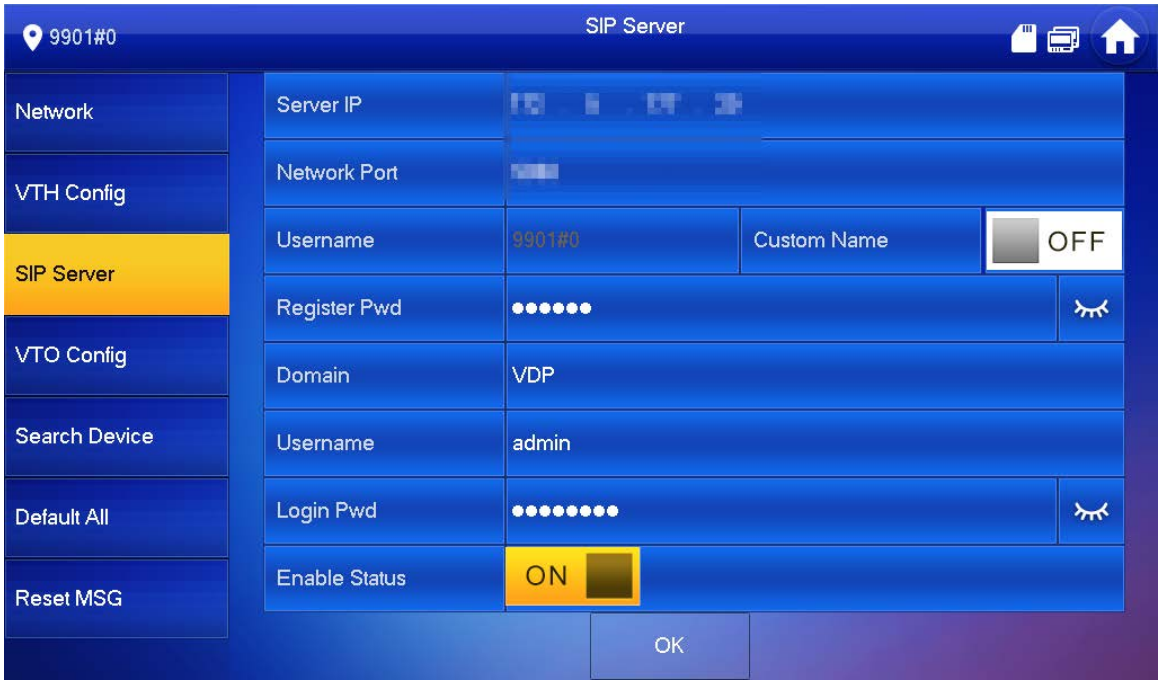
Domyślna nazwa użytkownika to**Admin**, a hasło to to, które zostało ustawione w poprzednim kroku.

Tryb bezpieczeństwa jest**NA**domyślnie i możesz zachować status domyślny.

3) Stuknij**OK**aby zapisać ustawienia.

Step 6 Uzyskiwać**Serwer SIP**.

Figure 2-6 Serwer SIP



1) Ustaw parametry**Serwer SIP**w odniesieniu do tabeli 2-1.

Tabela 2-1 Serwer SIP

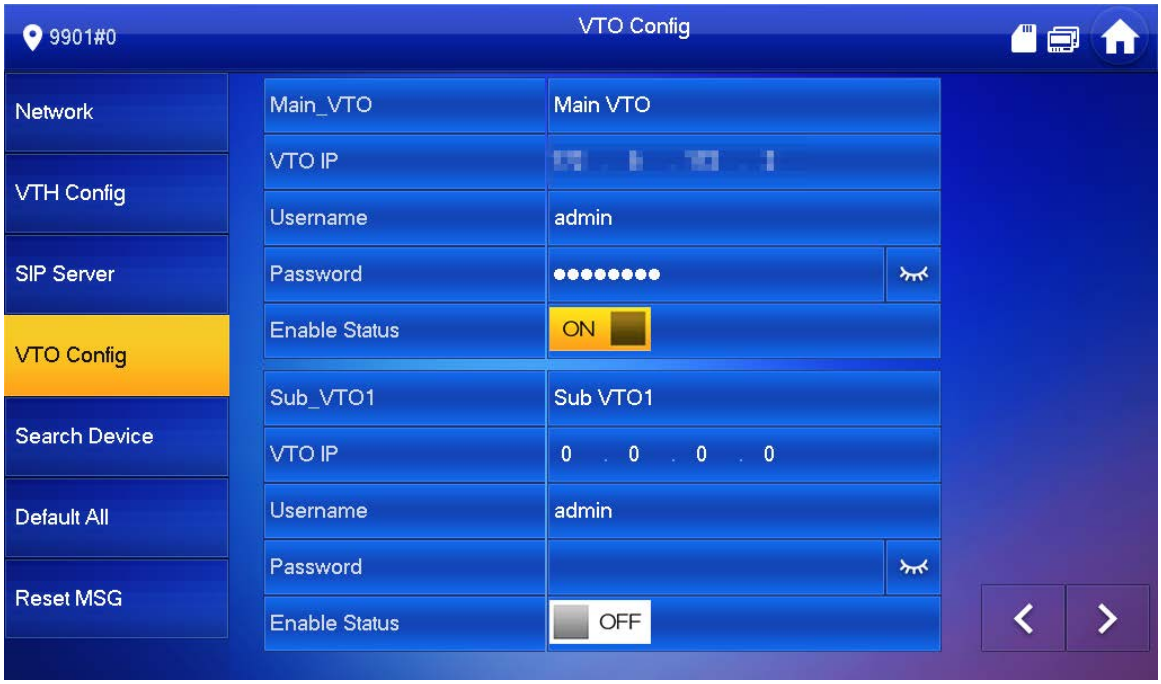
Parametr	Opis
IP serwera	● Gdy platforma działa jako serwer SIP, IP serwera jest adresem IP platformy. ● Gdy VTO pracuje jako serwer SIP, IP serwera jest adresem IP VTO.
Port sieciowy	● Gdy platforma pracuje jako serwer SIP, port sieciowy to 5080. Gdy ● VTO pracuje jako serwer SIP, port sieciowy to 5060.
Nazwa użytkownika Zarejestruj się	Użyj wartości domyślnej.
Domena	Domena rejestracyjna serwera SIP, która może być pusta. Gdy VTO pracuje jako serwer SIP, domeną rejestracyjną serwera SIP powinna być VDP.
Nazwa użytkownika Zaloguj się Pwd	Nazwa użytkownika i hasło umożliwiające zalogowanie się do serwera SIP.

2) Ustaw**Włącz stan**Do ON.

3) Stuknij**OK**.

Step 7 Uzyskiwać**Konfiguracja VTO**.

Figure 2-7 Konfiguracja VTO



Step 8 Dodaj VTO.

- Dodaj główne VTO.

1) Wprowadź główną nazwę VTO, adres IP VTO, nazwę użytkownika i hasło.

2) Ustaw**Włącz stan**Do ON.

Nazwa użytkownikaI**Hasło**powinno być takie samo jak nazwa użytkownika i hasło logowania do sieci WTO. W przeciwnym razie połączenie nie będzie możliwe.

- Dodaj podrzędne VTO.

1) Wprowadź nazwę podrzędnego VTO, podrzędny adres IP VTO, nazwę użytkownika i hasło.

2) Ustaw**Włącz stan**Do ON.

Uzyskiwać / aby przewrócić stronę i dodać więcej podrzędnych VTO.

2.3 Uruchomienie

2.3.1 VTO Wywołuje VTH

Wybierz numer pokoju VTH (np. 101) w VTO, aby zadzwonić do VTH. Pojawia się VTH monitorujący wideo i ikony obsługi. Zobacz rysunek 2-8.

Poniższy rysunek oznacza, że karta SD została włożona do VTH. Jeśli karta SD nie jest włożona, ikony nagrywania i migawki są szare.

Figure 2-8 Zadzwoń do VTH z VTO

2.3.2 VTH Monitoruje VTO

VTH jest w stanie monitorować VTO lub IPC. Weźmy na przykład VTO.

Wybierać**Monitor > Drzwi**. Zobacz rysunek 2-9. Wybierz VTO, aby wejść do monitoringu wideo. Zobacz rysunek 2-10.

Poniższy rysunek oznacza, że karta SD została włożona do VTH. Jeśli karta SD nie jest włożona, ikony nagrywania i migawki są szare.

Figure 2-9 Drzwi

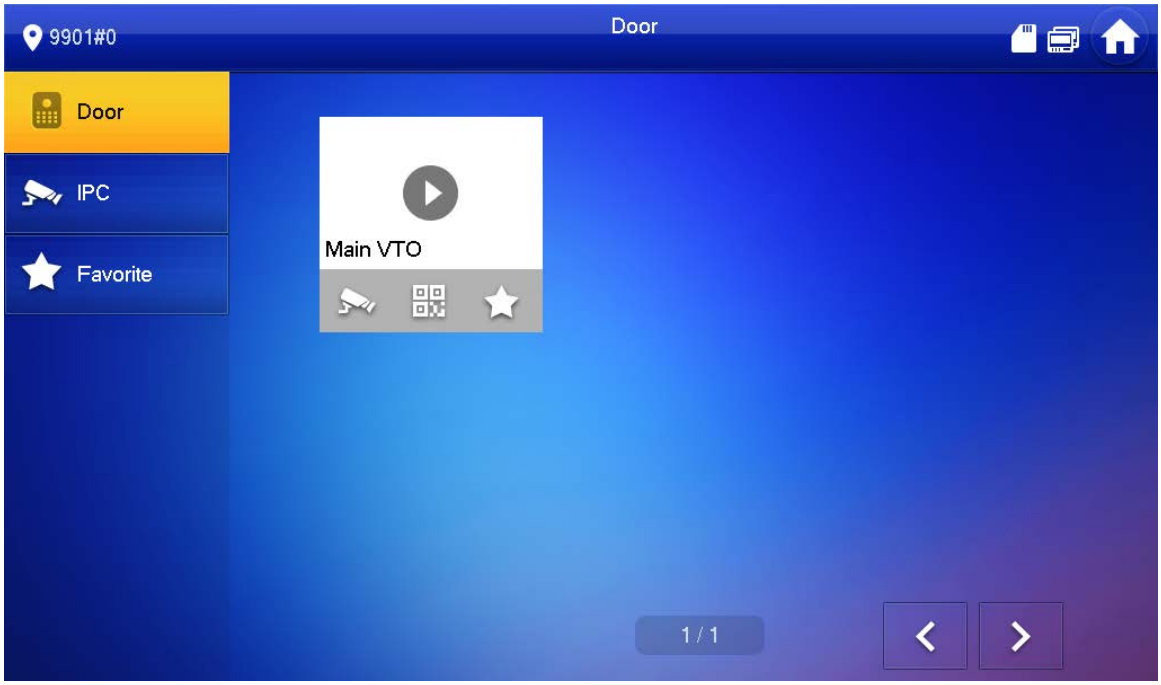
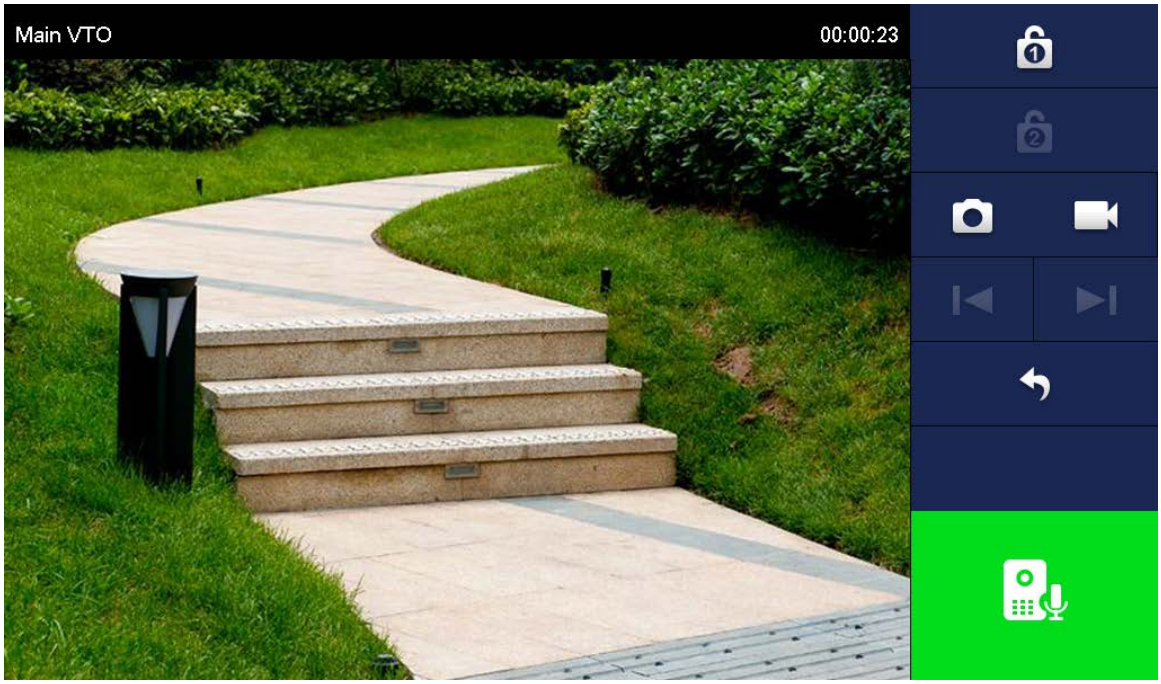


Figure 2-10 Monitorowanie wideo



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.