VTO3211D-P Krótki Przewodnik Instalacji

V1.0.1 (sierpień 2018r.)

Spis Treści

Zalecenia i oświadczenia dotyczące cyberbezpieczeństwa

Dziękujemy za zakup naszych urządzeń!
Niniejszy skrócony podręcznik został stworzony jako narzędzie referencyjne do Twojego systemu. Przed rozpoczęciem korzystania z produktów tej serii należy uważnie zapoznać się z niniejszymi instrukcjami dotyczącymi bezpieczeństwa oraz ostrzeżeniami. Podręcznik należy zachować, aby móc skorzystać z niego w przyszłości!

1. Uwaga

- Prosimy zmienić domyślne hasło po uruchomieniu urządzenia na wypadek kradzieży.
- Nie przechowuj ani nie montuj urządzenia w miejscu, na które bezpośrednio padają promienie słoneczne, ani w pobliżu urządzeń wytwarzających ciepło.
- Nie montuj urządzenia w miejscu wilgotnym, z dużą ilością pyłu lub sadzy.
- Dopilnuj, aby urządzenie zostało zamontowane poziomo lub w stabilnym miejscu, a także aby nie było zagrożone upadkiem.
- Upewnij się, że na urządzenie nie kapie ani nie pryska ciecz, a także że na urządzeniu nie stawiane jest naczynie z cieczą. Ma to na celu ochronę przed dostaniem się cieczy do urządzenia.
- Zamontuj urządzenie w dobrze wentylowanym miejscu i nie przysłaniaj jego otworów wentylacyjnych.
- Urządzenie powinno być wykorzystywane wyłącznie z przewidzianym dla niego zasilaczem,
- podłączanym do gniazda zasilającego o podanych parametrach.
- Nie demontuj samodzielnie urządzenia.

2. Ostrzeżenie

- Podczas instalacji i użytkowania należy używać przewodu zasilającego zalecanego w danym kraju i upewnić się, że podłączenie urządzenia spełnia obowiązujące normy.
- Zasilanie powinno być zgodne z wymogami dla instalacji niskonapięciowych (SELV), a napięcie znamionowe zasilacza powinno być zgodne z normą IEC60950-1. Dokładne wymagania dotyczące zasilania przedstawiono na etykiecie urządzenia.
- W przypadku korzystania z listwy zasilającej lub podobnego rozwiązania należy zadbać o to, aby urządzenie można było łatwo odłączyć.

3. Oświadczenie

- Szczegółowe informacje zawiera dokumentacja – niniejsza instrukcja ma charakter
- wyłącznie referencyjny.
- Instrukcja będzie regularnie aktualizowana zgodnie z aktualizacjami produktu. Aktualne informacje zostaną dodane do instrukcji bez uprzedzenia.
- Firma nie ponosi żadnej odpowiedzialności za szkody powstałe w skutek użytkowania urządzenia niezgodnie z instrukcją.
- W niektórych przypadkach faktyczne wartości mogą różnić się od wartości podanych w instrukcji ze względu na niestabilność faktycznego środowiska pracy i inne podobne przyczyny. W przypadku wątpliwości lub kontrowersji należy zwrócić się do nas z prośbą o wyjaśnienia.
- Pozostałe znaki towarowe i nazwy firm wymienione w niniejszych materiałach należą do ich prawowitych właścicieli.

Obowiązkowe działania do podjęcia celem zwiększenia cyberbezpieczeństwa

- **Zmieniaj hasła i wybieraj silne hasła**

Najczęstszym powodem zhakowania systemu jest słabe lub domyślne hasło. Zaleca się bezzwłoczną zmianę domyślnych haseł oraz wybranie silnego hasła zawsze, kiedy to tylko możliwe. Silne hasło powinno składać się z co najmniej 8 znaków i być kombinacją znaków specjalnych, cyfr oraz małych i wielkich liter.

- **Aktualizuj oprogramowanie sprzętowe**

Zgodnie ze standardowymi procedurami w branży technologicznej zalecamy aktualizowanie oprogramowania sprzętowego urządzeń NVR, DVR oraz kamer IP celem zapewnienia, że system jest aktualny oraz zostały zainstalowane najnowsze łatki i poprawki.

Zalecane działania nakierowane na zwiększenie bezpieczeństwa w sieci

1. **Regularnie zmieniaj hasło**

Regularnie zmieniaj dane logowania do swoich urządzeń celem zapewnienia, że tylko upoważnieni użytkownicy mogą uzyskać dostęp do systemu.

2. **Zmień domyślne porty HTTP i TCP**

- Zmień domyślne porty HTTP i TCP w systemie. Są to porty używane w komunikacji i do zdalnego wyświetlania sygnału wideo.
- Porty te można zmienić na dowolną liczbę z przedziału 1025–65535. Unikanie używania domyślnych numerów portów zmniejsza ryzyko, że osobom z zewnątrz uda się zgadnąć, których portów używasz.

3. **Włącz HTTPS/SSL**

Skonfiguruj certyfikat SSL, aby włączyć protokół HTTPS. Umożliwi to szyfrowanie komunikacji pomiędzy urządzeniami a rejestratorem.

4. **Włącz filtr adresów IP**

Włączenie filtra adresów IP uniemożliwi osobom z innymi niż wskazane adresami IP uzyskanie dostępu do systemu.

5. **Zmień hasło ONVIF**

W starszym oprogramowaniu sprzętowym kamer IP hasło ONVIF nie zmienia się wraz ze zmianą danych logowania do systemu. Konieczne jest albo zaktualizowanie oprogramowania sprzętowego kamer do najnowszej wersji, albo ręczne zmienienie hasła ONVIF.

6. **Ustaw przekierowanie tylko tych portów, których potrzebujesz**

- Przekieruj tylko te porty HTTP i TCP, których używasz. Nie przekierowuj dużej liczby portów do swojego urządzenia. Nie umieszczaj adresu IP urządzenia w strefie DMZ.
- Nie potrzebujesz przekierowywać żadnych portów do konkretnych kamer, jeśli są one

podłączone do rejestratora. Wystarczy przekierowanie do urządzenia NVR.

7. Wyłącz automatyczne logowanie w oprogramowaniu SmartPSS

Użytkownicy korzystający z oprogramowania SmartPSS bądź komputera, z którego korzystają również inne osoby, powinni wyłączyć automatyczne logowanie. Stanowi to dodatkową warstwę zabezpieczeń utrudniającą użytkownikom bez odpowiednich uprawnień uzyskanie dostępu do systemu.

8. Używaj innej nazwy użytkownika i hasła do oprogramowania SmartPSS

Nie chcesz, aby w przypadku naruszenia bezpieczeństwa kont w mediach społecznościowych, banku, poczcie e-mail itp. przestępca zebrał takie hasła i spróbował za ich pomocą dostać się do Twojego systemu monitoringu wizyjnego. Używanie innej nazwy użytkownika oraz hasła do systemu bezpieczeństwa sprawi, że trudniej będzie zgadnąć hasło dostępu do systemu.

9. Ogranicz funkcje na kontach gości

Jeśli Twój system skonfigurowany jest tak, aby obsługiwał wielu użytkowników, upewnij się, że każdy z nich ma uprawnienia do korzystania tylko z tych funkcji, które są mu potrzebne do wykonywania pracy.

10. UPnP

- UPnP spróbuje automatycznie przekierować porty w Twoim routerze lub modemie. W normalnych okolicznościach byłoby to pożądane. Jednak jeśli Twój system automatycznie przekieruje porty, a Ty zostawisz domyślne dane logowania, może się to skończyć wizytą nieproszonych gości.
- Nawet jeśli ręcznie przekierujesz porty HTTP i TCP w swoim routerze/modemie, tę funkcję i tak należy wyłączyć. Wyłączenie UPnP zaleca się też generalnie wtedy, gdy funkcja ta nie jest wykorzystywana.

11. SNMP

Wyłącz protokół SNMP, jeśli z niego nie korzystasz. Jeśli korzystasz z protokołu SMNP, należy włączać go tylko tymczasowo, wyłącznie do celów śledzenia i testowania.

12. Multicast

Funkcja Multicast służy do udostępniania strumieni wideo pomiędzy dwoma rejestratorami. Obecnie nie są znane żadne problemy dotyczące tej funkcji, ale jeśli z niej nie korzystasz, wyłączenie jej zwiększy bezpieczeństwo Twojej sieci.

13. Sprawdzaj dziennik systemu

Jeśli podejrzewasz, że ktoś uzyskał nieuprawniony dostęp do Twojego systemu, możesz sprawdzić dziennik systemu. Będzie on zawierał informacje na temat tego, jakie adresy IP były używane do logowania w systemie i do czego uzyskano dostęp.

14. Zabezpiecz urządzenie fizycznie

W idealnym scenariuszu chcesz zabezpieczyć swój system przed jakimkolwiek nieuprawnionym dostępem. Najlepszym sposobem, aby to osiągnąć, jest zamontowanie

rejestratora w zamykanej szafce, szafie serwerowej lub w pomieszczeniu zamykanym na klucz.

15. Podłącz kamery IP do portów PoE z tyłu urządzenia NVR

Kamery podłączone do portów PoE z tyłu urządzenia NVR są odizolowane od świata zewnętrznego i nie można do nich uzyskać dostępu zdalnego.

16. Odizoluj sieć urządzenia NVR i kamer IP

Sieć, w której działają Twoje kamery IP oraz urządzenia NVR, nie powinna być publiczną siecią komputerową. Dzięki temu nieproszeni goście nie będą mogli uzyskać dostępu do tej samej sieci, której do prawidłowego funkcjonowania potrzebuje system zabezpieczeń.

Aby uzyskać więcej najnowszych informacji na temat cyberbezpieczeństwa odwiedź stronę www.dahuasecurity.com/pl

O tym dokumencie

1. Niniejszy dokument służy wyłącznie do celów referencyjnych. Szczegółowe informacje zawiera dokumentacja produktu.
2. Niniejszy dokument służy jako materiał referencyjny do wielu różnych produktów, których konkretne działanie nie zostało tu opisane. Produkty należy obsługiwać zgodnie z ich dokumentacją.
3. Użytkownik ponosi pełną odpowiedzialność za wszelkie straty wynikające z naruszeń wytycznych podanych w niniejszym dokumencie.
4. Jeśli nie można otworzyć pliku PDF, należy zaktualizować program do odczytu takich plików do najnowszej wersji lub skorzystać z innych narzędzi do odczytu.
5. Firma zastrzega sobie prawo do wprowadzenia w dowolnym czasie zmian w informacjach zawartych w niniejszym dokumencie, a wprowadzane zmiany zostaną dodane w najnowszej wersji bez wcześniejszego powiadomienia. Przed wprowadzeniem zmian i po ich wprowadzeniu niektóre funkcje produktów mogą nieznacznie się różnić.
6. Dokument może zawierać nieścisłości techniczne, rozbieżności w zakresie funkcji i działania produktów, a także błędy w druku. Obowiązują finalne wyjaśnienia dostarczone przez firmę.

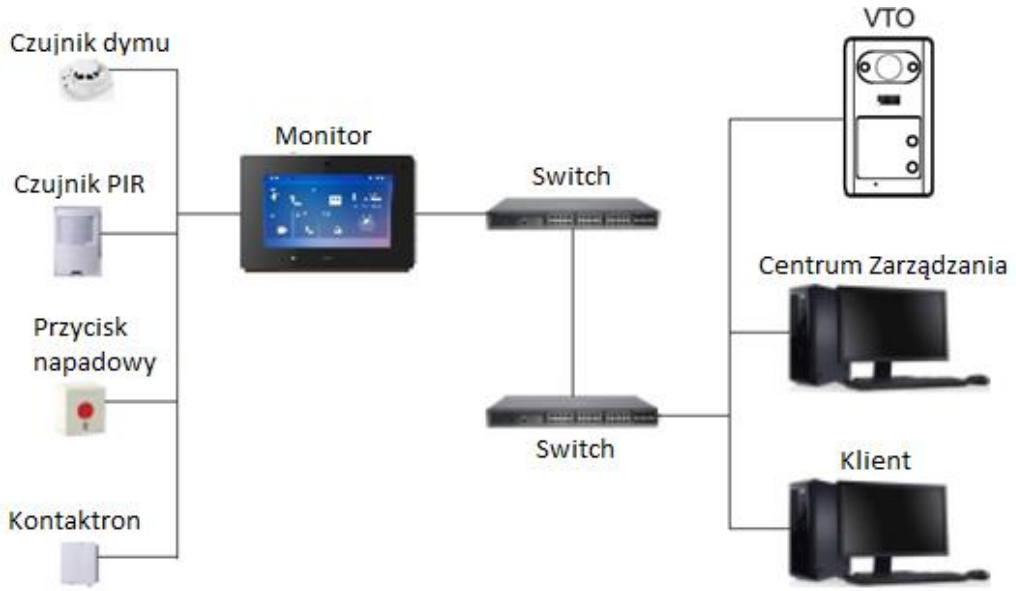
1 Opis ogólny produktu

1.1 Właściwości produktu

Stacja bramowa VTO umożliwia łatwe operowanie, można ją łatwo zainstalować i posiada następujące funkcje:

- Podgląd na żywo ze smartfona.
- Dzwonienie I intercom z monitorem VTH.
- Otwarcie drzwi kartą.
- Alarm w przypadku aktu wandalizmu.

1.2 Schemat połączeń sieciowych

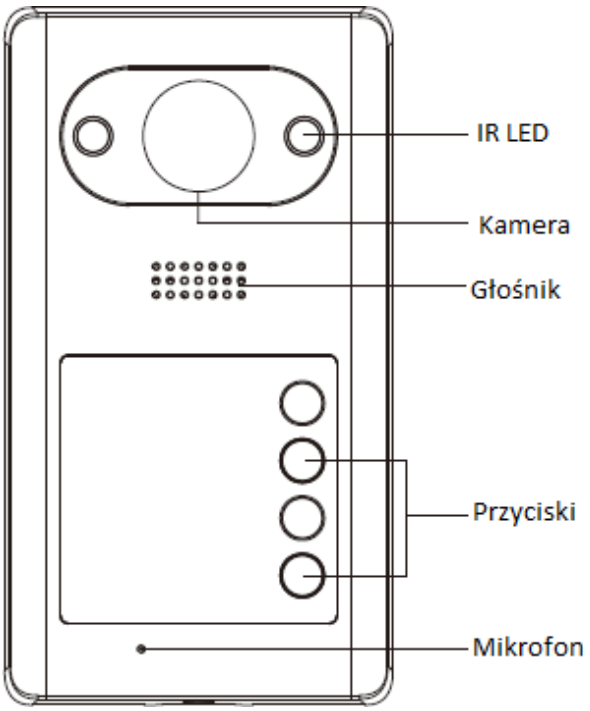


Rys. 1-1

2 Struktura

2.1 Panel Przedni

Liczba przycisków różni się w zależności od modelu. Na przykład: VTO3211D- P2 posiada 2 przyciski; VTO3211D-P4 - cztery. VTO3211D-P2 będzie podany dla przykładu.

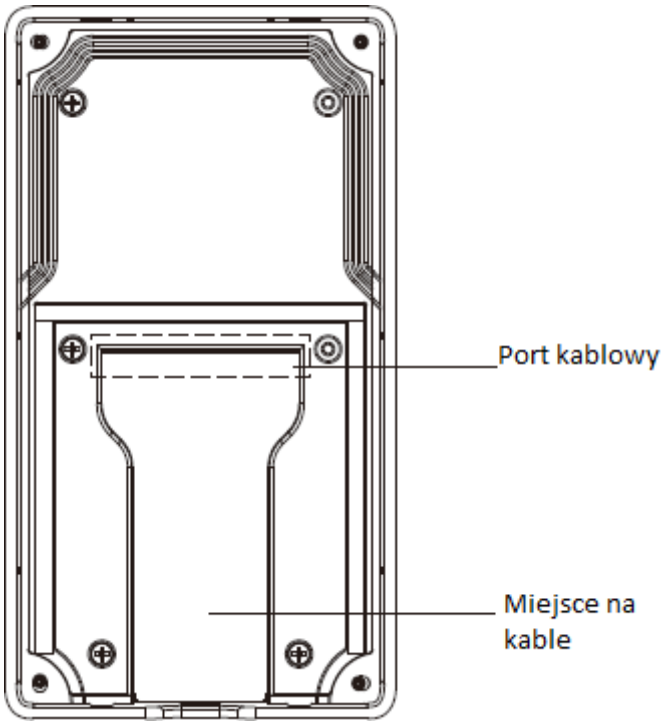


Rys. 2-1

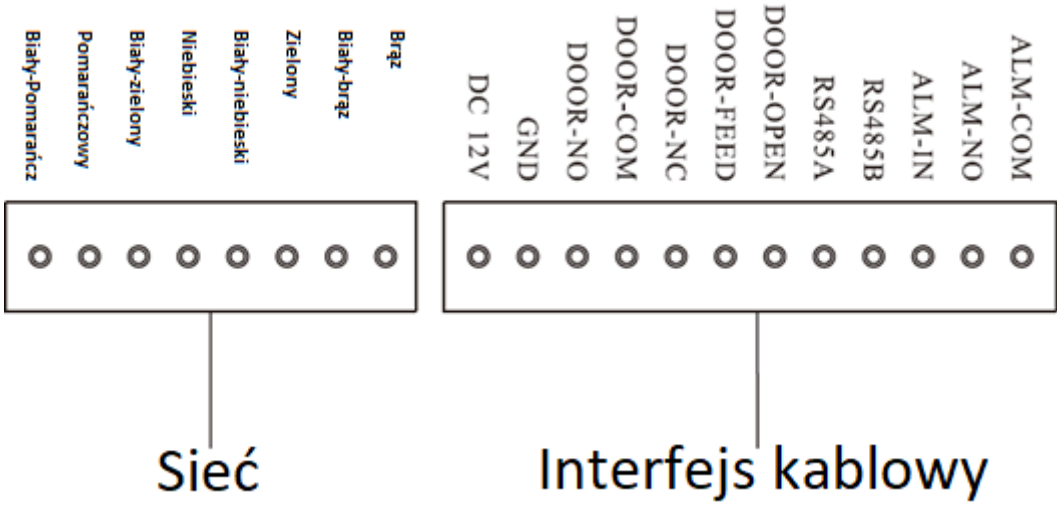
Nazwa	Opis
IR Fill Light	Zapewnia doświetlenie w przypadku ciemności.
Camera	Kamera.
Speaker	Głośnik.
Call Button	Przyciski dzwonienia. Uwaga: Model VTO3211D-P4 posiada 4 przyciski.
MIC	Mikrofon.

Tabela 2-1

2.2 Panel tylni



Rys. 1- 1



Rys. 2-2

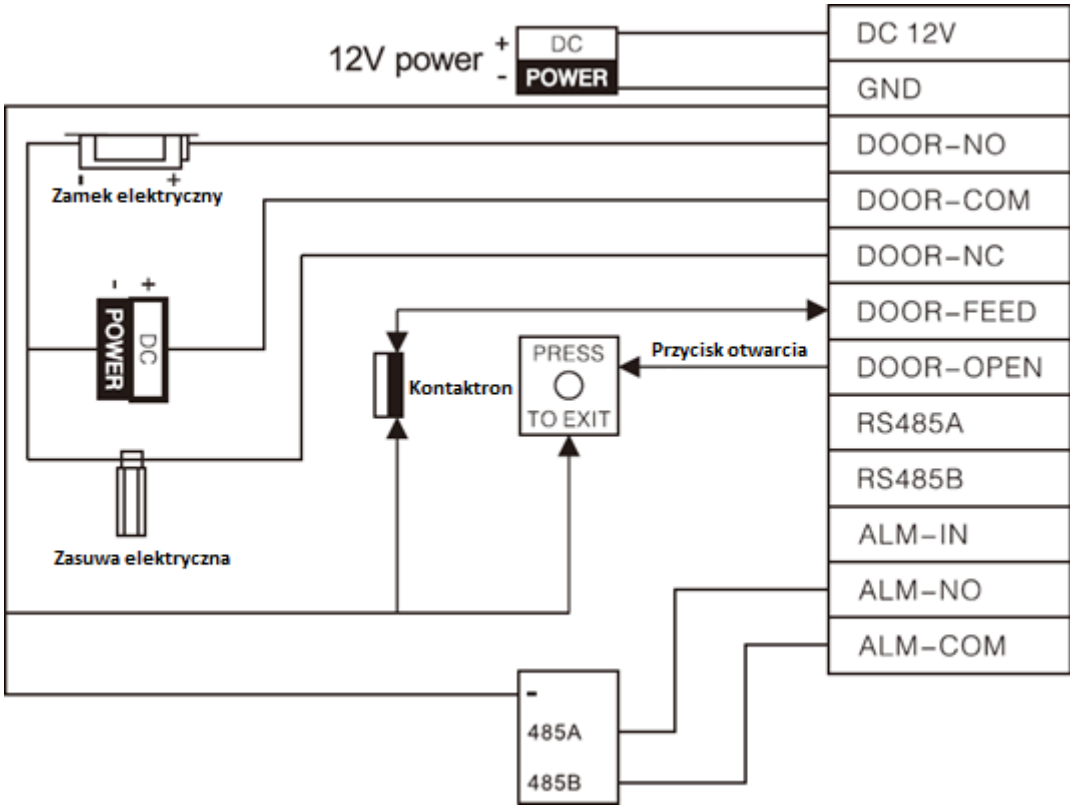
Oznakowanie	Uwaga
DC12V	Zasilanie DC12V
GND	Masa
DOOR-NO	Zacisk wyjścia NO zamka
DOOR-COM	Zacisk wspólny zamka

Label	Note
DOOR-NC	Zacisk wyjścia NC zamka
DOOR-FEED	Czujnik (kontaktron) drzwiowy
DOOR-OPEN	Przycisk otwarcia drzwi
RS485A	Komunikacja RS485
RS485B	
ALM-IN	Wejście Alarmowe
ALM-NO	Wyjście Alarmowe
ALM-COM	Zacisk wspólny alarmowy

Tabela 2-2

3 Instalacja i Programowanie

3.1 Okablowanie urządzenia



Rys. 3-1

3.2 Instalacja

Ostrzeżenie

- **Unikaj instalacji w miejscach niebezpiecznych takich jak narażenie na wysokie temperatury, zapylenie, zbyt dyuża wilgotność, itp.**
- **Instalację i zaprogramowanie urządzenia powinna wykonać osoba przeszkolona. NIE otwieraj urządzenia.**

3.2.1 Specyfikacja śrub

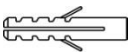
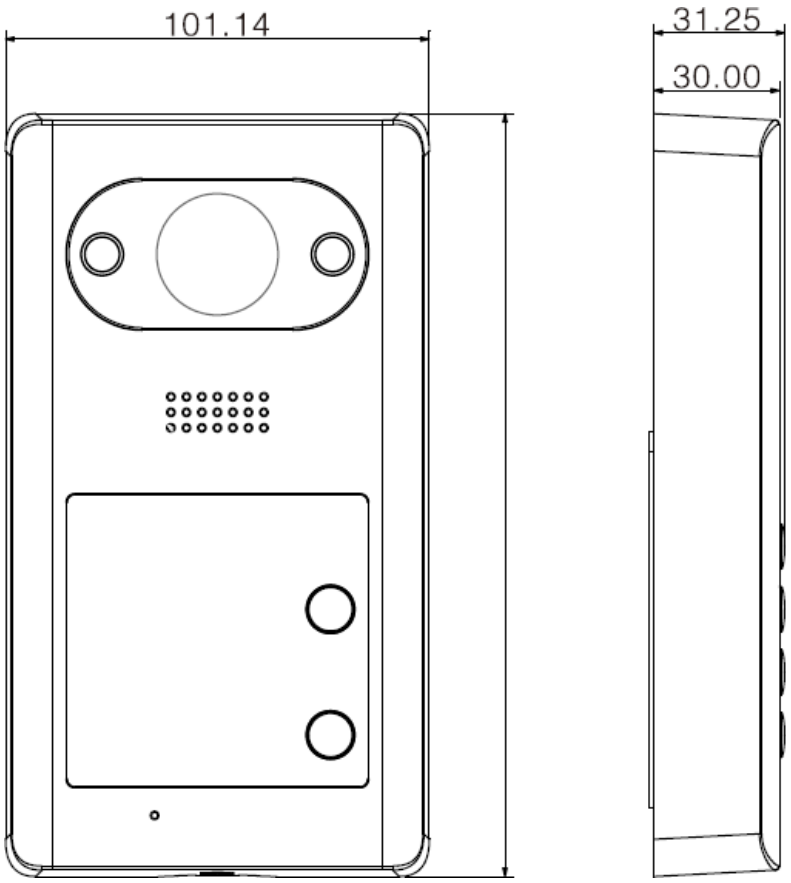
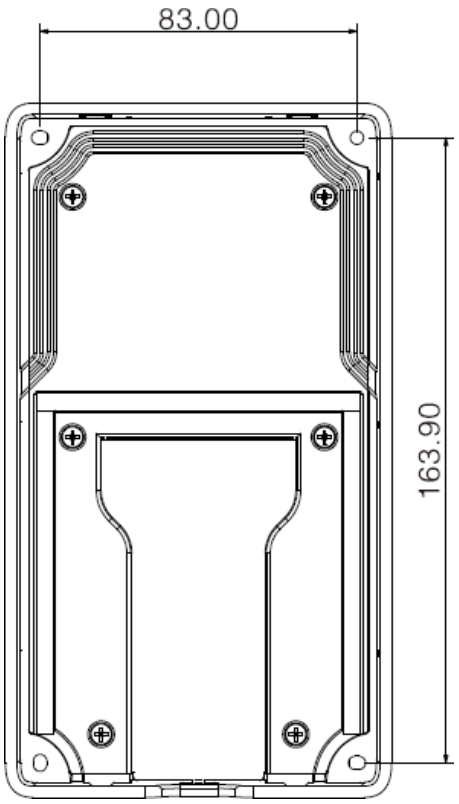
Nazwa składnika	Obraz	Ilość
Biały kołek rozporowy Φ6×30mm		4
ST3×20 samogwintująca		4
M3×6 mechaniczna		1

Tabela 3-1

3.2.2 Wymiary Instalacyjne



Rys. 3-2



Rys. 3-3

3.2.3 Kroki Instalacyjne

Przed instalacją, odkręć śrubę M3*6 od spodu urządzenia, zdejmij metalową obudowę, jak na Rys. 3-4.

Krok 1. W miejscach otworów w urządzeniu, zaznacz je na ścianie i wywierć otwory.

Krok 2. W otwory włóż kołki rozporowe.

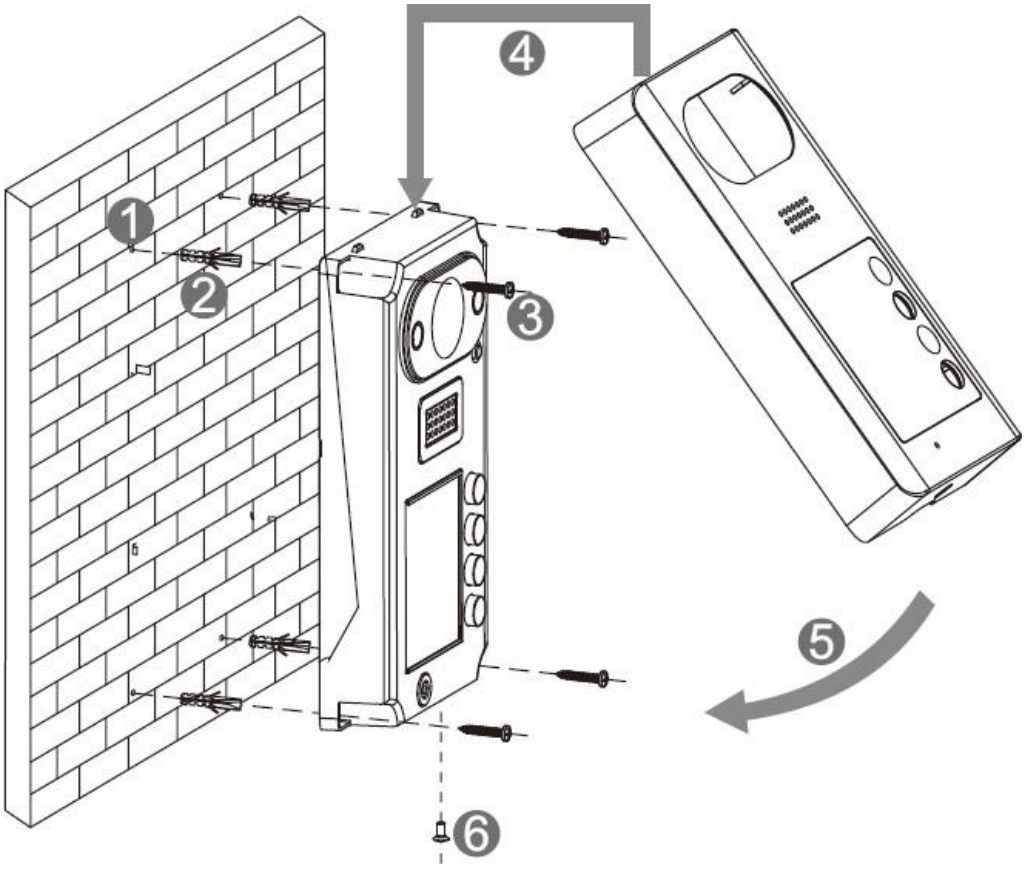
Krok 3. Przykręć urządzenie do ściany używając śrub samogwintujących

Krok 4. Załóż obudowę na urządzenie od góry urządzenia.

Krok 5. Przykręć obudowę od spodu śrubą M3*6.

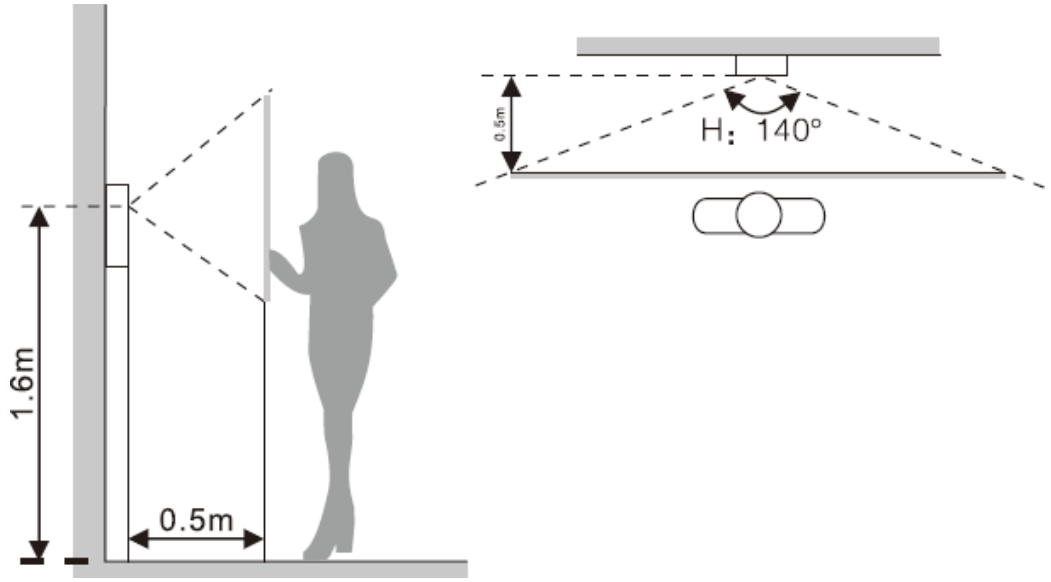
Uwaga:

Zalecana wysokość montażu od podłoża wynosi 1.4m-1.6m.



Rys. 3-4

Po instalacji stacja wygląda jak na Rys. 3-5.



Rys. 3-5

3.3 Programowanie

3.3.1 Zanim zaprogramujesz

Dla przykładu do zaprogramowania połączenia ze stacją bramową użyto typowego monitora 7”.

- Przed montażem, instalator powinien widzieć jak zainstalować urządzenie, okablować je, zaprogramować i używać.
- Przed zaprogramowaniem sprawdź okablowanie – czy nie ma przerwy lub zwarcia.
- Upewnij się, że monitor działa normalnie.

3.3.2 Ustawienia VTO

Domyślny adres VTO to 192.168.1.110. Zanim zaczniesz używać stacji bramowej musisz zmienić jej adres IP w taki sposób, żeby była w tej samej grupie adresowej co monitor.

Krok 1. Zasil urządzenie VTO.

Krok 2. W przeglądarce wpisz adres: 192.168.1.110.

Zobacz Rys 3-6.

Rys 3-6

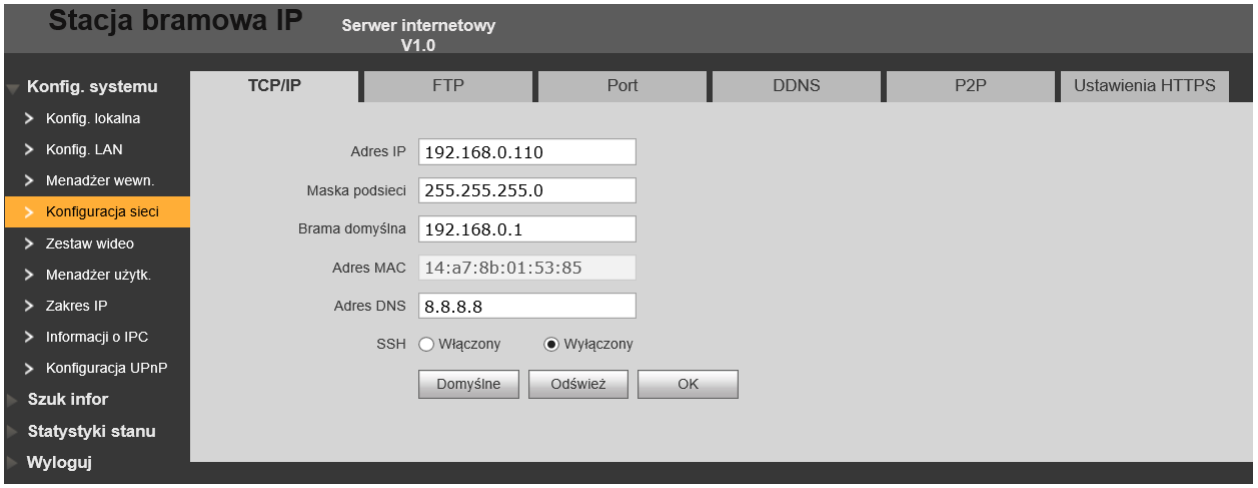
Krok 3. Wpisz nazwę użytkownika i hasło, Kliknij Login.

Uwaga:

Domyślne nazwy użytkownika I hasło to admin i admin. Przy pierwszym logowaniu będziesz musiał zmienić hasło.

Krok 4. Konfig. systemu>Konfiguracja sieci>TCP/IP. Zobacz Rys 3-7. Zmień adres IP

Po zakończeniu modyfikacji, należy odświeżyć stronę przeglądarki, wpisać nowy adres IP i przejść do strony logowania.

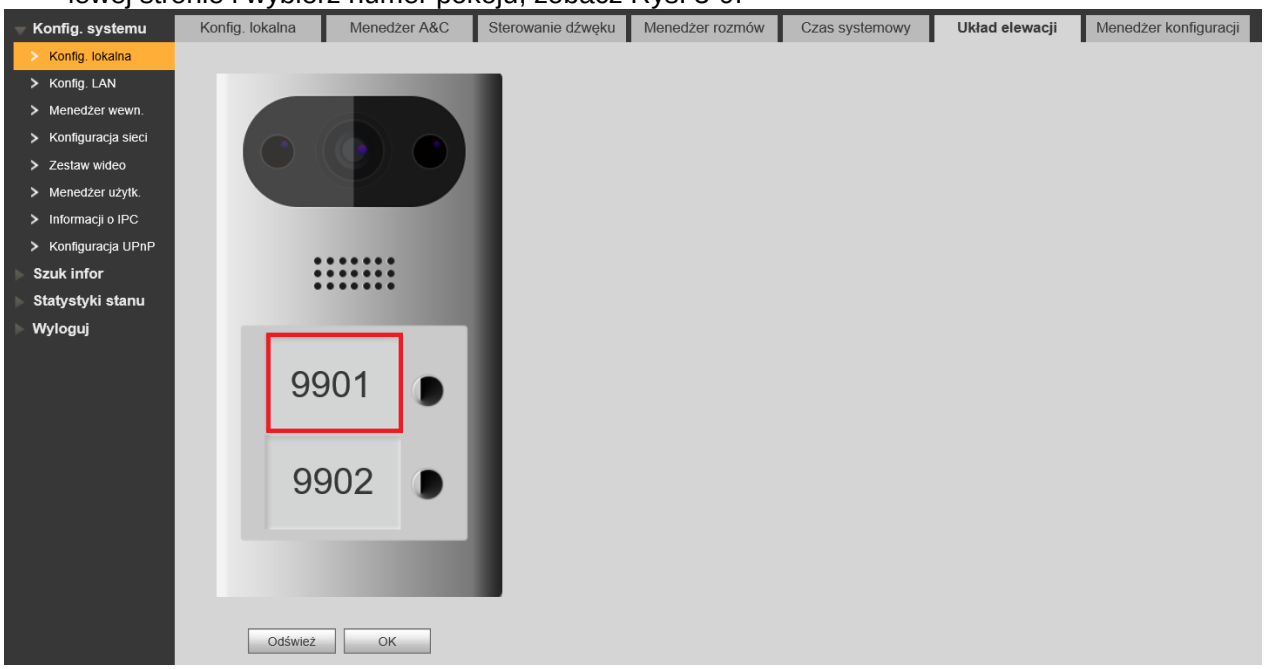


Rys 3-7

Krok 5. Wybierz Konfig. systemu>Menadżer wewn. Zobacz Rys. 3-8. Kliknij Dodaj, aby dodać informacje o VTH.

Rys 3-8

Krok 6. Kliknij Konfig.systemu> Konfig.lokalna >Układ elewacji, Kliknij na białe pole po lewej stronie i wybierz numer pokoju, zobacz Rys. 3-9.



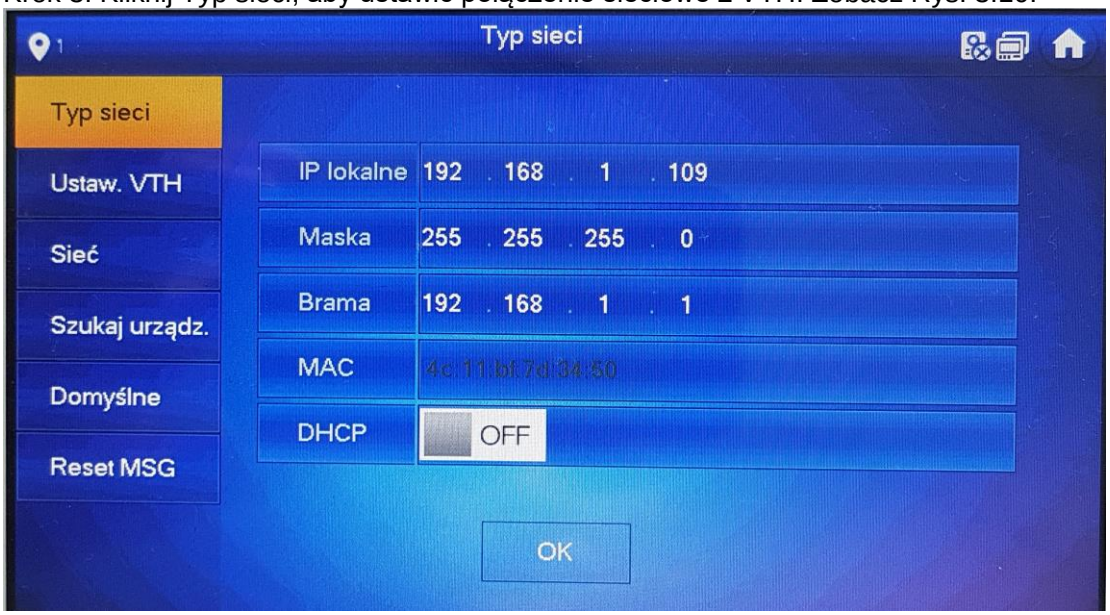
Rys. 3-9

3.3.3 Menadżer wewnętrzny

Krok 1. Na ekranie menu VTH przyciśnij i przytrzymaj przycisk Ustawień przez ok. 6-7 sek.

Krok 2. Wpisz hasło, aby uzyskać dostęp do programowania.

Krok 3. Kliknij Typ sieci, aby ustawić połączenie sieciowe z VTH. Zobacz Rys. 3.10.



Rys. 3-10

1. Wpisz adres IP, maskę i bramę monitora.
2. Kliknij OK.

   Powinieneś zobaczyć **tylko** ikonę w górnym, prawym rogu ekranu, co oznacza pomyślne połączenie ze stacją bramową.

   Uwaga:

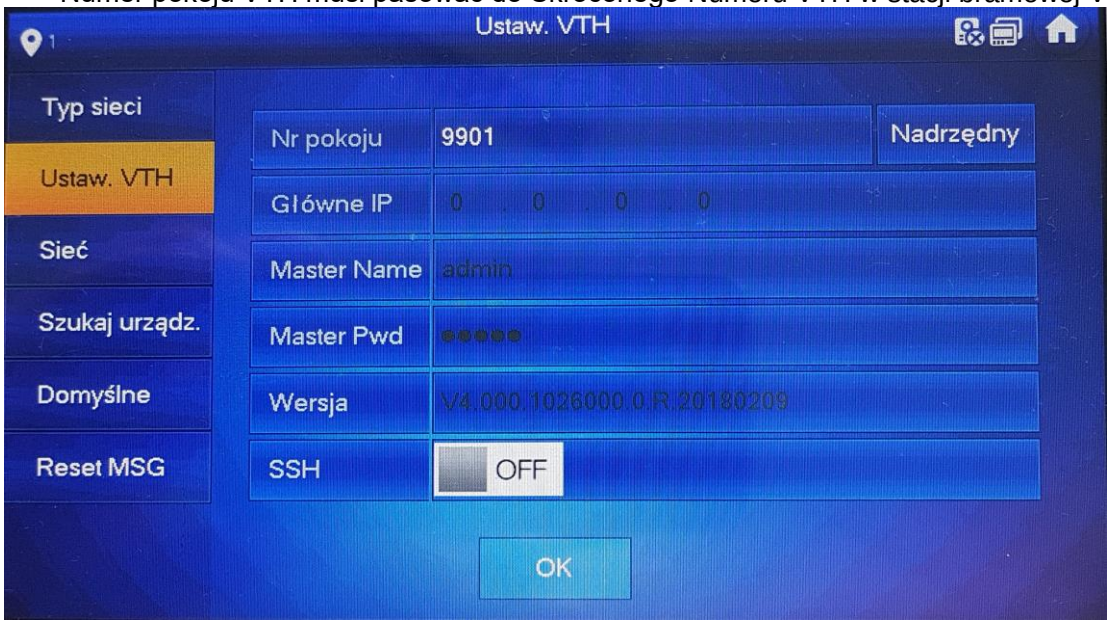
   Możesz również aktywować DHCP, aby automatycznie otrzymywać adres IP, maskę podsieci i bramę. Kliknij OK.

Krok 4. Kliknij Ustaw. VTH aby ustawić nr pokoju.

Zobacz Rys. 3-11.

Uwaga:

Numer pokoju VTH musi pasować do Skróconego Numeru VTH w stacji bramowej VTO.

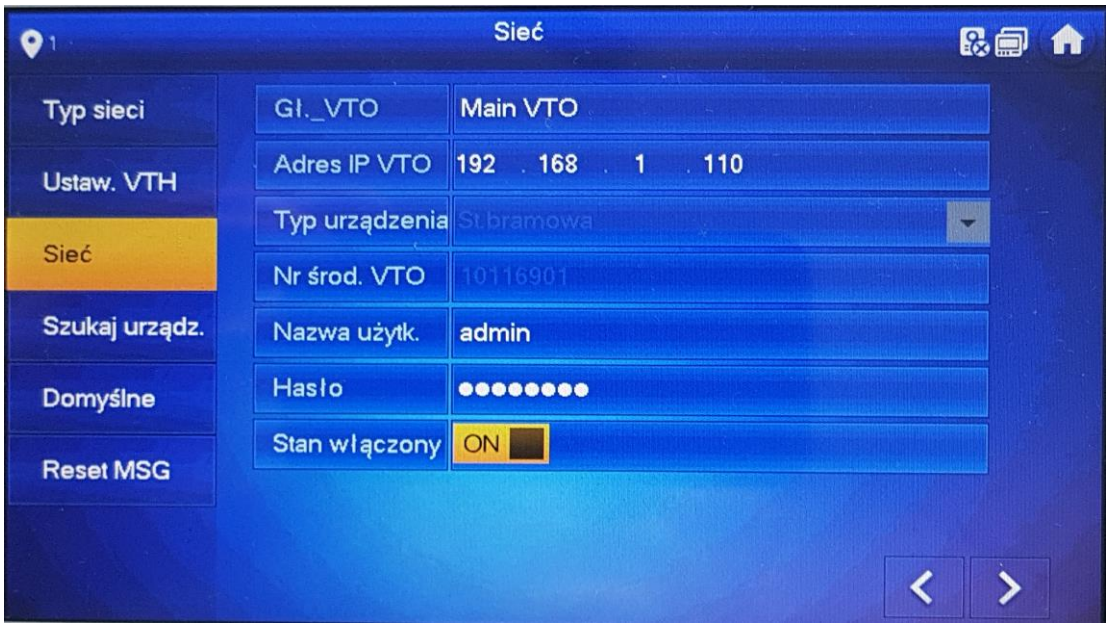


Rys. 3-11

- Jeśli chcesz, aby Twój monitor był monitorem głównym wybierz Nadrzędny. Wpisz numer pokoju i kliknij OK. Zobacz Rys. 3-11.
- Jeśli chcesz, aby Twój monitor był monitorem podrzędnym wybierz Rozszerzenie. Wpisz numer pokoju oraz adres IP monitora głównego i kliknij OK. Zobacz Rys. 3-11.

.

Krok 5. Kliknij Sieć, aby ustawić adres IP stacji bramowej VTO. Zobacz Rys. 3-12.



Rys. 3-12

1. Wpisz nazwę VTO oraz adres IP. Musisz też wpisać nazwę użytkownika i hasło.
2. Ustaw Stan włączony na ON.

4 Działanie

Uwaga:
Zajrzyj do instrukcji Użytkownika.

Na stacji bramowej VTO, naciśnik przycisk dzwonienia VTH. Na monitorze pojawi się okno z obrazem z kamery oraz przyciski rozpoczęcia konwersacji i otwarcia drzwi. Zobacz Rys. 4-1.

Programowanie jest zakończone sukcesem.

Rys. 4-1

5 Ustawienia smartfona

5.1 Ustawienia telefonu komórkowego

a) Pobierz aplikację na swój telefon. Użyj telefonu, aby zaskanować poniższy kod QR. Zobacz Rys. 5-1.

Rys. 5-1

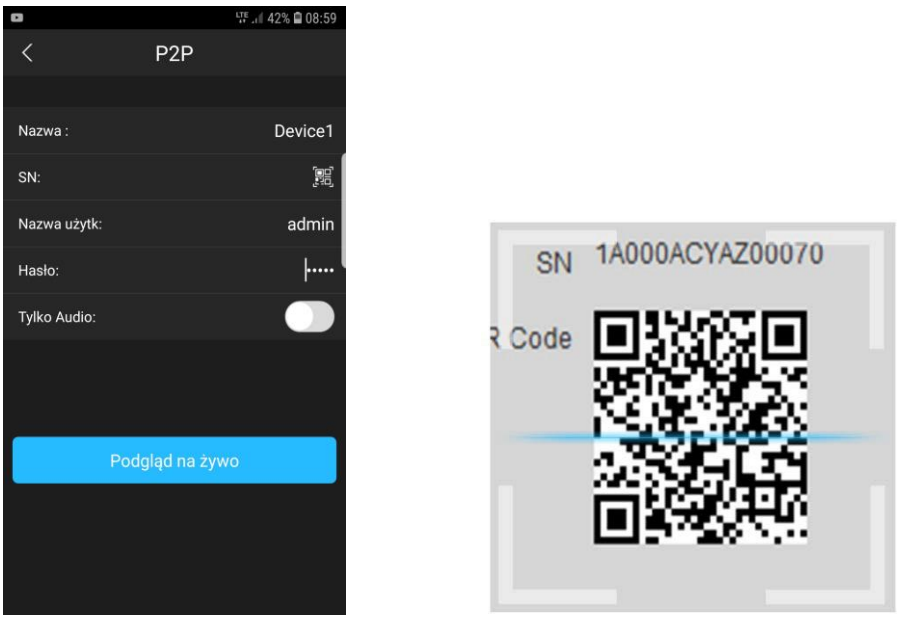
W przeglądarce, na stronie VTO> Menadżer Wewnętrzny, dla każdego monitora jest odzielny kod QR, który umożliwia użytkownikowi połączenie P2P z telefonem i wysyłanie powiadomień.

Kliknij  , wpisz nazwę użytkownika i hasło (najlepiej wcześniej utwórz nowego użytkownika w zakładce Menadżer Użytkowników) Kliknij OK, aby zobaczyć kody QR i numer seryjny urządzenia. Zobacz Rys. 5-2, Rys. 5-3.

Rys. 5-2

Rys. 5-3

b) Użyj telefonu, aby zeskanować kod QR. Zobacz Rys. 5-4.



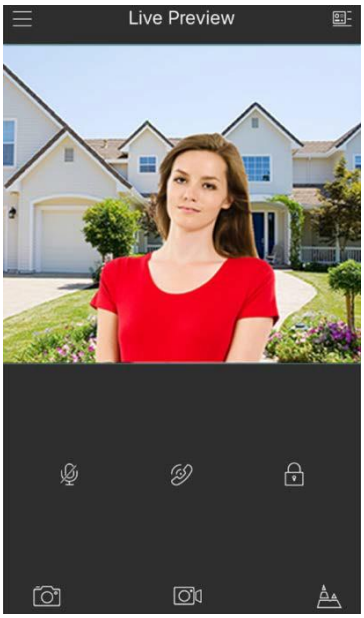
Rys. 5-4

c) Wpisz nazwę urządzenia. Kliknij na ikonę po prawej stronie wiersza z SN:. Zeskanuj kod QR z przeglądarki.

d) Włącz powiadomienie „push” w Menu Alarm / Powiadom o alarmie i przesuń suwak w prawą stronędla zaprogramowanego urządzenia.

5.2 Sprawdź rezultat

Kiedy stacja bramowa VTO dzwoni do monitora możesz usłyszeć powiadomienie na swoim telefonie. Otwórz wiadomość z powiadomieniem i powinieneś zobaczyć podgląd z kamery

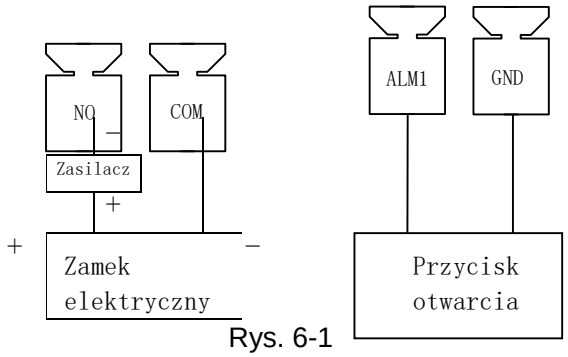


ze stacji bramowej na żywo. Rys. 5-6

6 Zamek elektryczny i kontaktron drzwiowy

6.1 Zamek elektryczny

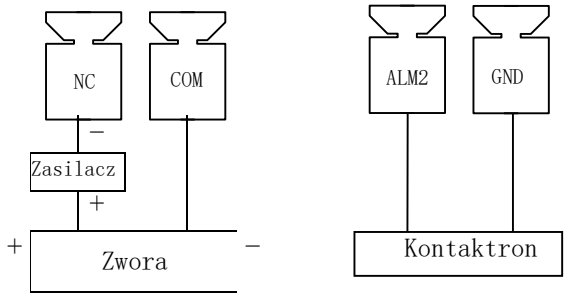
Kiedy chcesz podłączyć zamek elektryczny do stacji VTO podłącz plus do zacisków NO (poprzez zasilacz) oraz minus do zacisku COM.
Kiedy chcesz podłączyć przycisk otwarcia podłącz jeden koniec do ALM1 a drugi go zacisku GND. Zobacz Rys. 6-1.



Rys. 6-1

6.2 Kontaktron drzwiowy

Kiedy chcesz podłączyć zworę magnetyczną do VTO to podłącz plus (poprzez zasilacz) do wyjścia NC a minus do zacisku COM w stacji bramowej VTO).
Kiedy chcesz podłączyć kontaktron podłącz jeden koniec do ALM2 a drugi go zacisku GND. Zobacz Rys. 6-2.



Rys. 6-2

Załącznik 1 Specyfikacja Techniczna

Model		VTO3211D-P	VTO3211D
System	Gł. procesor	Mikrokontroler	
	Sys. operacyjny	Linux	
Video	Standard Kompresji	H.264	
Audio	Standard	G.711	
	Wejście	Dookolny mikrofon	
	Wyjście	Wbudowany głośnik	
	Rozmowa	Dwukierunkowa rozmowa	
Działanie	Wejście	Przycisk Mechaniczny	
Alarm	Wejście	1 przycisk otwarcia, 1 kontaktron	
	Wyjście	1 wyjście przekaźnika	
	Kamera	2.0 MP	
Sieć	Ethernet	10M/100Mbps	
Inne	Szyna 485	1-kanał	
	Karta pamięci	Max 64G	
Ogólne	Zasilanie	DC 12V lub standardowe PoE	DC 12V
	Zabezpieczenie	IK08	
	Klasa szczelności	IP65	
	Pobór mocy	Gotowość ≤1W; praca ≤7W	
	Wymiary (D×S×G)	182mm*101mm*30mm	

Uwaga:

- **Niniejsza instrukcja jest wyłącznie w celach referencyjnych. Ewentualne różnice w sprzęcie mogą mieć zastosowanie.**
- **Wszystkie elementy i oprogramowanie mogą być zmienione bez uprzedniego powiadomienia.**
- **Wszystkie zastrzeżone znaki handlowe są własnością odpowiednich właścicieli.**
- **W przypadku nieścisłości lub innych różnic, końcowe wyjaśnienie należy do firmy Dahua.**
- **Zajrzyj na naszą stronę lub skontaktuj się z lokalnym wsparciem w celu uzyskanie większej ilosci informacji.**