

REJESTRATOR ZKT F22

INSTRUKCJA OBSŁUGI

06.12.2014

Środki ostrożności

Przed montażem należy zapoznać się z poniższymi środkami ostrożności, aby zapewnić bezpieczeństwo użytkownika i zapobiec uszkodzeniu produktu.

Urządzenia nie należy instalować w miejscu narażonym na bezpośrednie działanie promieni słonecznych, wilgoć i kurz.

— Nie należy umieszczać magnesów w pobliżu produktu. Przedmioty magnetyczne, takie jak magnesy, monitory CRT, telewizory, monitory lub głośniki, mogą uszkodzić urządzenie.

Nie należy umieszczać urządzeń w pobliżu urządzeń grzewczych.

Nie dopuścić do przedostania się do wnętrza urządzenia płynów, takich jak woda, napoje lub środki chemiczne. Nie pozwalać dzieciom na dotykanie urządzenia bez nadzoru.

Nie upuszczaj ani nie uszkadzaj urządzenia.

Nie należy demontować, naprawiać ani modyfikować urządzenia.

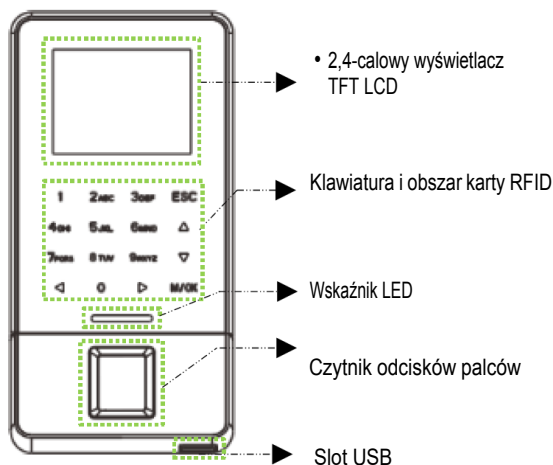
Nie używaj urządzenia do celów innych niż określone w instrukcji.

Urządzenie należy często czyścić, aby usunąć z niego kurz. Oznacza to, że nie należy spryskiwać urządzenia wodą, lecz wycierać je miękką ściereczką lub ręcznikiem.

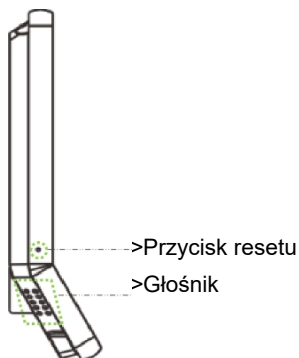
W razie problemów skontaktuj się ze swoim dostawcą!

Przegląd urządzenia

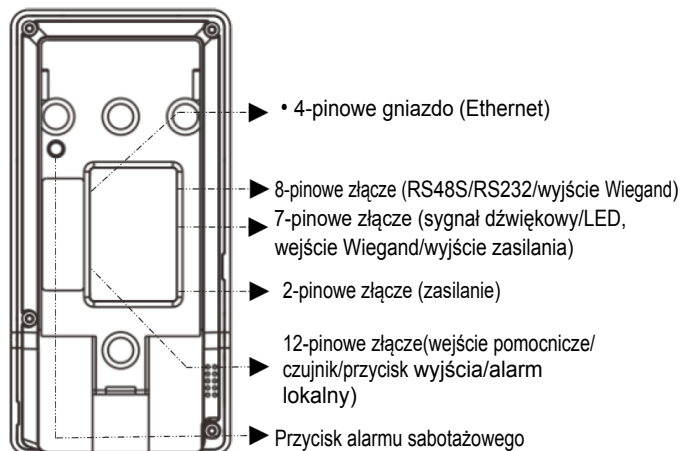
Przednia strona



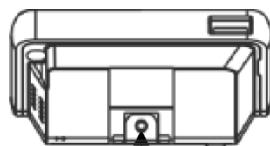
Bok



Tył

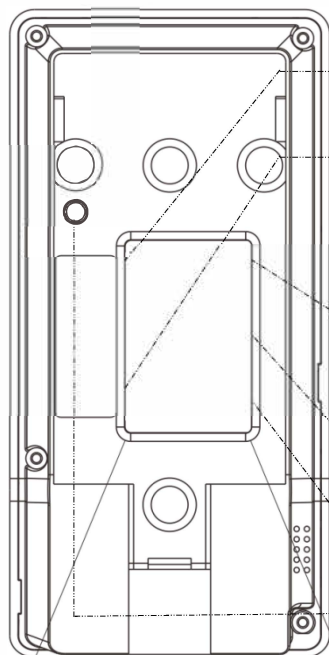


Spód



Otwór na śrubę w kształcie gwiazdy do mocowania urządzenia do płyty tylnej

Przegląd urządzenia



► 4 Pinowe wyjście Ethernet (TCP/IP)

► 12 Pinowe wyjście

► 8 Pinowe wyjście

► 7 Pinowe wyjście

► 2 Pinowe wyjście

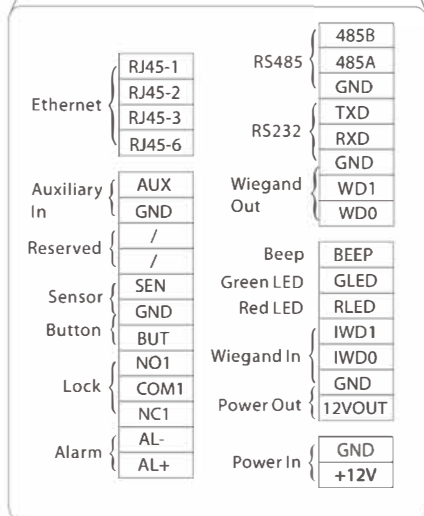
► przycisk Tamper

○ Auxiliary In
○ Reserved
○ Sensor
○ Button
○ Lock
○ Alarm

○ RS485
○ RS232
○ Wiegand Out

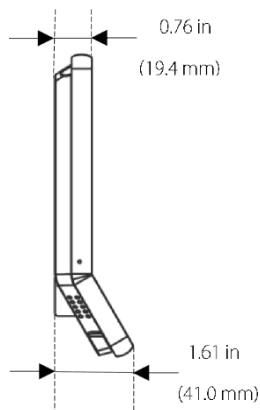
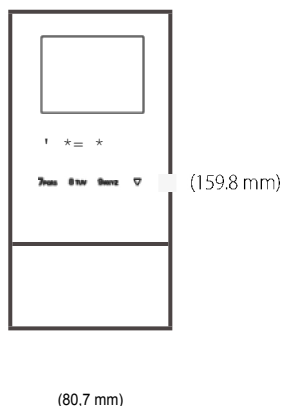
○ LED, Beep
○ Wiegand In
○ Power Out

○ Power In

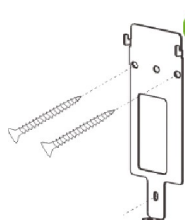


Wymiary urządzenia i montaż

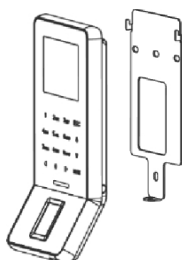
❖ Wymiary produktu



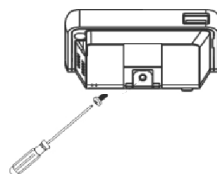
❖ Mocowanie urządzenia na ścianie



- 1 Przymocuj płytę tylną do ściany za pomocą śrub do montażu na ścianie.
Uwaga: Zalecamy wkręcanie śrub płyty montażowej w lite drewno (np. słupek/belkę). Jeśli nie można znaleźć słupka/belki, należy użyć dostarczonych plastikowych kołków do płyt gipsowo-kartonowych.



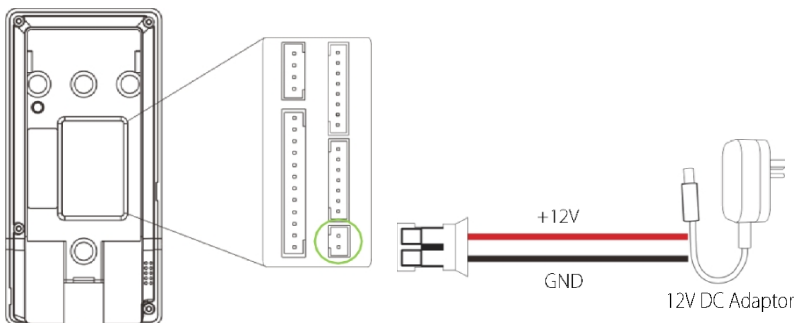
Wsuń urządzenie na płytę tylną.



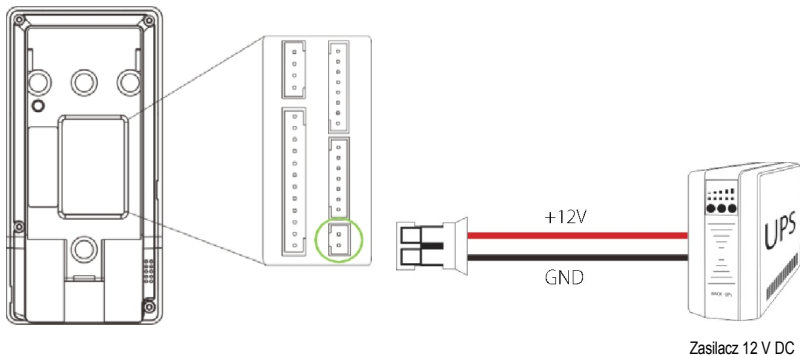
Użyj śrub zabezpieczających, aby przymocować urządzenie do płyty tylnej

Podłączenie zasilania

❖ Bez zasilacza awaryjnego (UPS)



❖ Z zasilaczem awaryjnym (opcjonalnie)

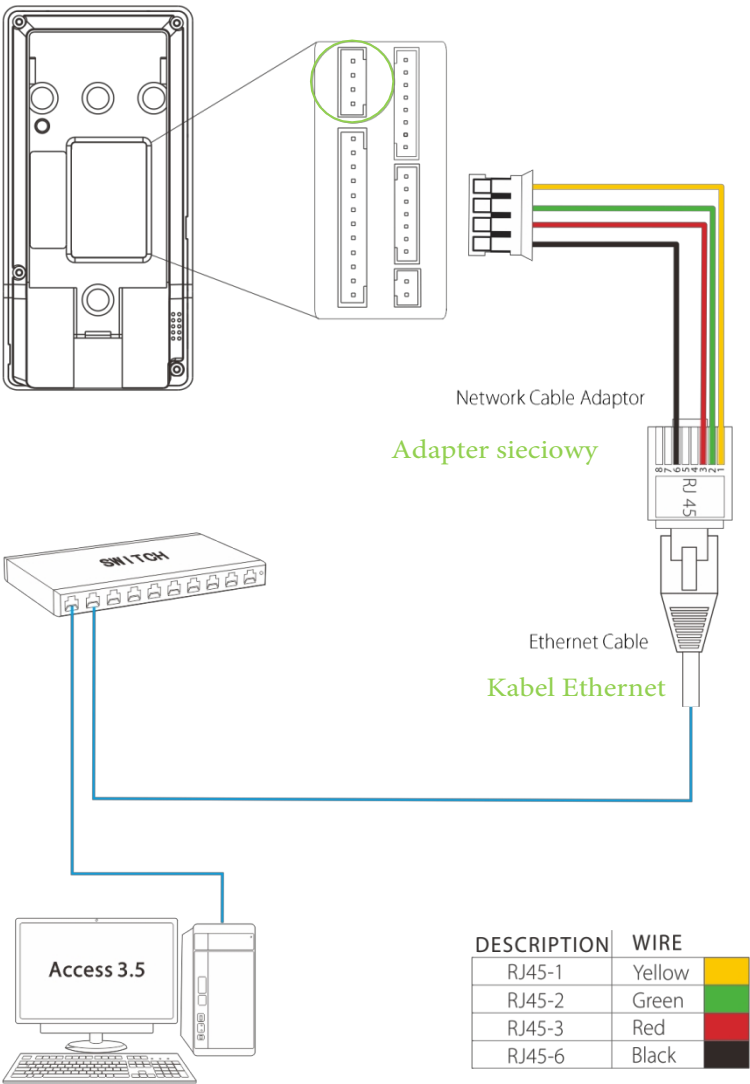


❖ Zalecane źródło zasilania

- 12 V +10%, co najmniej 500mA.
- Aby dzielić zasilanie z innymi urządzeniami, należy używać zasilacza o wyższej wartości prądu znamionowego.

Podłączanie do internetu

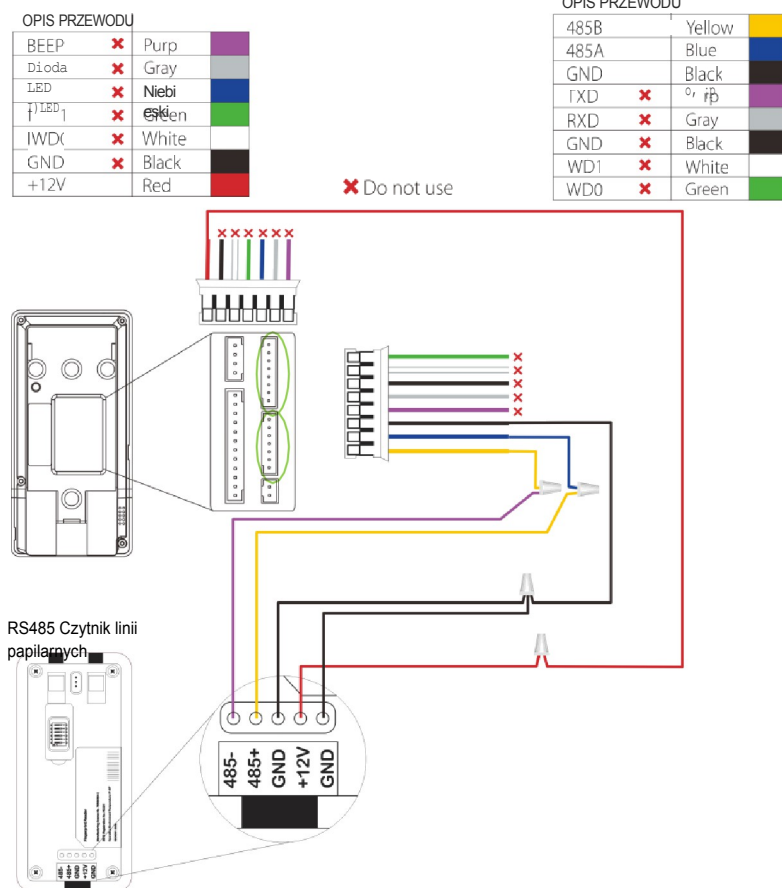
❖ Przez kabel LAN



Urządzenie może być podłączone przez kabel Ethernet do komputera

Połączenie RS485

❖ Podłączenie czytnika linii papilarnych RS485



❖ Ustawienia przełączników DIP

- ❖ Z tyłu czytnika linii papilarnych RS485 znajduje się sześć przełączników DIP; przełączniki 1–4 służą do ustawiania adresu RS485, przełącznik 5 jest zarezerwowany, a przełącznik 6 służy do redukcji zakłóceń na długich kablach RS485.
- ❖ Jeśli czytnik linii RS485 jest zasilany z terminala, długość powinien wynosić mniej niż 100 metrów lub 330 stóp.
- ❖ Jeśli długość kabla przekracza 200 metrów lub 300 ft., przełącznik nUIDuF Ó przełącznik powinien być ustawiony w pozycji ON, jak pokazano poniżej.

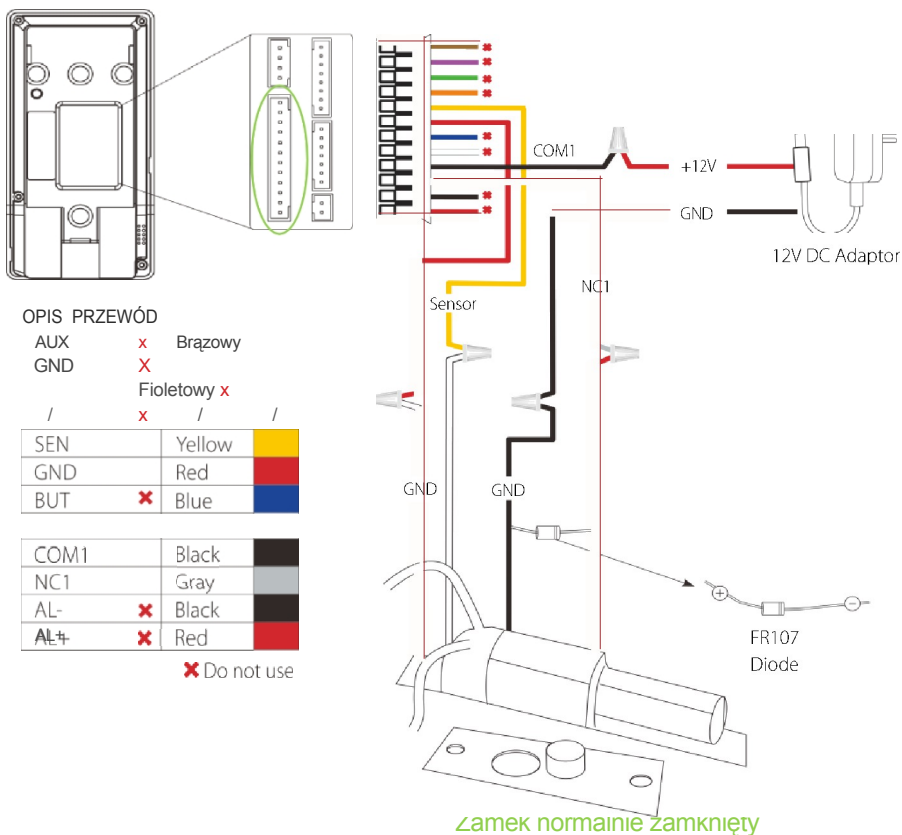
!

Długość: mniej niż 200 metrów

!

Podłączenie przekaźnika śluzu

❖ Urządzenie nie jest zasilane z zamka



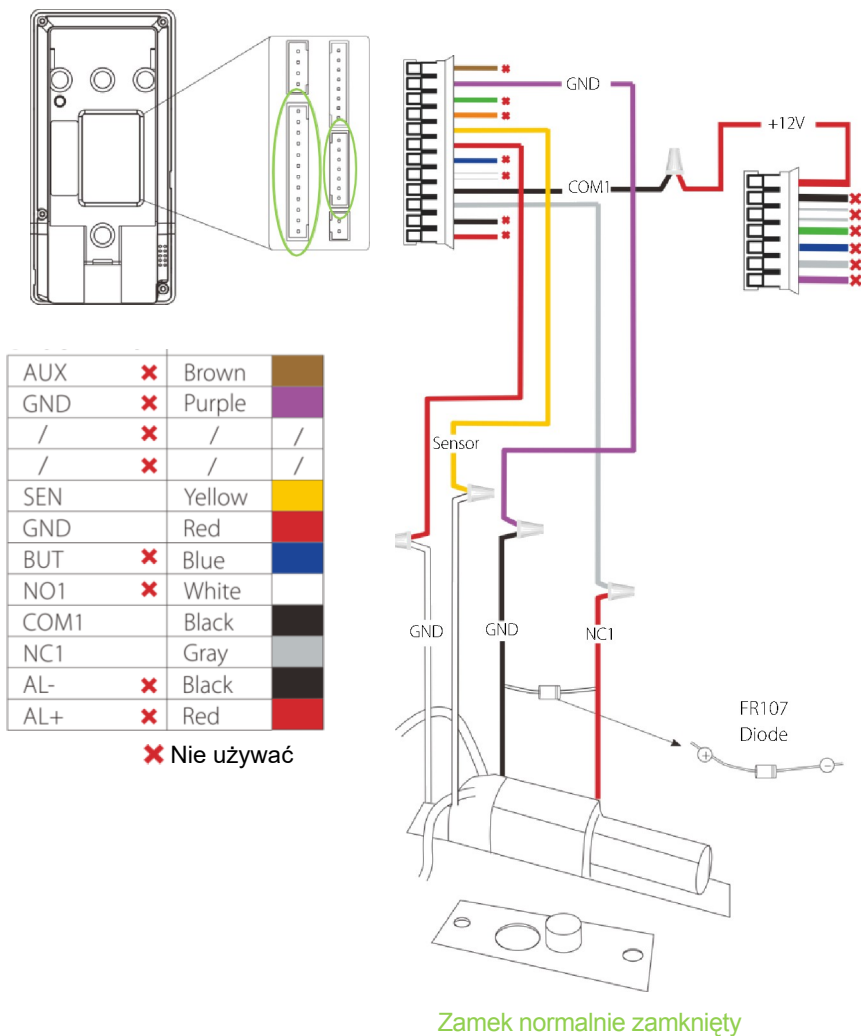
Uwagi:

1. System obsługuje zamki typu NO LOCK i NC LOCK. Na przykład zamek typu NO LOCK (normalnie otwarty przy zasilaniu) podłącza się do zacisków „NO1” i „COM1”, a zamek typu NC LOCK (normalnie zamknięty przy zasilaniu) podłącza się do zacisków „NC1” i „COM1”.
2. Gdy zamek elektryczny jest podłączony do systemu kontroli dostępu, należy podłączyć jeden przewód FR1 07 (znajdujący się w opakowaniu), aby zapobiec na system.

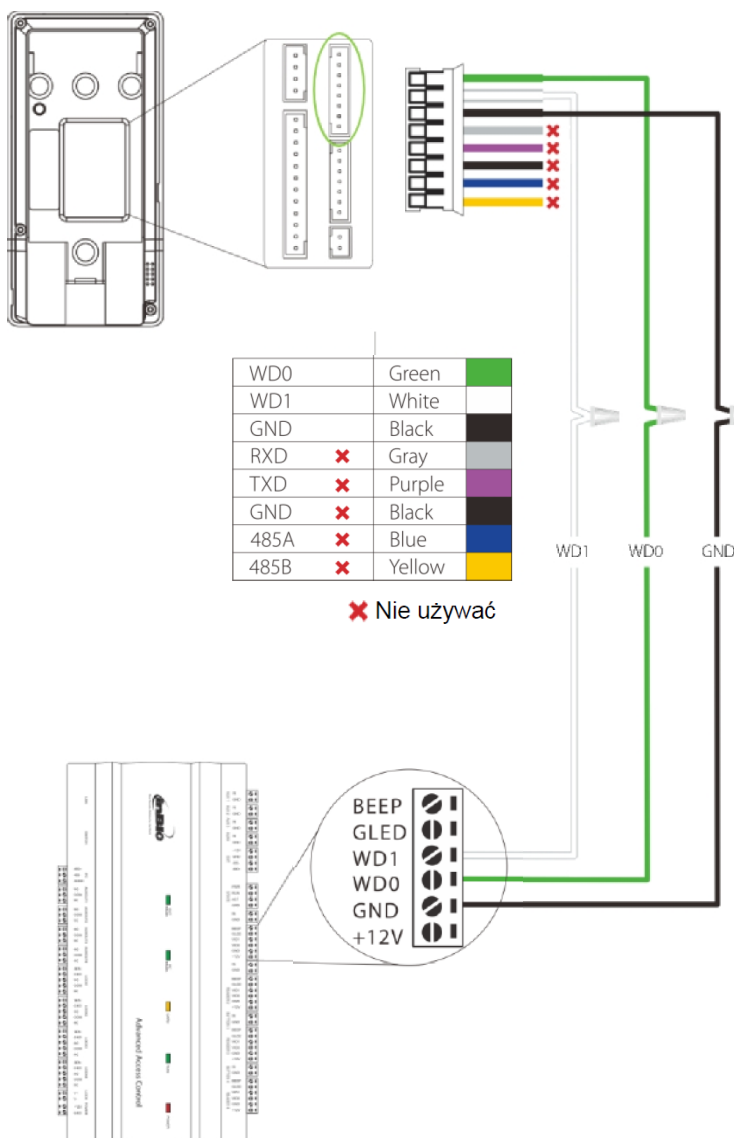
Nie należy odwracać polaryzacji.

Podłączenie przekaźnika zamka

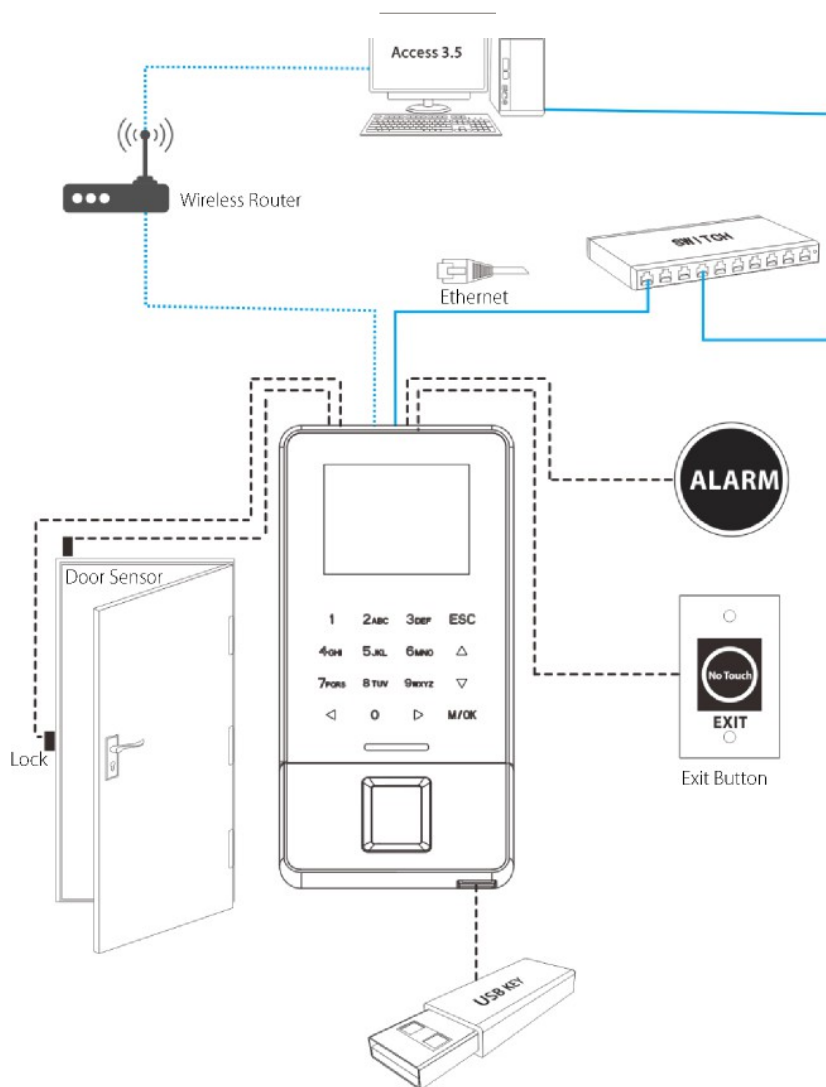
❖ Urządzenie dzielące zasilanie z zamkiem



Podłączenie wyjścia Wiegand

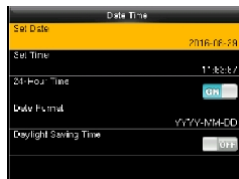
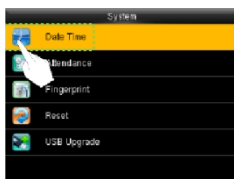


Instalacja autonomiczna



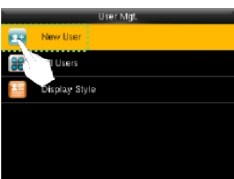
Działanie urządzenia

❖ Ustawienia daty i godziny



Naciśnij ikonę M/OK, aby przejść do menu głównego > System > Data i godzina w celu ustawienia daty i godziny

❖ Dodawanie użytkownika



Naciśnij ikonę M/OK, aby przejść do menu głównego > Zarządzanie użytkownikami > Nowy użytkownik i przejść do interfejsu dodawania nowego użytkownika. Ustawienia obejmują wprowadzenie identyfikatora użytkownika, nazwy użytkownika, wybór roli użytkownika (superadministrator / zwykły użytkownik), rejestrację numeru identyfikatora FP / numeru identyfikatora★ / hasła oraz ustawienie zasad kontroli dostępu.

❖ Ustawienia sieci Ethernet



Naciśnij przycisk M/OK, aby przejść do menu głównego > Konfiguracja > Ethernet.

Poniższe parametry są wartościami domyślnymi z fabryki. *Należy je dostosować zgodnie z rzeczywistą siecią. Adres IP: 192.168.1.201

Maska podsieci: 255.255.255.0

Brama: 0.0.0.0

DNS: 0.0.0.0

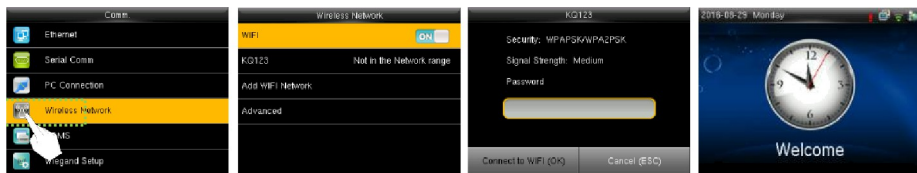
Port komunikacyjny TCP: 4370

DHCP: Dynamic Host Configuration Protocol, czyli protokół dynamicznej konfiguracji hostów, który służy do dynamicznego przydzielania adresów IP klientom za pośrednictwem serwera. Jeśli DHCP jest włączone, adresu IP nie można ustawić ręcznie.

Wyświetlanie na pasku stanu: Ustawia, czy ikona sieci ma być wyświetlana

na pasku stanu.

Działanie urządzenia

 Ustawienia Wi-Fi

1. Naciśnij ikonę M/OK, aby przejść do menu głównego › Komunikacja › Sieć bezprzewodowa;
 2. * naciśnij ikonę M/OK, aby włączyć Wi-Fi i wyszukać * dostępne sieci Wi-Fi w zasięgu;
 3. Wybierz dostępną ikonę W*I, Dress M/OK, aby wprowadzić hasło;
- ^ Po pomyślnym nawiązaniu połączenia z serwerem internetowym na początkowym ekranie pojawi się logo

 Ustawienia ADMS



Naciśnij ikonę M/OK, aby przejść do menu głównego > Komunikacja > ADMS i ustawić parametry używane *do połączenie z serwerem ADMS.

Po pomyślnym połączeniu się z serwerem WWW na początkowym interfejsie wyświetli się logo.

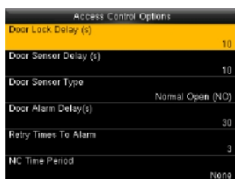
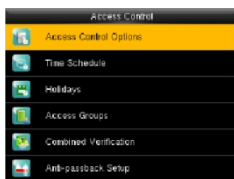
Włącz nazwę domeny: Gdy ta funkcja jest włączona, używany będzie tryb nazwy domeny „http://...”, np. www.1000ip.com. W tym trybie XXX oznacza nazwę domeny; gdy funkcja jest wyłączona, w polu XXX należy wprowadzić adres IP.

Adres serwera: adres IP serwera ADMS. Port serwera: port

używany przez serwer ADMS.

Włącz serwer proxy: Sposób włączenia serwera Droxy. Aby włączyć serwer Droxy, należy ustawić adres IP i numer portu serwera DrOxy. Adres IP DrOxy i adres serwera będą takie same.

❖ Ustawienia kontroli dostępu



Naciśnij ikonę M/OK, aby przejść do menu głównego › Access Cont Vol, aby przejść do ekranu kontroli dostępu. Aby uzyskać dostęp, zarejestrowany użytkownik musi spełnić następujące warunki:

Czas dostępu użytkownika mieścić się w jego osobistej strefie czasowej lub strefie czasowej grupy.

- Grupa użytkownika musi znajdować się w zestawie dostępu (gdy w tym samym zestawie dostępu znajdują się inne grupy, do odblokowania drzwi wymagana jest również weryfikacja członków tych grup).

Opcje kontroli dostępu: Służą do ustawiania parametrów zamka i innych powiązanych urządzeń.

Harmonogram czasowy: Jest to najmniejsza jednostka opcji kontroli dostępu.

Dni wolne: Należy ustawić niektóre dni jako dni wolne, a następnie skonfigurować harmonogram dla tych dni.

Grupy dostępu: Grupowanie służy do zarządzania pracownikami w grupach. Pracownicy w grupach korzystają ze strefy czasowej grupy jednostki czasu. Użytkownicy z grup mogą również ustawić własną strefę czasową.

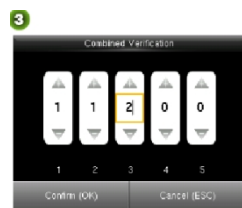
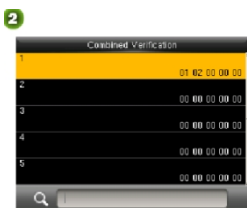
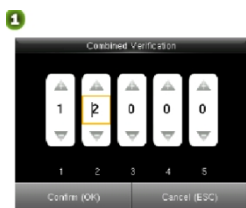
Weryfikacja łączna: Tworzenie różnych grup w ramach kontroli dostępu w celu uzyskania wielokrotnej weryfikacji oraz poprawy bezpieczeństwa

Konfiguracja zapobiegania wejściu za osobą: Aby uniemożliwić komuś wejście za pracownikiem do firmy.

Opcje sytuacji zagrożenia: Urządzenie otworzy drzwi jak zwykle, ale sygnał alarmowy zostanie wysłany do centrali alarmowej, gdy pracownik znajdzie się w sytuacji zagrożenia.

➤ Ustawienia kombinacji kontroli dostępu

Np.: Dodaj kombinację kontroli dostępu, która wymaga weryfikacji przez 2 demony *zarówno z grupy 1 (ustawionej w Zarządzaniu użytkownikami), jak i z grupy 2.



1. Na liście „Weryfikacja łączona” kliknij żądaną kombinację, aby ją zmodyfikować, a następnie wprowadź interfejs (jak pokazano na obrazku 1)

2. Kliknij „+/-”, aby zmienić liczbę, a następnie kliknij „Potwierdź”, aby zapisać zmiany i powrócić do listy „Weryfikacja łączna” (jak pokazano na obrazku 2)

Uwaga:

1. Pojedyncza kombinacja kontroli dostępu może składać się z maksymalnie 5 grup użytkowników (aby otworzyć drzwi, wymagana jest weryfikacja wszystkich 5 użytkowników).
2. Jeśli kombinacja jest ustawiona tak, jak pokazano na rysunku 3, użytkownik z grupy dostępu 2 musi uzyskać weryfikację od dwóch użytkowników z grupy dostępu 1, aby otworzyć drzwi.
3. Aby zresetować kombinację kontroli dostępu, należy ustawić wszystkie numery grup na zero.

Rozwiązywanie problemów

1. Odcisk palca nie jest odczytywany lub odczyt trwa zbyt długo?

- Sprawdź, czy palec lub czytnik odcisków palców nie są zabrudzone potem, wodą lub dust.
- Spróbuj ponownie po wytarciu palca i czujnika odcisków palców suchą chusteczką
- Jeśli odcisk palca jest zbyt rozmazany, wytrzyj palec i spróbuj ponownie.

2. Po weryfikacji wyświetla się komunikat „Nieprawidłowa strefa czasowa”?

- Skontaktuj się z administratorem, aby sprawdzić, czy użytkownik ma uprawnienia do uzyskania dostępu do tej strefy.

3. Weryfikacja przebiega pomyślnie, ale użytkownik nie może uzyskać dostępu?

- Sprawdź, czy uprawnienia użytkownika są prawidłowo ustawione.
- Sprawdź, czy okablowanie zamka jest prawidłowe.

4. Czy włącza się alarm sabotażowy?

- Tak, gdy przycisk antysabotażowy nie jest wciskany przez pokrywę urządzenia wtedy ikona  jest podświetlona w prawym górnym rogu, a głośnik wydaje sygnał dźwiękowy. Tylko wtedy, gdy opcja [Alarm głośnikowy] (Kontrola dostępu  Opcje kontroli dostępu – Alarm głośnikowy) jest w pozycji [Wł.], użytkownik usłyszy sygnał dźwiękowy.
Zainstaluj urządzenie prawidłowo.

