Instrukcja obsługi

Zamek elektroniczny klamka

Model: A209 50/72 TTLock Silver

Spis treści - Klamka

1. Specyfikacja techniczna
2. Elementy w zestawie
3. Metody odblokowania
4. Montaż zamka
5. Rysunek montażowy

---

1. Specyfikacja techniczna

Parametr	Wartość
Pojemność odcisków palców	100
Pojemność kart IC	200 zestawów
Liczba kluczy	2 sztuki
Temperatura pracy	-30°C do 60°C
Grubość drzwi	45–75 mm
Bramka Wi-Fi	Opcjonalna
Materiał	Aluminium
Kolor	Srebrny
Grubość drzwi	45–75 mm
Komunikacja	Bluetooth 4.0
Żywotność baterii	Średnio 10 miesięcy
Zasilanie	DC 6 V – 4 baterie AA
Metody odblokowania	Odcisk palca, karta 13.56 MHz, hasło, aplikacja, klucz mechaniczny
Czas odblokowania	0.5–1.5 sekundy
Temperatura pracy	–30 °C do +60 °C
Wilgotność robocza	10% – 95%
Pojemność użytkowników	200 kart dostępowych, 200 kodów, 100 odcisków palca
Wymiary	37 x 25 x 350 mm

Waga	Klamka z panelem przednim – 492 g, klamka z panelem tylnym – 437 g (łącznie 929 g)

2. Elementy w zestawie

Element	Ilość
Panel przedni	1 szt
Panel tylny	1 szt
Karta IC	2 szt
Komplet akcesoriów montażowych	1 szt

3. Metody odblokowania

Zamek obsługuje wygodne sposoby otwarcia:

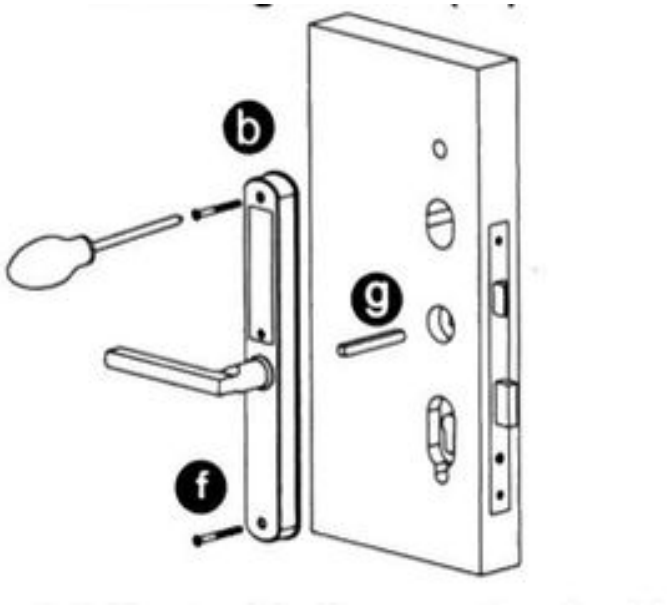
Metoda	Opis
Karta IC (13.56 MHz)	Zbliż kartę do panelu
Kod dostępu	Wprowadź na klawiaturze
Klucz mechaniczny	Awaryjne otwarcie
Aplikacja	Odblokowanie przez telefon
Odcisk palca	Czytnik biometryczny

4. Montaż zamka

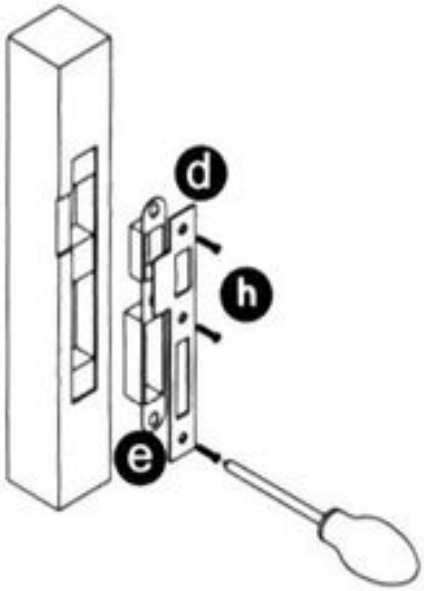
1. **Panel przedni** – przykręć od zewnątrz do zamontowanej w drzwiach wkładki.



2. **Panel tylny** – skręć z przednim dwiema śrubami.



3. **Strike Plate + Box** – zamocuj w ościeżnicy.

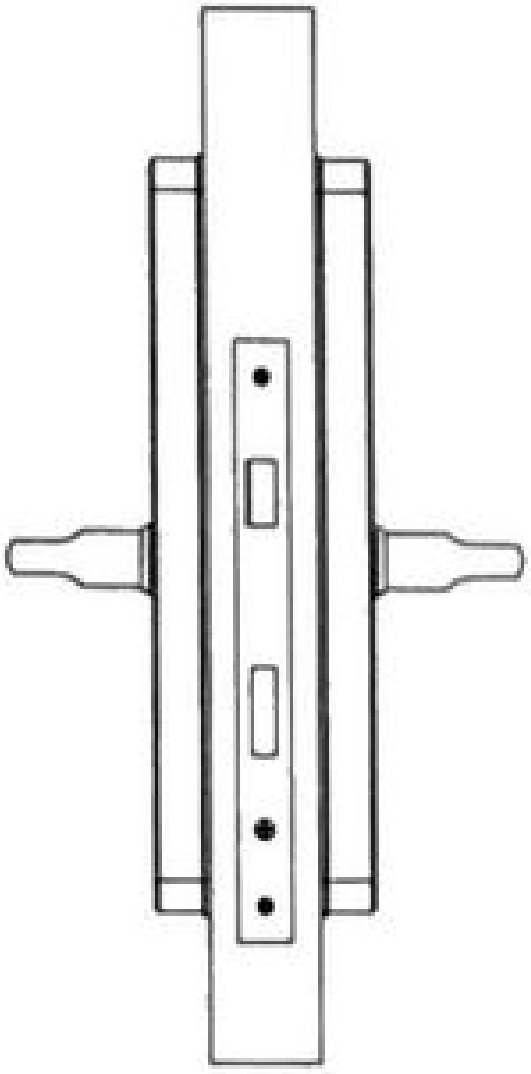


4. **Test klucza** – upewnij się, że wkładka działa gładko.



5. **Test elektroniczny** – włóż baterie; sprawdź kod 123456.

6. **Regulacja** – w razie potrzeby poluzuj/dokręć śruby.



UWAGI MONTAŻOWE

- Klamka może być zamontowana w istniejącej kasecie wyłącznie przy rozstawie 50/72. W pozostałych przypadkach szyld klamki nie będzie dopasowany do położenia zamka.
- Klamka posiada zdejmowalną osłonę (z napisem "LOCK"). Po jej zdjęciu możliwy jest dostęp do mechanicznego zamka (podgląd poniżej):



- Fabrycznie klamka przychodzi z rączką złożoną w dół. Aby ją rozłożyć konieczne jest jej przekręcenie śrubokrętem w zaznaczonym miejscu.



5. Rysunek montażowy

Spis treści - aplikacja TTLock

I. Wprowadzenie
II. Instalacja oprogramowania
III. Główne funkcje
1. Rejestracja i logowanie
1.1. Ustawienia pytań bezpieczeństwa
1.2. Logowanie i reset hasła
1.3. Metody weryfikacji logowania
1.4. Pomyślne logowanie
1.5. Asystent mieszkania
2. Zarządzanie zamkiem
2.1. Obsługiwane typy zamków
2.2. Dodawanie zamka
2.3. Aktualizacja zamka
2.4. Diagnostyka błędów i kalibracja czasu
3. Zarządzanie kluczami elektronicznymi
3.1. Typy kluczy elektronicznych
3.2. Jednorazowy kod dostępu z klucza
3.3. Zarządzanie kluczami elektronicznymi
3.4. Ostrzeżenie o wygaśnięciu dostępu
3.5. Wyszukiwanie historii zamka
4. Zarządzanie kodami dostępu
4.1. Stały kod dostępu
4.2. Kod czasowy
4.3. Jednorazowy kod dostępu
4.4. Kod czyszczący
4.5. Kod cykliczny
4.6. Kod niestandardowy
4.7. Udostępnianie kodu dostępu
4.8. Podgląd i zarządzanie kodami dostępu
5. Zarządzanie kartami
5.1. Podgląd i zarządzanie kartami
6. Zarządzanie odciskami palców
7. Otwieranie zamka przez Bluetooth
7.1. Otwieranie zamka przez Bluetooth
7.2. Otwieranie zamka przez bramkę sieciową
8. Zarządzanie obecnością
8.1. Zarządzanie pracownikami
8.2. Metody rejestracji obecności
8.3. Statystyki obecności
8.4. Sprawdzanie obecności
8.5. Ustawienia danych firmy
8.6. Ustawienia czasu pracy
8.7. Ustawienia dni roboczych
8.8. Ustawienia świąt
9. Ustawienia systemowe
9.1. Zarządzanie grupami kluczy

9.2. Przenoszenie praw administratora
9.3. Obsługa klienta AI
9.4. Informacje o aplikacji
10. Zarządzanie bramką
10.1. Dodawanie bramki
10.2. Lista zamków podłączonych do bramki

I. Wprowadzenie

Aplikacja **TTLock** to oprogramowanie do zarządzania inteligentnymi zamkami.

Aplikacja może być używana do obsługi różnych typów inteligentnych zamków, takich jak:

- zamki do drzwi
- zamki parkingowe
- zamki do sejfów
- zamki rowerowe
- inne kompatybilne urządzenia

Aplikacja oraz zamek komunikują się za pomocą technologii **Bluetooth BLE** (Bluetooth Low Energy – energooszczędny standard łączności bezprzewodowej), co umożliwia:

- odblokowanie i zablokowanie zamka
- aktualizację oprogramowania urządzenia
- odczyt historii operacji
- zarządzanie funkcjami zamka bezpośrednio z aplikacji

Klucz Bluetooth umożliwia również otwieranie zamka przy użyciu **smartwatcha** (zegarka inteligentnego).

II. Instalacja oprogramowania

Aplikację **TTLock** można pobrać na urządzenia mobilne.

iOS

Aplikację można pobrać z **App Store**.

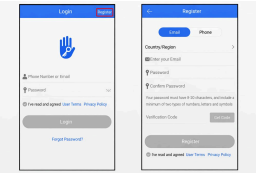
Android

Aplikację można pobrać z **Google Play**.

> **Wygląd aplikacji zależnie od oprogramowania (Android/iOS) może się różnić.**

III. Główne funkcje

1. Rejestracja i logowanie



Użytkownicy aplikacji **TTLock** mogą zarejestrować konto przy użyciu:

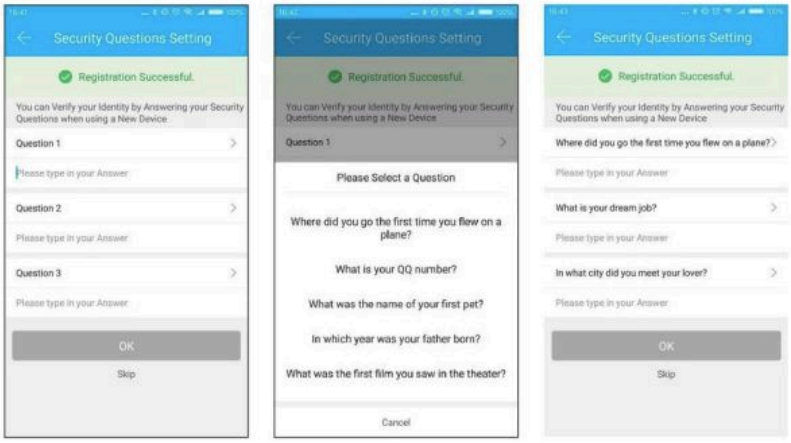
- numeru telefonu komórkowego,
- adresu e-mail.

Jak przebiega rejestracja

1. Wprowadź numer telefonu lub adres e-mail.
2. System wyśle **kod weryfikacyjny** na podany numer telefonu lub adres e-mail.
3. Wprowadź otrzymany kod w aplikacji.
4. Po poprawnej weryfikacji rejestracja zostanie zakończona.

Ważne: Upewnij się, że podczas rejestracji masz dostęp do podanego numeru telefonu lub skrzynki e-mail, ponieważ bez kodu weryfikacyjnego nie będzie możliwe założenie konta.

1.1. Ustawienia pytań bezpieczeństwa



Po pomyślnej rejestracji użytkownik zostanie przeniesiony do strony **ustawień pytań bezpieczeństwa**.

Pytania bezpieczeństwa służą do dodatkowej weryfikacji tożsamości użytkownika.

Do czego służą pytania bezpieczeństwa

Pytania bezpieczeństwa są wykorzystywane w sytuacji, gdy:

- logujesz się na **nowym urządzeniu**
- system wymaga **dodatkowej weryfikacji użytkownika**

Wskazówka: Wybierz pytania i odpowiedzi, które są łatwe do zapamiętania dla Ciebie, ale trudne do odgadnięcia przez inne osoby.

1.2. Logowanie i reset hasła

Aby zalogować się do aplikacji:

1. Otwórz stronę logowania.
2. Wprowadź: - numer telefonu komórkowego
   lub - adres e-mail.
3. Wprowadź hasło do konta.

Ważne informacje

- Numer telefonu jest **automatycznie rozpoznawany przez system**, dlatego zwykle nie trzeba

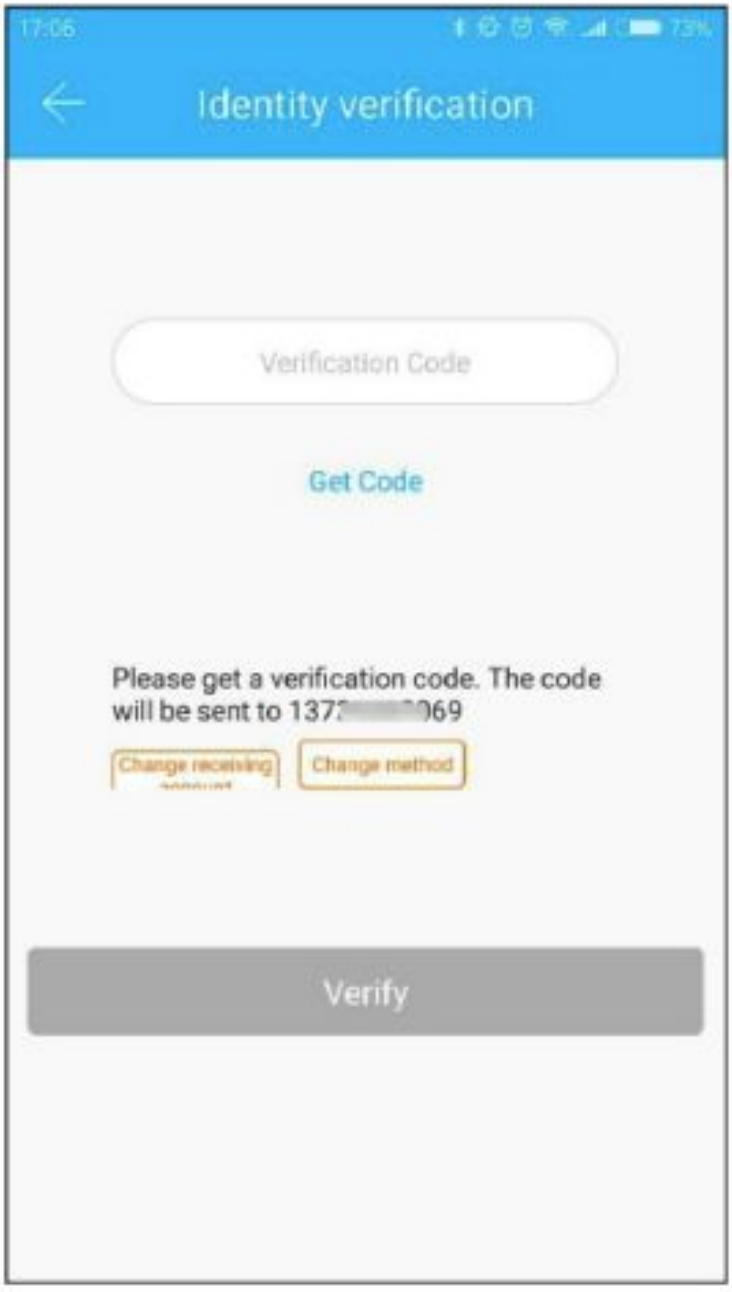
ręcznie wpisywać kodu kraju.

Resetowanie hasła

Jeżeli zapomnisz hasła:

1. Przejdź do strony **resetowania hasła**.
2. Poproś o wysłanie **kodu weryfikacyjnego**.
3. Kod zostanie wysłany na: - numer telefonu, - adres e-mail.
4. Po wprowadzeniu kodu możesz ustawić **nowe hasło**.

1.3. Metody weryfikacji logowania



Jeżeli konto zostanie użyte do logowania na **nowym telefonie**, wymagane będzie dodatkowe potwierdzenie tożsamości.

Procedura wygląda następująco:

1. System poprosi o przejście procesu weryfikacji.
2. Po pomyślnym zakończeniu weryfikacji możliwe będzie logowanie na nowym urządzeniu.
3. Wszystkie dane konta będą dostępne i możliwe do użycia na nowym telefonie.

System oferuje **dwie metody weryfikacji bezpieczeństwa**.

1. Weryfikacja za pomocą kodu

Kod weryfikacyjny jest wysyłany na:

- numer telefonu powiązany z kontem
- adres e-mail powiązany z kontem

Po wprowadzeniu poprawnego kodu użytkownik zostaje zweryfikowany.

2. Weryfikacja za pomocą pytań bezpieczeństwa

Użytkownik odpowiada na wcześniej ustawione pytania bezpieczeństwa.

Jeżeli w ustawieniach konta wybrano metodę **weryfikacji za pomocą pytań**, podczas logowania na nowym urządzeniu pojawi się opcja:

„Weryfikacja poprzez odpowiedź na pytania bezpieczeństwa”.

1.4. Pomyślne logowanie

Po pierwszym uruchomieniu aplikacji **TTLock** i zalogowaniu się do konta:

- jeśli konto **nie zawiera jeszcze żadnych zamków ani kluczy**, na ekranie głównym pojawi się przycisk umożliwiający **dodanie zamka**,



- jeśli konto **zawiera już dodany zamek lub klucz**, na ekranie głównym zostaną wyświetlone **informacje o zamku oraz dostępne funkcje zarządzania**.



Interfejs aplikacji umożliwia szybki dostęp do najważniejszych funkcji, takich jak:

- zarządzanie hasłami
- zarządzanie kluczami
- historia operacji
- ustawienia zamka
- inne funkcje administracyjne

1.5. Asystent mieszkania

Moduł **Apartment Assistant** (asystent mieszkania) jest dostępny w aplikacji tylko wtedy, gdy klucz do

zamka pochodzi z systemu zarządzania mieszkaniami, na przykład systemu wynajmu.

W module tym użytkownik może:

- opłacać czynsz
- zgłaszać naprawy
- sprawdzać należności związane z mieszkaniem

Właściciel mieszkania może korzystać z aplikacji **Room Master App** (aplikacja zarządcy obiektu), aby:

- zbierać opłaty od najemców,
- wysyłać rachunki do lokatorów.

Rachunki mogą obejmować między innymi:

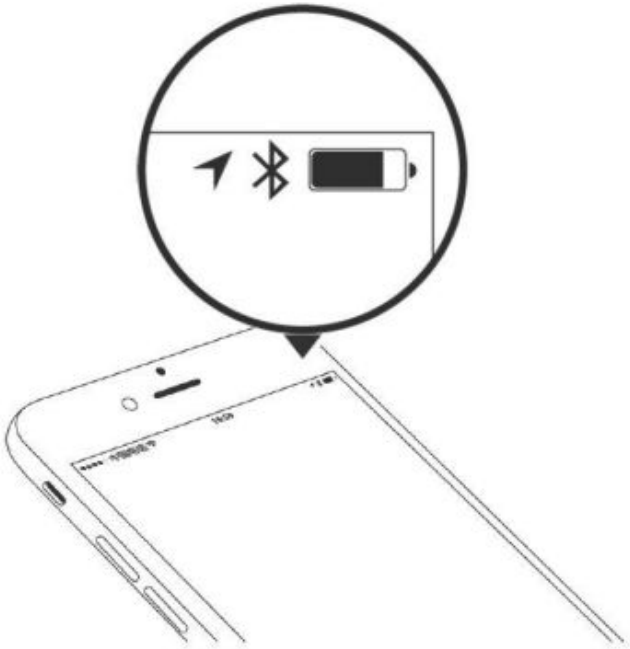
- czynsz
- opłaty za wodę
- opłaty za energię elektryczną
- opłaty za gaz
- opłaty administracyjne
- opłaty za internet (**broadband** – internet szerokopasmowy)
- inne opłaty związane z użytkowaniem mieszkania

UWAGA

Wszystkie z poniżej opisanych funkcji można wykonywać zdalnie **dopiero po połączeniu z dedykowaną bramką sieciową.** Bez bramki konfiguracja jest możliwa jedynie za pośrednictwem łączności bluetooth.

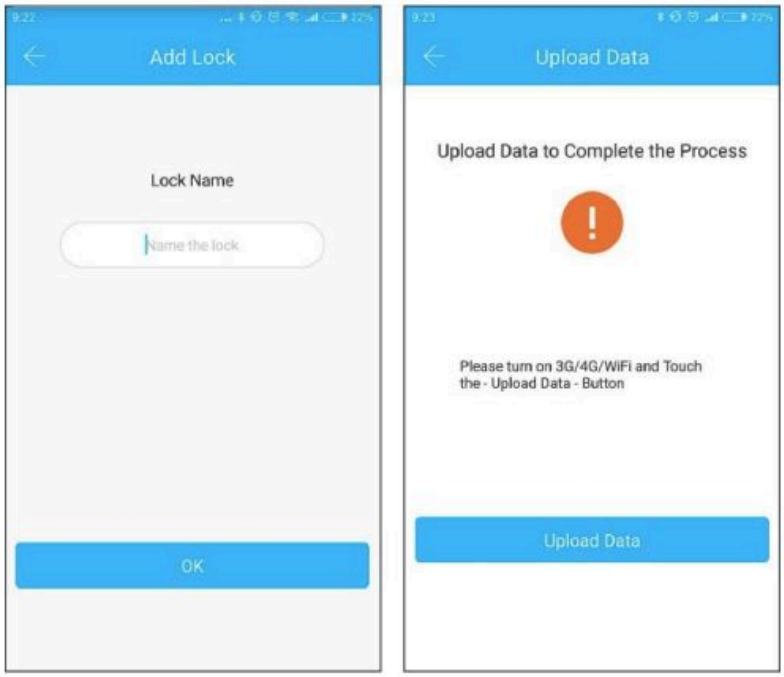
2. Zarządzanie zamkiem

Zanim zamek będzie mógł zostać użyty, musi zostać **dodany do aplikacji TTLock**.



Dodanie zamka polega na **inicjalizacji urządzenia poprzez komunikację Bluetooth pomiędzy telefonem a zamkiem**.

Dodawanie zamka – podstawowe informacje



1. Uruchom aplikację TTLock.
2. Wybierz opcję **dodania nowego zamka**.
3. Stań **w pobliżu zamka**, który chcesz dodać.
4. Aplikacja połączy się z zamkiem za pomocą **Bluetooth**.
5. Po pomyślnym dodaniu zamka będzie można zarządzać nim z poziomu aplikacji.

Po dodaniu zamka można

- wysyłać **klucze dostępu**
- generować **kody dostępu**
- zarządzać użytkownikami
- przeglądać historię operacji
- zmieniać ustawienia zamka

Administrator zamka

Osoba, która **dodaje zamek do aplikacji jako pierwsza**, zostaje automatycznie **administratorem zamka**.

Administrator posiada pełne uprawnienia do zarządzania urządzeniem.

Ważne informacje

- Po dodaniu zamka **nie można ponownie wprowadzić go w tryb konfiguracji przy użyciu klawiatury zamka**.
- Aby ponownie dodać zamek do aplikacji, **aktualny administrator musi najpierw usunąć zamek z aplikacji**.
- Operacja usunięcia zamka musi zostać wykonana **w pobliżu zamka przy użyciu połączenia**

Bluetooth.

Zarządzanie użytkownikami

W sekcji zarządzania użytkownikami można przeglądać listę osób posiadających dostęp do zamka.

Na liście użytkowników wyświetlane są informacje takie jak:

- imię i nazwisko użytkownika
- numer telefonu

Aby sprawdzić szczegóły:

1. Otwórz listę użytkowników zamka.
2. Wybierz użytkownika z listy.
3. Aplikacja wyświetli informacje dotyczące: - przypisanego zamka, - numeru pokoju lub pomieszczenia.

2.1. Obsługiwane typy zamków

Aplikacja **TTLock** obsługuje wiele typów inteligentnych zamków, między innymi:

- zamki do drzwi
- kłódki (**padlock** – kłódka)
- zamki do sejfów
- inteligentne cylindry zamków
- zamki parkingowe
- zamki rowerowe

Dodawanie urządzenia

Podczas dodawania urządzenia należy najpierw **wybrać typ zamka**.

Zamek można dodać do aplikacji dopiero po **wejściu urządzenia w tryb konfiguracji**.

Tryb konfiguracji

- Zamek, który **nie został jeszcze dodany do aplikacji**, może wejść w tryb konfiguracji po **dotknięciu klawiatury zamka**.
- Jeżeli zamek **został już wcześniej dodany**, należy go najpierw **usunąć z aplikacji**, aby ponownie przejść proces konfiguracji.

2.2. Dodawanie zamka

Podczas dodawania zamka dane inicjalizacyjne urządzenia muszą zostać **przesłane do sieci**.

Ważne informacje

- Proces dodawania zamka zostanie zakończony dopiero po **przesłaniu danych do serwera**.
- Jeżeli w momencie konfiguracji **brak jest dostępu do internetu**, dane zostaną przesłane później, gdy połączenie będzie dostępne.

Proces dodawania zamka

1. Wprowadź nazwę zamka.
2. Dodaj urządzenie w aplikacji.
3. Aplikacja zapisze dane inicjalizacyjne.

4. Dane zostaną przesłane do sieci w celu zakończenia procesu konfiguracji.

Ważne: Do samego wykrycia zamka potrzebny jest Bluetooth, ale do pełnego zakończenia konfiguracji potrzebny jest również dostęp do internetu.

2.3. Aktualizacja zamka

Użytkownik może zaktualizować oprogramowanie zamka (**firmware** – oprogramowanie wewnętrzne urządzenia) bezpośrednio z aplikacji **TTLock**.

Wymagania aktualizacji

- aktualizacja musi być wykonana **przez połączenie Bluetooth**,
- telefon musi znajdować się **w pobliżu zamka**.

Przebieg aktualizacji

1. Uruchom funkcję aktualizacji w aplikacji.
2. Połącz się z zamkiem przez Bluetooth.
3. Rozpocznij proces aktualizacji oprogramowania.

Podczas aktualizacji na ekranie pojawi się **wskaźnik postępu**.

Po zakończeniu aktualizacji

Po pomyślnym zakończeniu aktualizacji wszystkie dotychczasowe dane pozostają aktywne, w tym:

- zapisane klucze
- kody dostępu
- karty IC
- odciski palców

2.4. Diagnostyka błędów i kalibracja czasu

Funkcja diagnostyki błędów pomaga analizować problemy systemowe zamka.

Diagnostyka musi być wykonywana **przy zamku poprzez połączenie Bluetooth**.

Procedura diagnostyki

1. Zbliż telefon do zamka.
2. Uruchom funkcję diagnostyki w aplikacji.
3. Aplikacja przeanalizuje stan urządzenia i zidentyfikuje ewentualne problemy.

Kalibracja czasu

Jeżeli system korzysta z **bramki (Gateway)**:

- czas zostanie automatycznie **zsynchronizowany przez bramkę**.

Jeżeli **bramka nie jest dostępna**:

- synchronizacja czasu zostanie wykonana przez **telefon poprzez Bluetooth**.

---

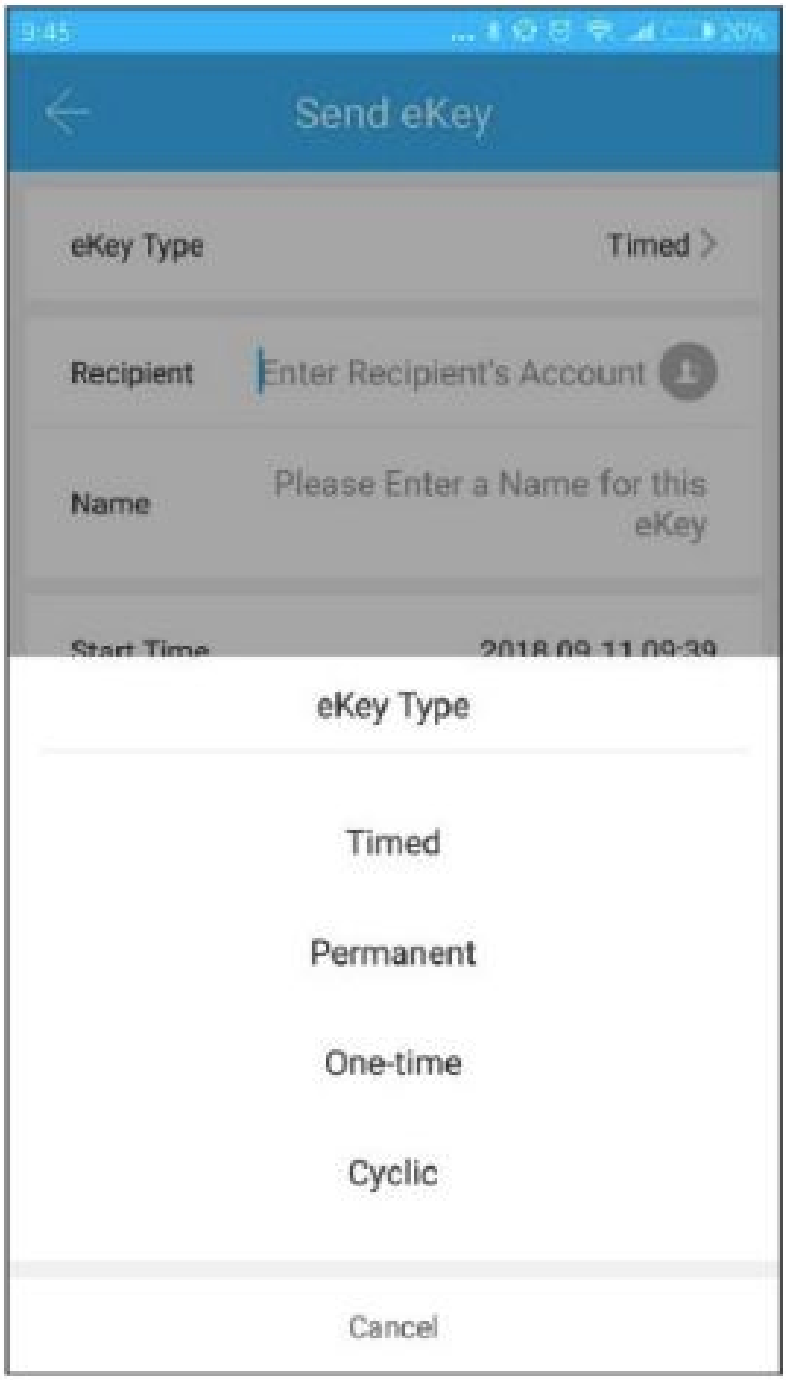
3. Zarządzanie kluczami elektronicznymi

Po pomyślnym dodaniu zamka administrator uzyskuje **najwyższe uprawnienia administracyjne** do zarządzania zamkiem.

Administrator może:

- wysyłać klucze dostępu innym użytkownikom
- zarządzać dostępem użytkowników
- przedłużać ważność kluczy, które wkrótce wygasną
- kontrolować uprawnienia dostępu

3.1. Typy kluczy elektronicznych



Po wybraniu zamka w aplikacji dostępne są różne typy kluczy.

Klucz czasowy

Time-limited eKey – klucz elektroniczny z ograniczeniem czasowym:

- klucz jest ważny tylko przez **określony czas**.

Klucz stały

Permanent eKey – klucz elektroniczny stały:

- klucz może być używany **bez ograniczenia czasowego**.

Klucz jednorazowy

One-time eKey – klucz elektroniczny jednorazowy:

- klucz zostaje **automatycznie usunięty po jednorazowym użyciu**.

3.2. Jednorazowy kod dostępu z klucza

Klucz wysłany z aplikacji **Room Master App** umożliwia uzyskanie **jednorazowego kodu dostępu**.

Kod jednorazowy:

- może zostać użyty tylko **raz**
- po użyciu zostaje **automatycznie dezaktywowany**
- zapewnia wysoki poziom bezpieczeństwa podczas udostępniania dostępu

Kod taki jest często wykorzystywany w sytuacjach takich jak:

- jednorazowy dostęp dla gościa
- krótkoterminowy dostęp serwisowy
- dostęp dla kuriera lub personelu technicznego

3.3. Zarządzanie kluczami elektronicznymi

Administrator zamka może zarządzać kluczami elektronicznymi w aplikacji.

Dostępne operacje obejmują:

- usuwanie klucza (**Delete eKey** – usuń klucz elektroniczny)
- resetowanie klucza (**Reset eKey** – reset klucza elektronicznego)
- wysyłanie klucza do innych użytkowników
- modyfikowanie uprawnień klucza
- wyszukiwanie historii operacji zamka

Administrator może w każdej chwili sprawdzić, którzy użytkownicy posiadają dostęp do zamka.

3.4. Ostrzeżenie o wygaśnięciu dostępu

System wyświetla ostrzeżenia dotyczące wygasania kluczy przy użyciu kolorów.

Kolory ostrzeżeń

- **Żółty** – oznacza, że ważność klucza **wkrótce wygaśnie**.
- **Czerwony** – oznacza, że klucz **już wygasł**.

Dzięki temu administrator może szybko zidentyfikować klucze wymagające przedłużenia lub usunięcia.

3.5. Wyszukiwanie historii zamka

Administrator ma możliwość sprawdzenia **historii odblokowań zamka**.

W historii zapisywane są informacje takie jak:

- data i godzina otwarcia zamka

- użytkownik, który użył klucza
- metoda odblokowania, na przykład klucz elektroniczny lub kod

Funkcja ta umożliwia kontrolę dostępu i analizę wykorzystania zamka.

---

4. Zarządzanie kodami dostępu

Po wprowadzeniu kodu na klawiaturze zamka należy nacisnąć przycisk **odblokowania**, aby otworzyć zamek.

Kody dostępu mogą być różnych typów, między innymi:

- kod stały
- kod czasowy
- kod jednorazowy
- kod czyszczący
- kod cykliczny
- kod niestandardowy

4.1. Stały kod dostępu

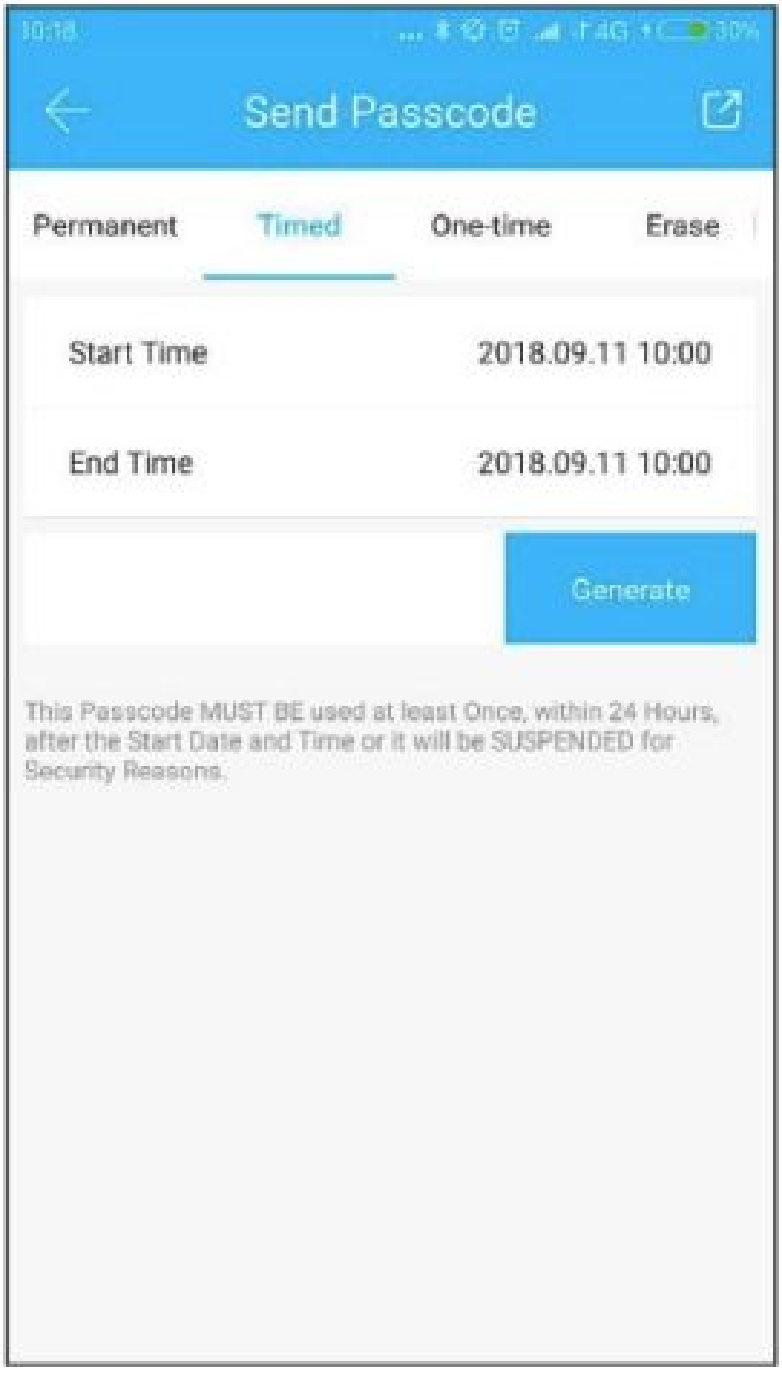


Stały kod dostępu musi zostać użyty **w ciągu 24 godzin od momentu wygenerowania**.

Jeżeli kod nie zostanie użyty w tym czasie, zostanie **automatycznie unieważniony**.

Po pierwszym użyciu kod działa jako **stały kod dostępu**, dopóki nie zostanie usunięty lub zmieniony przez administratora.

4.2. Kod czasowy



Kod czasowy (**Time-limited Passcode** – kod z ograniczeniem czasowym) posiada określony **okres ważności**.

Zakres ważności

- minimalny czas ważności: **1 godzina**
- maksymalny czas ważności: **3 lata**

Dokładność czasu

- jeśli okres ważności jest **krótszy niż rok** – czas ustawiany jest z dokładnością do **godziny**,
- jeśli okres ważności jest **dłuższy niż rok** – dokładność ustawiana jest z dokładnością do **miesiąca**.

Kod czasowy należy użyć **w ciągu 24 godzin od momentu jego wygenerowania**, w przeciwnym razie zostanie automatycznie anulowany.

Zmiana kodu dostępu

Aby zmienić kod dostępu:

1. Wprowadź aktualny kod dostępu.
2. Wprowadź nowy kod.
3. Naciśnij **#**, aby potwierdzić.

Schemat zmiany kodu:

```
aktualny kod # nowy kod (4-6 cyfr) # ponownie nowy kod #
```

> **Uwaga:** Jeżeli kod nie zostanie aktywowany przez pierwsze użycie w ciągu 24 godzin, może przestać działać, mimo że został poprawnie wygenerowany.

4.3. Jednorazowy kod dostępu



Jednorazowy kod dostępu (**One-time Passcode** – kod jednorazowy) może zostać użyty **tylko jeden raz**.

Czas ważności takiego kodu wynosi **6 godzin** od momentu jego wygenerowania.

Po użyciu kod zostaje **automatycznie usunięty z systemu**.

4.4. Kod czyszczący



Kod czyszczący (**Clear Code** – kod usuwający) służy do **usunięcia wszystkich zapisanych kodów dostępu w zamku**.

Cechy kodu czyszczącego

- usuwa wszystkie wcześniej ustawione kody,
- jest ważny przez **24 godziny od momentu wygenerowania**.

Po użyciu kodu czyszczącego wszystkie zapisane kody dostępu zostaną usunięte z pamięci zamka.

> **Ważne:** Z tego kodu należy korzystać ostrożnie, ponieważ usuwa on wszystkie zapisane kody, a nie tylko wybrany kod.

4.5. Kod cykliczny



Kod cykliczny (**Cyclic Passcode** – kod powtarzalny) może być używany **w określonych przedziałach czasu**, które powtarzają się według ustalonego harmonogramu.

Przykładowe tryby użycia

- codziennie (**daily** – codziennie)
- w dni robocze (**weekday** – dni robocze)
- w weekendy (**weekend** – weekendy)

- w określonych godzinach

Kod cykliczny jest szczególnie przydatny w sytuacjach takich jak:

- dostęp dla pracowników
- dostęp dla personelu sprzątającego
- regularny dostęp serwisowy

4.6. Kod niestandardowy

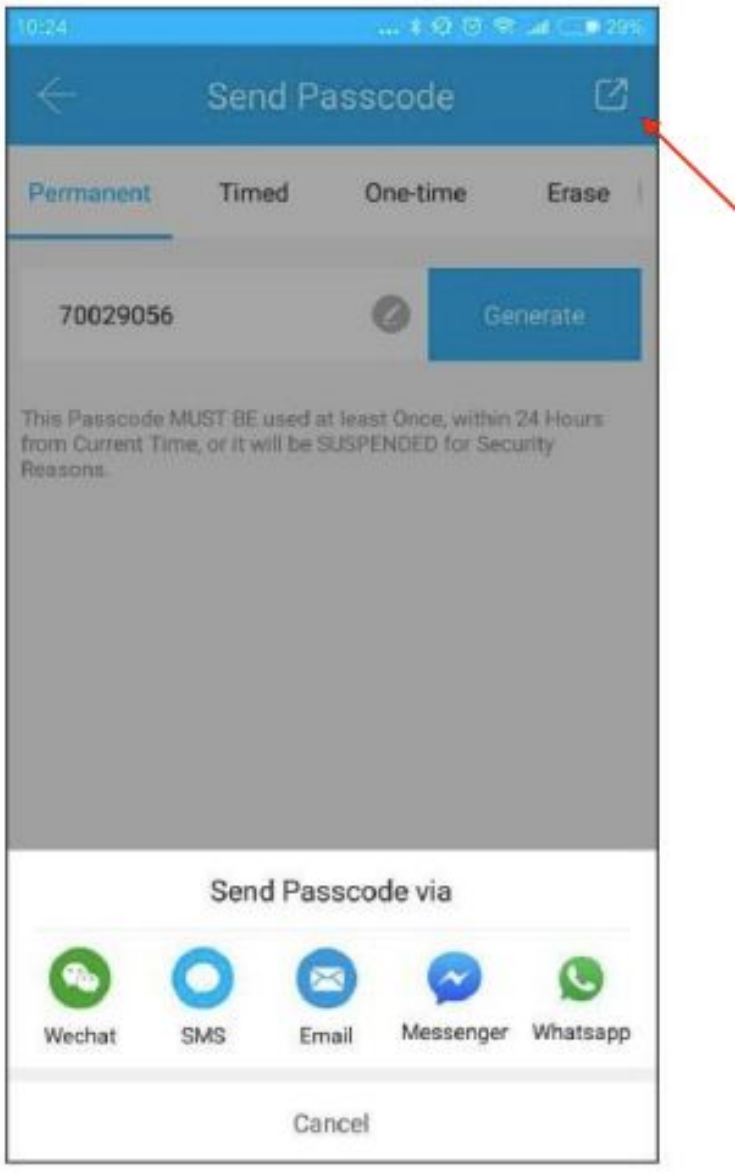
Kod niestandardowy (**Custom Passcode** – kod własny) pozwala ustawić **dowolny kod dostępu oraz okres jego ważności**.

Możliwe ustawienia

- indywidualny kod dostępu
- dowolny czas rozpoczęcia ważności

Kod niestandardowy pozwala dopasować dostęp do konkretnych potrzeb użytkownika.

4.7. Udostępnianie kodu dostępu



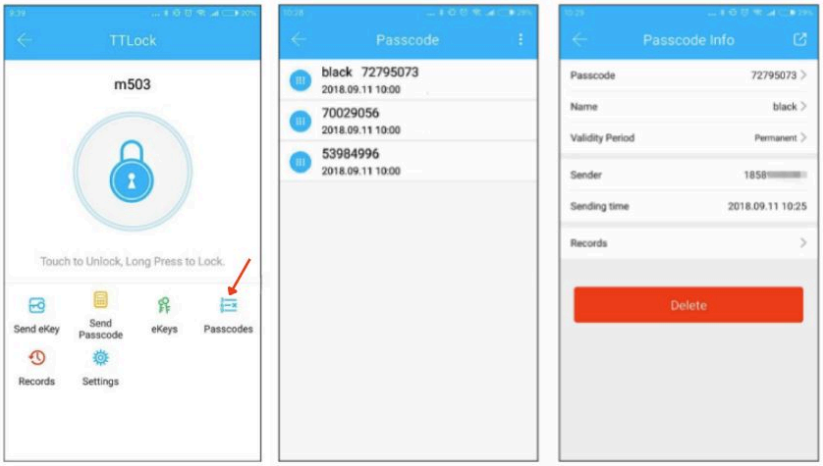
Aplikacja umożliwia łatwe **udostępnianie kodów dostępu innym osobom**.

System umożliwia wysłanie kodu między innymi poprzez:

- **Facebook Messenger**
- **WhatsApp**
- wiadomość SMS
- e-mail
- inne aplikacje komunikacyjne

Dzięki temu administrator może szybko przekazać kod dostępu użytkownikowi bez konieczności ręcznego przepisywania.

4.8. Podgląd i zarządzanie kodami dostępu



Wszystkie wygenerowane kody dostępu można przeglądać i zarządzać nimi w module **zarządzania kodami** w aplikacji.

Dostępne operacje obejmują:

- zmianę kodu dostępu
- usunięcie kodu
- resetowanie kodu
- odblokowanie kodu

Administrator może w każdej chwili sprawdzić szczegóły kodu oraz zarządzać jego uprawnieniami.

---

5. Zarządzanie kartami

Aby korzystać z kart dostępu **IC**, należy najpierw dodać kartę w aplikacji.

Dodawanie karty IC

Cały proces musi zostać wykonany **przy zamku za pomocą aplikacji mobilnej**.

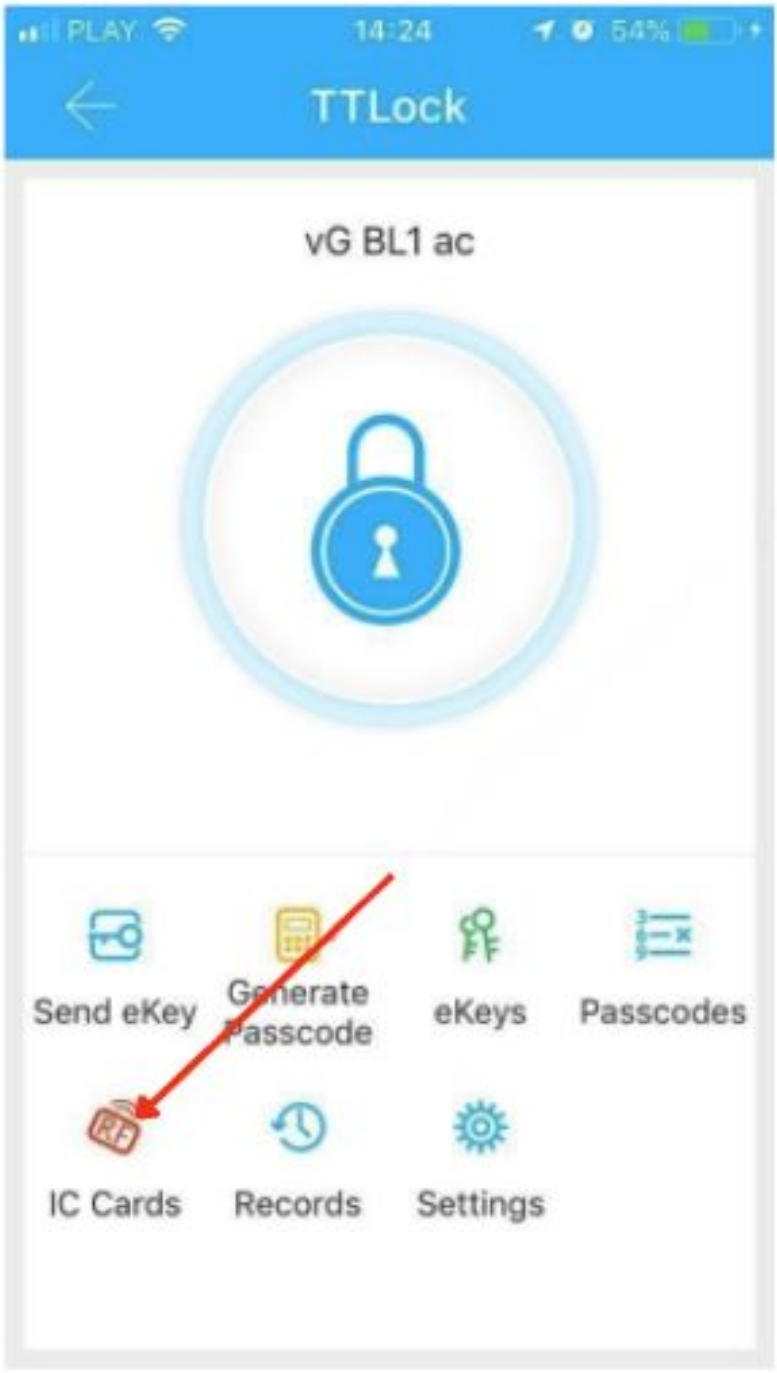
Ustawienia ważności karty

Okres ważności karty IC można ustawić jako:

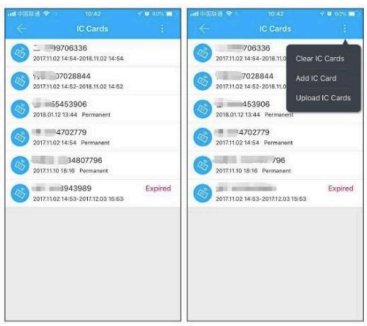
- **stały**
- **czasowy**

Dzięki temu administrator może kontrolować okres dostępu dla użytkowników korzystających z kart.

5.1. Podgląd i zarządzanie kartami



Wszystkie karty IC można przeglądać i zarządzać nimi w module **zarządzania kartami IC**.



Administrator może:

- sprawdzić listę kart
- usuwać karty
- zmieniać ustawienia kart
- kontrolować okres ważności kart

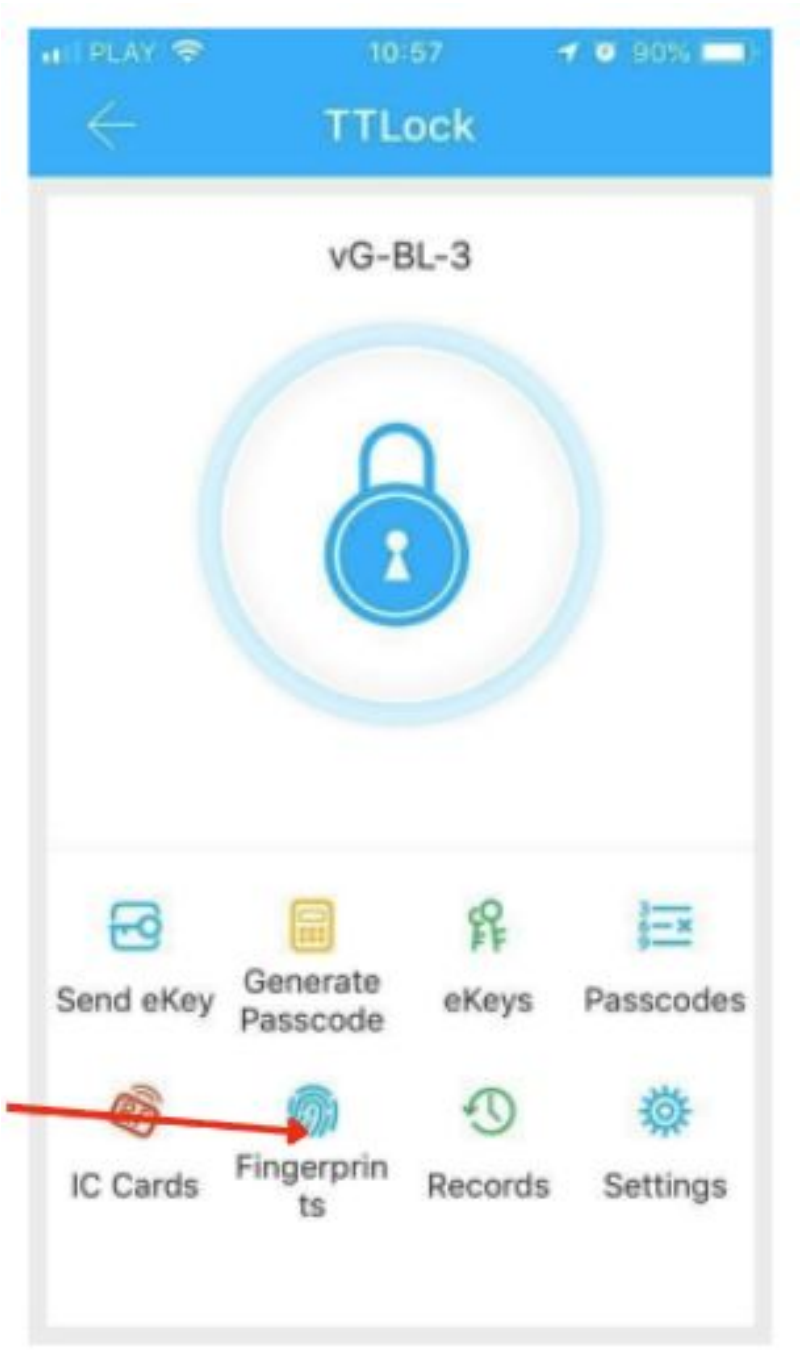
Zdalne wydawanie kart

Funkcja **zdalnego wydawania kart** jest dostępna tylko wtedy, gdy system korzysta z **bramki (Gateway)**.

Jeżeli bramka nie jest zainstalowana, opcja ta nie będzie widoczna w aplikacji.

---

6. Zarządzanie odciskami palców



Zarządzanie odciskami palców działa podobnie jak zarządzanie kartami IC.

Po dodaniu odcisku palca użytkownik może **otwierać drzwi za pomocą czytnika linii papilarnych**.

Administrator może:

- dodawać nowe odciski palców
- usuwać zapisane odciski
- zarządzać dostępem użytkowników

Uwaga: Dodawanie i usuwanie odcisków palców zwykle wymaga bezpośredniego połączenia z zamkiem przez Bluetooth i przebywania w jego pobliżu.

---

7. Otwieranie zamka przez Bluetooth

Użytkownik może **otwierać drzwi za pomocą połączenia Bluetooth** z poziomu aplikacji.

Dodatkowo możliwe jest **udostępnianie klucza Bluetooth innym użytkownikom**.

Sposoby otwierania drzwi

Istnieją dwa sposoby odblokowania zamka:

7.1. Otwieranie zamka przez Bluetooth

Dotknięcie panelu zamka, aby go aktywować, a następnie odblokowanie.

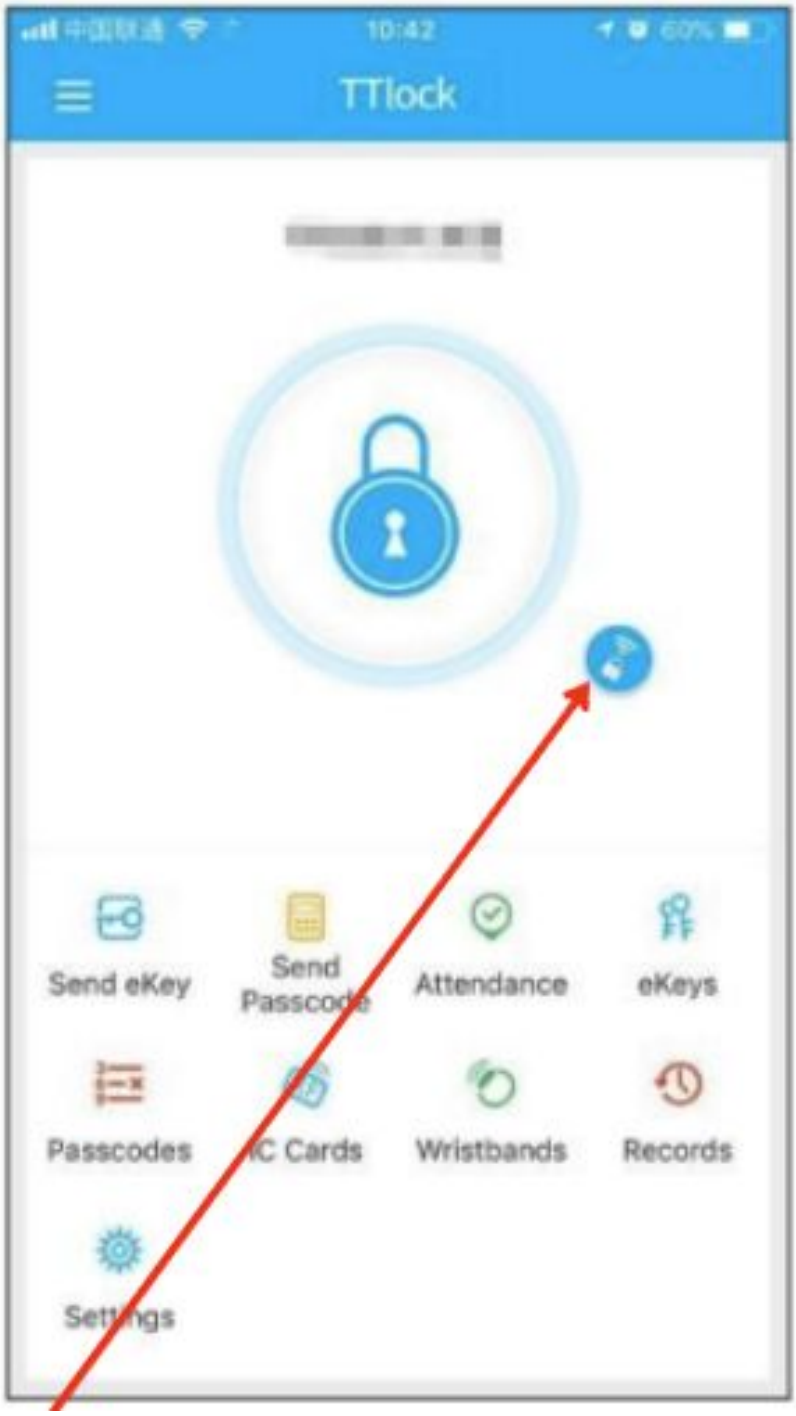


Ważne: Do odblokowania przez Bluetooth telefon musi mieć włączony Bluetooth oraz znajdować się w zasięgu zamka.

7.2. Otwieranie zamka zdalnie poprzez bramkę sieciową

Naciśnięcie przycisku **w kształcie kłódki** w aplikacji mobilnej. Ta opcja jest dostępna wtedy, gdy zamek współpracuje z **bramką sieciową**.

Bluetooth umożliwia szybkie i wygodne sterowanie zamkiem bez konieczności używania kodu lub karty.



---

8. Zarządzanie obecnością

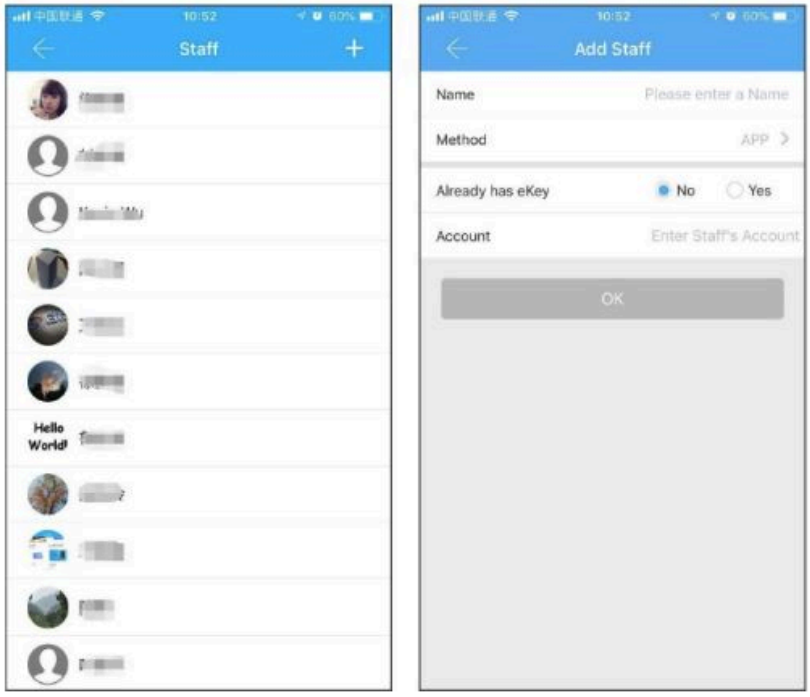
Jedną z funkcji systemu Kejixia jest **kontrola dostępu**, która może być wykorzystywana do **zarządzania obecnością pracowników w firmie**.

Aplikacja zawiera funkcje takie jak:

- zarządzanie pracownikami
- statystyki obecności
- kontrola czasu wejścia i wyjścia

Wszystkie zamki drzwiowe posiadają funkcję rejestracji obecności.
Można ją **włączyć lub wyłączyć w ustawieniach zamka**.

8.1. Zarządzanie pracownikami



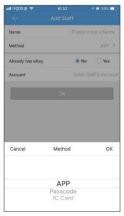
Administrator może przeglądać i zarządzać informacjami o pracownikach w module **zarządzania personelem**.

W module tym można:

- przeglądać listę pracowników
- dodawać nowych pracowników
- edytować informacje o pracownikach
- zarządzać uprawnieniami dostępu

Dzięki temu administrator może łatwo kontrolować dostęp do systemu oraz przypisywać pracownikom odpowiednie uprawnienia.

8.2. Metody rejestracji obecności

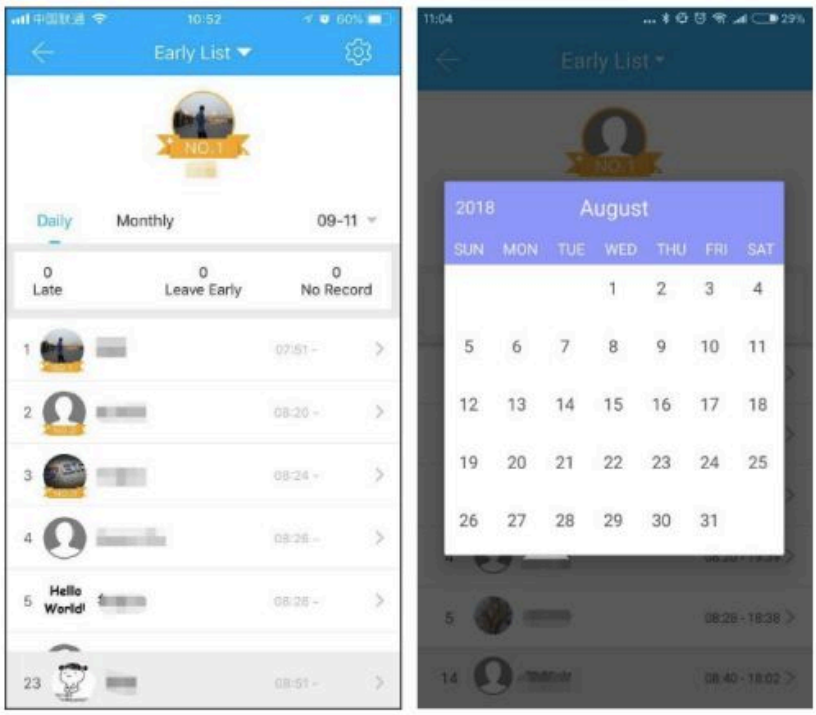


System obsługuje trzy sposoby rejestrowania obecności pracowników:

1. **Aplikacja mobilna**
2. **Kod dostępu**
3. **Karta IC**

Administrator może skonfigurować jedną lub kilka metod w zależności od potrzeb organizacji.

8.3. Statystyki obecności



W tym module można sprawdzić obecność wszystkich pracowników w danym dniu.

System analizuje:

- czas przybycia pracownika do firmy
- czas opuszczenia miejsca pracy
- spóźnienia
- wcześniejsze wyjścia
- brak rejestracji wejścia lub wyjścia

Status obecności jest oznaczany **trzema różnymi kolorami**, co ułatwia szybkie rozpoznanie sytuacji pracownika.

Funkcja ta umożliwia administratorowi:

- monitorowanie punktualności pracowników
- analizowanie czasu pracy
- generowanie raportów obecności

8.4. Sprawdzanie obecności



W tym module można sprawdzić obecność pracowników w różnych miesiącach.

Aby przeglądać dane:

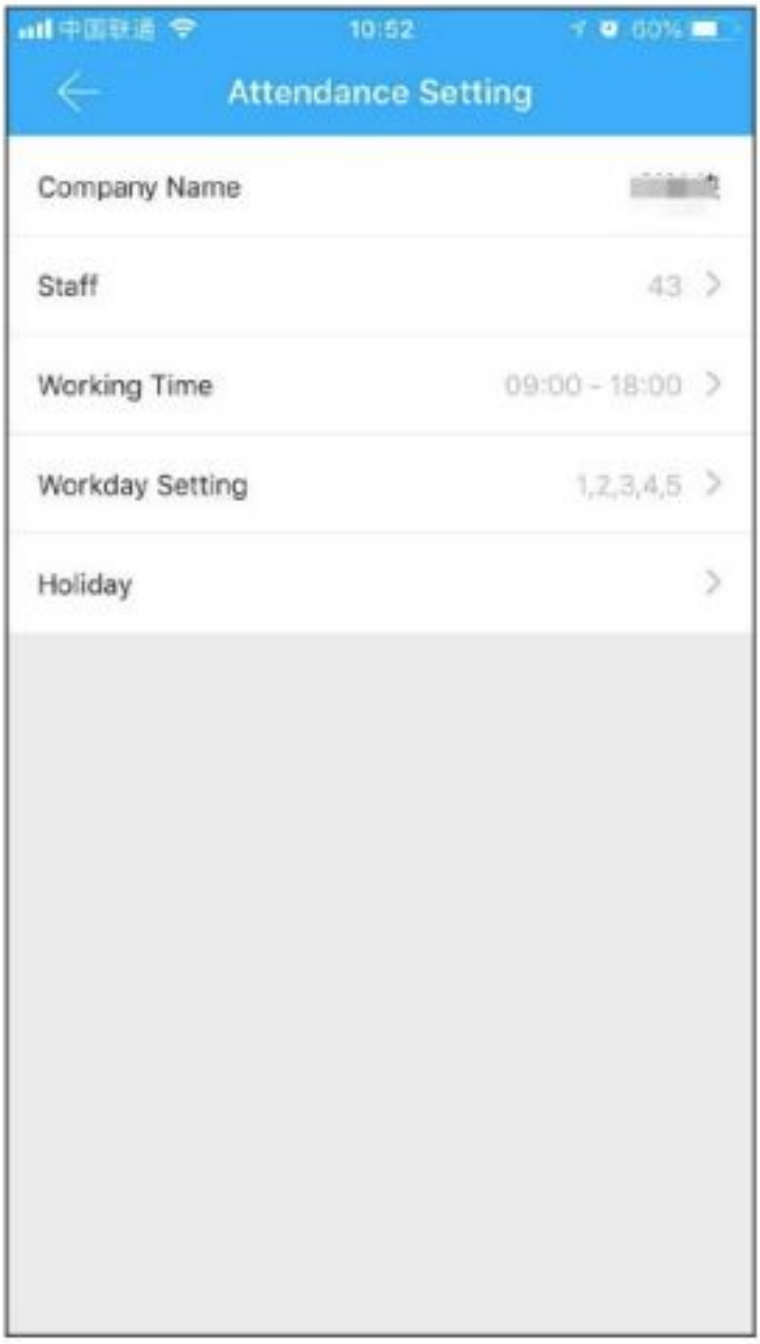
- przesuń ekran **z lewej do prawej**, aby wyświetlić dane obecności dla różnych miesięcy.

Widok kalendarza umożliwia szybkie sprawdzenie:

- dni obecności
- spóźnień
- wcześniejszych wyjść
- dni bez rejestracji obecności

Dzięki temu administrator może łatwo analizować historię obecności pracowników.

8.5. Ustawienia danych firmy



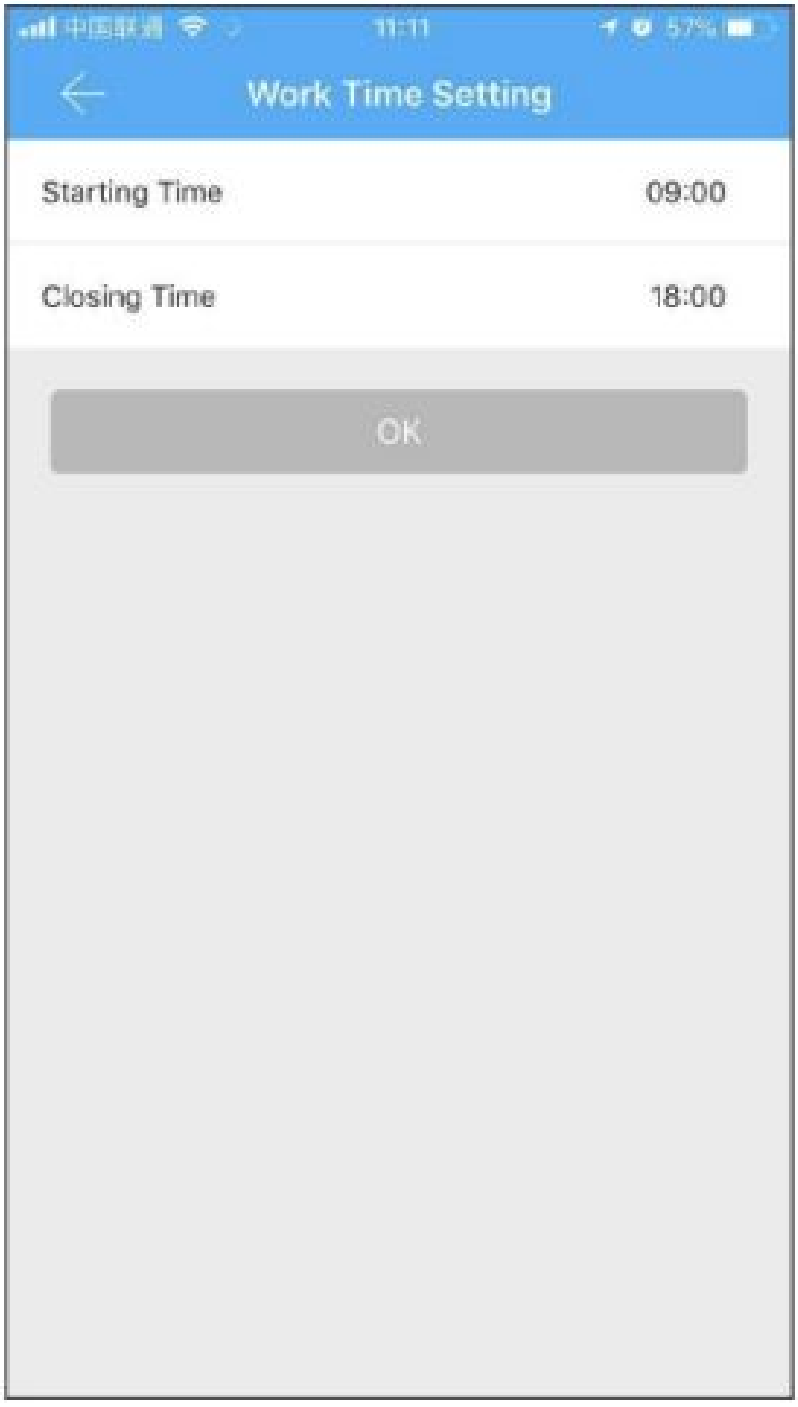
W tym module można skonfigurować podstawowe ustawienia organizacji.

Dostępne opcje obejmują:

- nazwę firmy
- działy w firmie
- godziny pracy
- dni robocze
- dni wolne i święta

Ustawienia te są wykorzystywane przez system do prawidłowego obliczania obecności pracowników.

8.6. Ustawienia czasu pracy



W tym module można ustawić **godziny pracy pracowników**.

System wykorzystuje te ustawienia do określenia:

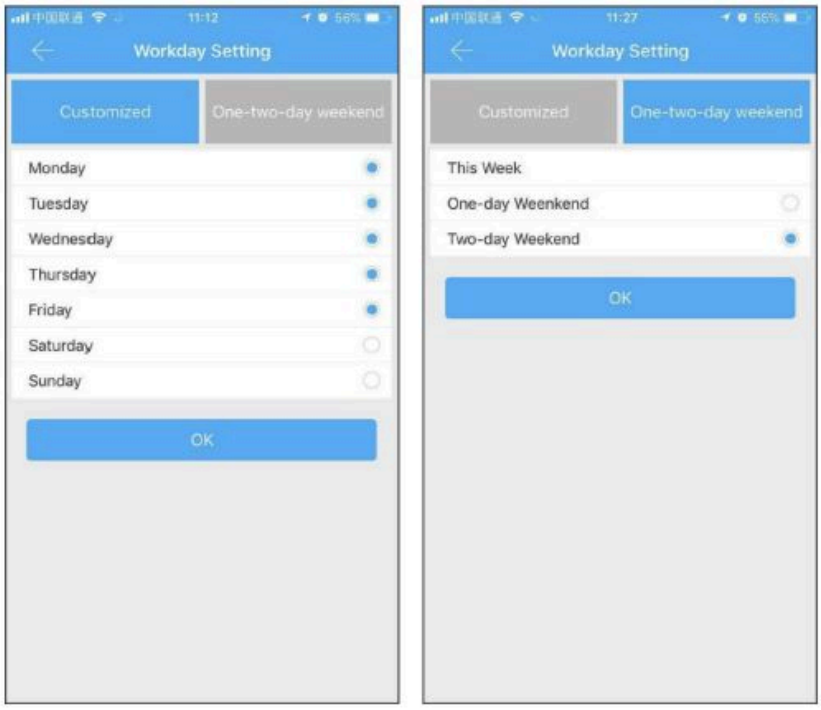
- czy pracownik się spóźnił,
- czy pracownik wyszedł wcześniej z pracy.

Można skonfigurować między innymi:

- godzinę rozpoczęcia pracy
- godzinę zakończenia pracy

Na podstawie tych danych system automatycznie analizuje zapisy obecności.

8.7. Ustawienia dni roboczych



W tym module można określić **które dni tygodnia są dniami roboczymi**.

Administrator może wybrać:

- poniedziałek
- wtorek
- środę
- czwartek
- piątek
- sobotę
- niedzielę

Możliwe jest także ustawienie dodatkowych parametrów, takich jak:

- tydzień pracy
- progi dni wolnych
- inne ustawienia związane z harmonogramem pracy

Dzięki temu system może poprawnie interpretować dane dotyczące obecności pracowników.

8.8. Ustawienia świąt





W tym module można definiować **dni wolne oraz dni robocze** zgodnie z potrzebami organizacji.

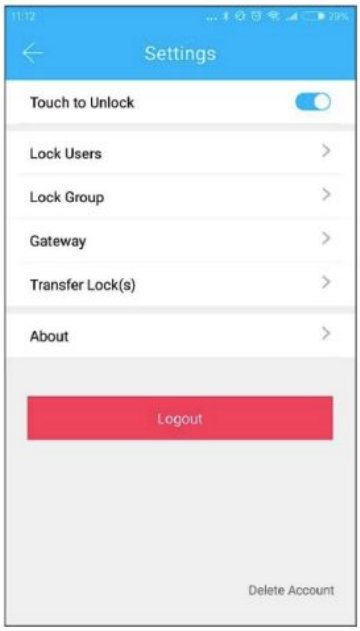
Administrator może:

- ustawić dni świąteczne
- oznaczyć dni wolne od pracy
- zmienić dni robocze

Dzięki temu system obecności może poprawnie interpretować harmonogram pracy pracowników.

---

9. Ustawienia systemowe



W sekcji **ustawień systemowych** dostępne są różne opcje konfiguracyjne aplikacji.

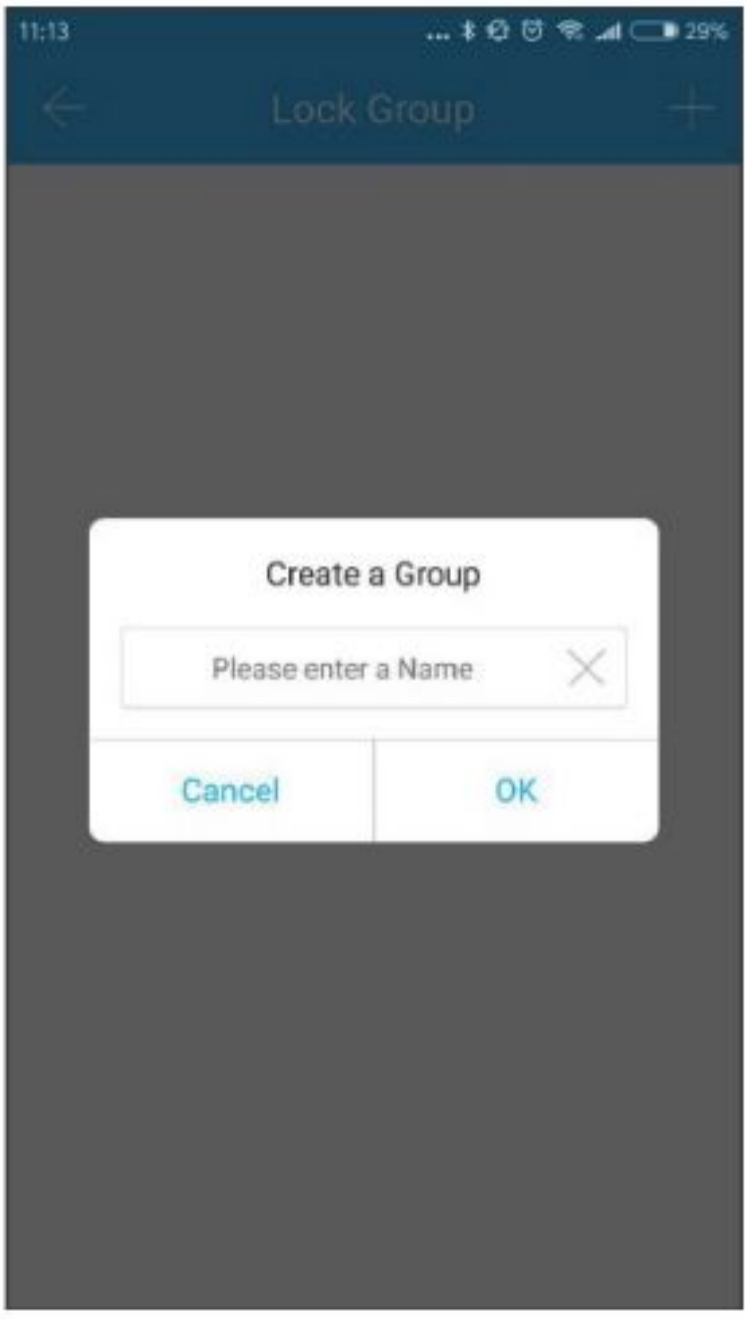
Do najważniejszych należą:

- włącznik odblokowania przez dotyk (**Touch Unlock** – odblokowanie dotykiem)
- zarządzanie grupami
- zarządzanie bramką (**Gateway** – bramka)
- ustawienia bezpieczeństwa
- przypomnienia systemowe
- przenoszenie zarządzania zamkiem

Odblokowanie przez dotyk

Opcja **Touch Unlock** określa, czy drzwi mogą być otwierane poprzez dotknięcie panelu zamka.

9.1. Zarządzanie grupami kluczy



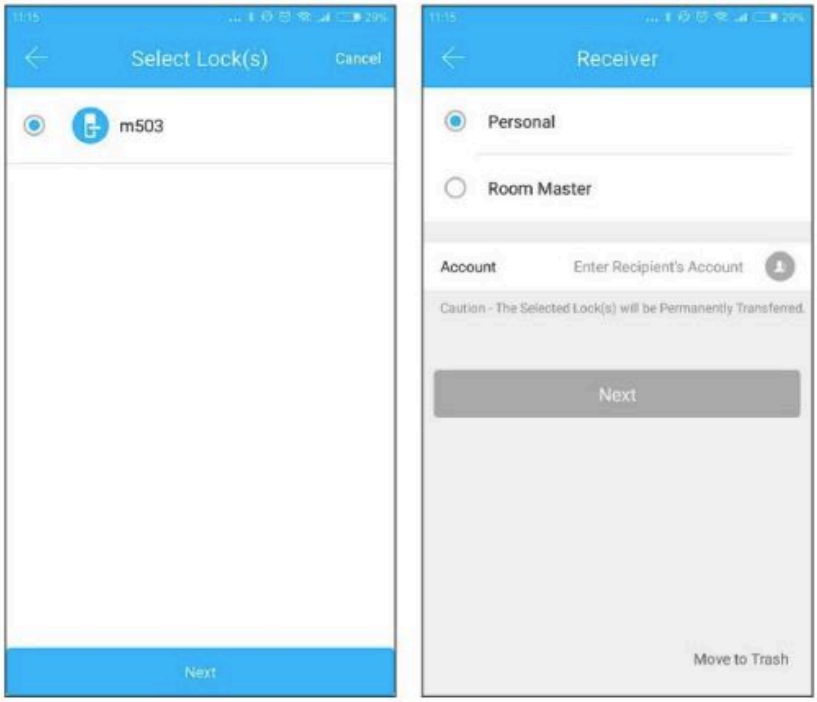
W przypadku dużej liczby kluczy administrator może korzystać z modułu **zarządzania grupami**.

Funkcja ta umożliwia:

- tworzenie grup kluczy
- przypisywanie kluczy do konkretnych grup
- łatwiejsze zarządzanie dużą liczbą użytkowników

Dzięki temu zarządzanie dostępem do zamków jest bardziej uporządkowane i przejrzyste.

9.2. Przenoszenie praw administratora



Administrator może przekazać zarządzanie zamkiem innemu użytkownikowi lub użytkownikowi przypisanemu do pokoju (**Room Master** – zarządca pokoju / obiektu).

Tylko konto, które aktualnie zarządza zamkiem, posiada uprawnienia do przekazania administracji.

Procedura przekazania

1. Wprowadź konto użytkownika, któremu chcesz przekazać zarządzanie.
2. System wyśle kod weryfikacyjny.
3. Wprowadź poprawny kod w aplikacji.
4. Po potwierdzeniu zarządzanie zamkiem zostanie przekazane.

> **Ważne:** Konto, które otrzymuje przekazanie zarządzania, musi posiadać uprawnienia administratora lub możliwość ich przejęcia zgodnie z zasadami systemu.

9.3. Obsługa klienta AI

Użytkownicy mogą korzystać z modułu **obsługi klienta AI**, aby:

- uzyskać pomoc techniczną
- zadać pytania dotyczące działania aplikacji
- przesłać opinie i sugestie

System umożliwia komunikację bezpośrednio przez aplikację.

9.4. Informacje o aplikacji

W sekcji **Informacje o aplikacji** można sprawdzić między innymi:

- numer wersji aplikacji
- informacje o systemie
- dane producenta

Aby kontrolować zamek zdalnie, konieczne jest dokupienie bramki sieciowej. Poniżej znajduje się instrukcja zarządzania bramką.

---

10. Zarządzanie bramką

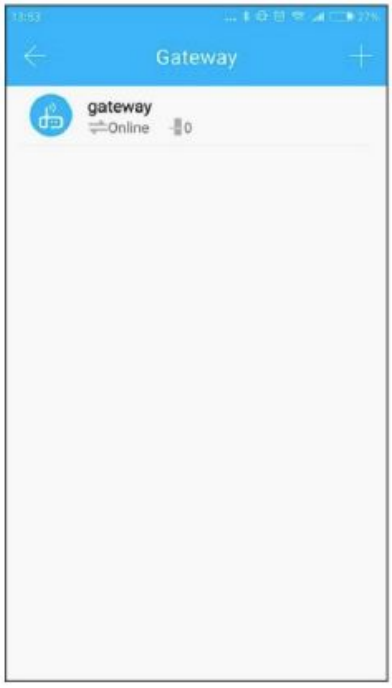
Zamek TTLock komunikuje się bezpośrednio przez **Bluetooth**, dlatego nie jest bezpośrednio podłączony do sieci.

Bramka (**Gateway** – urządzenie pośredniczące) działa jako **most między zamkiem a siecią Wi-Fi**.

Dzięki bramce użytkownik może:

- zdalnie odblokować drzwi
- synchronizować czas zamka
- sprawdzać historię otwarć
- zdalnie usuwać lub zmieniać hasła dostępu

10.1. Dodawanie bramki





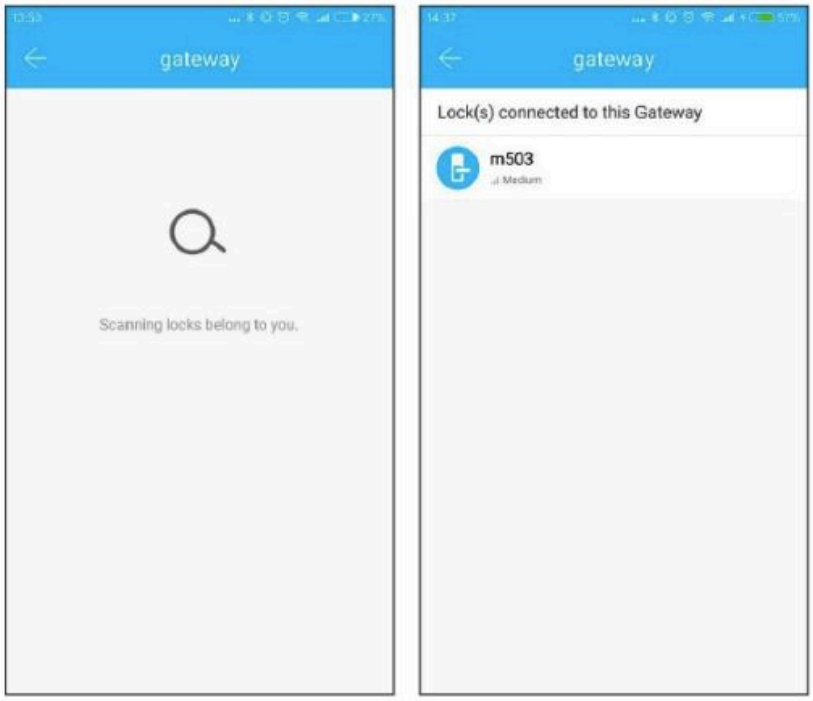
Aby dodać bramkę w aplikacji:

1. Połącz telefon z siecią **Wi-Fi**, z którą będzie połączona bramka.
2. W aplikacji kliknij przycisk **„+”** w prawym górnym rogu.
3. Wprowadź: - nazwę sieci Wi-Fi - hasło Wi-Fi - nazwę bramki
4. Kliknij **OK**, aby potwierdzić.
5. Naciśnij i przytrzymaj przycisk ustawień na bramce przez około **5 sekund**.

Gdy zapali się **zielona dioda**, oznacza to, że bramka weszła w tryb dodawania.

> **Ważne:** Telefon podczas konfiguracji powinien być połączony z tą samą siecią Wi-Fi, z którą ma pracować bramka.

10.2. Lista zamków podłączonych do bramki



Po krótkim czasie aplikacja wyświetli listę zamków znajdujących się w zasięgu bramki.

Po powiązaniu zamka z bramką możliwe jest:

- zdalne zarządzanie zamkiem
- odczyt historii otwarć
- zdalna konfiguracja ustawień zamka

> **Wskazówka:** Jeżeli zamek nie pojawia się na liście, sprawdź, czy znajduje się w zasięgu bramki oraz czy bramka została poprawnie połączona z siecią Wi-Fi.

Dziękujemy za wybór naszego produktu! W razie pytań – skontaktuj się z naszym **Działem Obsługi Klienta**.