



Instrukcja aplikacji TTlock



Uwaga! Niniejsza instrukcja obsługi opisuje wszystkie opcje aplikacji mobilnej. Należy pamiętać, że funkcje wyświetlane w aplikacji są zależne od posiadanego modelu urządzenia.

PROGRAMOWANIE URZĄDZEŃ I OBSŁUGA POPRZEZ APLIKACJĘ MOBILNĄ TTlock

W celu zaprogramowania urządzenia należy pobrać aplikację TTlock z GooglePlay dla urządzeń z systemem Android lub z AppStore dla urządzeń z systemem iOS, a następnie postępować zgodnie z poniższą instrukcją.



QR - Android



QR - iOS

1. Rejestracja konta w aplikacji

- 1.1. w prawym górnym rogu aplikacji należy kliknąć „Rejestracja”;
- 1.2. należy wybrać sposób rejestracji telefoniczny/ e-mailowy
- 1.3. wpisać numer telefonu /adres e-mail
- 1.4. ustawić hasło
- 1.5. pobrać kod weryfikacyjny klikając „Uzyskaj kod”
- 1.6. wprowadzić kod otrzymany SMS'em /e-mailem
- 1.7. należy wpisać odpowiedzi na pytania pomocnicze w przypadku zagubienia hasła – należy odpowiedzieć na 3 pytania wybrane z listy odpowiedzi.

2. Logowanie do aplikacji

Po założeniu konta należy zalogować się do aplikacji wpisując login, tj. nr telefonu / adres e-mail oraz ustalone hasło.

3. Dodawanie urządzeń

Dodawanie pierwszego urządzenia:

W przypadku dodawania pierwszego urządzenia należy kliknąć w okrągłe pole ekranu startowego z napisem „Dodaj zamek”, a następnie należy przejść do czynności opisanych od punktu „3.3.”

Dodawanie kolejnych urządzeń:

- 3.1. W lewym górnym rogu aplikacji należy kliknąć ikonkę z symbolem trzech poziomych kreslek rozwijającą główne menu aplikacji.
- 3.2. Z menu należy wybrać pierwszą pozycję „Dodaj zamek”.
- 3.3. Jeżeli Bluetooth w telefonie nie jest włączony, aplikacja zapyta o włączenie, aby dodać zamek należy wyrazić zgodę.
- 3.4. Z menu wyboru rodzaju urządzeń, należy wybrać pierwszą pozycję „Zamek do drzwi”.
- 3.5. w celu wprowadzenia urządzenia w stan parowania, należy dotknąć jego klawiatury.
- 3.6. Po zakończeniu wyszukiwania, aplikacja wyświetli listę znalezionych urządzeń.
- 3.7. Z listy należy wybrać dodawane urządzenie.

Uwaga! w celu bezproblemowego przejścia przez proces parowania, urządzenia należy dodawać pojedynczo.

4. Menu główne aplikacji

Menu główne aplikacji dostępne jest po kliknięciu ikonki z trzema poziomymi kreskami znajdującej się w lewym górnym rogu ekranu. Opcje dostępne z pozycji menu głównego:

- 4.1. **„Dodaj zamek”** – umożliwi dodanie urządzeń
- 4.2. **„Bramki WiFi”** – umożliwi rozszerzenie funkcjonalności urządzeń poprzez dodanie bramki WiFi ACA-20B9
- 4.3. **„Wiadomości”** – wgląd w informacje systemowe dotyczące np. migracji urządzenia na konto innego użytkownika, logowania na koncie z innego urządzenia itp.
- 4.4. **„Obsługa klienta”** – FAQ – zbiór najczęściej zadawanych pytań i odpowiedzi
- 4.5. **Ustawienia**

Uwaga! Wszystkie aktywowane funkcje w opcjach użytkownika są automatycznie zastosowane do wszystkich urządzeń dodanych do aplikacji.

- 4.5.1. **„Dźwięk”** – Włączenie/ wyłączenie dźwięku powiadomień w aplikacji
- 4.5.2. **„Dotknij, aby odblokować”** – Funkcja umożliwia zwolnienie rygla po przyciśnięciu dowolnego klawisza klawiatury na ok. 3 sekundy.

Uwaga! Opcja wymaga komunikacji aplikacji z urządzeniem, w związku z czym działa wyłącznie w przypadku, gdy aplikacja TTLock jest włączona.

- 4.5.3. **„Powiadomienia push”** – Włączenie/ wyłączenie powiadomień z aplikacji
 - 4.5.4. **„Zablokuj użytkowników”** – funkcja umożliwia blokadę użytkowników, którzy otrzymali cyfrowy klucz dostępu do urządzenia „eKey”
 - 4.5.5. **„Autoryzowany administrator”** – funkcja umożliwia nadanie praw administratora innemu użytkownikowi aplikacji
 - 4.5.6. **„Zablokuj grupę”** – umożliwia zablokowanie działania grupy urządzeń
 - 4.5.7. **„Transfer zamka”** – umożliwia przeniesienie praw super administratora innemu użytkownikowi
 - 4.5.8. **„Transfer bramy”** – umożliwia przeniesienie praw do korzystania z bramy WiFi innemu użytkownikowi
 - 4.5.9. **„Języki”** – wybór języka obsługi aplikacji
 - 4.5.10. **„Blokada ekranu”** – umożliwia dostęp do aplikacji po zwerfikowaniu użytkownika za pomocą odcisku palca, identyfikatora twarzy lub hasła
 - 4.5.11. **„Ukryj niedostępny dostęp”** – pozwala na ukrycie kodów dostępu, kluczy cyfrowych, kart i odcisków palców do urządzeń, do których nie mamy dostępu na określony czas.
 - 4.5.12. **„Zamek wymaga telefonu online”** – smartfon użytkownika musi mieć połączenie z zamkiem w celu odblokowania rygla
 - 4.5.13. **„Usługi”** – płatne usługi umożliwiające ustawienie własnych szablonów SMS, e-mail, itp.
 - 4.5.14. **„O nas”** – informacje o twórcach aplikacji
- 4.6. „Współpracuje z”** – Lista urządzeń i platform z którymi współpracują urządzenia obsługiwane przez aplikację TTLock
- 4.6.1. Programator kart
 - 4.6.2. WeChat mini app
 - 4.6.3. Hotel PMS
 - 4.6.4. Open platform
 - 4.6.5. Amazon Alexa
 - 4.6.6. Google Home

5. Obsługa urządzenia

- 5.1. **Ikona dużej kłódki** widniejącej w górnej części ekranu aplikacji pozwala na zwolnienie zamka będącego w zasięgu nadajnika Bluetooth urządzenia, na którym zainstalowana jest aplikacja.

Uwaga! Po rozbudowie urządzenia o bramkę WiFi istnieje możliwość zdalnego otwierania zamka.

- 5.2. **eKey** – eKey to cyfrowe klucze dostępu, które przesyłamy innym użytkownikom aplikacji, najczęściej dedykowane są dla personelu obsługującego chronione pomieszczenie. Klucze umożliwiają otwieranie zamka będącego w zasięgu nadajnika Bluetooth, aby wysłać eKey należy:
 - 5.2.1. Wybrać ikonę eKey
 - 5.2.2. Kliknąć przycisk „Wyšli eKey”, a następnie ustawić parametry, wybierając zakres czasowy oraz rodzaj klucza: czasowy, stały, jednorazowy lub cykliczny.
 - 7.4.2.3. W polu „Odbiorca” wpisać nazwę konta użytkownika, któremu przekazujemy klucz
 - 7.4.2.4. W polu „Nazwa” należy wpisać nazwę klucza
 - 7.4.2.5. W przypadku wyboru klucza czasowego należy określić jego datę ważności
 - 7.4.2.6. Wysłać klucz, klikając „Wyšlij”

W celu otwarcia drzwi za pomocą eKey należy kliknąć w aplikacji mobilnej w ikonkę dużej kłódki.

W przypadku wygenerowania kluczy po kliknięciu ikony eKeys pojawi się ich lista z informacjami o kluczach – rodzaj klucza, status aktywności.

Z pozycji listy możliwe jest usunięcie klucza, aby to zrobić należy przytrzymać palec na danym kluczu aż do pojawienia się przycisku „Kasuj” po jego naciśnięciu klucz zostanie trwale usunięty.

Uwaga! Usunięcie aktywnego klucza z listy w aplikacji przed czasem jego wygaśnięcia jest możliwe, aby tego dokonać urządzenie z aplikacją musi mieć dostęp do Internetu, a klucz zostanie usunięty dopiero, gdy osoba otrzymująca klucz również podłączy się do Internetu w tym czasie informacja o przed czasowym usunięciu klucza zostanie pobrana z serwera.

Z pozycji listy istnieje możliwość usunięcia wszystkich kluczy jednocześnie, w tym celu należy kliknąć w ikonkę „Reset” znajdującą się w prawym górnym rogu ekranu. Proces kasowania musi być autoryzowany poprzez wpisanie hasła administratora aplikacji.

5.3. „Hasła” – to kody dostępu wysyłane gościom, pracownikom lub innym osobom odwiedzającym, aby wysłać kod dostępu należy wybrać ikonkę „Hasła”, a następnie:

5.3.1. Wybrać rodzaj kodu:

- **stały** – kod bezterminowy – kod musi być użyty chociaż jednokrotnie w przeciągu 24 godzin od ustanowienia, w innym przypadku traci ważność
- **czasowy** – kod czasowy, kod musi być użyty chociaż jednokrotnie w przeciągu 24 godzin od ustanowienia, w innym przypadku traci ważność
- **jednorazowy** – kod jednorazowy – musi być użyty w przeciągu 6 godzin od ustanowienia, w przeciwnym razie traci ważność
- **zwyczajny** – kod manualny – pozwala na pełne spersonalizowanie kodu dzięki możliwości wyboru czasu działania oraz numeru kodu (4-9 znaków)
- **cykliczny** – kod cykliczny pozwala na ustawienie wg schematu, istnieje możliwość wyboru dnia tygodnia oraz godzin działania tego kodu – kod musi być użyty chociaż jednokrotnie w przeciągu 24 godzin od ustanowienia, w innym przypadku traci ważność
- **wymazać** – kod czyszczący – należy go użyć przed upływem 24h, w innym przypadku wygaśnięcie. Po jego użyciu wszystkie kody przypisane do danego urządzenia zostaną usunięte. Aby lista kodów w aplikacji została wyczyszczona należy dokonać synchronizacji aplikacji i szyldu, najłatwiej tego dokonać za pomocą otwarcia drzwi za pomocą ikonki z kłódką

5.3.2. Wygenerować kod klikając przycisk „Wygeneruj hasło”

5.3.3. Kliknąć w przycisk „Kompletny” w celu zakończenia operacji lub „Share” w celu udostępnienia kodu.

W przypadku wygenerowania kodów dostępu po kliknięciu ikony „Hasła” pojawi się ich lista z informacjami o kodach – rodzaj, status aktywności.

Z pozycji listy możliwe jest usunięcie kodu, aby to zrobić należy przytrzymać palec na danym kodzie, aż do pojawienia się przycisku „Kasuj” po jego naciśnięciu kod zostanie trwale usunięty.

Uwaga! Usunięcie aktywnego kodu z listy w aplikacji przed czasem jego wygaśnięcia jest możliwe, aby tego dokonać urządzenie z aplikacją musi mieć dostęp do Internetu lub należy zsynchronizować urządzenie z aplikacją za pomocą Bluetooth.

Z pozycji listy istnieje możliwość usunięcia wszystkich kodów jednocześnie, w tym celu należy kliknąć w ikonkę „Reset” znajdującą się w prawym górnym rogu ekranu. Proces kasowania musi być autoryzowany poprzez wpisanie hasła administratora aplikacji.

5.4. „Karty IC” – urządzenia kontroli dostępu posiadają wbudowany czytnik kart zbliżeniowych Mifare 13,56 Mhz, klikając w ikonkę „Karty IC” wchodzimy w panel zarządzania kartami dostępu.

Aby dodać kartę Mifare należy:

- kliknąć w przycisk „Dodaj kartę IC”
- w polu „Nazwa” wpisać nazwę karty
- wybrać rodzaj dostępu – stały, czasowy, cykliczny
- w przypadku wyboru dostępu czasowego należy ustawić termin ważności
- kliknąć „OK” i czekać na sygnał z szyldu
- po usłyszeniu komunikatu dźwiękowego przyłożyć kartę w okolicę cyfry „5” znajdującej się na klawiaturze numerycznej urządzenia

W przypadku dodania kart po kliknięciu ikony „Karty IC” pojawi się ich lista z informacjami – rodzaj, status aktywności.

Z pozycji listy możliwe jest usunięcie karty, aby to zrobić należy przytrzymać palec na danej nazwie, aż do pojawiania się przycisku „Kasuj” po jego naciśnięciu karta zostanie trwale usunięty.

Uwaga! Usunięcie aktywnej karty z listy w aplikacji przed czasem wygaśnięcia jej ważności jest możliwe, aby tego dokonać urządzenie z aplikacją musi mieć dostęp do Internetu lub należy zsynchronizować urządzenie z aplikacją za pomocą Bluetooth.

Z pozycji listy istnieje możliwość usunięcia wszystkich kart jednocześnie, w tym celu należy kliknąć w ikonkę „Reset” znajdującą się w prawym górnym rogu ekranu. Proces kasowania musi być autoryzowany poprzez wpisanie hasła administratora aplikacji.

5.5. **„Odciski palców”** – niektóre urządzenia wyposażone są w czytnik linii papilarnych, dzięki czemu możliwe jest zwolnienie zamka po przyłożeniu palca do czytnika.

Aby dodać odcisk palca należy:

- kliknąć w przycisk „Dodaj odcisk palca”
- wybrać rodzaj dostępu – stały, czasowy, cykliczny
- w polu „Nazwa” wpisać nazwę użytkownika
- w przypadku wyboru dostępu czasowego należy ustawić termin ważności
- przyłożyć kilkakrotnie opuszek palca do czytnika urządzenia

W przypadku dodanych użytkowników identyfikowanych odciskami palców po kliknięciu ikony „Odciski palców” pojawi się ich lista z informacjami – rodzaj dostępu, status aktywności.

Z pozycji listy możliwe jest usunięcie użytkownika, aby to zrobić należy przytrzymać palec na danym użytkowniku aż do pojawiania się przycisku „Kasuj” po jego naciśnięciu użytkownik zostanie trwale usunięty.

Uwaga! Usunięcie aktywnego użytkownika z listy w aplikacji przed czasem jego wygaśnięcia jest możliwe, aby tego dokonać urządzenie z aplikacją musi mieć dostęp do Internetu, a użytkownik zostanie usunięty dopiero, gdy osoba otrzymująca klucz również podłączy się do Internetu w tym czasie informacja o przed czasowym usunięciu klucza zostanie pobrana z serwera.

Z pozycji listy istnieje możliwość usunięcia wszystkich kluczy jednocześnie, w tym celu należy kliknąć w ikonkę „Reset” znajdującą się w prawym górnym rogu ekranu. Proces kasowania musi być autoryzowany poprzez wpisanie hasła administratora aplikacji.

5.6 – **„Remote”** – funkcja umożliwia dodanie pilotów do zdalnego sterowania urządzeniami – dodawanie i zarządzanie pilotami wygląda analogicznie do dodawania kart IC – patrz punkt 5.4.

5.7 **„Dokumentacja”** – dziennik logów urządzenia

5.8. **„Ustawienia”**

5.8.1. **„Podstawy”**

- Numer zamka
- MAC/ID – adres MAC
- Bateria – status baterii
- Termin ważności – Ważność dostępu
- Nazwa zamka – w tym miejscu możemy wprowadzić nazwę szyldu np. Pokój 308
- Zablokuj grupę – w tym miejscu możemy utworzyć grupę do której możemy przypisać szyldy np. Piętro 1

5.8.2. Klawiatura bezprzewodowa – istnieje możliwość dodania zewnętrznej klawiatury sterującej urządzeniem.

Lock clock – opcja do synchronizacji zegarów aplikacji i szyldu

Fault Diagnosis – diagnozowanie problemów zamka

Lock upgrade – aktualizacja oprogramowania

Attendance – „frekwencja”

Unlocking alert – informacje o odyłowaniu szyldu