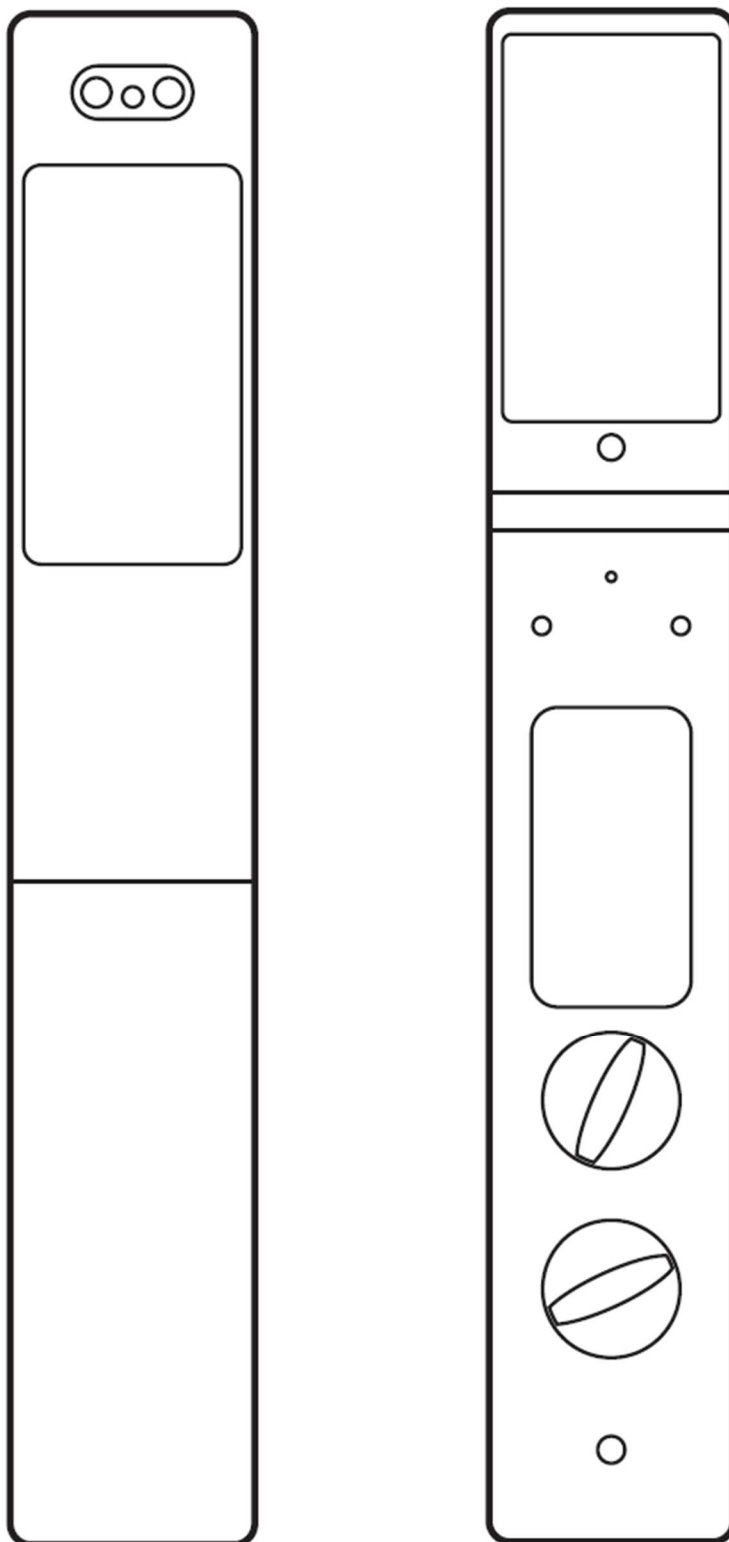


Smart Klamka **Darfi Rivio**

Instrukcja obsługi



Opis ustawień

Ustawienia początkowe

1. Naciśnij i przytrzymaj przycisk ustawień przez 5 sekund, a usłyszysz komunikat: „Przywróć ustawienia fabryczne, NIE(*) TAK(#)”.
2. Naciśnij przycisk #, aby potwierdzić, a system uruchomi się ponownie do stanu początkowego.
3. W stanie początkowym urządzenie można odblokować za pomocą twarzy, odcisku palca, hasła lub karty. Przywrócenie ustawień fabrycznych nie spowoduje skasowania ustawionego kierunku otwierania drzwi ani parametrów momentu obrotowego.

Ostrzeżenie o niskim poziomie naładowania baterii

Jeśli poziom naładowania baterii systemu spadnie poniżej 25%, system wyda komunikat głosowy „Niski poziom naładowania”. Bateria może nadal odblokować zamek około 50 razy, ale należy ją naładować w odpowiednim czasie (lub wymienić).

Zewnętrzne zasilanie awaryjne USB-C

Używając zasilania awaryjnego USB -C, odblokowanie zajmuje około 30 sekund.

Alarm o nielegalnym użytkowniku

Po nieudanej próbie odblokowania zamka 3–5 kolejnych próbach, z komunikatem głosowym: „Nielegalny użytkownik, nielegalne włamanie, powiadomiono właściciela”. Po piątej próbie system zostaje zablokowany na 90 sekund. W tym czasie użytkownik nie ma możliwości odblokowania zamka. Należy spróbować ponownie po upływie 90 sekund.

Hasło wirtualne

Podczas odblokowywania za pomocą hasła, przed i po prawidłowym hasle można dodać dowolną cyfrę, co zwiększa bezpieczeństwo hasła cyfrowego. Na przykład, jeśli hasło to „123456”, można wprowadzić „426123456745”, aby odblokować.

Uwaga: System rozpoznaje tylko pierwsze 16 cyfr.

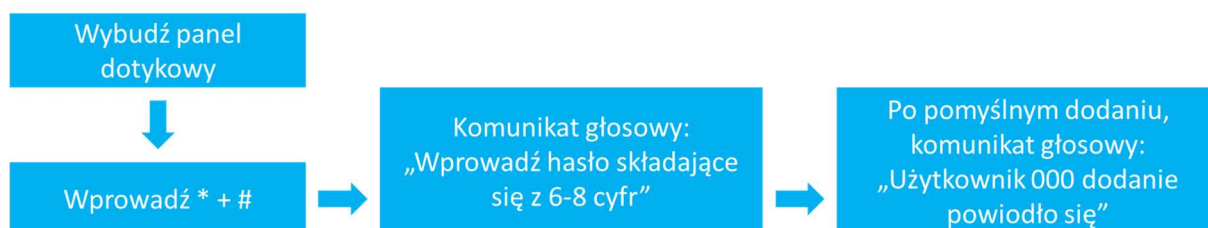
Należy spróbować ponownie po upływie 90 sekund.

Numer wersji

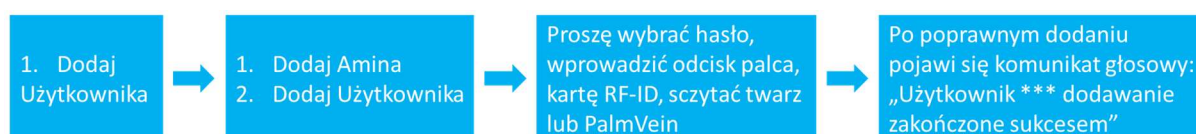
Wprowadź 999 #, aby odczytać numer wersji systemu.

Funkcja i obsługa

Ustawienia użytkownika dodaj hasło administratora po raz pierwszy



Dodaj Użytkownika



- **Twarz: Komunikat głosowy „Zapisz twarz”**

Użytkownik musi ustawić twarz równolegle do kamery w odległości 30–80 cm.

Postępuj zgodnie z instrukcjami głosowymi, aby zakończyć ciągłe nagrywanie twarzy.

- **Palm vein (lub biometria żył dłoni) - technologia biometryczna, która identyfikuje osoby poprzez unikalny wzór żył w ich dłoniach.**

Użytkownik musi ustawić otwartą dłoń / żyłami równolegle do kamery w odległości 10–30 cm.

- **Odcisk palca:**

Użytkownik przykładá palec do czujnika odcisku palca, a komunikat głosowy brzmi „Naciśnij ponownie”. Następnie użytkownik przykładá ten sam palec do czujnika, aby zakończyć ciągłe nagrywanie odcisku palca.

- **Hasło:**

Użytkownik wprowadza hasło składające się z 6–8 cyfr i potwierdza je, naciskając klawisz #.

- **Karta:**

Użytkownik zbliża kartę do obszaru wykrywania karty RF-ID na klawiaturze dotykowej, a system automatycznie odczytuje i zapisuje informacje o karcie.

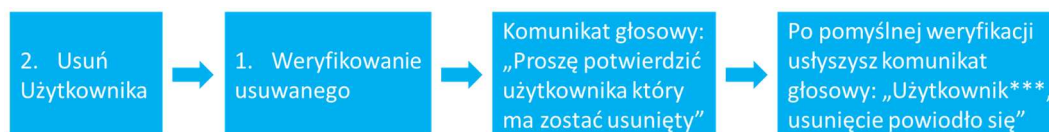
Uwaga:

Liczba użytkowników zarządzających: numeracja 000–009 (łącznie 10)

Liczba użytkowników zwykłych: numeracja 010–249 (łącznie 240).

Usuń Użytkownika

1. Weryfikowanie usuwanego



Metoda weryfikacji:

Odcisk palca:

Przyłóż palec, który chcesz usunąć, do czytnika linii papilarnych.

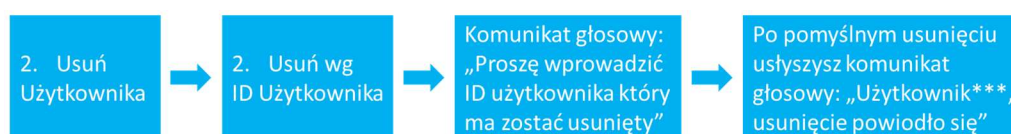
Hasło:

Wprowadź hasło, które chcesz usunąć.

Karta RF-ID:

Karta mikroprocesorowa, którą chcesz usunąć musi znajdować się w pobliżu obszaru wykrywania klawiatury dotykowej. Jeśli użytkownik istnieje w systemie, komunikat głosowy będzie brzmiał: „Sukces”; jeśli użytkownik nie istnieje, komunikat głosowy będzie brzmiał: „Niepowodzenie”.

2. Usuwanie po nr ID Użytkownika



Ustawienia systemowe

Ustawienia daty i godziny

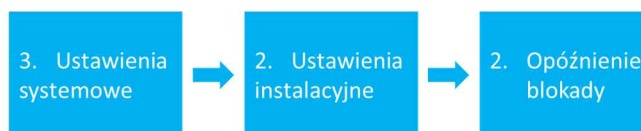


Ustawienie kierunku otwierania drzwi



Uwaga: Kierunek otwierania drzwi należy ustawić w kierunku otwierania zamka na zewnątrz drzwi.

Automatyczna blokada



Uwaga: Opóźnione blokady oznacza ustawienie stałego czasu blokady dolnego zamknięcia. Użytkownicy mogą wybrać czas automatycznego blokowania po: 10 s, 15 s, 20 s, 25 s lub N – wyłączenie automatycznej blokady.

Ustawienia blokady

Alarm antysabotażowy



Uwaga: Po aktywacji alarmu antysabotażowego, jeśli zamek drzwi zostanie naruszony, system wyświetli komunikat alarmowy: „Nielegalny użytkownik, nielegalne włamanie, powiadomiono właściciela”. Jeśli urządzenie jest podłączone do sieci, wyśle informację o alarmie na telefon.

Moment obrotowy silnika



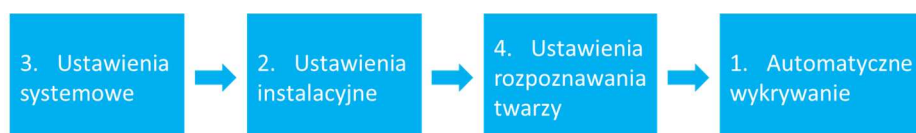
Uwaga: Moment obrotowy silnika jest związany z siłą momentu obrotowego silnika.

Alert przebywania / postoju



Uwaga: Jeśli w ciągu 1 minuty zostanie wykryta obecność człowieka przez łącznie 20 sekund, zostanie uruchomiony alarm postojowy. Urządzenia sieciowe z włączonym alarmem domyślnie nie będą odbierać alarmów dźwiękowych i świetlnych.

Ustawienia rozpoznawania twarzy



Uwaga:

1. Klasyfikacja funkcji sensorycznych człowieka:

- Wykrywanie obecności człowieka [wył.: Inteligentny zamek do drzwi nie będzie wykrywał obecności człowieka w trybie czuwania.

- Wykrywanie obecności człowieka [inteligencja]: Inteligentny zamek do drzwi nie będzie wykrywał obecności człowieka po otwarciu drzwi.

- Wykrywanie obecności człowieka [otwarty]: Inteligentny zamek do drzwi będzie wykrywał obecność człowieka w dowolnym stanie.

2. Jeśli nastąpi 10 kolejnych wybudzeń i nie zostanie wykryte żadne rozpoznanie twarzy, wykrywanie obecności człowieka zostanie domyślnie wyłączone na 5 minut.

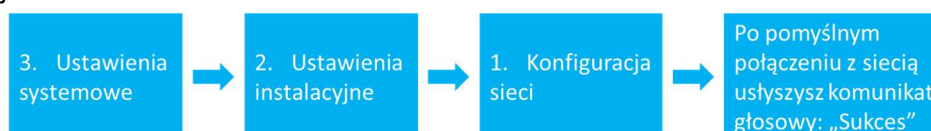
Odległość wykrywania



Uwaga: Odległość wykrywania [blisko]: około 30–50 cm; Odległość wykrywania [średnia]: 50–70 cm; Odległość wykrywania [daleko]: 70–80 cm.

Ustawienia funkcji

Konfiguracja sieci



(Szczegółowe informacje dotyczące obsługi produktów sieciowych znajdują się w załączniku do instrukcji).

Uwaga: Funkcja dystrybucji obsługuje tylko jeden telefon komórkowy. Ponowne przejście do konfiguracji sieciowej spowoduje automatyczne usunięcie ostatnich danych dystrybucji. Użytkownicy powinni zachować ostrożność podczas korzystania z funkcji.

Głośność urządzenia

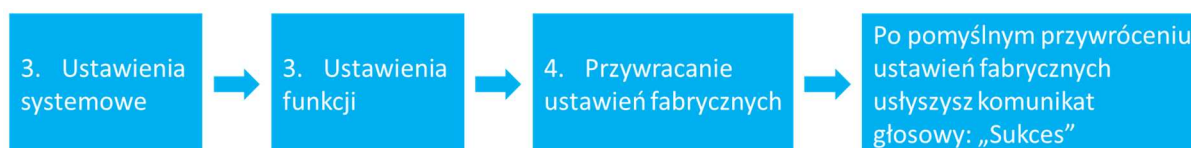


Podwójne uwierzytelnianie



Uwaga: Podwójne uwierzytelnianie możliwe jest wyłącznie przy odblokowywaniu zwykłym kluczem. Aby odblokować pomyślnie, należy zweryfikować dwa różne zwykłe klucze użytkownika. Użytkownicy z uprawnieniami administratora mogą odblokować bezpośrednio.

Przywracanie ustawień fabrycznych



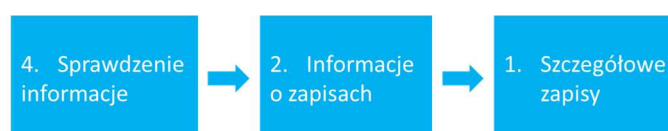
Uwaga: Po przywróceniu ustawień fabrycznych wszystkie dane użytkownika zostaną usunięte. Prosimy o zachowanie ostrożności.

Informacje o wprowadzonych danych do urządzenia

Liczba użytkowników



Odczyt zapisów



Uwaga: Szczegółowe zapisy rozpoczynają się od najnowszych informacji, naciśnij 8 aby wyszukać następny element lub 2, aby wyszukać poprzedni element.

Odczyt zapisów wg czasu



ZAŁĄCZNIK

Obsługa aplikacji Tuya

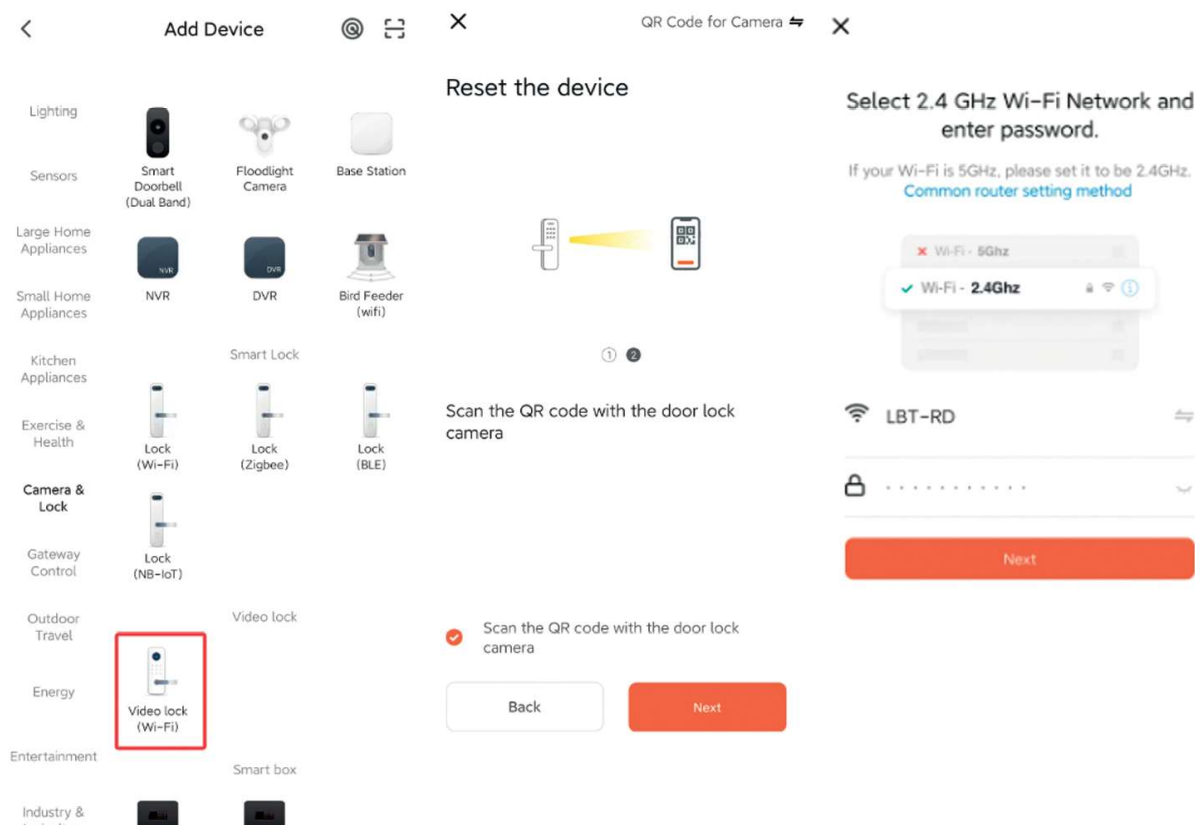
Wyszukiwarka App Store [Smart Life] Pobierz i zaloguj się.

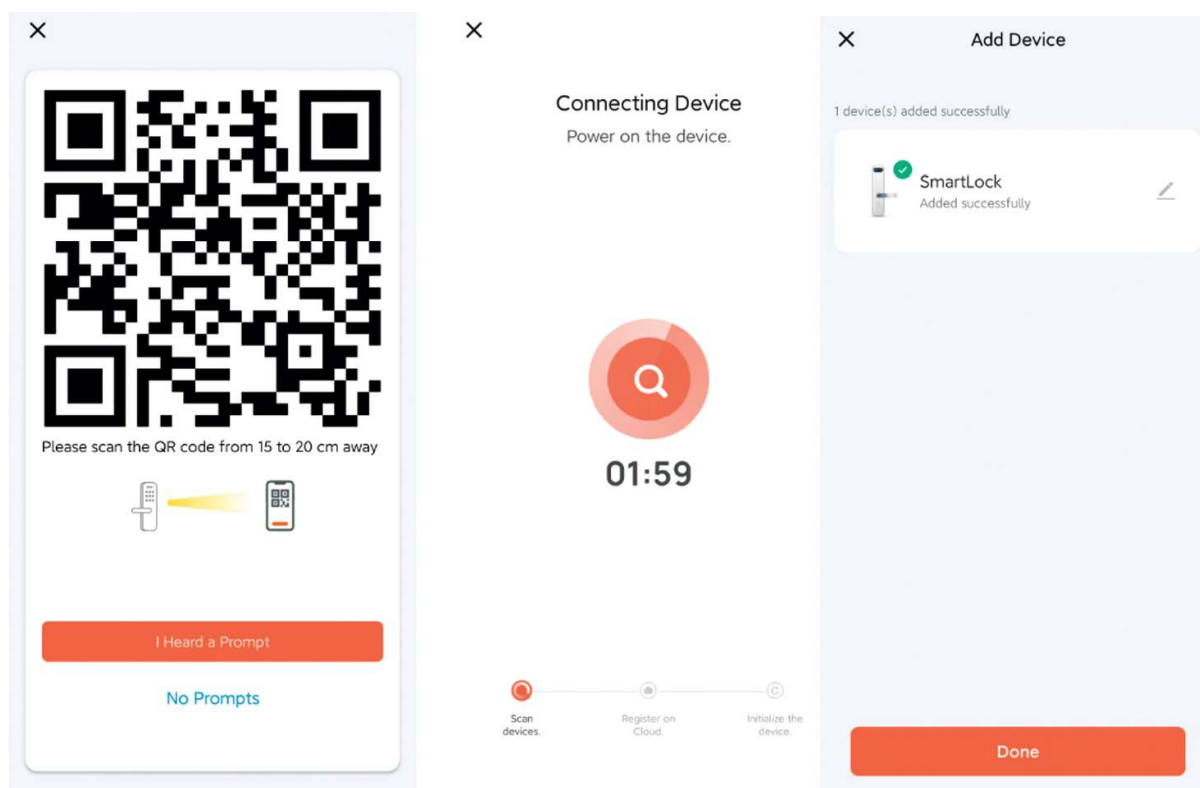
1. Dodaj urządzenie

Po uruchomieniu aplikacji kliknij „+” w prawym górnym rogu strony głównej, aby dodać urządzenie i przejść do strony „Dodaj urządzenie”;

1) Dwuwymiarowa sieć dystrybucji kodu

- Wybierz [Kamera i blokada] i kliknij „Blokada wideo (Wi-Fi)”, aby przejść do następnej strony.
- Interfejs „Resetuj urządzenie”, kliknij Dalej, zaznacz opcję Zeskanuj kod QR za pomocą kamery zamka drzwi, kliknij [Dalej].
- Wybierz Wi-Fi i wprowadź hasło, kliknij [Dalej].
- Po przejściu do strony „Resetuj urządzenie” poczekaj, przejdź do obsługi inteligentnego zamka drzwi i poczekaj, aż przejdzie w tryb sieciowy.
- Skieruj kod QR telefonu komórkowego w stronę kamery. Gdy koniec zamka odtworzy dźwięk „stuknięcia”, kliknij „Usłyszałem komunikat”, aby przejść do trybu dystrybucji.

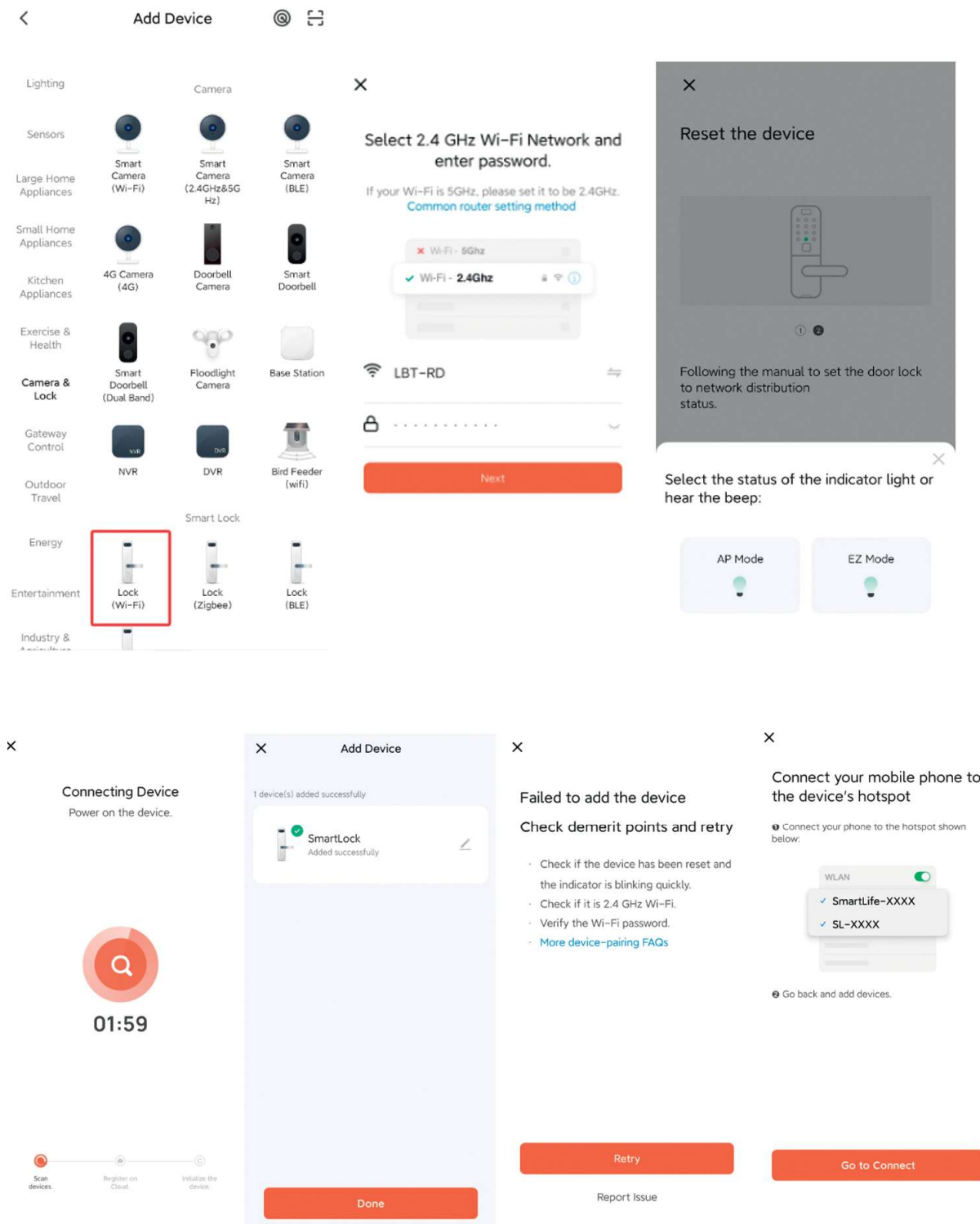




2) Sieć dystrybucji Wi-Fi

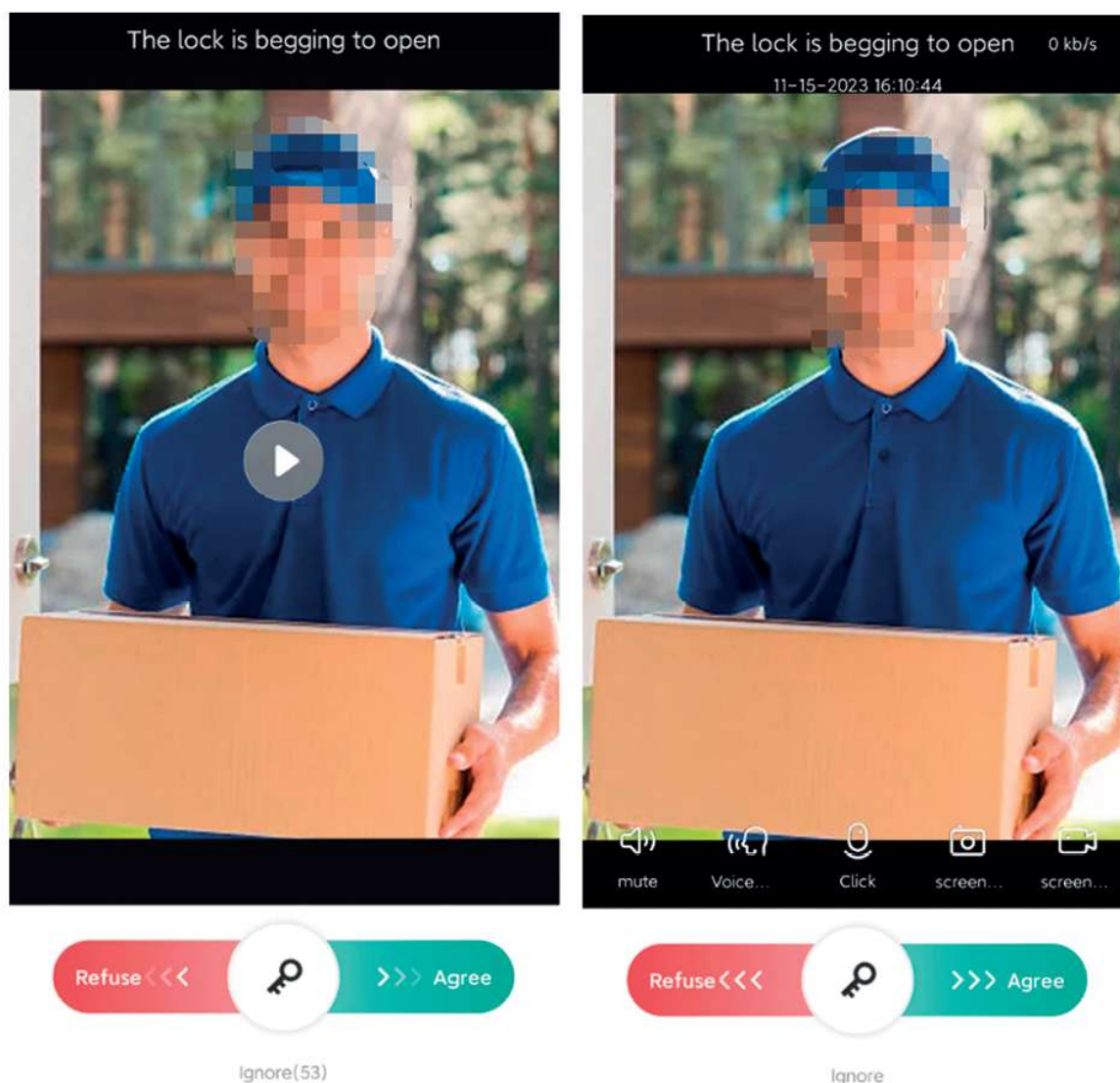
- Wybierz [Kamera i blokada] i kliknij „Zablokuj (Wi-Fi)”, aby przejść do następnej strony.
- Wybierz Wi-Fi i wprowadź hasło, kliknij [Dalej].
- Interfejs „Resetuj urządzenie”, kliknij Dalej, wybierz [Tryb EZ].
- Po wejściu na stronę „Dodaj urządzenie” należy odczekać, przejść do trybu obsługi inteligentnego zamka drzwi i poczekać na przejście w tryb sieciowy.
- W przypadku awarii dystrybucji zasilania można wybrać opcję „Przełącz tryb dystrybucji zasilania” lub wybrać tryb hotspotu. Połącz się z hotspotem Wi-Fi za pomocą aplikacji SmartLife i skonfiguruj sieć zgodnie z instrukcjami telefonu komórkowego.

Uwaga: Nazwy niektórych hotspotów urządzeń mogą być zdefiniowane przez użytkownika.



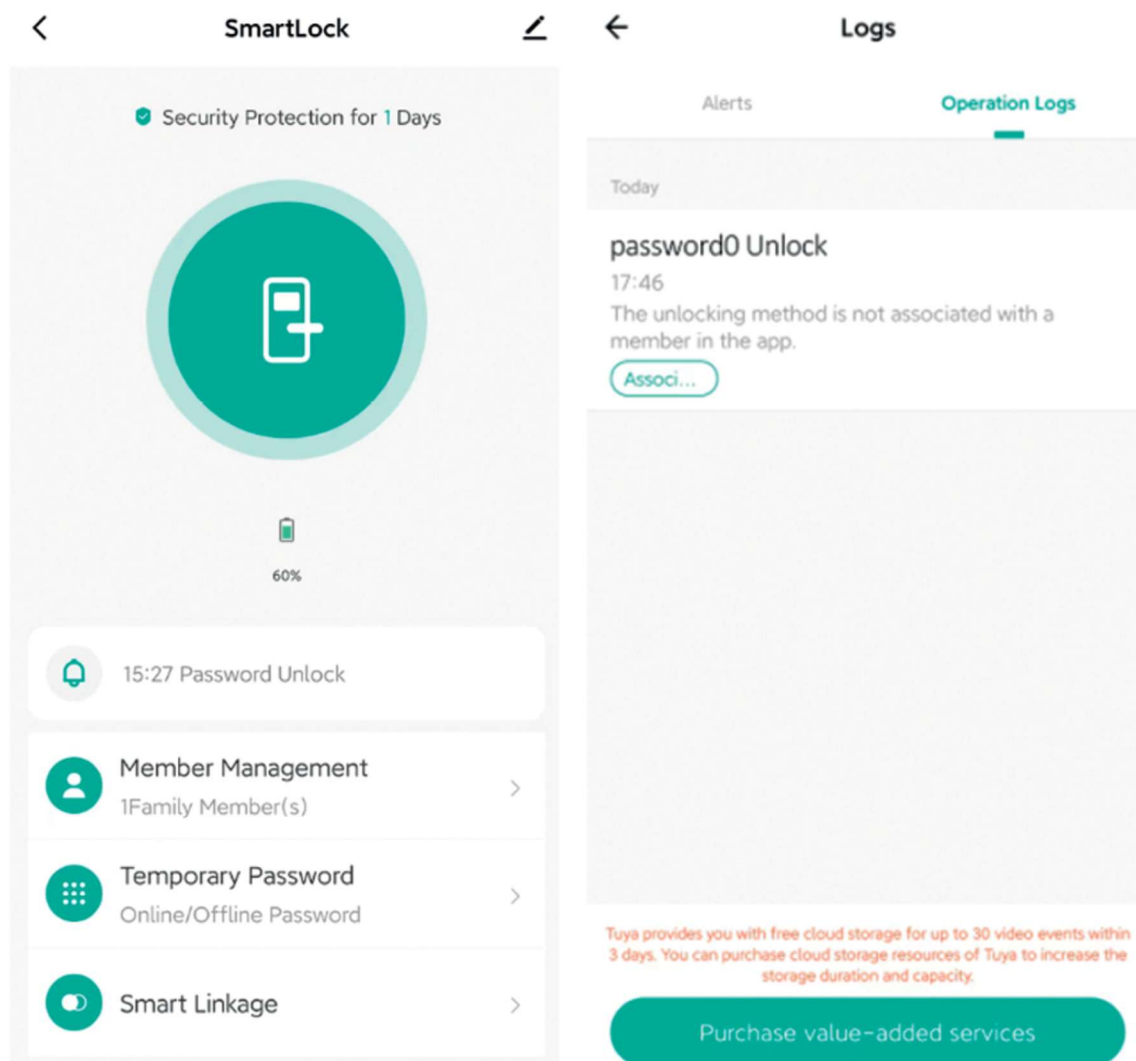
2. Zdalne odblokowanie

- Goście dzwonią dzwonkiem do drzwi, a telefon komórkowy użytkownika może odebrać prośbę o zdalne odblokowanie.
- Kliknij przycisk transmisji adaptacyjnej aby porozmawiać z gościem.
- Przesuń przycisk zwalniający w prawo, aby odblokować zdalnie.



3. Sprawdzanie rejestrów

Wiadomości takie jak naciśnięcie dzwonka do drzwi, niedozwolony użytkownik, niski poziom naładowania baterii i odblokowanie można sprawdzić w dzienniku.

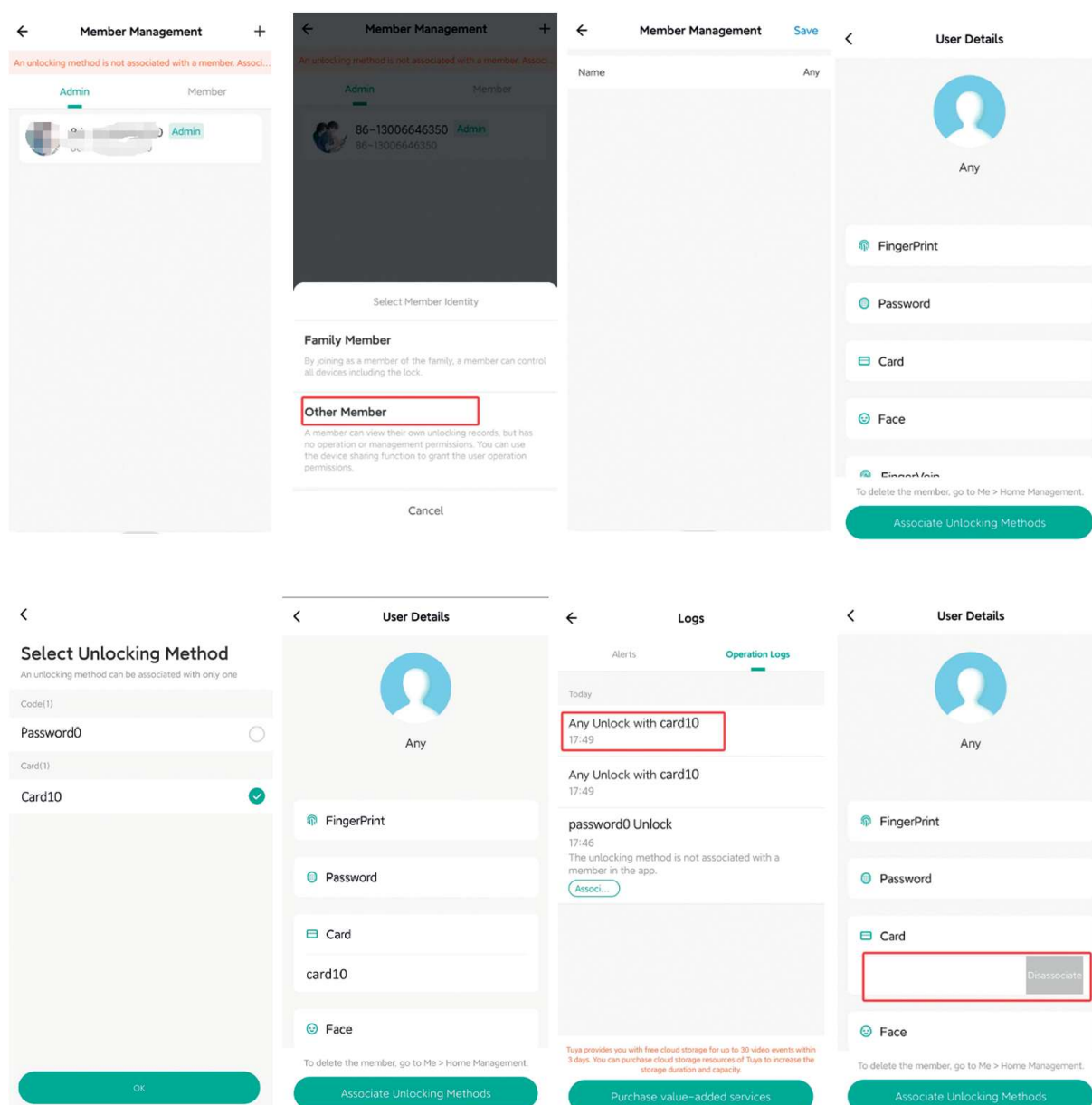


4. Zarządzanie członkami domu

Kliknij [Zarządzanie członkami], aby przejść do strony zarządzania członkami.

- Kliknij [+] w prawym górnym rogu, aby wybrać innych członków.
- Wprowadź imię i nazwisko członka, którego chcesz przypisać.
- Na stronie informacji o członku kliknij Zarządzaj trybem odblokowania.
- Wybierz numer użytkownika, który chcesz powiązać i kliknij OK.

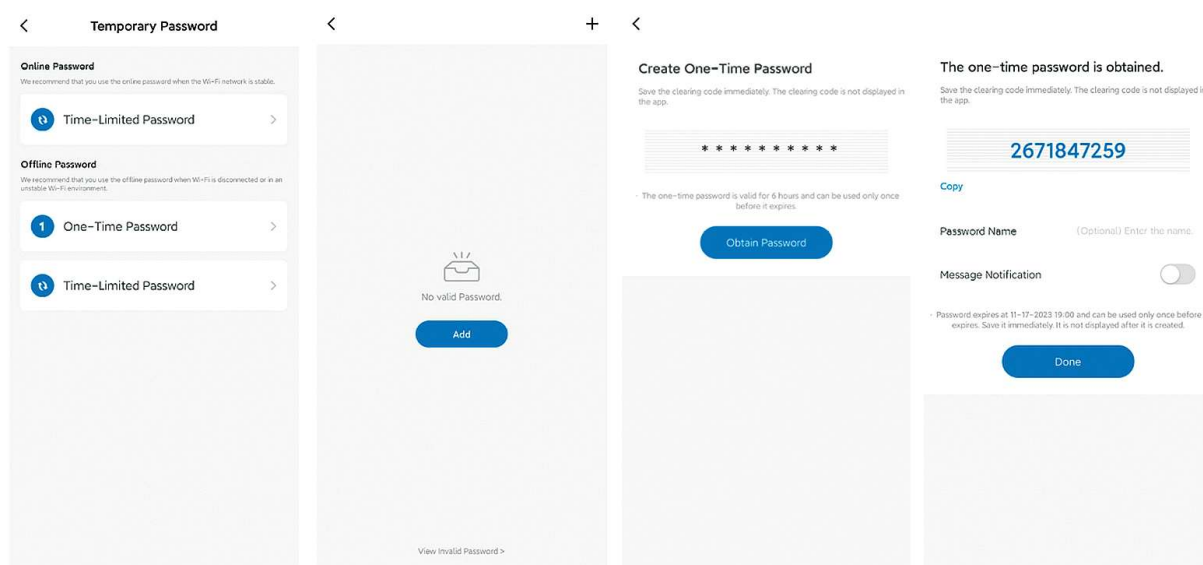
Uwaga: Numer konta – kod użytkownika generowany podczas dodawania zamka drzwi.



5. Hasło tymczasowe

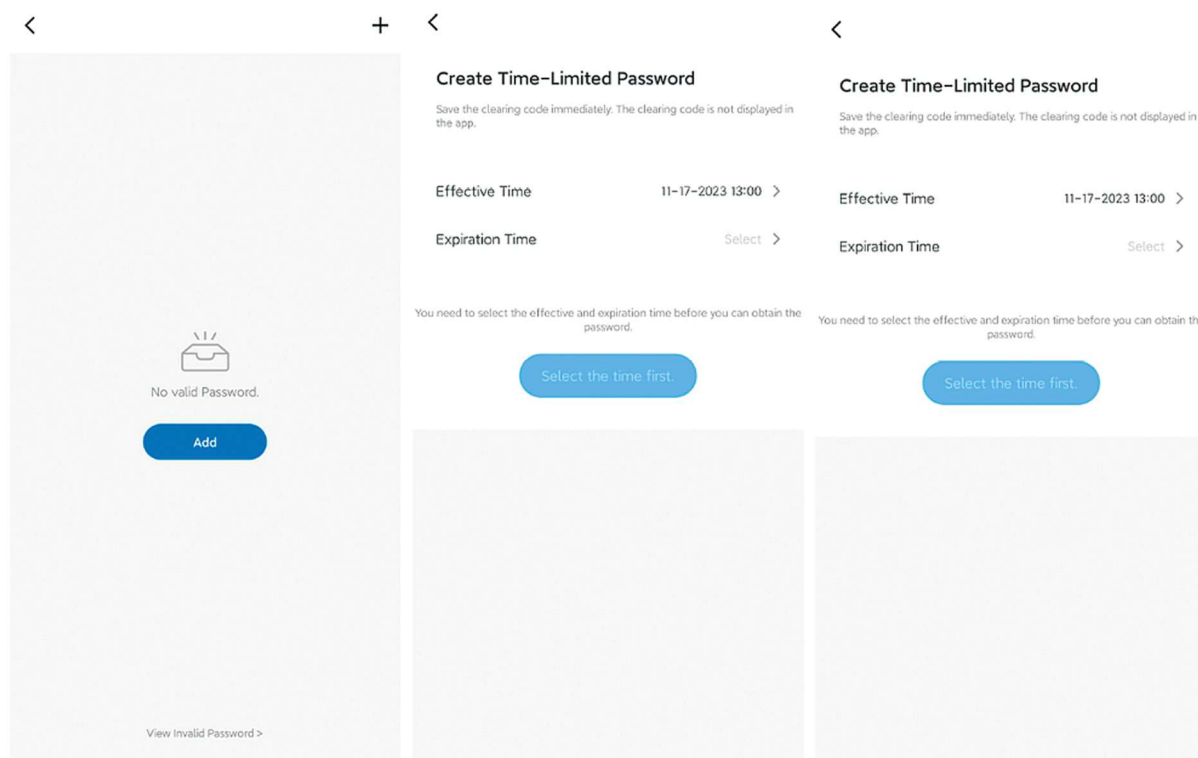
1) Hasło jednorazowe

Wybierz hasło jednorazowe i kliknij „Dodaj” lub znak „+” w prawym górnym rogu. Kliknij, aby uzyskać hasło. System automatycznie wygeneruje dziesięciocyfrowy zestaw haseł. Kliknij, aby zakończyć. Hasło musi zostać użyte w ciągu 6 godzin od wygenerowania. Hasło może zostać użyte tylko raz w okresie ważności.



2) Nieograniczone hasło

Wybierz nieograniczone hasło i kliknij „Dodaj” lub znak „+” w prawym górnym rogu; Wybierz czas obowiązywania i czas wdrożenia; Kliknij, aby uzyskać hasło. System automatycznie wygeneruje zestaw dziesięciocyfrowych haseł. Kliknij, aby zakończyć.



(1) Tryb gościa

W trybie gościa użytkownicy mogą generować hasła o ograniczonym czasie obowiązywania, trwające od 1 do 59 minut, licząc od aktualnego czasu. Hasła te tracą ważność po upływie tego czasu.

(2) Tryb wynajmu

W trybie najmu krótkoterminowego użytkownicy mogą generować hasła o dowolnym czasie obowiązywania. Czas obowiązywania hasła musi być dłuższy niż czas obowiązywania hasła i czas aktualny. Maksymalny okres obowiązywania hasła nie może przekraczać 60 dni. Wygenerowane hasło tymczasowe należy wprowadzić w ciągu 24 godzin od momentu jego wejścia w życie. W przeciwnym razie hasło traci ważność.

(3) Tryb niani

W trybie niani użytkownicy mogą ustawić dopuszczalne okresy czasu odblokowywania każdego dnia. Czas utraty ważności hasła musi przypadać później niż czas jego wejścia w życie. Wygenerowane hasło należy wprowadzić w ciągu 24 godzin, w przeciwnym razie będzie ono nieważne.

(4) Zarządzanie hasłami

Funkcja zarządzania hasłami umożliwia usunięcie haseł o ograniczonym czasie obowiązywania, które są już aktywne na zamku. Nie można jednak usunąć hasła czasowego, które obowiązuje przez 24 godziny, hasła administratora ani hasła użytkownika standardowego. Aby unieważnić wszystkie hasła czasowe, należy najpierw usunąć użytkownika 000 z blokady, a następnie dodać go ponownie.