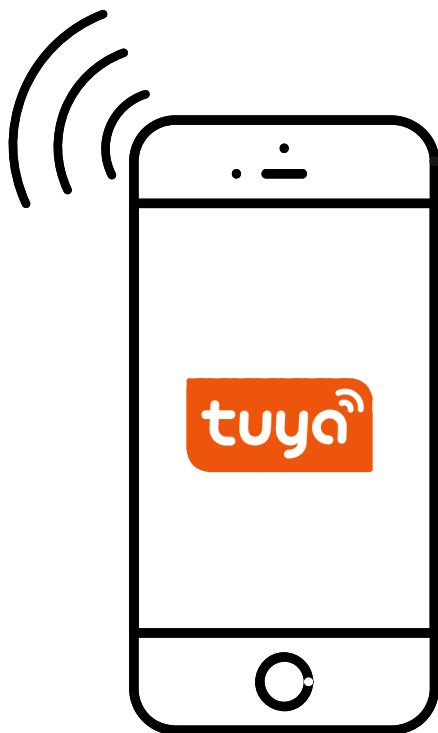


V I D O S

Podręcznik użytkownika aplikacji

Do obsługi zamków szyfrowych z funkcją Wi-Fi

ZS42-X ZS44-X ZS45-X



1. Pobierz aplikację

Pobierz aplikację TUYA właściwą dla systemu operacyjnego Twojego telefonu



IOS



ANDROID



Zarejestruj się lub zaloguj używając jednej z dostępnych metod.

2. Dodaj urządzenie

Aby dodać urządzenie do aplikacji, najpierw zaloguj się do trybu administratora (domyślny kod administratora **999999**) na zamku szyfrowym, a następnie wprowadź kod uruchamiający skanowanie dostępnych sieci Wi-Fi.

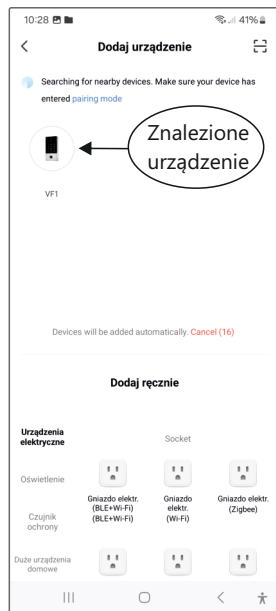
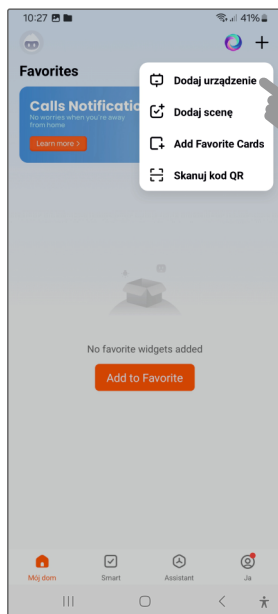
Kod uruchamiający skanowanie sieci Wi-Fi dla zamka szyfrowego **ZS44-X**

* Kod admin # 08

dla zamka szyfrowego **ZS42-X i ZS45-X**

* Kod admin # 73 #

Zielona dioda zacznie migać.



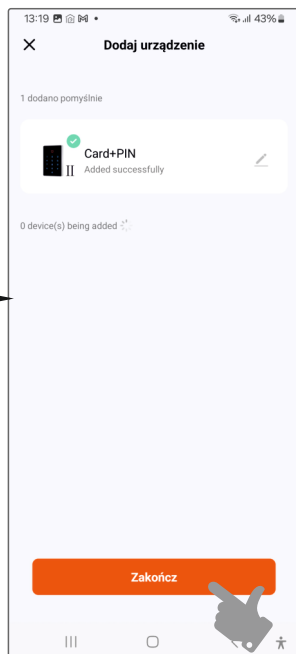
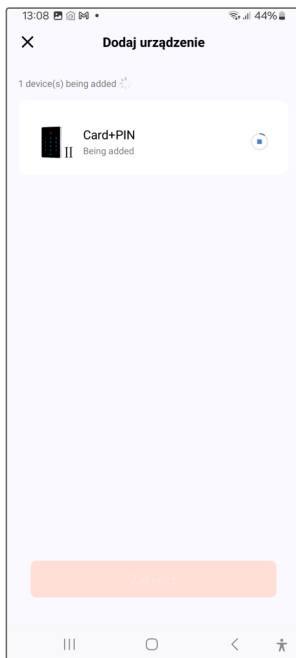
Upewnij się, że telefon i kontroler działają w tej samej sieci.
Na ekranie początkowym wybierz opcję **Dodaj urządzenie**.
Wyraż zgodę na wyszukiwanie urządzeń w sieci lokalnej, jeżeli aplikacja Cię o to poprosi.

Aplikacja zacznie skanować otoczenie w poszukiwaniu kompatybilnych urządzeń.
Po znalezieniu urządzenia, wybierz je.

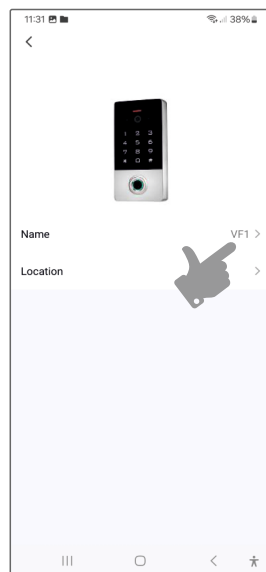
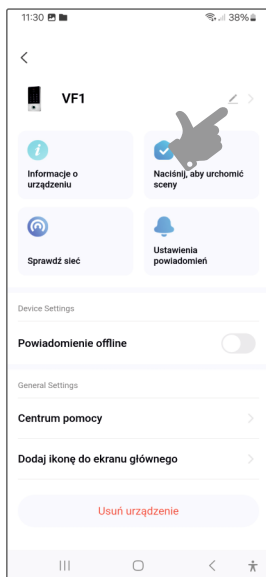
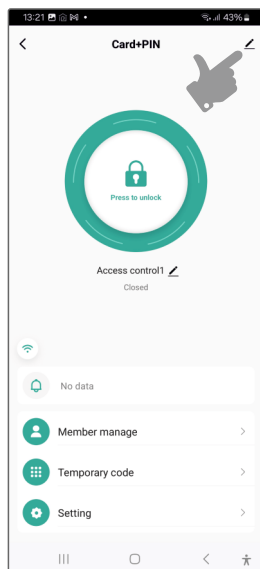
3. Połącz z siecią Wi-Fi



Wybierz sieć Wi-Fi (SSID) i wpisz hasło, aby połączyć zamek sztyfcowy z lokalną siecią bezprzewodową.



Nawiąż połączenie z odnalezionym urządzeniem.
Po zakończeniu procesu parowania system wyświetli komunikat potwierdzający prawidłowe dodanie urządzenia do aplikacji.



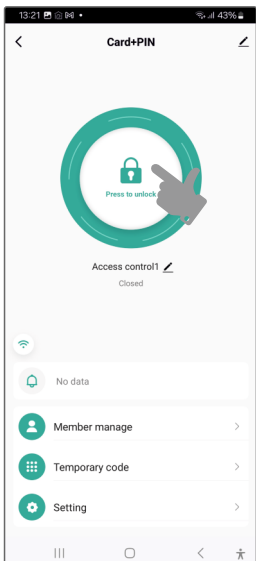
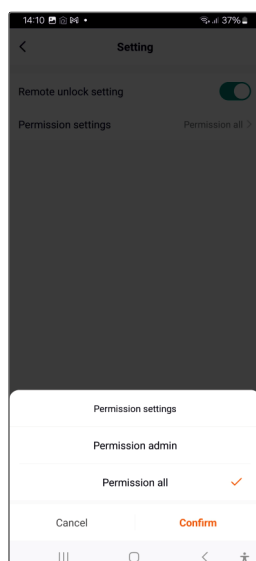
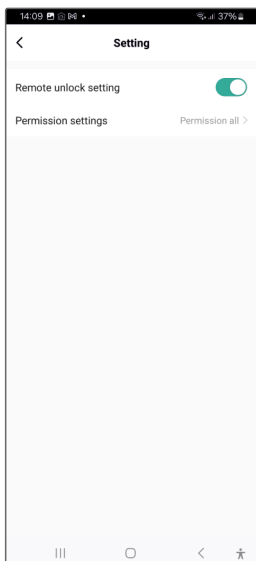
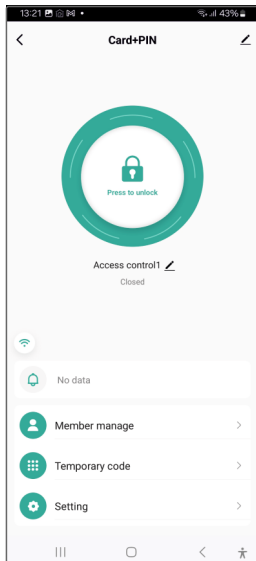
Możesz nadać własną nazwę dla kontrolera, aby łatwiej go identyfikować.

4. Włącz funkcję zdalnej obsługi

Na ekranie głównym otwórz menu ustawień, wybierając **Settings**, a następnie przesuwaj suwak **Remote unlock setting**, aby zmienił kolor na zielony. Funkcja zdalnej obsługi zostanie aktywowana.

W tym miejscu możesz również zapisać ustawienia uprawnień, wybierając opcję **Permission Setting**. Dostępne są dwie możliwości:

- **Permission Admin** - Tylko administrator (użytkownik, który dodał urządzenie lub posiada najwyższe uprawnienia) może wykonywać określone działania. Pozostali użytkownicy mają ograniczony dostęp lub nie mają go wcale.
- **Permission All** - Wszyscy użytkownicy mający dostęp do urządzenia w aplikacji Tuya mogą korzystać z tej funkcji. Nie są wymagane uprawnienia administratora.



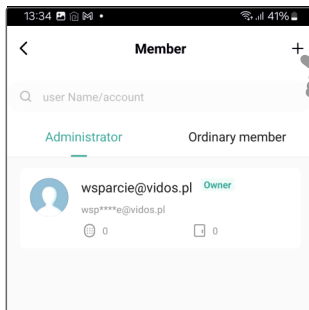
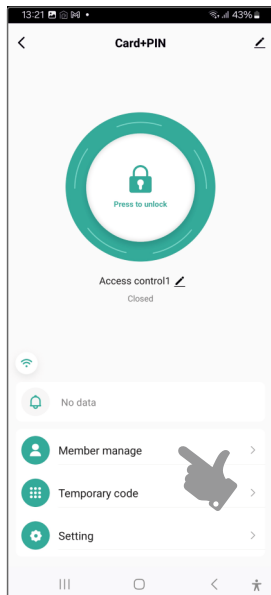
Urządzenie jest gotowe do pracy.

Otwieranie wejścia:

Aby otworzyć wejście, przytrzymaj zielone pole **Press to unlock**, aż zmieni kolor.

W tym miejscu możesz nadać nazwę **użytkownika**. Aby tego dokonać, naciśnij **Access control**.

5. Dodaj administratora i użytkownika



Na ekranie głównym wybierz z menu zakładkę **Member manage**.

Otworzy się panel zarządzania użytkownikami.

Wybierz **Administrator** lub **Ordinary member**, w zależności od tego, jakie uprawnienia ma posiadać.

Administrator może zarządzać urządzeniami i użytkownikami.

Użytkownik tylko otwiera wejście i przegląda zapis zdarzeń.

W prawym, górnym rogu ekranu wybierz **+**, otworzy się panel dodawania użytkowników.

W przypadku dodania kolejnego **Administradora**, jego uprawnienia są automatycznie ustawione na czas nieokreślony. Natomiast w przypadku **Użytkownika (Ordinary Member)** istnieje możliwość ustawienia czasu trwania uprawnień.

User name

przyjazna nazwa użytkownika

Country / Area

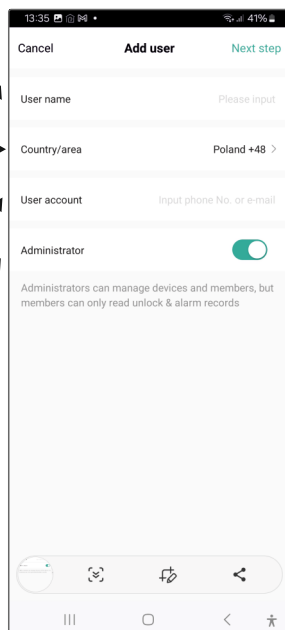
Kraj / numer kierunkowy

User account

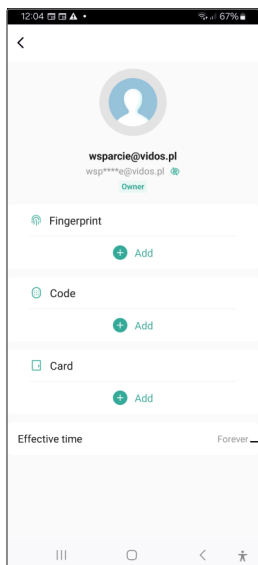
Użytkownik (email lub tel.*)

Zaznacz jeżeli użytkownik ma być administratorem

* Wprowadź adres email lub nr telefonu zarejestrowanego użytkownika aplikacji TUYA.



6. Sposób otwierania wejścia



Określ sposób otwierania wejścia dla administratora lub użytkownika (*Ordinary member*)

Do wyboru są trzy sposoby autoryzacji:

- **Odcisk palca (tylko ZS44-X)**
- **Kod PIN**
- **Karta zbliżeniowa**

Jedyną metodą otwarcia jaką możesz zaprogramować zdalnie i bez udziału użytkownika to kod PIN.

Każda pozostała metoda będzie wymagała obecności użytkownika przy terminalu w celu zbliżenia palca do czytnika linii papilarnych lub zbliżenia karty do czytnika, aby ją zaprogramować.

Określ czas trwania uprawnień

W przypadku dodania kolejnego **Administratora**, jego uprawnienia są automatycznie ustawione na czas nieokreślony. Natomiast w przypadku **Użytkownika (Ordinary Member)** istnieje możliwość ustawienia czasu trwania uprawnień.

Forever - uprawnienia na czas nieokreślony

Customize - określ czas trwania uprawnień

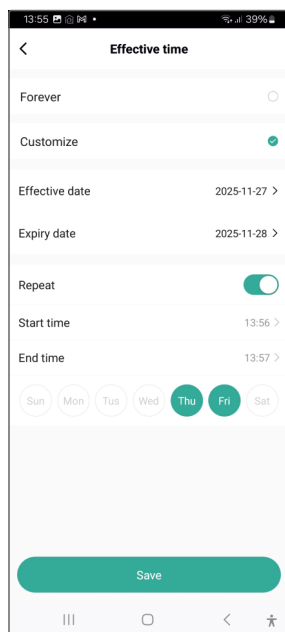
Na czas od _____ →

Na czas do _____ →

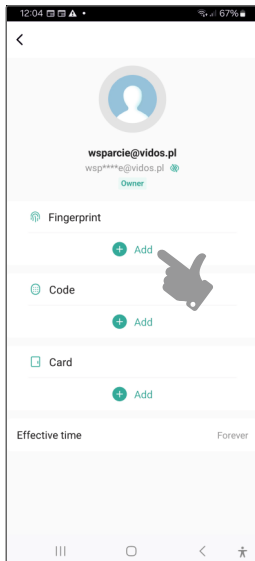
Powtórz _____ →

W tym miejscu możesz określić dni i godziny uprawnień

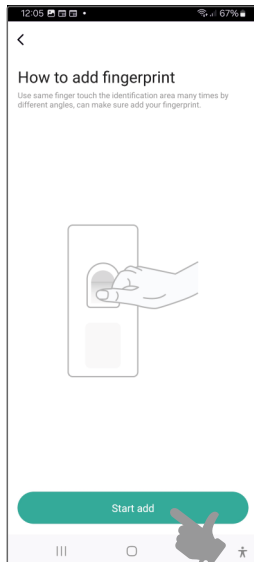
Zapisz ustawienia _____ →



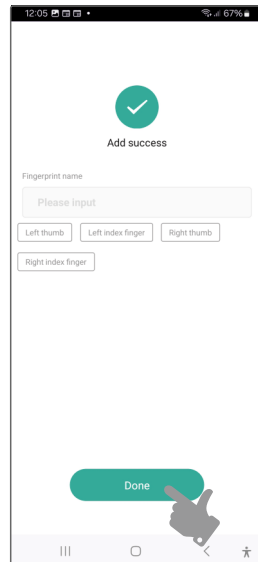
7. Dodaj odcisk palca (ZS-44X)



Naciśnij **Add** w zakładce **Fingerprint**

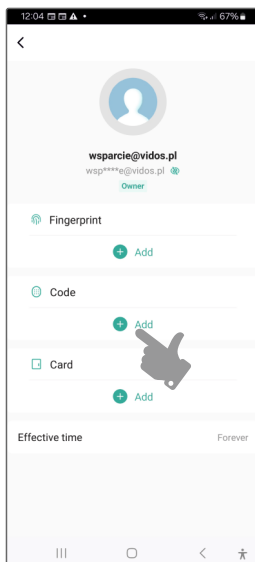


Naciśnij **Start add**, a następnie **dwukrotnie** przyłóż ten sam palec do czytnika linii papilarnych kontrolera

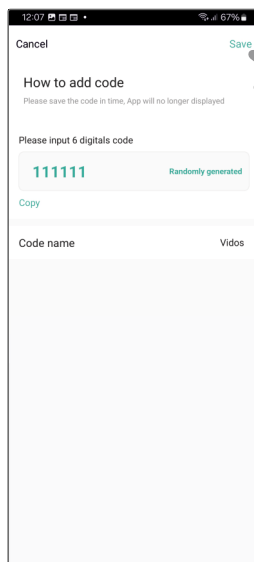


Wpisz nazwę użytkownika i kliknij **Done**

8. Dodaj kod PIN

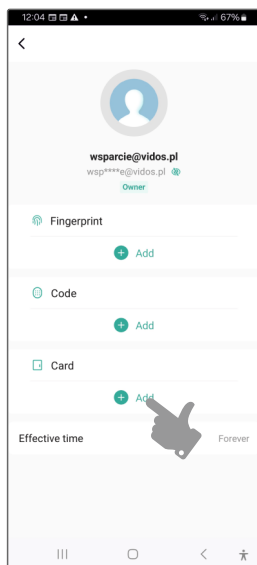


Naciśnij **Add** w zakładce **Code**

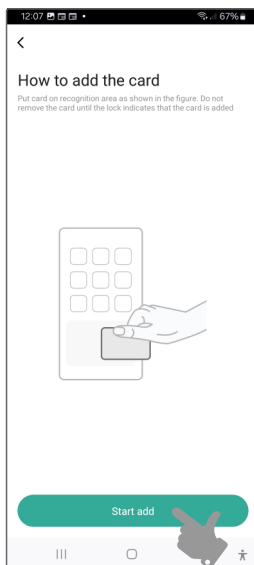


Wpisz 6 cyfrowy kod lub wygeneruj go naciskając **Randomly generated**, wpisz nazwę, a następnie zakończ naciskając **Save**

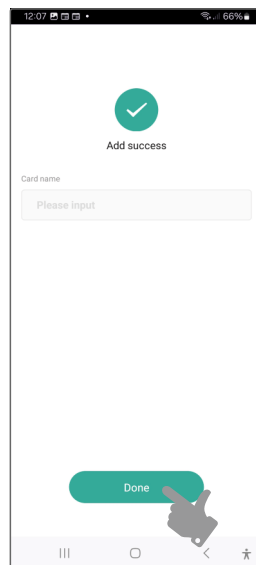
9. Dodaj kartę RFID



Naciśnij **Add**
w zakładce **Card**



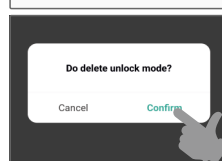
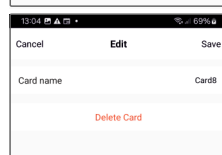
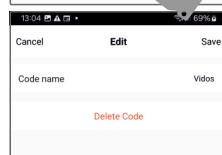
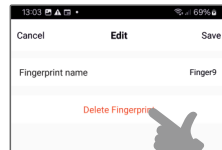
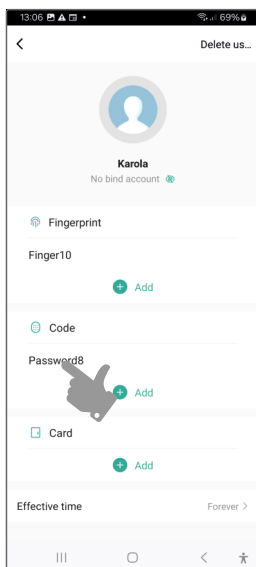
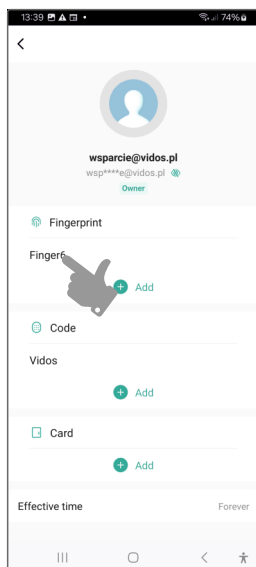
Naciśnij **Start add**, a następnie
przyłóż kartę do czytnika kontrolera



Wpisz nazwę użytkownika
i kliknij **Done**

10. Usuń odcisk palca / kod PIN / kartę

Usunięcie odcisku palca, kodu lub karty zarówno Administratora, jak i Użytkownika odbywa się w ten sam sposób.



Wybierz wcześniej zarejestrowany **odcisk palca, kod lub kartę**.

W kolejnym oknie wyświetli się komunikat **Delete Fingerprint / Code / Card** — naciśnij go.

Następnie pojawi się komunikat **Do delete unlock mode?**. Potwierdź, naciskając **Confirm**.

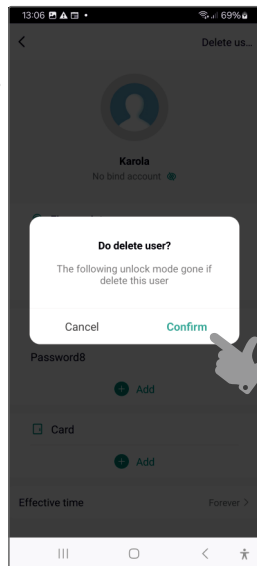
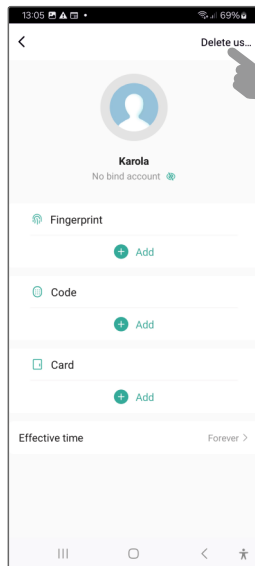
11. Usuń Użytkownika

Aby usunąć Użytkownika, otwórz zakładkę **Member Manage** → **Administrador** lub **Ordinary Member**.

Wybierz profil użytkownika, którego chcesz usunąć i kliknij **Delete User** w prawym górnym rogu ekranu.

Wyświetli się komunikat **Do delete user?**

Potwierdź operację, klikając **Confirm**.

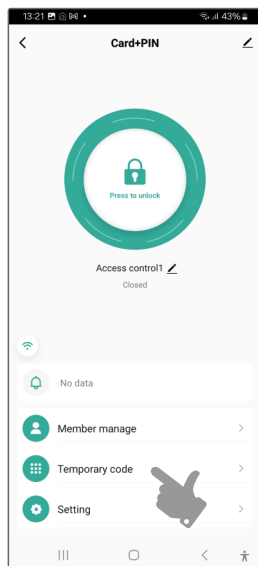


Uwaga:

Przed usunięciem konta użytkownika należy usunąć przypisane do niego kody dostępu - odcisk palca, kod PIN, karta (rozdział 10). W przeciwnym razie, pomimo usunięcia konta, przypisane kody dostępu nadal będą aktywne i umożliwią dostęp do systemu.

Dotyczy również kodów dostępu Administratora Owner. Przypisanie zamka szyfrowego do nowego konta, nie usuwa tych danych.

12. Nadaj tymczasowy lub jednorazowy kod dla gościa



Kod czasowy lub jednorazowy

Nadaj 6 cyfrowy kod wejścia lub wygeneruj automatycznie

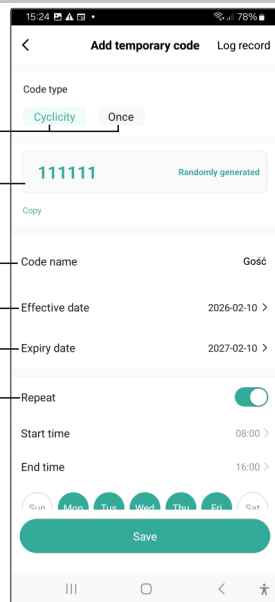
Nazwa (np. imię gościa)

Na czas od

Na czas do

Powtórz

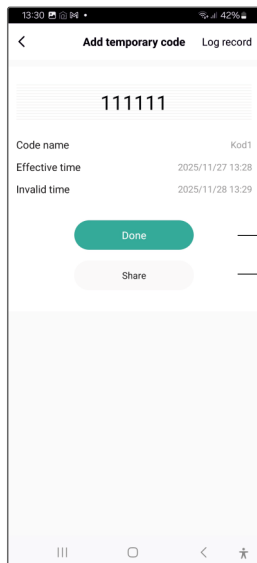
W tym miejscu możesz określić dni i godziny uprawnień



Aby nadać zdalnie uprawnienia do otwierania wejścia kodem, wybierz w menu głównym opcję **Temporary code**.

Wybierz opcję **Cyclicity** dla kodu tymczasowego, wprowadź kod, nadaj mu nazwę, ustaw czas rozpoczęcia oraz zakończenia jego obowiązywania, określ, czy kod ma być cykliczny, a następnie kliknij **Save**.

12. Nadaj tymczasowy lub jednorazowy kod dla gościa cd.

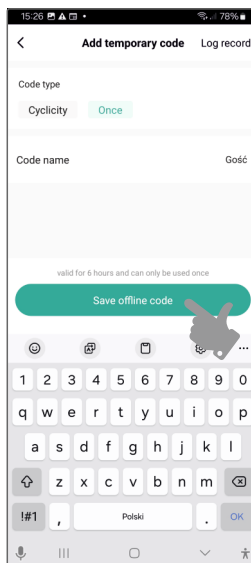


Nazwa kodu i
czas na jaki
został nadany

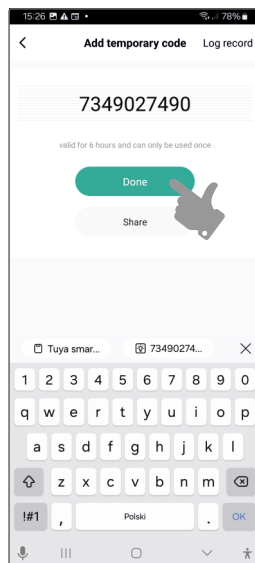
Zatwierdź

Udostępnij kod

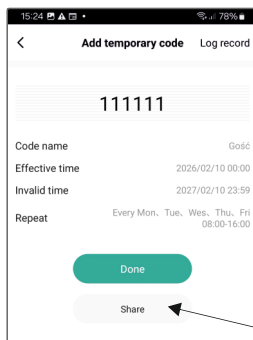
Uwaga: Po wprowadzeniu kodu w zakładce **Cyclicity**, nie ma możliwości usunięcia go. Wygaśnie automatycznie po upływie ustawionego czasu.



Wybierz opcję **Once** dla kodu jednorazowego użytku, nadaj mu nazwę, a następnie wybierz **Save offline code**. Na ekranie automatycznie wyświetli się wygenerowany jednorazowy kod dostępu. Kod jest ważny przez 6 godzin i wygasa po jednokrotnym użyciu.



13. Udostępnianie kodu



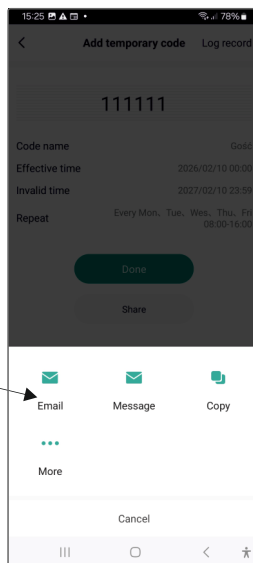
Aby udostępnić kod nadany dla czasowego użytkownika, wybierz **SHARE**, a następnie określ metodę udostępnienia.

Email - wyślij kod e-mailem

Message - wyślij kod SMSem

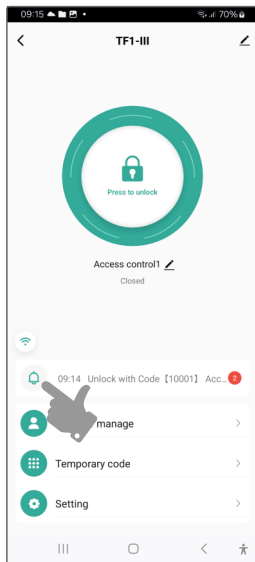
Copy - skopiuj kod

More - skorzystaj z dodatkowych opcji udostępniania

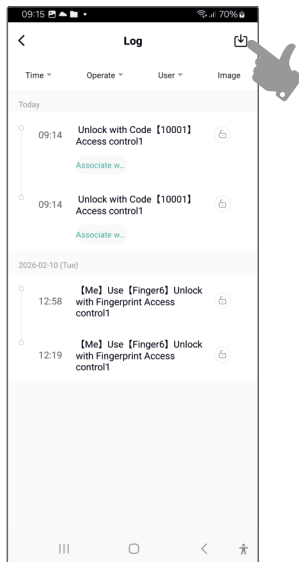


14. Historia zdarzeń

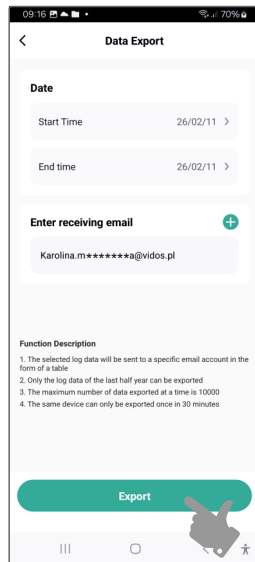
W tym miejscu możesz przejrzeć historię zarejestrowanych wejść (**Time**), wybrać, które zdarzenia mają się wyświetlać (**Operate**), oraz określić, wejścia którego użytkownika mają być widoczne (**User**). Masz również możliwość wyeksportowania listy zarejestrowanych zdarzeń w postaci pliku Excel i wysłania jej na podany adres e-mail. Aby to zrobić, wybierz ikonę .



Aby przejrzeć historię zarejestrowanych wejść, na głównej stronie aplikacji wybierz ikonę .



Wyświetli się lista wszystkich wejść zarejestrowanych za pomocą odcisku palca, kodu lub karty.



Aby wyeksportować listę zarejestrowanych wejść, wpisz adres e-mail i naciśnij przycisk **Export**.

15. Usuń urządzenie z listy urządzeń

