Arckey

OIKOS
ARCHITETTURE D'INGRESSO



Guida Utente Arckey
Versione 4.0

GET IT ON Google Play

Download on the App Store

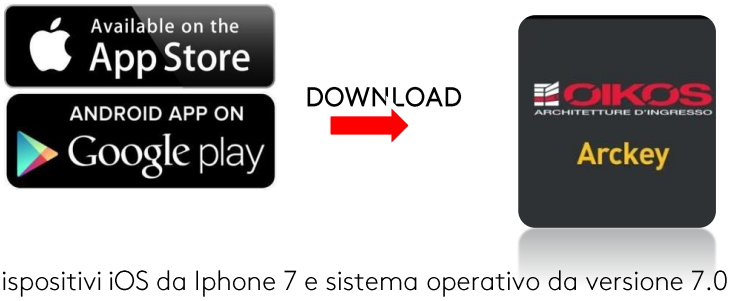
Cos'è Arckey? 2
Requisiti di funzionamento 2
Bluetooth 5.0 2
Primo Avvio di Arckey 5
Info 6
Modalità Programmazione 7
Admin Card 7
Entrare in Modalità Programmazione 8
Modalità Programmazione tramite Login (senza Admin Card) 9
Memorizzazione Utenti 10
Memorizzazione Smartphone 10
Apertura Porta con Smartphone 11
Memorizzazione Oikos Card, Chiave Transponder, Card con tecnologia RFID 12
Memorizzazione codice PIN 13
Memorizzazione Impronta digitale 14
Memorizzazione Utente tramite Telefono con UID ARCKEY 15
Inviti 16
Memorizzazione Inviti 16
Utilizzo Invito: 17
Lista Utenti 18
Cancellazione rapida di un utente: 18
Copiare Utenti 19
Backup 20
Creazione Backup Utenti 20
Ripristino Backup Utenti 21
Impostazioni Utente 22
Dettaglio Utente 22
PIN utente (solo per utenti di tipo Smartphone) 23
Blocco Utenti Standard 24
Modalità Ufficio 25
Restrizioni di apertura 26
Validità dal primo utilizzo: 26
Abilita controllo orario: 26
Info Porta 27
Modalità Ufficio Programmata 28
Funzioni Avanzate 29
Eventi 30
Periferiche Wireless 31
Aggiungi Periferiche Wireless 31
Rimuovere Periferica Wireless 32
Utility 33
Gateway 34
Panoramica di funzionamento 34
Accedere ad Arckey da Remoto 35
Installazione e configurazione iniziale Gateway 36
Aggiungere Serratura al Gateway 38
Utilizzo Arckey da Remoto 40
Menù Gateway 41
Aggiungere Account Utente Al Gateway 42
Rimuovere Account Utente Gateway 43

Cos'è Arckey?

Arckey è un sistema integrato di gestione degli accessi con apertura elettronica.
Attraverso l'App Arckey, disponibile per Smartphone e tablet Android e iOS, si può dialogare con serrature compatibili e configurare autorizzazioni e modalità di accesso fino ad un numero massimo di 300 utenze, suddivise tra Smartphone, Card Rfid (es. carta di credito, tessera della metropolitana ecc.), combinazioni di PIN, impronte digitali, inviti e controllo remoto.
Tramite l'app l'amministratore del sistema può, in modo facile ed intuitivo, non solo aggiungere, modificare o eliminare utenti al sistema ma anche configurare regole di accesso dividendo le utenze tra standard e "VIP", assegnare fasce orarie di accesso, durate temporali delle credenziali e molto altro ancora.
L'amministratore è inoltre messo in condizione di copiare utenti da una serratura ad un'altra e di supervisionare ogni attività del dispositivo di apertura mediante la consultazione dell'elenco degli ultimi 1000 eventi che si sono verificati.

Requisiti di funzionamento

L' App Arckey è gratuitamente scaricabile dall'App Store (iOS) o da Google Play (Android).



Arckey è compatibile con dispositivi iOS da Iphone 7 e sistema operativo da versione 7.0 in avanti
Android da versione 4.3 (Jelly Bean) in avanti.

L' App Arckey lavora in modo combinato con la serratura elettronica motorizzata, montata nella porta Oikos.
La serratura incorpora un motore elettrico controllato da un potente microprocessore di ultima generazione.
In caso di assenza di alimentazione (da batteria o da rete elettrica) l'azionamento del catenaccio è sempre garantito dal tradizionale movimento della chiave meccanica.

Prima di iniziare ad utilizzare Arckey è sempre necessario assicurarsi che il Bluetooth del dispositivo sia attivo.

Bluetooth 5.0

Dai primi mesi del 2022 è stato introdotto l'utilizzo delle serrature con tecnologia Bluetooth 5.0; questa nuova tecnologia consiste in un miglioramento delle prestazioni e la possibilità di utilizzare il Gateway per il controllo della serratura da remoto (vedi pag. "Dispositivo Gateway" Pag.20)

Per capire se siamo di fronte ad una serratura con Bluetooth 5.0 è sufficiente visualizzare l'icona della serratura nella schermata principale dell'App:


Icona serratura con versioni Bluetooth precedenti

Icona Serratura con Bluetooth 5.0

Credenziali d'accesso

L'accesso dall'esterno può essere eseguito tramite le seguenti modalità:

Apertura con Smartphone e Tablet tramite App:

Cliccando sul pulsante bianco della App nella schermata principale da uno Smartphone o un Tablet, la serratura eseguirà il comando di apertura (fig.1)

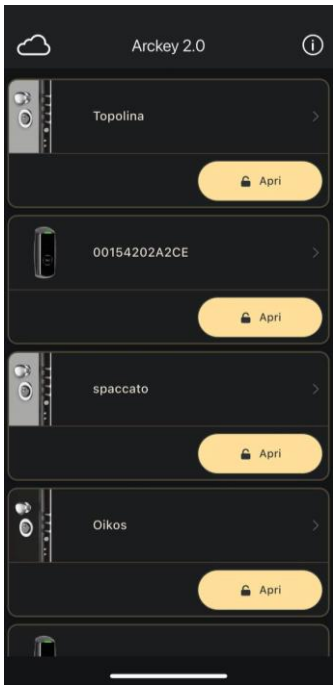


fig.1

Apertura con Card o Transponder:

Accostando al lettore esterno o alla Tastiera Touch, una chiave Trasponder (fig.2), una Oikos Card (fig.3) o una Card con tecnologia RFID (fig.4) (es. carta di credito, tessera della metropolitana ecc.) la serratura eseguirà il comando di apertura.

Le card RFID devono essere Mifare compatibili 13,56 Mhz e generalmente necessitano una lettura più ravvicinata (fig.2)


fig.2


fig.3


fig.4

Apertura con Codice PIN (solo in presenza di tastierino numerico o tastiera touch):

Digitando il codice numerico (minimo 4, massimo 8 caratteri) seguito dal tasto INVIO ↵ la serratura eseguirà il comando di apertura (fig.6-7).



fig.6


fig.7

Apertura tramite lettura di impronta digitale:
Se nella porta è installato il lettore d'impronta, appoggiando il dito di cui è stata memorizzata l'impronta si dà alla serratura il comando di apertura (fig.8)


fig.8

Apertura tramite dispositivo Wireless:
Se nella porta è presente almeno un lettore Rfid, un tastierino numerico oppure la tastiera touch è possibile installare, anche successivamente un dispositivo Wireless per l'apertura della porta.


Lettore Rfid Wireless



Tastiera Touch Wireless



Tastiera Touch + lettore d'impronta Wireless

Apertura da remoto tramite dispositivo Gateway:
Se nella porta è installato il dispositivo Gateway (fig.9) (vedi pag. 20), Attraverso l'App sarà possibile aprire la porta o controllare lo stato della porta da qualsiasi parte del mondo senza essere necessariamente in prossimità della stessa.



fig.9

Attenzione: il Dispositivo Gateway può essere installato solamente in una serratura che possiede la tecnologia Blutetooth 5.0 (vedi capitolo "Bluetooth 5.0" pag.2)

Primo Avvio di Arckey

Prima di iniziare ad usare l'App ricordarsi di attivare il Bluetooth nel dispositivo che si sta utilizzando.

Quando si avvia l'App verranno visualizzate tutte le serrature disponibili nel raggio d'azione del segnale Bluetooth (fig.10). Al primo accesso il numero della porta sarà il numero di ordine interno utilizzato. Si consiglia di rinominarla (vedi pag. "Info Porta")



fig.10

Info

Cliccando sull'icona Informazioni ⓘ in alto a destra si ottengono i dati sulla versione dell'App e sul software.

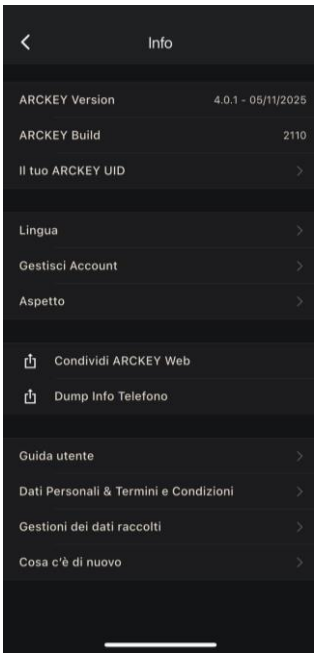


fig.11

ARCKEY Version: indica la versione dell'App installata.

ARCKEY Build: indica la build installata dell'App;

il tuo ARCKEY UID: è un codice alfanumerico univoco del dispositivo su cui è installata l'App che lo identifica unicamente; può servire per registrare il dispositivo come utente di apertura (Vedi "Memorizzazione Utente tramite Arckey UID" pag.);

Lingua: modifica la lingua dell'interfaccia dell'App;

Gestisci Account: permette di gestire il proprio Account del Cloud Iseo. E' obbligatorio per la configurazione del Gateway (pag.);

Aspetto: questa funzione permette di modificare l'aspetto dell'App "Modalità Chiara", "Modalità Scura" oppure "Modalità di Sistema";

Condividi ARCKEY Web: permette di condividere un link per l'accesso da altri dispositivi ad Arckey da Remoto;

Dump info Telefono: crea un file .csv con le informazioni tecniche del dispositivo;

Guida Utente: da qui si accede al portale con le istruzioni complete del sistema Arckey;

Dati Personali & Termini e Condizioni: da qui si accede al portale con la documentazione relativa alla Privacy;

Cosa c'è di Nuovo: vengono descritti brevemente le migliorie e cambiamenti dell'App.

Modalità Programmazione

Admin Card

Le **Admin Card** consentono all'amministratore di entrare in Modalità Programmazione per configurare e gestire il sistema di controllo accessi Oikos Arckey.

ATTENZIONE: Il set di 3 Admin Card viene sigillato in fabbrica al termine dei controlli qualità interni.
Le Admin Card in dotazione vi permettono di divenire l'unico amministratore del sistema ed eseguire le operazioni descritte nel presente manuale. Custoditele con cura ed evitate di smarrirle!

Il sistema (OIKOS Security Code System) prevede tre livelli di sicurezza per l'accesso ai parametri di funzionamento della serratura. Ad ogni livello di sicurezza corrisponde una Admin Card di colore diverso:

Admin Card Verde - **Livello 1**
Admin Card Grigia - **Livello 2**
Admin Card Rossa - **Livello 3**



Al momento del primo utilizzo sarà possibile accedere alla Modalità Programmazione del sistema Arckey accostando al lettore esterno l'Admin Card Verde.
In qualsiasi momento si perda il controllo (per esempio per furto o smarrimento) della Admin Card verde, si può passare al livello di sicurezza grigio, semplicemente accostando al lettore della porta la Admin Card di livello successivo Grigia. Un segnale acustico conferma l'avvenuta lettura e si **annullerà** il funzionamento della Admin Card verde. Attendere il secondo segnale acustico di conferma dopo 10 secondi.

In qualsiasi momento si perda il controllo della Admin Card Grigio, semplicemente accostando alla porta l'Admin Card Rosso (un segnale acustico conferma l'avvenuta lettura) si annullerà il funzionamento dell'Admin Card Grigia. Attendere il secondo segnale acustico di conferma dopo 10 secondi.

Attenzione: l'eventuale smarrimento della Admin Card di colore Rosso preclude qualsiasi possibilità di poter entrare in programmazione per gestire le funzionalità del sistema Arckey.
Si consiglia quindi, arrivati a questo punto di richiedere immediatamente un nuovo kit di Admin Card (Verde-Grigio-Rosso).

Accostando l'Admin Card Verde del nuovo kit alla porta (un segnale acustico conferma l'avvenuta lettura) si annullerà il funzionamento del vecchio kit ripristinando così la funzionalità originale.
Attendere il secondo segnale acustico di conferma dopo 10 secondi.

Durante il passaggio da una Admin Card a quella successiva tutte le impostazioni del sistema e degli utenti non subiscono alcuna modifica.

Entrare in Modalità Programmazione

- Attivare il Bluetooth nel proprio dispositivo.
- Aprire L'App Arckey.
- Accostare la tessera l'Admin Card al lettore esterno della porta (o alla tastiera touch o al lettore nascosto).
- Il lettore emetterà un segnale luminoso e sonoro di conferma; contemporaneamente nell'App, il banner che identifica la porta apparirà la scritta Login (fig.12)
- Cliccare sulla serratura.



fig.12

Attenzione: durante la Modalità Programmazione e in tutte le sue funzioni interne non è possibile chiudere o mettere in standby l'App e si perderà la connessione con la serratura.

Modalità Programmazione tramite Login (senza Admin Card)

Dopo la prima volta, è' possibile entrare nella modalità programmazione senza l'utilizzo delle tessere ma utilizzando la modalità "Login" del dispositivo (vedi pag.9)

Basterà tenere premuto il banner della serratura fino a che il bordo della stessa diventa completamente evidenziato (fig.13) oppure premendo nell'icona della serratura una volta e accedendo al sottomenù di apertura (fig.14).

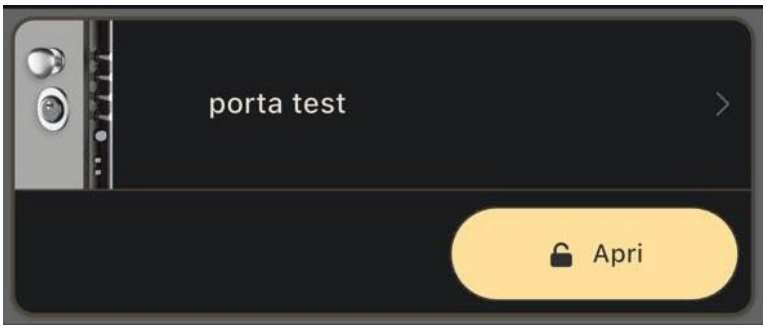


fig.13

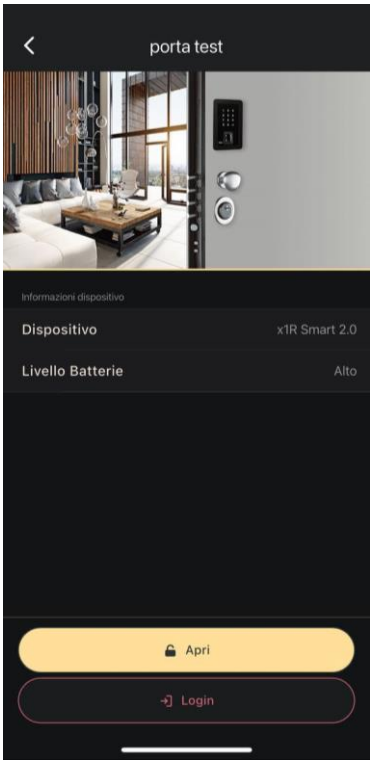


fig.14

Premere la scritta "Login" per accedere alla Modalità Programmazione della serratura.

Attenzione: è comunque fortemente consigliato conservare le Admin Card per poter accedere in caso di necessità o di sostituzione/smarrimento del dispositivo.

Memorizzazione Utenti

Memorizzazione Smartphone

Dopo il primo accesso verrà richiesto di aggiungere il dispositivo come Credenziale per aprire la serratura (fig.15). Questa operazione deve essere eseguita per ogni Smartphone che si desidera memorizzare sulla serratura.

Modificare, se desiderato, il nome identificativo dello Smartphone e cliccare su "**Fatto**" in alto a destra. Ora il dispositivo compare nella scheda degli utenti registrati e abilitati ad aprire la porta (fig.16).

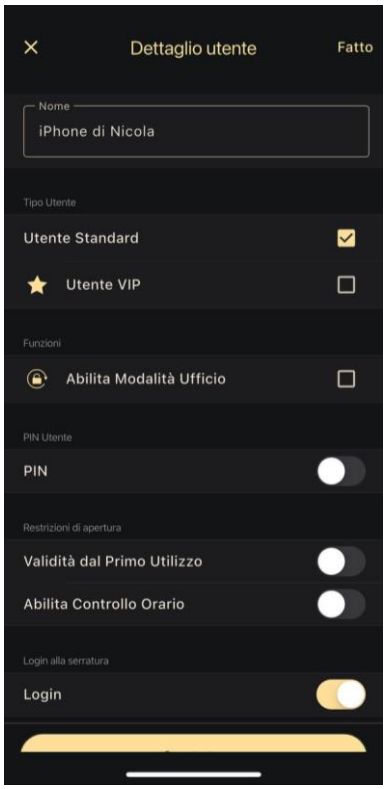


fig.15

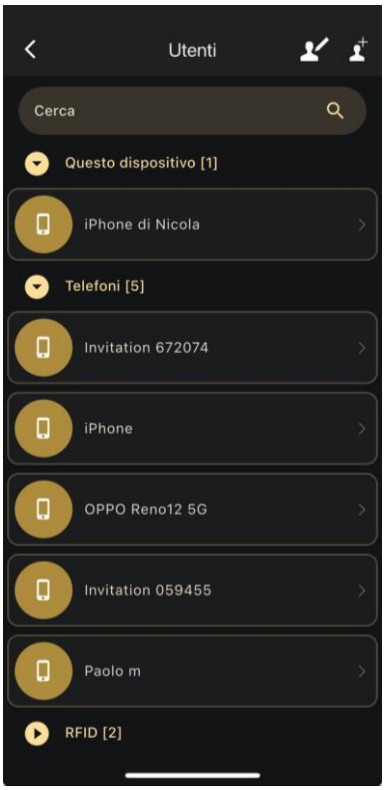
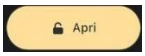
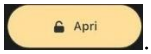


fig.16

La scheda Utenti visualizza la lista di tutti gli utenti associati alla porta, divisi per sistema di accesso: Smartphone e Tablet, Carte (Oikos card, carte con tecnologia RFID, chiave transponder), PIN, Impronte digitali e Inviti.

Apertura Porta con Smartphone

All'interno dell'App, premere sul pulsante 

della serratura da aprire (fig.17) oppure premere nel banner della porta interessata per accedere al sottomenù di apertura e successivamente premere 

. La serratura farà rientrare i catenacci.

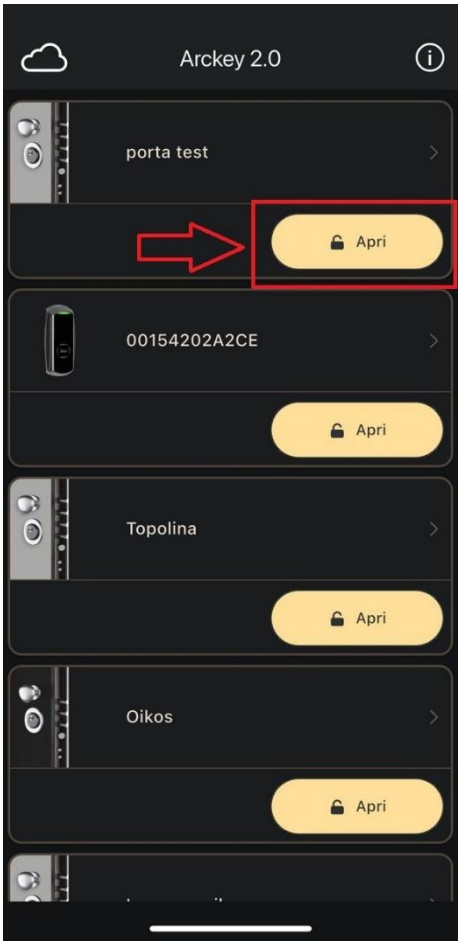


fig.17

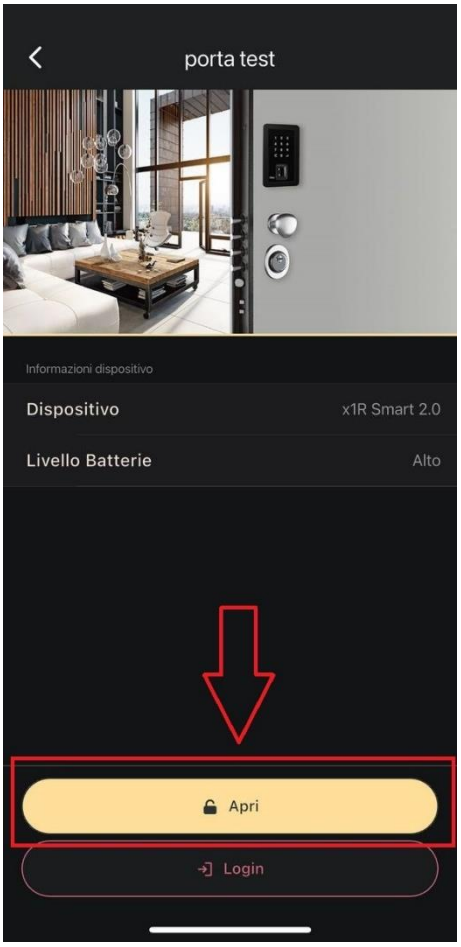


fig.18

Memorizzazione Oikos Card, Chiave Transponder, Card con tecnologia RFID

- Entrare in programmazione (vedi pag. 8);
- avvicinare la chiave o la card al lettore esterno della porta. Attendere il segnale di conferma. La card comparirà ora nell'elenco utenti a conferma dell'avvenuta memorizzazione.

Aggiunta manuale di Card Utente Rfid

E' possibile aggiungere delle card anche senza averle fisicamente in mano, memorizzandole attraverso il loro codice (fig.19).



fig.19

Questa funzione risulta utile nel caso per esempio che le card siano state già distribuite agli utenti.

Procedimento:

- Entrare in programmazione (vedi pag. 7);
- Premere la voce Utenti (fig.20);
- Premere nell'icona in alto a destra (fig.21);
- Selezionare la tipologia di utente RFID (fig.22);
- Selezionare il tipo di tessera da inserire (fig.23);
- Inserire un nome ed il numero identificativo riportato sulla card. Cliccare su Fatto in alto a destra (fig.24).

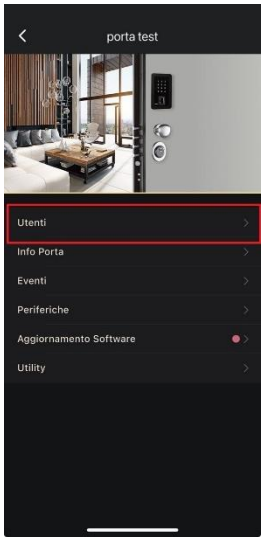


fig.20

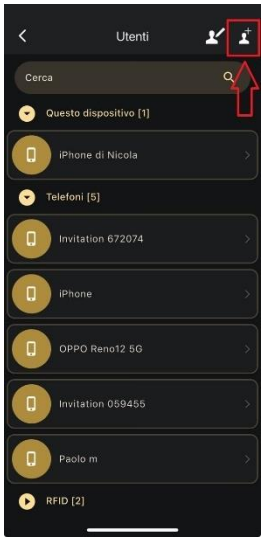


fig.21



fig.22

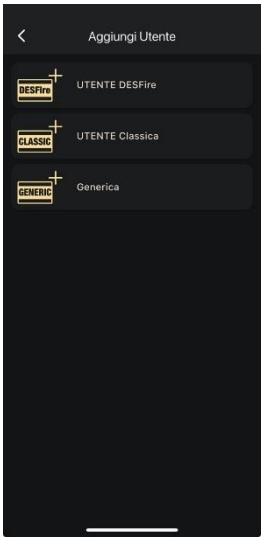


fig.23



fig.24

Memorizzazione codice PIN

Attenzione: Per ragioni di sicurezza i codici PIN non sono mai visibili in chiaro nell'App

Procedimento:

- Entrare in programmazione (vedi pag. 8);
- Premere la voce "Utenti" (fig.25);
- Premere nell'icona in alto a destra (fig.26);
- Selezionare la tipologia di utente "PIN" (fig.27);
- Assegnare un nome al codice e digitare il pin sui campi PIN e PIN verifica. Il codice deve essere di almeno 4 cifre. Premere su Fatto (fig.28);

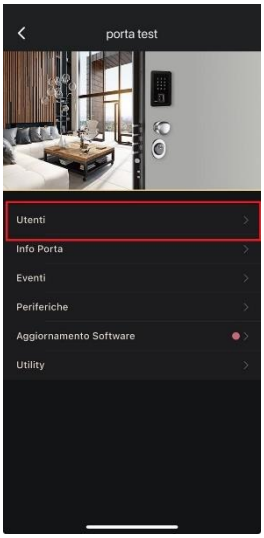


fig.25

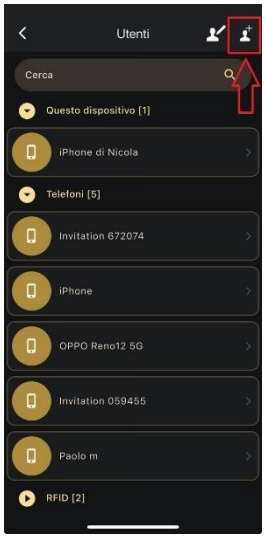


fig.26



fig.27

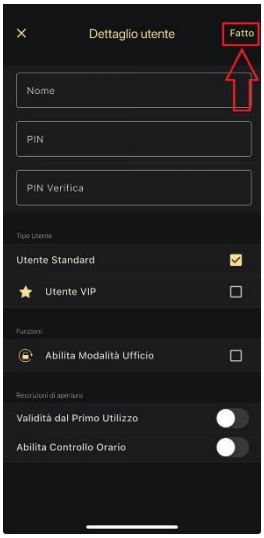


fig.28

Memorizzazione Impronta digitale

- Entrare in Modalità Programmazione (vedi pag.8);
- Premere la voce "Utenti"(fig.29);
- Premere nell'icona in alto a destra (fig.30);
- Selezionare la tipologia di utente "Impronte Digitali" (fig.31);
- Selezionare il dispositivo da utilizzare per la registrazione dell'impronta (potrebbe essere una Periferica Wireless vedi pag.);

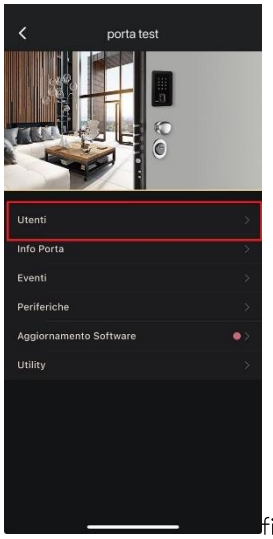


fig.29

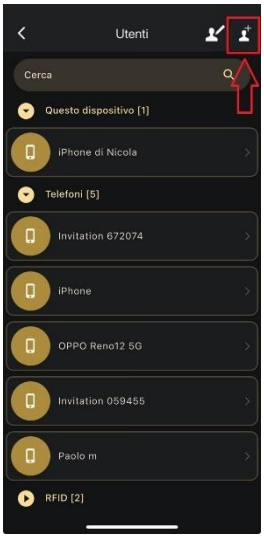


fig.30



fig.31

- Il lettore d'impronta selezionato, inizierà a lampeggiare; posizionare il dito sul lettore come indicato dall'animazione e rimuoverlo quando richiesto (fig.32). L'App chiederà di leggere l'impronta diverse volte al fine di ottenere una registrazione di buona qualità;

  Attenzione: Per una corretta lettura, il dito deve essere appoggiato e non "strisciato" sul lettore. La lettura dell'impronta può risultare più difficoltosa da fattori quali eccessiva umidità del dito o della superficie del lettore, superficie del lettore non sufficientemente pulita, scarsa leggibilità del polpastrello ecc...

  Ad ogni passaggio, il lettore attribuirà un punteggio all'impronta che serve a stabilirne la bontà per la registrazione. Se il punteggio non è abbastanza alto potrebbe rifiutare la registrazione e l'operazione va ripetuta (fig.33).
- Premere "OK" (fig.34);
- Compilare il "Dettaglio Utente";
- Una volta completato il tutto premere "Fatto" in alto a destra (fig.35).



fig.32

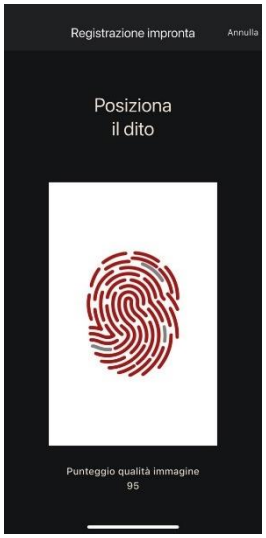


fig.33

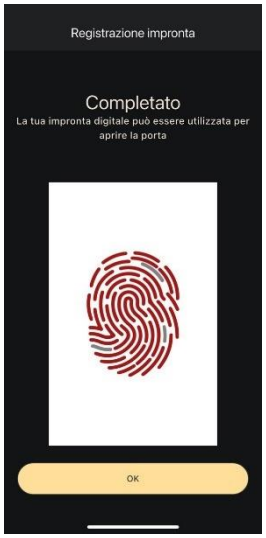


fig.34

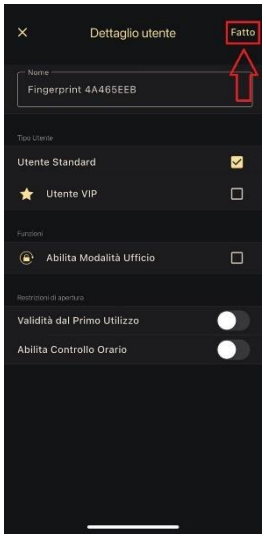


fig.35

Memorizzazione Utente tramite Telefono con UID ARCKEY

E' possibile memorizzare un dispositivo qualsiasi con l'App Arckey installata semplicemente inserendo l'UID ARCKEY.

L'UID ARCKEY è un codice alfanumerico che identifica unicamente il dispositivo (vedi "Info" pag.27)

Questo codice varia da dispositivo a dispositivo quindi in caso di smarrimento o cambio smartphone l'operazione dovrà essere ripetuta;

Procedimento:

- Entrare in Modalità Programmazione (vedi pag. 8);
- Premere la voce "Utenti" (fig.36);
- Premere nell'icona in alto a destra (fig.37);
- Selezionare la tipologia di utente "Telefono con UID ARCKEY" (fig.38);
- Digitare il codice alfanumerico del dispositivo da associare;
- Premere "Fatto" in alto a destra per confermare (fig.39);

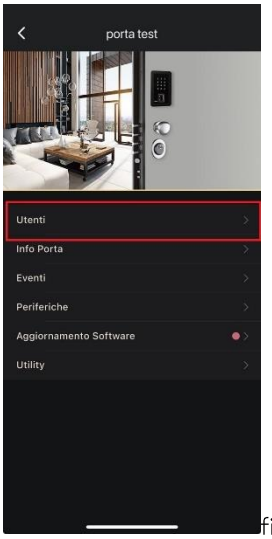


fig.36

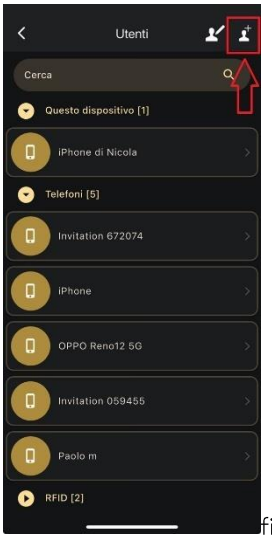


fig.37



fig.38

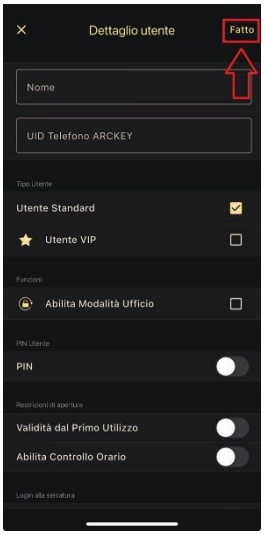


fig.39

Inviti

Memorizzazione Inviti

Gli inviti permettono ad un Amministratore di creare delle credenziali con cui permettere l'accesso successivamente ad altri Utenti;

Per farlo l'Amministratore deve precedentemente aver aggiunto nella memoria della serratura un Codice Invito, che può anche direttamente essere inviato alla persona a cui deve consentire l'accesso.

Creazione Invito:

- Entrare in Modalità Programmazione (vedi pag.8);
- Premere la voce "Utenti" (fig.40);
- Cliccare sull'icona "Aggiungi utente" e poi su Inviti (fig.41);
- Si apre la schermata di configurazione dell'Utente; modificare il nome utente e **memorizzare il codice di accesso da utilizzare per abilitare l'utente (di default sarà il nome dell'Invito)**;
- Viene chiesto se si desidera inviare un messaggio di invito (fig.43) Premere Si per inviarlo subito, oppure No se si vuole inviarlo in un secondo momento.

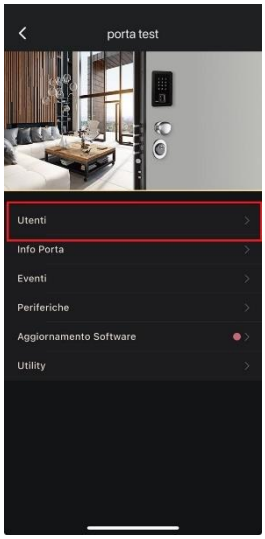


fig.40



fig.41

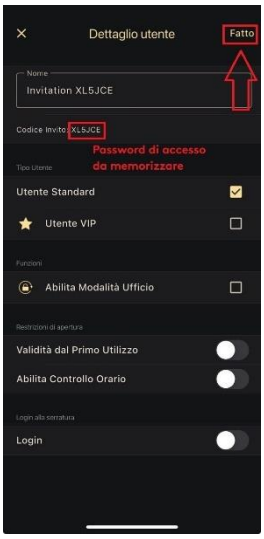


fig.42

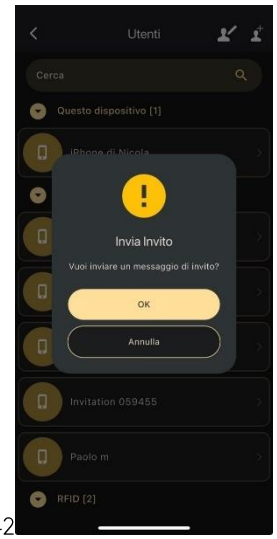


fig.43

Il messaggio inviato non è nient'altro che un testo generato automaticamente con la spiegazione, passo dopo passo, di come usare l'invito per accedere alla porta. Vengono inoltre, riportate le informazioni di validità dell'accesso se presenti.
Le istruzioni possono essere inviate via e-mail, o attraverso un programma di messaggistica (WhatsApp, Telegram, e-mail ecc...). L'invito compare ora nella lista degli inviti. Da qui è possibile inviare nuovamente l'invito se necessario.

Utilizzo Invito:

L'Utente che riceve l'invito deve prima di tutto scaricare e installare l'App Arckey sul suo dispositivo.
Con il Bluetooth attivo e l'App Oikos Arckey avviata, l'utente si deve avvicinare alla porta affinché la serratura possa essere rilevata:

- Selezionare nel banner della serratura da aprire e accedere al sottomenù di apertura (fig.44);
- Selezionare "inserisci codice d'invito"
- Inserire la password comunicata per l'abilitazione dell'Utente;
- La serratura arretrerà i catenacci e si aprirà;

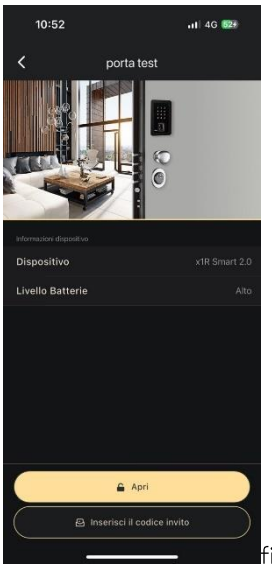


fig.44

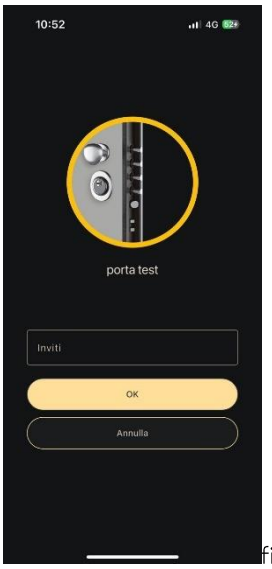


fig.45

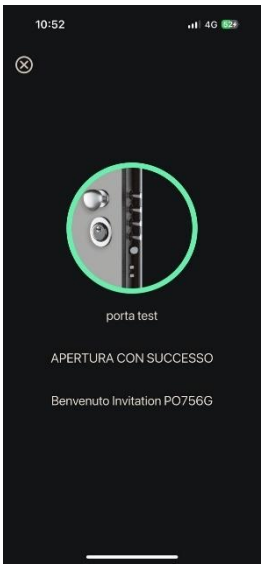


fig.46

- Da questo momento l'utente invitato sarà memorizzato all'interno della lista utenti ed avrà le caratteristiche impostate precedentemente dall'Amministratore che ha generato l'Invito.

Lista Utenti

Cancellazione utenti

- Entrare in Modalità Programmazione (vedi pag.8);
- Selezionare la voce "Utenti" (fig.47);
- Cliccare sull'icona in alto a destra (fig.48);
- Selezionare l'utente da cancellare (fig.49)
- Premere sull'icona cestino per confermare l'eliminazione;
- Volendo è possibile eliminare tutti gli utenti rapidamente premere l'icona per selezionare tutti gli Utenti. E' possibile eliminare anche solamente gli Utenti senza funzione "Login";

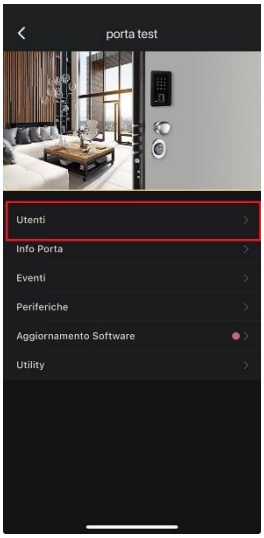


fig.47

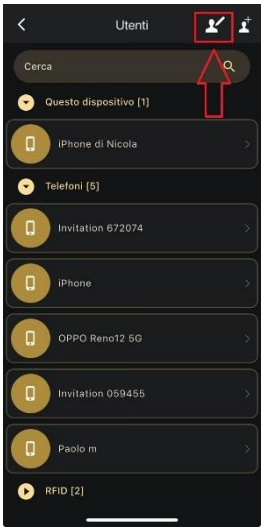


fig. 48

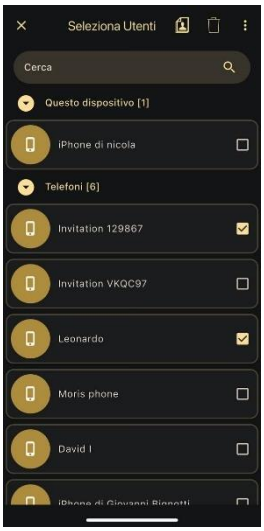


fig.49

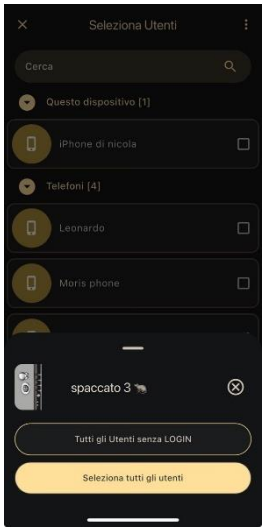


fig.50

Cancellazione rapida di un utente:

- Sempre nella schermata con l'elenco di tutti gli utenti, "scorrere" da destra a sinistra banner dell'utente da rimuovere;
- Premere la sezione rossa "Elimina" (fig.54) e successivamente confermare;



fig.54

Copiare Utenti

Operazione da effettuare se si vogliono copiare rapidamente più utenti con le loro impostazioni di accesso, da una serratura ad un'altra utilizzando lo stesso smartphone senza dover procedere alla loro registrazione:

- Entrare in Programmazione (vedi pag.8);
- Selezionare la voce "Utenti";
- Cliccare sull'icona in alto a destra (fig.51);
- Selezionare utenti da copiare;
- Selezionare e scegliere "Copia Utenti" (fig.52) **gli utenti ora saranno salvati sullo smartphone;**

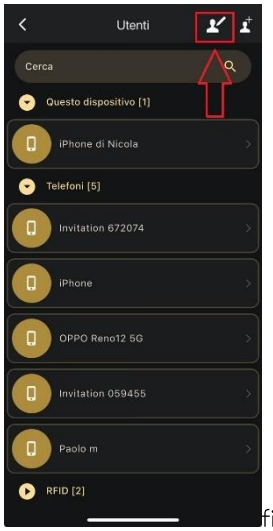


fig.51

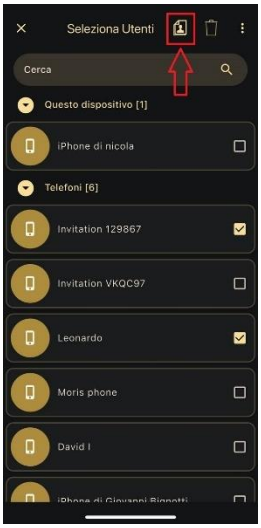


fig.52

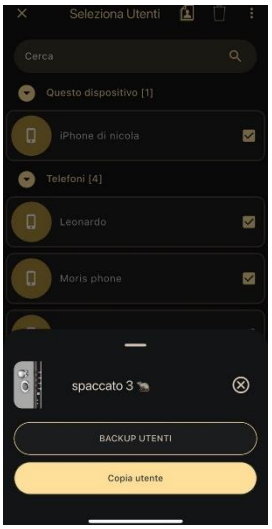


fig.53

- Entrare in modalità programmazione della serratura su cui copiare gli utenti;
- Selezionare "Utility" (fig.55);
- Nella voce "Spedire Utenti selezionati" premere su Invia Utenti (fig.56);
- Apparirà un messaggio che confermerà che il trasferimento è andato a buon fine;

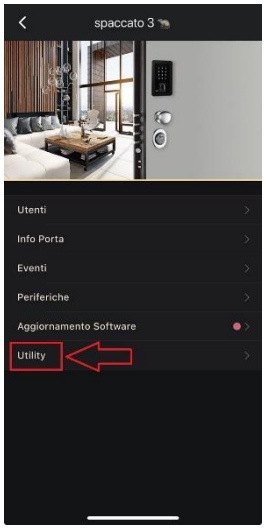


fig.55

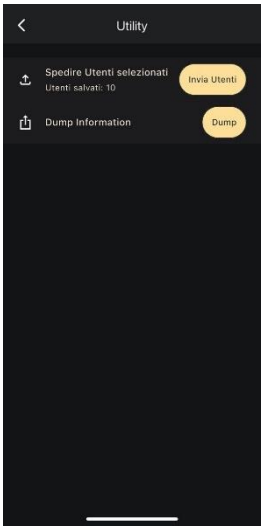


fig.56

Ora se si accede alla sezione "Utenti" di quella serratura ci saranno registrati tutti gli utenti copiati dalla serratura precedente.

Backup

Creazione Backup Utenti

Con la funzione Backup è possibile esportare gli utenti in un file protetto per poterli ripristinare successivamente in caso di reset della serratura oppure in un'altra serratura;

- Entrare in Programmazione (vedi pag.8);
- Selezionare la voce "Utenti" (fig.57);
- Cliccare sull'icona in alto a destra (fig.58);
- Selezionare utenti di cui realizzare il Backup;

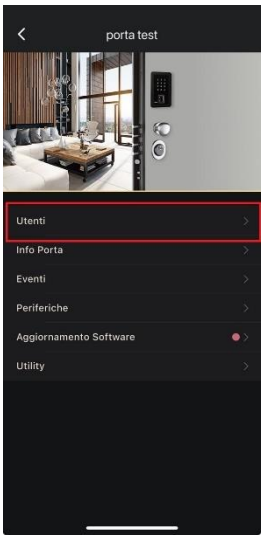


fig.57

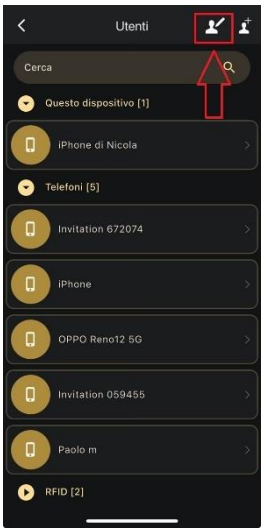


fig.58

- Una volta selezionati premere (fig.59) e scegliere "Backup Utenti" (fig.60);
- Scegliere una password per il ripristino successivo del Backup (fig.61);
- Selezionare dove salvare o se spedire il file generato.

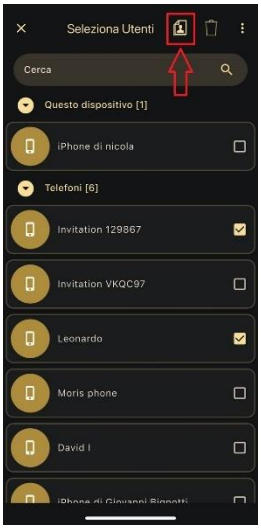


fig.59

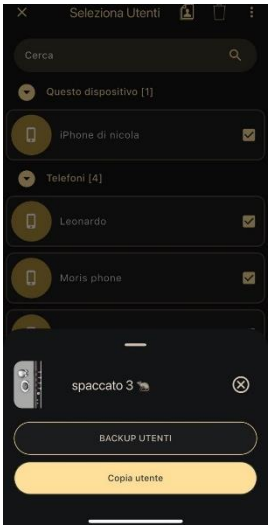


fig.60

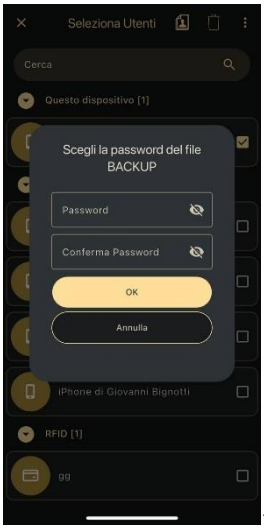


fig.61

Ora è stato creato un file digitale protetto da password con all'interno il backup di tutti gli utenti selezionati con le loro impostazioni.

Ripristino Backup Utenti

Operazione da effettuare per ripristinare gli utenti e le loro impostazioni di accesso da un backup precedentemente (vedi "Creazione Backup Utenti" pag.20).

- Selezionare il file da ripristinare e utilizzarlo con l'App Arckey del dispositivo in cui effettuare il ripristino;
- Immettere la password (fig.62) per il ripristino del backup (questa password è quella che è stata scelta in fase di creazione del file backup); Apparirà un messaggio che ci informa di entrare in programmazione nella serratura in cui dobbiamo inserire gli utenti salvati (fig.63);



fig.62



fig.63

- Entrare in programmazione della serratura in cui immettere gli utenti;
- Selezionare "Utility" (fig.64);
- Nella voce "Spedire Utenti selezionati" premere su 

(fig.65);
- Apparirà un messaggio che confermerà che il trasferimento è andato a buon fine;

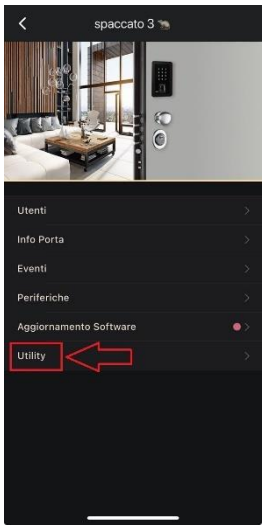


fig.64

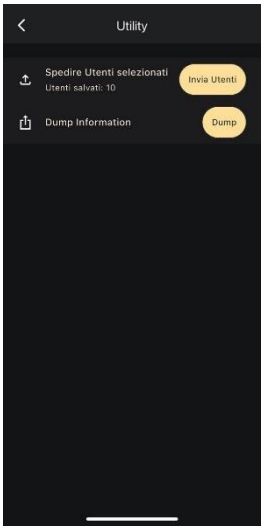


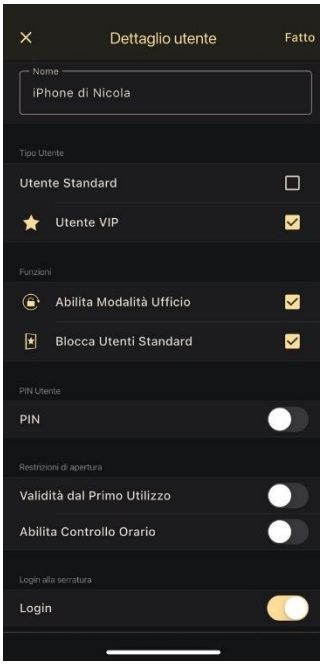
fig.65

Impostazioni Utente

Dettaglio Utente

Di seguito la lista delle impostazioni che è possibile configurare nei vari utenti contenuti nella serratura;

Ogni tipologia di utente (Smartphone, card, PIN, lettore di impronta, Invito) può godere delle stesse funzioni e impostazioni, tranne dove specificato di seguito.



Nome utente: Identifica l'utente (massimo 32 caratteri) .

Utente VIP: gli può essere assegnata la facoltà di bloccare gli Utenti Standard (vedi pag.).

Utente Standard: gli può essere negato l'accesso dagli utenti VIP (vedi pag.);

Abilita Modalità Ufficio: Consente di abilitare o meno l'utente all'attivazione o meno della Modalità Ufficio (vedi pag.);

Blocca Utenti Standard: Consente di abilitare o meno l'utente VIP ad abilitare o disabilitare l'utilizzo della serratura agli Utenti Standard (vedi.pag.)

PIN utente (solo per utenti di tipo Smartphone): L'accesso via Smartphone dell'utente può essere ulteriormente reso più sicuro dalla richiesta di un PIN da digitare con lo Smartphone al momento dell'apertura o per entrare in programmazione tramite Login.

Validità Dal Primo Utilizzo: selezionando questa opzione è possibile impostare un conteggio di tempo in minuti, ore o giorni la quale l'utente potrà utilizzare la serratura. Scaduto il tempo non potrà più accedervi (vedi pag.).

Abilità Controllo Orario: selezionando questa opzione è possibile impostare una precisa data di inizio e di fine utilizzo della serratura da parte di quell'utente; è possibile anche impostare fino a 2 fasce orarie e giornaliere che daranno la possibilità all'utente di utilizzare la serratura (vedi pag.)

Login: abilitando questa opzione sarà possibile per l'utente, accedere alla Modalità Programmazione senza l'utilizzo delle Admin Card (vedi pag.)

PIN utente (solo per utenti di tipo Smartphone)

L'apertura della porta via Smartphone o l'accesso alla modalità programmazione può essere ulteriormente resa più sicuro dalla richiesta di un PIN.

Attivando l'opzione PIN nel "Dettaglio Utente" inserire un PIN e poi ripeterlo nella sezione PIN VERIFICA. Successivamente attivare quale opzione è permessa solo con l'utilizzo del PIN (apertura porta o Login) (fig.66)

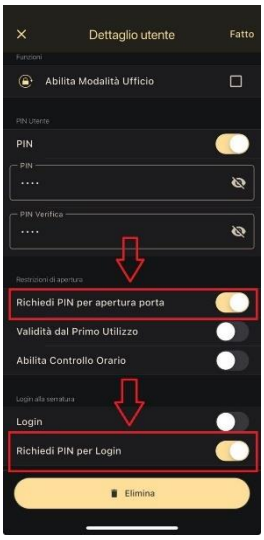


fig.66

E' possibile cambiare questo PIN senza accedere alla programmazione;

- Premere il banner della serratura;
- Si aprirà il sottomenù di apertura; premere "Cambia Pin" (fig.67)
- Inserire il PIN attuale e poi digitare il nuovo PIN e confermarlo su PIN Verifica (fig.68)
- Premere "Cambia PIN" per confermare (fig.68);

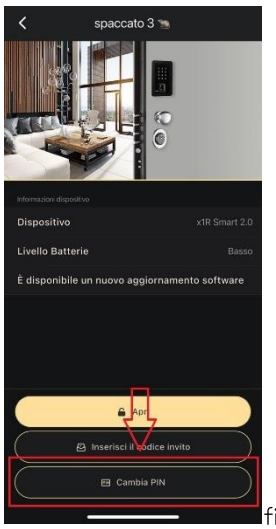


fig.67

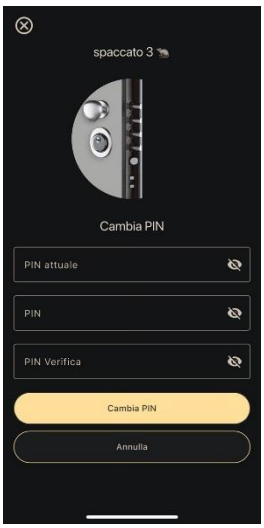


fig.68

Blocco Utenti Standard

Questa funzione, si utilizza per bloccare l'accesso alla porta a tutti gli Utenti Standard.
Quando l'impostazione "Blocca Utenti Standard" è abilitata, solo gli Utenti VIP potranno aprire la porta.

Attenzione: non bisogna confondere Utenti VIP e Utenti Standard con la funzione "Login". Infatti un'Utente Standard può avere la funzione "Login" abilitata e viceversa. L'utilizzo del Blocco Utenti Standard serve solamente a gestire, se necessario, un privilegio di entrata.

Per poterla utilizzare **non è necessario entrare in programmazione.**

- Selezionare il banner della porta sulla quale si vuole attivare la funzione;
- Si aprirà il sottomenù di apertura;
- Selezionare "Blocca Utenti Standard" (fig.69);
- Il banner della porta apparirà il simbolo ★ e il messaggio "Modalità VIP attiva" (fig.70);
- Fintanto che è attiva solo gli Utenti VIP potranno aprire la serratura

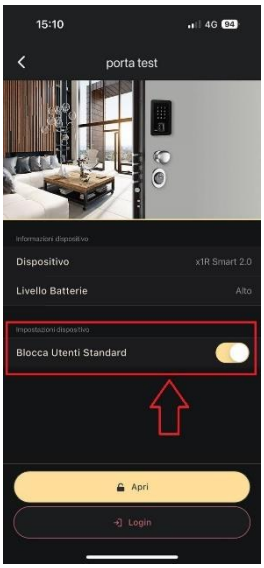


fig.69

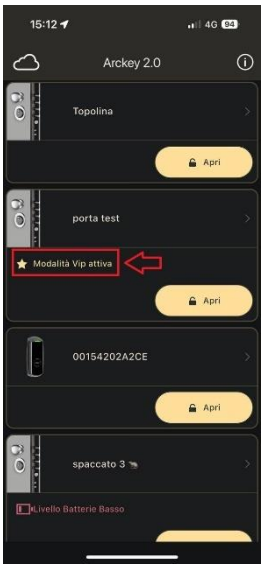


fig.70

Modalità Ufficio

La Modalità Ufficio è una modalità di utilizzo della serratura che serve ad utilizzare la serratura solamente con lo scrocco senza far fuoriuscire i catenacci di sicurezza.

Sono configurabili due tipologie di Modalità Ufficio:

- **Modalità Ufficio Light:** la serratura arretra i catenacci, rimanendo in chiusura solo con lo scrocco. L'apertura con credenziali autorizzate arretra solo lo scrocco, permettendo un maggior risparmio di energia e una minor usura meccanica.;
- **Modalità Ufficio Free:** la serratura arretra i catenacci e trattiene lo scrocco. In questa modalità la porta è sempre aperta a qualsiasi utente che desideri accedervi, senza l'utilizzo di credenziali autorizzate;

Per poter modificare la tipologia di Modalità Ufficio vedi "Funzioni Avanzate".

Una volta configurata correttamente per attivarla e disattivarla **non è necessario entrare in programmazione.**

- Selezionare il banner della porta sulla quale si vuole attivare la Modalità Ufficio;
- Si aprirà il sottomenù di apertura;
- Selezionare "Attiva modalità Ufficio" (fig.71);
- Sul banner della porta apparirà il simbolo e il messaggio "Modalità Ufficio Attiva" (fig.72)

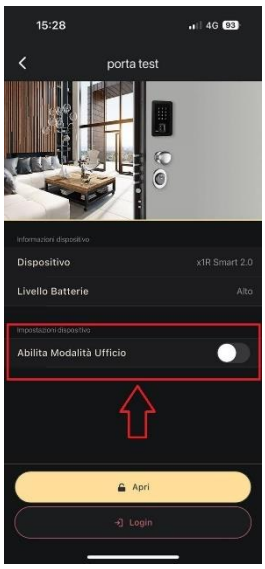


fig.71



fig.72

Per la programmazione oraria della Modalità Ufficio vedi Modalità Ufficio Programmata (pag.)

Restrizioni di apertura

Per ogni Utente registrato é possibile impostare delle restrizioni temporali di apertura della serratura.

Per accedere a queste impostazioni è necessario accedere al Dettaglio Utente.

Validità dal primo utilizzo: questo controllo permette di assegnare una validità "a termine".

Per esempio può essere necessario assegnare un accesso limitato di due giorni ad un tecnico che esegue una manutenzione. Allo scadere del secondo giorno l'accesso sarà inibito.

- Abilitare la voce "Validità dal primo utilizzo" (fig.73);
- Assegnare una durata che può essere in giorni/ore/minuti a partire dalla prima apertura della porta (fig.73);
- Premere su "Fatto" in alto a destra.

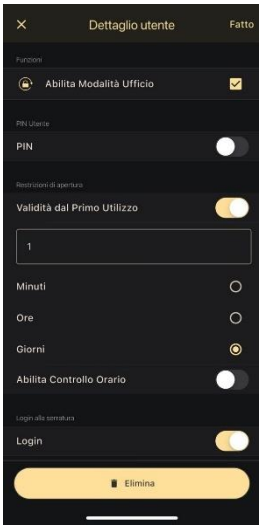


fig.73

Abilita controllo orario: Permette di assegnare una durata temporale di validità per un Utente da una data ad una data.

Fasce Orarie: Permettono un controllo più preciso delle restrizioni, all'interno del periodo di abilitazione. E' possibile indicare quali sono i giorni della settimana e la fascia oraria per i quali la serratura sarà valida per quell'Utente.

Esempio: il personale delle pulizie è abilitato all'accesso ma può accedere solo al sabato dalle ore 10 alle ore 12.

Si possono gestire due fasce orarie differenti per una programmazione più flessibile delle restrizioni di accesso.
Una volta configurato il periodo di validità ed eventuali fasce orarie, premere "Fatto" in alto a destra.

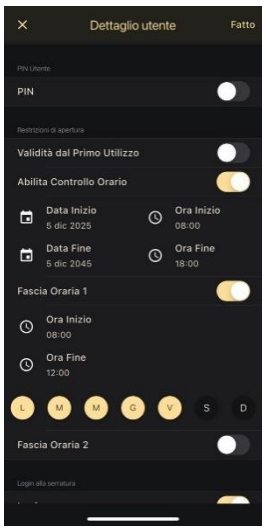
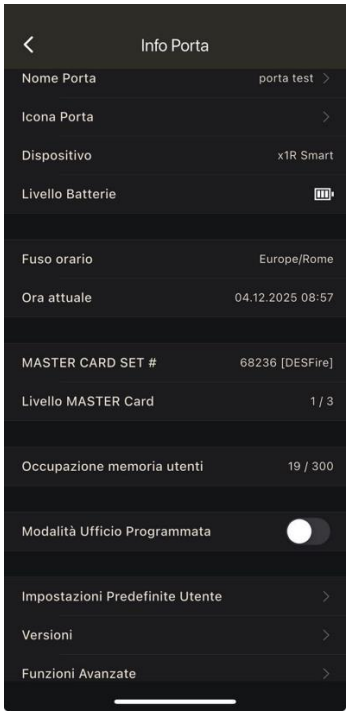


fig.74

Info Porta

La scheda Info Porta mostra l'elenco di tutte le informazioni relative alla porta. Per visualizzare queste informazioni accedere alla Modalità Programmazione (pag 8):



Nome Porta: può essere personalizzato sostituendo il numero di serie iniziale. Il nuovo nome assegnato verrà visualizzato nella schermata principale dell'App;

Icona Porta: E' possibile personalizzare l'icona presente nel banner della serratura

Dispositivo: indica il nome tecnico della serratura ISEO;

Livello Batteria: indica il livello di carica delle batterie di alimentazione della serratura;

Fuso orario / Ora attuale: indica l'orario dell'orologio della serratura. In caso di utilizzo da remoto potrebbe essere fondamentale per la gestione delle restrizioni orarie d'ingresso;

MASTER CARD SET #/Livello Admin Card: identifica il livello di sicurezza della Admin Card attiva; 1/3 significa che è Attiva l'Admin Card Verde;

Occupazione memoria utenti: indica il numero degli Utenti registrati (massimo 300);

Modalità Ufficio Programmata: consente di attivare la Modalità Ufficio Programmata a fasce orarie e di impostarne i programmi 1 e 2 (vedi pag.)

Impostazioni Predefinite Utente: consente di definire quali funzioni si vogliono attribuire di default ai nuovi Utenti creati (se utenti vip o standard, se attribuire restrizioni ecc...);

Versioni: contiene le informazioni di versione dei vari componenti della serratura (utili in caso di necessità di assistenza);

Funzioni Avanzate: all'interno sono contenuti dei parametri tecnici che possono modificare le caratteristiche di funzionalità della serratura. **Attenzione: si sconsiglia l'uso da parte di personale non tecnico; la modifica dei parametri contenuti all'interno di Funzioni Avanzate può compromettere il funzionamento regolare della serratura.**

Modalità Ufficio Programmata

Questa funzione permette di impostare due programmi, per abilitare e disabilitare automaticamente la Modalità Ufficio

- Entrare in Modalità Programmazione (pag.8);
- Accedere a "Info Porta";
- Abilitare "Modalità Ufficio Programmata" (fig.75);

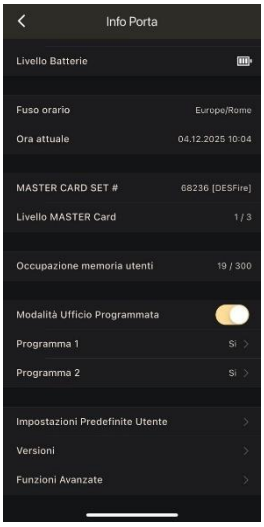


fig.75



fig.76

Abilita Programma (1 o 2)

E' possibile gestire 2 programmi per la Modalità Ufficio;

Attivazione Automatica

La Modalità Ufficio si attiverà e disattiverà automaticamente negli orari prestabiliti

Con Ingresso Primo Utente

La Modalità Ufficio si attiverà solamente con l'ingresso del primo utente che vi accederà. Poi resterà attiva fino alla scadenza impostata

Funzioni Avanzate

All'interno di questa sezione ci sono dei parametri di funzionamento del sistema che possono essere modificati.

Attenzione: Si sconsiglia l'uso da parte di personale non tecnico; la modifica dei parametri contenuti all'interno di Funzioni Avanzate può compromettere il funzionamento regolare della serratura.

Tra le varie funzionalità è' possibile modificare la Configurazione della Modalità Ufficio (fig.77) da Light a Free e viceversa (fig.78) (vedi "Modalità Ufficio")



fig.77

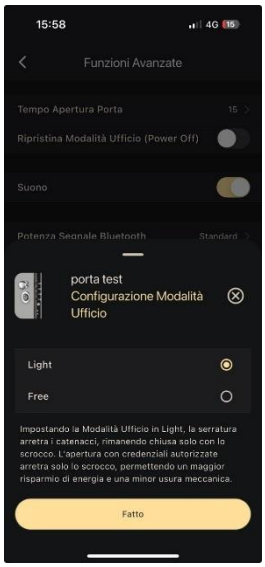


fig.78

Eventi

La scheda Eventi visualizza l'elenco degli ultimi 1000 eventi relativi alla porta (fig.79)
Come Eventi si intende qualsiasi azione meccanica, elettrica o elettronica avvenuta nella serratura.



fig.79

È possibile effettuare una ricerca rapida digitando il valore desiderato nell'apposito campo Cerca dopo aver cliccato sulla barra superiore (per esempio tutti gli eventi legati ad una certa card ID).

La lista può essere inviata via e-mail dopo aver cliccato sull'icona  in alto a destra.

Periferiche Wireless

Sono delle periferiche wireless a batterie che possono essere associate alla serratura in modo da implementarne le funzionalità (es. lettore d'impronta non installato nella porta).



Attenzione: queste periferiche devono comunicare con un lettore Bluetooth già presente nella porta. Non diventano un ricevente di segnale bluetooth e soprattutto non fungono da lettore per Admin Card.
La stessa serratura può avere più di una periferica ma una periferica non può comandare più serrature.

Aggiungi Periferiche Wireless

- Entrare in Modalità Programmazione (vedi pag.8);
- Selezionare "Periferiche";
- Selezionare "Aggiungi nuova Periferica"(fig.80); verranno visualizzate tutte le periferiche a disposizione;
- Selezionare la Periferica Wireless rilevata da aggiungere e attendere l'associazione;
- Impostare il nome della Periferica Wireless;
- Selezionare "Proteggi la procedura di RESET" <u>solamente</u> se abbiamo la necessità di proteggere ulteriormente la Periferica Wireless;
  Attenzione: in questo modo la Periferica Wireless viene associata all'Account Arckey da Remoto presente nel dispositivo che si sta utilizzando per associarla e viene protetta in caso di HARD RESET manuale;
- Ora la Periferica Wireless è associata alla serratura e apparirà nell'elenco delle Periferiche associate a quella serratura;

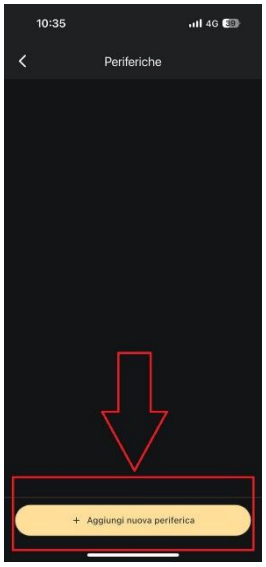


fig.80



fig.81

Con l'aggiunta della Periferica Wireless viene implementata la possibilità di aggiungere credenziali d'ingresso che prima non erano disponibili. Esempio: se la porta non presenta tastierino numerico e viene aggiunta un Tastiera Wireless, ora, quando si farà "Aggiungi Utente" sarà presente la possibilità di memorizzare un PIN.

Inoltre Tessere Rfid e PIN eventualmente già registrati nella serratura funzioneranno comunque senza doverli ri-memorizzare

Rimuovere Periferica Wireless

- Entrare in Modalità Programmazione (vedi pag.8);
- Selezionare "Periferiche";
- Scorrere da destra a sinistra e premere "Disassocia" (fig.82), oppure, premere sul banner della Periferica per accedere al sottomenù, premere su "Disassocia" in basso e confermare (fig.83);
- Ora è possibile associare la Periferica ad un'altra serratura.

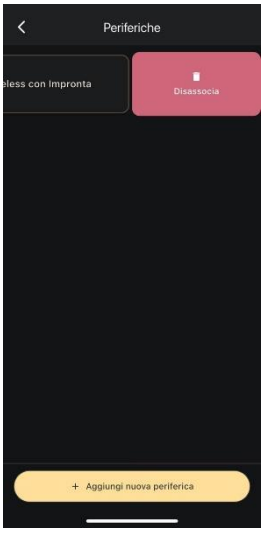


fig.82

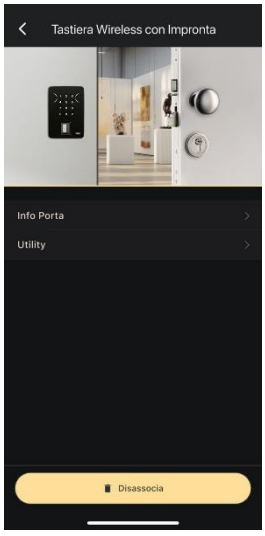


fig.83

Utility

Nella scheda Utility è possibile accedere a varie funzioni di manutenzione.

Spedire Utenti Selezionati: Se nella Lista Utenti sono stati copiati degli utenti (vedi "Lista Utenti" pag.) sono indicati qui.

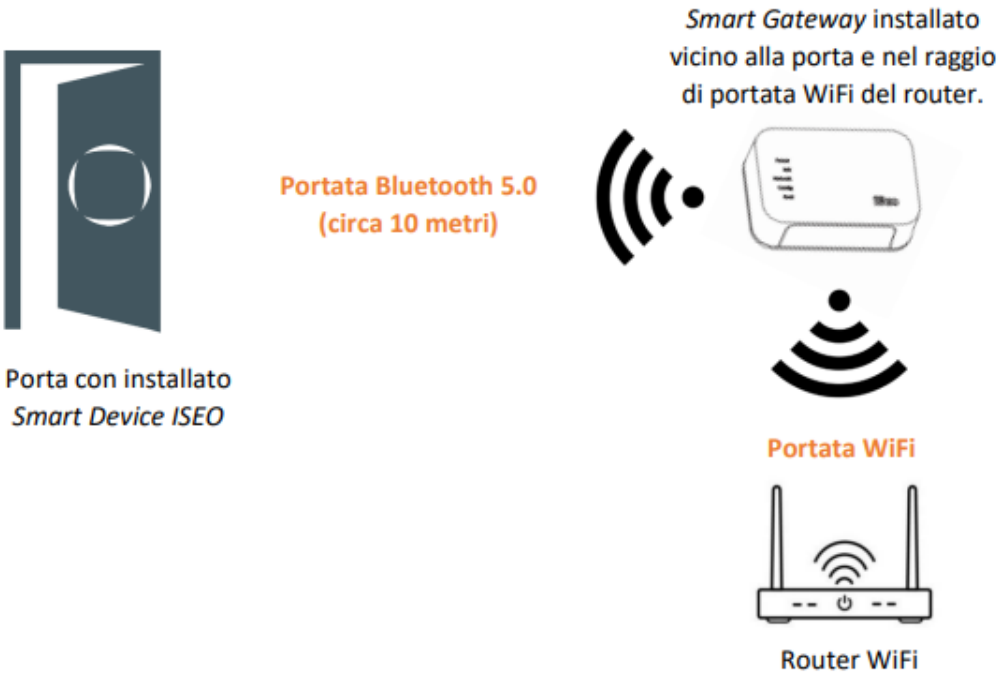
Aggiornamento software: controlla e scarica gli aggiornamenti dell'App. In presenza di un aggiornamento disponibile basterà cliccare sul pulsante per eseguire l'aggiornamento del software della serratura.
Non allontanare lo Smartphone dalla porta fino al completamento dell'aggiornamento.

Attenzione: è fortemente consigliato scaricare sempre tutti gli aggiornamenti rilasciati per mantenere il sistema allineato ai massimi standard di sicurezza e prestazioni.

Dump Information: consente di generare ed inviare un file di diagnostica completo della serratura estremamente utile in caso di malfunzionamenti della porta per un analisi approfondita dei vari parametri.

Gateway

Panoramica di funzionamento



Attraverso il Dispositivo Gateway è possibile gestire le credenziali e l'apertura della porta da qualsiasi parte del mondo senza trovarsi in prossimità della stessa tramite un servizio cloud gestito da ISEO.

Per poterlo utilizzare è necessario:

- Serratura con Bluetooth 5.0 (vedi pag.2);
- Posizionare il Gateway ad una distanza che permetta la comunicazione Bluetooth tra Gateway e Serratura (di solito non deve superare i 10m di distanza ma è opportuno tenere conto anche di eventuali ostacoli, fonti elettromagnetiche ecc.);
- Posizionare il Gateway ad una distanza che permetta la comunicazione con il Wi-Fi;
- Connessione internet sul dispositivo utilizzato per la configurazione;

Legenda Led Gateway:

Power Indica lo stato di alimentazione del Gateway. Se spento significa che non è alimentato;

BLE Indica lo stato di Connessione Bluetooth con la serratura. Quando lampeggia significa che sta comunicando con la serratura tramite il Bluetooth.

Network Indica lo stato di connessione del Gateway con la rete Internet Se spento significa che non è associato a nessuna rete.

Config Quando fisso significa che il Gateway è pronto per la configurazione; una volta configurato resta spento nell'utilizzo normale.

Boot Indica che il Gateway dopo l'accensione o il RESET si sta inizializzando per l'utilizzo.

Accedere ad Arckey da Remoto

- Nella schermata principale dell'App. Selezionare il simbolo ☁ in altro a sinistra (fig.84) Si verrà reindirizzati alla piattaforma cloud di ISEO.
- Se si possiede già un account ISEO accedere con le credenziali in possesso (fig.85). Altrimenti premere "Registrati" e completare il processo di registrazione al Cloud ISEO (fig.86).



fig.84



fig.85

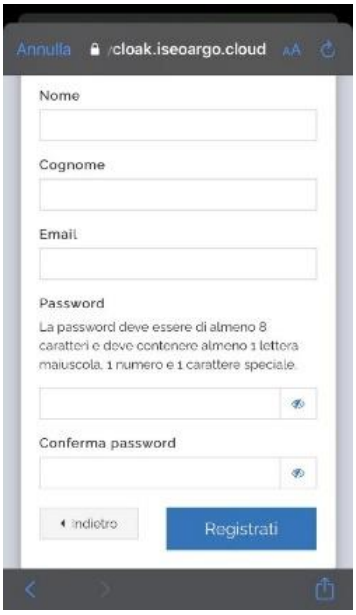


fig.86

- Successivamente accettare termini e condizioni per il trattamento dei dati personali (fig.87).
- Una volta completata la registrazione è necessario confermare l'email tramite il proprio account, anche attraverso browser pc (fig.88);
- Una volta confermata la mail è possibile accedere al Cloud Iseo con le credenziali appena registrate (fig.89). Per i successivi utilizzi, se spuntiamo "Ricordami" verranno memorizzate le credenziali e l'accesso al dispositivo sarà automatico.
- Siamo correttamente autenticati e connessi (fig.90).



fig.87



fig.88



fig.89

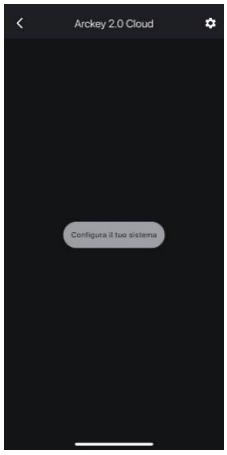


fig.90

Installazione e configurazione iniziale Gateway

Collegare il Dispositivo Gateway all'alimentazione e attendere che smetta di lampeggiare il led rosso "Boot" (fig.91) e rimanga fisso il led "Config" (fig.92). Ora è possibile procedere al rilevamento e all'installazione.



fig.91



fig.92

Attenzione: la configurazione iniziale può essere effettuata da un solo dispositivo che sarà l'Amministratore del Gateway. Una volta inizializzato, solamente questo dispositivo può permettere l'utilizzo del Gateway da parte di altri Account.

fig.

- Dalla schermata principale di Arckey da Remoto selezionare "Configura il tuo sistema"
- Premere "Si" se è verificata la situazione descritta (fig.93).
- Successivamente verrà chiesto di inserire un codice presente nel retro del Gateway per poterlo associare ad una rete Wi-Fi che servirà al Gateway per comunicare tramite la connessione internet. Può essere fatto inserendo manualmente i codici come in figura (fig.95) oppure molto più semplicemente inquadrando il QR code con la fotocamera del proprio dispositivo.

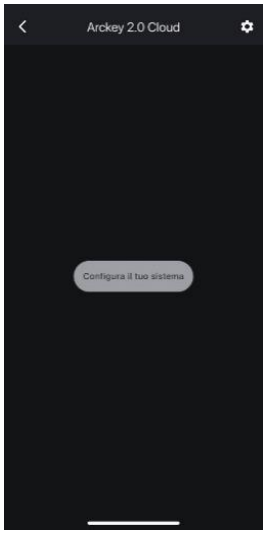


fig.93



fig.94


fig.95



fig.96

- Successivamente viene chiesto di collegare il dispositivo ad una rete Wi-Fi in prossimità del Gateway (fig.97)
- Inserire la Password della rete Wi-Fi (fig.98);

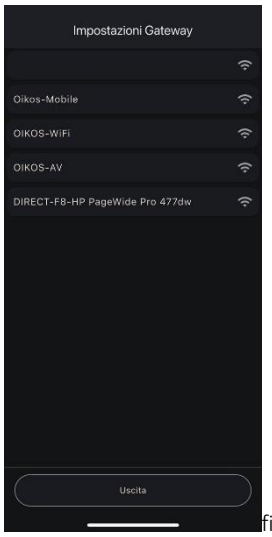


fig.97

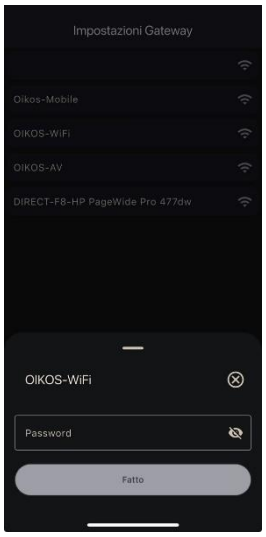


fig.98

- Dopo la configurazione compilare il nome del Gateway (fig.99);
- E' possibile ora aggiungere una serratura oppure farlo successivamente (fig.100); una volta completato l'associazione del Gateway con la rete WiFi devono essere illuminati i led "**Power**" e **Network**".



. fig.99



fig.100

Aggiungere Serratura al Gateway

Attenzione: per aggiungere una qualsiasi serratura al dispositivo Gateway è necessario trovarsi in prossimità della stessa con l'Admin Card corretta (vedi pag.);

Procedimento:

- Dalla schermata principale del Cloud selezionare l'icona in alto a destra (fig.101);
- Selezionare "Serrature"(fig.102);
- Selezionare "Aggiungi Serratura" (fig.103) il dispositivo ora cercherà le serrature nelle vicinanze;
- Passare l'Admin Card corretta nella serratura che si vuole associare;
- Premere su "Aggiungi Serratura"

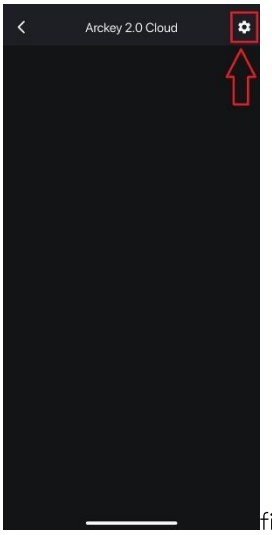


fig.101

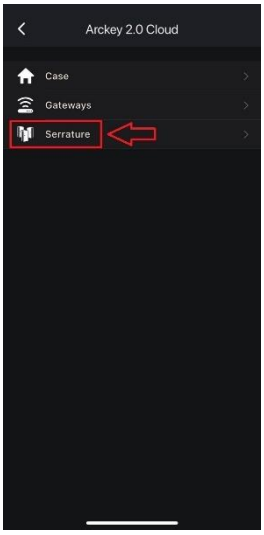


fig.102

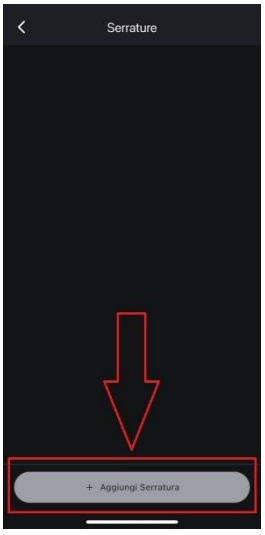


fig.103

- Passare l'Admin Card corretta nella serratura che si vuole associare (fig.104);
- Premere su "Aggiungi Serratura" e attendere che l'operazione di associazione sia completata **(non chiudere l'App durante questa operazione) (fig 105)**



fig.104

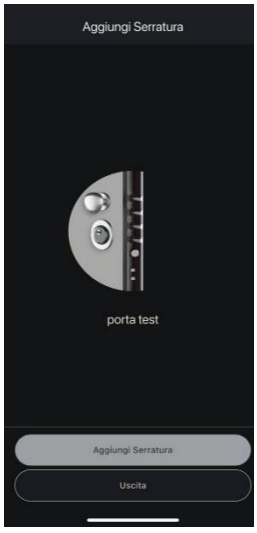


fig.105

Una volta stabilita la connessione tra Gateway e serratura, la schermata successiva (fig.106) permette di impostare:

- Nome Account è il nome dell'Account a cui è associata la serratura
- Password Account Serratura è la password da scegliere per l'apertura della porta. Servirà per aprire la porta da remoto.
- Verifica la Password Account Serratura ripetere la password scelta;
- Seleziona Casa permette di raggruppare serrature che fanno parte dello stesso sistema all'interno dello stesso gruppo Casa;

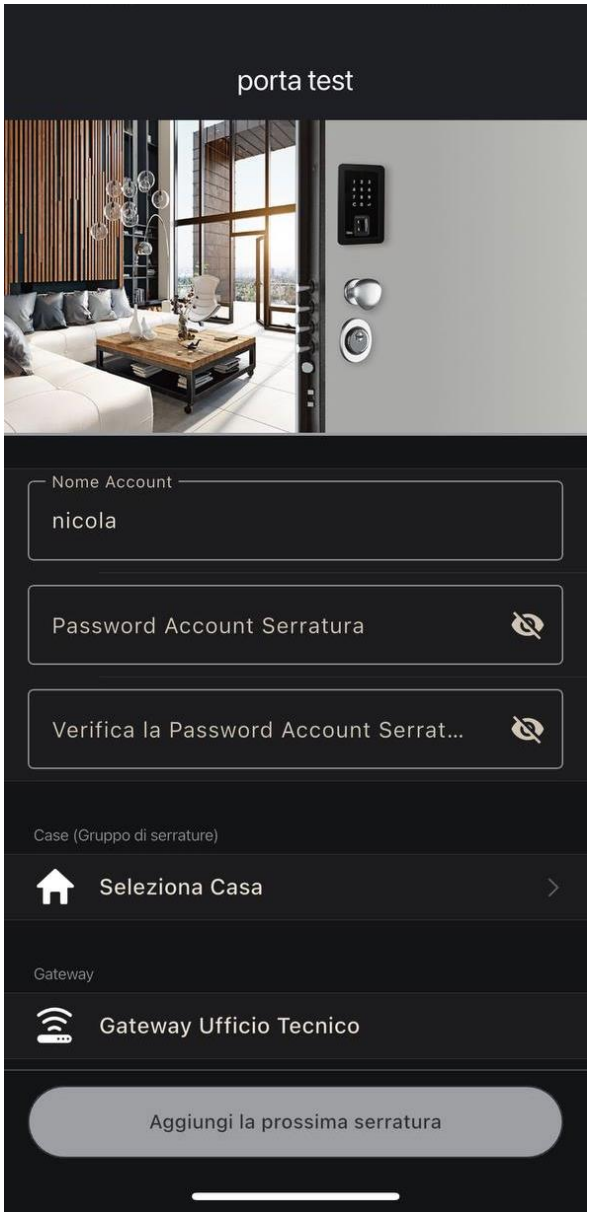


fig.106

Se si vogliono aggiungere altre serrature premere "Aggiungi la prossima serratura"
Altrimenti premere su "Termina Operazione" (appare una volta impostata la Password Account Serratura).

Utilizzo Arckey da Remoto

Una volta associata correttamente al proprio Account la serratura comparirà nella schermata principale di Arckey 2.0 Cloud.

Nella versione di Arckey da Remoto i pulsanti che solitamente sono gialli qui sono di colore grigio ma hanno le stesse funzionalità. Infatti da remoto è possibile:

- **Aprire la serratura:** Premere la serratura desiderata e digitare la Password Serratura impostata durante l'associazione al Gateway. (nei dispositivi iOS è possibile settare la propria impronta digitale o Face ID per la compilazione automatica della Password). Per ragioni di sicurezza viene richiesta una seconda conferma per l'apertura della porta (fig.107);
- **Accedere alla "Modalità Programmazione"** della serratura attraverso la funzionalità Login con cui è possibile:
    - Aggiungere, modificare o eliminare Utenti;
    - Leggere lo storico eventi; vengono precaricati gli eventi nel proprio dispositivo ed è quindi necessario aggiornare la pagina per caricare gli eventi in tempo reale;
    - Aggiungere altri Account per la gestione da remoto (fig.109);

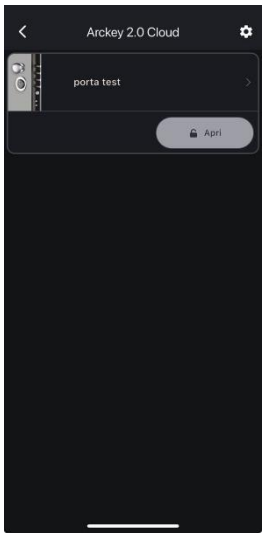


fig.107

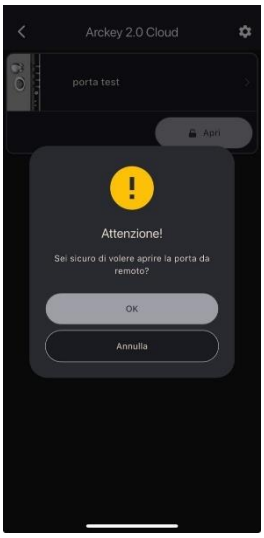


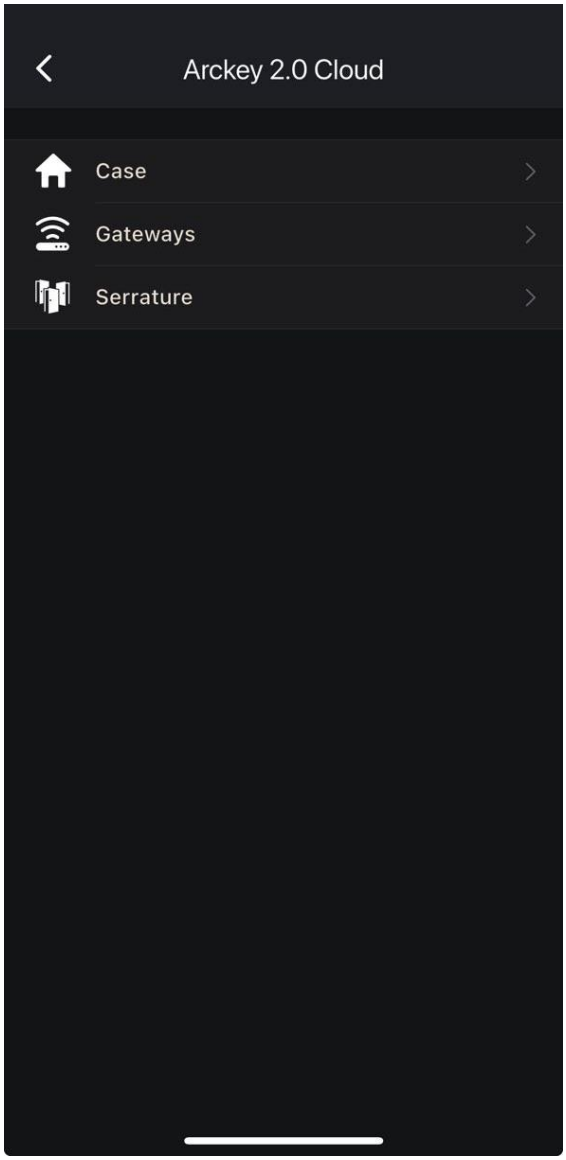
fig.108



fig.109

Menù Gateway

Dalla schermata principale di Arckey da Remoto selezionando il pulsante in alto a destra ⚙ si accede al Menù Gateway.



Casa: Permette aggiungere, rinominare e cancellare le Case che raggruppano le diverse serrature;

Gateways: Permette di aggiungere, rinominare e cancellare i dispositivi Gateway associato all'Account.

Serrature: Permette di aggiungere, rinominare e cancellare le serrature raggiungibili; attraverso questa sezione è possibile anche associare la serratura ad una "Casa". **Per aggiungere una serratura è comunque necessario essere di fronte alla serratura da registrare con la Admin Card (pag.).**

Aggiungere Account Utente Al Gateway

L'Amministratore Gateway può aggiungere altri Account Utenti per il controllo della serratura. Per fare questo bisogna:

- Accedere ad Arckey Remoto;
- Fare "Login" alla serratura;
- Premere icona
- Premere icona
- Indicare Nome e Indirizzo Email dell'Account presente nel Cloud ISEO dell'Utente che si vuole aggiungere
- Scegliere i permessi che si vogliono concedere al nuovo Utente
- Premere "FATTO" in alto a destra

Il nuovo utente riceverà una e-mail all'indirizzo associato con il nome della serratura e una TEMPORARY PASSWORD che gli permetterà di sbloccare la serratura.

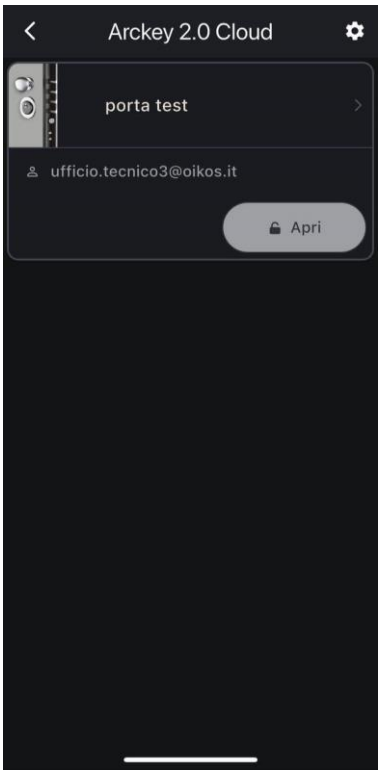


fig.110

Ora, al nuovo Utente che tramite l'app avrà effettuato l'accesso al Cloud ISEO, apparirà l'elenco delle serrature a cui si è stati invitati con indicato l'indirizzo email **dell'Amministratore Gateway.**

Per aprire la serratura il nuovo Utente dovrà utilizzare la Password TEMPORANEA contenuta nella e-mail di invito.

Successivamente attraverso la funzione "Login" e selezionando il proprio Account è possibile modificare la Password Serratura che andrà a sostituire quella Temporanea. La Password Serratura è associata all'Account che viene utilizzato in quel momento, quindi per la stessa serratura ogni Account può avere una password diversa.

Rimuovere Account Utente Gateway

Per rimuovere un Account Gateway è necessario:

- Accedere ad Arckey da Remoto;
- Entrare nella Modalità Programmazione della serratura tramite "Login";
- Selezionare "Utenti";
- Eliminare l'Account Utente che sarà presente nella sezione "Account" scorrendo da destra verso sinistra il banner dell'Utente oppure all'interno del dettaglio dell'Utente;

Ora ogni Account Utente può visualizzare in autonomia la serratura ma non potrà effettuare a sua volta inviti.

Attenzione: L'Account Utente Invitato non può cancellare l'Amministratore del Gateway

