Arckey

OIKOS
ARCHITETTURE D'INGRESSO

Sistema integrato di gestione degli accessi con apertura elettronica attraverso App

Manuale d'Uso

Riservato All'Amministratore Di Sistema

GET IT ON Google Play

Download on the App Store

INDICE

COS'E' 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 DI 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)

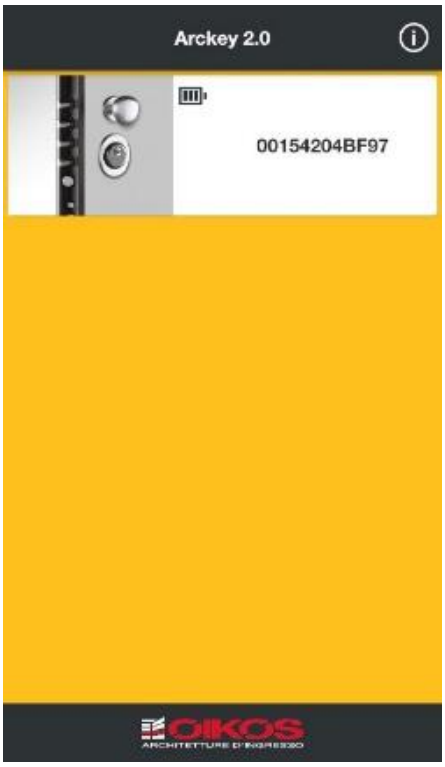


fig.1

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 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 sul telefono

Quando si avvia l'App sul display dello Smartphone 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.33 "Info Porta")

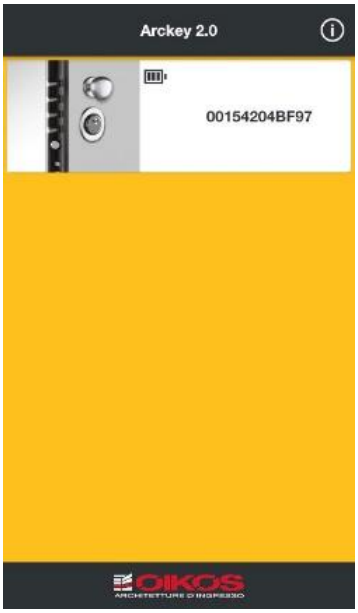


fig.10

Cliccando sull'icona Informazioni ⓘ in alto a destra si ottengono i dati sulla versione dell'App e sul software dei dispositivi supportati. E' inoltre possibile cambiare la lingua di utilizzo dell'App, visualizzare la guida utente nella lingua scelta e abilitare e disabilitare l'Accesso da Remoto (fig.11).

fig.11

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 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.

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 MODALITA' PROGRAMMAZIONE

Attivare il bluetooth nel proprio dispositivo.

Aprire 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 pulsante bianco che identifica la porta si colorerà di rosso (fig.12)

Cliccare sulla serratura.

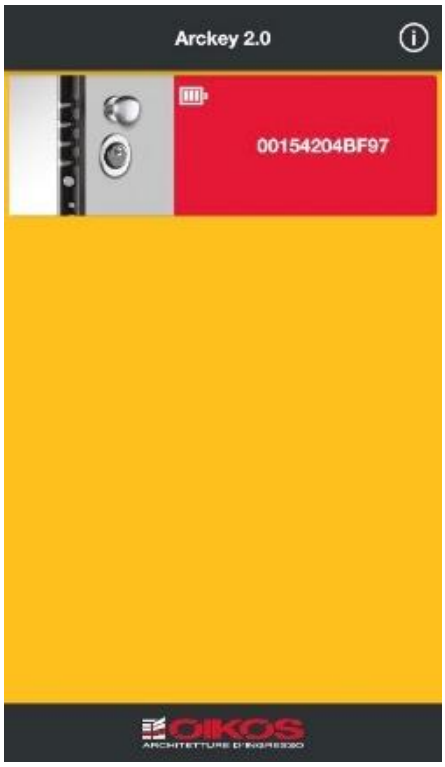


fig.12

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.

AGGIUNGERE LO SMARTPHONE COME CREDENZIALE DI ACCESSO

Dopo l'accoppiamento verrà richiesto di aggiungere lo Smartphone come Credenziale per aprire la serratura (fig.13). Questa operazione deve essere eseguita per ogni Smartphone che si desidera memorizzare sulla serratura.

fig.13

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.14)
In seguito saranno spiegate nel dettaglio le singole funzioni

fig.14

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.

APRIRE LA PORTA

Uscire dalla modalità programmazione cliccando sull'icona  in alto a sinistra.

Cliccare sul banner bianco che identifica la porta per mandare un impulso di apertura alla serratura. La serratura farà rientrare i catenacci.

MEMORIZZAZIONE UTENTI

Memorizzazione Oikos Card, Chiave Transponder, Card con tecnologia RFID

Entrare in programmazione (vedi pag. 7).
Una volta all'interno dell'elenco utenti, 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 e PIN

E' possibile aggiungere delle card anche senza averle fisicamente in mano, memorizzandole attraverso il loro codice (fig.14).

fig.14

Questa funzione risulta utile nel caso per esempio che le card siano state già distribuite agli utenti.
Entrare in programmazione (vedi pag. 7).

fig.15

fig.16

fig.17

Cliccare sull'icona aggiungi utente in alto a destra e scegliere che tipologia di utilizzo si vuole inserire (fig.15):

Carta DESfire, Carta Utente Classica o Card RFID Generica (fig.16).

Inserire un nome ed il numero identificativo riportato sulla card (fig.17). Cliccare su Fatto in alto a destra.

Memorizzazione codice PIN (solo in presenza di tastierino numerico)

Entrare in programmazione (vedi pag. 7).

Una volta all'interno dell'elenco utenti, digitare il codice numerico (minimo 4, massimo 8 caratteri) seguito dal tasto INVIO ↵. Attendere il segnale di conferma. Il codice PIN comparirà nell'elenco utenti a conferma dell'avvenuta memorizzazione.

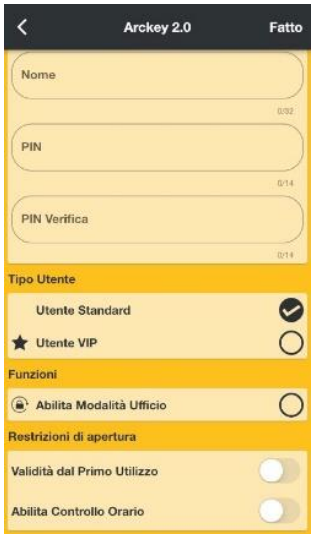


fig.18

Se si vuole aggiungere un PIN senza digitarlo sulla tastiera, cliccare su PIN, assegnare un nome e digitare due volte il codice, sui campi PIN e PIN verifica. Il codice deve essere almeno di 4 cifre. Cliccare su Fatto (fig.18).

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

Memorizzazione Impronta digitale (solo in presenza di lettore d'impronta)

Entrare in programmazione. Con il lettore d'impronta è necessario accostare la Admin Card al lettore nascosto.

Cliccare sull'icona aggiungi utente in alto a destra (fig.14) e scegliere Impronte Digitali .

Il lettore di impronta inizierà a lampeggiare. Posizionare il dito sul lettore, come indicato dall'animazione (fig.19).

L'App chiederà di leggere l'impronta svariate volte al fine di ottenere una registrazione di buona qualità (fig.20).

fig.19

fig.20

fig.21

fig.22

Cliccare su OK (fig.21). Successivamente è possibile modificare il nome dell'utilizzatore e altre impostazioni. Una volta completato il tutto premere su "Fatto" (fig.22).

Ora l'impronta è riconosciuta come credenziale valida per aprire la porta.

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…

Memorizzazione Inviti

Gli Inviti permettono a un utente (Smartphone o Tablet), di auto-registrarsi nella memoria della serratura come utente abilitato all'accesso, usando un codice di invito precedentemente memorizzato nella serratura dall'Amministratore.

Per esempio, la funzione Inviti permette al gestore di un Bed and Breakfast di poter abilitare l'accesso a un cliente, ancora prima che egli arrivi presso la struttura.
Per farlo l'Amministratore in precedenza ha aggiunto nella memoria della serratura un Codice Invito, che verrà inviato alla persona a cui deve consentire l'accesso.

Cosa deve fare l'Amministratore per creare un invito:

Entrare in programmazione utente. Cliccare sull'icona "Aggiungi utente" e poi su Inviti .
Si apre la schermata di configurazione utente.
Inserire un nome che identifichi questo invito ed eventualmente impostare i parametri desiderati.
Premere Fatto per confermare.
Viene chiesto se si desidera inviare un messaggio di invito (fig.23).
Premere Si per inviarlo subito, oppure No se si vuole inviarlo in un secondo momento.

fig.23

Un testo viene generato automaticamente con una 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 (Skype, WhatsApp, Telegram ecc…). L'invito compare ora nella lista degli inviti. Da qui è possibile inviare nuovamente l'invito se necessario.

Cosa deve fare l'utente che riceve l'invito:

L'utente che riceve l'invito deve prima di tutto scaricare e installare l'App 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. Cliccando sul pulsante bianco che identifica la porta, viene chiesto il codice di invito precedentemente

ricevuto.
La porta si apre e lo Smartphone compare ora tra la lista degli Smartphone registrati.
L'invito, in quanto "accettato", sparisce dalla lista degli inviti.

CANCELLAZIONE E SALVATAGGIO DI UTENTI

Cliccare sull'icona Modifica in alto a destra (fig.14).
Selezionare l'utente da cancellare o salvare (fig.24) oppure premere l'icona per selezionarli tutti (attenzione, in questo modo saranno eliminati/salvati tutti gli utenti).
Premere sull'icona cestino per confermare l'eliminazione oppure per salvare gli utenti selezionati o creare un backup. Gli utenti saranno salvati nello Smartphone e potranno essere recuperati in caso di necessità o duplicati su un'altra serratura senza doverli riconfigurare da capo

fig. 24

Cancellazione rapida di un utente:

Dalla lista degli utenti: su sistemi Android tenere premuto l'utente da cancellare. Su sistemi iOS "scorrere" verso destra l'utente.
Confermare la cancellazione.

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:

- Selezionare e scegliere quali tipi di utenti copiare (tutti oppure solo quelli senza la funzione LOGIN);
- Premere e scegliere "COPIA UTENTI" (fig.25);

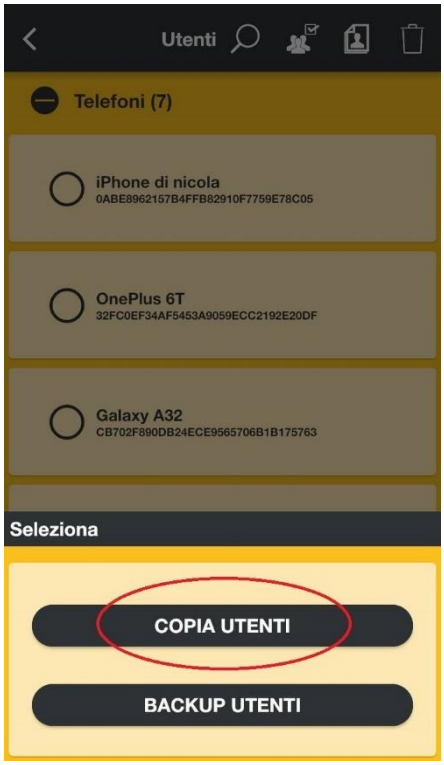


fig.25

- Premere copia; gli utenti ora saranno salvati sullo smartphone;
- Entrare in modalità programmazione (vedi pag.7 ”Modalità Programmazione”) e selezionare la serratura in cui si vuole copiare gli utenti;
- Premere Utility ⚙
- Premere “Spedire Utenti selezionati” e successivamente premere “OK” (fig.26)

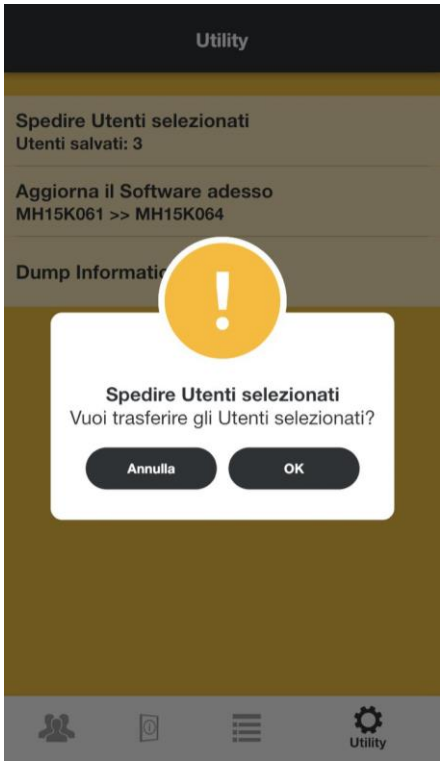


fig.26

- Apparirà un messaggio che confermerà che il trasferimento è andato a buon fine.

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

Backup Utenti

Operazione da effettuare se è necessario effettuare un backup degli utenti con le loro impostazioni di accesso, per un eventuale ripristino successivo.

- Selezionare e scegliere quali tipi di utenti copiare in un backup (tutti oppure solo quelli senza la funzione LOGIN)
- Premere e scegliere “BACKUP UTENTI” (fig.27).

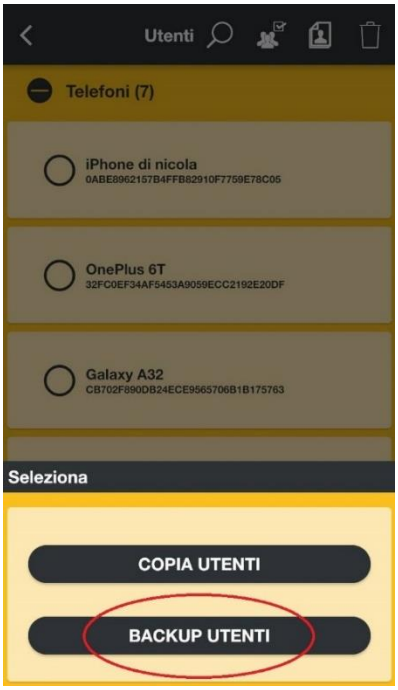


fig.27

- Premere BACKUP UTENTI; gli utenti ora sono inseriti in un file di backup;
- Inserire una password da associare al file backup (fig.28). Questa password servirà per ripristinare il backup successivamente;

fig.28

- Scegliere come e dove inviare il file di backup (email, whatsapp ecc);

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 "Backup Utenti").

- Selezionare il file da ripristinare e aprirlo con l'App Arckey del dispositivo in cui effettuare il ripristino;
- Immettere la password (fig.29) 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.30)

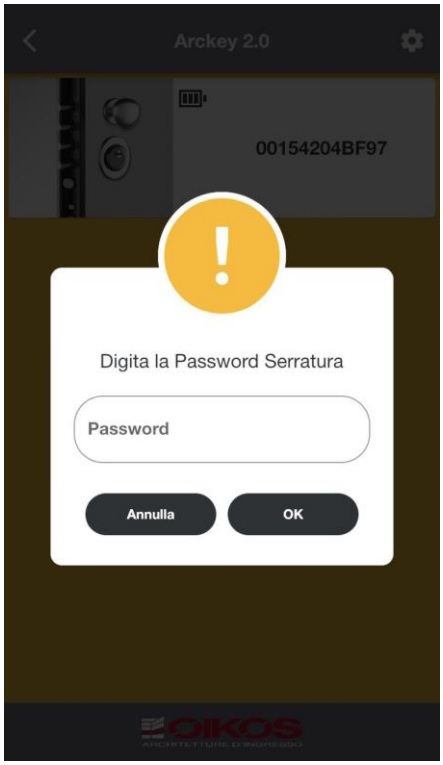


fig.29

fig.30

- Entrare in programmazione della serratura in cui immettere gli utenti;
- Premere Utility; ⚙
- Premere "Spedire Utenti selezionati" e successivamente premere "OK";
- Apparirà un messaggio che confermerà che il trasferimento è andato a buon fine.

IMPOSTAZIONI UTENTE

Dalla lista utenti scegliere l'utente da impostare.

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

fig.31

fig.32

Nome utente: Cliccare sul campo Nome per assegnare un nome identificativo allo Smartphone o Tablet (massimo 32 caratteri) (fig.31).

Tipo Utente: Selezionare se l'utente sarà di tipo standard o VIP (fig.31).

Utente VIP: può aprire sempre la porta, senza limitazioni. Gli può essere assegnata la facoltà di bloccare gli utenti standard. Può inoltre abilitare la Modalità Ufficio (vedi pag. 21).

Utente Standard: può essere disabilitato nell'accesso dagli utenti VIP. Può abilitare la Modalità Ufficio (vedi pag. 18).

Nella lista utenti l'utente VIP viene contraddistinto dal simbolo ★ (fig.32)

Funzioni: Consente di assegnare all'utente la possibilità di abilitare la Modalità Ufficio (vedi pag. 21) e di bloccare l'accesso agli utenti standard (fig.31). Solo gli utenti VIP possono bloccare l'accesso agli utenti standard. La possibilità di attivare la modalità ufficio viene indicata con l'icona (fig.33), la possibilità di bloccare gli utenti standard viene indicata con l'icona (fig.34).

fig.33

fig.34

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 sulla tastiera dello Smartphone al momento dell'apertura, se configurato nelle restrizioni di apertura (fig.35).

fig.35

fig.36

La presenza di un PIN utente viene indicata con l'icona OPEN (fig.36).

Restrizioni di Apertura: l'impostazione consente di limitare il passaggio agli utenti. Ad ogni utente possono essere assegnate delle restrizioni, per esempio per limitarne la validità nel tempo ad una durata in giorni a partire dal primo accesso oppure ad una predefinita fascia oraria (esempio: il personale di servizio può accedere solo un determinato giorno della settimana ad un determinato orario). Sono programmabili due fasce orarie per ogni utente.

Se presente, una restrizione di apertura viene indicata tramite l'icona (fig.37)

Modalità Masterphone (solo per utenti di tipo Smartphone): La modalità Masterphone consente all'utente di tipo Smartphone di poter entrare in programmazione senza dover presentare la Admin card che viene sostituita dallo Smartphone. In questo modo l'utente diventa di fatto un amministratore.

Se configurato, l'uso della modalità Masterphone può essere messa in ulteriore sicurezza con l'attivazione di un PIN utente.

L'abilitazione della funzione Masterphone viene indicata dall'icona LOGIN (fig.38)

fig.37

fig.38

BLOCCO UTENTI STANDARD

Questa funzione, quando abilitata, impedisce 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.

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

Toccare e tenere premuto il Pulsante che identifica la porta sulla quale si vuole attivare la funzione Blocca utenti standard. Comparirà il menù per abilitare/disabilitare la funzione (fig.39).

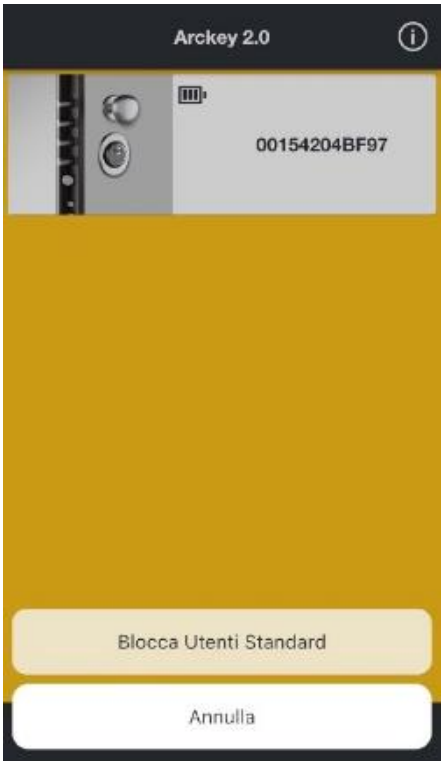


fig.39

Nel pulsante bianco comparirà un simbolo ★ che indica la funzione abilitata (fig.40). Eseguire l'operazione contraria per disabilitare la funzione (fig.41).

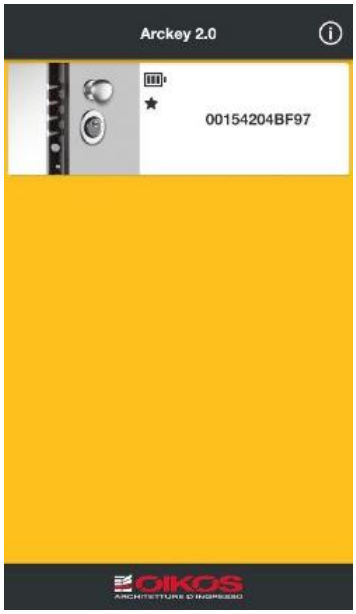


fig.40

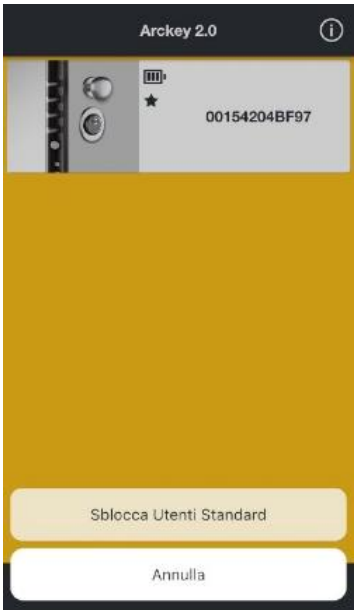


fig.41

MODALITA' UFFICIO

Gli utenti Smartphone abilitati possono, dalla schermata principale dell'App, attivare la modalità ufficio. In questa modalità la serratura funziona solo con lo scrocco e le mandate sono ritirate.
In questa modalità la porta è accostata ma non è chiusa in sicurezza.

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

Toccare e tenere premuto il Pulsante che identifica la porta sulla quale si vuole attivare la funzione Modalità Ufficio. Comparirà il menù per abilitare/disabilitare la funzione (fig.42).

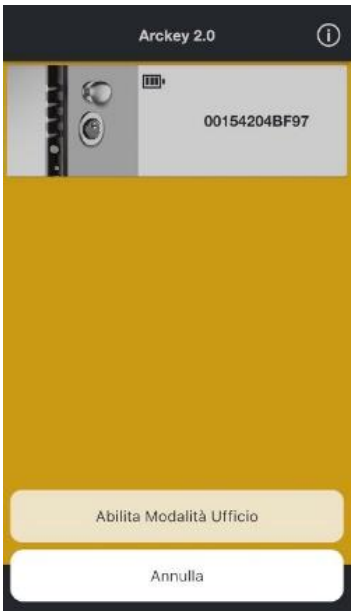


fig.42

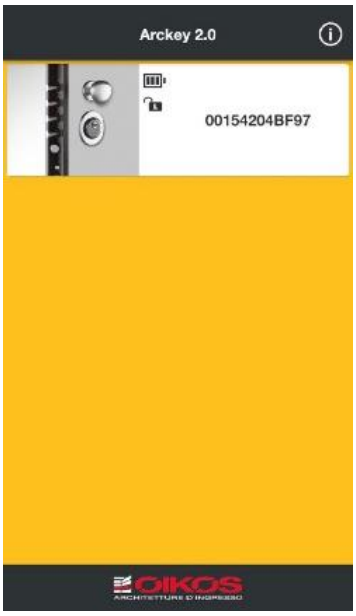


fig.43

Nel pulsante Bianco comparirà il simbolo che indica la funzione abilitata (fig.43).

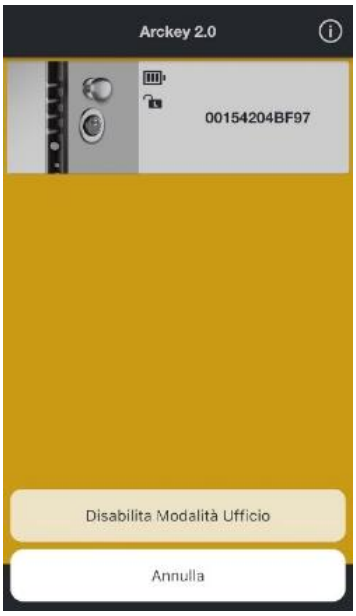


fig.44

Eseguire l'operazione contraria per disabilitare la funzione (fig.44).

Vedi anche pagina 30 per una gestione programmata della modalità ufficio.

MODALITA' MASTERPHONE

Questa funzione permette di entrare in Programmazione direttamente tramite Smartphone, senza l'utilizzo della Admin Card. L'utente diventa di fatto un amministratore.

Toccare e tenere premuto il pulsante bianco che identifica la porta sulla quale si vuole entrare in programmazione eseguendo il login. Comparirà il menù (fig.45).
Eseguire il login premendo Login.

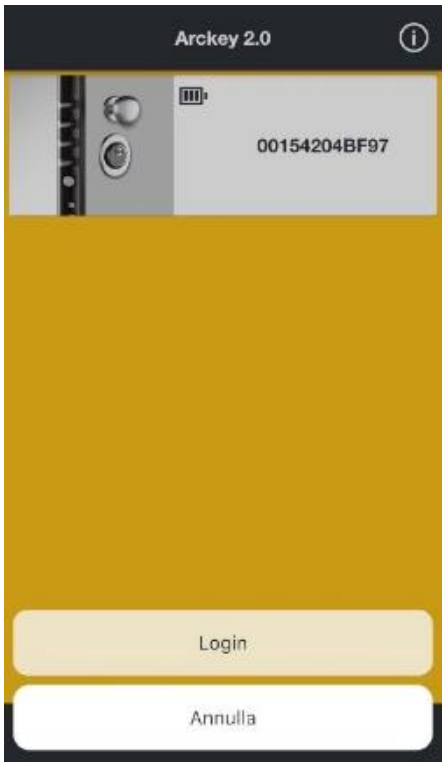
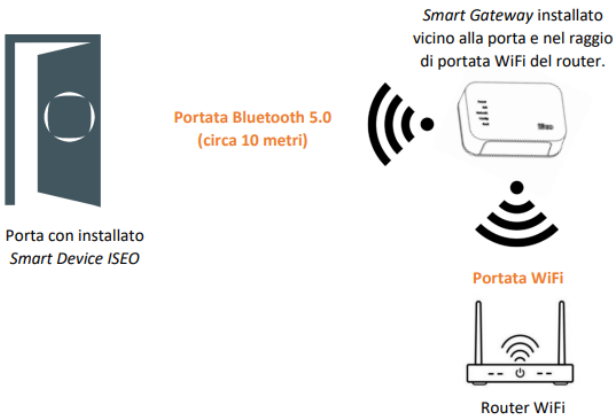


fig. 45

La sicurezza può essere aumentata aggiungendo alla funzione di login un PIN utente (vedi pag.15).
In questo caso il PIN viene richiesto per autorizzare l'accesso.

E' COMUNQUE FORTEMENTE CONSIGLIATO CONSERVARE LE ADMIN CARD PER POTER ACCEDERE IN CASO DI NECESSITÀ O DI SOSTITUZIONE/SMARRIMENTO DEL DISPOSITIVO MASTERPHONE.

DISPOSITIVO GATEWAY



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

LEGENDA LED:

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

BLE (LAMPEGGIA BIANCO): Indica lo stato di Connessione Bluetooth con la serratura. Quando lampeggia significa che sta comunicando con la serratura tramite il Bluetooth.

Network (BIANCO): Indica lo stato di connessione del Gateway con la rete WI-FI- Se spento significa che non è associato a nessuna rete Wi Fi.

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

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

INSTALLAZIONE

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;

Collegare il Dispositivo Gateway all'alimentazione e attendere che smetta di lampeggiare il led rosso "Boot" (fig.46) e rimanga fisso il led "Config" (fig.47). Ora è possibile procedere al rilevamento e all'installazione.

fig.46

fig.47

ATTENZIONE: questa installazione di gestione può essere effettuata da un solo dispositivo (Amministratore Gateway - pag.29). Una volta inizializzato, solamente questo dispositivo può permettere l'utilizzo del Gateway da parte di altri dispositivi.

Attraverso il menù “info” attivare **“Abilita Arckey da Remoto”** (fig.48).

Le funzionalità del Gateway sono utilizzabili anche senza attivare il bluetooth.

fig.48

Ora nella schermata principale è apparsa l’icona in alto a sinistra (fig.49). Una volta premuto si verrà reindirizzati al sito ISEO per la gestione del proprio account.

fig.49

Premere “Registrati”.

fig.50

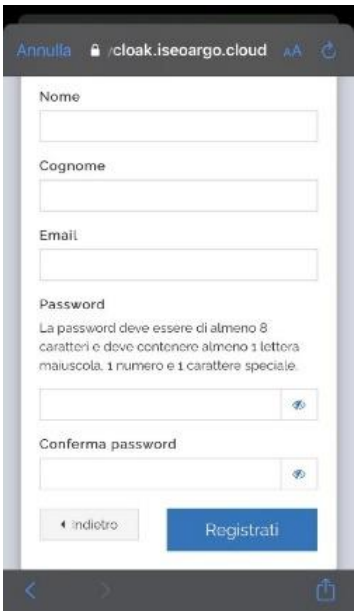


fig.51

Se si possiede già un account ISEO accedere con le credenziali in possesso (fig.50). Altrimenti premere “Registrati” e completare il processo di registrazione al Cloud ISEO (fig.51).

Successivamente accettare termini e condizioni per il trattamento dei dati personali (fig.52).

Una volta completata la registrazione è necessario confermare l’email tramite il proprio account, anche attraverso browser pc (fig.53).

fig.52

fig.53

Una volta confermata la mail è possibile accedere al Cloud Iseo con le credenziali appena registrate (fig.54).

fig.54

Per i successivi utilizzi, se spuntiamo “Ricordami” verranno memorizzate le credenziali e l’accesso al dispositivo sarà automatico.

Siamo correttamente autenticati e connessi. Infatti i bordi dell’app saranno di grigio chiaro e non più scuri.

fig.55

Premere “Configura il tuo sistema” (fig.55)

fig.56

fig.57

fig.58

Premere "Si" se è verificata la situazione descritta (fig.56).

Successivamente verrà chiesto di inserire un codice presente nel retro del Gateway per poterlo associare ad una rete Wifi che servirà al Gateway per comunicare tramite la connessione internet. Può essere fatto inserendo manualmente i codici come in figura (fig.57-58) oppure molto più semplicemente inquadrando il QR code con la fotocamera del proprio dispositivo.

fig.59

fig.60

fig.61

Successivamente viene chiesto di collegare il dispositivo ad una Rete Wifi in prossimità del Gateway (fig.59) e se necessario con una password della rete WiFi (fig.60). Dopo la configurazione compilare il nome della Rete Gateway (fig.61)

Una volta completato l'associazione del Gateway con la rete WiFi devono essere illuminati i led "Power" e Network"(fig.62).

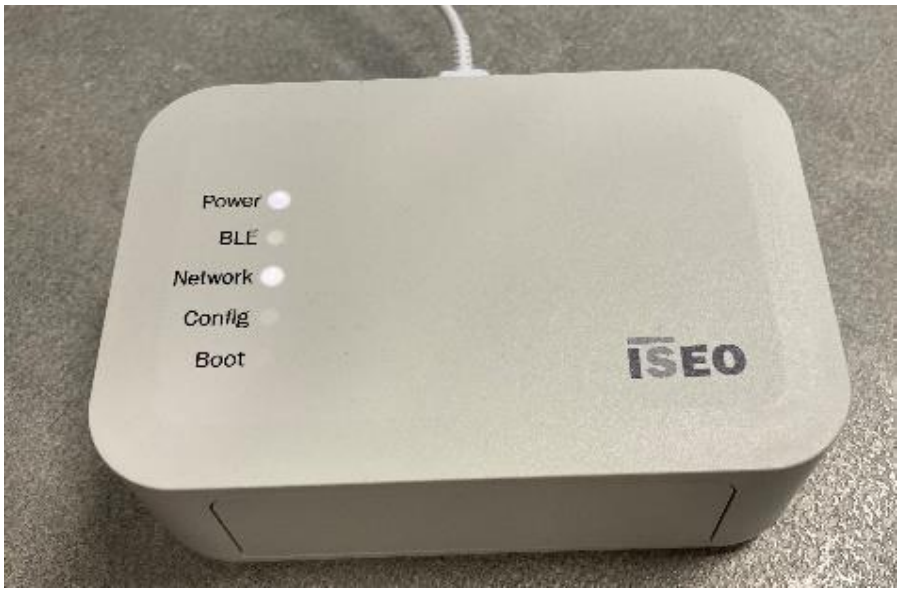


fig.62

AGGIUNGERE SERRATURA CON GATEWAY (NECESSARIA ADMIN CARD)

Ora nella schermata impostazioni Gateway premere su “Serratura “, ”Aggiungi una nuova serratura”. Il dispositivo ricercherà le serrature disponibili all’associazione.

fig.63

Ora è necessario essere di fronte alla serratura e accostare la Admin Card al lettore della serratura che si vuole configurare entro un breve tempo (fig.63). **Utilizzare l’Admin Card in essere (vedi pag.6).**

fig.64

Premere “Aggiungi Serratura” (fig.64) e attendere che l’operazione di associazione sia completata **(non chiudere l’App durante questa operazione)**

fig.65

Attraverso la successiva schermata è necessario impostare una Password Serratura che servirà per l'apertura della serratura da remoto (fig.65). La Password Serratura può essere diversa dalla password del proprio account ISEO.

fig.66

Premere "Aggiungi la prossima serratura" se siamo in presenza di più serrature da configurare con il Gateway oppure "Termina configurazione" per completare l'operazione (fig.66). Attendere che la configurazione sia completata e la serratura verrà aggiunta al nostro elenco delle serrature.

E' presente la possibilità di raggruppare le varie serrature per "Case" e quindi gestire in modo più semplice le diverse serrature disposte in diversi paesi e luoghi del mondo (vedi pag.32).

APERTURA PORTA CON DISPOSITIVO GATEWAY

fig.67

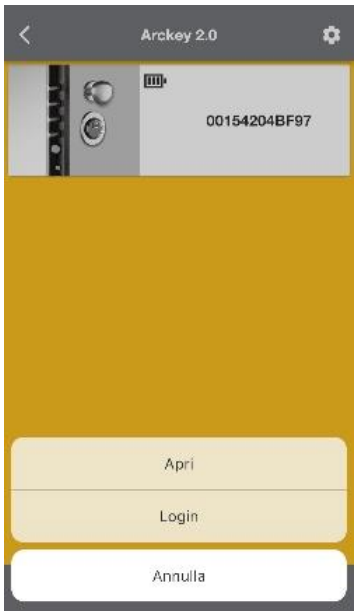


fig.68

fig.69

Premere la serratura desiderata e digitare la Password Serratura (fig.67) (nei dispositivi iOS è possibile settare la propria impronta digitale o Face ID per la compilazione automatica della Password)

Premendo “Apri” (fig.68) e successivamente “Ok” (fig.69) la serratura si aprirà.

Attraverso “Login” sarà possibile:

- Aggiungere, modificare o eliminare Utenti;
- Leggere lo storico Eventi
- Aggiungere Account Utente standard di utilizzo

Aggiungere, modificare o eliminare Utenti:

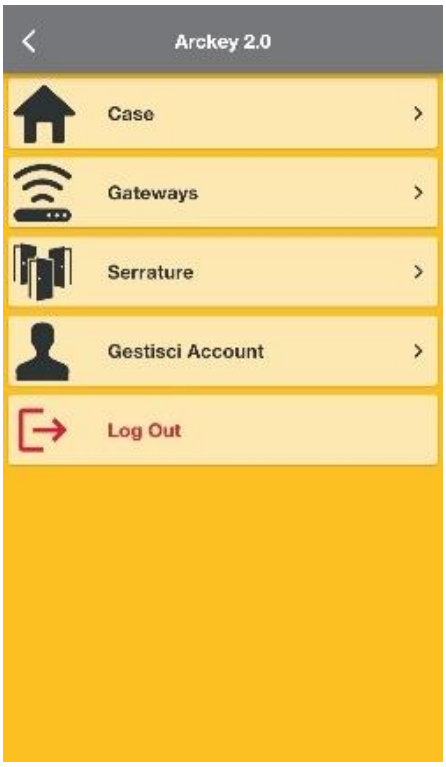
L’interfaccia Utenti in remoto ha le stesse funzionalità dell’interfaccia in locale (pag.17)

Leggere lo storico Eventi

L’interfaccia Eventi in remoto è la stessa dell’interfaccia in locale. Vengono precaricati gli eventi nel proprio dispositivo ed è quindi necessario aggiornare la pagina per caricare gli eventi in tempo reale.

MENU' GATEWAY

Premendo il pulsante ⚙ 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 diversi dispositivi Gateway; se l'icona si presenta con in rosso significa che il Gateway non è connesso a nessuna rete internet. Viceversa se si presenta in verde significa che comunica regolarmente con la rete internet.

- **Serrature:** Permette di aggiungere, rinominare e cancellare diverse 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. 22).**

-**Gestisci Account:** In questa schermata è possibile visualizzare le informazioni relative al proprio account e abilitare o disabilitare il Face ID o il Touch ID presente in alcuni dispositivi che permettono di sostituirsi all'inserimento manuale delle password. E' inoltre possibile modificare la password dell'account e cancellare l'account stesso.

L'Amministratore Gateway

L'Amministratore Gateway è una nuova identità strettamente correlata all'utilizzo dell'App Arckey da Remoto.

L'Amministratore Gateway non deve essere confuso con l'Amministratore Locale; Sono due identità separate che possono comunque coesistere nella stessa serratura. **Arckey prevede che ci possano essere più Amministratori locale ma solamente un Amministratore Gateway.**

L'Amministratore Gateway è fondamentalmente il proprietario del Gateway ovvero primo che ha creato un account nel Cloud ISEO, configurato il Gateway (pag.20) e aggiunto le serrature al proprio account.

Successivamente l'Amministratore Gateway può invitare altri Utenti che possiedono un account nel Cloud ISEO, ad utilizzare il Gateway.

ATTENZIONE: Solo l'Amministratore Gateway può eliminare se stesso.

AGGIUNGERE ACCOUNT UTENTE AL GATEWAY

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

- Accedere ad Arckey Remoto;
- Fare "Login" alla serratura (pag.22)
- 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.

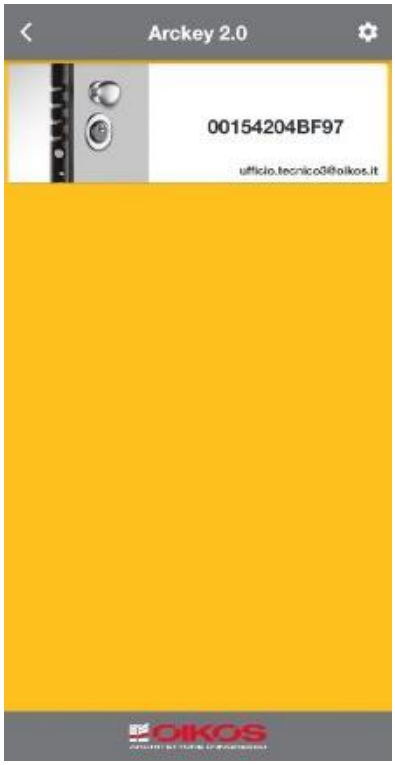


fig.70

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 (fig.70).

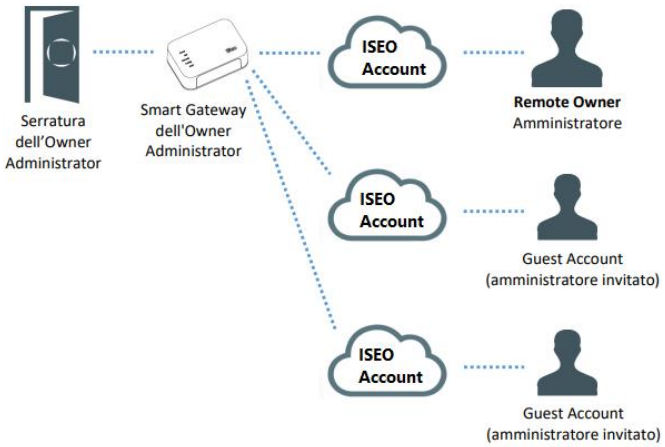
Per aprire la serratura il nuovo Utente dovrà utilizzare la Password TEMPORANEA contenuta nella e-mail di invito.

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 AMMINISTRATORE GATEWAY

Per poter rimuovere l'Account Amministratore del Gateway è necessario cancellare le serrature associate ad essa dal dispositivo.

Questa operazione cancellerà a tutti gli Utenti Invitati la possibilità di accedere al Gateway



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

RESTRIZIONI DI APERTURA

Per ogni utente si possono impostare delle restrizioni temporali all'apertura, intesa come durata o come fascia oraria.

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.71) e assegnare una durata che può essere in giorni/ore/minuti a partire dalla prima apertura della porta (fig.72).
Premere su Fatto in alto a destra.

fig.71

fig.72

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

Attivare la funzione Abilita Controllo Orario (fig.73). In questa configurazione tipo per un'impresa di pulizie, l'utente è abilitato all'utilizzo della serratura dalle 18:00 di venerdì 18 febbraio 2022 quando gli uffici sono vuoti fino alle 08:00 di lunedì 21 febbraio 2022.

fig.73

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 restrizione è attiva.

Esempio: il personale delle pulizie è abilitato all'accesso per un periodo di 20 anni, ma può accedere solo al sabato dalle ore 10 alle ore 12 (fig.74).

fig.74

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.

INFO PORTA

La scheda Info Porta mostra l'elenco di tutte le informazioni relative alla porta associata:

fig.75

Nome Porta: può essere personalizzato sostituendolo al "numero ordine porta" di default.
Il nuovo nome assegnato verrà visualizzato nella schermata di Home della App (fig.75).

Tipo Serratura: indica la tipologia di serratura montata(fig.75).

Livello Batteria: indica il livello di carica delle batterie interne alla serratura: OK, Low, Very Low, End (fig.75).

Livello Admin Card: identifica il livello di sicurezza della card attiva (fig.76).

Utenti in Memoria: Totale degli utenti registrati divisi per categorie (massimo 300) (fig.75).

fig.76

Modalità Ufficio Programmata: Consente di attivare la modalità ufficio a fasce orarie e di impostarne i programmi 1 e 2 (vedi pag.35) (fig.76).

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…) (fig.76).

Versioni: Vengono riportate le versioni dei componenti della serratura (utili in caso di necessità di assistenza) (fig.76).

Funzioni Avanzate: Sono parametri tecnici da utilizzare **solo** su richiesta dell'Assistenza Tecnica.

Si sconsiglia l'uso a personale non tecnico.
La modifica dei parametri contenuti all'interno delle funzioni avanzate può modificare o compromettere il funzionamento della serratura.

MODALITA' UFFICIO PROGRAMMATA

Questa funzione permette di impostare due programmi, per abilitare e disabilitare automaticamente la Modalità Ufficio. Questo significa che la serratura andrà automaticamente in Modalità Ufficio, seguendo fino a due programmi impostati.

Entrare in programmazione ed aprire "Info Porta".
Abilitare Programma 1 per iniziare la configurazione. (Per il Programma 2 valgono le stesse regole).
A seconda delle necessità, si possono impostare 3 modalità differenti d'uso della modalità ufficio:

fig.77

fig.78

fig.79

Modalità Ufficio con Richiusura Automatica:

In questa modalità l'attivazione avviene manualmente da un utente abilitato, ma si può programmare la richiusura automatica ad una certa ora.
Selezionare l'orario di richiusura automatica ed i giorni per i quali la programmazione è valida (Lo standard proposto è feriali, ovvero tutti i giorni eccetto sabato e domenica).
Premere Fatto per confermare (fig.77).

Modalità Ufficio con Attivazione Automatica e Richiusura Automatica:

In questa modalità sia l'attivazione che la richiusura avvengono in modo automatico. Selezionare l'orario di attivazione automatica, l'orario di richiusura automatica ed i giorni per i quali la programmazione è valida. Lo standard è feriali, ovvero tutti i giorni eccetto sabato e domenica (fig.78).

Modalità Ufficio con Attivazione Automatica con Primo Ingresso e Richiusura Automatica (C):

Come il punto precedente solo che la reale attivazione della modalità ufficio avverrà con l'ingresso del primo utente abilitato. Questa soluzione è molto utile per la sicurezza, perché evita che una serratura vada in Modalità Ufficio automaticamente, quando non c'è alcun utente all'interno dell'edificio o della stanza (per esempio il giorno di Natale

potrebbe cadere in una giornata in cui è programmata la modalità ufficio automatica, ma in questo caso non si dovrebbe attivare!) (fig.79).

EVENTI

La scheda Eventi visualizza l'elenco degli ultimi 1000 eventi relativi alla porta (fig.80)
Come Eventi si intende qualsiasi azione meccanica, elettrica o elettronica avvenuta nella serratura.

fig.80

È possibile effettuare una ricerca rapida digitando il valore desiderato nell'apposito campo Cerca dopo aver cliccato sull'icona in modo da filtrare gli eventi (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.

UTILITY

Nella scheda Utility è possibile accedere a funzioni di manutenzione:

fig.81

Spedire Utenti Selezionati: Gli utenti copiati nella memoria del telefono possono essere trasferirti in un altro dispositivo.
Entrare in programmazione della serratura nella quale si vuole copiare gli utenti (vedi pag. 7).
Entrare in Utility e premere il tasto Spedire Utenti Selezionati (fig.81).
Cliccare OK sulla richiesta di conferma (fig.82).

fig.82

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.

E' consigliato scaricare sempre tutti gli aggiornamenti rilasciati da Oikos per mantenere il sistema allineato ai massimi standard di sicurezza e prestazioni.

Dump Information: consente di inoltrare via e-mail tutti i dati di diagnostica della serratura. Da utilizzare SOLO se specificatamente richiesto dal Centro di Assistenza Oikos.