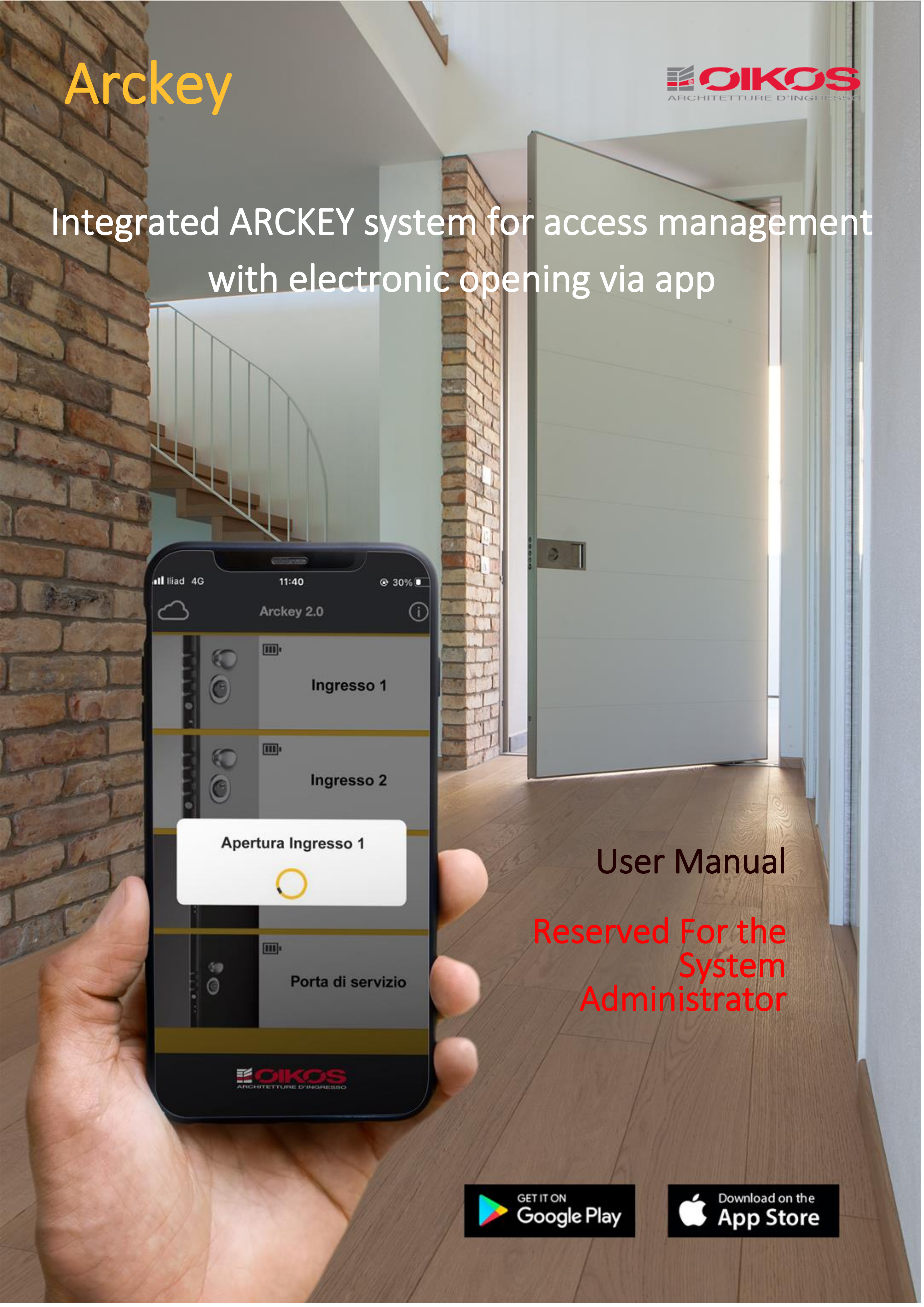
Arckey

OIKOS
ARCHITETTURE D'INGRESSO

Integrated ARCKEY system for access management with electronic opening via app



User Manual

Reserved For the System Administrator

GET IT ON Google Play

Download on the App Store

INDEX

WHAT IS ARCKEY?

Arckey is an integrated access management system with electronic opening.
Through the Arckey App, available for Smartphone, as well as for Android and iOS tablets, it is possible to interact with compatible locks and configure permissions and access modes up to a maximum number of 300 users, divided among Smartphone, RFID Card (e.g., credit card, subway card, etc.), PIN combinations, fingerprints, invitations and remote control.
Through the app the system the administrator can, in an easy and intuitive way, not only add, edit or delete system users but also configure access rules by dividing users between standard and "VIP" users, assigning access time slots, credentials time durations and much more.
The administrator is also enabled to copy users from one lock to another and to supervise any activity of the opening device by consulting the list of the last 1000 events that have occurred.

OPERATING REQUIREMENTS

The Arckey App can be downloaded for free from the App Store (iOS) or from Google Play (Android).

Available on the App Store
ANDROID APP ON Google play
DOWNLOAD
OIKOS ARCHITETTURE D'INGRESSO
Arckey

Arckey is compatible with the following devices:

iOS starting from iPhone 7 and operating system version 7.0 or later
Android starting from version 4.3 (Jelly Bean) or later.

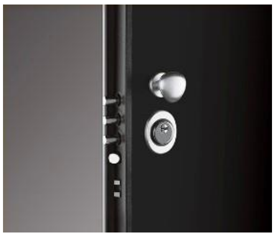
The Arckey App works in combination with the motorized electronic lock, mounted in the Oikos door.
The lock incorporates an electric motor controlled by a powerful state-of-the-art microprocessor.
In case of power failure (from the battery or mains supply), the dead bolt enabling is always ensured by the traditional mechanical key movement.

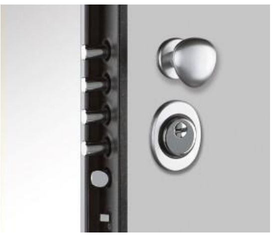
Before starting to use Arckey, you should always make sure that the Bluetooth on your device is enabled.

BLUETOOTH 5.0

As of early 2022, the use of locks with Bluetooth 5.0 technology has been deployed; this new technology offers improved performance and the ability to use the Gateway to control the lock remotely (see "Gateway Device" on p.20)

To know if your lock is a Bluetooth 5.0 one, simply check the lock icon on the main screen of the App:


Lock icon with older Bluetooth versions

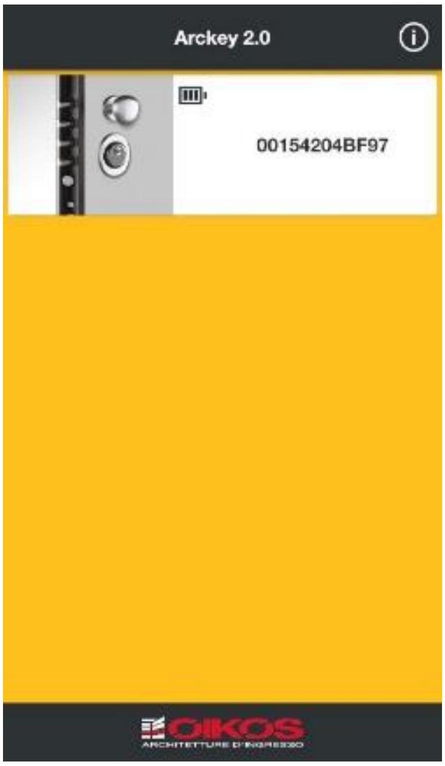

Lock Icon with Bluetooth 5.0

LOGIN CREDENTIALS

Access from the outside can be performed as follows:

Opening using a smartphone or a tablet via App:

Clicking on the **App white button** on the main screen from a smartphone or a tablet will execute the lock opening command (fig.1)



Arckey 2.0

00154204BF97

fig.1

Opening using a card or a transponder:

By approaching a transponder key (fig.2), an Oikos Card (fig.3) or a Card with RFID technology (fig.4) (e.g. a credit card, subway card, etc.) to the external reader or the touchpad the lock will execute the open command.

RFID cards must be 13.56 Mhz Mifare compatible and generally require a closer reading (fig.2)

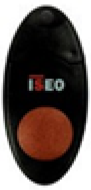


fig.2

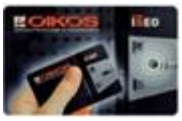


fig.3

fig.4

Opening using a PIN Code (only with numeric keypad or touchpad):

By entering the numeric code (minimum 4 and maximum 8 characters) followed by the ENTER key ↵ the lock will execute the opening command (fig.6-7).

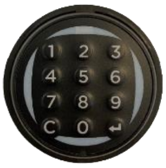


fig.6

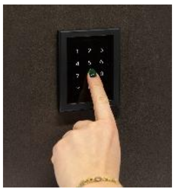


fig.7

Opening by reading the fingerprint:

If the fingerprint reader is installed in the door, by placing the finger whose fingerprint has been saved gives the lock the command to open (fig.8)

fig.8

Remote opening via Gateway device:

If the Gateway device (fig.9) is installed in the door (see p. 20), through the App it will be possible to open the door or check the status of the door from anywhere in the world without necessarily being near it.

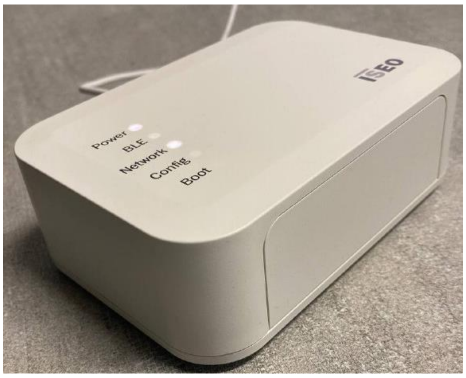


fig.9

CAUTION: The Gateway Device can only be installed in a lock featuring the Bluetooth 5.0 technology (see chapter "Bluetooth 5.0" p.2)

ARCKEY FIRST COMMISSIONING

Before starting to use the App, remember to enable the Bluetooth function on your smartphone.

When starting the App, on the smartphone display all available locks within range of the Bluetooth signal are displayed (fig.10). Upon the first access, the door number will correspond to the used internal order number. We recommend renaming it (see p.33 "Door Info").

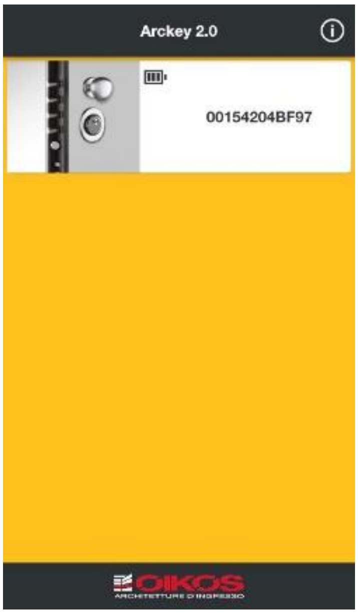
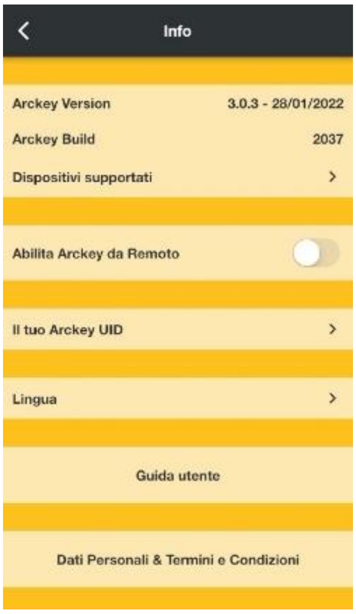


fig.10

Clicking on the Info icon ⓘ on the upper right corner, the data on the App version and on the software of supported devices is provided. It is also possible to change the language for using the App, for displaying the user guide in the chosen language, and enabling and disabling the Remote Access (fig.11).



Info

Arckey Version	3.0.3 - 28/01/2022
Arckey Build	2037
Dispositivi supportati	›
Abilita Arckey da Remoto	○
Il tuo Arckey UID	›
Lingua	›

Guida utente

Dati Personali & Termini e Condizioni

fig.11

ADMIN CARD

Admin Cards allow the administrator to enter the programming mode to configure and manage the Oikos Arckey access control system.

CAUTION: The set of 3 Admin Cards is factory sealed upon completion of internal quality checks.
The Admin Cards provided allow you to become the sole administrator of the system and perform the operations described in this manual. Keep them carefully stored and avoid losing them!

The system (OIKOS Security Code System) provides three security levels for the access to the lock operating parameters. Each security level corresponds to a different color Admin Card:

Green Admin Card - Level 1
Gray Admin Card - Level 2
Red Admin Card - Level 3

Upon its first use, it will be possible to access the Arckey system programming mode by placing the Green Admin Card close to the external reader.
At any time, if you lose control (for example through theft or loss) of the green Admin Card, you can switch to the gray security level by simply placing the next level gray Admin Card close to the door reader. An audible signal confirms the reading, and the operation of the green Admin Card will be stopped. Wait for the second confirmation beep after 10 seconds.

At any time, if you lose control of the Gray Admin Card, simply by placing the Red Admin Card close to the door (an audible signal confirms that it has been read) you will stop the operation of the Gray Admin Card. Wait for the second confirmation beep after 10 seconds.

Any loss of the Red Admin Card hinders any possibility of being able to enter the programming mode to manage the Arckey system functionalities.

It is therefore recommended that, having reached this point, you immediately apply for a new Admin Card kit (Green-Grey-Red).

Placing the Green Admin Card of the new kit close to the door (an audible signal confirms that it has been read) will stop the operation of the old kit, thus restoring the original functionality.
Wait for the second confirmation beep after 10 seconds.

When switching from one Admin Card to the next, all system and user settings remain unaffected.

ENTERING THE PROGRAMMING MODE

Enable the Bluetooth function on your device.

Open the Arckey App.

Place the Admin Card close to the door external reader (or touchpad or hidden reader).

The reader will emit a confirmation light and sound signal; at the same time, in the App, the white button identifying the door will turn red (fig.12)

Click on the lock.

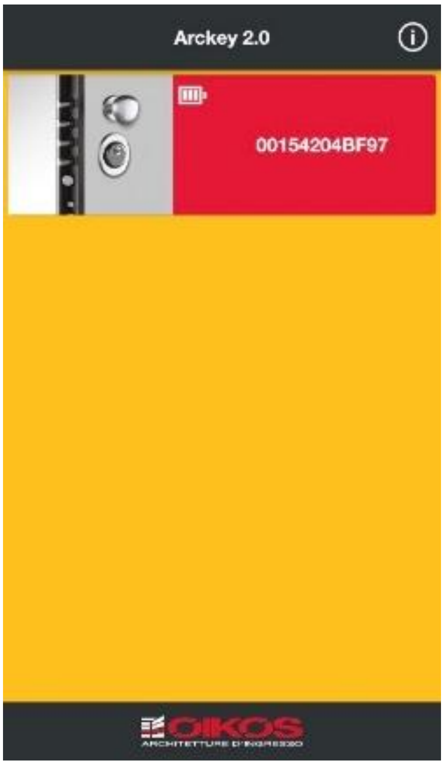
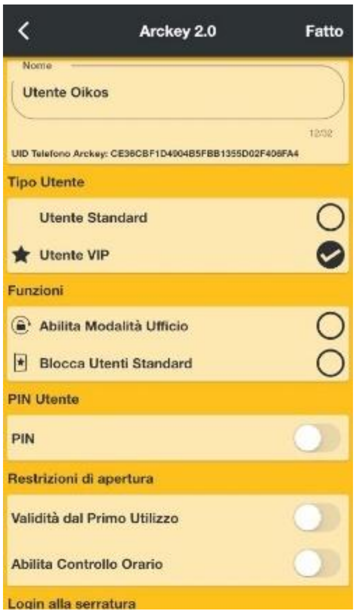


fig.12

CAUTION: During the use of the Programming Mode and of all its internal functions, it is not possible to close the App or put it on standby and the connection with the lock will be lost.

ADDING A SMARTPHONE AS LOGIN CREDENTIAL

After pairing, you will be asked to add the smartphone as a credential to open the lock (fig.13).
This operation must be performed for each smartphone you wish to save on the lock.



Arckey 2.0 Fatto

Nome: Utente Oikos
12/32
UID Telefono Arckey: CE36CBF1D4904B5FBB1355D02F406FA4

Tipo Utente
- Utente Standard ○
- Utente VIP ●

Funzioni
- Abilita Modalità Ufficio ○
- Blocca Utenti Standard ○

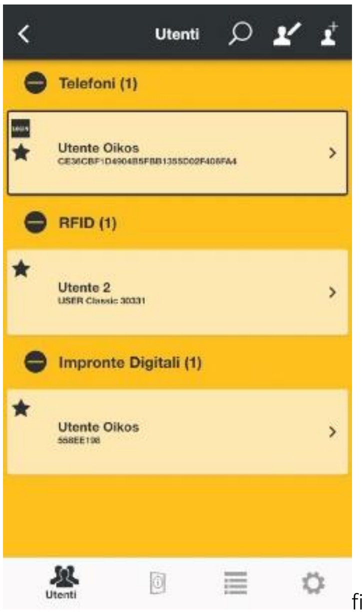
PIN Utente
- PIN ○

Restrizioni di apertura
- Validità dal Primo Utilizzo ○
- Abilita Controllo Orario ○

Login alla serratura

fig.13

If you wish so, change the smartphone ID name and click on Done on the upper right corner. Now the device appears in the tab of the users registered and enabled to open the door (fig.14).
Individual functions will be explained in detail below.



Utenti

Telefoni (1)
- Utente Oikos
  CE36CBF1D4904B5FBB1355D02F406FA4

RFID (1)
- Utente 2
  USER Classic 30331

Impronte Digitali (1)
- Utente Oikos
  558EE198

fig.14

The Users tab displays the list of all users associated with the door, divided by access system: smartphones and tablets, cards (Oikos card, cards with RFID technology, transponder key), PINs, fingerprints and invitations.

OPENING THE DOOR

Exit the programming mode by clicking on the icon on the upper left corner.

Click on the white banner identifying the door to send an opening pulse to the lock. The lock will retract the dead bolts.

USER SAVING

Saving the Oikos Card, transponder key, card with RFID technology

Enter the programming mode (see p. 7).

Once inside the user list, place the key or the card close to the door external reader. Wait for the confirmation signal.

The card will now appear in the user list confirming that it has been saved.

Manual addition of cards and PINs

It is possible to add cards even without physically holding them, saving them through their code (fig.14).

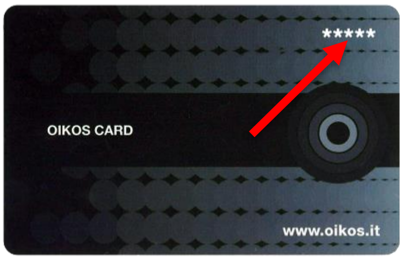


fig.14

This function is useful when, for example, the cards have already been distributed to users.

Enter the programming mode (see p. 7).

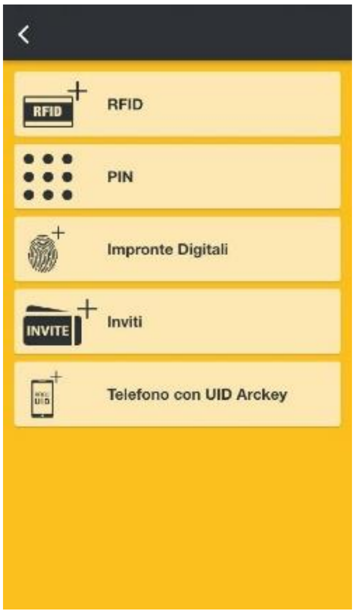


fig.15

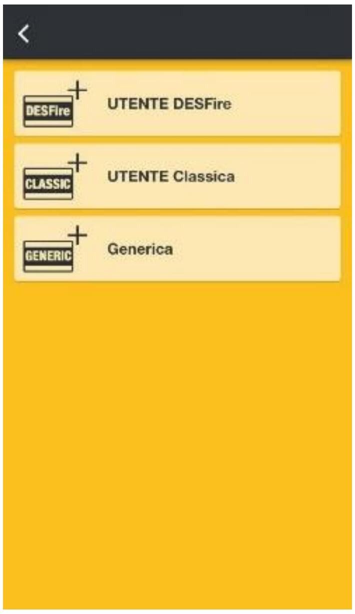
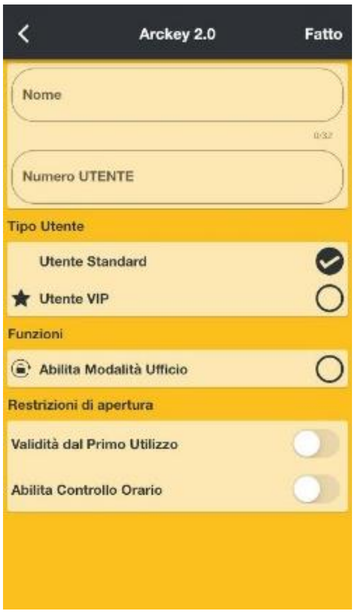


fig.16



Nome

Numero UTENTE

Tipo Utente

Utente Standard ●

★ Utente VIP ○

Funzioni

Abilita Modalità Ufficio ○

Restrizioni di apertura

Validità dal Primo Utilizzo

Abilita Controllo Orario

fig.17

Click on the Add user icon on the upper right corner and choose what type of use you want to enter (fig.15):

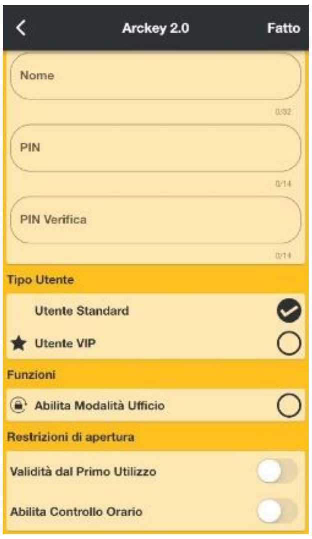
DESfire Card, Classic User Card or Generic RFID Card (fig.16).

Enter a name and the ID number shown on the card (fig.17). Click on Done on the upper right corner.

Saving the PIN code (only if a numeric keypad is available)

Enter the programming mode (see p. 7).

Once inside the user list, type in the numeric code (minimum 4 and maximum 8 characters) followed by the ENTER key ↲. Wait for the confirmation signal. The PIN code will appear in the user list confirming that it has been saved.



Arckey 2.0 Fatto

Nome 0/32

PIN 0/14

PIN Verifica 0/14

Tipo Utente

Utente Standard ●

Utente VIP ○

Funzioni

Abilita Modalità Ufficio ○

Restrizioni di apertura

Validità dal Primo Utilizzo

Abilita Controllo Orario

fig.18

If you want to add a PIN code without typing it on the keypad, click on PIN, assign a name and type the code twice, in the PIN and PIN verification fields. The code must be at least 4 digits long. Click on Done (fig.18).

Caution: For security reasons, PIN codes are never visible in plain text in the App

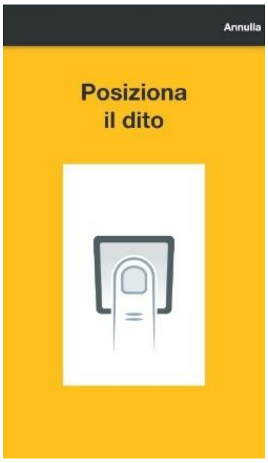
Saving fingerprints (only when a fingerprint reader is available)

Enter the programming mode. With the fingerprint reader, it is necessary to place the Admin Card close to the hidden reader.

Click on the add user icon on the upper right corner (fig.14) and choose Fingerprints .

The fingerprint reader will start flashing. Place your finger on the reader, as indicated by the animation (fig.19).

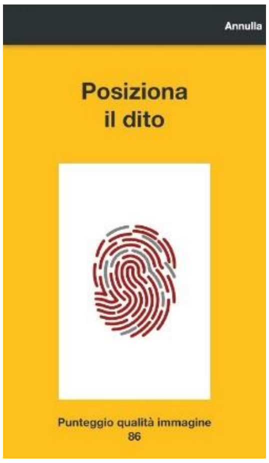
The App will ask you to perform the fingerprint reading several times in order to get a good quality recording (fig.20).



Annulla

Posiziona il dito

fig.19

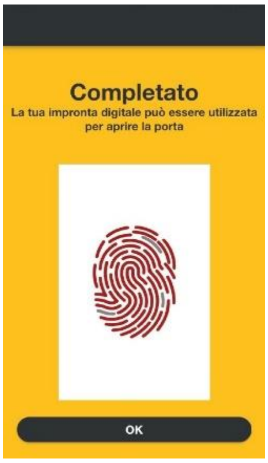


Annulla

Posiziona il dito

Punteggio qualità immagine 86

fig.20

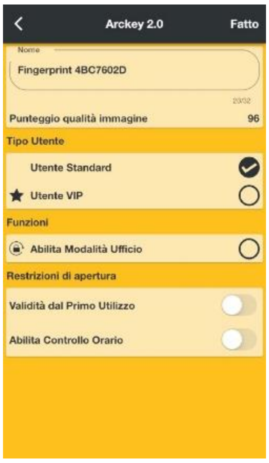


Completato

La tua impronta digitale può essere utilizzata per aprire la porta

OK

fig.21



Arckey 2.0 Fatto

Nome: Fingerprint 4BC7602D 20/32

Punteggio qualità immagine 96

Tipo Utente

Utente Standard ●

Utente VIP ○

Funzioni

Abilita Modalità Ufficio ○

Restrizioni di apertura

Validità dal Primo Utilizzo

Abilita Controllo Orario

fig.22

Click on OK (fig.21). Then it is possible to change the user name and other settings. Once the process has been completed, press "Done" (fig.22).

Now the fingerprint is recognized as a valid credential to open the door.

Caution: For a proper reading, the finger must be resting on the reader and not swiping on it.

The fingerprint reading may be made more difficult by factors such as excessive moisture on the finger or reader surface, insufficiently clean reader surface, poor fingertip readability, etc.

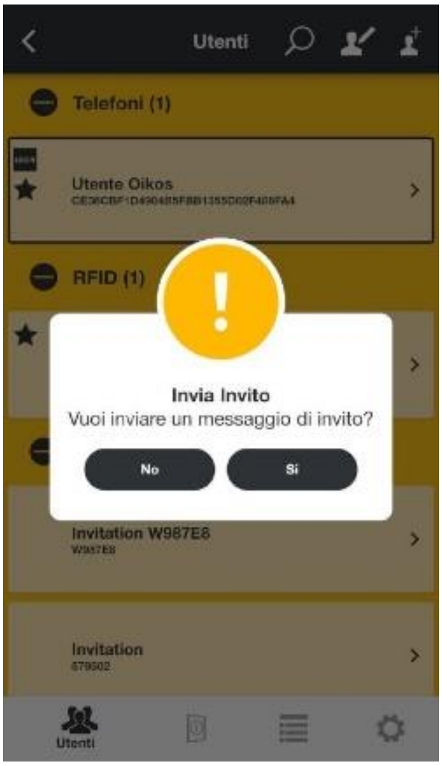
Saving Invitations

Invitations allow a user (smartphone or tablet), to self-register in the lock memory as an access-enabled user, using an invitation code previously saved in the lock by the Administrator.

For example, the Invitations feature allows the manager of a Bed and Breakfast to be able to enable access to a guest, even before he or she arrives at the facility.
To do this, the Administrator previously added an Invitation Code to the lock memory, which will be sent to the person to whom the manager is to grant access.

What the Administrator must do to create an invitation:

Enter the user programming mode. Click on the "Add User" icon 👤+ and then on Invitations INVITE+ .
The user configuration screen opens.
Enter a name that identifies this invitation and possibly set the desired parameters.
Press **Done** to confirm.
You are asked if you want to send an invitation message (fig.23).
Press Yes to send it immediately, or No if you want to send it later.



Invia Invito
Vuoi inviare un messaggio di invito?

fig.23

A text is automatically generated with a step-by-step explanation of how to use the invitation to access the door. Also, access validity information is reported, if any.
Instructions can be sent via e-mail or through a messaging program (Skype, WhatsApp, Telegram, etc.). The invitation now appears in the invitation list. From here it is possible to resend the invitation, if necessary.

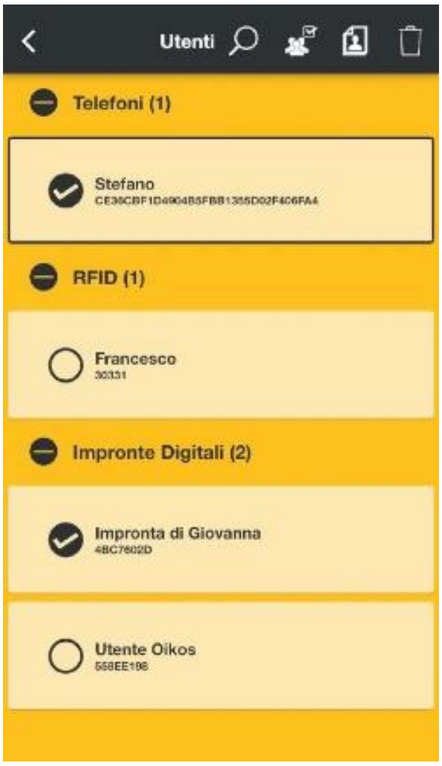
What should the user who receives the invitation do:

The user who receives the invitation must first of all download and install the App on his or her device.
With the enabled Bluetooth and the Oikos Arckey App started, the user must get closer to the door so that the lock can be detected. Clicking on the white button identifying the door prompts the entering of the previously received invitation code.

The door opens and the smartphone now appears among the list of the registered smartphones.
The invitation, as "accepted", disappears from the invitation list.

DELETING AND SAVING USERS

Click on the Edit icon on the upper right corner (fig.14).
Select the user to be deleted or saved (fig.24) or press the icon to select them all (caution! this will delete/save all users).
Press on the bin icon to confirm the deletion or on to save the selected users or create a backup. Users will be saved in the smartphone and can be retrieved if needed or duplicated on another lock without having to reconfigure them all over again.



Telefoni (1)

● Stefano
CE36CBF1D4904B5FBB1355D02F406FA4

RFID (1)

○ Francesco
30331

Impronte Digitali (2)

● Impronta di Giovanna
4BC7602D

○ Utente Oikos
558EE198

fig. 24

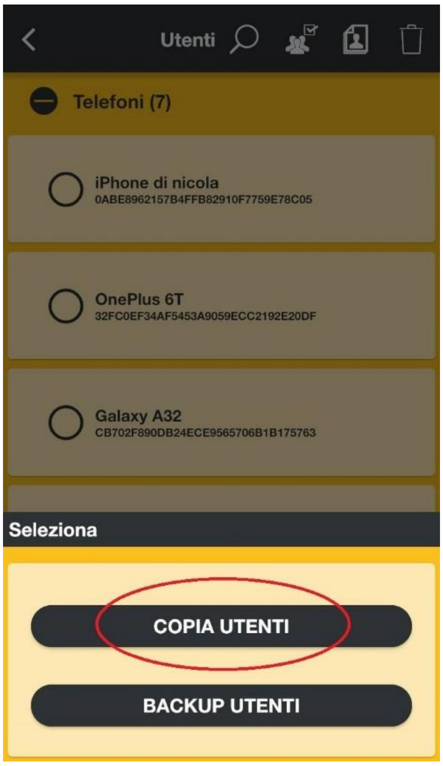
Quick deletion of a user:

From the list of users: on Android systems, keep pressed the user to be deleted. On iOS systems "swipe" the user to the right.
Confirm the deletion.

Copy Users

Operation to be carried out if you want to quickly copy multiple users with their access setting, from one lock to another using the same device:

- Select and choose which types of users to copy (all or only those without "LOGIN" function);
- Press and choose "COPY USERS" (fig.25);



Telefoni (7)

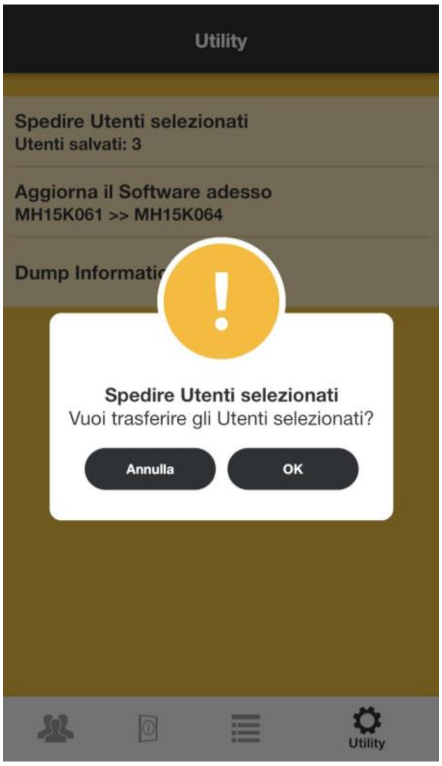
○ iPhone di nicola
0ABE8962157B4FFB82910F7759E78C05

○ OnePlus 6T
32FC0EF34AF5453A9059ECC2192E20DF

○ Galaxy A32
CB702F890DB24ECE9565706B1B175763

fig.25

- Press copy; the users are now saved on the smartphone;
- Enter Programming Mode (see p.7."Entering Programming Mode") and choose the lock in which you want to register the users;
- Press Utility ⚙
- Press "Send Selected Users" and then press"OK" (fig.26)



Spedire Utenti selezionati
Utenti salvati: 3

Aggiorna il Software adesso
MH15K061 >> MH15K064

Dump Informatic

Spedire Utenti selezionati
Vuoi trasferire gli Utenti selezionati?

fig.26

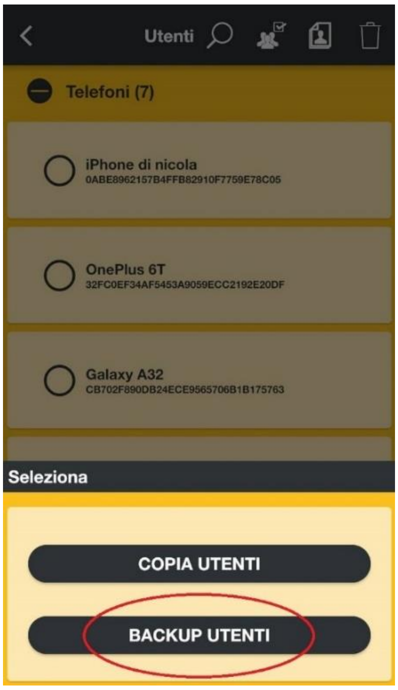
- A message will then appear confirming that the transfer was successful

Now if you access the "Users" section of that lock, all the users copied from the previous lock will be registered.

Users Backup

Operation to be carried out if it is necessary to make a backup of the users with their access settings for a future recovery.

- Select and choose which types of users to copy (all or only those without “LOGIN” function);
- Press and choose “USERS BACKUP” (fig.27).



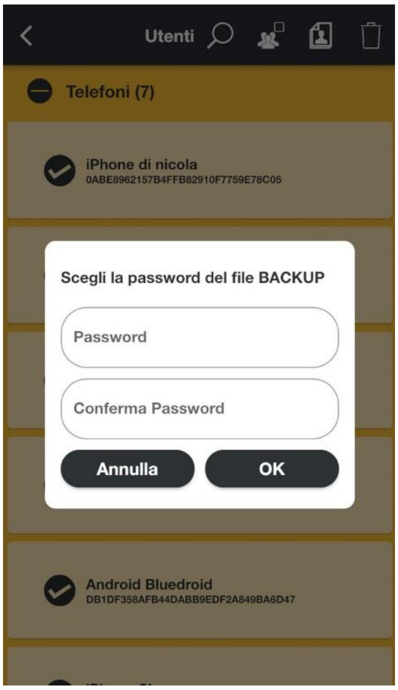
iPhone di nicola
0ABE8962157B4FFB82910F7759E78C05

OnePlus 6T
32FC0EF34AF5453A9059ECC2192E20DF

Galaxy A32
CB702F890DB24ECE9565706B1B175763

fig.27

- Press USERS BACKUP; now the users and their settings are included in a backup file
- enter a password to associate with the backup file (fig.28). This password is used to restore the backup;



iPhone di nicola
0ABE8962157B4FFB82910F7759E78C05

Scegli la password del file BACKUP

Android Bluedroid
DB1DF358AFB44DABB9EDF2A849BA6D47

fig.28

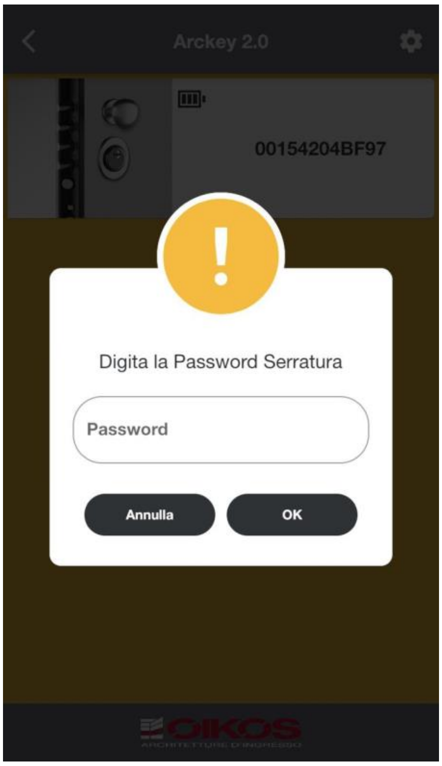
- Choose the destination and method of sending the file (email, whatsapp ecc);

Now a password protected digital file has been created containing the backup of all the selected users, with their respective settings

User Backup Restore

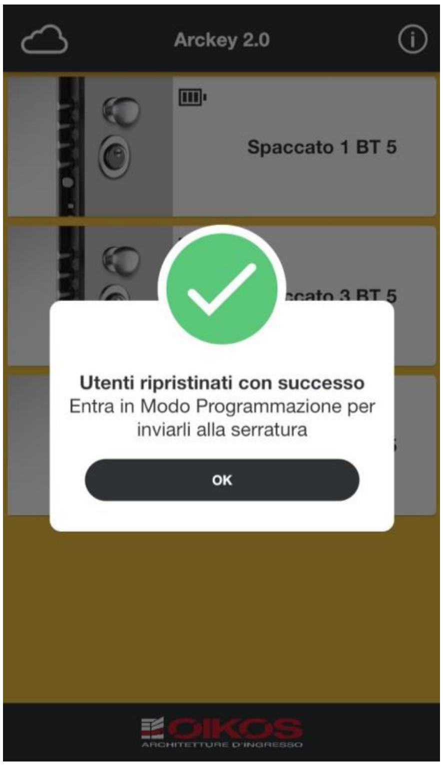
Operation to be carried out to restore users and their access settings from a previous backup (see "User Backup").

- Select the file to restore and open it with the Arckey App of the device to be restored;
- Enter the password (fig.29) for restoring the backup (this password is the one chosen when creating the backup file); A message will appear informing us to enter programming in the lock where we must enter the saved users (fig.30);



Digita la Password Serratura

fig.29



Utenti ripristinati con successo
Entra in Modo Programmazione per inviarli alla serratura

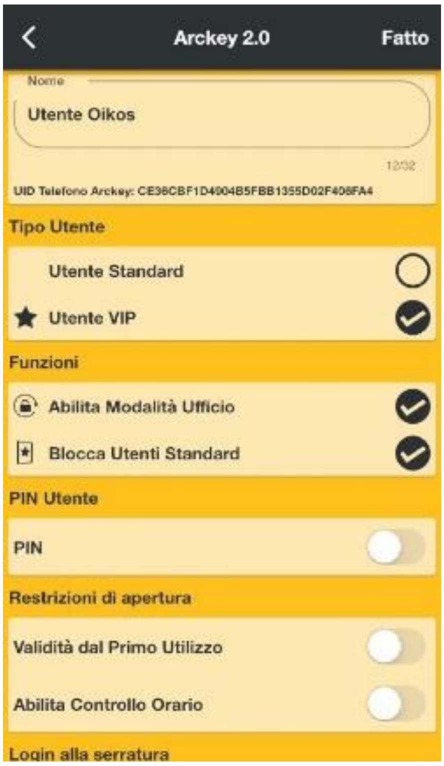
fig.30

- Enter Programming Mode (see pag.”Entering Programming Mode”) of the lock that we want to restore;
- Press Utility; ⚙
- Press “Send Selected Users” and then press“OK”;
- A message will then appear confirming that the transfer was successful

USER SETTINGS

From the user list, select the user to be set up.

Each type of user (smartphone, card, PIN, fingerprint reader, invitation) can have the same functions and settings, except where specified below.



Arckey 2.0 Fatto

Nome

Utente Oikos

12/32

UID Telefono Arckey: CE36CBF1D4904B5FBB1355D02F406FA4

Tipo Utente

Utente Standard ○

★ Utente VIP ✓

Funzioni

Abilita Modalità Ufficio ✓

Blocca Utenti Standard ✓

PIN Utente

PIN ○

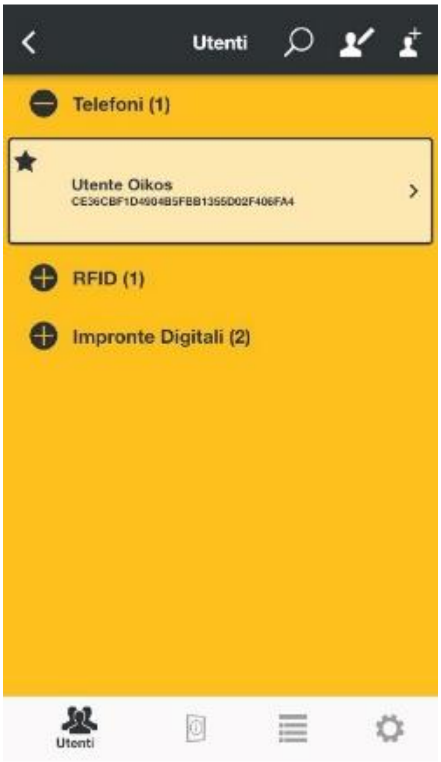
Restrizioni di apertura

Validità dal Primo Utilizzo ○

Abilita Controllo Orario ○

Login alla serratura

fig.31



Utenti

Telefoni (1)

★ Utente Oikos
CE36CBF1D4904B5FBB1355D02F406FA4

RFID (1)

Impronte Digitali (2)

fig.32

Username: Click on the Name field to assign an identifying name to the smartphone or tablet (maximum 32 characters) (fig.31).

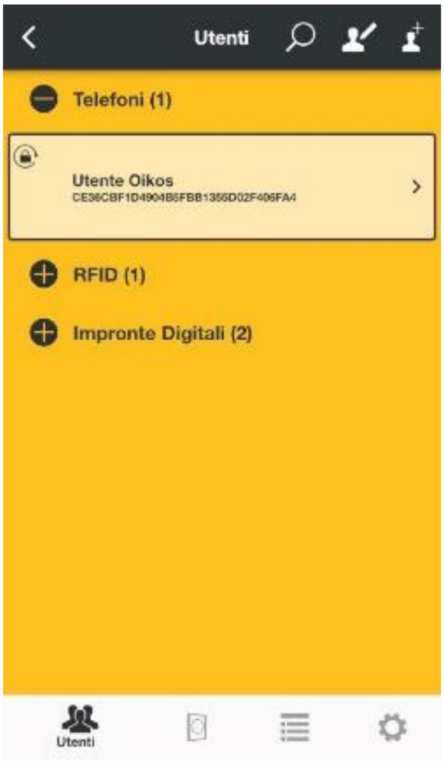
User type: Select whether the user will be a standard or VIP one (fig.31).

VIP user: can always open the door, without any limitations. These users can be assigned the power to block standard users. They can also enable the Office Mode (see p. 18).

Standard User: their access can be disabled by VIP users. These users can enable the Office Mode (see p. 18).

In the user list, the VIP user is identified by the symbol ★ (fig.32)

Functions: This setting allows the user to be assigned the ability to enable the Office Mode (see p. 18) and block access to standard users (see p. 17) (fig.31). Only VIP users can block access to standard users. The ability to activate the Office Mode is indicated with the icon 🔓 (fig.33), the ability to lock out standard users is indicated with the icon ★ (fig.34).


Utenti

Telefoni (1)

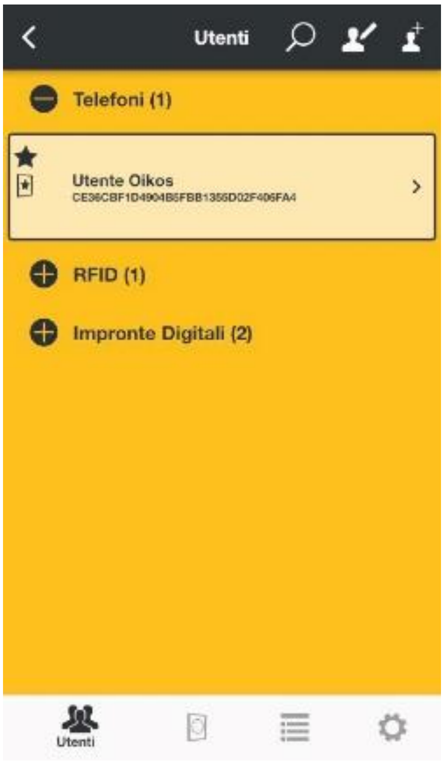
Utente Oikos
CE36CBF1D4904B5FBB1355D02F406FA4

RFID (1)

Impronte Digitali (2)

Utenti

fig.33


Utenti

Telefoni (1)

Utente Oikos
CE36CBF1D4904B5FBB1355D02F406FA4

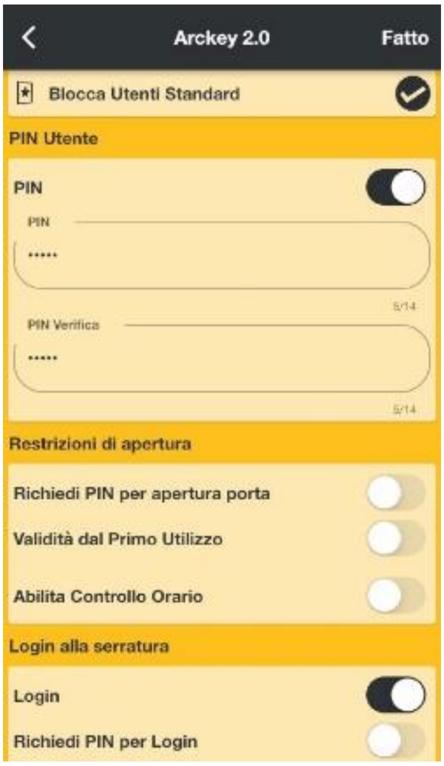
RFID (1)

Impronte Digitali (2)

Utenti

fig.34

User PIN (only for smartphone type users): Access via the user smartphone can be further secured by requiring a PIN to be entered on the smartphone keypad when the door is opened, if configured in the opening restrictions (fig.35).


Arckey 2.0 Fatto

Blocca Utenti Standard ✓

PIN Utente

PIN ●

PIN
•••••
5/14

PIN Verifica
•••••
5/14

Restrizioni di apertura

Richiedi PIN per apertura porta ○

Validità dal Primo Utilizzo ○

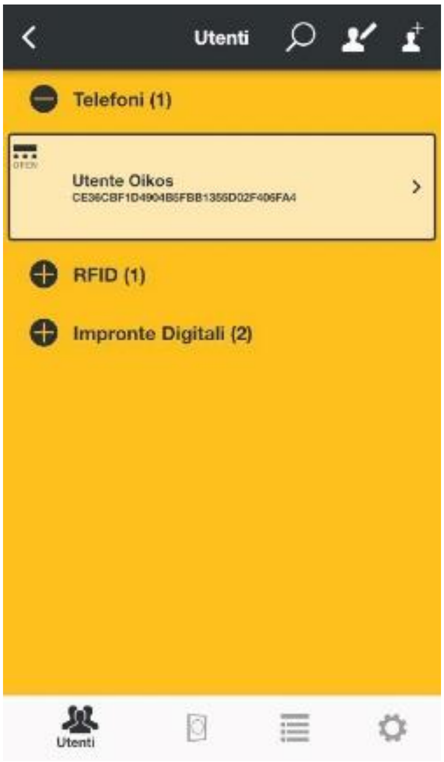
Abilita Controllo Orario ○

Login alla serratura

Login ●

Richiedi PIN per Login ○

fig.35


Utenti

Telefoni (1)

OPEN
Utente Oikos
CE36CBF1D4904B5FBB1355D02F406FA4

RFID (1)

Impronte Digitali (2)

Utenti

fig.36

The presence of a user PIN is indicated by the icon OPEN (fig.36).

Opening restrictions: This setting allows restricting the opening for users. Restrictions can be assigned to each user, for example, to limit their validity in time to a duration in days starting from the first access or to a predefined time slot (example: service personnel can only access a certain day of the week at a certain time). Two time slots are programmable for each user.

If present, an opening restriction is indicated by the icon 🕘 (fig.37)

Masterphone mode (for smartphone type users only): Masterphone mode allows the smartphone type user to be able to enter the programming mode without having to show the Admin card, which is replaced by the smartphone. In this way the user becomes actually an administrator.

If configured, the use of the Masterphone mode can be further secured by activating a user PIN.

The enabling of the Masterphone function is indicated by the icon LOGIN (fig.38)

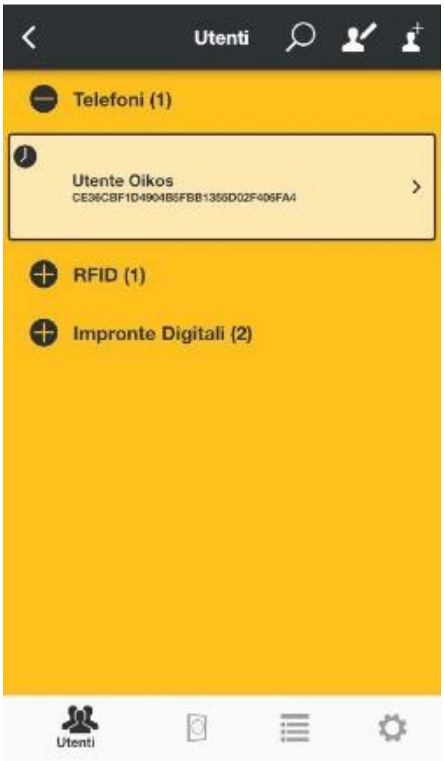


fig.37

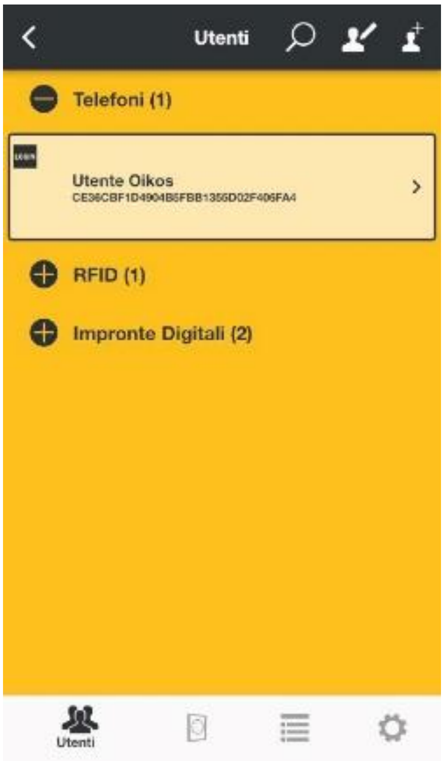


fig.38

STANDARD USER BLOCK

This function, when enabled, prevents all Standard users from accessing the door.
When the "Standard User Block" setting is enabled, only VIP Users will be able to open the door.

To be able to use this function, **it is not necessary to enter the programming mode**.

Touch and keep pressed the button identifying the door on which you want to enable the Standard User Block function. The menu to enable/disable this function will appear (fig.39).

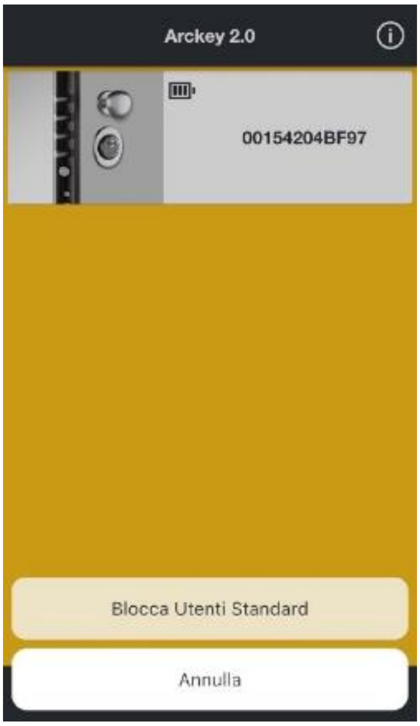


fig.39

A symbol will appear in the white button ★ indicating the enabled function (fig.40). Perform this operation in the opposite order to disable this function (fig.41).

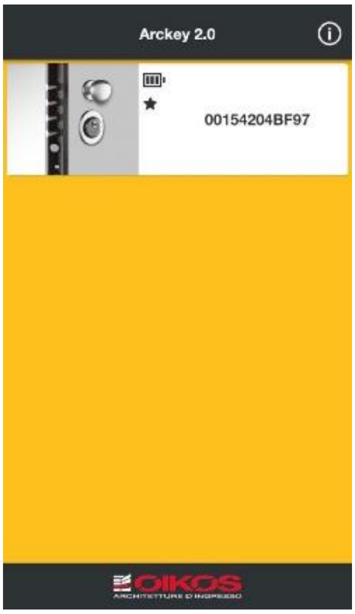


fig.40

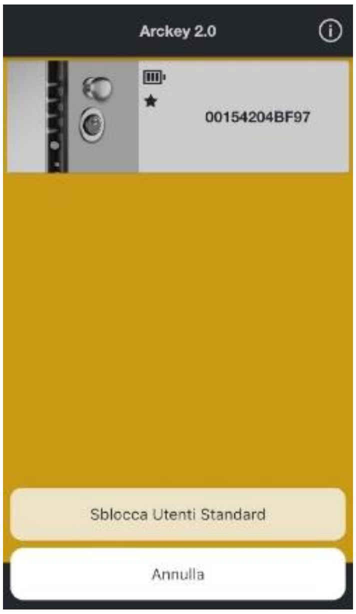


fig.41

OFFICE MODE

Smartphone enabled users can, from the App main screen, activate the Office Mode. In this mode, the lock operates only with the latch and the dead bolts are withdrawn.
In this mode, the door is left ajar and it is not securely closed.

To be able to use this function, **it is not necessary to enter the programming mode**.

Touch and keep pressed the button identifying the door on which you want to enable the Office Mode function. The menu to enable/disable this function will appear (fig.42).

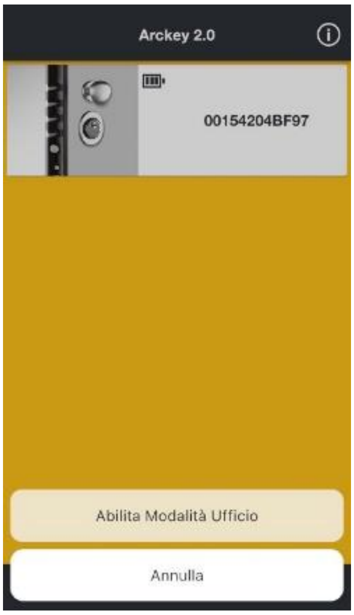


fig.42

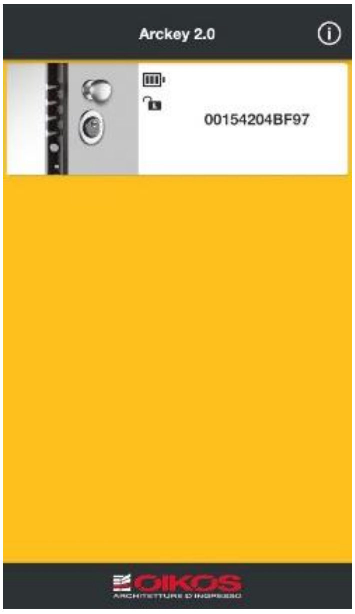


fig.43

A symbol will appear in the white button 🔓 indicating the enabled function (fig.37).

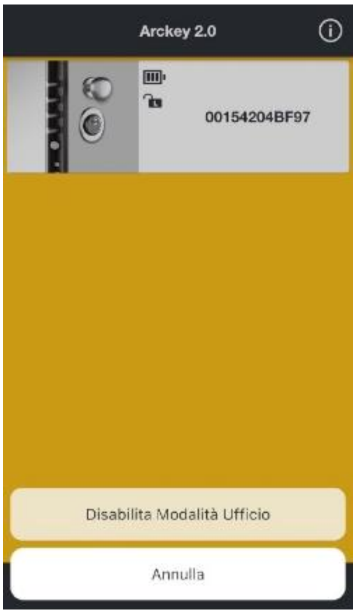


fig.44

Perform this operation in the opposite order to disable this function (fig.44).

See also page 30 for a scheduled management of the Office Mode.

MASTERPHONE MODE

This function allows you to enter the programming mode directly via smartphone, without using the Admin Card. The user becomes actually an administrator.

Touch and keep pressed the white button identifying the door on which you want to enter the programming mode performing the login. The menu will appear (fig.45).
Log in by pressing Login.

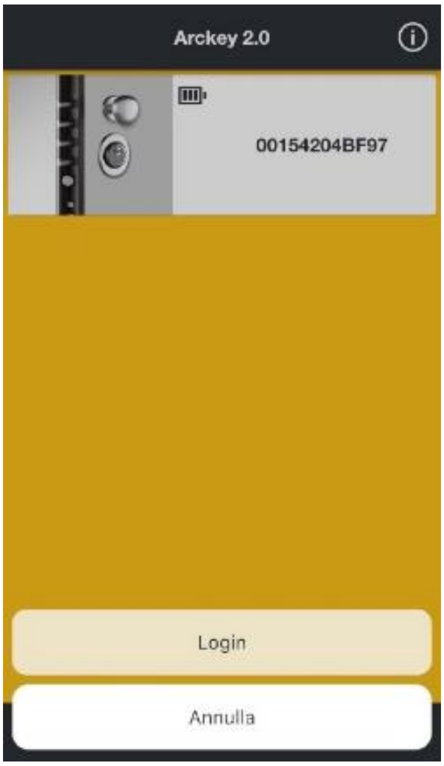
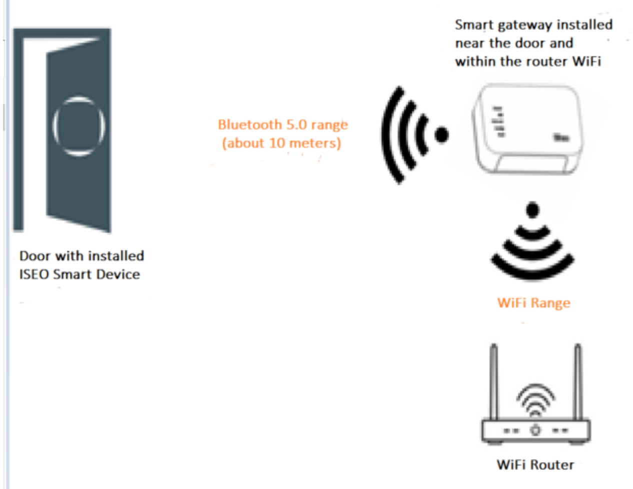


fig. 45

Security can be increased by adding a user PIN to the login function (see p.15).
In this case, the PIN is required to authorize the access.

HOWEVER, IT IS STRONGLY RECOMMENDED TO RETAIN THE ADMIN CARDS IN ORDER TO GAIN ACCESS IN CASE OF NEED OR REPLACEMENT/LOSS OF THE MASTERPHONE DEVICE.

GATEWAY DEVICE


Smart gateway installed near the door and within the router WiFi
Bluetooth 5.0 range (about 10 meters)
Door with installed ISEO Smart Device
WiFi Range
WiFi Router

Through the Gateway Device, the inputs and door opening can be managed from anywhere in the world without being close to the door via a cloud service managed by ISEO.

LED LEGEND:

Power (WHITE): It indicates the Gateway power status. If off, it means it is not powered.

BLE (IT FLASHES WHITE): It indicates the status of Bluetooth connection with the lock. When it flashes, it means it is communicating with the lock via Bluetooth.

Network (WHITE): It indicates the connection status of the Gateway with the WI-FI network. If it is off, it means it is not associated with any WiFi network.

Config (WHITE): When it is steady, it means that the Gateway is ready for configuration; once configured it remains off in normal use.

Boot (RED): It indicates that the Gateway after power on or RESET is initializing for use.

INSTALLATION

In order to be able to use it, the following is needed:

- Lock with Bluetooth 5.0 (see p.2).
- Place the Gateway at a distance that allows Bluetooth communication between the Gateway and the lock (usually it should not exceed 10m distance, but any obstacles, electromagnetic sources, etc. should also be taken into account).
- Place the Gateway at a distance that allows Wi-Fi communication.
- Internet connection on the device being used.

Connect the Gateway device to the power supply and wait until the red "Boot" LED stops flashing (fig.46) and the "Config" LED remains steady lit (fig.47). You can now proceed with the detection and installation.

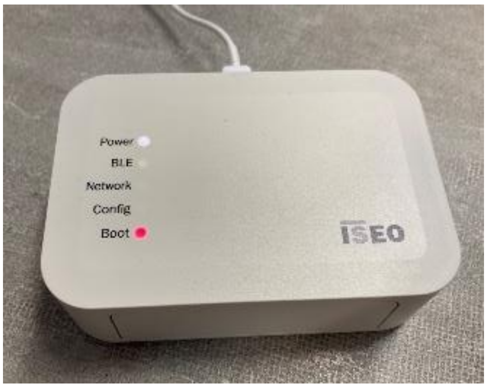


fig.46

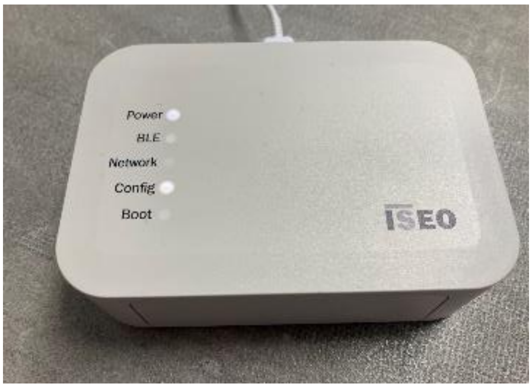
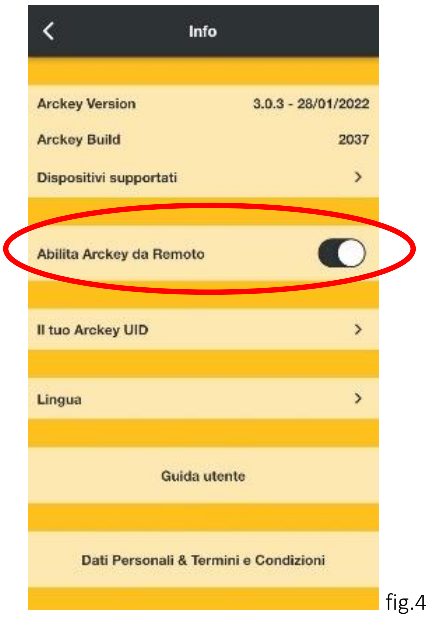


fig.47

CAUTION: This management installation can be done by one device only (Gateway Administrator - p.29). Once initialized, only this device can allow other devices to use the Gateway.

Through the "Info" menu, activate the **"Enable Arckey from Remote"** function (fig.48).

The Gateway functionalities can be used even without activating the Bluetooth mode.



Info

Arckey Version 3.0.3 - 28/01/2022

Arckey Build 2037

Dispositivi supportati

Abilita Arckey da Remoto

Il tuo Arckey UID

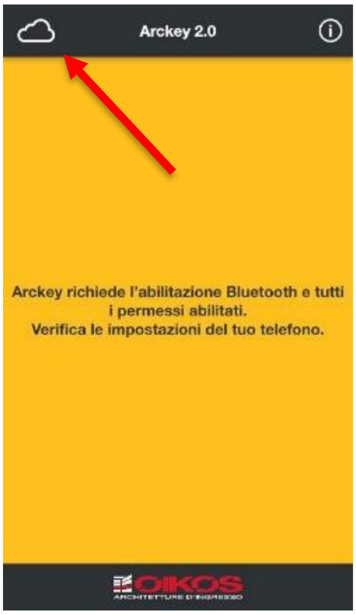
Lingua

Guida utente

Dati Personali & Termini e Condizioni

fig.48

Now on the main screen the icon ☁ has appeared on the upper left corner (fig.49). Once pressed, you will be redirected to the ISEO website to manage your account.

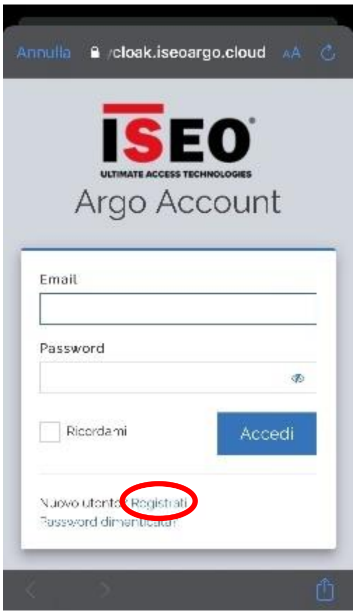


Arckey 2.0

Arckey richiede l'abilitazione Bluetooth e tutti i permessi abilitati.
Verifica le impostazioni del tuo telefono.

fig.49

Press "Register".



Annulla /cloak.iseoargo.cloud

ISEO ULTIMATE ACCESS TECHNOLOGIES

Argo Account

Email

Password

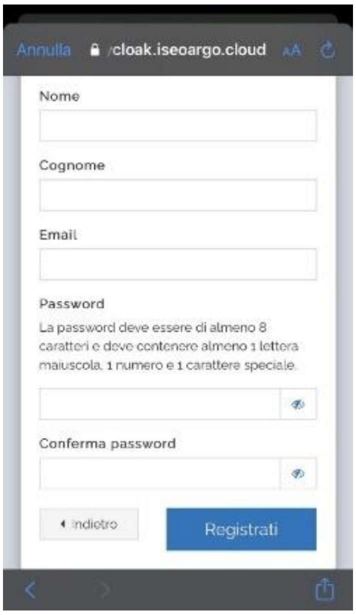
□ Ricordami

Accedi

Nuovo utente? Registrati

Password dimenticata?

fig.50



Annulla /cloak.iseoargo.cloud

Nome

Cognome

Email

Password

La password deve essere di almeno 8 caratteri e deve contenere almeno 1 lettera maiuscola, 1 numero e 1 carattere speciale.

Conferma password

‹ Indietro

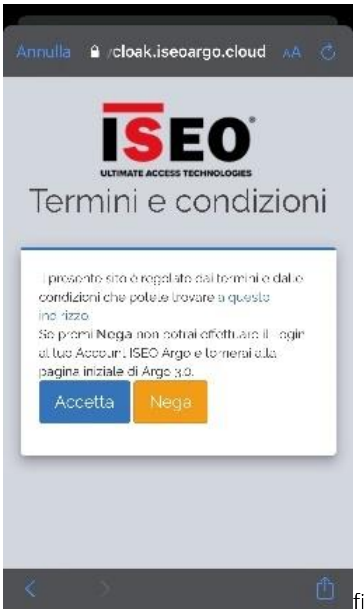
Registrati

fig.51

If you already have an ISEO account log in with the credentials you have (fig.44). Otherwise, press "Register" and complete the registration process for the ISEO Cloud (fig.51).

Then accept the terms and conditions concerning the processing of personal data (fig.52).

Once the registration is completed, it is necessary to confirm the e-mail address through your account, also through a PC browser (fig.53).



Annulla /cloak.iseoargo.cloud

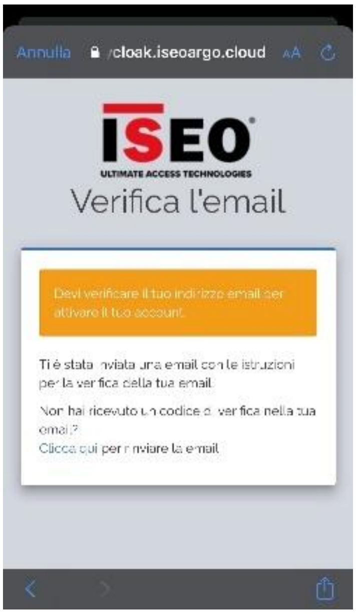
ISEO ULTIMATE ACCESS TECHNOLOGIES

Termini e condizioni

Il presente sito è regolato dai termini e dalle condizioni che potete trovare a questo indirizzo.
Se premi **Nega** non potrai effettuare il login al tuo Account ISEO Argo e tornerai alla pagina iniziale di Argo 3.0.

Accetta Nega

fig.52



Annulla /cloak.iseoargo.cloud

ISEO ULTIMATE ACCESS TECHNOLOGIES

Verifica l'email

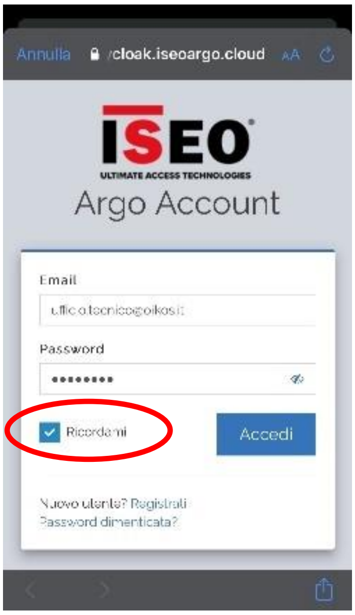
Devi verificare il tuo indirizzo email per attivare il tuo account.

Ti è stata inviata una email con le istruzioni per la verifica della tua email.

Non hai ricevuto un codice di verifica nella tua email?
Clicca qui per rinviare la email.

fig.53

Once the e-mail address has been confirmed, it is possible to access the Iseo Cloud with the just registered credentials (fig.5).



Argo Account

Email

ufficiotecnico@oikos.it

Password

••••••••

☑ Ricordami

Nuovo utente? Registrati
Password dimenticata?

fig.54

For subsequent uses, if you check "Remember me", the credentials will be saved and access to the device will be automatic.

In this way, you'll be properly authenticated and connected. In fact, the edges of the app will be light gray and no longer dark.

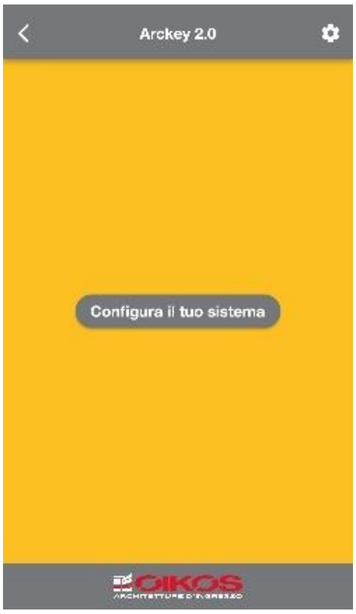
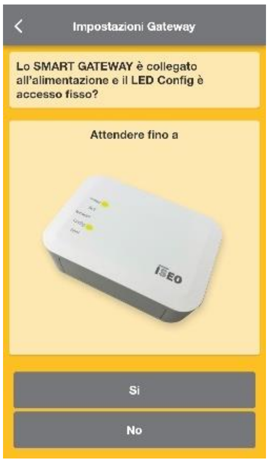


fig.55

Press "Configure your system" (fig.49)



Impostazioni Gateway

Lo SMART GATEWAY è collegato all’alimentazione e il LED Config è accesso fisso?

Attendere fino a

Si

No

fig.56

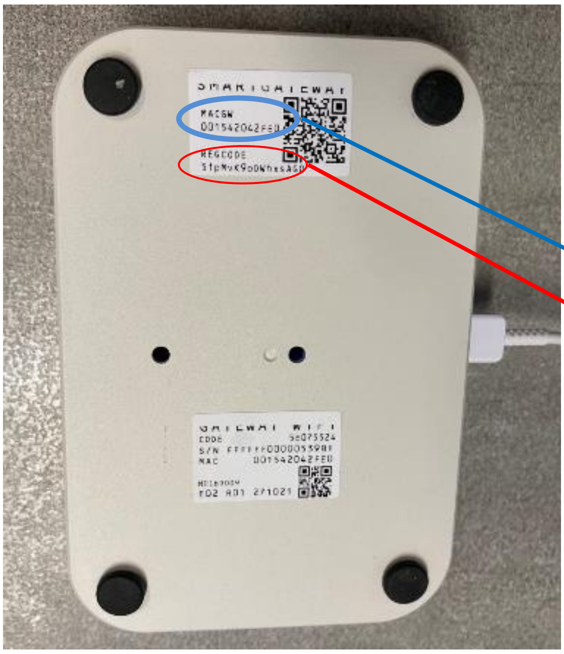
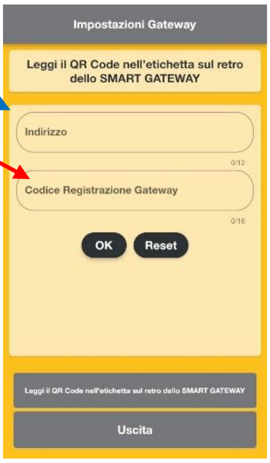


fig.57



Impostazioni Gateway

Leggi il QR Code nell’etichetta sul retro dello SMART GATEWAY

Indirizzo

0/12

Codice Registrazione Gateway

0/16

OK Reset

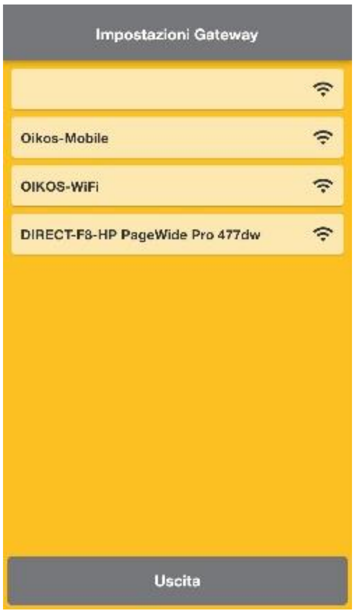
Leggi il QR Code nell’etichetta sul retro dello SMART GATEWAY

Uscita

fig.58

Press "Yes", if the described situation is confirmed (fig.56).

Then, you will be asked to enter a code available on the back of the Gateway in order to associate it with a WiFi network that will be used by the Gateway to communicate via the Internet connection. This can be done by manually entering the codes as shown in the figure (fig.57-58) or in a much simpler way by reading the QR code with your device camera.



Impostazioni Gateway

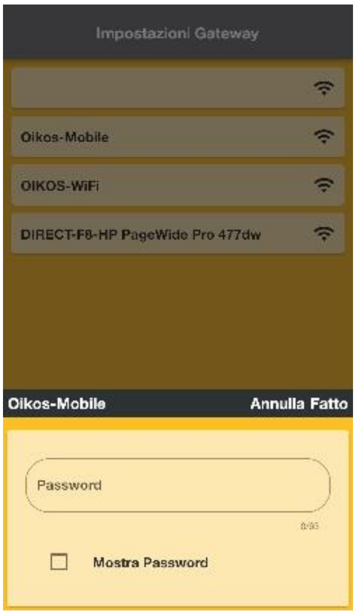
Oikos-Mobile

OIKOS-WiFi

DIRECT-F8-HP PageWide Pro 477dw

Uscita

fig.59



Impostazioni Gateway

Oikos-Mobile

OIKOS-WiFi

DIRECT-F8-HP PageWide Pro 477dw

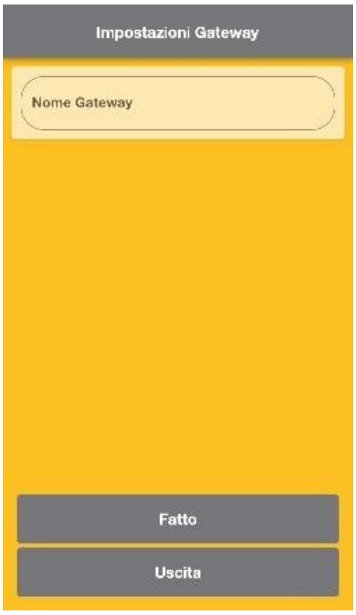
Oikos-Mobile Annulla Fatto

Password

0/63

□ Mostra Password

fig.60



Impostazioni Gateway

Nome Gateway

Fatto

Uscita

fig.61

Then, you'll be prompted to connect the device to a WiFi network in the vicinity of the Gateway (fig.59) and if necessary adding a WiFi Network password (fig.60). After the configuration, fill in the name of the Gateway network (fig. 61).

Once the association of the Gateway with the WiFi network is completed, the "Power" and "Network" LEDs should be lit (fig.62).

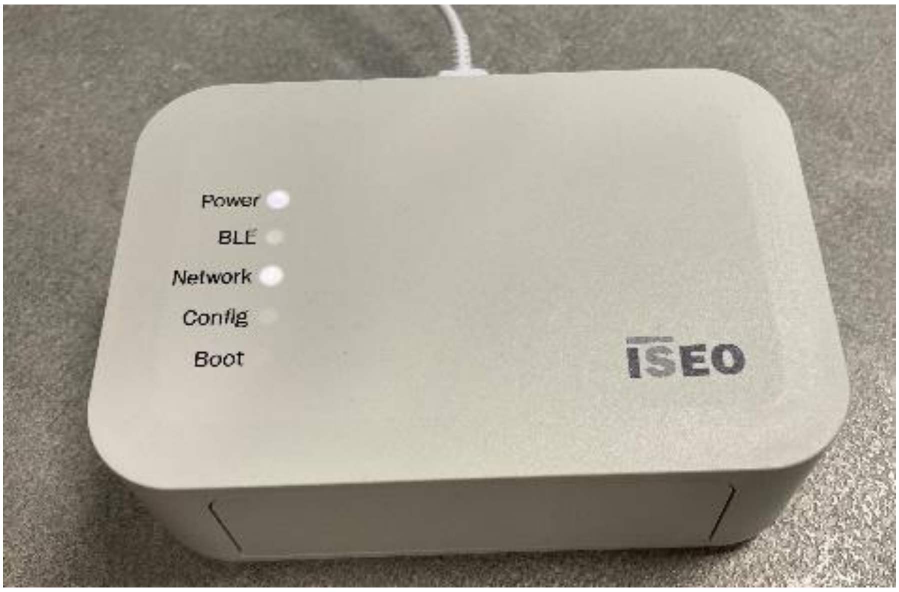
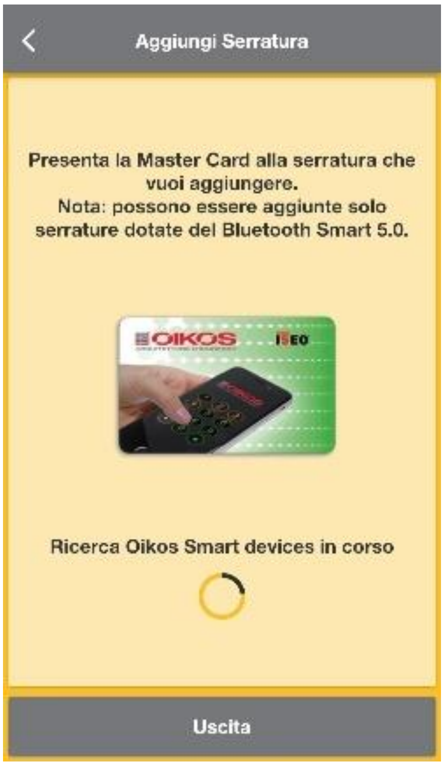


fig.62

ADDING A LOCK WITH GATEWAY (ADMIN CARD REQUIRED)

Now in the Gateway settings screen press on "Lock" and then on "Add a new lock". The device will search for locks available for pairing.



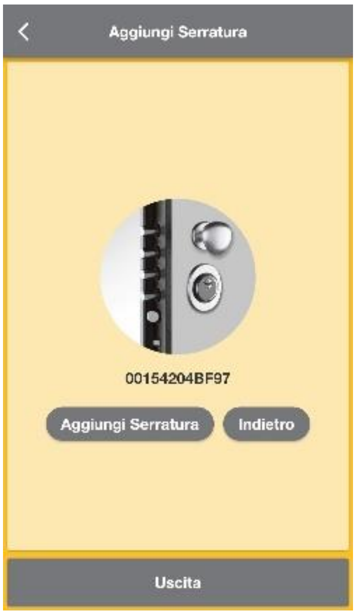
Aggiungi Serratura

Presenta la Master Card alla serratura che vuoi aggiungere.
Nota: possono essere aggiunte solo serrature dotate del Bluetooth Smart 5.0.

Ricerca Oikos Smart devices in corso

fig.63

Now you need to be in front of the lock and place the Admin Card close to the reader of the lock you want to configure within a short time (fig.63). **Using the existing Admin Card (see p.6).**



Aggiungi Serratura

00154204BF97

fig.64

Press "Add Lock" (fig.64) and wait for the pairing operation to be completed **(do not close the App during this operation)**.

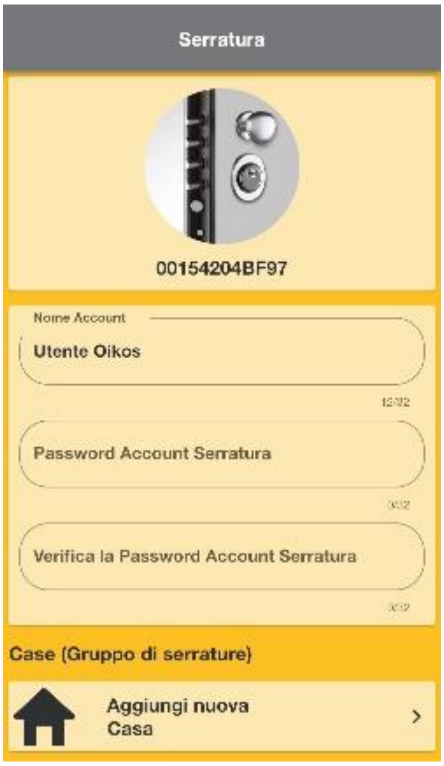

Serratura
00154204BF97
Nome Account
Utente Oikos
12/32
Password Account Serratura
0/32
Verifica la Password Account Serratura
0/32
Case (Gruppo di serrature)
Aggiungi nuova Casa
›

fig.65

Through the next screen you need to set a lock password that will be used for opening the lock remotely (fig.65). **The lock password can be different from your ISEO account password.**

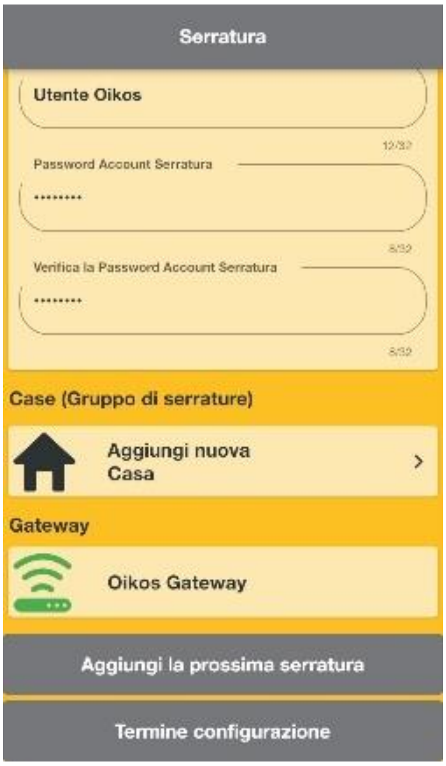
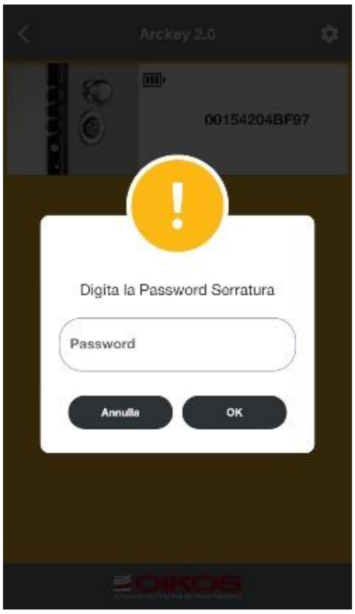

Serratura
Utente Oikos
12/32
Password Account Serratura
••••••••
8/32
Verifica la Password Account Serratura
••••••••
8/32
Case (Gruppo di serrature)
Aggiungi nuova Casa
›
Gateway
Oikos Gateway
Aggiungi la prossima serratura
Termine configurazione

fig.66

Press "Add next lock", if there are multiple locks to be configured with the Gateway or press "End configuration" to complete the operation (fig.66). Wait for the configuration to be completed and the lock will be added to your list of locks.

It is possible to group the various locks by "Houses" and thus to manage in an easier way the different locks used in different countries and places around the world (see p.32).

DOOR OPENING WITH GATEWAY DEVICE



Digita la Password Serratura

fig.67

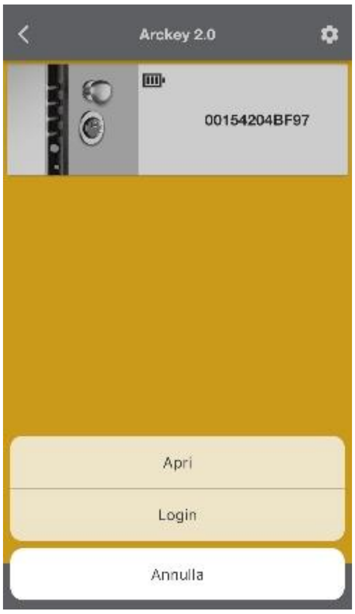
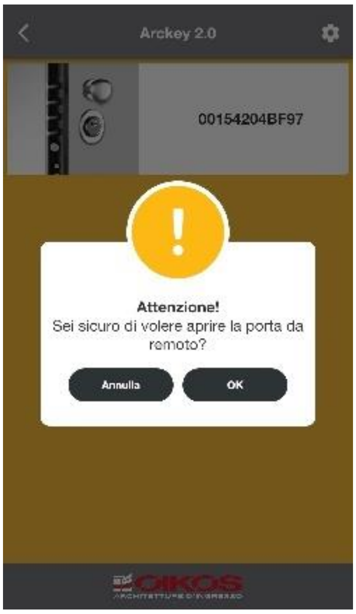


fig.68



Attenzione!
Sei sicuro di volere aprire la porta da remoto?

fig.69

Press the desired lock and enter the lock password (fig.67) (on iOS devices, it is possible to set one's own fingerprint or Face ID to automatically fill in the password)

Pressing "Open" (fig.68) and then "Ok" (fig.69) the lock will open.

Through "Login" it will be possible to:

- Add, edit or delete users.
- Read the event log.
- Add a standard user account to be used.

Adding, editing or deleting users:

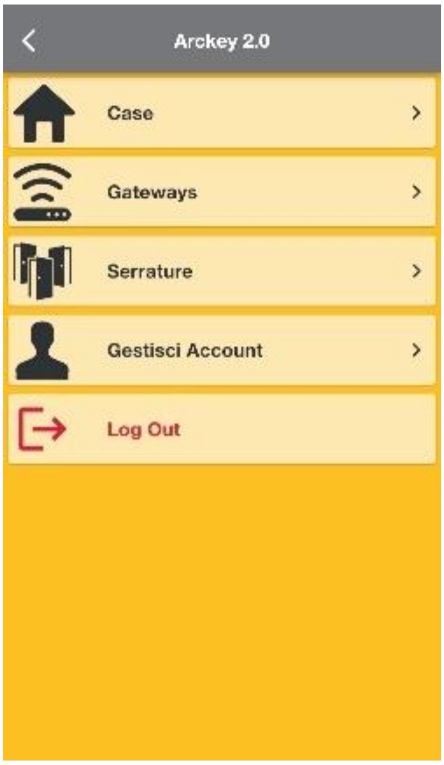
The remote user interface has the same functionality as the local interface (p.17).

Reading the event log.

The Events interface in remote is the same as the local interface. Events are preloaded on your device, and you then need to refresh the page to load the events in real time.

GATEWAY MENU

By pressing the ⚙ button, access to the Gateway menu is granted.



- **Home:** It allows adding, renaming and deleting houses that group different locks.

- **Gateways:** It allows adding, renaming, and deleting different Gateway devices; if the icon is displayed in red, it means that the Gateway is not connected to any Internet network. Conversely, if it displayed in green, it means that it is properly communicating with the Internet.

- **Locks:** It allows adding, renaming and deleting several reachable locks; through this section, it is also possible to associate the lock to a "House". **To add a lock, it is in any case necessary to be in front of the lock to be registered with the Admin Card (p. 22).**

-**Manage Account:** In this screen, it is possible to view the information concerning one's own account and to enable or disable the Face ID or Touch ID function available on some devices that allow to use these functions to replace the manual password entry. It is also possible to change the account password and delete the account.

The Gateway Administrator

The Gateway Administrator is a new identity closely related to the remote use of the Arckey App.

The Gateway Administrator should not be confused with the Local Administrator. These are two separate identities that can still coexist on the same lock. **Arckey allows the possibility to have multiple Local Administrators but only one Gateway Administrator.**

The Gateway Administrator is basically the owner of the Gateway i.e. the first person who has created an account in the ISEO Cloud, configured the Gateway (p.20) and added the locks to his account.

Later on, the Gateway Administrator can invite other Users who have an account in the ISEO Cloud, to use the Gateway.

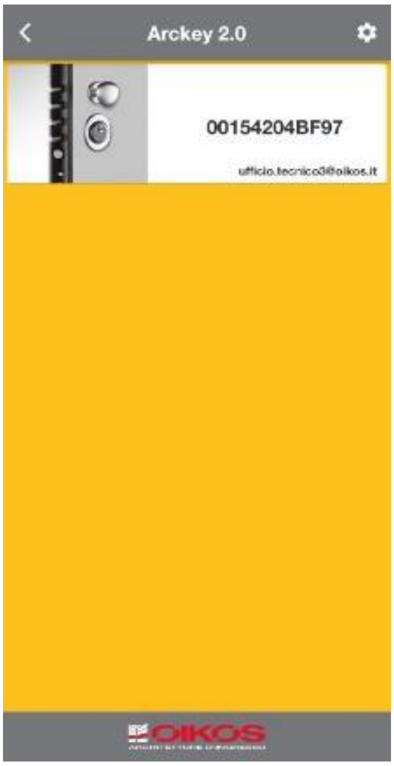
CAUTION: Only the Gateway Administrator can delete himself.

ADDING A GATEWAY USER ACCOUNT

The Gateway Administrator can add additional User Accounts for lock control. To do this, proceed as follows:

- Access Remote Arckey.
- Perform the "Login" to the lock (p.22).
- Press the icon .
- Press the icon .
- Enter the Name and E-mail address of the account present in the ISEO Cloud of the user you want to add.
- Select the permissions you want to grant to the new user.
- Press "DONE" on the upper right corner.

The new user will receive an e-mail to the associated e-mail address with the name of the lock and a TEMPORARY PASSWORD that will allow him/her to unlock the lock.



Arckey 2.0

00154204BF97

ufficio.tecnico3@oikos.it

fig.70

Now, the new User, who through the app will have logged in to the ISEO Cloud, will be able to see the list of locks to which he has been invited, together with the Gateway Administrator e-mail address (fig.70).

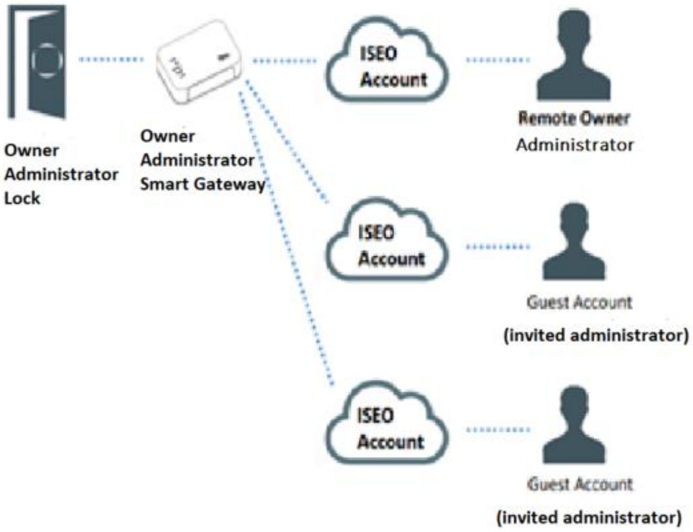
To open the lock, the new user must use the TEMPORARY password contained in the invitation e-mail.

Then, through the "Login" function and by selecting your own account, you can change the Lock password that will replace the temporary one. The Lock password is associated with the account being used at that time, so for the same lock each account may have a different password.

REMOVING THE GATEWAY ADMINISTRATOR ACCOUNT

In order to remove the Gateway Administrator account, it is necessary to delete the locks associated with it from the device.

This operation will cancel all Invited users’ ability to access the Gateway.



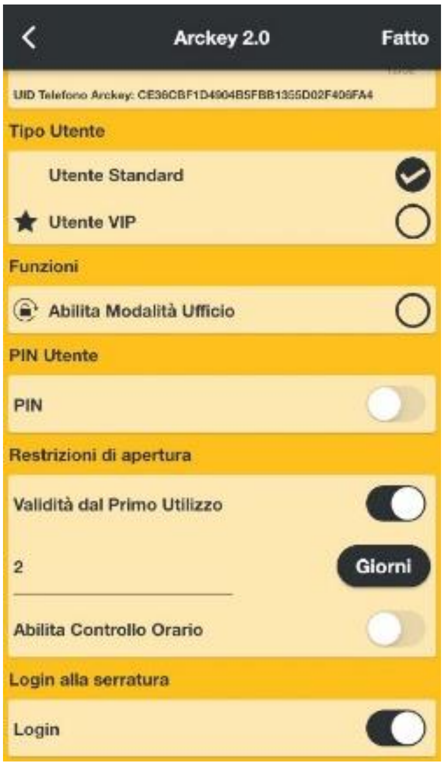
Now each account can independently view the lock but will **not** be able to make invitations themselves.

OPENING RESTRICTIONS

Time restrictions can be set for each user with reference to the opening, understood as the duration or time slot.

Validity from the first use: this control allows to assign a "term" validity.

For example, it may be necessary to assign two days limited access to a technician performing maintenance. At the end of the second day, access will be inhibited.
Enable the "Validity from first use" item (fig.71) and assign a duration, which can be expressed in days/hours/minutes from the first time the door is opened (fig.72).
Press on Done on the upper right corner.



Arckey 2.0 — Fatto

UID Telefono Arckey: CE36CBF1D4904B5FBB1355D02F406FA4

Tipo Utente

Utente Standard ●

Utente VIP ○

Funzioni

Abilita Modalità Ufficio ○

PIN Utente

PIN: off

Restrizioni di apertura

Validità dal Primo Utilizzo: on

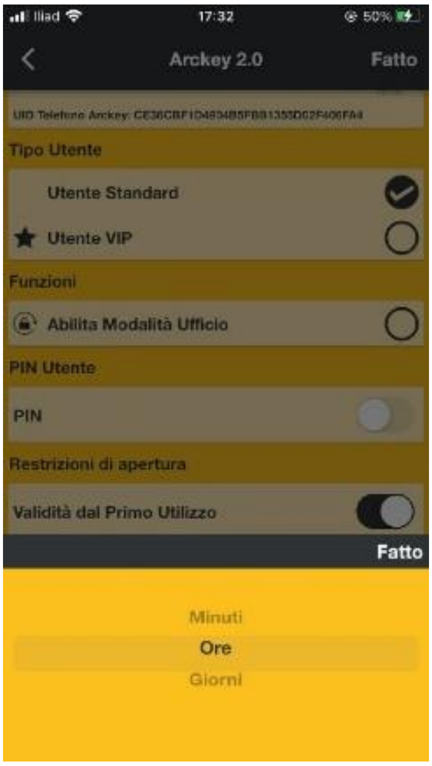
2 — Giorni

Abilita Controllo Orario: off

Login alla serratura

Login: on

fig.72



Iliad 17:32 50%

Arckey 2.0 — Fatto

UID Telefono Arckey: CE36CBF1D4904B5FBB1355D02F406FA4

Tipo Utente

Utente Standard ●

Utente VIP ○

Funzioni

Abilita Modalità Ufficio ○

PIN Utente

PIN

Restrizioni di apertura

Validità dal Primo Utilizzo: on

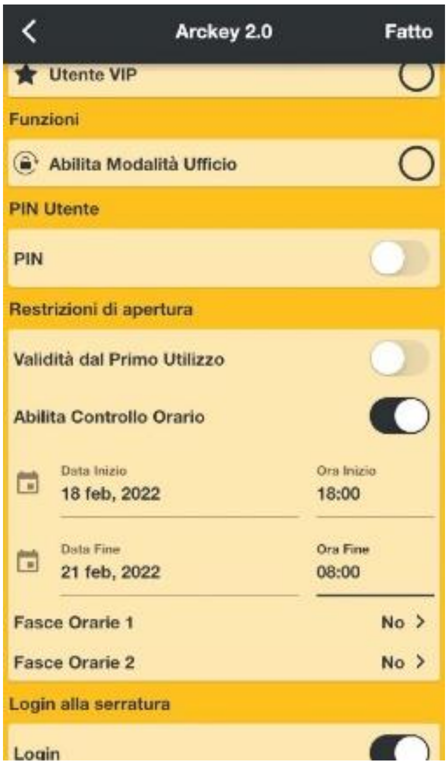
Fatto

Minuti
Ore
Giorni

fig.72

Enable time control: It allows assigning a time duration for the validity for a user (from a date to another one).

Activate the Enable Time Control function (fig.73). In this typical configuration for a cleaning company, the user is enabled to use the lock from 18:00 on Friday, February 18, 2022, when the offices are empty until 08:00 on Monday, February 21, 2022.



Arckey 2.0 Fatto

Utente VIP ○

Funzioni

Abilita Modalità Ufficio ○

PIN Utente

PIN

Restrizioni di apertura

Validità dal Primo Utilizzo

Abilita Controllo Orario

Data Inizio 18 feb, 2022 — Ora Inizio 18:00

Data Fine 21 feb, 2022 — Ora Fine 08:00

Fasce Orarie 1 No >

Fasce Orarie 2 No >

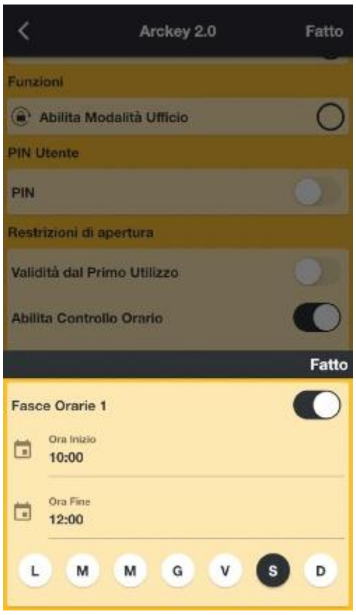
Login alla serratura

Login

fig.73

Time Slots: They allow a more precise control of the restrictions, within the enabling period. It is possible to indicate on which days of the week and for which time slots the restriction is active.

Example: the cleaning staff are granted access for a period of 20 years, but they can only access on Saturdays from 10 a.m. to noon (fig.74).



Arckey 2.0 Fatto

Funzioni

Abilita Modalità Ufficio ○

PIN Utente

PIN

Restrizioni di apertura

Validità dal Primo Utilizzo

Abilita Controllo Orario

Fatto

Fasce Orarie 1

Ora Inizio 10:00

Ora Fine 12:00

L M M G V S D

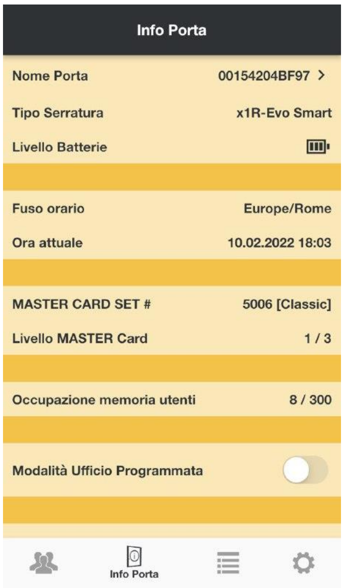
fig.74

Two different time slots can be managed for a more flexible scheduling of access restrictions.

Once you have configured the validity period and any time slots, press "Done" on the upper right corner.

DOOR INFO

The door Info tab shows the list of all information about the associated door:



Info Porta

Nome Porta	00154204BF97 >
Tipo Serratura	x1R-Evo Smart
Livello Batterie	
Fuso orario	Europe/Rome
Ora attuale	10.02.2022 18:03
MASTER CARD SET #	5006 [Classic]
Livello MASTER Card	1 / 3
Occupazione memoria utenti	8 / 300
Modalità Ufficio Programmata	

fig.75

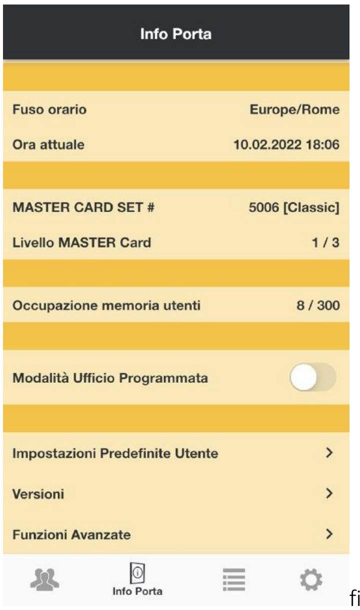
Door Name: It can be customized by replacing the default "door order number".
The newly assigned name will be displayed on the App Home screen (fig.75).

Lock type: It indicates the type of mounted lock (fig.75).

Battery level: It indicates the charge level of the batteries present inside the lock: OK, Low, Very Low, End (fig.75).

Admin Card level: It identifies the security level of the active card (fig.76).

Saved Users: Total registered users divided by categories (maximum 300) (fig.75).



Info Porta

Fuso orario	Europe/Rome
Ora attuale	10.02.2022 18:06
MASTER CARD SET #	5006 [Classic]
Livello MASTER Card	1 / 3
Occupazione memoria utenti	8 / 300
Modalità Ufficio Programmata	
Impostazioni Predefinite Utente	>
Versioni	>
Funzioni Avanzate	>

fig.76

Scheduled Office Mode: It allows activating
the time slots for the Office Mode as well as setting its programs 1 and 2 (see p.35) (fig.76).

User default settings: It allows defining what functions you want to assign by default to newly created users (VIP or standard user categorization, applicable restrictions, etc.) (fig.76).

Version: Versions of the lock components are shown (useful in case assistance is needed) (fig.76).

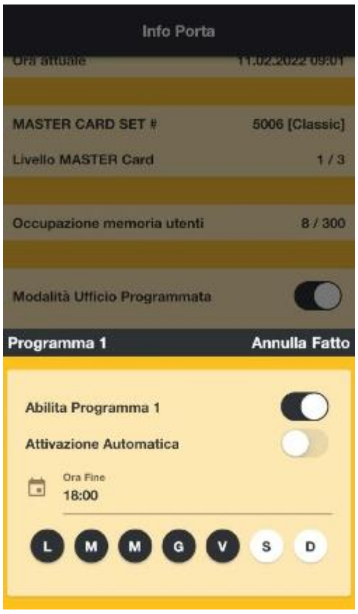
Advanced functions: These are technical parameters to be used **only** at the request of the Technical Support.

Use by non-technical personnel is not recommended.
Changing the parameters contained in the advanced functions may change or affect the operation of the lock.

SCHEDULED OFFICE MODE

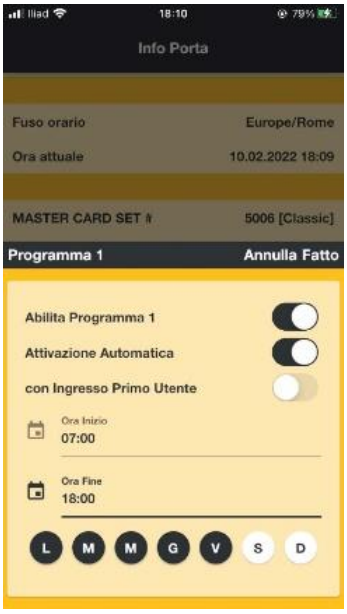
This function allows two programs to be set to automatically enable and disable the Office Mode. This means that the lock will automatically go into Office Mode, following up to two set programs.

Enter the programming mode and open "Door Info".
Enable the Program 1 to begin the configuration. (The same rules apply to Program 2).
Depending on the need, 3 different modes for using the Office Mode can be set:



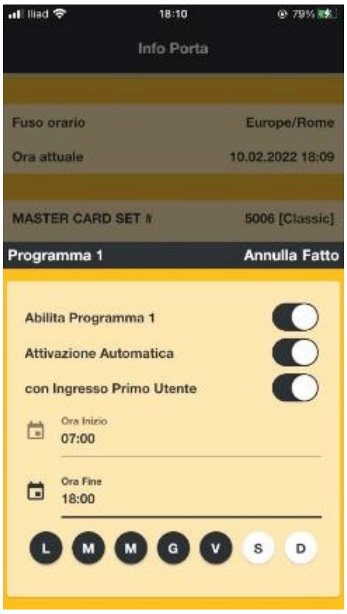
Info Porta
Ora attuale 11.02.2022 09:01
MASTER CARD SET # 5006 [Classic]
Livello MASTER Card 1 / 3
Occupazione memoria utenti 8 / 300
Modalità Ufficio Programmata
Programma 1 Annulla Fatto
Abilita Programma 1
Attivazione Automatica
Ora Fine 18:00
L M M G V S D

fig.77



Iliad 18:10 79%
Info Porta
Fuso orario Europe/Rome
Ora attuale 10.02.2022 18:09
MASTER CARD SET # 5006 [Classic]
Programma 1 Annulla Fatto
Abilita Programma 1
Attivazione Automatica
con Ingresso Primo Utente
Ora Inizio 07:00
Ora Fine 18:00
L M M G V S D

fig.78



Iliad 18:10 79%
Info Porta
Fuso orario Europe/Rome
Ora attuale 10.02.2022 18:09
MASTER CARD SET # 5006 [Classic]
Programma 1 Annulla Fatto
Abilita Programma 1
Attivazione Automatica
con Ingresso Primo Utente
Ora Inizio 07:00
Ora Fine 18:00
L M M G V S D

fig.79

Office Mode with automatic closing:

In this mode, the activation is done manually by an enabled user, but the automatic closing can be scheduled at a certain time.
Select the automatic closing time and the days for which the schedule is valid (The proposed standard is weekdays, that is, every day except Saturday and Sunday).
Press Done to confirm (fig.77).

Office Mode with automatic activation and automatic closing:

In this mode, both activation and closing occur automatically. Select the automatic activation time, the automatic closing time and the days for which the schedule is valid. The standard is weekdays, i.e. every day except Saturday and Sunday (fig.78).

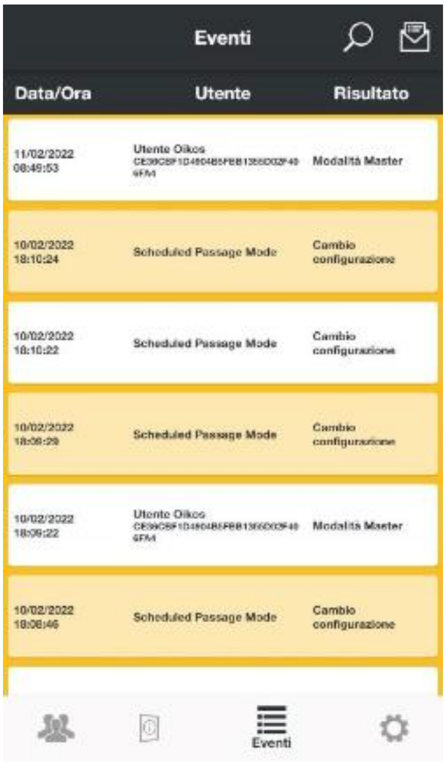
Office Mode with automatic activation upon first access and automatic closing (C):

It is as the previous point, only the actual activation of the Office Mode will occur with the access by the first enabled user. This solution is very useful for security because it prevents a lock from going into Office Mode automatically when there is no user inside the building or room (for example, Christmas Day

might fall on a day when automatic Office Mode is scheduled, but in this case it should not be activated!) (fig.79)

EVENTS

The Events tab displays the list of the last 1,000 events related to the door (fig.80).
Events are defined as any mechanical, electrical or electronic action that occurred in the lock.



Eventi

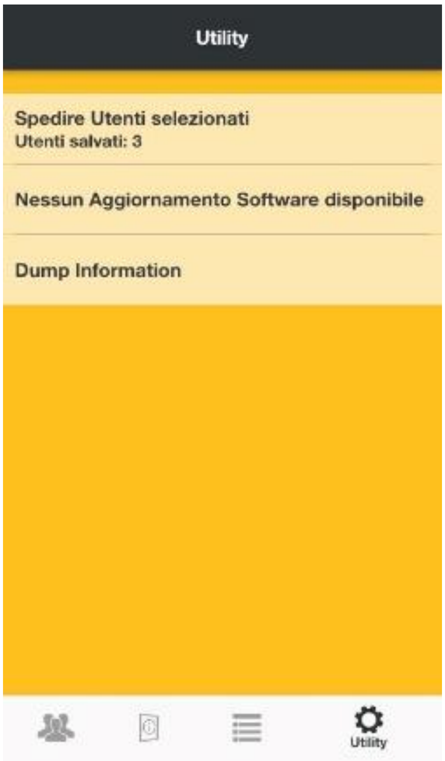
Data/Ora	Utente	Risultato
11/02/2022 08:49:53	Utente Oikos CE39CBF1D4804B5FEB1366D02F40 6FA4	Modalità Master
10/02/2022 18:10:24	Scheduled Passage Mode	Cambio configurazione
10/02/2022 18:10:22	Scheduled Passage Mode	Cambio configurazione
10/02/2022 18:09:29	Scheduled Passage Mode	Cambio configurazione
10/02/2022 18:09:22	Utente Oikos CE39CBF1D4804B5FEB1366D02F40 6FA4	Modalità Master
10/02/2022 18:08:46	Scheduled Passage Mode	Cambio configurazione

fig.80

It is possible to perform a quick search by typing the desired value in the available Search field after clicking on the ⌕ icon in order to filter events (for example, all events related to a certain card ID).
The list can be e-mailed after clicking on the ✉ icon on the upper right corner.

UTILITY

The Utility tab provides access to the maintenance functions:



Utility

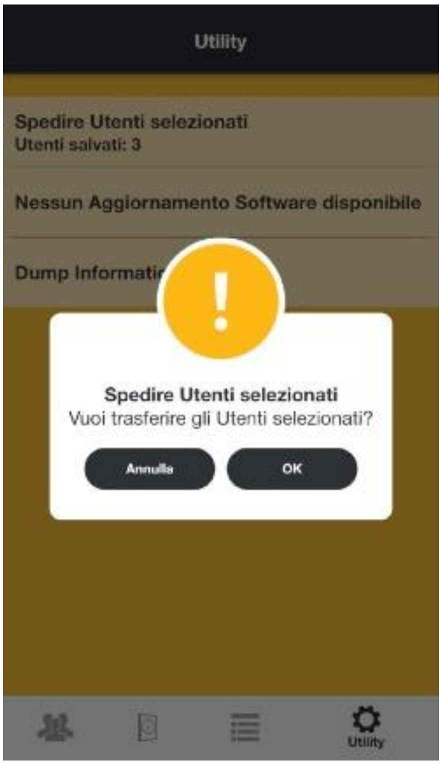
Spedire Utenti selezionati
Utenti salvati: 3

Nessun Aggiornamento Software disponibile

Dump Information

fig.81

Sending selected users: Users copied to the smartphone memory can be transferred to another device.
Enter the programming mode for the lock into which you want to copy the users (see p. 7).
Access the Utility tab and press the Send selected users button (fig.81).
Click OK when a confirmation is prompted (fig.82).



Utility

Spedire Utenti selezionati
Utenti salvati: 3

Nessun Aggiornamento Software disponibile

Dump Informati

Spedire Utenti selezionati
Vuoi trasferire gli Utenti selezionati?

fig.82

Software update: This function checks and downloads App updates.
If there is an update available, simply click on the button to perform the lock software update.
Do not move the smartphone away from the door until the update is complete.

It is recommended to always download all updates released by Oikos to keep the system aligned with the highest security and performance standards.

Dump Information: This function allows all lock diagnostic data to be forwarded via e-mail. To be used ONLY if specifically requested by the Oikos Service Center.