Arckey

OIKOS
ARCHITETTURE D'INGRESSO

# Integrated System for access management with electronic opening via App.


## Instruction Manual

## Reserved to the System Administrator

INDICE

## WHAT'S ARCKEY

Arckey is an integrated system for managing electronically the doors opening.
By means of the Arckey App, available for Android and IoS mobiles and tablets, you can communicate with compatible locks and set all the authorizations and access modalities up to a maximum number of 300 users, divided between Smartphone, Rfid cards, combinations of PINs, fingerprints and invitations.

Through the App, the administrator of the system can easily and intuitively add, modify or delete users from the system or set new access rules dividing the users between standard and "vip", establishing time-based access, temporary access credentials and much more.

The administrator can also copy the users' list from a lock to another one supervising all its activities by consulting the log which store the latest 1000 events occurred since that moment.

## OPERATIONAL REQUIREMENTS

The Arckey App is downloadable for free from App Store (iOS) or from Google Play (Android).


Arckey is consistent with the following devices

**IoS** from Iphone 7 and operative system from 7.0 version

**Android** from 4.3 version (Jelly Bean).

The Arckey App works together with the motorized electronic lock installed in the Oikos door. The lock incorporates an electric engine controlled by a powerful state-of-the-art- microprocessor.

In case of power failure (due to the batteries or to the power grid) the actuation of the bolts is always granted by the traditional movement of the mechanic key.

Before using the Arckey system the Bluetooth of the device bust be enabled.

## LOGIN CREDENTIALS

The access from the outside is allowed through the following modes:

### Opening with Smartphone and Tablet through App

By clicking **the white button in the App** of a tablet or mobile home screen, the lock will run the opening command (1)

1

### Opening with Card or Transponder:

Approaching a Transponder Key (2), an Oikos Card (3)or a card with RFID technology (4) (as a credit card, a metro card etc…)to the external reader, the lock will run the opening command. The RFID cards must be compatible with Mifare 13,56 Mhz and they usually need a closer reading.

2

3


4

### Opening with PIN Code ( only in case of keypad ) :

By entering the number code (minimum 4 characters, maximum 8 characters) followed by the hash symbol #, the lock will run the opening command (5)


5

### Opening with fingerprint reader:

If the door is provided with a fingerprint reader (optional), by placing the finger (whose fingerprint has been saved) on the reader the lock will receive the opening command (6)


6

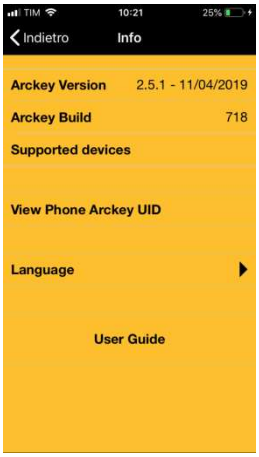
## FIRST START OF ARCKEY

Before using the App remember to activate Bluetooth on your smartphone

When the App is launched, the display of your smartphone will show all the available locks within range. (7).

7

By clicking the symbol “Information” ⓘ at the top right the user will get the data concerning the software of the devices supported by the App and its version. It is also possible to change the language preferences and visualize the user guide in the chosen language (8).



8

## ADMIN CARDS

**Admin Cards** allow the administrator to enter the setting mode in order to program and run Oikos Arckey access managing system.

ATTENTION: The kit of 3 Admin Cards is sealed at the company after the internal quality control.
These Admin Cards allow you to become the sole administrator of the system and to run the operations described in the current manual. Guard them with care and avoid to lose them.

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

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


At the time of the first use, you can enter the Arckey programming mode by approaching the Green Admin Card to the external reader.

Any time the user loses the control of his Green Admin Card (in case of theft or loss), he can move to the Grey security level, simply approaching the following Grey Admin Card to the external reader. An acoustic signal will confirm the real reading and the Green Admin Card will stop functioning. Wait for the second acoustic confirmation signal after 10 seconds.

Any time the user loses the control of his Grey Admin Card (in case of theft or loss), simply approaching the following Red Admin Card to the external reader (an acoustic signal will confirm the real reading) the Grey Admin Card will stop functioning. Wait for the second acoustic confirmation signal after 10 seconds.

The possible loss of the Red Admin Card precludes any possibility to enter the programming mode and run the Arckey system functions.

Therefore, at this point we suggest you to ask for a new kit of Admin Cards (Green-Grey-Red).

By approaching the Green Admin Card of the new kit to the door (an acoustic signal will confirm the reading) the old kit will be deactivated reactivating the original functions. Wait for the second acoustic confirmation signal after 10 seconds.

When the user moves from an Admin Card to another one the user and system settings won't be subject to any modifications.

## ENTER THE PROGRAMMING MODE

Approach the Green Admin Card to the external reader of the door.

The reader will emit an audible and light confirmation signal; at the same time, in the App, the white button indicating the door will become red (9)

Click on the button

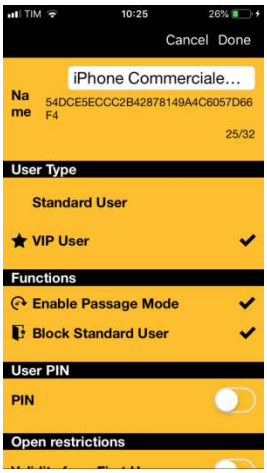
9

The App will match the Smartphone with the lock.

## ADD THE SMARTPHONE AS A LOGIN CREDENTIAL

After the match you'll be asked to add the Smartphone as a login credential to open the lock (10).

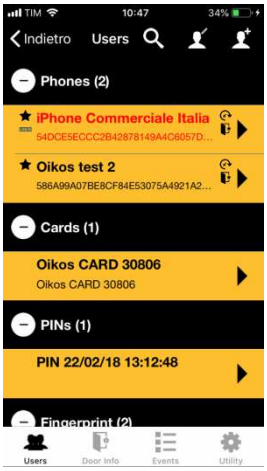
This operation must be done for every Smartphone the user wants to save on the lock.



10

If desired, the user can modify the identifying name of the Smartphone and then click on Done at the top right. After then, the device will appear in the list of saved users, enabled to open the door (11)

Each tasks will be explained in the following chapters.



11

The User Sheet shows the list of all the users connected to the door, divided according to the access mode: Smartphone and tablet, Cards (Oikos cards, cards with RFID technology, Transponder Key), PIN, Fingerprints and invitations.

## OPEN THE DOOR

Leave the programming mode by clicking the button  at the top left.

Click the white banner that identifies the door in order to send an opening pulse to the lock. The lock will pull the bolt back.

## USAGE STORAGE

### Oikos Card, Transponder Key, Card with RFID technology Storage

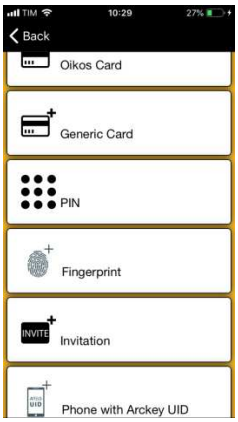
Enter the programming mode (see page 6).
Once inside the users' list, approach the key or the card to the external reader of the door. Wait for the confirmation signal. Now the card will appear in the users' list as a confirmation of the correct saving.

### PIN code Storage ( only in case of number keypad)

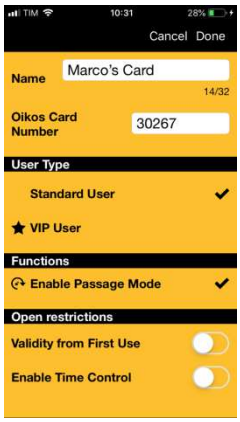
Enter the programming mode (see page 6).
Once inside the users' list, enter the number code (minimum 4 characters, maximum 8 characters) followed by the hash symbol #. Wait for the confirmation signal. The PIN code will appear in the users' list as a confirmation of the correct saving.

### Manual addition of cards and PINs

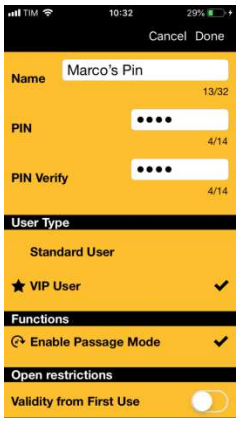
It is possible to add any cards even if we don't have them physically, saving them by their code. This task is useful in case the cards are previously given to the users.
Enter the programming mode (see page 6).



12



13



14

Click the button add user at the top right and choose the type of card to add (Oikos card or general RFID Card (12)
Enter the name and the identifying number indicated on the card. Click on Done. (13)

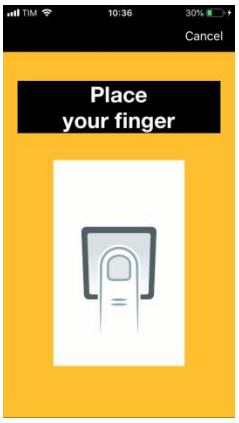
If the user wants to add a PIN without typing it on the keypad, click on PIN, enter a name and type the code twice in the field PIN and PIN confirmation. Click on Done. (14)

Attention: For security reasons the PIN codes will never be clearly visible in the App

## Fingerprint Storage

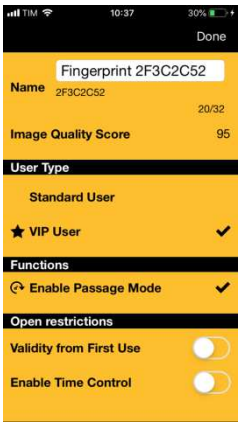
Enter the programming mode (see page 6).

Click the button add user at the top right (11) and choose Fingerprints (12)
The fingerprint reader will start flashing. Put the finger on the reader, as illustrated in figure (15).
The App will ask to read the fingerprint more than once in order to have a good quality record



15

16



17

Click on OK (16) and then on Done (17).
Now the fingerprint is recognized as a valid credential to open the door.

Attention: For a correct reading, the finger has to be leant on the scanner and not rubbed. The fingerprint reading can be difficult due the following factors: an excessive humidity of the finger or the scanner surface, a dirty scanner surface, a weak legibility of the fingertip etc..

## Invitations Storage

Invitations allow a user (Smartphone or Tablet) to auto-register on the memory of the lock as a user authorized to access, using an invitations code, previously saved on the Administrator's lock.

For example, this function allows a Bed and Breakfast manager to authorize a client to access to his building, even before he gets to the B&B.
To do this, the Administrator will add on the memory of the lock an invitation code which will be sent to the person authorized to access.

**What the Administrator has to do to create an invitation:**

Enter the programming mode.

Click the button add user at the top right (11) and then on Invitations (12).

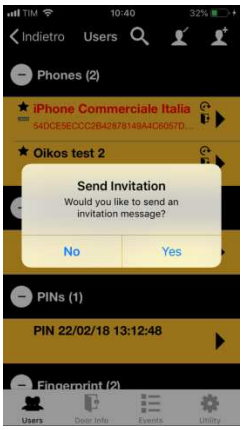
You will get a window with the user configuration.

Enter a name to identify this invitation and set the desired parameters.

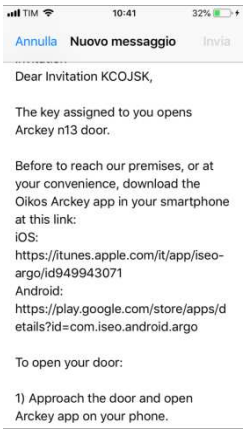
Click on **Done** to confirm.

The user will be asked if he wants to send an invitation message (18).

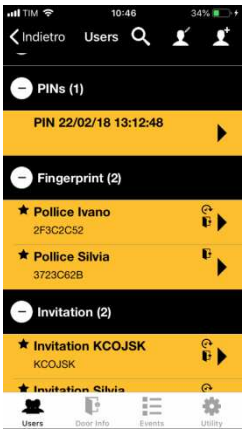
Click Yes to send it immediately or NO to send it at a later time.




18




19




20

A text will be automatically created with the explication, step by step, of how to use the invitation to open the door (19).

All the information concerning the access validity will be reported, if any. (see page 14).

Instructions may be sent by email or through a messaging program (as Skype, Whatsapp, etc..). The invitation will appear in the invitations list (20).

**What the user who receives the invitation has to do:** First of all, the user who receives the invitation has to download the App on his device. After activating the Bluetooth and the Oikos Arckey App, the user must approach the door to allow the lock to be detected. Clicking on the white button identifying the door, the invitation code, previously received, will be asked.

The door will open and the Smartphone will appear in the list of the saved Smartphones.

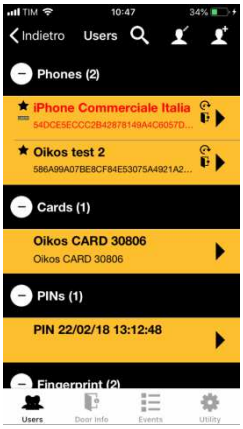
The invitation, since it has been "accepted", will disappear from the invitations list.

## USER REMOVAL AND SAVING

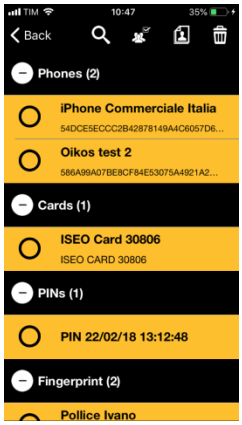
Click on the icon Edit at the top right (21).

Select the user you want to delete or to save or push the icon to select them all (22) (pay attention, in this way all the users will be deleted/saved).

Click on the Trash icon to confirm to remove the user or the icon to save it.




21




22

Users will be saved in the Smartphone and in case of need they can be recovered or duplicated on another lock without needing to reconfigure them again (see page 23).

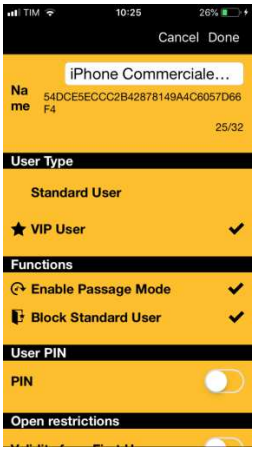
### Quick removal of a user:

From the users' list: on Android systems hold down the user to delete. On IoS systems rub the user to the right. Confirm the removal.

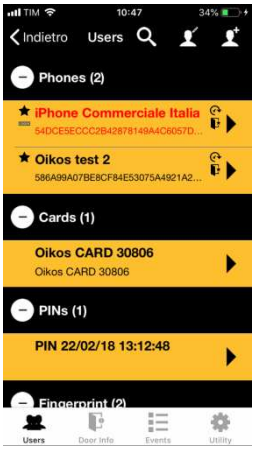
## USER SETTING

From the users' list choose the user to set.

Every kind of user (Smartphone, card, PIN, fingerprint reader, Invitation) enjoy the same functions and settings, except in the cases indicated as follows.




23




24

24

**User Name :** Click on the field Name to assign an identifying name to the Smartphone or Tablet (maximum 32 characters) (23).

**User Type:** Select if the user is a standard user or a VIP user (23).

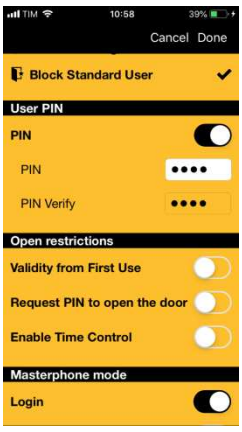
**VIP User:** he can always open the door, with no limits. He is entitled to block the access to standard users. He can also enable the Passage mode.(see page 15)

**Standard User:** he can be disabled by the VIP Users. He can enable the Passage mode.

In the users' list, the VIP user is marked by the symbol ★ (24)

**Functions:** It allows the user to enable the Passage mode (see page 16) and to block the access to standard users (see page 15) (23). Only VIP users can block the access to standard users. The possibility to activate the Passage mode is indicate with the , the possibility to block a user is indicated with the (24).

**User PIN (only for Smartphone users):** The access of a user via Smartphone can be made safer with the creation of a PIN code to enter on the keypad of the Smartphone at the time of opening, if set in the opening restrictions. (25)




25

The presence of a User PIN code is indicated with the icon (24)

Opening Restrictions: This setting allows limiting the access to users. Restrictions may be assigned to every user, for example limiting the validity of their authorization in terms of time. The access may be set only for a defined amount of days or since the first entrance or at a defined time zone (for example, the cleaning staff is authorized to open the door only one day a week at a defined hour). Two time slots can be set for each user.

The icon indicates the opening restriction, if any (24)

Masterphone Mode (only for Smartphone users): The Masterphone Mode allows the smartphone user to enter the programming mode without needing the physical presence of the Admin Card which is replaced by the Smartphone. In this way the user becomes the administrator of the system.

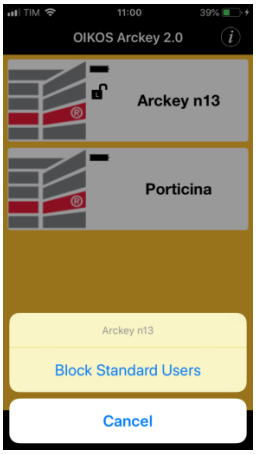
If configured, the use of Masterphone mode can be made safer by the activation of a User PIN code.

The activation of the Masterphone mode is indicated with the icon Login LOGIN or by the icon Login + PIN LOGIN if the PIN code is enabled (24)

## BLOCK STANDARD USERS

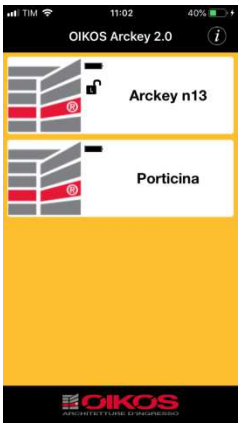
This function, when activated, prevents access to all Standard users. When the setting “Block Standard Users” is activated only VIP users can open the door.

Touch and hold down the button which identifies the door on which the user wants to set the function “Block standard users”. The menu to activate/deactivate the function will appear. (26)



26

Inside the white button a symbol ★ indicating the enabled function will appear (27)



27

28

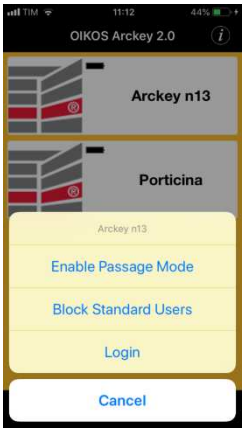
Perform the opposite action to deactivate the function (28)

## PASSAGE MODE

The enabled Smartphone users (see page 13) can activate the passage mode from the home screen of the APP. In this operating mode the opening and closing of the bolts can take place only through the mechanical key of the cylinder.

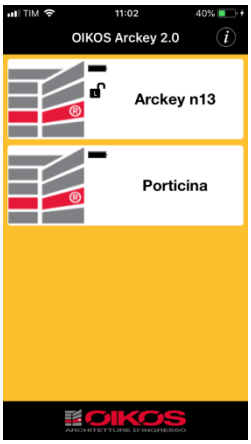
**In this operating mode the door is closed but it's not secured.**

Touch and hold down the button identifying the door on which the user wants to enable the Passage Mode. The menu to activate/deactivate the function will appear (29)



29

Inside the white button a symbol indicating the enabled function will appear (30)



30

31

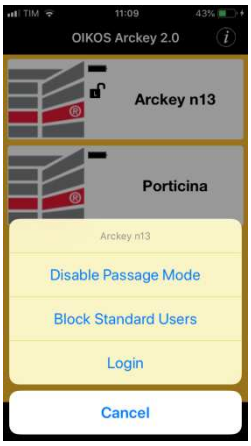
Perform the opposite action to deactivate the function (31).

See also page 21 for a scheduled management of the Passage Mode.

## MASTERPHONE MODE

This function allows the user to enter the programming mode directly from the Smartphone, without using the Admin Card. The user actually becomes the Administrator of the System.

**Touch and hold down the white button identifying the door on which the user wants to enter the programming mode with the login.** The menu will appear (32)
Push Login to Login.



32

The security of the door may be increased by adding a User PIN to the Login function. (see page 14)
In this case the PIN is required to authorize the access.

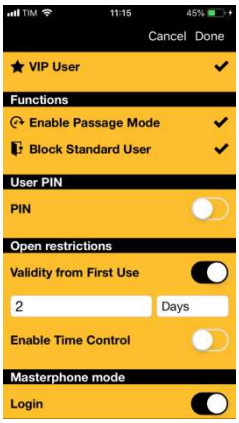
## OPENING RESTRICTIONS

There is the possibility for every user to set time restrictions to the opening of the door defining its duration or time slots.

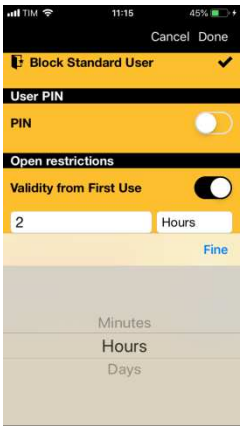
**Validity from the first use:** this command allows to assign a "fix-term" validity.

For example, it may be necessary to assign a two-day limited access to a technician for maintenance issues. Upon the expiry of the second day the access will be inhibited. Enable the function "Validity from First Use" (33) and assign a duration in terms of days/hours/minutes starting from the first opening of the door (34).

Push on Done at the top right.



33

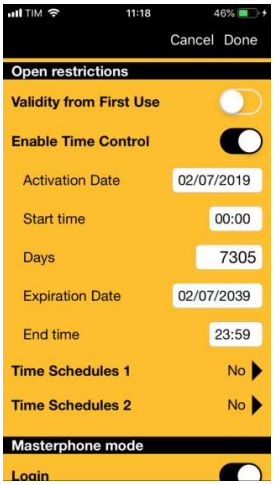


34

**Enable time control:** It allows assigning a time duration for a user (from a date to a date).

Activate the function "Enable Time Control (35) and indicate a start and end day and hour (the end date is calculated automatically if the number of the days of duration are indicated). The default is twenty years (7305 days).

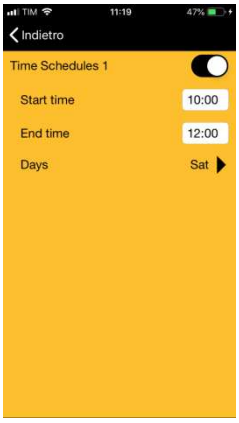
As illustrated below, this user will have unrestricted access to the door for a duration of twenty years starting from the midnight of 02/07/2019



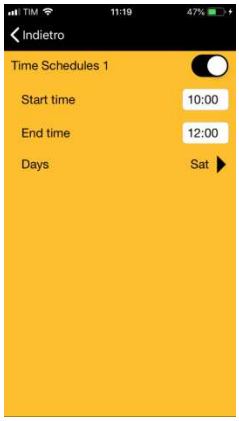
35

**Time Slots:** They allow to control restrictions in a more precise way, within the validity period. It's possible to indicate which are the  days of the week and the time slot in which the restriction is enabled.

Example: the cleaning staff is authorized to access for a period of 20 years but only on Saturday from 10.00am to 12.00 am (36-37)



36



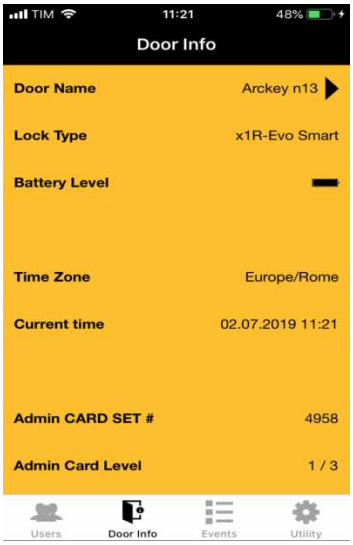
37

There can be two different time slots for a more flexible programming of the access restrictions.

Once you configure the validity period and every possible time slot, click on Done at the top right.

## DOOR INFO

The section “Door Info” shows the list of the information concerning the door connected to the device:



38

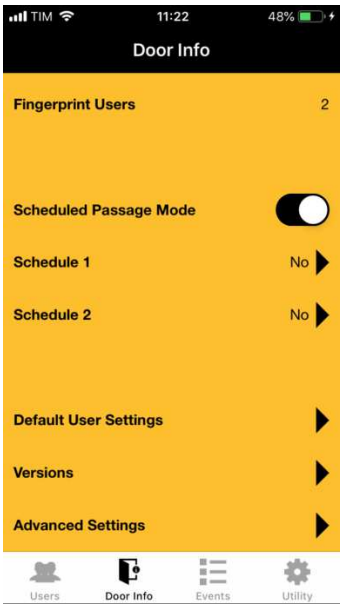
**Door Name:** it can be personalised by replacing the default door number. The new name will appear in the home screen of the App (38)

**Battery Level:** it indicates the charge level of the batteries inside the lock: Ok, Low, Very Low, End (38)

**Admin CARD SET#**: it indicates the number code, reported on the back of every card identifying the set of cards used (38)

**Admin Card Level:** it identifies the security level of the active card (38)

**Users in memory:** The total number of saved users divided into categories (maximum 300) (38)



39

**Scheduled Passage Mode:** It allows to activate the Passage Mode with time slots setting programs 1 and 2(see page 21) (39)

**Default User Settings:** it allows to define which functions the user wants to attribute by default to the new users (VIP or Standard Users, opening restrictions etc…) (39) (see page 13)

**Versions:** The versions of the lock components are reported (useful in case of assistance need) (39)

**Advanced Settings:** They are technical parameters to use **only** on request of the Technical Assistance.

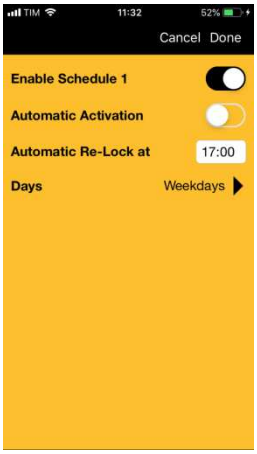
Use is not recommended for a non-technical staff.
The modification of the parameters in the Advanced Settings can modify or compromise the functioning of the lock.

## SCHEDULED PASSAGE MODE

With this function the user can set 2 programs, to enable and disable automatically the Passage Mode.
This means that the lock will enter automatically the Passage Mode, following up to two scheduled programs.

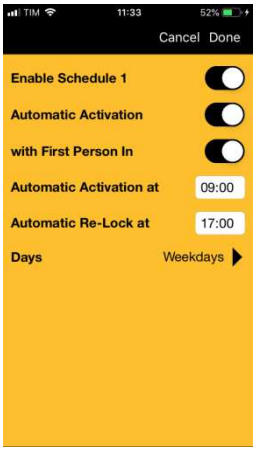
Enter the programming mode and open Door Info (see page 6).
Enable Schedule 1 to start configuring (for Schedule 2 the same rules apply).

According to needs, 3 different modes of the Passage Mode:



40


41



42

**Passage Mode with Automatic Re-Lock:** With this mode the activation is made manually by an enabled user (see page 12), but the automatic Re-Lock can be programmed for a certain hour.
Select the automatic Re-Lock time and days in which the program is valid (The standard rule considers the working days, that is all the days except Saturday and Sunday).

Click on Done to confirm (40)

**Passage Mode with Automatic Activation and Re-lock:** In this mode both the activation and the Re-Lock are automatic . Select the time of the automatic activation, the re-Lock time and the days in which this program will be active . The standard rule considers the working days, that is all the days except Saturday and Sunday (41)

**Passage Mode with Automatic Activation with First Entry and Automatic Re-Lock (C):** It's like the previous point but the activation of the passage mode will occur with the first access of an enabled user. This solution is very useful for the security because it avoids that the lock enters the Passage Mode automatically, without any user inside the building or the room (for example the Christmas Day could be a day in which the passage mode is activated automatically, but in this case it wouldn't be activated!) (42)

## EVENTS

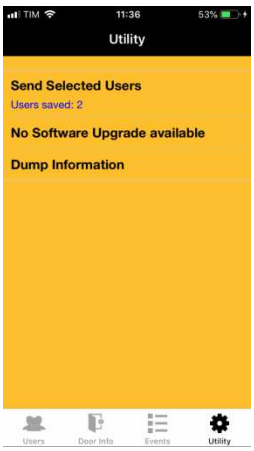
The page Events shows the list of last 1000 events relative to the door (43)
As “Events” is intended every mechanic, electric or electronic action occurred in the lock.

43

It’s possible to make a quick search entering the desired value on the appropriate field “search” after clicking on the magnifying glass icon 🔍 in order to filter the events (for example all the events connected to an ID card).
The list can be sent via e-mail after clicking the icon ✉ at the top right.

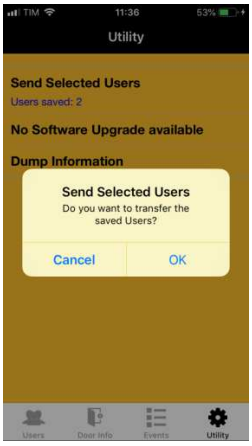
## UTILITY

In the page Utility it's possible to access to the maintenance functions:



44

**Send Selected Users:** The users copied in the phone memory can be transferred to another Device (see page 12).
Enter the programming mode of the lock from which the user wants to copy the users (see page 7).
In the Utility page press the key "Send Selected Users" (44).
Click OK on the confirmation request (45).



45

**Software Update:** control and download the App updates.
If an update is available click on the button to update the software of the lock (42)
Keep the mobile close to the door until the software is updated.

It is suggested to download always the updates released by Oikos to keep the system aligned to the maximum security and performance standards.

**Dump Information:** It allows to forward via e-mail all the lock diagnostic data. To use ONLY if specifically asked by Oikos Assistance Centre (44).