ISEO

ARGO

USER MAUAL

Argo 2.7

ISEO

About this manual

Dear Customer,

Thanks for choosing this innovative ISEO product, designed and developed following the highest standard of production, for an effective user-friendly and, at the same time, powerful and flexible access control.

This manual explains, in an easy and intuitive way, the functions, configurations and characteristics of *Argo* and the *ISEO Zero1* Access control devices, Smart series.

For commercial documents, technical documents and certifications, refers to the *ISEO Zero1* website at the following link:

http://gamma.iseozero1.com/en/controllo-accessi/

Notices

- Please read this manual before using *Argo* to ensure a safe and proper use.
- Images and screenshots may vary by device, software or service provider.
- Applications and their functions may vary by country, region or hardware specification.
- *Argo* is supported only in the official releases of *iOS* and *Android*. ISEO is not liable for performance issues or incompatibilities caused by jailbroken phones.

Information icons

For an easy reading of the manual, take note of the following icons:

CAUTION: important information or situation that could cause damage to your device or other equipment.

NOTE: notes, suggestions and additional information.

How to use this manual

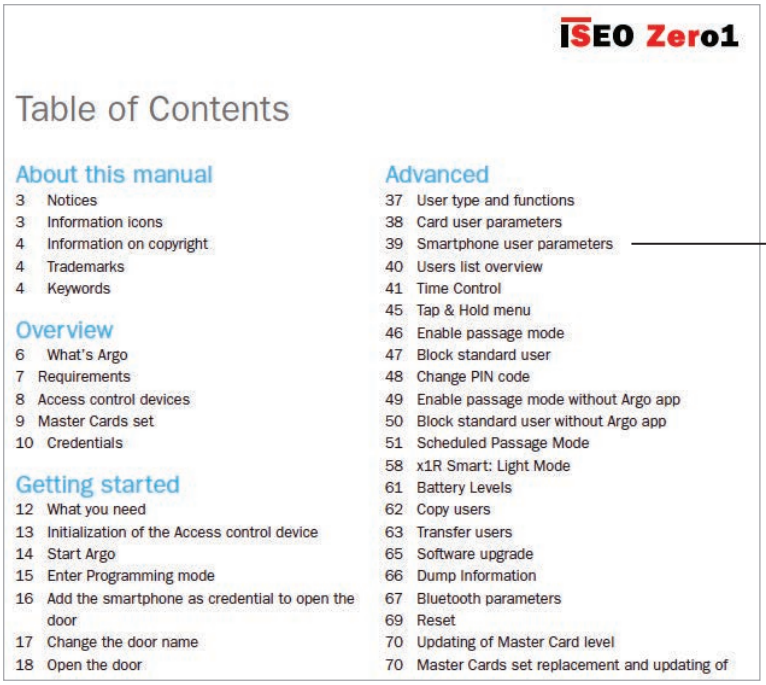


Table of Contents

In the *Table of Contents*, click on the argument or page number, to directly go to the related paragraph or chapter.

Getting Started

Start Argo

When you start the *Argo app* you will see in the smartphone display, all the *Access control devices* available, identified by its serial number.

Before starting the *Argo app* make sure *Bluetooth* is enabled on your phone.

Go back to *Table of Contents* clicking on the chapter small title.

Information on copyright

Trademarks

Keywords

- **Access Control Device**: electronic and mechanical device that allows selective access through a door.
- **Argo UID**: it is the Unique IDentifier of the Argo App installed in your smartphone. The Phone Argo UID is 16 bytes (32 characters hexadecimal).
- **Complications**: in horology a complication refers to any feature beyond the simple display of time. In the context of the Apple Watch a complication is basically a little quick access app icon set in the main watch screen (called face). Adding Argo complication you can quickly open the Argo app directly from the watch face.
- **Contactless Card**: electronic card that can be read by the *Access control device*, by simply bringing it closer to the same, without physical contact.
- **Credential**: device that allows to identify the user and authorize or not authorize access through a door. For example: smartphone, tablets, Mifare cards or Mifare tags.
- **Door**: passage which access is electronically controlled by the *Access control device*.
- **Door Opening time**: it is the time that allows the user to open the door, following an opening command. If the door is not opened during this time, it will automatically re-lock.
- **Door Status Advice**: the *Doors Status Advice* allows to see directly on the button of your smartphone if the door is left OPEN or CLOSED and SECURE.
- **Invitations**: it's the function that allows telephones to self-register in the lock as users.
- **Invitation Code**: it is the code sent by the *Invitation email* that the *User* need to type, to open the lock and self-register the phone at the same time.

Keywords

- **Light Mode**: it's a function related only to *x1R Smart* and means the lock is closed only by latch and not bolts.
- **Login**: it's the function that allows your smartphone to be able to enter *Programming Mode* without the *Master Card*.
- **Master Card**: *Contactless card* used to program the system.
- **Master Card Set**: set of three *Master Cards* numbered from 1 to 3, belonging to the same *System code*. The *Master Card* of higher number disable the *Master Card* of lower number.
- **Mifare (classic)**: it's a communication technology used in contactless smart cards and proximity cards. It works in the 13.56 MHz frequency.
- **Mifare DESFire**: was introduced after Mifare Classic with improved hardware and software security features (AES 128 bit encryption). The lastest version called MIFARE DESFire EV2 further improves security protocol.
- **Open Restrictions**: it's related to the *Argo* parameters that can be enabled to limit the temporal validity of a credential. It includes: *Validity from First Use, Time Control, Time Schedules*.
- **Passage Mode**: it's a function that allows the door to be always open for any user who wishes to gain access, without the use of authorized credentials.
- **Programming Mode**: software condition, feasible by *Master Card*, that allows software modification to the *Device*.
- **Scheduled Passage Mode**: this function allows you to set 2 schedules, to automatically enable and disable the Passage Mode function.
- **Smart Series**: *Access control device* which embeds Bluetooth radio module, to communicate to compatible smartphones by the *Argo app*.
- **System Code**: unique number associated to a *Master Card set*.
- **Time Control**: this function is used to set the validity of the assigned credential (date and time of activation and expiration).
- **Time Schedules**: in additon to the *Time Control*, you can set for each user, two time schedules that can be selected for each day of the week.
- **User**: it's the person enabled to open an *Access control device* by a credential.
- **User Card**: *Contactless card* used to open one or more doors.
- **Users List**: list of *Users* enabled to open an *Access control device.*
- **Validity from First Use**: with this function is possible to set the validity from the moment of the first use of the credential (in days, hours or minutes).
- **Widget**: generically a widget is an element of the smartphone graphical user interface (GUI) that provides a specific way for the user to interact with the operating system or an application. On Android phones widgets can be created and added to the smartphone GUI like any other app. On iOS phones widgets can be added to the *Today View* page. Argo widget is basically a shortcut icon that allows you to open your doorlock simply by tapping on it without opening the argo app (faster and easy to use).

Table of Contents

Table of Contents

Service

Appendix

Troubleshooting

Overview

What's Argo

Argo is an app for smartphone, the ideal solution for managing residential or "light commercial" environments, like bed and breakfasts, shops, small offices, small businesses, and professional studios.
By simply installing the *Argo* app on an *iOS* or *Android* smartphone, the user will have the possibility of managing, monitoring and opening all the doors upon which the Smart series ISEO Zero1 devices are installed (even at a distance of up to 10 meters), with no need for any additional software or an Internet connection. All this thanks to *Bluetooth Smart* technology, which allows the smartphone to communicate with the devices.
Using the app installed on the smartphone, the user can organise the access permissions for up to 300 users, and view the last 1000 events detected on each door (entries, attempts at unauthorised entry, etc.).
In addition to smartphones, the doors can also be opened using ISEO cards and pre-existing RFID cards (contactless credit cards, public transport tickets, access control cards, etc.).

300 USERS

Up to 300 users can be added, deleted and edited for extra functionalities. The list of users can be transferred from door to door.

1000 EVENTS

Administrators can read out the last 1000 events of each door and send the report via e-mail.

Requirements

You can find *Argo app* free for download from the *App Store* (iOS) or *Google Play* (Android).

iOS

- From iPhone 5 with iOS 10 and above (September 21, 2012).

Android™

- From version 5.0 and above (November 3, 2014).

Visit *https://app.iseo.com/* website, to find the last updated smartphone supported list and much more information about the *Argo app*.

Remember to enable the *Bluetooth* on your smartphone prior to use the *Argo app*.

Access control devices

The following ISEO Zero1 *Access control devices*, *Smart series*, are conceived to work with *Argo*.

Libra Smart

Electronic European profile cylinder of ISEO Zero1 product range. It is battery operated and can be easily installed both on new and existing doors. It is compatible with any mechanical lock with European cylinder hole and the installation doesn't require any wiring, allowing a rapid and easy replacement of any mechanical cylinder.

Aries Smart

Electronic trim set of ISEO Zero1 product range. Thanks to the flexible and simple installation, can be fit on most doors, and it is conceived to be used with the majority of mechanical locks. *Aries Smart* combined with *Argo App* is suitable for private houses, apartment blocks, light commercial (offices, single entrance of commercial, server rooms, etc...).

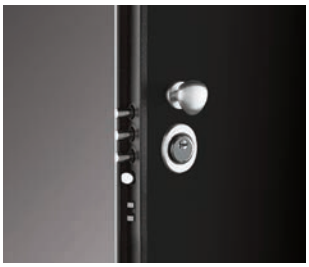
Stylos Smart LED

Credential reader of ISEO Zero1 product range. In combination with the electronic actuator it is able to control any electrical device. *Stylos Smart LED* combined with *Argo App* is suitable for private houses, apartment blocks, light commercial (offices, single entrance of commercial, server rooms, etc...).

Stylos Smart Display with Keyboard

In addition to *Stylos Smart LED* features, it has display and keyboard, to improve the user experience and interaction, and to add a PIN code to open the door.

Access control devices

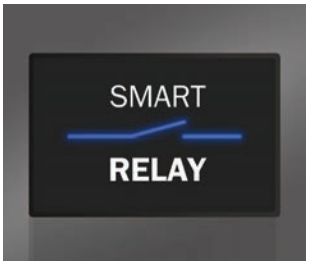


x1R Smart

Electronic motorized lock for armored doors of ISEO Zero1 product range. It works with an electric motor controlled by a powerful microprocessor and the deadbolt action is always guaranteed by the mechanical operation of the key, even in case of power supply failure.

Smart Locker

Smart Locker is a lock that can be installed on a wide range of lockers and cupboards to keep people's property safe while they're in the office, in the gym, swimming pool, or any other situation where personal belongings need to be temporarily safeguarded.



Smart Relay

The Smart Relay allows to open electric locks, motorized gate or any electrical actuator which can be activated closing a contact. The Smart Relay close a contact if a smartphone is registered in the device.

To simplify the reading of this manual, pictures and descriptions are mainly referred to **Libra Smart**. The same information are also applicable to the other *Smart series* devices. Any differences will be properly specified.

Master Cards set

Master Cards are used to configure and manage the *Access control system*. The set of *Master Cards* consists of 3 cards numbered from 1 to 3.

Each set of master credentials has a univocal system's code. During the initialization phase with *Master Cards*, the system's code and the relative set of *Master Cards* is associated to the devices.

An improper method and sequence of use of the master credentials could damage the system; therefore we recommend to pay attention to use it in the right way.

Note that only *Master Card 1 and 2* can initialize the system. *Master Card 3* must be considered as the updating card for the new *Master Card Set*, since its loss could irreversibly compromise the possibility to modify or update the system.

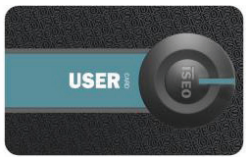
In case a *Master Card* is lost or damaged, see the related chapter *Updating of Master Card level and Master Card Set replacement*.

If you loose *Master Card 1 and 2* it is strongly recommended to purchase a new set of *Master Cards*.

Overview

Credentials

ISEO cards or legacy *Mifare* cards, *Mifare DESFire* or ISO14443 A or B cards with UID (Unique IDentifier) or tags, can be used as door keys. Just present the credentials a few centimeters from the reader. The *ISEO cards* are more secure than legacy cards as they have the UID protected and encrypted.



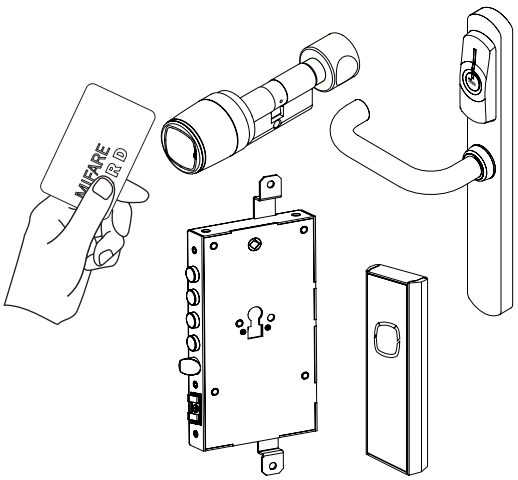
ISEO cards
(Mifare Classic or DESFire)

Tags

Mifare cards
Mifare DESFire (UID reading only)

NFC phones
(NFC static UID required)

Used to “activate” the device.



Mifare is a brand of contactless card with several card types: Classic, Ultralight, DESFire...
All *Mifare* cards works in *Argo* by reading the UID (unique identified number).

Notes on NFC Phones

- *ISEO Smart Devices* are able to read the UID of NFC phones in Mifare card emulation.
- The UID is generated from the *NFC Secure Element*. The *Secure Element* can be either embedded in the phone, by the phone manufacturer, or in the SIM, supplied from the *Mobile Telecom Operator*. ISEO cannot track all possible combinations (phones models and mobile operator SIM), in this fast evolving technology world.
- The UID must be static (always the same). We are aware that many phones generate a random (rolling) UID, which might depend from the SIM or from the embedded *Secure Element* in the phone, and this will, in most cases, depend on the phone configuration. Phones random UID will not work on the doorlock, as the UID is memorized, but the second time will not open as it is different.
- Some smartphones generates random UID at each connection while others use the same UID for all phones of same brand or model. In this case if a phone is memorized by NFC, all the other with same UID will open the door as well. ISEO cannot control this situation and as consequence the security.
- ISEO cannot guarantee that the UID is not replicated or emulated from other devices or phones, as it is always readable from the phone, and it is transmitted not encrypted to the doorlock.

Notes on Mifare Cards UID

- ISEO *Smart Devices* are able to read the UID of Mifare card.
- Iseo cannot guarantee that the UID is not replicated or emulated from other devices or phones as it is always readable from the card and it is transmitted not encrypted to the doorlock.

Note about ISEO Cards

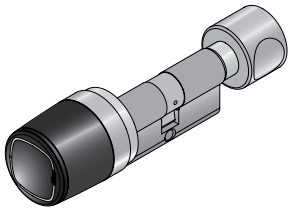
ISEO Cards is a particular Mifare Card (1K), specifically developed by Iseo, with an encrypted UID. This allow an higher level of security in the trasmission between the card and the doorlock.

As result of the above notes

To obtain the best security, ISEO recommends to use for phone the *Argo app,* and for cards the ISEO Cards.

Getting Started

What you need



Access control devices, Smart series.

Argo app installed on your smartphone.

Master Card set.

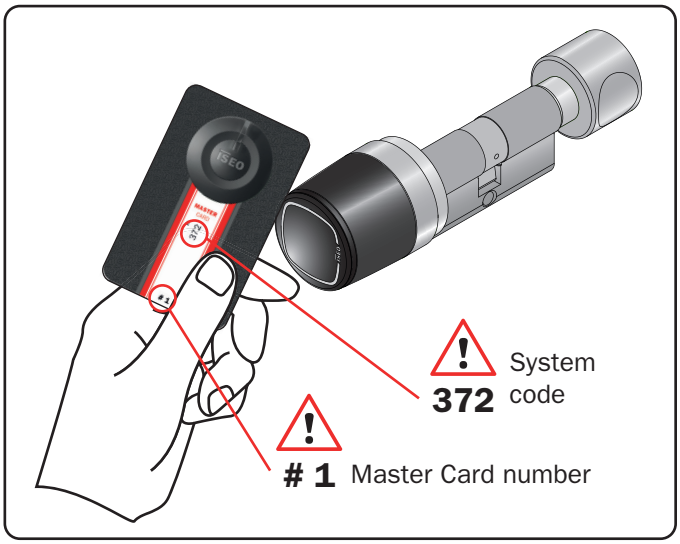
Set of User cards.

Initialization of the Access control device

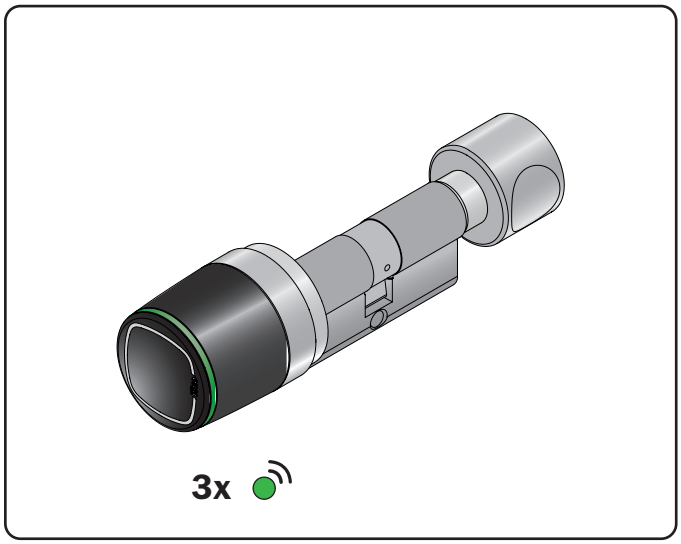
The new device is in *Factory mode* configuration, meaning with the list of authorized user empty and no system code yet assigned.

A *Factory mode* configured device can be opened by any Mifare card or tag. The orange light flashes 2 times, before the standard opening signal, to show the device not initialized.

The system initialization take place through the programming of the *System code*, using the *Master Card 1*.



1. Bring *Master Card 1* closer to the device.



2. The device emits 3 acoustic signal together with 3 green light signals.

For the system's initialization, use exclusively *Master Card 1*, and put cards 2 and 3 in a safe place. The use of *Master Cards 2* and 3 will be required only if *Master Card 1* is lost or damaged.

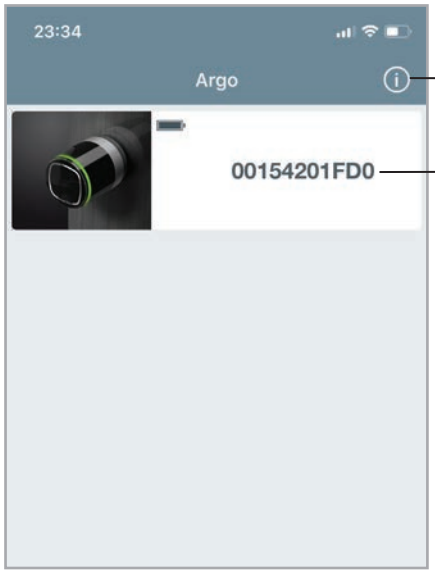
All *Access control devices* must be initialized or updated with the same *Master Card*.

Note that only *Master Card 1 and 2* can initialize the system. *Master Card 3* must be considered as the updating card for the new *Master Card Set*, since its loss could irreversibly compromise the possibility to modify or update the system.

Start Argo

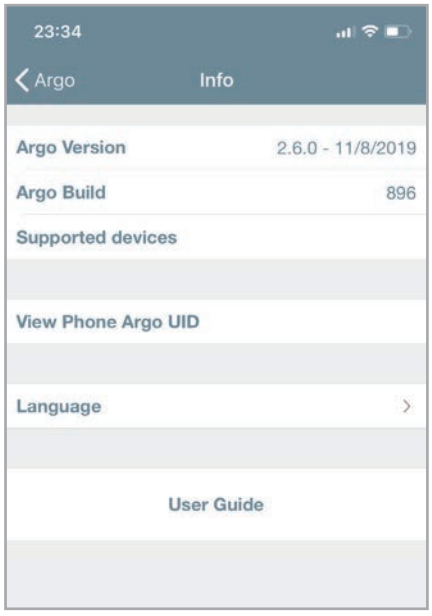
When you start the *Argo app* you will see in the smartphone display, all the *Access control devices* available, identified by its serial number.

Before starting the *Argo app* make sure *Bluetooth* is enabled on your phone.



Info app menu

Available *Access control device* up to a distance of 10mt.



Info app menu

Information on the app version and the software of the ISEO devices, that are supported from the app.

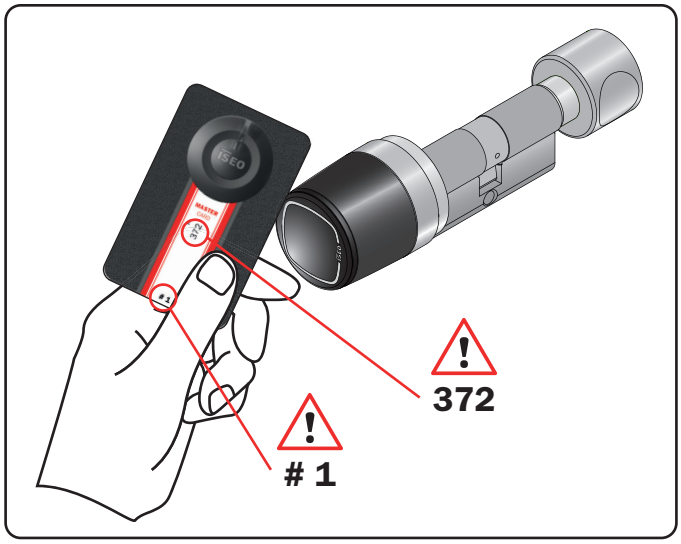
To know more see *Advanced, Add Phone with Argo UID*

To change the app's language.

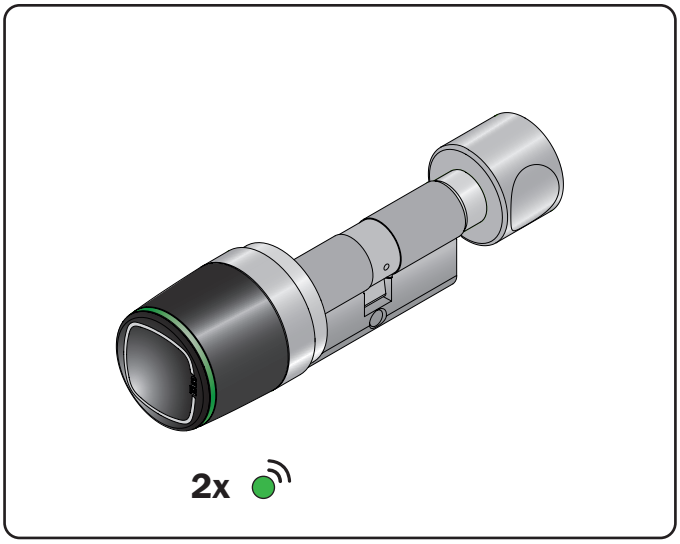
Link to *http://app.iseo.com/*
In this website you can find this manual and much more information about the Argo app.

Enter programming mode

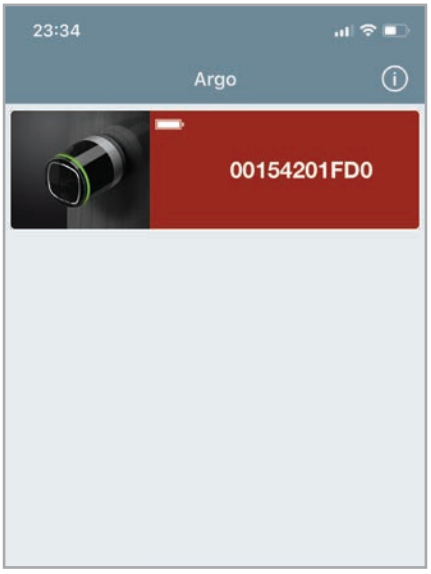
Present the *Master Card 1* to the device: the button in the app will turn red, and pressing it you will enter in *Programming mode*.



1. Present the *Master Card 1* to the device.



2. The device emits 3 acoustic signals together with 2 green light signals.

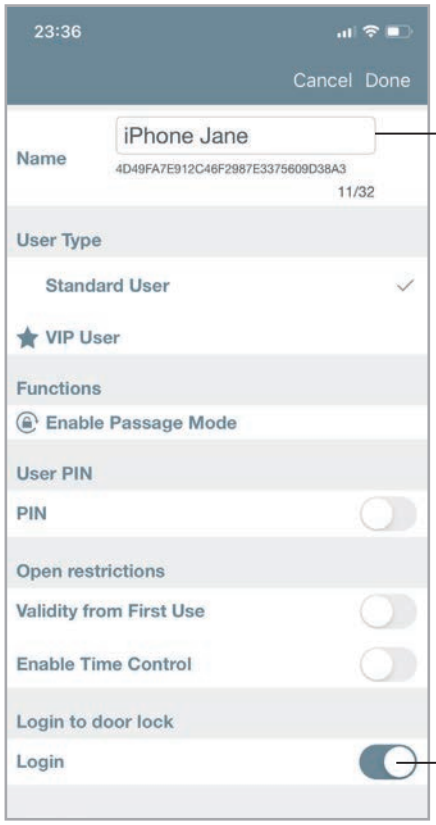


3. The button in the app will turn red. Press it to enter in *Programming mode*.

To know more about the *Bluetooth* technology and the *Argo* feature, called “in-app pairing”, see the related page in the *Advanced* chapter.

Add the smartphone as credential to open the door

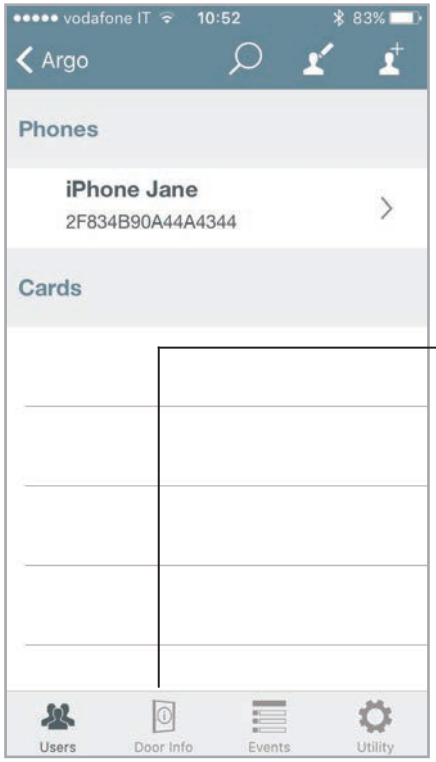
As soon as you enter in *Programming Mode* the app requests to add the smartphone as credential to open. This operation has to be done for each smartphone you want to memorize in the door.



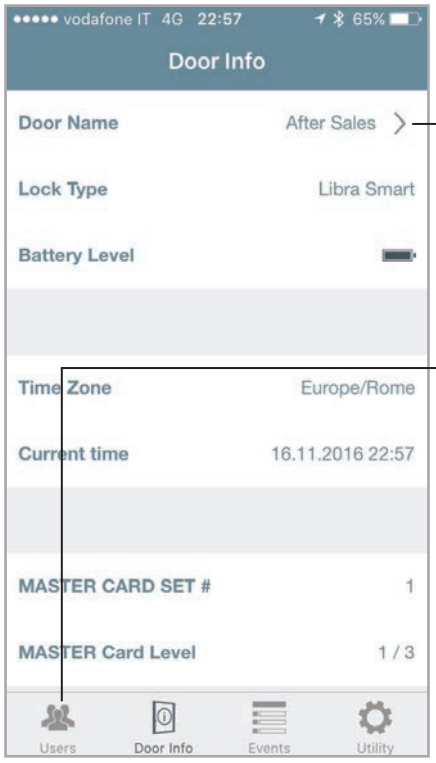
1. Change the name of your phone.
2. Tap **Done** to memorize your phone as opening Credential.
3. Tap **Cancel** if you decide to not memorize your phone now.
4. Enable **Login** if the user is also the *System Administrator* (to know more about Login go to *Advanced, Administrator login without Master Card* and *Login (without Master Card*).

5. You can see your phone appearing in the *Users list*.

Change the door name



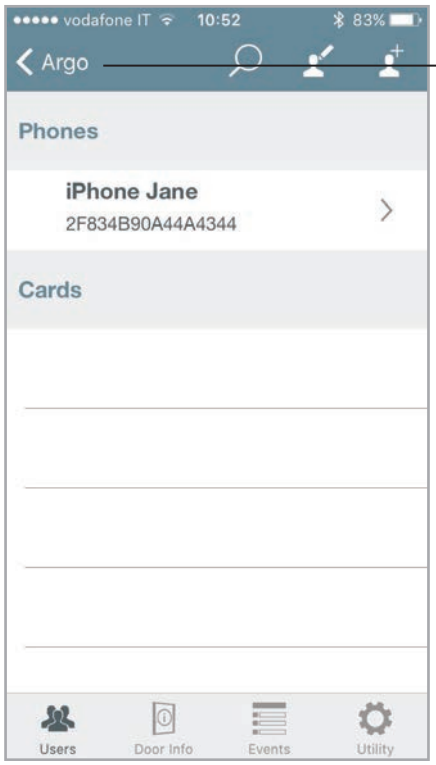
1. Tap **Door Info** and then **Door Name** to give a real door name to the lock.



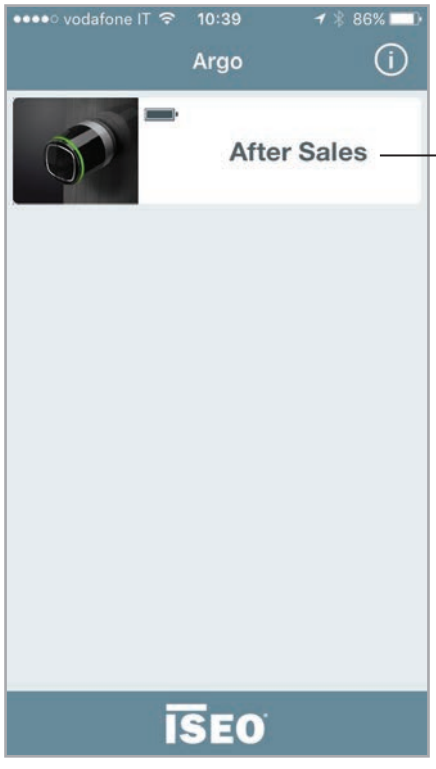
2. Change the name and confirm.

3. Tap **Users** to go back to the main menu.

Open the door



1. Tap **Back** to exit *Programming mode*.

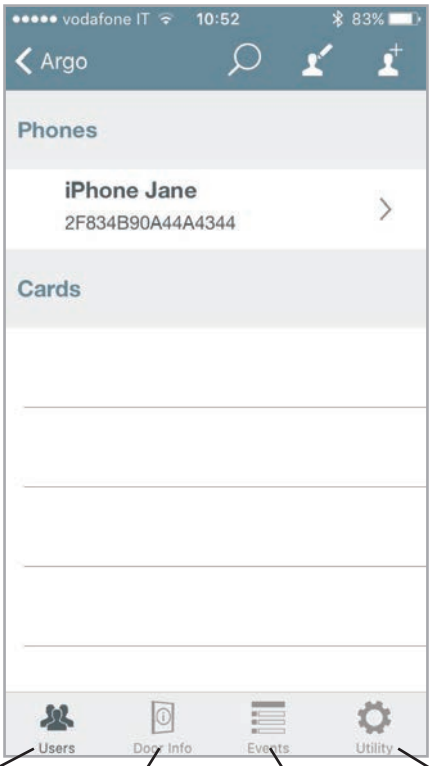


2. Tap the icon button to open the door.

Basics

Users menu

Enter *Programming mode*. The display shows the *Users list* as main menu. You can move to other menu by pressing the icons in the bottom bar. To exit *Programming mode* you need to go back to main menu first.



Users

- Show the users list
- Add Users
- Search Users
- Delete Users

Door Info

- Change the door name
- Show device information
- Scheduled Passage Mode
- Advanced Settings

Events

- See the last 1000 events
- Search events
- Send events by e-mail

Utility

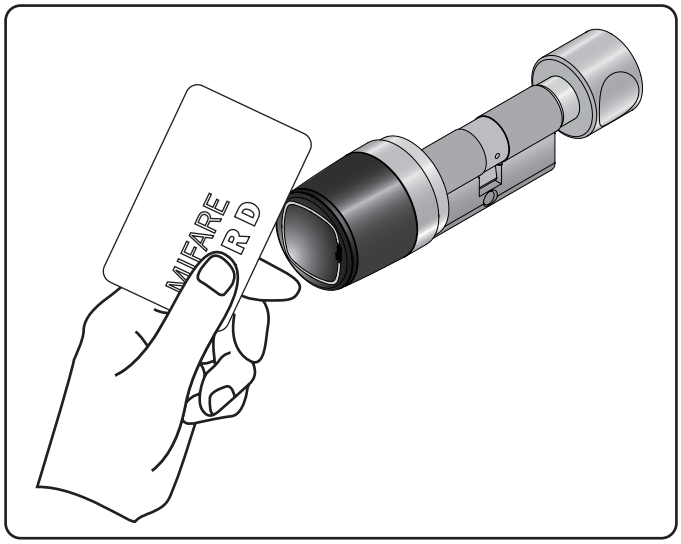
- Transfer the users list
- Software upgrade
- Dump information

To enter the *Users menu* it is always necessary to present the *Master Card* to the device.

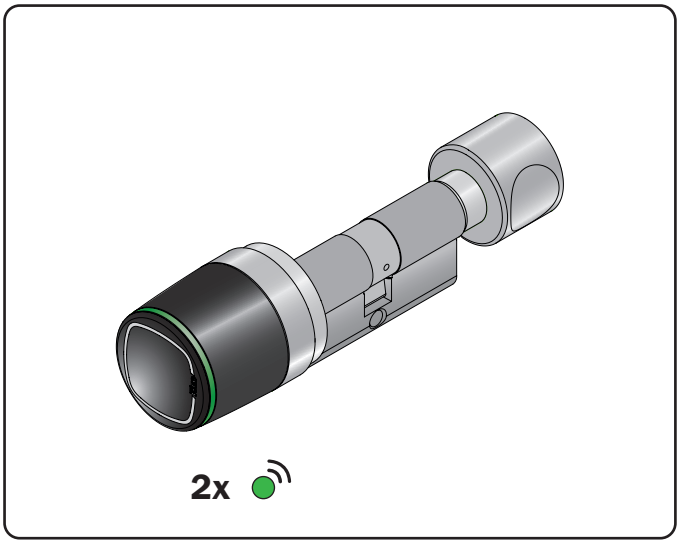
Basics

Add users

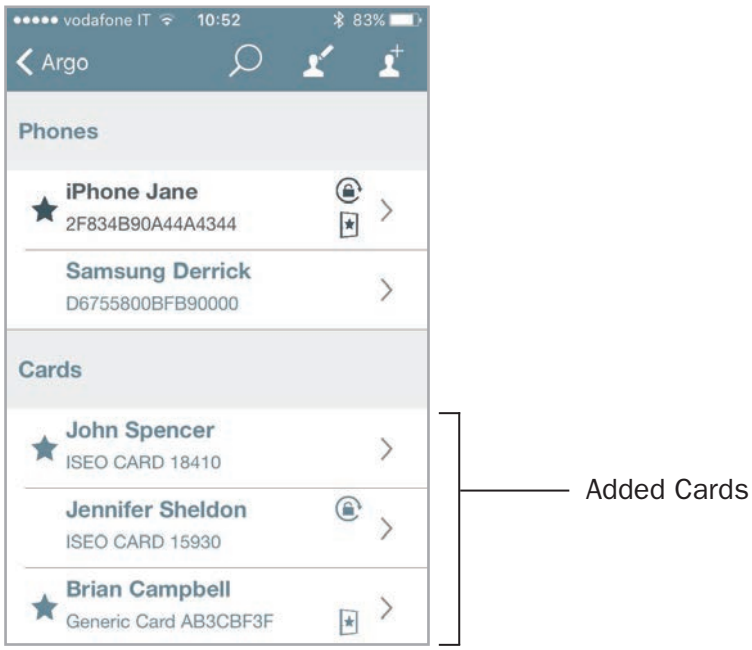
Enter *Programming mode* first. You can then add users just presenting the credentials to the device, and those will be displayed in the smartphone.
Last card will be on the top of the list. You can read ISEO and Mifare cards, tags and enabled NFC phones (NFC static UID required).



1. Present the card to add to the device.



2. The device emits 2 acoustic signals together with 2 green light signals.

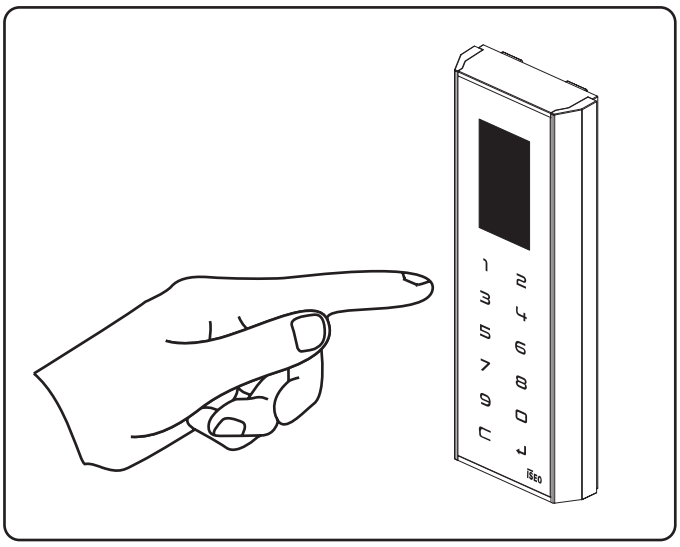


Basics

Add PIN users

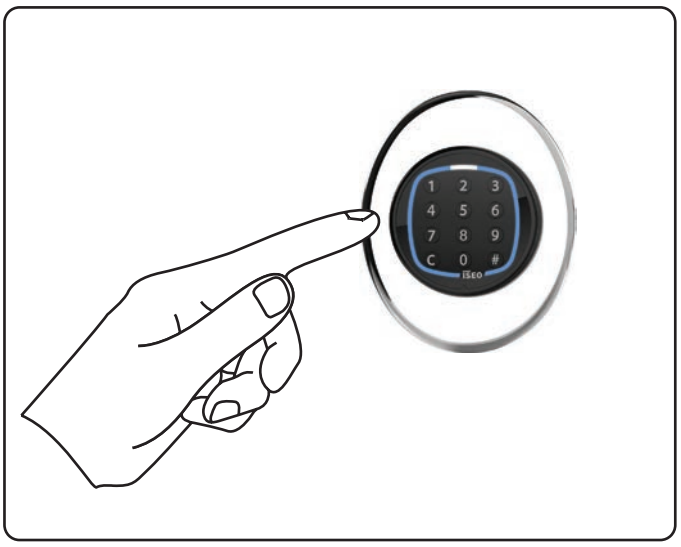
On *Stylos Smart Display* and *x1R Smart*, you can also add a *PIN code* as credential to open, using the keyboard available on both devices. Enter *Programming mode* first. You can then add the PIN just entering the code in the keyboard. Last PIN will be on top of the list.

STYLOS SMART DISPLAY

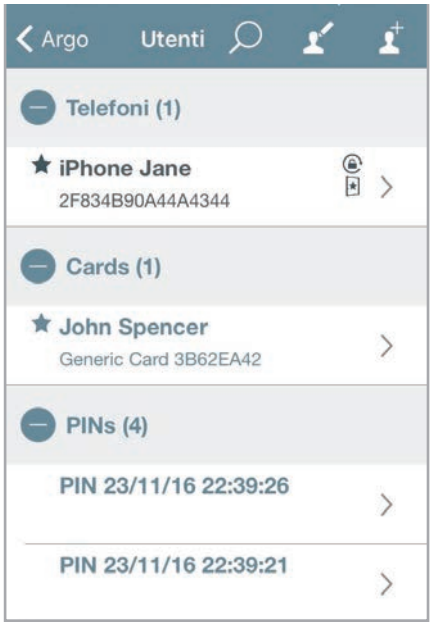


Enter your PIN code, from 4 to 14 characters, and confirm by enter ↵. Press **C** to clear all the numeric code.

x1R SMART



Enter your PIN code, from 4 to 14 characters, and confirm by enter **#**. Press **C** to clear all the numeric code.

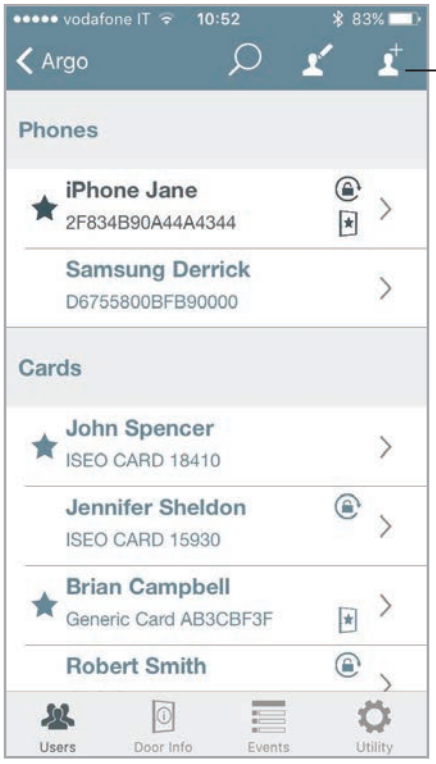


Added PINs are visible in the Argo app with name *PIN* plus *date & time* of when they were added.

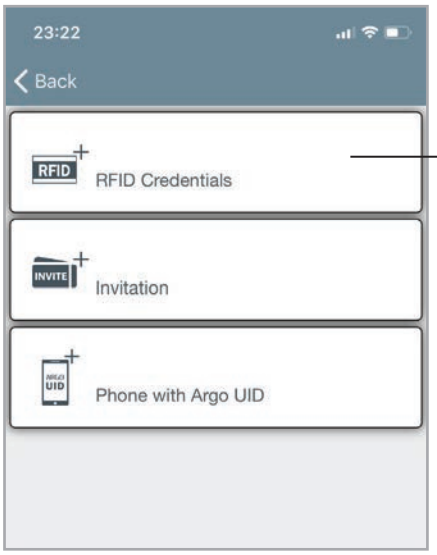
For security reasons PIN codes are never visible in the Argo app: neither in the *Users list*, nor in the historical *Events*, nor in the *Dump Information* (see *Dump Information* specific paragraph).

Add users typing ISEO card number

Enter *Programming mode*. You can add users without having the card or the tag, just typing the ISEO card number. This can be useful if you have already distributed the cards to the users.



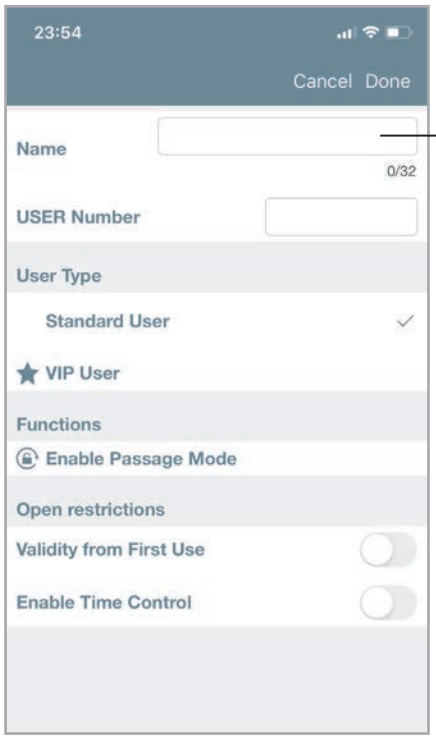
1. Tap the *add user* icon 



2. Tap **RFID Credentials**

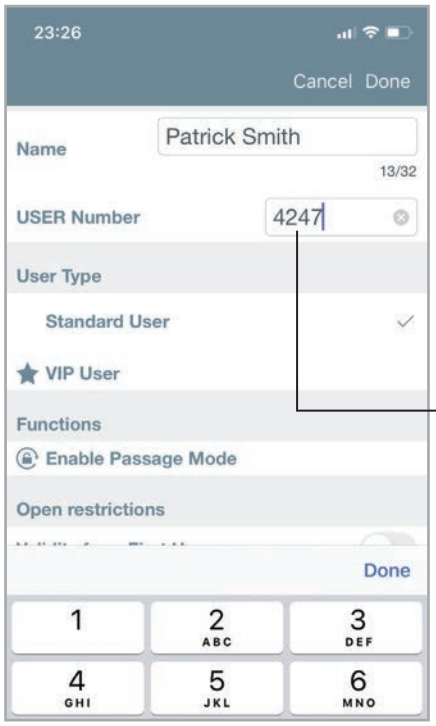
Add users typing ISEO card number

3. Choose **USER DESFire** or **USER Classic**.
Both are ISEO cards: the first is related to *Mifare DESFire*, while the second to *Mifare Classic*.
To know more about *Mifare DESFire* go to *Advanced* then *Mifare DESFire cards*.



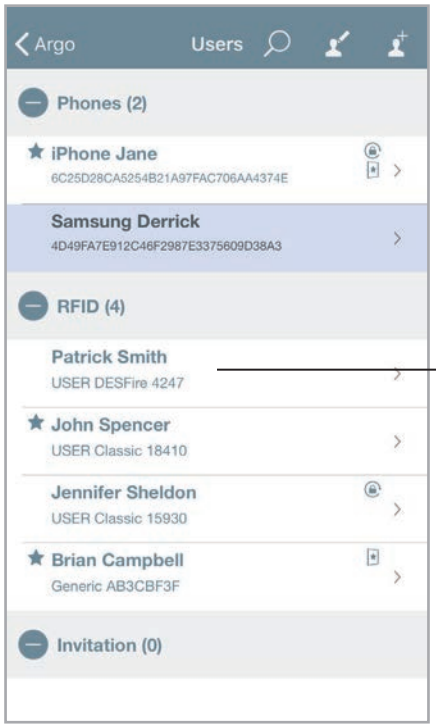
4. Tap **Name** box

Add users typing ISEO card number



5. Type the user name and the ISEO card or tag number.

6. Tap **Done** to confirm the operation.

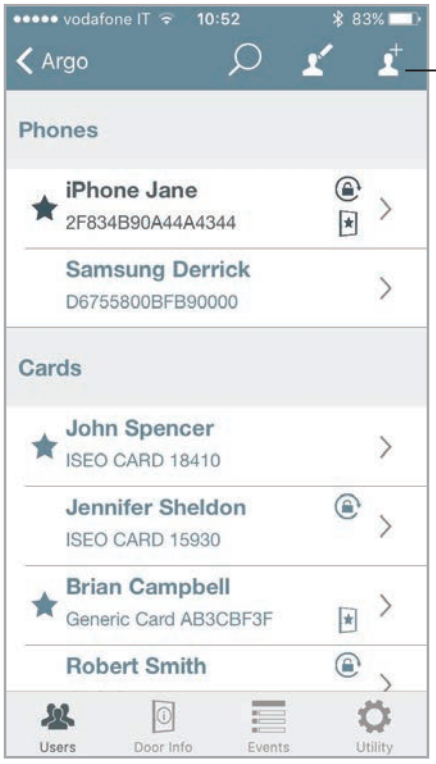


7. The ISEO card is added to the *Users list*.

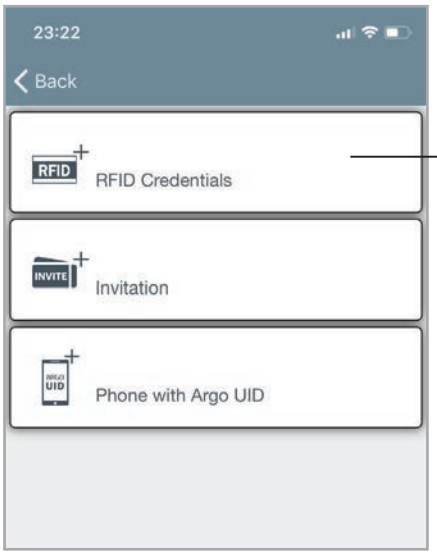
This function is only available using ISEO cards and tags.

Add users typing Mifare card UID

It is possible to add a *Mifare card* to the device *Users List*, writing the *UID*, the *unique identifier number*.
This function is useful, for example, if you know the credential UID of the user that need to access the door, but you don't physically have his card, to present to the lock.

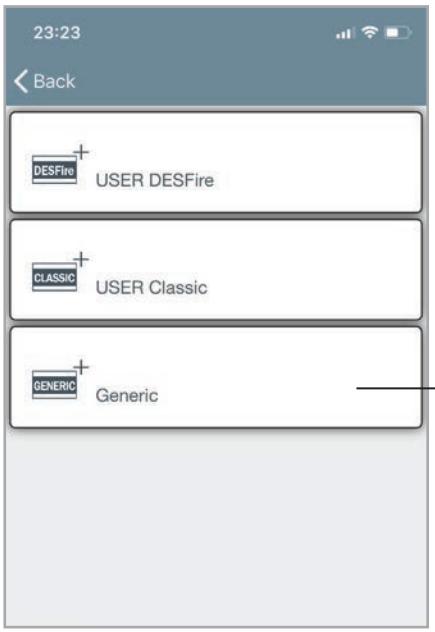


1. Tap the *add user* icon 

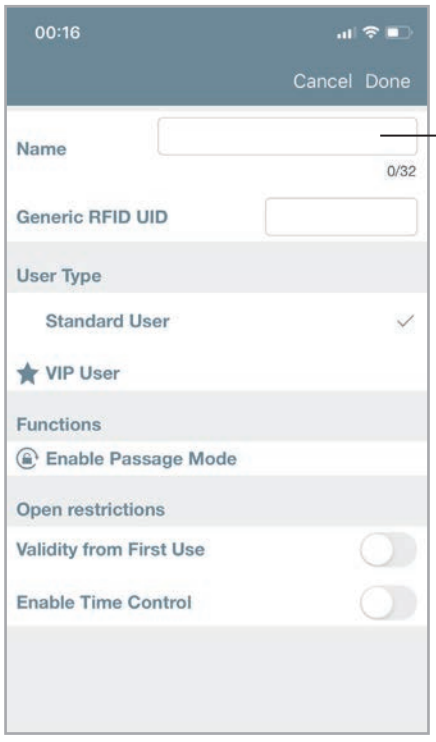


2. Tap **RFID Credentials**

Add users typing Mifare card UID

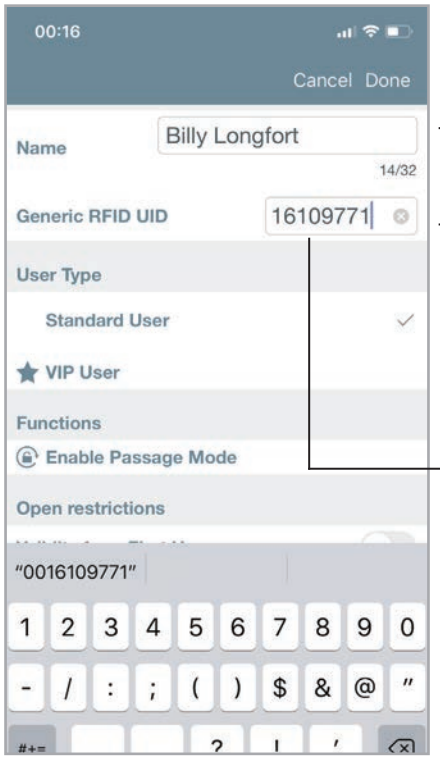


3. Tap **Generic**

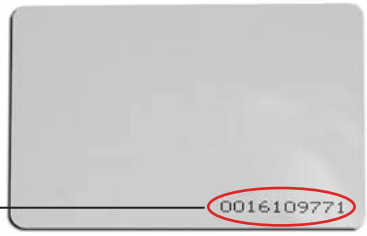


4. Tap **Name** box

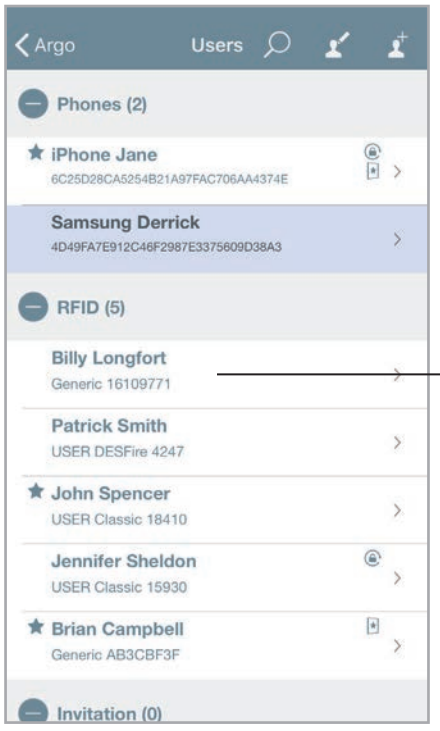
Add users typing Mifare card UID



5. Type the user name and the *Generic card UID.*



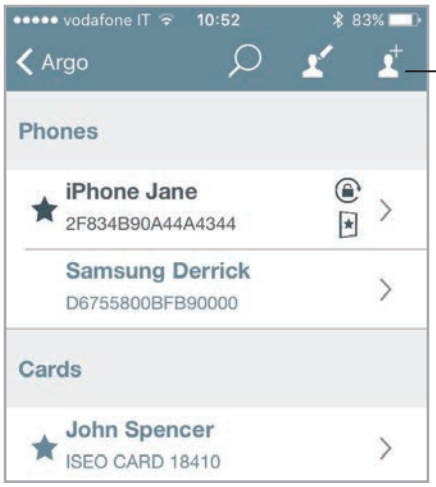
6. Tap **Done** to confirm the operation.



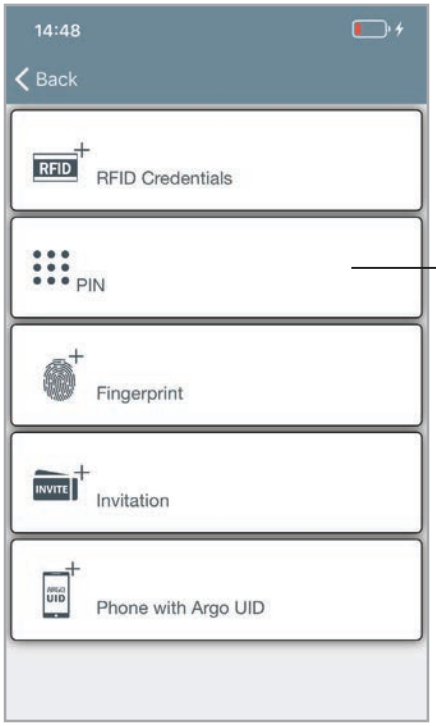
7. The *Mifare card* is added to the *Users list*.

Add users typing PIN code

On *Stylos Smart Display* and *x1R Smart*, you can also add a PIN code as credential to open, using the keyboard available on both devices. You can enter the PIN directly from the device keyboard.

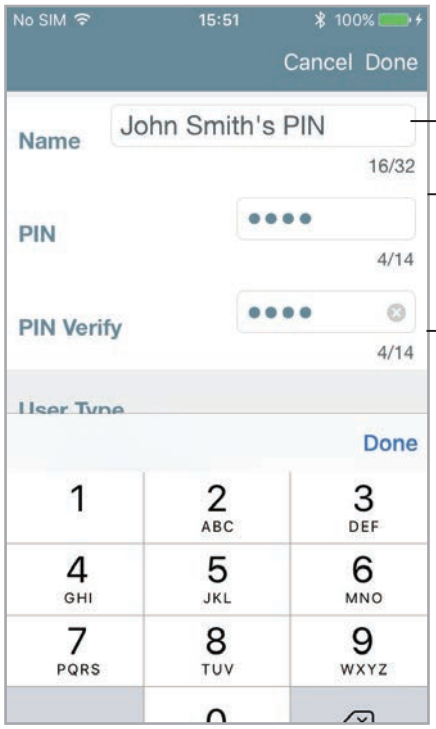


1. Tap the *add user* icon 



2. Tap **PIN**

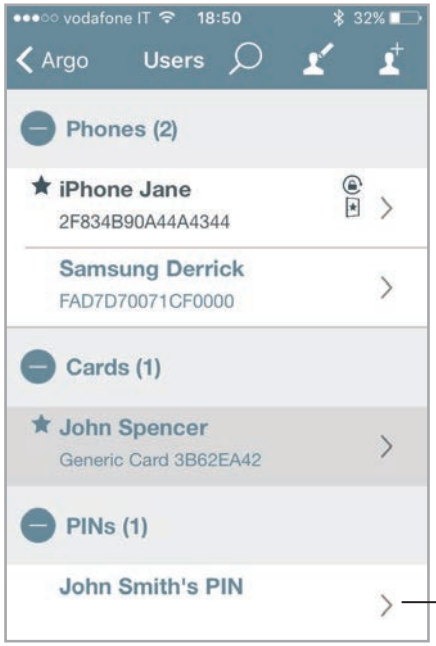
Add users typing PIN code



1. Enter the name related to the *PIN code*.

2. Enter a *PIN code* from 4 to 14 characters by device keyboard. Confirm the code in the box *PIN Verify.*

4. Touch **Done** in the smartphone keyboard to confirm the code, and **Done** in upper right corner to save the operation.

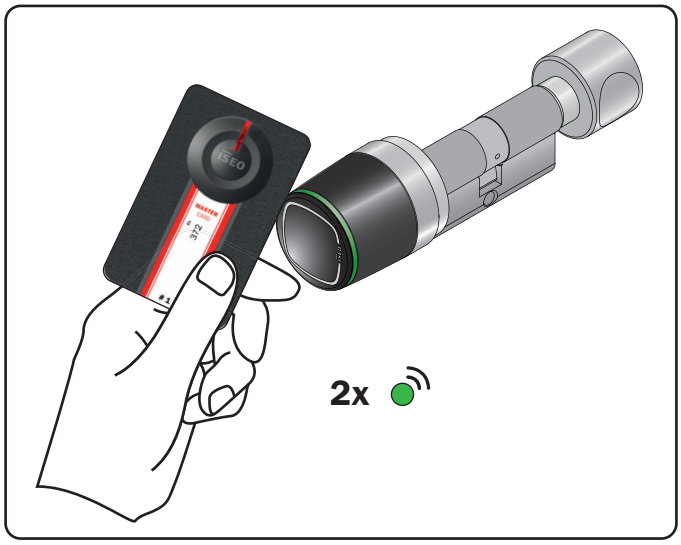


The *PIN code* appears in the *User list*, in the PIN list, with the assigned name.

For security reasons, the PIN is never visible, neither in the *Users list*, nor in the historical *Events*, nor in the *Dump Information*.

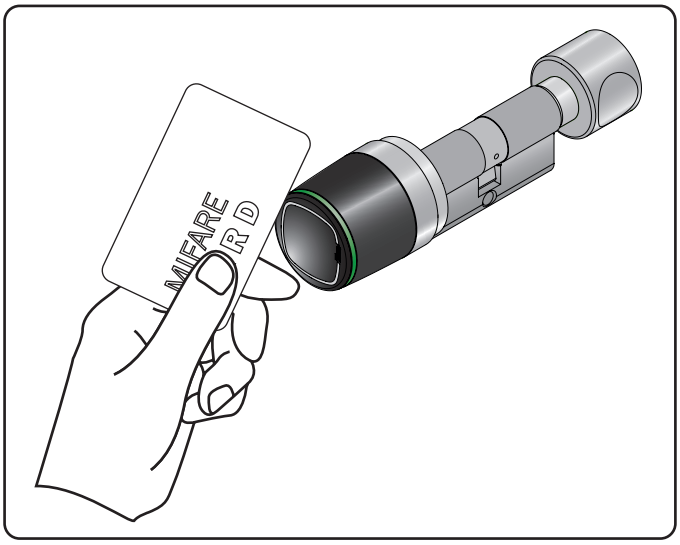
This function is only available on *x1R Smart* and *Stylos Smart Display.*

Add users without Argo app



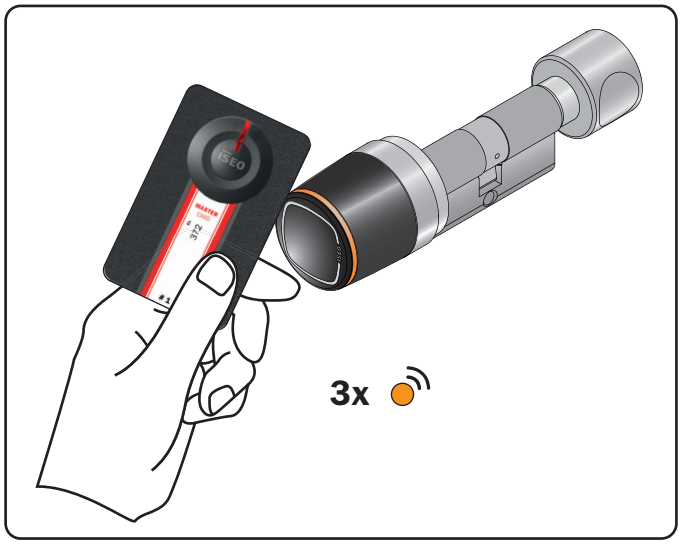
1. Present the *Master Card 1* to the device to enter in *Programming mode*.

2. The device emits 3 acoustic signals together with 2 green light signals.



3. Read the card to add to the *Users list*.

4. For each card the device emits 2 acoustic signals together with 2 green light signals, to confirm the operation.

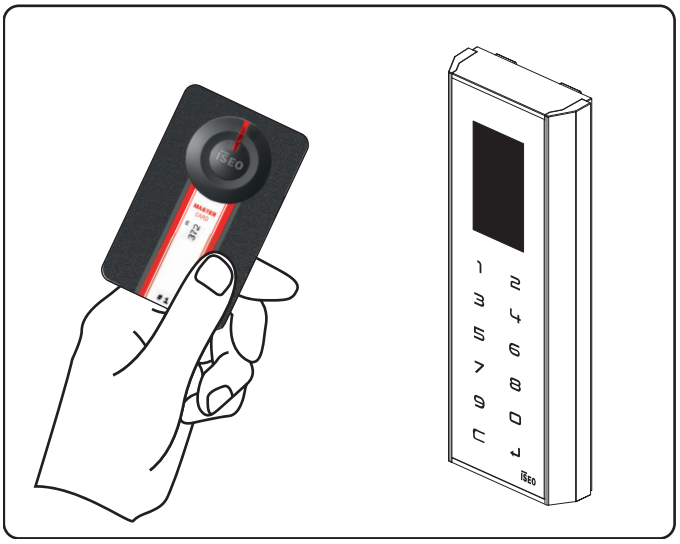


5. At the end of the operation present again the *Master Card 1* to the device to go out the *Programming mode*.

The device goes automatically out of *Programming mode* after 5min. of inactivity.

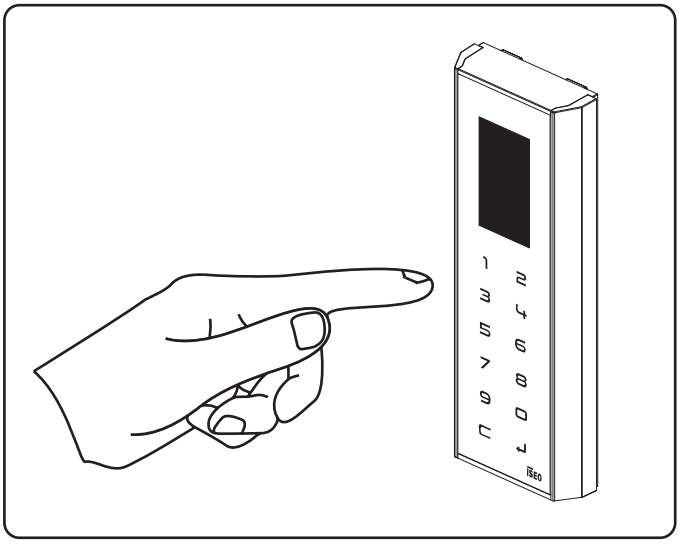
Add PIN code without Argo app

On *Stylos Smart Display* and *x1R Smart*, you can also add a PIN code as credential to open, using the keyboard available on both devices. Pictures below refer to *Stylos* but the procedure is the same for *x1R* as well.



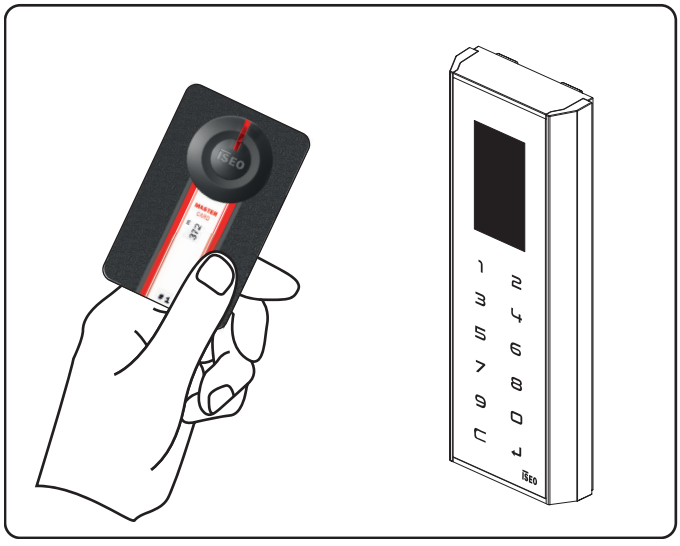
1. Present the *Master Card 1* to the device to enter *Programming mode*.

2. The device emits 3 acoustic signals.



3. Enter your PIN code, from 4 to 14 characters, and confirm by enter ↵ .Press **C** to clear all the numeric code.

4. For each memorized code the device emits 2 acoustic signals, to confirm the operation.



5. At the end of the operation present again the *Master Card 1* to the device to go out the *Programming mode*.

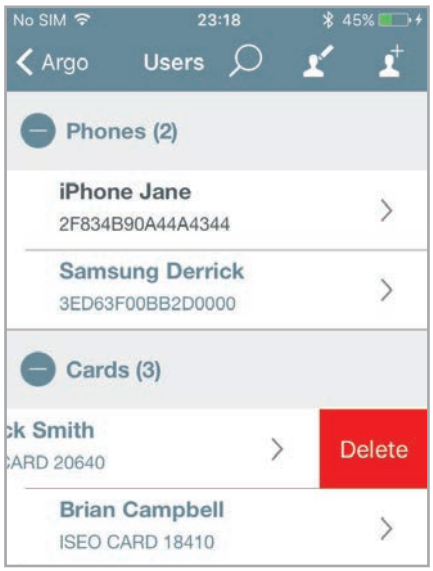
The PIN code must be from minimum 4 to maximum 14 characters.
This function is only available on S*tylos Smart Display and x1R Smart*.

Delete users

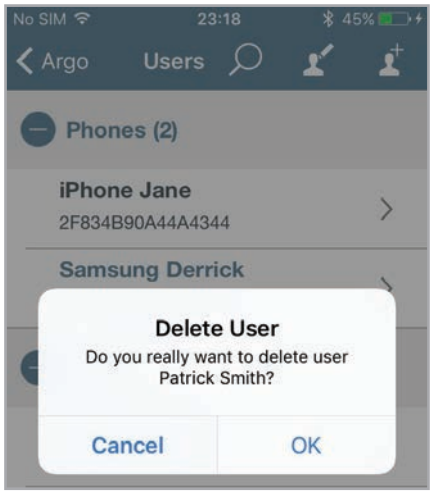
There are two ways to delete users from the user list:

- Single user delete functionality
- Multiple users delete functionality

Single user delete functionality: enter *Programming Mode* then swipe (right to left), to delete a single user from the user list.



1. Swipe on the user you want to delete.

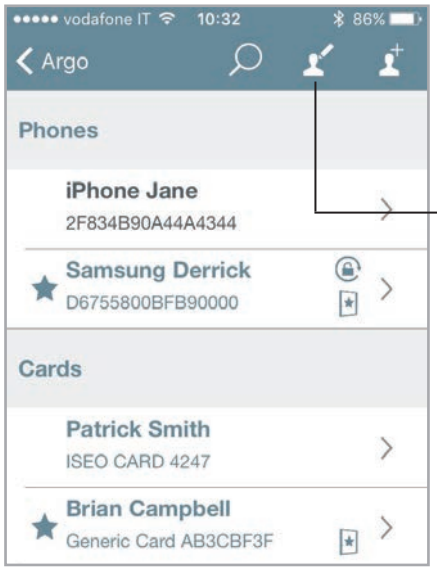


2. Confirm the operation.

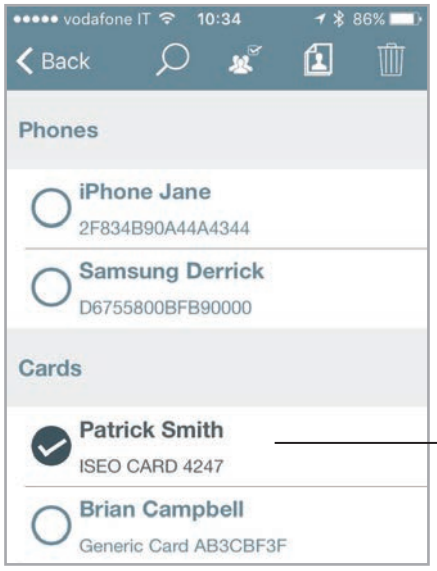
On Android phones, at the place of the swipe action, you need to tap and hold on the user.

Delete users

Multiple users delete functionality: enter in *Programming mode*, press the *edit* icon in the *Users list*, and select the users to be deleted.



1. Tap *edit* icon.

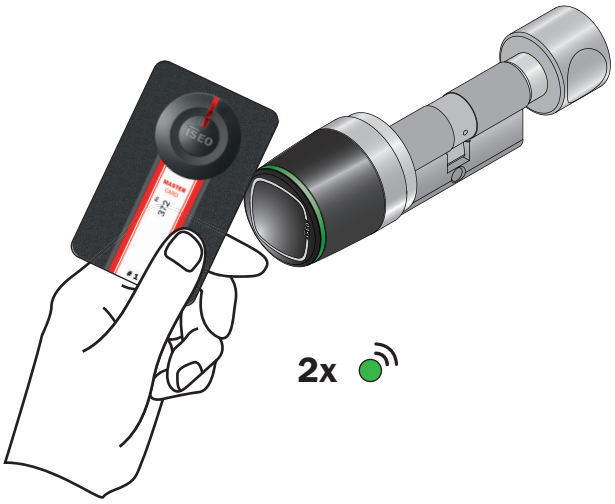


2. Select the users to remove.
   You can also select all users tapping on

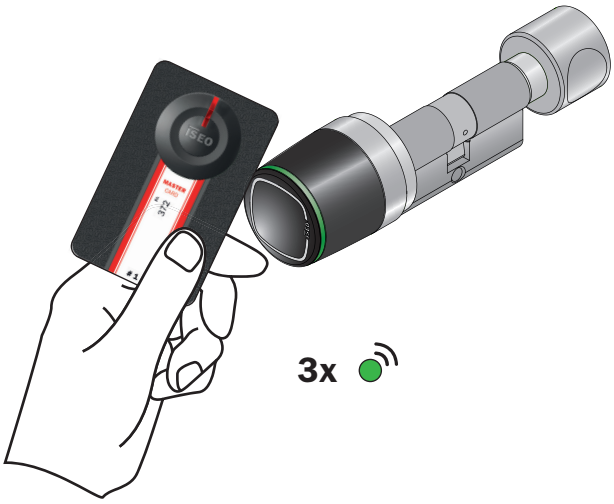
3. Tap the *trash bin* icon to confirm the operation.

You can also search the users to delete by the *Lens* tool.

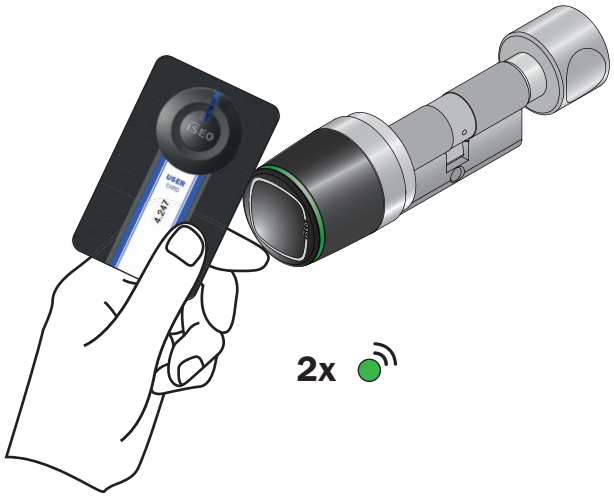
Delete users without Argo app



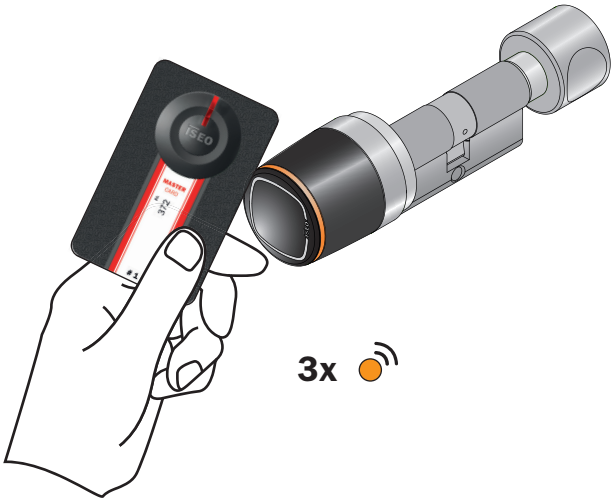
1. Present the *Master Card 1* to the device.
2. The device emits 3 acoustic signals together with 2 green light signals.



3. Present a second time the *Master Card 1*.
4. The device emits 4 acoustic signals together with 3 green light signals.



5. Now read the cards to be deleted.
6. For each deleted card the device emits 2 acoustic signals together with 2 green light signals, to confirm the operation.



7. At the end of the operation present again the *Master Cards 1* to the device.
8. The device emits 4 acoustic signals together with 3 orange light signals.

It is also possible to **delete the entire user's list**. To do that present the *Master Card 1* to the device for 5 seconds (until you hear a sound). Then remove the card, and repeat it again for 3 times. Specifics acoustics and light signals will guide you through the operation.

Basics

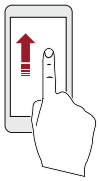
Read Events

Present the *Master Card* to the device, to enter *Programming mode*, and press **Events** icon.

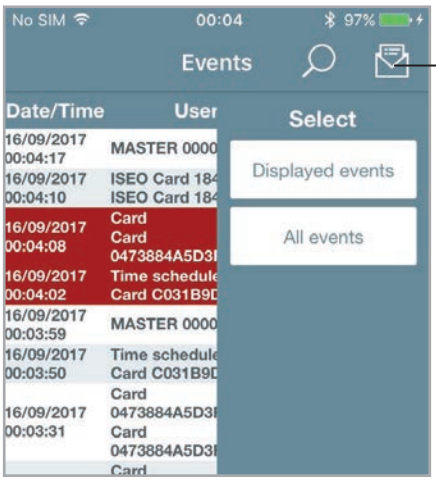
The last 1000 events are stored in the lock. The events are loaded from the most recent, and scrolling down allows you to automatically load new events.

Tap the *lens icon* to show the *search box,* to search by user name, card number or result.

Events list: scroll up to show and load previous events.



Denied events are highlighted in red for an easy and fast reading.



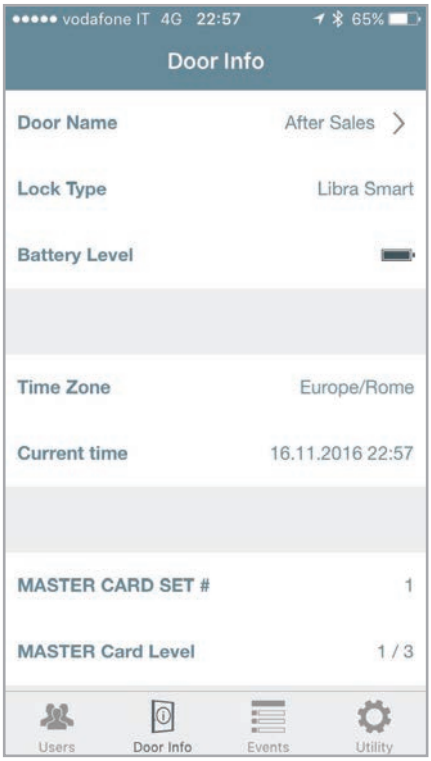
Tapping the envelope you can send by email:

- **Displayed events**: the events loaded by "manual scrolling", or filtered in the search box.
- **All events***:* all the lock events (max 1000 events).

Events sent by email come also in a *CSV file*, which can be imported by excel or similar software.

Door info

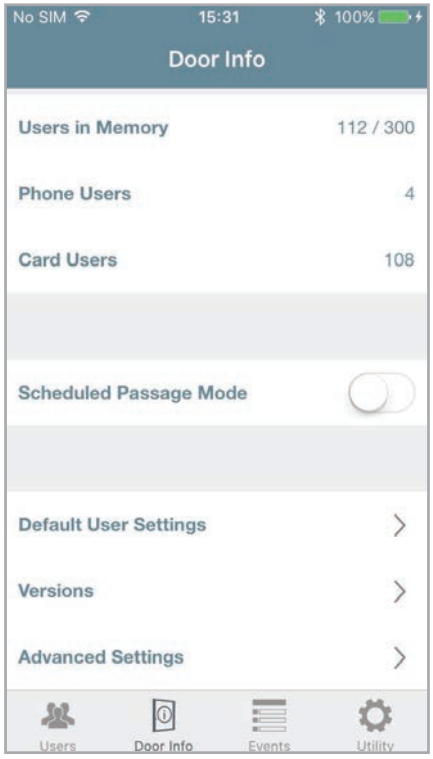
In this menu you can change the *door name* and you can find many information about the device configuration, as showed in the picture below.



Tap to change the *Door name.*

Check battery level.

Other available info.



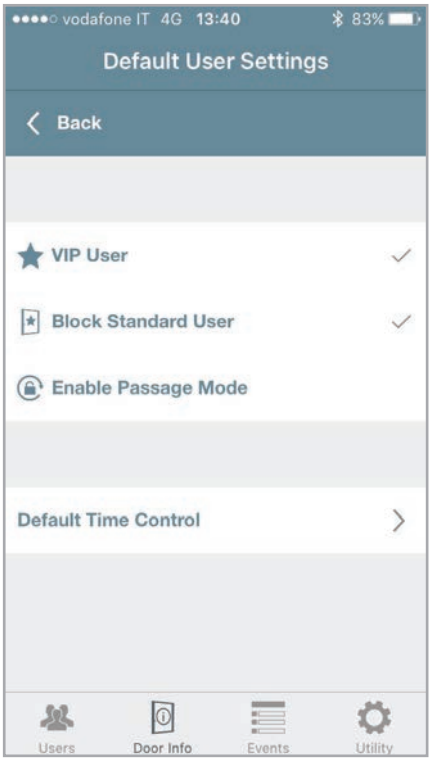
Other available info.

To know more about this function see the related chapter in the Advanced section.

To know more about those sub-menus see the following chapters.

Default User Settings

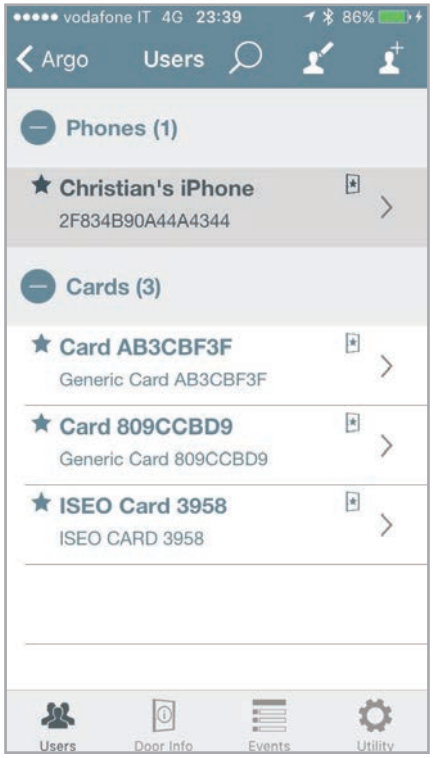
In this menu you can set *User Type* and *Functions* as default. That means the selected functions will be automatically added to each new memorized credential (user).



User type and *Functions*.
In the example aside, set as default *VIP User* and *Block Standard User*.

You can set as default also *Time Control*.

To know more about this function see the related paragraph in the *Advanced* chapter.



Following the above example, all new added users will be *VIP* users, with *Block Standard User* function automatically enabled, because previously set as default.

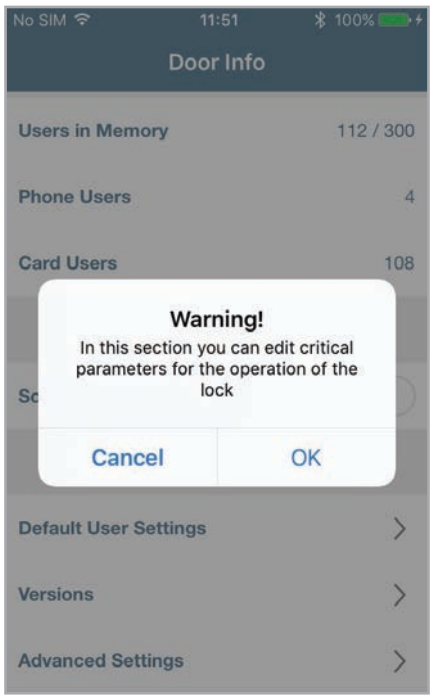
Versions

In this menu you can find the software versions of all the electronic boards included in the device.

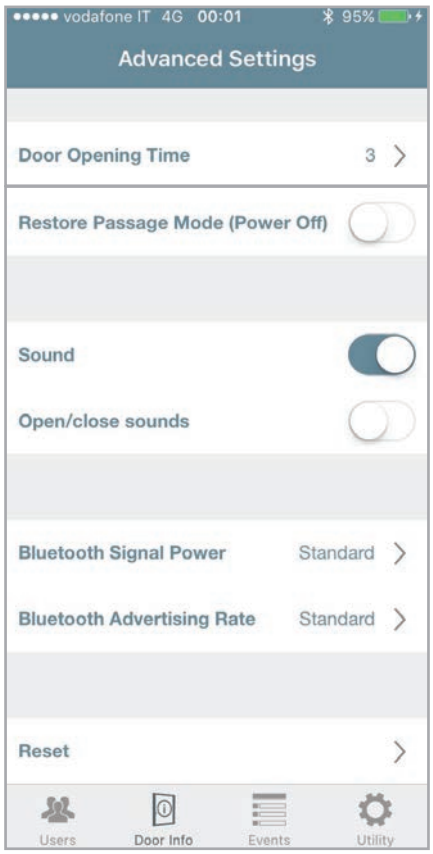
Look at the *Main Board Software version*. This is the version that you can update by the *software upgrade procedure,* described in the next pages.

Advanced settings

In the *Door Info* menu, all functions considered advanced, because they have an important impact on the device functionality, are now grouped under a new menu "*Advanced Function*". This is extremely useful for example in case of *x1R Smart*, that has many advanced functions.



When you enter this menu, a pop-up notifies you that you are changing critical parameters for the lock, and a confirmation is required to continue and to save the data.



Tap to change the *Door Opening Time* (5 seconds by default).

If this function is enabled, a lock already set in *Passage Mode*, following a power OFF, will restore automatically the *Passage Mode* function when ON again.

You can disable all sounds.
If *Sound* is enabled you can also add open and close sounds to the device (except on *x1R Smart* since it has the opening and closing sounds by default).

To know more about those functions see the related paragraph in the *Advanced* chapter.

To know more about this function see the related chapter in the *Advanced* chapter.

Advanced

User type and functions

You can edit the added users to define extra functionalities. There are different *user types* and *functions*, and to easily recognize it on Argo, all are identified by specific icons.

USER TYPE

Standard user: this is the default user, for whom access can be denied if the *Standard User Block* function is active.

VIP user: this type of user can also access the doors on which *Block standard users* function is active.

FUNCTIONS

Enable passage mode: a user can put a door in *Passage Mode* also called *Office Mode*. In this state, the door will be remain open for any user who wishes to pass through, without any need for authorised credentials.

Block standard user: this function is only available for *VIP user.* Enabling this function, a *VIP user* can block the access for all the *Standard users*.

Override privacy: with this function enabled, the user can access the door even if the *Privacy function* has been activated from the inside (for *Aries Smart* only).

USER PIN

PIN: a single *PIN code* can be set and used to either open the door by smartphone or login and program the lock without the need of the *Master Card* (or for both cases). This icon indicates that the PIN has been assigned to a user, but it hasn't yet been associated with either the opening function or the login function.

Advanced

OPEN RESTRICTIONS

Enable Time Control: allows to set, for each user, the credential *Activation* and *Expiration* date & time. Futhermore it enables 2 *Time Schedules,* selectable for each day of the week.

Validity from First Use: allows to set the validity from the moment of the first use of the credential (in days, hours or minutes). *Validity from First Use* can be combined with activation and expiration date, and with the time schedules of the credential.

Request PIN to open the door: to increase security a *PIN code* has been set to open the door by phone.

LOGIN TO DOORLOCK

Login: the user can enter *Programming Mode* by phone without the use of the *Master Card*.

Request PIN to login: to increase security a *PIN code* has been set to login by phone.

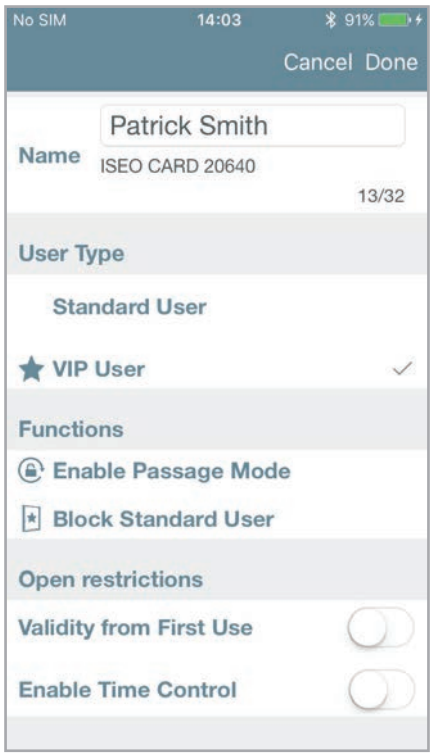
Login and request PIN to open the door: user can enter *Programming Mode* by phone and a *PIN code* has been set to open the door.

Request PIN to login and to open the door: for the maximum security the user can use the same *PIN code* both to login and to open the door by phone.

Advanced

Card user parameters

From the *Users list*, tap a card name to enter the card edit mode. Now you can change the user name and the other following parameters:



User name and credential *Unique Identifier Number* (UID).

Available characters for the user's name (tot 32 chr).

User Type

- *Standard users* can be blocked temporarily if a *VIP* card has the function of *Block Standard Users* enabled.
- *VIP* users can always access to the door.

Functions

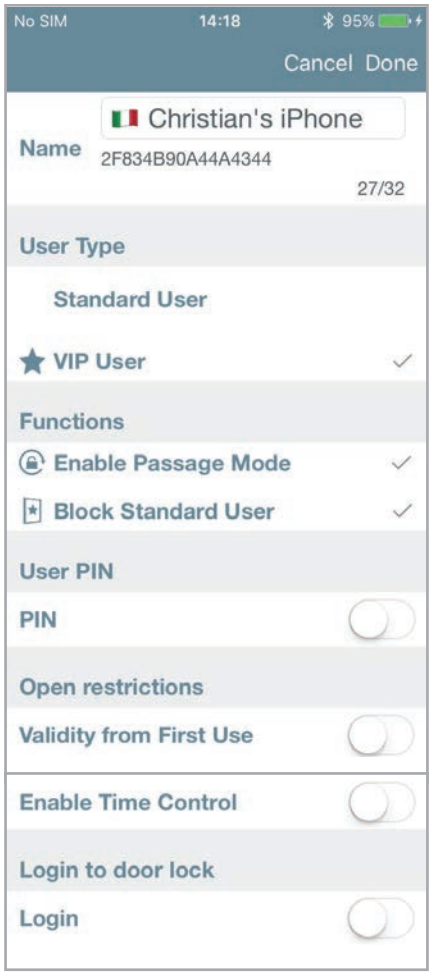
- *Enable Passage Mode* allows a user to put the lock in *Passage Mode* (office function).
- *Block Standard User* is enabled only if the user is *VIP*. With this function enabled a *VIP* user can temporarily block the access to all *Standard Users*.

Open resctrictions

- *Validity from First Use* allows the credential activation from the first use, until the set time in minutes, hours or days.
- *Enable Time Control* sets credential activation and expiration date & time. Futhermore it enables 2 *Time Schedules,* selecteable for each day of the week.

Phone user parameters

From the user list, tap a phone name to enter the smartphone *edit mode*.



User name and phone *Unique identifier number* (UID).

Available characters for the user's name (tot 32 chr).

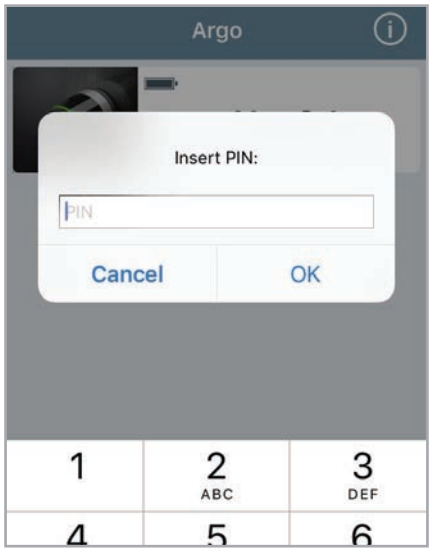
Same *User Type* and *Functions* of *Card user parameters* menu.

You can set a *PIN code (4 digits)*, that can be used to open the door and/or to *Login* without *Master Card*.

You can enable the the *Validity from First Use* or/and the *Time Control* (see *Card user Parameters*).

You can enable the *Login* without *Master Card*: in this way you can enter *Programming Mode* directly with the smartphone without the use of the Master Card.

When you enable the *PIN* to open the door, the code will be asked at every open command with your smartphone.



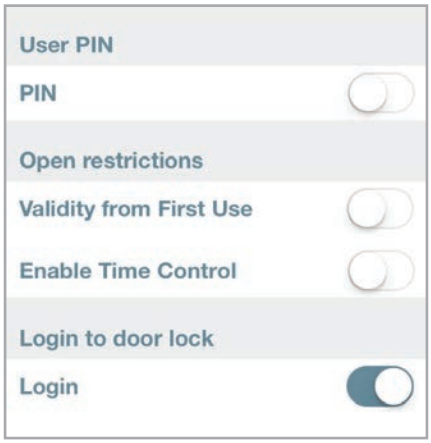
Enter the 4 digits *PIN code* and press **OK** to open the door.

Advanced

Administrator Login without Master Card LOGIN

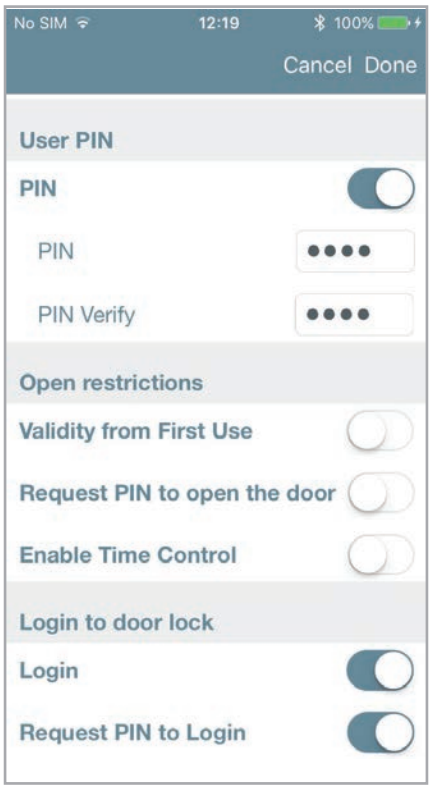
This function allows your smartphone to enter *Programming Mode* without the need of the *Master Card.* You can finally keep your *Master Card* in a safe place and enter *Programming Mode* by the *Tap & Hold* function (see *Tap & Hold menu* paragraph). You can also add a *PIN code*, or you maximum security, that will be asked every time you enter *Programming Mode*.

To enable *Administrator Login without Master Card* enter *Phone user parameters* menu.



Enable **Login**

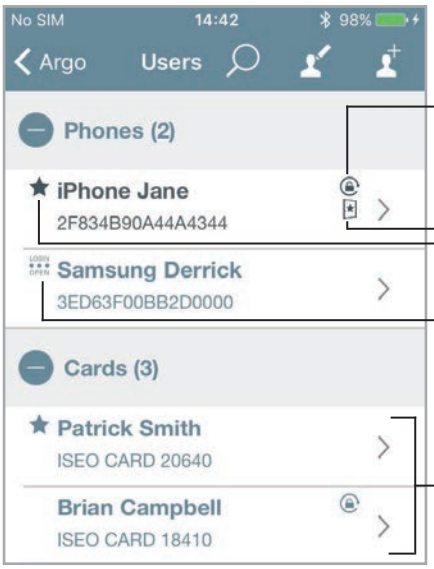
To add a PIN code to the *Administrator Login without Master Card*.



1. Enable **PIN**
2. Choose your PIN code
3. Enable **Login**
4. Enable **Request PIN to Login**

User List overview

In this menu, you can see the *Users names* and which are the active parameters of the corresponding users.



Enable passage mode active.

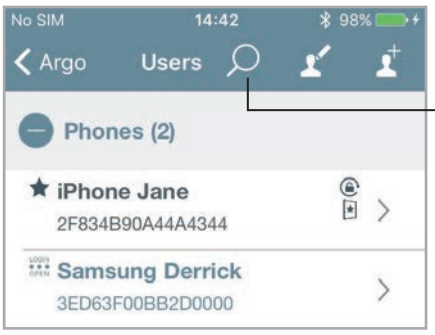
Block standard users active.

VIP user.

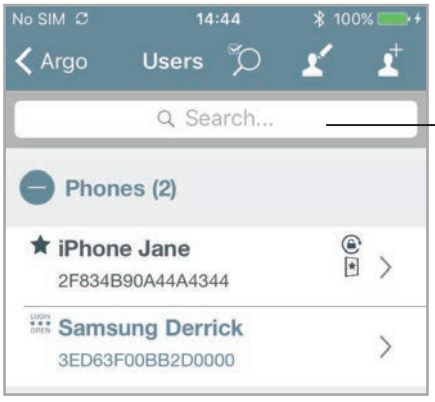
Enable PIN code request to open the door and to login without *Master Card* active

User name and credential *UID*

You can also search for a specific user using the *Lens icon*.



1. Click on the *Lens icon*.



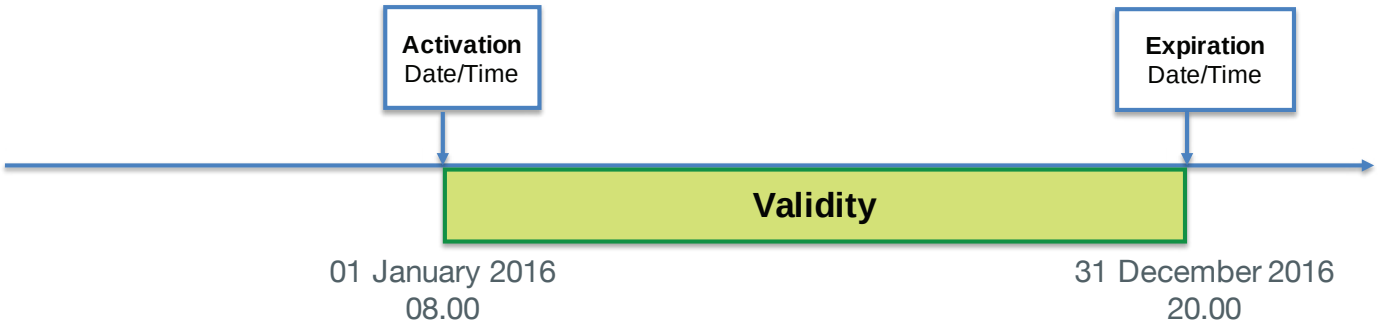
2. Write in the box the name to search and press **Find** in the phone keyboard tool.

Advanced

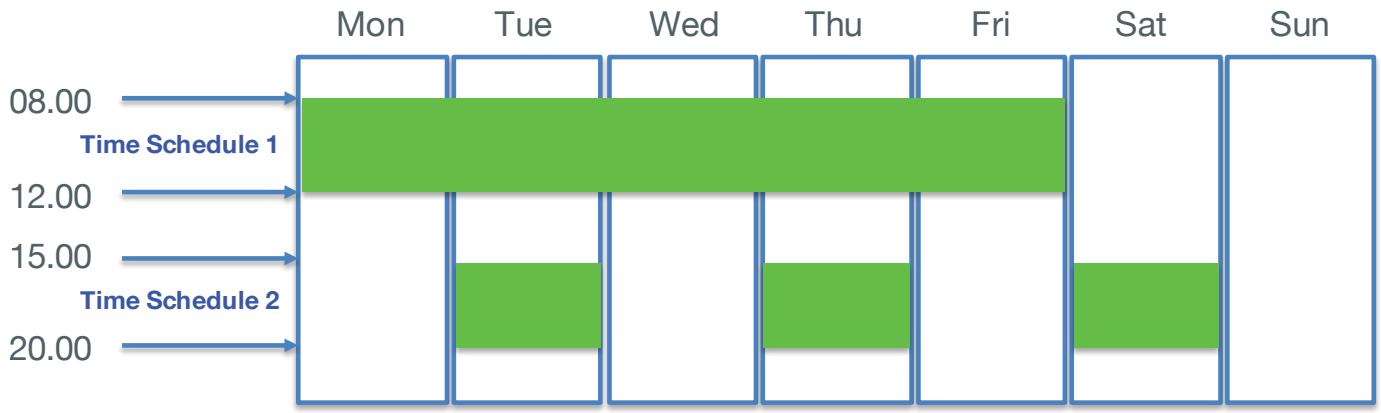
Time Control

For every user you can set the *Validity*, composed by credential *activation* and *expiration* date & time*, and 2 Time Schedules,* selectable for each day of the week.

Validity



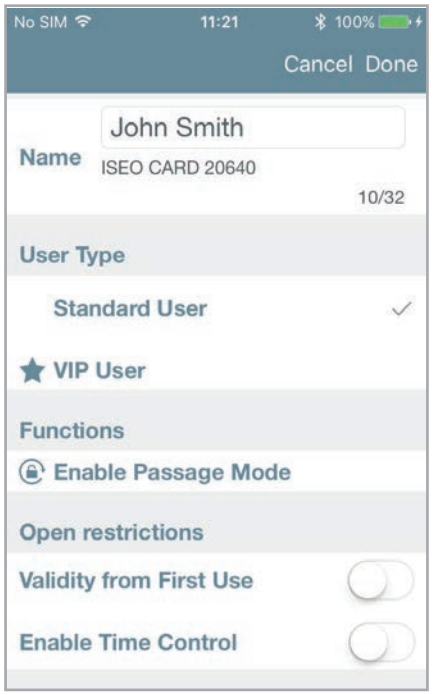
Time Schedules



Advanced

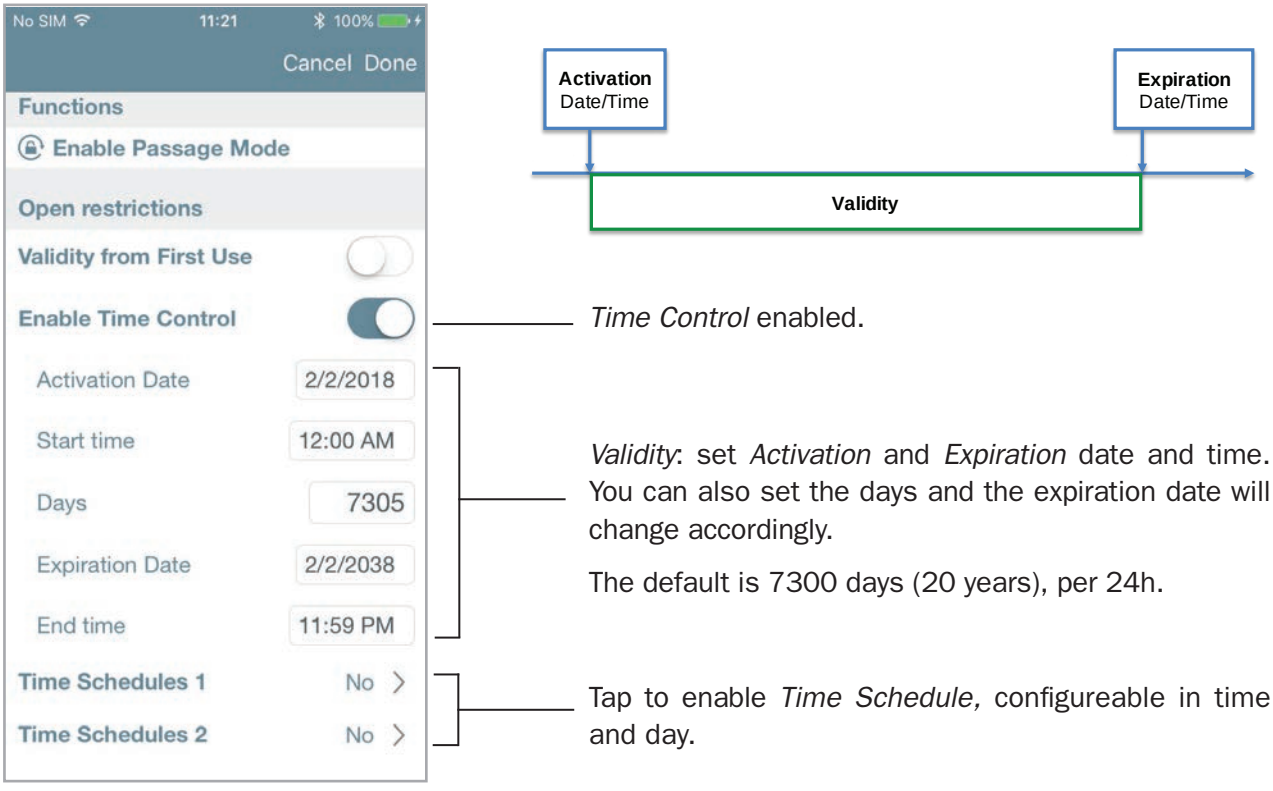
Time Control

To enable *Time Control* enter *Card* or *Smartphone User Parameters* menu.



Enable Time Control.

Validity



Time Control enabled.

Validity: set *Activation* and *Expiration* date and time. You can also set the days and the expiration date will change accordingly.

The default is 7300 days (20 years), per 24h.

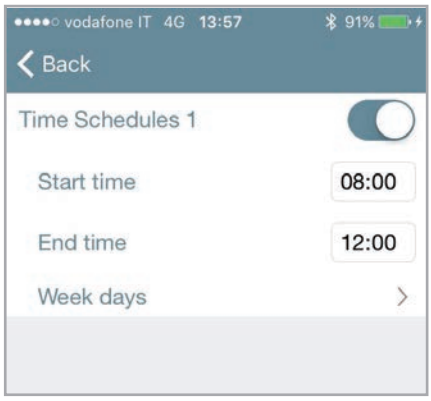
Tap to enable *Time Schedule,* configureable in time and day.

Time Schedules can be configured only if *Time Control* has been previously enabled for the user.

Advanced

Time Control

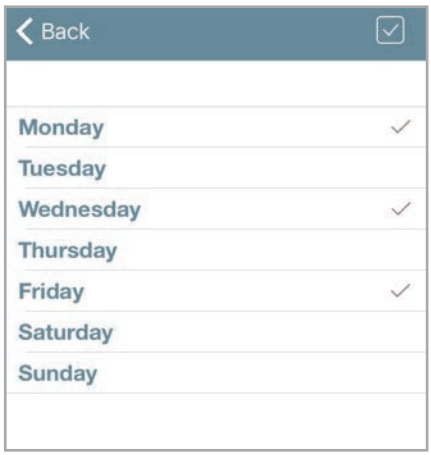
Time Schedules



Time Schedule 1 enabled.

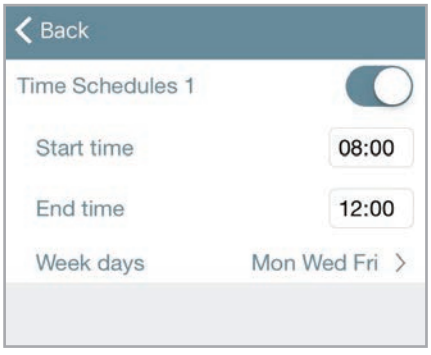
Set *Time Schedules start and end time.*
The default of *Time Schedue 1* is 8:00 - 12:00, while the default of *Time Schedue 2* is 14:00 - 18:00.

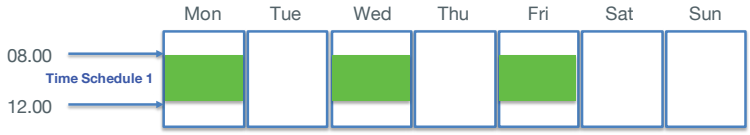
Select the days.



Check/uncheck all days with one touch.

You can manually select multiple or single days.
In this example the user will access the door on Monday, Wednesday and Friday.



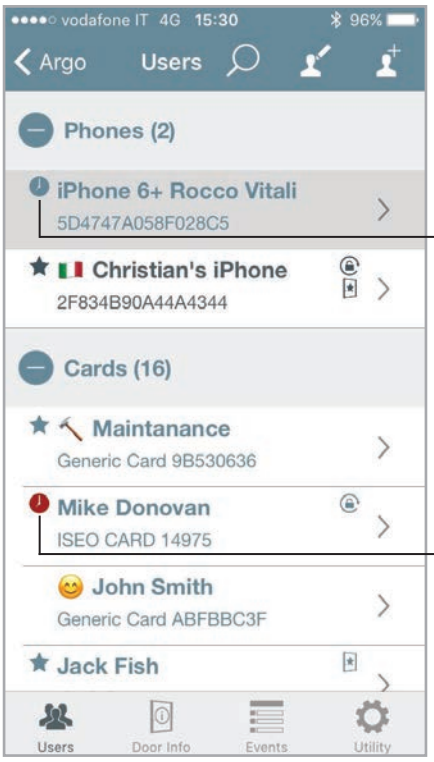


You can see selected days in the *Time Schedule* menu.

Advanced

Time Control

User list overview

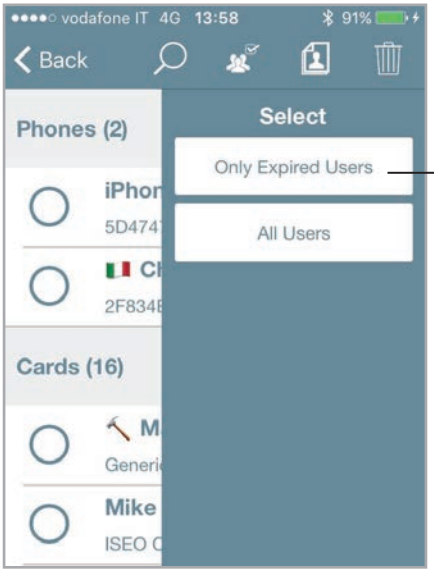


The clock means that user has enabled the *Time Control.*

The red clock means *expired* user.

You can select and delete only the *expired* users.

Press the *edit* icon in the *Users list*, then press *select all* icon and a right-side menu will appear.



Tap **Only Expired Users** and then press the *trash bin* icon to confirm the operation.

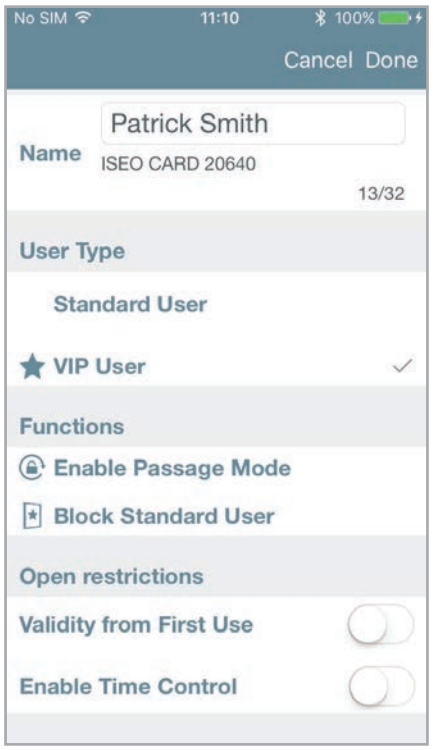
See also *Delete users* paragraph on *Basics* chapter.

Advanced

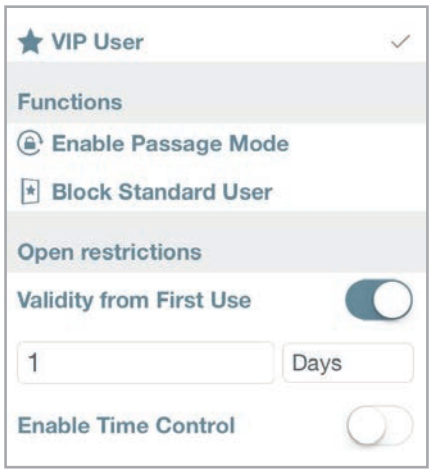
Validity from First Use

For every user you can set the credential *Validity from First Use*, in minutes, hours or days. With this function enabled the set credential validity will start at the moment of the first use, to access the door.
V*alidity from First Use* can be also combined with the *Time Control Validity* (*Activation* and *Expiration date and time*), and the 2 *Time Schedules*, in order to have endless possibilities and the maximum flexibility in the credential time management.

To enable *Validity from First Use* enter *Card* or *Phone User Parameters* menu.



Enable **Validity from First Use**.



Select the validity in **Minutes**, **Hours** or **Days**.

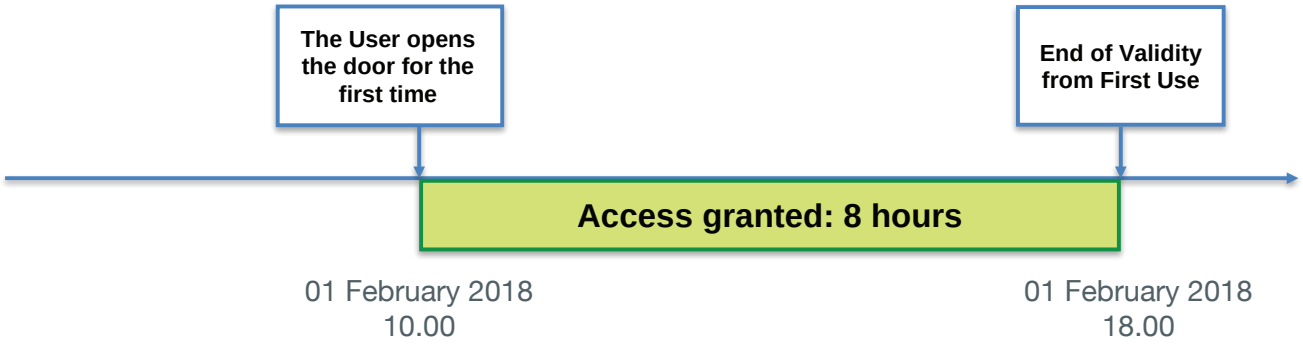
Advanced

Validity from First Use

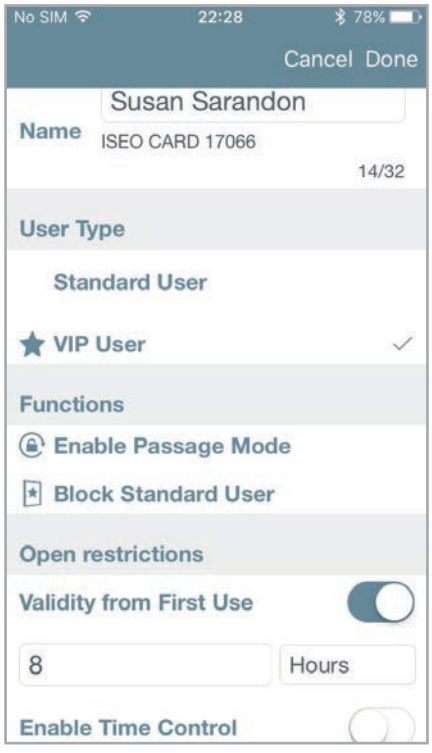
When the *User* opens the door for the first time, the *Validity from First Use* become the date and the time of that moment, and the credential will expire according to the validity set. To show what's happens on the *Argo app* using the *Validity from First Use*, see the next examples.

Example 1: Validity from First Use 8 hours

The user can access the door for 8 hours after the first opening.



Enter *Programming mode,* then enter *Card or Phone User Parameters*.



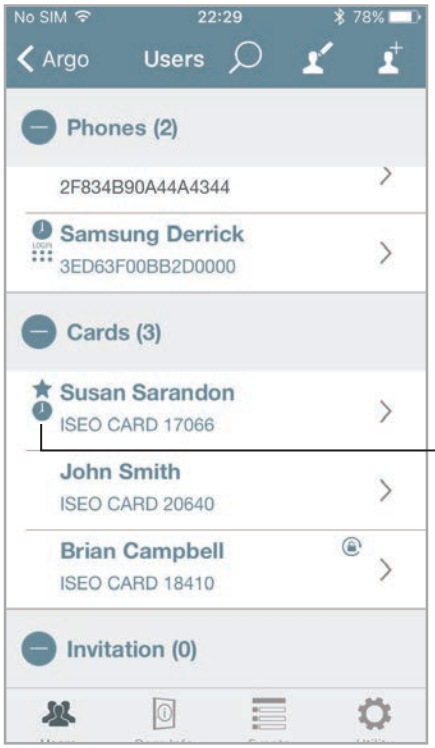
Enable **Validity from First Use**

Set **8 Hours**

Advanced

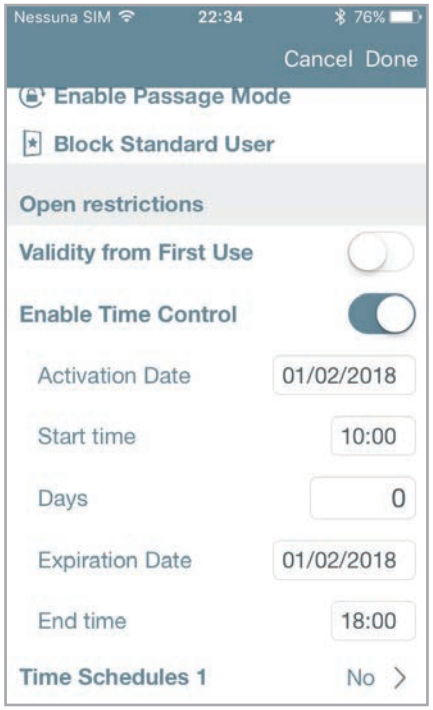
Validity from First Use

User List overview:



The clock means that user has enabled the *Validity from First Use.*

The *User* opens the door for the first time. The *Administrator* enter *Programming mode* to check the credential status.



The **Validity from First Use** is now disabled since it has already been used.

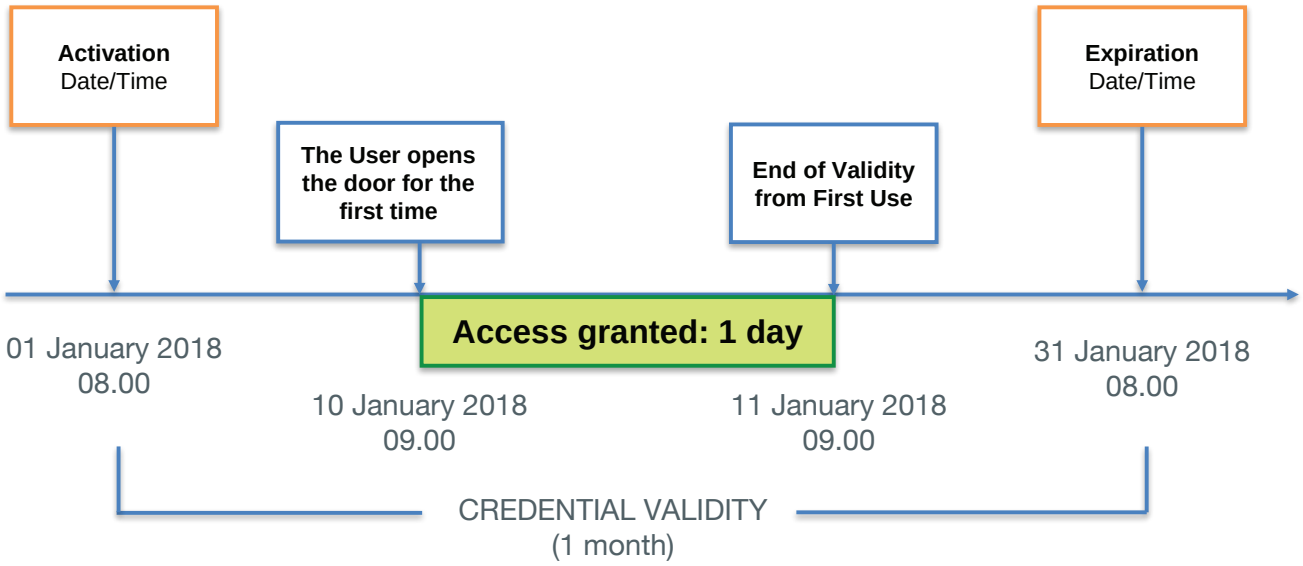
The **Time Control** is now enabled since the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** are automatically set, adding 8 hours to the **Start Time**.

Advanced

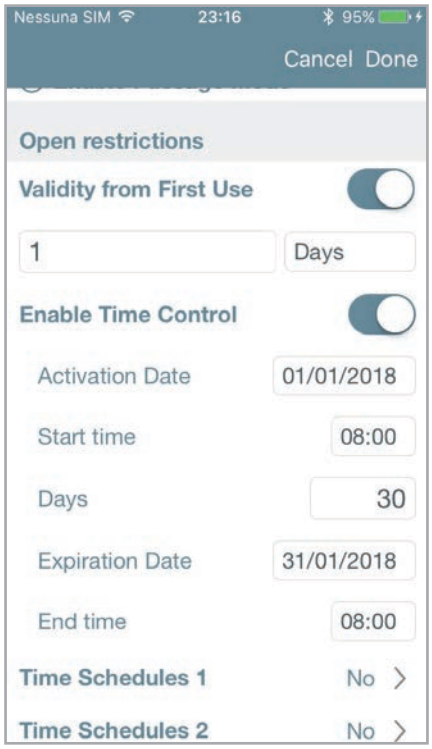
Validity from First Use

Example 2: Time Control AND Validity from First Use 1 day

The user can access for 1 day after the first opening but only within the month of January 2018.



Enter *Programming mode,* then enter *Card or Phone User Parameters*.



Enable **Validity from First Use**

Set **1 Days**

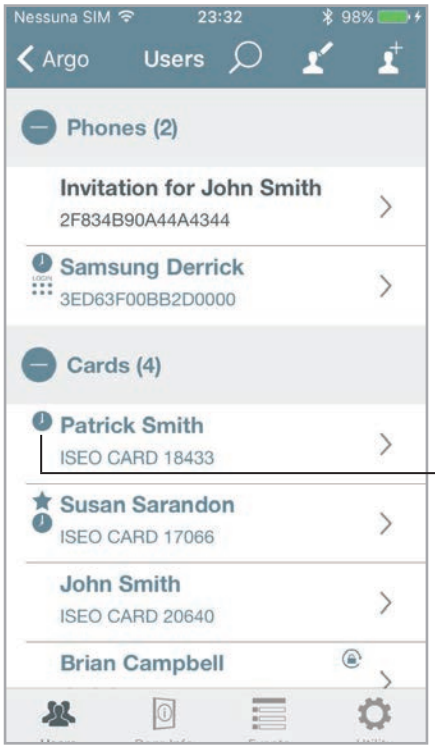
Enable **Time Control**

Set the overall credential *Validity*: **Activation Date**, **Expiration Date**, **Start Time** and **End Time**.

Advanced

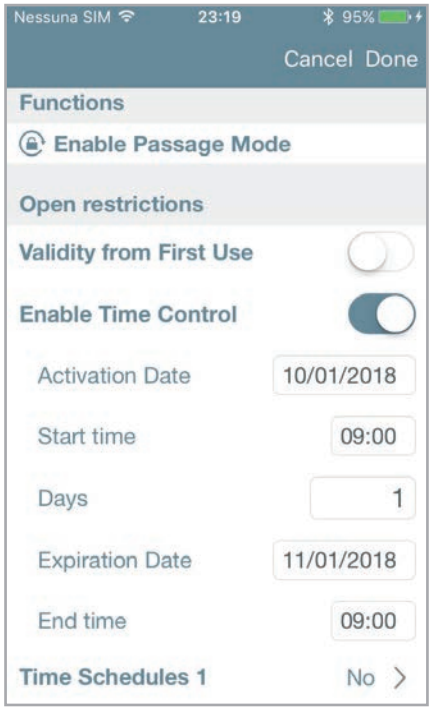
Validity from First Use

User List overview:



The clock means that user has enabled both *Validity from First Use* and *Time Control*.

The *User* opens the door for the first time. The *Administrator* enter *Programming mode* to check the credential status.



The **Validity from First Use** is now disabled since it has already been used.

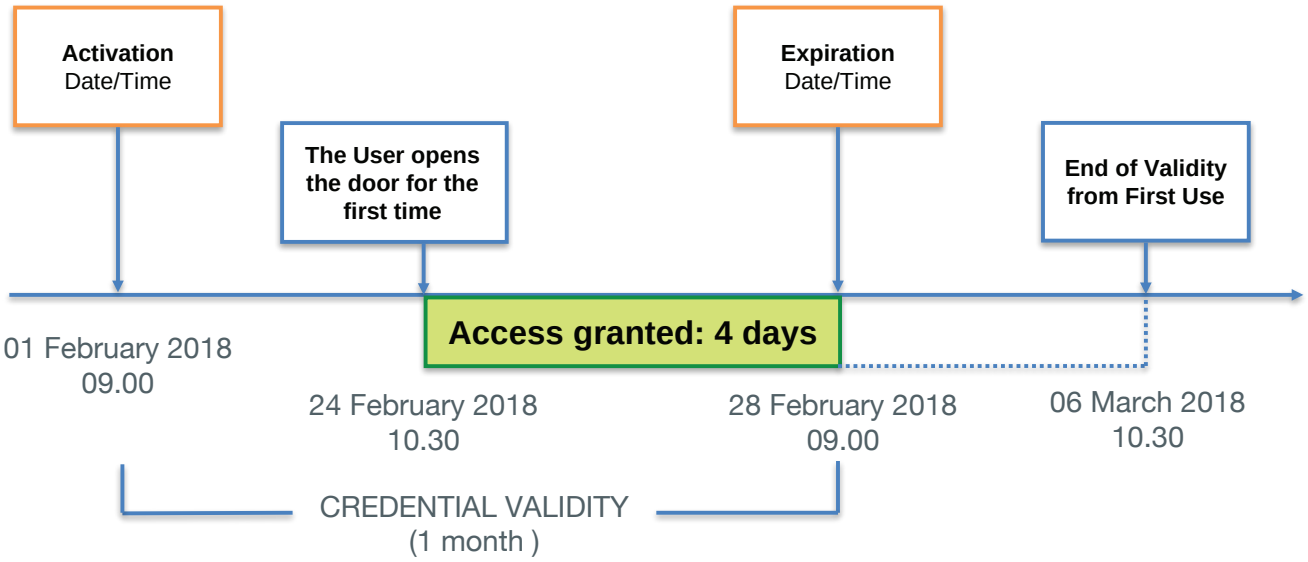
In the **Time Control** the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** are automatically set, adding 1 day to the **Activation Date**.

Advanced

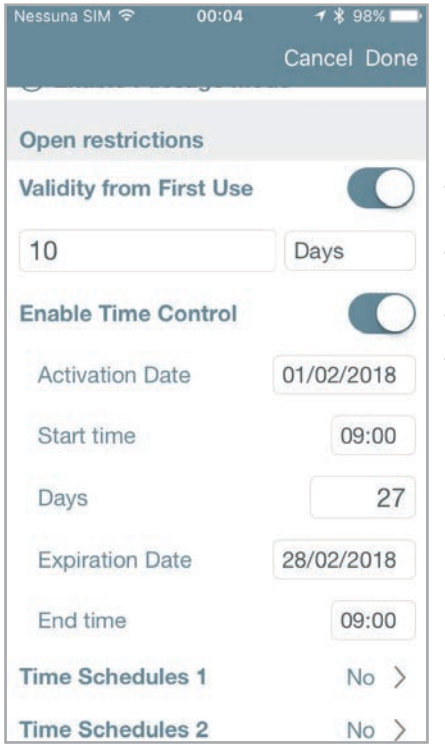
Validity from First Use

Example 3: Time Control AND Validity from First Use 10 days

The *User* can access for 10 days after the first opening but only in the month of February 2018. If the *User* opens the door for the first time at the end of February, the *Validity from First Use* ends at the credential *Expiration Date*, that has priority over the *End of Validity from First Use*.



Enter *Programming mode,* then enter *Card or Phone User Parameters*.



Enable **Validity from First Use**

Set **10 Days**

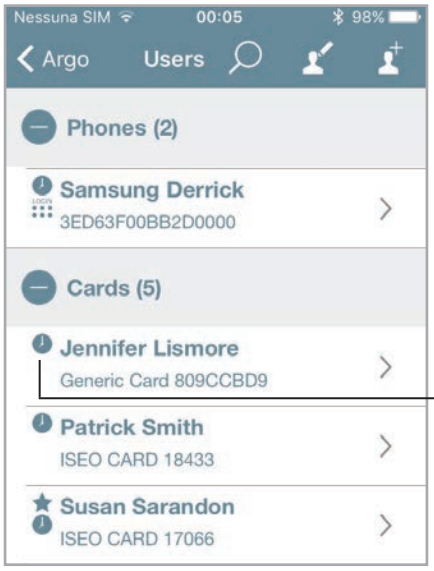
Enable **Time Control**

Set the overall credential *Validity*: **Activation Date**, **Expiration Date**, **Start Time** and **End Time**.

Advanced

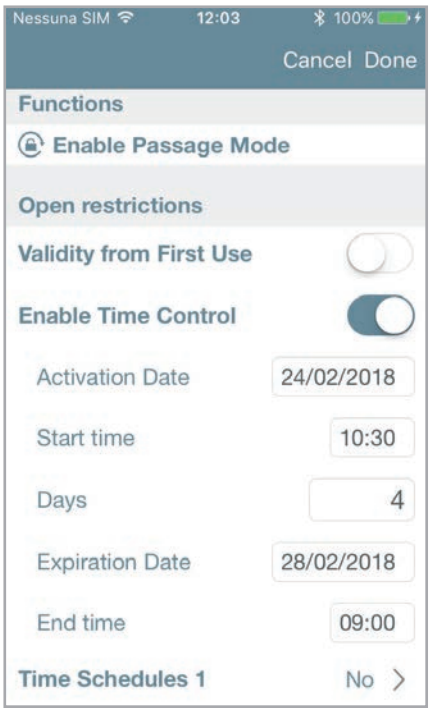
Validity from First Use

User List overview:



The clock means that user has enabled both *Validity from First Use* and *Time Control.*

The *User* opens the door for the first time. The *Administrator* enter *Programming mode* to check the credential status.



The **Validity from First Use** is now disabled since it has already been used.

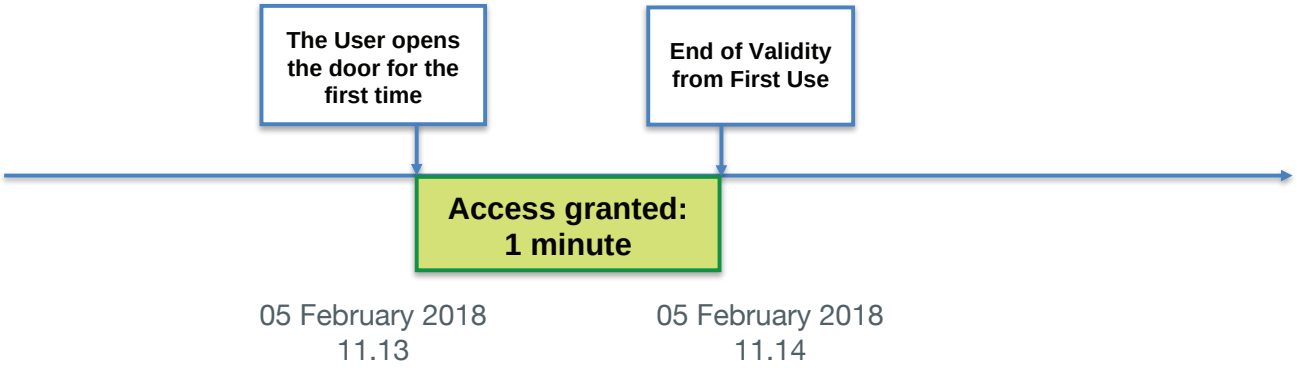
In the **Time Control** the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** remains the same previously set.

Credential *Expiration Date* doesn't change, since it has priority over the *End of Validity from First Use*. In the example above *Expiration Date* has remained the same: 28/02/2018. That means *Validity from First Use* has changed from 10 to 4 days, to not exceed the credential *Expiration Date*.

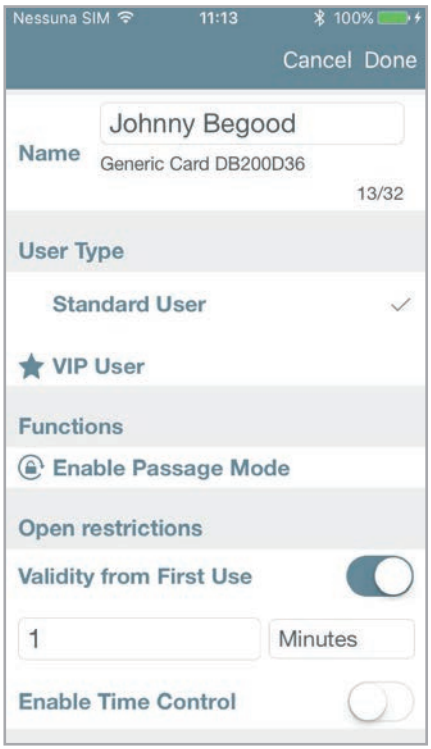
Validity from First Use

Example 4: Validity from First Use 1 minute

With this solution the *User* will enter the door just for 1 minute, from the first access. It is basically a very effective way to create a *one shot* entrance credential.



Enter *Programming mode,* then enter *Card or Phone User Parameters*.



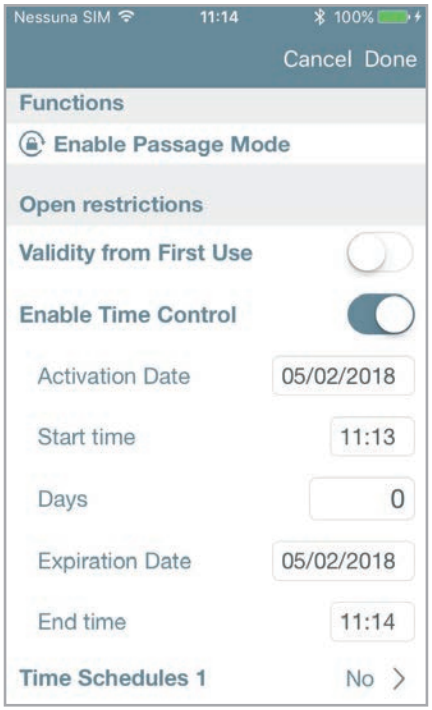
Enable **Validity from First Use**

Set **1 Minutes**

Advanced

Validity from First Use

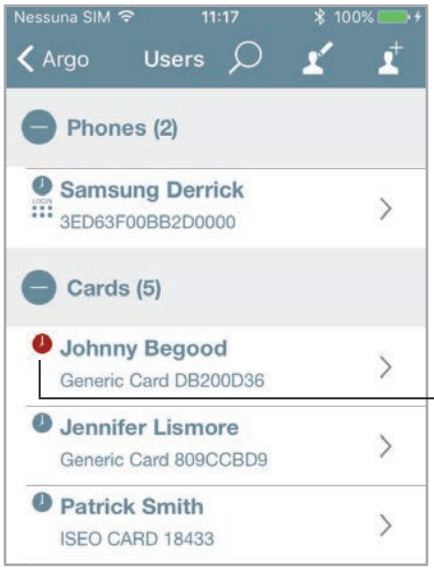
The *User* opens the door for the first time. The *Administrator* enter *Programming mode* to check the credential status.



The **Validity from First Use** is now disabled since it has already been used.

The **Time Control** is now enabled since the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** are automatically set, adding 1 minute to the **Start Time**.

User List overview after 1 minute has passed:

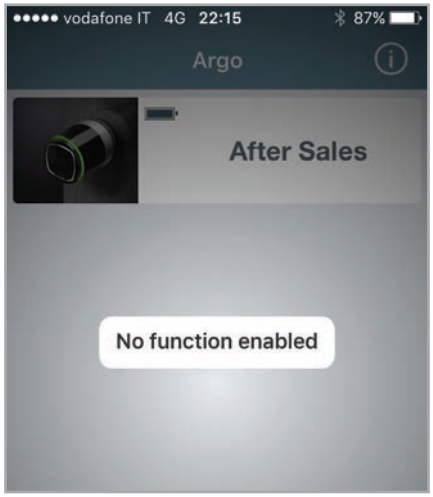


The red clock means that *User* has expired, since 1 minute has passed (one shot entrance).

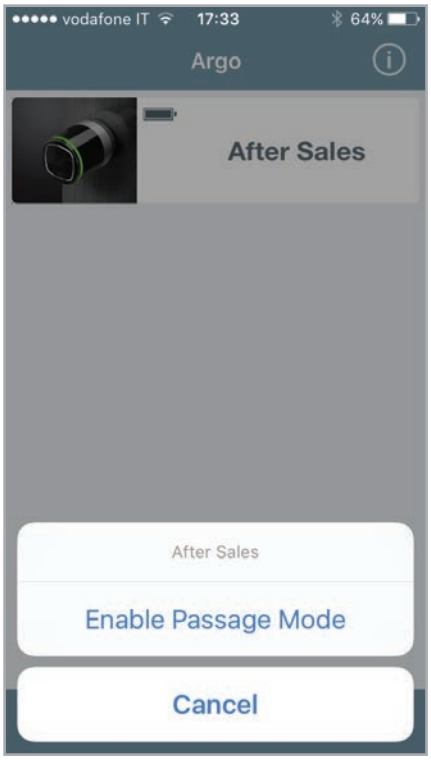
Advanced

Tap & Hold menu

The *Tap & Hold* menu shows only the Smarpthone's enabled functions. If no function is enabled, you will get the message as per picture below.



If I enable a function instead, for example *Passage Mode*, I will then see it available in the *Tap & Hold* menu.

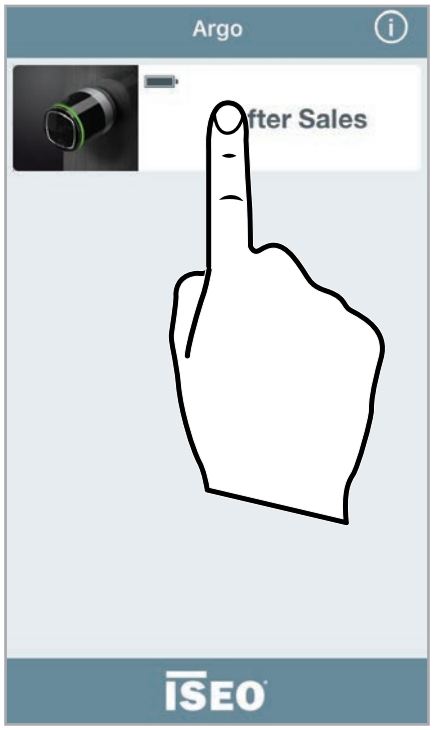


See also the *Video tutorial,* explaining in detail the *Tap & Hold* functions, at link:
https://app.iseo.com/?parm=ARGO&lang=en&folder=video-tutorial

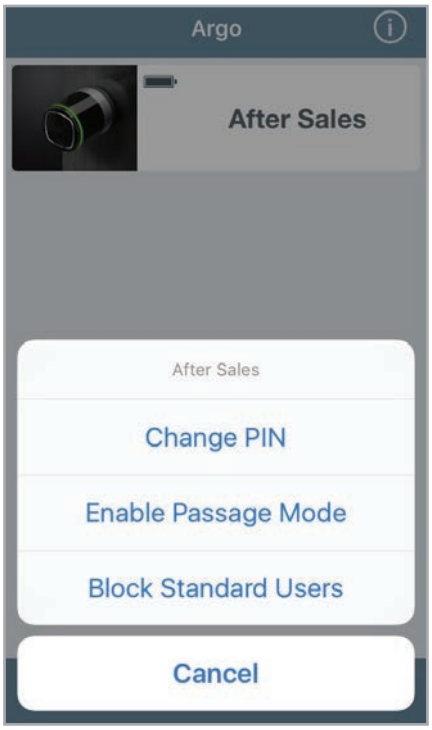
Advanced

Enable Passage Mode

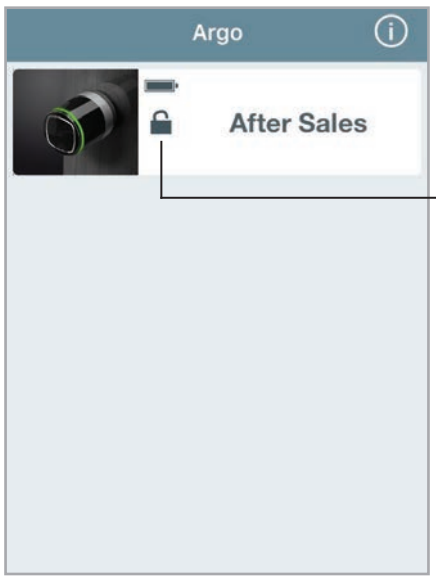
Enabling *Passage Mode* into the lock, the door will be always opened for any user who wishes to gain access, without the use of authorized credentials.



1. Tap and hold the *Door name button* on which you want to enable the *Passage mode.*



2. A bottom menu will appear.
3. Tap **Enable Passage Mode**.



4. You will see in the button a symbol showing the *enabled function*.

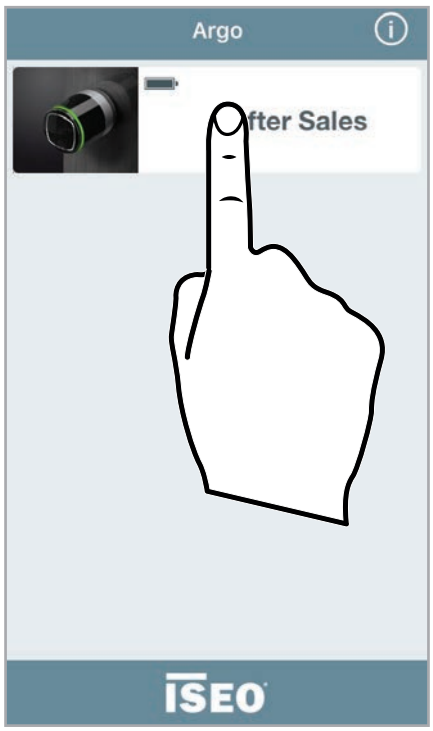
5. Follow the same procedure to disable the function.

Remember to set before the function *Enable Passage Mode* on your smartphone (see *Smartphone user parameters*). When passage mode is active no logs are created in order to save events.

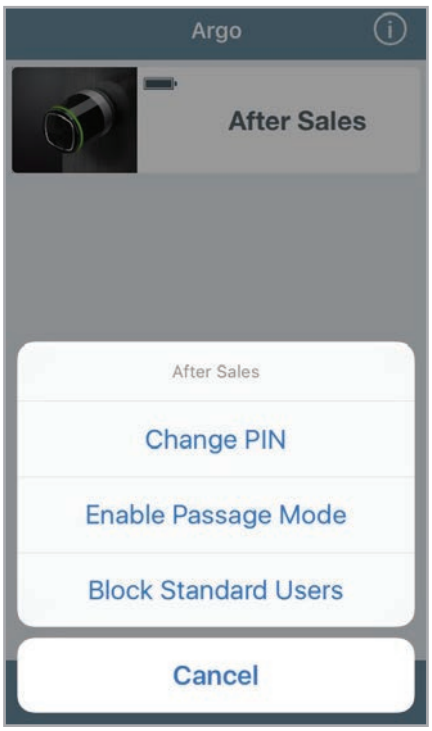
Advanced

Block Standard Users

This function, when enabled, blocks the access to the door to all users, called *Standard.* Only *VIP* users can enter.



1. Tap and hold the *Door name button* on which you want to enable the *Block Standard User* function.



2. A bottom menu will appear.
3. Tap **Block Standard Users**.

4. You will see in the button a symbol showing the *enabled function*.

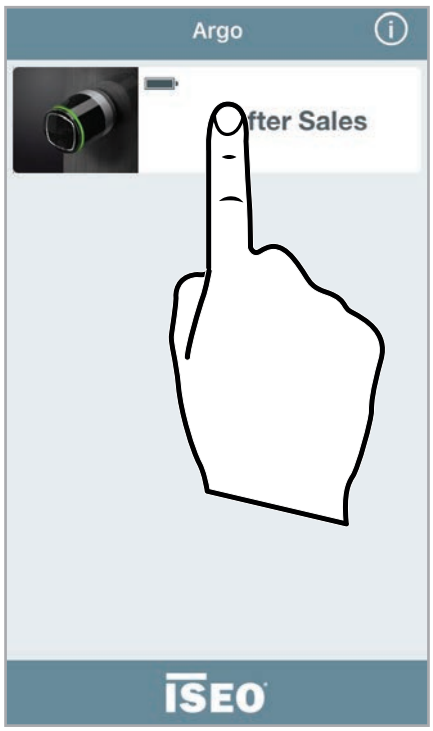
5. Follow the same procedure to disable the function.

Remember to set before the functions *Block Standard Users* on your smartphone (the user must be a VIP user ★). To do that see *Smartphone user parameters*.

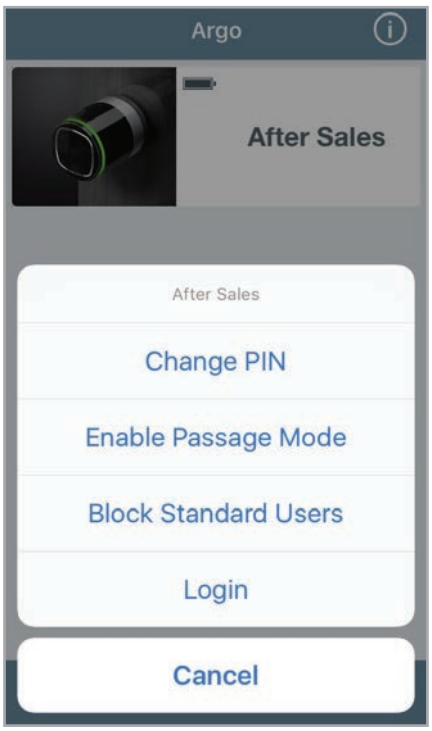
Advanced

Login (without Master Card) LOGIN

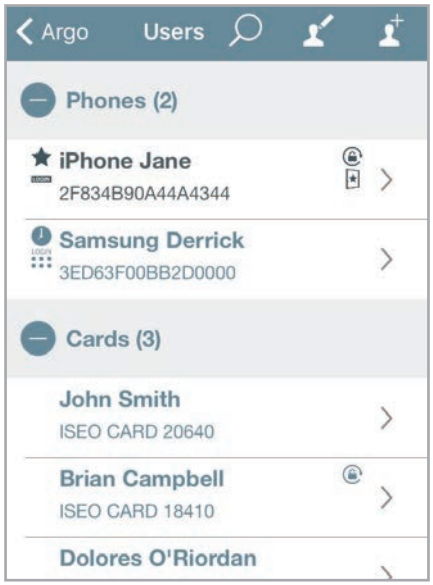
This function allows your smartphone to enter *Programming Mode* without the need of the *Master Card.*



1. Tap and hold the *Door name button*.



2. A bottom menu will appear.
3. Tap **Login**.



4. You will enter *Programming Mode*.

The LOGIN icon in the user list means this phone can enter *Programming Mode* without *Master Card.*

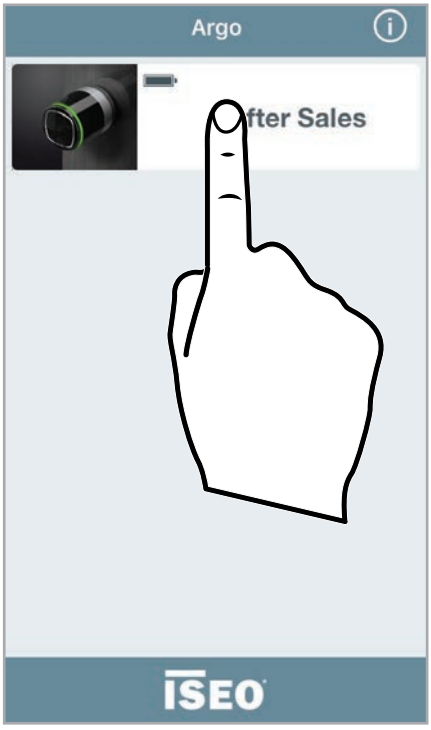
The LOGIN icon in the user list means this phone can enter *Programming Mode* without *Master Card* but a *PIN code* previously set is required.

For the maximum security, you can add a *PIN code* to enter *Programming Mode* with your smarpthone, as described at paragraph: *Administrator Login without Master Card*.

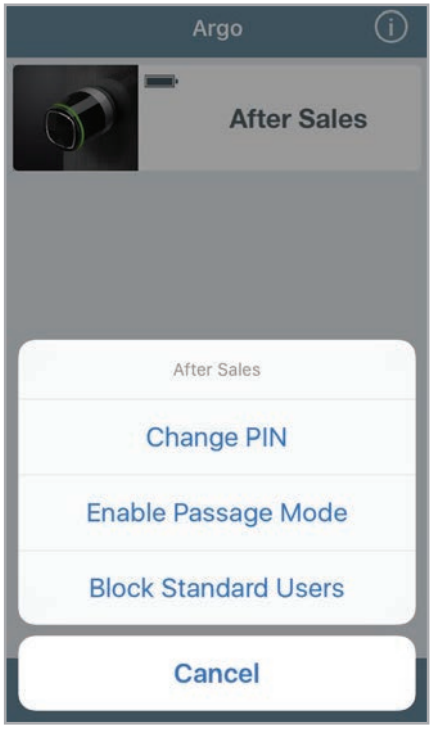
Advanced

Change the PIN code

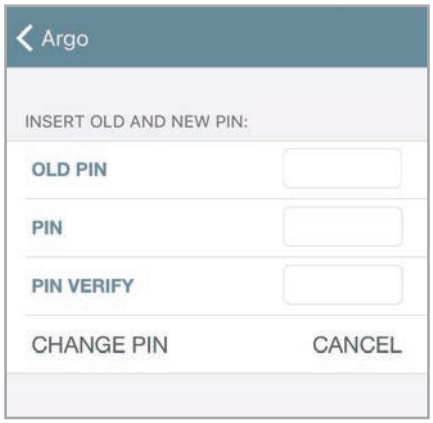
This function allows to change the *PIN code* if previously set in the smartphone. This *PIN code (4 digits)*, could be set to open the door and/or to *Login* without *Master Card* (see *User type and functions* and *Smartphone user parameters* pragraphs).



1. Tap and hold the *Door name button.*



2. A bottom menu will appear.
3. Tap **Change PIN**.



4. Enter the old *PIN code*.
5. Enter the new *PIN code* two times, then press **CHANGE PIN**.

Advanced

Enable Passage Mode without Argo app

1. Take a card with *Passage Mode function* enabled (see *Card user parameters)*.

2. Read the card for 3 sec. The device emits 3 acoustic signals together with 3 orange light signals.

Follow the same procedure to disable the *Passage Mode function*.

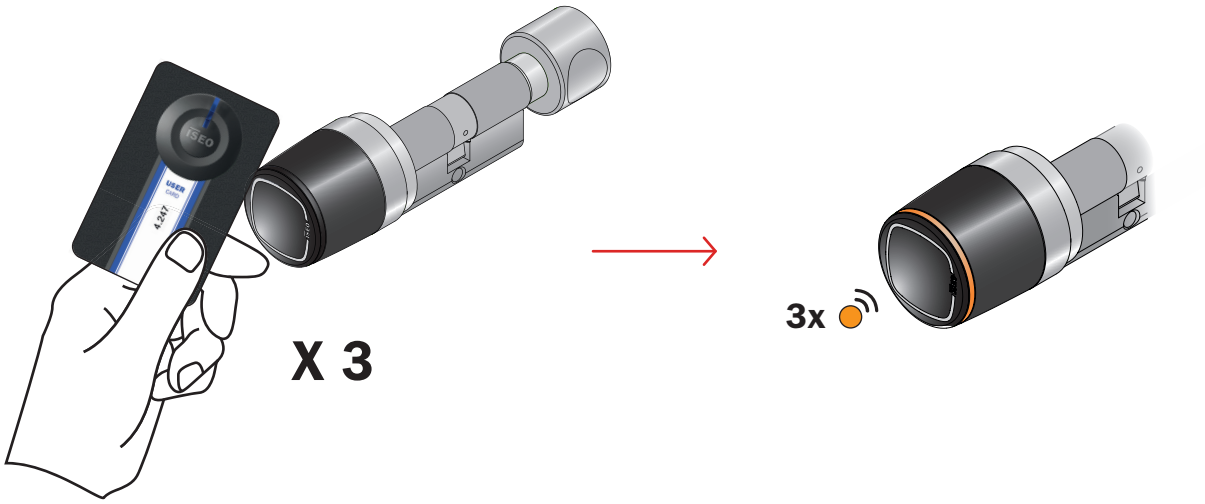
Advanced

Block Standard User without Argo app

1. Take a card with *Block Standard User* enabled (see *Card user parameters*).

2. Read the card 3 times consecutively during the opening time:
   - the first time the device opens;
   - the second time the device emits 1 acoustic signal togheter with a green light;
   - the third time the device emits 3 acoustic signals together with 3 orange lights.

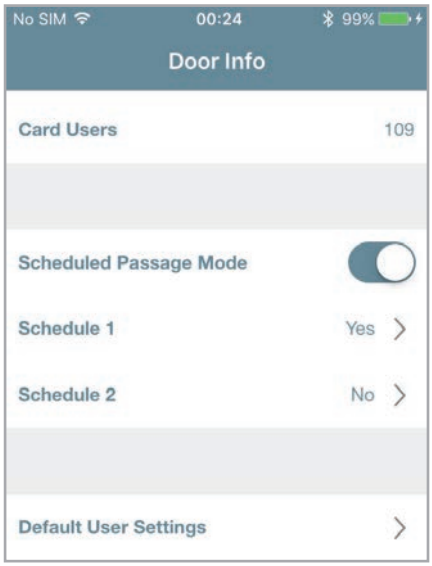
Follow the same procedure to disable the *Block Standard User* function.



Advanced

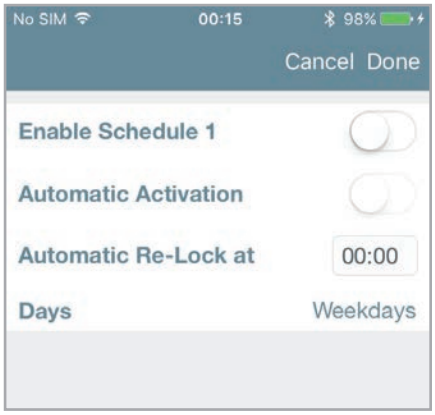
Scheduled Passage Mode

This function allows you to set 2 schedules, to automatically enable and disable the *Passage Mode* function in the smart devices *Libra*, *Aries*, *Stylos* e *x1R* (see *Enable Passage Mode* paragraph). That means the lock will automatically go in *Passage Mode*, following the set program.



Enable **Schedule Passage Mode** to see the two schedules available.

Tap on **Schedule 1** to enter the related programming menu.



Touch **Enable Schedule 1** to start the configuration.

At the end touch **Done**.

For each of the 2 programs, you can set 3 different behaviours, depending on your needs.

1. Passage Mode with Automatic Re-Lock.
2. Passage Mode with Automatic Activation and Automatic Re-Lock.
3. Passage Mode with Automatic Activation and Automatic Re-Lock with First Person In.

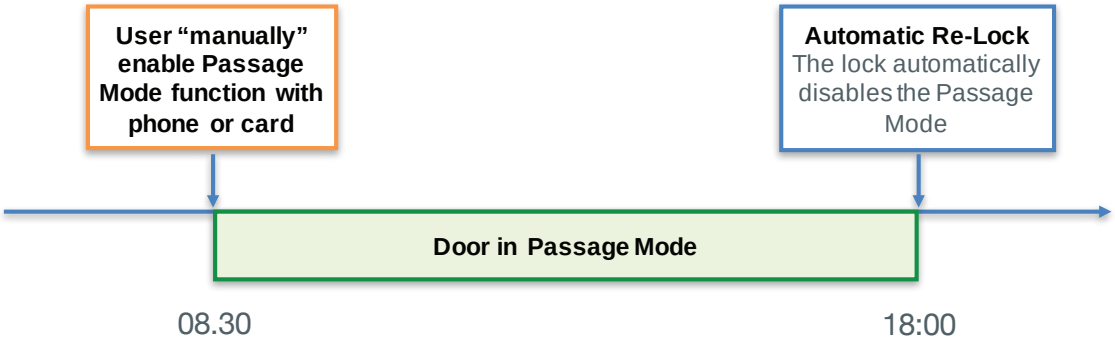
If *Stylos Smart* activates a device with an electric coil (electric lock or electric strike), before enable the *Passage Mode*, make sure the device can be kept always energized for a long time, without damage itself.

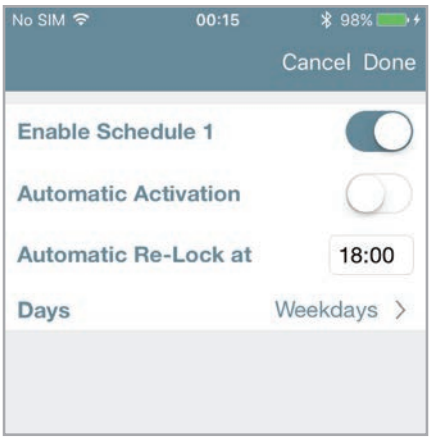
Advanced

Scheduled Passage Mode

1. Passage Mode with Automatic Re-Lock

With this program you need to “manually” enable in the device the *Passage Mode*, by smartphone (see *Enable Passage Mode*), or by card (see *Enable Passage Mode without Argo app*). But you don’t need to disable it, since you can set it automatically in the defined time and day.

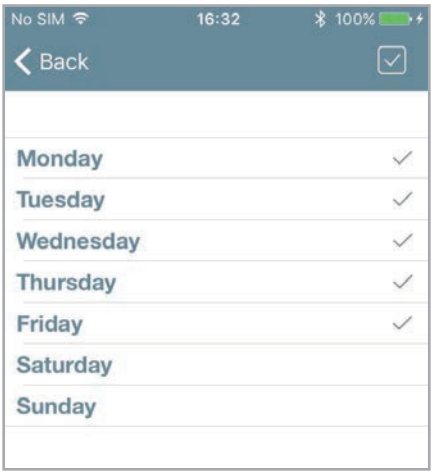




Switch on **Enable Schedule 1** to set **Automatic Re-Lock at**.

Select the time the lock will automatically disable the *Passage Mode*, if active, becoming cosed.

Touch to select the days on which the *Automatic Re-Lock* take place. The default is *Weekdays*: all days excluded Saturday and Sunday.



Check/uncheck all days with one touch.

Select multiple or single days, one by one.

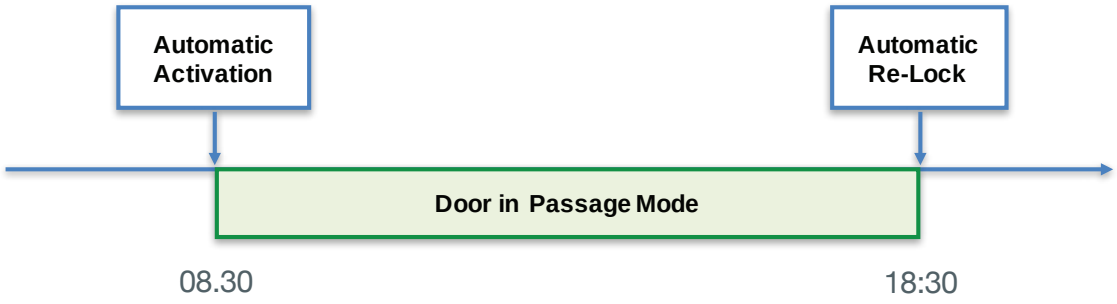
At the end press **Back**, then **Done**.

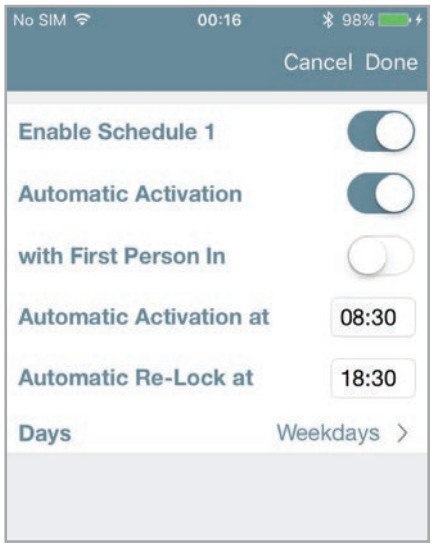
Advanced

Scheduled Passage Mode

2. Passage Mode with Automatic Activation and Automatic Re-Lock

With this program you can automatically enable and disable the *Passage Mode* in the doorlock, at certain time and days of the week.



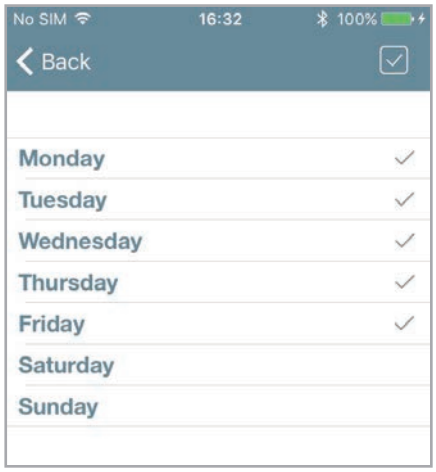


Swith on **Enable Schedule 1**.

Swith on **Automatic Activation**.

Select *Passage Mode* automatic activation time and re-lock time.

Select the days on which the program take place. The default is *Weekdays*: all days excluded Saturday and Sunday.



Check/uncheck all days with one touch.

Select multiple or single days, one by one.

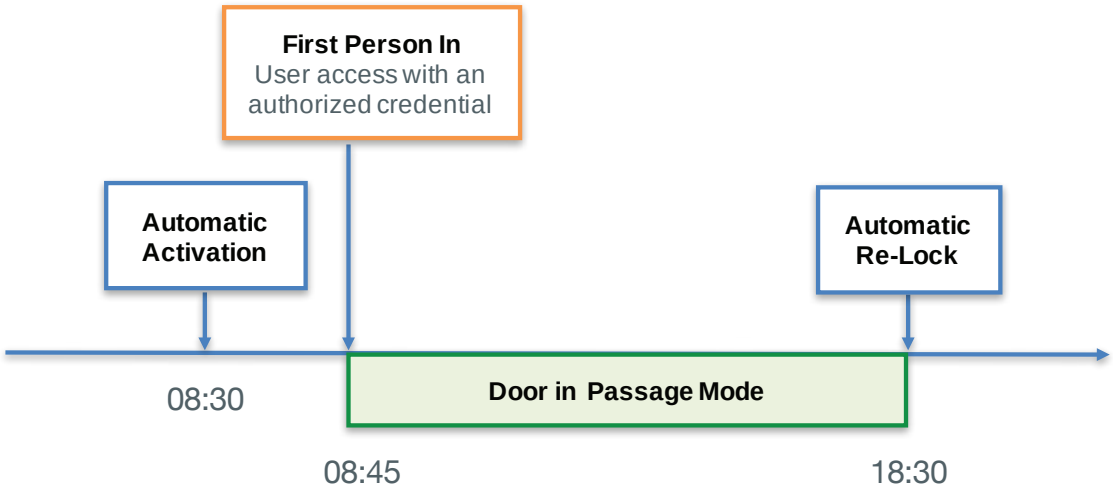
At the end press **Back**, then **Done**.

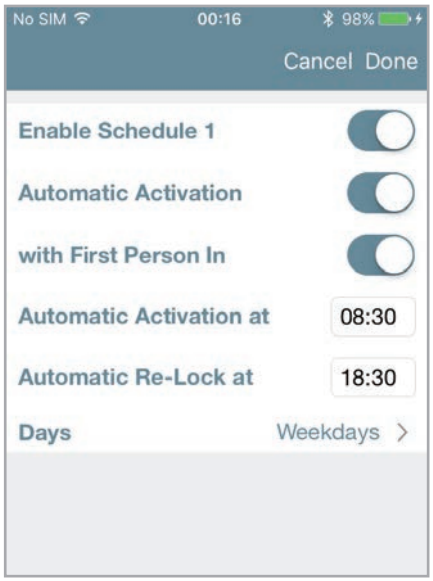
Advanced

Scheduled Passage Mode

3. Passage Mode with Automatic Activation and Automatic Re-Lock with First Person In.

With this program you can automatically enable and disable the *Passage Mode* in the doorlock, at certain time and days of the week, with one condition: the *Passage Mode* will actually start only after the first user entered the door, presenting a valid credential. The door at the activation time, will then be in a "potential" state of passage mode, which will only change after the first authorized entry (*First Person In*).





Swith on **Enable Schedule 1**.

Swith on **Automatic Activation**.

Swith on **with First Person In**.

Select *Passage Mode* automatic activation time and re-lock time.

Select the days on which the program take place. The default is *Weekdays*: all days excluded Saturday and Sunday.

At the end touch **Done**.

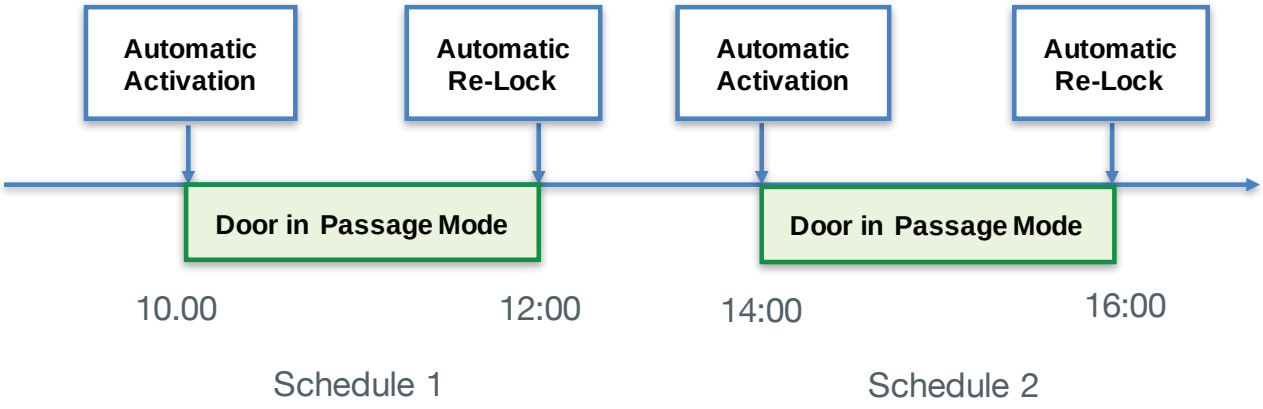
This solution is really useful in term of security and avoids the automatic *Passage Mode* activation when no user is inside the building or the room.

Advanced

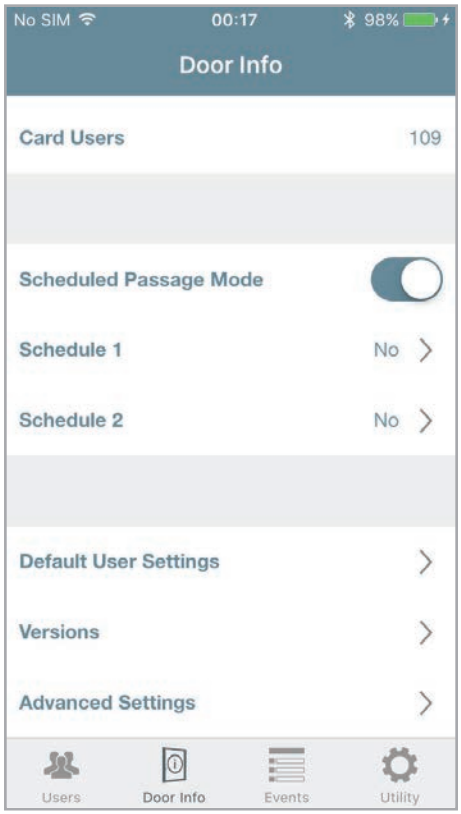
Scheduled Passage Mode

Configuration example: meeting room with Libra Smart

Inside a facility with offices, the meeting room door, equipped with *Libra Smart*, needs to be opened for all people on Tuesday and Thursday, from 10am to 12pm and from 14pm to 16pm.



Enter *Programming Mode,* then enter *Door Info* menu.



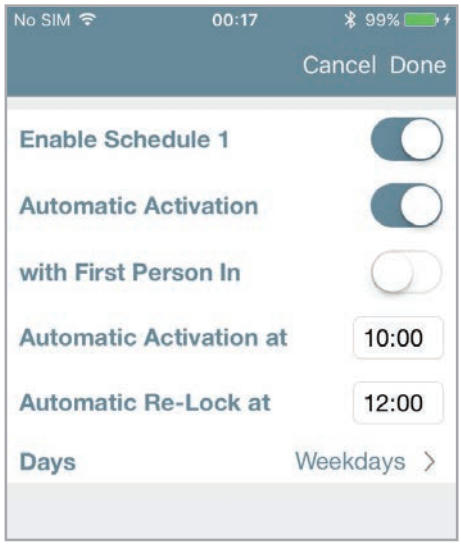
Enable **Schedule Passage Mode** to see the two schedules available.

Touch **Schedule 1** and then **Schedule 2**, to configure the 2 schedules.

Advanced

Scheduled Passage Mode

Configuration example: meeting room with Libra Smart

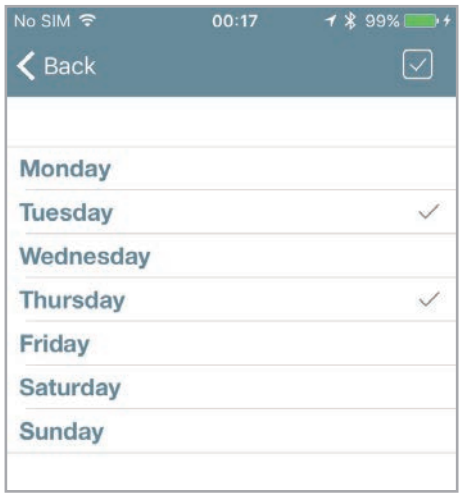


Switch on **Enable Schedule 1**.

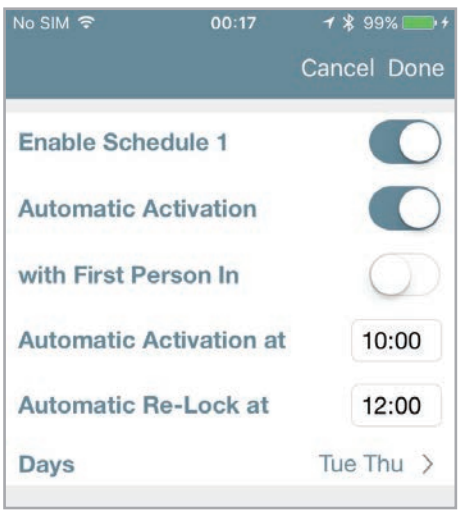
Swith on **Automatic Activation**.

Select *Passage Mode* automatic activation time and re-lock time, according to schedule 1.

Touch to select the days.



Select Tuesday and Thursday then tap **Back**.



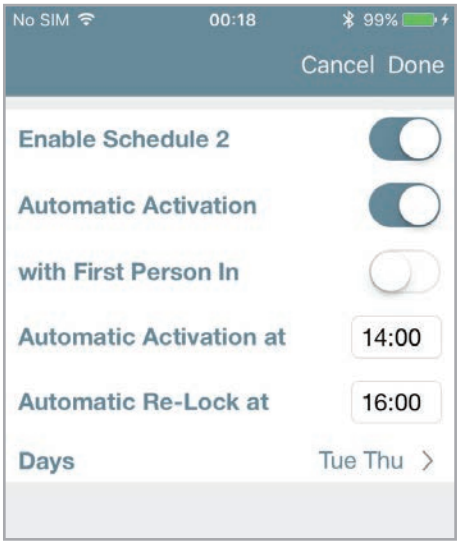
Tap **Done**.

Advanced

Scheduled Passage Mode

Configuration example: meeting room with Libra Smart

Repeat the same procedure for the *Schedule 2*, changing the timetables.

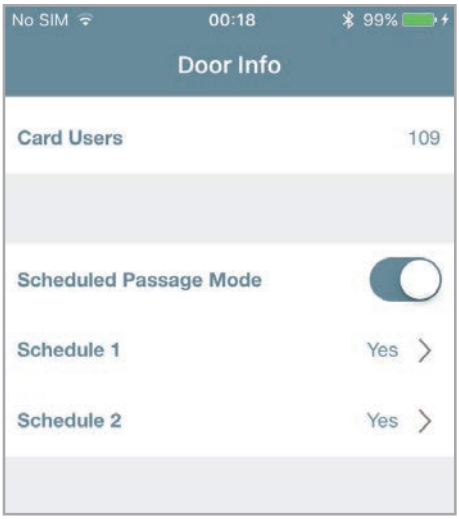


Switch on **Enable Schedule 2**.

Swith on **Automatic Activation**.

Select *Passage Mode* automatic activation time and re-lock time, according to schedule 2.

Touch to select Tuesday and Thursday.



The programming is finisched.

To turn off all the scheduling, simply turn off the **Scheduled Passage Mode** slide button.
When the button is switched on again, all programming previoulsy done will resume.

Argo keeps always in memory the last programming made. To temporarely disable a scheduling, simply turn off the *Scheduled Passage Mode* slide button. When the button is switched on again, all previous programming will be restored.

Advanced

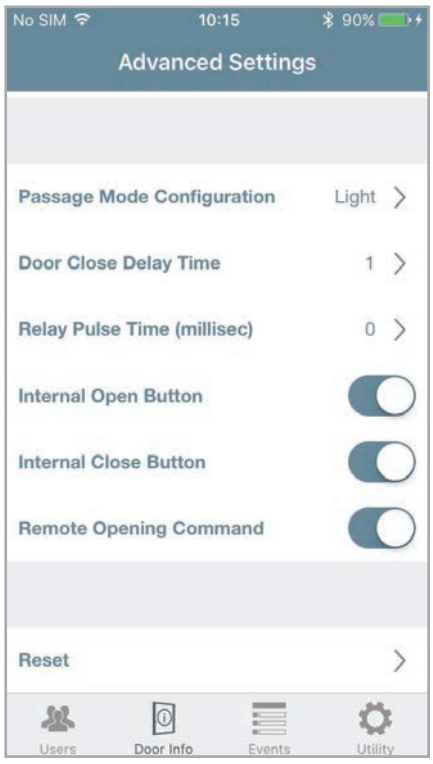
x1R Smart: Light Mode

A door in *Passage Mode* is always opened for any user who wishes to gain access, without the use of authorized credentials. We can also say the door is “Free”, as free to entrance, since the devices (Libra, Aries, Stylos and x1R), are always mechanically engaged, to ensure to always open the door.

In the electronic motorized locks for armoured doors market, used in offices aplications (common doors with hight transit of people), the needs is different: the door should not be always opened but closed only with the latch. This state is called “Light”, just because the lock, not closing the bolts, is not completely secure.

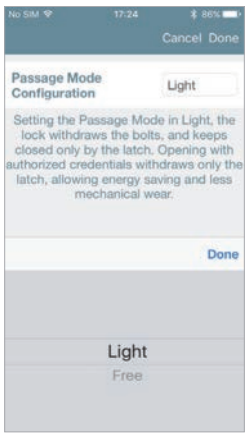
This solution combined to with *x1R Smart* is very useful and effective because it has the following advantages:

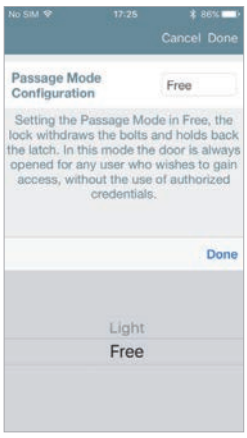
- high battery saving;
- reduced mechanical wear of lock, bolts, rods and deviators;
- higher opening speed;
- less noise during opening and closing movement.



This configuration is only present in the *Advanced Settings* menu of *x1R Smart*.

Enter *Advanced Settings* menu and touch to change the *Passage Mode Configuration* from *Light* to *Free*. *Light* mode on *x1R Smart* is set by default.





Only *x1R Smart* can be set in *Passage Mode Free* or *Light*. On all the other devices this menu is not present

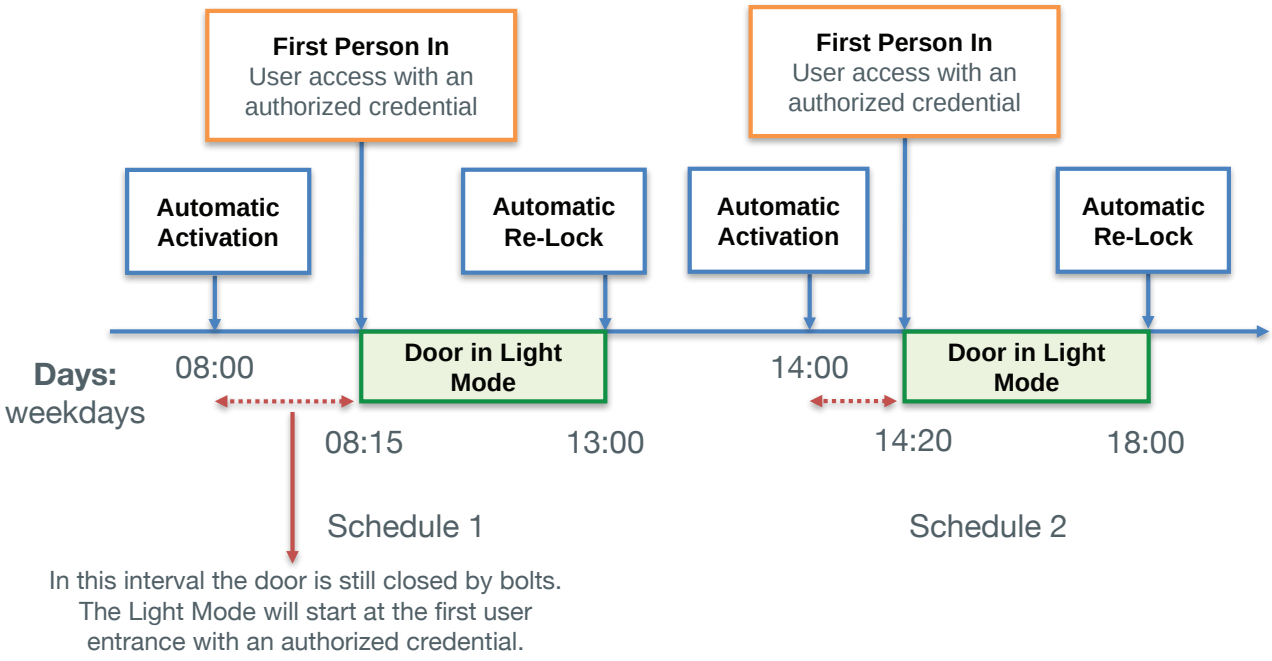
To know more about *x1R Smart Light* function, read the *x1R Smart User Manual*, available at site *https://app.iseo.com*.

Advanced

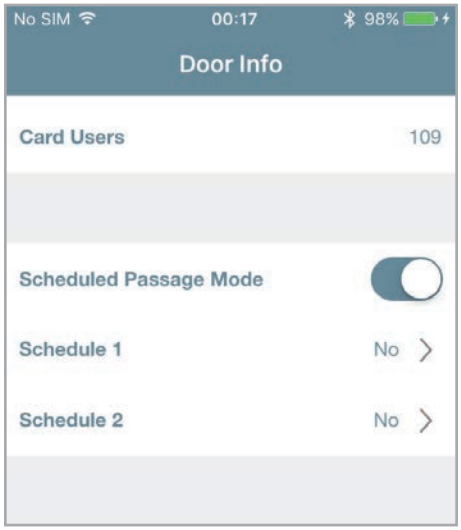
x1R Smart: Light Mode

Configuration example: main offices entrance with x1R Smart

Inside a facility with offices, the main entrance, equipped with *x1R Smart*, needs to enter in *Light Mode* on weekdays, from 8am to 13pm and from 14pm to 18pm. But only after the first employee or authorized user has entered the door.



Enter *Programming Mode,* then enter *Door Info* menu.



Enable **Schedule Passage Mode** to see the two schedules available.

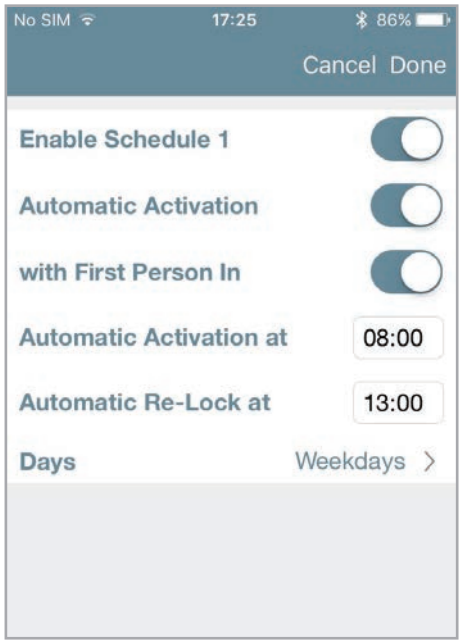
Touch **Schedule 1** and then **Schedule 2**, to configure the 2 schedules.

Light mode on *x1R Smart* is set by default.

Advanced

x1R Smart: Light Mode

Configuration example: main offices entrance with x1R Smart



Switch on **Enable Schedule 1**.

Swith on **Automatic Activation**.

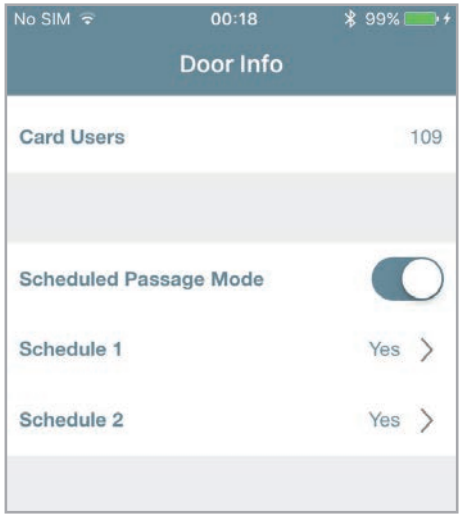
Switch on **with First Person In**.

Select *Ligh Mode* automatic activation time and re-lock time, according to schedule 1.

Weedays are already set by deafult.

At the end touch **Done**.

Repeat the same procedure for the *Schedule 2*, changing the timetables (14:00 - 18:00).



The programming is finisched.

To turn off all the scheduling, simply turn off the **Scheduled Passage Mode** slide button.
When the button is switched on again, all programming previoulsy done will resume.

Argo keeps always in memory the last programming made. To temporarely disable a scheduling, simply turn off the *Scheduled Passage Mode* slide button. When the button is switched on again, all previous programming will be restored.

Advanced

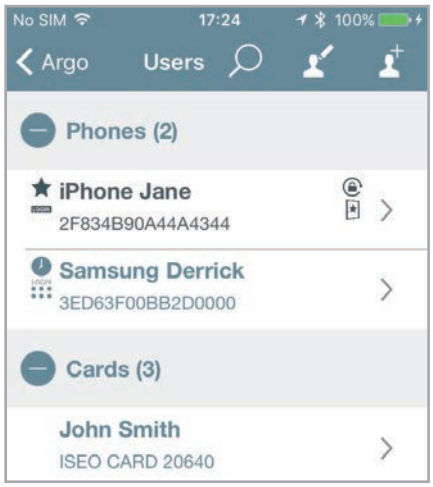
Invitations

Invitations allows smartphones to self-register into the lock as users, by using an *Invitation Code*, previously memorized in the doorlock by the *Administrator*.
In a company scenario, for example, with the *Invitation* function is possible to allow staff members to add their smartphone to the *Argo User List*, without needing to be physically in front of the door, with the phone to login. To do that the *Administrator* previously add an *Invitation Code* to the lock, as one of the 300 users, and send this code to the person to whom he/she must grant access. When the *User* arrives in front of the door, opens the *Argo app* and types the *Invitation Code* by phone. The door will open and the smartphone will self-register into the lock *User list*, for the period of time specified in the invitation.

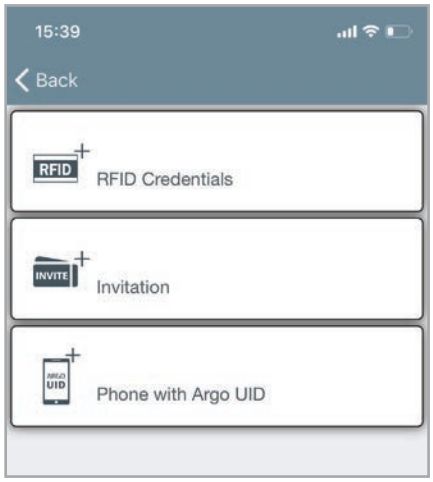
To fully explain how to program, manage and use *Invitations* by *Argo*, we can describe it in 3 main steps:

- Step 1: the *Administrator* adds and sends the invitation code to the *User*.
- Step 2: the *User* receives the invitation code and access to the door.
- Step 3: the *Administrator* enter *Programming Mode* to manage the *User list.*

Step 1: the Administrator adds and sends the Invitation Code to the User



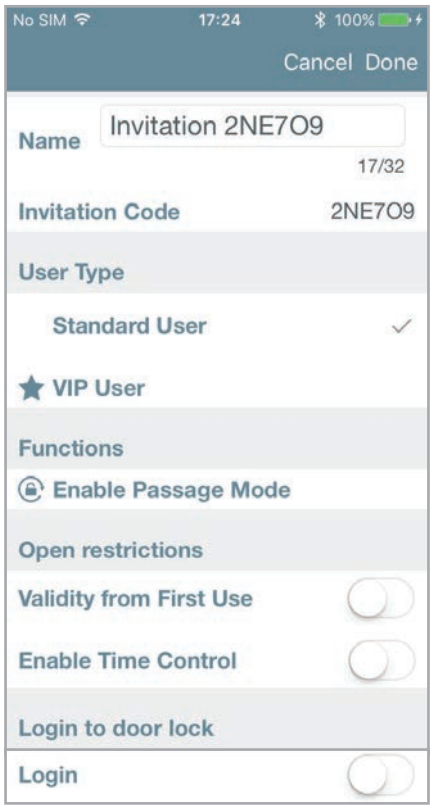
1. Enter *Programming Mode*
2. Tap the *add user* icon



3. Tap **Invitation**

Advanced

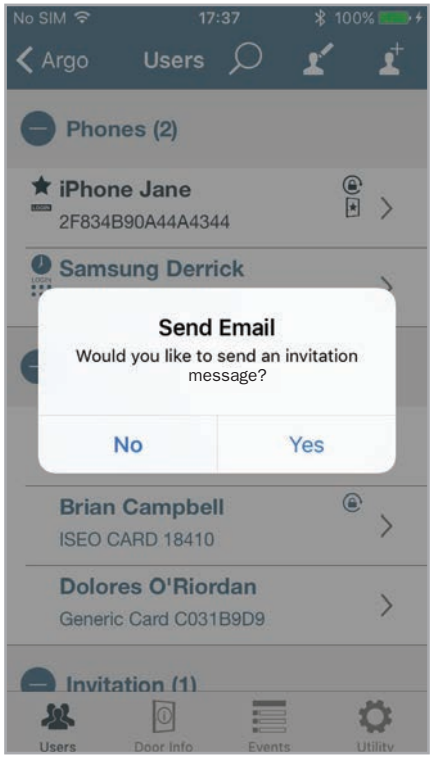
Invitations



4. The name box is automatically compiled with the **Invitation Code**, but you are free to change it as you like. For example with the name of the user to whom the invitation is reserved, or adding a personal progressive number (i.e.: Invitation 1)

5. You can enable all the smartphone user parameters like any other user. You can select the **User Type**, the **Functions**, the **Open Restrictions** and even the **Login to Doorlock** if required (for more information see *Smartphone user parameters*).

6. Press **Done** in the top right corner.

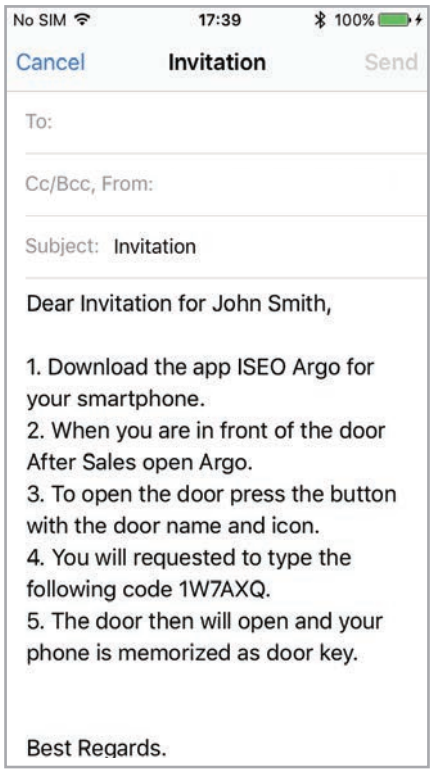


7. An automatic pop-up message will ask you to send a message with the *Invitation Code*.
   - Press **Yes** if you want to send it immediately.
   - Press **No** if you want to send it afterwards.

You can send the invitation message with any communication app: email, whatsapp, sms...
In the following example we show by email.

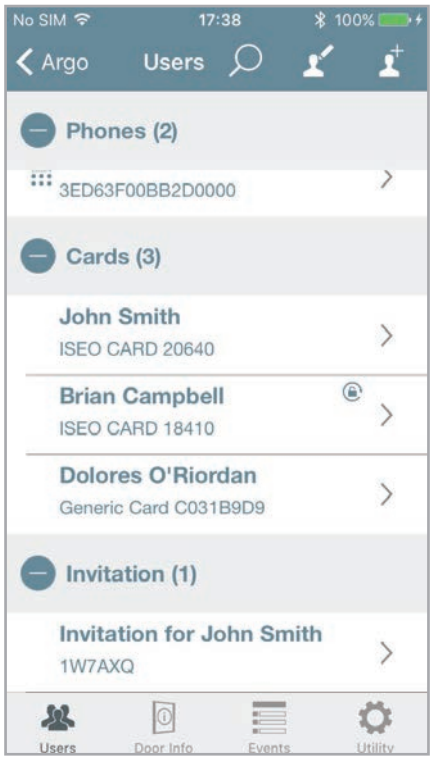
Advanced

Invitations



8. An email is automatically generated with a pre-compiled text that explains, step by step, how to use the *Invitation Code* to access the door. The recipient of the email infact may not know *Argo* and how to use it.
Just add the recipient's email address then press **Send**.

If the invitation has a *Validity* (*Activation* and *Expiration* date and time), or a *Validity from First Use*, or even *Time Schedules*, all those information will be automatically reported in the email. In this way the recipient of the invitation will be immediately aware about its open restrictions.



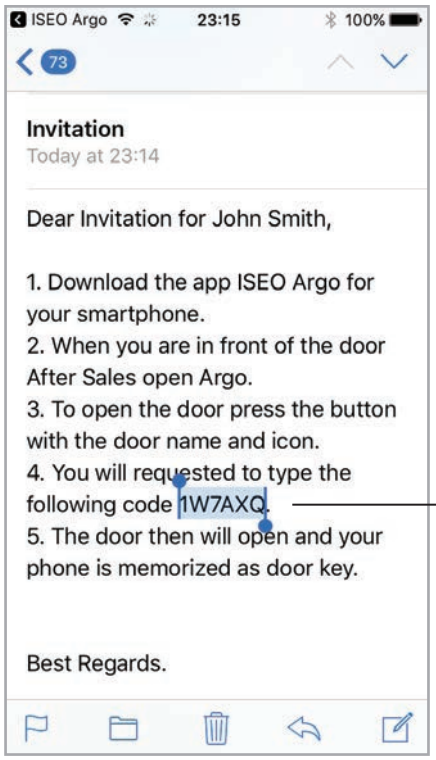
9. You can see in the *Argo User List* the added invitation, in the **Invitations** user field.
You can always modify the existing invitations like any other credential, adding or changing functionalities: *User Type*, *Functions*, *Open restrictions*, *Login to Doorlock*.

If you modify an invitation after the email has already been sent, remember to send it again, to inform the recipient about the modification done.

Advanced

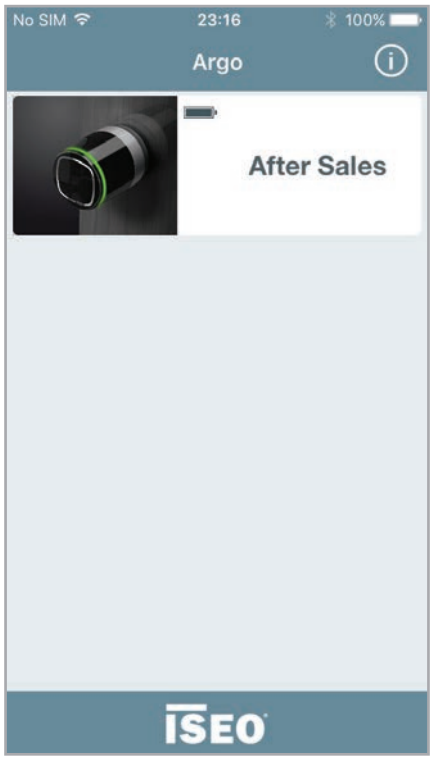
Invitations

Step 2: the User receives the Invitation Code and access to the door



1. The *User* receives the email with the step by step instructions and the *Invitation Code*.

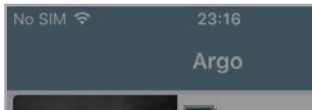
Invitation Code



2. When the *User* is in front of the door, he/she can press the button with the door name and icon to open the door.

Advanced

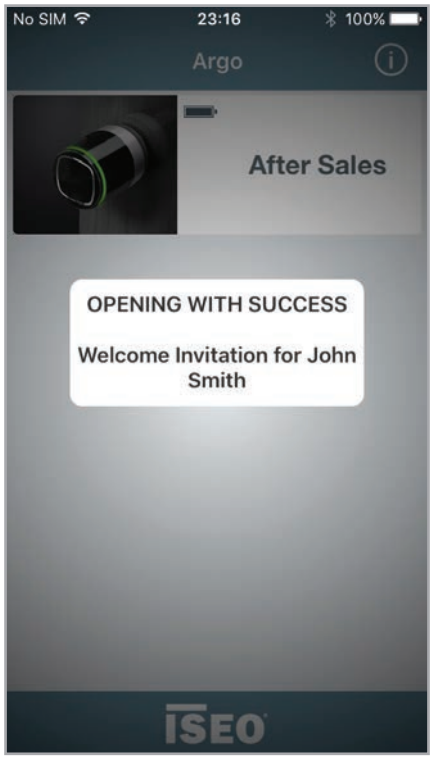
Invitations



3. A pop-up message will ask to type the *Invitation Code* to access the door.

   Type the *Invitation Code* previously received by email and press **OK**.

To easily type the *Invitation Code* you can also take advantage of the copy and paste text smartphone functionality.



4. If the *Invitation Code* is valid the door opens.

At the next openings the code will no longer be required, since the phone has been self-registered into the lock.

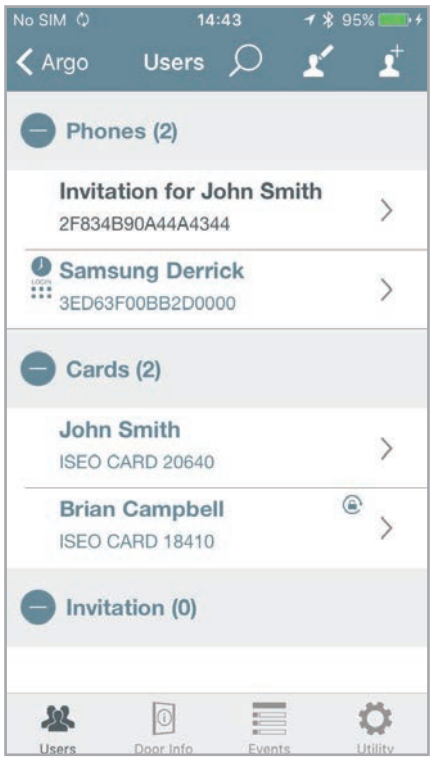
The invitation will expire at its expiration time and date, if previously set.

The *Invitation Code* can be used once only.

Invitations

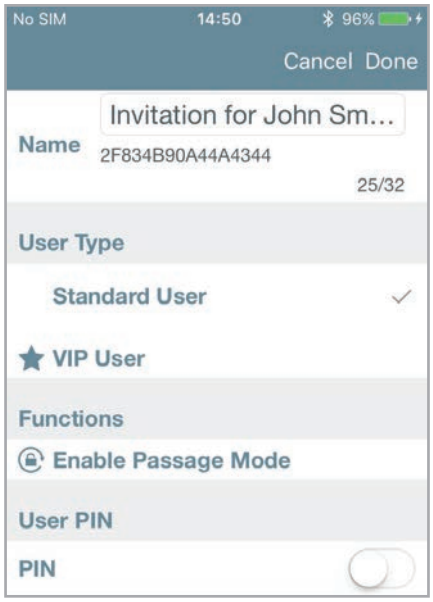
Step 3: the Administrator enter Programming Mode to manage the User list.

In the *User list*, the *Administrator* will see that *Invitation* once consumed, become a phone, like any other one in the user list, inheriting all the data, functions and open restrictions previously set in the invitation.



The *Invitation*, once consumed, become a phone and you can see it in the *User List* like any other memorized phone.

No more pending *Invitation* are present in the *User List*.



Entering the *Phones user parameters* you will see all the data inherited from the consumed invitation.

The *Invitation Code* has been replaced by the *UID* of the self-registerd phone.

Advanced

Invitations

Questions and answers

Following are reported some of the most commons questions, with related answers, about *Invitations*.

1. How many *Invitations* can I create and send?
   Answer: *Invitations* are memorized in the *Argo User List* like any other user, so theoretically you could create up to 300 *Invitations* (maximum nr. of users).

2. Can I use the same *Invitation* for more doors? For example: if there is a common passage door, before the door the user has to open by the *Invitation*, can I extend the *Invitation* also to this common door?
   Answer: yes, the *Administrator* once has created the *Invitation* on one door, by the *Copy and Transfer User* functions (see related paragraphs), can copy the same *Invitation* to other doors. The user will type the *Invitation Code* in all the doors on which the *Invitation* has been copied, self-registering at the same time its phone on that doors.

3. Can I send the *Invitation* by *SMS* message or *WhatsApp*?
   Answer: yes, from *Argo 2.4* you can send *Invitations* by any communication app. In addition you're always free to copy the *Invitation Code to* send it or manage it as you like.

4. Can I modify an *Invitation*?
   Answer: yes, the *Administrator* can always modify an *Invitation* entering *Programming Mode,* like any other user. At every modification done, *Argo* always asks if you want to send the email with the *Invitation Code*.

5. Can I send an *Invitation* to a staff member later on, even if I'm not in front of the door?
   Answer: yes, the *Administrator* can send the email whenever he/she wants. Just confirm *No* to the *Invitation email* pop-up message.
   Remember on *Argo,* to create *Invitations*, you need to be in front of the door as *Administrator*, to enter *Programming Mode* and manage the lock. Then taking advantage of the *Validity from First Use* function, and sending the email for example to yourself for data record purpose, you could then send it afterwards to your staff member, when you prefer.

6. Is the 6 digits *Invitation Code* secure?
   Answer: yes, it is an alfanumeric code and all the possible combinations are more than 2 billions. Trying all possible combinations (it's called "brute force attack"), by an automatic machine that tries a different code every 1 second, it would require about 70 years.

Advanced

Invitations

Questions and answers

7. Could it happen that *Argo* generates an *Invitation Code* equal to the previous one?
   Answer: no, it's practically impossible. The *Invitation Codes* are randomly generated by using a random number generator that complies to the NIST specifications (National Institute of Standard). The NIST ensures the maximum uniform distributions of random codes and it's one of the most competent authorities in the field.

8. Could the *Invitation Code* be read throught the email by an hacker?
   Answer: usually email are cripted, but in case you don't trust the email security, you're free to deliver the *Invitation Code* as you like: by voice, taking advantage of WhatsApp end to end encryption, or by other more complicated encryption way or software.

Advanced

Argo for Apple Watch

Argo App is compatible to Apple Watch from Series 3, running WatchOS 4. With Apple Watch you can unlock the ISEO Smart Devices exaclty like the Argo app: just launch the Argo Apple Watch App and press your ISEO Smart door lock button. You can add Argo as complication in the Apple Watch allowing a shortcut from your default smartwatch screen (face). Since the Apple Watch can be paired uniquely with one iPhone, the iPhone and the Apple Watch are the same key to open your door lock.

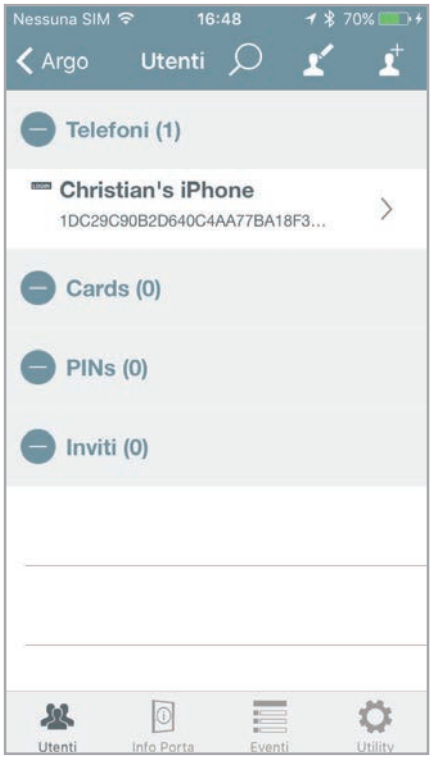
Minimum iPhone requirements

- Apple Watch Series 3 (GPS + Cellular) requires an iPhone 6 or later with iOS 11 or later.
- Apple Watch Series 3 (GPS) requires an iPhone 5s or later with iOS 11 or later.

In horology, a complication refers to any feature beyond the simple display of time (see *Keywords*).

To enable the Apple Watch to open an ISEO Smart device, follows the next steps.

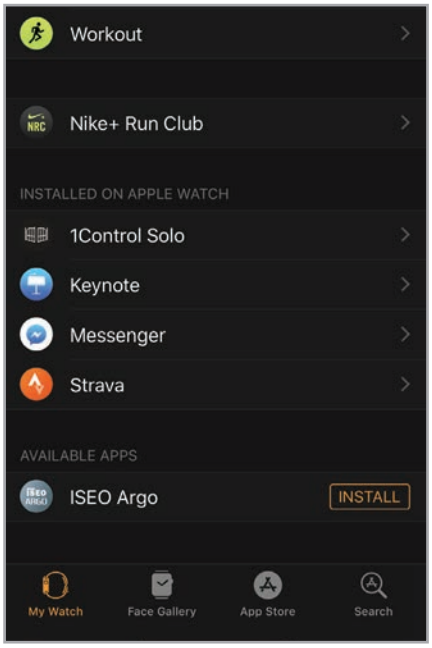
Step 1: add your smarpthone to the ISEO Smart device user list



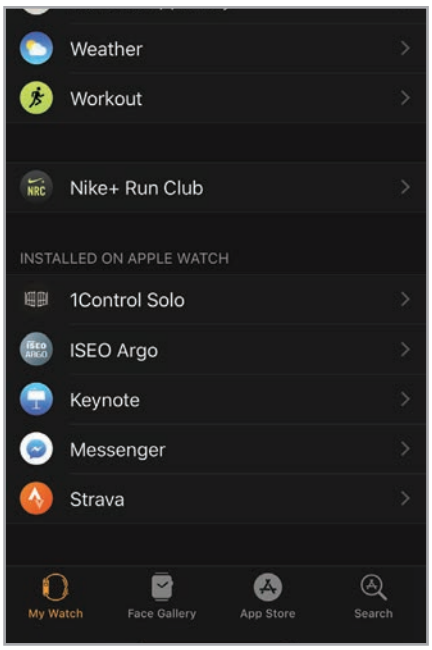
Smartphone added to the *User List*.

Argo for Apple Watch

Step 2: install Argo in the iPhone Watch app.



Tap **INSTALL**.



Argo app correctly installed on Apple Watch.

Installing apps in the Apple Watch, may take a long time.

For specific and detailed Apple Watch instruction, refer to the *Apple Watch User Guide* available at *support.apple.com.*

Argo for Apple Watch

Step 3: open Argo app in the Apple Watch

Tap on ISEO Argo icon

Only at the first installation of the Argo app in the Apple Watch, it is requested to open the Argo app in the iPhone. Then it will no longer be necessary unless you uninstall Argo from the Watch or from the iPhone.

Open the Argo app on your iPhone, then touch Open Argo app in the Watch.

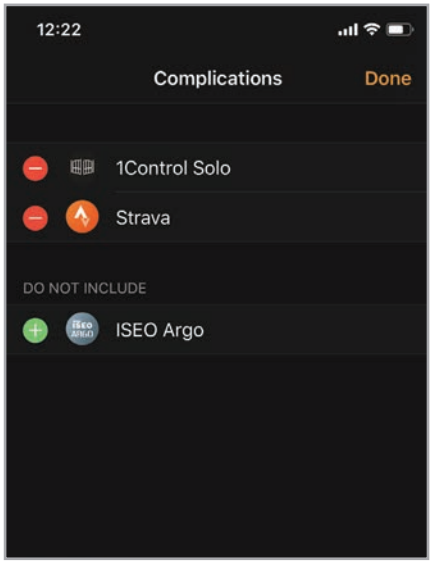
Advanced

Argo for Apple Watch

Touch the door name button to open the related ISEO Smart Device.

To add Argo app as complication in the Watch Faces, follows the next steps.

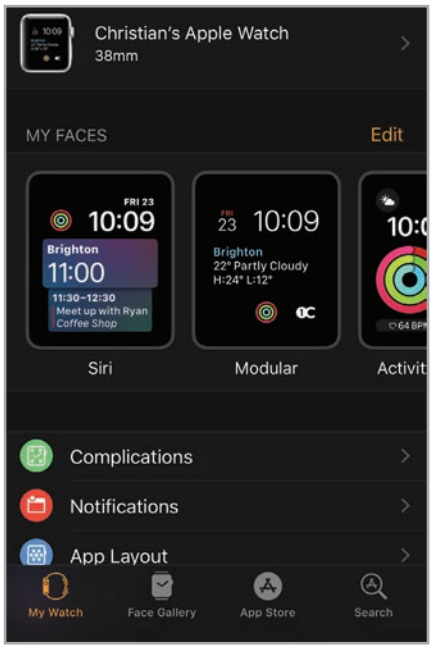
Step 1: add Argo app as complication in the Watch app.



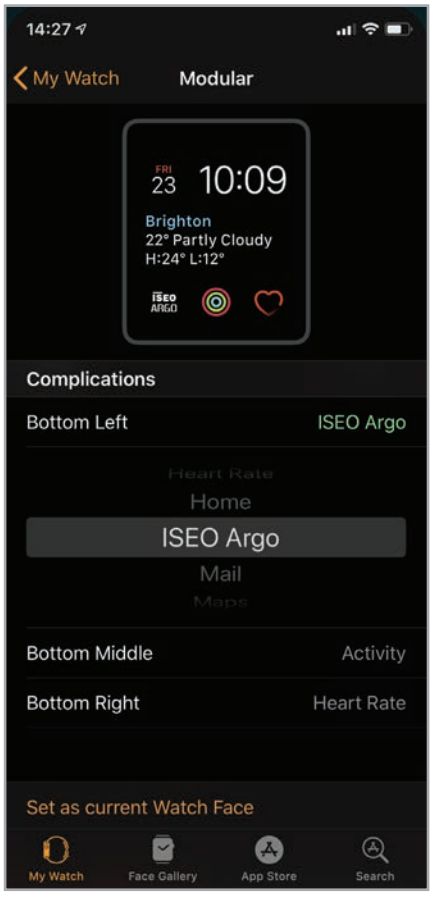
Tap **+** to add ISEO Argo as complication available in the Watch faces.

Argo for Apple Watch

Step 2: customize your Watch Face adding Argo complication (by iPhone)



On **MY FACES** chose the Watch Face to modify.



Example:
select ISEO Argo as Bottom Left complication.

Argo for Apple Watch

You can also customize Watch Faces by the Apple Watch.

Step 2bis: customize your Watch Face adding Argo complication (by Apple Watch)

With the watch face showing, firmly press the display, then tap **Customise**.

If a face offers complications, they’re shown on the last screen.
Tap a complication to select it, then turn the Digital Crown to choose ISEO Argo. When you’re finished, press the Digital Crown to save your changes, then tap the face to switch to it.

Advanced

Argo for Apple Watch

You can add ISEO Argo complication in different Faces and position. Depending on the Face type (Circular, Modular, Utility...), complication position and Watch case size, ISEO Argo complication may look different. See below some examples with differenct Faces.

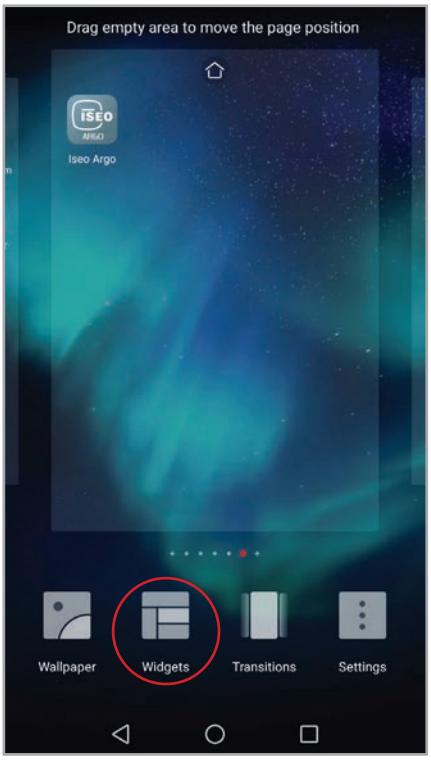
Advanced

Widgets for Argo app

The Argo widgets allows you to unlock directly your door lock without launching the Argo App (see *Keywords* for widget meaning). By using a widget infact Argo App will automatically start, open the ISEO Smart device and close. Widgets configuration and behaviour differs from iOS to Android as explained in the following configuration procedures.

Step 1: configure Argo widgets for Android

In Android phones when you add a widget, you can define which doorlock to open and you can position the widget in any place of the screen as a shortcut.



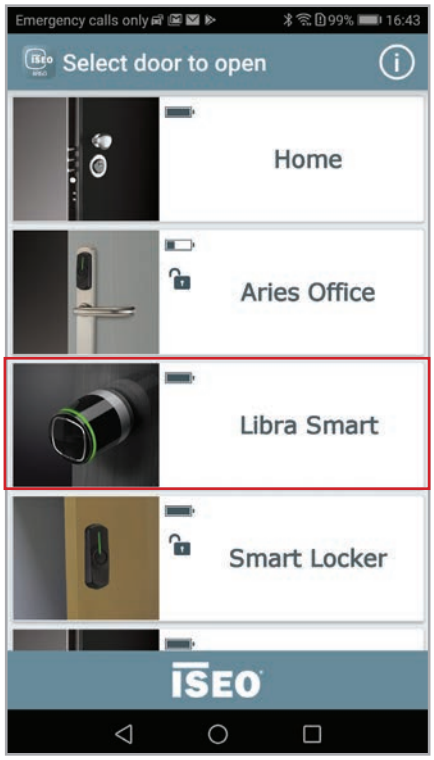
In the home screen, firmly press an empty area of the display, then tap **Widgets** in the bottom bar.

Widgets configuration on Android phones may vary depending on phone model and operating system.

Tap on **Argo Widget** or drag it into an empty area of the screen.

Advanced

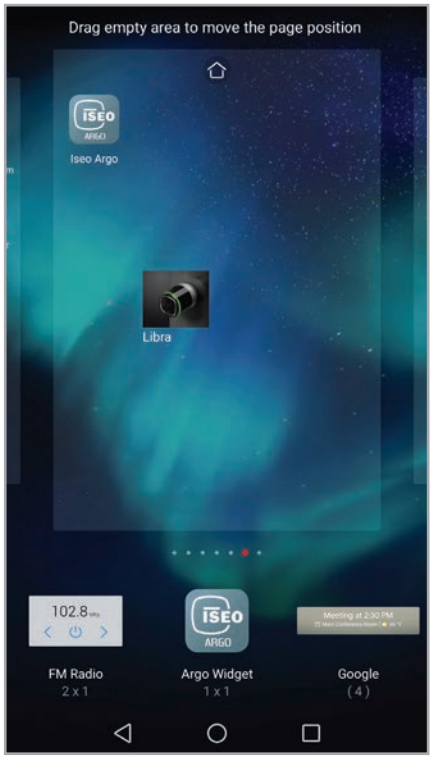
Widgets for Argo app



Argo app automatically opens.

Tap on the doorlock you wish to open by widget (Select door to open). For example: Libra Smart.

If you do not choose any device and close the application, an “empty” Argo icon is however automatically created in the phone home screen. When you tap it, it will open the same “Select door to open” screen, in order to choose which door open.

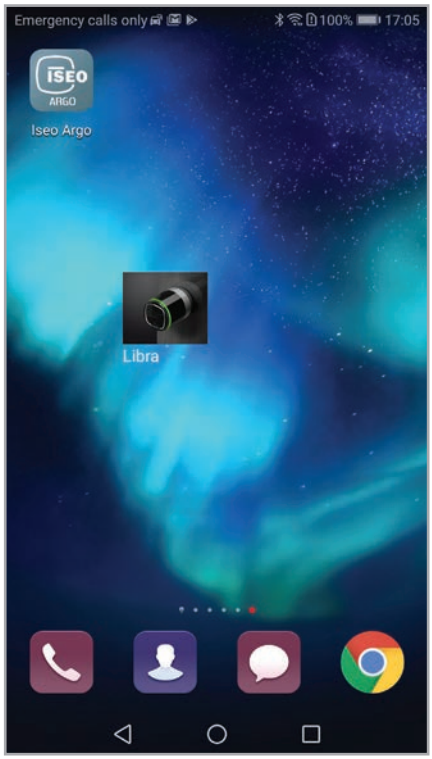


The Libra icon widget is automatically created.

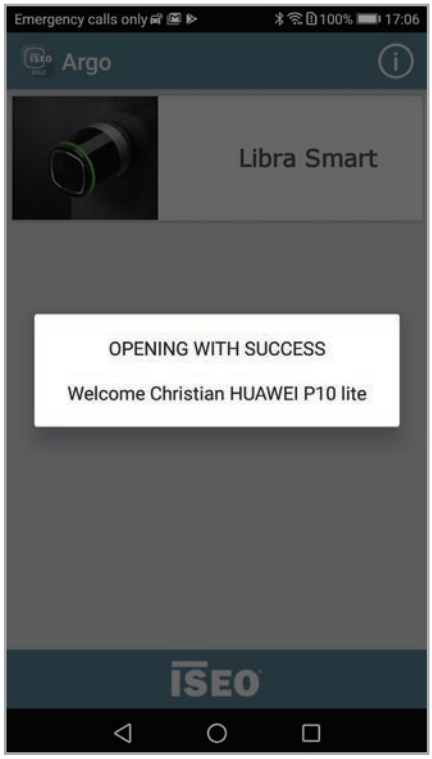
Tap an empty area of the screen to exit the configuration mode.

Widgets for Argo app

Step 2: open the door by Android widget



Tap the Libra icon widget.



Argo app automatically starts and opens the door. When finished the app automatically closes.

You can create a widget even if your phone has not been added to the user list of the device but tapping the widget you will get the message: “Phone not enabled: not in memory”.

Advanced

Widgets for Argo app

Additional notes for Android widgets

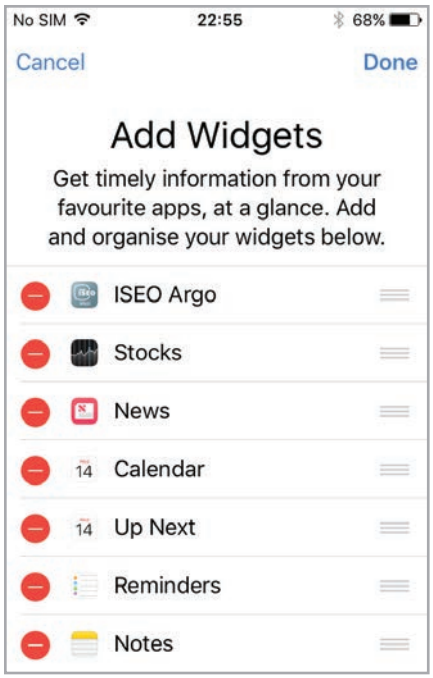
Android widgets can be freely customized in size.

You can create how many widgets you need. Each product has its corresponding widget icon.

Widgets for Argo app

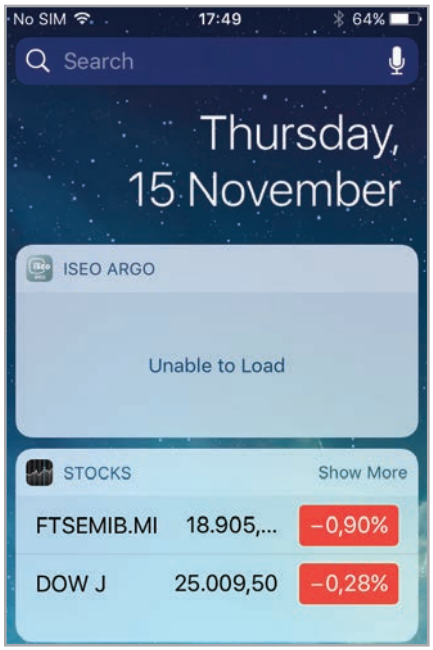
Step 1: configure Argo widgets for iOS

In iOS devices the widgets configuration and management is completely different from Android. While on Android you can create widgets even if you're not enrolled as user in the device, with iOS you need to open before the device, at least one time, by Argo app.



Add ISEO Argo widget to the Today View of your iOS device (iPhone or iPad).

For the instruction about Today View configuration read *Use widgets on your iPhone, iPad* available at *support.apple.com*

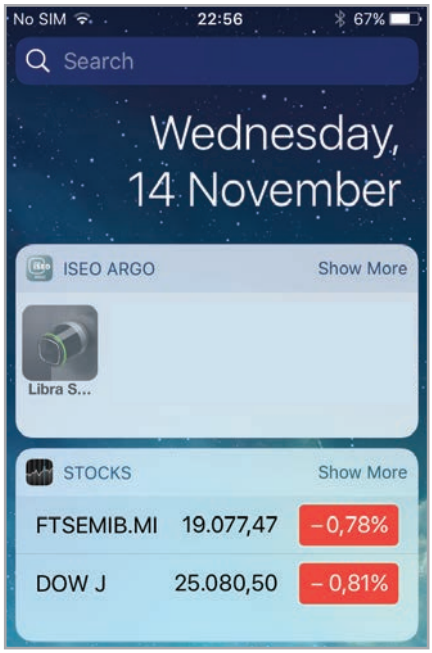


ISEO Argo widget will be empty: you need to open a door before, to get the shortcut.

Widgets for Argo app

Step 2: open the door by iOS widget

First open the door, you wish to add as widget in the Today View.

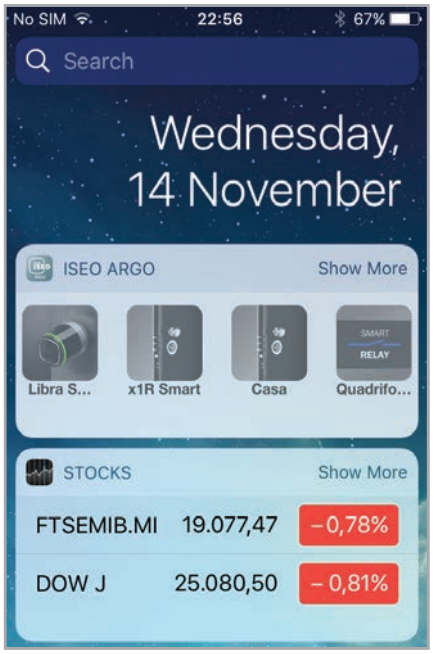


You will see the door icon in the today view. Tap it to automatically open the door by Argo app. Argo app starts and opens the door. When finished the app automatically closes.

You cannot see the door icon in the Today View if your phone has not been added to the door *User List* and if you don't have opened the door at least one time.

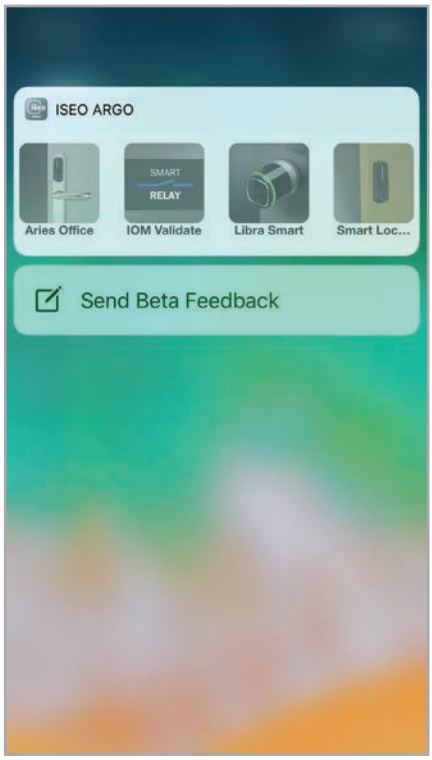
Widgets for Argo app

Additional notes for iOS widgets



As soon as you open doors by phone the shortcut icon is automatically added to the ISEO Argo widget in the Today View, in the first position.
You can see the last 4 door locks you have opened.

Tap **Show More** to see the last 8 door locks you have opened (extended view).



From iPhone 6s and above you can use 3D Touch as a shortcut to ISEO Argo widgets. Simple force touch on Argo icon to immediately open the last 4 opened doors.

Doors opened in the past, belonging for example to other plants, are always displayed until new opened doors replace them, moving the old ones over the eigth position.

It is not possible to delete the ISEO Argo widget icon list even removing and re-adding the widget from the Today View. Last opened doors keeps in the Today View memory.

Advanced

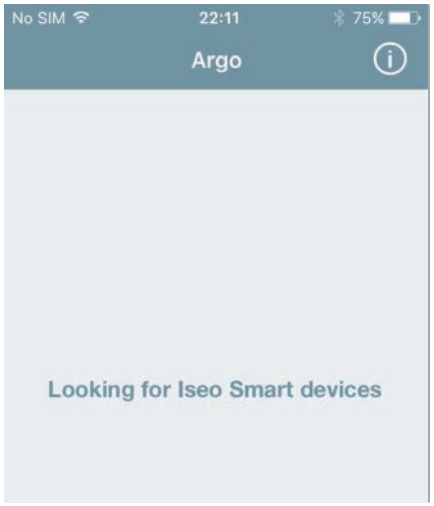
Add phone with Argo UID

Administrators can add a smartphone in the device *User List* by typing the phone *Argo UID*. The goal is the same as the *Invitations* (see *Invitations* paragraph), with the difference that by *Argo UID* the user does not need to type any code. The phone *Argo UID* is the *Unique IDentifier* of the Argo App installed in your smartphone. It is a globally unique number (32 characters), which identifies your smartphone in the Argo smart devices.

To add phone with *Argo UID* follow the next steps:

- Step 1: *User* sends the phone *Argo UID* to the *Administrator*.
- Step 2: *Administrator* adds the phone *Argo UID* to the device *User List*.

Step 1: User sends the phone Argo UID to the Administrator

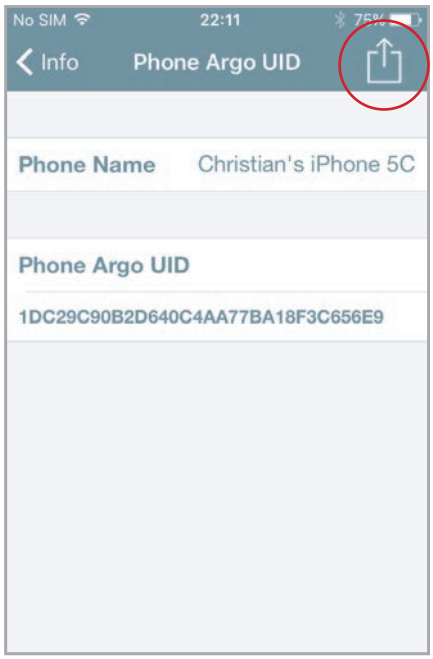


User downloads and installs the *Argo app* on his phone.

1. Tap *info app* icon

2. Tap **View Phone Argo UID**

Add phone with Argo UID



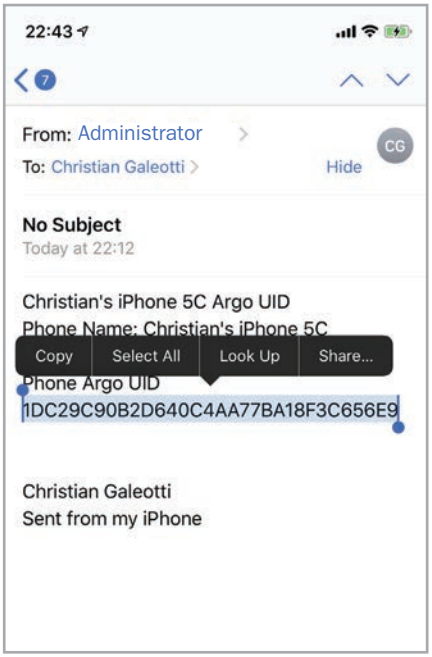
3. Tap share icon.

4. Send the phone Argo UID to the Administrator by any communication app: email, whatsapp, sms...

   In the following example we show by email.

Add phone with Argo UID

Step 2: Administrator adds the phone Argo UID to the device User List.

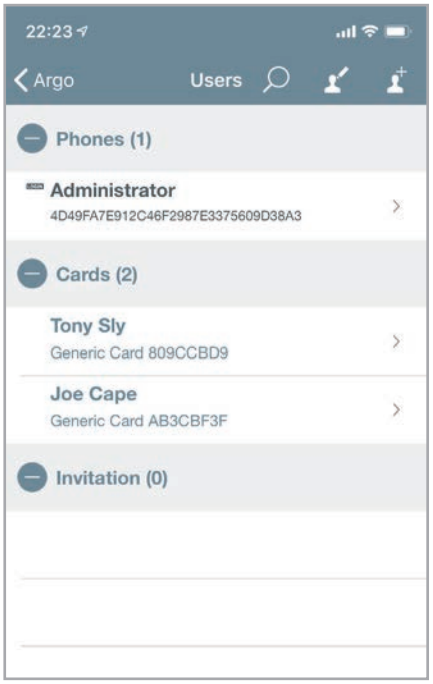


Administrator receives the email from the User.

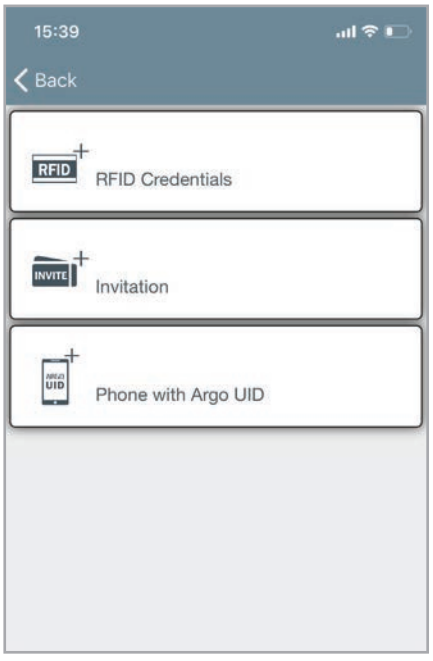
1. Copy the phone Argo UID

2. Approach the device where you wish to add the user phone and enter *Programming Mode*.

Add phone with Argo UID

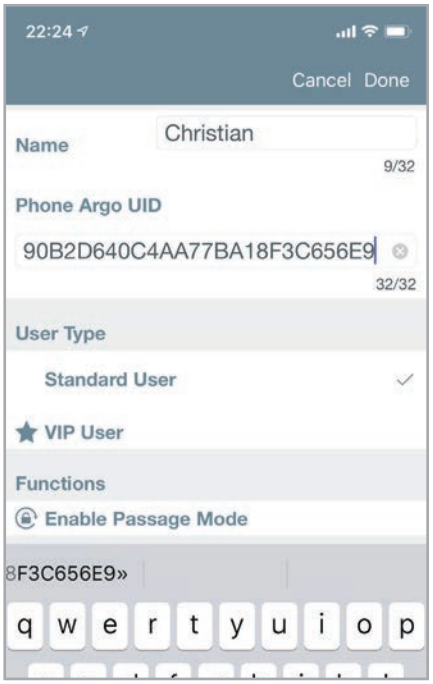


3. Tap the *add user* icon 



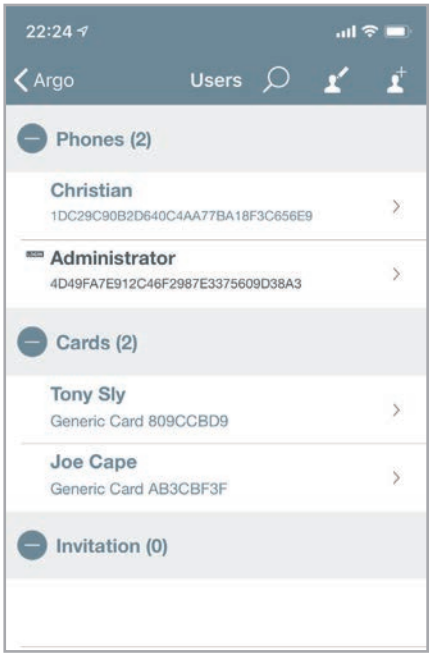
4. Tap **Phone with Argo UID**

Add phone with Argo UID



5. Type the User name

6. Paste the phone Argo UID previously copied then touch **Done**.

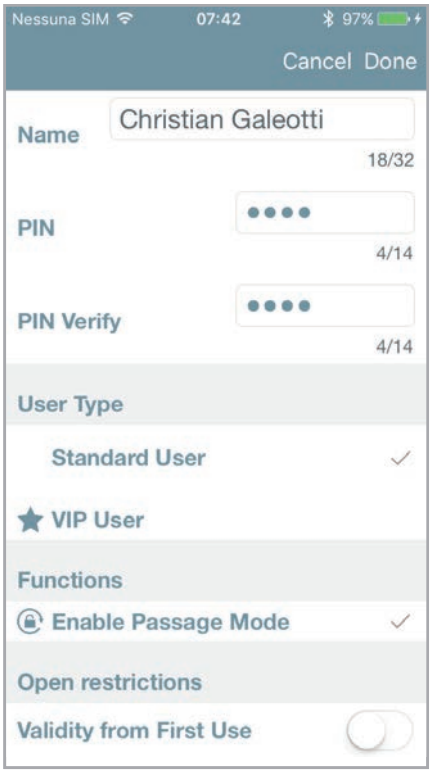


7. The User has been added to the device User list by phone Argo UID.

Advanced

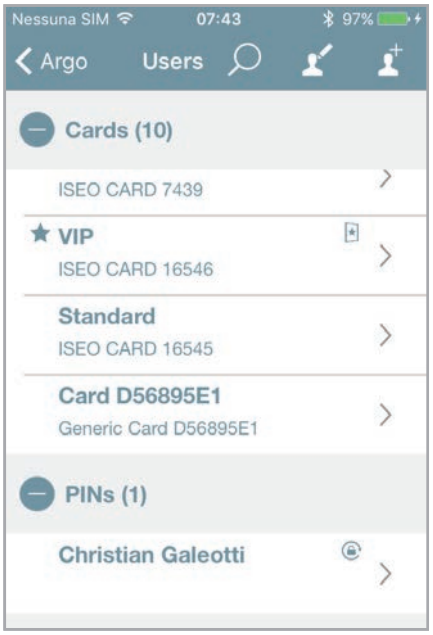
Passage mode with PIN code

The ISEO Smart devices equipped with external keyboard (i.e. *Stylos Display* and *x1R Smart*), have the possibility to enable the *Passage Mode* function for PIN codes, as we do for Cards/Tags and Smartphones (i.e. see *Card User Parameters*). The PIN with *Passage Mode* enabled, will automatically enable and disable the *Passage Mode* in the door lock every time the code is entered.



Enter a user PIN code (see *Add users typing PIN code* in the *Basics* chapter).

Tap **Enable Passage Mode**.

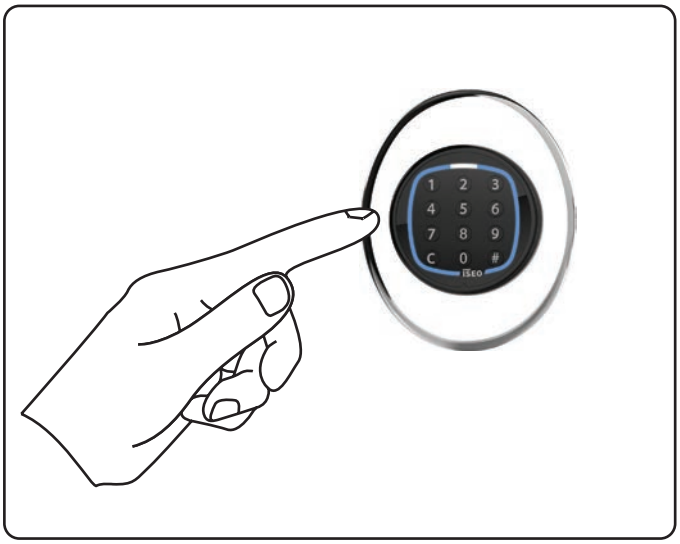


PIN code has now *Passage Mode* capability.

Advanced

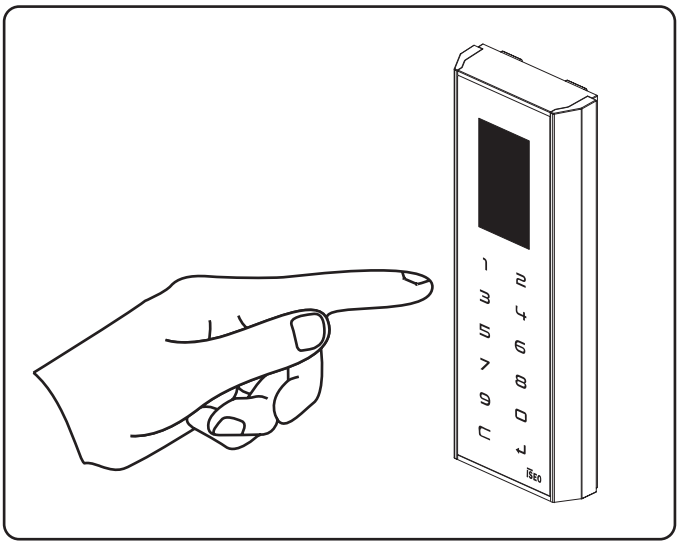
Passage mode with PIN code

x1R SMART

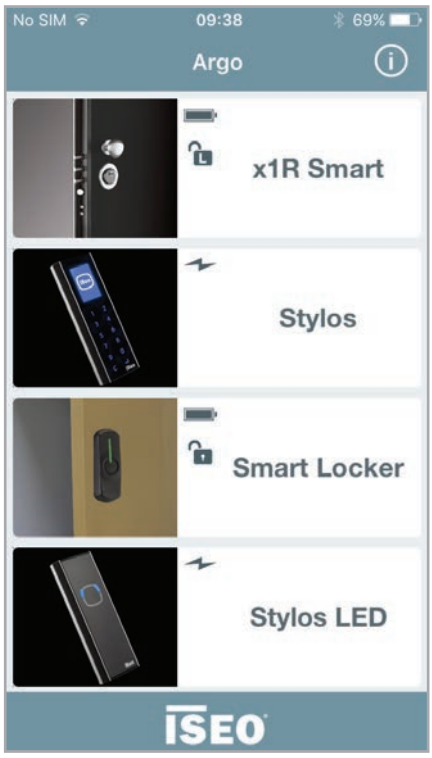


Enter the PIN code with *Passage Mode* enabled, and confirm by enter # .

STYLOS SMART DISPLAY



Enter the PIN code with *Passage Mode* enabled, and confirm by enter ↵.



Example with x1R Smart

x1R Smart is now in *Passage Mode* (Light).

When you enter the PIN code with *Passage Mode* enabled, the door first opens and then automatically set the *Passage Mode*.

When you enter again the PIN code with *Passage Mode* enabled, the door closes going automatically out from the *Passage Mode* function.

The PIN code with *Passage Mode* enabled can only be used to enable and disable the *Passage Mode* function (toggle mode).

On x1R Smart *Passage Mode* can be Light or Free as configured by Argo.

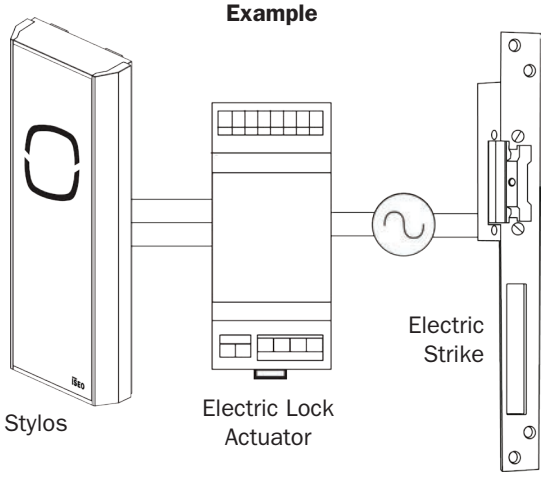
Advanced

Passage mode capability

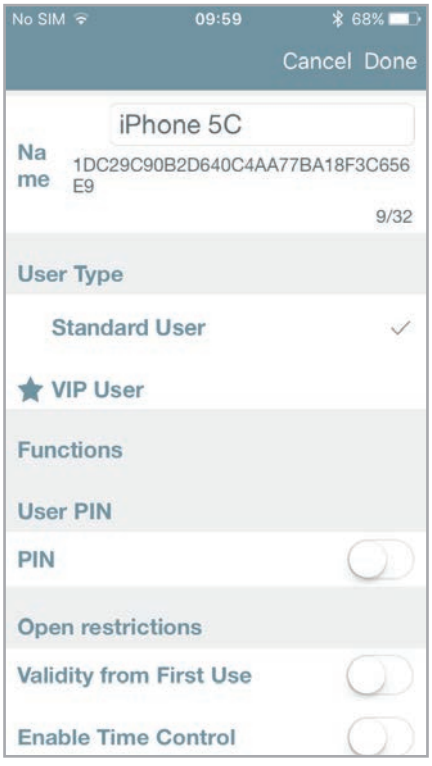
The *Passage Mode* function, once enabled, keeps the doorlock in a constant “opening condition”. You can set it by phone or card (see *Enable passage mode* and *Enable passage mode without Argo* paragraphs), and now with PIN code is even easier.

But with Stylos this condition could be dangerous for the electrical device the Stylos may drive.

Example



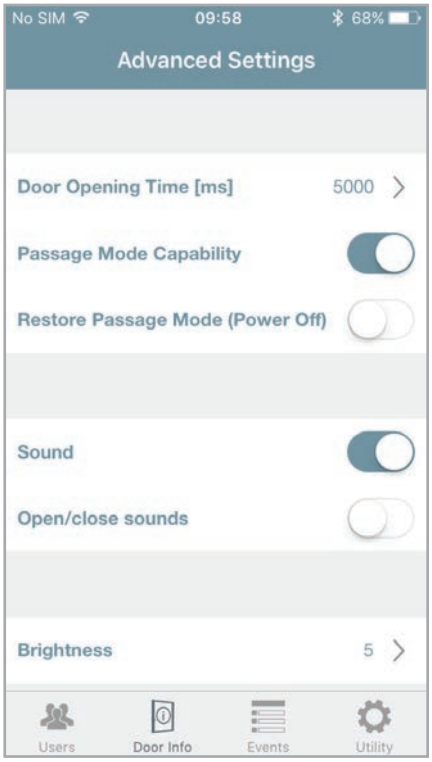
The *Stylos* infact, by the *Electric Lock Actuator,* it often drives an appliance with a coil (i.e electric locks, electric strikes...), that could not stand to be in a constant opening condition (coil always excited could burn). That’s why the *Passage Mode* function in the Stylos is disabled by default. However the Administrator, knowing the application, can freely enable it by the Argo app.



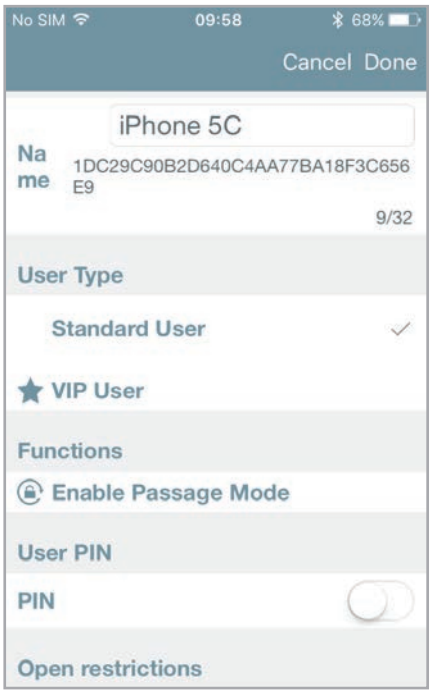
In the Stylos the *Passage Mode* function for Phones, Cards and PINs is not displayed, since *Passage Mode* capability is not enabled by default.

Passage mode capability

To enable the *Passage Mode* capability on Stylos follow the next procedure: open the Argo app, enter *Programming Mode*, touch *Door Info* menu and then *Advanced Settings*.



Enable **Passage Mode Capability** then touch done

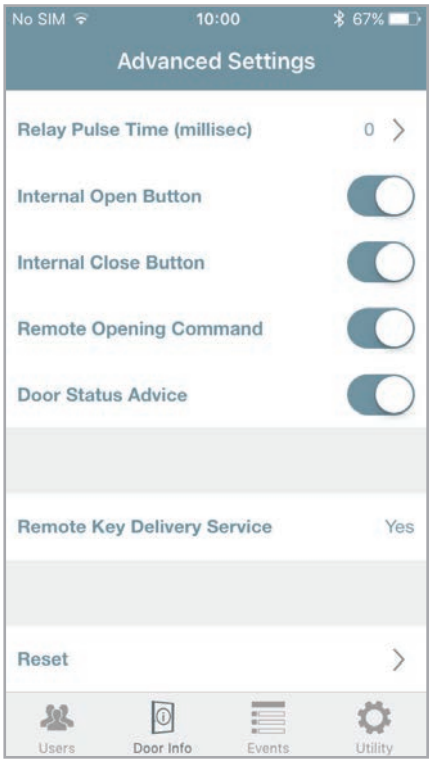


Now *Passage Mode* function for Phones, Cards and PINs is displayed and can be set accordingly.

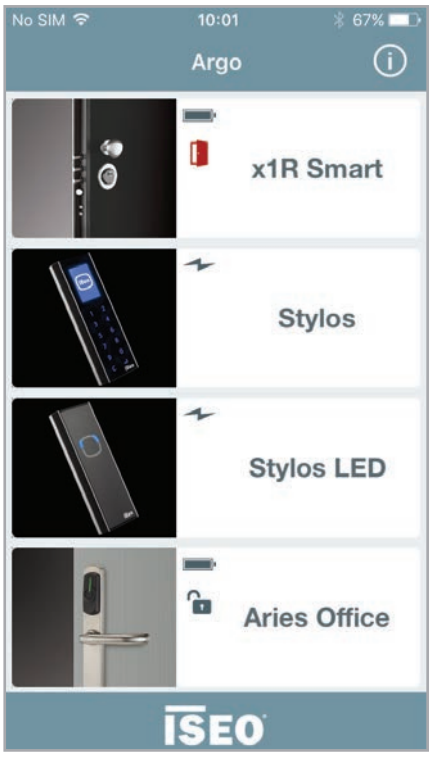
Advanced

Door status advice

The *Doors Status Advice* allows to see directly by Argo, in the door name button, when the door is left open. It is available in doorlocks having the door status sensor (i.e. x1R Smart). To display the *Door Status Advice* open the Argo app, enter *Programming Mode*, touch *Door Info* menu and then *Advanced Settings*.



Enable **Door Status Advice** then touch done

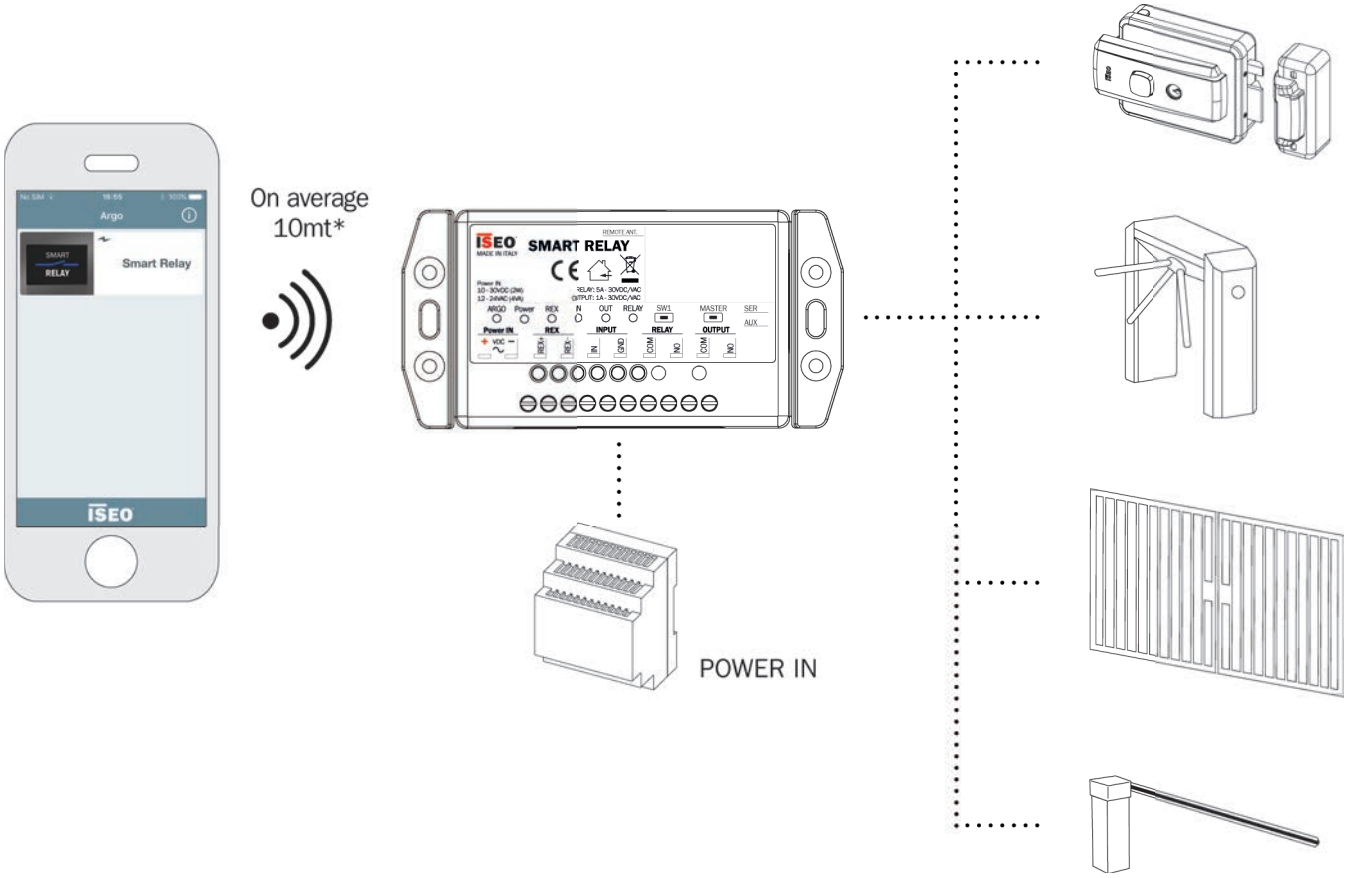


As soon as the door opens you can see a red door icon displayed in the button. When the door is closed and secure the icon disappear.

Advanced

Smart Relay

The *Smart Relay* allows to open any electrical device, like electric locks, motorized gate, bars, turnstile or in general any electrical actuator which can be activated closing a contact.

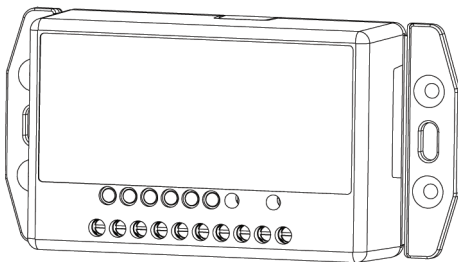


The *Smart Relay* exclusively works with smartphones by *Argo app*, since it does not have any other credential reader (i.e. RFID reader, keyboard).

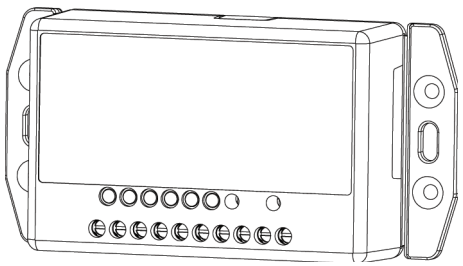
Advanced

Smart Relay

The *Smart Relay* comes in 2 different models to select upon installations requirements.

1. 

Smart Relay (with built in BLE module): the Bluetooth is embedded in the Smart Relay box.

2. 

Smart Relay with Remote BLE module: the Bluetooth module can be positioned outside, at a max distance of 3 meter from the unit.

Remote BLE module

Max cable length = 3mt

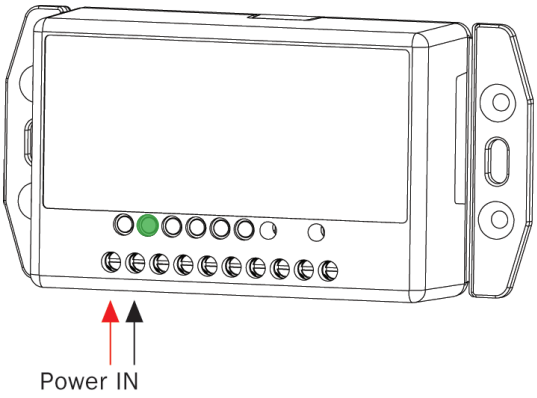
For more detailed technical information about *Smart Relay* (i.e. technical data, dimensions, installation examples), read the *Smart Relay Installation Guide* available at *app.iseo.com.*

Advanced

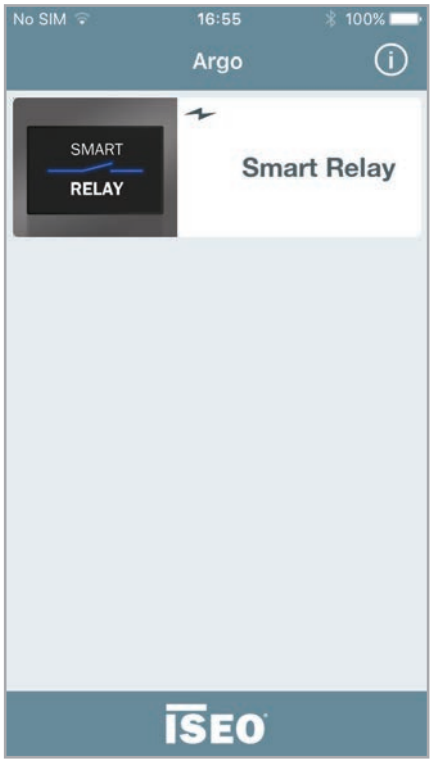
Smart Relay

To configure the *Smart Relay* at the first installation you need to enter *Programming Mode* with a smartphone by the Argo app. Since *Smart Relay* doens't have any RFID credential reader you cannot use the *Master Card,* as we usually do for all the other ISEO Smart devices. To do that you need to press a button in the *Smart Relay*, as showed in the next procedure.

First installation: enter Programming Mode to add the first smartphone



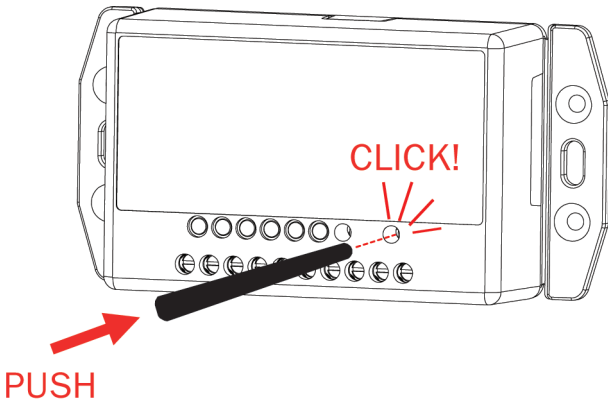
1. Power on the *Smart Relay*.
   The green LED **Power** switch ON.



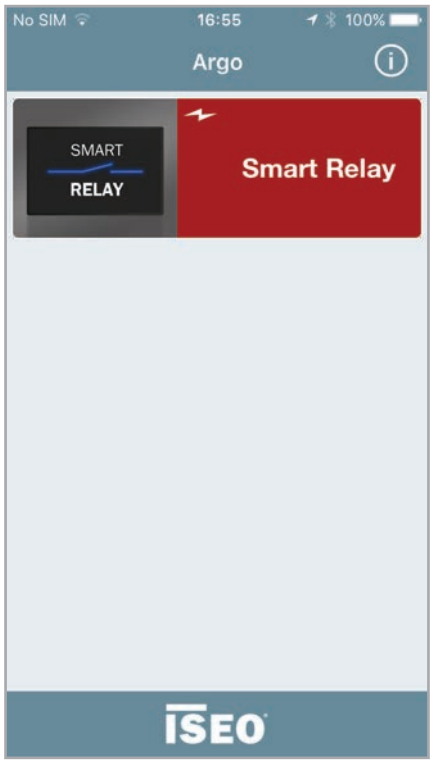
2. Open the Argo app, you will see the *Smart Relay* icon.

Advanced

Smart Relay



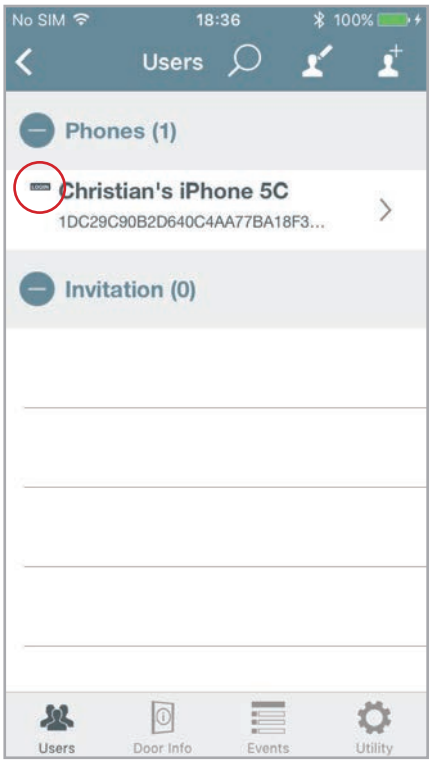
3. Push the **MASTER** button in the *Smart Relay* by the plastic pin provided in the box or by any other similar tool.



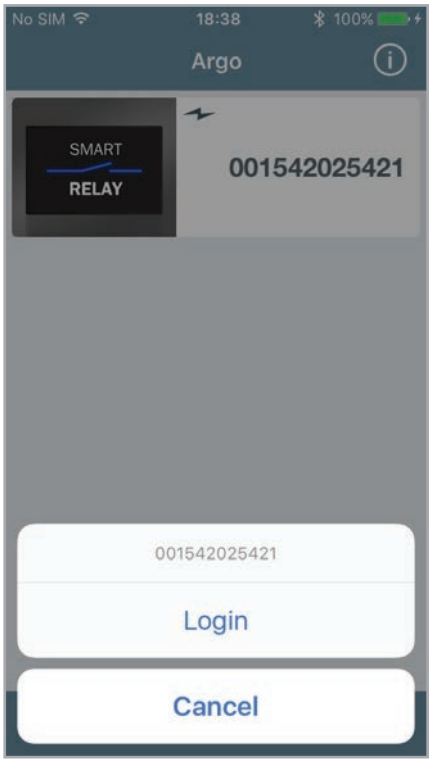
4. The button in the *Argo app* will turn red, and pressing it you will enter *Programming mode,* like we usually do presenting the *Master Card 1* to the other ISEO Smart devices.

The *Master button* is a microswitch and allows to enter *Programming Mode*. This is required to enroll the first Administrator phone when the device comes from the factory or after a factory reset (go to *Reset Doorlock to Factory Mode*).

Smart Relay



5. Add the first Administrator phone with **Login** function enabled (for more information go to *Administrator Login without Master Card*).



6. *Tap and hold* the door button: the smartphone can now login without *Master Card.*

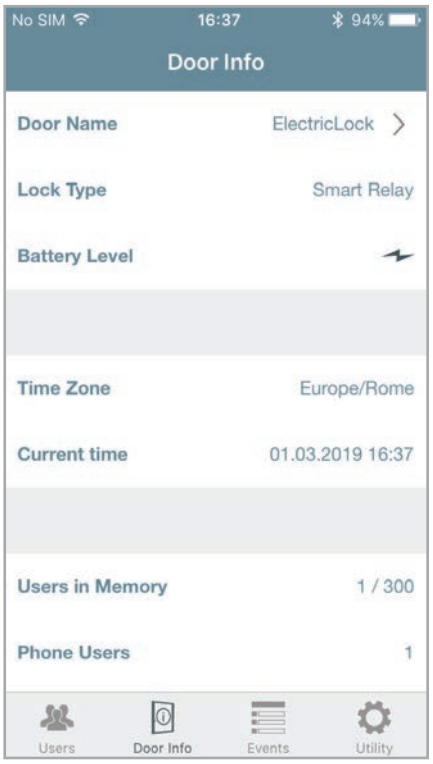
   To add other smartphones to the user list the Administrator can:

   - prepare invitations with or without login function (to know more go to *Invitations*).
   - Add smartphones with Argo UID function (to know more go to *Add phone with Argo UID*).

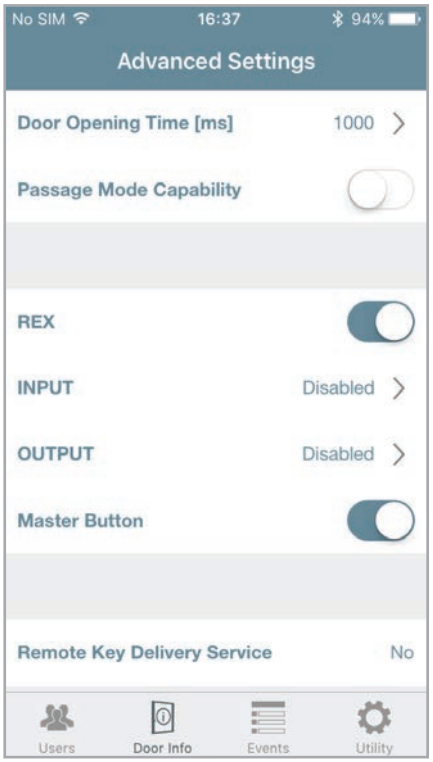
Advanced

Smart Relay

First installation: set door name and change opening time



Enter **Door Info** menu then give a real **Door Name** (for more information go to *Door Name* paragraph).

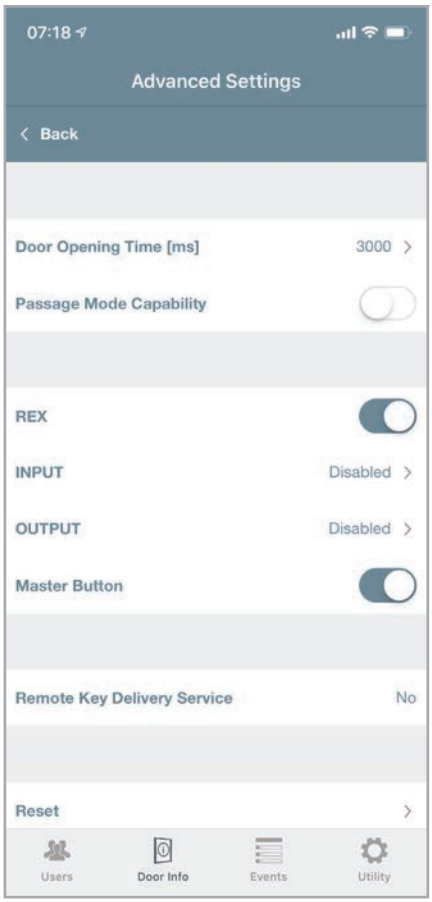


Enter **Advanced Settings** menu, then change the **Door Opening Time** according to the electrical device connected to *Smart Relay* requirements (for more information about *Door Opening Time* go to *Advanced Setting)*.

Advanced

Smart Relay

Advanced menu



Enable **Passage Mode Capability** if the electrical device connected to *Smart Relay* can stand constant opening condition (for more information go to *Passage mode capability* paragraph).

Disable **REX** = *REquest to Exit* input (also called remote opening command).

You can configure **INPUT** and **OUTPUT** if connected. To know more about those functions go to the related paragraph.

You can disable the **Master Button** in the *Smart Relay* for security reasons. In this way if someone physically push the button in the Smart Relay, to enter *Programming Mode*, it won't have any effect (the button in the *Argo app* won't turn red).

If the *Administrator* disables the *Master Button* it is strongly recommended to create before some *Invitations*, sending the invitation codes to themself, in order to keep it as "spare/emergency invitations", to be used in case of needs (i.e. the phone with login function get lost or broken).

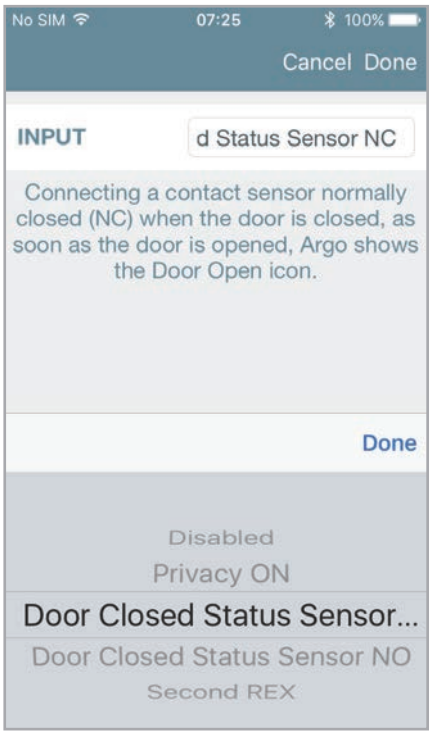
If *Master Button* has been disabled and no users have the login function or no pending invitations have been created, and the administrator's phone has broken or stolen, you won't be able to enter *Programming Mode* anymore. To recover this situation you need to perform an hardware device factory reset that will bring the *Smart Relay* to the original factory setting, with the *Master Button* enabled by default. To do this emergency procedure please contact your local *IseoZero1 Technical Support.*

Advanced

Smart Relay

INPUT configurations

INPUT (clean contact) can be configured by *Argo* in different ways, to program the *Smart Relay* with different functionality to satisfy various solutions.



Enter **Advanced Settings** menu then touch **INPUT**. Scroll the list below and choose the desired setting. A brief decription on Argo explains each setting feature.

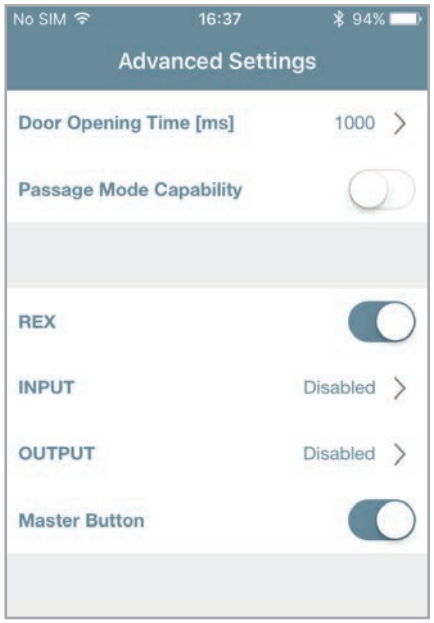
In the next table are shown the INPUT possible configurations and related descriptions.

INPUT	Description EN
Disabled	
Privacy ON	Connecting a switch, when pressed (closed contact), Argo shows the moon Privacy icon.
Door Closed Status Sensor NC	Connecting a contact sensor normally closed (NC) when the door is closed, as soon as the door is opened, Argo shows the Door Open icon.
Door Closed Status Sensor NO	Connecting a contact sensor normally open (NO) when the door is closed, as soon as the door is opened, Argo shows the Door Open icon.
Second REX	Connecting a push button it can be used as a second Request to Exit command (REX). Connecting a switch, when closed, it is possible to enable the Passage Mode function.

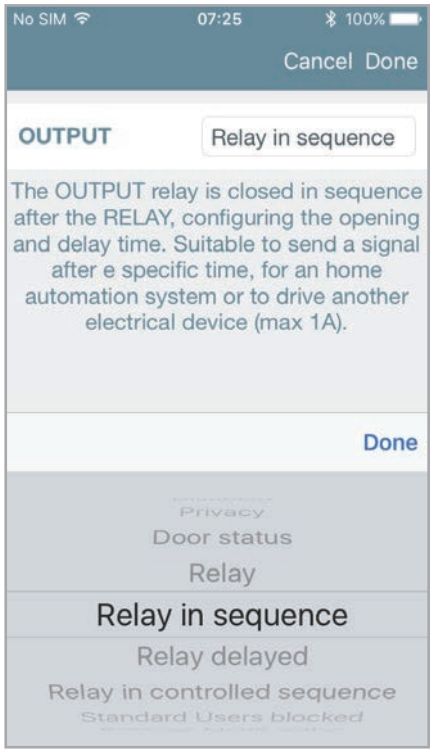
Smart Relay

OUTPUT configurations

OUTPUT (signal relay 1A), can be configured by *Argo* in different ways, to program the *Smart Relay* with different functionality to satisfy various solutions.



Enter **Advanced Settings** menu then touch **OUTPUT**.



Scroll the list below and choose the desired setting. A brief decription on Argo explains each setting feature.

Advanced

Smart Relay

In the next table are shown the OUTPUT possible configurations and related descriptions.

OUTPUT	Description
Disabled	
Privacy	Setting the INPUT in Privacy ON, the OUTPUT relay activates at the privacy enabling.
Door Status	Setting the INPUT in Door Closed Status Sensor NC or NO, the OUTPUT relay activates when the door is open.
Relay *	The OUTPUT relay replicates the RELAY behaviour. Suitable for an home automation system or to drive another electrical device (max 1A).
Relay in sequence *	The OUTPUT relay is closed in sequence after the RELAY, configuring the opening and delay time. Suitable to send a signal after e specific time, for an home automation system or to drive another electrical device (max 1A).
Relay delayed *	The OUTPUT relay replicates the RELAY behaviour adding a configureable delay and opening time. Suitable for example to drive a courtesy light.
Relay in controlled sequence *	The OUTPUT relay is closed in sequence after the RELAY, configuring the opening and delay time, only if the INPUT Door Closed Status Sensor NC or NO activates. Suitable for example to drive an automatic swing door operator.
Standard Users blocked	Enabling the Block Standard User function on Argo, the OUTPUT relay closes. Useful to show for example by an external light, this condition to end users.
Passage Mode active	Enabling the Passage Mode function on Argo, the OUTPUT relay closes. Useful to show for example by an external light, this condition to end users.
Lithium Battery low	The OUTPUT relay closes when the lithium internal battery, used to power the Smart Relay clock in the absence of mains, drops under 2,8Vdc. OUTPUT relay can be connected for example to a buzzer or to a red light, to show this battery low status.
Alarm for Power Supply LOW	The OUTPUT relay closes when the main power supply voltage, drops under 6,8Vdc. OUTPUT relay can be connected for example to a buzzer or a red light to show this status.

* See a graphic explanation of the relay configurations in the next pages.

Advanced

Smart Relay

OUTPUT relay graphic explanation

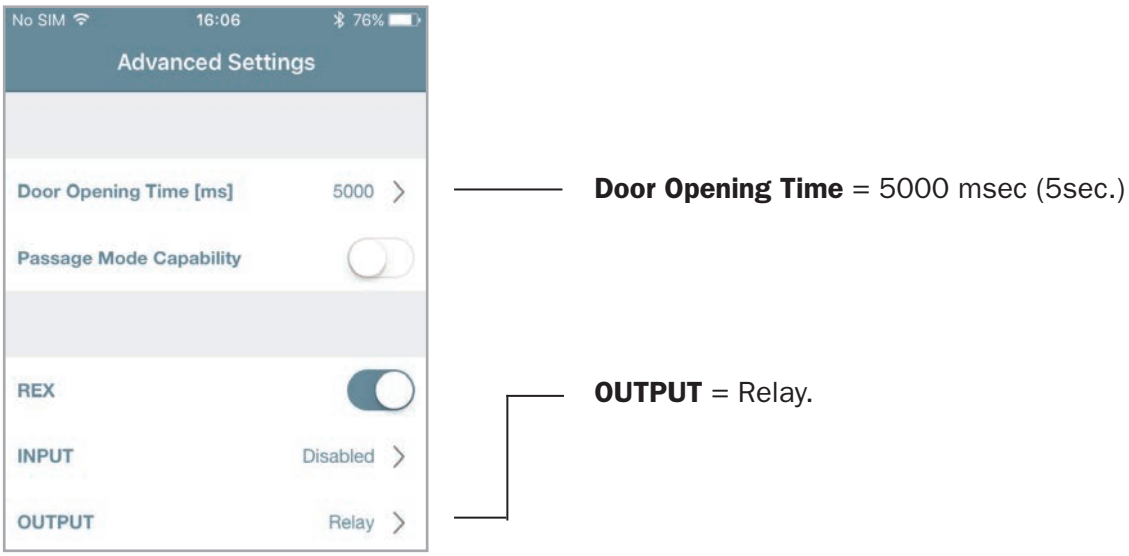
OUTPUT relay configuration can be one of the follows:

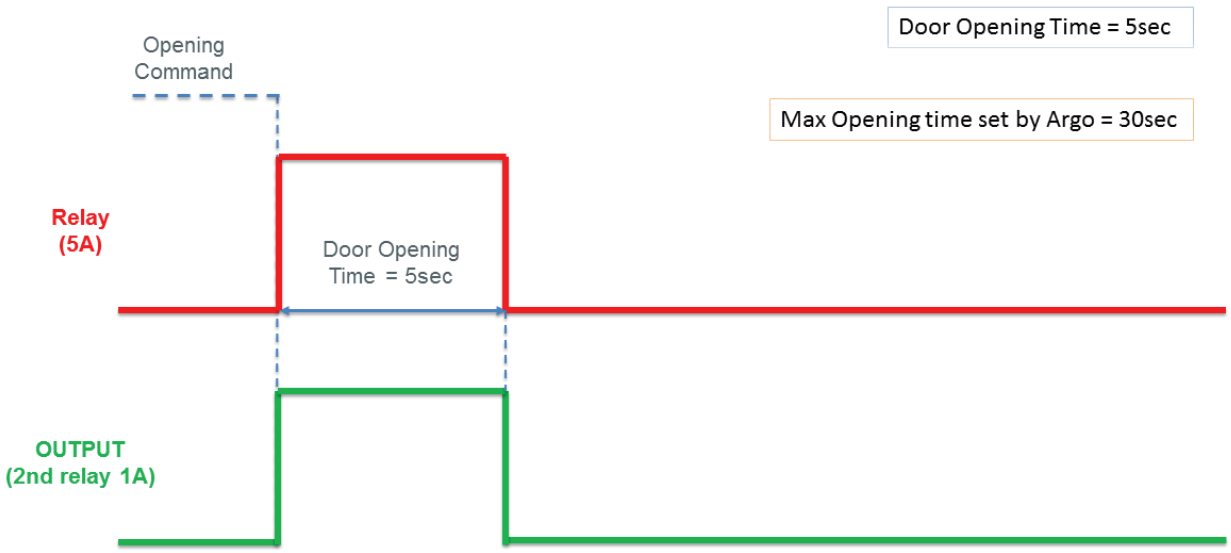
- Relay
- Relay in sequence
- Relay delayed
- Relay in controlled sequence.

See below a detailed and graphic explanation of each of these configrations.

Relay

This setting allows the OUTPUT signal relay to replicates the power RELAY. It could be used for example to drive another device or as an input for an home automation system.



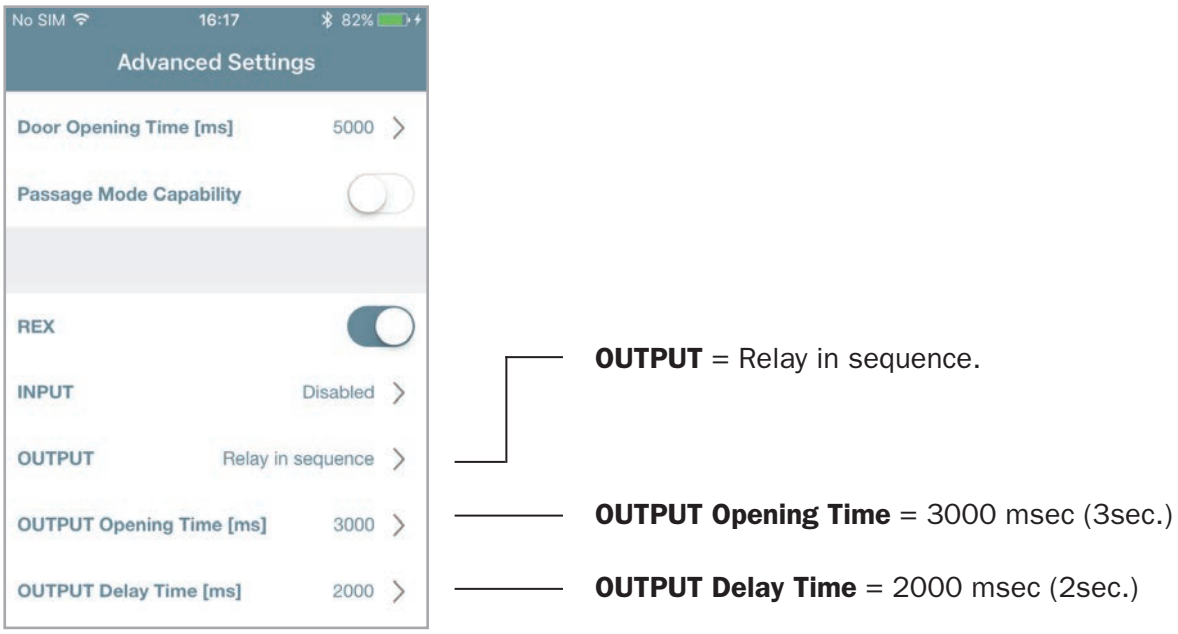


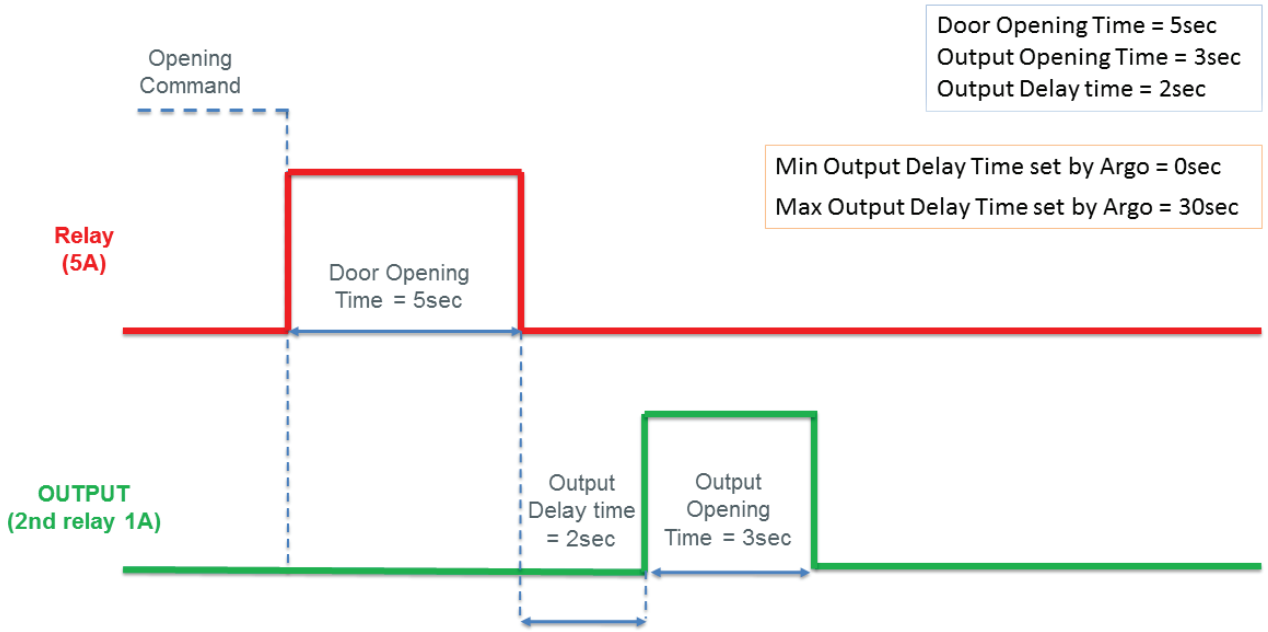
Advanced

Smart Relay

Relay in sequence

This setting activates the OUTPUT relay after the power RELAY, in a configureable sequence, configuring by Argo the *Output Opening Time* and the *Output Delay Time*. Use case scenario: to send a signal after a specific time to an home automation system or to drive another device.



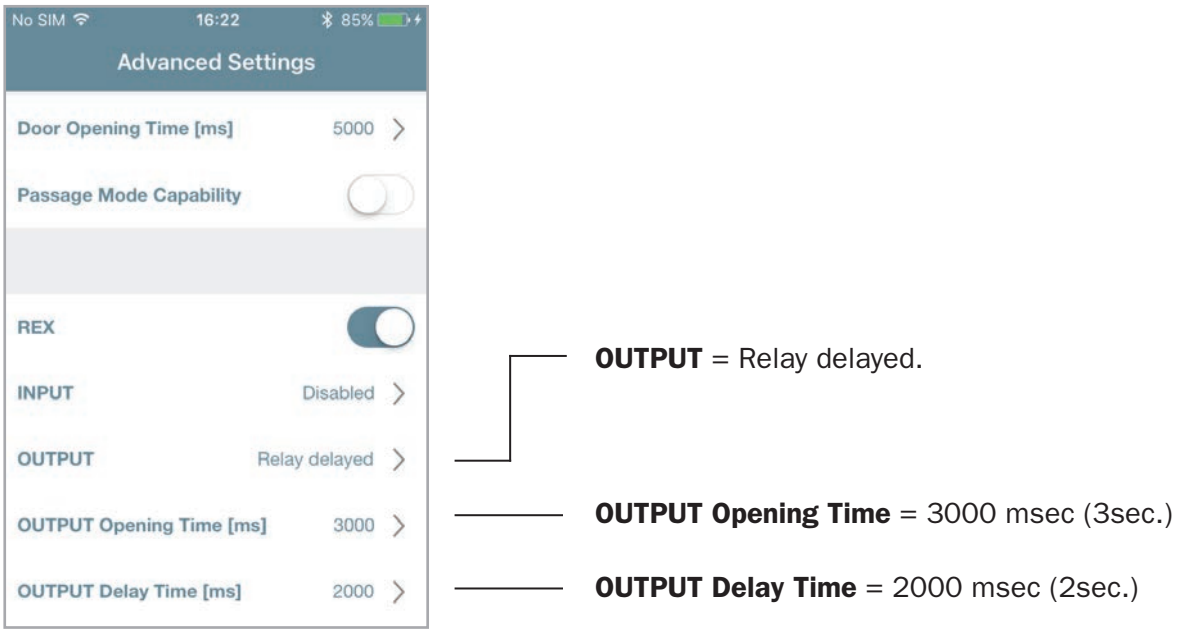


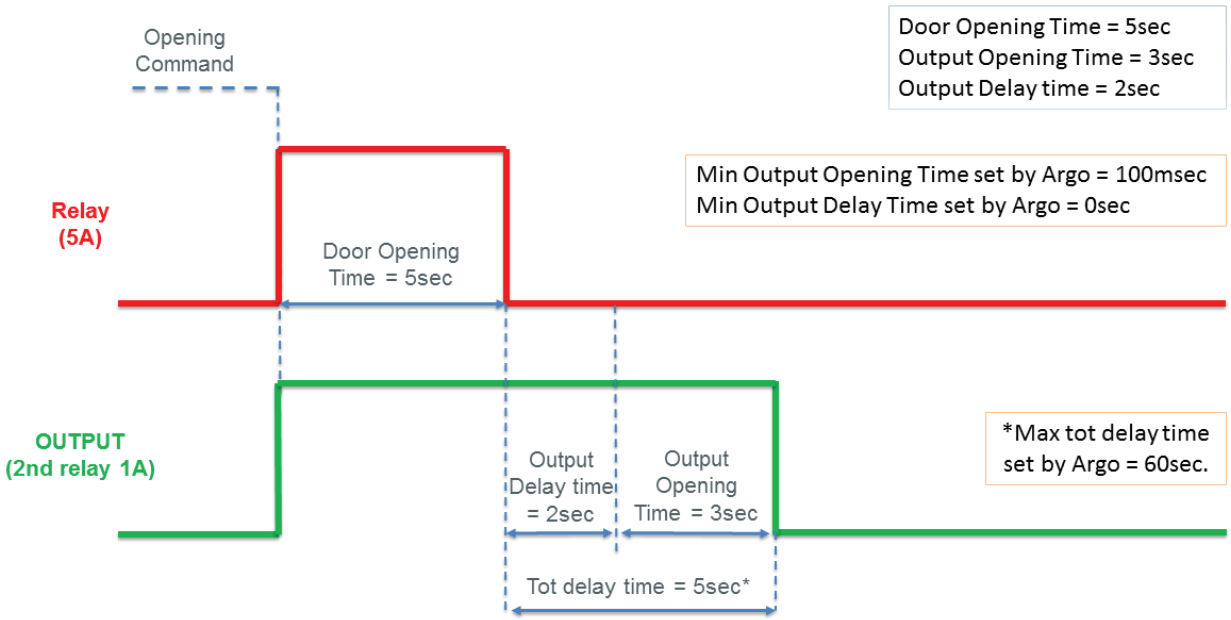
Advanced

Smart Relay

Relay delayed

This setting allows the OUTPUT relay to replicates the power RELAY, adding a configureable delay by the parameters: *Output Opening Time* and the *Output Delay Time*. Use case scenario: to switch on a courtesy light when the door opens, and to keep it on for a specific time.





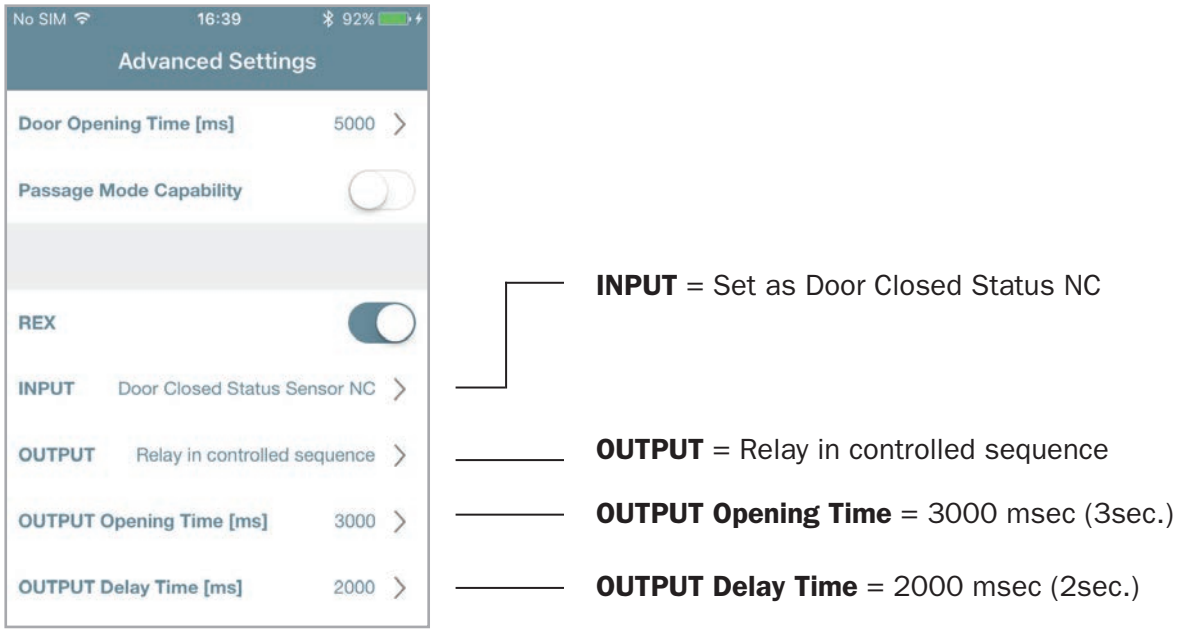
The total delay time is given by the the sum of the *Output Opening Time* and the *Output Delay Time*. Note that the maximum delay time is 60sec since the max opening time and the max delay time set by Argo can be 30sec.

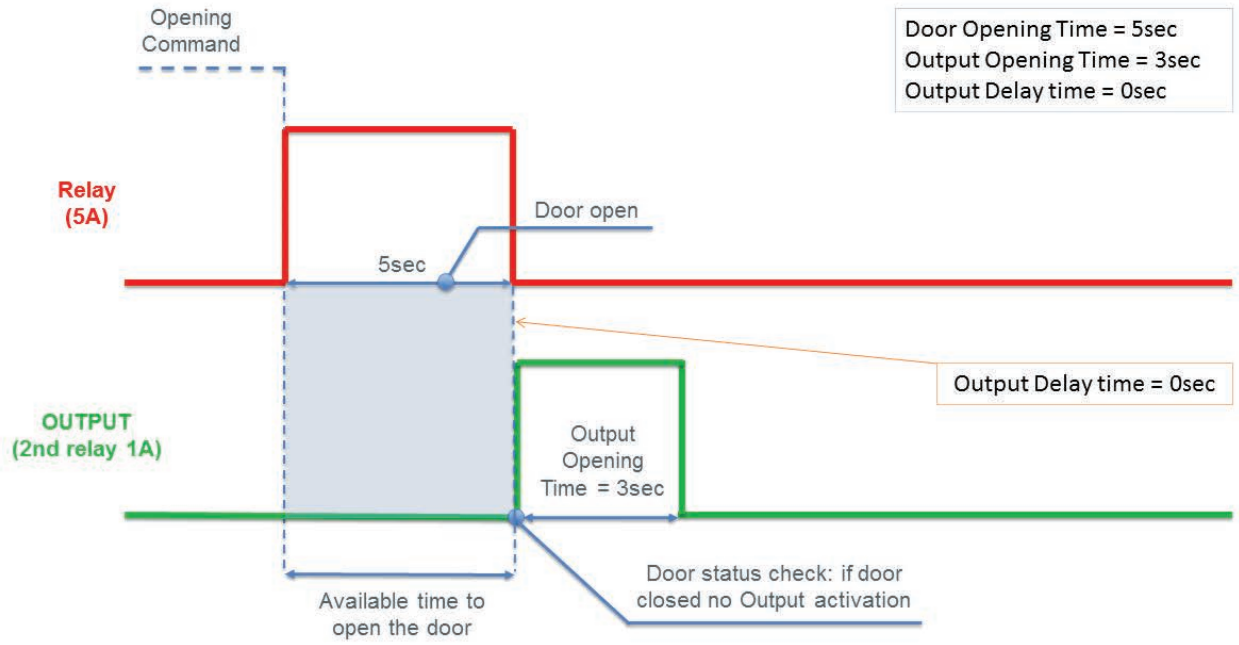
Advanced

Smart Relay

Relay in controlled sequence

This setting activates the OUTPUT relay after the power RELAY, in a configureable sequence, ONLY if the INPUT, previosuly set as *Door Closed Status Sensor* (NC or NO), changes during the *Door Opening Time* plus the *Output Delay Time*. Use case scenario: too start an automatic swing door operator ONLY if the electric lock inside the door is unlocked. The electric lock in this example needs to provide the door status signal as INPUT for the *Smart Relay*.





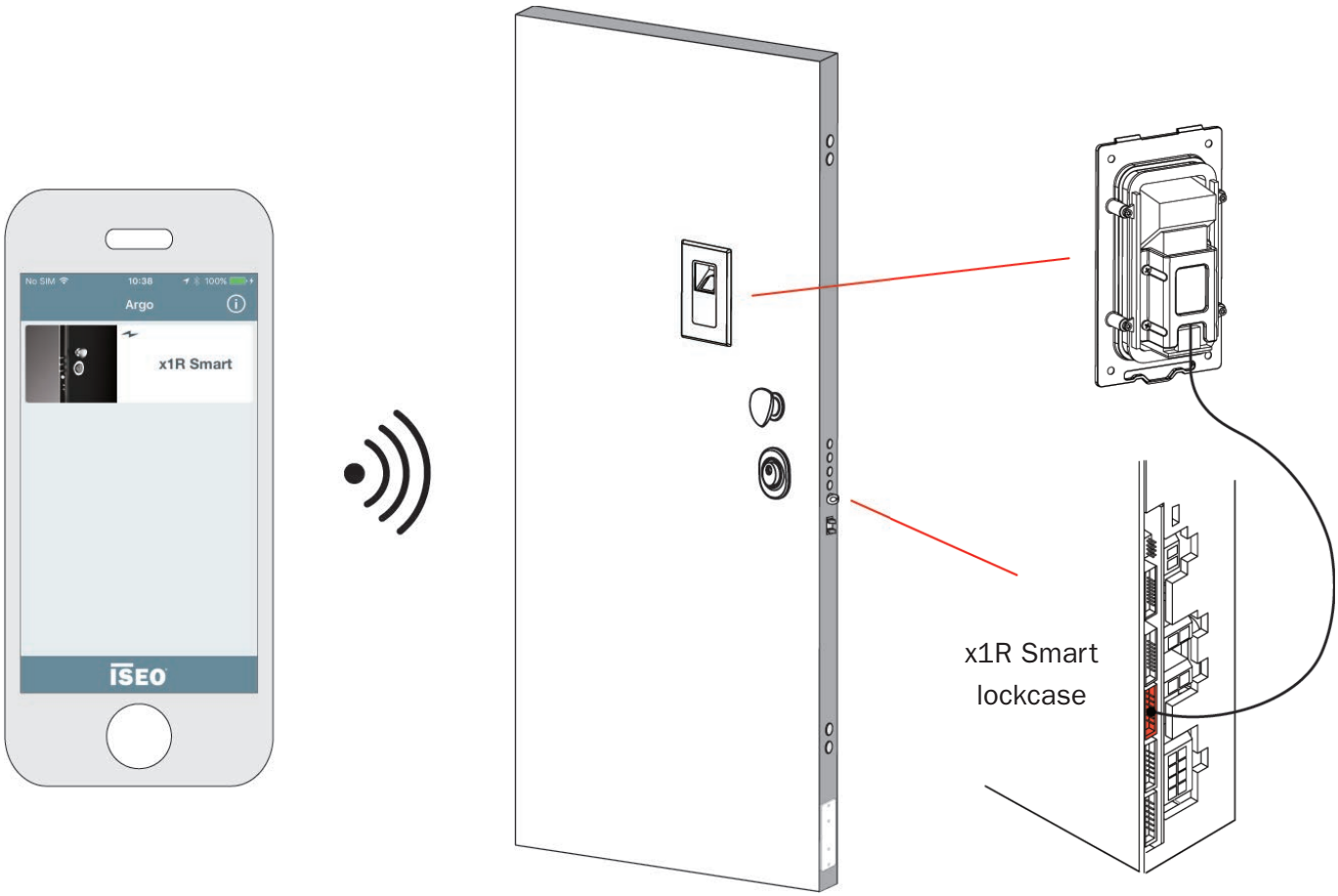
If the door is not opened during the available time (door status signal doesn't change), the OUTUPT relay will not activate.

Advanced

Fingerprint reader

Argo app fully integrates the fingerprint biometric authentication with *x1R Smart*. By Argo you can add users' fingerprints, manage the user list and even upgrade the fingerprint reader software. The unique features are:

- Directly connected to *x1R Smart* electronic board.
- Fully integrated with *Argo app*.
- Battery operated.
- Software upgrade by *Argo app*.



The *Fingerprint reader* exclusively works with *x1R Smart*.
The *Fingerprint reader* module does not have *Bluetooth* inside, so it always requires in addition the *External Control Module* (RFID Reader, Keypad RFID Reader, Hidden RFID Reader).

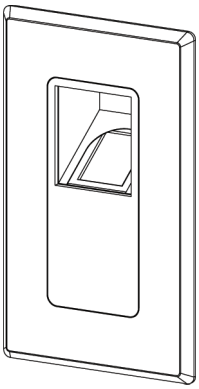
Advanced

Fingerprint reader

The *Fingerprint reader* is available in 2 different models to select upon installations requirements:

- EMBEDDED READER
- SURFACE MOUNTED READER

1.



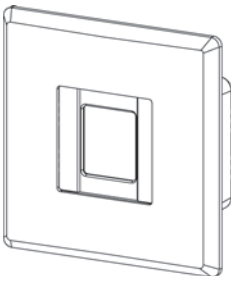
FLUSH

PROTRUDING

EMBEDDED READER

The *x1R Smart* embedded reader has the optical reader placed at 45° allowing a very convenient user experience. The embedded reader is available in two different models allowing the following mounting options: FLUSH and PROTRUDING.

2.



SURFACE MOUNTED READER

SURFACE MOUNTED READER

The surface mounted reader is applied on the door surface with minimal insertion on the outside door panel without impact on the door structure.

For *Fingerprint reader* dimensions, installation examples and electrical connection, read the *x1R Smart Finger Reader Installation Guide*, available at *app.iseo.com.*

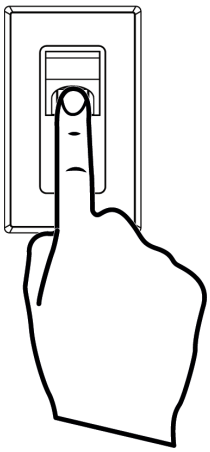
For technical information about fingerprint technology, biometric template and identification process and for the commercial literatures, read the *Fingerprint* brochure, available at *iseo.com*.

Advanced

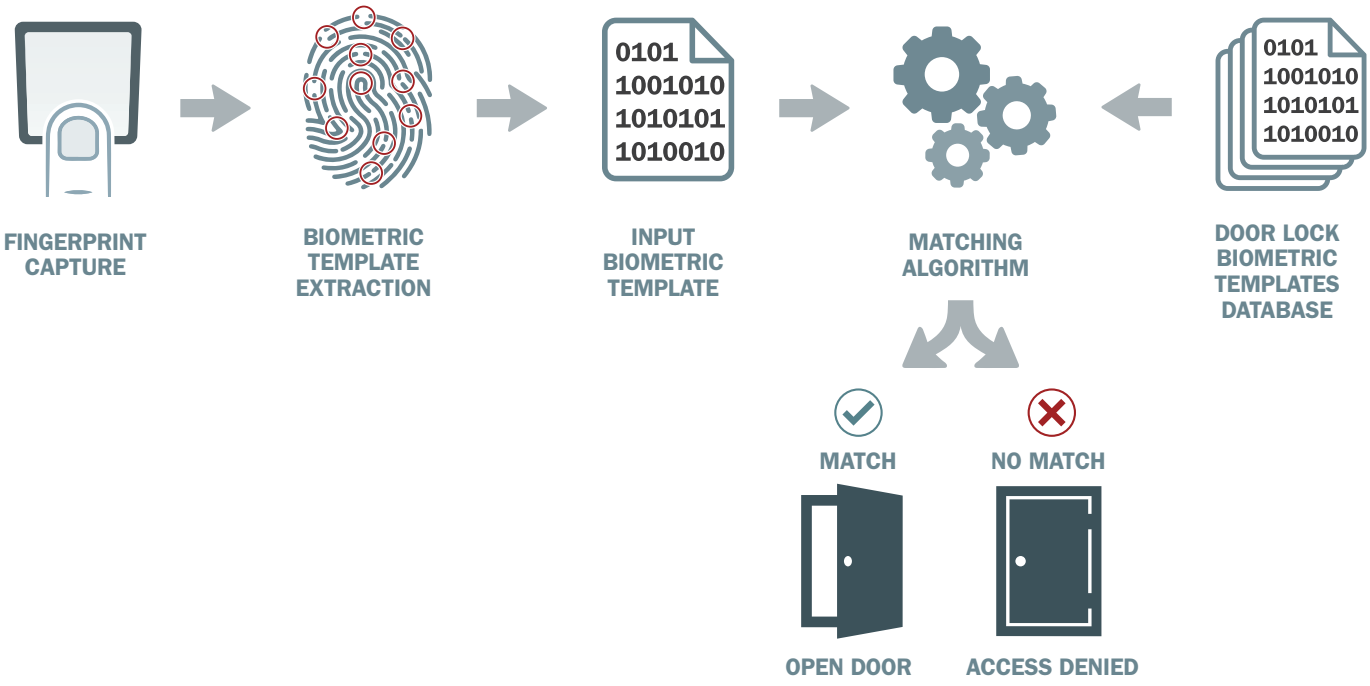
Fingerprint reader

Principle of working

When the user place his finger in the reader, to open the x1R Smart, a matching algorithm compares the user's biometric template*, extracted from the captured image, with all the templates previously stored in the door lock's user list, identifying the right one.
The entire matching process takes less than 1 second.



*The biometric template is a digital reference stored in the door lock memory, created from the minutiae map. It is used for future comparison with other biometric templates of fingerprints presented at the reader.
To know more about biometric template and minutiae map, read the *Fingerprint* brochure, available at *iseo.com*.

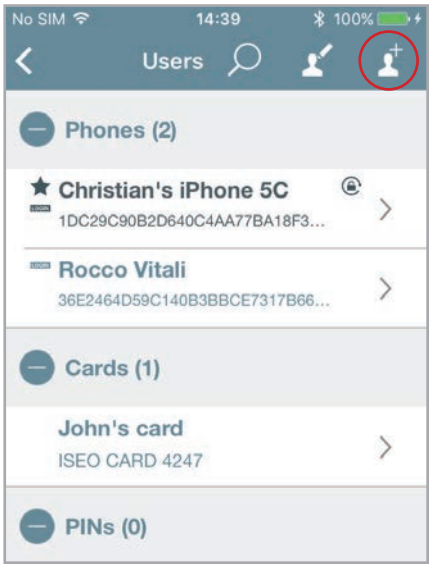


During the entire fingerprint identification process no fingerprint images are stored on the door lock, and a fingerprint image cannot be recreated from the biometric template.

Fingerprint reader

Add fingerprint users

To add a fingerprint open the *Argo app*, enter *Programming Mode* and follow the next steps.



1. Touch add user icon.

2. Touch **Fingerprint**.

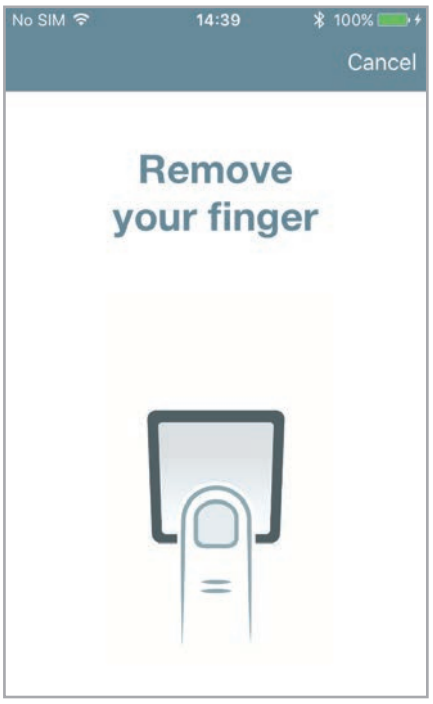
Advanced

Fingerprint reader

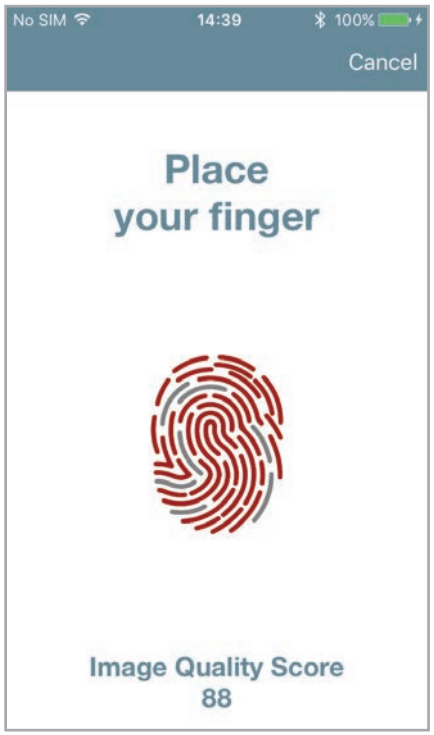
3. Follow the instruction on the phone display that guides you through the correct enrolling process.

1

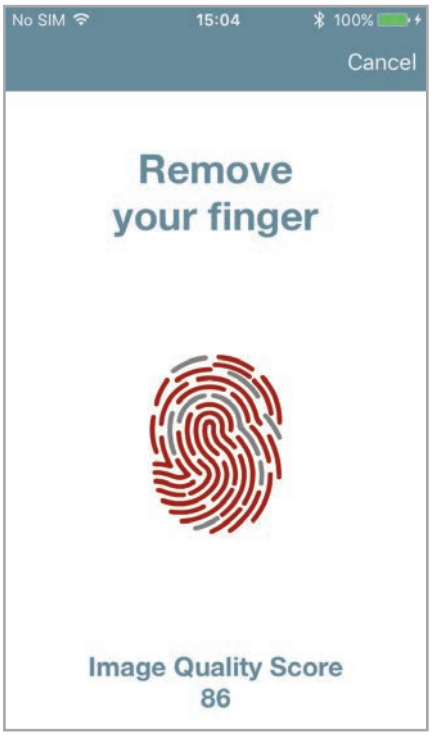
2



3



4



To know more about *Image Quality Score* go to the related paragraph.

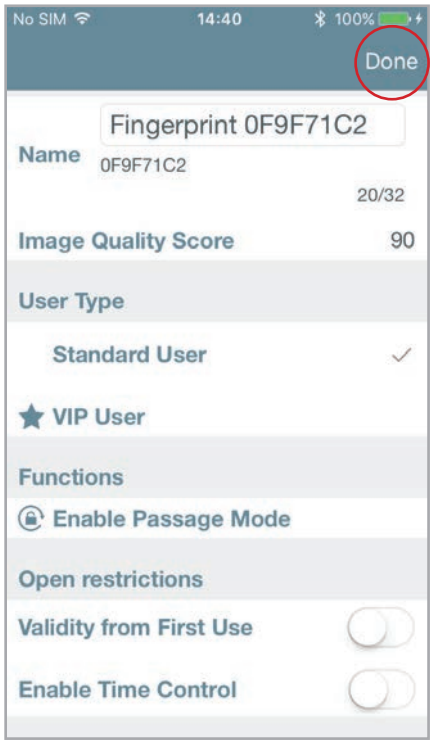
Advanced

Fingerprint reader

4. Continue with the enrollment process until you get the next message:

5. The fingerprint enrolling process has ended.

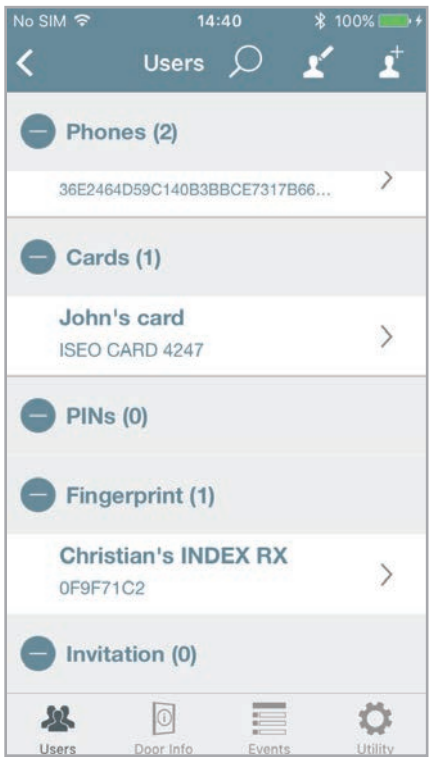
6. Touch **OK**



7. Write the fingerprint **Name**, set additional functions if required (VIP User, Open restrictions), then touch **Done**.

This is the best **Image Quality Score** obtained from the entire enroll process. It is permanently assigned to the user biometric template and it is the reference for the subsequent user's identification process. Higher is the value, better will be the fingerprint reading (lower reading errors). To know more about quality score go to *Image quality score* paragrapgh.

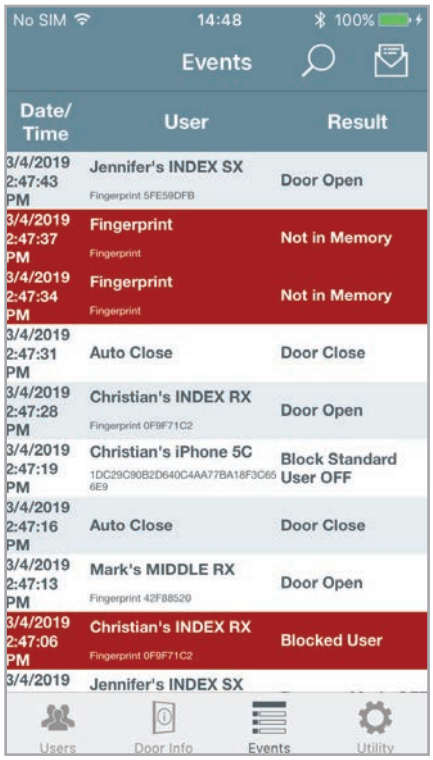
Fingerprint reader



8. The fingerprint is now added to the *User List* and can be used to open the door.

Fingerprints events

In the **Events** list we can see all the user's fingerprints transaction: both authorized and denied events.



Not in Memory events can be caused by:

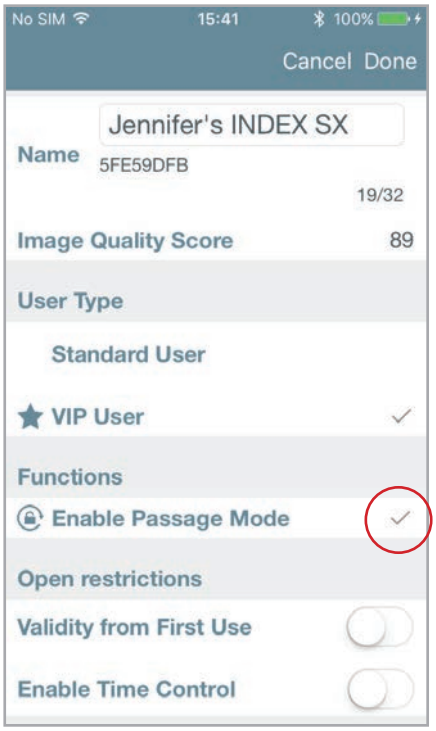
- finger not present in the *User List*.
- Finger not correctly identified (reading errror).

Advanced

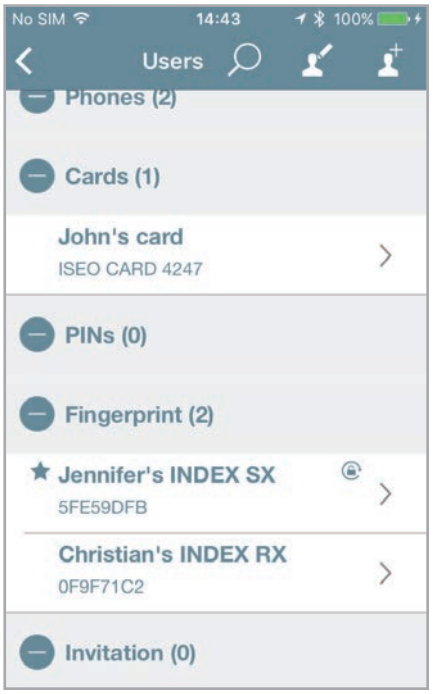
Fingerprint reader

Passage mode with fingerprint

Enabling the *Passage Mode* function to a fingerprint user, it will work like the *PIN code* (for more information go to *Passage mode with PIN code*): the fingerprint user, at every access to the door, will open and at the same time will enable and disable the *Passage Mode* in the door.



Touch **Enable Passage Mode**.



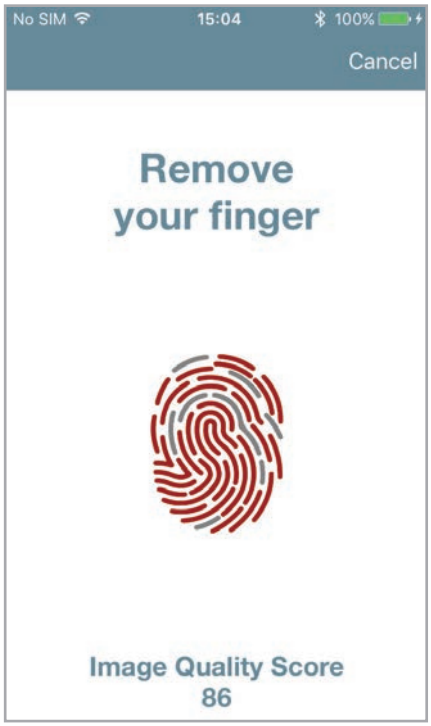
The user has now *Passage Mode* capability and will automatically enable and disable the *Passage Mode* in the door lock every time the finger is presented.

Advanced

Fingerprint reader

Image quality score

This parameter is the quality of the image of the *biometric template*, that will be the reference in the subsequent user's identification process. That means a good image quality score will generate a better reference biometric template, therefore a better reading identification capability. In simple words the better is the quality the easier is the indentification. That's why the enrolling process (which is done only once), is fundamental for a good functioning of the reader. The purpose of showing this parameter during the enrolling process, is to help the user improving the image quality, by putting the finger the best he can in the reader, in order to obtain the best score. For this reason the image, during the whole enrolling process, is captured several times (for more info go to *Finger enroll accuracy*).



Try to obtain an high **Image Quality Score** correctly positioning the finger during the entire enrolling process.

The *Image Quality Score* value range is from 50 to 100%. Scores < 50 are automatically discarded (no fingeprint images saved).

Exmples of *Image quality score*:

No quality score (< 50)

Poor quality score

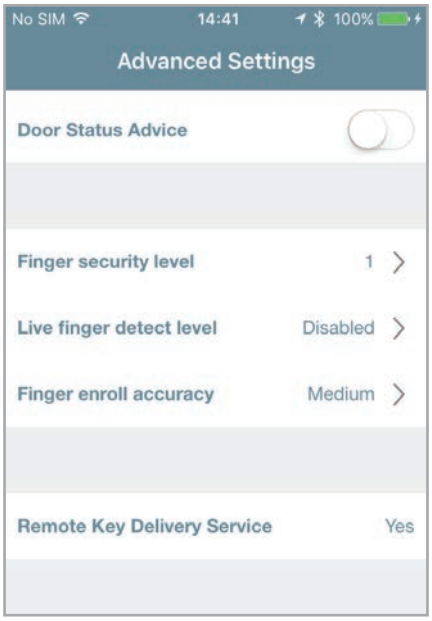
Good quality score

Fingerprint reader

Advanced setting

In the Argo *Advanced Settings* we have 3 new menu related to the fingerprint reader:

- Finger security level
- Live finger detect level
- Finger enroll accuracy



Fingerprint reader advanced settings.

Fingerprint security level

Defines FAR (False Acceptance Rate) and FRR (False Rejection Rate) values. A higher level of security means a more restrictive fingerprint control in the reading phase.

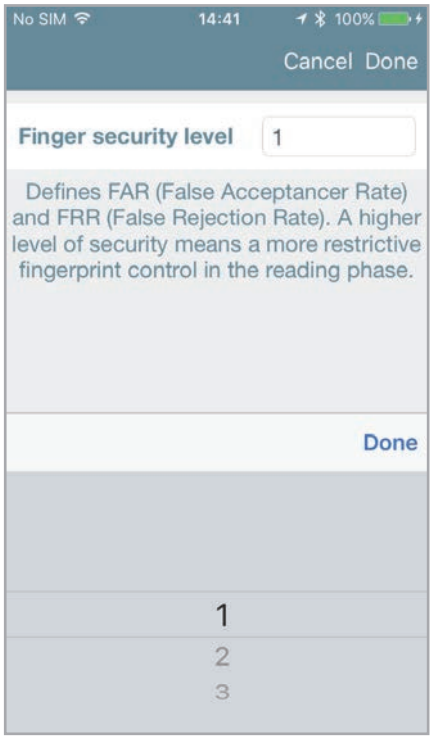
- **FALSE ACCEPTANCE RATE**
  The FAR (False Acceptance Rate) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. In simple words, it's the number of times people get identified when they should not be identified and consequently authorized to open the door.

- **FALSE REJECTION RATE**
  The FRR (False Rejection Rate) is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. In simple words, it's the number of times people do not get identified when they should be identified and authorized to open the door.

Advanced

Fingerprint reader

Fingerprint security level



By default the *Finger security level* is set at level **1**.

Select the desired security level, scrolling through the values according to your needs and following the table below.

SECURITY LEVEL	**FAR** (False Acceptance Rate)	**FRR** (False Rejection Rate)
1	1 OUT OF 200.000	1 OUT OF 10.000
2	1 OUT OF 1.000.000	1 OUT OF 6.000
3	1 OUT OF 10.000.000	1 OUT OF 4.000

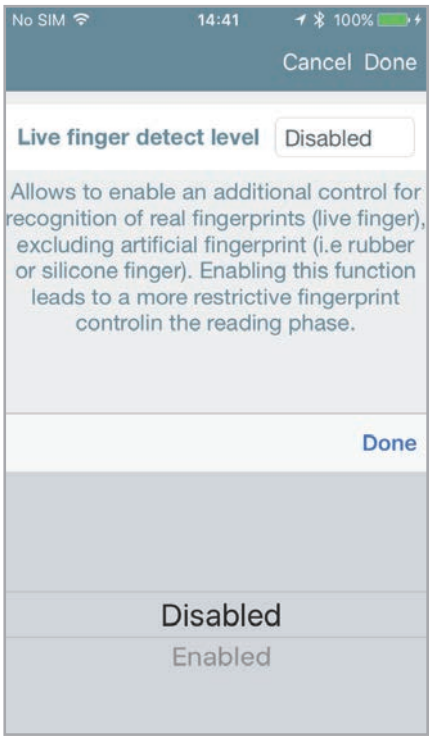
Higher is the security level the more secure is the access control, but at the same time it will be less convenient to use, because users will be more easily falsely rejected by the system. In other words users could not get identified during access because not recognized from the reader, even if present in the user list. This especially happens in case of users with low *Image Quality Score*, that's why a high score is always reccomended to improve the fingerprint reading capability.

Advanced

Fingerprint reader

Live finger detect level

Allows to enable an additional control for recognition of real fingerprints (live finger), excluding artificial fingerprint (i.e rubber or silicone finger). Enabling this function leads to a more restrictive fingerprint control in the reading phase.



By default the *Live finger detect level* is **Disabled**.

A fake fingerprint is an artificial fingerprint made from silicone, rubber, paper, gel, or film. It is used to defeat common biometric readers. The optical fingerprint sensor detects both LIVE and FAKE finger using a combination of a human capacitance sensor and infrared light reflection technology.

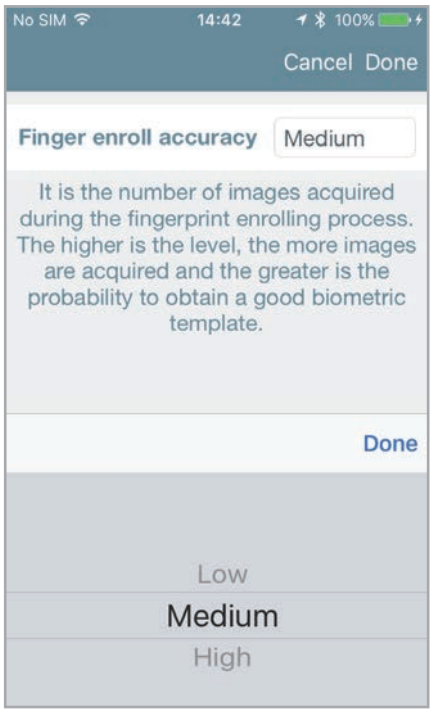
Enabling the *Live finger detect level* more secure will be the access control system but, at the same time, increases the probability to exclude correct fingerprints. Users therefore could not get identified during access, because not correctly recognized from the reader. This especially could happen in case of users with low *Image Quality Score*, that's why a high score is always reccomended to increase the fingerprint reading capability.

Advanced

Fingerprint reader

Finger enroll accuracy

It is the number of images acquired during the fingerprint enrolling process. The higher is the level, the more images are acquired and the greater is the probability to obtain a good biometric template.



By default the *Finger enroll accuracy* is set to **Medium** level. That means a maximum of 20 fingerprints reading can be requested to the user during the enrolling process.

The fingerprint registration process is the most important part of the correct biometric template creation and subsequent fingerprint identification. The best enroll accuracy is important for a good fingerprint reader operation.

See below the minimum and the maximum number of fingerprints reading requested to the user, depending on the *Finger enroll accuracy* level set.

- Low = the acquired images vary from 4 to 10.
- Medium = the acquired images vary from 10 to 20
- High = the acquired images vary from 16 to 40

During the enrolling process a sophisticated algorithm determines when to stop the images acquisition, if a good *Image Quality Score* is reached. That's why the actual number of readings requested to the user can change: higher is the quality score, shorter will be the enrolling process.

Advanced

Fingerprint reader

INFORMATION ABOUT BIOMETRIC AUTHENTICATION

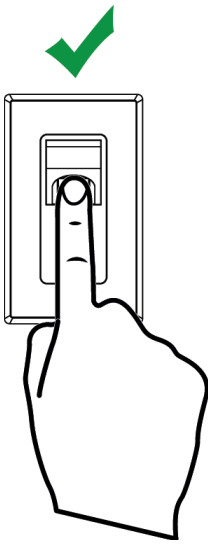
- The fingerprint registration process is the most important part of the correct biometric template creation and subsequent fingerprint identification.
- Biometric authentications may vary depending from person, environmental conditions or incorrect use: exposure to abrasive surfaces, glues, solvents, powders, cement, excessive moisture, could compromise the fingerprint biometric authentication. Dirty, wet, dry, cut or damaged fingers may not be properly registered or identificated
- Children up to 5 years old could not be properly registered. A children's fingerprint should be registered every 6 months.
- It is recommended to register index, middle or ring finger as the thumb and little finger could be more difficult to register and use.
- Try to not press too hard or too soft on the optical sensor. Firmly place your finger on the sensor with appropriate pressure. A wet or too dry finger may not be properly registered or identificated.
- It is recommended to memorize for each user not only the fingerprint but also other credentials like PIN, cards, smartphones, to be used in case the fingerprint technology does not work.
- It is recommended to add more than one fingerprint for the same person. In this way in case your finger fails to be recognized for example because cut, scarred or damaged, you can use the other one.
- Make sure finger is always placed in the center of the optical sensor and placed firmly down. Always touch with the center of the fingerprint (fingerprint's core), as the tip of the finger will not register correctly.

Advanced

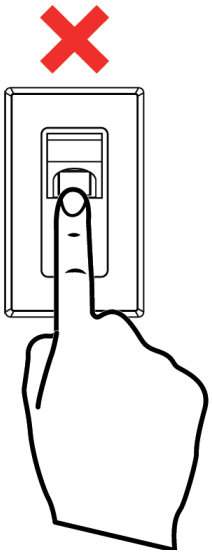
Fingerprint reader

CORRECT AND INCORRECT FINGER POSITION

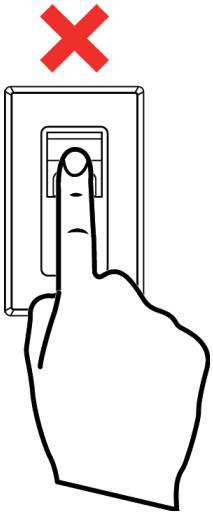
See in the next pictures the correct and some incorrect finger position examples.



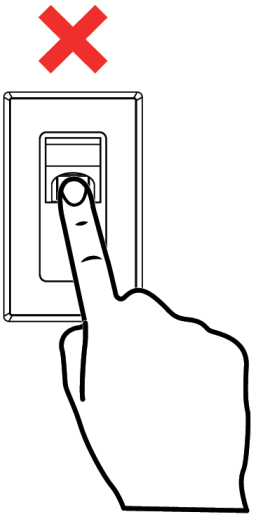
Correct position



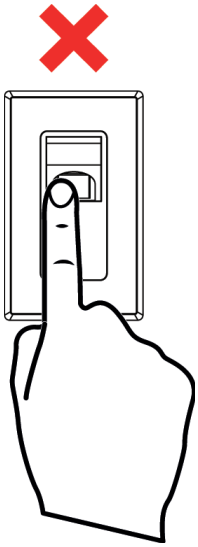
Too low



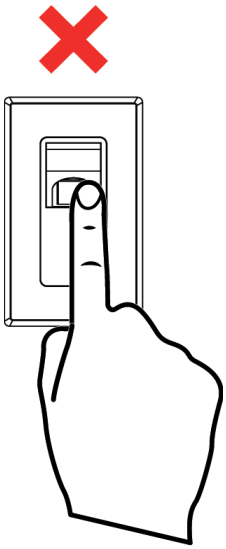
Too high



Not straight



Too much on the left side



Too much on the right side

Advanced

Mifare DESFire cards

Argo and the *ISEO Smart devices* can work with both *Mifare* card technologies: *Mifare Classic* and *Mifare DESFire* (see *Keywords* paragraph for a basic explanation).

Mifare DESFire and in particular the *Mifare DESFire EV2* model is currently considered the "state of the art" for security, since the authentication between the card and the lock is protected by the standard *AES 128 Encryption*.

The *DESFire* card type for both *Argo Master* and *User cards* is *Mifare DESFire EV2 2K*, that means 2Kbyte of memory space available. That's more than enough for *Argo* since it's a "data on devices" system, that means datas are stored in the Smart devices memory.

Notes:

- Argo DESFire cards functionality are exactly the same of Mifare model but adding security.
- For a better identification, *DESFire* cards comes in a new design for both *Master* and *User Cards*.

Master Cards

The *Master Card* have outside printed the same information of the current *Master Card* in *Mifare Classic* (plant code and Master sequence number). The plant code number is always unique independently from credential technology (to know more about plant code number go to *Overview* then *Master Cards Set*).
A new more modern graphic has been designed in oder to identify the card technology.
A file inside the ISEO application directory will protect the same data of the current Master. To read this file the doorlock will need to perform a cryptographic authentication and in this way it is impossible to clone the data.
It's always possible to upgrade from *Master Mifare* to *Master DESFire* performing the *Master Cards set replacement* procedure (to know more go to *Master Cards set replacement and updating of system code*).

FRONT

BACK

Advanced

Mifare DESFire cards

User Card

The *User DESFire* cards have outside printed the *Card Number:* it is the ISEO assigned unique number (DESFire UID), that can be used on Argo to add credential by the *Add USER DESFire* function (to know more about this function go to *Basics* then *Add users typing Mifare card UID*).

A new more modern graphic has been designed in oder to identify the card technology.

A file inside the ISEO application directory will protect the Card ID, therefore to read this file the doorlock will need to perform a cryptographic authentication.

FRONT

BACK

Technical data summary

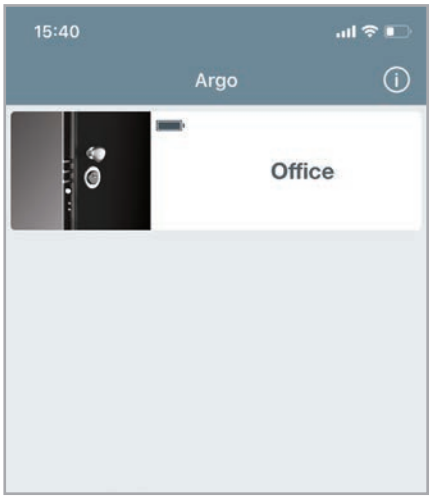
- **Model**: Mifare DESFire EV2 2K
- **Memory Size**: 2 Kbytes
- **Encryption**: AES 128 bit with different encryption key for each card.
- **User Card**: outside printed card number (Argo UID), protected by secure authentication.
- **Master Card**: outside printed plant code and Master sequence number, protected by secure authentication.

Siri Shortcuts voice commands to open (iOS only)

On *iPhone* and *iPad*, starting from *iOS 12*, by the *Shortcuts* app you can add a voice command to open any *Iseo Smart device*.
The next step by step procedure shows how to configure a shortcut to open an *x1R Smart* named *Office* by voice command.

Step 1: enable Siri Shortcuts on Argo

Siri Shortcuts on *Argo* is disable by default. To use voice commands you need to enable it first.



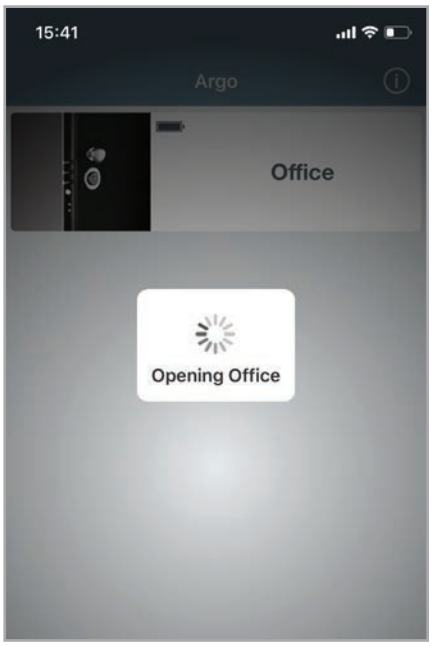
Open Argo app and touch *Info app* menu.

Enable **Siri Shortcuts**

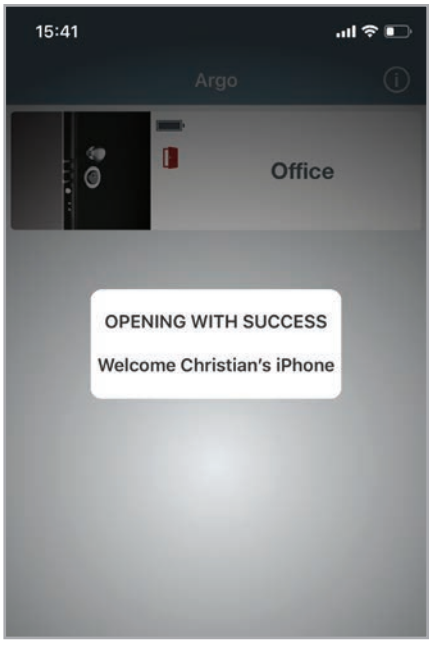
Siri Shortcuts voice commands to open (iOS only)

Step 2: open the door with Argo

Open the door for which you want to create the voice command, by *Argo*. This will automatically configure the shortcut action that will be then associated to the voice command.



Tap the icon button to open the door.

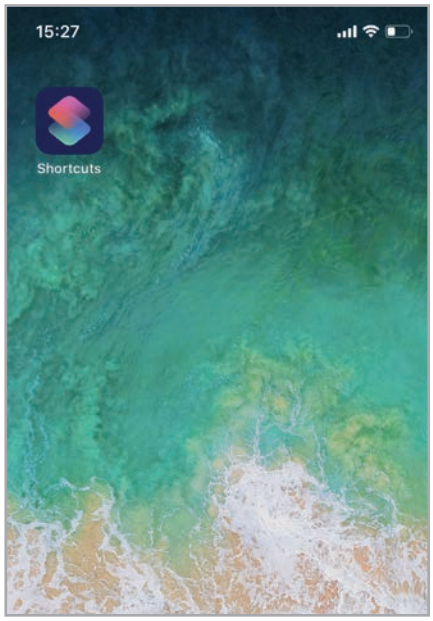


Door succesfully open.

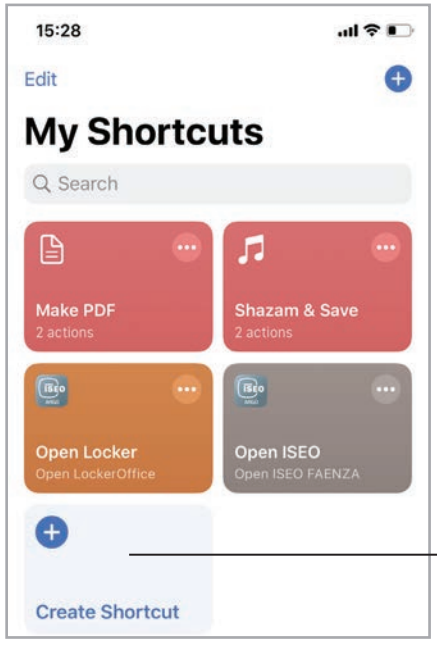
Siri Shortcuts voice commands to open (iOS only)

Step 3: create the shortcut

Create the *Siri Shortcut* by the **Shortcuts** app available from *iOS 12.*



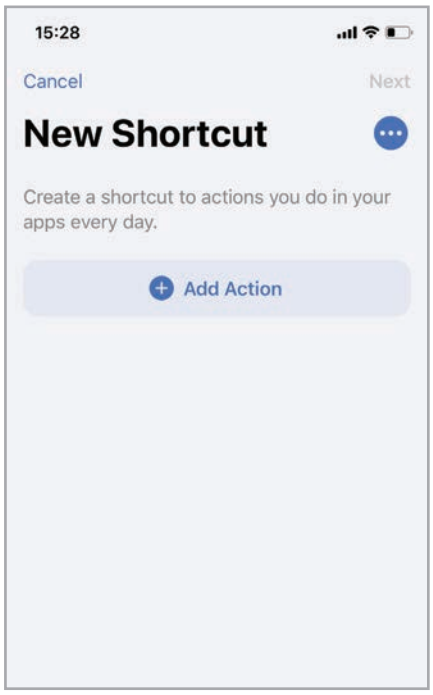
Open **Shortcuts**.



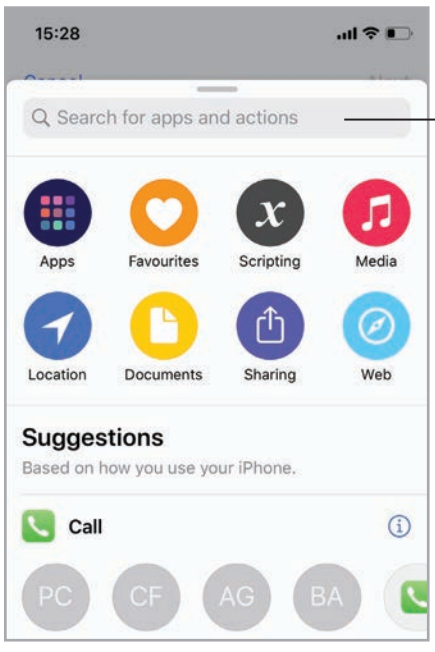
Tap **Create Shortcut**.

Siri Shortcuts voice commands to open (iOS only)

Step 3: create the shortcut



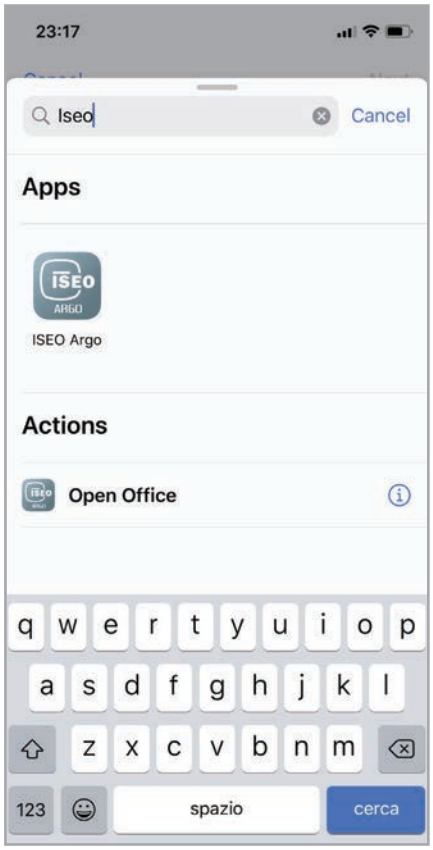
Tap **Add Action**.



Search for **ISEO Argo**.

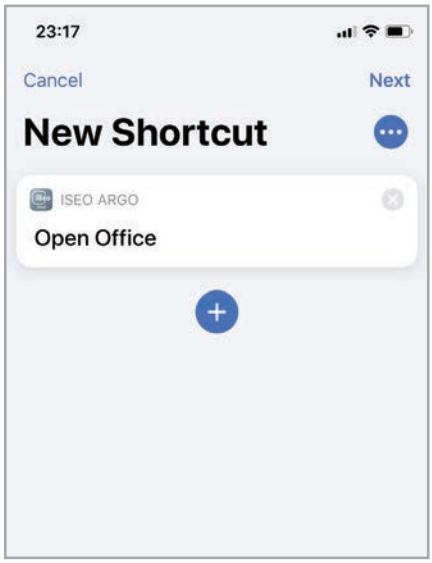
Siri Shortcuts voice commands to open (iOS only)

Step 3: create the shortcut



Select the last action: **Open Office**

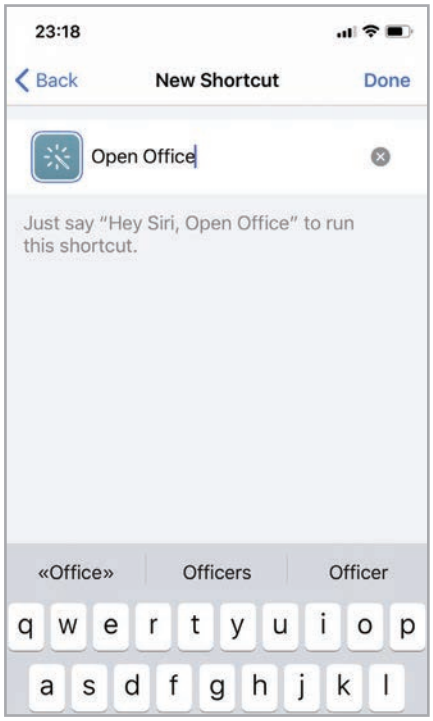
If *ISEO Argo* does not appear in the search list, that could mean *Siri Shortcuts* has not been enabled on the *Argo info app* menu (see *Step 1: enable Siri Shortcuts on Argo*).



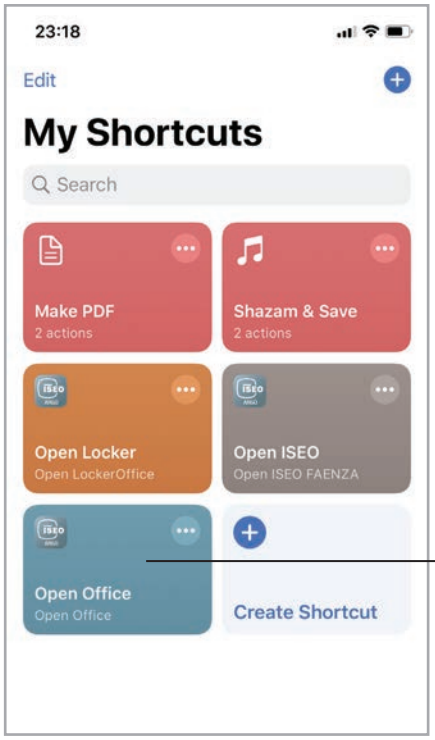
Tap **Next**.

Siri Shortcuts voice commands to open (iOS only)

Step 3: create the shortcut



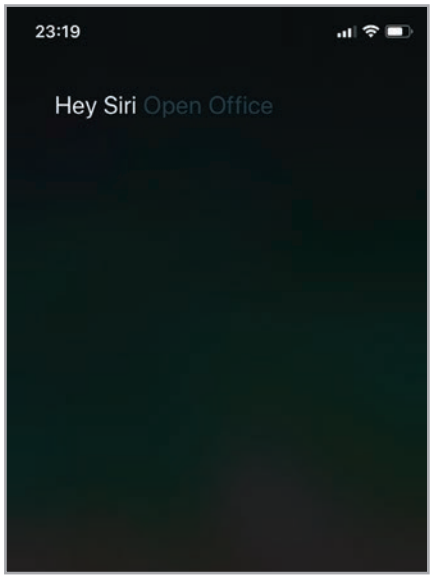
Write the voice command that will be used to open the door: for example **Open Office**. Then tap **Done**.



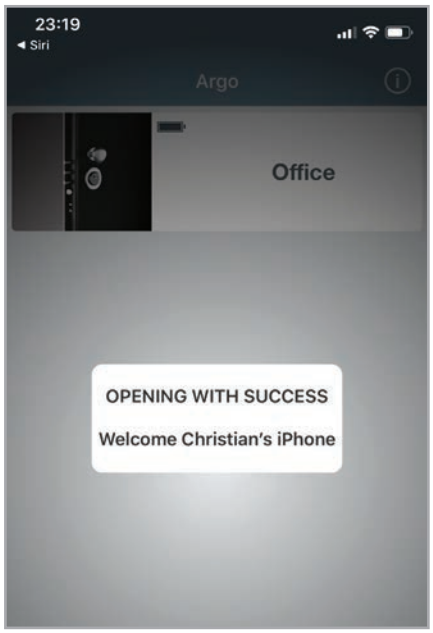
The new shortcut just created appears in the *My Shortcuts* page.

Siri Shortcuts voice commands to open (iOS only)

Step 4: open with voice command



——— Say: *Hey Siri Open Office*.



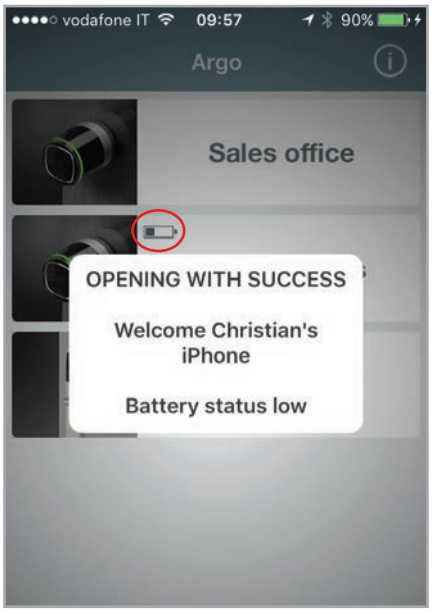
——— Door will open in a few second.

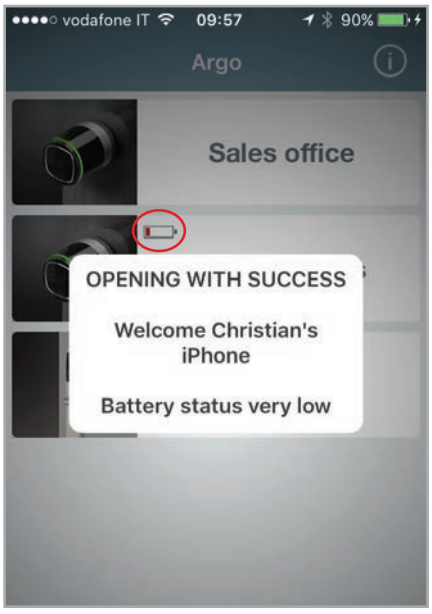
For security reason, when the phone is locked, the voice command to open the door cannot be execute: you need to unlock your phone first, as also suggested by *Siri*. In case the *Face ID* is enabled on your phone, the door opening process will be automatic: it is enough to look at your phone to unlock it and automatically the voice opening command previously sent will be execute on Argo and the door will open in a few seconds.

Service

Battery levels

The lock *Battery level* icon is always displayed in the *Argo App* or when opening with card with specific light signals on the smart device. As there are 4 levels of battery level the user get early notification of low battery.





Battery OK: **green light** flashes on the device during opening time (standard opening signal).

Battery Low: warning message in the app and **orange light** flashes during opening time.

Battery Very Low: warning message in the app and **red light** flashes for 3 seconds before the opening signal (opening delayed).

Battery Empty: warning message in the app and **red light** illuminates for 3 seconds without opening.

After the first *Low battery* signal, change the batteries with new ones as soon as possible.

Battery replacement does not affect *Events* and data stored in the *Users list.*

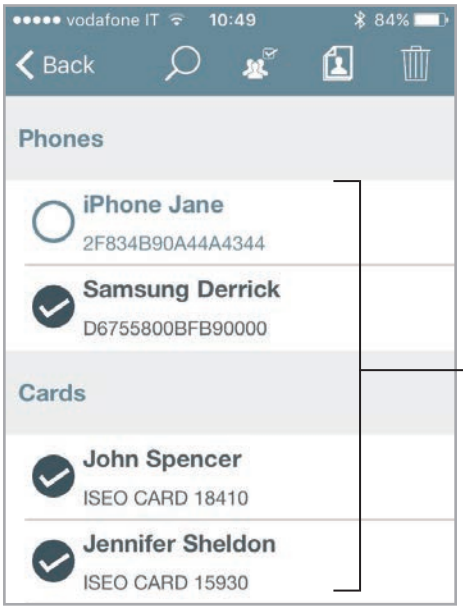
If the device is powered by mains, like Stylos, you will see the *lightning* at the place of the *battery* icon.

Service

Copy users

You can copy the *Users list* programmed in a *door lock* to send it to another device, in order to quickly get the same access rights.

Enter *Programming mode* and tap the E*dit user* icon.



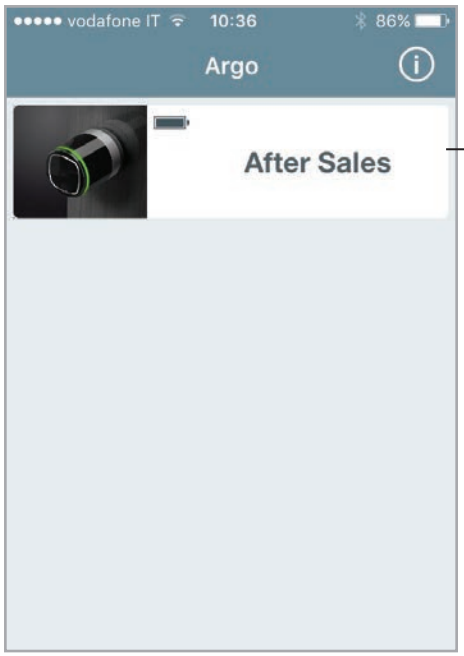
1. Select the users to be transferred.
   You can also select all users tapping on
2. Tap the *Copy* icon.

Copied users are kept in the phone memory until you close the app.

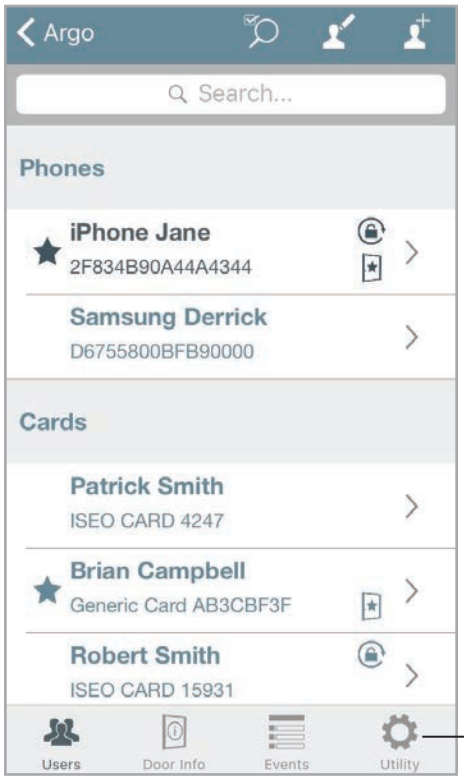
Service

Transfer users

Copied users in the phone memory can be transferred into another device.

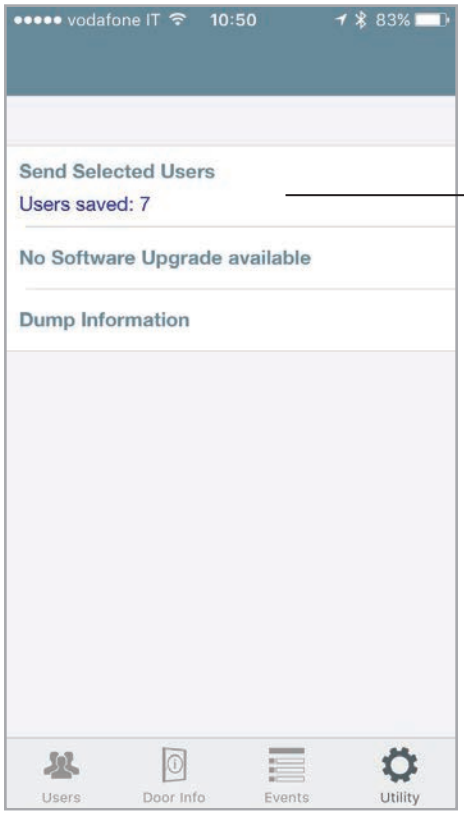


1. Enter *Programming mode* in the device where you want to transfer the users, by *Master Card.*

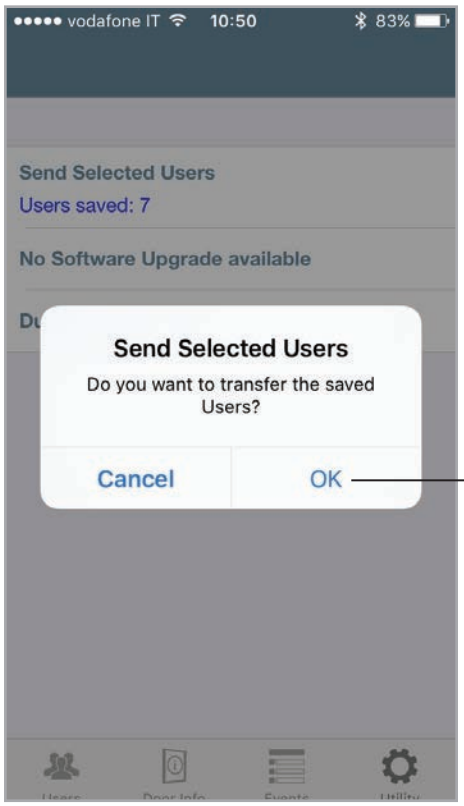


3. Tap **Utility** icon.

Transfer users



4. Tap **Send Selected Users**.



5. Tap **OK**.

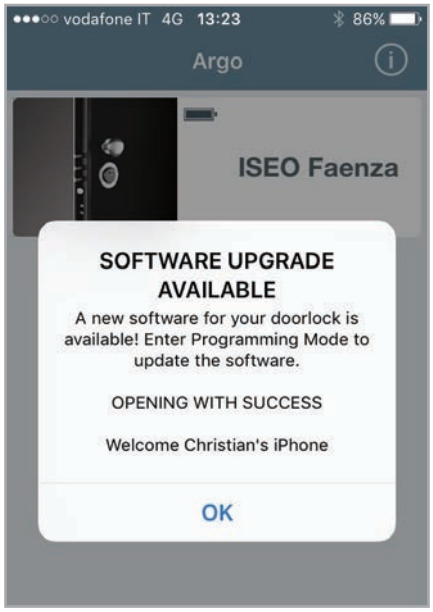
Service

Software Upgrade

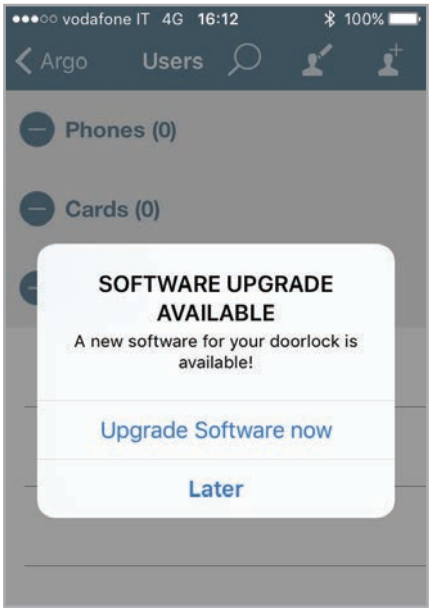
When a new *Software version* is available for your *Access control device*, your smartphone always notifies you when opening the door (image *1. Door opening*).
Moreover everytime you enter *Programming Mode*, a pop-up message will appear, and you can decide if upgrade software immediately or not (image *2. Programming Mode*).

- If you touch **Upgrade Software now** the upgrade will immediately start.
- If you touch **Later** you can do it in another moment by *Utility* menu (image *3. Utility Menu).*

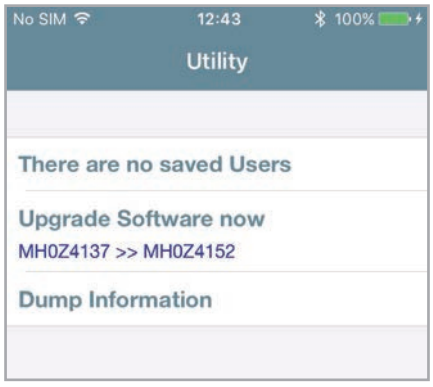
1. Door opening



2. Programming Mode



3. Utility Menu (Progr. Mode)



1. Tap **Utility** in the bottom bar.
2. Tap on **Upgrade Software now**.
3. The upgrade will start showing a progress bar.

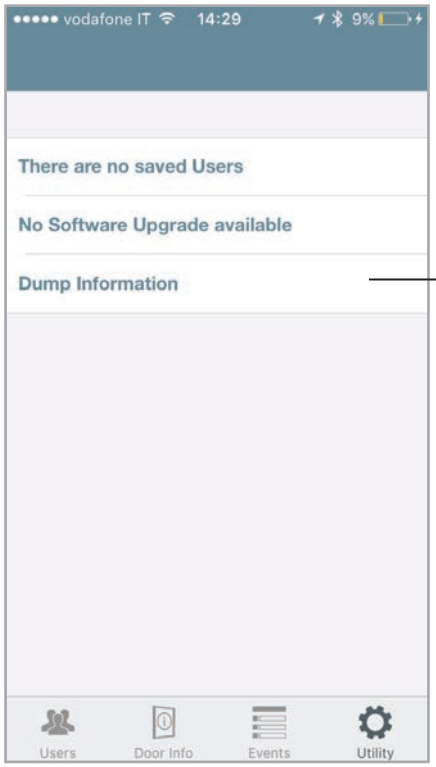
If you upgrade from *Argo* to *Argo 2.2*, watch before the tutorial "*Argo 2.0 Software Upgrade"*, or read the manual "*Argo 2.0 Upgrade Procedure*", both available at:
https://app.iseo.com/?parm=ARGO&lang=en&folder=argo-update

Service

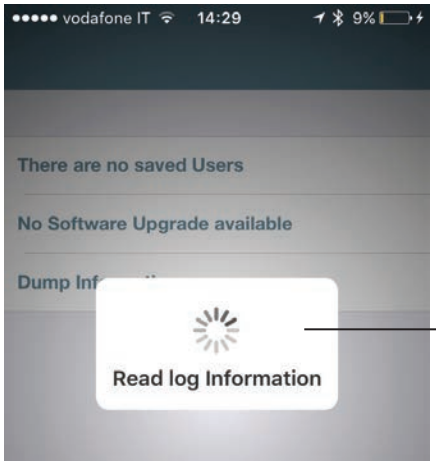
Dump Information

This function allows to collect all device's data into a unique compressed file, that has to be send to *IseoZero1 Technical Support*, via email. This is really useful for device's analysis pourpose. By receiving this file in fact, the technical support will receive all the necessary information to properly analyse the issue.

The file is protected by password and only *IseoZero1 Technical Support* can open it. By sending this file customer agreed to send all the device's information to *IseoZero1 Technical Support*.



1. Enter *Programming mode.*
2. Tap **Utility** in the bottom bar.
3. Tap on **Dump Information**.

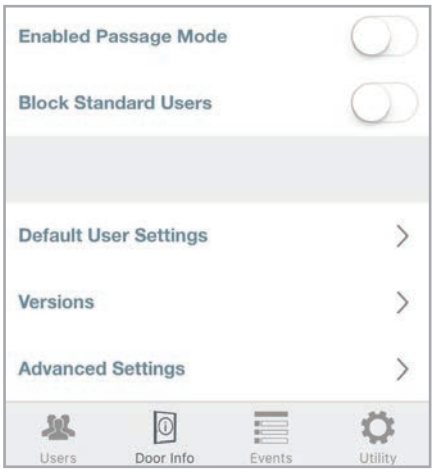


4. Wait until the log reading pop-up disappear (about 2 or 3 min.).
5. An *email* will be automatically created.
6. Send it to *IseoZero1 Technical Support*.

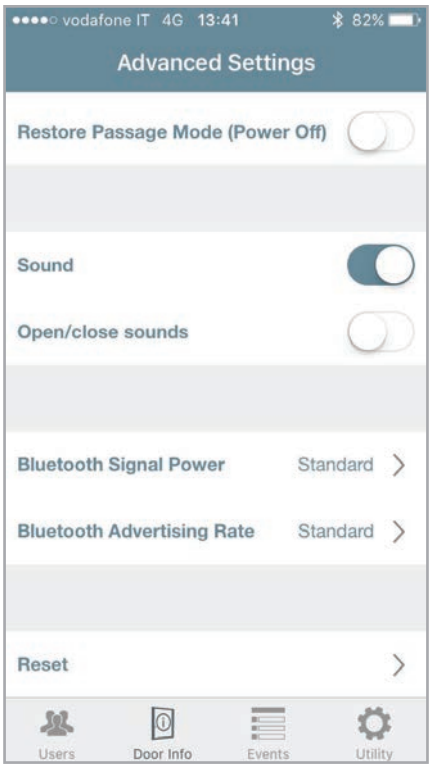
Service

Bluetooth parameters

This function allow you to change the *Bluetooth Signal Power* and the B*luetooth Advertising Rate* from *Standard* to *High*. This setting has been introduced just to improve the Argo performance during demo, in fairs or exibithions. In those kind of environments in fact, there is usually a high concentration of electromagnetic noise, due to the large numbers of routers, access points, smartphones and other different electronic devices present at the same time. In this condition the *Bluetooth signal* could be compromised, resulting in delays in communications, connection errors and a shorter trasmission and receiving distance, between the Argo app, running in the smartphone, and the device. That's why, only for those cases, it is recommended to set both parameters to *High*. In this way *Bluetooth Signal power* and *Advertising Rate* will increase, but increasing as consequence the device battery consumption.

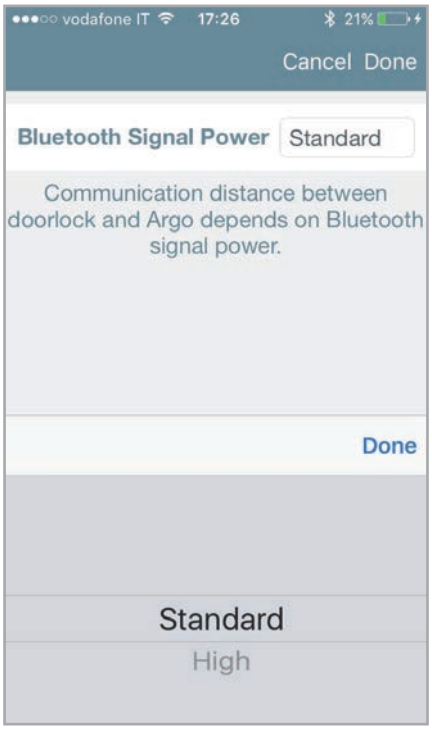


Enter **Door Info** and then **Advanced Setttings** menu.



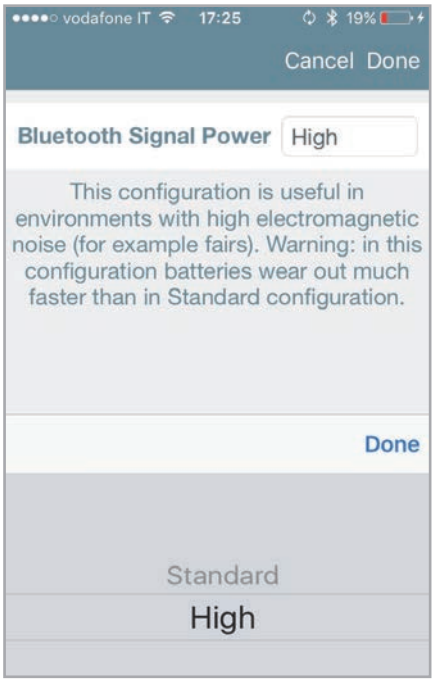
Tap *Bluetooth Signal Power* or B*luetooth Advertising Rate.*

Bluetooth parameters



A short text explains you the meaning of the feature.

Change the setting from **Standard** to **High** only in case of fairs or exibithions.



A message explains you the use and the risks of the **High** setting.

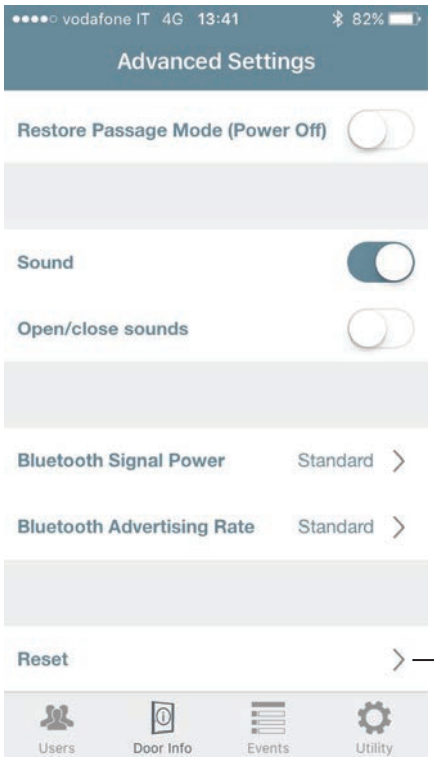
In order to avoid a faster battery consumption, remember to set the *Bluetooth parameters* back to *Standard* setting, at the end of the fairs or exibithion.

Service

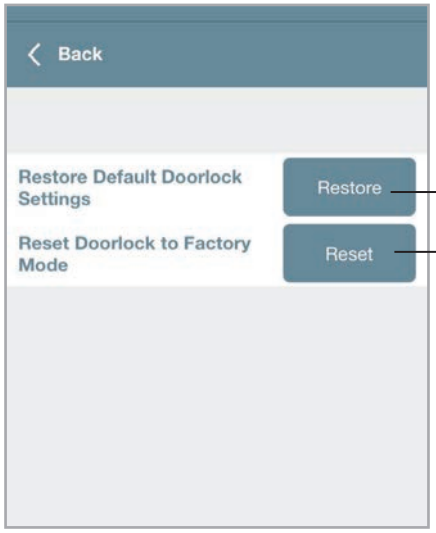
Reset

In this menu you can find 2 different and powerful kinds of reset:

- **Restore Default Doorlock Settings**.
- **Reset Doorlock to Factory Mode**.



Enter **Door info** and then **Advanced Settings** menu. Then tap **Reset**.



Tap this button to **restore all the device settings** to the default ones. All the editable parameters, like for example *Default User Settings, Door Opening Time, Sound, Bluetooth parameters*, ecc...Will change back to the default values, originally set in the *Argo app*.

Tap this button to **complete reset your doorlock**. This function is useful for example, when you need to send back the device for repair and you need to remove the *Master Card* plant code from it.
A warning pop-up will advise you that it will cause the removal of the *Master Card* and the cancellation of the entire user list. All device parameters will come back to *Factory mode*.

Reset Doorlock to Factory Mode operation, for security reasons, doesn't delete the events log.

Updating of Master Card level

If a *Master Card* is lost or damaged, in order to disable it, just read on the device the following *Master Card* of the same set:

- Presenting *Master Card 2* to the device, *Master Card 1* is disabled.
- Presenting *Master Card 3* to the device, *Master Card 2* is disabled.

In case the *Master Card* of lower number is disabled by mistake, this can be re-activated.
Read the *Master Card* of higher number to the device, than read the *Master Card* you want to re-activate:

- *Master Card 3* re-activates *Master Card* 2 and 1.
- *Master Card 2* re-activates *Master Card 1*.

You cannot update from *Master Card 1* to *Master Card 3* of a different set, since it is assumed that if you have only *Master Card 3,* you need to purchase a new *Master Card Set* to restore the security.

Master Card Set replacement and updating of System Code

If both *Master Cards* 1 and 2 are lost, in order to ensure the system's security, you must update the *Access control devices* with a new set of *Master Cards*.

To do that you need to present the *Master Card 3* of the old set to the device, followed by *Master Card 1* of the new set.

Master Card 3 must be considered as the updating card for the new *Master Card Set*, since its loss could irreversibly compromise the possibility to modify or update the system.

During *Master Card Set* update no change is made to the *Users list* of the devices.

Argo is compatible with both *Simply PAD* and *Simply Sequence Master Card Set*, to allow existing customers to upgrade the new *Smart line* system.

Events log messages

(Common to all devices)

Result	Meaning / Notes
Battery Empty	Door not open due to exhausted battery.
Blocked User	Standard Users not allowed to enter the door. Access granted only to VIP Users.
Block Standard User ON	Block Standard User function enabled. Standard user cannot enter the door.
Block Standard User OFF	Block Standard User function disabled.
Bluetooth advertising rate set to level high	High setting is recommended only in case of demo or exibithions.
Bluetooth advertising rate set to standard level	Default level. Best batteries performance.
Bluetooth signal power set to level high	High setting is recommended only in case of demo or exibithions.
Bluetooth signal power set to standard level	Default level. Best batteries performance.
Configuration changed	Scheduled Passage Mode configuration has been changed.
Delayed Close	Close delayed due to battery very low.
Delayed Open	Open delayed due to battery very low.
Device in software setup	Device software upgrade has been started.
Door Open	User enabled, standard opening.
Enter Programming Mode	Enter Argo Programming Mode by Master Card.
Exit Programming Mode	Exit Argo Programming Mode.
Expired	Credential validity expired. User cannot access the door.
Memory Full	The user list has reached the maximum number of allowed users in memory (300).
New MASTER Level	Updating of Master Card 1 to 2 or 3, of the same set.

Events log messages

(Common to all devices)

Result	Meaning / Notes
New MASTER Set	Updating of Master Card Set to a new set.
Not in Memory	Credential never memorized in the door.
Not yet valid	Credential validity not yet started. Credential not yet active.
Out of time schedule	User not allowed to access the door due to Time Schedule not respected.
Passage Mode OFF	Passage Mode function disabled.
Passage Mode ON	Passage Mode function enabled: lock always open.
Phone not Paired	Phone requires Bluetooth pairing. It is probably not running Argo 2.1 (in-app Pairing). Download the new Argo app.
Power ON reset	It is recorded at every device switch on (power cycle). Argo shows also the current device software version.
Reset Doorlock to Factory mode succesfull	Full device reset has been performed. Device is no more initialized and the user list is clean. Events are still present.
Restore Default Doorlock Setting succesfull	Restore of default setting has been performed. The device is still initialized but all settings come back to the factory default.
Software Upgrade	Device software upgrade has been performed. Argo shows from which version to which version the software has been upgraded.
User Added	Added user to the users list.
User Deleted	Deleted user from the users list.
User List clear	Entire users list deleted.
User Updated	Modified user parameters (Name, Functions, Time Control...).
Wrong PIN	Wrong PIN inserted in the smartphone to open the door.

To not quickly overwrite the Events Log, after 30 consecutive invalid reading error, the next are not recorded for 15 minutes.

Events log messages

(Only Aries Smart)

Result	Meaning / Notes
Open with Internal Handle*	Lock opened from the inside by the internal handle.
Open with Mechanical Key*	Lock opened by mechanical key.
Set Privacy OFF	Privacy set OFF by rotating the privacy button.
Set Privacy ON	Privacy set ON by rotating the privacy button.
User blocked for Privacy ON	Users without Override Privacy function are not allowed to enter the door when privacy is ON.

* To not show duplicates of the same event, when repeated in a short time, this event is recorded 1 time per minute.

(Only Stylos Smart)

Result	Meaning / Notes
Communication error with electric lock actuator	Actuator OFF, disconnected or not working. Or exchange of coded keys not correctly performed.
Exchange of coded keys performed	Exchange of key succesfully completed between Stylos and Actuator.
Open by remote opening button	Lock opened by remote opening button.

Events log messages

(Only x1R Smart)

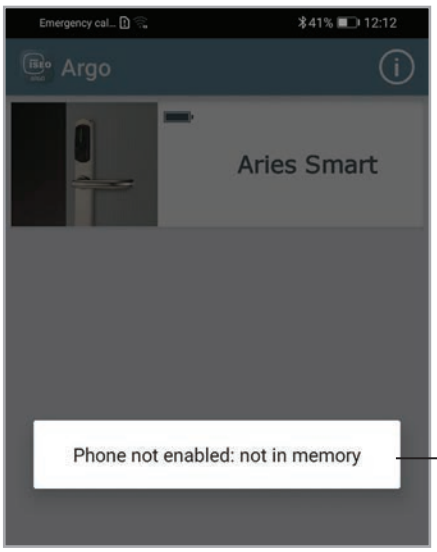
Result	Meaning
Close with Mechanical Key	Lock closed by mechanical key.
Door Close	Door closed, x1R bolts automatically close. Maximum security.
Door Close Light	Door closed with Light Mode enabled. Only latch in, bolts not out.
Functional Mode change	The functional mode Outside Knob/Outside Handle has changed. This function is only available on *x1R Smart Standard*.
Lock bolts in half-way by handle	Bolts have been moved by handle but not completely in. Just 1 shot (half-way).
Lock bolts in half-way by key	Bolts have been moved by key but not completely in. Just 1 shot (half-way).
Lock not close due to motor extra-current error	It happens when there is an excessive friction of latch or bolts during closing.
Lock not close due to sensor time-out error	It may happen when motor does not engage the mechanic during closing.
Lock not open due to motor extra-current error	It happens when there is an excessive friction of latch or bolts during opening.
Lock not open due to sensor time-out error	It may happen when motor does not engage the mechanic during opening.
Open with Internal Handle	Lock opened from the inside by the internal handle.
Open with Mechanical Key	Lock opened by mechanical key.
Open by remote opening button	Lock opened by remote opening button.
Open denied due to internal handle pressed	It happens when, during opening by electrical command, the internal handle is sighlty down enough to activate its internal sensor. It may happen for example in case of x1R combined with panic bar device, when installation has not been correctly done.
Passage Mode Change	Passage Mode has changed from Light to Free or viceversa.

Android Argo app uninstall

For security reasons, deleting the *Argo App* on Android phones, will delete also the identity (Argo UID). As consequence, even if you re-install the app in the same Android phone, you will need to register again the phone in all the locks where was previously added as user or administrator.
From the other side iOS phones will continue to work as before: deleting and re-installing the Argo App the identity is kept, since iOS has built-in a mechanism that restores the identity data in a secure way.
ISEO will continue to monitor the evolution of Android phones and in case Android will implement a secure built in mechanism like iOS, to restore the identity data in a secure way, ISEO will also implement the same feature on Argo.

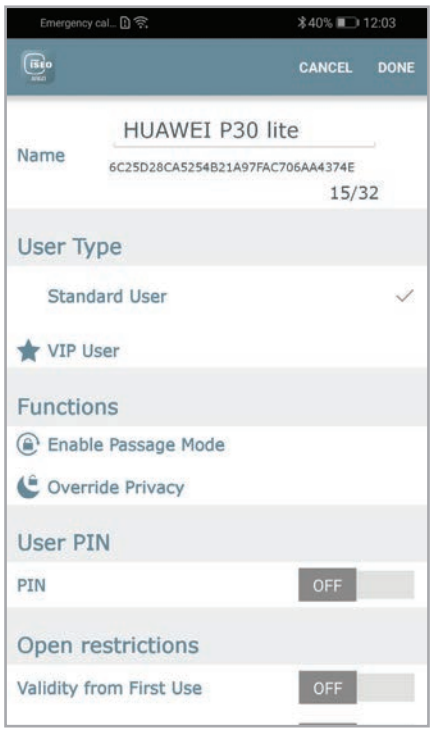
On all Android phones, uninstalling the Argo app and re-installing it again, you will need to register the phone in all the locks where it was previously added as user or administrator.

In case of Argo app UPDATE from Play Store the phone will continue to work as before since the identity is the same. So it will be enabled on all the locks where it was previously registered.

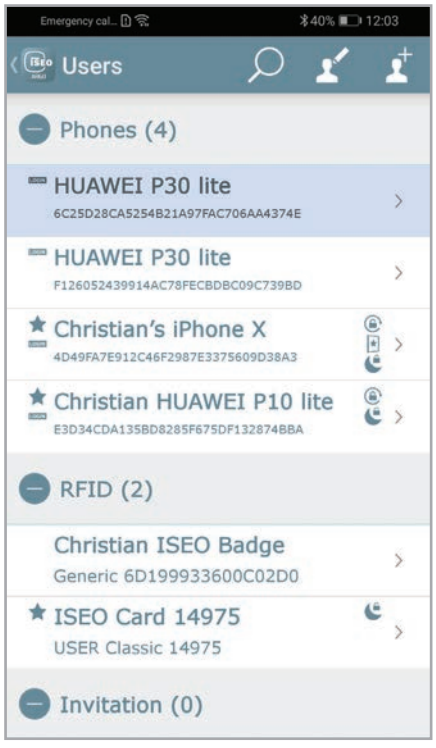


When Argo app has installed again, the Android phone won't work anymore on locks where it was previously enabled.

Android Argo app uninstall



To register the phone again enter *Programming Mode* by *Master Card*.



After phone registration you will find in the user list two Android phones:

- the highlighted one is the one with the new Argo UID after Argo re-installing.
- The other one is the old ones, with the previous Argo UID that has been deleted uninstalling the Argo app. This phone can be deleted since it doesn't exist anymore.

Backup and Restore user list

Backup user list function allows to save and store outside Argo all the memorized users of any *ISEO Smart Device. Restore* function instead allows to import back the previously exported users, in order to load it into another *ISEO Smart device*.
This function can be really useful for service: in case of device replacement, for example, we can backup the user list and restore it later on the new device, avoiding to manually re-program all users that had acess to the replaced device. Or we can simply backup a users list just to keep it for future reference or needs: to load it on new devices or even in the same one if something has changed and we want to restore back the original list.

Backup Vs Copy users

Copy users function, showed in the previous paragraph, has two important differences respect the *Backup* function, as explained in the next points.

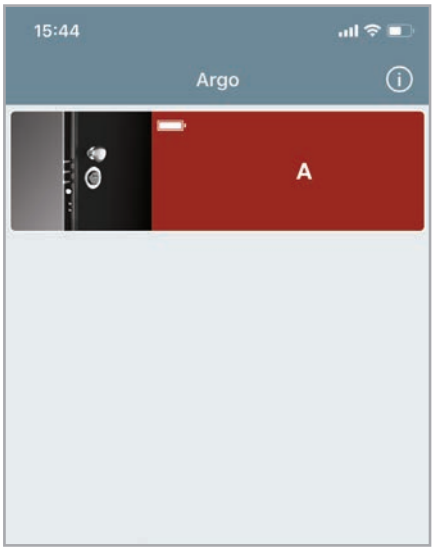
• *Copy users* (see *Copy users* paragraph) **temporarily** save the selected users in the *Argo app* memory. That means the saved users will be deleted as soon as the app is closed; in other words you need to **immediately** *transfer* the copied users into another device before to get them lost.

• *Backup users* function instead, **permanently** save the selected users outside the *Argo app*. That means the exported users will always be available to be *restored* **anytime** in the future.

Backup and Restore example

The next procedure shows an example on how to make a *Backup* and *Restore* of the user list from one *x1R Smart* called *A* to another one called *B*.

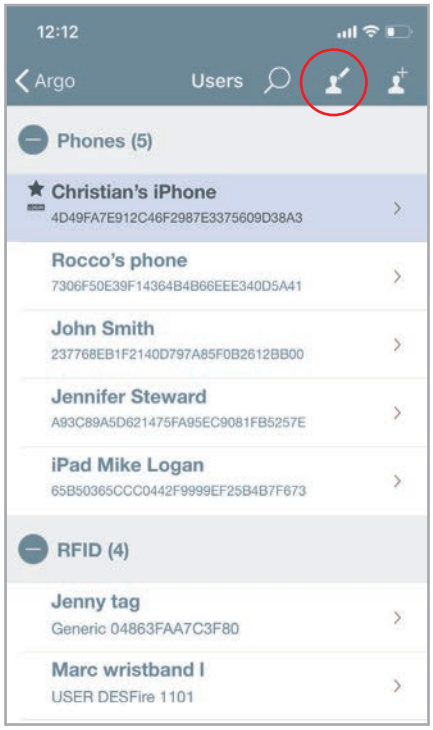
Step 1: Backup user list



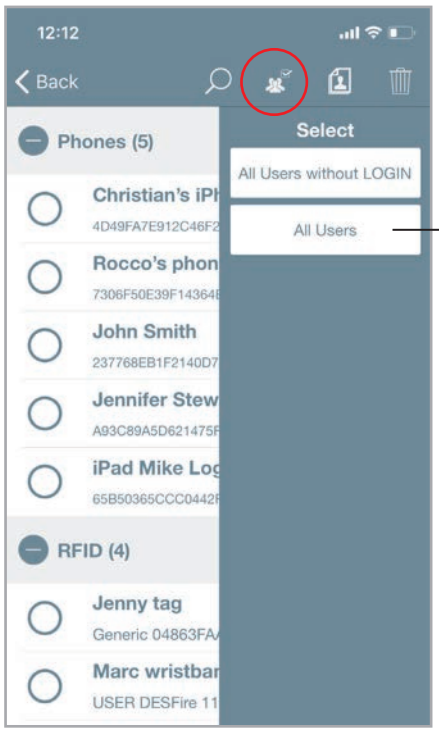
On *x1R Smart A*, open *Argo app* and enter *Programming Mode.*

Backup and Restore user list

Step 1: Backup user list



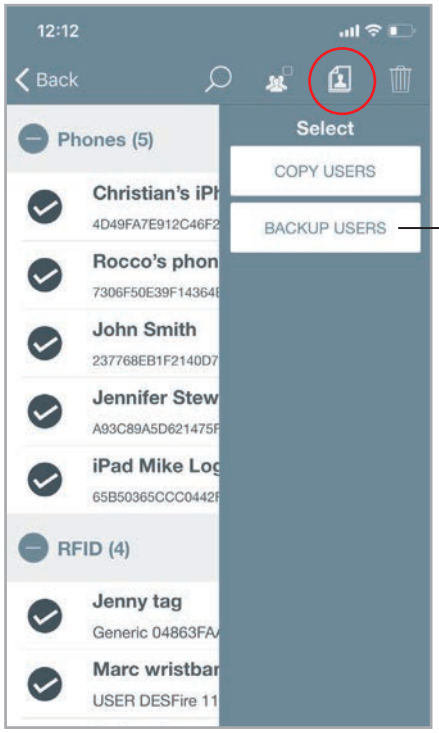
Tap *edit users* icon.



1. Tap *select users.*
2. Tap **All Users**

Backup and Restore user list

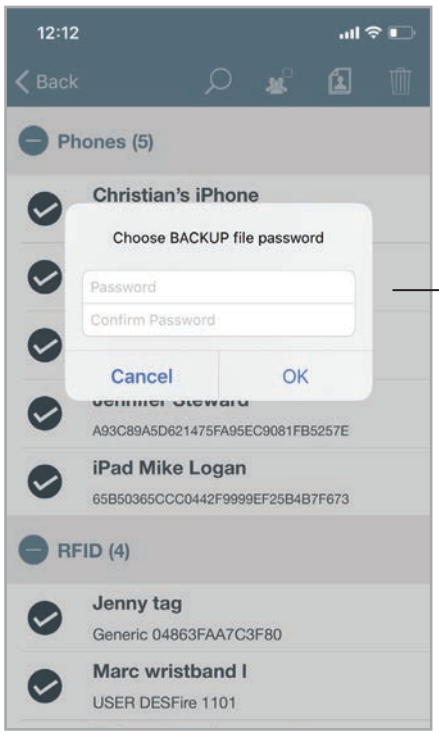
Step 1: Backup user list



1. Tap *copy users* icon.

2. Tap **BACKUP USERS**

In case of many fingerprints present in the user list, the backup may require time since biometrics templates are bigger size files. A spinning wheel shows the loading progress status.

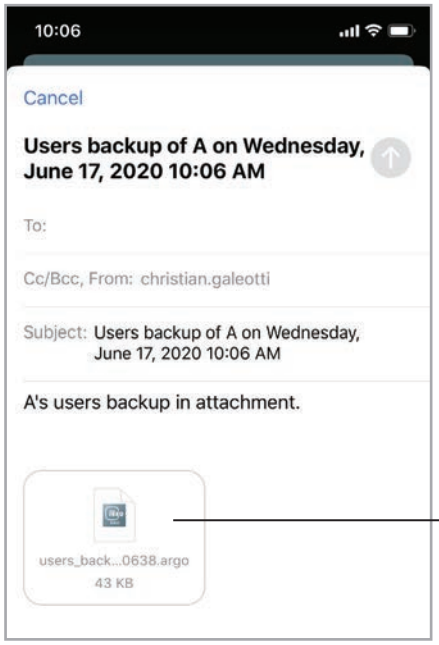


Write and confirm a personal password then tap **OK**. Password must be at least 4 characters long.

The backup is an encrypted file protected by password. Password is mandatory for security reason since the backup contains personal users' data. In this way only the Administrator can restore it since he's the unique owner of the password.

Backup and Restore user list

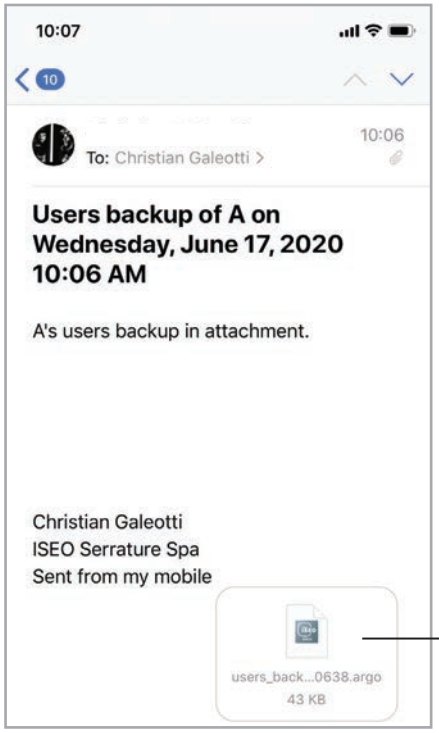
Step 1: Backup user list



An email with the encrypted backup file attached is automatically generated. Send it to your email address to receive it back in your inbox folder.

Users_backup.argo encrypted file attached. The file name also includes backup date (yy-mm-dd) and time (hh-mm-ss). I.e.: *users_backup_A_200617_100638*

Step 2: Restore user list

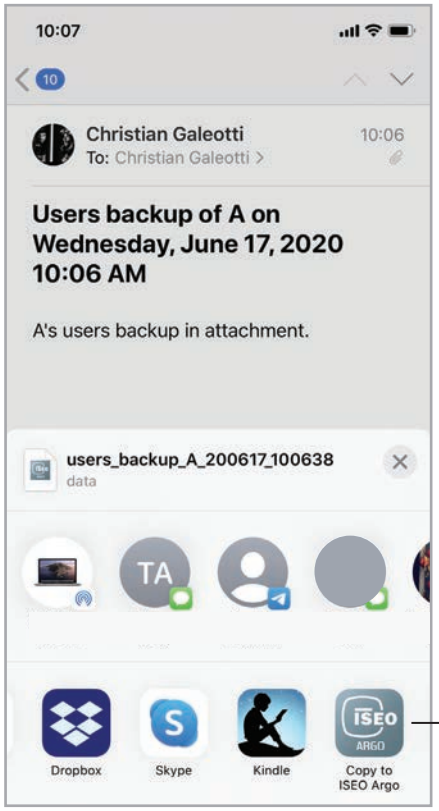


Open the received email and tap the attachment to open it.

Tap the attachment to open it.

Backup and Restore user list

Step 2: Restore user list

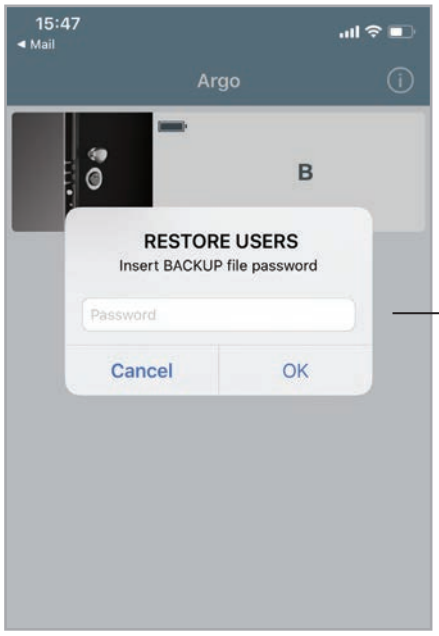


iOS only

Scroll through the available apps, then select **Copy to ISEO Argo** to open the backup file by the *Argo app*.

Android phones

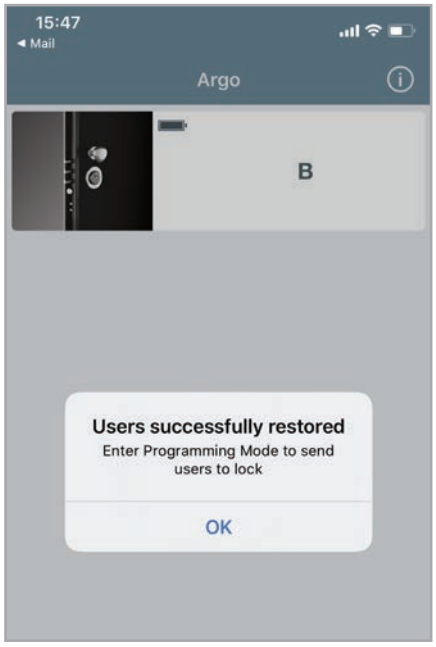
On Android phones, once you tap the attachment, the file download starts and at the end it will automatically open with *Argo app*.



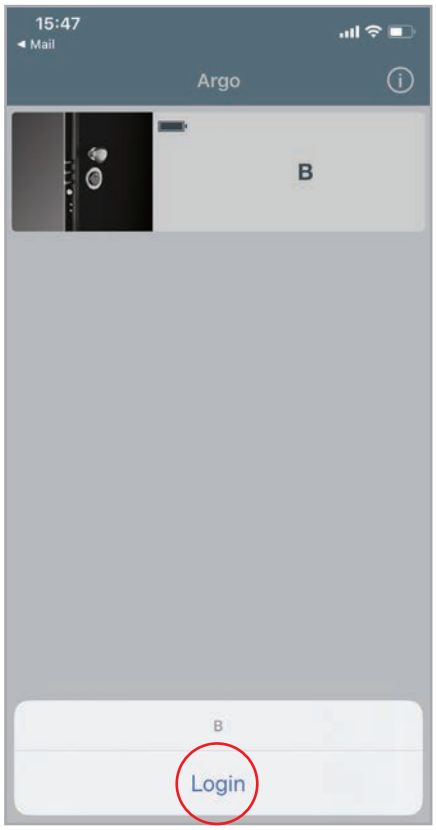
Write the backup file password previously chosen and tap **OK**.

Backup and Restore user list

Step 2: Restore user list



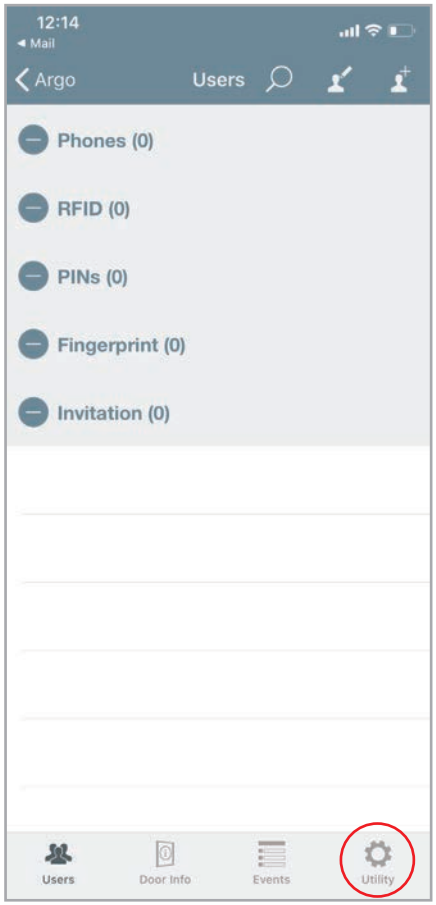
The backup users are now in the *Argo app* memory exactly like the *Copy user* function (see *Copy users* paragraph).



Go nearby *x1R Smart B* and enter *Programming Mode*.

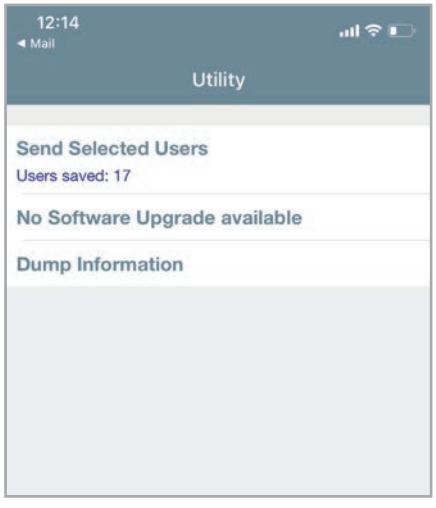
Backup and Restore user list

Step 2: Restore user list



x1R Smart B empty user list.

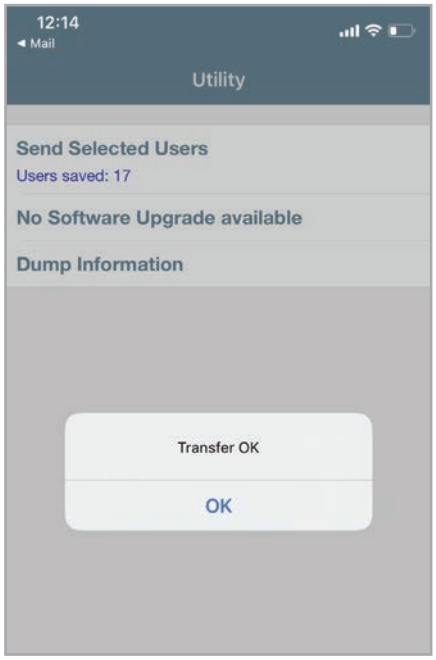
Tap **Utility**



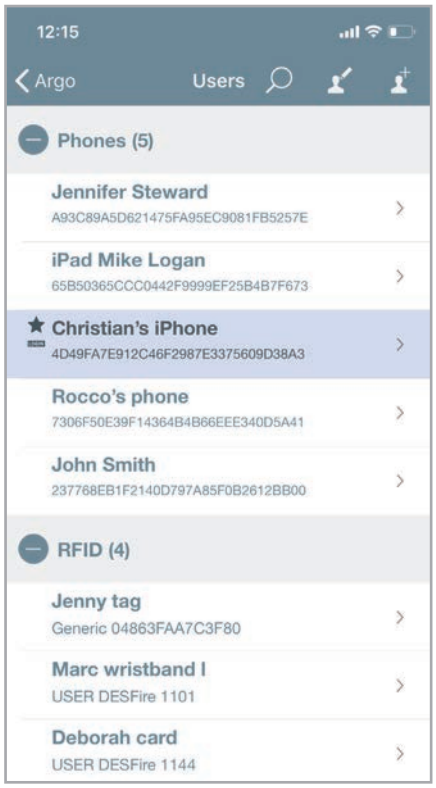
Tap **Send Selected Users** (see also *Transfer users* paragraph).

Backup and Restore user list

Step 2: Restore user list



Wait the confirmation message then tap **OK**.



x1R Smart A user's backup has been completely restored on *x1R Smart B*.

- Restore operation does not affect already existing users in the target device user list. Existing users will not be modified, nor deleted or overwritten. The restore acts as a merge operation.
- In case some users that are going to be restored, are already present in the target device user list, the restored users will overwrite the existing ones, since we consider the backup the correct and safe reference.

Appendix

Operations summary without Argo app

Operation	What to do
Add Users	1. Present the Master Card to the device. 2. Read the cards to be added. 3. Present the Master Card to the device.
Delete Users	1. Present the Master Card to the device. 2. Present a second time the Master Card to the device. 3. Read the cards to be deleted. 4. Present the Master Card to the device.
Delete entire Users List	1. Present the Master Card ot the device for 5 sec. 2. Repeat the operation for 3 times consecutively.
Enable and Disable Passage Mode	1. Read a card with t Mode function enabled for 3 sec.
Block and Unlock Standard User	1. Read a card with Block Standard User function enabled. 2. Repeat the operation for 3 times consecutively.
Updating of the Master Card	1. Present the next Master Card of the same set to the device.
Master Card Set replacement	1. Present the Master Card 3 of the current set to the device. 2. Present the Master Card 1 of the new set to the device.

Updating of *Master Card* and *Master Card Set* replacement are critical operations that must be performed only by the *System manager* or trained personnel. For more information refer to the related chapter.

Appendix

Technical data summary table

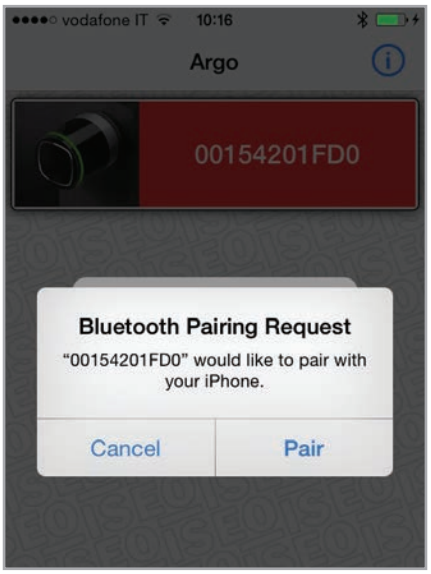
Feature description	Value	Device
Max nr. of users	300	All
Max. nr. of recorded events	1000	All
Compatible phones	*iOS*: from iPhone 4s with iOS 7 and above. *Android*: from version 4.3 (Jelly Bean), featuring *Bluetooth Smart Ready* hardware.	All
Compatible credentials	1. ISEO cards, tags 2. Mifare* cards, tags 3. ISO14443 A or B cards with UID (Unique IDentifier) 4. Mifare DESFire* (works reading the UID) 5. NFC phones (13,56Mhz, NFC static UID required) See "*Notes on NFC phones*" on *Credentials* chapter.	All
Max Door Name length	12 Characters	All
Max phone/card name length	32 Characters	All
Max generic card UID length	32 Characters	All
Phone PIN code length	4 Characters	All
Opening Time range	From 1 to 30 sec. (deafult 5sec.)	Aries-Libra
	From 100msec. to 30.000msec. (deafult 5.000msec.)	Stylos
	From 1 to 30 sec. (deafult 15sec.)	x1R
PIN code length (keyboard)	14 Characters	Stylos Displ. x1R
Close Delay Time	From 1 to 5 sec. (deafult 1sec.)	x1R
Time Schedules	2 time schedules available per user.	All
Scheduled Passage Mode	2 schedules available per device.	All

* *Mifare* is a brand of contactless card with several card types: Classic, Ultralight, DESFire...
All *Mifare* cards works in *Argo* by reading the UID (unique identified number).

Appendix

In-app pairing

Pairing is the *Bluetooth* technology process used to set-up the initial linkage between two devices, in our context the smartphone and the lock, to consequently allow communications between them and all data transfer to be encrypted.
It is normally managed by the smartphone operating system, and it is recognizable by the fact that, in the Bluetooth menu, in the phone settings, you can see all the paired devices



On the previous version of *Argo*, when you connected to the *Access control device*, you were requested to pair the smartphone.
This operation was requested only the first time, and allowed all data transfer to be encrypted from the smartphone to the lock, avoiding any security attack.

From *Argo 2.0* the *Bluetooth pairing* is managed by the app, not through the phone operating system, that's why it is called "in-app pairing".

The advantages are the next:
1. An higher number of compatible Android phones.
2. Faster Communication.
3. More security in data transfer.

To take advantage of the in-app pairing it is necessary to:
- Update *Argo app* to version 2.0 or higher.
- Update devices' software to the new version, included in the app.

It is important to know that the previous version of *Argo* is not compatible to devices updated to the new software. While starting from *Argo 2.0* is always compatible, because it manages both, in-app pairing as well as pairing through the operating systems.
That's why it is strongly recommended to update all smartphone to *Argo 2.0,* or higher version, in order to avoid any kind of incompatibility

To know more about **software upgrade** to *Argo 2.0* and to get the step by step procedure, we recommend you to watch the tutorial "*Argo 2.0 Software Upgrade*" and read the related manual; both available at link: *https://app.iseo.com/?parm=ARGO&lang=en&folder=argo-update*

Appendix

In-app pairing improves security

In-app pairing improves security in data transfer. Thanks to the *Bluetooth* technology and the *in-app pairing* feature, it is possible to use the most advanced encryption security protocols, in terms of communication between the *Argo app*, through the Smartphone, and the doorlock. In more technical details *Argo* take advantages of the next important technologies:

- AES 128 secure Encryption over the air
- AES Session Keys generated with DHEC (Diffie Hellman Elliptic Curves)
- NIST (National Institute of Standard) compliant Random Number Generator

To explain the above points in a simple way, we can make an example, describing what happens during the communication between the smartphone and the doorlock, by the *Argo app*, when we open the door or we enter the *Programming Mode*.

The communication between the phone and the doorlock is always encrypted using the *AES128* (*Advanced Encryption Standard*) with a key of 128 bits. *AES* is nowadays one of the most difficult and complex protocol to decrypt. It is used to protect secret documents and informations by the major national governments, bodies and military forces. Just as an example, to decrypt the *AES 128 bits* protocol (2 powered to 128 possible combinations), trying all possible combinations (it's called "brute force attack"), all the computers in the world, running at the same time, at maximum performance, would need thousands of years, and a such amount of energy that nowadays would not be possible to provide.

In addition to that, the *AES 128* encryption key is a session key generated with the *Diffie-Hellman Elliptic Curves* algorithm (*DHEC*). This is a specific method of securely exchanging cryptographic keys over a public channel. Basically at every phone and doorlock communication, it is generated what is called an "AES session key", which is valid only for the time of this specific communication. When I end this communication, for example going out from *Programming Mode*, or after door has opened, this session key expires, and if I communicate again a new and different session key is generated, always by the *DHEC* algorithm. Thanks to this technology if someone is trying to "listen" (sniffing) the communication between the phone and doorlock, using some advanced tools (it's called "man in the middle attack"), he won't be able to understand it.

Furthermore the "AES session key" generated at every communication between phone and doorlock is random, and the "randomness" is defined by another algorithm, certified by one of the most competent authorities in the field: the *National Institute of Standard* (called *NIST*). Basically the *NIST* algorithm ensures that generation of random numbers is really random.

We can therefore conclude that, by *Argo app*, we can now offer the best technology available today, in terms of secure authetication in communications.

Appendix

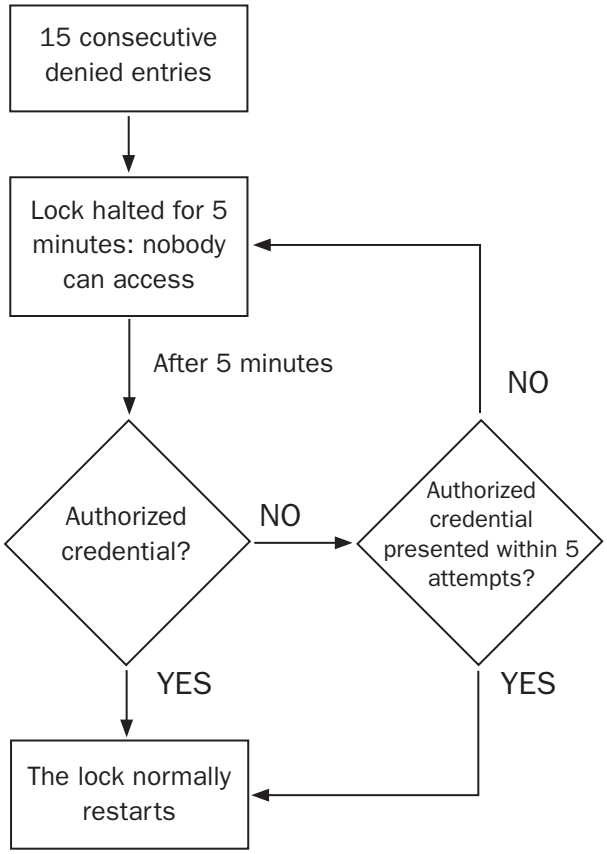
Penalty algorithm against brute force attack & Events protection

A *brute force attack* consists in systematically checking all possible codes performing an exhaustive code search. It might be possible to try all combinations in a relative short period of time (example 4 digit PIN).
The results of a *brute force attack* in a short period of time are:

- weakness of security;
- events erasure.

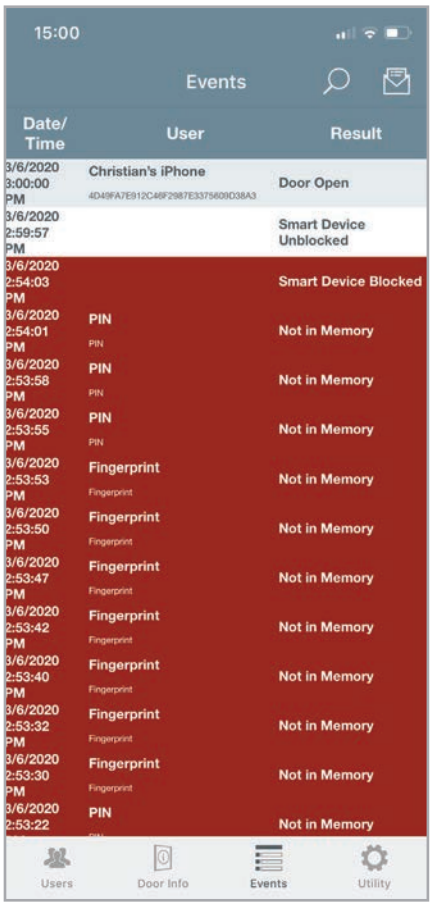
Argo takes advantage of a *penalty algorithm* against *brute force attacks* with the following characterstics and rules:

- after 15 consecutive denied entries like wrong pin codes or credentials reading (card, fingerprint, phone opening attempts), the lock halts for 5 minutes.
- During this period of time nobody can open the lock or enter *Programming Mode*, even the *System Admnistrator*, neither with Master card nor by phone login.
- After the 5 minutes of halting if a correct pin code is typed or an authorized credentialis presented, the lock normally restarts but, if a not correct pin code is typed or anauthorized credentialis presented for 5 additional consecutive times, the lock halts for another 5 minutes. And so on.
- With this kind of *penalty algorithm* the overall *brute force attack* time calculation per lock is 1 trial per minute, which leads to consider it as a good level of security. For example to discover a 4 characters pin code by *brute force attacks* procedure, considering 1 trial per minute for 10.000 possible combinations, almost 1 week is required trying for 24h per day.



Penalty algorithm against brute force attack & Events protection

The lock register the block condition in the event list. While lock blocked no events are recorded to prevent event erasure. To see the blocking condition, when the lock restarts after 5 minutes, enter *Programming Mode* and go to *Events*.



Smart Device Unblocked event: authorized entry, presented within 5 attempts, after the 5 min. of blocking condition.

Smart Device Blocked event.
While lock blocked no further events are recorded to prevent event erasure.

15 consecutive denied entries.

When the device is blocked nobody can access the device, even the *System Adminstrator*. This has been decided in order to let “no holes” in the security of the system. In a perfect “protected system” infact you cannot leave any “open possibility”: once the equipment is blocked the behaviour must be the same in all the circumstances and with all credentials type. If it was left the possibility to the *System Adminstrator* to access or if it had been considered this feature only valid for PIN code and not for cards, fingerprints or phones, “informatically” it would have been created a “breaking possibility”, also called “security hole”.

Troubleshooting

Argo app error messages

Error	Meaning	What to do
Phone not enabled: not in memory	The smartphone is not enabled to opening.	Enter Programming Mode by Master Card to enable the phone.
Connection error	The phone is not able to communicate to the device.	1) Switch OFF and ON the Bluetooth on your phone. 2) Enter Programming Mode by Master Card.
	Smartphone never memorized in the device.	Memorize the smartphone using the Master Card.
	The device has been updated to Argo 2.0 but not the phone.	Update Argo app to Argo 2.0 version to make the phone compatible to the new device's firmware.
	The device and the phone have been updated to Argo 2.0, but it has not be followed the right procedure.	Follow the right procedure as described in the manual *"Argo 2.0 upgrade procedure"*, available at *"app.iseo.com"* website: 1) Forget the device from the Bluetooth paired device list (only for iOS). 2) Quit the app. 3) Swith OFF and ON the Bluetooth or re-start your smartphone.
Operation error: too many invalid opening attempts. The next invalid attempts will not be recorded for 15 minutes.	Too many invalid attempts might quickly overwrite the Events Log. After 30 invalid attempts, the next are not recorded for 15 minutes.	Valid operations are immediately recorded and reset the count of invalid attempts.
Unknown error	Generic error.	1) Try to enter Programming Mode by Master Card. 2) Quit the app. 3) Switch OFF and ON your smartphone.
Link lost	The Access Control Device went out from Programming Mode due to inactivity timeout or other reasons (for example end of software upgrade).	It's not an issue. Enter again Programming Mode by Master Card if you need.

Argo app error messages

Error	Meaning	What to do
Download software failed	The download of the new software has been interrupted.	Repeat the procedure. The device is still working with previous software.
Lock clock not synchronized. Connect with Master Card to set the clock.	The clock inside the device is not synchronized with the phone. It may happen if device battery empty or phone with wrong date and time.	1) Check device battery status. Replace the battery if necessary. 2) Check the phone date and time if correct. 3) Enter Programming Mode to automatically synchronize the clock.
Quit the Argo app, then remove the device from the list of the Bluetooth paired devices and restart your smart-phone.	The device is paired to the phone via Bluetooth, but from Argo 2.0 this is not more necessary since there is the in-app pairing. Android phones usually does this operation automatically, while on iOS is required to do it manually.	Quit the Argo app and then remove the device from the list of the Bluetooth paired devices. At the end restart your smart-phone or switch OFF and ON the Bluetooth.
There is a new version of Argo available. Upgrade your Argo downloading it from the App Store or Google Play.	The phone by Argo, advise you that the device has inside a new software version, respect the one present in the phone's app. That means Argo in this phone is outdated.	Download and install on your phone the new Argo version, from the App Store or Google Play.
Device offline	**Stylos** cannot communicate with actuator. See also the specific error in the app events log.	Check the actuator connections and the exchange of coded keys procedure. See the video available at "*app.iseo.com*" website.
Opening denied	**x1R** cannot be opened since a wrong internal sensor state. For example if the internal handle is pressed during opening.	Check the specific error in the app events log. Check the internal handle if free and completely up.

Troubleshooting

Light and acoustic signals

n = *programmed opening time (default = 5sec.)*

Light & acoustic signal	Meaning	Notes / State
2 x 🟠 + **n x** 🟢	Opening device not initialized.	*NOT INITIALIZED*
3 x 🟢	Device initialization by Master Card.	*NOT INITIALIZED*
1 x + **2 x** 🟢	Enter Programming Mode.	*PROGRAMMING MODE*
3 x 🟠	Exit Programming Mode.	*PROGRAMMING MODE*
2 x 🟢	Added Card.	*PROGRAMMING MODE*
2 x 🔴	Card already present in the User List	*PROGRAMMING MODE*
	Device opening not allowed.	1. User not enabled 2. Block Standard User function enabled 3. Privacy function enabled (only Aries) 4. User expired 5. User not yet valid 6. Out of Time schedule
5 x 🔴 fast	Card not in memory.	Credential never memorized in the door.
3 x 🟠	Enable Passage Mode. Block Standard User.	
5 x 🟠	Disable Passage Mode. Unlock Standard User.	
1 x 🟢	Card enabled but door in Passage Mode.	
3 x 🟠 + **n x** 🟢	Battery low.	During opening time.
3 x 🔴 + **n x** 🟢	Battery very low.	Before opening time (delayed opening).
🔴 **x 3 sec**	Battery empty.	No opening.

Technical assistance

For any help please contact *ISEOZero1 Technical Support*. You can find your country telephone number at: *http://iseozero1.com/iseozero1/index.html#contacts*.

When you contact the *ISEOZero1 Technical Support,* please provide the next information:

- A*rgo app* software version.
- *Smartphone* model and software version.
- *Access control device*, involved in the issue, product code and software version.
- Precise description of the issue.

ISEO Zero1
ELECTRONIC SOLUTIONS

ITALY
Via Don Fasola 4
I-22069 Rovellasca (CO)
iseozero1@iseo.com
+39
800-728722
ELECTRONIC SUPPORT SERVICE

GERMANY
ISEO Deutschland GmbH
zero1-de@iseo.com
0700-00473601
ELECTRONIC SUPPORT SERVICE

FRANCE
ISEO France s.a.s.
zero1-fr@iseo.com
+33 1 64835858

SPAIN
Cerraduras Iseo Ibérica S.L.
zero1-es@iseo.com
900-126356
ELECTRONIC SUPPORT SERVICE

ASIA
ISEO Asia Pacific SDN. BHD.
zero1-asia@iseo.com
+603 80753331

ISEO Beijing
zero1-cn@iseo.com
+8610 58698079

UNITED ARAB EMIRATES
Iseo Projects and Access Control DMCC
iseoprojects@iseo.com
+971 4 5136162

SOUTH AFRICA
ISEO South Africa (Pty) LTD
zero1-za@iseo.com

ROMANIA
Feroneria Prod S.A.
zero1-ro@iseo.com

ISEO
www.iseo.com

Iseo Serrature s.p.a.
Via San Girolamo 13
25055 Pisogne (BS)
ITALY
iseo@iseo.com

EC Declarations of conformity available at:
https://www.iseo.com/it/en/download