

ARGO
USER MANUAL



ISEO[®]
ULTIMATE ACCESS TECHNOLOGIES

About this manual

ARGO 3.5 - April 2025

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* Access control devices, Smart series.

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

www.iseo.com

Notices

- Please read this manual before using *Argo* to ensure 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.

About this manual

How to use this manual

Table of Contents

About this manual

- 3 Notices
- 3 Information icons
- 4 Information on copyright
- 4 Trademarks
- 4 Keywords

Overview

- 6 What's Argo
- 7 Requirements
- 8 Access control devices
- 9 Master Cards set
- 10 Credentials

Getting started

- 12 What you need
- 13 Initialization of the Access control device
- 14 Start Argo
- 15 Enter Programming mode
- 16 Add the smartphone as credential to open the door
- 17 Change the door name
- 18 Open the door

Advanced


- 37 User type and functions
- 38 Card user parameters
- 39 Smartphone user parameters
- 40 Users list overview
- 41 Time Control
- 45 Tap & Hold menu
- 46 Enable passage mode
- 47 Block standard user
- 48 Change PIN code
- 49 Enable passage mode without Argo app
- 50 Block standard user without Argo app
- 51 Scheduled Passage Mode
- 58 x1R Smart: Light Mode
- 61 Battery Levels
- 62 Copy users
- 63 Transfer users
- 65 Software upgrade
- 66 Dump Information
- 67 Bluetooth parameters
- 69 Reset
- 70 Updating of Master Card level
- 70 Master Cards set replacement and updating of

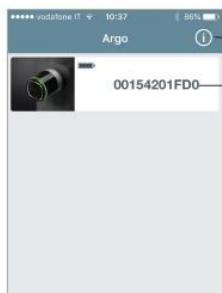
In the *Table of Contents*, click on the argument or page number, to directly go to the related paragraph or chapter.

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.



Info app menu

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

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

Information on copyright

- No part of this guide may be reproduced, distributed, translated, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or storing in any information storage and retrieval system, without the prior written permission of ISEO.
- ISEO reserves the right to change the specifications of the hardware and software described in this manual at any time and without prior notice.
- ISEO will not be held liable for any damages resulting from the use of this product.

Trademarks

- The Apple logo, Apple™, iPhone™, iPad™ and App Store™ are trademarks of APPLE Inc.
- The Android logo, Google™, YouTube™, Google Play™ Store are trademarks of Google Inc.
- Bluetooth® is a registered trademark of Bluetooth® SIG, Inc. worldwide.
- IOS is a trademark or registered trademark of Cisco in the U.S. and other countries.
- MIFARE® is a registered Trademark of NXP B. V.
- All other trademarks and copyrights are the property of their respective owners.

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.

Table of Contents

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 latest 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 addition 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

Sommario

About this manual 3

Notices	3
Information icons	3
How to use this manual	4
Information on copyright	5
Trademarks	5
Keywords	5
Keywords	6

Overview 11

What's Argo	11
Requirements	12
Access control devices	13
Master Cards set	15
Credentials	16

Getting Started 18

What you need	18
Initialization of the Access control device	19
Start Argo	20
Enter programming mode	21
Add the smartphone as credential to open the door	22
Change the door name	24
Open the door	25

Basics 26

Users menu	26
Add users	27
Add PIN users	28

Table of Contents

Add users typing ISEO card number	29
Add users without Argo app	37
Add PIN code without Argo app	38
How to pair 1NCA Reader Cable Free	39
Delete users	42
Delete users without Argo app	44
Read Events	45
Door info	46
Default User Settings	47
Versions	48
Advanced settings	49

Argo from Remote 50

Principle of working	50
Smart Gateway	51
Smart Gateway models	52
Smart Gateway technical data	53
Bluetooth 5.0 ISEO Smart Devices	54
New aesthetic logo	54
Create your Argo Account	56
Login to the Argo Account	61
Configure the Smart Gateway	62
Add locks to the system (Master Card required)	67
Connect to the lock from remote	71
Argo from Remote menu overview	77
Delete the Account	93
Questions & Answers	96
Troubleshooting	101

Advanced 107

Card user parameters	107
----------------------	-----

Table of Contents

Phone user parameters	108
Administrator Login without Master Card	109
User List overview	110
Time Control	111
Validity from First Use	115
Tap & Hold menu	124
Enable Passage Mode	125
Block Standard Users	126
Login (without Master Card)	127
Change the PIN code	128
Enable Passage Mode without Argo app	129
Block Standard User without Argo app	130
Argo for Apple Watch	149
Widgets for Argo app	156
Add phone with Argo UID	163
Passage mode with PIN code	168
Passage mode capability	170
Door status advice	172
Smart Relay	173
Fingerprint reader	187
Mifare DESFire cards	202
Siri Shortcuts voice commands to open (iOS only)	204
Service	211
Battery levels	211
Copy users	212
Transfer users	213
Software Upgrade	215
Dump Information	216
Bluetooth® parameters	217
Reset	219

Table of Contents

Updating of Master Card level	220
Master Card Set replacement and updating of System Code	220
Events log messages	221
Android Argo app uninstalls	225
Backup and Restore user list	227

Appendix 235

Operations summary without Argo app	235
Technical data summary table	236
In-app pairing	237
In-app pairing improves security	238
Penalty algorithm against brute force attack & Events protection	239

Troubleshooting 241

Argo app error messages	241
Argo app error messages	242
Technical assistance	244

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 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.).

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

300 USERS



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

1000 EVENTS



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*

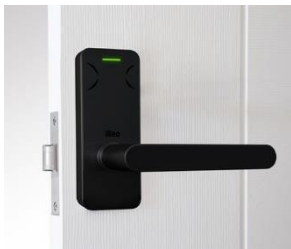
Access control devices

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



Libra Smart

Electronic European profile cylinder of ISEO 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.



MA1A Smart

MA1A Smart is the new electronic lock of the ISEO Connected products range which allows to manage the access with simplicity in residential, "light commercial" environments, B&B. MA1A with its compact and stylish design is an excellence of Made in Italy and represents the perfect retrofit solution for internal doors.



Aries Smart

Electronic trim set of ISEO 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...).



1NCA Smart

1NCA Smart Readers is an innovative range of multi-standard, wall-mounted and weatherproof readers of ISEO Connected products line, designed for access management in residential and light commercial buildings. These readers can be easily installed and can manage internal doors but also outdoor gates since they have the IP66 certification.

Overview



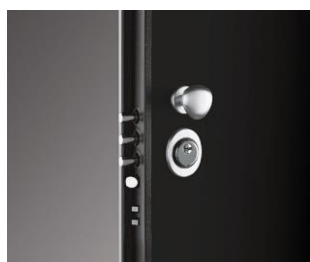
Stylos Smart Readers

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



Multiblindo Smart

The new ISEO self-closing motorized lock is the perfect combination of comfort of use and safety in all situations. The great innovation of Multiblindo Smart is the possibility of choosing between different configurations, completely battery powered, or mains powered, with or without backup battery, to be used in the event of an electrical blackout.



x1R Smart

Electronic motorized lock for armored doors of ISEO 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 closes a contact if a smartphone is registered in the device.



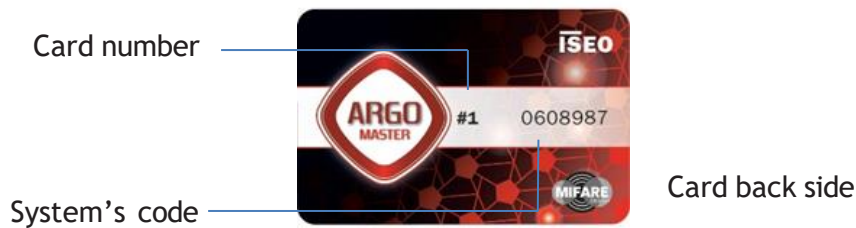
To simplify the reading of this manual, pictures and descriptions are mainly referred to **Libra Smart**. The same informations are also applicable to the other *Smart series* devices. Any differences will be properly specified.

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

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)

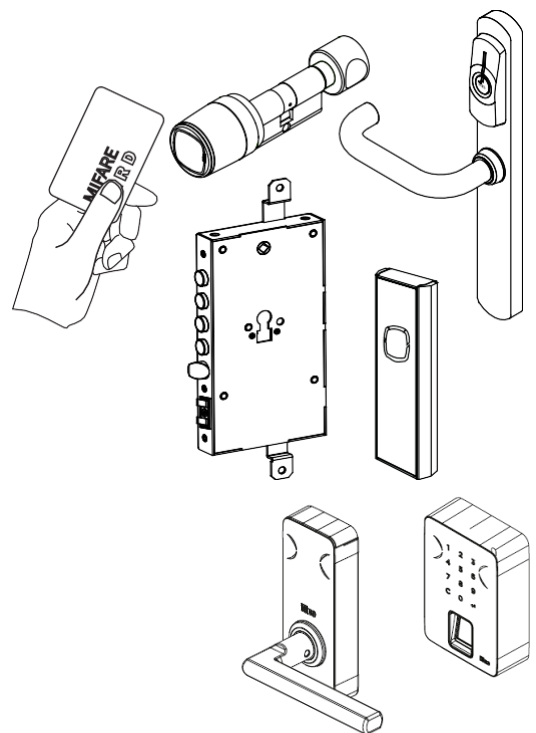


Tags



Mifare cards
Mifare DESFire (UID reading only)

Used to “activate” the device.



Mifare is a brand of contactless card with several card types: Classic, Ultralight, DESFire... All Mifare cards work 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

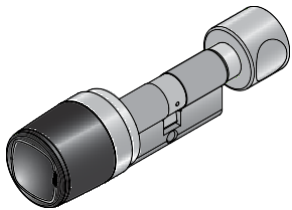
ISEO Cards is a particular Mifare Card (1K), specifically developed by Iseo, with an encrypted UID. This allows an higher level of security in the trasmission between the card and the doorlock.

As result of the above notes

To obtain the best security, ISEO recommends to use the Argo app for phone, 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.

Getting Started

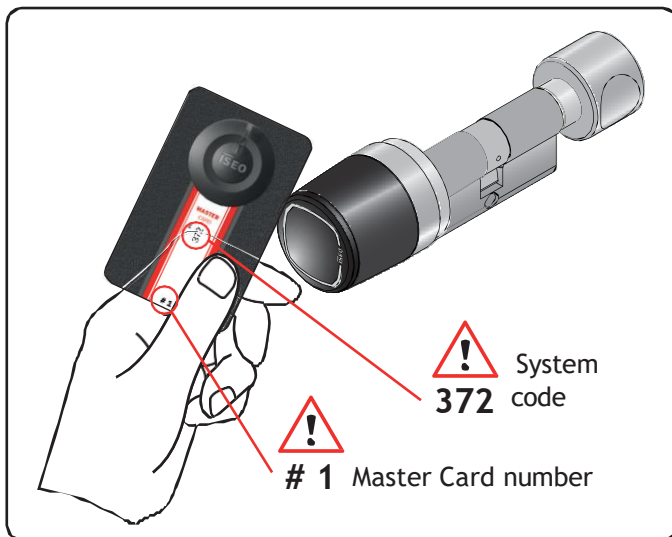
Initialization of the Access control device

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

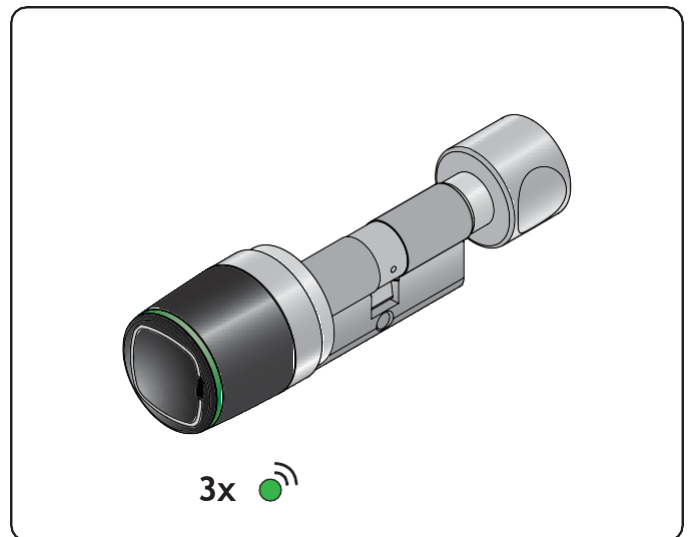


A *Factory mode* configured device can be opened by any Mifare card or tag. The orange light flashes 2 times, before the standard opening signal, to show the device not initialized.

The system initialization takes 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.

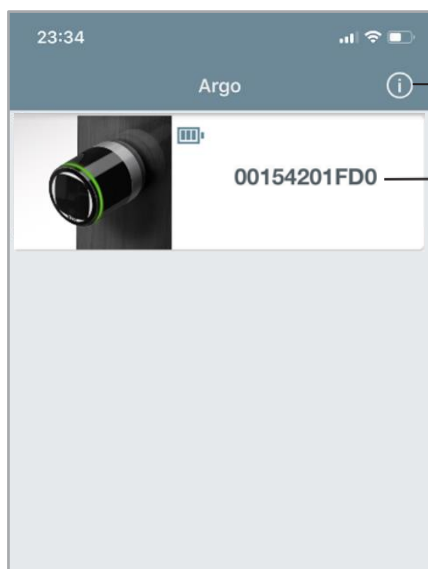
Getting Started

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.



Info app menu

Available *Access control device* up to 10mt.



Info app menu

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

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

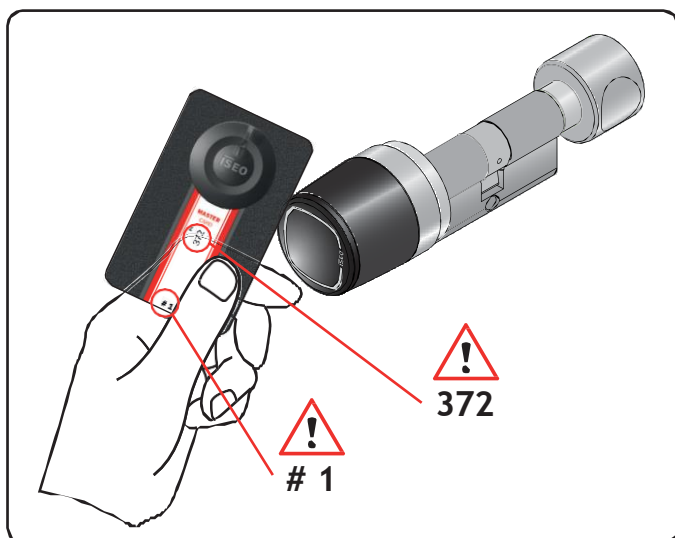
To change the app's language.

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

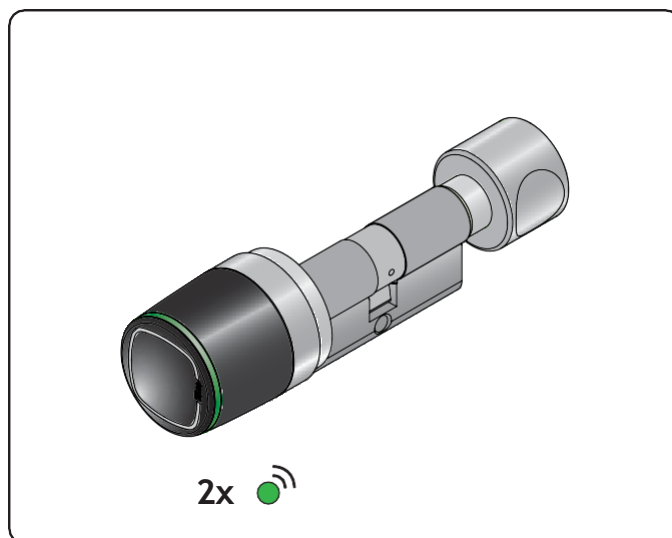
Enter programming mode

This is the procedure applicable to all RFID devices equipped with Master cards. The procedure dedicated to the Multiblindo Smart lock is described on the following page.

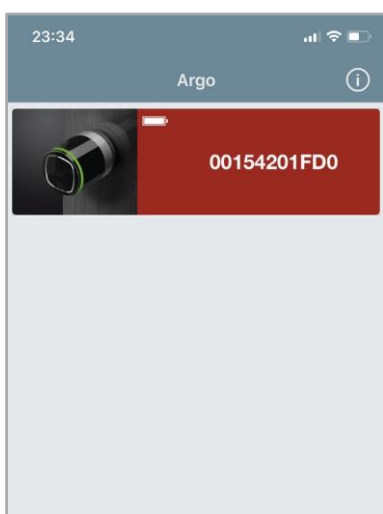
Present the **Master Card 1** to the device: the button in the app will turn red, and pressing it you will enter in **Programming mode**.



1. Present 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.

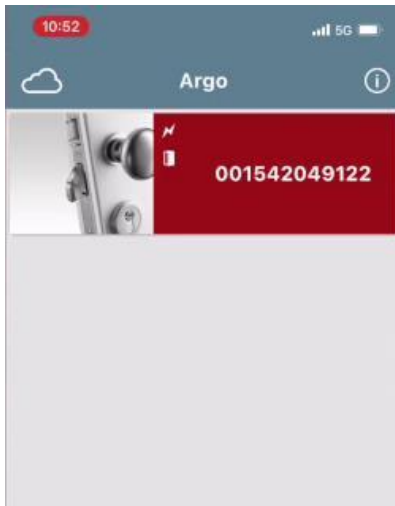
Getting Started

For the **Multiblindo Smart** lock, the "Programming Mode" procedure is carried out using the cylinder and mechanical key, as it does not come with an onboard RFID, making it impossible to use Master cards. Naturally, if positioned on the outside of the door, the cylinder can also be used for emergency mechanical opening.

Starting from a configuration with the door closed, perform the following actions:

- 1) Open the lock with the key and move the door so that the door status sensor detects the opening.
- 2) Close the door so that the door status sensor detects the closing.
- 3) Open the lock a second time with the key and move the door so that the door status sensor detects the opening.

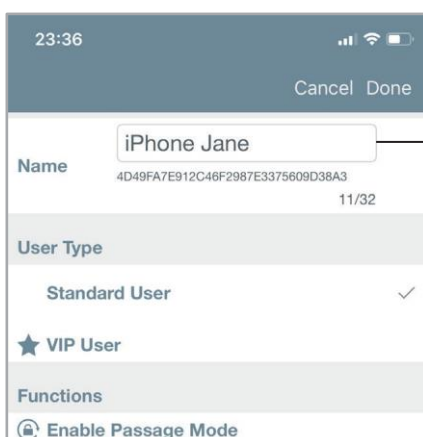
The button in the app will turn red and pressing it you will enter in Programming mode.



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

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.

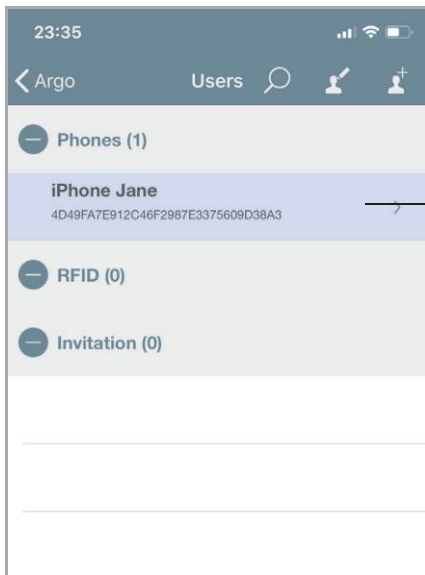


1. Change the name of your phone.
2. Tap **Done** to memorize your phone as opening Credential.

Getting Started

3. Tap **Cancel** if you decide to not memorize your phone now.

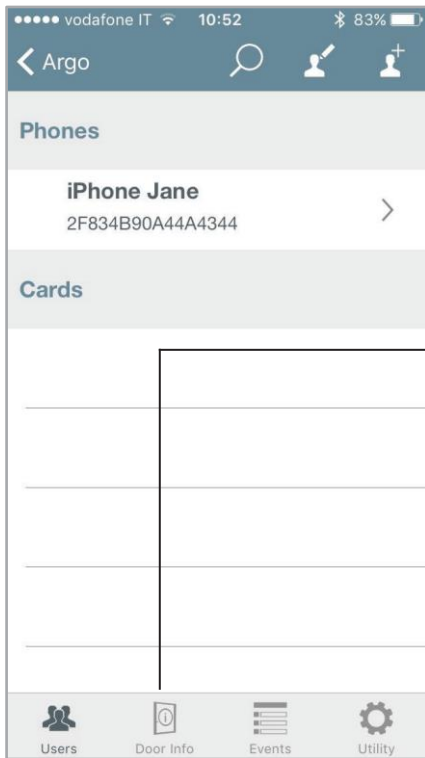
4. Enable **Login** if the user is also the *System Administrator* (to know more about Login go to *Advanced, Administrator login without Master Card and Login (without Master Card)*).



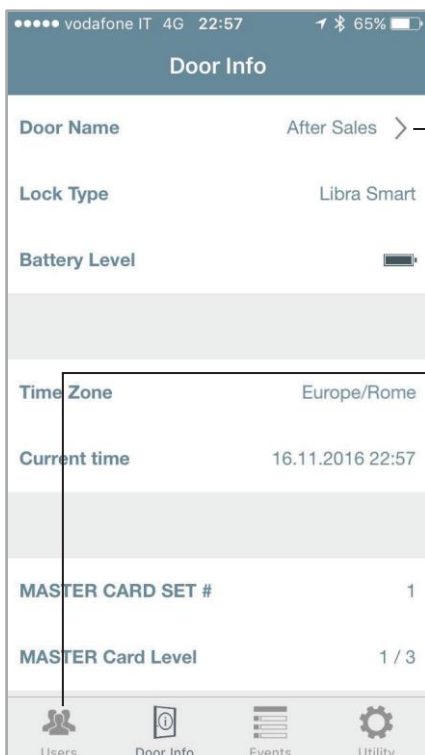
5. You can see your phone appearing in the *Users list*.

Getting Started

Change the door name



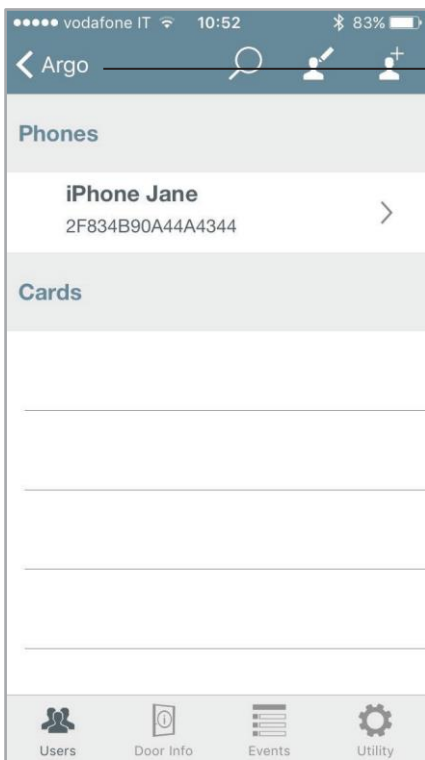
1. Tap **Door Info** and then **Door Name** to give a real door name to the lock.



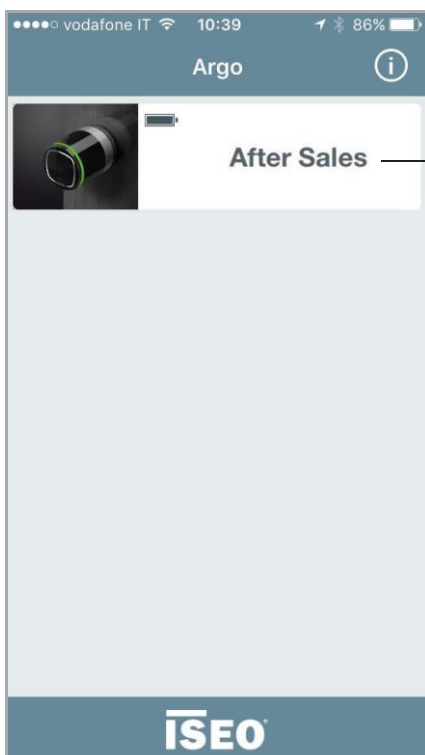
2. Change the name and confirm.
3. Tap **Users** to go back to the main menu.

Getting Started

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 another menu by pressing the icons in the bottom bar. To exit *Programming mode*, you need to go back to main menu first.



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

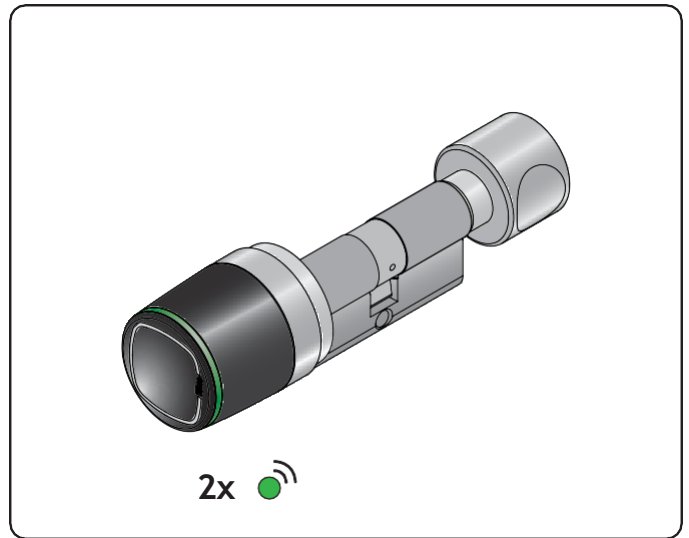
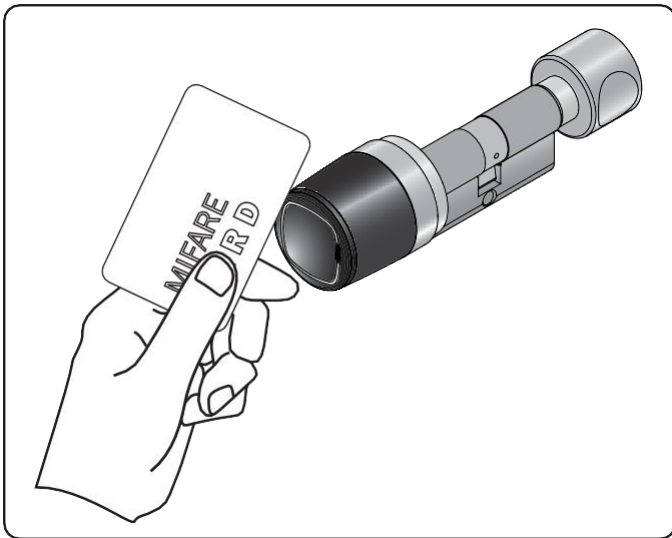
Basics

Add users



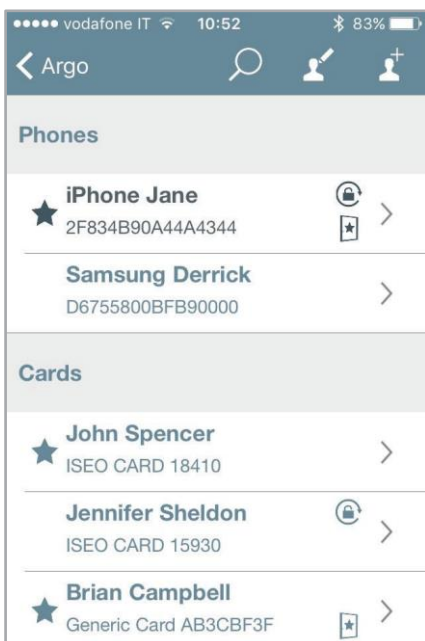
Enter **Programming mode** first. You can then add users just by presenting the credentials to the device, and those will be displayed in the smartphone.

The 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.



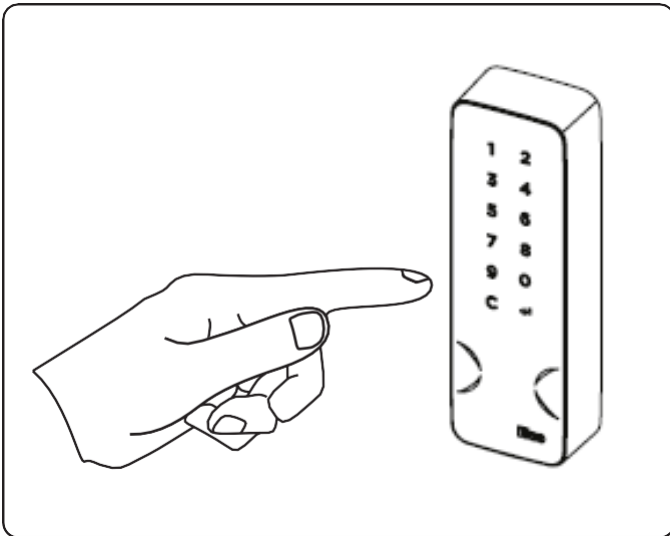
Added Cards

Add PIN users



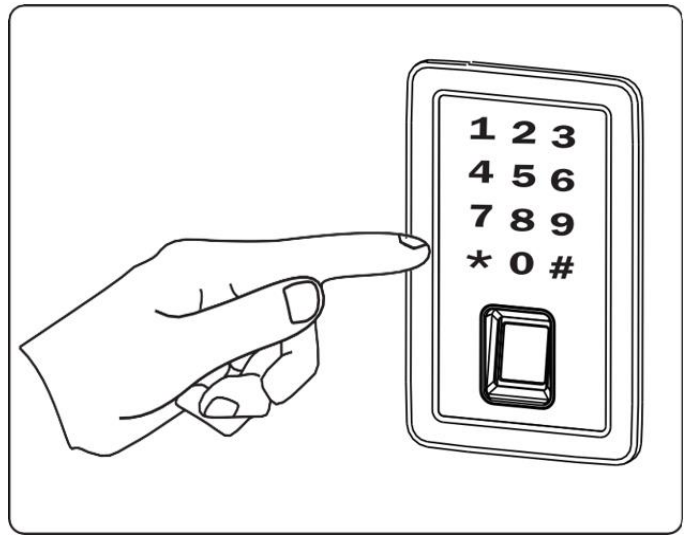
On 1NCA Smart Readers, *Stylos Smart Display* and *x1R Smart*, you can also add a *PIN code* as credential to open, using the keyboard available on both devices. Enter *Programming mode* first. You can then add the PIN just entering the code in the keyboard. Last PIN will be on top of the list.

1NCA SMART MULLION KEYBOARD

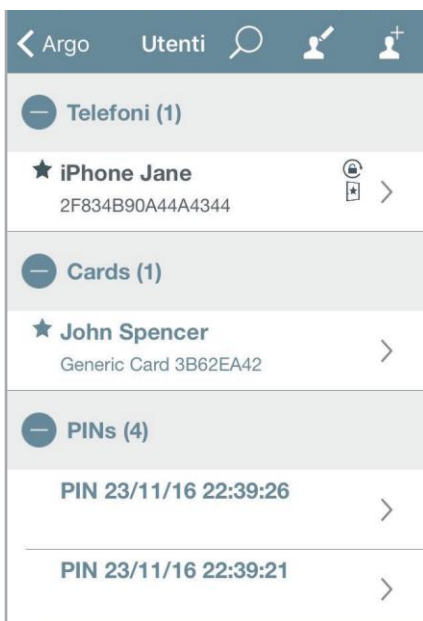


Enter your PIN code, from 4 to 14 characters, and confirm by enter ↵. Press **C** to clear all the numeric code.

x1R SMART MULTI-READER



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.

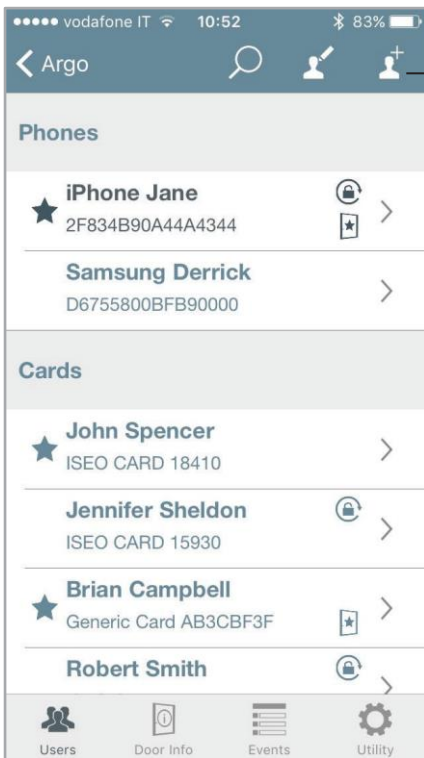


For security reasons PIN codes are never visible in the Argo app: neither in the *Users list*, nor in the *historical Events*, nor in the *Dump Information* (see *Dump Information* specific paragraph).

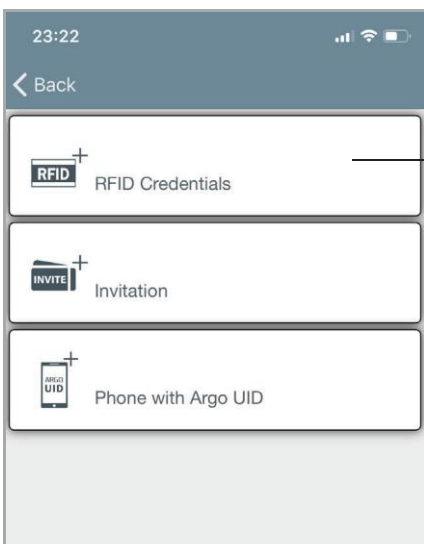
Add users typing ISEO card number



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

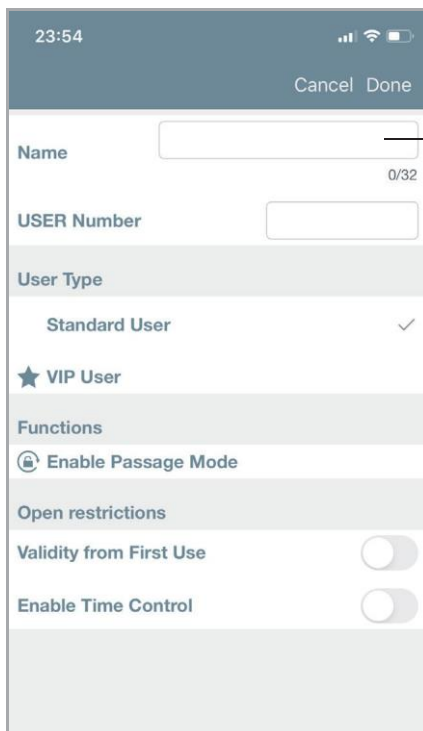


2. Tap **RFID Credentials**

Basics

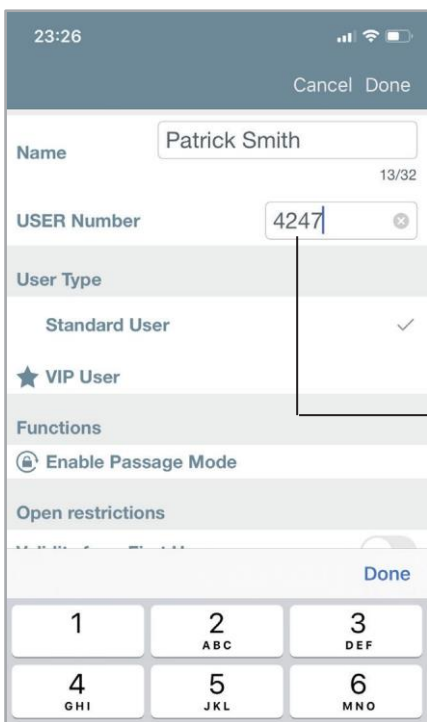


3. Choose **USER DESFire** or **USER Classic**. Both are ISEO cards: the first is related to *Mifare DESFire*, while the second to *Mifare Classic*. To know more about *Mifare DESFire* go to *Advanced* then *Mifare DESFire* cards.



4. Tap Name box

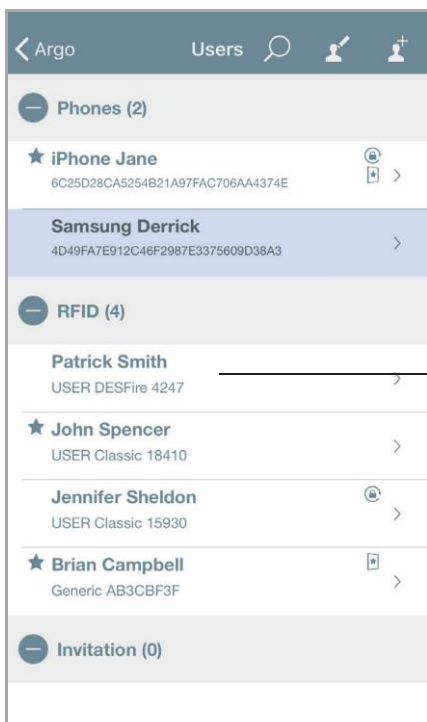
Basics



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



6. Tap Done to confirm the operation.



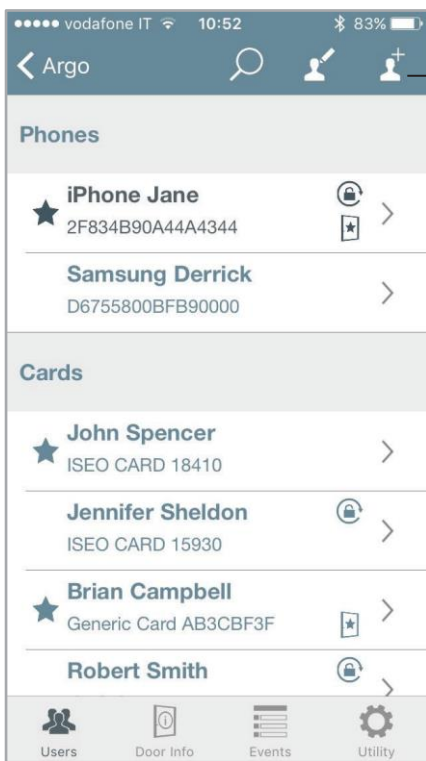
7. The ISEO card is added to the *Users list*.



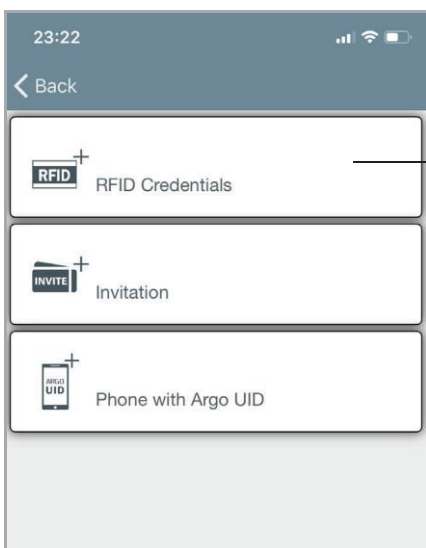
This function is only available using ISEO cards and tags.

Basics

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.

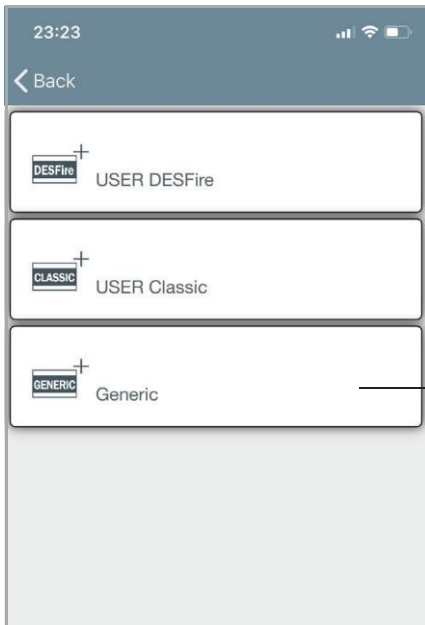


1. Tap the *add user* icon

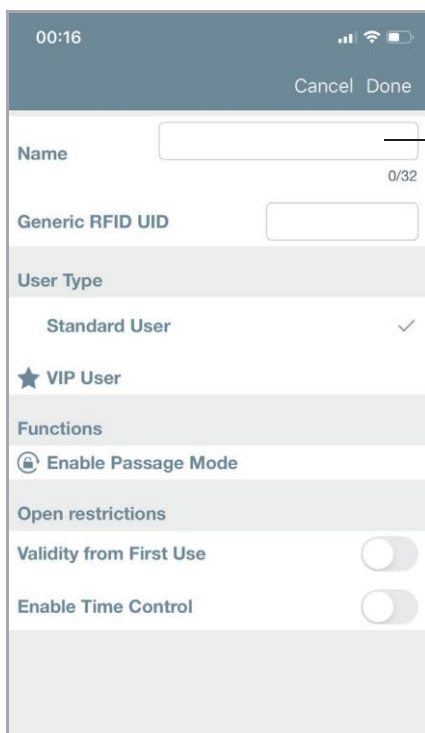


2. Tap **RFID Credentials**

Basics

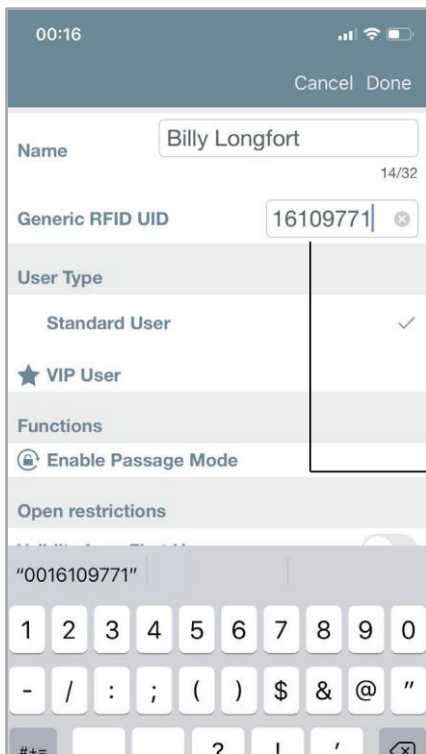


3. Tap **Generic**

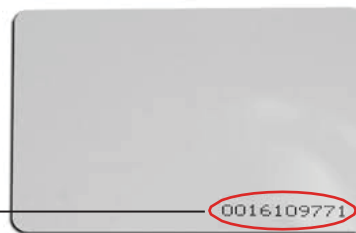


4. Tap **Name** box

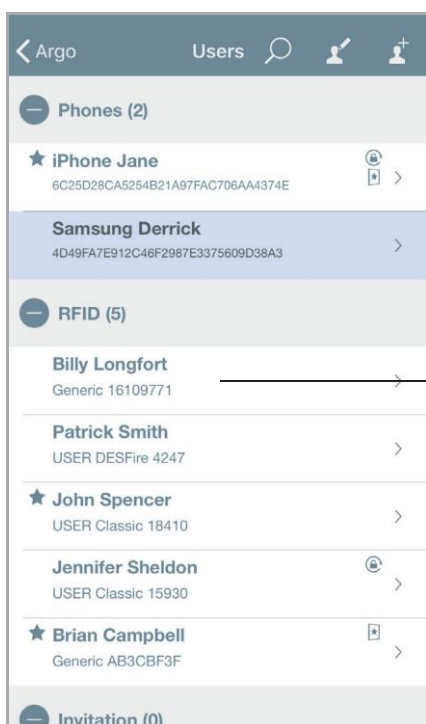
Basics



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



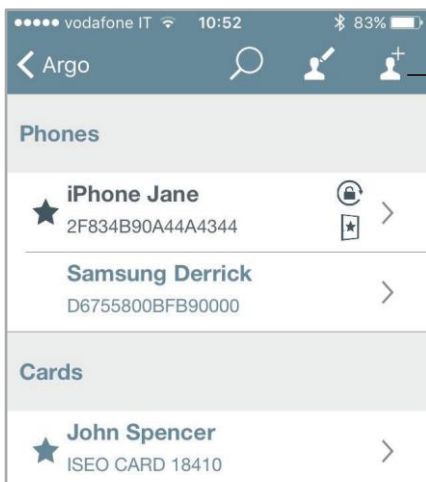
6. Tap **Done** to confirm the operation.



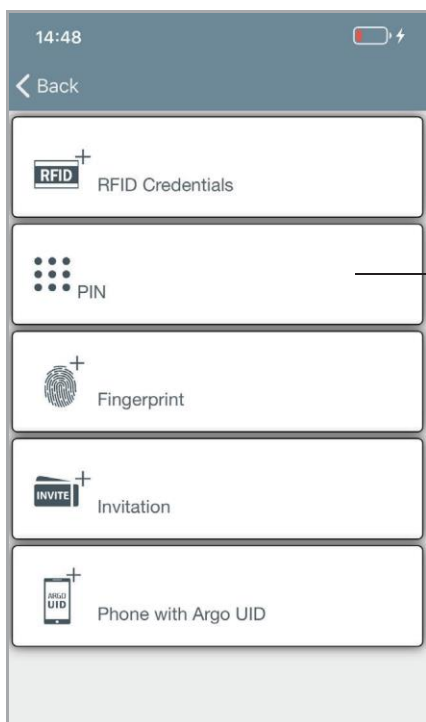
7. The *Mifare card* is added to the *Users list*.

Basics

On 1NCA Smart Readers, *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**

Basics

16/32

4/14

4/14

User Type		
1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
0		

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.

Phones (2)

★ iPhone Jane
2F834B90A44A4344

Samsung Derrick
FAD7D70071CF0000

Cards (1)

★ John Spencer
Generic Card 3B62EA42

PINs (1)

John Smith's PIN

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

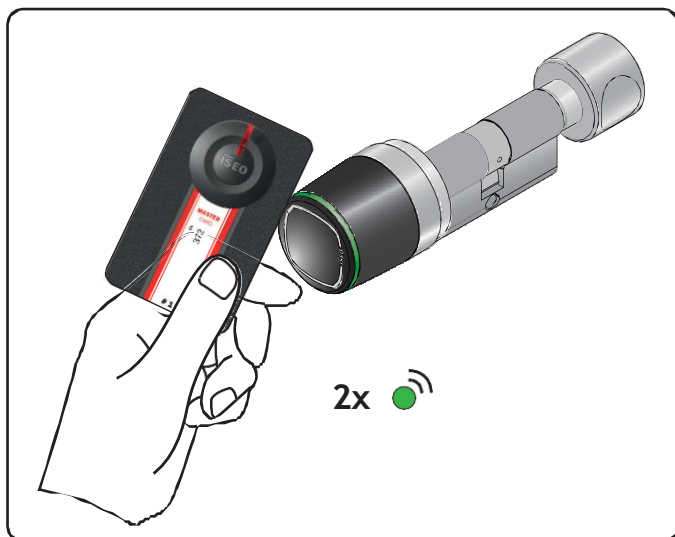


For security reasons, the *PIN* is never visible, neither in the *Users list*, nor in the historical *Events*, nor in the *Dump Information*.

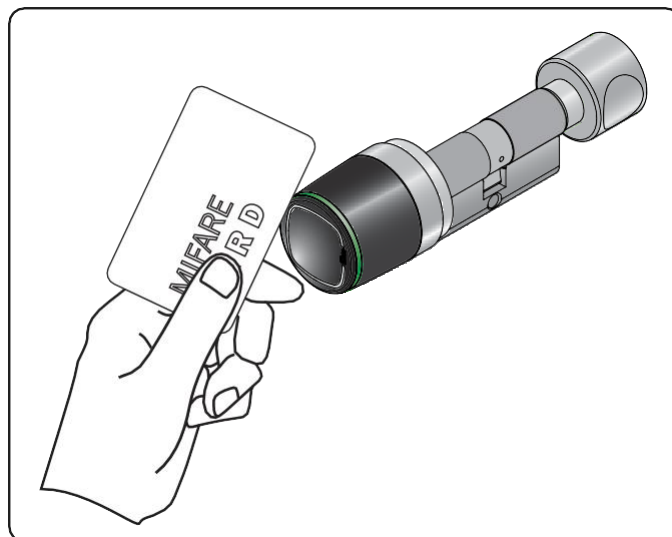


This function is only available on *x1R Smart*, *1NCA Smart Readers* and *Stylos Smart Display*.

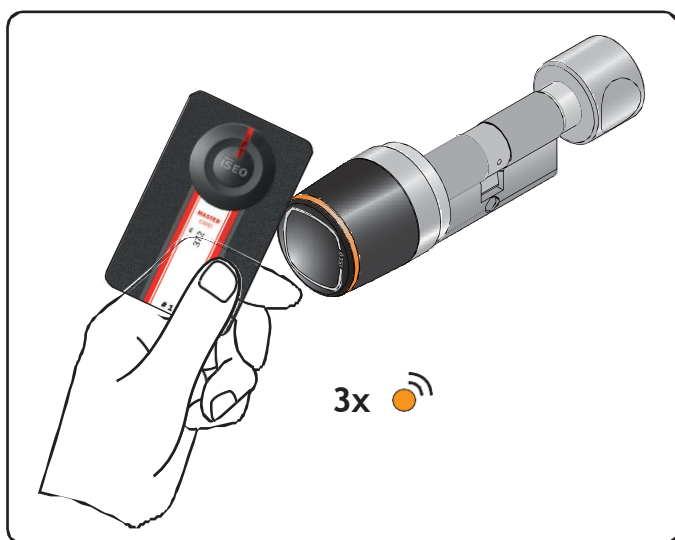
Add users without Argo app



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*.

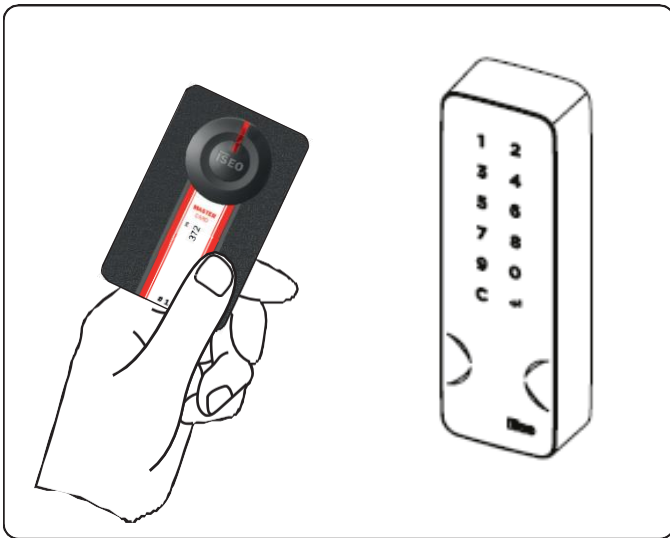


The device goes automatically out of *Programming mode* after 5min. of inactivity.

Basics

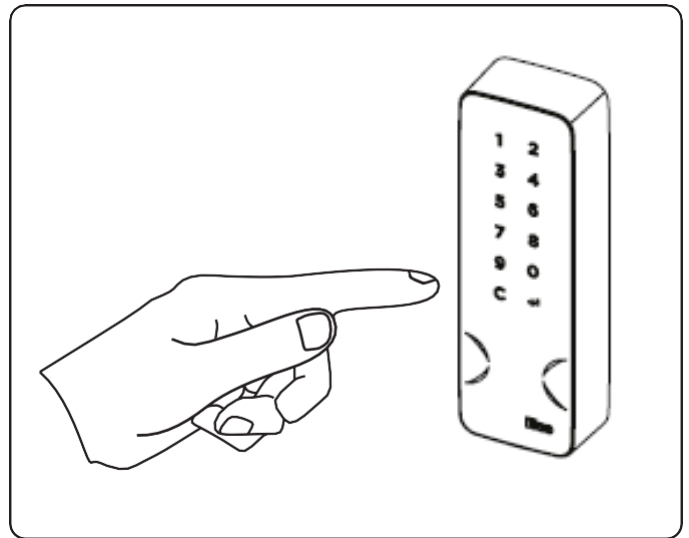
Add PIN code without Argo app

On *1NCA Smart Readers*, *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 *1NCA Smart Reader*, but the procedure is the same for *Stylos* and *x1R Accessories* as well.



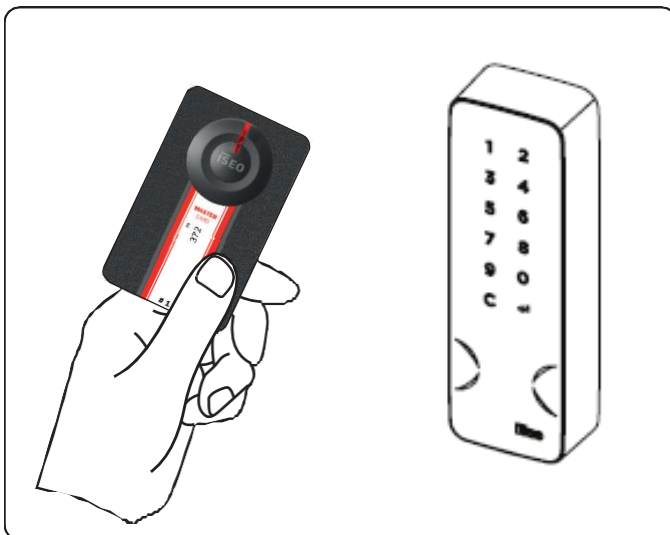
1. Present the **Master Card 1** to the device to enter **Programming mode**.

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**.



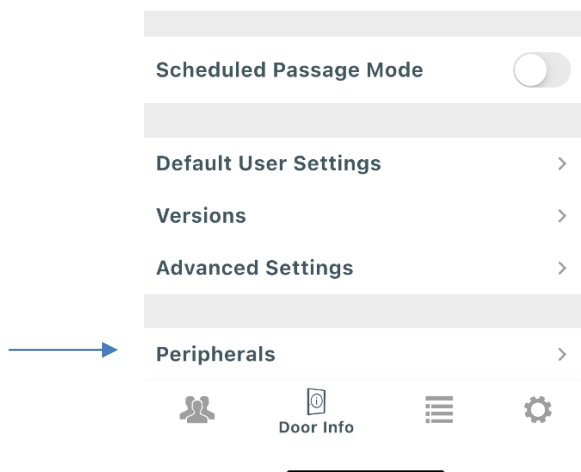
The PIN code must be from minimum 4 to maximum 14 characters.

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

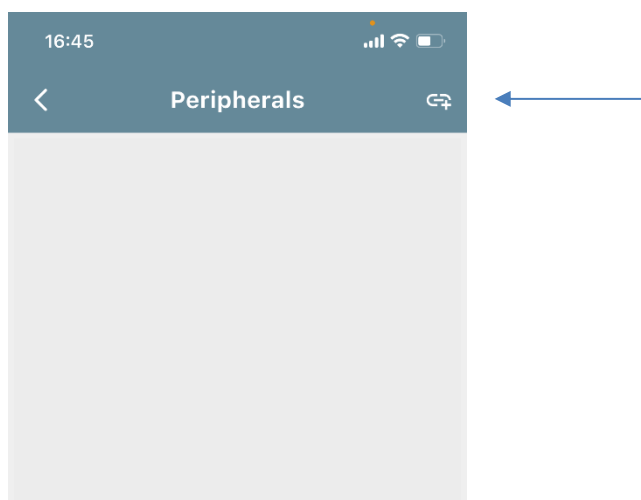
How to pair 1NCA Reader Cable Free

1NCA Readers Cable Free can be paired with an ISEO product from the Connected range to expand opening possibilities. To do this, it is necessary to use the pairing procedure with a Cable Free reader, available for all ISEO Argo platform products. Just follow a few simple steps:

- 1) Enter in the programming mode of the Argo device you wish to pair with the Cable Free reader.
- 2) Go to the Door Info screen, scroll down, and select Peripherals.

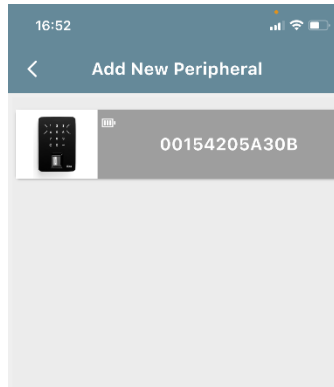


- 3) In the Peripherals screen, click the icon at the top right to add a new peripheral.

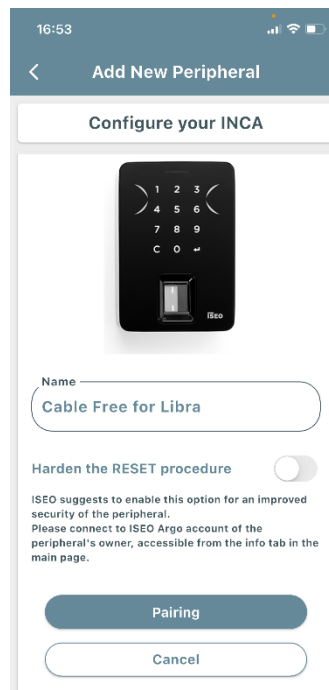


Basics

4) If the 1NCA Reader Cable Free is properly powered and within the Bluetooth signal range of the phone, it will be automatically detected and will appear on the screen as shown in the figure.

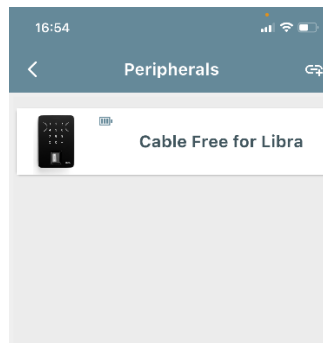


5) By clicking on the device icon, you can access the configuration page, where it's possible to assign a name to the device. To validate the peripheral, press the Pairing button.

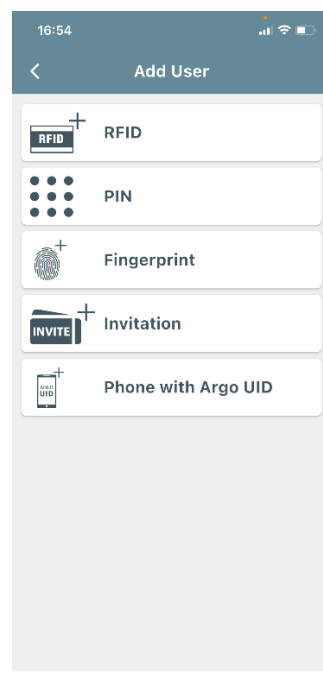


Basics

6) At this point, the 1NCA Cable Free device is initialized and paired with the corresponding ARGO device (in this case, the LIBRA electronic cylinder).



7) At this point, by entering the credential configuration menu (of the Libra, for example), it will be possible to select all the credentials included in the paired 1NCA Cable Free device, increasing the capabilities offered by the ARGO device.



Basics

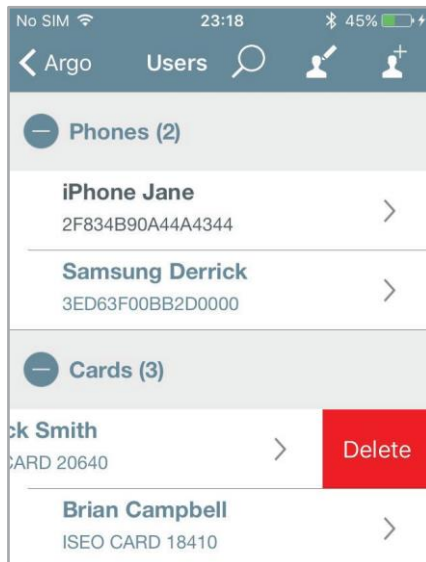
Delete users



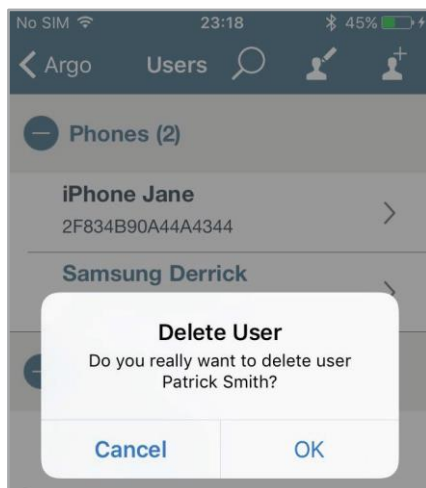
There are two ways to delete users from the user list:

- 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.



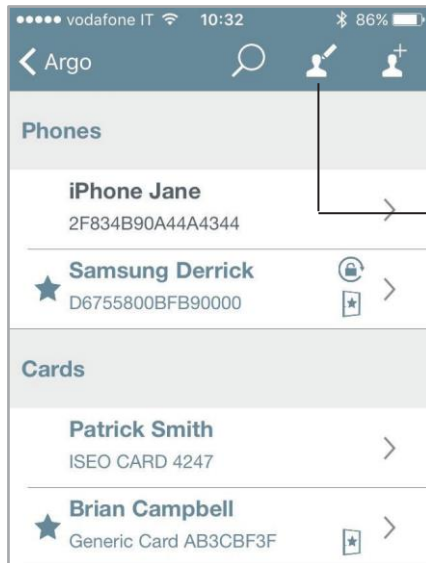
2. Confirm the operation.



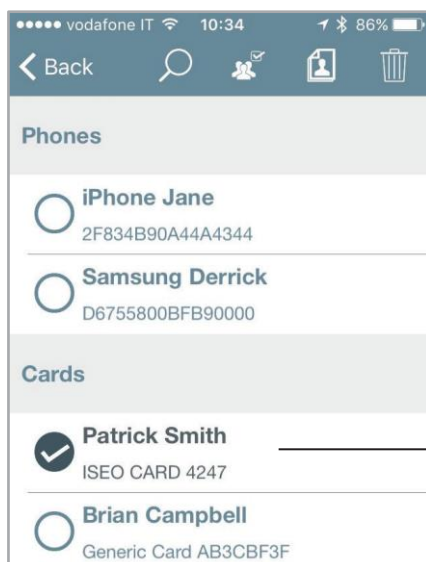
On Android phones, at the place of the swipe action, you need to tap and hold on the user.

Basics

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

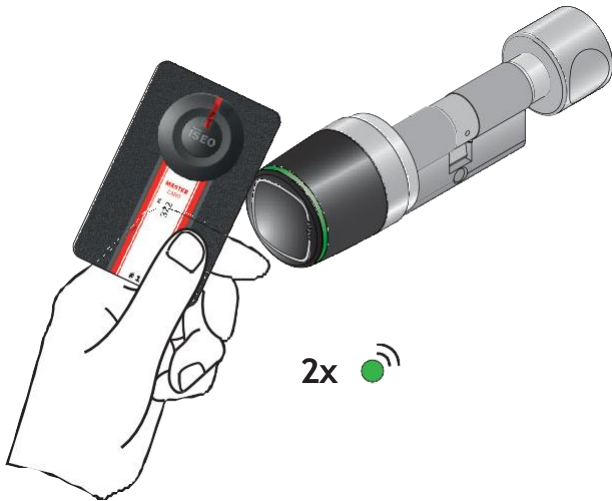


3. Tap the *trash bin* icon to confirm the operation.

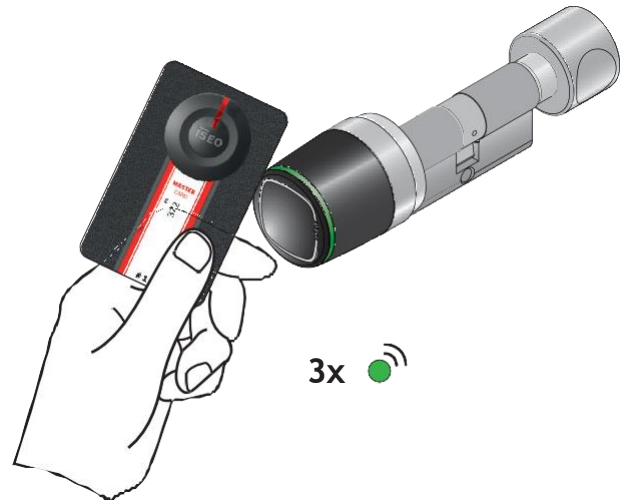


You can also search the users to delete by the *Lens* tool.

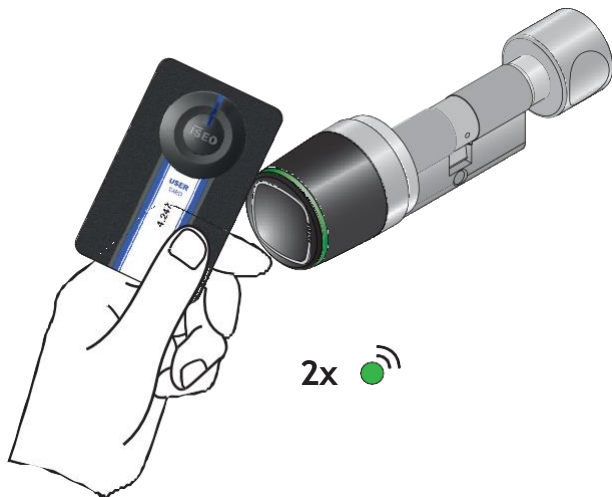
Delete users without Argo app



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.

Read Events



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

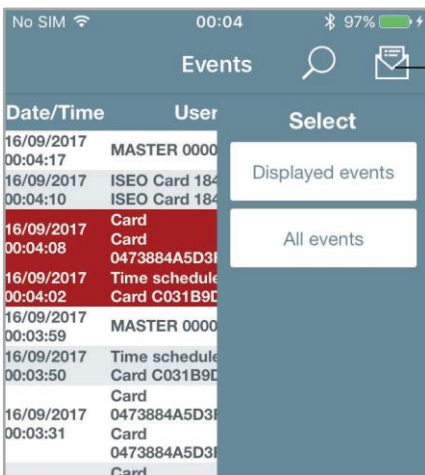
The last 1000 events are stored in the lock. The events are loaded from the most recent, and scrolling down allows you to automatically load new events.



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:

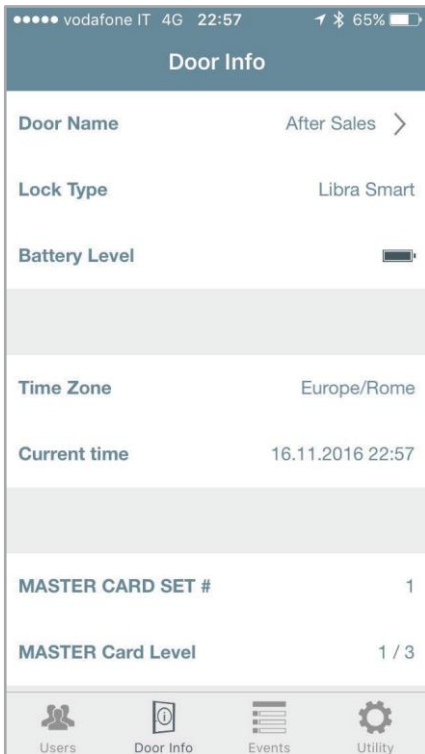
- **Displayed events**: the events loaded by “manual scrolling”, or filtered in the search box.
- **All events**: all the lock events (max 1000 events).

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

Door info



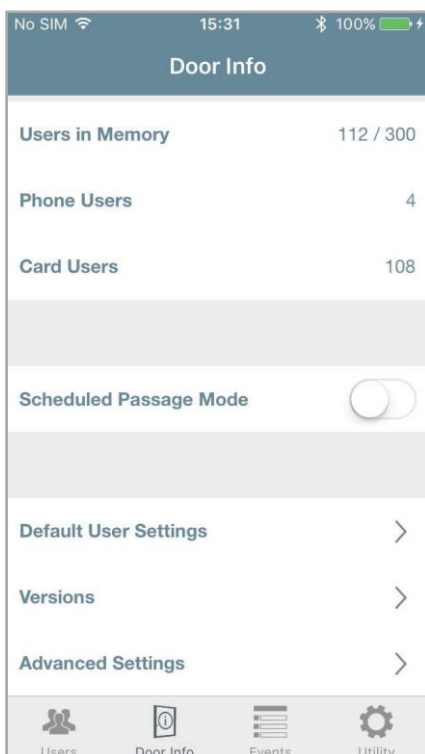
In this menu you can change the **door name** and you can find many information about the device configuration, as showed in the picture below.



Tap to change the **Door name**.

Check battery level.

Other available info.



Other available info.

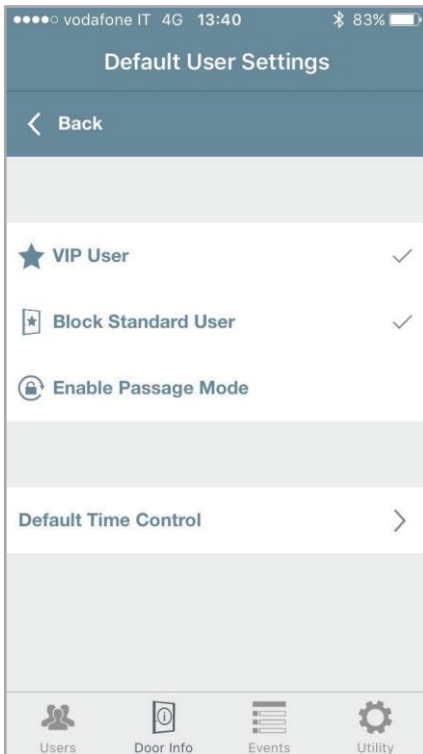
To know more about this function see the related chapter in the Advanced section.

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

Default User Settings



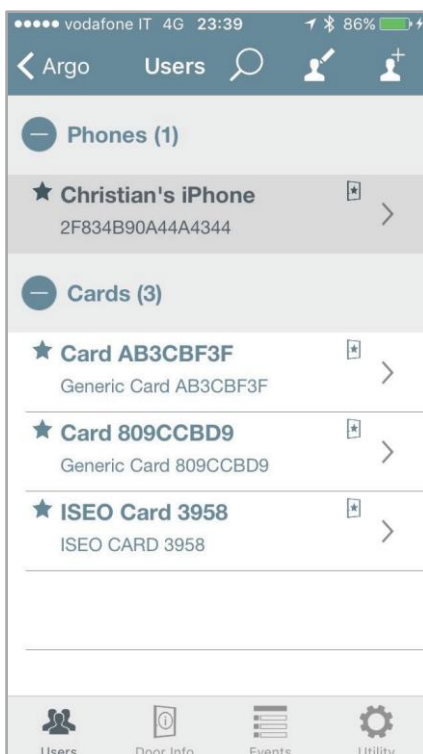
In this menu you can set *User Type* and *Functions* as default. That means the selected functions will be automatically added to each new memorized credential (user).



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.



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

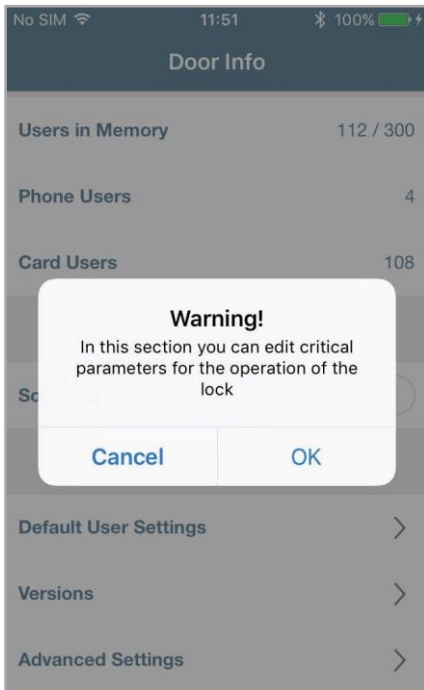


Look at the *Main Board Software version*. This is the version that you can update by the *software upgrade procedure*, described in the next pages.

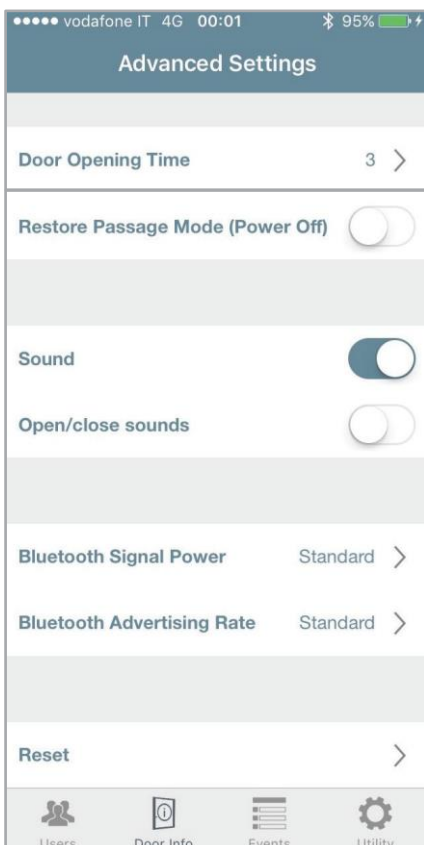
Advanced settings



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.

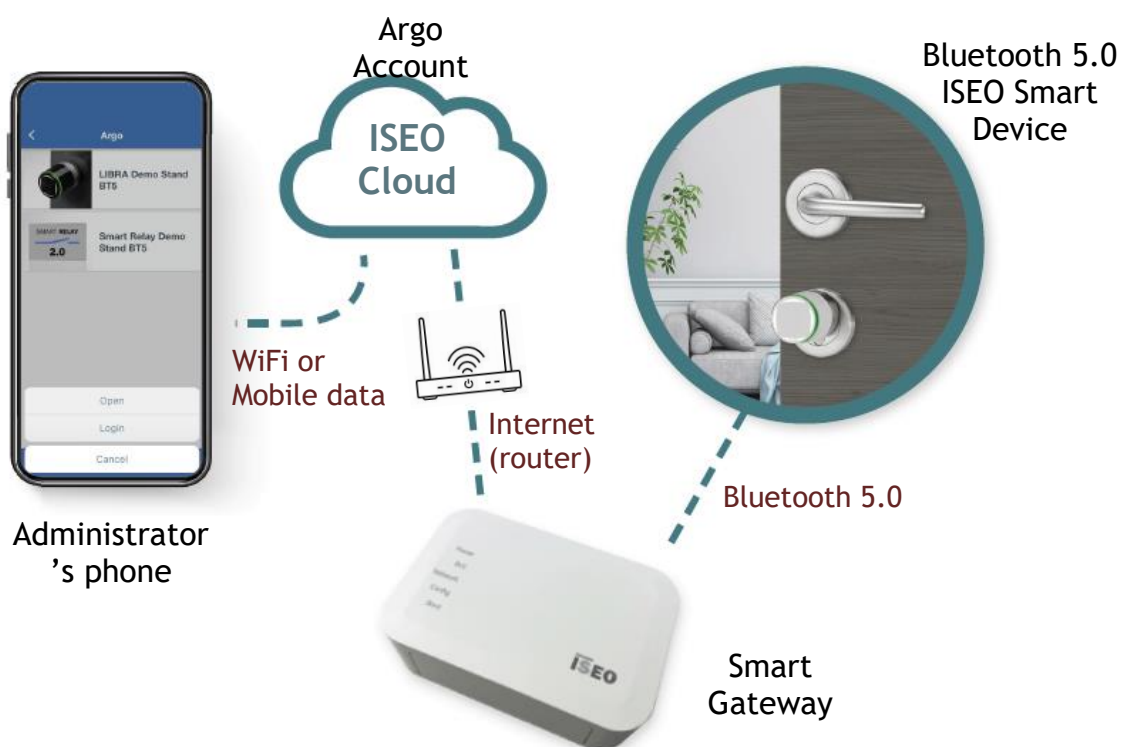
To know more about this function see the related chapter in the *Advanced* chapter.

Argo from Remote

Argo 3.0 combined to the new generation of ISEO Smart devices featuring Bluetooth 5.0 and the Smart Gateway, allows to manage the system from remote. That means that the Administrator can connect to the lock to add users or read events also without being nearby the door.

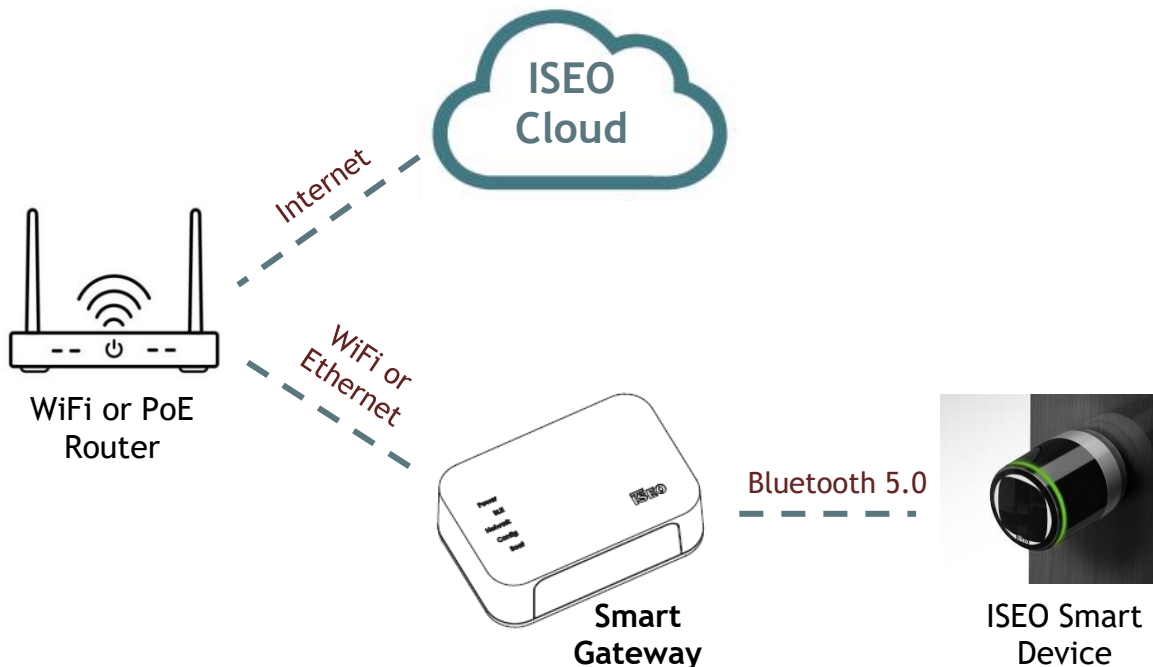
Principle of working

The phone is able to reach the Smart Gateway through the personal Argo account created in the ISEO Cloud free service. The phone communicates to the ISEO Cloud through mobile data or WiFi connection if available. The ISEO Cloud communicates to the Smart Gateway through Internet connection, by a router to which the Gateway is connected (home or company router – not provided by ISEO). The Gateway must be properly configured to reach the router and through the router the Argo Account. The Gateway must be placed nearby the lock, in the Bluetooth range capability, and eventually communicates to the lock via Bluetooth 5.0 technology.



Smart Gateway

The *Smart Gateway* connects the *ISEO Cloud* to the *ISEO Smart Device*. It communicates with the cloud via Internet through a WiFi router, and to the lock via *Bluetooth Smart 5.0*. The *Smart Gateway* can manage all the *ISEO Smart Devices* in the *Bluetooth* range capability (around 10 meters depending on environment conditions).



The Router is not provided by ISEO.
in the case of multiple ISEO Smart Devices, more than 10 meters away from each other, it is possible to add other Gateways connected to the same network.

The *Smart Gateway* is a powerful Linux machine with an *ARM 7* processor and extends the *Argo* capabilities to remote, providing the same level of security as in local. It allows a security architecture with direct connectivity to the lock with end-to-end encryption. The *ISEO Cloud* in fact is used only as tunnelling and does not store any sensible data for the door-lock.

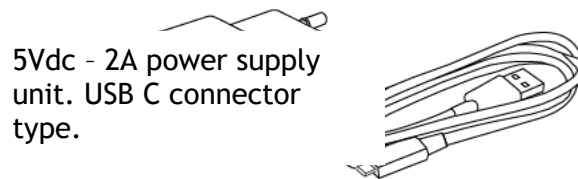
The *Smart Gateway*, by *Linux Operating System* and provided *APIs*, can be used from *ISEO Argo Developers* (integrators) by the *Argo SDK*, to write their software and their application on it, in the most efficient and simple way. Moreover, *Linux OS* assures stability and greater security from external threats or virus attacks.

Smart Gateway models

The *Smart Gateway* is available in two models:

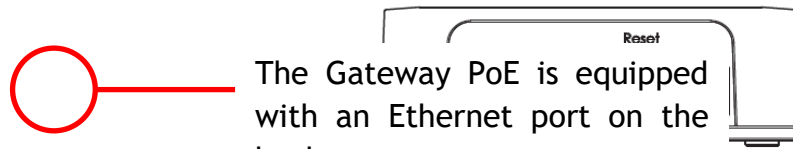
WiFi Gateway

- It requires a WiFi router.
- It must be powered by a 10W power supply unit.



Gateway PoE (Powered over Ethernet)

- It requires a PoE router.
- It must be connected by LAN cable to the PoE port of the router.



- Alternatively, it can be connected by LAN cable to a standard router (not PoE Ethernet port), but in this case it must be additionally powered by the 10W power supply unit.



Gateway PoE requires a router with **DHCP enabled** to automatically receive a valid IP address.

LAN cable is not provided by ISEO.

The 10W power supply unit must be separately ordered. It is not included in the *Smart Gateway* box.

Smart Gateway technical data

Features	WiFi	PoE (Power over Ethernet)
Functionality	<ul style="list-style-type: none"> Converts from WIFI data to BLE 5 Dual Band WIFI at 2.4 GHz and 5 GHz 	<ul style="list-style-type: none"> Converts from Ethernet to BLE 5
Power Supply	<ul style="list-style-type: none"> Powered by USB C +5VDC input power 2A (10W) Power supply not included (accessory to order) 	<ul style="list-style-type: none"> PoE (Power over Ethernet) Requires PoE Switch IEEE 802.3af up to 15,4W Delivery of data and power over CAT5e/CAT6 ethernet cable. Maximum power consumption 10W Optionally powered by USB C +5VDC input power 2A (10W) Power supply not included (accessory to order)
Dimensions	<ul style="list-style-type: none"> 125x40x85mm (LxDxH) 	<ul style="list-style-type: none"> 125x40x85mm (LxDxH)
Operating conditions	<ul style="list-style-type: none"> Operating Temperature: 0°C/+50°C Storage Temperature: -25°C/+75°C 	<ul style="list-style-type: none"> Operating Temperature: 0°C/+50°C Storage Temperature: -25°C/+75°C
Installation	<ul style="list-style-type: none"> Desktop Wall Fixing option (accessory to order) 	<ul style="list-style-type: none"> Desktop Wall Fixing option (accessory to order)
Connection ports	<ul style="list-style-type: none"> USB C female 	<ul style="list-style-type: none"> USB C female Ethernet TCP/IP 10/100 baseT
Signalling LEDs	<ul style="list-style-type: none"> Power (white): ON = Power Supply connected BLE (white): ON = BLE transmission in progress Network (white) ON = Gateway connected to Cloud Config (white): ON = Gateway to be configured Boot (red): ON = Gateway starting up 	<ul style="list-style-type: none"> Power (white): ON = Power Supply connected BLE (white): ON = BLE transmission in progress Network (white) ON = Gateway connected to Cloud Config (white): ON = Gateway to be configured Boot (red): ON = Gateway starting up
CPU, Memory, Operating System	<ul style="list-style-type: none"> ARM A7 based CPU module 512 MB RAM 8 GB Flash eMMC Non volatile Memory Operating System: embedded Linux 	<ul style="list-style-type: none"> ARM A7 based CPU module 512 MB RAM 8 GB Flash eMMC Non volatile Memory Operating System: embedded Linux
Push buttons	<ul style="list-style-type: none"> Reset (reboot or factory mode status) 	<ul style="list-style-type: none"> Reset (reboot or factory mode status)
OEM version	<ul style="list-style-type: none"> Available OEM version for Argo Integrators with SDK 	<ul style="list-style-type: none"> Available OEM version for Argo Integrators with SDK

Bluetooth 5.0 ISEO Smart Devices

The new *ISEO Smart Devices* series take advantage of the *Bluetooth 5.0* technology (also called *BLE 5*). This technology allows multiple connections at the same time. For example: while someone is opening the door-lock with the smartphone, the *Administrator* can connect from remote through *the Smart Gateway*, and the lock will be able to perform both tasks at the same time.

From the shape and mechanical point of view, the new *ISEO Smart Devices* are the same of the previous ones embedding *Bluetooth 4.0* technology. What changes and makes them different is:

- *Bluetooth 5.0* chip embedded in the electronic board.
- New aesthetic logo design to immediately identify the new *Bluetooth 5.0* technology.

New aesthetic logo

The new *Argo 3.0* logo is showed in all the new *ISEO Smart Devices* embedding the *Bluetooth 5.0* technology. This new logo aims to communicate the technological evolution of the product which brings new and unique features and functionalities:

- increased communication performance of the *ISEO Smart Devices*.
- Multiple connectivity at the same time.
- *Argo* remote management by a new device: the *Smart Gateway*.

Argo & ISEO Smart Devices Logo evolution



Argo 2.7 & Bluetooth 4.0
Smart Devices

Argo 3.0 & Bluetooth
5.0 Smart Devices

Argo 2.7 to Argo 3.0 app logo evolution



Argo 2.7 & Bluetooth 4.0



Argo 3.0 & Bluetooth 5.0



On *Argo 3.0* app the new *Bluetooth 5.0* devices are identified by a new icon (see *Basic, Create your Argo Account*).

ISEO Smart Devices logo evolution examples



Libra Smart Bluetooth 4.0



Libra Smart Bluetooth 5.0



Stylos Smart Bluetooth 4.0



Stylos Smart Bluetooth 5.0



x1R Smart reader



x1R Smart reader



On *x1R Smart* the *Bluetooth 5.0* electronic board is placed in the external reader that also shows the new logo design.

This section explains how to configure *Argo 3.0* in order to manage the system from remote.

To configure *Argo from Remote* you need to:

1. Create your *Argo Account*.

Advanced

2. Login to the *Argo Account*.
3. Configure the *Smart Gateway*.
4. Add locks to the system (*Master Card* required).

Create your Argo Account

At the first system configuration you need to create your *Argo Account* by using a valid email address, reachable from your phone or tablet. To do that follow the next simple steps.

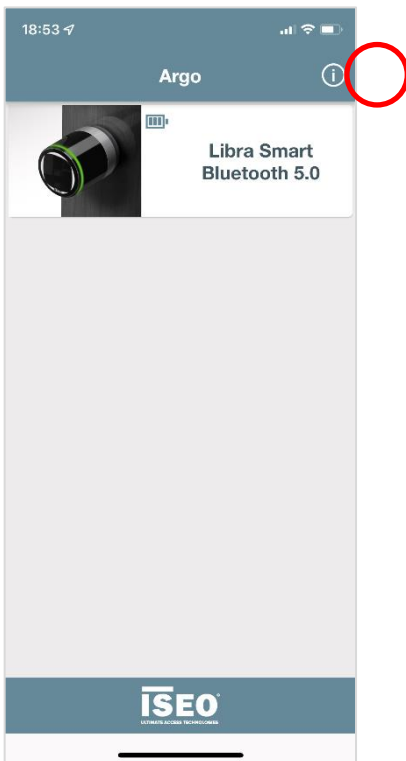
1. Start **Argo 3.0**



———— New *Argo 3.0* icon &

2. Tap the **Info App** menu

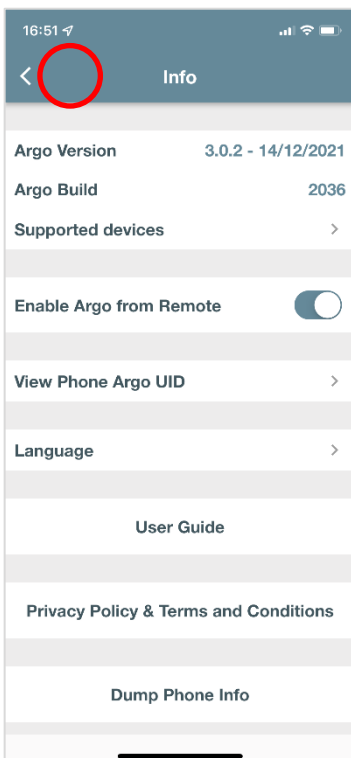
Advanced



Note the new Libra icon to immediately identify the *Bluetooth 5.0* devices.

All the new *BLE 5.0* devices present a new icon to easily recognize them from the *BLE 4.0* models.

3. Enable Argos From Remote, then go back to the main menu.



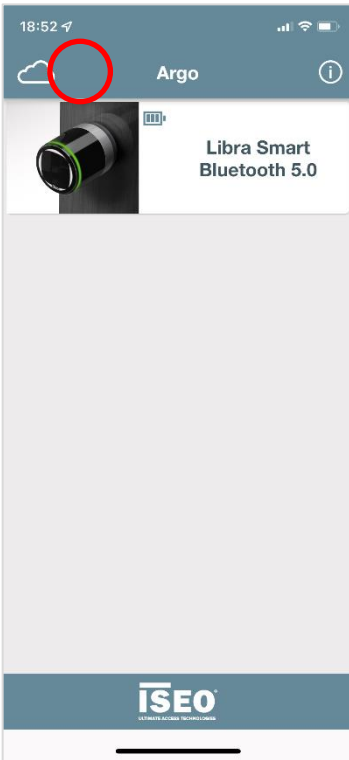
————— Argos . . . from Remote



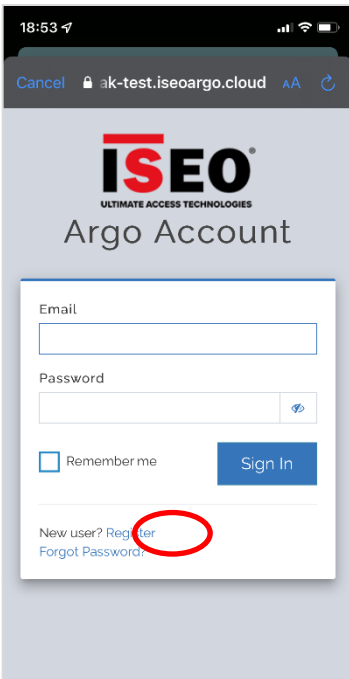
A warning message appears explaining *Argos from Remote* features and requirements. Read and accept to continue.

4. After enabling Argos From Remote a Cloud icon appears. Tap the Cloud Icon.

Advanced



5. Tap **Register** to start a new user registration in the *ISEO Cloud*. Then follow the step-by-step procedure.



User registration needs to be performed only at the first configuration, to create the *Argo Account*.

6. Insert all required data and tap **Register** at the end.

Advanced

20:17

Cancel ak-test.iseoargo.cloud AA

First name
Stephen

Last name
Marley

Email
stephen.marley74@gmail.com

Password
The password must be at least 8 characters and must contain at least 1 capital letter, 1 numeric digit and 1 special character.

Confirm password

Back Register

— Insert a valid email address that can be reached from the device on which the registration is made.

— A strong rule password is mandatory.

7. Accept the Terms & Conditions.

20:18

Cancel ak-test.iseoargo.cloud AA

ISEO
ULTIMATE ACCESS TECHNOLOGIES

Terms and
Conditions

Use of this application is subject to the terms and conditions that you can find [here](#). If you tap Decline you cannot Login to your ISEO Argo Account and you will return to the Argo 3.0 home page.

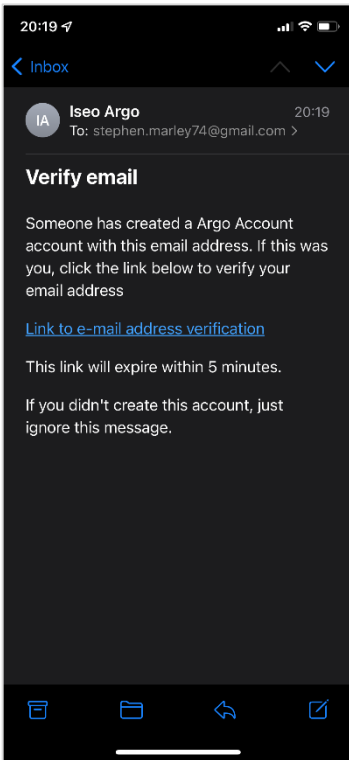
Accept Decline



If you tap **Decline** you will return to the *Argo Home page*. To reach again this step Login with the email and password registered at the previous step

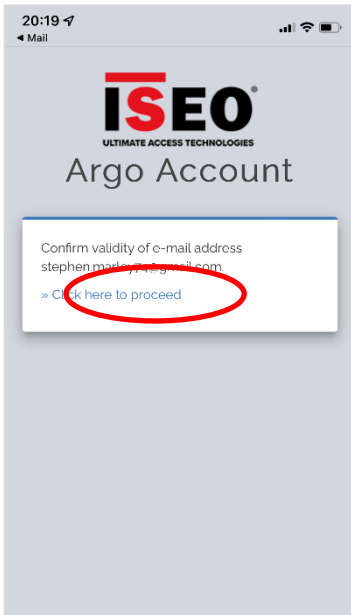
8. Wait the email verification from the *ISEO Cloud service*. Then open it and tap on the link.

Advanced



— Tap the link to confirm the email address.

9. Confirm the email address validity and wait for the verification message.
Then return to *Argo Home page*.



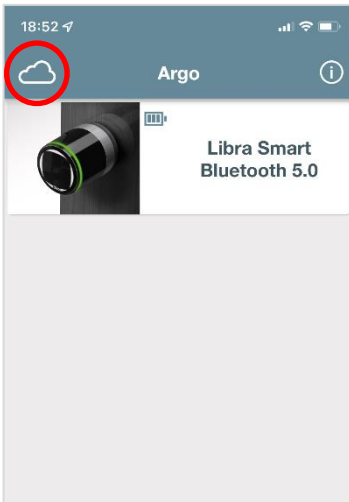
Advanced

Login to the Argo Account

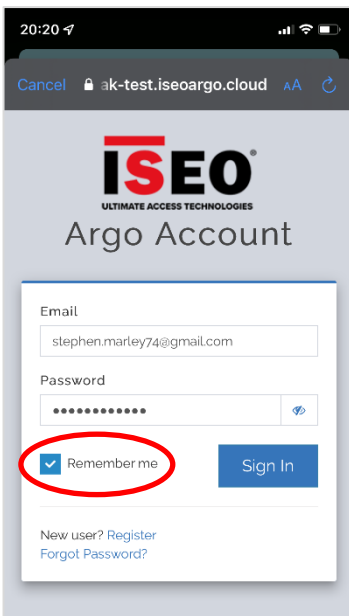
Once your *Argo Account* has been created in the *ISEO Cloud* you can login.

In the *Argo 3.0 Home page*:

1. Tap the **Cloud** icon.



2. Login with the email address and password previously chosen during the *Argo Account* registration.



————— Tap Sign In to Login



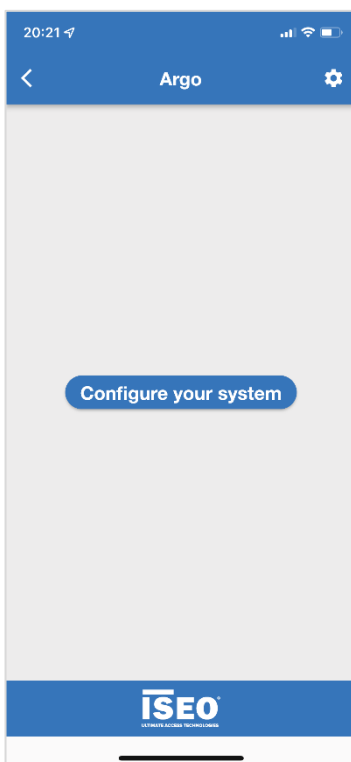
Selecting *Remember me* you won't need to type the email and password at the next login. This until a certain time defined by the app or until you manually logout from the account (to know more about logout go to *Advanced*).

Advanced

Configure the Smart Gateway

When you login to the *Argo Account* for the first time, you need to configure the *Smart Gateway* to start using *Argo from Remote*. The *Smart Gateway* in fact is the “tool” that allows your phone “to reach” the remote lock. That’s why as soon as you open *Argo from Remote* you get the message: *Configure your system*.

1. Tap **Configure your system**.



The top and bottom bars have a different colour from *Argo Local*. This to indicate the remote environment (*Argo from Remote*).

2. **Power-up** the *Smart Gateway*, then follow the step-by-step procedure embedded in the app.



Smart Gateway's boot keeps about 1 minute.

Advanced



Step-by-step configuration



If the *Gateway Config light* is NOT ON, touch **No** and the app will show how to reset the Gateway to factory mode.

3. Read the *Smart Gateway QR-Code* using your Smartphone.



There are two *QR-Codes* on the back of the Gateway:

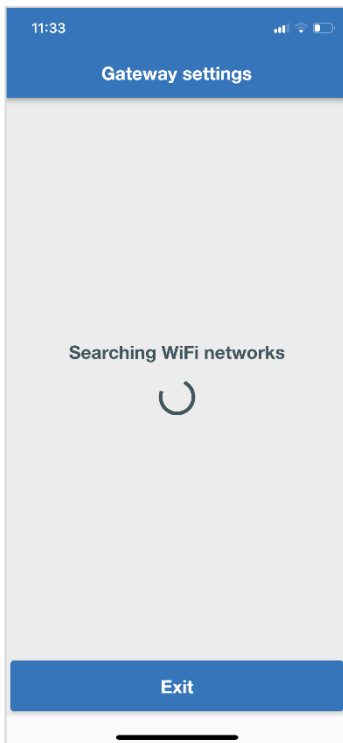
- Product Serial Number
- Registration Code.

Argo automatically reads only the correct one: the **Registration Code**.

In case of problems reading the *QR-Code*, it is also possible to add the *Registration Code* manually by tapping **Add manually**.

Advanced

- Once the *QR-Code* with the *Registration Code* has been read, the **wizard** starts searching the WiFi networks around the phone range.

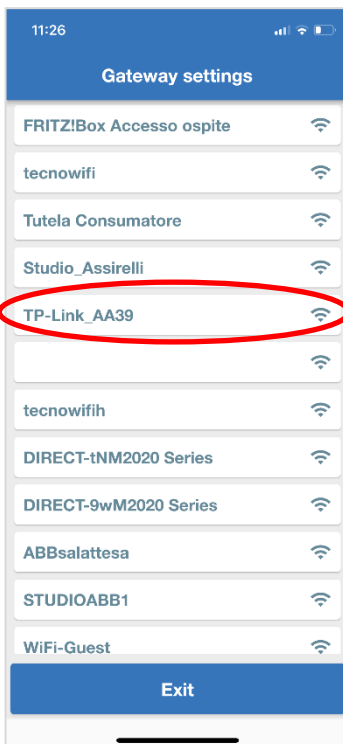


In case of *Smart Gateway PoE* go to step 7.

Steps 4, 5 and 6 are only valid for the *Smart Gateway WiFi*.

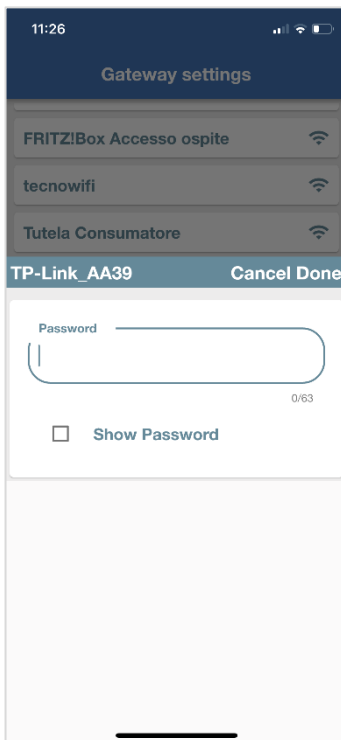
This because the *Gateway PoE* is directly connected to the router by LAN cable, and automatically receives an IP address by DHCP protocol.

- Choose and tap the **WiFi network** provided by your router.

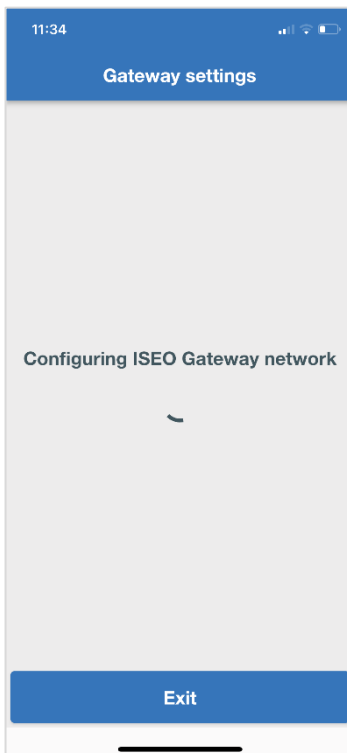


- Insert your personal WiFi password and tap **Done**.

Advanced



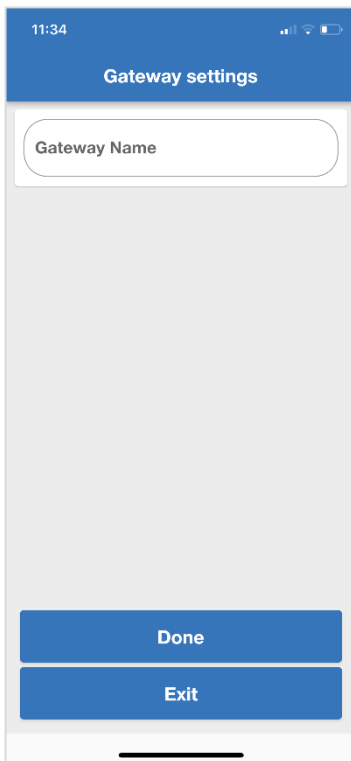
7. Wait the *Smart Gateway* network automatic configuration.



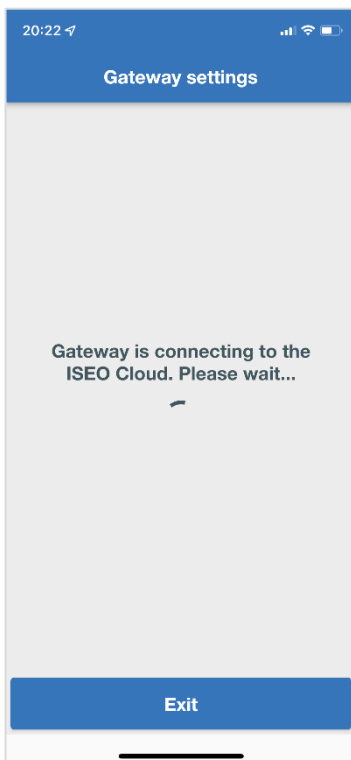
At this stage the Gateway is connecting to your router WiFi network. If an error occurs repeat the process and double-check the router password. To know more about the error types, go to *Troubleshooting* chapter.

8. As soon as the *Smart Gateway* has successfully connected to the router, you can assign a name to the Gateway to better identify it. Then tap **Done**.

Advanced



9. Wait now for the *Smart Gateway* to reach and connect to your *Argo Account* in the *ISEO Cloud*.



At this stage the Gateway is connecting to the *ISEO Cloud*. If an error occurs it may be caused by different reasons:

- No internet connection.
- Slow internet connection (network latency).
- Error in communication due to router settings or Firewall.

Repeat the procedure. If the problem persists, check the router and your internet connection.

To know more about error types, go to *Troubleshooting* chapter.

10. When the *Smart Gateway* connects to the *ISEO Cloud* a successful message is shown: **Smart Gateway is ONLINE**. You can now add locks to the system.

Advanced



Add locks to the system (Master Card required)

Adding locks to the system means to connect your *ISEO Smart Devices* to the configured *Smart Gateway*, to reach them from remote through your *Argo Account* created in the *ISEO Cloud*.

To communicate with the *Smart Gateway*, the *ISEO Smart Devices* must be:

- *Bluetooth 5.0* version.
- Placed in the *Smart Gateway* Bluetooth range.

You can add as many *ISEO Smart Devices* as you want, there's not a defined limit. The *Gateway* behaves like a smartphone running *Argo*: it can detect any device in the Bluetooth range.

The unique limit is the distance between *Gateway* and devices that must not exceed on average about 10mt, which may vary depending on the environmental conditions: wall thickness, corners, electromagnetic noise around, *Gateway* installation place, position and height.

Gateway Installation example

Advanced

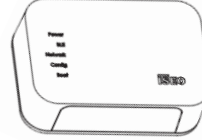


Door with *ISEO Smart Devices* installed on it.

Bluetooth 5.0 range
(about 10mt)



Smart Gateway installed nearby the door and in the router WiFi range.



WiFi range



WiFi router

1. Tap **Add new locks**, then follow the installation wizard. Be sure to be in front of the lock to add, in order to present the *Master Card* when required from the app.

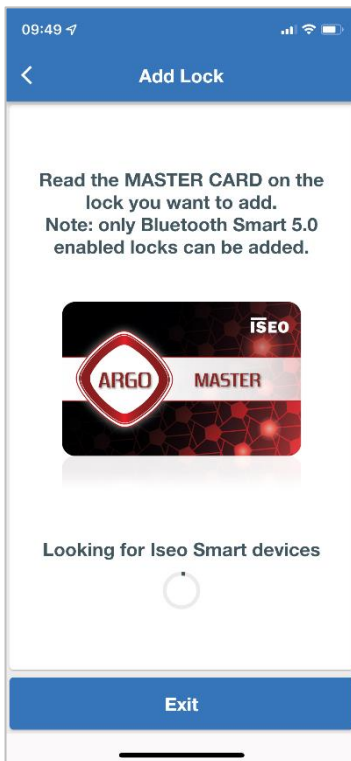


This procedure **requires the Master Card** and the Administrator must be in front of the lock.

You can also add locks later, by the related menu reachable in the *Argo from Remote Home page*. To know more about the menu functions, go to *Advanced* chapter.

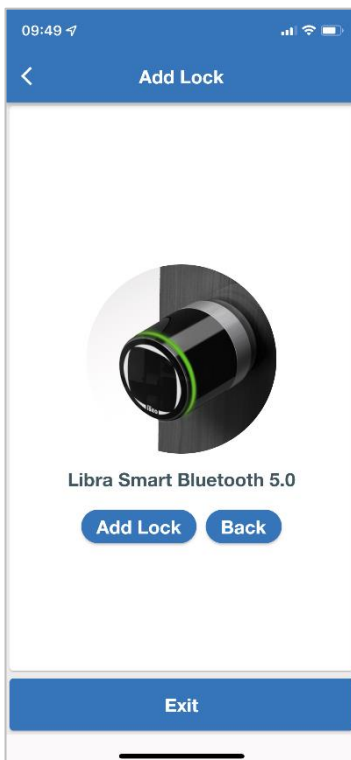
2. The app starts searching for nearby *Bluetooth 5.0 ISEO Smart Devices*. As soon as devices have been found, follow the instruction in the app.

Advanced



Present the **Master Card** with the unique system code assigned to your plant.

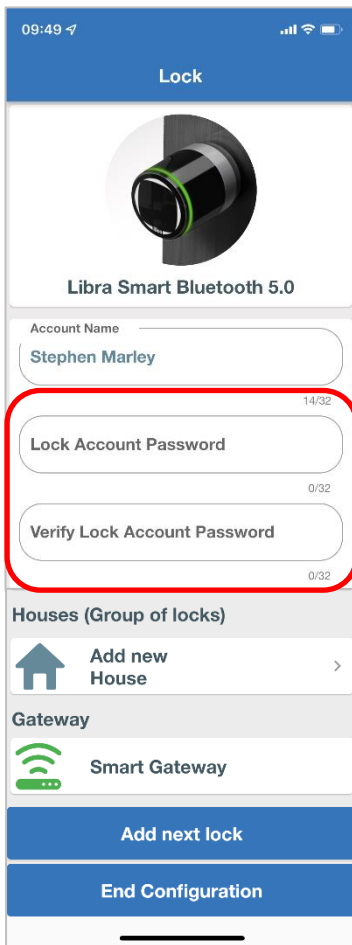
3. Tap **Add lock** to confirm and wait for the lock configuration.



The lock name is automatically taken by *Argo Local*. To change the lock name, you need to change it as usual by *Argo Local* in the *Door Info* menu. The lock name will be automatically updated in *Argo from Remote* at the next Login.

4. Choose the **Lock Account Password**. This password is an additional security to protect the communication toward the lock, and it is stored in the most secure place: inside the lock.

Advanced



The password can be automatically associated to the smartphone biometric identifications (fingerprint or face-id), for the best user experience and convenience.

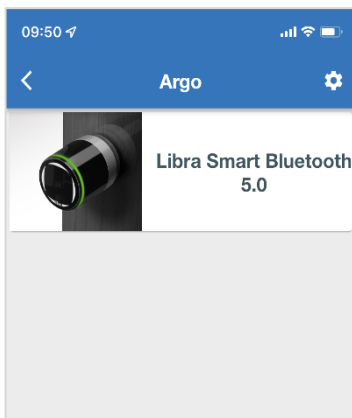
You can create a *House* in which to place the lock. To know more about *House*, go to the *Advanced* chapter

This is the *Smart Gateway* connected to the lock, previously configured



To know more about security on *Argo From Remote*, consult the *Argo 3.0* leaflet available at iseo.com.

5. Wait the end of the configuration: the lock, protected by the chosen password, will be added to the *Argo Account* in the *ISEO Cloud*. As soon as it has been done, you will see the lock icon and button showing in the *Argo from Remote Home* page.



The added lock is now showing in the *Argo from Remote Home* page.

Connect to the lock from remote

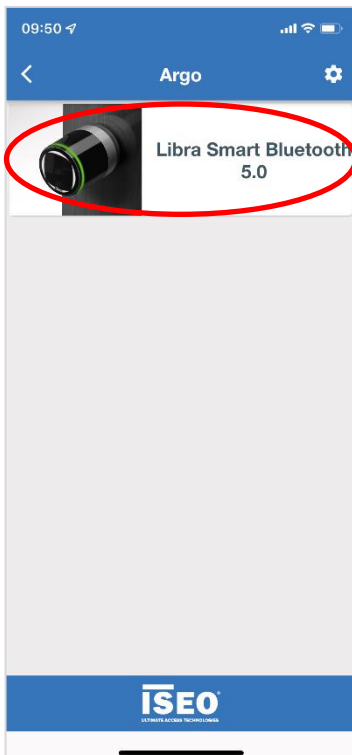
Once the *Argo Account* has been created, the *Smart Gateway* has been configured and the lock has been added to the system (see *Basics*), you can now connect from remote to the *ISEO Smart Device* to perform the next operations:

- Open the lock from remote.
- Login to the lock from remote.

Open the lock from remote

With *Argo 3.0* is possible to open a door from remote. This can be useful in case of specific needs or emergency, for example if you need to let someone enter the door when you are not inside or nearby. To do that *Login* to the *Argo Account* (see *Basics, Login to the Argo Account*) and follow the next steps.

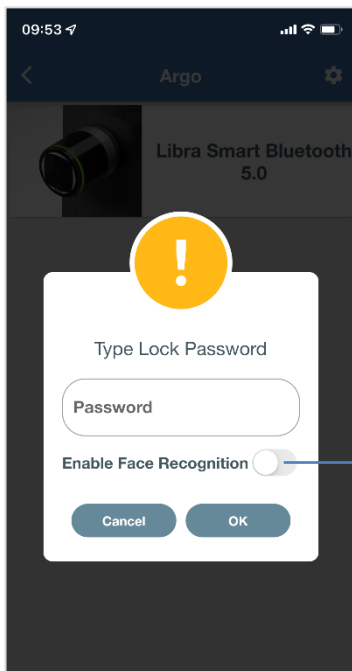
1. Tap the lock with the door name and icon and wait for the connection.



On *Argo from Remote* the *Tap & Hold* function used in *Argo Local* to show the additional functionalities, is not present. Whether you tap one time or tap & hold, the result is the same: the app always shows the enabled functions.

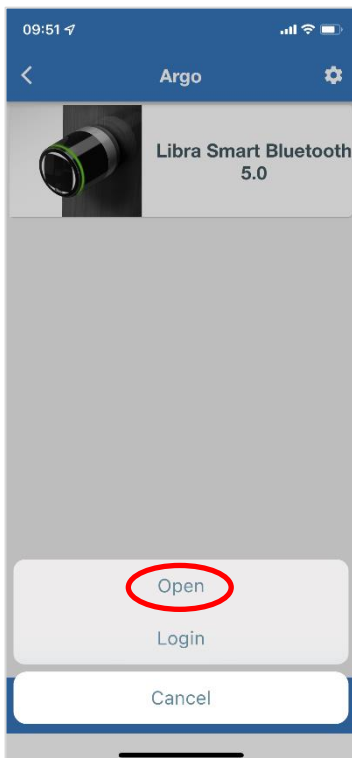
2. Type the **Lock Account Password** previously set (*Basics, Add locks to the system*). This password guarantees the security of the system and it is stored in the most secure place: inside the lock.

Advanced



Enable the Face or Fingerprint recognition to associate this password to your smartphone biometric identification. In this way at the next operations, you won't need to type the password.

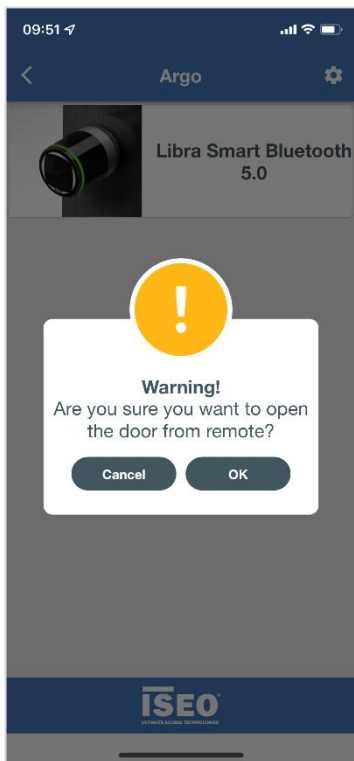
3. Tap Open.



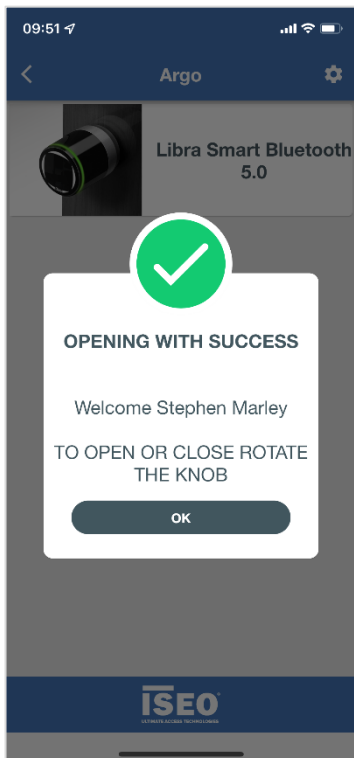
Login is always present by default because it is the basic requirement for the *Administrator* to manage the lock from remote. The *Remote Owner Administrator* has the *Open* function by default.

4. Opening a door from remote is a critical operation because you are not in front of the door. Confirm the operation a second time tapping **OK** at the warning message.

Advanced



5. Wait for the opening successful message.

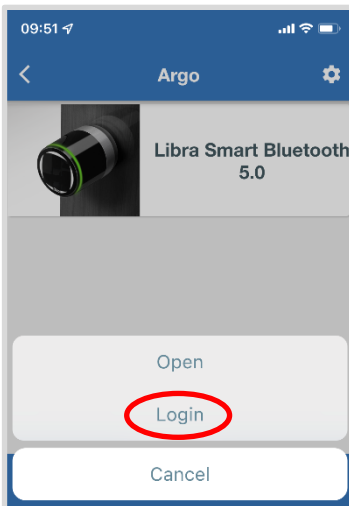


Advanced

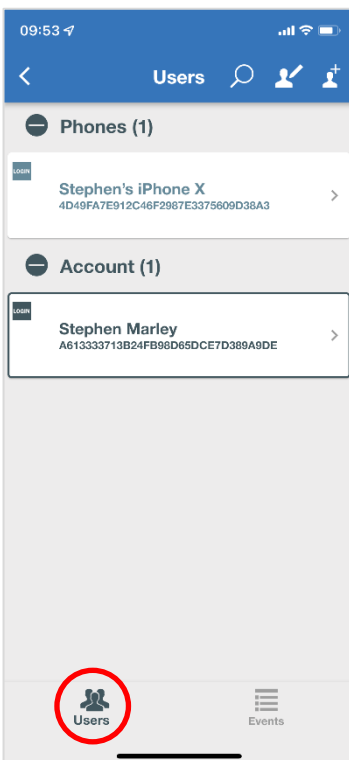
Login to the lock from remote

By *Argo 3.0* the *Administrator* can login to the lock from remote to manage the users list or read events, without the need to be in front of the door, in the *Bluetooth* range. To login from remote:

1. Tap Login



2. Type the **Lock Account Password** if not yet associated to the smartphone biometric identification (see *Open the lock from remote, step 2*).
3. After the connection time you will directly enter in the lock *User List* from remote.



Phone user with Login capability. It is called **Local Administrator**.

Administrator Account. It is called **Remote Owner Administrator**.



An *Administrator* can be only *Local* and not *Remote* or vice-versa; or he could have both identities, like in the above example. *Local Administrator* cannot login from remote and vice-versa.

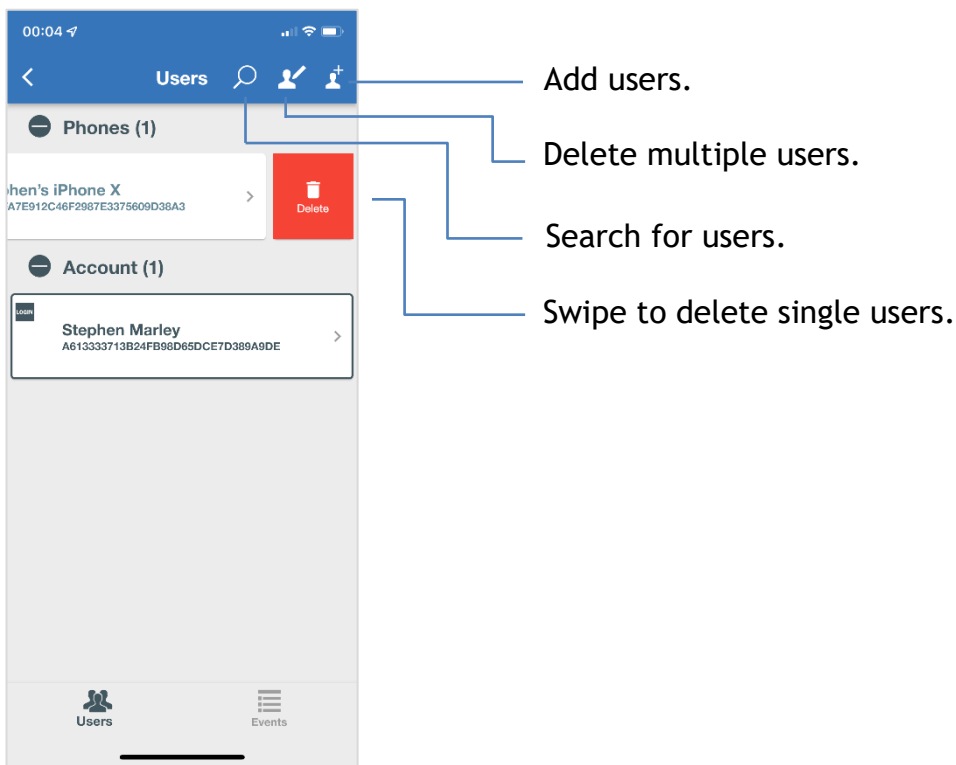
After login you can:

Advanced

- Add, edit or delete *Users*.
- Read the history *Events*.
- Add *Guest Account* (this topic is covered in the *Advanced* chapter).


Add, edit or delete Users

Like *Argo Local* you can search, add, edit or delete users but from remote.

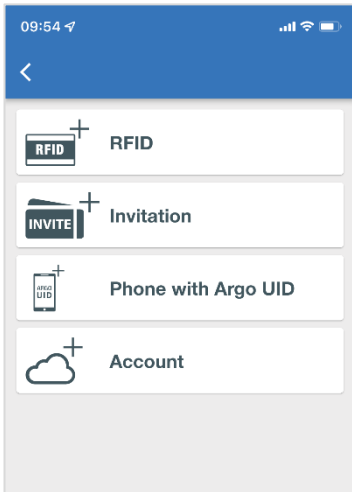


Argo from Remote user interface is the same as *Argo Local*: same logic, same aesthetic, same buttons and icons. This to provide the best user experience and convenience of use: who knows *Argo Local* will also know how to use *Argo From Remote* straightforward.

To discover about *Argo Local* read the *Argo 2.7 User Manual* available at iseo.com.

Tap **Add user** icon  to see the credentials that can be added, depending on the *ISEO Smart Device* type. The credential to be added are the same of *Argo Local* plus a new one: *Account* (see *Advanced* chapter)

Advanced

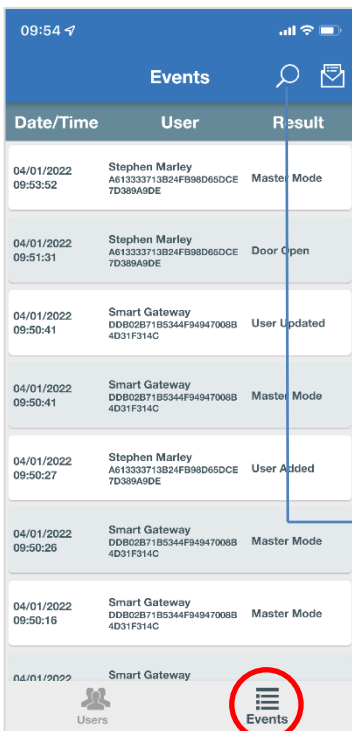


In this example the *ISEO Smart Device* is a *Libra Smart*, therefore we cannot add PIN codes.

The *Add Fingerprint* option, available for *x1R Smart* on *Argo Local*, is not present on *Argo from Remote*, due to the kind of enrolling procedure that requires the on-site presence of the user.

Read the History events

Tapping the *Events* menu, you can see all the lock events from remote. The *Events* are shown with the same user interface of *Argo Local*, in order to provide the best user experience and convenience of use and always following the *Argo* philosophy: simplicity and effectiveness.



Tap to send the displayed events by email or by any other communication app.


Differently from *Argo Local* you cannot send all events in one shot, but just the ones pre-loaded in the phone memory. Scroll down the event list to show more events. All the showed events can be sent via email.

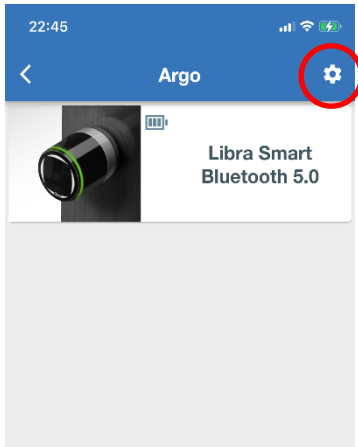
Tap to open the search box tool to search events by *Date/Time*, *User* or *Result*, even with just some letters or numbers (partial words).

Advanced

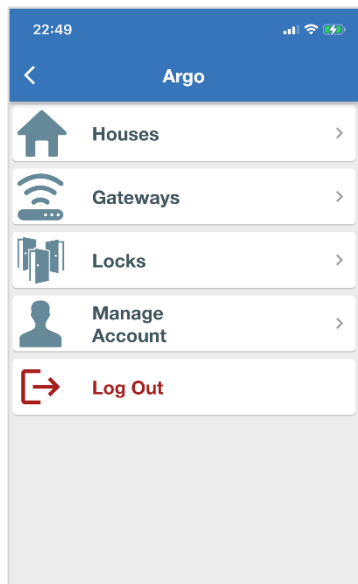
Argo from Remote menu overview

In this advanced section you can find the *Argo from Remote* menu explanation and all the related functions. After the menu overview, each function is also individually explained.

1. Login to your **Argo Account** and tap the menu icon 



2. In this page there are all the related sub-menus.



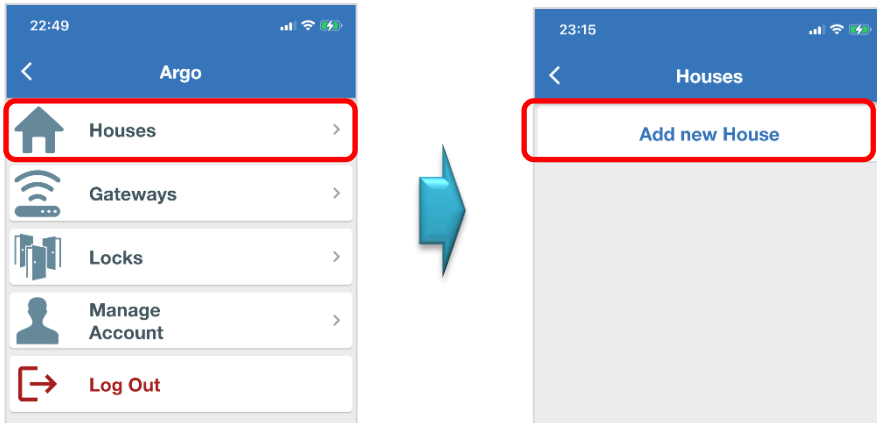
- Add, delete, rename **Houses**.
- Add, delete, rename **Gateways**.
- Add, delete, rename **Locks**.
- - Account info
 - Enable Face or Fingerprint recognition
 - Reset Account password
 - Delete Account
- Account logout

Advanced Houses

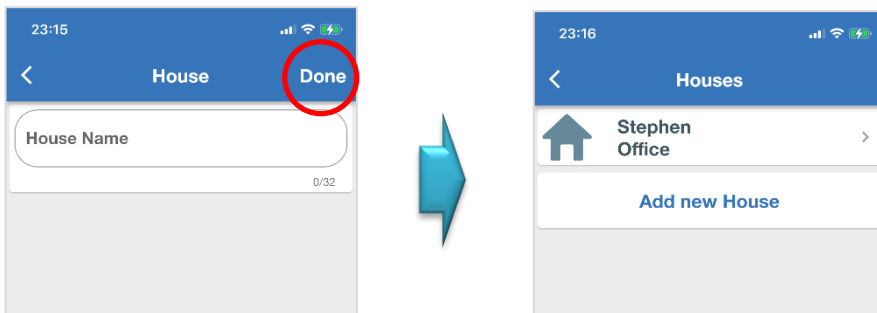
In this menu you can add a new *Houses* or manage the existing ones (delete or rename).

To add a new **House**:

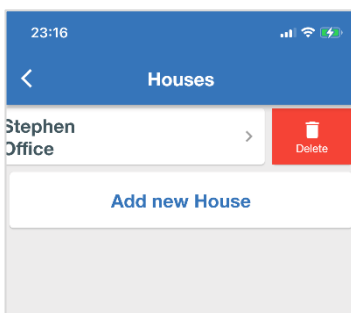
1. Tap **Houses** and then tap **Add new House**.



2. Type the **House Name** and then tap **Done**. The *House* is then created.



3. To delete a *House* swipe from right to left.



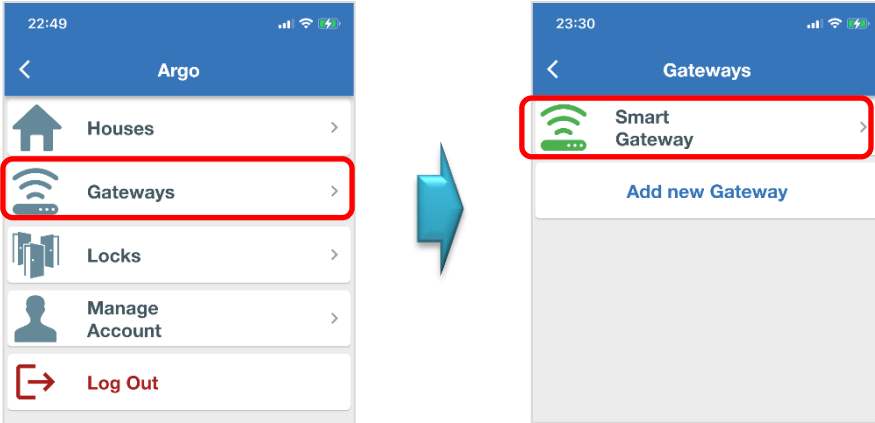
4. To rename a *House* simply tap on the *House* name to enter edit mode and rename it.



In this menu you can add a new *Gateway* or manage the existing ones: delete, rename and get info.

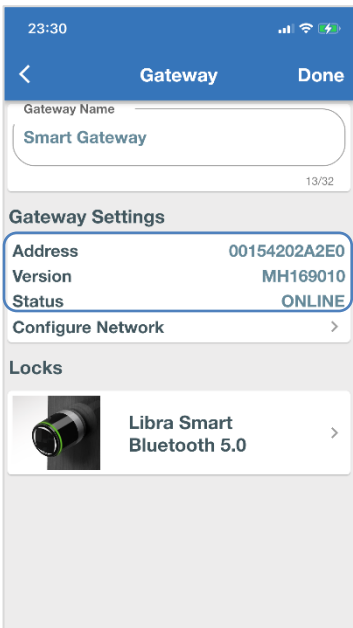
To see **Gateway** info:

1. Tap **Gateways** and then tap on the gateway name.



A green coloured *Gateway* icon means that the *Gateway* is online. A red icon means *Gateway* offline (not connected to Internet). Tap **Add a new Gateway** to start the wizard previously showed (go to *Basics, Configure the Smart Gateway*)

2. In this page you can see all the *Gateway* information.



Tap to rename the gateway.

Gateway software information.

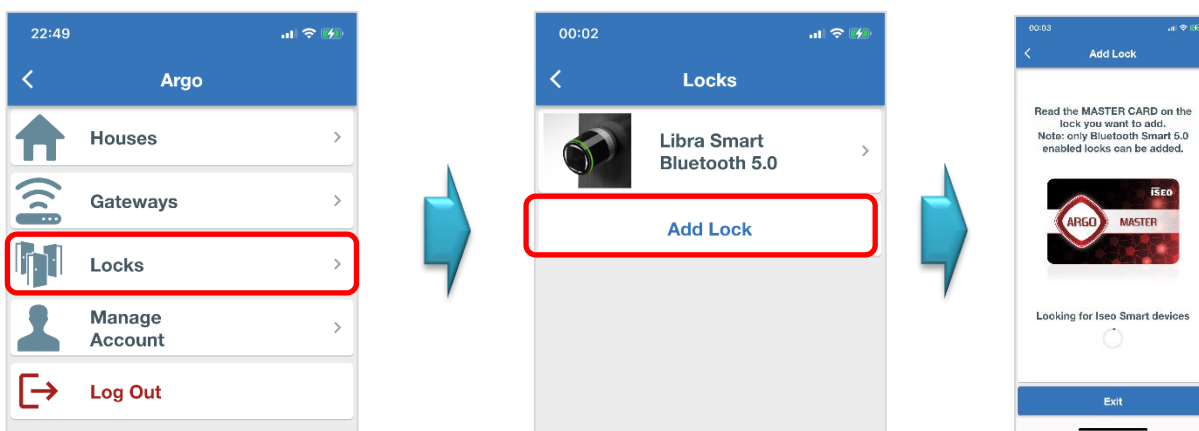
Tap to re-configure the gateway WiFi. For example: this can be useful in case of router replacement

Lock connected to this Gateway. Tap the lock name and icon to directly enter the *Locks* menu, also reachable from the main menu (see *Locks*).

In this menu you can add and delete *Locks* or assign and change house to the existing ones.

Add a new Lock

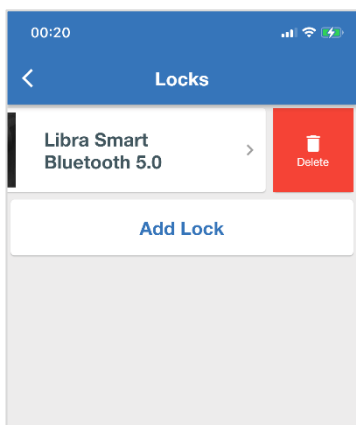
- Tap **Locks** and then tap **Add Lock**. It will start the same wizard previously described (go to *Basics*, *Add locks to the system*).



For this operation the Administrator need to be in front of the lock and the Master Card is required.

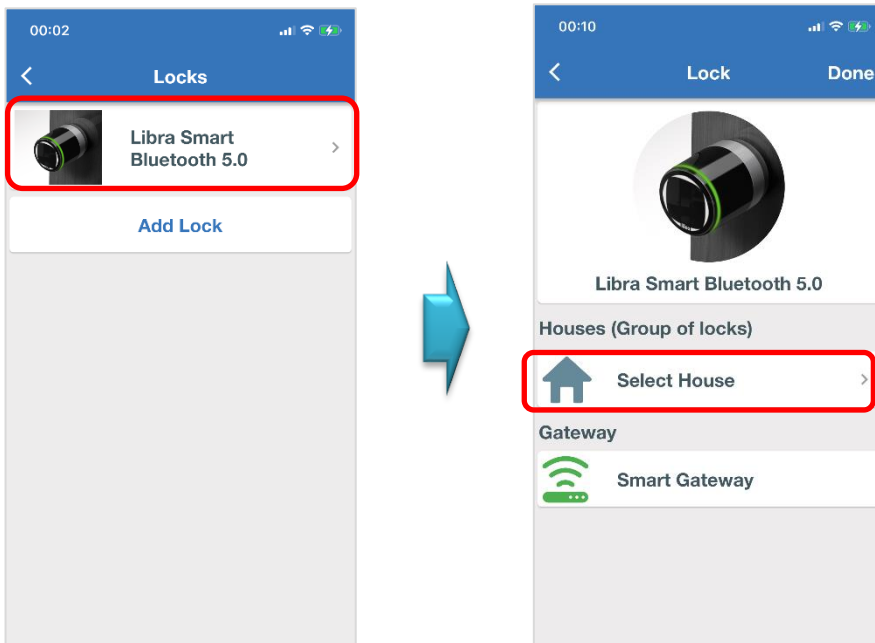
Delete a lock

- Tap **Locks** and then simply swipe to delete the lock. Confirm the warning message with OK.

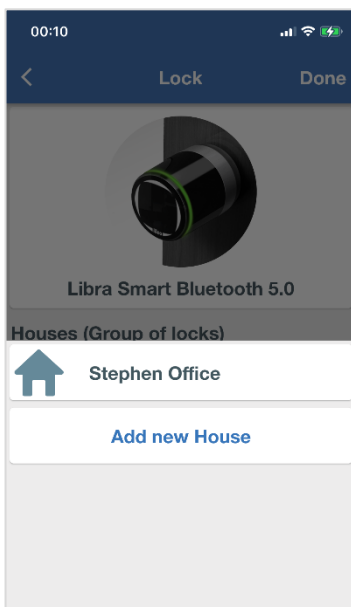


Advanced Assign locks to House

1. In the *Locks* menu tap the lock name and icon and then tap **Select House**.



2. Choose the *House* to assign (i.e. Stephen Office) or **Add a new House** to create a new one.



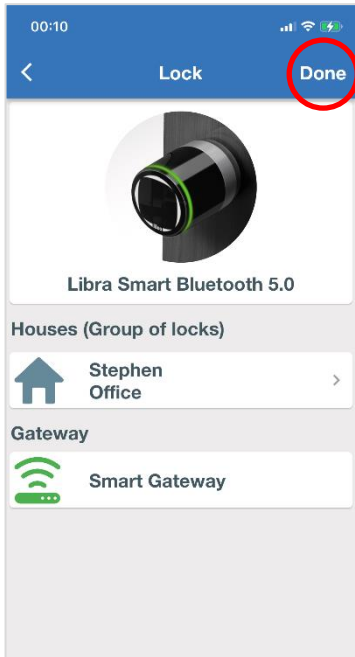
House previously configured in the system.



It is also possible to create Houses during the first system configuration (*Basics, Add locks to the system*), or directly in the *House* menu.

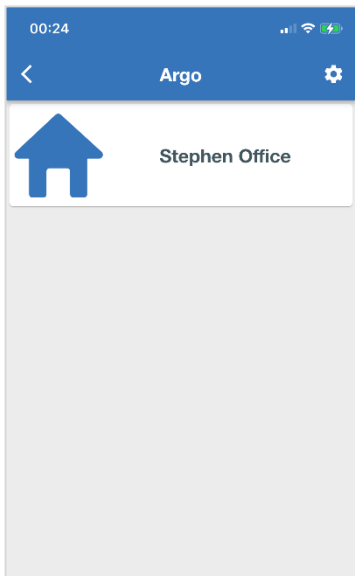
Advanced

3. Tap **Done** at the end to save the configuration.



————— **House** assigned to this lock.

4. After the *House* has been assigned to the lock, the *Argo 3.0 Home page* changes as follows:



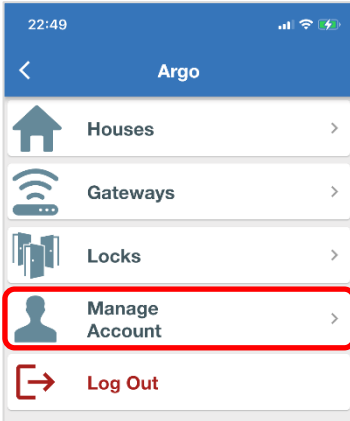
————— **Home page:** the lock now is “inside” the *House*. Tap the *House* name and icon to see the locks belonging to this house.

Manage Account

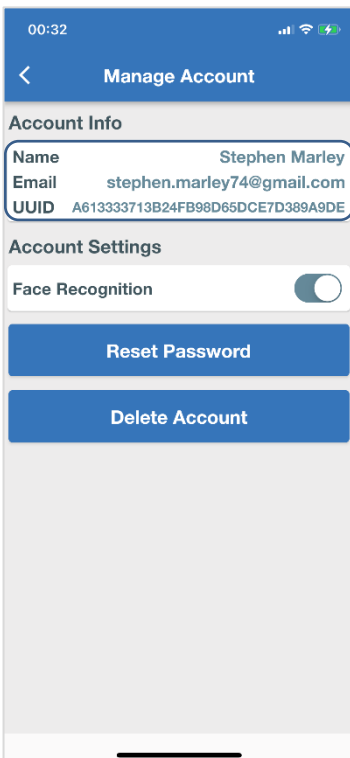


In this menu you can read the *Account* info and perform some other important operations as showed in the following instruction.

1. Tap **Manage Account**.



2. In the **Manage Account** menu you can read the next information:



Account info.

Enable the *Face or Fingerprint* recognition, (depending on the technology of your smartphone), in order to associate the lock password to your biometric identification, and consequently speed up the connection process for the best user experience and convenience of use.

Tap to reset your account password, then follow the step-by-step instructions

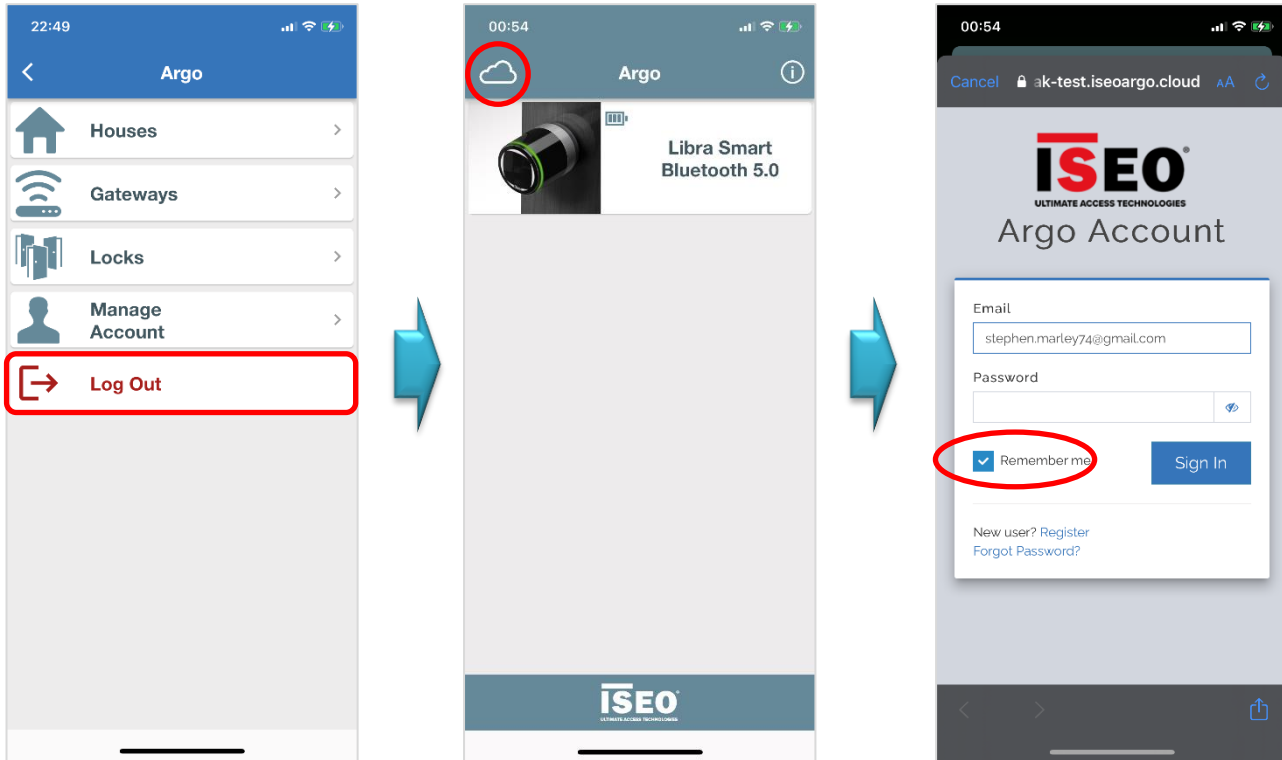
Tap to permanently delete your *Account*. Delete the account is a critical operation if there are inside configured devices (Locks and Gateways). To find out how to correctly delete an account, go to *Delete the Owner Administrator*

Advanced

Log Out

Tapping **Log Out** the *Administrator* is immediately logged out from the *Account*. To login again *Administrator* needs to insert the personal account password. To logout from the *Account*:

1. Tap **Log Out** to exit *Argo from Remote*. Tap the *Cloud* icon to login again.



Log Out overrides the *Remember me* function; so it can be useful for security reasons to be sure nobody can enter your account even if someone gets hold of your phone.

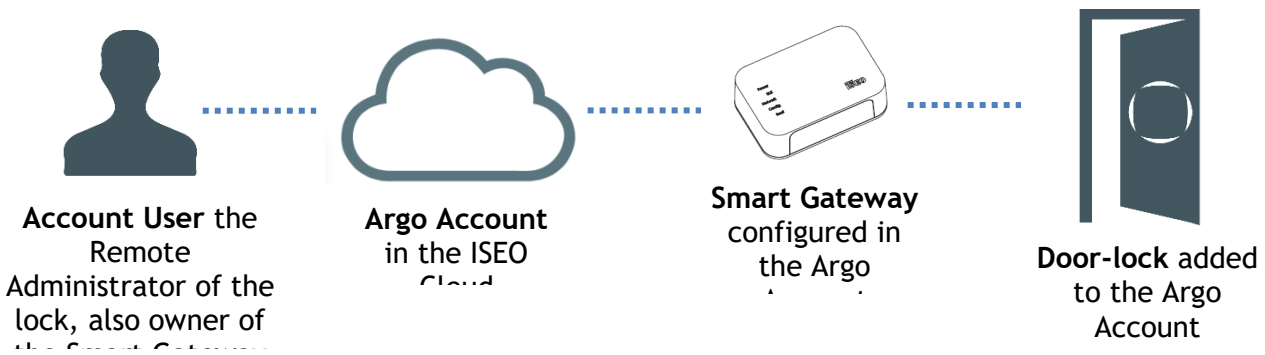
The **Remember me** function allows to quick login to the *Account* without inserting the password again. This situation persists for a limited time automatically set by the app.

Advanced

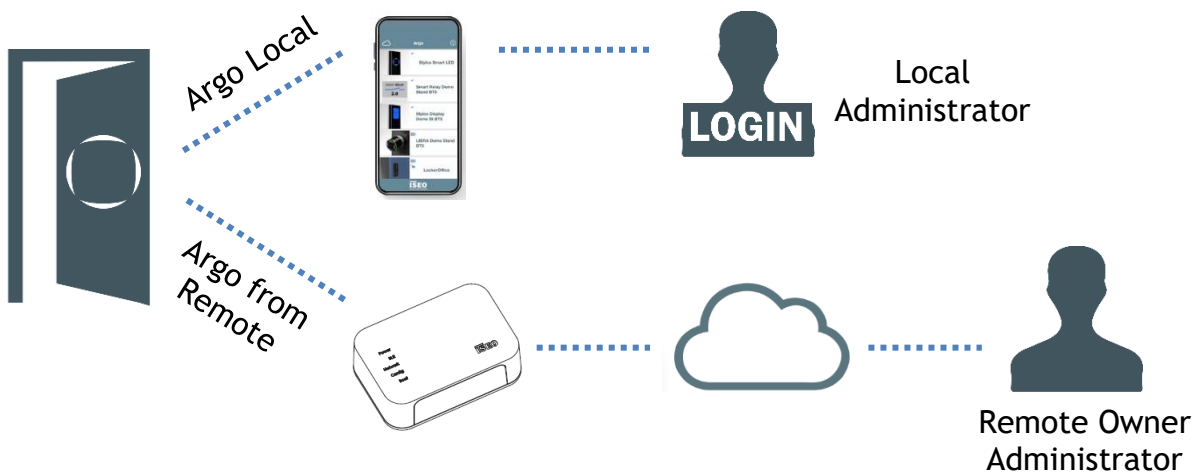
Account user



The *Account User* is a new identity strictly related to *Argo from Remote*. It is basically the *Remote Administrator*. The *Remote Administrator* in fact needs to have an *Argo Account* to exist, a space in the *ISEO Cloud*, to take advantage of *Argo from Remote*. This is fundamental to reach the lock through a *Smart Gateway*.



The *Remote Administrator* must not be confused with the *Local Administrator* (see *Keywords*). These are two different identities which can also coexist in the same lock. A *Local Administrator* is what we've managed so far with *Argo Local*: it is any smartphone user with Login capability. *Argo* can have many *Local Administrators* for the same lock, with the same access rights. In fact *Argo Local* does not have different *Administrator's authorizations*: all the *Administrators* are at the same hierarchical level. Note that any *Local Administrator* can enroll other *Administrators* (with *Login* function enabled) without any limitation: by *Master Card* or by *Invitation* or *Add Phone with Argo UID* functions.



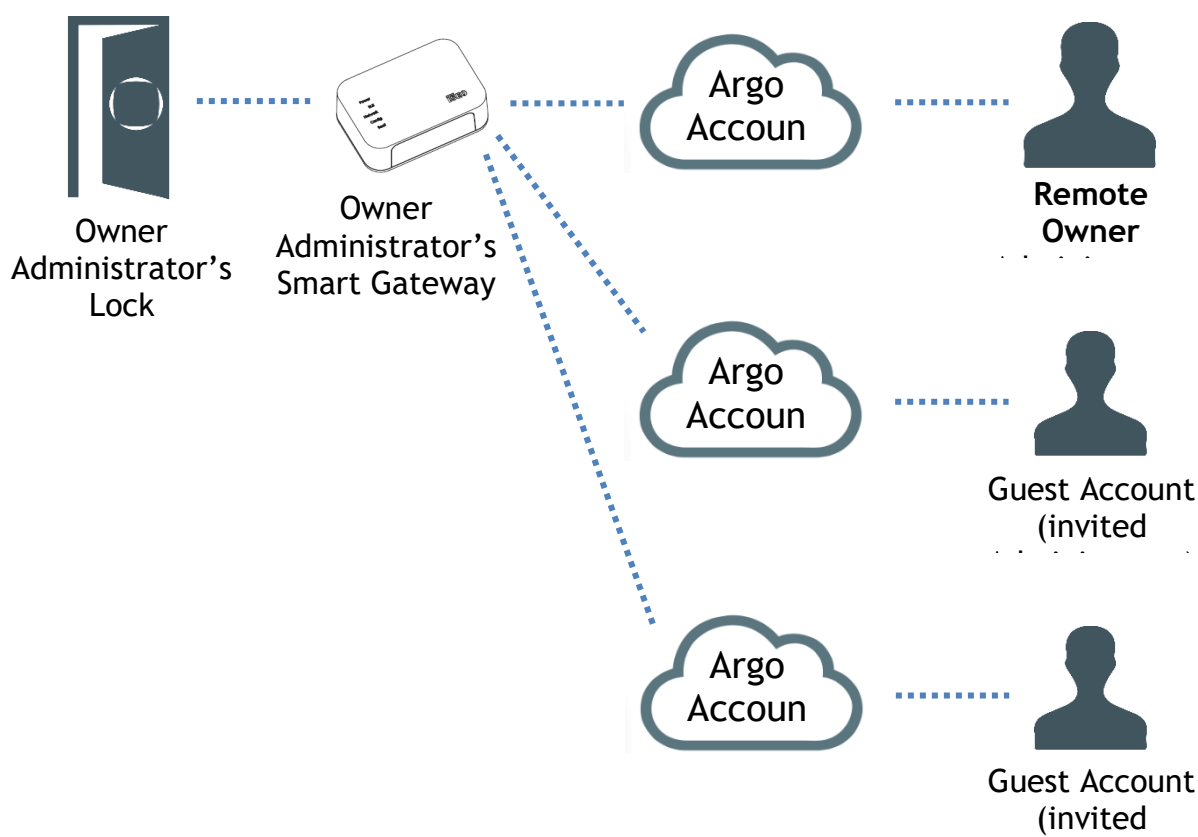
Guest Account



Advanced

The *Remote Administrator*, the first one who created the *Argo Account*, configured the *Smart Gateway* and added the locks to the system (see *Basics*), it is basically the owner of the Gateway, the owner of this system, that's why it is called *Remote Owner Administrator*. The *Owner Administrator* can also invite other Remote Administrators, to help him managing a lock from remote; for example, to open the door in case of emergency situations, or to login to add users or check events. These invited *Remote Administrators* are called *Guest Account*.

Guest Account must have a valid *Argo Account* to operate through the *ISEO Cloud*, but they don't need a *Gateway* since they will use the Owner Administrator's Gateway to communicate to the lock to which they are invited to.



Argo from Remote, differently from *Argo Local*, gives the possibility to assign different *Administrator's permissions* to the *Guest Account* (to find out more go to *Add Account*).


Add Account (invite Remote Administrator)

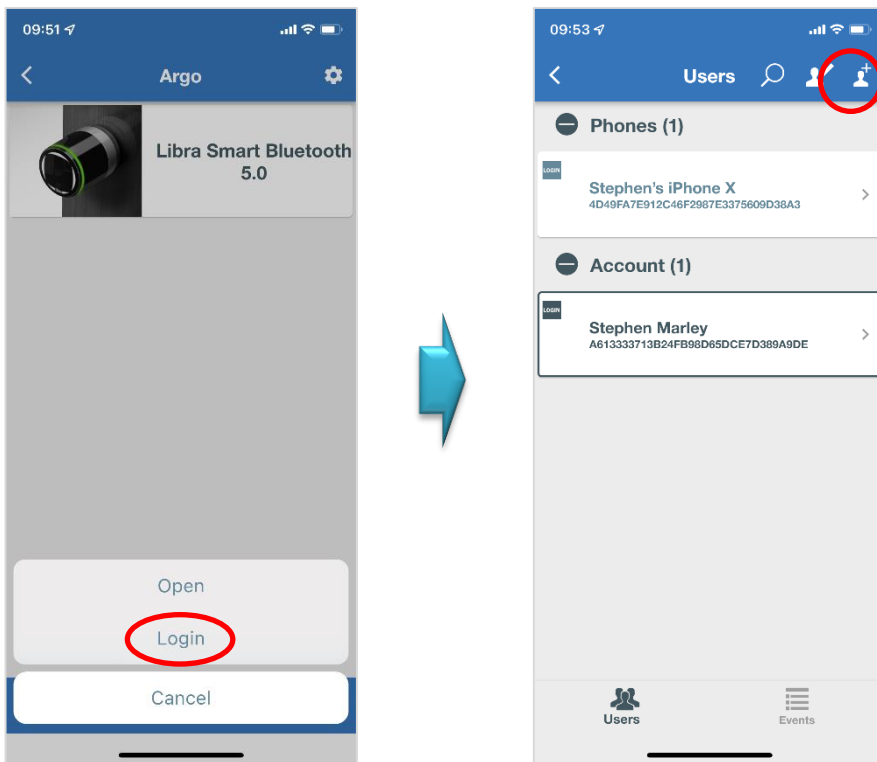


Advanced

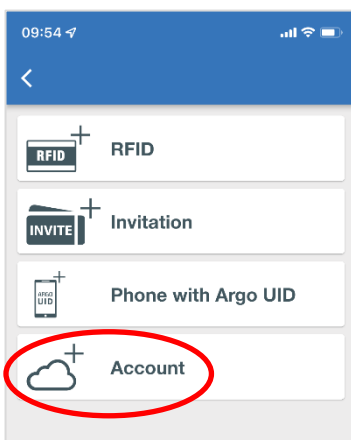
The *Remote Owner Administrator* can add one or more *Administrators* to help him managing the lock from remote. This function is called *Add Account* and allows to invite a new *Remote Administrator* called *Guest Account*. To add a *Guest Account* to the lock, proceed as follows.

1st Part: the Owner Administrator send the invitation to the Guest Account.

1. Login to the lock then tap **Add User** 

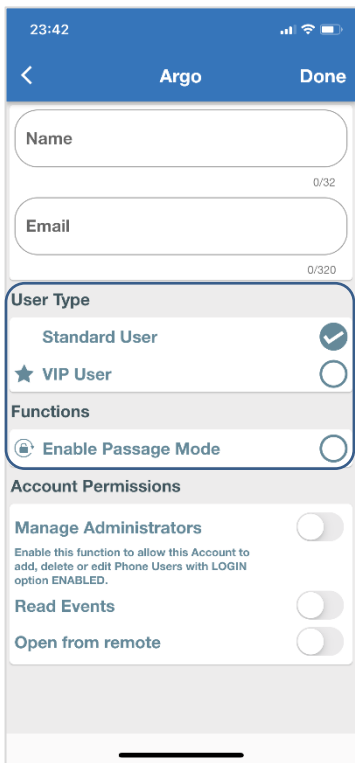


2. Tap **Add Account** 



3. Type **Name** and **Email** address of the *Account Administrator* to invite. Enable the required functions and the authorized permissions as showed in the picture below.

Advanced



Guest account name.

Guest account email address.

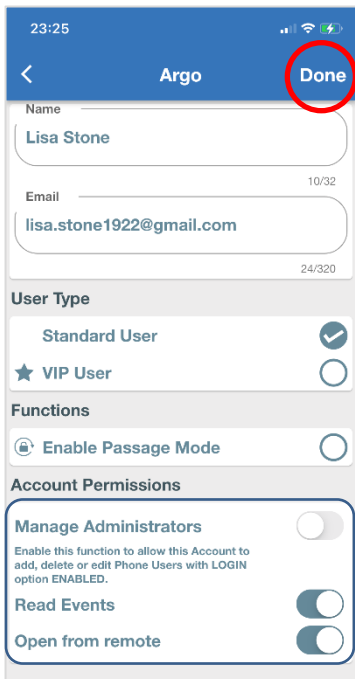
Standard Argo functionalities (to know more read the *Argo 2.7 User manuals* at *iseo.com*).

Go to *Manage Administrators* paragraph.

Enabling this function, the *Guest Account* will have the possibility to read the lock *Events*.

Enabling this function, the *Guest Account* will have the possibilities to open the lock from remote (the lock to which it has been invited).

4. Tap **Done** at the end.

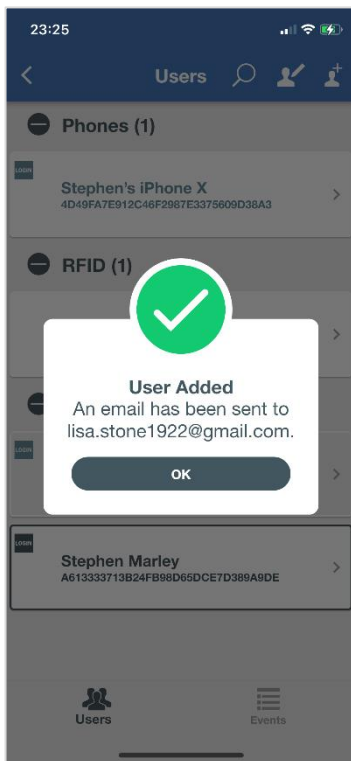


The *Invited Administrator* must have a valid *Argo Account* already registered in the *ISEO Cloud* otherwise he/she cannot be added as *Guest Account* (an error message occurs - to know more about errors go to *Troubleshooting*). It is possible to create an *Argo Account* without having any *Smart Gateway* and *Locks* configured.

In this example the *Invited Administrator* can **Read Events** and **Open from Remote** (enabled *Account Permissions*).

5. Wait the **User Added** confirmation message, then tap **OK**.

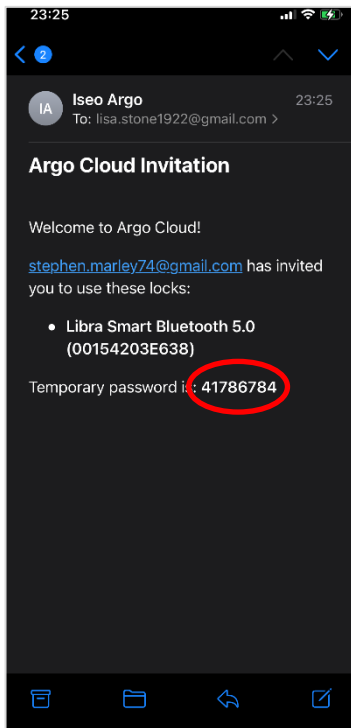
Advanced



Notifies the *Guest Account*, which will soon receive an invitation email.

2nd part: the Invited Administrator (Guest Account) receive the email.

1. The *Invited Administrator* receives an email like the example below.

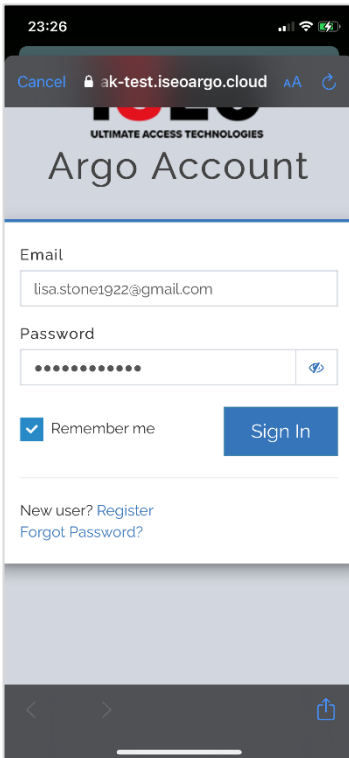


The *Temporary password* is automatically generated in the invitation message and it will be the *Account Lock Password*. It is necessary for the *Guest Account* to communicate to the lock (open and login).

For security reasons, once logged-in for the first time, the *Guest Account* should change the temporary password typing a personal one.

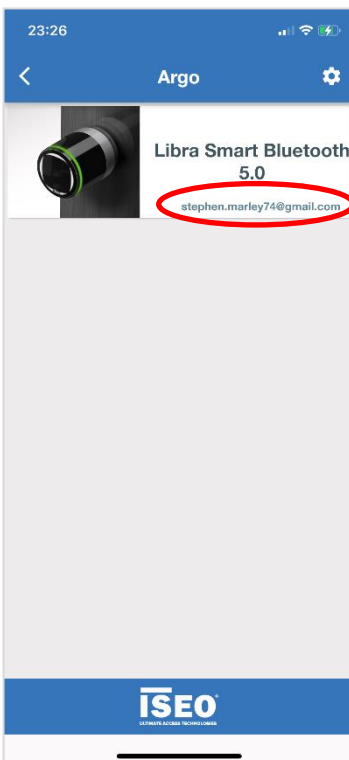
2. The *Invited Administrator* logs in to its Argo from *Remote Account*.

Advanced



The *Invited Administrator* must have a valid *Argo Account* in the *ISEO Cloud* otherwise he/she cannot be invited from the *Owner Administrator* (to find out how to set up a new Account go to *Basics, Create your Argo Account*). It is possible to create an *Argo Account* without having any *Smart Gateway* and locks configured.

3. The *Invited Administrator* will find the lock to which he/she has been invited to, in the *Argo from Remote Home page*.



The new lock belonging to the *Owner administrator* Stephen Marley, now appearing in the Lisa Stone Account home page.

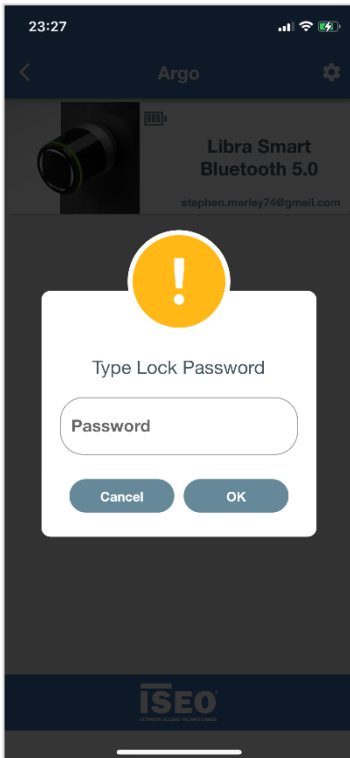


Underneath the lock name and icon, it is reported the *Owner Administrator* email address, to immediately notify this lock is belonging to another *Argo Account*.

The message *Configure your system* is not showed up since this *Account* will use the *Gateway* of the lock *Owner Administrator*. This *Account* can always add an own gateway in the *Gateways* menu.

4. Tap the lock name and icon to start the communication. The temporary *Lock Account Password* is required to connect to the lock.

Advanced

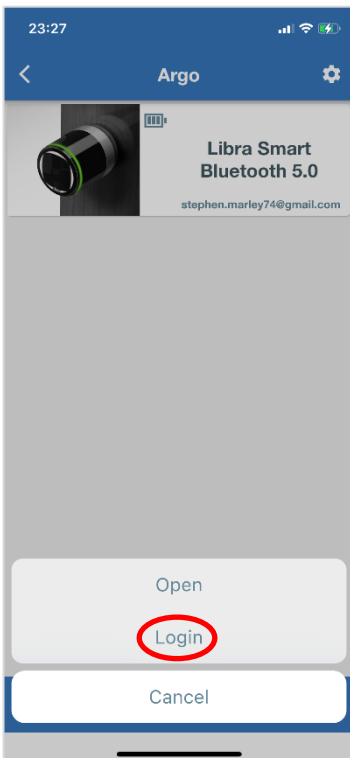


Type the temporary *Lock Password* received in the invitation email.



Enable *Face* or *Fingerprint* recognition in the *Manage Account* menu to associate the password to your phone biometric identification.

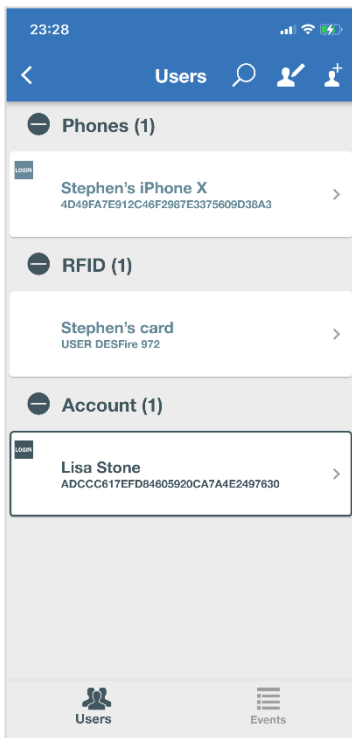
5. Tap Login.



Open available because enabled in the *Account Permission* by the *Owner Administrator*.

6. *Argo from Remote User List* appears.

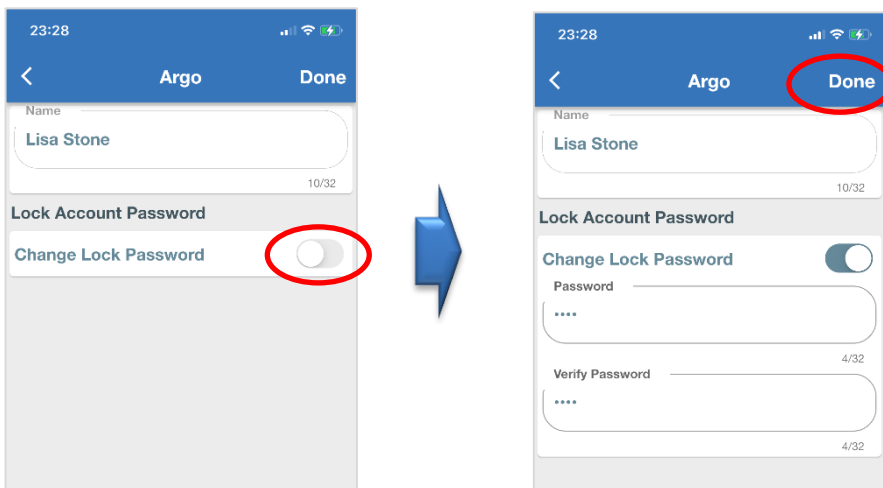
Advanced



The *Owner Administrator* account is not visible from the *Guest Account*. The latter in fact cannot change any setting of the lock owner.

————— *Guest Account*

7. Tapping on her *Account*, Lisa Stone can only change the *Lock Password*. For security reason it is strictly recommended to change the lock temporary password with a personal one. To change the password, enable the slide button, type the new password and press **Done**. The system will return to the *Argo from Remote Home* page. Finally tap the lock name and icon and insert the new password to connect.

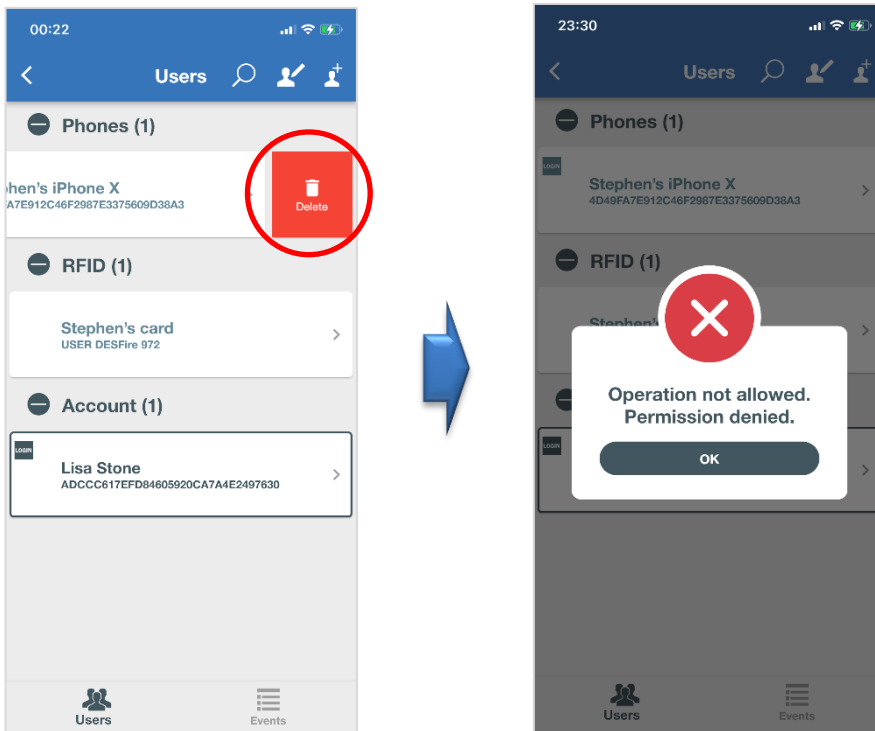


Enable *Face or Fingerprint* recognition in the *Manage Account* menu to associate the password to your phone biometric identification.

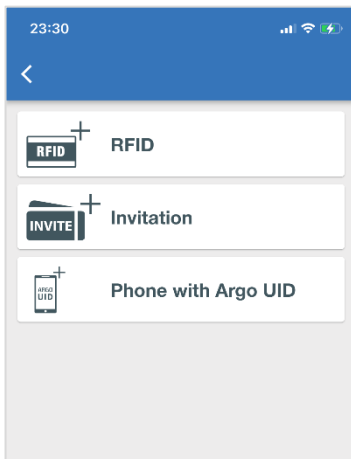
8. Considering the *Account Permissions* set by the *Owner Administrator*, Lisa Stone can *Open from Remote* and *Read Events*, but she cannot *Manage Administrators*. That means she cannot add, delete or edit *Phone Users* with login. For example: if Lisa Stone tries to delete the *Phone User*

Advanced

Administrator Stephen's iPhone, she will get the error message as per picture below, and the operation will not be completed.



9. Lisa can Login, Add, Edit or Delete any type of credential, since these are the basic and fundamental operations for any *Administrator*. But she cannot add any *Guest Account* since she is not the owner of the lock.



Only the *Owner Administrator* can add *Guest Accounts* to his lock (invite other Administrators).

Delete the Account

Advanced

Deleting an *Account* is a critical operation since it involves all configured *Gateways* and *Locks*. An *Account* might also have one or more *Guest Accounts* sharing some of its locks.


To summarize, before deleting an *Account*, we need to take into consideration:

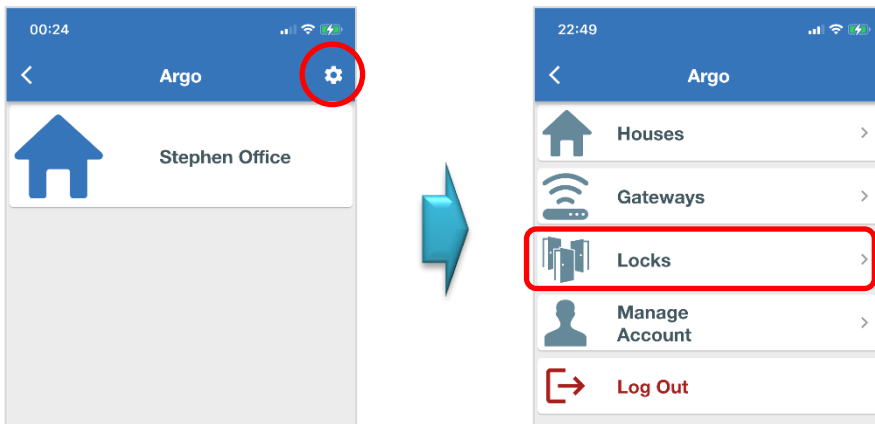
- Number of **Gateways** configured in the Account.
- Number of **Locks** connected to Gateways.
- Any **Guest Accounts** sharing one or more locks.



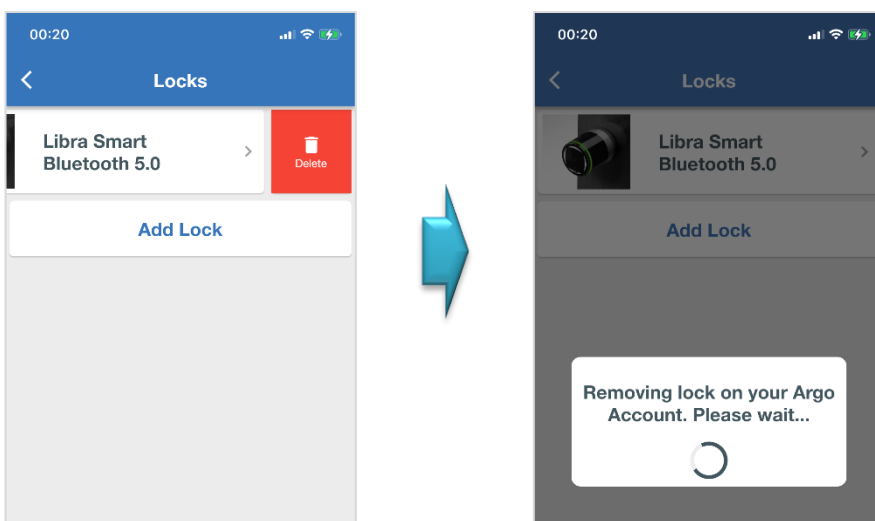
Only the *Owner Administrator* can delete his/her *Account* and the invited *Guest Accounts*. If the *Owner Administrator* deletes the *Account*, all the *Guest Accounts* belonging to it will be automatically deleted.

In the next example we're going to delete the *Account* previously created (*Basic, Create your Argo Account*).

1. Login to the **Account** and tap the menu icon  , then tap **Locks**.



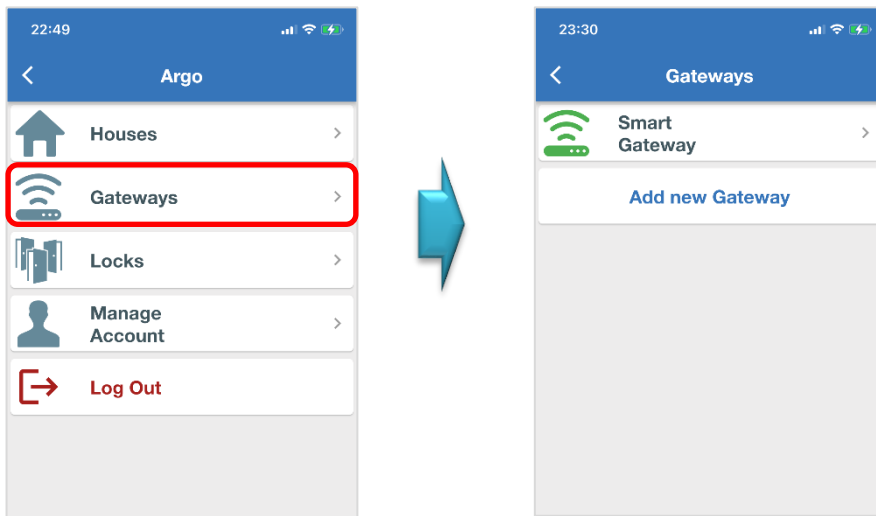
2. Delete all the **Locks** one by one, providing the lock password or by phone biometric identification.



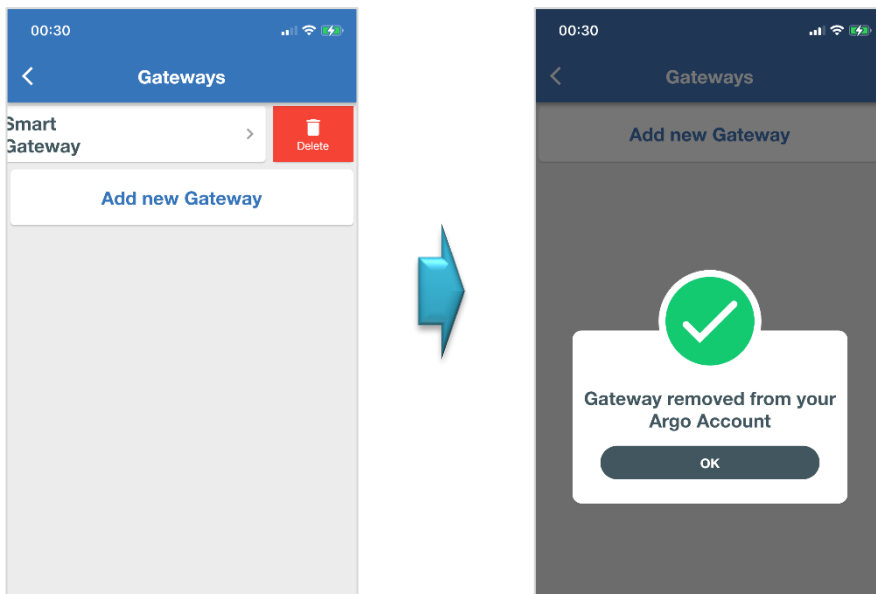
Removing a *Lock* from the *Owner Administrator Account*, the lock will be automatically removed from all the *Guest Account* invited, if any. The same happens when the *Owner Administrator* deletes the *Guest Account* from the Lock.


3. Go

Advanced



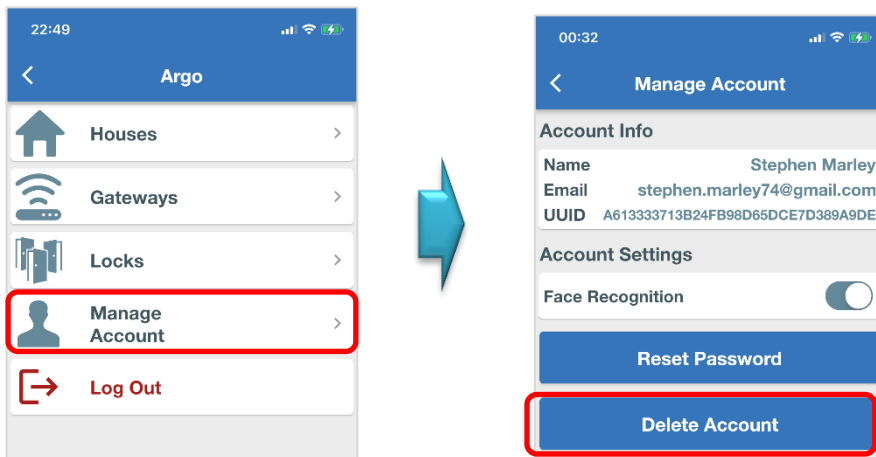
4. Delete the **Gateway**, always swiping from right to left, and confirm the message.



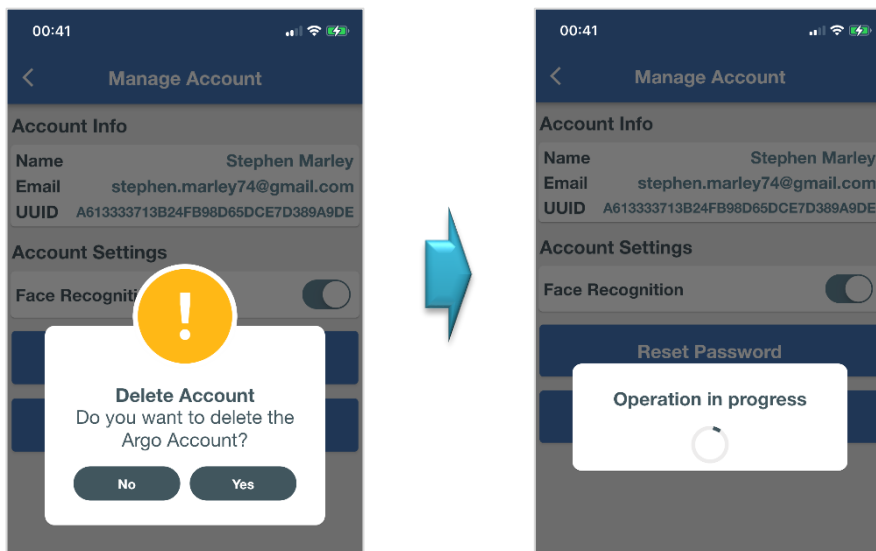
 A **Gateway** connected to a *Lock* cannot be removed and the app will give an error message. Be sure all the *Locks* have been deleted before deleting a *Gateway* (for more info about errors go to *Troubleshooting*).

5. Go back to the main menu and tap **Manage Account**, then tap **Delete Account**.

Advanced



6. Confirm **Yes** at the warning message and wait for the *Account* to be deleted.



- ! Any **Houses** will be automatically removed during the *Account* cancellation.
If you try to login to a deleted *Account*, you will get the message: *Invalid username or password*. This is showed for security reasons, to not reveal existing or not existing accounts when somebody tries inserting email address by chance.

Questions & Answers

Advanced

Below some of the most commons questions and the related answers.

1. Is the *Argo Account* secure? What happens if a hacker, in some way, enters my *Account*? Can the hacker open the door from remote or perform any other operation?

Answer: even if someone succeeds to enter your *Argo Account*, the hacker cannot perform any operation to the *Lock* since the *Account Lock Password* is required. And this password is stored in the most secure place: inside the lock. The *Account* is only used as a tunnel.

2. Is the *Gateway* secure? What happens if a hacker, in some way, reach and connect to my *Gateway*? Can the hacker open the door from remote or perform any other operation?

Answer: if someone is able to connect to the *Gateway*, the hacker cannot do anything since the *Gateway* is used only as a tunnel. No information is stored in the *Gateway*. The *Gateway* is just a tunnel used to reach and communicate to the *Lock*. All the relevant information are in the most secure place, inside the lock and protected by password.

3. How many locks can be connected to a *Smart Gateway*?

Answer: there are not a defined number. The *Smart Gateway* act like a smartphone with *Argo*, so the answer is: all the locks in the *Bluetooth* range capability of the *Gateway*.

4. What happens if I have different *ISEO Smart Devices*, but they are further than 10 meters apart? Is it possible to configure more than 1 *Gateway* with the same *Account*, so all the smart devices can be connected and reached?

Answer: yes, you can add more *Gateways* to your *Argo Account*, to reach different locks far away from each other.

5. Can I connect *Bluetooth 4.0 ISEO Smart Devices* to the *Gateway*? Does the *Gateway* also work in *Bluetooth 4.0* technology?

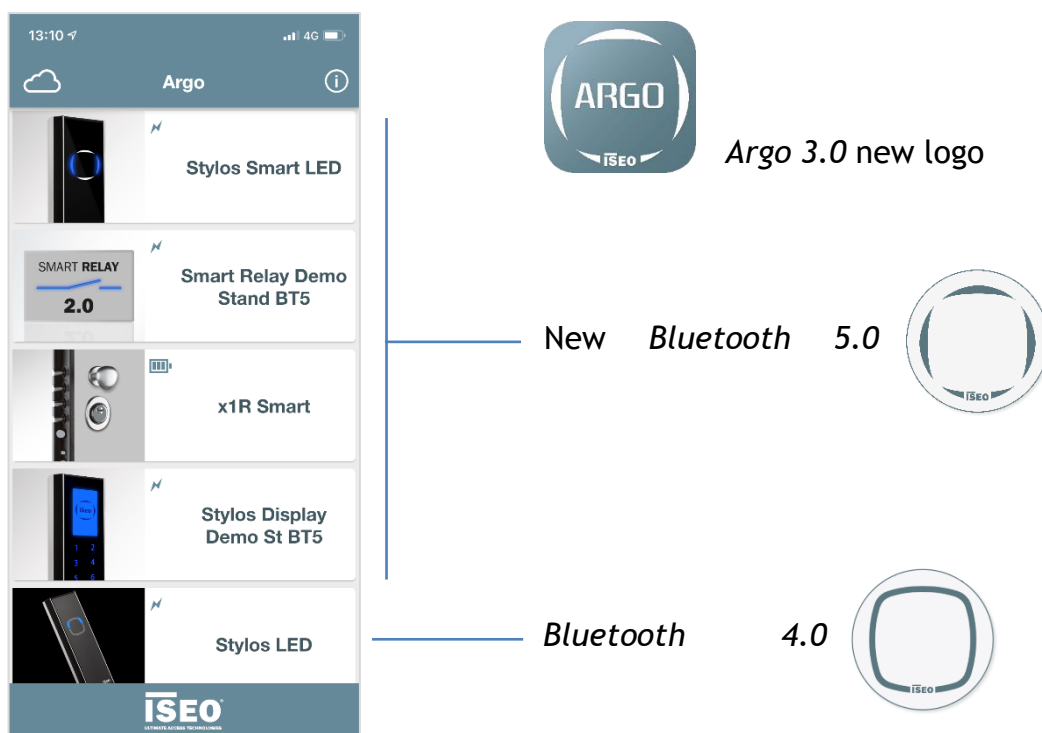
Answer: no, the *Smart Gateway* is only compatible to *Bluetooth 5.0 ISEO Smart Devices*, and it only works via *Bluetooth 5.0* technology. This technology in fact allows multiple connections at the same time, that is mandatory to work with *Argo from Remote*.

6. How can I recognize *Bluetooth 5.0 ISEO Smart Device*?

Answer: you can recognize it by the new logo design, aimed to show the *Bluetooth 5.0* technology evolution. The new logo is printed in all the *BLE 5 ISEO Smart Devices* aesthetic covers. It is also possible to recognize

Advanced

Bluetooth 5.0 ISEO Smart Device by the Argo app: the new devices come up in the *Home* screen with a new icon showing the new logo design.



7. Can I upgrade *Bluetooth 4.0 ISEO Smart Devices* to *Bluetooth 5.0* technology, to manage them from remote through a *Smart Gateway*?

Answer: no, all the *Bluetooth 4.0 ISEO Smart Devices*, except *x1R Smart*, cannot be upgraded to *Bluetooth 5.0*. It is necessary to replace the entire device to manage it from remote. *x1R Smart* is the unique exception because this lock is composed by 2 devices: the mechanical lock inside the door and the credential reader, that embeds the *Bluetooth*, usually placed on the outside of the door. To upgrade *x1R Smart* to *Bluetooth 5.0* you need to:

- Replace the entire reader with a *Bluetooth 5.0* version.
- Upgrade the *x1R Smart* firmware by a service app called *ISEO App Tool*. Tutorial video available at link: <https://www.youtube.com/watch?v=W0gmzzra0f8>



This operation is only intended for competent and properly trained installers or staff

8. *Argo Local* allows 300 *Users* to be memorized in the door-lock. What happens when I add a *Gateway* and the *Lock* in the *Argo Account*? Does it change the *Users* capability of the *Lock*? **Answer:** yes, during the configuration the *Gateway* and the *Owner Administrator Account* are registered in the *Lock* memory. These are considered 2 credentials: that's why the users' capability changes. For example: if 300 *Users* then becomes

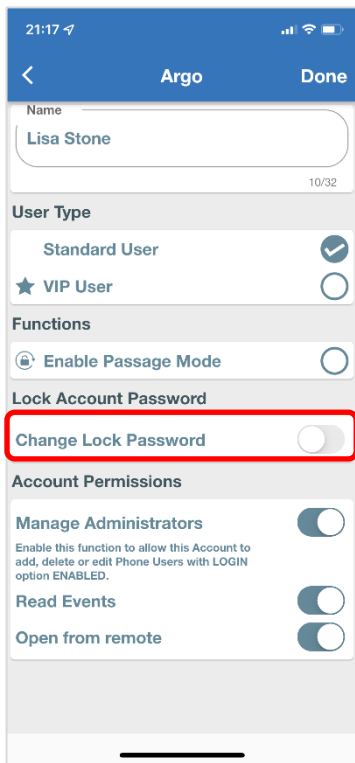
Advanced

298 Users. This is due to the principle of working of Argo called *data on device*. And this is also the strongness of Argo about security: the *Gateway* is just used as a tunnel; all the data are in the most secure place, inside the lock.

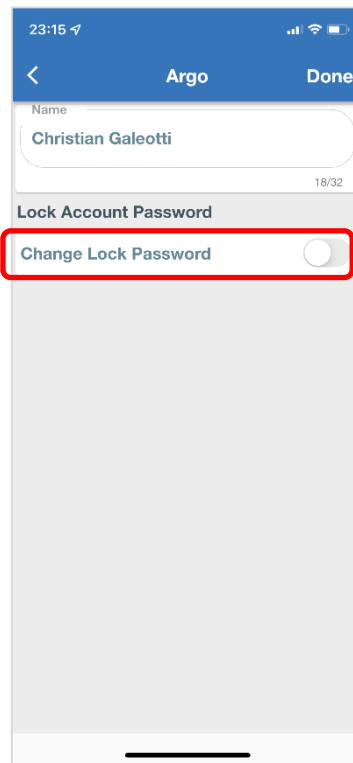
9. Where can I change the *Lock Account Password*? I cannot find it.

Answer: the *Lock Account Password* is stored in the most secure place, inside the lock. It is strictly related to each lock and can differ from lock to lock, depending on Administrator's choice. It also differs from *Account* to *Account* when different *Remote Administrators* manages the same lock (*Guest Accounts*). That's why to change it you need to *Login* to the specific lock, enter the *Administrator Account* settings and change the *Lock Account Password*.

Lock Password - Owner
Administrator Account setting



Lock Password - Guest
Administrator Account



10. How can I disconnect a *Lock* from a *Gateway*?

Answer: in the *Argo Account*, go to *Lock* menu and then delete the *Lock* from the *Account* (simply swiping from right to left). Note that: if you *Reset to Factory* the lock by *Argo Local*, the lock will be also removed from the *Account*.

Advanced

11. Does the *Gateway PoE* also work via WiFi?

Answer: no, the *Gateway PoE* doesn't have WiFi on-board; it can only be connected to a router LAN port via Ethernet cable. And it can be both powered by the router through a PoE port or by an external power supply unit if the router doesn't provide the PoE port.

12. I don't remember the *Lock Account Password*. What can I do?

Answer: for security reasons there's no way to recover the *Lock Account Password*. The unique solution for the *Administrator* is to delete the *Lock* from the *Account* (see *Advanced, Locks, Delete a Lock*), and then re-add it again by using the proprietary *Master Card* (see *Advanced, Locks, Add a Lock*).

13. Are there any phones that are not *Bluetooth 5.0* compatible?

Answer: no, all *Bluetooth 4* compatible phones are automatically compatible with *Bluetooth 5.0*.

14. *Bluetooth 5.0* is multi-channel, meaning it allows multiple connections at the same time. But how many users can connect to a lock at the same time?

Answer: to preserve optimal system performance and usability, avoiding conflicts in operations, a maximum of 2 users can be connected. For example: a user who opens the door locally and at the same time an administrator user who remotely LOGIN into the lock. This is also the most common and frequent situation.

15. Is it possible to add more *Gateways* to the same system? How are they managed by the system? How does the lock know which gateway to report to?

Answer: yes, it is possible to add more *Gateways* just because the locks could be more than 10m away from each other. The Gateway-Lock assignment takes place during the configuration process and is managed by the Argo app, which automatically connects to the closest gateway (powerful signal) and consequently associates the lock with it. Even during remote connection, the process is automatically managed by the app.

16. Is it possible to open the door while an administrator user is connected from remote and he's performing operations on the lock?

Answer: yes, it is possible because *Bluetooth 5.0* is multi-channel (see also point 14).

17. Can I change the lock name from remote?

Answer: no, the name of the lock can only be locally changed. It will then be automatically updated from remote at the next Argo Account login.

Advanced

18. Can I add a fingerprint for x1R Smart from remote?

Answer: no, the fingerprint can only be added locally. This is due to the need of a direct user's interaction that is required during fingerprint registration. You can remotely add PIN codes, UID credentials, phones and invitations.

19. Can anyone open an *Argo account* even if they have no locks or *Gateway*?

Answer: yes, anyone can open an *Argo account*. It is just required a valid e-mail address and a free-choice password. For example: an administrator invited by the owner must necessarily register an *Argo account*, even if he does not own any system. This in order to be able to manage the lock to which he has been invited.

20. Is it possible to share the same *Gateway* between different *Argo accounts* owners with different system codes (*Master Card*)? This is the case, for example, of the common door of a condominium shared between the various apartments, where each apartment is a distinct Argo system.

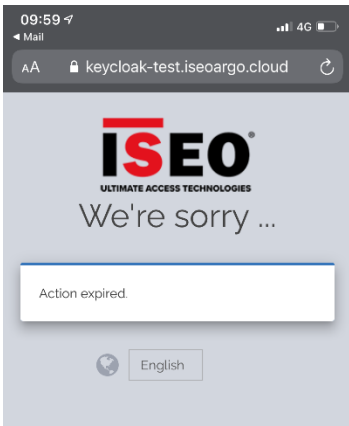
Answer: no, for security and reliability reasons of the system and of the software structure, a *Gateway* is assigned to a single system and the owner administrator is unique. The owner administrator can still invite other administrators to manage the lock. In the case of the example of the common door of the condominium, it can be managed by the condominium administrator who will be able to guarantee access to the tenants managing their access authorizations accordingly.

Troubleshooting

See below the most common errors messages and the related explanation.

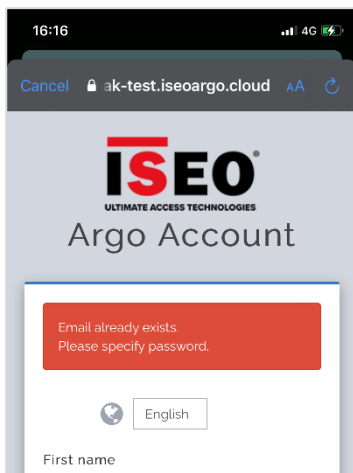
Error	Meaning	What to do
-------	---------	------------

Advanced



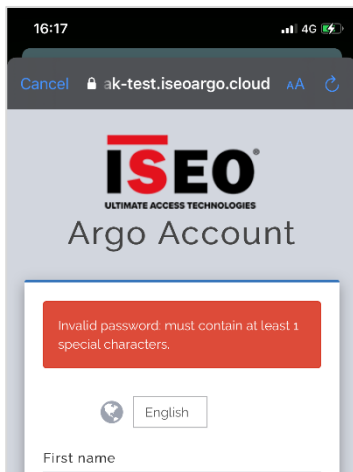
You took too much time to complete a step in the Account registration procedure. For security reason there is a time-out and once expired you get this error message.

Repeat the operation faster.



You inserted an already existing email during the Argo Account registration.

Choose a different email address to register a new account or use the already existing one.

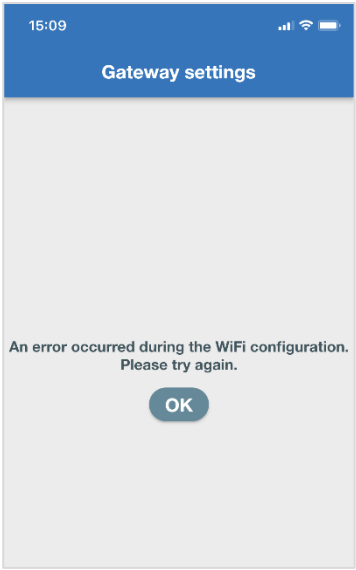
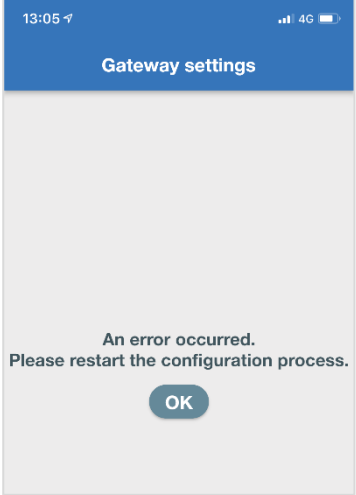
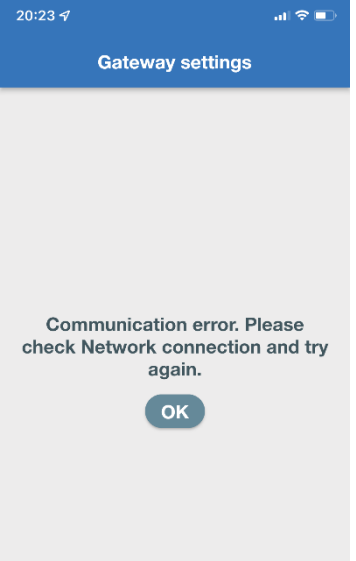


You didn't type a strong rule password.

Please type a password with at least 8 characters that contains 1 capital letter, 1 number and 1 special character.

Error	Meaning	What to do
-------	---------	------------

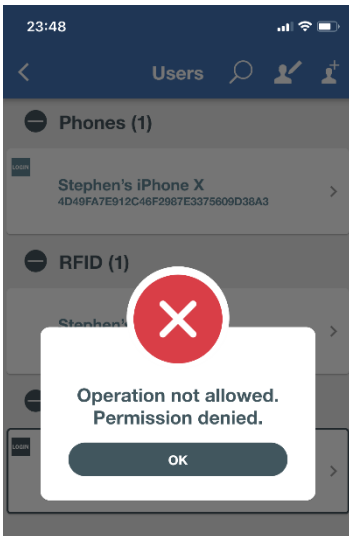
Advanced

	<p>This error could happen during the Gateway configuration, at the 1st step, when the Gateway is trying to connect to the WiFi router. This usually means wrong router password inserted.</p>	<p>Tap OK to restart the process and try again. Take care to insert the correct router password. Use the password view function to double-check the password.</p> <p>If the problem persists check your WiFi router if reachable by any other device (PC, Smartphone, tablet).</p> <p>If the problem cannot be solved, please contact the <i>ISEO Service Operation Center</i> (go to <i>Technical Support</i>).</p>
	<p>This error could happen during the Gateway configuration, at the 1st step, when the Gateway is trying to connect to the WiFi router. The password is correct but for some reason, the router rejected the Gateway connection.</p>	<p>Tap OK to restart the process and try again.</p> <p>If the problem persists check your WiFi router if reachable by any other device (PC, Smartphone, tablet).</p> <p>If the problem cannot be solved, please contact the <i>ISEO Service Operation Center</i> (go to <i>Technical Support</i>).</p>
	<p>This error could happen during the Gateway configuration, at the 2nd step, when the Gateway is trying to connect to the ISEO Cloud, to be loaded in the Argo Account. For some reason the communication between Gateway and Cloud failed. This problem can be caused by different issues:</p> <ol style="list-style-type: none"> 1. Slow Internet connection 2. Firewall blocking the communication 3. Error during data exchange 	<p>Tap OK to restart the process and try again.</p> <p>If the problem persists check your Internet connection: check if any other device like PC, Smartphone, can surf the web as usual. Perform an Internet speed test to check the communication performance.</p> <p>If the problem cannot be solved, please contact the <i>ISEO Service Operation Center</i> (go to <i>Technical Support</i>).</p>
<p>Error</p>	<p>Meaning</p>	<p>What to do</p>

Advanced

	<ol style="list-style-type: none"> 1. Your Account has just been deleted 2. The ISEO Cloud is not reachable. 	<ol style="list-style-type: none"> 1. If you have just deleted your Argo Account this is a correct message. 2. Try again later and check your device Mobile or WiFi Internet connection. If the problem persists, please contact the <i>ISEO Service Operation Center</i> (go to <i>Technical Support</i>).
	<p>This error could happen at the beginning of the Gateway configuration, during the QR-Code reading. The system warns you that this Gateway has already been registered in the ISEO Cloud.</p>	<ol style="list-style-type: none"> 1. Use a different Gateway since this has already been assigned to an Argo Account. 2. Delete this Gateway from the current Argo Account and then you can use it for another Account. Note: to connect the Gateway to another Argo Account you will need to reset it as showed in the configuration wizard.
	<ol style="list-style-type: none"> 1. The Lock Account Password is not correct. 2. The Lock Account Password has been associated to the smartphone Biometric Identification, but later this password has been changed. The phone at the first attempt recalls from the memory the first associated password, that actually has changed: that's why it is no longer correct. 	<ol style="list-style-type: none"> 1. Insert the correct Lock Account Password. 2. Repeat the procedure: the app will ask to manually type the new password after the Biometric Identification failed 2 times.
<p>Error</p>	<p>Meaning</p>	<p>What to do</p>

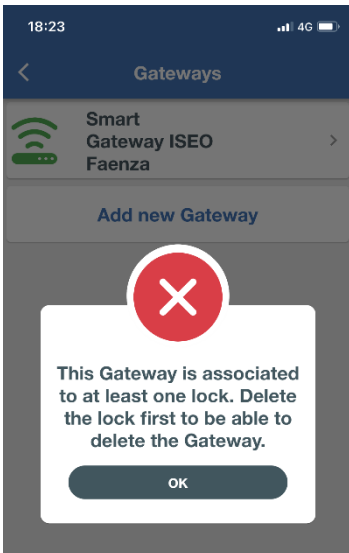
Advanced



In this example a Guest Account was trying to delete a Phone User with Login (Local Administrator), without having the Manage Administrators permission enabled by the Owner Administrator.

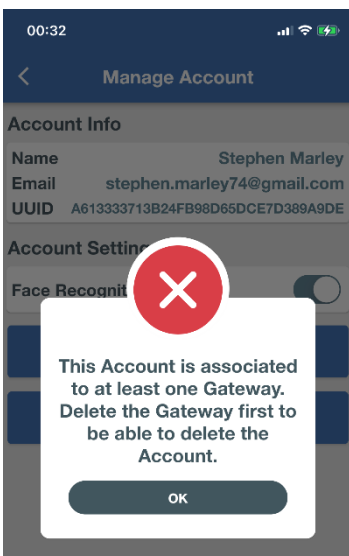
You cannot perform operations not authorized by the Owner Administrator. Ask the permission to the Owner Administrator.

The same error happens every time the Guest Account try to make an operation not allowed by the Owner Administrator (i.e. Open Door, Read Events)



In this example the Owner Administrator is trying to delete the Gateway but there are locks configured in the system.

Delete all locks first, one by one, then at the end you can delete the Gateway.

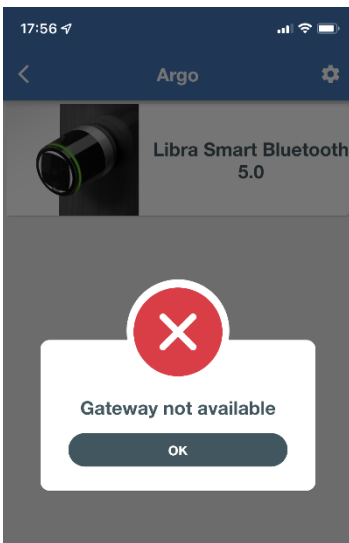


In this example the Owner Administrator is trying to delete the Argo Account but there is a Smart Gateway configured into the system.

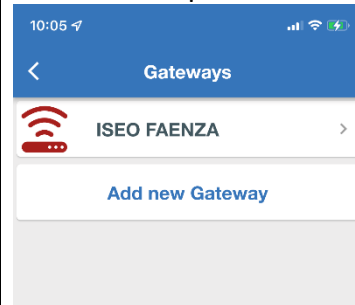
Delete the Smart Gateway first (deleting all the locks before), and finally you can permanently delete the Argo Account.

Error	Meaning	What to do
-------	---------	------------

Advanced



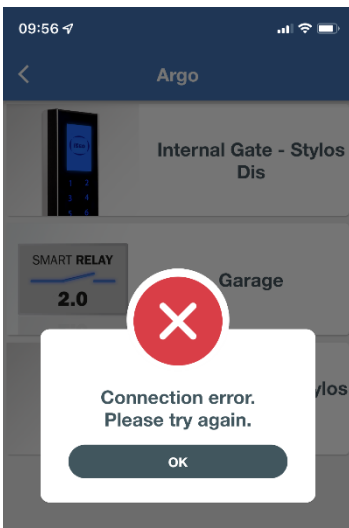
The Smart Gateway is not reachable. It could be OFF or for some reason not properly working. The icon in the Gateway menu is red like the example below.



Check if:

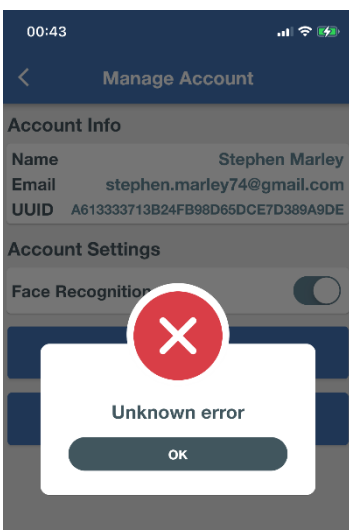
- The Gateway is ON with the Network led ON.
- The Gateway is correctly installed to communicate to the router.
- The router is properly working.

If YES, all the above, restart the Gateway and check if it is now working. If the problem cannot be solved, please contact the *ISEO Service Operation Center* (go to *Technical Support*).



A problem happened trying to connect to the locks from remote. The Gateway is available, but the locks cannot be reached.

- Check locally if the lock is properly working.
- Replace the lock battery if empty.
- Check the lock position if in the Gateway Bluetooth range.



An unexpected and unknown error happened. This error has not been yet translated in the system. A numeric code inside square brackets might follow the text (software error code).

Try the operation again to check if it is a recurrence error.

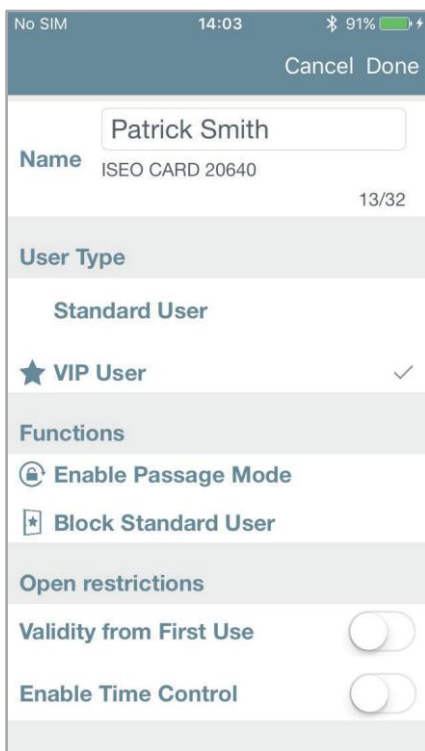
If the problem persists, please contact the *ISEO Service Operation Center* (go to *Technical Support*), providing the numeric code if present.

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 restrictions

- **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. Furthermore 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.

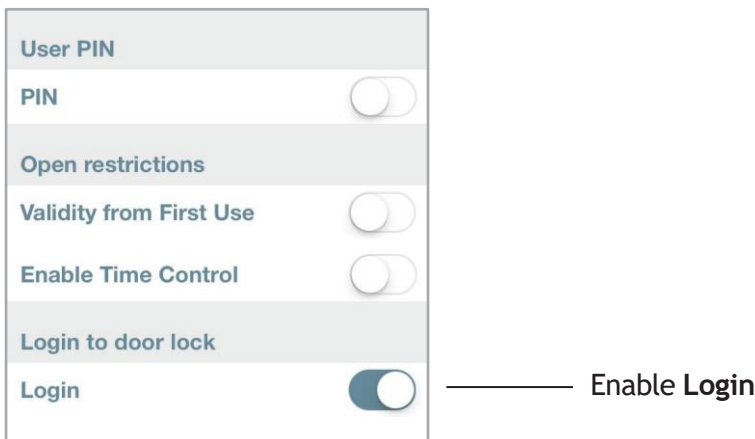
————— Enter the 4 digits *PIN code* and press **OK** to open the door.

Administrator Login without Master Card

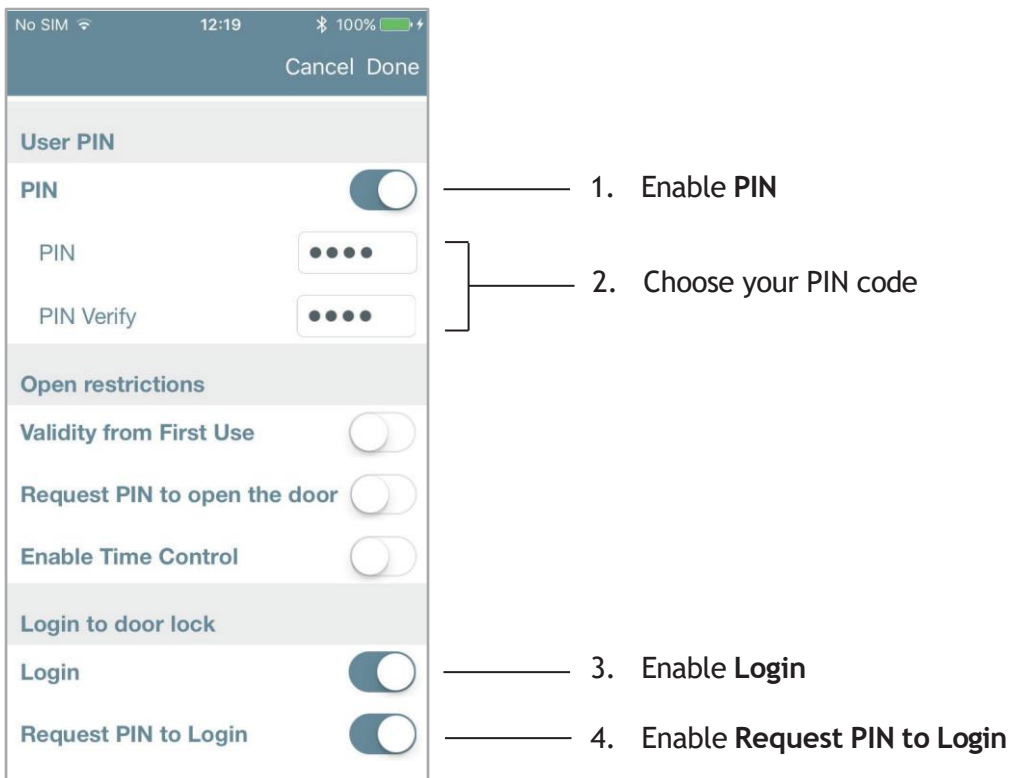
LOGIN

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 your maximum security, that will be asked every time you enter *Programming Mode*.

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



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



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.

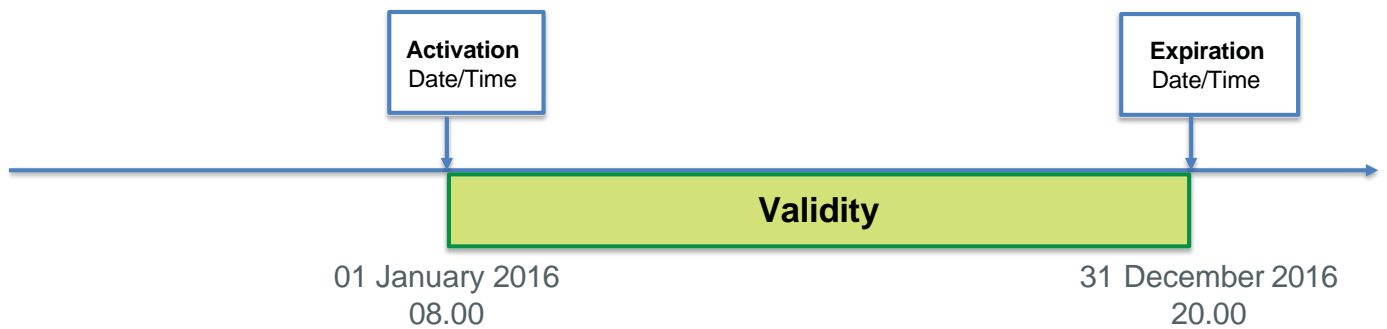
Advanced

Time Control

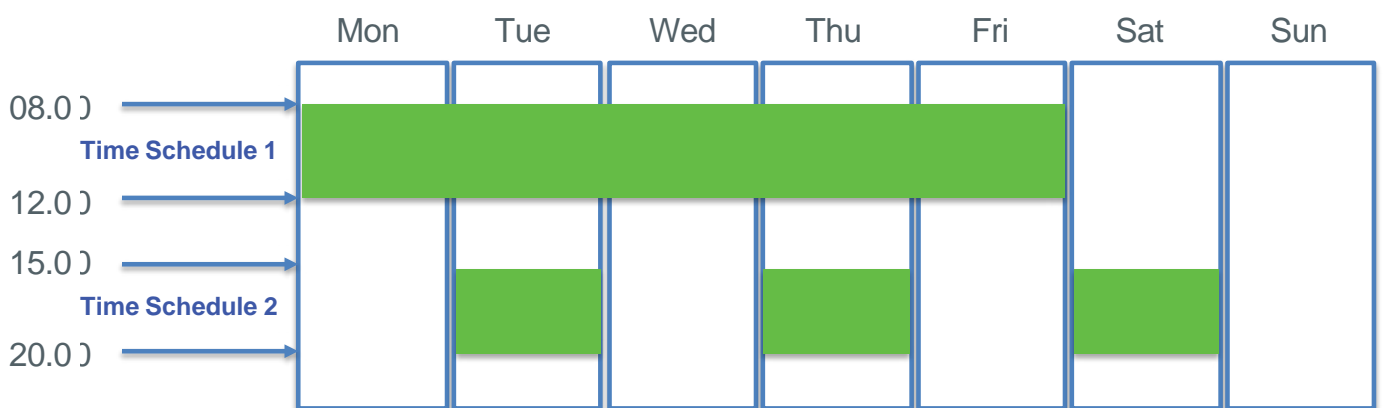


For every user you can set the *Validity*, composed by credential *activation* and *expiration* date & time, and 2 *Time Schedules*, selectable for each day of the week.

Validity



Time Schedules



Advanced

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

A screenshot of a mobile application interface. At the top, it shows 'No SIM', signal strength, time '11:21', and battery '100%'. Below the status bar are 'Cancel' and 'Done' buttons. The main content area has a header 'John Smith' and 'ISEO CARD 20640' with a '10/32' indicator. Under 'User Type', 'Standard User' is selected with a checkmark, and '★ VIP User' is also visible. Under 'Functions', 'Enable Passage Mode' is shown with a lock icon. Under 'Open restrictions', there are two toggle switches: 'Validity from First Use' (disabled) and 'Enable Time Control' (disabled).

Enable Time Control.

Validity

A screenshot of the same mobile application interface, but with 'Enable Time Control' toggled on. Below this, several fields are visible: 'Activation Date' (2/2/2018), 'Start time' (12:00 AM), 'Days' (7305), 'Expiration Date' (2/2/2038), and 'End time' (11:59 PM). At the bottom, there are two 'Time Schedules' (1 and 2), both currently set to 'No' with right-pointing chevrons.



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.

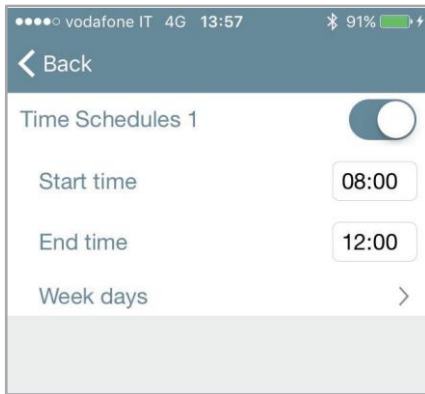
Tap to enable *Time Schedule*, configureable in time and day.



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

Advanced

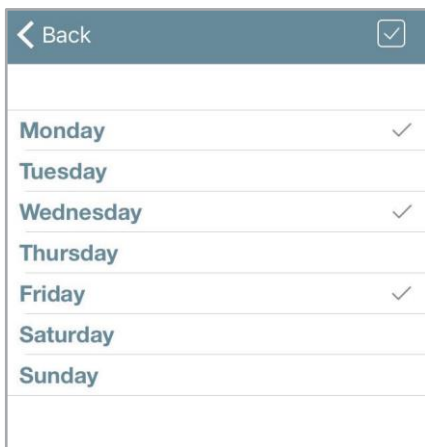
Time Schedules



Time Schedule 1 enabled.

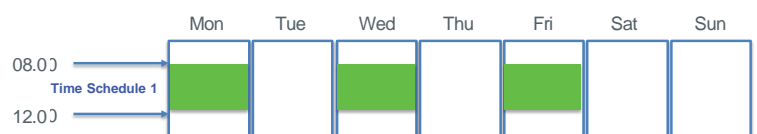
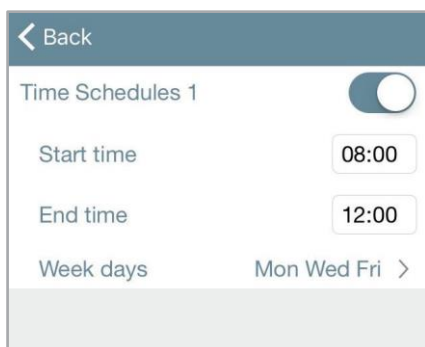
Set *Time Schedules* start and end time.
The default of *Time Schedule 1* is 8:00 - 12:00, while
the default of *Time Schedule 2* is 14:00 - 18:00.

Select the days.



Check/uncheck all days with one touch.

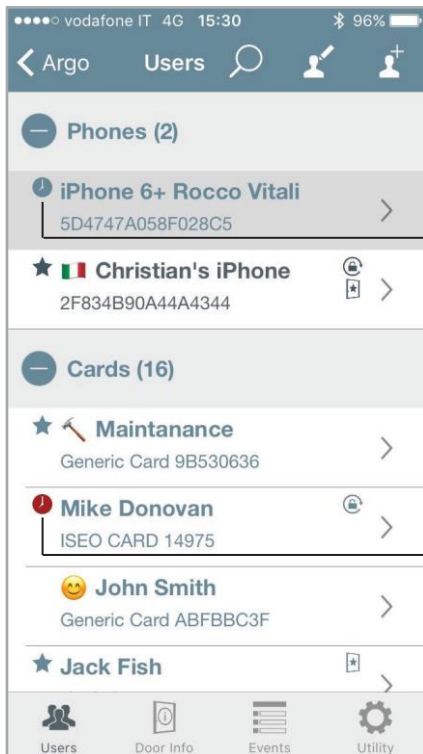
You can manually select multiple or single days.
In this example the user will access the door on
Monday, Wednesday and Friday.



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

Advanced

User list overview

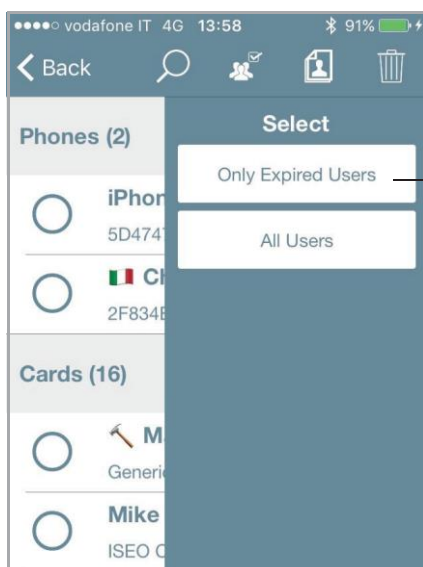


The clock means that user has enabled the *Time Control*.

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.

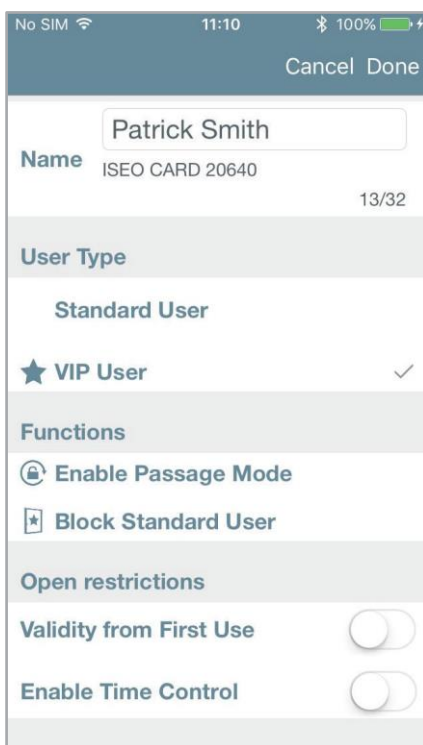
See also *Delete users* paragraph on *Basics* chapter.

Validity from First Use

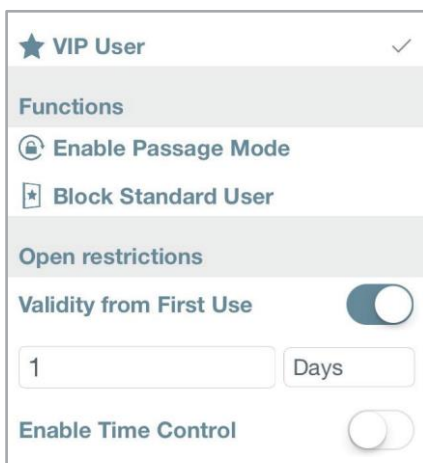


For every user you can set the credential *Validity from First Use*, in minutes, hours or days. With this function enabled the set credential validity will start at the moment of the first use, to access the door. *Validity from First Use* can be also combined with the *Time Control Validity (Activation 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.



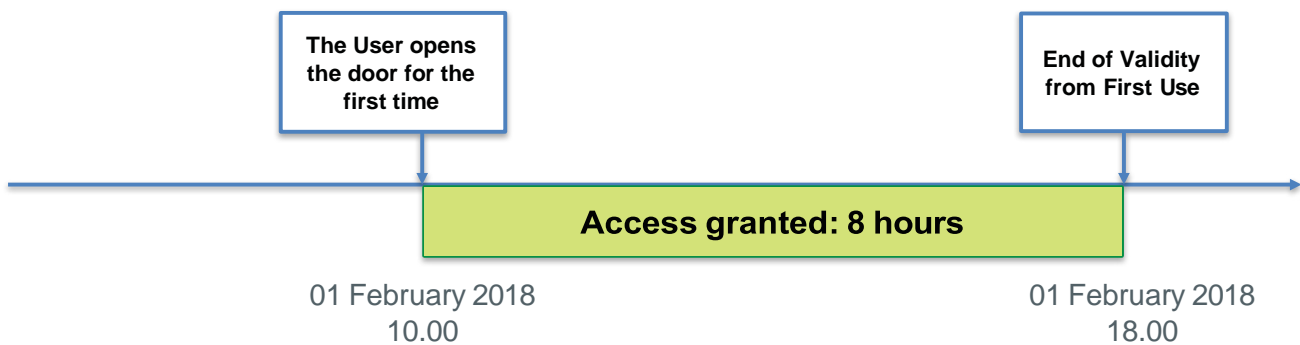
Select the validity in Minutes, Hours or Days.

Advanced

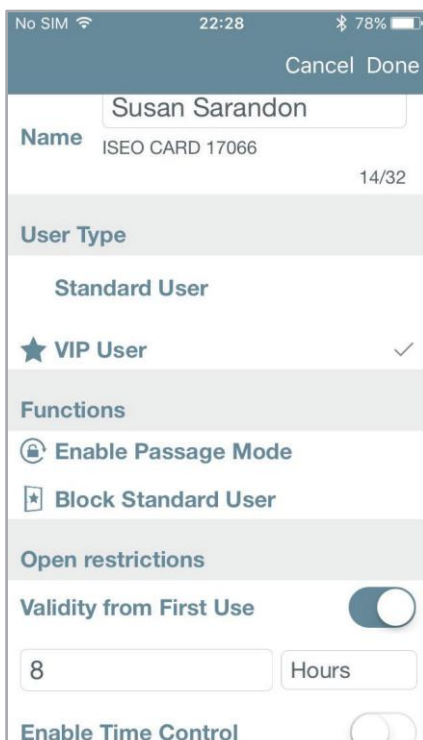
When the *User* opens the door for the first time, the *Validity from First Use* become the date and the time of that moment, and the credential will expire according to the validity set. To show what's happens on the *Argo* app using the *Validity from First Use*, see the next examples.

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*.

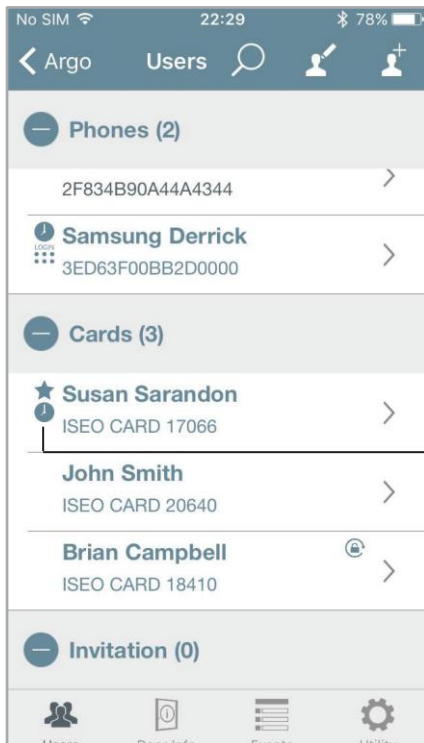


Enable Validity from First Use

Set 8 Hours

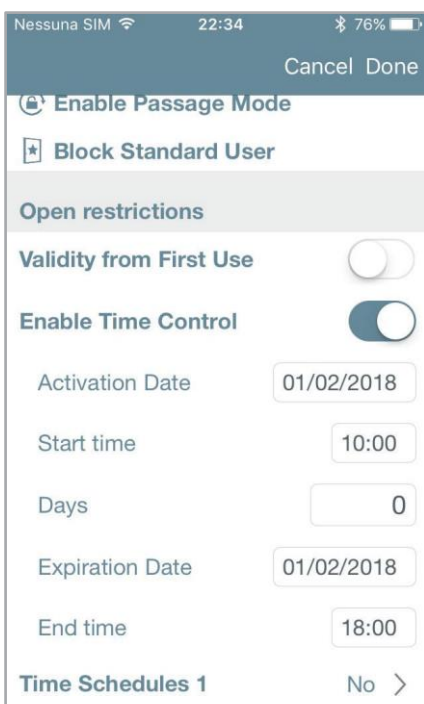
Advanced

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.



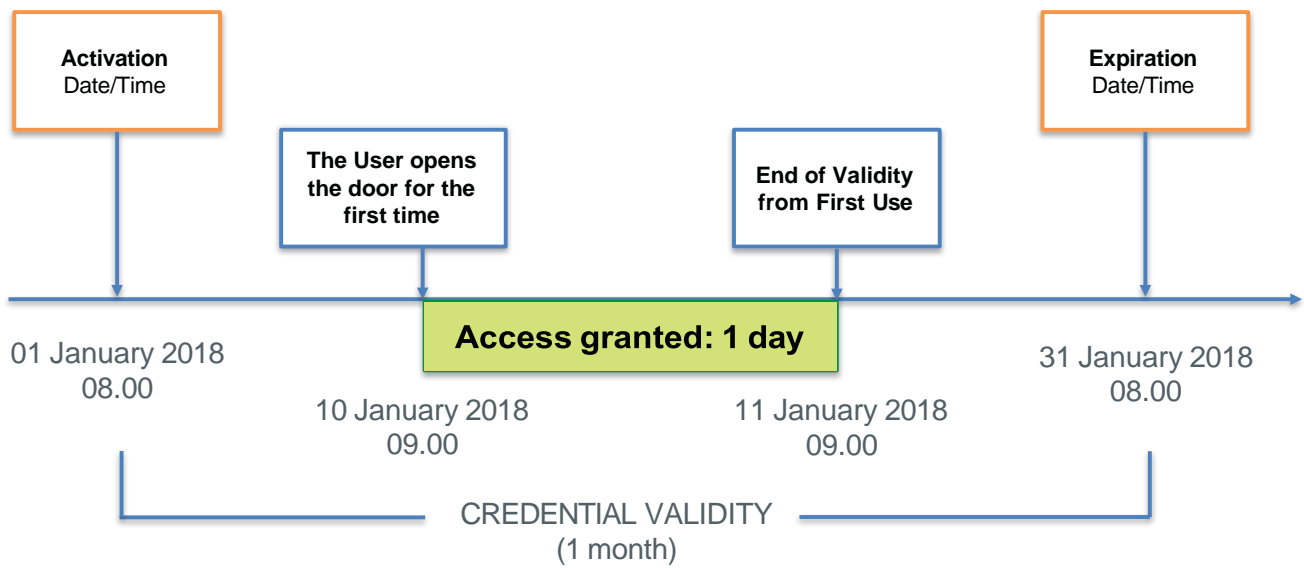
The **Validity from First Use** is now disabled since it has already been used.

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**.

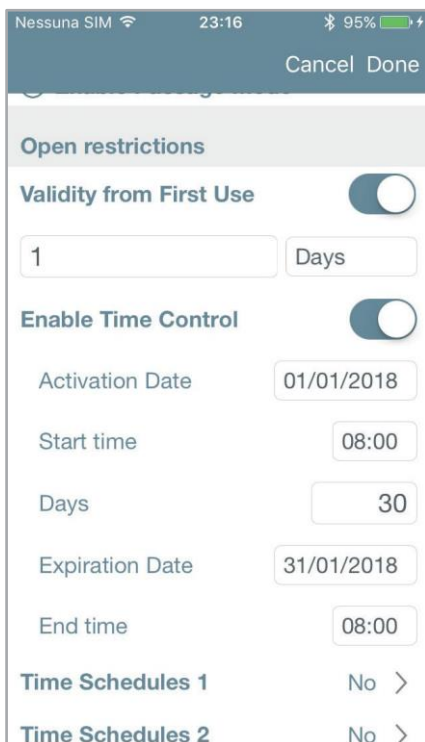
Advanced

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

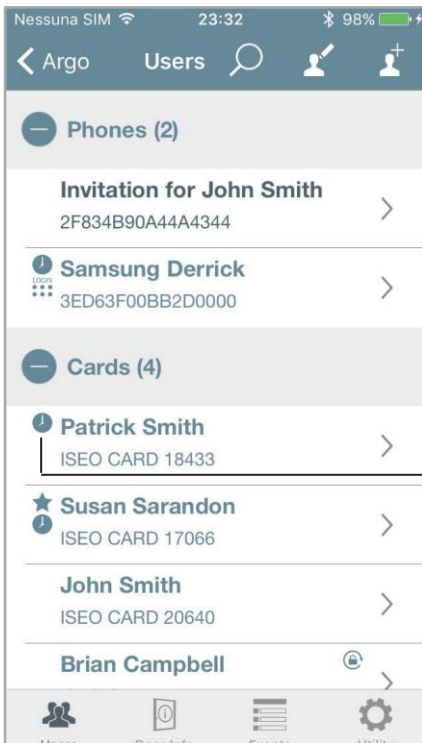
Set 1 Days

Enable Time Control

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

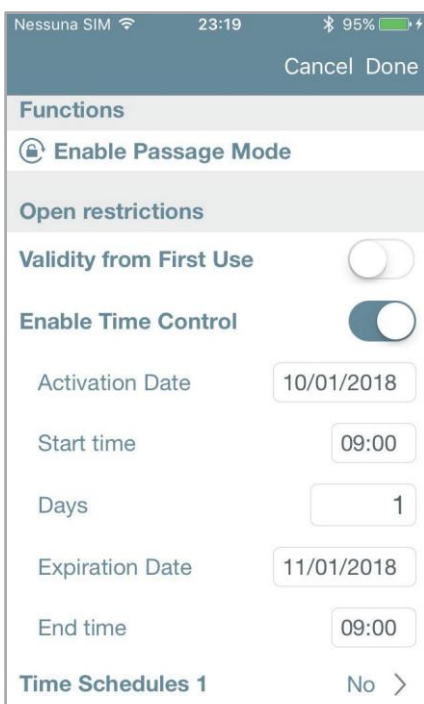
Advanced

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.

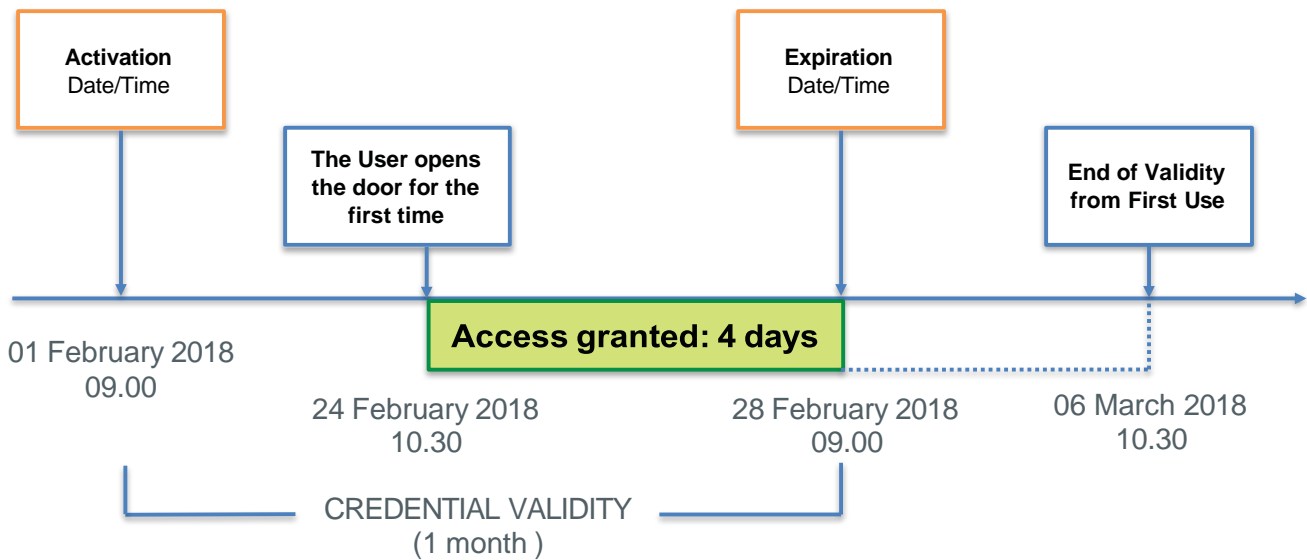


The **Validity from First Use** is now disabled since it has already been used.

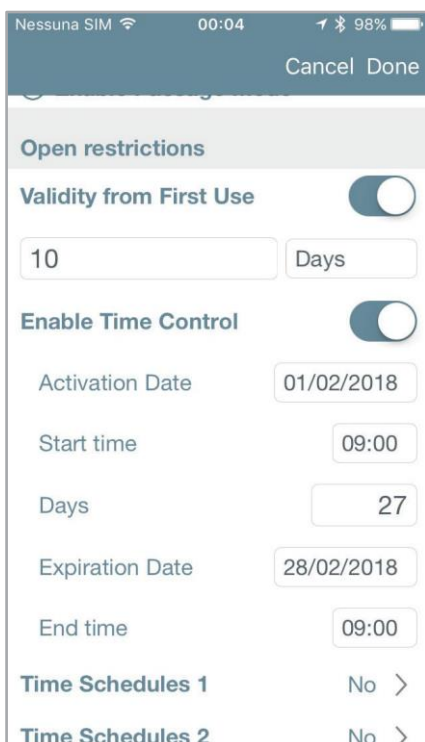
In the **Time Control** the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** are automatically set, adding 1 day to the **Activation Date**.

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*.



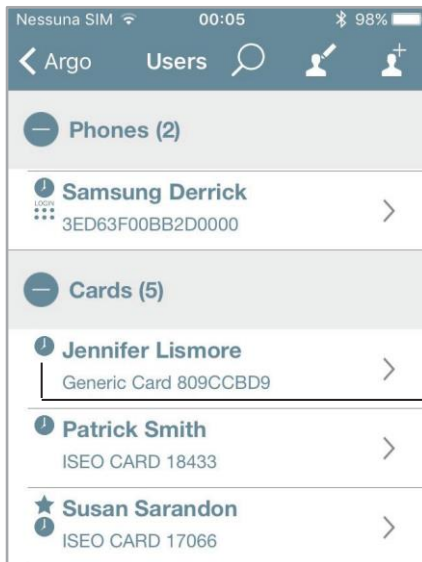
Enter *Programming mode*, then enter *Card or Phone User Parameters*.



- _____ 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.**

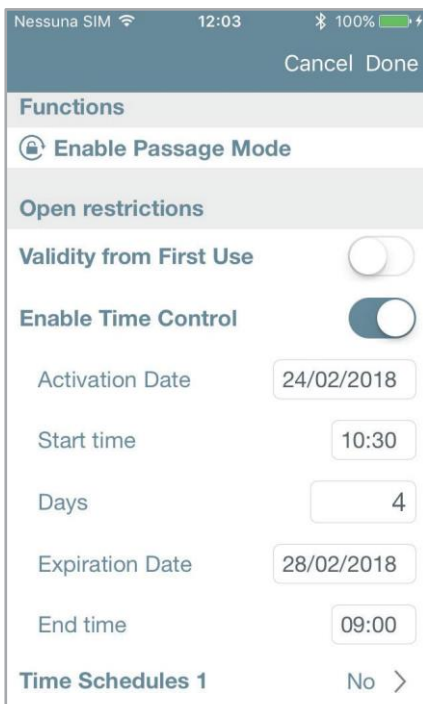
Advanced

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.

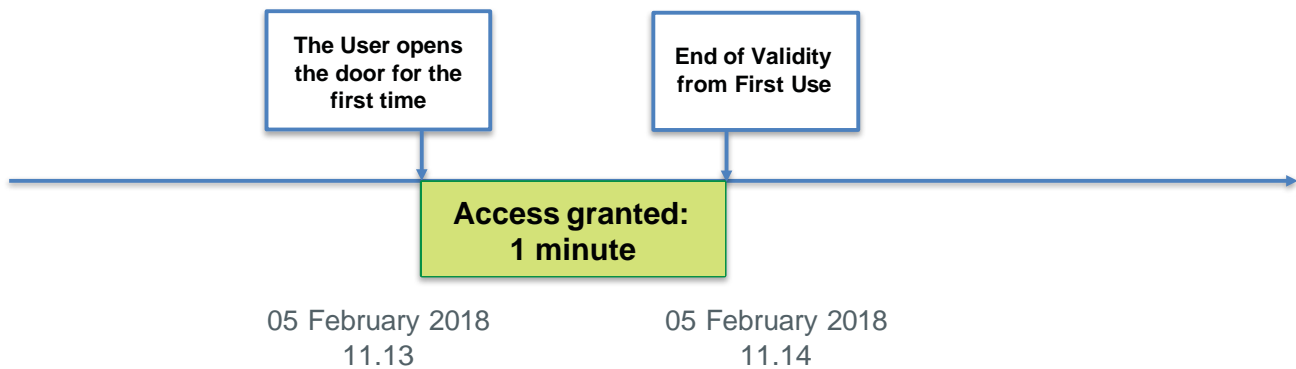
In the **Time Control** the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** remains the same previously set.



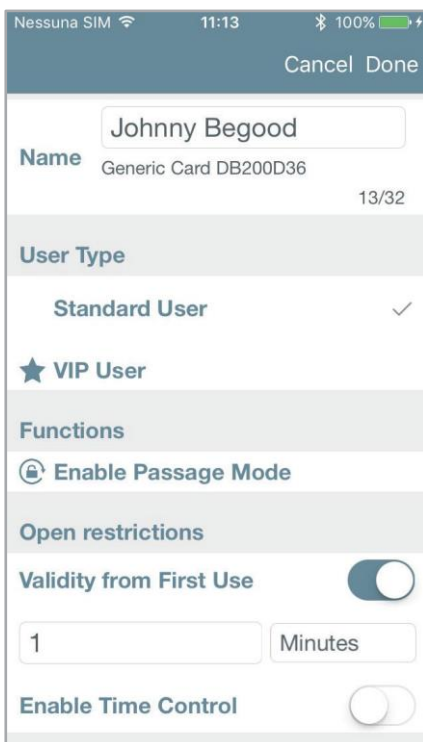
Credential *Expiration Date* doesn't change, since it has priority over the *End of Validity from First Use*. In the example above *Expiration Date* has remained the same: 28/02/2018. That means *Validity from First Use* has changed from 10 to 4 days, to not exceed the credential *Expiration Date*.

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.



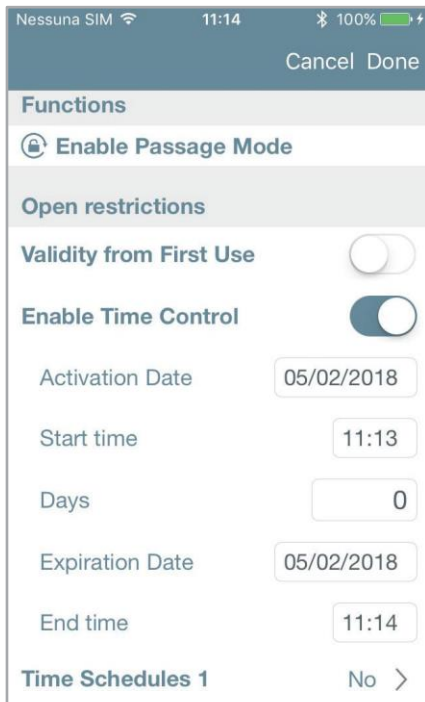
Enter *Programming mode*, then enter *Card or Phone User Parameters*.



_____ Enable Validity from First Use
_____ Set 1 Minutes

Advanced

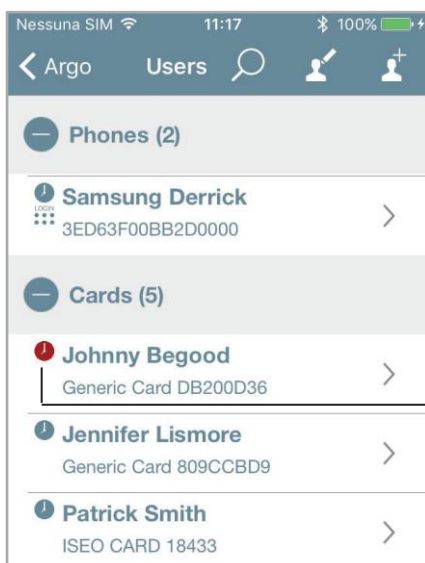
The *User* opens the door for the first time. The *Administrator* enter *Programming mode* to check the credential status.



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:

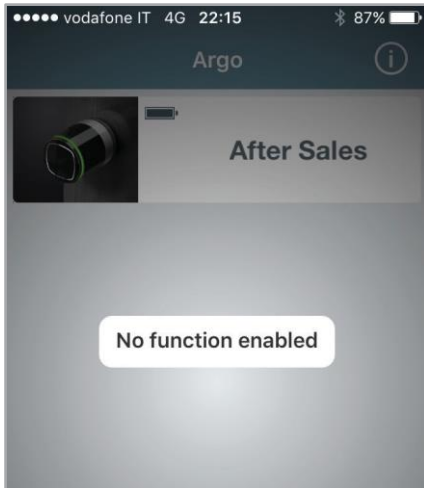


The red clock means that *User* has expired, since 1 minute has passed (one shot entrance).

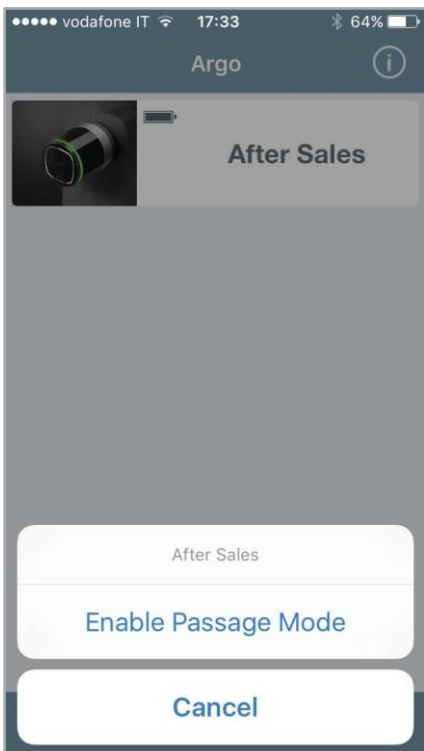
Advanced

Tap & Hold menu

The *Tap & Hold* menu shows only the Smartphone'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.



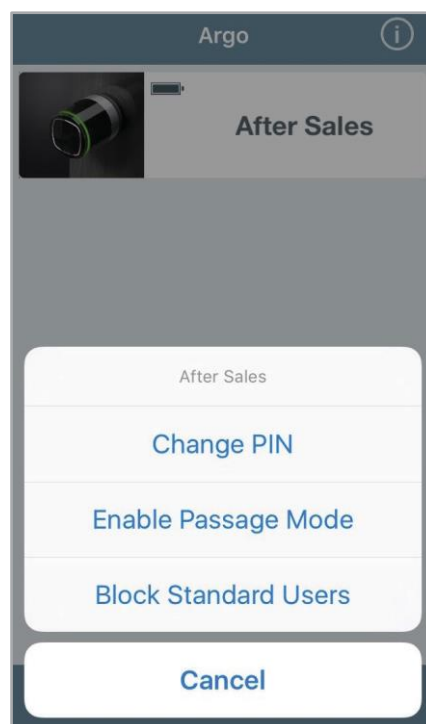
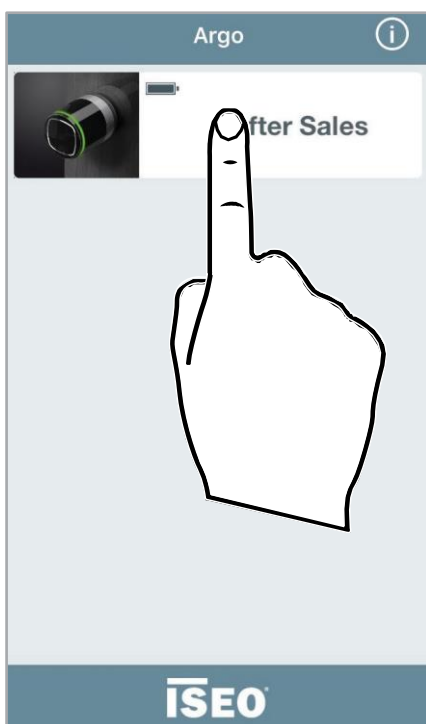
See also the *Video tutorial*, explaining in detail the *Tap & Hold* functions, at link: <https://app.iseo.com/?parm=ARGO&lang=en&folder=video-tutorial>

Advanced

Enable Passage Mode

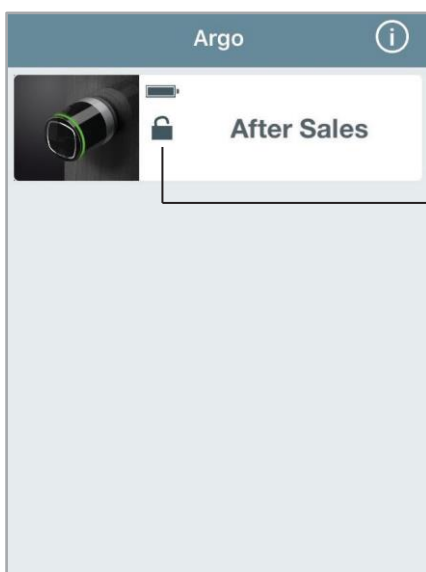


Enabling **Passage Mode** into the lock, the door will be always opened for any user who wishes to gain access, without the use of authorized credentials.



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.

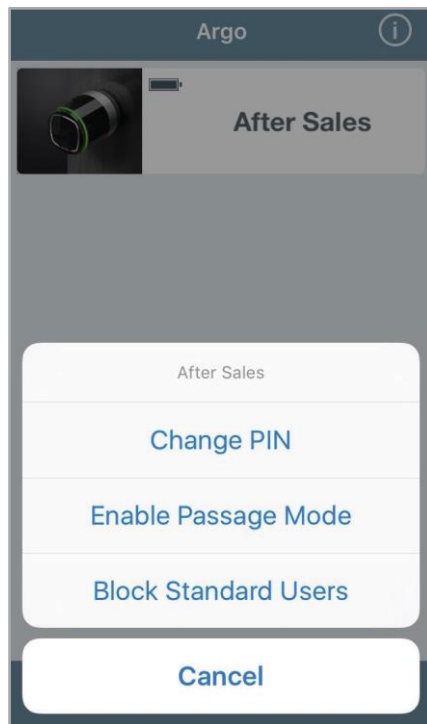
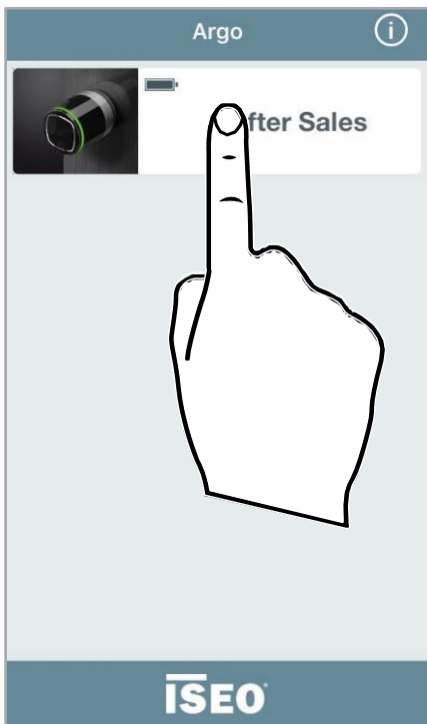


Remember to set before the function **Enable Passage Mode**  on your smartphone (see **Smartphone user parameters**). When passage mode is active no logs are created in order to save events.

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.

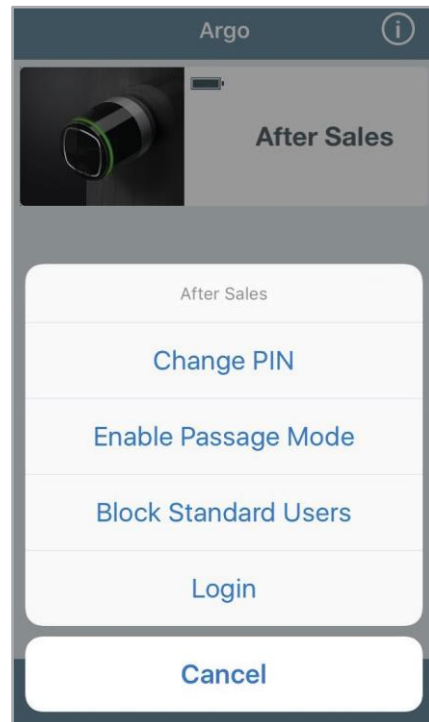
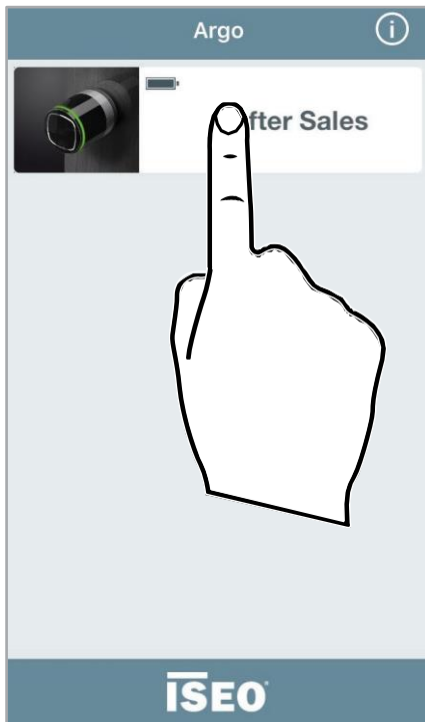


Remember to set before the functions **Block Standard Users**  on your smartphone (the user must be a VIP user ). To do that see **Smartphone user parameters**.

Advanced Login (without Master Card)

LOGIN

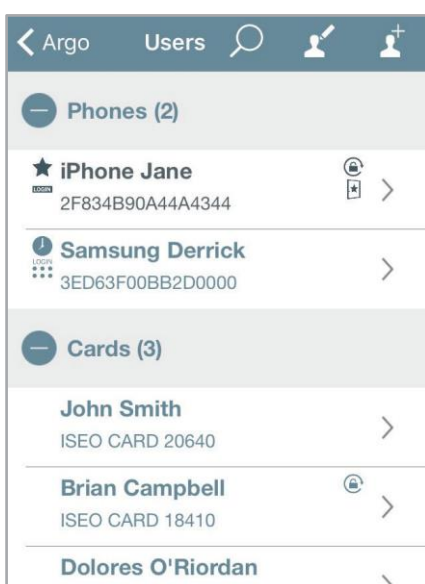
This function allows your smartphone to enter *Programming Mode* without the need of the *Master Card*.



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

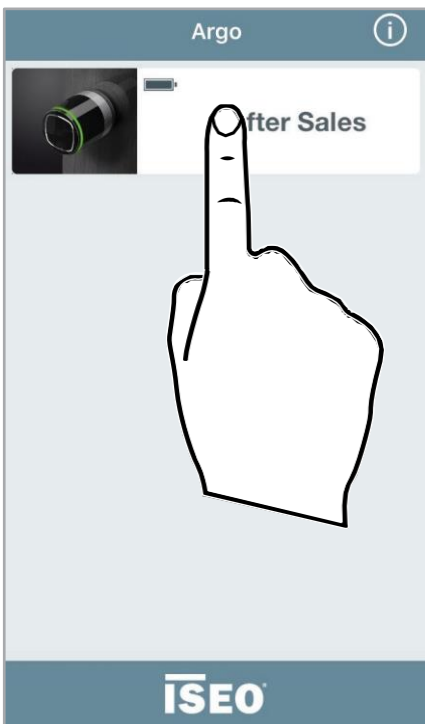


For the maximum security, you can add a *PIN* code to enter *Programming Mode* with your smartphone, as described at paragraph: *Administrator Login without Master Card*.

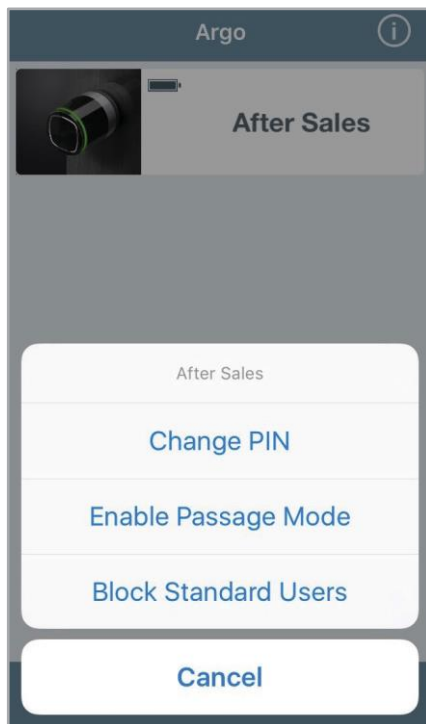
Change the PIN code



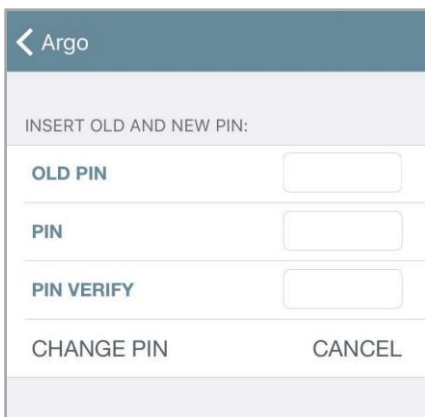
This function allows to change the *PIN code* if previously set in the smartphone. This *PIN code (4 digits)*, could be set to open the door and/or to *Login without Master Card* (see *User type and functions* and *Smartphone user parameters* paragraphs).



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



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



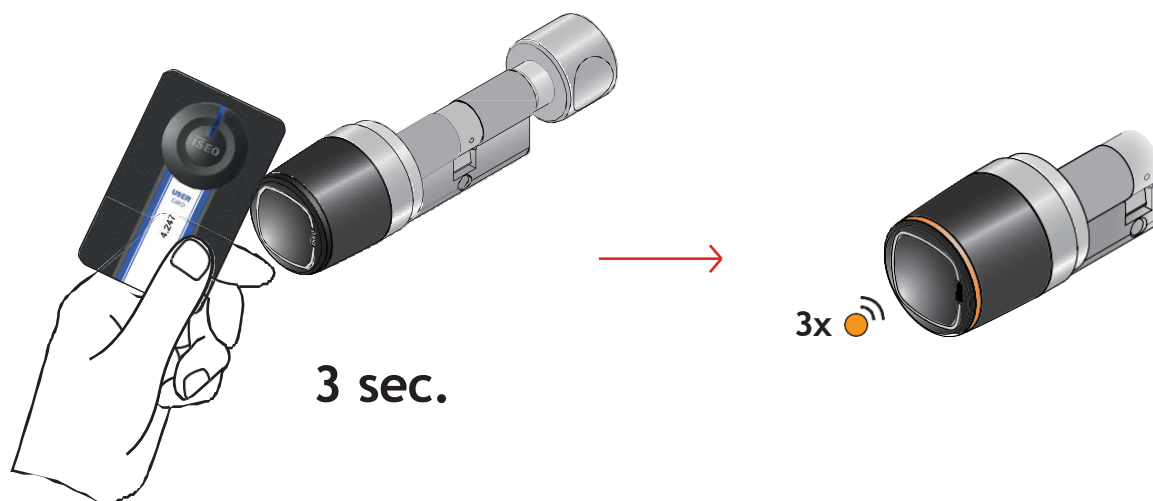
4. Enter the old *PIN code*.
5. Enter the new *PIN code* two times, then press **CHANGE PIN**.

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*.

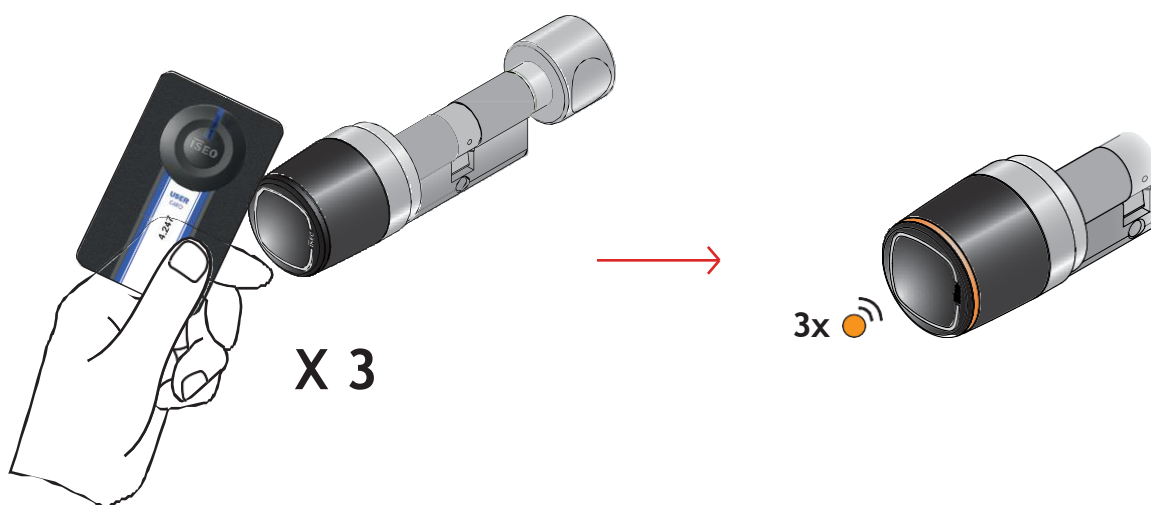


Advanced

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 together with a green light;
 - the third time the device emits 3 acoustic signals together with 3 orange lights.

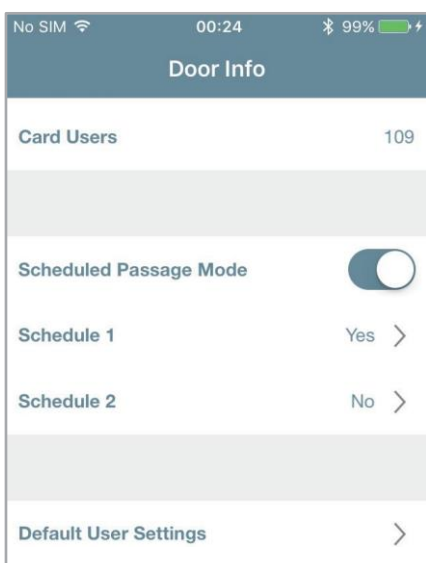
Follow the same procedure to disable the **Block Standard User** function.



Scheduled Passage Mode

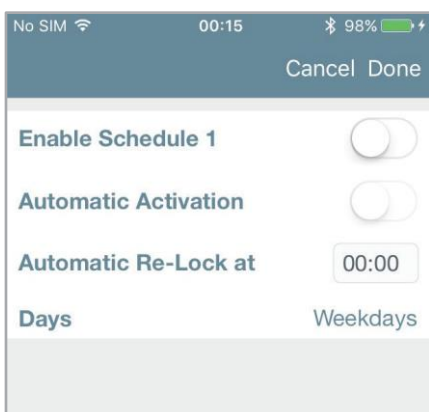


This function allows you to set 2 schedules, to automatically enable and disable the *Passage Mode* function in the smart devices *Libra*, *Aries*, *1NCA*, *MA1A*, *Stylos e x1R* (see *Enable Passage Mode* paragraph). That means the lock will automatically go in *Passage Mode*, following the set program.



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.

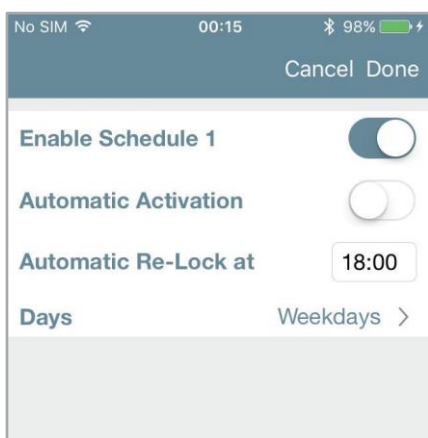
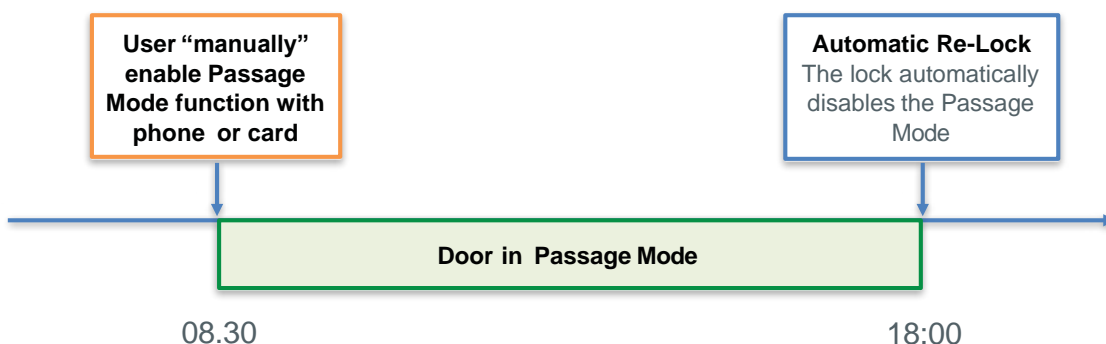
1. Passage Mode with Automatic Re-Lock.
2. Passage Mode with Automatic Activation and Automatic Re-Lock.
3. Passage Mode with Automatic Activation and Automatic Re-Lock with First Person In.



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

Passage Mode with Automatic Re-Lock

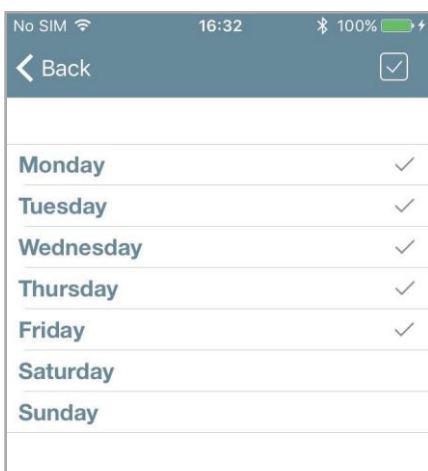
With this program you need to “manually” enable in the device the *Passage Mode*, by smartphone (see *Enable Passage Mode*), or by card (see *Enable Passage Mode without Argo app*). But you don’t need to disable it, since you can set it automatically in the defined time and day.



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 closed.

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



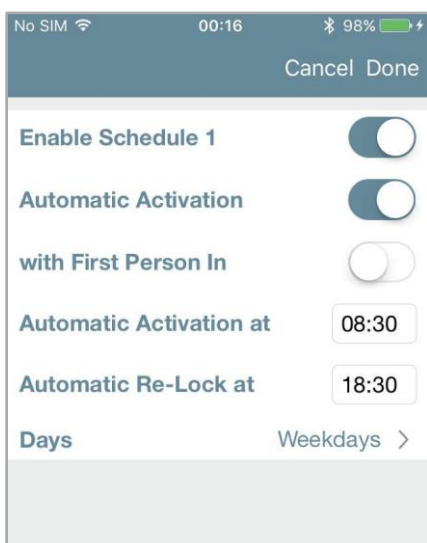
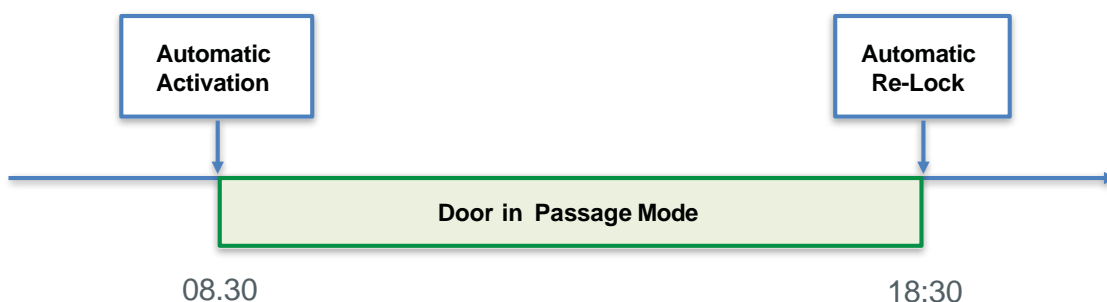
Check/uncheck all days with one touch.

Select multiple or single days, one by one.

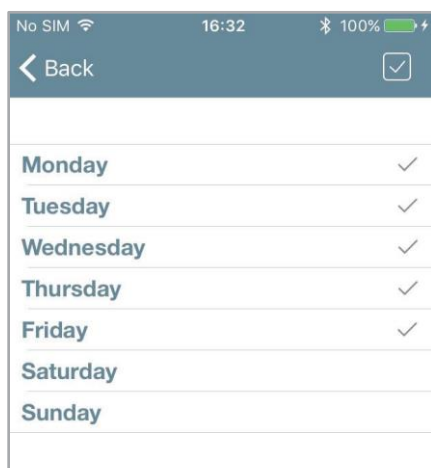
At the end press **Back**, then **Done**.

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.



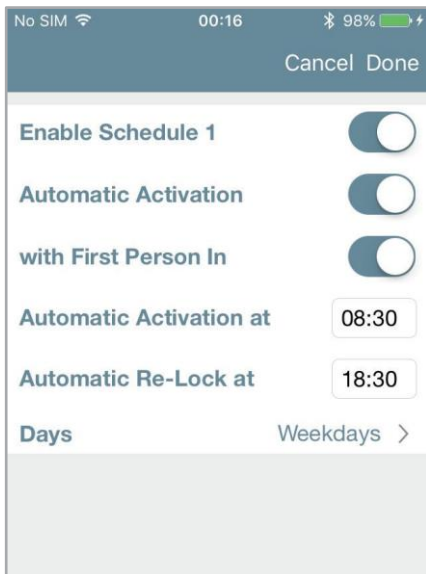
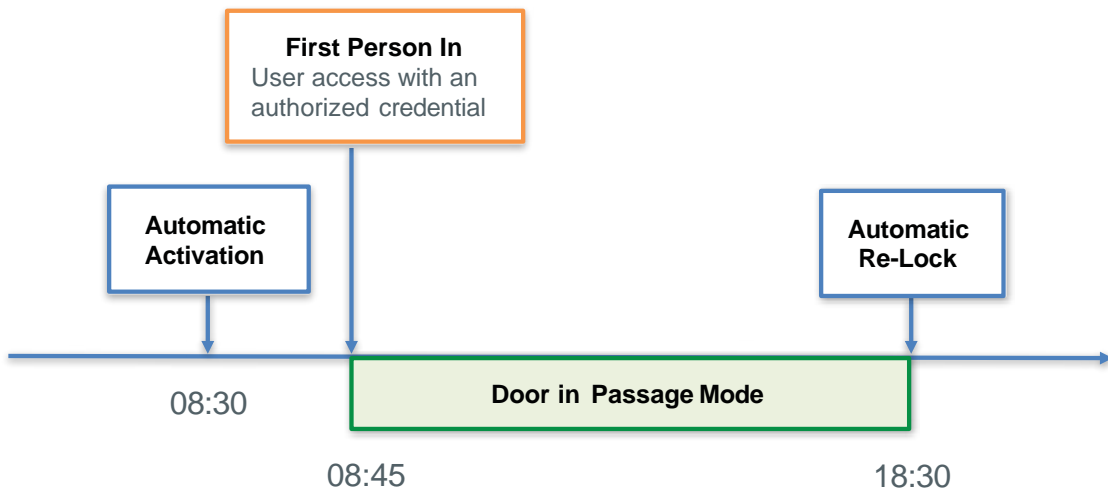
- Switch on **Enable Schedule 1**.
- Switch on **Automatic Activation**.
- Select *Passage Mode* automatic activation time and re-lock time.
- Select the days on which the program take place. The default is *Weekdays*: all days excluded Saturday and Sunday.



- Check/uncheck all days with one touch.
- Select multiple or single days, one by one.
- At the end press **Back**, then **Done**.

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*).



- _____ Switch on **Enable Schedule 1**.
 - _____ Switch on **Automatic Activation**.
 - _____ Switch 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**.

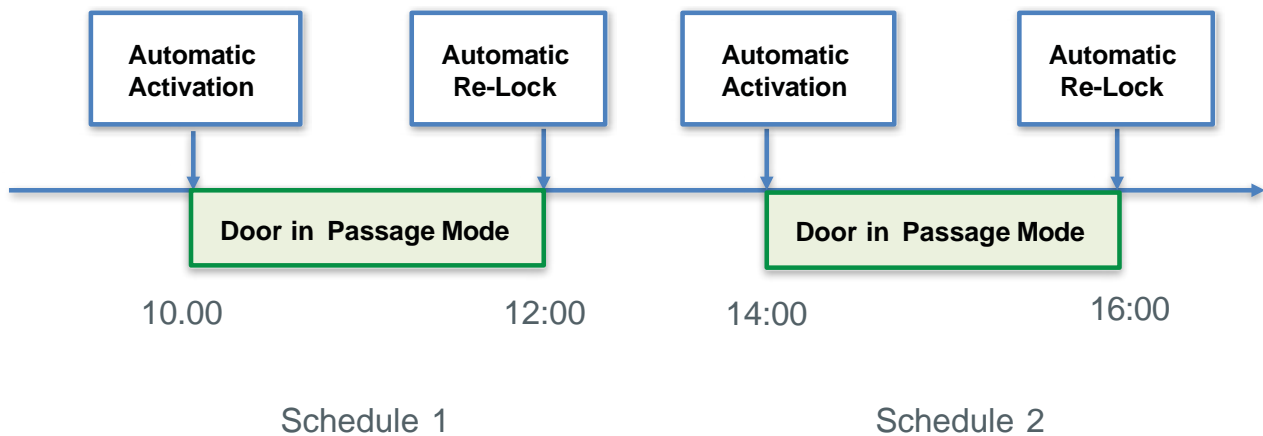


This solution is really useful in term of security and avoids the automatic *Passage Mode* activation when no user is inside the building or the room

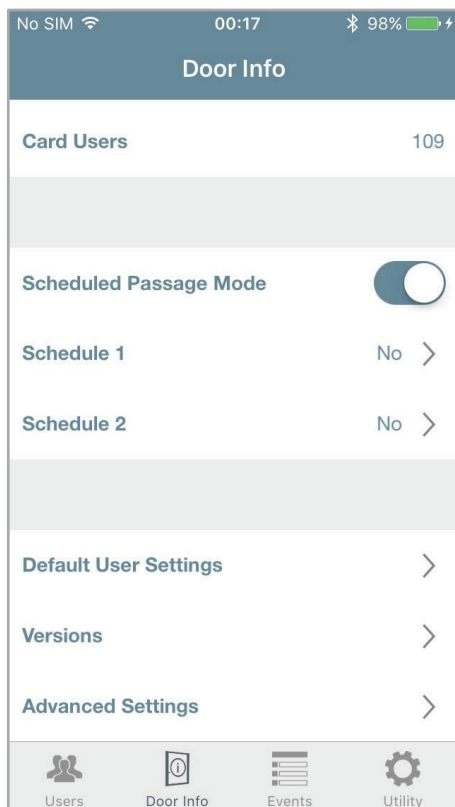
Advanced

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.

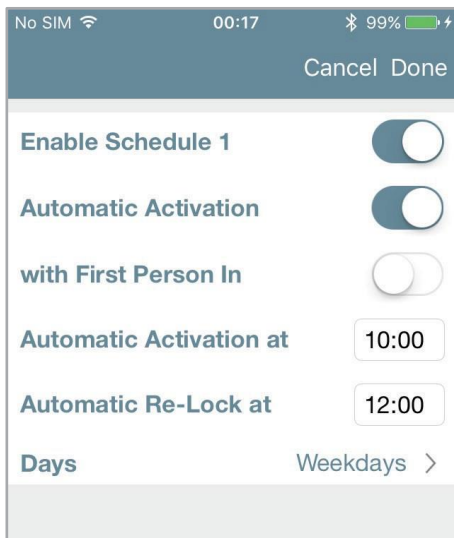


Enable **Schedule Passage Mode** to see the two schedules available.

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

Advanced

Configuration example: meeting room with Libra Smart

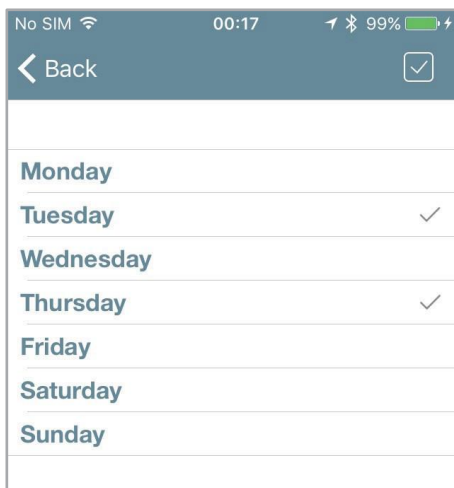


Switch on **Enable Schedule 1**.

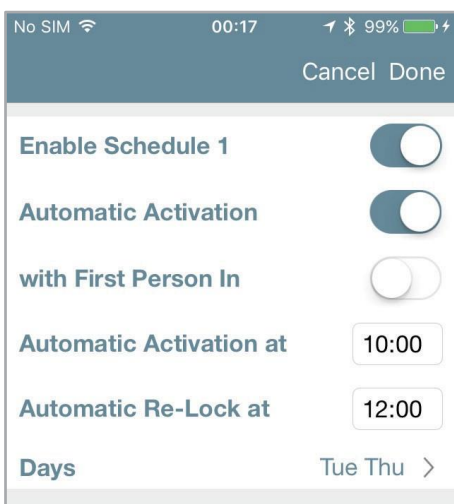
Switch on **Automatic Activation**.

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**.

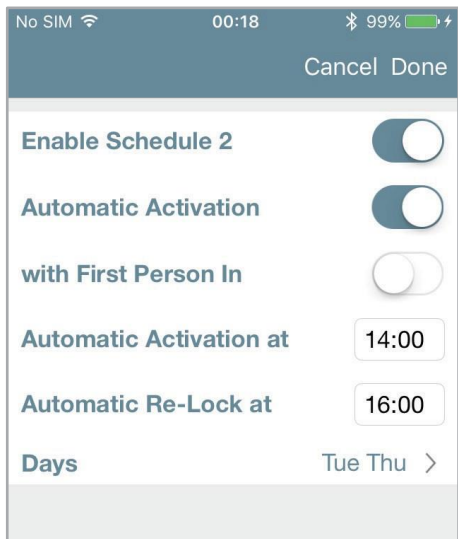


Tap **Done**.

Advanced

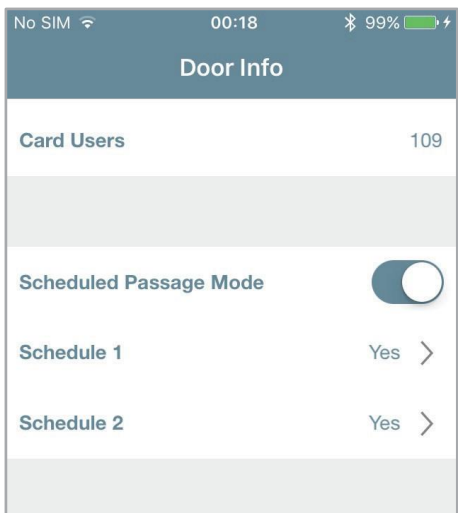
Configuration example: meeting room with Libra Smart

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



Cancel Done

- Enable Schedule 2 Switch on **Enable Schedule 2**.
- Automatic Activation with First Person In Switch on **Automatic Activation**.
- Automatic Activation at 14:00 Select *Passage Mode* automatic activation time and re-lock time, according to schedule 2.
- Automatic Re-Lock at 16:00
- Days Tue Thu > Touch to select Tuesday and Thursday.



Door Info

Card Users 109

Scheduled Passage Mode The programming is finished.

Schedule 1 Yes > To turn off all the scheduling, simply turn off the **Scheduled Passage Mode** slide button. When the button is switched on again, all the programming previously done will resume.

Schedule 2 Yes >



Argo keeps always in memory the last programming made. To temporarily 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.

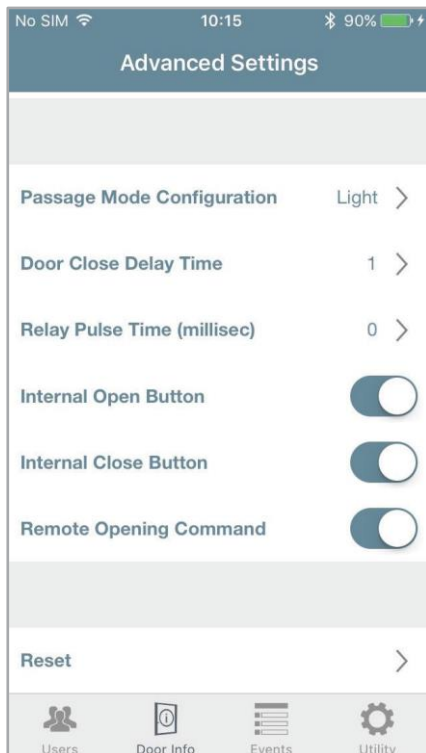
Advanced x1R Smart: Light Mode

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 armored doors market, used in offices applications (common doors with high 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.

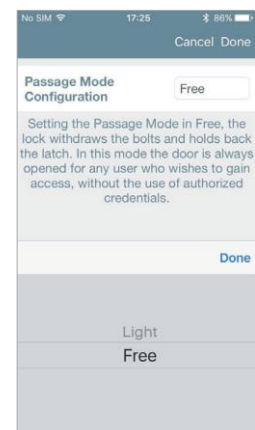
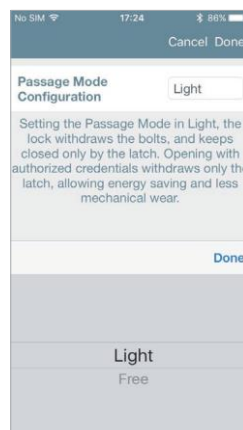
This solution combined to with *x1R Smart* is very useful and effective because it has the following advantages:

- 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.



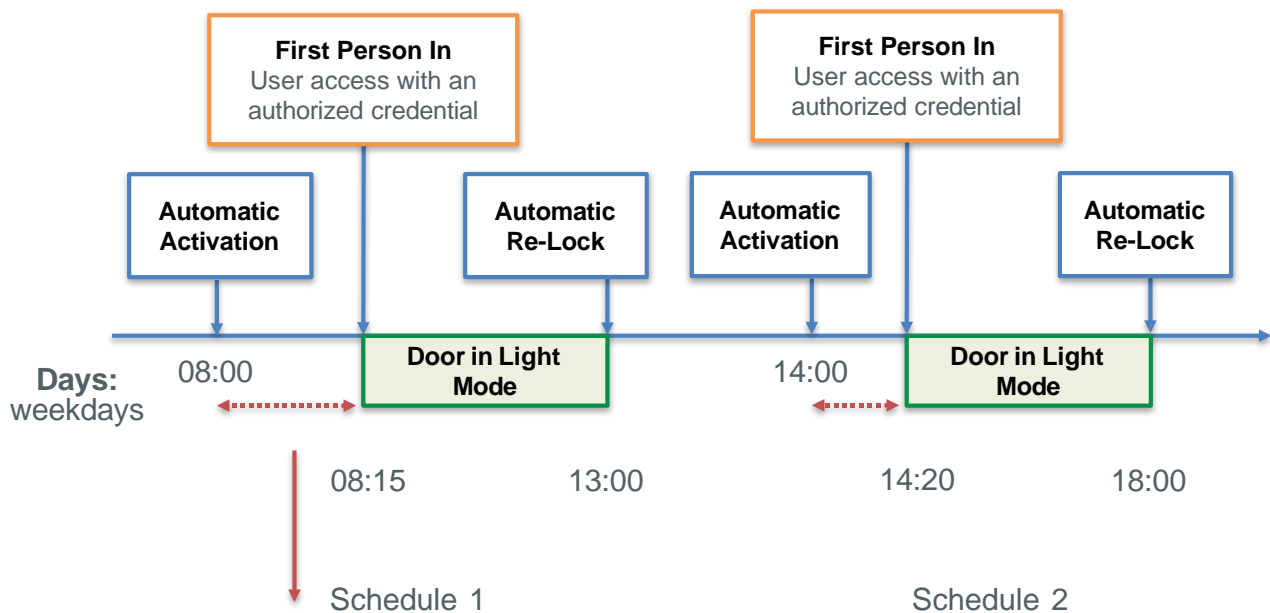
Only *x1R Smart* can be set in *Passage Mode Free* or *Light*. On all the other devices this menu is not present

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

Advanced

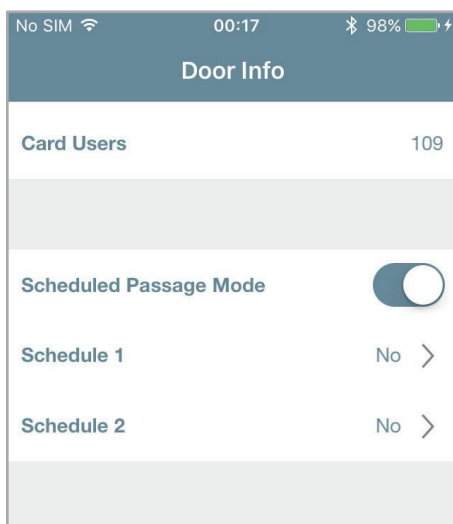
Configuration example: main offices entrance with x1R Smart

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.



In this interval the door is still closed by bolts.
The Light Mode will start at the first user entrance with an authorized credential.

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



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

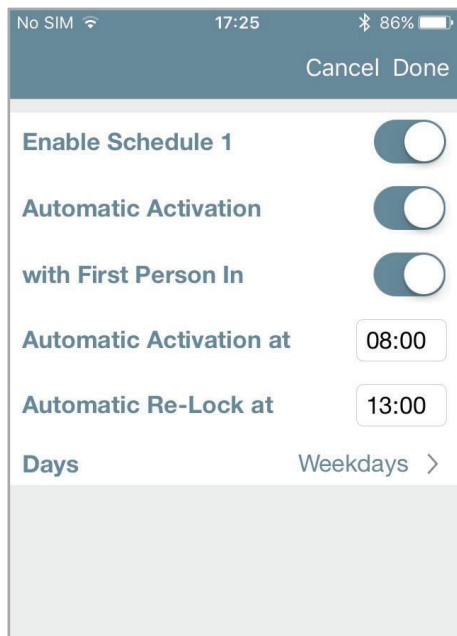
Touch **Schedule 1** and then **Schedule 2**, to configure the 2 schedules.



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

Advanced

Configuration example: main offices entrance with x1R Smart



Switch on **Enable Schedule 1**.

Switch on **Automatic Activation**.

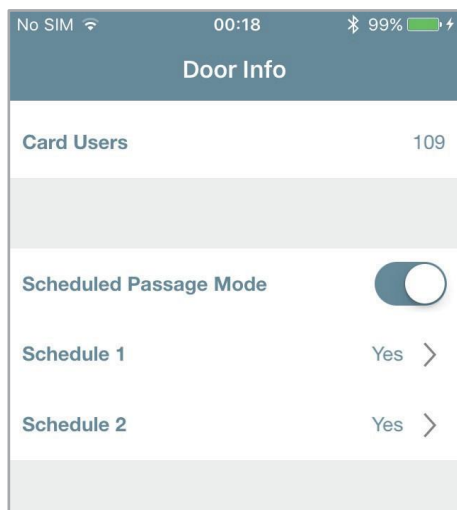
Switch on **with First Person In**.

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

Weekdays are already set by default.

At the end touch **Done**.

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



The programming is finished.

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



Argo keeps always in memory the last programming made. To temporarily 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



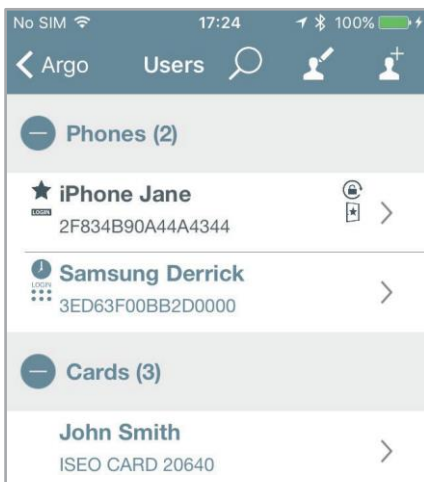
Invitations allows smartphones to self-register into the lock as users, by using an *Invitation Code*, previously memorized in the doorlock by the *Administrator*.

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:

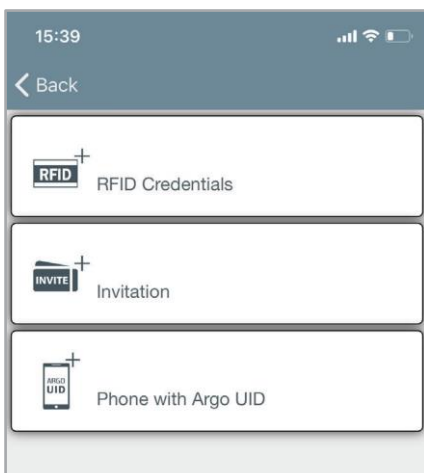
- Step 1: the *Administrator* adds and sends the invitation code to the *User*.
- Step 2: the *User* receives the invitation code and access to the door.
- Step 3: the *Administrator* enter *Programming Mode* to manage the *User list*.

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



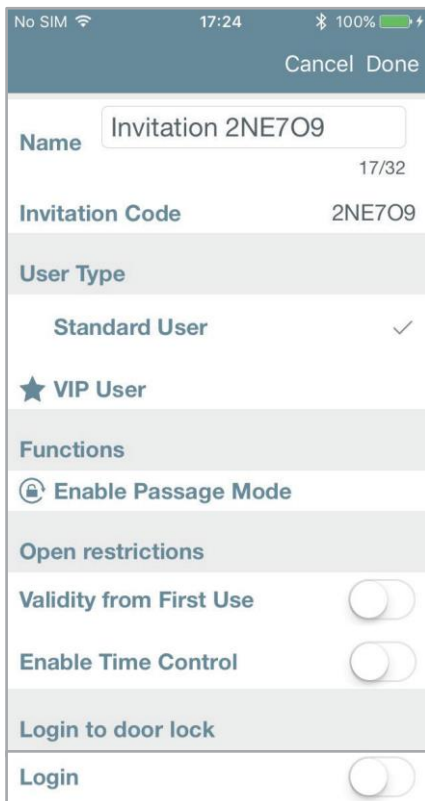
1. Enter *Programming Mode*

2. Tap the *add user* icon

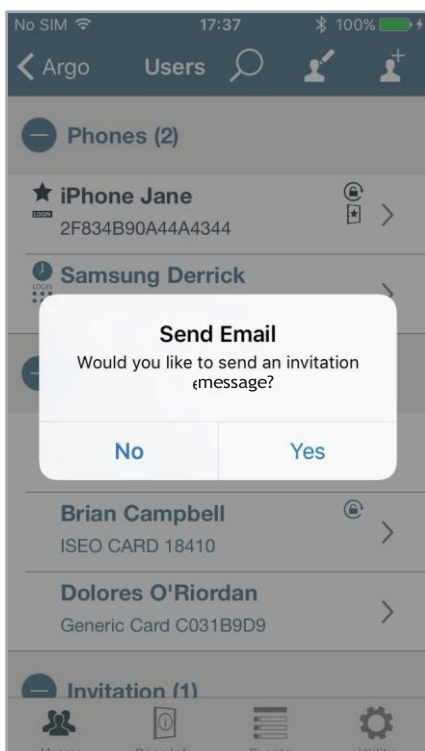


3. Tap *Invitation*

Advanced



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.

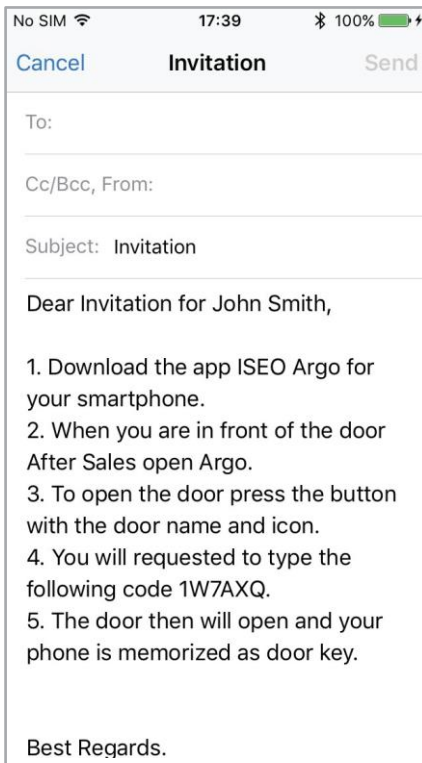


7. An automatic pop-up message will ask you to send a message with the *Invitation Code*.
 - Press **Yes** if you want to send it immediately.
 - Press **No** if you want to send it afterwards.



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

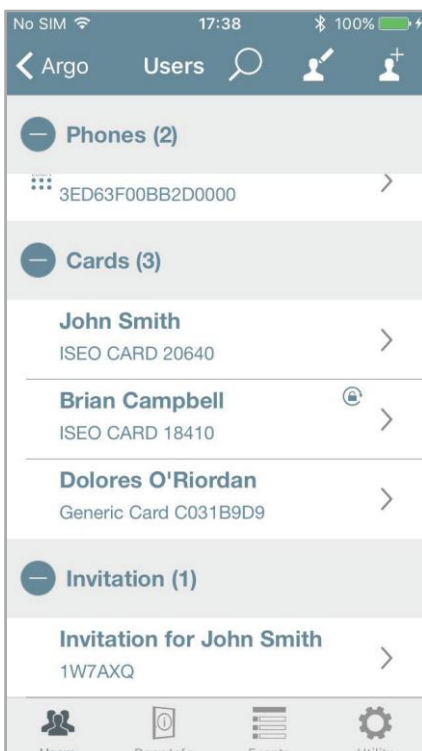
Advanced



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.



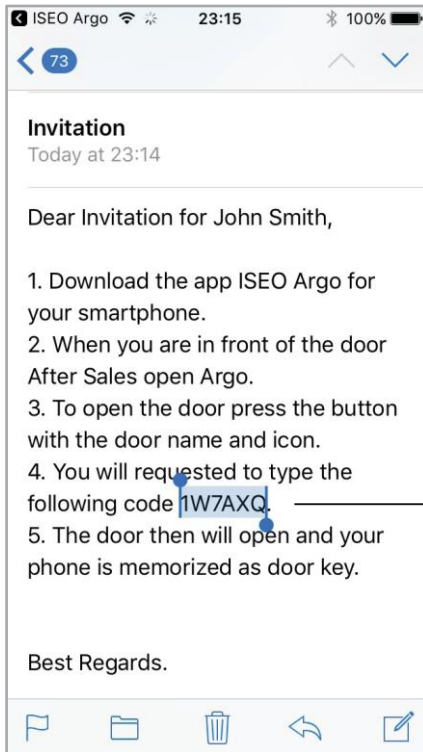
9. You can see in the *Argo User List* the added invitation, in the **Invitations** user field. You can always modify the existing invitations like any other credential, adding or changing functionalities: *User Type, Functions, Open restrictions, Login to Doorlock*.



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.

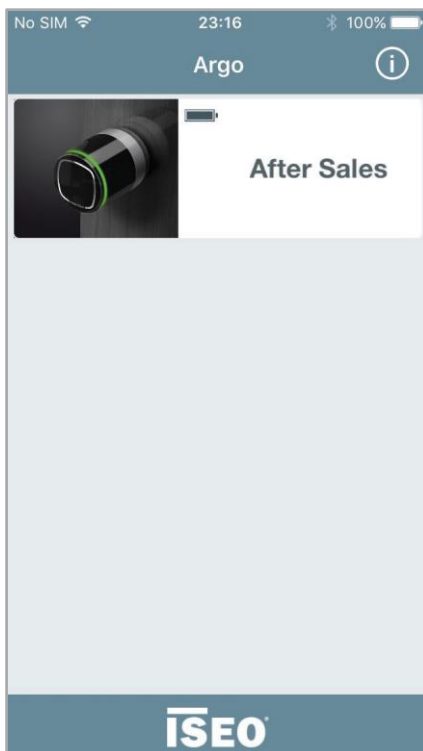
Advanced

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



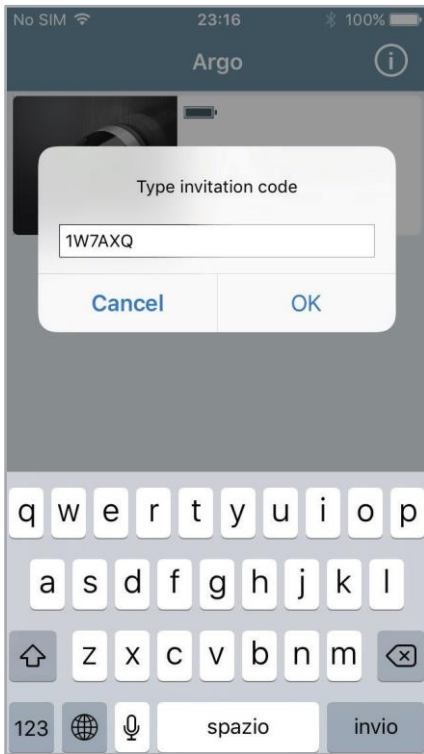
1. The *User* receives the email with the step by step instructions and the *Invitation Code*.

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

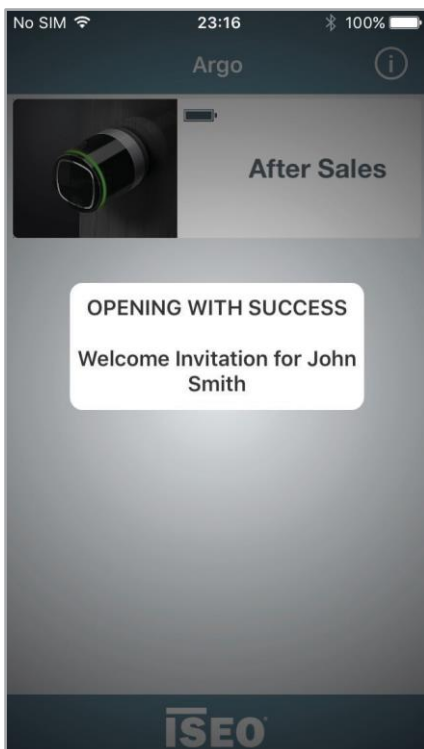


3. A pop-up message will ask to type the *Invitation Code* to access the door.

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.

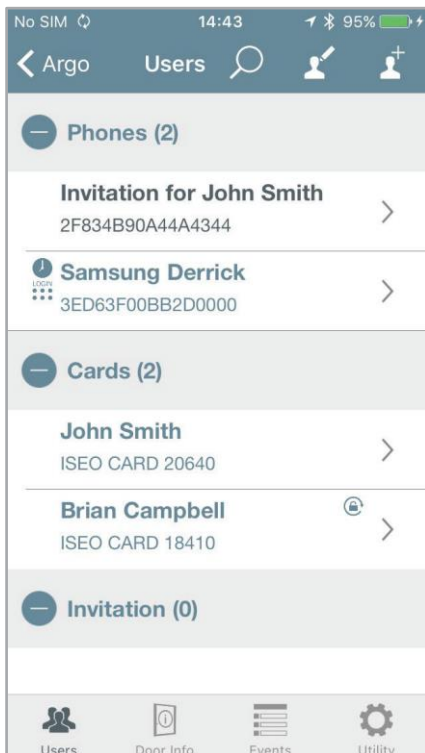
The invitation will expire at its expiration time and date, if previously set.

The *Invitation Code* can be used once only.

Advanced

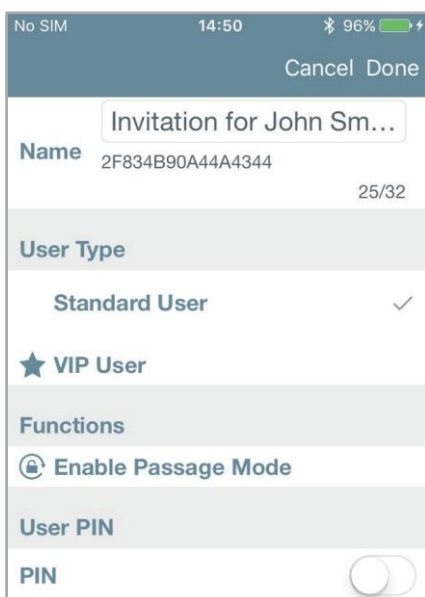
Step 3: the Administrator enter Programming Mode to manage the User list.

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-registered phone.

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 alphanumeric 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

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.

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 exactly 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.



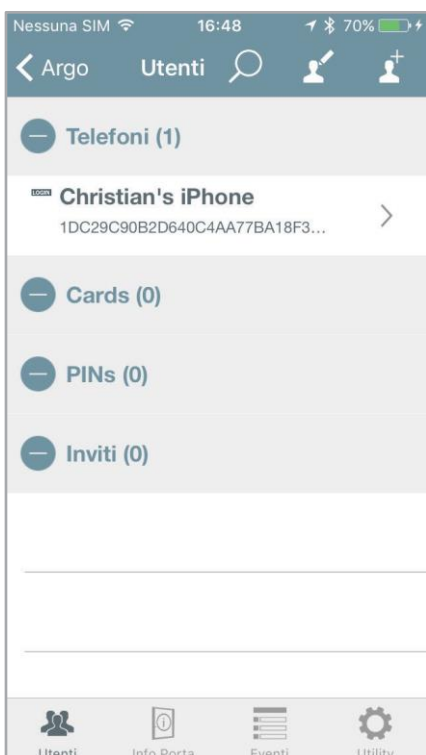
Minimum iPhone requirements

- 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.

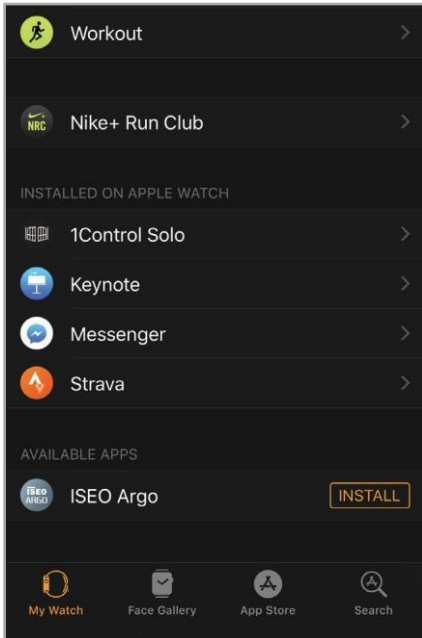
Step 1: add your smartphone to the ISEO Smart device user list



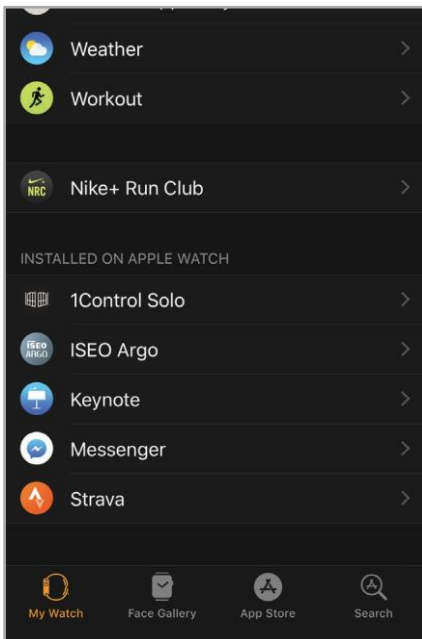
Smartphone added to the *User List*.

Advanced

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.

Advanced

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.

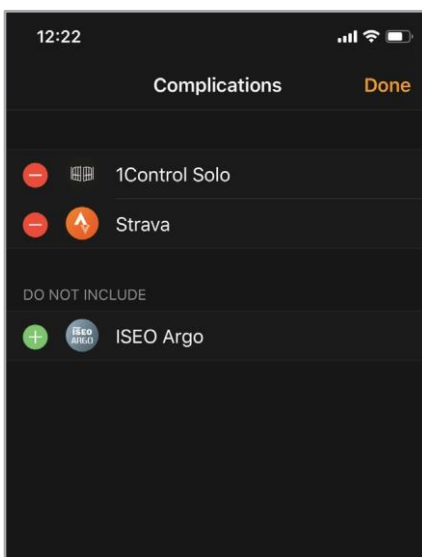
Advanced



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.

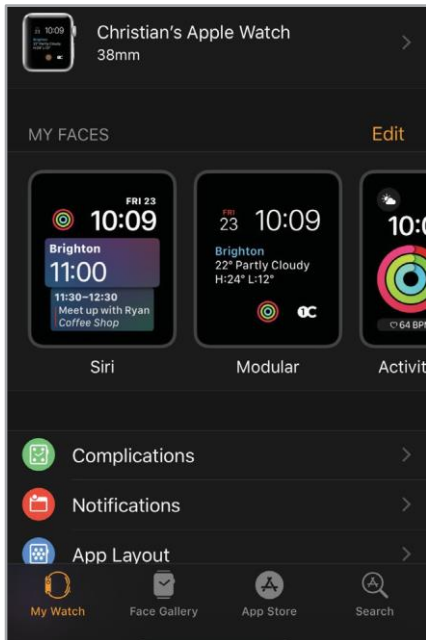
Step 1: add Argo app as complication in the Watch app.



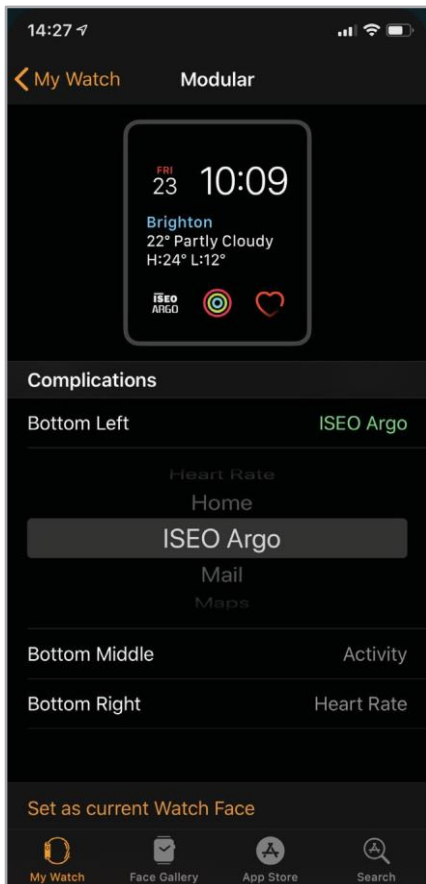
Tap + to add ISEO Argo as complication available in the Watch faces.

Advanced

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.

Advanced

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

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 different Faces.

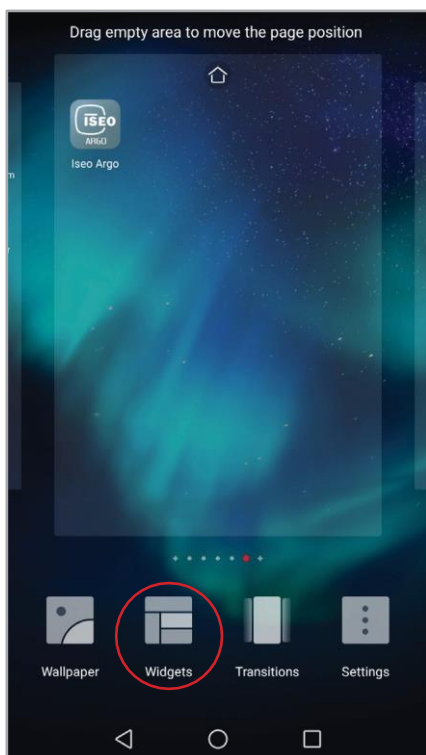


Widgets for Argo app

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

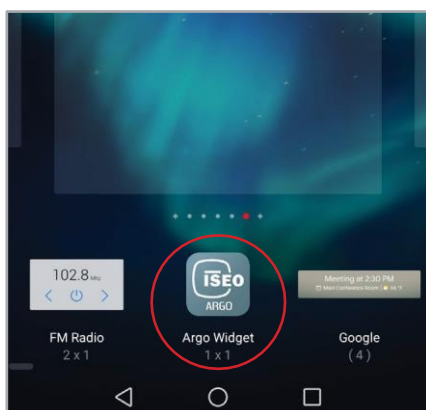
In Android phones when you add a widget, you can define which doorlock to open and you can position the widget in any place of the screen as a shortcut.



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

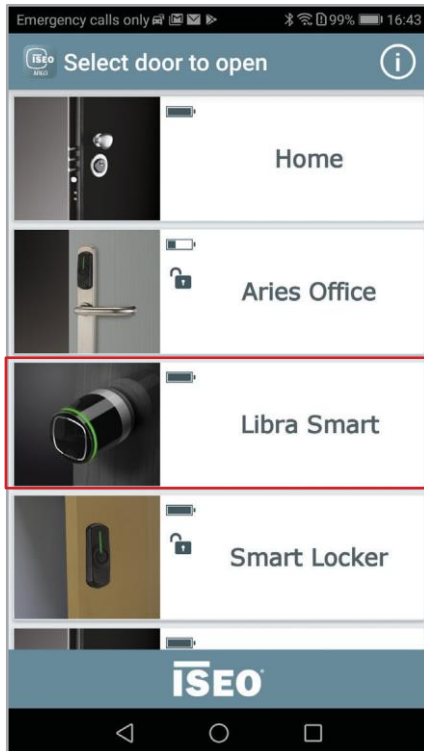


Widgets configuration on Android phones may vary depending on phone model and operating system.



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

Advanced

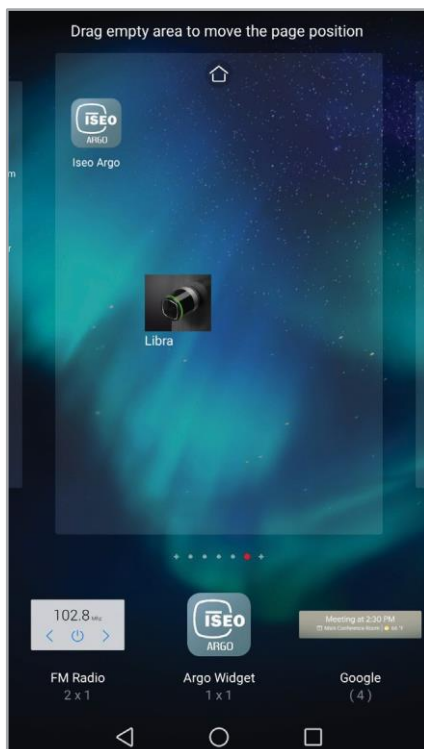


Argo app automatically opens.

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.

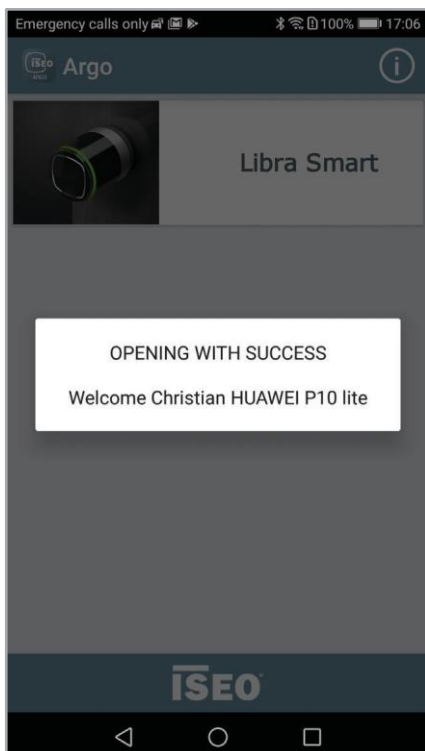
Tap an empty area of the screen to exit the configuration mode.

Advanced

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

Additional notes for Android widgets



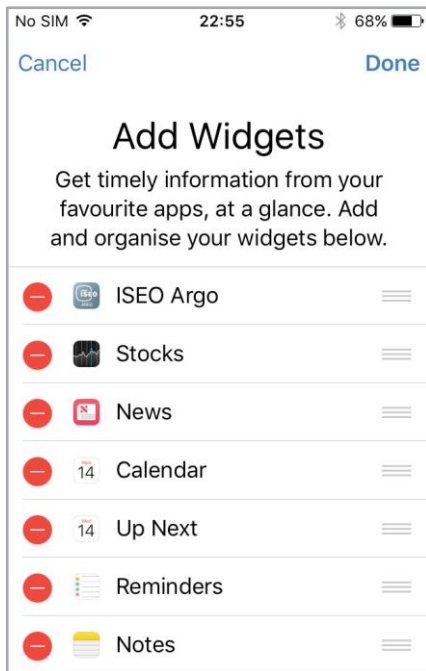
Android widgets can be freely customized in size.



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

Step 1: configure Argo widgets for iOS

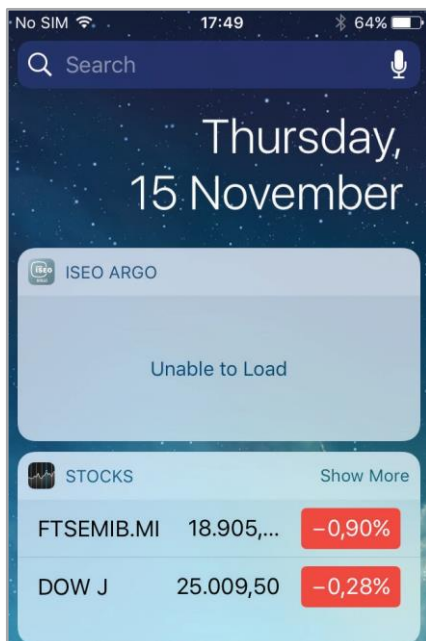
In iOS devices the widgets configuration and management is completely different from Android. While on Android you can create widgets even if you're not enrolled as user in the device, with iOS you need to open before the device, at least one time, by Argo app.



———— 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



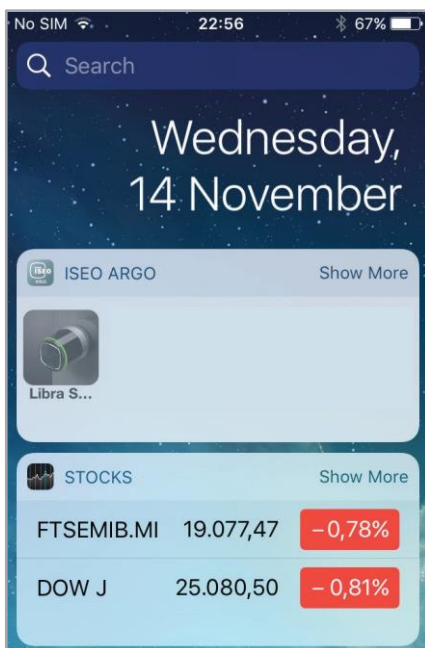
———— ISEO Argo widget will be empty: you need to open a door before, to get the shortcut.

Advanced

Step 2: open the door by iOS widget



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

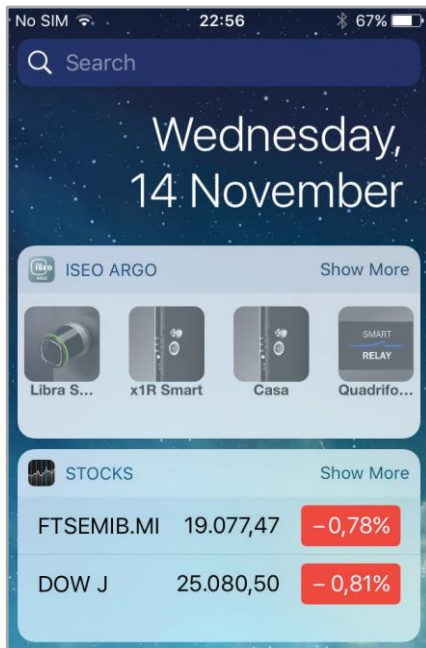


You will see the door icon in the today view. Tap it to automatically open the door by Argo app. Argo app starts and opens the door. When finished the app automatically closes.



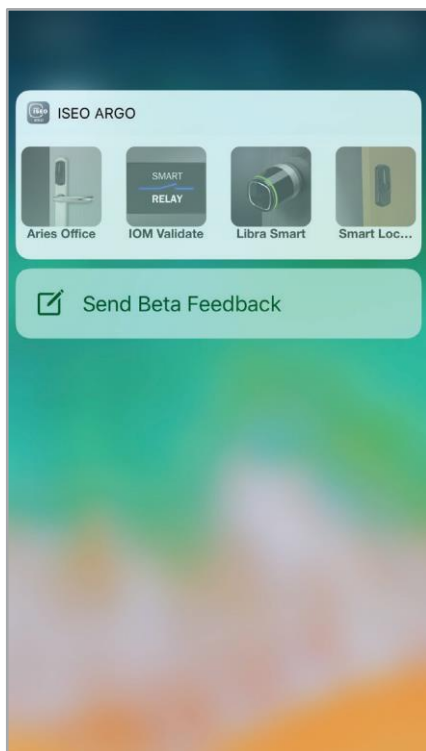
You cannot see the door icon in the Today View if your phone has not been added to the door *User List* and if you don't have opened the door at least one time.

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 eighth 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.

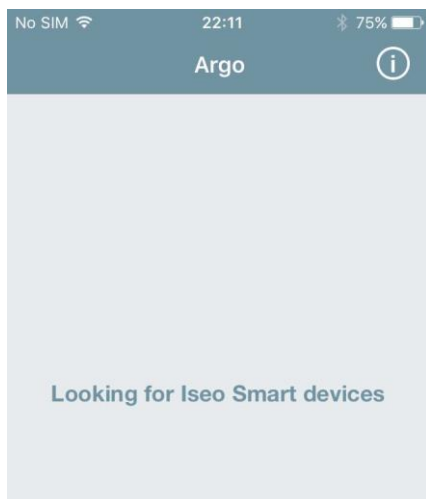
Add phone with Argo UID

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



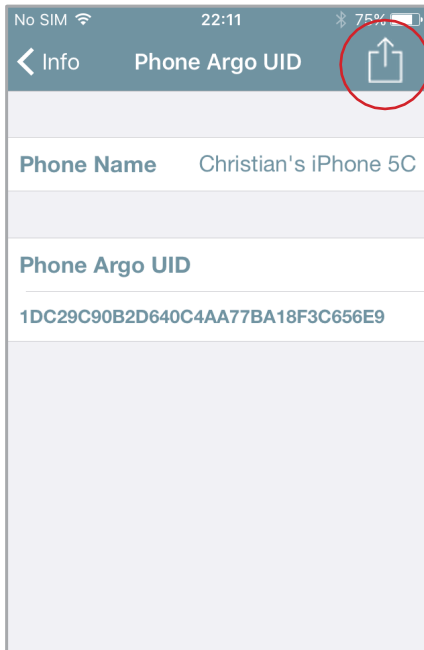
User downloads and installs the Argo app on his phone.

1. Tap info app icon

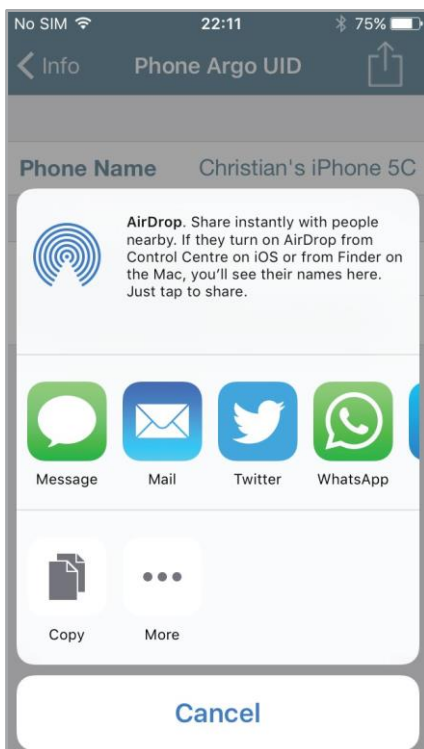


2. Tap View Phone Argo UID

Advanced



3. Tap share icon.

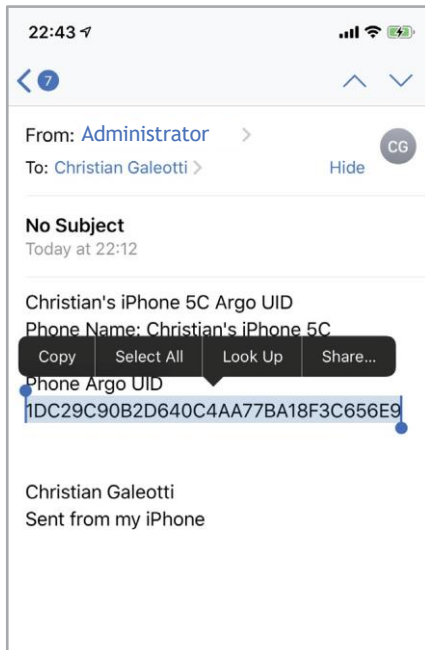


4. Send the phone Argo UID to the Administrator by any communication app: email, whatsapp, sms...

In the following example we show by email.

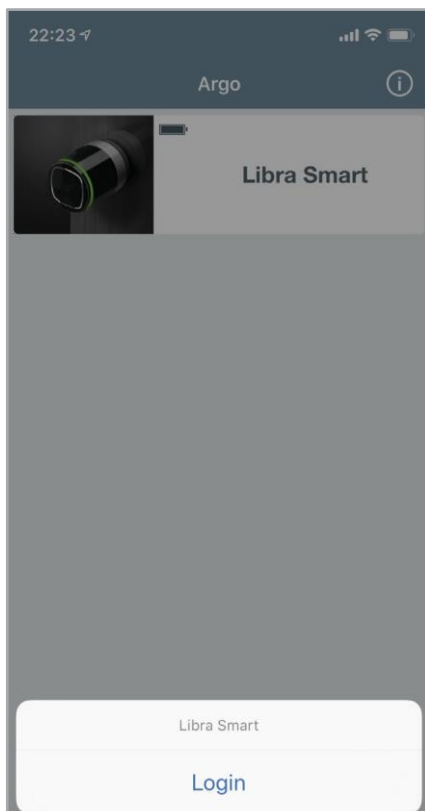
Advanced

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



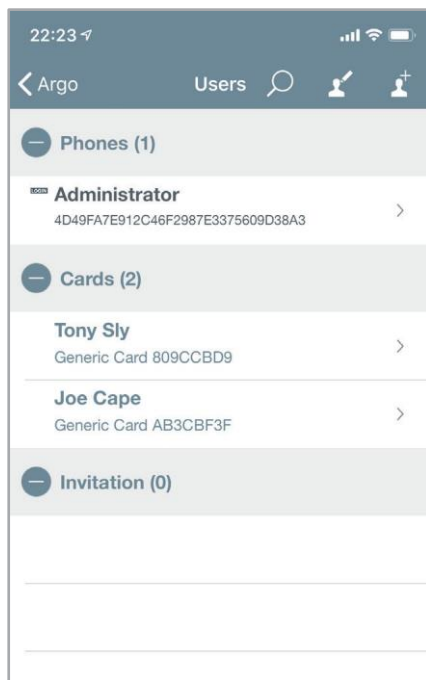
Administrator receives the email from the User.

1. Copy the phone Argo UID



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

Advanced



3. Tap the *add user* icon



4. Tap **Phone with Argo UID**

Advanced

22:24

Cancel Done

Name Christian 9/32

Phone Argo UID 90B2D640C4AA77BA18F3C656E9 32/32

User Type

Standard User ✓

★ VIP User

Functions

Enable Passage Mode

8F3C656E9»

q w e r t y u i o p

5. Type the User name

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

22:24

< Argo Users

Phones (2)

Christian
1DC29C90B2D640C4AA77BA18F3C656E9 >

Administrator
4D49FA7E912C46F2987E3375609D38A3 >

Cards (2)

Tony Sly
Generic Card 809CCBD9 >

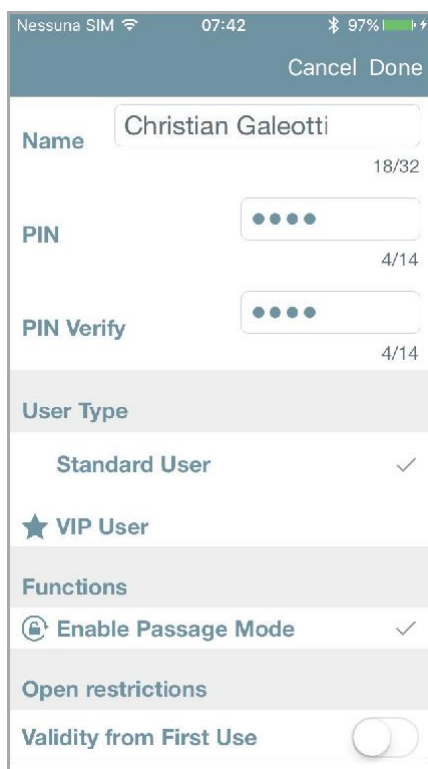
Joe Cape
Generic Card AB3CBF3F >

Invitation (0)

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

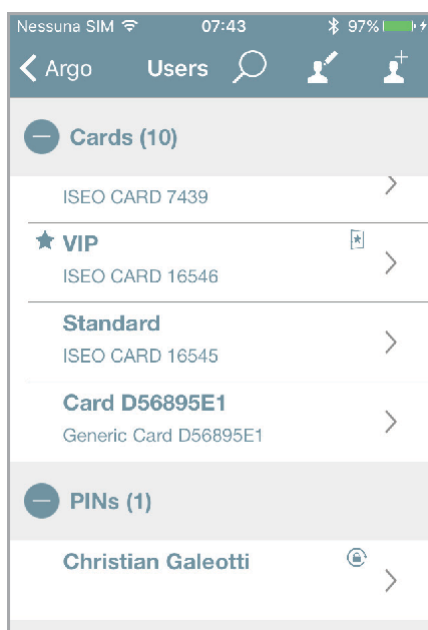
Passage mode with PIN code

The ISEO Smart devices equipped with external keyboard (i.e. 1NCA Smart Readers, *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.



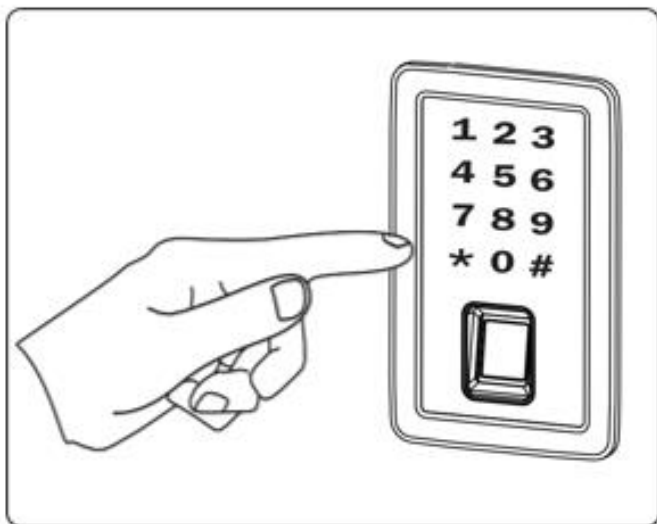
Enter a user PIN code (see *Add users typing PIN code* in the *Basics* chapter).

Tap **Enable Passage Mode**.



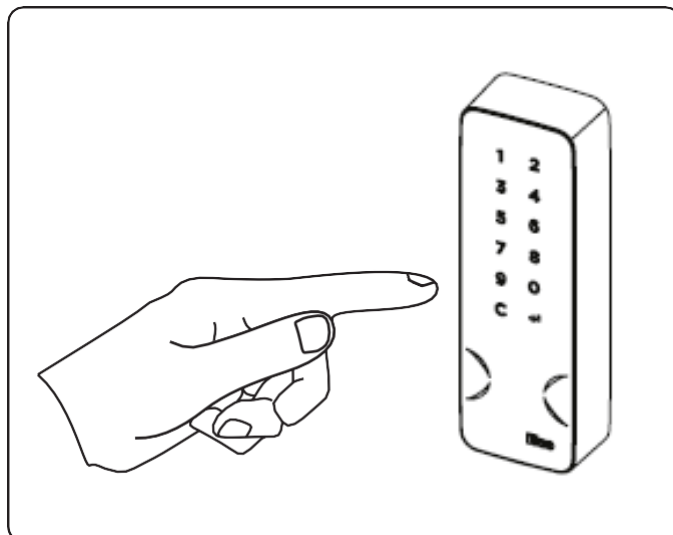
PIN code has now *Passage Mode* capability.

x1R SMART MULTI-READER

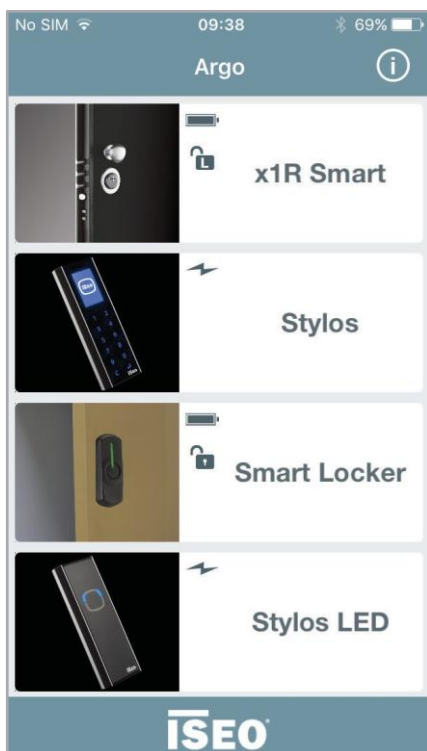


Enter the PIN code with *Passage Mode* enabled, and confirm by enter # .

1NCA SMART MULLION KEYBOARD



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).

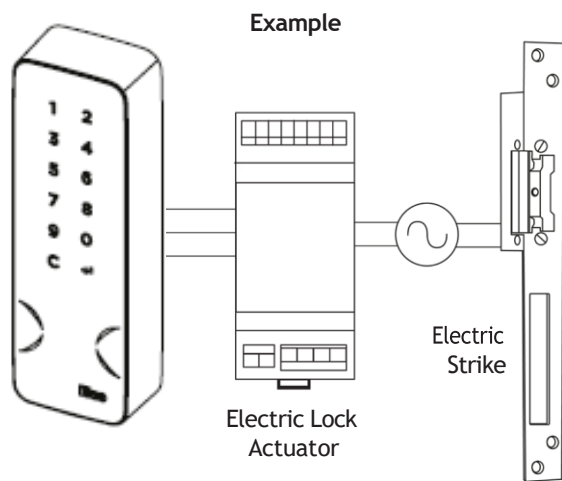


On x1R Smart *Passage Mode* can be Light or Free as configured by Argo.

Passage mode capability

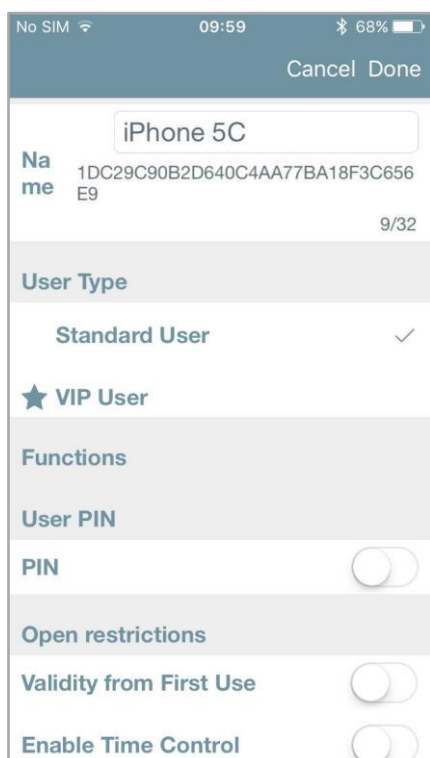
The *Passage Mode* function, once enabled, keeps the doorlock in a constant “opening condition”. You can set it by phone or card (see *Enable passage mode* and *Enable passage mode without Argo* paragraphs), and now with PIN code is even easier.

But with 1NCA Smart Reader this condition could be dangerous for the electrical device the reader may drive.



1NCA Smart Mullion Lockbus

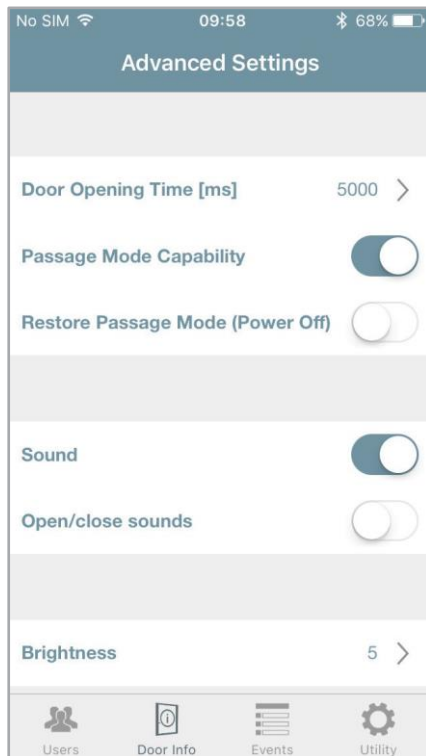
The 1NCA Smart Mullion Lockbus in fact, by the *Electric Lock Actuator*, it often drives an appliance with a coil (i.e. electric locks, electric strikes...), that could not stand to be in a constant opening condition (coil always excited could burn). That's why the *Passage Mode* function in the 1NCA Reader is disabled by default. However, the Administrator, knowing the application, can freely enable it by the Argo app.



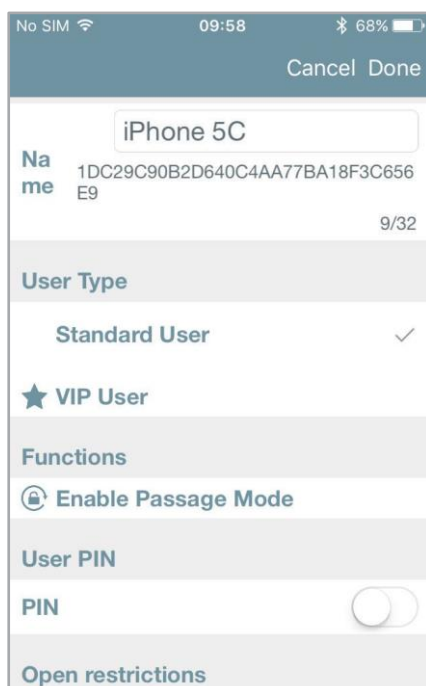
In the 1NCA Smart Reader the *Passage Mode* function for Phones, Cards and PINs is not displayed, since *Passage Mode* capability is not enabled by default.

Advanced

To enable the *Passage Mode* capability on 1NCA Smart Readers 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

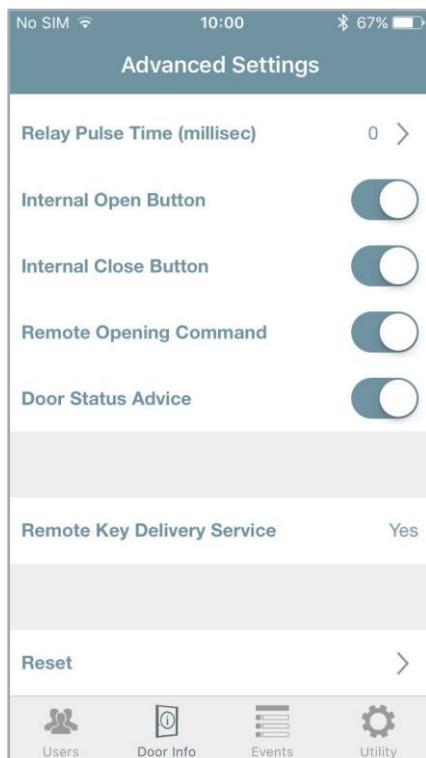


Now *Passage Mode* function for Phones, Cards and PINs is displayed and can be set accordingly.

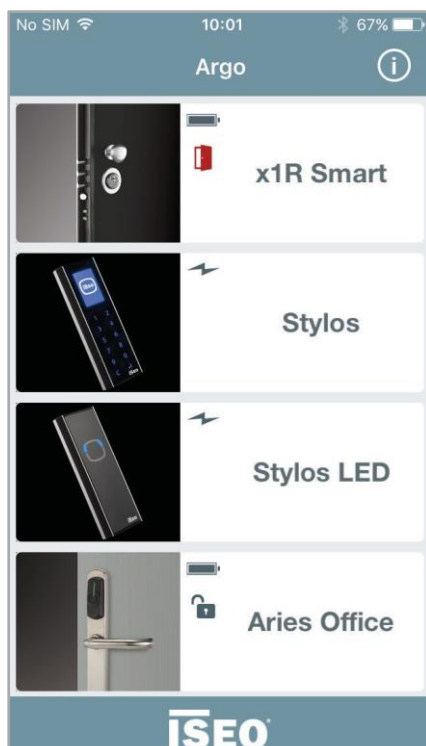
Advanced

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, Multiblindo SMart). To display the *Door Status Advice* open the Argo app, enter *Programming Mode*, touch *Door Info* menu and then *Advanced Settings*.



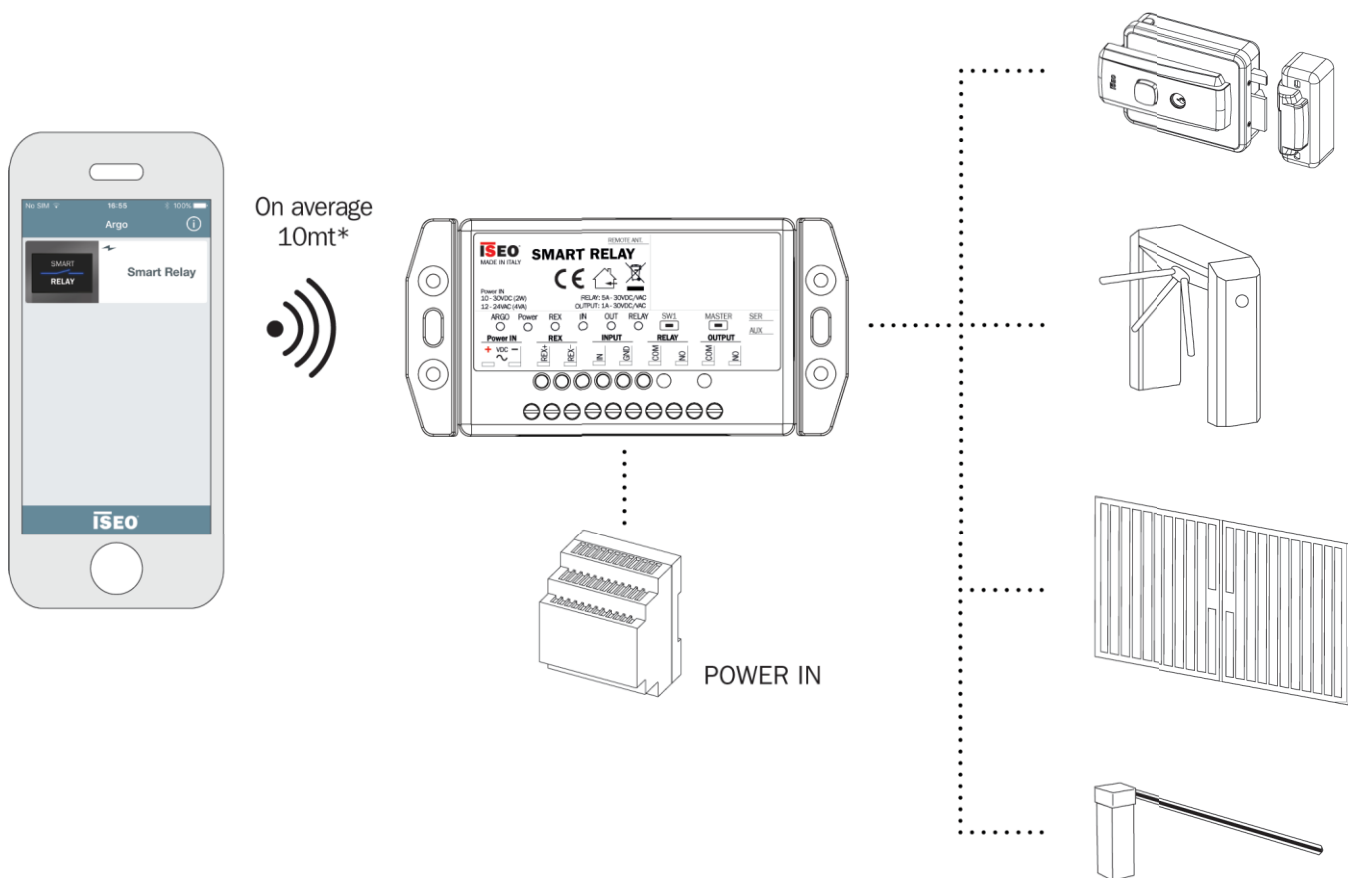
Enable **Door Status Advice** then touch done



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 disappears.

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.

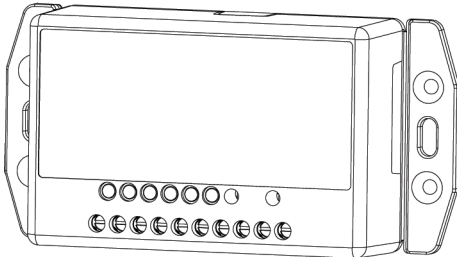


The *Smart Relay* exclusively works with smartphones by *Argo app*, since it does not have any other credential reader (i.e. RFID reader, keyboard).

Advanced

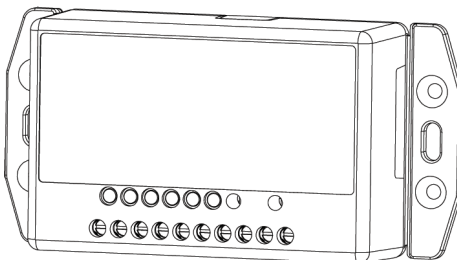
The *Smart Relay* comes in 2 different models to select upon installations requirements.

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

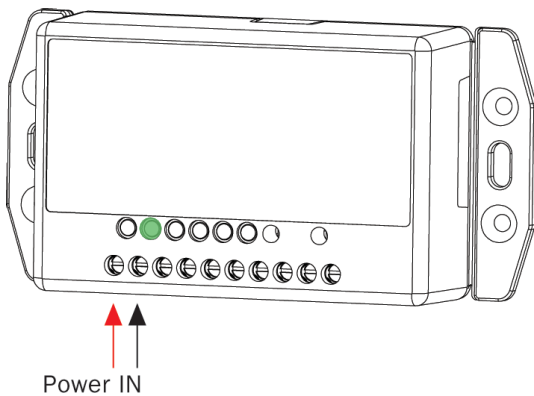


For more detailed technical information about *Smart Relay* (i.e. technical data, dimensions, installation examples), read the *Smart Relay Installation Guide* available at app.iseo.com.

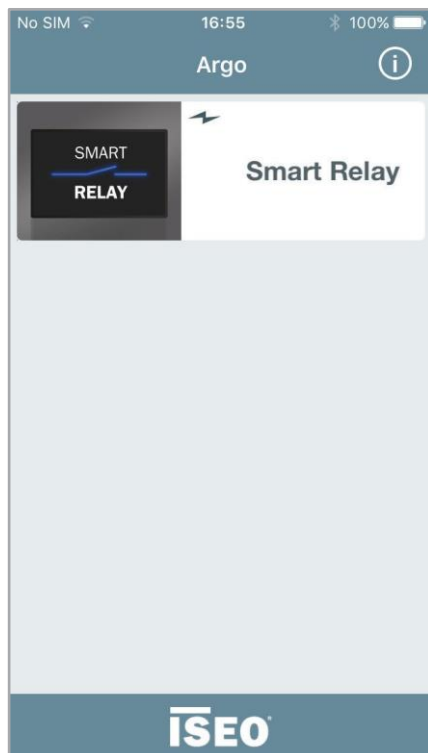
Advanced

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* doesn'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

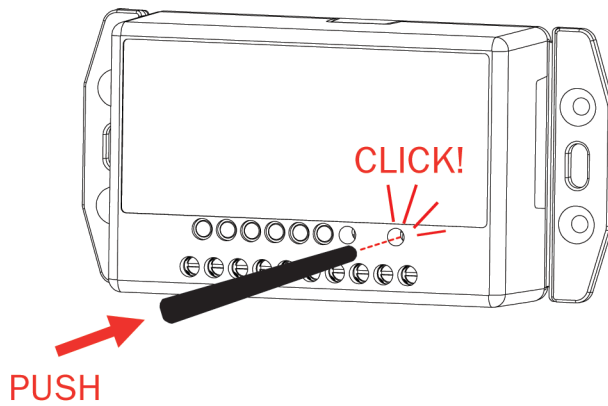


1. Power on the *Smart Relay*.
The green LED Power switch ON.

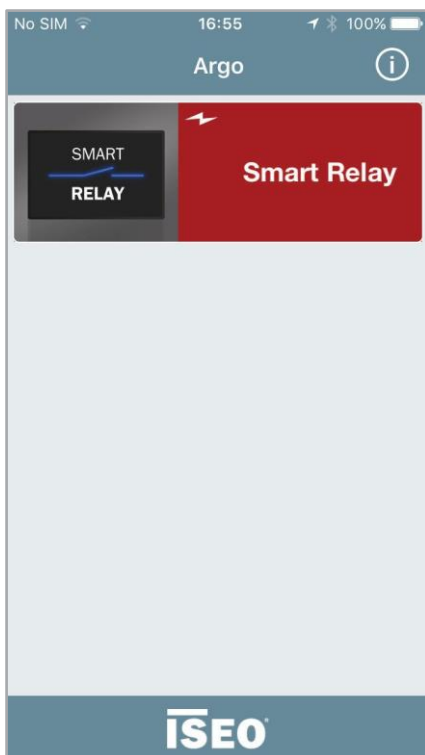


2. Open the *Argo* app, you will see the *Smart Relay* icon.

Advanced



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

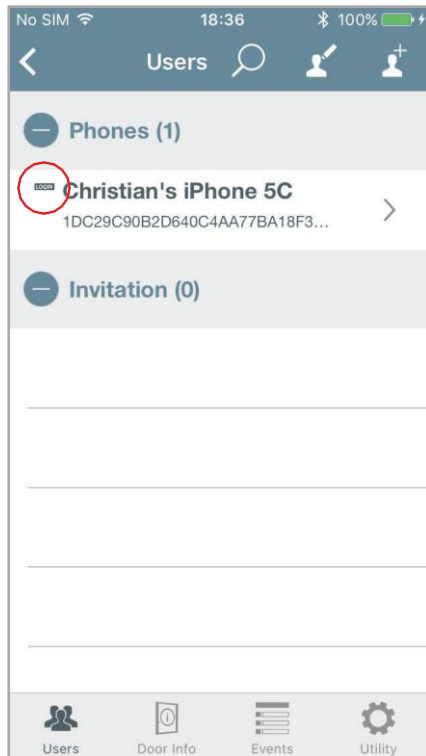


4. The button in the *Argo app* will turn red, and pressing it you will enter *Programming mode*, like we usually do presenting the *Master Card 1* to the other ISEO Smart devices.

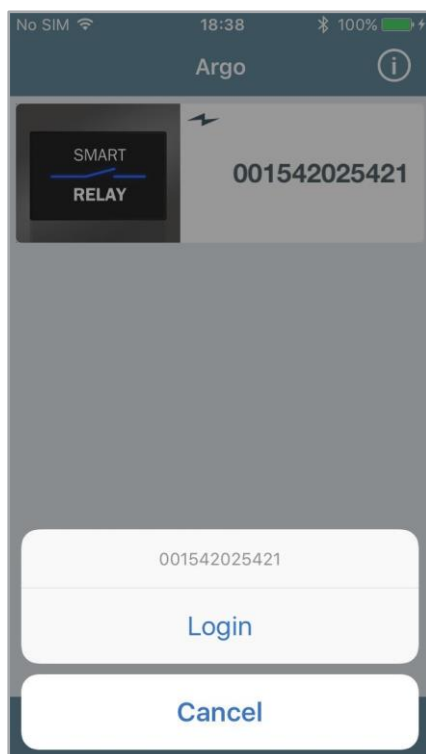


The *Master button* is a microswitch and allows to enter *Programming Mode*. This is required to enroll the first Administrator phone when the device comes from the factory or after a factory reset (go to *Reset Doorlock to Factory Mode*).

Advanced



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



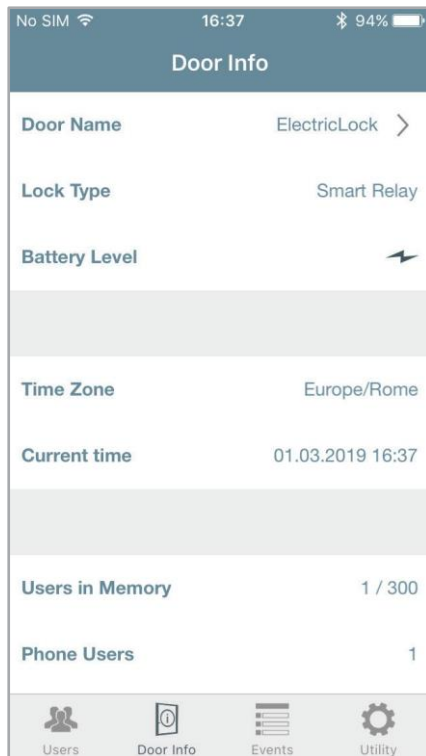
6. *Tap and hold* the door button: the smartphone can now login without *Master Card*.

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

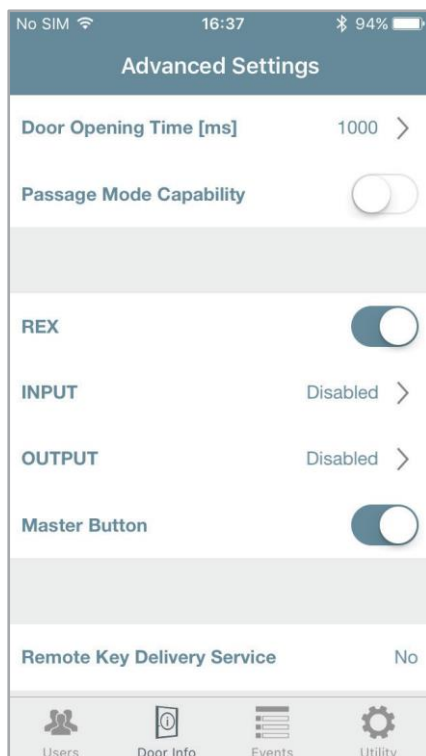
- prepare invitations with or without login function (to know more go to *Invitations*).
- Add smartphones with Argo UID function (to know more go to *Add phone with Argo UID*).

Advanced

First installation: set door name and change opening time



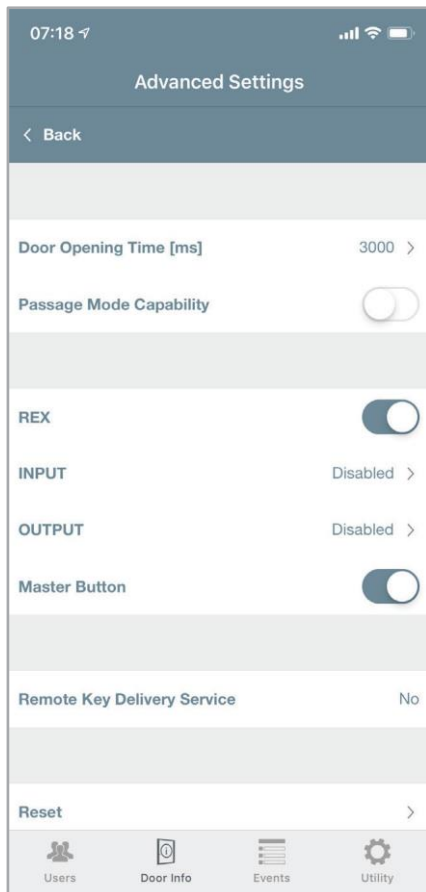
Enter **Door Info** menu then give a real **Door Name** (for more information go to *Door Name* paragraph).



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

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).

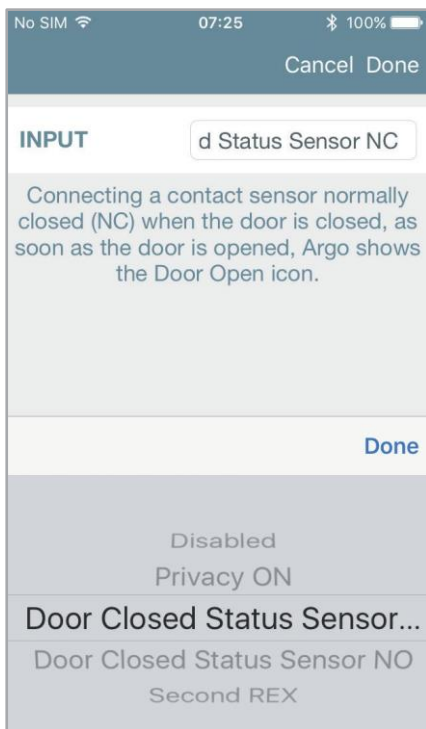


If the *Administrator* disables the *Master Button* it is strongly recommended to create before some *Invitations*, sending the invitation codes to themselves, in order to keep it as “spare/emergency invitations”, to be used in case of needs (i.e. the phone with login function get lost or broken).

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*.

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 description on Argo explains each setting feature.

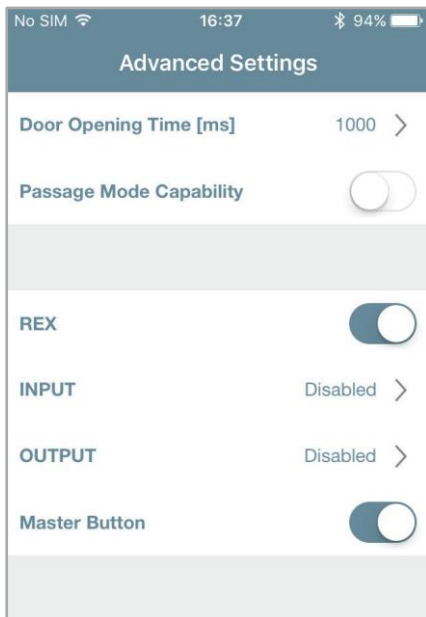
In the next table are shown the INPUT possible configurations and related descriptions.

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.

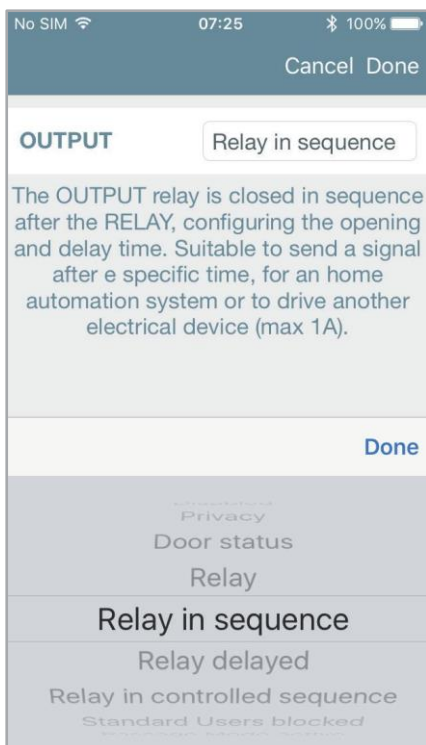
Advanced

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 description on Argo explains each setting feature.

Advanced

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.

OUTPUT relay graphic explanation

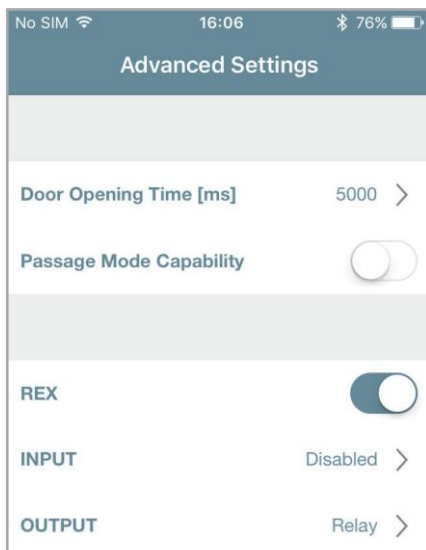
OUTPUT relay configuration can be one of the follows:

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

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

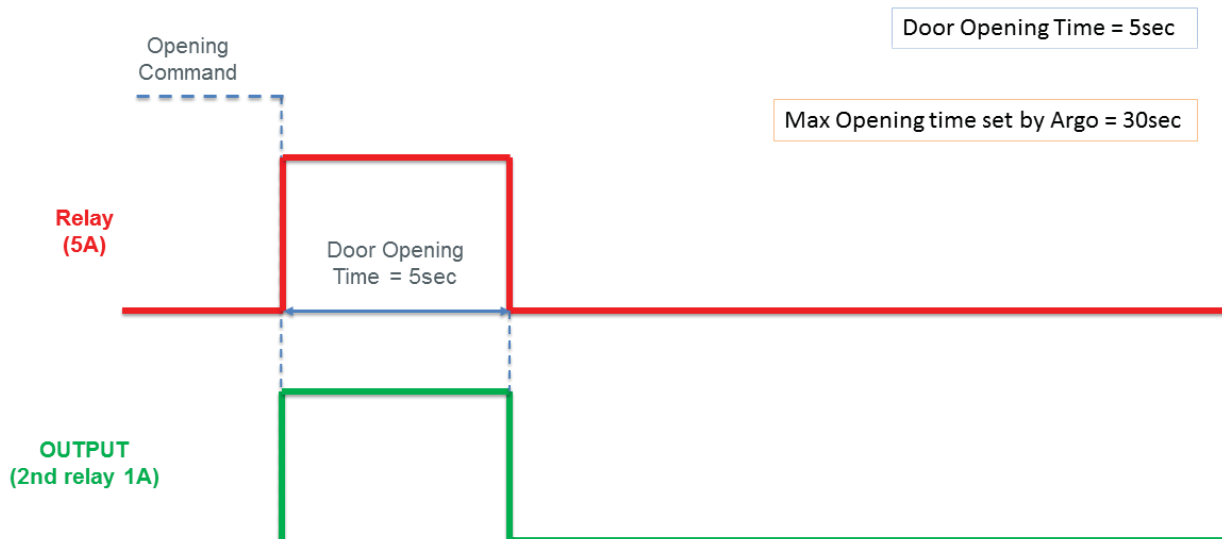
Relay

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



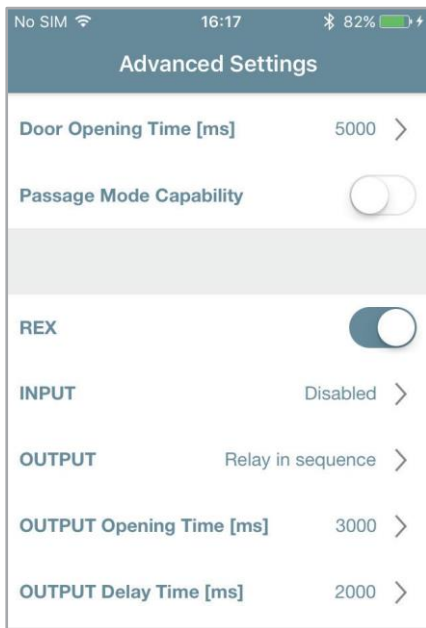
Door Opening Time = 5000 msec (5sec.)

OUTPUT = Relay.

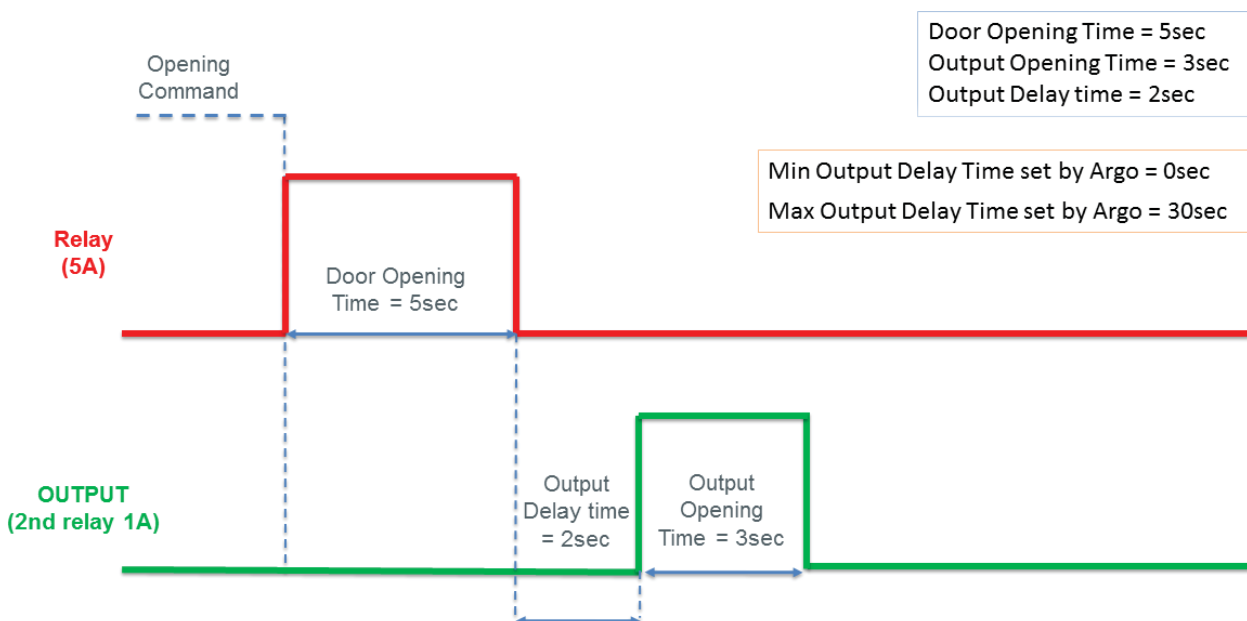


Relay in sequence

This setting activates the OUTPUT relay after the power RELAY, in a configurable 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.

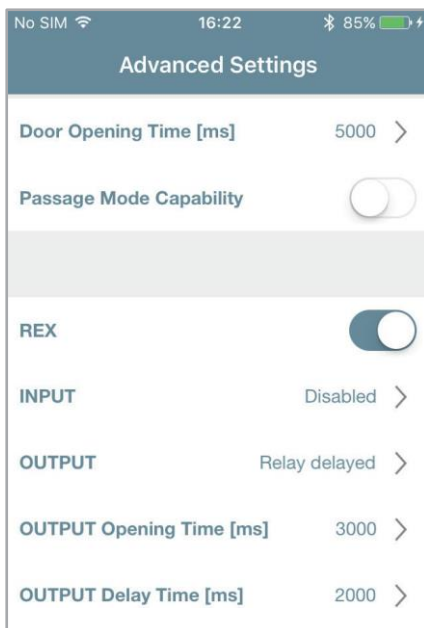


- OUTPUT = Relay in sequence.
- OUTPUT Opening Time = 3000 msec (3sec.)
- OUTPUT Delay Time = 2000 msec (2sec.)

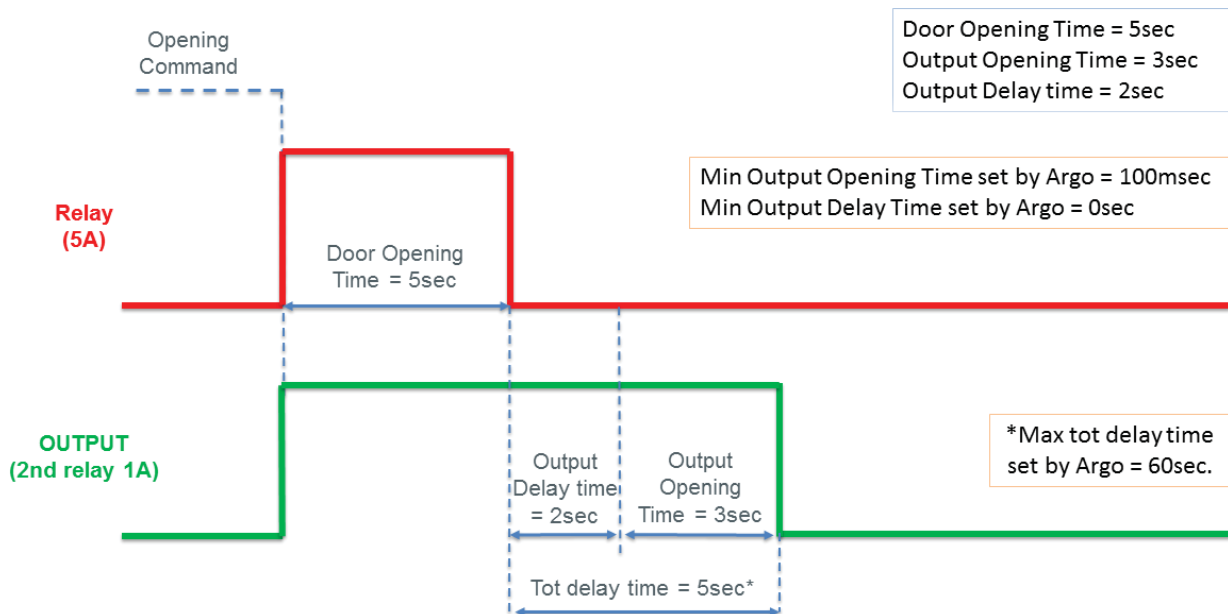


Relay delayed

This setting allows the OUTPUT relay to replicate the power RELAY, adding a configurable 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.



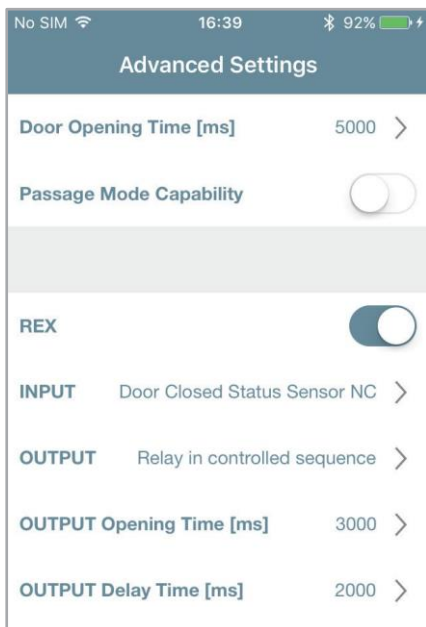
- OUTPUT = Relay delayed.
- OUTPUT Opening Time = 3000 msec (3sec.)
- OUTPUT Delay Time = 2000 msec (2sec.)



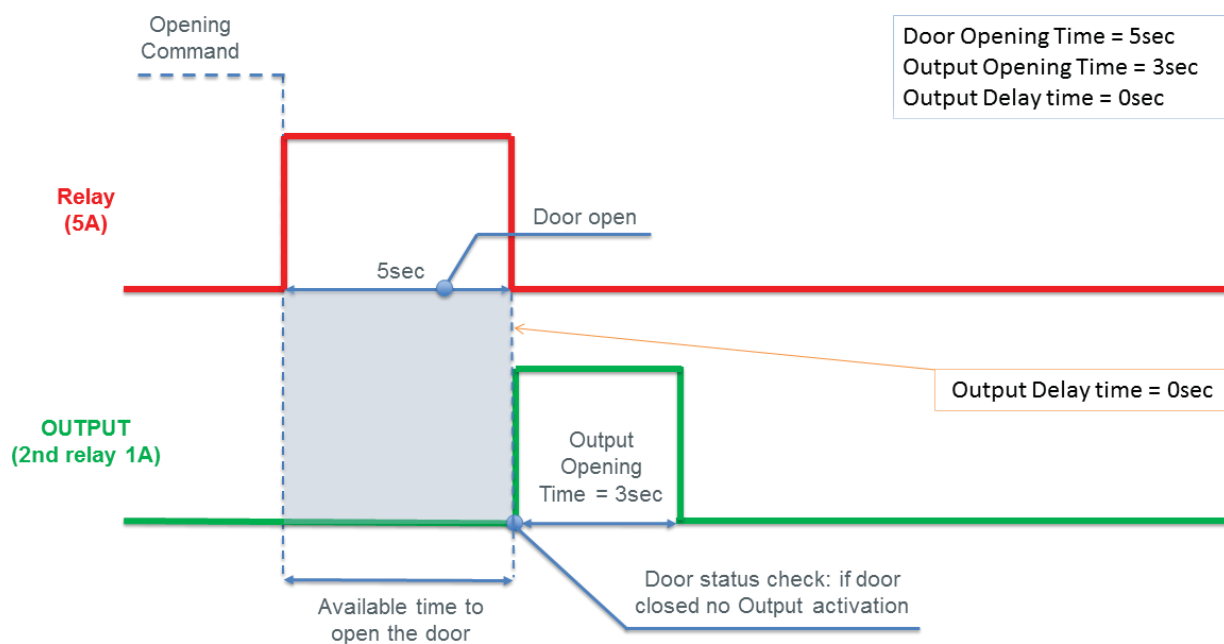
The total delay time is given by the the sum of the *Output Opening Time* and the *Output Delay Time*. Note that the maximum delay time is 60sec since the max opening time and the max delay time set by Argo can be 30sec.

Relay in controlled sequence

This setting activates the OUTPUT relay after the power RELAY, in a configurable sequence, ONLY if the INPUT, previously 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*.



- INPUT = Set as Door Closed Status NC
- OUTPUT = Relay in controlled sequence
- OUTPUT Opening Time = 3000 msec (3sec.)
- OUTPUT Delay Time = 2000 msec (2sec.)

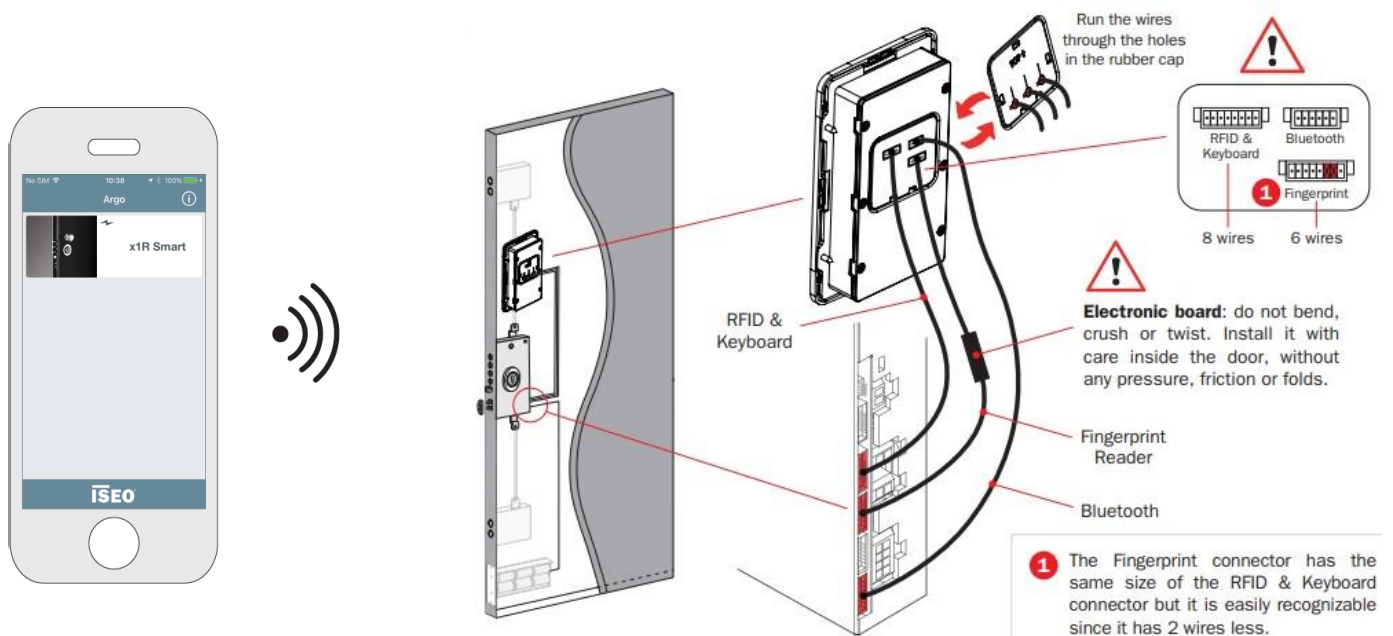


If the door is not opened during the available time (door status signal doesn't change), the OUTPUT relay will not activate.

Fingerprint reader

Argo app fully integrates 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*.

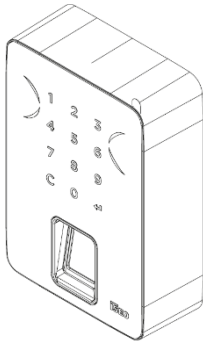


The *Multi-Reader* exclusively works with *x1R Smart*.

Advanced

The *Fingerprint readers* is available in 1NCA Smart Reader range and in X1R Smart Accessories:

1.

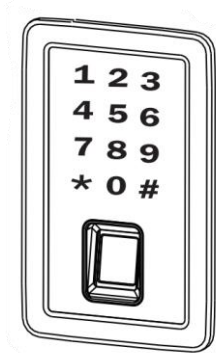


1NCA Smart Standard Finger

1NCA Smart Readers

In the 1NCA Smart Readers range, the fingerprint reader is available on both the Standard (RS485) and Cable Free devices, allowing the fingerprint credential to be associated with all ARGO devices.

2.



X1R Multi-Reader

X1R Smart Accessories

Fingerprint readers are available in various accessories for the x1R. The Multireader with fingerprint reader also includes Bluetooth®, RFID, and a numeric keypad.

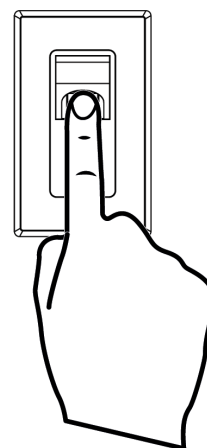


For X1R Smart *Multi-Reader* dimensions, installation examples and electrical connection, read the *x1R Smart Multireader Installation Guide*, available on www.iseo.com.

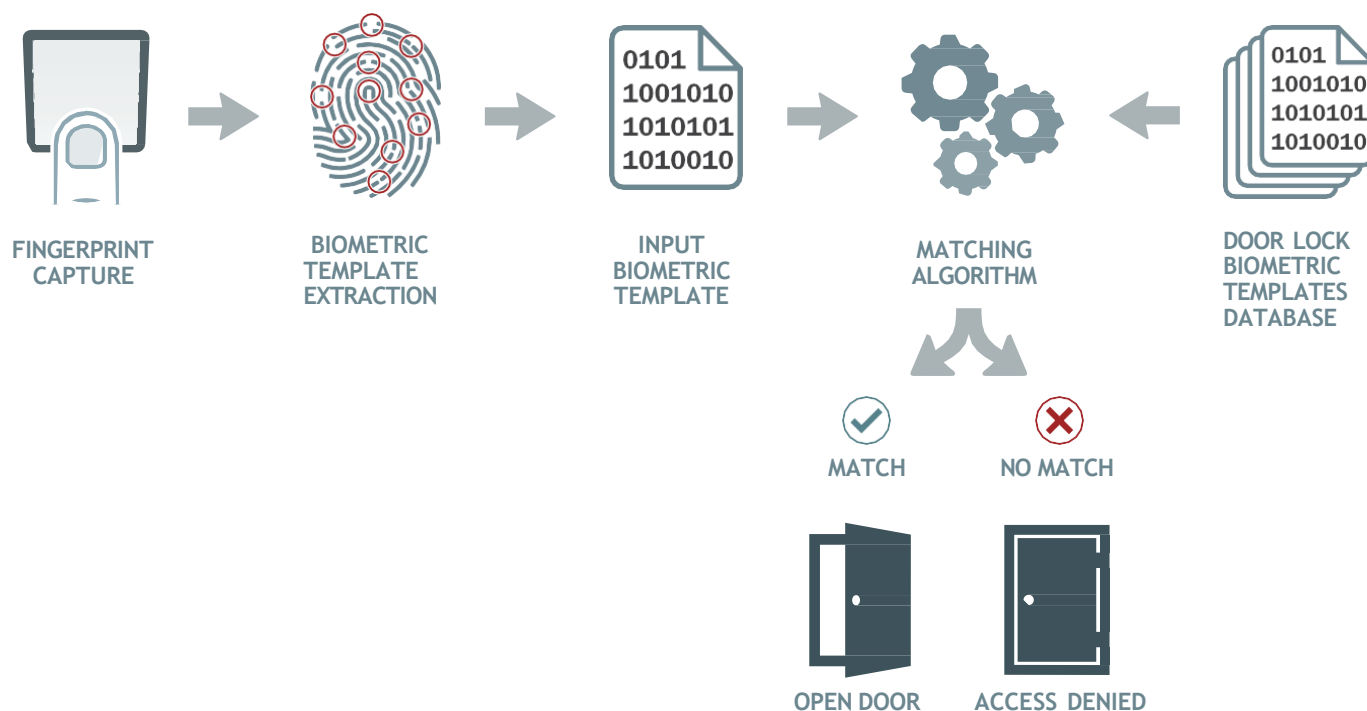
Principle of working

When the user places 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.



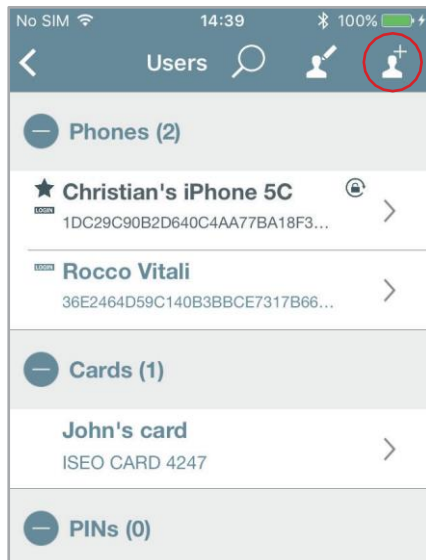
During the entire fingerprint identification process no fingerprint images are stored on the door lock, and a fingerprint image cannot be recreated from the biometric template.

Advanced

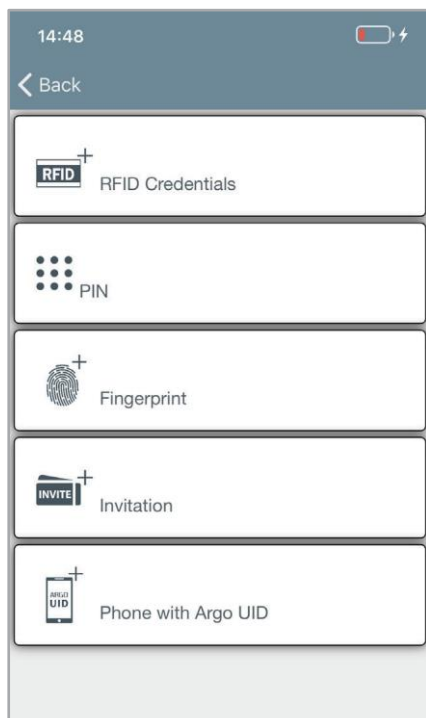


Add fingerprint users

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



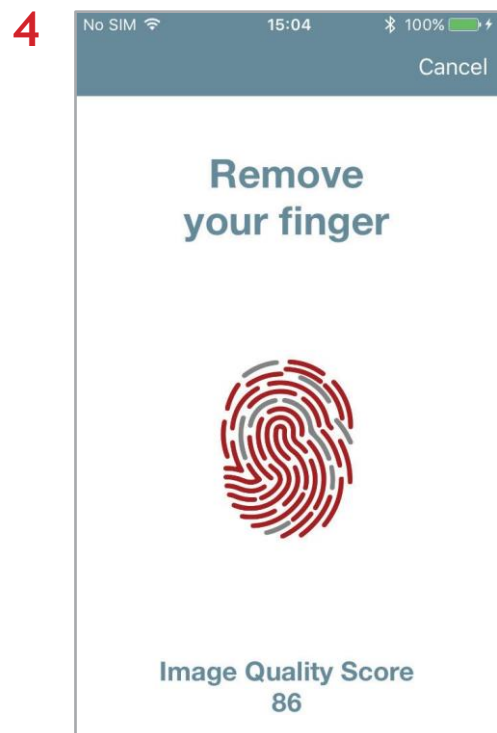
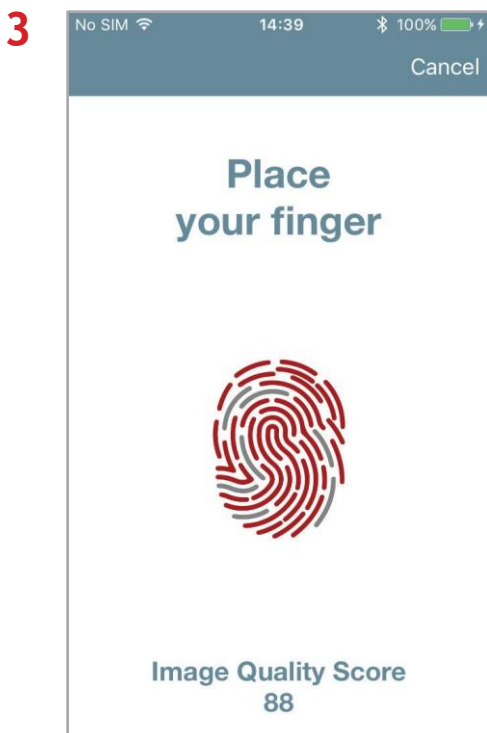
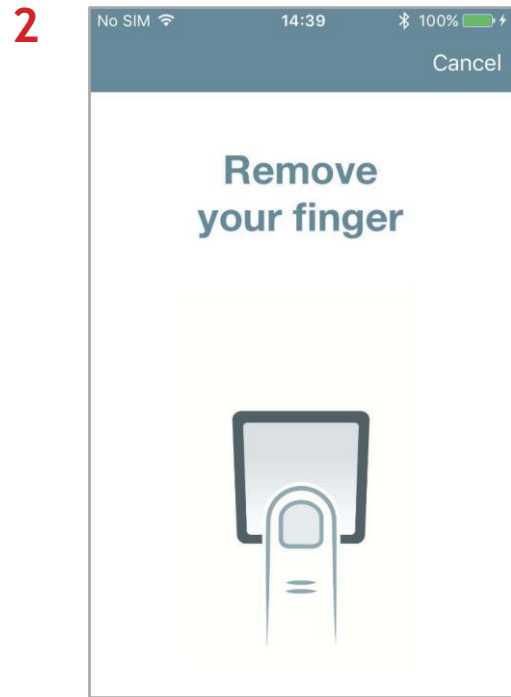
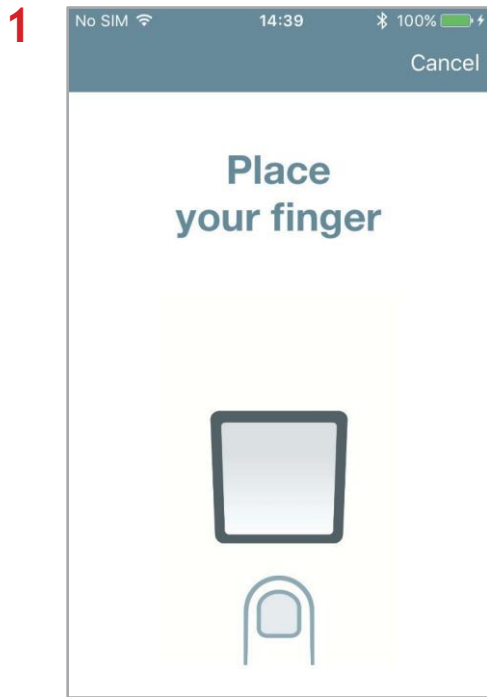
1. Touch add user icon.



2. Touch Fingerprint.

Advanced

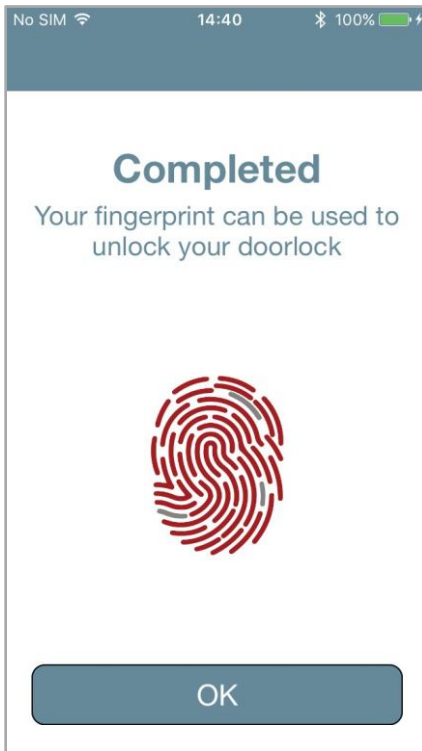
3. Follow the instruction on the phone display that guides you through the correct enrolling process.



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

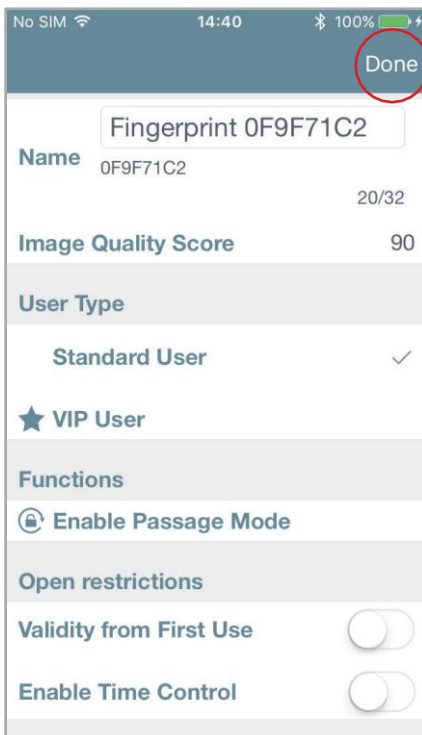
Advanced

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



5. The fingerprint enrolling process has ended.

6. Touch OK

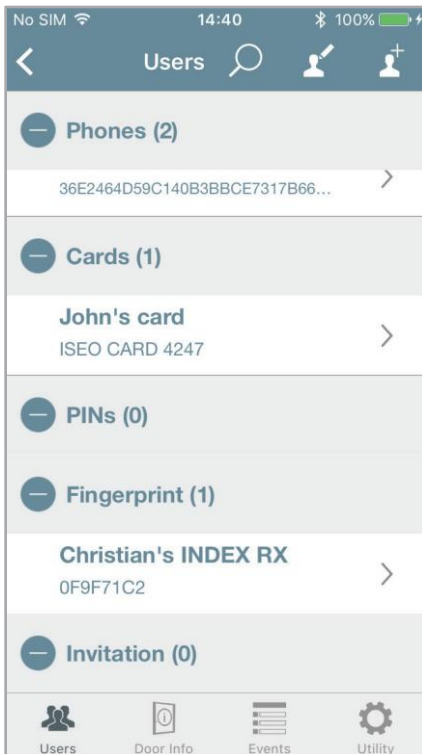


7. Write the fingerprint **Name**, set additional functions if required (VIP User, Open restrictions), then touch **Done**.



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* paragraph.

Advanced



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.

Date/Time	User	Result
3/4/2019 2:47:43 PM	Jennifer's INDEX SX Fingerprint 5FE59DFB	Door Open
3/4/2019 2:47:37 PM	Fingerprint	Not in Memory
3/4/2019 2:47:34 PM	Fingerprint	Not in Memory
3/4/2019 2:47:31 PM	Auto Close	Door Close
3/4/2019 2:47:28 PM	Christian's INDEX RX Fingerprint 0F9F71C2	Door Open
3/4/2019 2:47:19 PM	Christian's iPhone 5C 1DC29C90B2D640C4AA77BA18F3C656E9	Block Standard User OFF
3/4/2019 2:47:16 PM	Auto Close	Door Close
3/4/2019 2:47:13 PM	Mark's MIDDLE RX Fingerprint 42F88520	Door Open
3/4/2019 2:47:06 PM	Christian's INDEX RX Fingerprint 0F9F71C2	Blocked User
3/4/2019	Jennifer's INDEX SX	

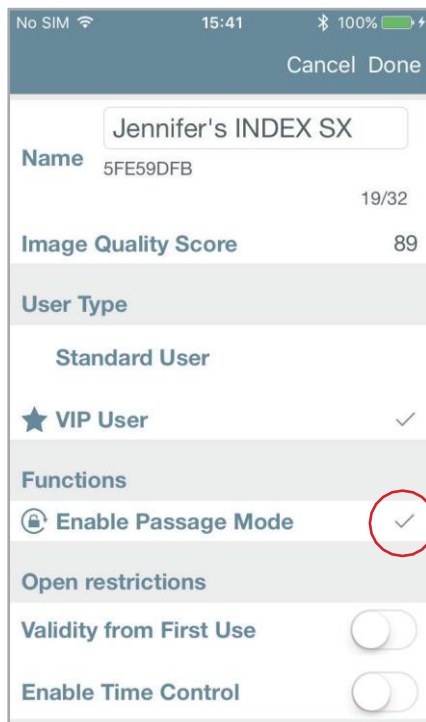
Not in Memory events can be caused by:

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

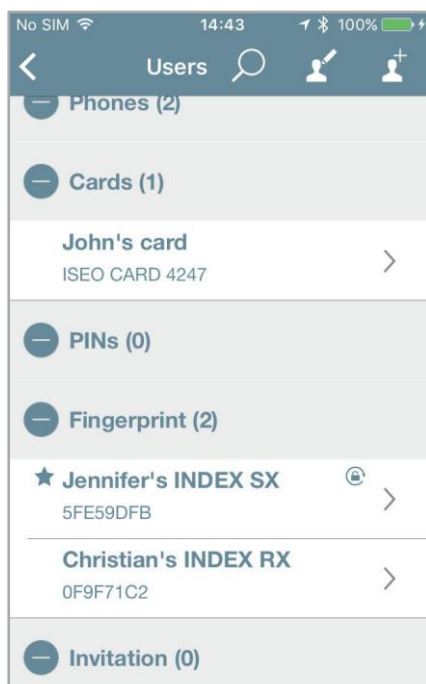
Advanced

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.



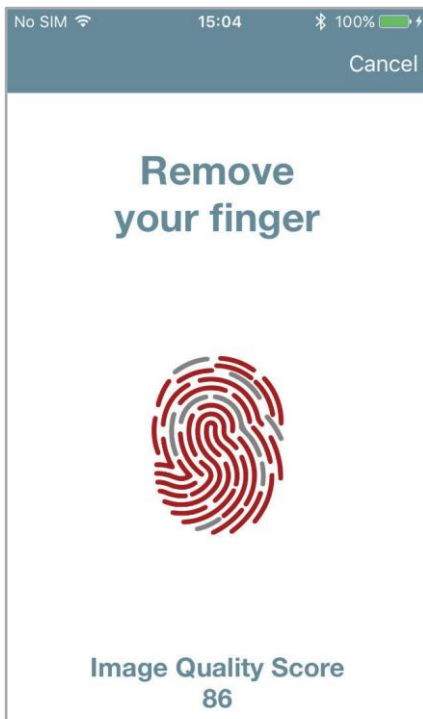
Touch **Enable Passage Mode**.



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.

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 identification. 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 fingerprint images saved).

Exmples of *Image quality score*:



No quality score (< 50)



Poor quality score



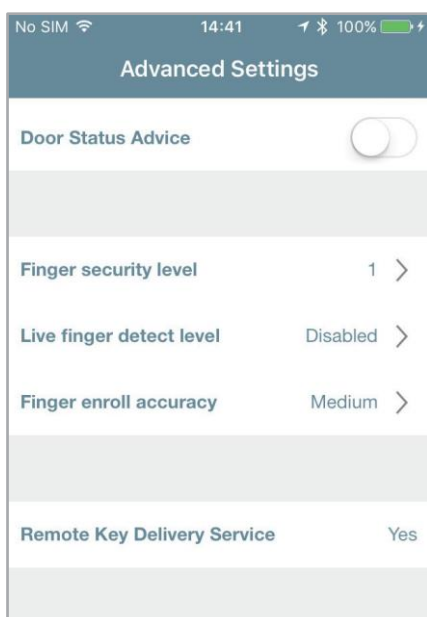
Good quality score

Advanced

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

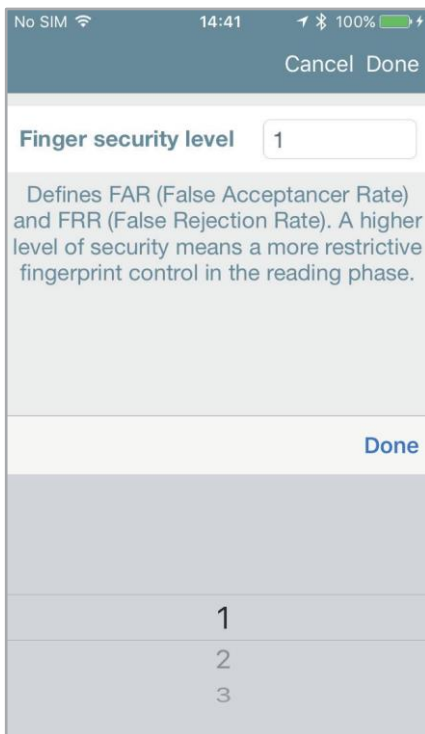
The FAR (False Acceptance Rate) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. In simple words, it's the number of times people get identified when they should not be identified and consequently authorized to open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

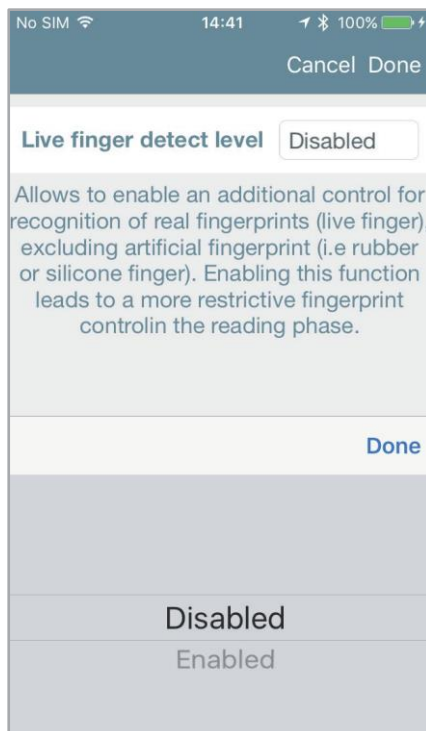


Higher is the security level the more secure is the access control, but at the same time it will be less convenient to use, because users will be more easily falsely rejected by the system. In other words users could not get identified during access because not recognized from the reader, even if present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

Advanced

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.

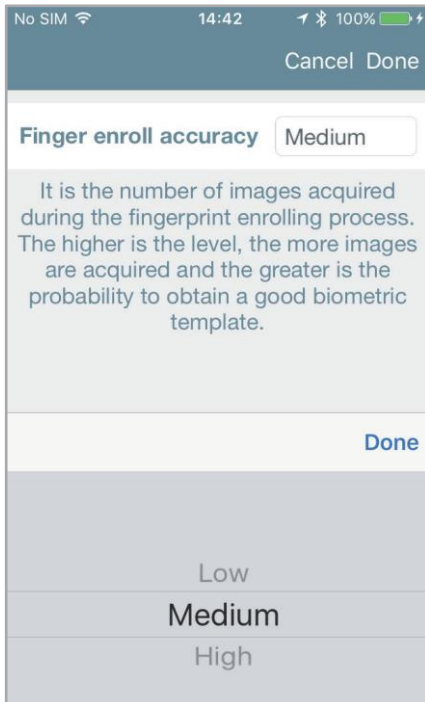


Enabling the *Live finger detect level* more secure will be the access control system but, at the same time, increases the probability to exclude correct fingerprints. Users therefore could not get identified during access, because not correctly recognized from the reader. This especially could happen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

Advanced

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.

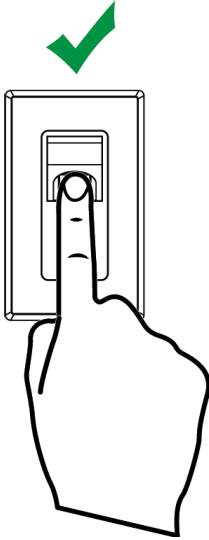
INFORMATION ABOUT BIOMETRIC AUTHENTICATION

- 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 identified
- 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 identified.
- 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.

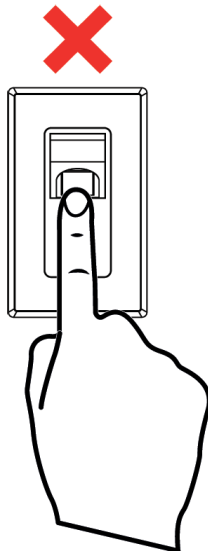
Advanced

CORRECT AND INCORRECT FINGER POSITION

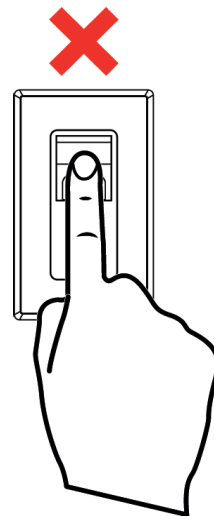
See in the next pictures the correct and some incorrect finger position examples.



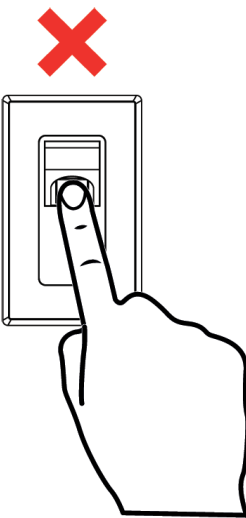
Correct position



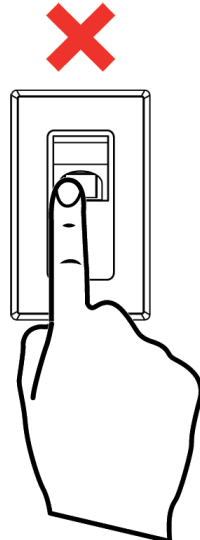
Too low



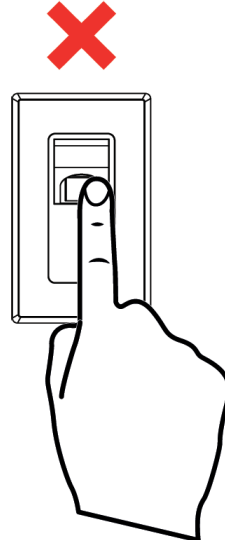
Too high



Not straight



Too much on the left side



Too much on the right side

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 order 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).



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 order 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.



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.

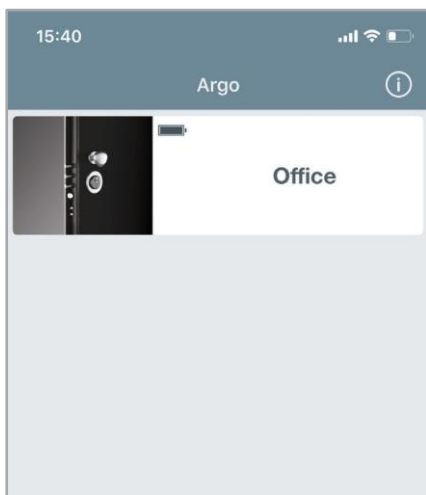
Siri Shortcuts voice commands to open (iOS only)

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 disabled by default. To use voice commands you need to enable it first.



Open Argo app and touch *Info app* menu.

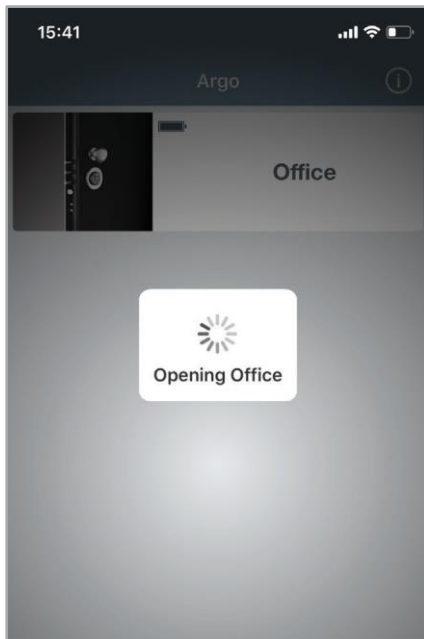


Enable Siri Shortcuts

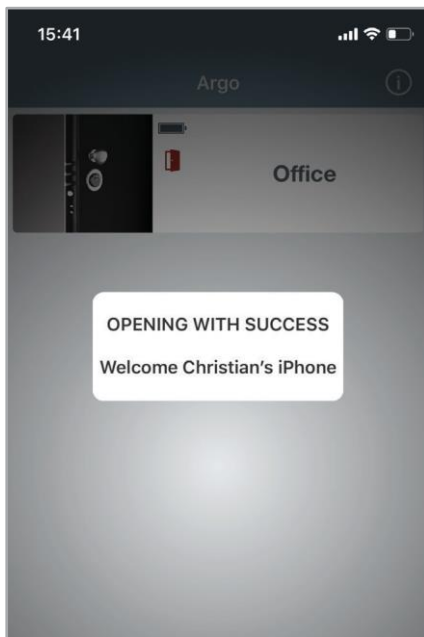
Advanced

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 successfully open.

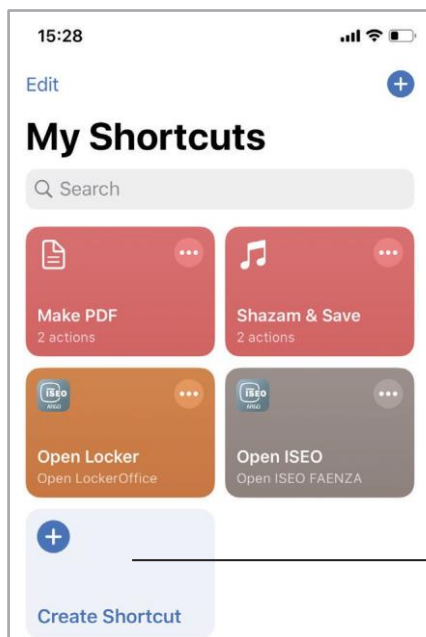
Advanced

Step 3: create the shortcut

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



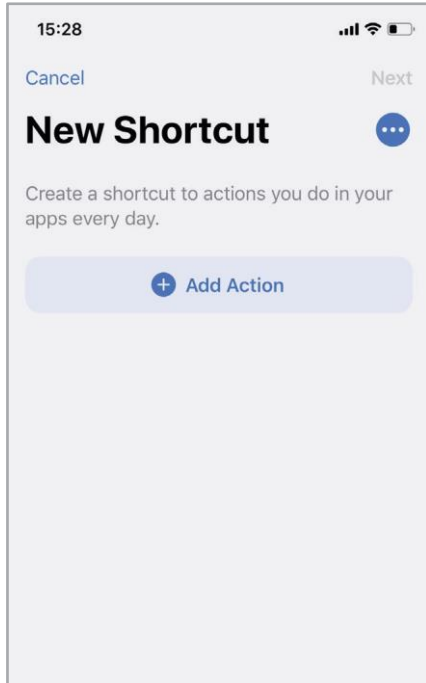
Open Shortcuts.



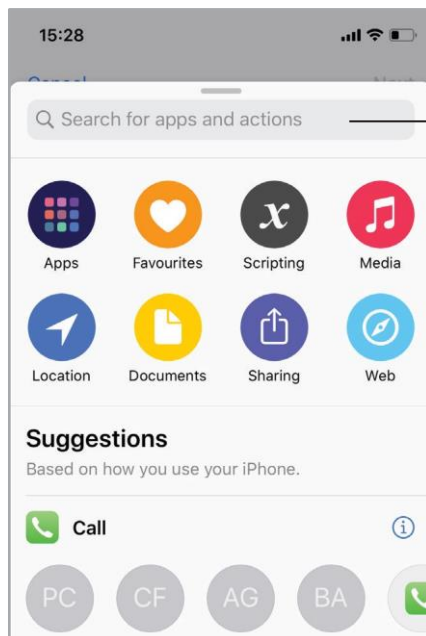
Tap Create Shortcut.

Advanced

Step 3: create the shortcut



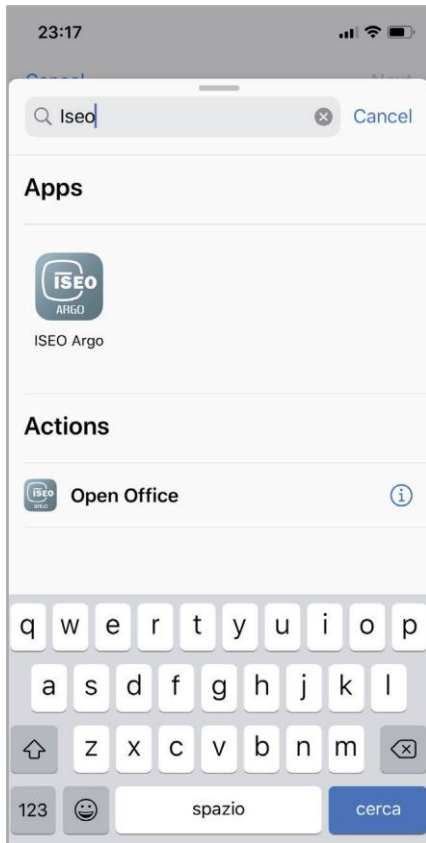
Tap Add Action.



Search for ISEO Argo.

Advanced

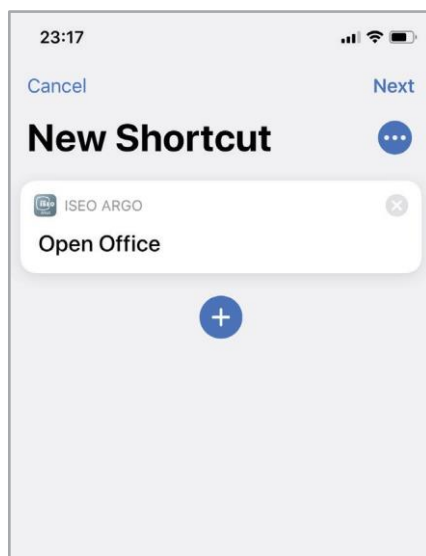
Step 3: create the shortcut



————— Select the last action: **Open Office**



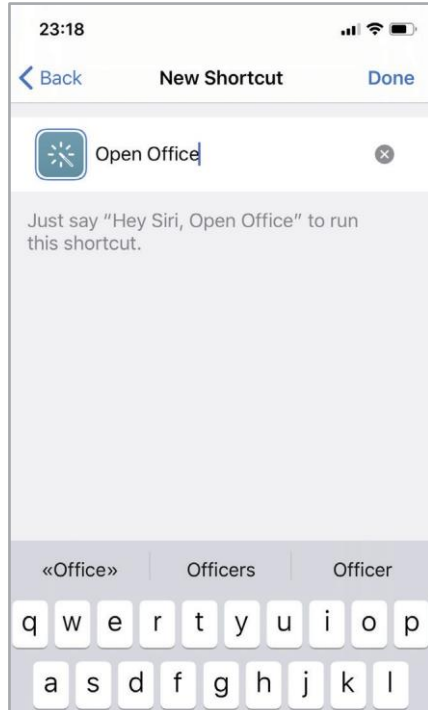
If *ISEO Argo* does not appear in the search list, that could mean *Siri Shortcuts* has not been enabled on the *Argo info app* menu (see *Step 1: enable Siri Shortcuts on Argo*).



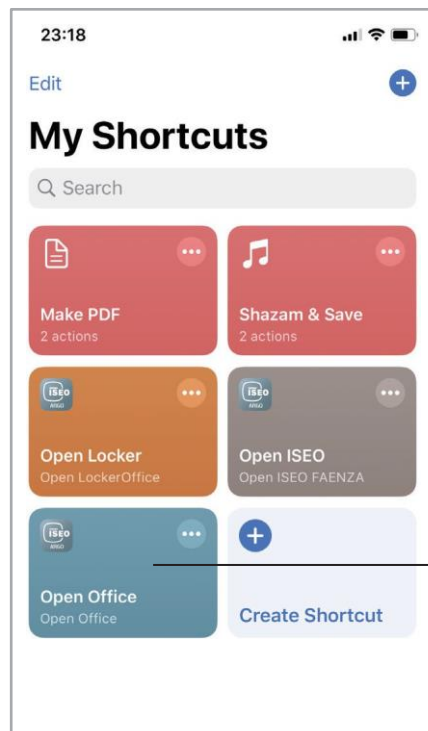
————— Tap Next.

Advanced

Step 3: create the shortcut



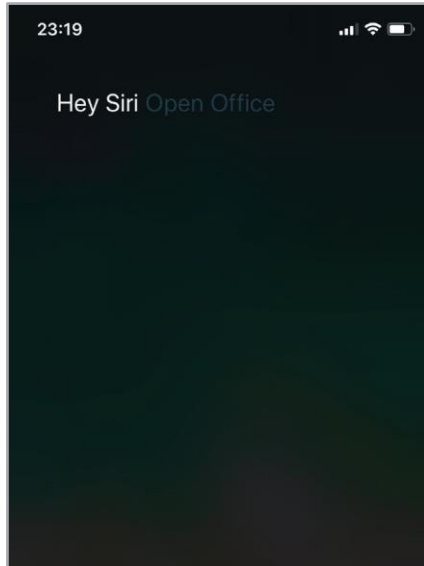
Write the voice command that will be used to open the door: for example **Open Office**. Then tap **Done**.



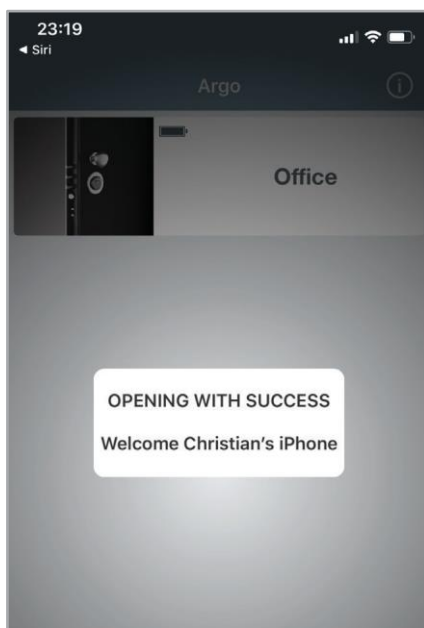
The new shortcut just created appears in the *My Shortcuts* page.

Advanced

Step 4: open with voice command



———— Say: *Hey Siri Open Office.*



———— Door will open in a few second.



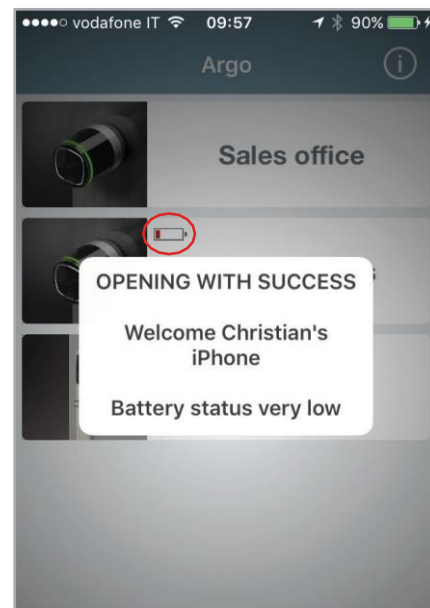
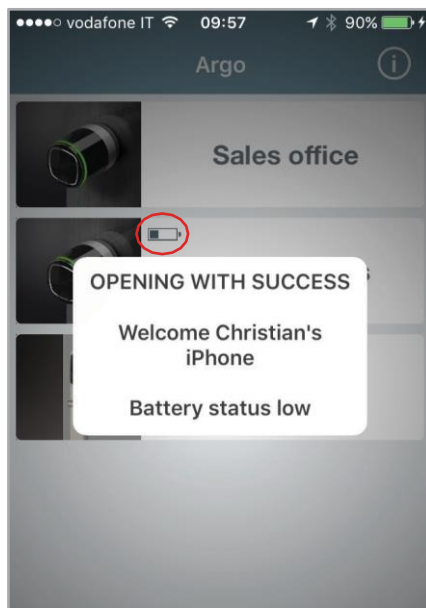
For security reason, when the phone is locked, the voice command to open the door cannot be execute: you need to unlock your phone first, as also suggested by *Siri*. In case the *Face ID* is enabled on your phone, the door opening process will be automatic: it is enough to look at your phone to unlock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

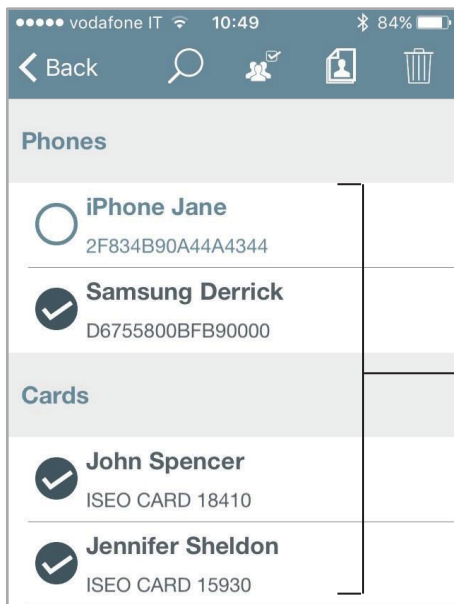
Service

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 *Edit user* icon.



1. Select the users to be transferred.
You can also select all users tapping on



2. Tap the **Copy** icon.

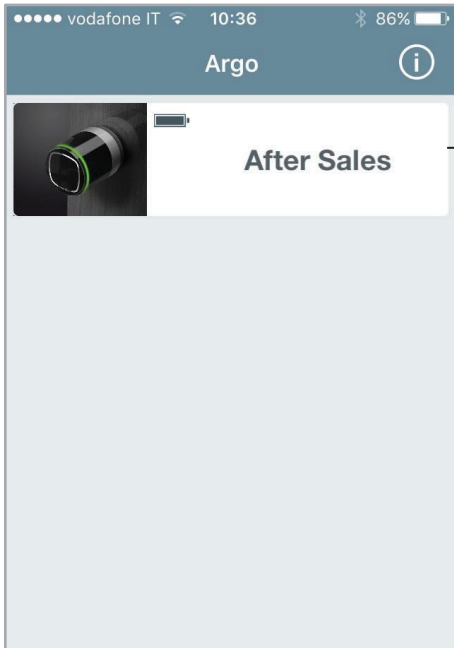


Copied users are kept in the phone memory until you close the app.

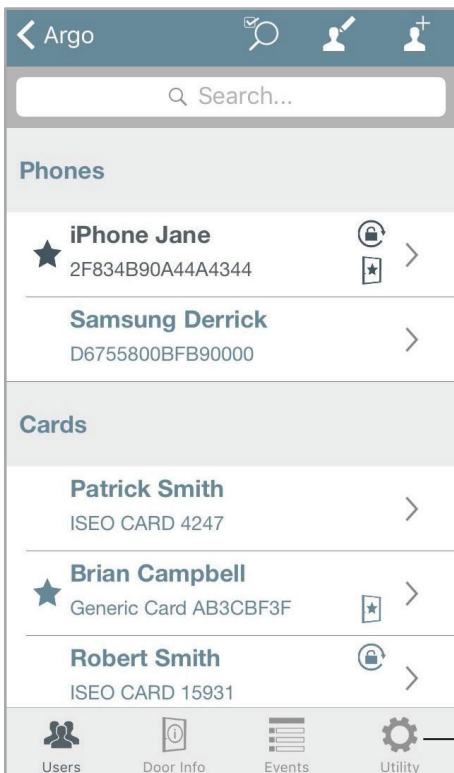
Transfer users



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

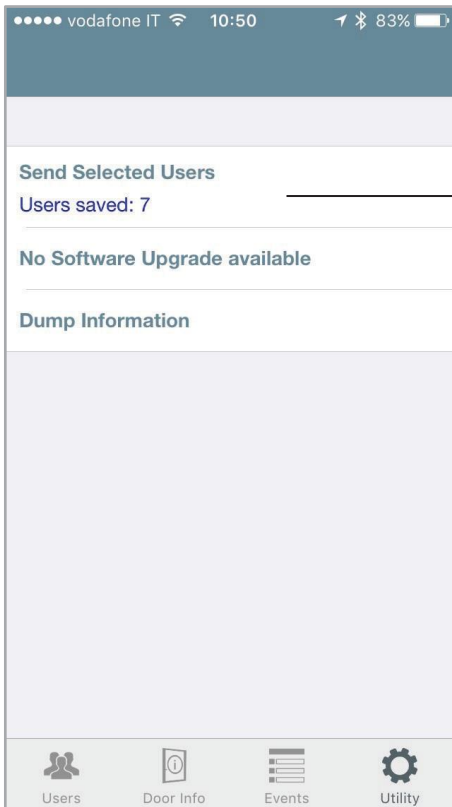


1. Enter **Programming mode** in the device where you want to transfer the users, by **Master Card**.

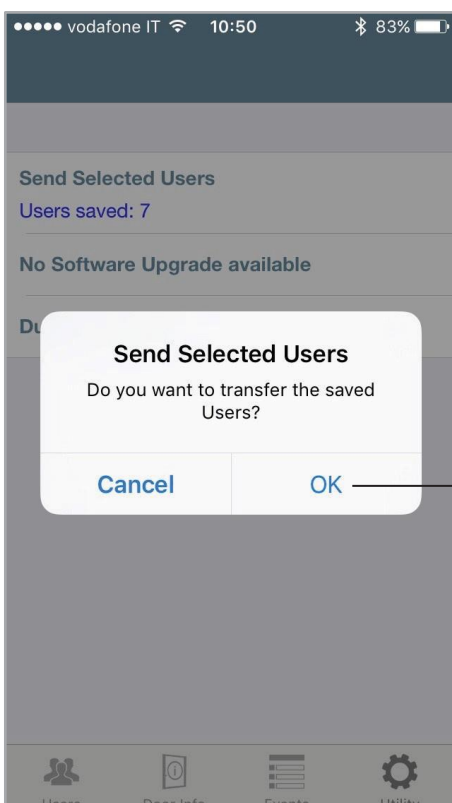


3. Tap **Utility** icon.

Service



4. Tap Send Selected Users.



5. Tap OK.

Software Upgrade

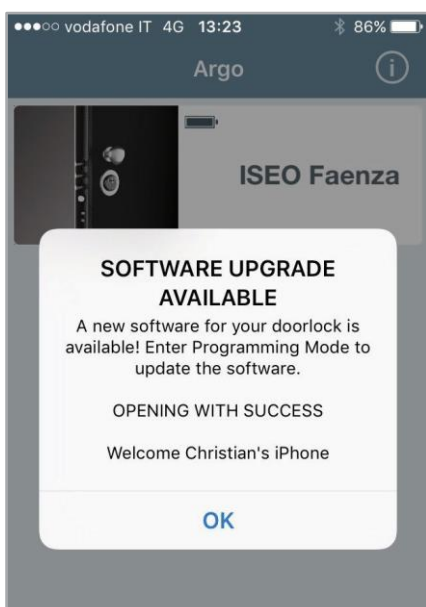


When a new **Software version** is available for your **Access control device**, your smartphone always notifies you when opening the door (image 1. *Door opening*).

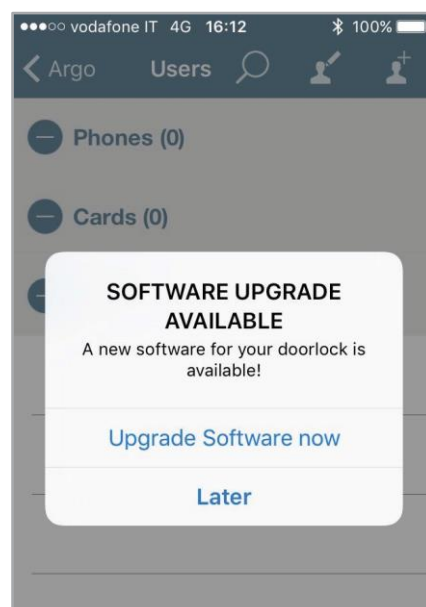
Moreover everytime you enter **Programming Mode**, a pop-up message will appear, and you can decide if upgrade software immediately or not (image 2. *Programming Mode*).

- 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.




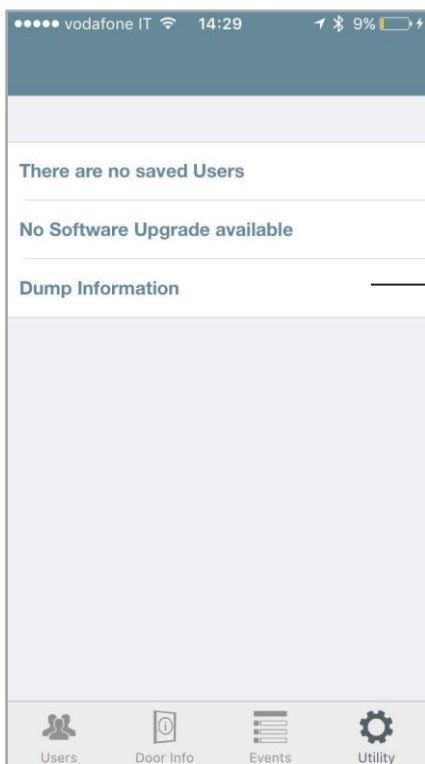
If you upgrade from *Argo* to *Argo 2.2*, watch before the tutorial “*Argo 2.0 Software Upgrade*”, or read the manual “*Argo 2.0 Upgrade Procedure*“, both available at:
<https://app.iseo.com/?parm=ARGO&lang=en&folder=argo-update>


Dump Information

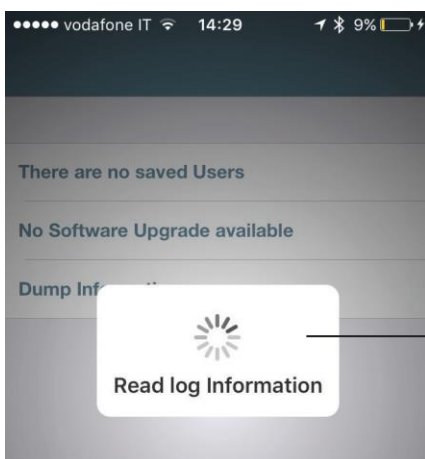


This function allows to collect all device's data into a unique compressed file, that has to be send to *IseoZero1 Technical Support*, via email. This is really useful for device's analysis pourpose. By receiving this file in fact, the technical support will receive all the necessary information to properly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

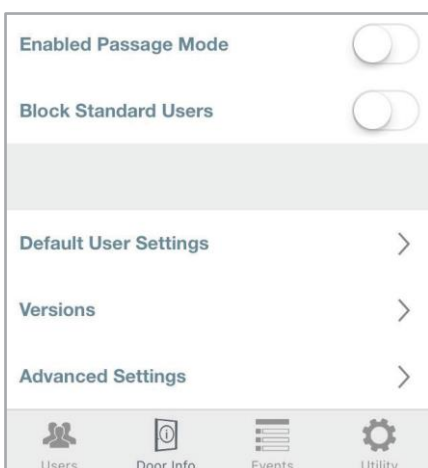


4. Wait until the log reading pop-up disappear (about 2 or 3 min.).
5. An *email* will be automatically created.
6. Send it to *IseoZero1 Technical Support*.

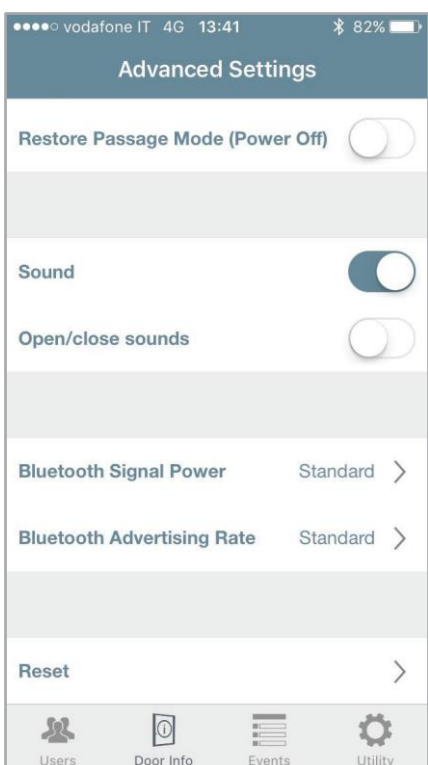
Bluetooth® parameters



This function allow you to change the *Bluetooth® Signal Power* and the *Bluetooth® Advertising Rate* from *Standard* to *High*. This setting has been introduced just to improve the Argo performance during demo, in fairs or exhibithions. 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.

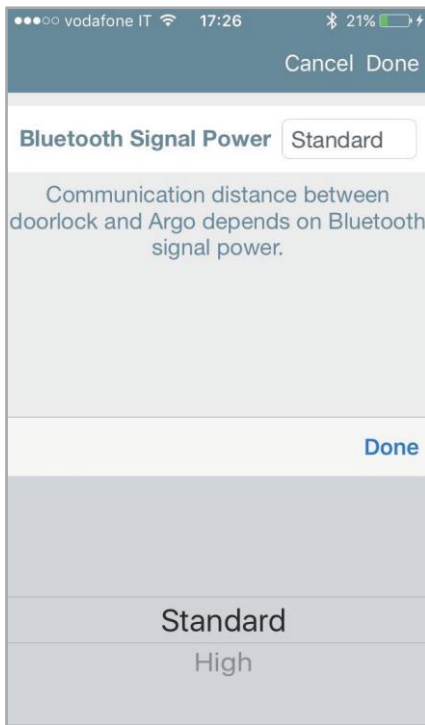


Enter **Door Info** and then **Advanced Settings** menu.



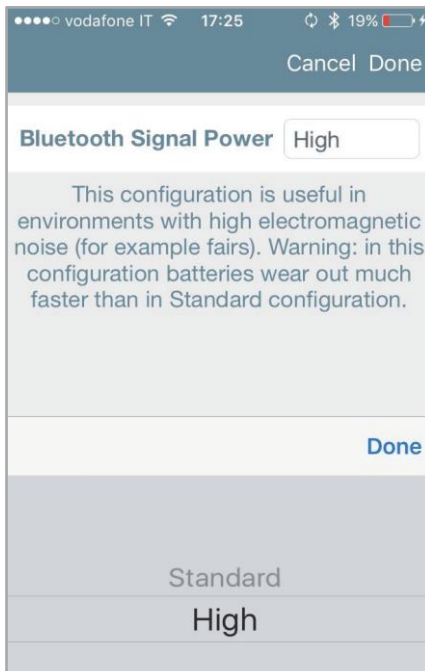
Tap *Bluetooth® Signal Power* or *Bluetooth® Advertising Rate*.

Service



A short text explains you the meaning of the feature.

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



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



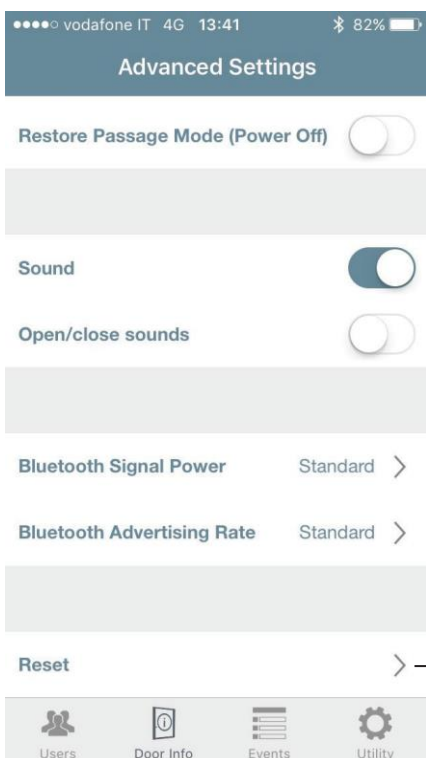
In order to avoid a faster battery consumption, remember to set the *Bluetooth® parameters* back to *Standard* setting, at the end of the fairs or exhibition.

Reset

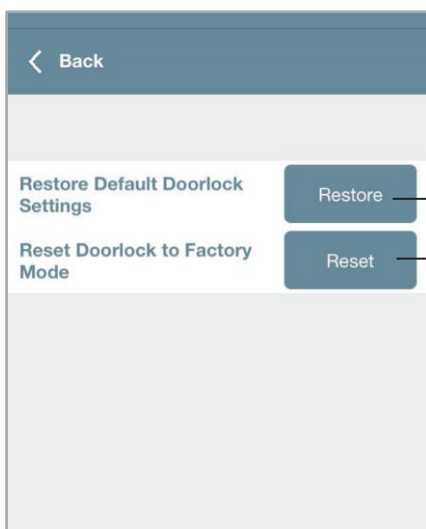


In this menu you can find 2 different and powerful kinds of reset:

- **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 exhibitions.
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 exhibitions.
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.

Service

(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.

Service

(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 successfully completed between Stylos and Actuator.
Open by remote opening button	Lock opened by remote opening button.

Service

(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 <i>x1R Smart Standard</i> .
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 slightly 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 uninstalls

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.

On 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.

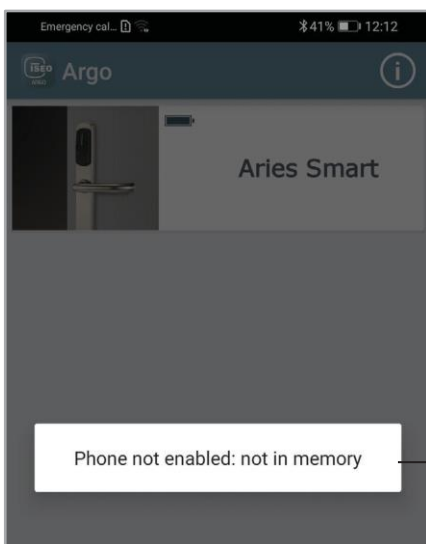
ISEO will continue to monitor the evolution of Android phones and in case Android will implement a secure built in mechanism like iOS, to restore the identity data in a secure way, ISEO will also implement the same feature on Argo.



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.

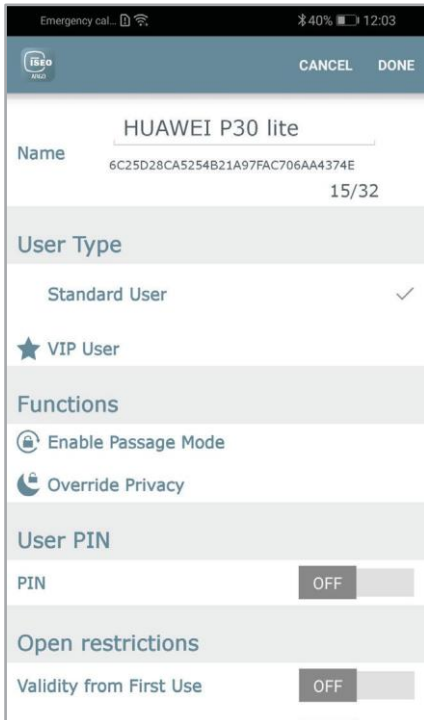


In case of Argo app UPDATE from Play Store the phone will continue to work as before since the identity is the same. So it will be enabled on all the locks where it was previously registered.

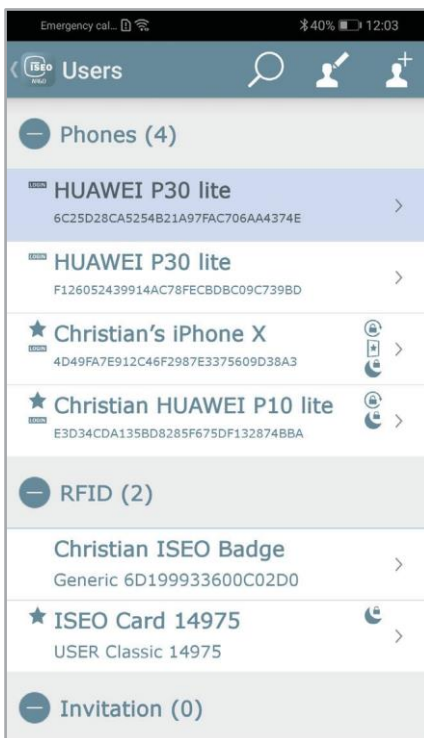


When Argo app has installed again, the Android phone won't work anymore on locks where it was previously enabled.

Service



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.

Service

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 access 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

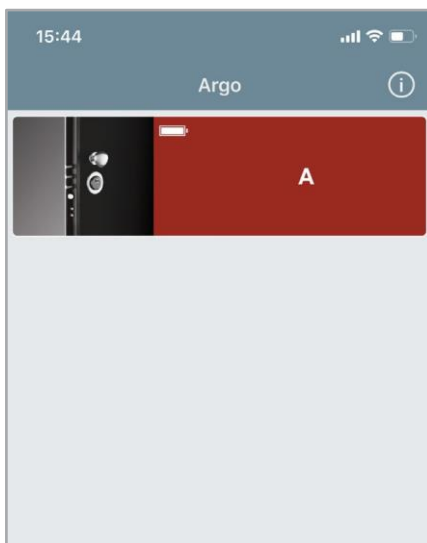
Copy users function, showed in the previous paragraph, has two important differences respect the *Backup* function, as explained in the next points.

- *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*.

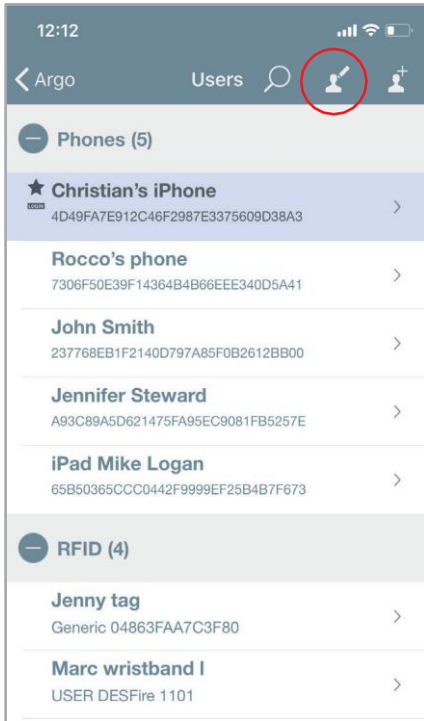
Step 1: Backup user list



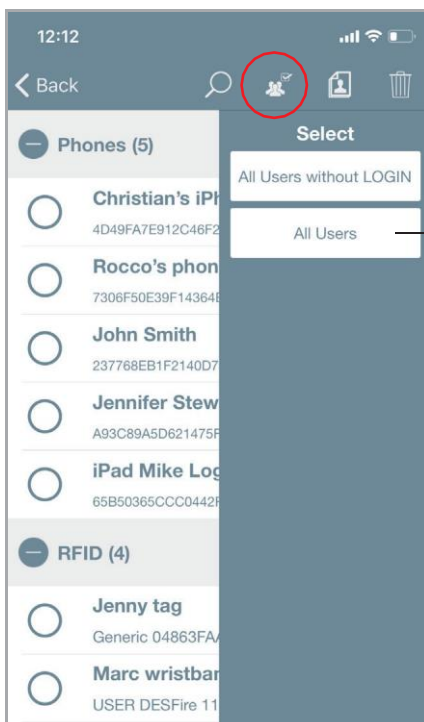
On *x1R Smart A*, open *Argo app* and enter *Programming Mode*.

Service

Step 1: Backup user list



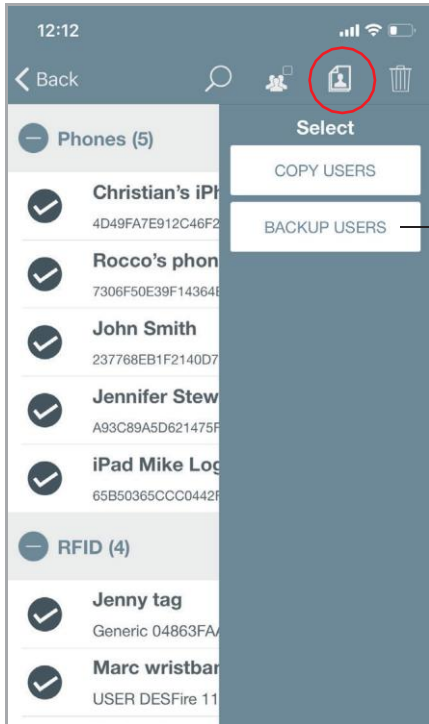
_____ Tap *edit users* icon.



_____ 1. Tap *select users*.

_____ 2. Tap **All Users**

Step 1: Backup user list

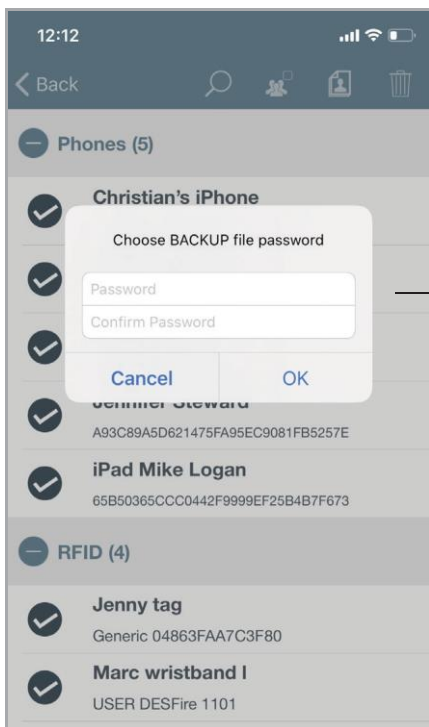


1. Tap *copy users* icon.

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.



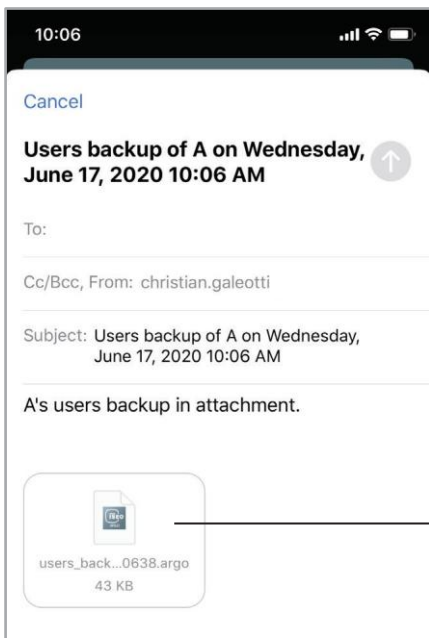
Write and confirm a personal password then tap **OK**. Password must be at least 4 characters long.



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.

Service

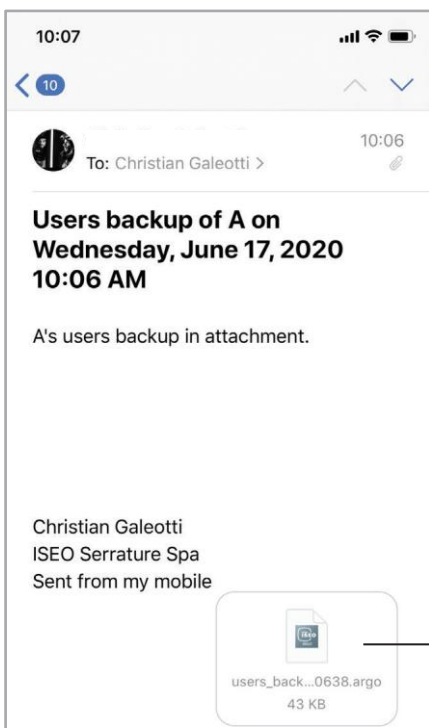
Step 1: Backup user list



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

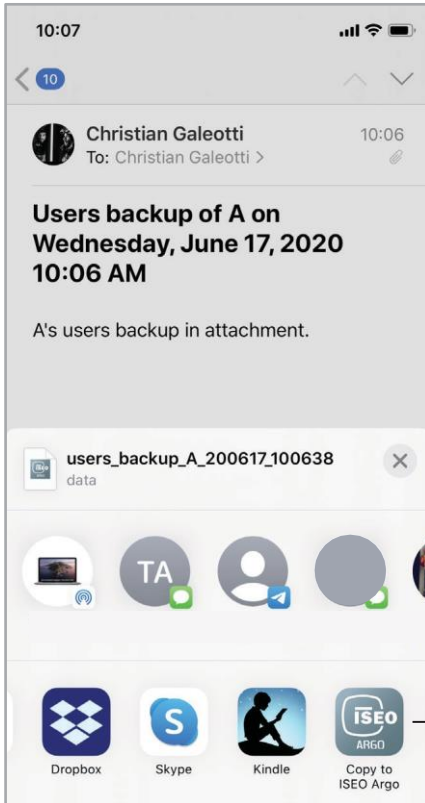


Open the received email and tap the attachment to open it.

Tap the attachment to open it.

Service

Step 2: Restore user list

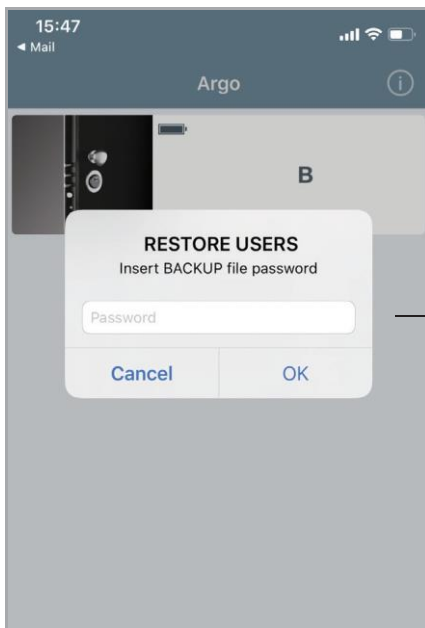


iOS only

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

Android phones

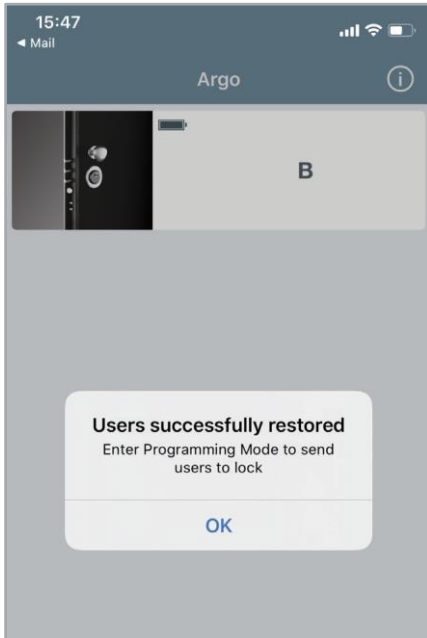
On Android phones, once you tap the attachment, the file download starts and at the end it will automatically open with *Argo* app.



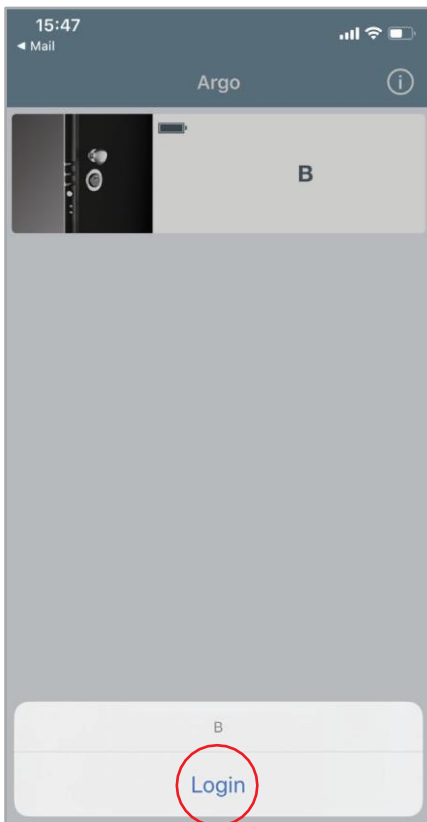
Write the backup file password previously chosen and tap **OK**.

Service

Step 2: Restore user list



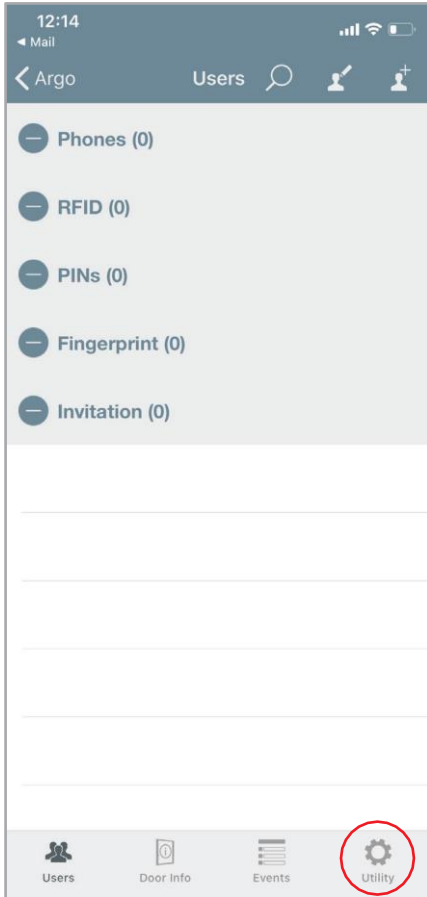
— The backup users are now in the *Argo app* memory exactly like the *Copy user* function (see *Copy users* paragraph).



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

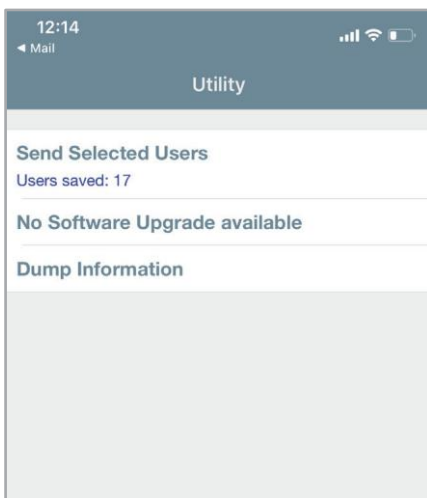
Service

Step 2: Restore user list



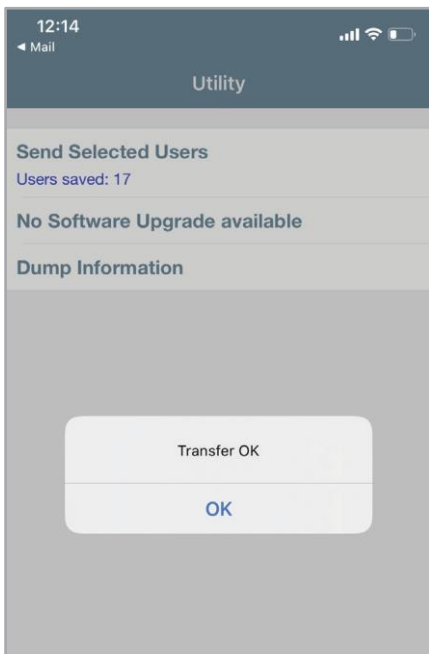
x1R Smart B empty user list.

Tap **Utility**

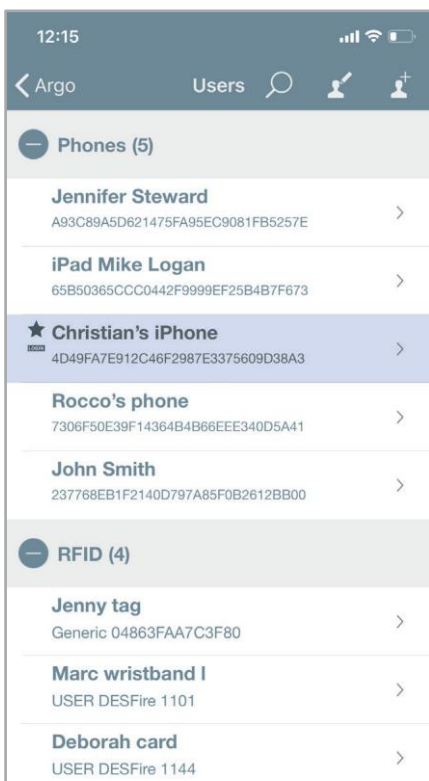


Tap **Send Selected Users** (see also *Transfer users* paragraph).

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 over written. 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 over write 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	<ol style="list-style-type: none">1. Present the <i>Master Card</i> to the device.2. Read the cards to be added.3. Present the <i>Master Card</i> to the device.
Delete Users	<ol style="list-style-type: none">1. Present the <i>Master Card</i> to the device.2. Present a second time the <i>Master Card</i> to the device.3. Read the cards to be deleted.4. Present the <i>Master Card</i> to the device.
Delete entire Users List	<ol style="list-style-type: none">1. Present the <i>Master Card</i> to the device for 5 sec.2. Repeat the operation for 3 times consecutively.
Enable and Disable Passage Mode	<ol style="list-style-type: none">1. Read a card with t Mode function enabled for 3 sec.
Block and Unlock Standard User	<ol style="list-style-type: none">1. Read a card with Block Standard User function enabled.2. Repeat the operation for 3 times consecutively.
Updating of the Master Card	<ol style="list-style-type: none">1. Present the next <i>Master Card</i> of the same set to the device.
Master Card Set replacement	<ol style="list-style-type: none">1. Present the <i>Master Card</i> 3 of the current set to the device.2. Present the <i>Master Card</i> 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.

Technical data summary table

Feature description	Value	Device
Max nr. of users	300	All
Max. nr. of recorded events	1000	All
Compatible phones	<i>iOS</i> : from iPhone 4s with iOS 7 and above. <i>Android</i> : from version 4.3 (Jelly Bean), featuring Bluetooth® Smart Ready hardware.	All
Compatible credentials	<ol style="list-style-type: none"> 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 <i>Credentials</i> 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

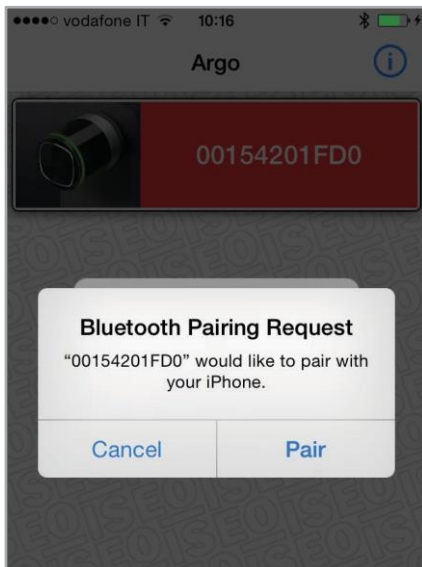


* *Mifare* is a brand of contactless card with several card types: Classic, Ultralight, DESFire...
All *Mifare* cards works in *Argo* by reading the UID (unique identified number).

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>

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 authentication in communications.

Penalty algorithm against brute force attack & Events protection

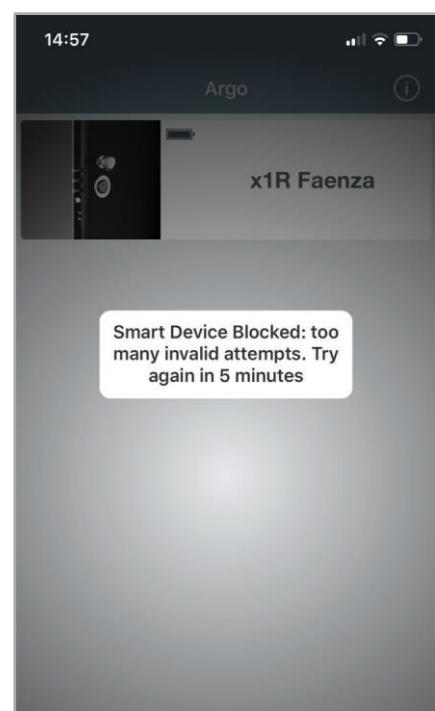
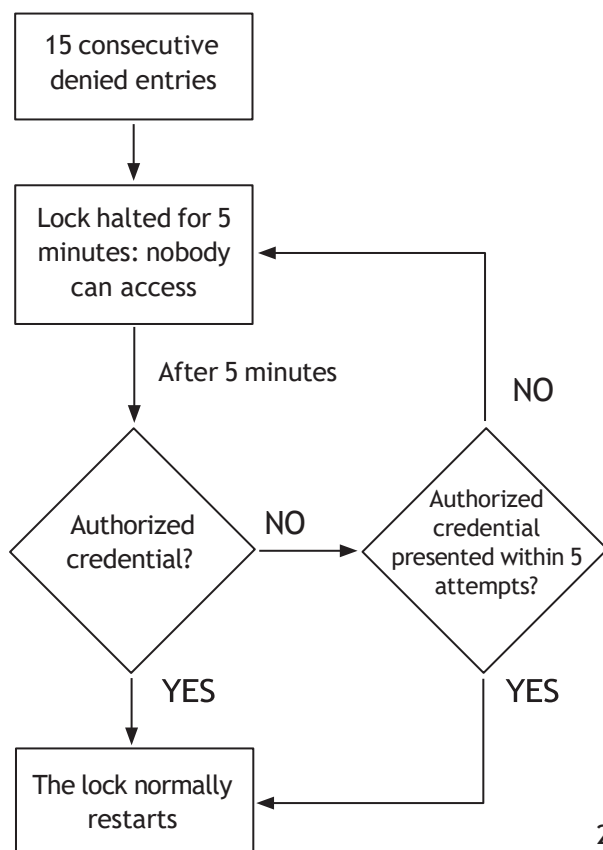
A *brute force attack* consists in systematically checking all possible codes performing an exhaustive code search. It might be possible to try all combinations in a relative short period of time (example 4 digit PIN).

The results of a *brute force attack* in a short period of time are:

- weakness of security;
- events erasure.

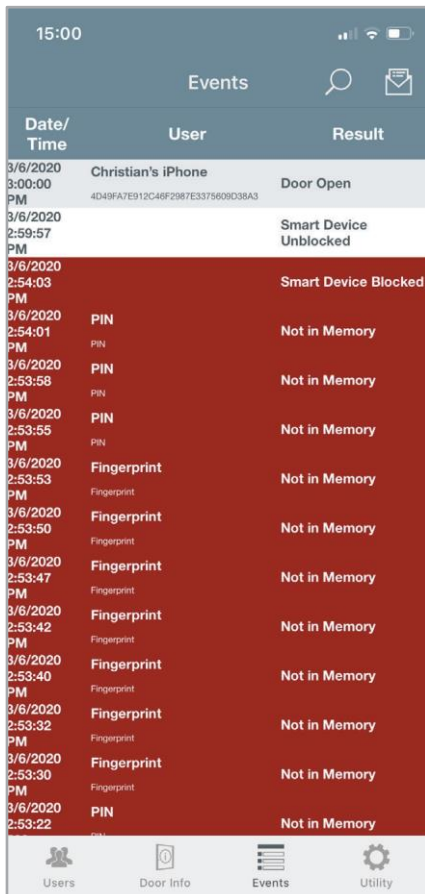
Argo takes advantage of a *penalty algorithm* against *brute force attacks* with the following characteristics and rules:

- 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 Administrator*, neither with *Master card* nor by phone login.
- After the 5 minutes of halting if a correct pin code is typed or an authorized credential is presented, the lock normally restarts but, if a not correct pin code is typed or an unauthorized credential is 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.



Appendix

The lock registers 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*.



Date/Time	User	Result
3/6/2020 3:00:00 PM	Christian's iPhone 4D48FA7E912C46F2987E3375609D38A3	Door Open
3/6/2020 2:59:57 PM		Smart Device Unblocked
3/6/2020 2:54:03 PM		Smart Device Blocked
3/6/2020 2:54:01 PM	PIN	Not in Memory
3/6/2020 2:53:58 PM	PIN	Not in Memory
3/6/2020 2:53:55 PM	PIN	Not in Memory
3/6/2020 2:53:53 PM	Fingerprint	Not in Memory
3/6/2020 2:53:50 PM	Fingerprint	Not in Memory
3/6/2020 2:53:47 PM	Fingerprint	Not in Memory
3/6/2020 2:53:42 PM	Fingerprint	Not in Memory
3/6/2020 2:53:40 PM	Fingerprint	Not in Memory
3/6/2020 2:53:32 PM	Fingerprint	Not in Memory
3/6/2020 2:53:30 PM	Fingerprint	Not in Memory
3/6/2020 2:53:22 PM	PIN	Not in Memory

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 Administrator*. 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 Administrator* 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 " <i>Argo 2.0 upgrade procedure</i> ", available at " <i>app.iseo.com</i> " 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.	<ol style="list-style-type: none"> 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.

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.	<ol style="list-style-type: none"> 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:

- *Argo 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



ARGO 3.5
04/2025.

Non-contractual document. Subject to change. Images for illustrative purposes only.

ISEO Serrature s.p.a.
Via San Girolamo, 13
25055 Pisogne BS, Italy
Tel. +39 0364 8821
iseo@iseo.com

iseo.com