ISEO

ARGO

USER MANUAL

Argo 2.3

About this manual

Dear Customer,

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

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

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

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

Notices

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

Information icons

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

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

NOTE: notes, suggestions and additional information.

How to use this manual

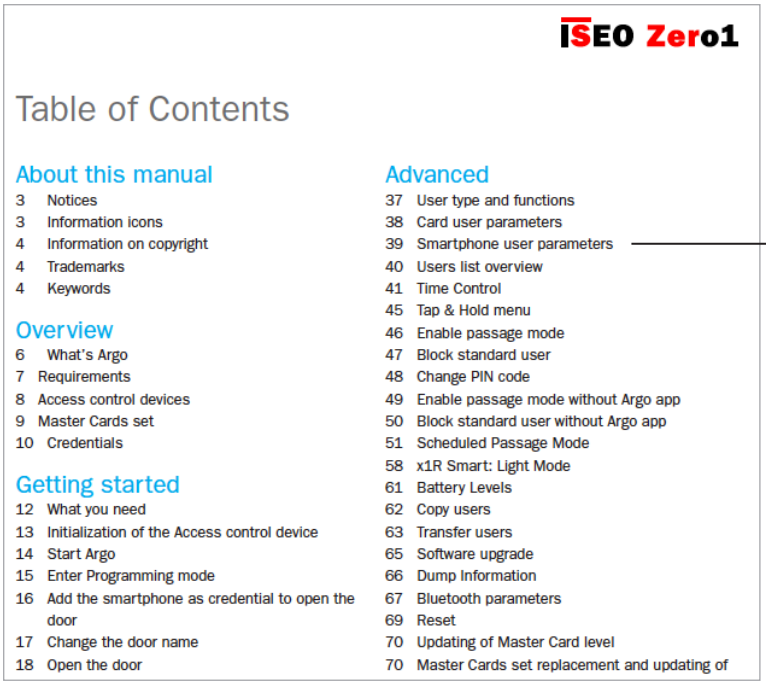


Table of Contents

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

Getting Started

Start Argo

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

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

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

About this manual

Information on copyright

Trademarks

Keywords

- **Access Control Device**: electronic and mechanical device that allows selective access through a door.
- **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.
- **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.
- **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.

Keywords

- **Open Restrictions**: it's related to the *Argo* parameters that can be enabled to limit the temporal validity of a credential. It includes: *Validity from First Use, Time Control, Time Schedules*.
- **Passage Mode**: it's a function that allows the door to be always open for any user who wishes to gain access, without the use of authorized credentials.
- **Programming Mode**: software condition, feasible by *Master Card*, that allows software modification to the *Device*.
- **Scheduled Passage Mode**: this function allows you to set 2 schedules, to automatically enable and disable the Passage Mode function.
- **Smart Series**: *Access control device* which embeds Bluetooth radio module, to communicate to compatible smartphones by the *Argo app*.
- **System Code**: unique number associated to a *Master Card set*.
- **Time Control**: this function is used to set the validity of the assigned credential (date and time of activation and expiration).
- **Time Schedules**: in additon to the *Time Control*, you can set for each user, two time schedules that can be selected for each day of the week.
- **User**: it's the person enabled to open an *Access control device* by a credential.
- **User Card**: *Contactless card* used to open one or more doors.
- **Users List**: list of *Users* enabled to open an *Access control device.*
- **Validity from First Use**: with this function is possible to set the validity from the moment of the first use of the credential (in days, hours or minutes).

Table of Contents

Overview

What's Argo

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

300 USERS

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

1000 EVENTS

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

Requirements

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

iOS

- From iPhone 4s with iOS 7 and above.

Android™

- From version 4.3 (Jelly Bean), featuring *Bluetooth Smart Ready* hardware.

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

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

Access control devices

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

Libra Smart

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

Aries Smart

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

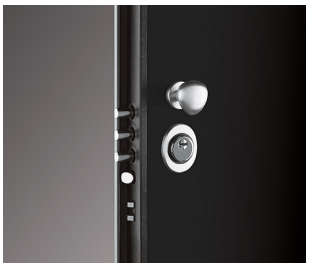
Stylos Smart LED

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

Stylos Smart Display with Keyboard

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

Access control devices



x1R Smart

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

Smart Locker

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

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

Master Cards set

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

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

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

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

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

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

Overview

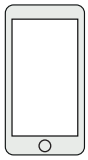
Credentials

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

ISEO cards

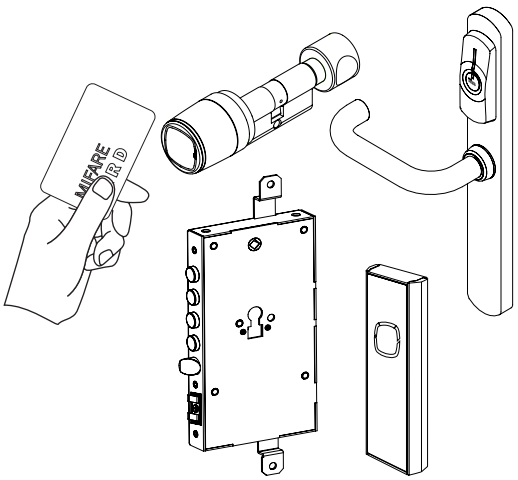
Tags

Mifare cards
MIfare Desfire (UID reading)



NFC phones
(NFC static UID required)

Used to “activate” the device.



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

Notes on NFC Phones

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

Notes on Mifare Cards UID

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

Note about ISEO Cards

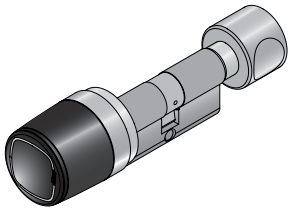
ISEO Cards is a particular Mifare Card (1K), specifically developed by Iseo, with an encrypted UID. This allow an higher level of security in the trasmission between the card and the doorlock.

As result of the above notes

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

Getting Started

What you need



Access control devices, Smart series.

Argo app installed on your smartphone.

Master Card set.

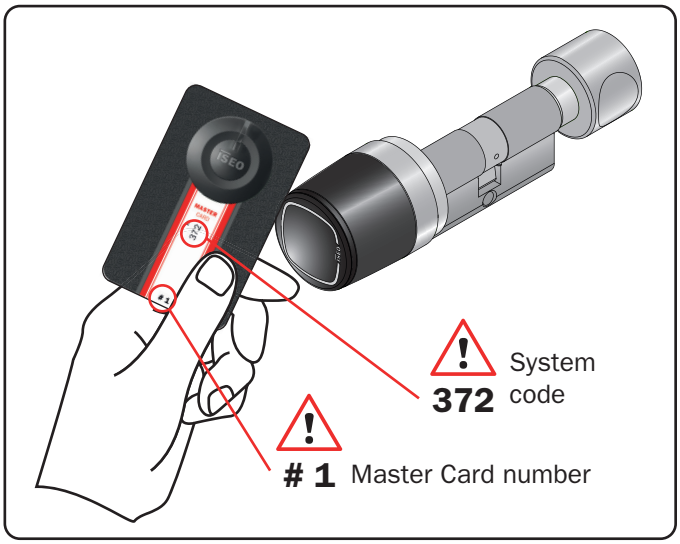
Set of User cards.

Initialization of the Access control device

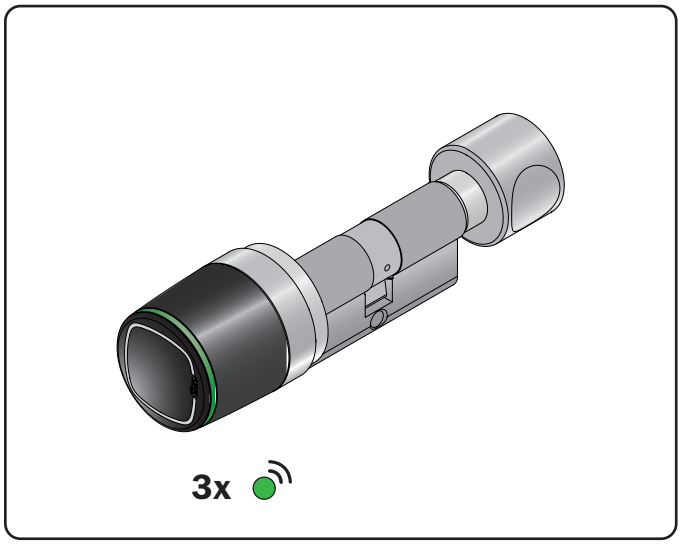
The new device is in *Factory mode* configuration, meaning with the list of authorized user empty and no system code yet assigned.

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

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



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



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

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

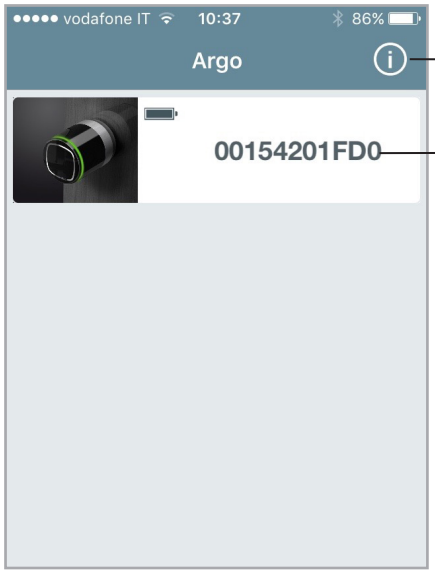
All *Access control devices* must be initialized or updated with the same *Master Card*.

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

Start Argo

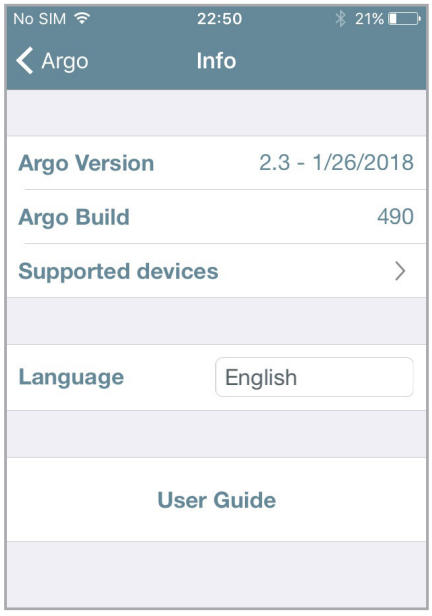
When you start the *Argo app* you will see in the smartphone display, all the *Access control devices* available, identified by its serial number.

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



Info app menu

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



Info app menu

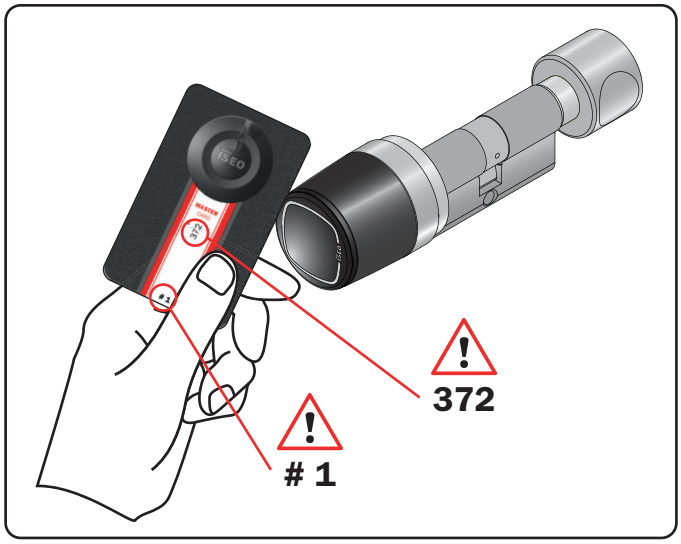
Information on the app version and the software of the ISEO devices, that are supported from the app.

To change the app's language. 17 languages are currently available.

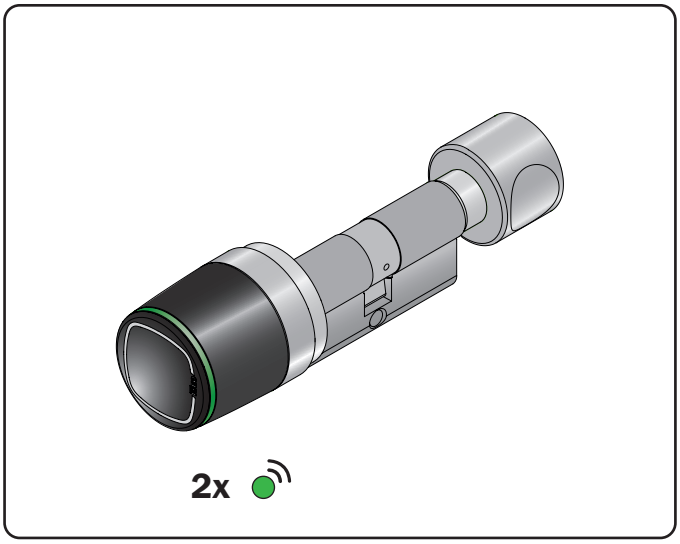
Link to *http://app.iseo.com/*
In this website you can find this manual and much more information about the Argo app.

Enter programming mode

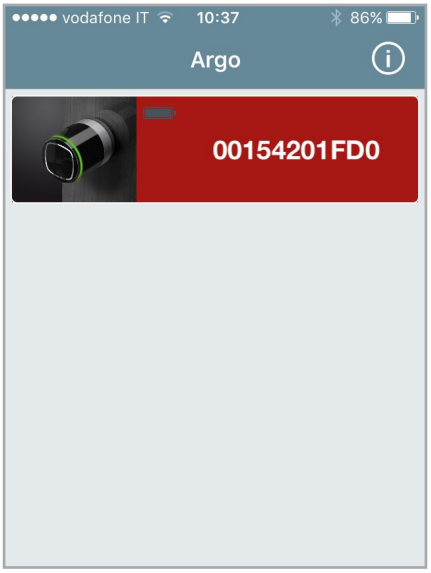
Present the *Master Card 1* to the device: the button in the app will turn red, and pressing it you will enter in *Programming mode*.



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



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

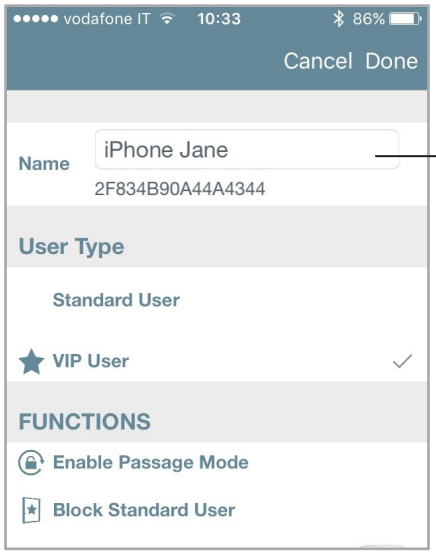


3. The button in the app will turn red. Press it to enter in *Programming mode*.

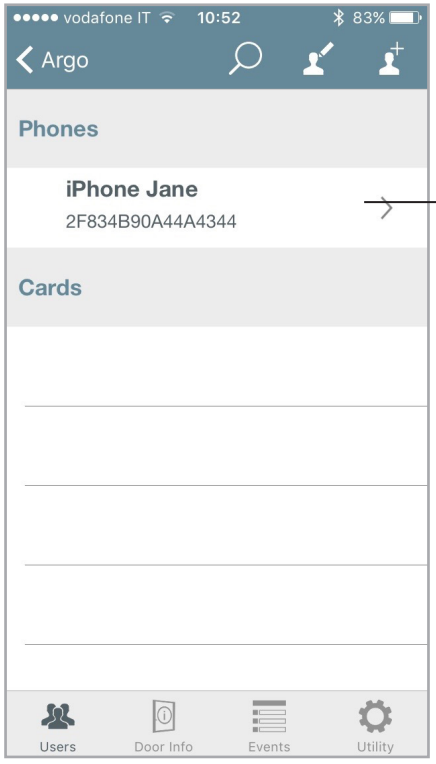
To know more about the *Bluetooth* technology and the *Argo* feature, called “in-app pairing”, see the related page in the *Advanced* chapter.

Add the smartphone as credential to open the door

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

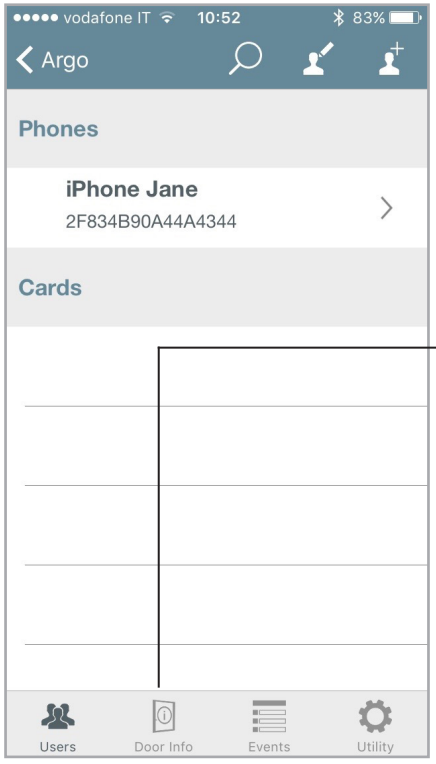


1. Change the name of your phone.
2. Tap **Done** to memorize your phone as opening Credential.
3. Tap **Cancel** if you decide to not memorize your phone now.

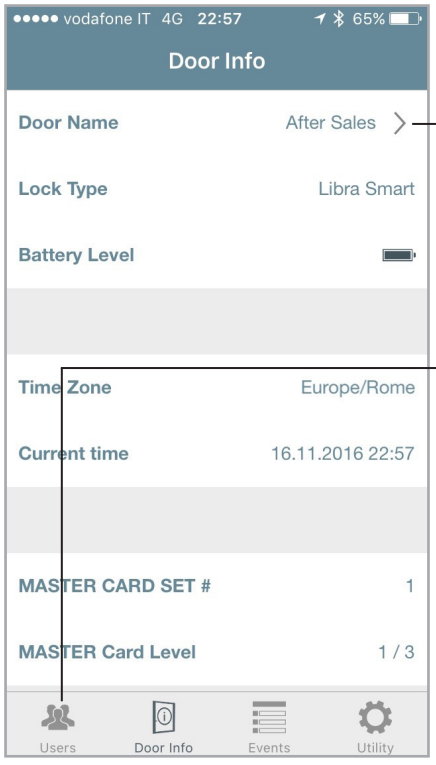


4. You can see your phone appearing in the *Users list*.

Change the door name



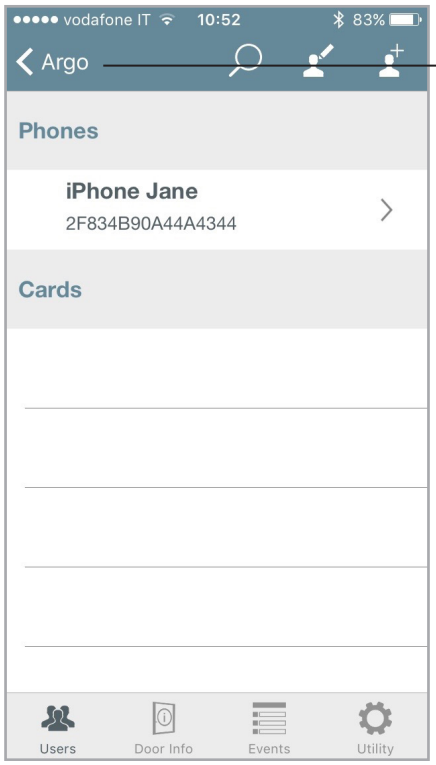
1. Tap **Door Info** and then **Door Name** to give a real door name to the lock.



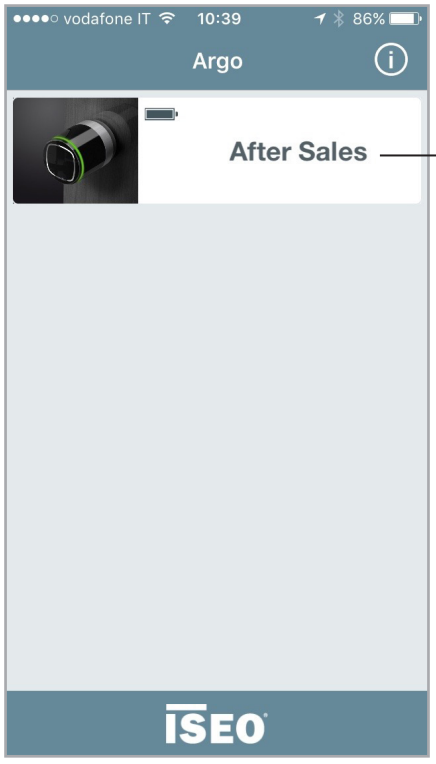
2. Change the name and confirm.

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

Open the door



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

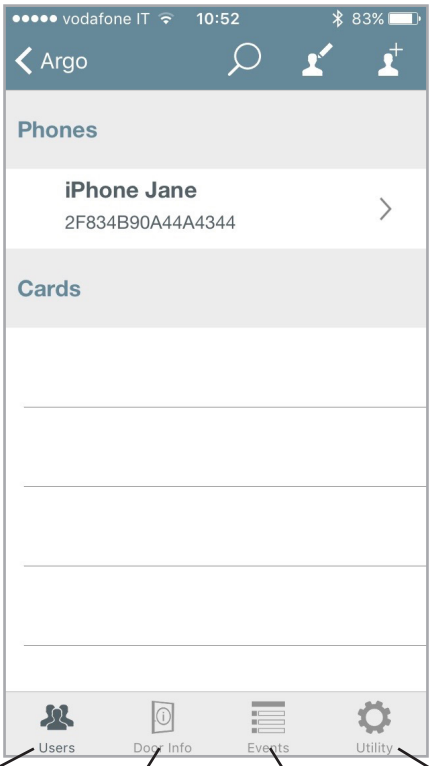


2. Tap the icon button to open the door.

Basics

Users menu

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



Users

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

Door Info

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

Events

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

Utility

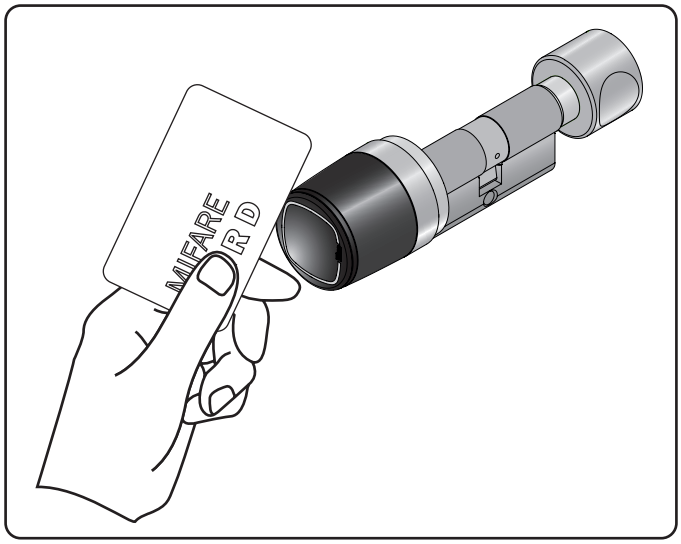
- Transfer the users list
- Software upgrade
- Dump information

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

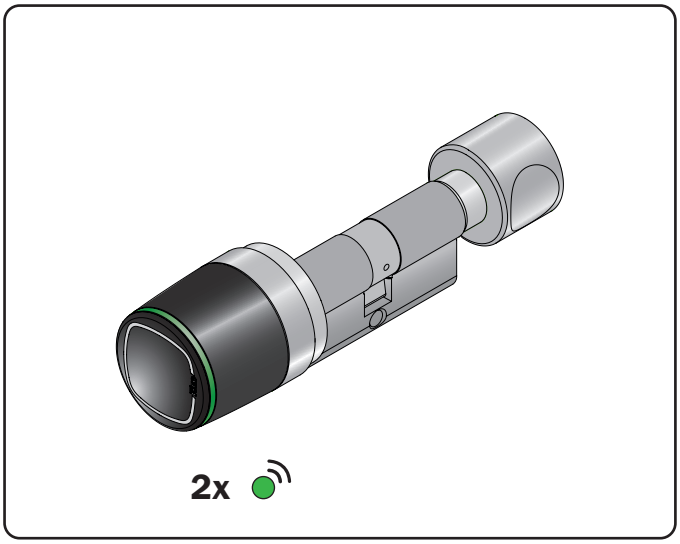
Basics

Add users

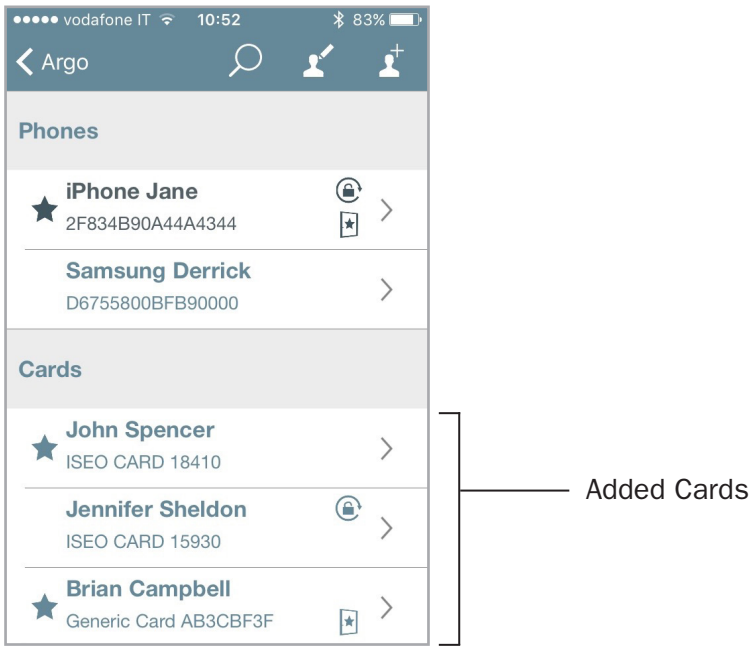
Enter *Programming mode* first. You can then add users just presenting the credentials to the device, and those will be displayed in the smartphone.
Last card will be on the top of the list. You can read ISEO and Mifare cards, tags and enabled NFC phones (NFC static UID required).



1. Present the card to add to the device.



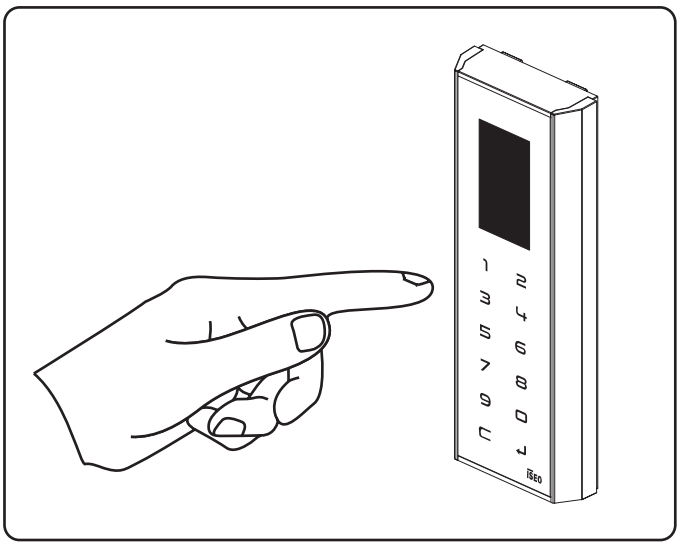
2. The device emits 2 acoustic signals together with 2 green light signals.



Add PIN users

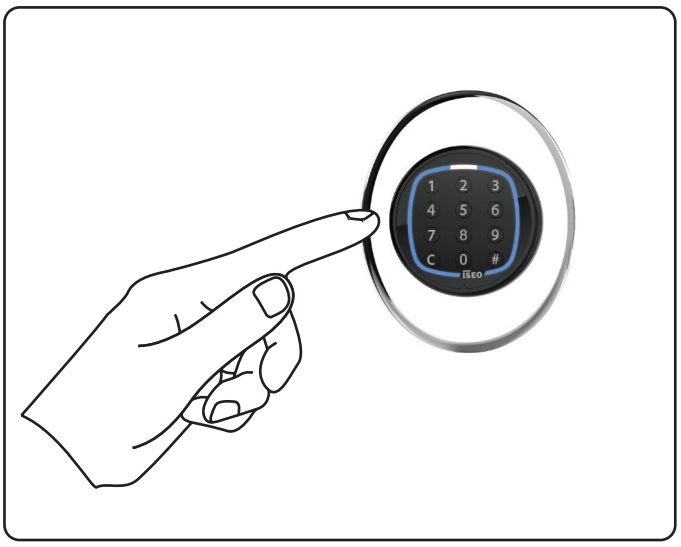
On *Stylos Smart Display* and *x1R Smart*, you can also add a *PIN code* as credential to open, using the keyboard available on both devices. Enter *Programming mode* first. You can then add the PIN just entering the code in the keyboard. Last PIN will be on top of the list.

STYLOS SMART DISPLAY

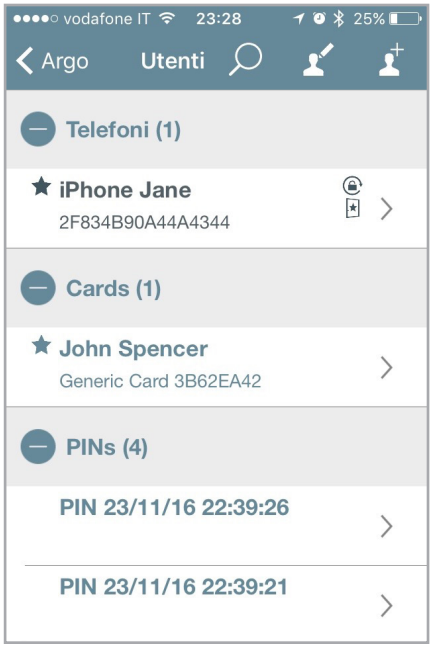


Enter your PIN code, from 4 to 14 characters, and confirm by enter ↵.

x1R SMART



Enter your PIN code, from 4 to 14 characters, and confirm by enter **#**.

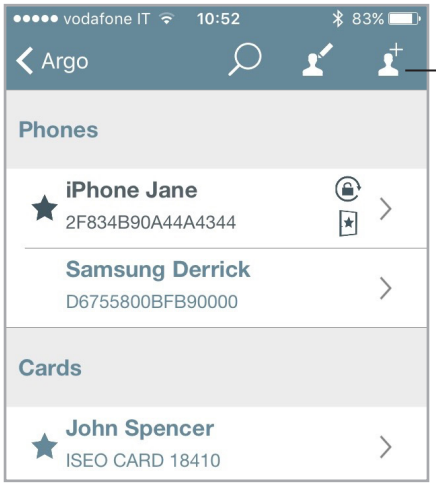


Added PINs are visible in the Argo app with name *PIN* plus *date & time* of when they were added.

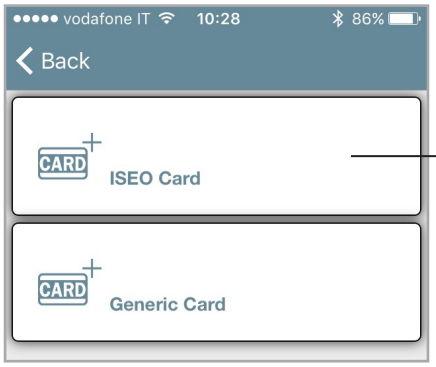
For security reasons PIN codes are never visible in the Argo app: neither in the *Users list*, nor in the historical *Events*, nor in the *Dump Information* (see *Dump Information* specific paragraph).

Add users typing ISEO card number

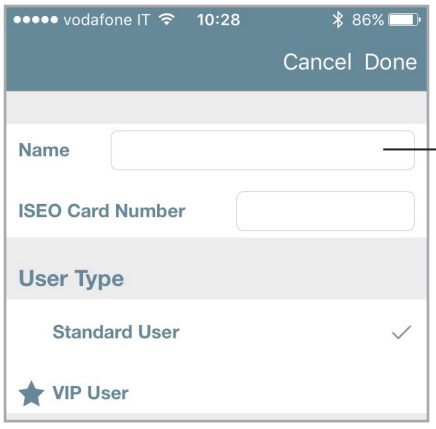
Enter *Programming mode*. You can add users without having the card or the tag, just typing the ISEO card number. This can be useful if you have already distributed the cards to the users.



1. Tap the *add user* icon 

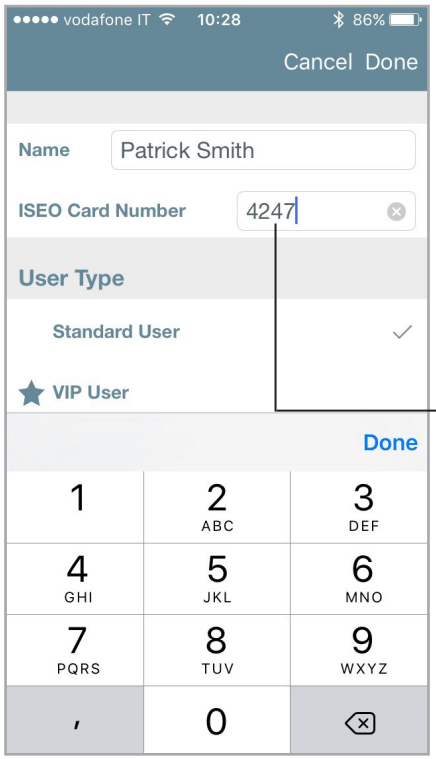


2. Tap **ISEO Card**



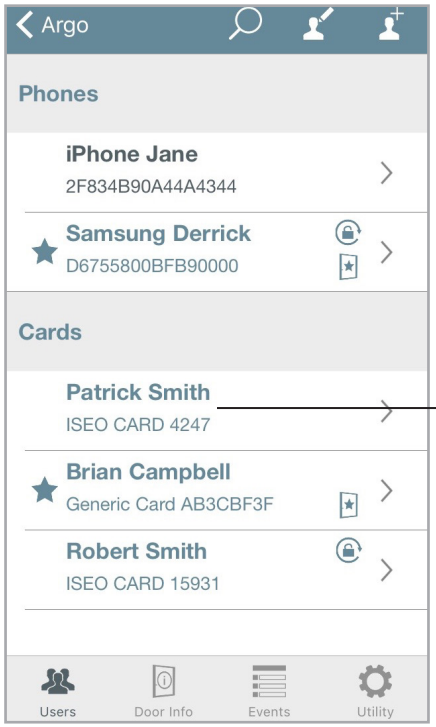
2. Tap **Name** box

Add users typing ISEO card number



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

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

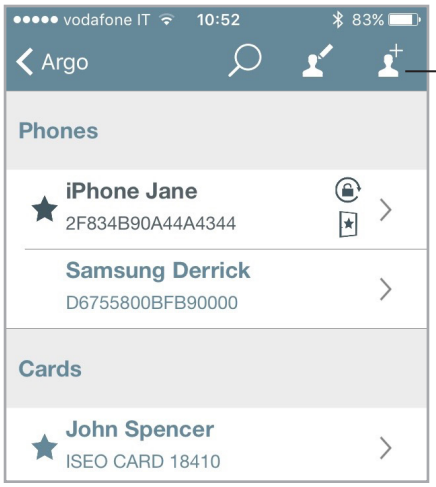


5. The ISEO card is added to the *Users list*.

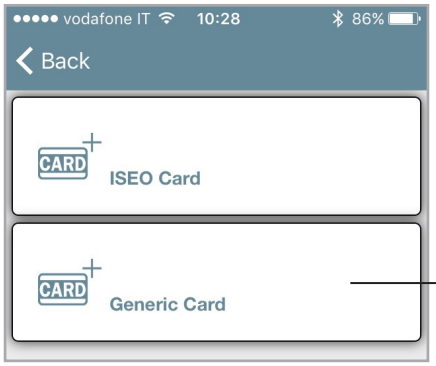
This function is only available using ISEO cards and tags.

Add users typing Mifare card UID

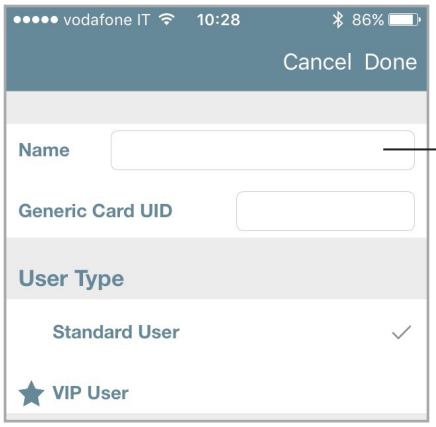
It is possible to add a *Mifare card* to the device *Users List*, writing the *UID*, the *unique identifier number*. This function is useful, for example, if you know the credential UID of the user that need to access the door, but you don't physically have his card, to present to the lock.



1. Tap the *add user* icon 

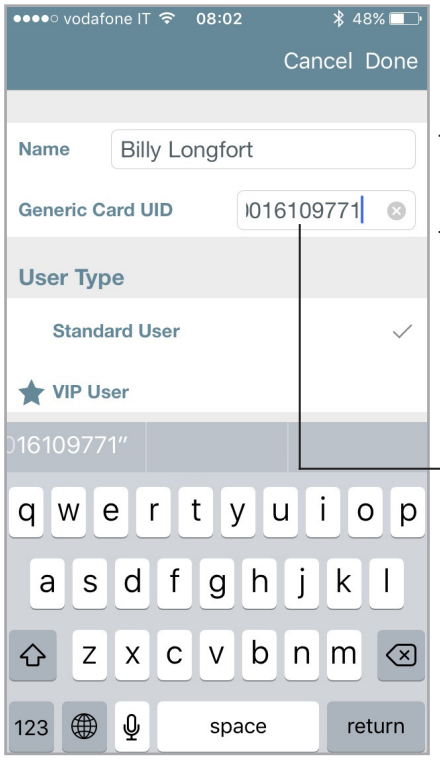


2. Tap **Generic Card**

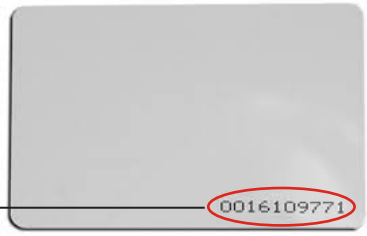


2. Tap **Name** box

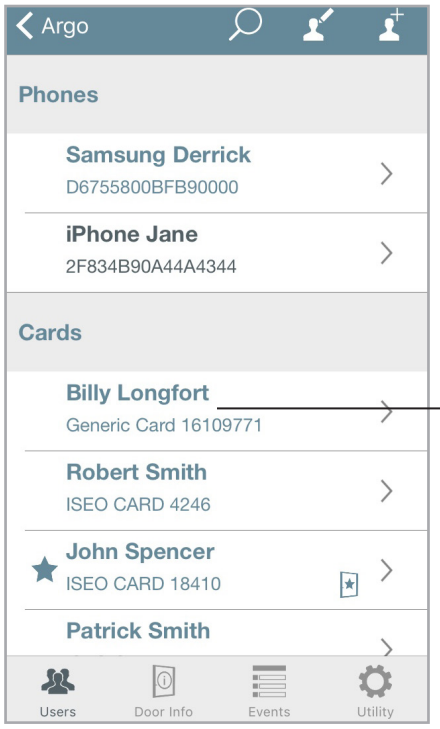
Add users typing Mifare card UID



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



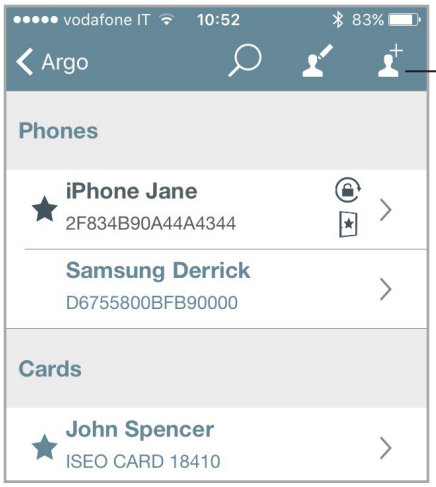
4. Tap **Done** to confirm the operation.



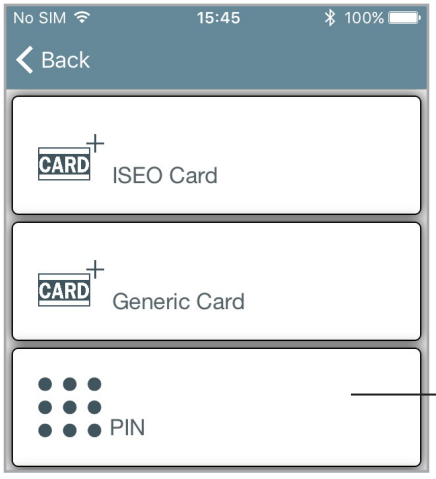
5. The *Mifare card* is added to the *Users list*.

Add users typing PIN code

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

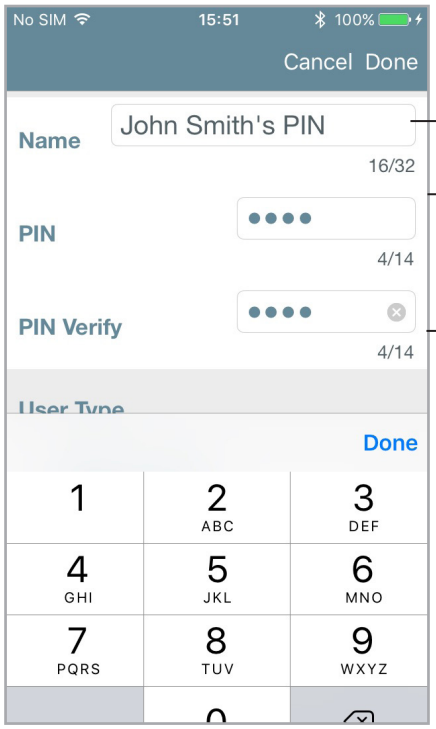


1. Tap the *add user* icon 



2. Tap **PIN**

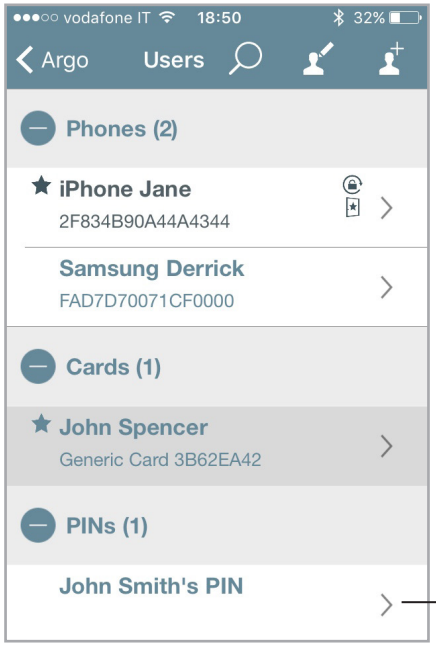
Add users typing PIN code



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

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

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

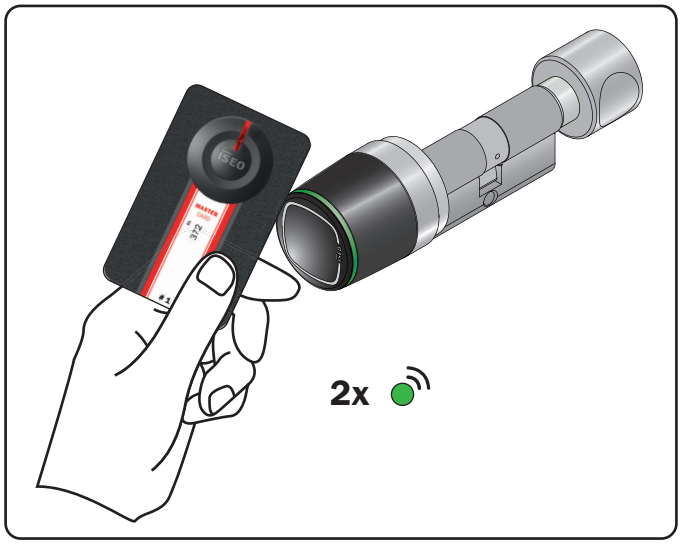


The *PIN code* appears in the *User list*, in the PIN list, with the assigned name.

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

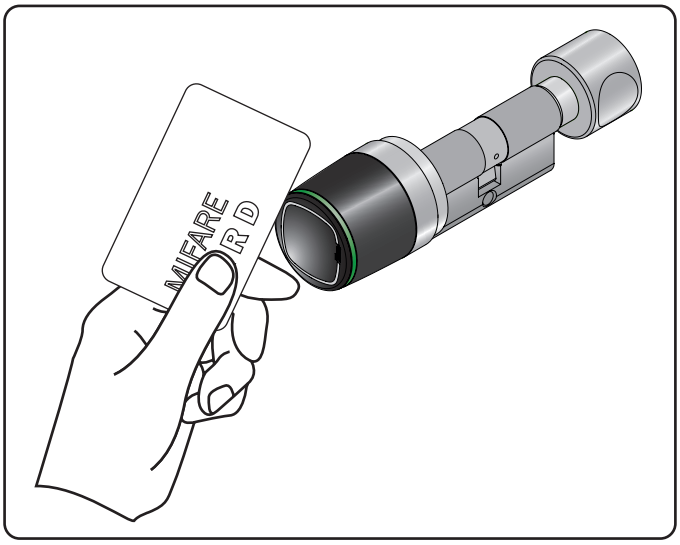
This function is only available on *x1R Smart* and *Stylos Smart Display.*

Add users without Argo app



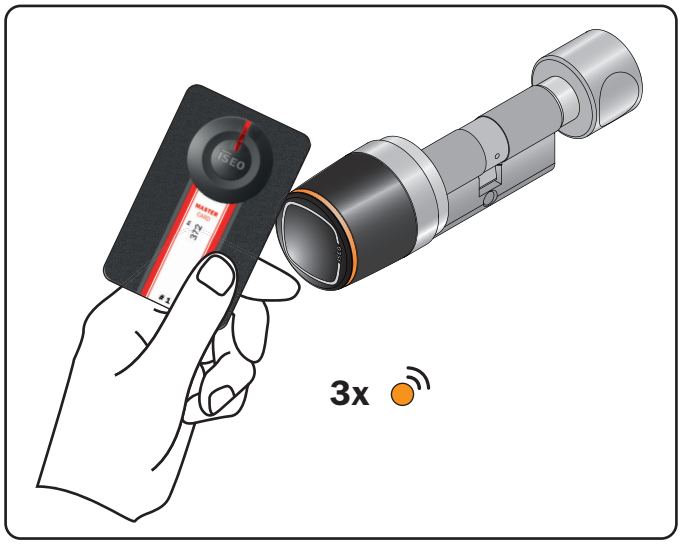
1. Present the *Master Card 1* to the device to enter in *Programming mode*.

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



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

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

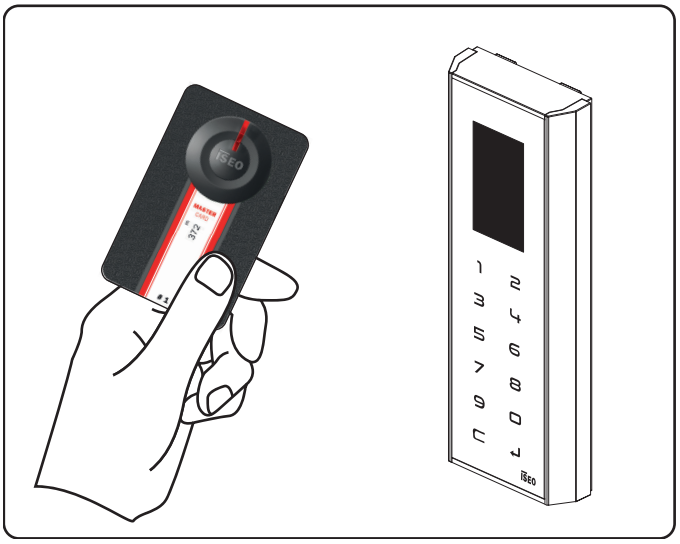


5. At the end of the operation present again the *Master Card 1* to the device to go out the *Programming mode*.

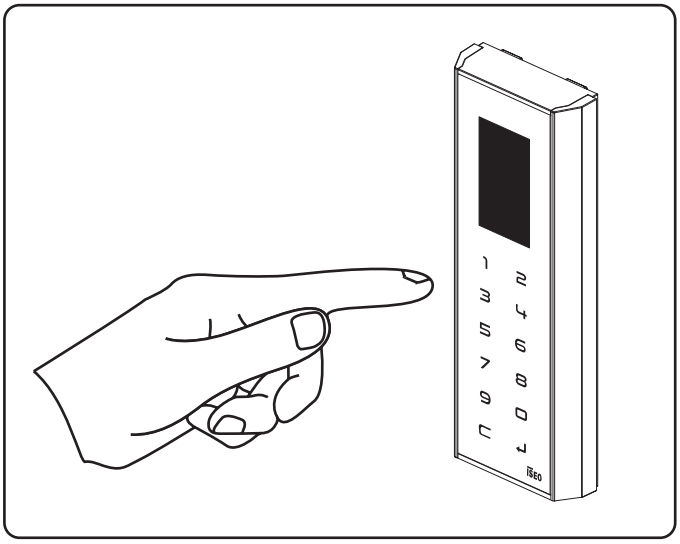
The device goes automatically out of *Programming mode* after 5min. of inactivity.

Add PIN code without Argo app

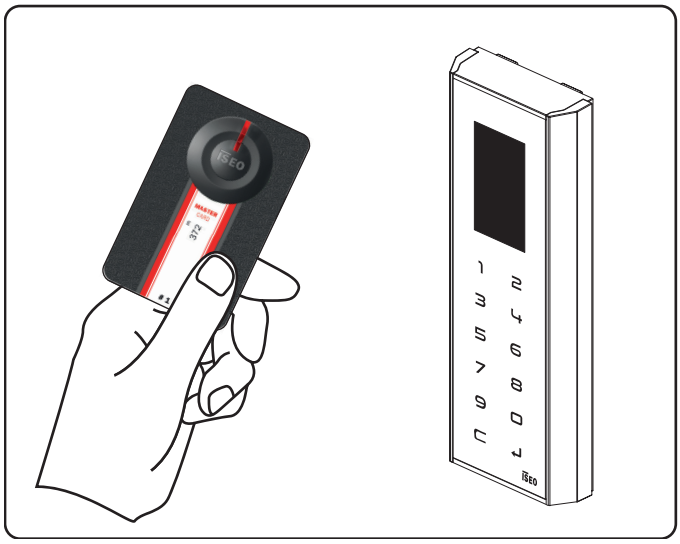
On *Stylos Smart Display* and *x1R Smart*, you can also add a PIN code as credential to open, using the keyboard available on both devices. Pictures below refer to *Stylos* but the procedure is the same for *x1R* as well.



1. Present the *Master Card 1* to the device to enter *Programming mode*.
2. The device emits 3 acoustic signals.



3. Enter your PIN code, from 4 to 14 characters, and confirm by enter.
4. For each memorized code the device emits 2 acoustic signals, to confirm the operation.



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

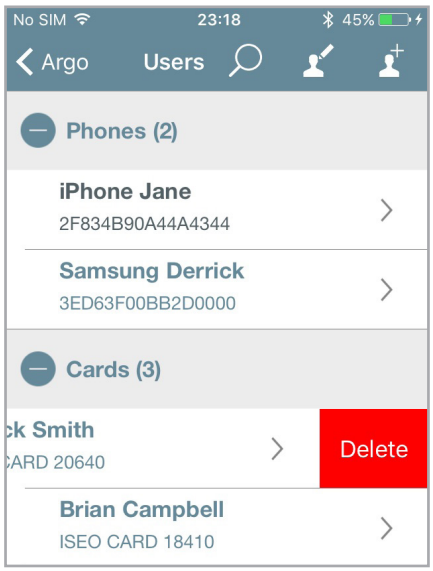
The PIN code must be from minimum 4 to maximum 14 characters.
This function is only available on S*tylos Smart Display and x1R Smart*.

Delete users

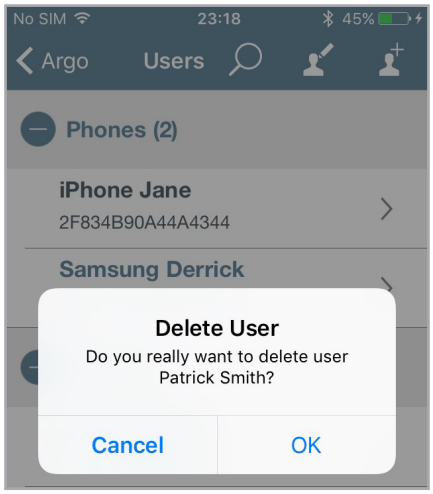
There are two ways to delete users from the user list:

- Single user delete functionality
- Multiple users delete functionality

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



1. Swipe on the user you want to delete.

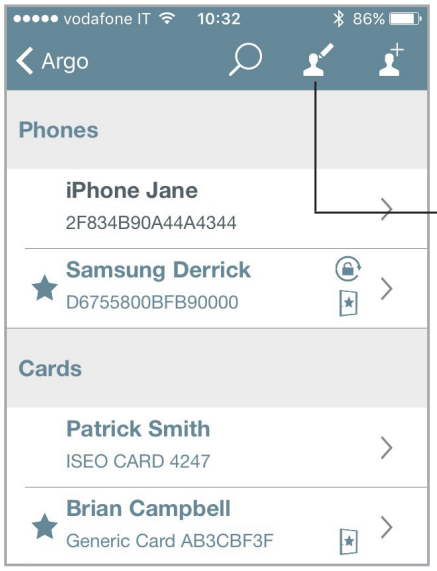


2. Confirm the operation.

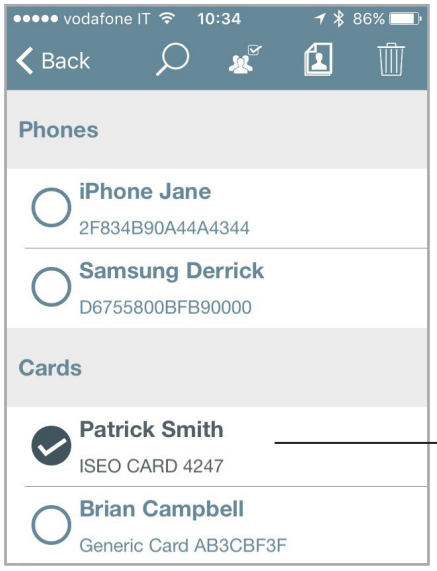
On Android phones, at the place of the swipe action, you need to tap and hold on the user.

Delete users

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



1. Tap *edit* icon.

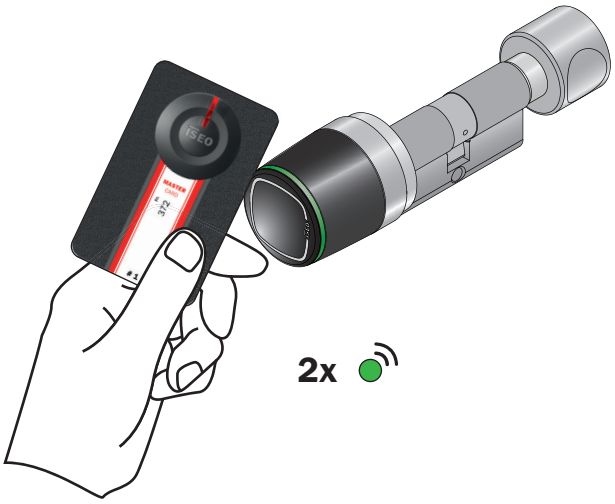


2. Select the users to remove.
   You can also select all users tapping on

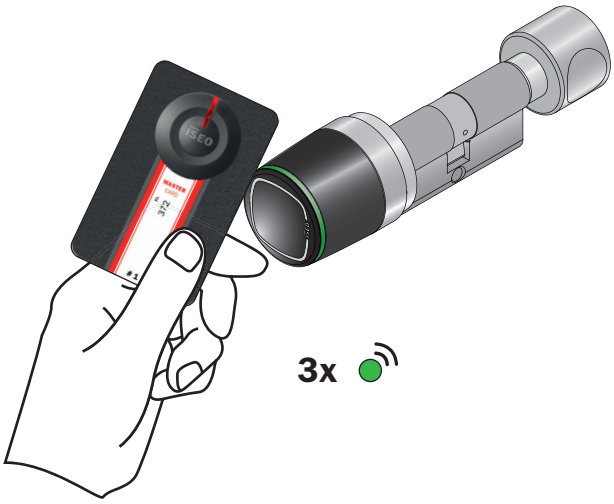
3. Tap the *trash bin* icon to confirm the operation.

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

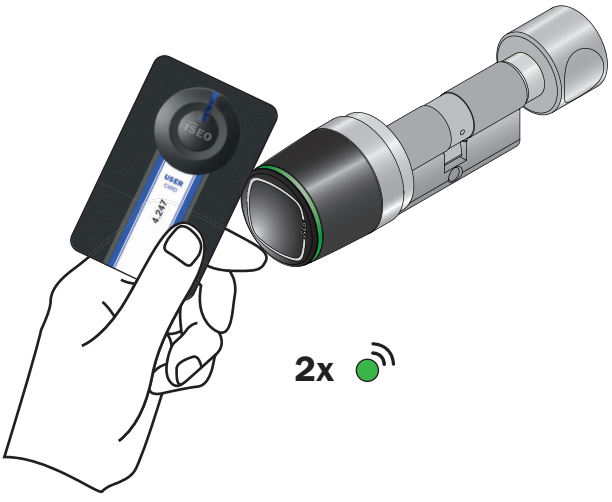
Delete users without Argo app



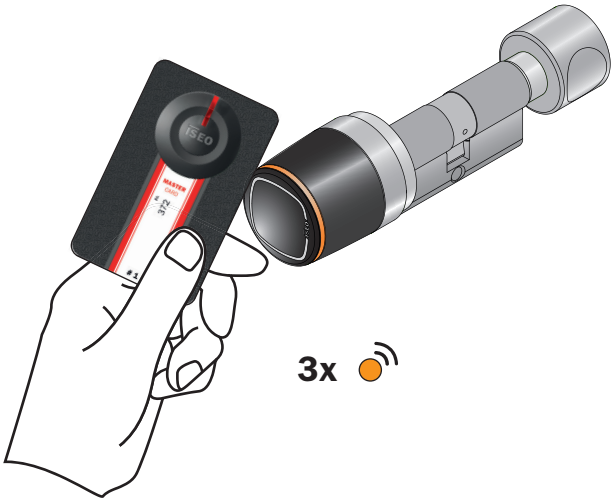
1. Present the *Master Card 1* to the device.
2. The device emits 3 acoustic signals together with 2 green light signals.



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



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



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

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

Basics

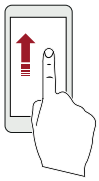
Read Events

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

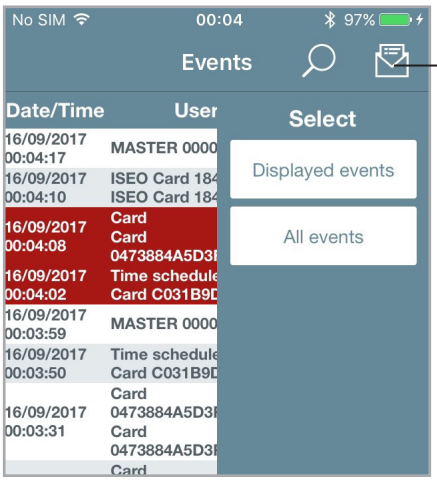
The last 1000 events are stored in the lock. The events are loaded from the most recent, and scrolling down allows you to automatically load new events.

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

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



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



Tapping the envelope you can send by email:

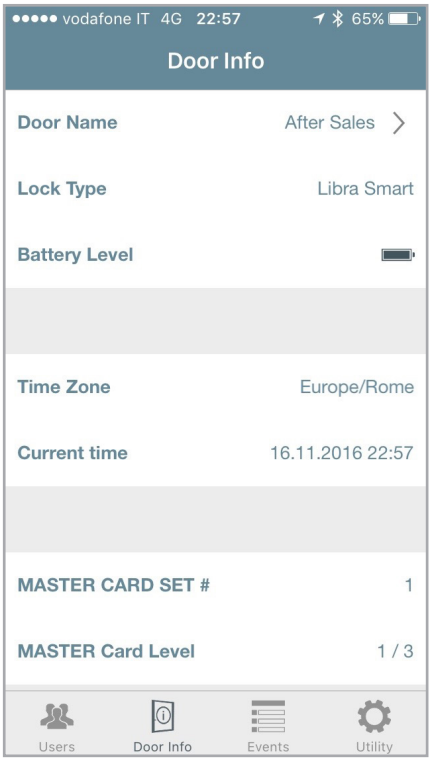
- **Displayed events**: the events loaded by "manual scrolling", or filtered in the search box.
- **All events***:* all the lock events (max 1000 events).

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

Basics

Door info

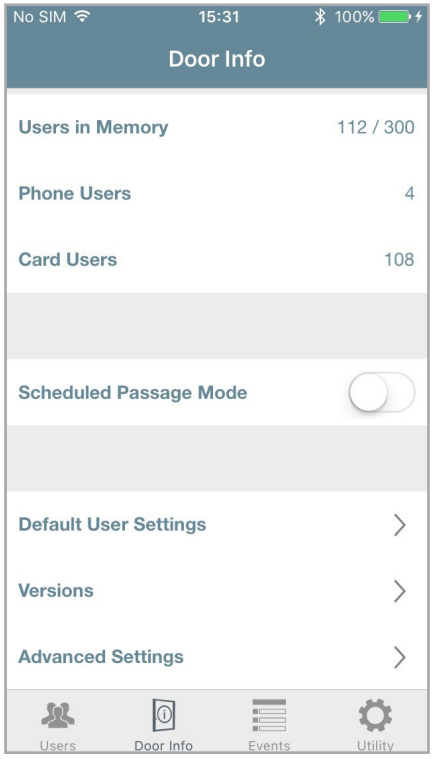
In this menu you can change the *door name* and you can find many information about the device configuration, as showed in the picture below.



Tap to change the *Door name.*

Check battery level.

Other available info.



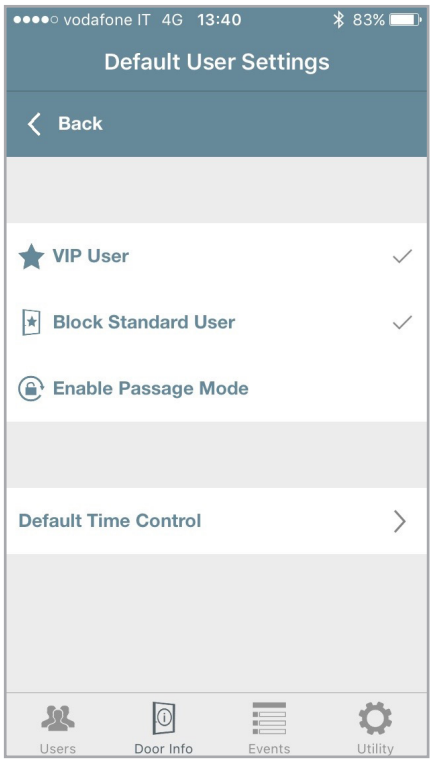
Other available info.

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

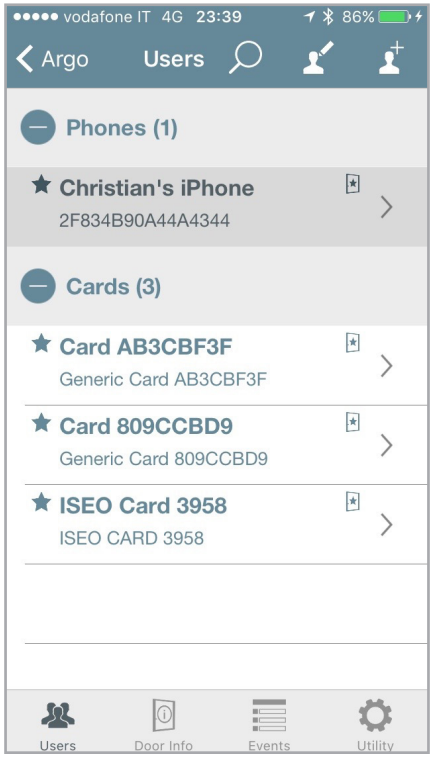
In this menu you can set *User Type* and *Functions* as default. That means the selected functions will be automatically added to each new memorized credential (user).



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.

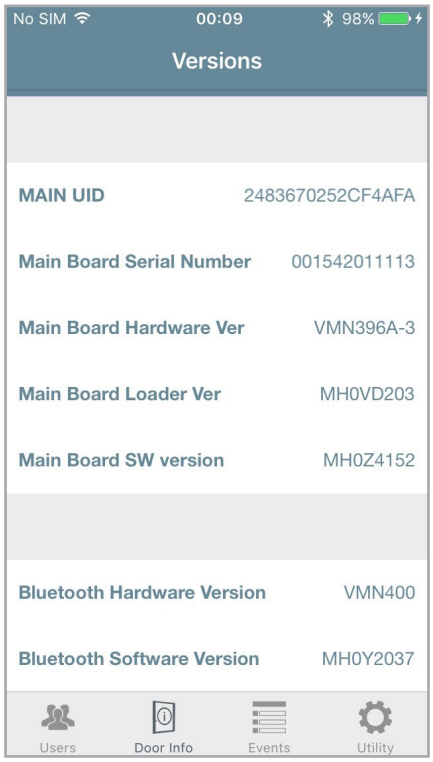


Following the above example, all new added users will be *VIP* users, with *Block Standard User* function automatically enabled, because previously set as default.

Basics

Versions

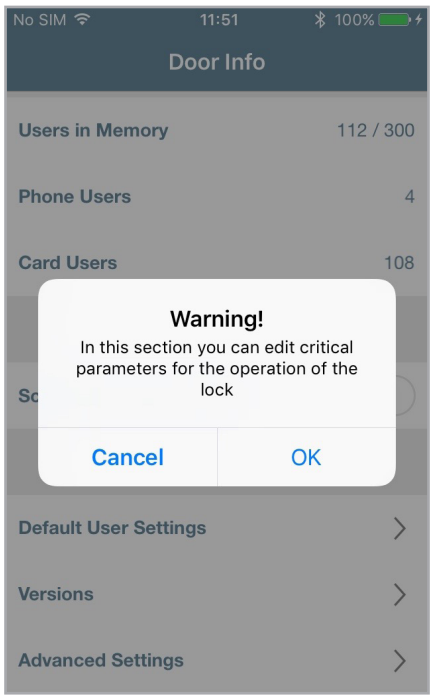
In this menu you can find the software versions of all the electronic boards included in the device.



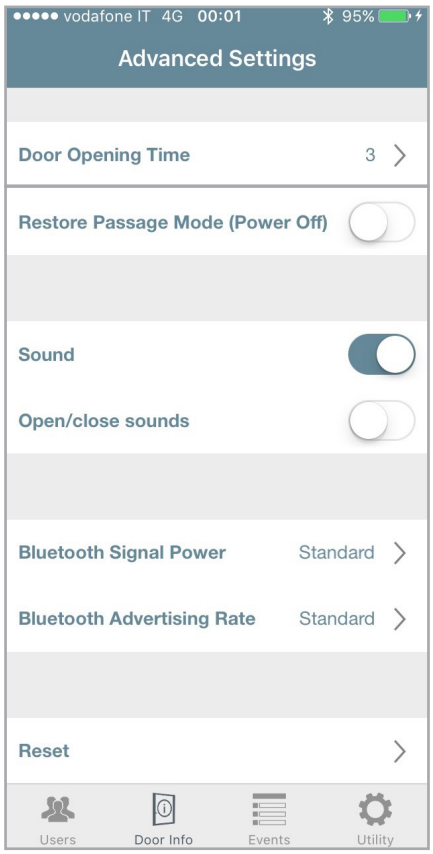
Look at the *Main Board Software version*. This is the version that you can update by the *software upgrade procedure,* described in the next pages.

Advanced settings

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



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



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

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

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

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

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

Advanced

User type and functions

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

USER TYPE

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

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

FUNCTIONS

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

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

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

USER PIN

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

OPEN RESTRICTIONS

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

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

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

LOGIN TO DOORLOCK

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

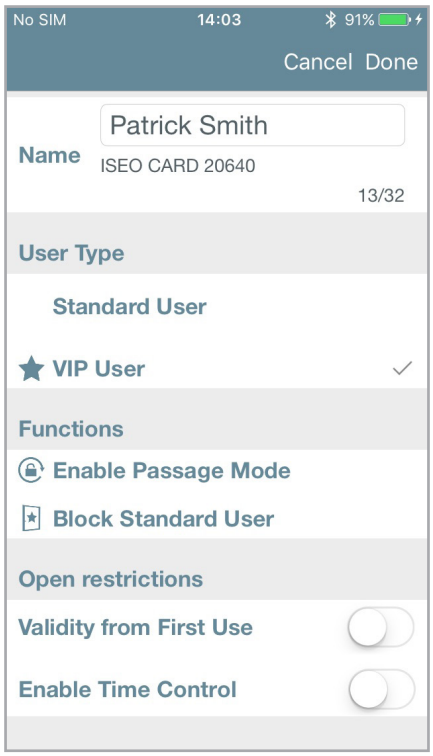
Request PIN to login: to increase security a *PIN code* has been set to login by phone.

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

Advanced

Card user parameters

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



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

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

User Type

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

Functions

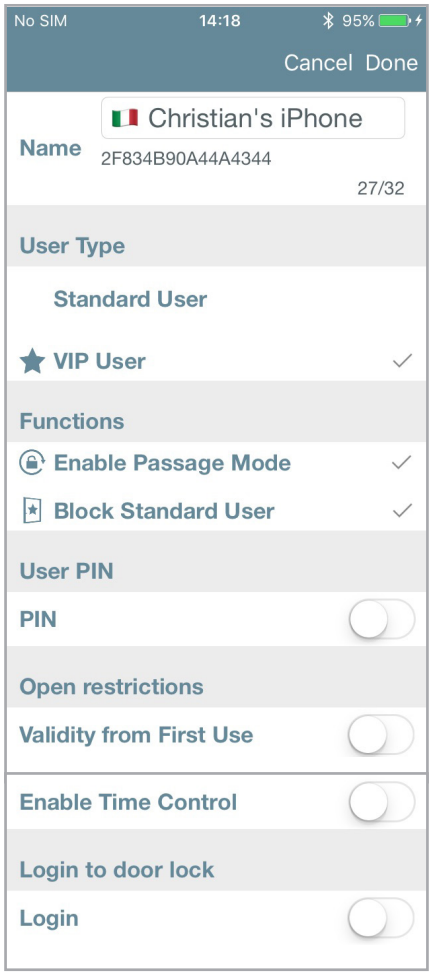
- *Enable Passage Mode* allows a user to put the lock in *Passage Mode* (office function).
- *Block Standard User* is enabled only if the user is *VIP*. With this function enabled a *VIP* user can temporarily block the access to all *Standard Users*.

Open resctrictions

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

Phone user parameters

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



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

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

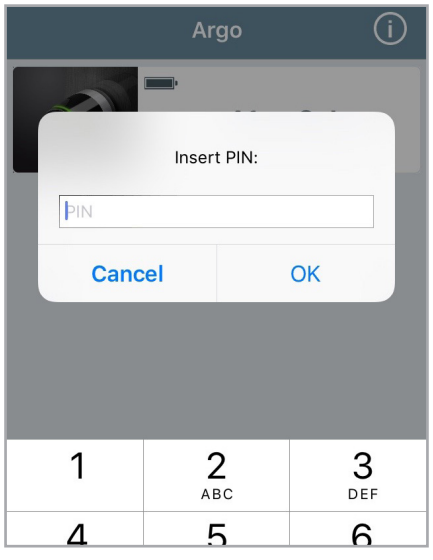
Same *User Type* and *Functions* of *Card user parameters* menu.

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

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

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

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



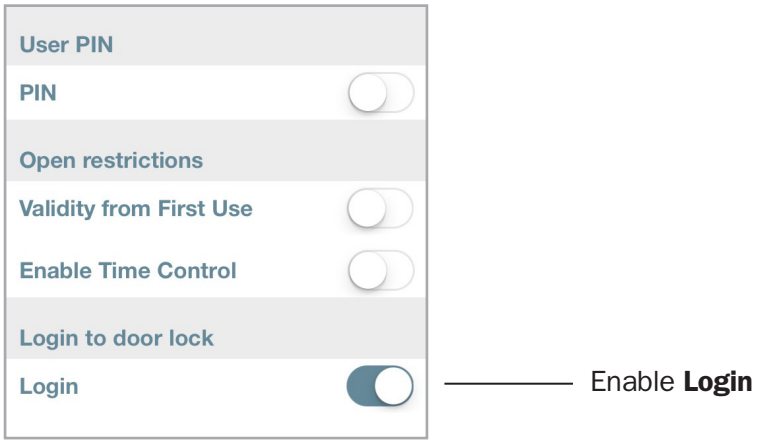
Enter the 4 digits *PIN code* and press **OK** to open the door.

Advanced

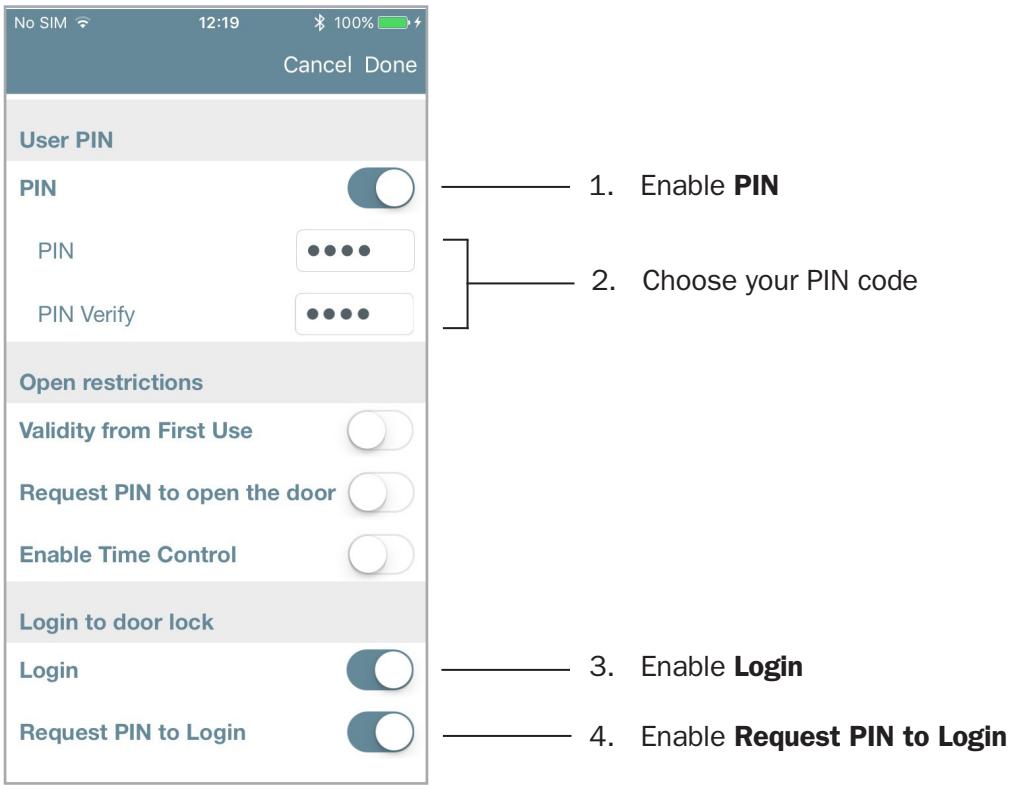
Administrator Login without Master Card LOGIN

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

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



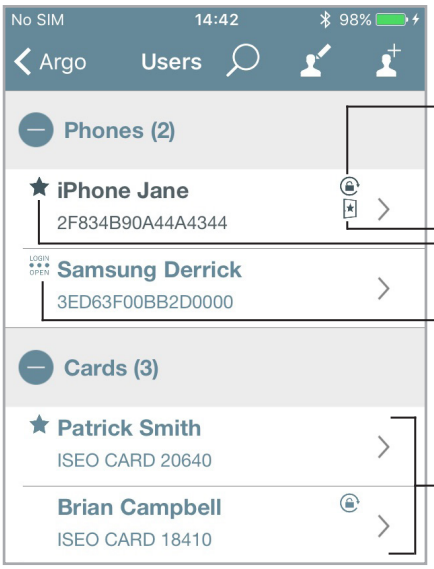
To add a PIN code to the *Administrator Login without Master Card*.



Advanced

User List overview

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



Enable passage mode active.

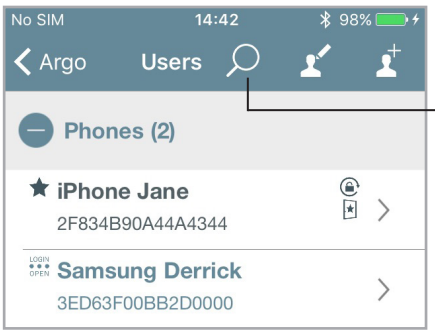
Block standard users active.

VIP user.

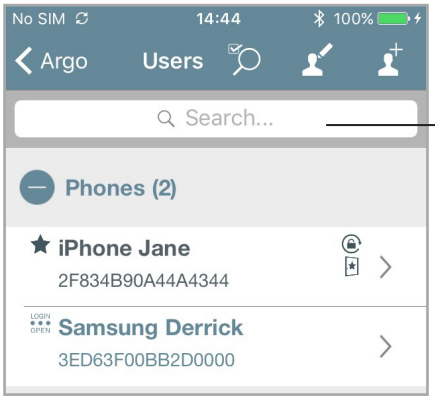
Enable PIN code request to open the door and to login without *Master Card* active

User name and credential *UID*

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



1. Click on the *Lens icon*.



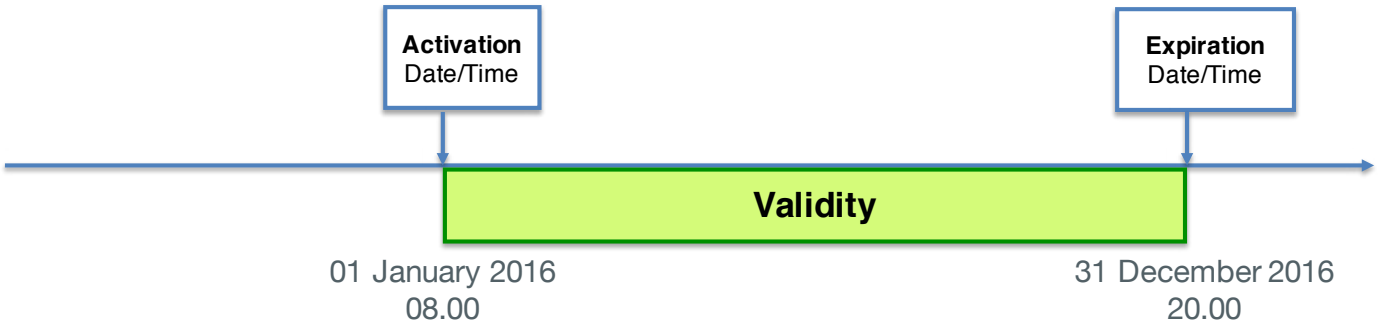
2. Write in the box the name to search and press **Find** in the phone keyboard tool.

Advanced

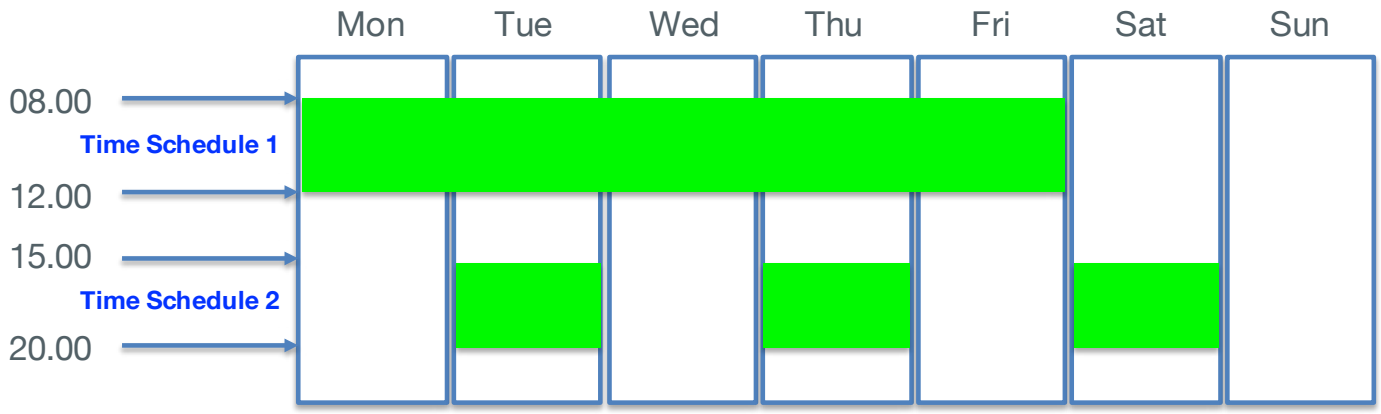
Time Control

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

Validity



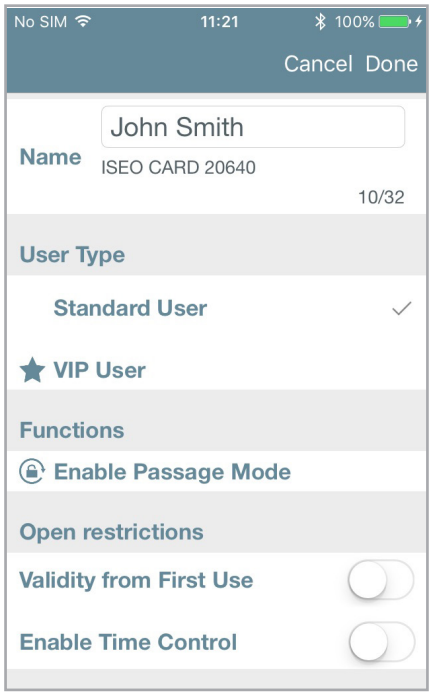
Time Schedules



Advanced

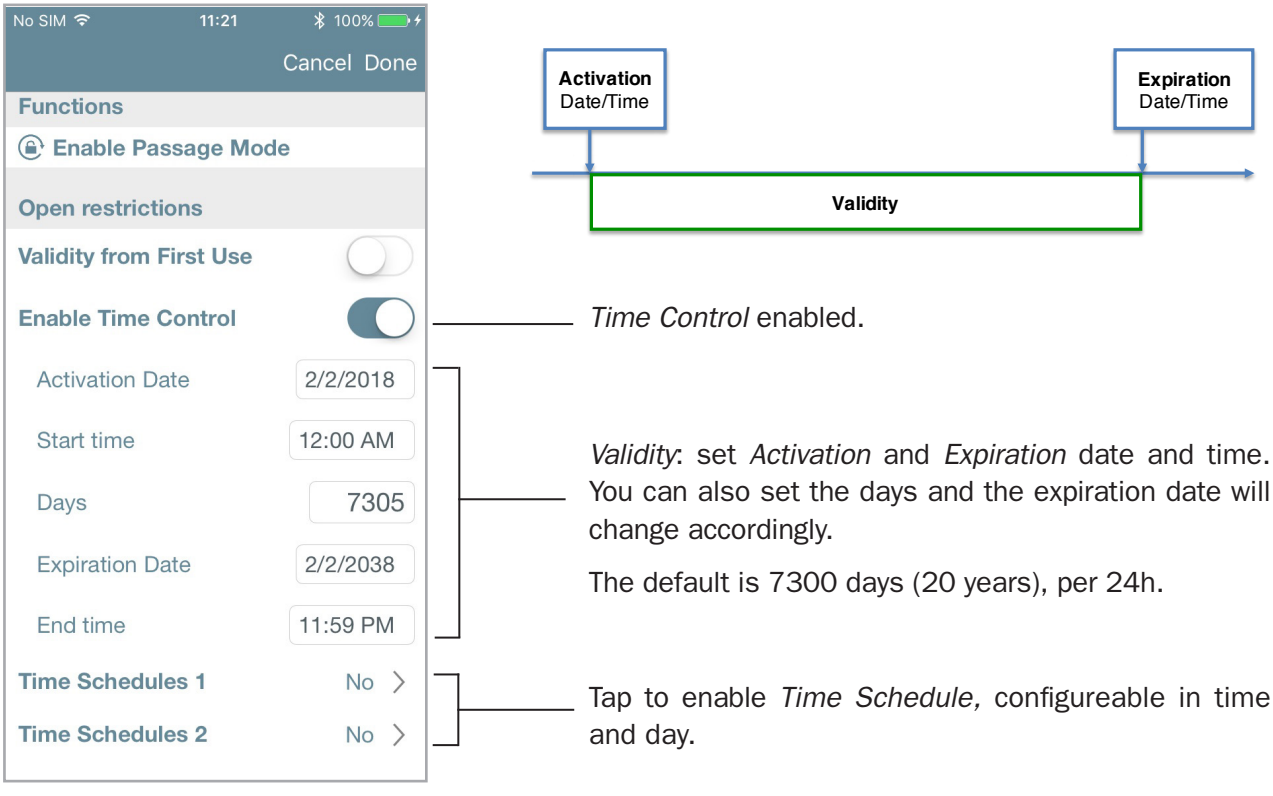
Time Control

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



Enable Time Control.

Validity



Time Control enabled.

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

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

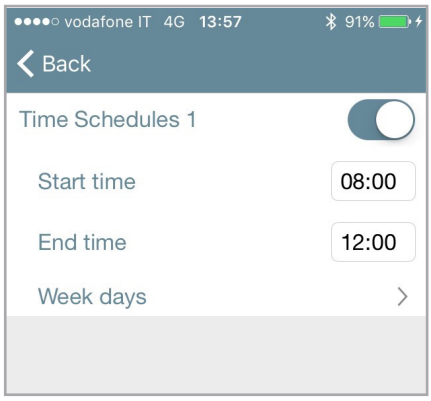
Tap to enable *Time Schedule,* configureable in time and day.

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

Advanced

Time Control

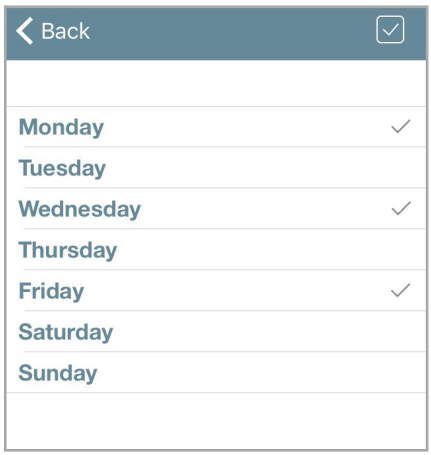
Time Schedules



Time Schedule 1 enabled.

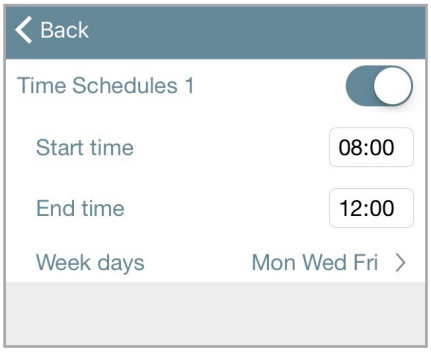
Set *Time Schedules start and end time.*
The default of *Time Schedue 1* is 8:00 - 12:00, while the default of *Time Schedue 2* is 14:00 - 18:00.

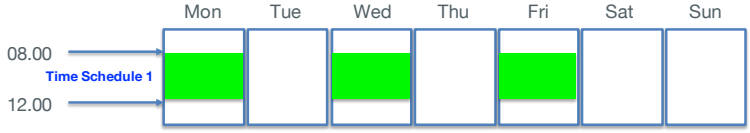
Select the days.



Check/uncheck all days with one touch.

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



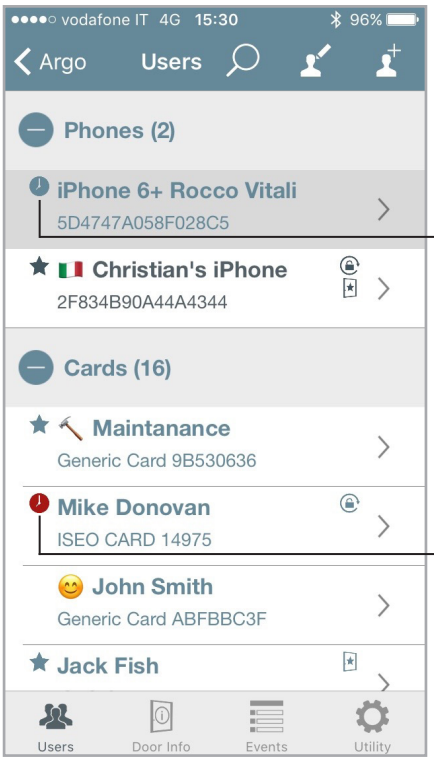


You can see selected days in the *Time Schedule* menu.

Advanced

Time Control

User list overview

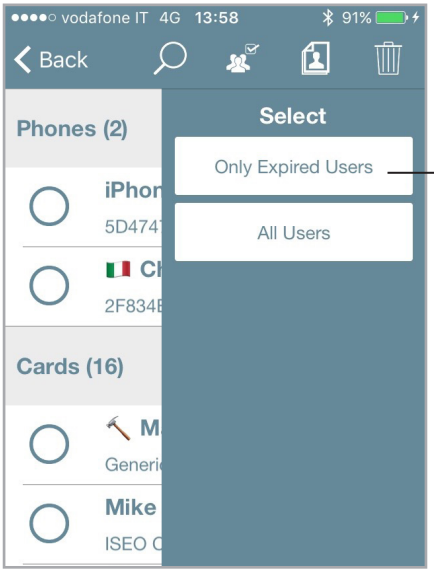


The clock means that user has enabled the *Time Control.*

The red clock means *expired* user.

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

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



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

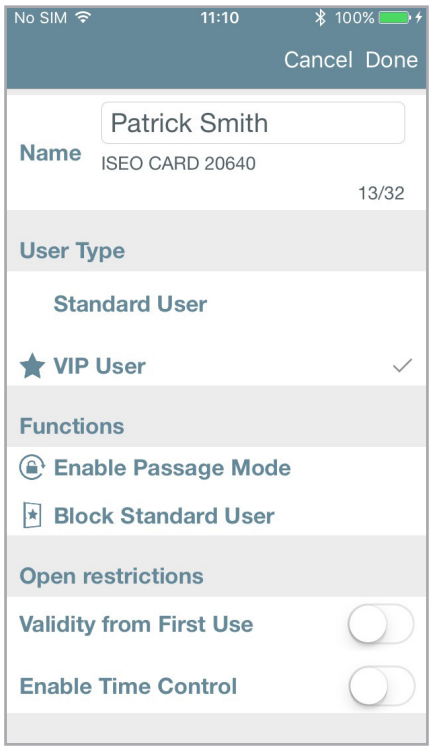
See also *Delete users* paragraph on *Basics* chapter.

Advanced

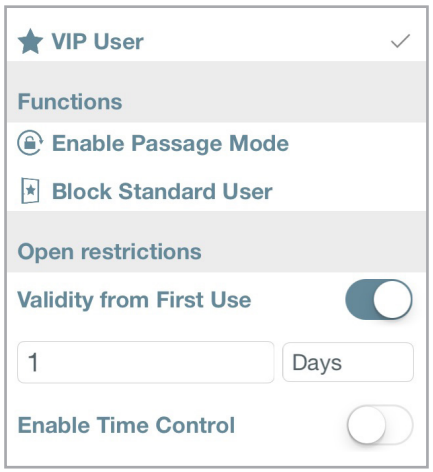
Validity from First Use

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

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



Enable **Validity from First Use**.



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

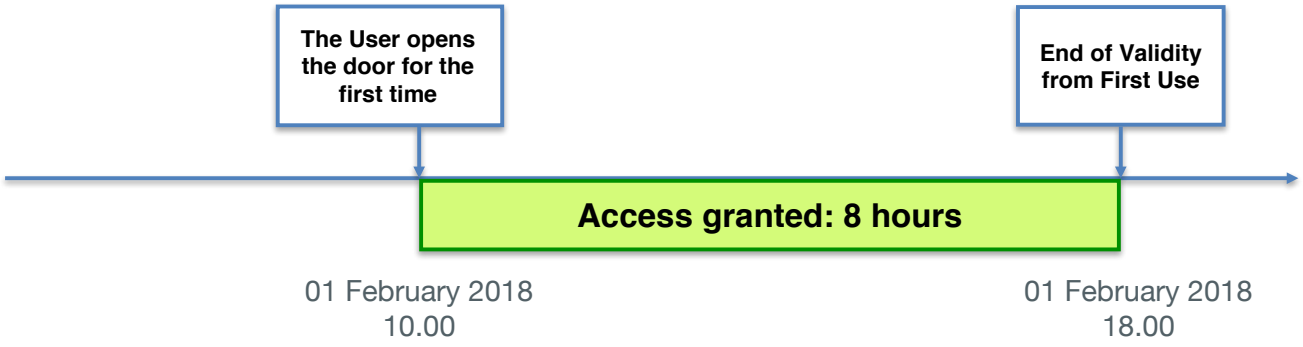
Advanced

Validity from First Use

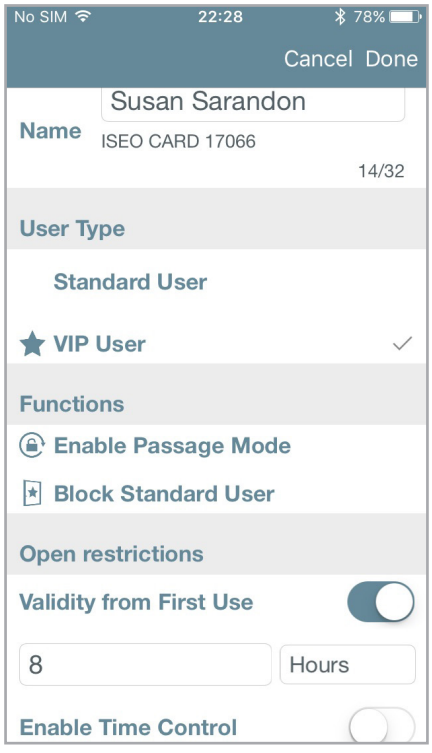
When the *User* opens the door for the first time, the *Validity from First Use* become the date and the time of that moment, and the credential will expire according to the validity set. To show what's happens on the *Argo app* using the *Validity from First Use*, see the next examples.

Example 1: Validity from First Use 8 hours

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



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



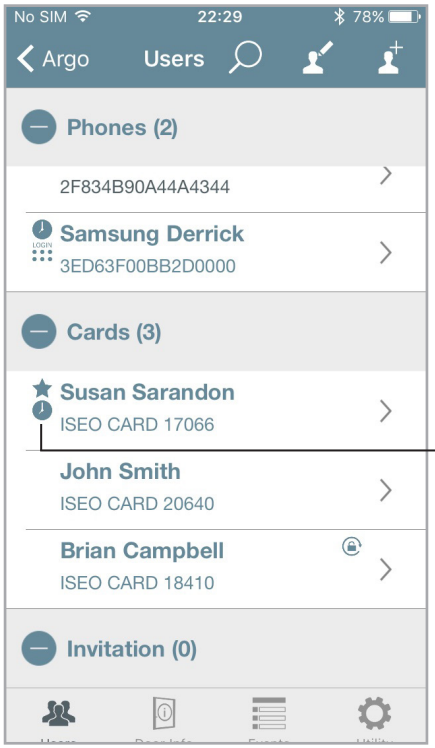
Enable **Validity from First Use**

Set **8 Hours**

Advanced

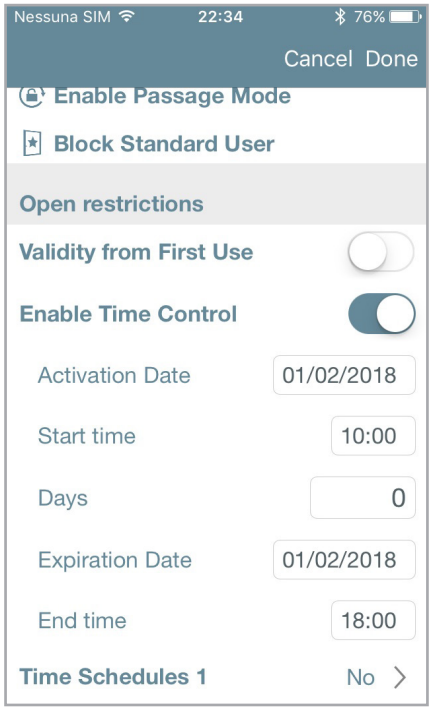
Validity from First Use

User List overview:



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

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



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

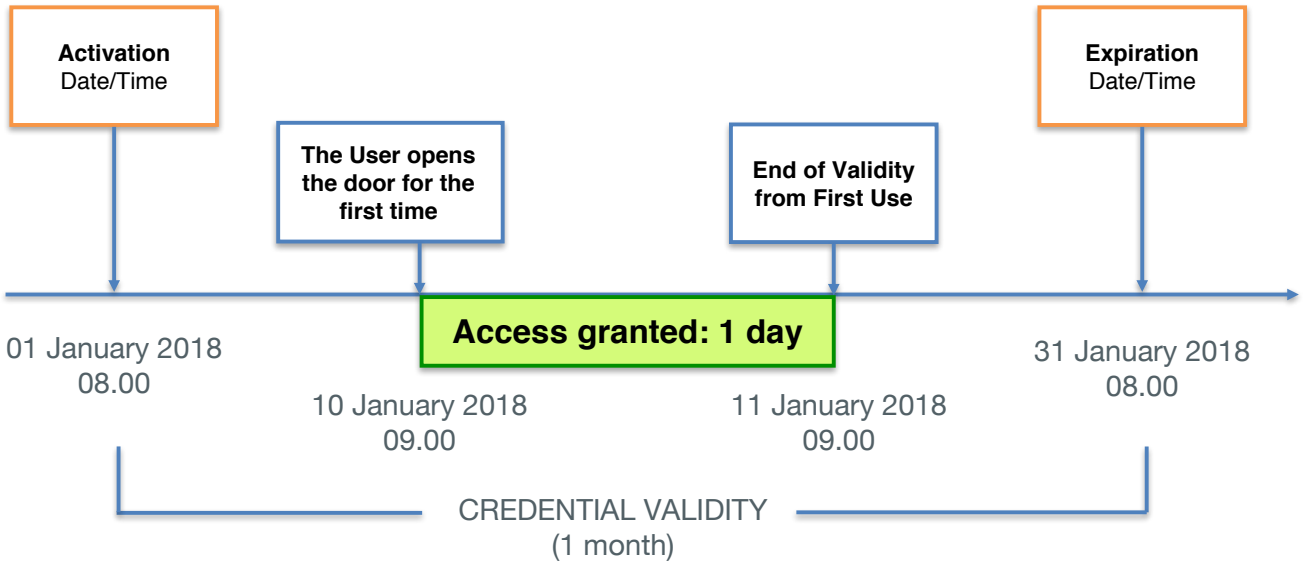
The **Time Control** is now enabled since the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** are automatically set, adding 8 hours to the **Start Time**.

Advanced

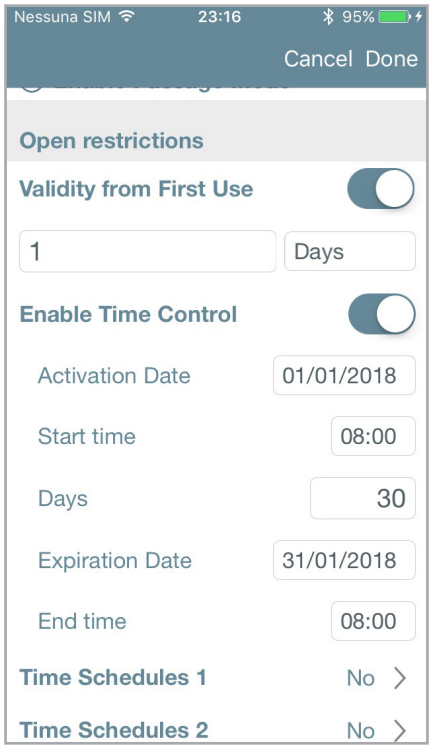
Validity from First Use

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

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



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



Enable **Validity from First Use**

Set **1 Days**

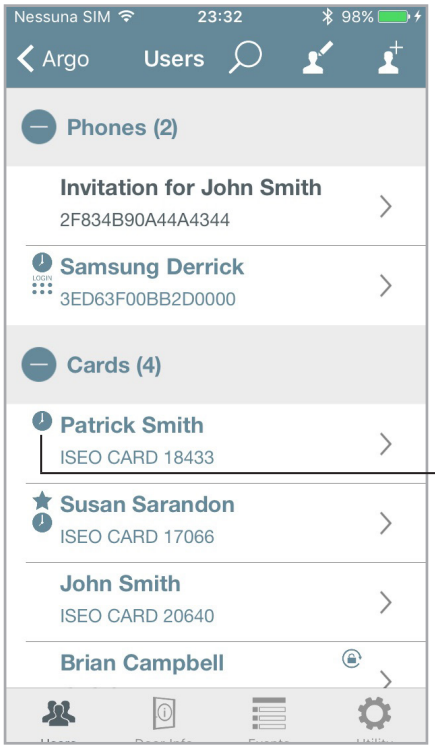
Enable **Time Control**

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

Advanced

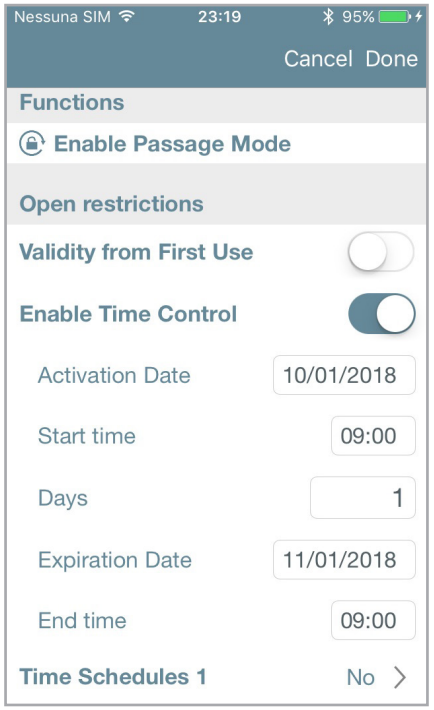
Validity from First Use

User List overview:



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

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



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

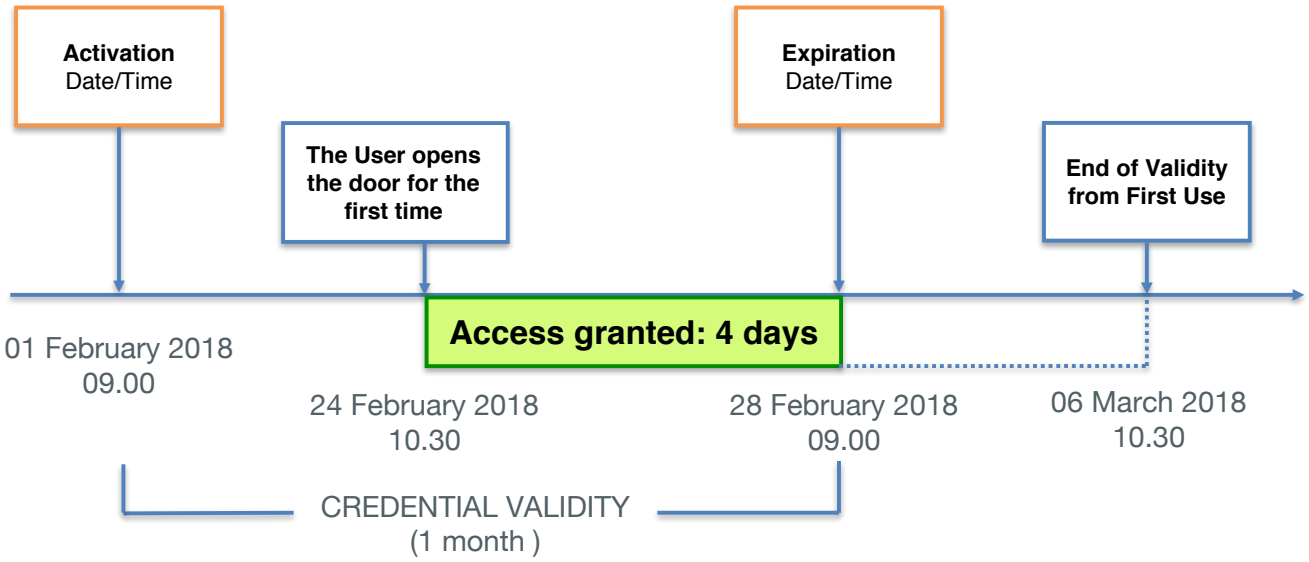
In the **Time Control** the *Validity from First User* has become the date and time when the *User* opened the door for the first time. The **Expiration Date** and the **End Time** are automatically set, adding 1 day to the **Activation Date**.

Advanced

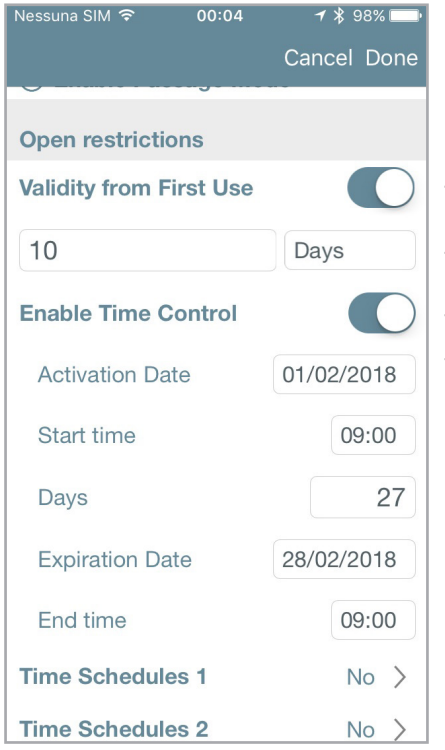
Validity from First Use

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

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



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



Enable **Validity from First Use**

Set **10 Days**

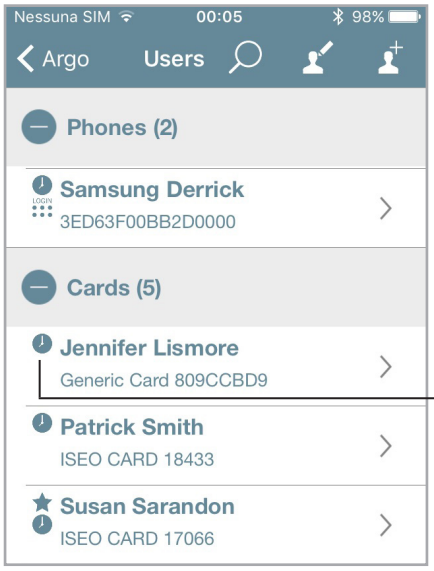
Enable **Time Control**

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

Advanced

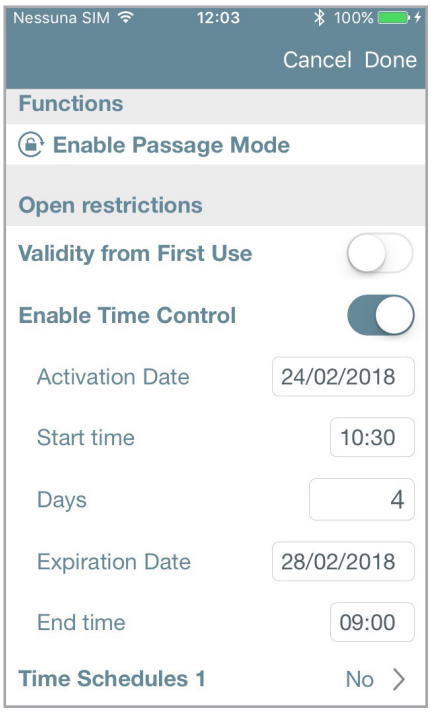
Validity from First Use

User List overview:



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

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



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

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

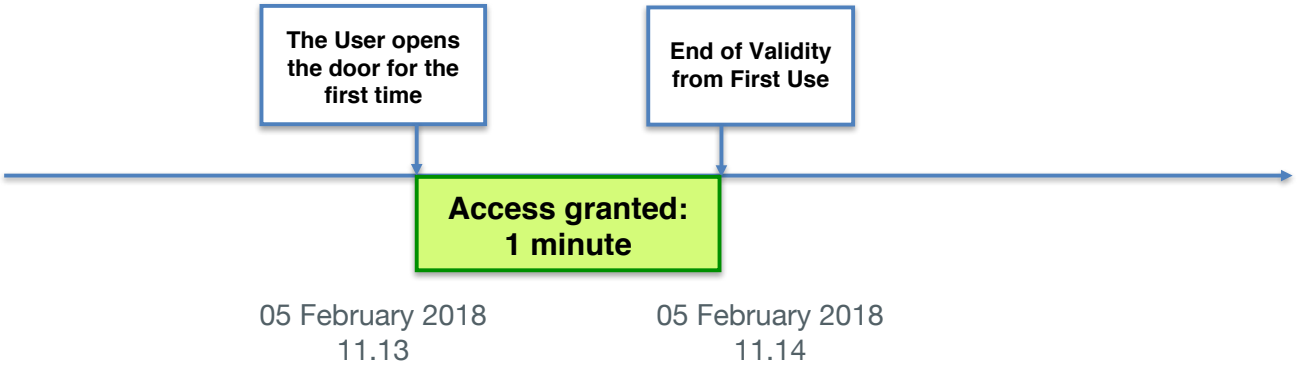
Credential *Expiration Date* doesn't change, since it has priority over the *End of Validity from First Use*. In the example above *Expiration Date* has remained the same: 28/02/2018. That means *Validity from First Use* has changed from 10 to 4 days, to not exceed the credential *Expiration Date*.

Advanced

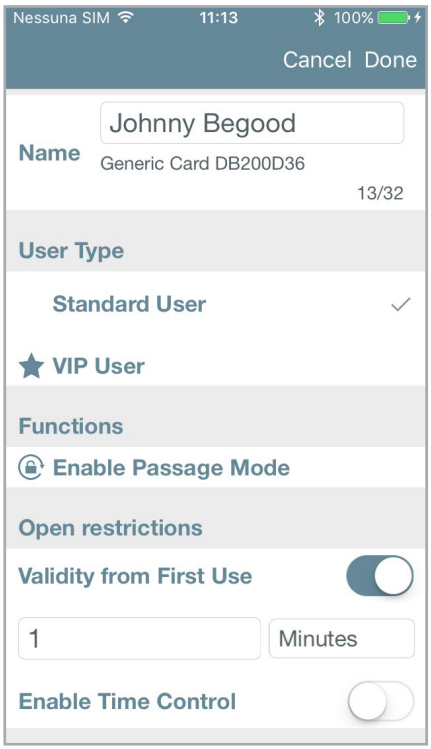
Validity from First Use

Example 4: Validity from First Use 1 minute

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



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



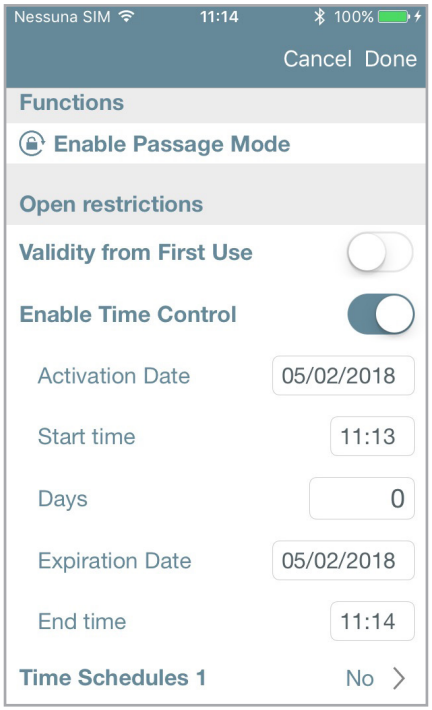
Enable **Validity from First Use**

Set **1 Minutes**

Advanced

Validity from First Use

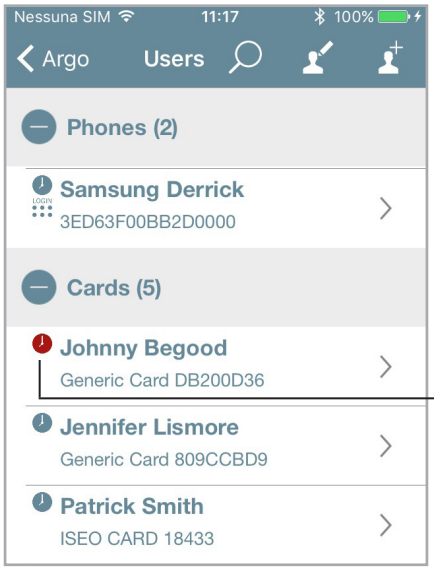
The *User* opens the door for the first time. The *Administrator* enter *Programming mode* to check the credential status.



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

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

User List overview after 1 minute has passed:

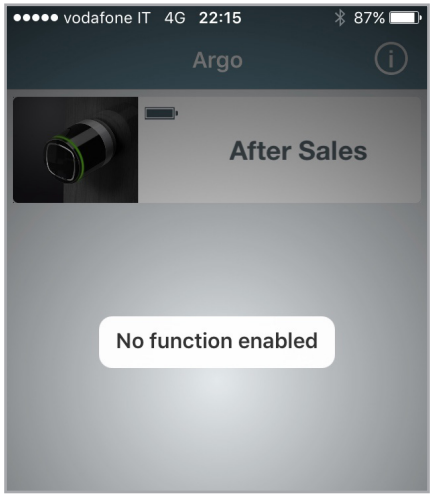


The red clock means that *User* has expired, since 1 minute has passed (one shot entrance).

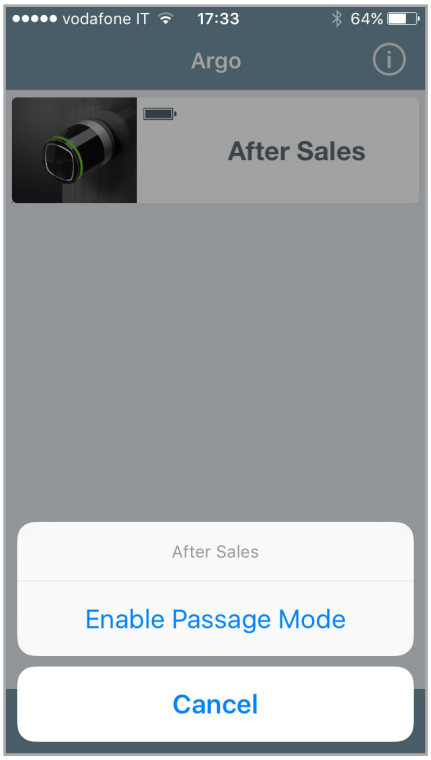
Advanced

Tap & Hold menu

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



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

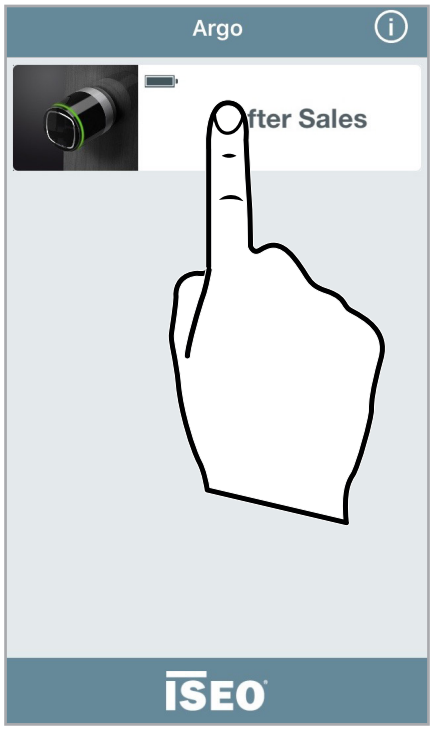


See also the *Video tutorial,* explaining in detail the *Tap & Hold* functions, at link: *https://app.iseo.com/?parm=ARGO&lang=en&folder=video-tutorial*

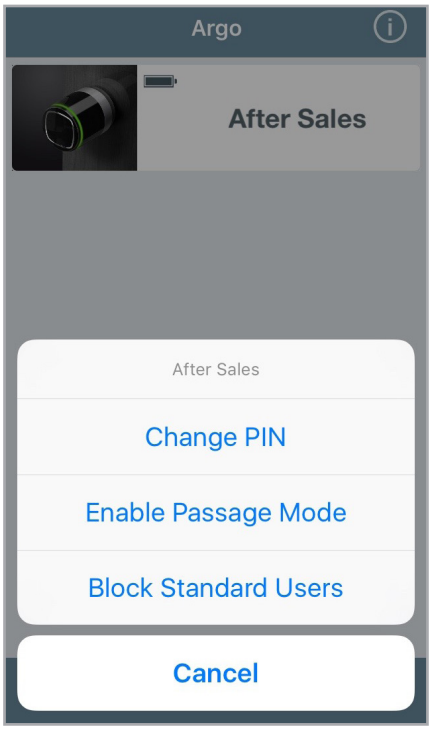
Advanced

Enable Passage Mode

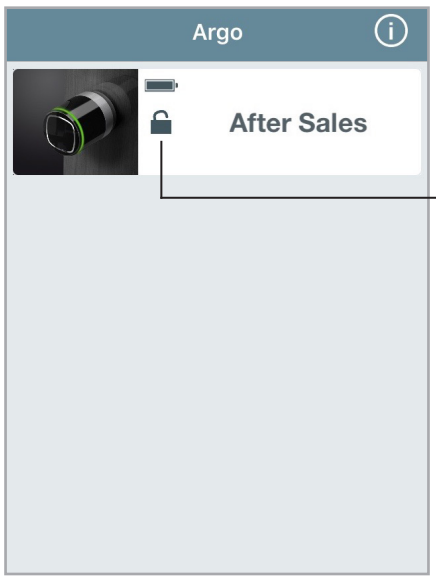
Enabling *Passage Mode* into the lock, the door will be always opened for any user who wishes to gain access, without the use of authorized credentials.



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



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



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

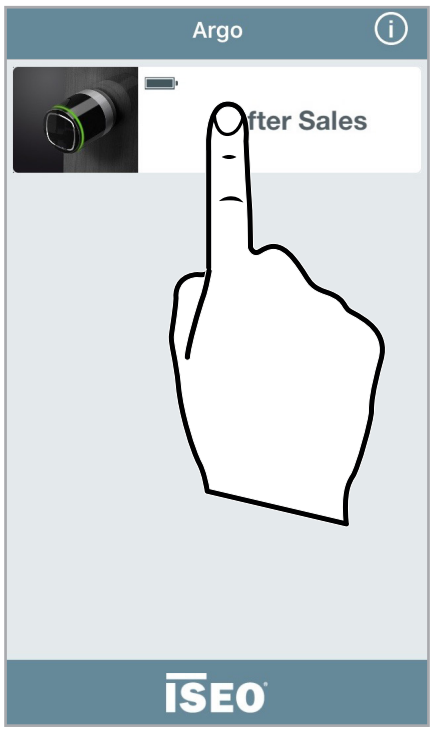
5. Follow the same procedure to disable the function.

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

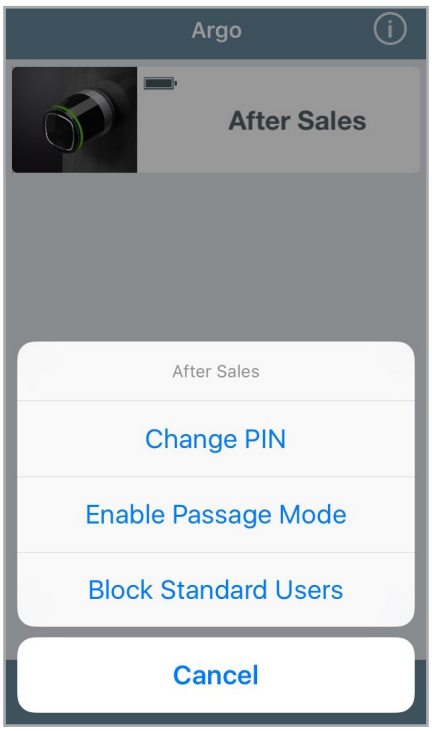
Advanced

Block Standard Users

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



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



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

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

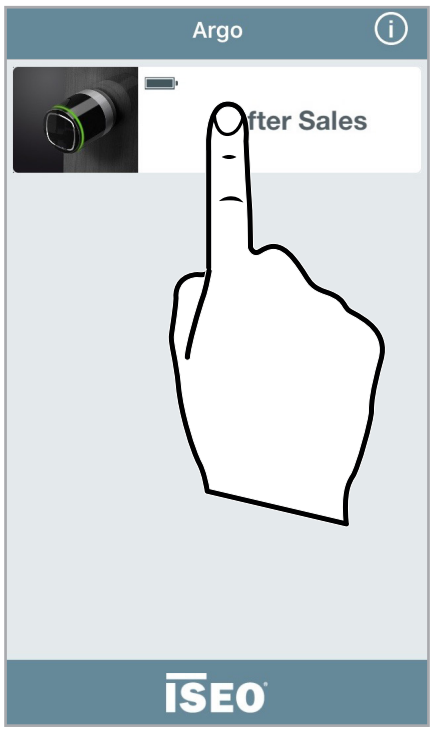
5. Follow the same procedure to disable the function.

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

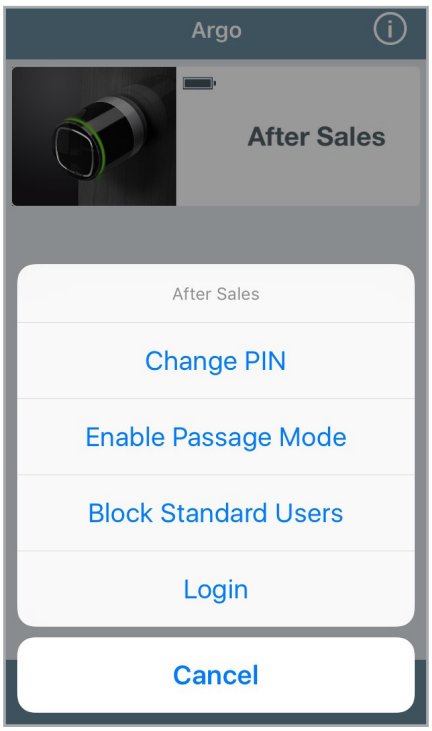
Advanced

Login (without Master Card) LOGIN

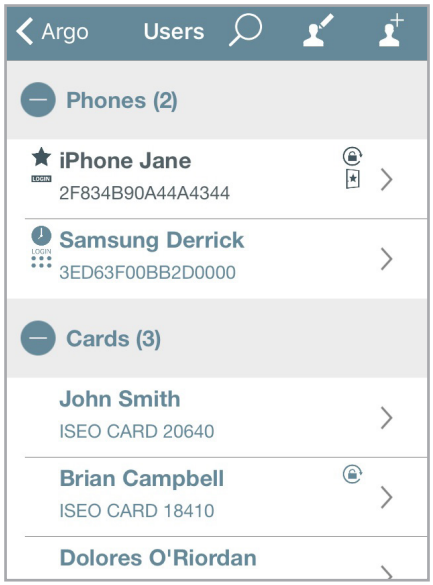
This function allows your smartphone to enter *Programming Mode* without the need of the *Master Card.*



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



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



4. You will enter *Programming Mode*.

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

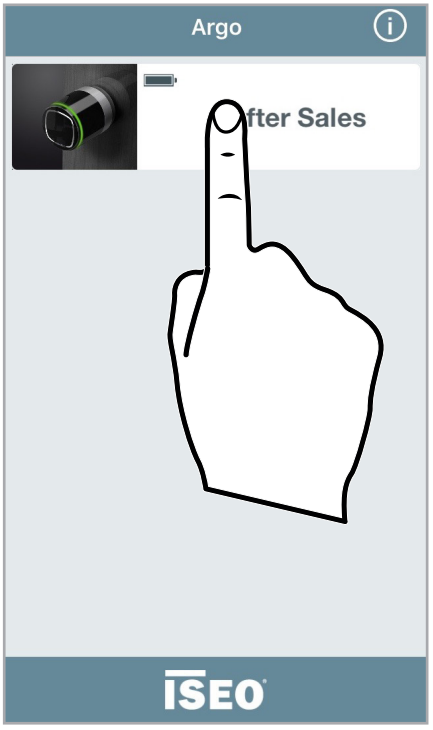
The LOGIN icon in the user list means this phone can enter *Programming Mode* without *Master Card* but a *PIN code* previously set is required.

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

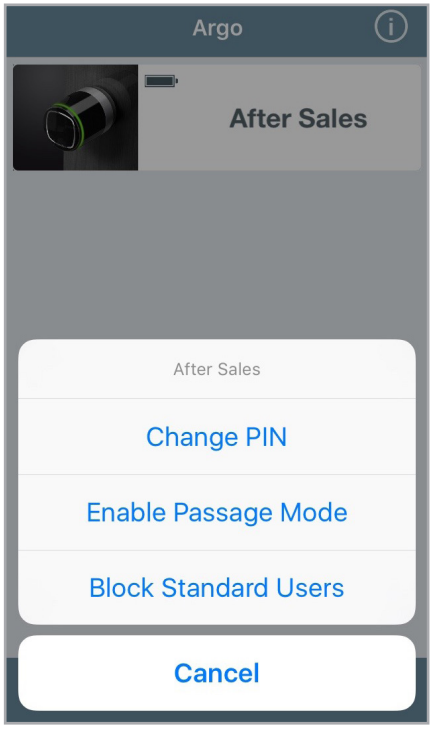
Advanced

Change the PIN code

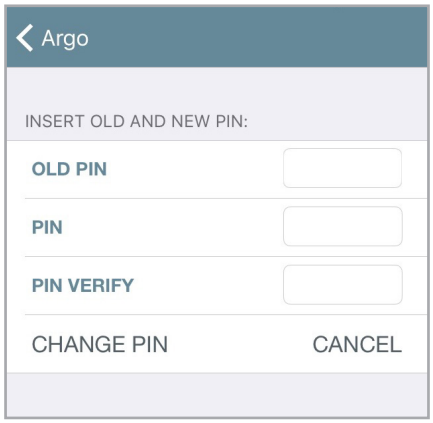
This function allows to change the *PIN code* if previously set in the smartphone. This *PIN code (4 digits)*, could be set to open the door and/or to *Login* without *Master Card* (see *User type and functions* and *Smartphone user parameters* pragraphs).



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



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



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

Advanced

Enable Passage Mode without Argo app

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

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

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

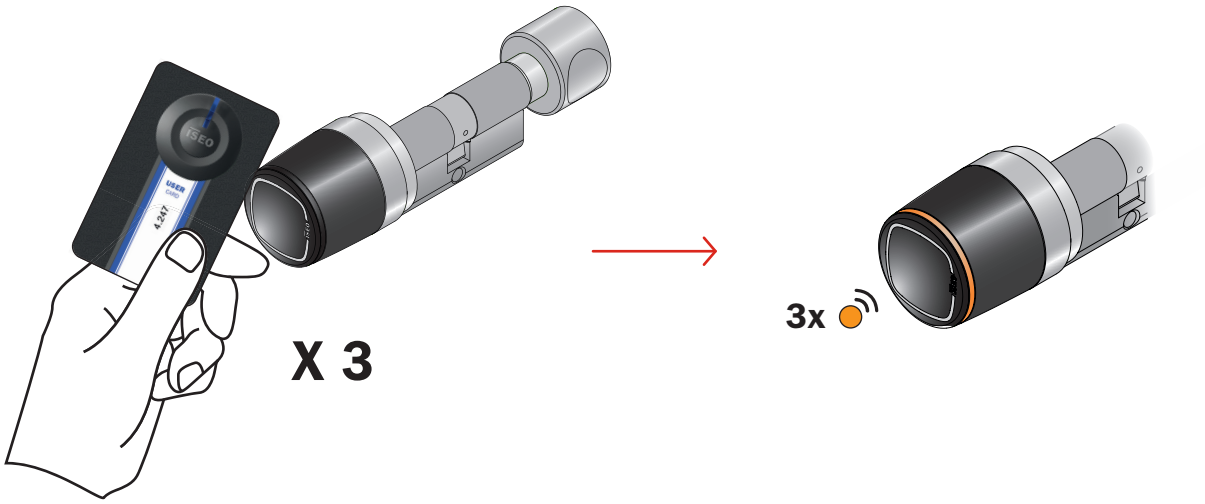
Advanced

Block Standard User without Argo app

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

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

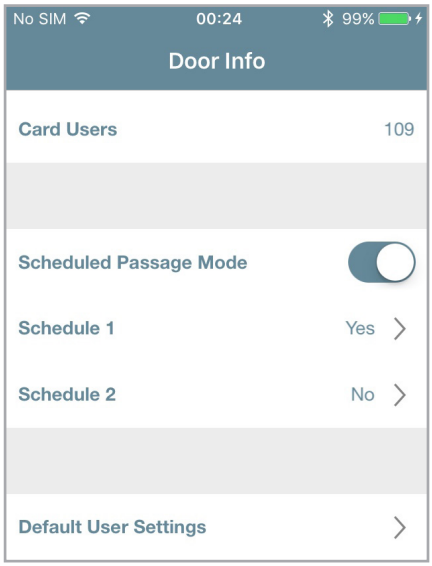
Follow the same procedure to disable the *Block Standard User* function.



Advanced

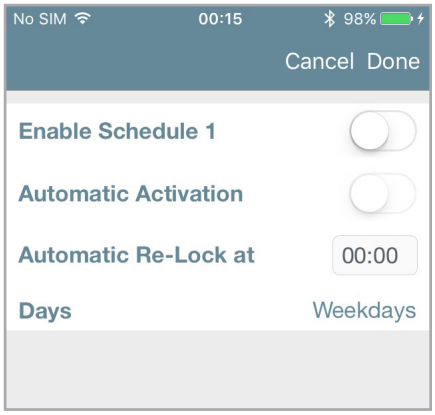
Scheduled Passage Mode

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



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

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



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

At the end touch **Done**.

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

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

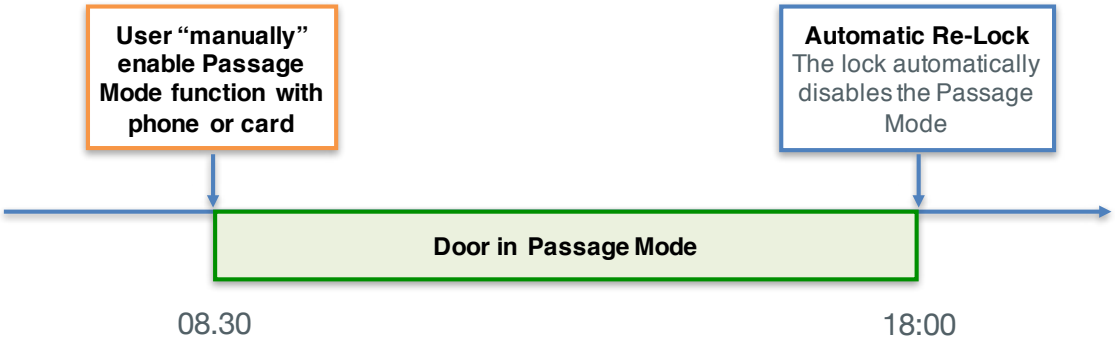
If *Stylos Smart* activates a device with an electric coil (electric lock or electric strike), before enable the *Passage Mode*, make sure the device can be kept always energized for a long time, without damage itself.

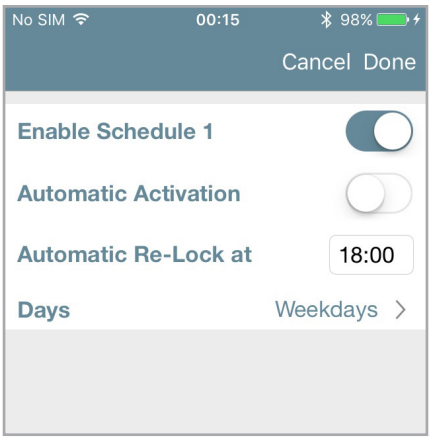
Advanced

Scheduled Passage Mode

1. Passage Mode with Automatic Re-Lock

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

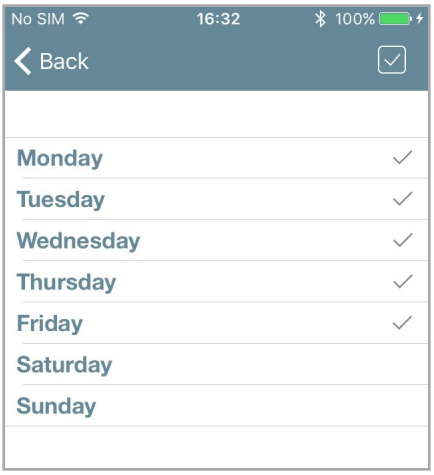




Switch on **Enable Schedule 1** to set **Automatic Re-Lock at**.

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

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



Check/uncheck all days with one touch.

Select multiple or single days, one by one.

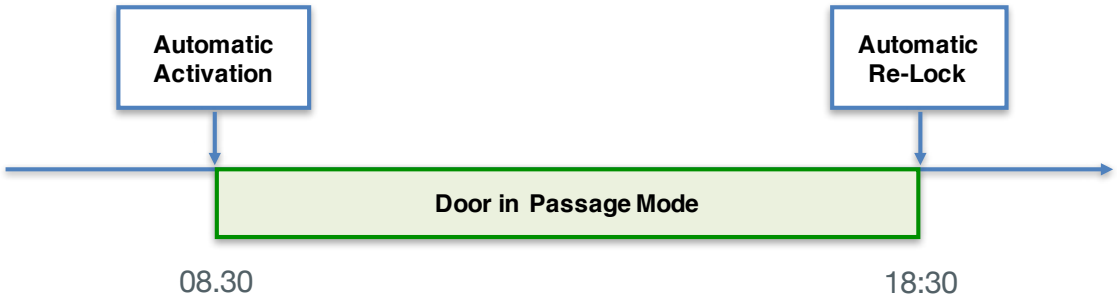
At the end press **Back**, then **Done**.

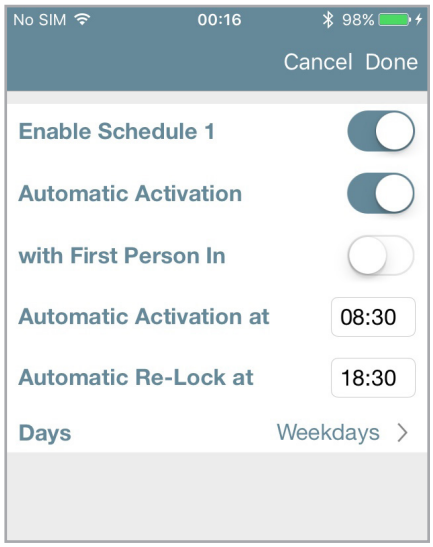
Advanced

Scheduled Passage Mode

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

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



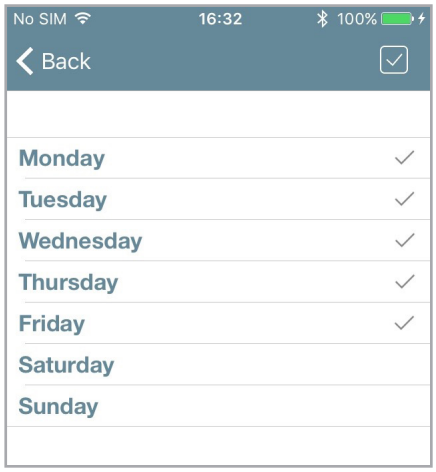


Swith on **Enable Schedule 1**.

Swith on **Automatic Activation**.

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

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



Check/uncheck all days with one touch.

Select multiple or single days, one by one.

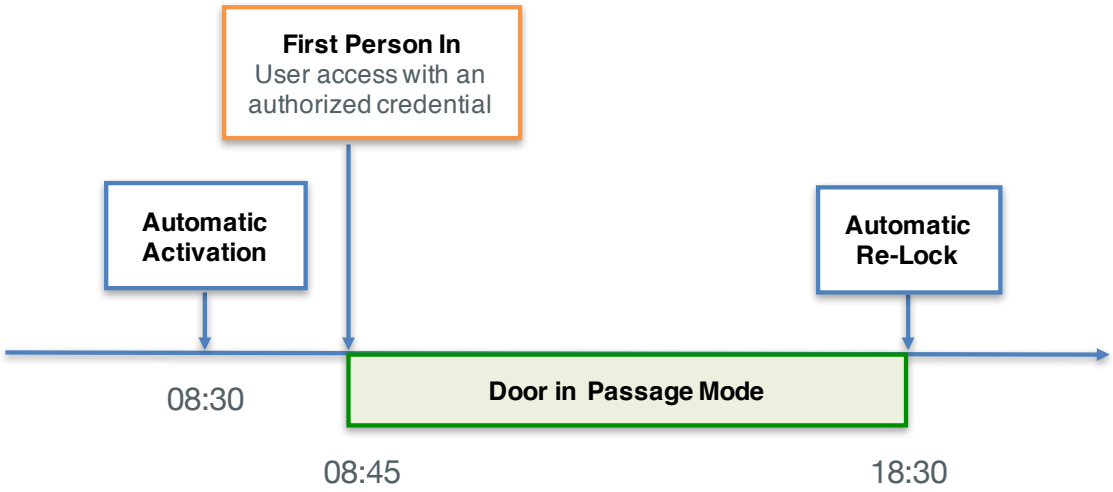
At the end press **Back**, then **Done**.

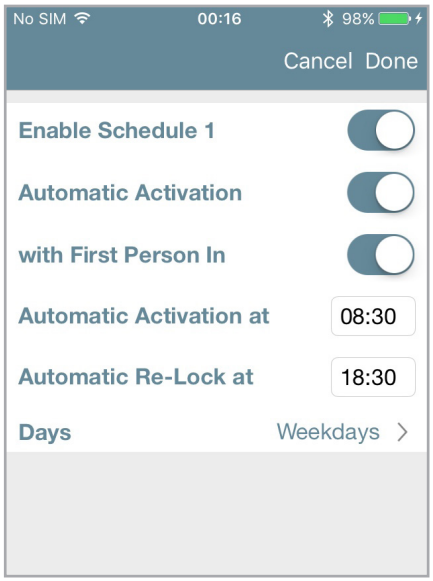
Advanced

Scheduled Passage Mode

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

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





Swith on **Enable Schedule 1**.

Swith on **Automatic Activation**.

Swith on **with First Person In**.

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

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

At the end touch **Done**.

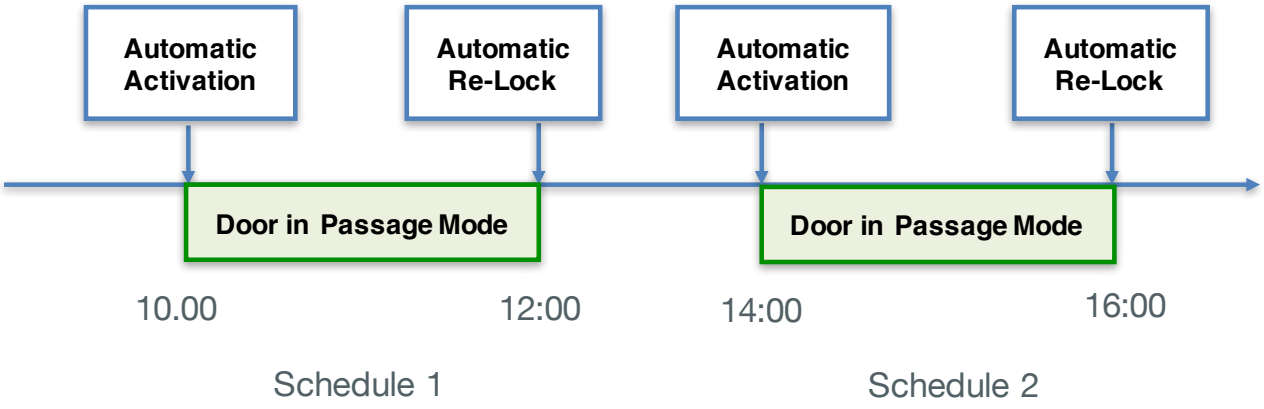
This solution is really useful in term of security and avoids the automatic *Passage Mode* activation when no user is inside the building or the room.

Advanced

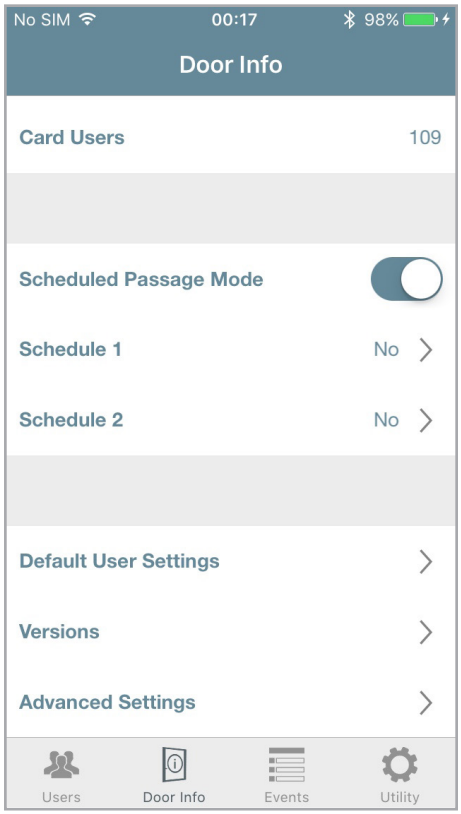
Scheduled Passage Mode

Configuration example: meeting room with Libra Smart

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



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



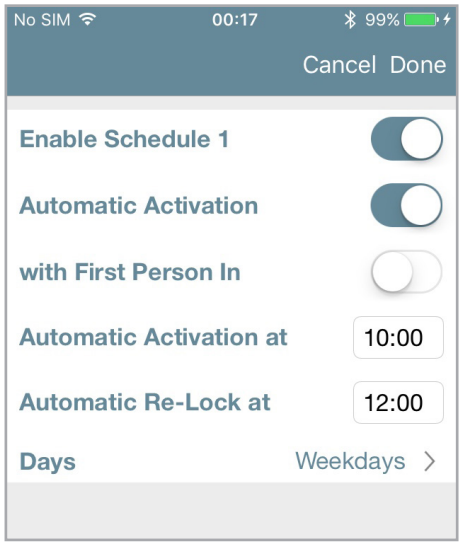
Enable **Schedule Passage Mode** to see the two schedules available.

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

Advanced

Scheduled Passage Mode

Configuration example: meeting room with Libra Smart

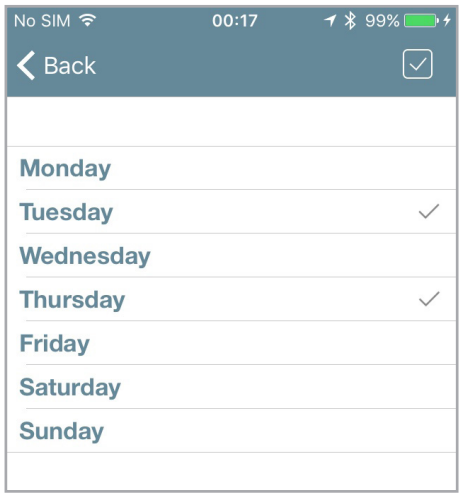


Switch on **Enable Schedule 1**.

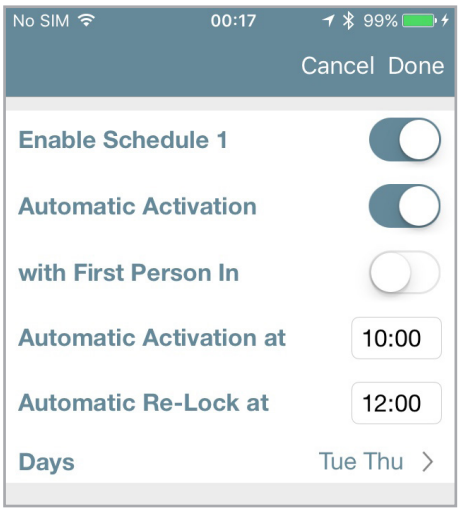
Swith on **Automatic Activation**.

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

Touch to select the days.



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



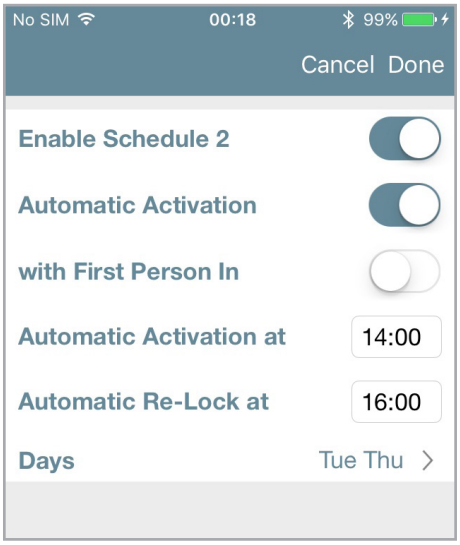
Tap **Done**.

Advanced

Scheduled Passage Mode

Configuration example: meeting room with Libra Smart

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

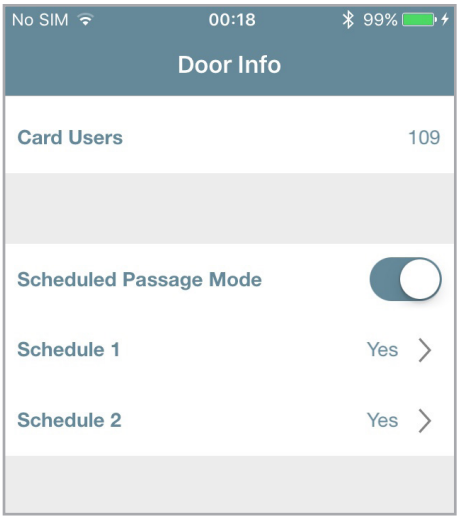


Switch on **Enable Schedule 2**.

Swith on **Automatic Activation**.

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

Touch to select Tuesday and Thursday.



The programming is finisched.

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

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

Advanced

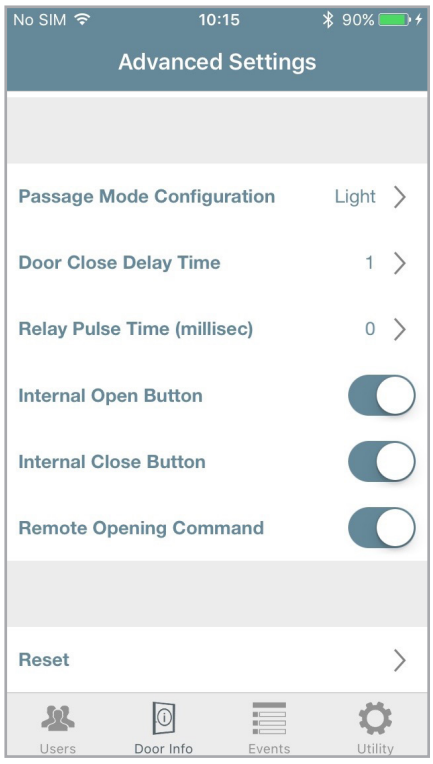
x1R Smart: Light Mode

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

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

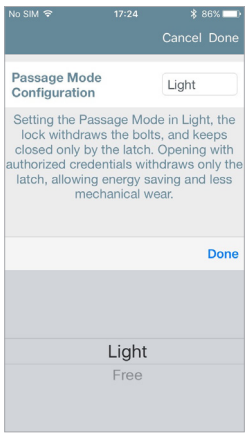
This solution combined to with *x1R Smart* is very useful and effective because it has the following advantages:

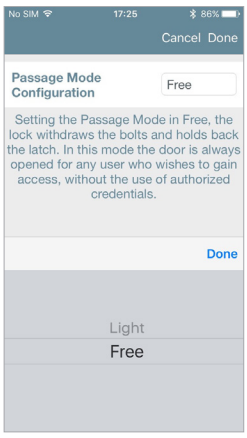
- high battery saving;
- reduced mechanical wear of lock, bolts, rods and deviators;
- higher opening speed;
- less noise during opening and closing movement.



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

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





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

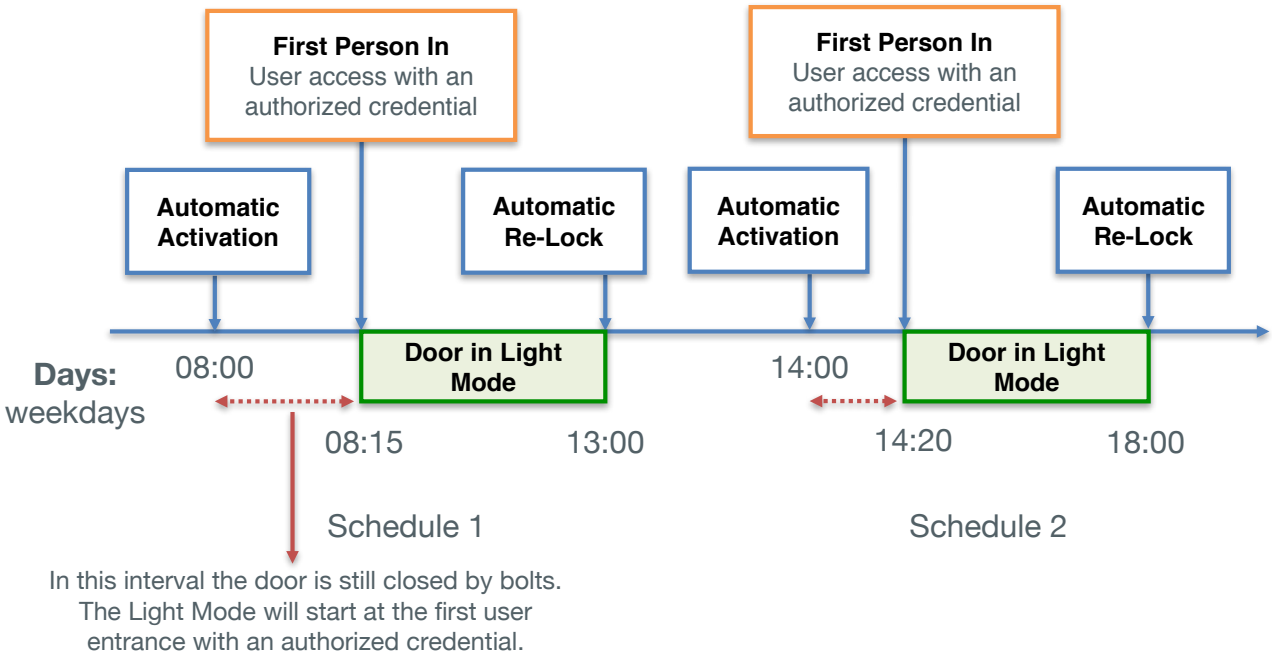
To know more about *x1R Smart Light* function, read the *x1R Smart User Manual*, available at site *https://app.iseo.com*.

Advanced

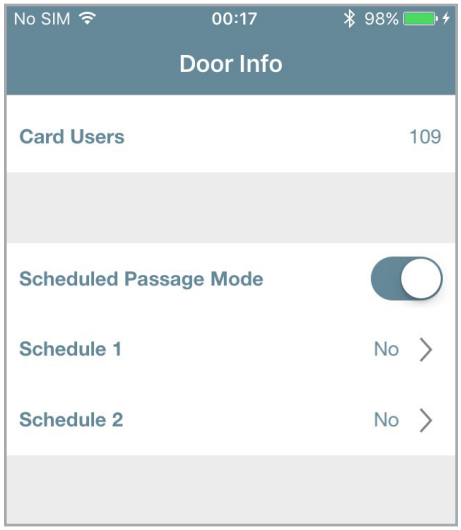
x1R Smart: Light Mode

Configuration example: main offices entrance with x1R Smart

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



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



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

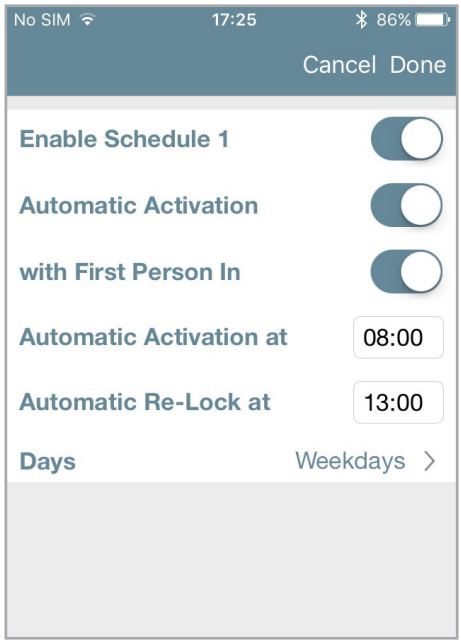
Touch **Schedule 1** and then **Schedule 2**, to configure the 2 schedules.

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

Advanced

x1R Smart: Light Mode

Configuration example: main offices entrance with x1R Smart



Switch on **Enable Schedule 1**.

Swith on **Automatic Activation**.

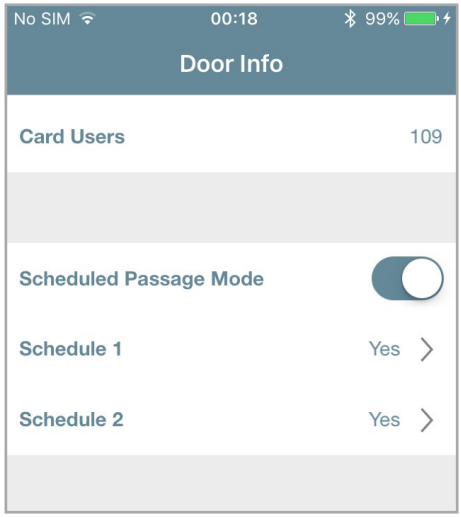
Switch on **with First Person In**.

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

Weedays are already set by deafult.

At the end touch **Done**.

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



The programming is finisched.

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

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

Advanced

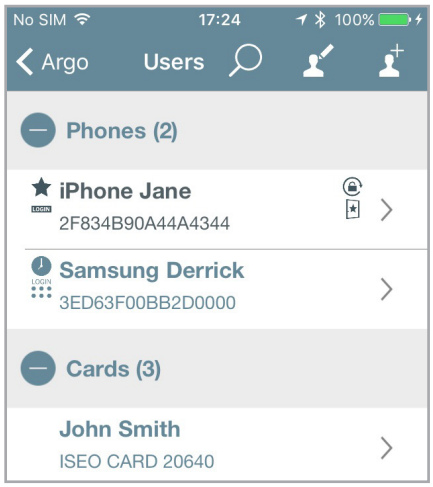
Invitations

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

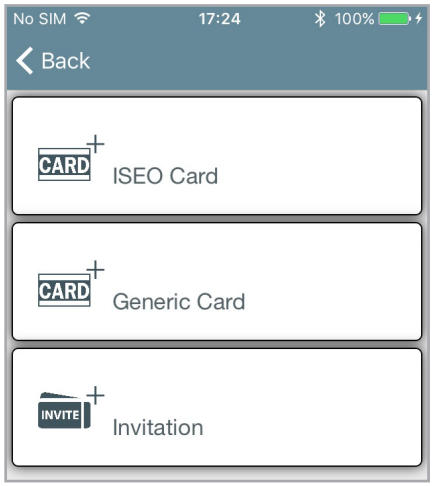
To fully explain how to program, manage and use *Invitations* by *Argo*, we can describe it in 3 main steps:

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

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



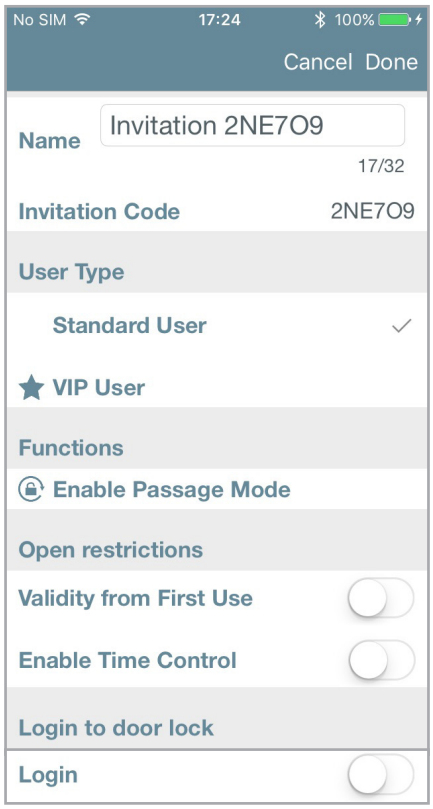
1. Enter *Programming Mode*
2. Tap the *add user* icon 



3. Tap **Invitation**

Advanced

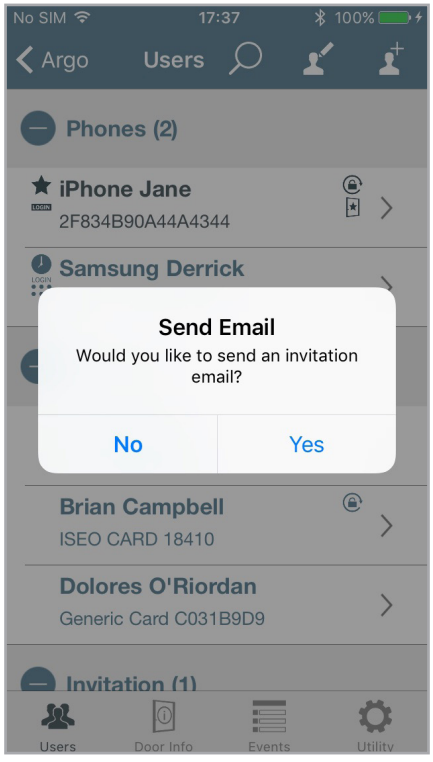
Invitations



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

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

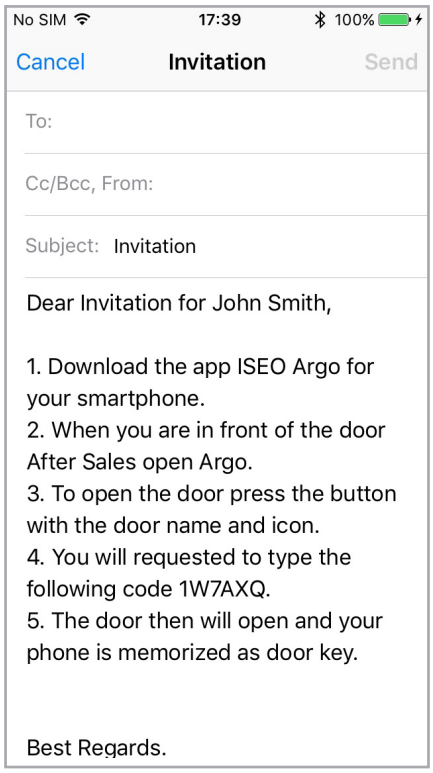
6. Press **Done** in the top right corner.



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

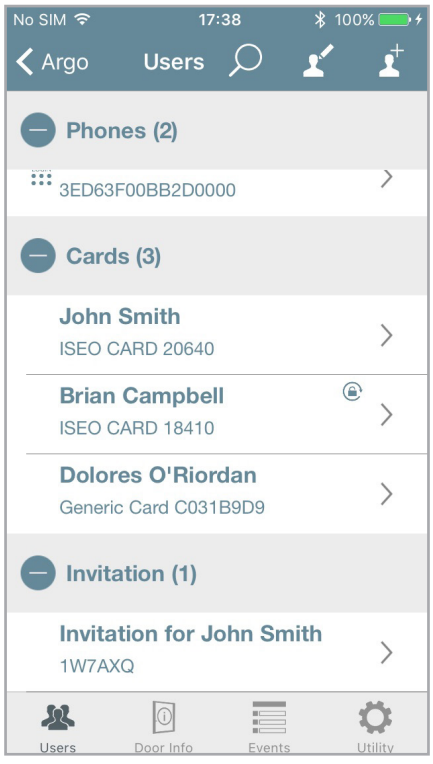
Advanced

Invitations



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

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



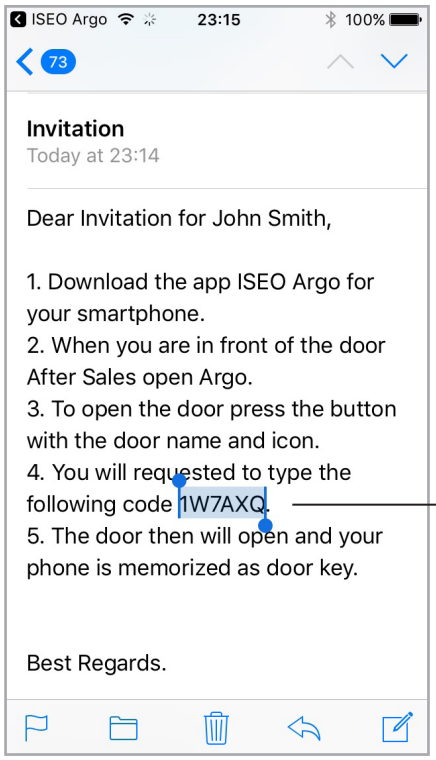
9. You can see in the *Argo User List* the added invitation, in the **Invitations** user field.
You can always modify the existing invitations like any other credential, adding or changing functionalities: *User Type*, *Functions*, *Open restrictions*, *Login to Doorlock*.

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

Advanced

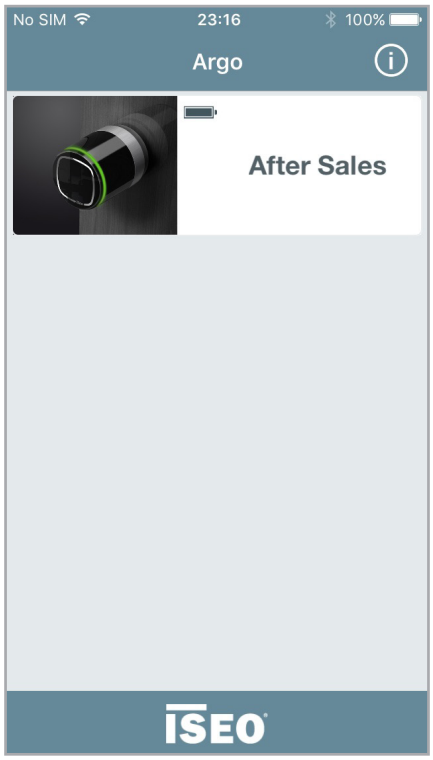
Invitations

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



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

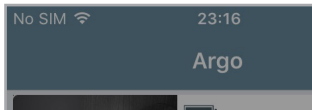
Invitation Code



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

Advanced

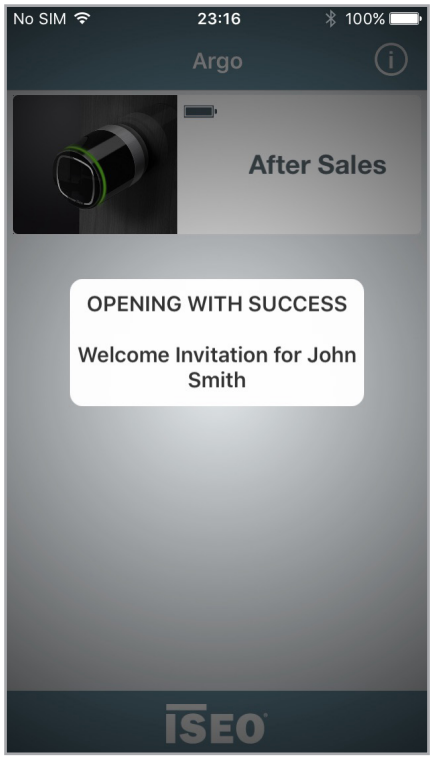
Invitations



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

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

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



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

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

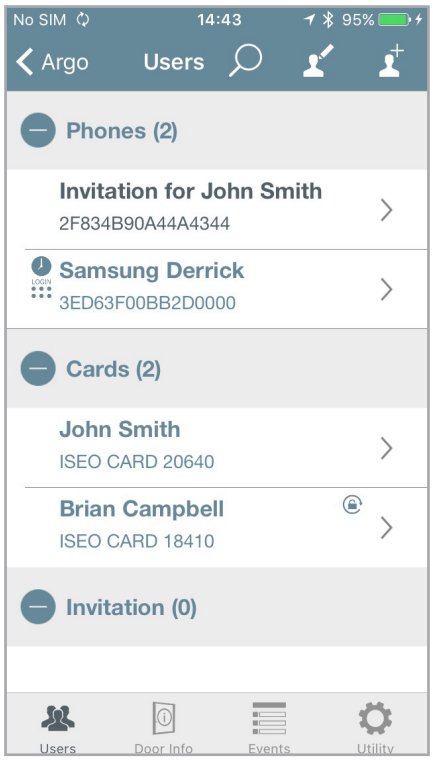
The invitation will expire at its expiration time and date, if previously set.

The *Invitation Code* can be used once only.

Invitations

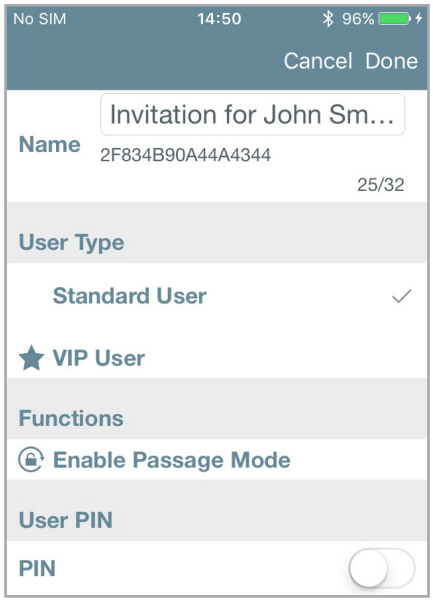
Step 3: the Administrator enter Programming Mode to manage the User list.

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



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

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



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

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

Advanced

Invitations

Questions and answers

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

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

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

3. Can I send the *Invitation* by *SMS* message or *WhatsApp*?
   Answer: no, by *Argo* you can send *Invitations* only by email. But you're free to copy the *Invitation Code to* send it or manage it as you like.

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

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

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

Advanced

Invitations 

Questions and answers

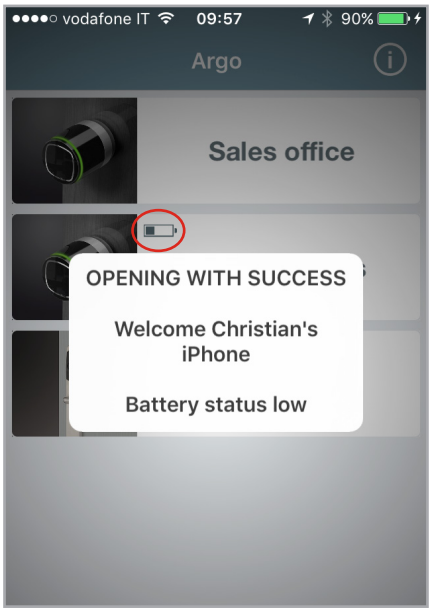
7. Could it happen that *Argo* generates an *Invitation Code* equal to the previous one?
   Answer: no, it's practically impossible. The *Invitation Codes* are randomly generated by using a random number generator that complies to the NIST specifications (National Institute of Standard). The NIST ensures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

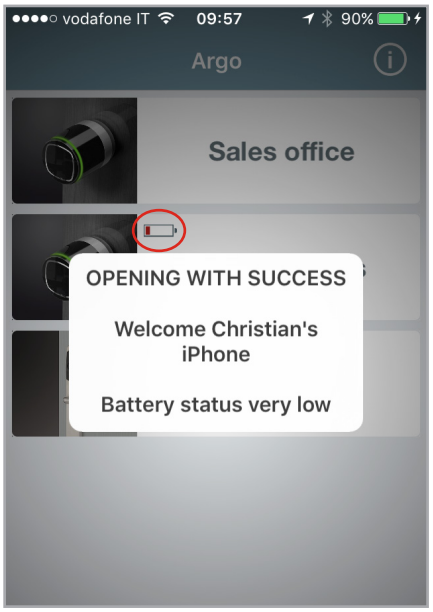
8. Could the *Invitation Code* be read throught the email by an hacker?
   Answer: usually email are cripted, but in case you don't trust the email security, you're free to deliver the *Invitation Code* as you like: by voice, taking advantage of WhatsApp end to end encryption, or by other more complicated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

Advanced

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.*

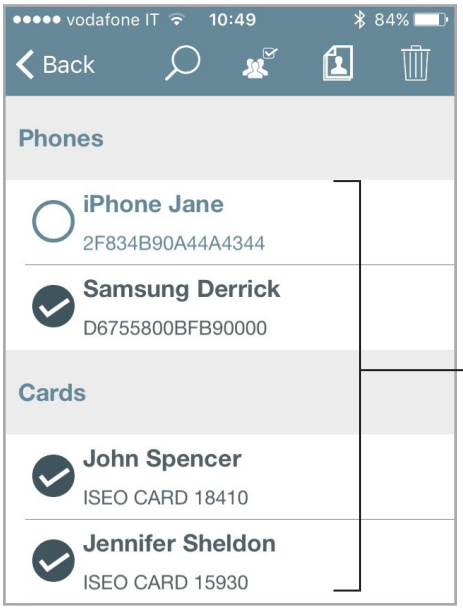
If the device is powered by mains, like Stylos, you will see the *lightning* at the place of the *battery* icon.

Advanced

Copy users

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

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



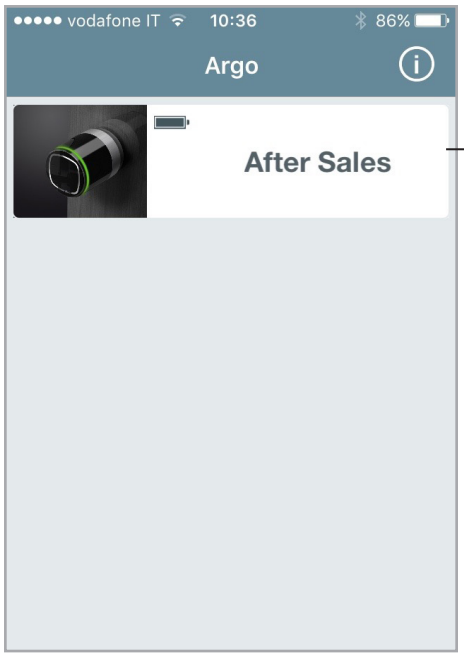
1. Select the users to be transferred.
   You can also select all users tapping on
2. Tap the *Copy* icon.

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

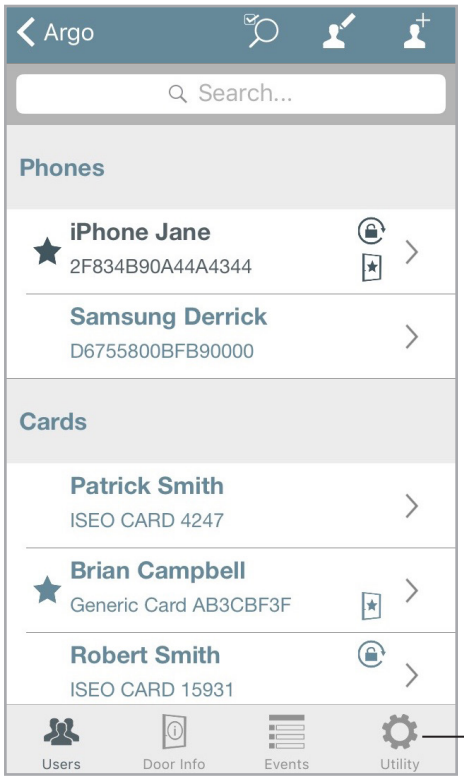
Advanced

Transfer users

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



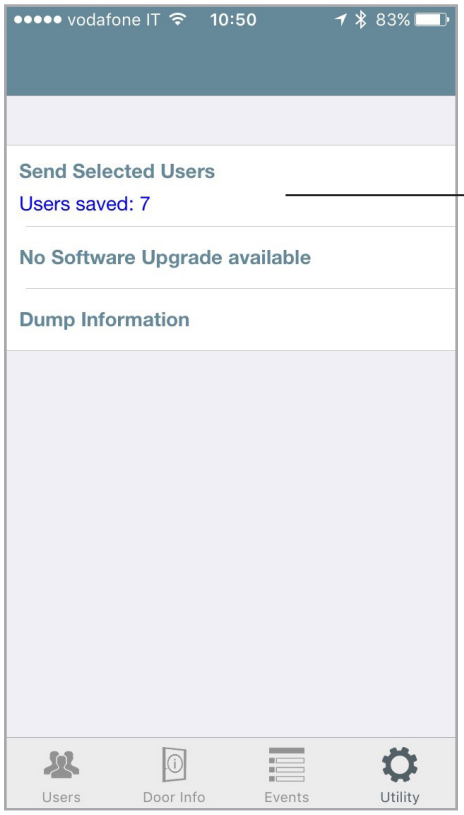
1. Enter *Programming mode* in the device where you want to transfer the users, by *Master Card.*



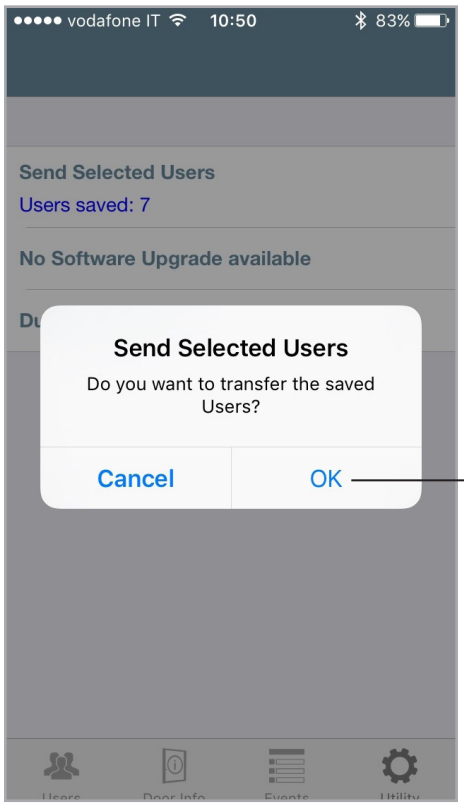
3. Tap **Utility** icon.

Advanced

Transfer users



4. Tap **Send Selected Users**.



5. Tap **OK**.

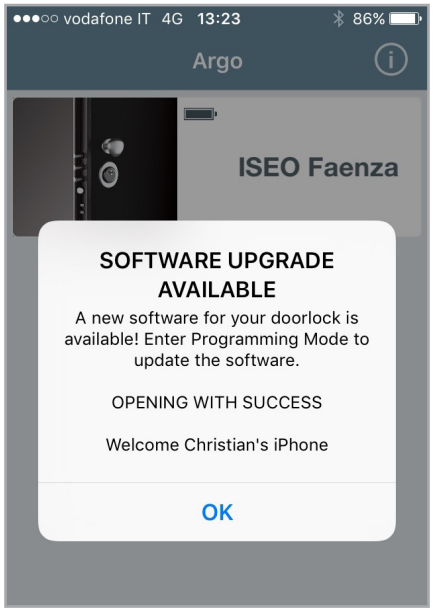
Advanced

Software Upgrade

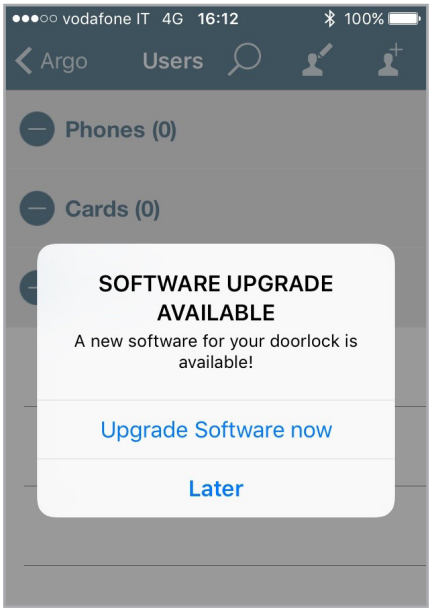
When a new *Software version* is available for your *Access control device*, your smartphone always notifies you when opening the door (image *1. Door opening*).
Moreover everytime you enter *Programming Mode*, a pop-up message will appear, and you can decide if upgrade software immediately or not (image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

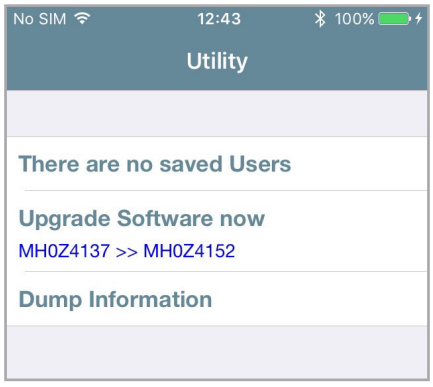
1. Door opening



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.

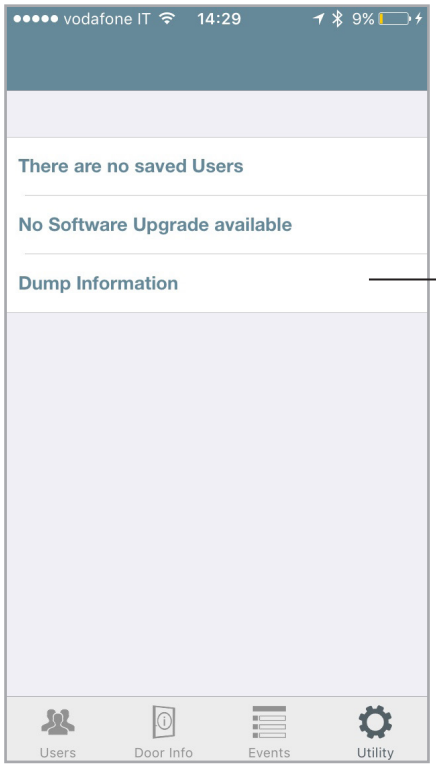
If you upgrade from *Argo* to *Argo 2.2*, watch before the tutorial "*Argo 2.0 Software Upgrade*", or read the manual "*Argo 2.0 Upgrade Procedure*", both available at:
https://app.iseo.com/?parm=ARGO&lang=en&folder=argo-update

Advanced

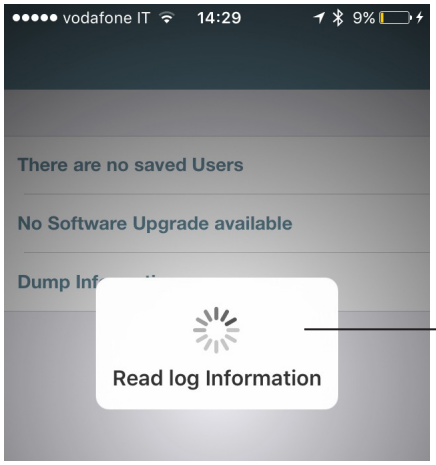
Dump Information

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**.

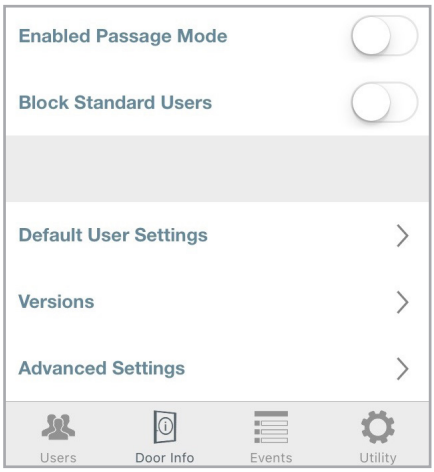


4. Wait until the log reading pop-up disappear (about 2 or 3 min.).
5. An *email* will be automatically created.
6. Send it to *IseoZero1 Technical Support*.

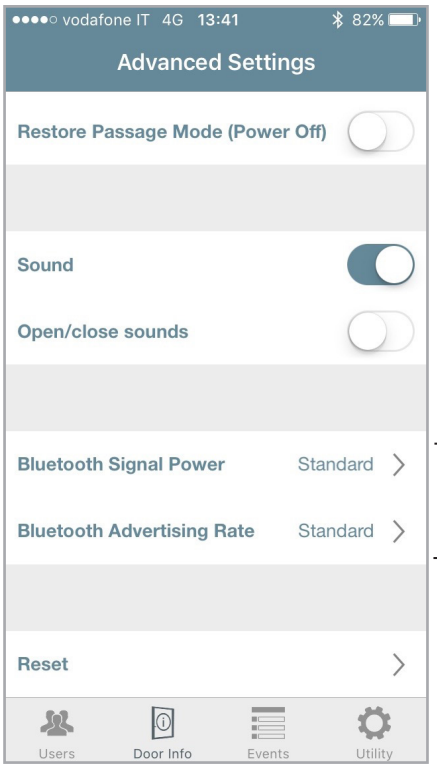
Advanced

Bluetooth parameters

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



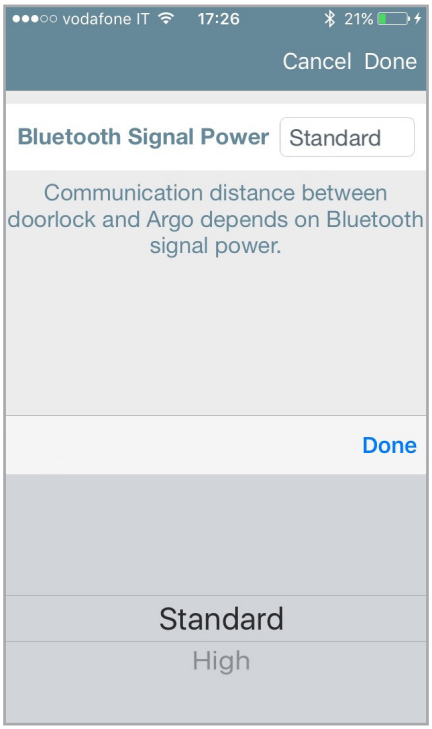
Enter **Door Info** and then **Advanced Setttings** menu.



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

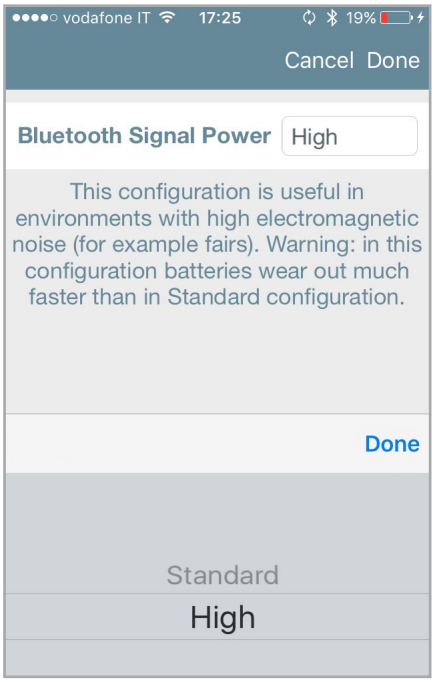
Advanced

Bluetooth parameters



A short text explains you the meaning of the feature.

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



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

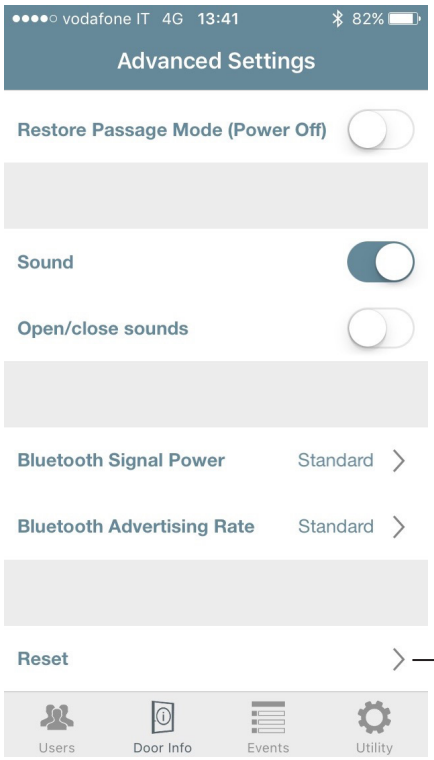
In order to avoid a faster battery consumption, remember to set the *Bluetooth parameters* back to *Standard* setting, at the end of the fairs or exibithion.

Advanced

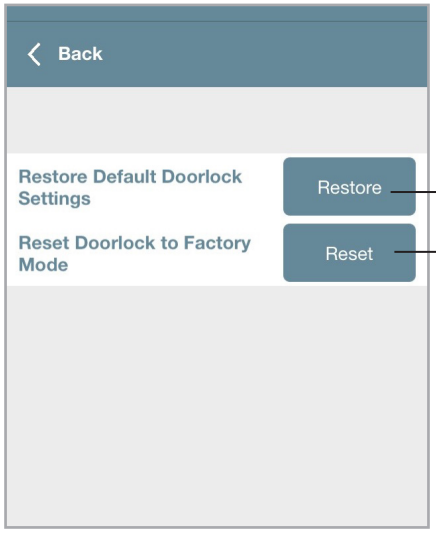
Reset

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

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



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



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

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

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

Updating of Master Card level

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

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

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

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

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

Master Card Set replacement and updating of System Code

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

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

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

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

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

Events log messages

(Common to all devices)

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

Events log messages

(Common to all devices)

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

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

Events log messages

(Only Aries Smart)

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

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

(Only Stylos Smart)

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

Advanced

Events log messages

(Only x1R Smart)

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

Operations summary without Argo app

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

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

Advanced

Technical data summary table

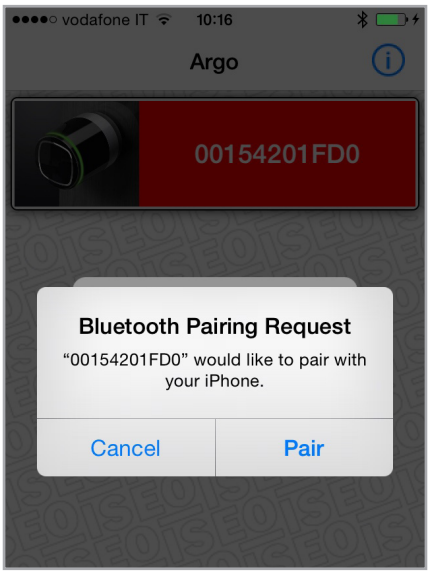
Feature description	Value	Device
Max nr. of users	300	All
Max. nr. of recorded events	1000	All
Compatible phones	*iOS*: from iPhone 4s with iOS 7 and above. *Android*: from version 4.3 (Jelly Bean), featuring *Bluetooth Smart Ready* hardware.	All
Compatible credentials	1. ISEO cards, tags 2. Mifare*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

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

Advanced

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*

Advanced

In-app pairing improves security

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

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

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

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

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

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

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

Troubleshooting

Argo app error messages

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

Argo app error messages

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

Troubleshooting

Light and acoustic signals

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

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

Technical assistance

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

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

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

ISEO®

www .iseo .com

Iseo Serrature s.p.a.
via San Girolamo 13
25055 Pisogne (BS)
Italy
Tel. +39 0364 8821
Fax + 39 0364 882263
iseo@iseo.com

ISEO Zero1
ELECTRONIC SOLUTIONS