ARGO 3.0 FROM REMOTE USER MANUAL

E N G L I S H

ISEO®

ULTIMATE ACCESS TECHNOLOGIES

About this manual

This manual is about *Argo 3.0* and the remote environment.

Argo 3.0 is the new Argo version updating the previous one (Argo 2.7), and it comes with a new series of *ISEO Smart Devices* embedding the innovative *Bluetooth 5.0* technology. Taking advantage of this technology, *Argo 3.0* combined with the new *ISEO Smart Devices*, allows to **manage the system from remote**. That's why *Argo 3.0* is also called **Argo From Remote**.

To know more about *Argo* and all the standard *Argo* functionalities and related menus, please refer to the *Argo 2.7 User Manual* available at *iseo.com* website, at link:
https://www.iseo.com/data/updati/manuali/ISEOZERO1ELECTRONICSOLUTIONS_SISTEMAARGO_ARGOAPPSISTEMADIGESTIONE/Argo%202.7_User%20Manual_EN_01_20200611.pdf

For all the other related documentation, such as leaflet, brochure, certifications, go to:
https://www.iseo.com/it/en/detail-product/argo-app--management-system

This manual clarifies *Argo 3.0* configuration and features related to the *Basic* and *Advanced* chapters. For the *Basics* section watch the video *Argo 3.0 From Remote Basics*, at link: https://youtu.be/bFrKiuZqZmE

Information icons

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

WARNING: important information for the proper functioning of the system.

NOTE: notes, suggestions and additional information.

IDEA: idea, solution, to make an operation easier or faster.

How to use this manual

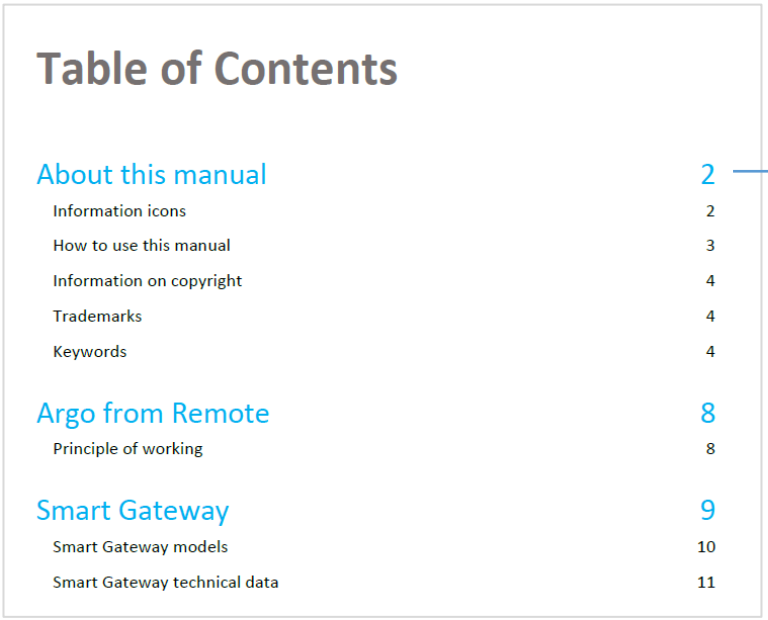


Table of Contents

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

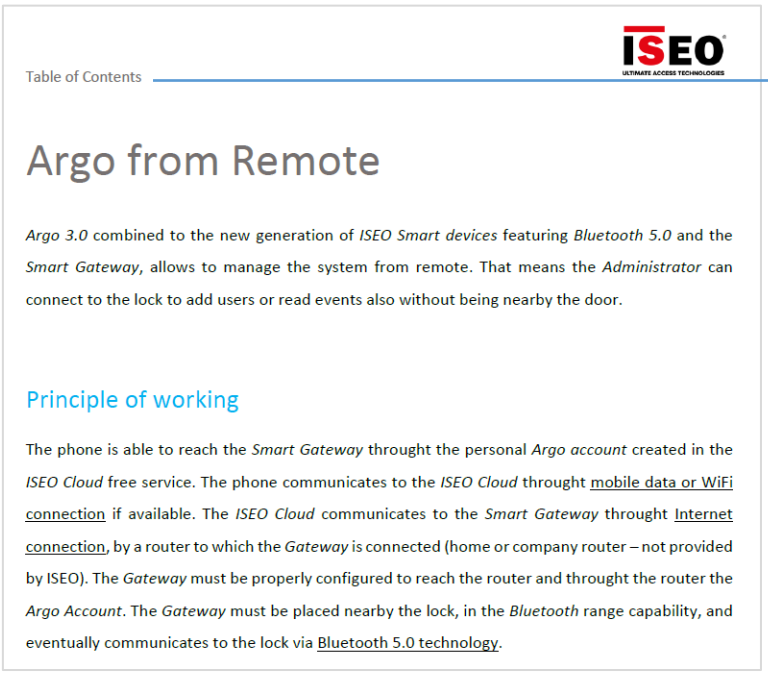


Table of Contents

Argo from Remote

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

Principle of working

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

From any page click *Table of Contents* to go back to the index.

Information on copyright

Trademarks

Keywords

- **Argo Account**: it is fundamental to start-up *Argo from Remote* system. It is first created during the end-user's registration to the *ISEO Cloud* service. It allows to reach the *Smart Gateway* and to manage the system from remote. It is free and to create it a valid email address is mandatory.
- **Argo Local**: when the Administrator or the end-user directly connects to the *ISEO Smart Device* by phone via *Bluetooth*. Local means to be in front of the lock, in the *Bluetooth* range, capable to see in the own smartphone the door-lock list nearby.
- **Argo from Remote**: when the *Administrator* connects to the *ISEO Smart Device* by phone, through the *Argo* Account via data connection, and through the *Smart Gateway* placed nearby the lock. Remote means that the *Administrator* is out of the door-lock *Bluetooth* range capability but can still reach and communicate to the lock by the *ISEO Cloud* service.
- **Bluetooth 5.0**: also called *BLE 5*, it is a new technology that updates the previous *Bluetooth 4.0* and allows multi-channels communication. While *BLE 4* can only communicate to one device per time (single channel), *BLE 5* can communicate to more devices per time. For example: while someone is opening the door-lock with the smartphone, the *Administrator* can connect from remote through the *Smart Gateway*, and the lock will be able to perform both tasks at the same time.

- **Guest Account**: go to *Remote Invited Administrator***.**
- **Houses**: showed in the Argo from Remote user-interface, it means a group of locks and allows to better identify door-locks installed in different locations, in order to organize and tidy-up the *Argo from Remote Home page*.
- **ISEO Cloud**: the free cloud service infrastructure on which *Argo from Remote* works. In order to connect this service an *Argo Account* is first required.
- **ISEO Smart Devices**: the ISEO electronic locks installed in the doors now feature *Bluetooth 5.0* technology. Also called door-locks it is basically the same hardware used in previous *Argo* versions, but with *Bluetooth 5.0* chip embedded in the electronic board. Also the product logo has changed to quickly and easily identify the new technology.
- **Local Administrator**: in the *Argo User List* it is any *Phone User* with LOGIN capability. In fact, LOGIN automatically gives users *Administrator* rights. The *Local Administrator* can therefore login to the door-lock but only in the *Bluetooth* range (*Argo local*).
- **Lock Account Password**: to communicate with the lock by the Argo Account, to open or login, a password is required and it is called Lock Account Password. It is configured during the Argo Account configuration when the lock is added and it is created for each single lock. It can be also associated to the smartphone biometric identification for the best user convenience. By the Lock Account Password, even if someone is able to enter your Argo Account or steal your phone, they could not open or login to the lock from remote, since this password is required at every communication attempt.
- **Remote Owner Administrator**: it is the *Account identity* now present in the *Argo from Remote User List*, the *Administrator* that first created the *Argo Account* to manage the system from remote. This administrator is the owner of the system and owner of the *Smart Gateway* used to connect the locks to the Cloud. He/she can invite other administrators to help him managing the lock from remote (see *Remote Invited Administrator*).
- **Remote Invited Administrator (Guest Account)**: it is another type of *Account identity* in the *Argo from Remote User List*. It is the *Administrator* that has been invited by a *Remote Owner Administrator* to help managing the locks from remote. It is also called *Guest Account* because it is like a guest who uses a *Smart Gateway* to reach locks owned by another administrator: the *Owner Administrator*. Note that the *Invited Administrator* cannot delete the *Owner Administrator* and cannot delete himself from the lock to which it has been invited. He/she needs to ask the *Owner Administrator* for that.
- **Smart Gateway**: the ISEO electronic powered device is able to connect the *ISEO Smart Devices* to the *ISEO Cloud*. It must be connected to a WiFi or PoE router to reach the *Argo Account*, and communicates to the door-locks via *Bluetooth 5.0* technology. It must be installed in the locks *Bluetooth* range and it only works with the *ISEO Smart Devices* featuring *Bluetooth 5.0* technology. It is available in 2 models: WiFi and PoE version.

For more *Argo Keywords*, read the *Argo 2.7 User Manual* available at *iseo.com*.

Table of Contents

Argo from Remote

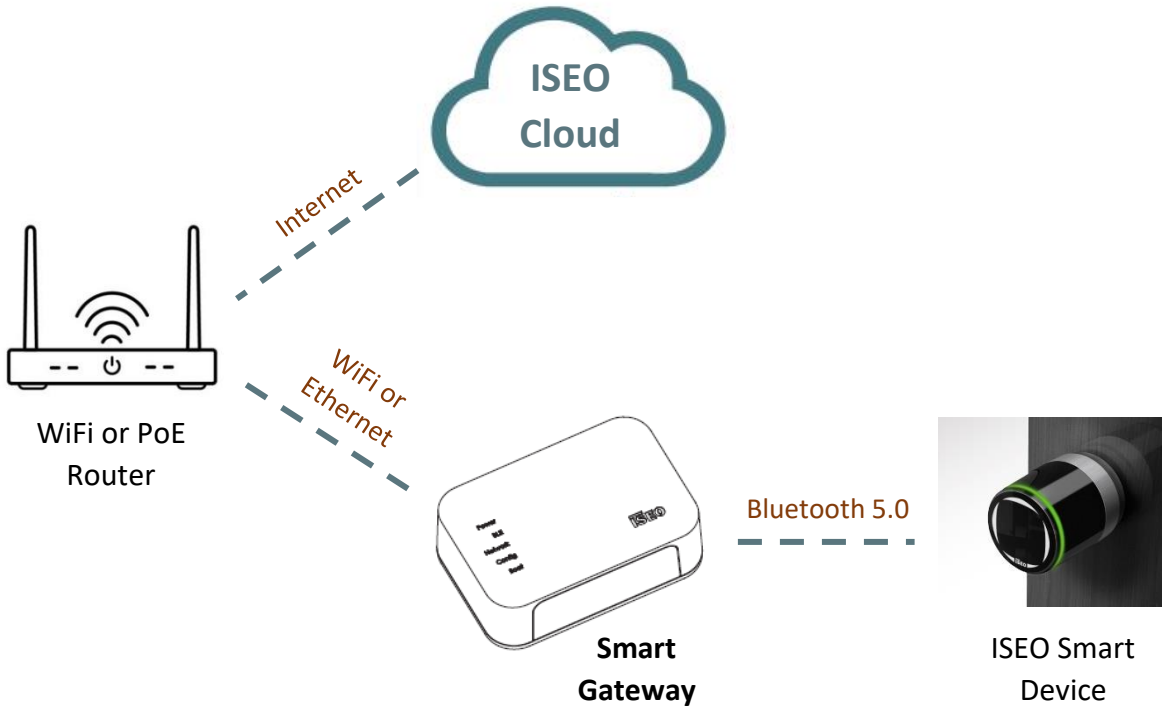
Argo 3.0 combined to the new generation of *ISEO Smart devices* featuring *Bluetooth 5.0* and the *Smart Gateway*, allows to manage the system from remote. That means that the *Administrator* can connect to the lock to add users or read events also without being nearby the door.

Principle of working

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

Smart Gateway

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



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

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

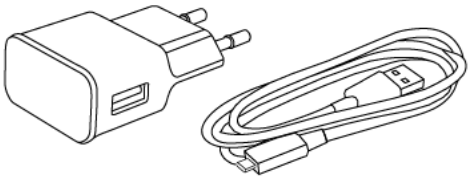
The *Smart Gateway*, by *Linux Operating System* and provided *APIs'*, can be used from *ISEO Argo Developers* (integrators) by the *Argo SDK*, to write their software and their application on it, in the most efficient and simple way. Moreover, *Linux OS* assures stability and greater security from external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

Smart Gateway models

The *Smart Gateway* is available in two models:

WiFi Gateway

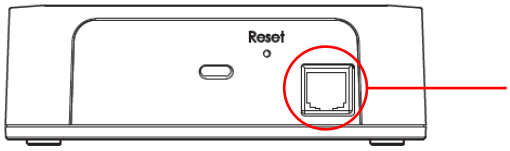
- It requires a WiFi router.
- It must be powered by a 10W power supply unit.



5Vdc – 2A power supply unit.
USB C connector type.

Gateway PoE (Powered over Ethernet)

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



The Gateway PoE is equipped with an Ethernet port on the back.

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

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

LAN cable is not provided by ISEO.

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

Smart Gateway technical data

Features	WiFi	PoE (Power over Ethernet)
Functionality	▪ Converts from WIFI data to BLE 5 ▪ Dual Band WIFI at 2.4 GHz and 5 GHz	▪ Converts from Ethernet to BLE 5
Power Supply	▪ Powered by USB C +5VDC input power 2A (10W) ▪ Power supply not included (accessory to order)	▪ PoE (Power over Ethernet) ▪ Requires PoE Switch IEEE 802.3af up to 15,4W ▪ Delivery of data and power over CAT5e/CAT6 ethernet cable. ▪ Maximum power consumption 10W ▪ Optionally powered by USB C +5VDC input power 2A (10W) ▪ Power supply not included (accessory to order)
Dimensions	▪ 125x40x85mm (LxDxH)	▪ 125x40x85mm (LxDxH)
Operating conditions	▪ Operating Temperature: 0°C/+50°C ▪ Storage Temperature: -25°C/+75°C	▪ Operating Temperature: 0°C/+50°C ▪ Storage Temperature: -25°C/+75°C
Installation	▪ Desktop ▪ Wall Fixing option (accessory to order)	▪ Desktop ▪ Wall Fixing option (accessory to order)
Connection ports	▪ USB C female	▪ USB C female ▪ Ethernet TCP/IP 10/100 baseT
Signalling LEDs	▪ Power (white): ON = Power Supply connected ▪ BLE (white): ON = BLE transmission in progress ▪ Network (white) ON = Gateway connected to Cloud ▪ Config (white): ON = Gateway to be configured ▪ Boot (red): ON = Gateway starting up	▪ Power (white): ON = Power Supply connected ▪ BLE (white): ON = BLE transmission in progress ▪ Network (white) ON = Gateway connected to Cloud ▪ Config (white): ON = Gateway to be configured ▪ Boot (red): ON = Gateway starting up
CPU, Memory, Operating System	▪ ARM A7 based CPU module ▪ 512 MB RAM ▪ 8 GB Flash eMMC Non volatile Memory ▪ Operating System: embedded Linux	▪ ARM A7 based CPU module ▪ 512 MB RAM ▪ 8 GB Flash eMMC Non volatile Memory ▪ Operating System: embedded Linux
Push buttons	▪ Reset (reboot or factory mode status)	▪ Reset (reboot or factory mode status)
OEM version	▪ Available OEM version for Argo Integrators with SDK	▪ Available OEM version for Argo Integrators with SDK

Bluetooth 5.0 ISEO Smart Devices

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

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

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

New aesthetic logo

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

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

Argo & ISEO Smart Devices Logo evolution

Argo 2.7 & Bluetooth 4.0 Smart Devices

Argo 3.0 & Bluetooth 5.0 Smart Devices

Argo 2.7 to Argo 3.0 app logo evolution

Argo 2.7 &
Bluetooth 4.0

Argo 3.0 &
Bluetooth 5.0

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

ISEO Smart Devices logo evolution examples

Libra Smart
Bluetooth 4.0

Libra Smart
Bluetooth 5.0

Stylos Smart
Bluetooth 4.0

Stylos Smart
Bluetooth 5.0

x1R Smart reader
Bluetooth 4.0

x1R Smart reader
Bluetooth 5.0

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

Basics

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

To configure *Argo from Remote* you need to:

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

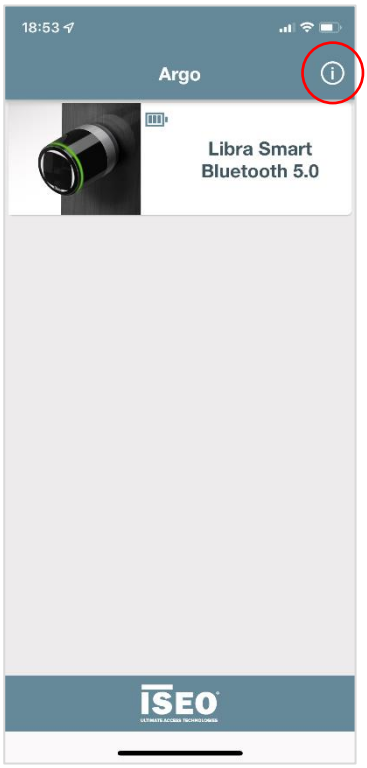
Create your Argo Account

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

1. Start **Argo 3.0**

New *Argo 3.0* icon & logo.

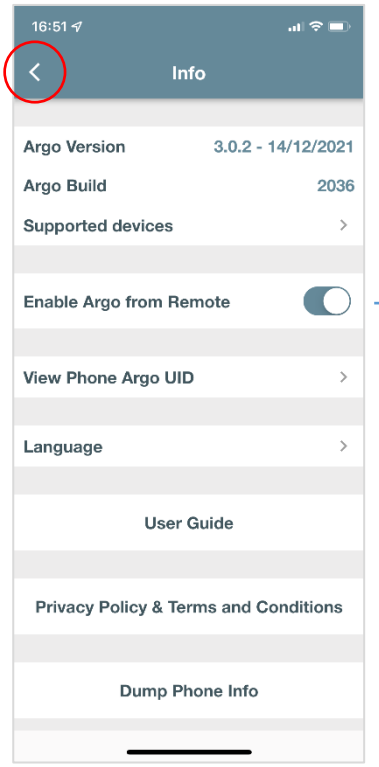
2. Tap the **Info App** menu



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

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

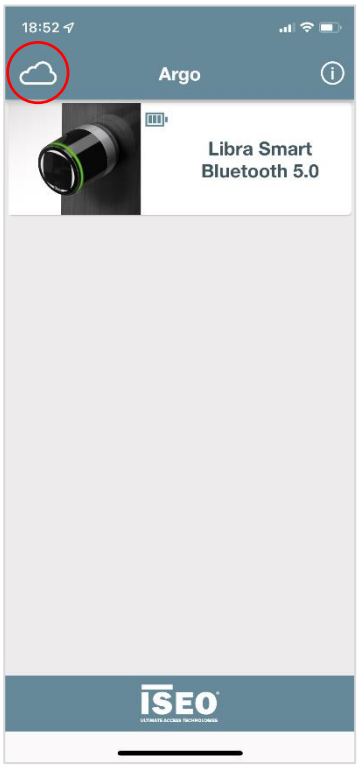
3. **Enable Argo From Remote**, then go back to the main menu.



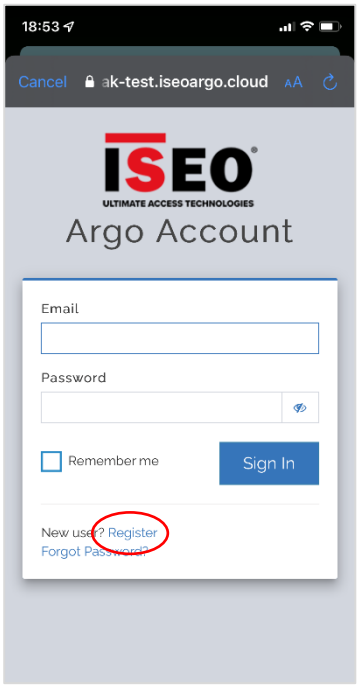
Argo from Remote enabled

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

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

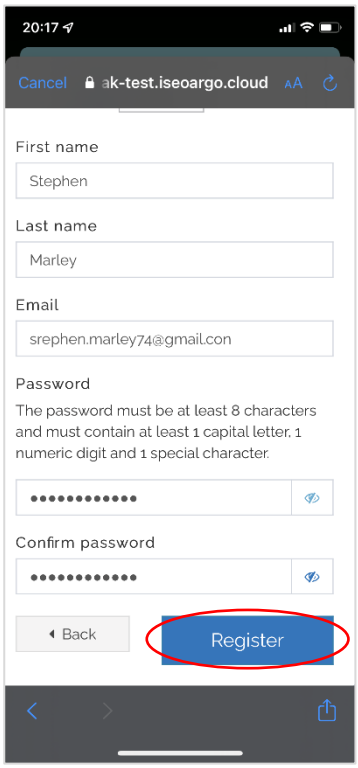


5. Tap **Register** to start a new user registration in the *ISEO Cloud*. Then follow the step-by-step procedure.



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

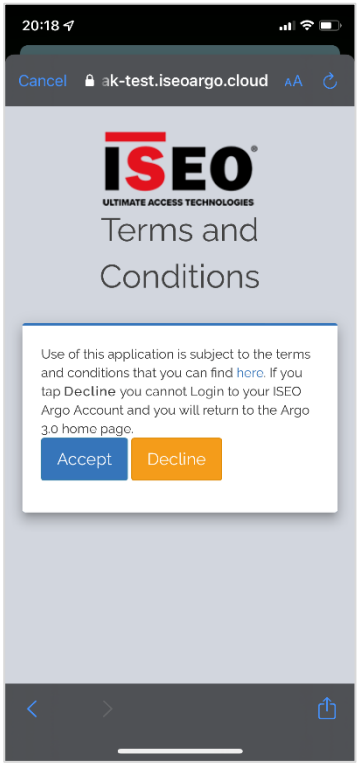
6. Insert all required data and tap **Register** at the end.



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

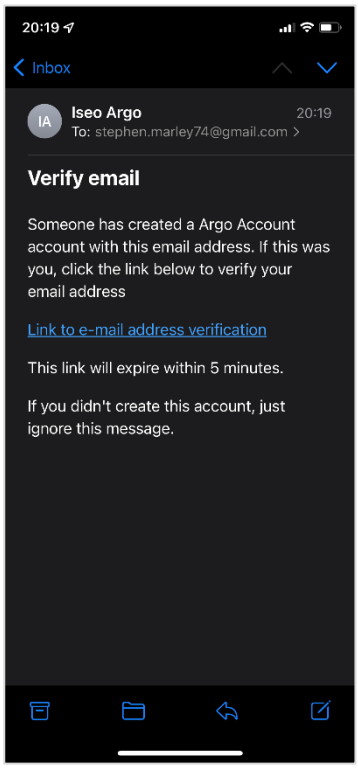
A strong rule password is mandatory.

7. **Accept** the Terms & Conditions.



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

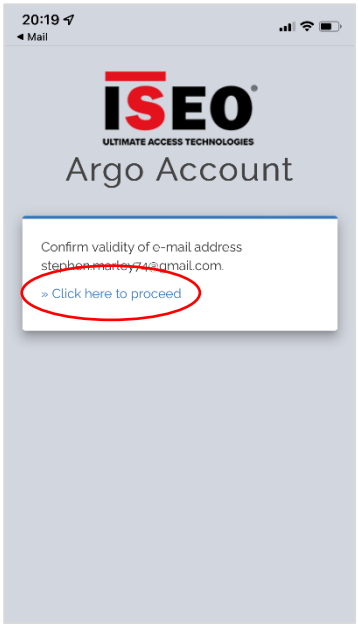
8. Wait the email verification from the *ISEO Cloud service*. Then open it and tap on **the link**.



Tap the link to confirm the email address.

9. Confirm the email address validity and wait for the verification message.

   Then return to *Argo Home page*.

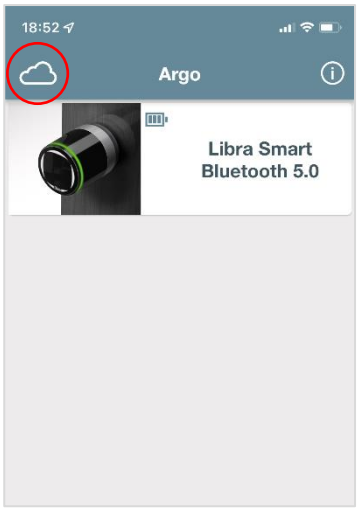


Login to the Argo Account

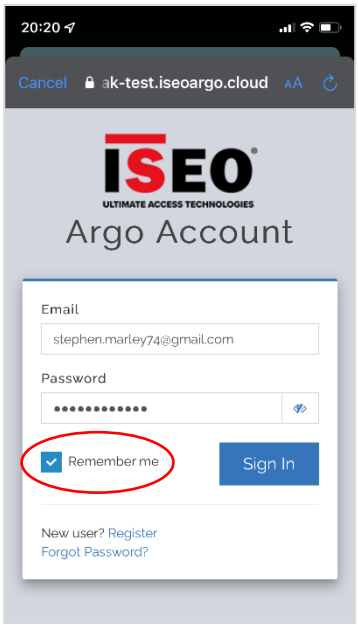
Once your *Argo Account* has been created in the *ISEO Cloud* you can login.

In the *Argo 3.0 Home page*:

1. Tap the **Cloud** icon.



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



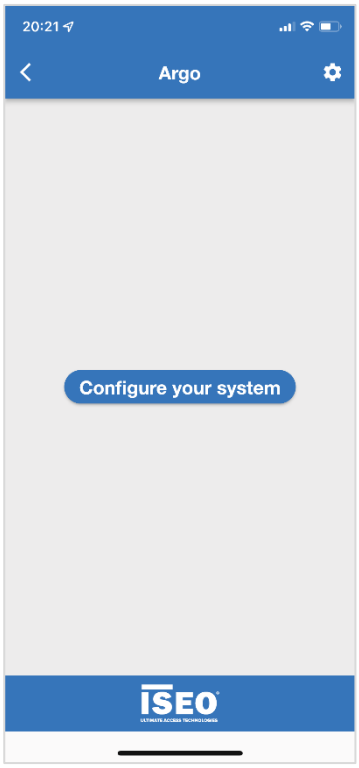
Tap **Sign In** to Login

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

Configure the Smart Gateway

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

1. Tap **Configure your system**.



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

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

Smart Gateway's boot keeps about 1 minute.

Step-by-step configuration wizard.

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

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

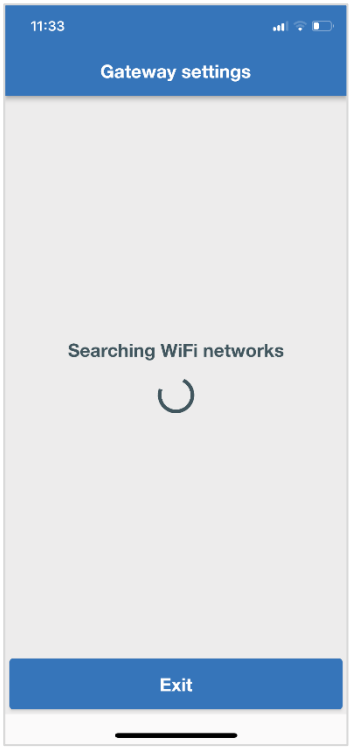
There are two *QR-Codes* on the back of the Gateway:

- Product Serial Number
- Registration Code.

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

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

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

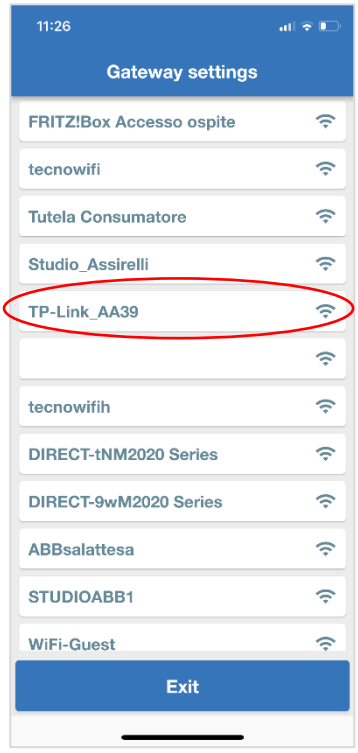


In case of *Smart Gateway PoE* go to step 7.

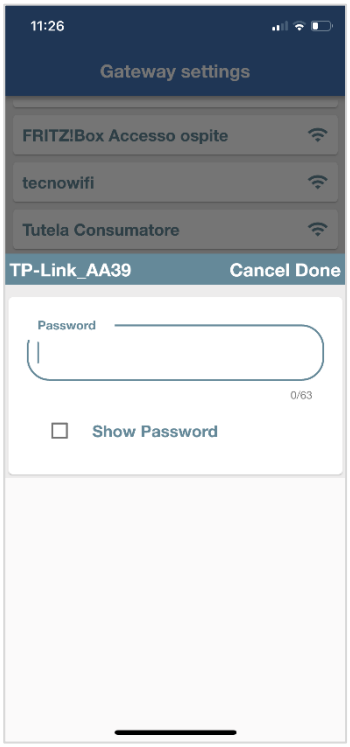
Steps 4, 5 and 6 are only valid for the *Smart Gateway WiFi*.

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

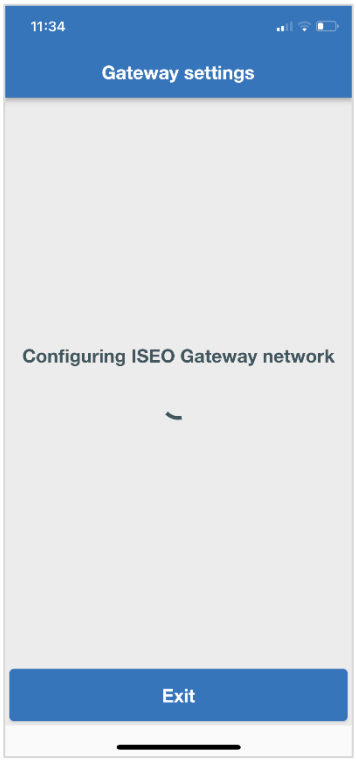
5. Choose and tap the **WiFi network** provided by your router.



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



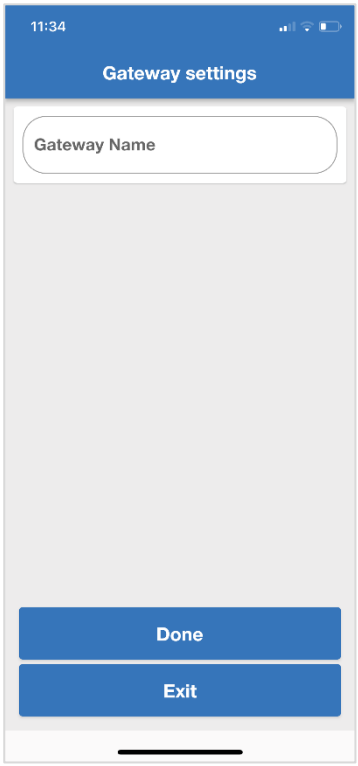
7. Wait the *Smart Gateway* network automatic configuration.



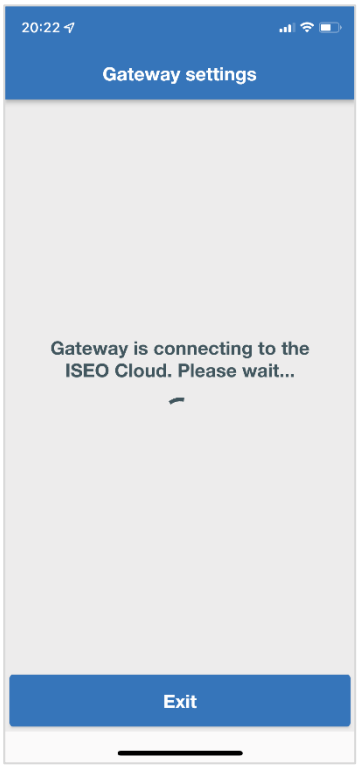
At this stage the Gateway is connecting to your router WiFi network. If an error occurs repeat the process and double-check the router password.

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

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



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



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

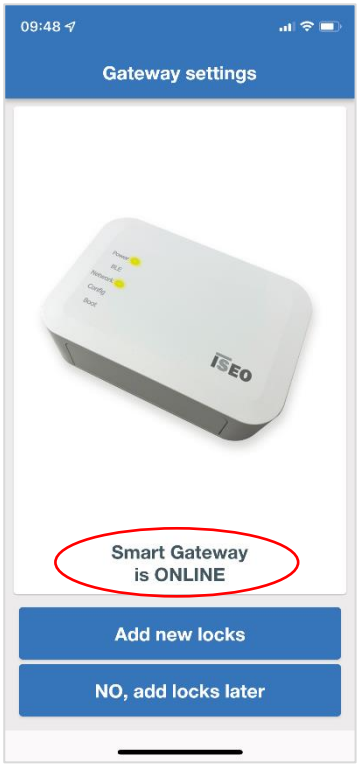
- No internet connection.
- Slow internet connection (network latency).
- Error in communication due to router settings or Firewall.

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

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

10. When the *Smart Gateway* connects to the *ISEO Cloud* a successful message is shown:

    Smart Gateway is ONLINE. You can now add locks to the system.



Add locks to the system (Master Card required)

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

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

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

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

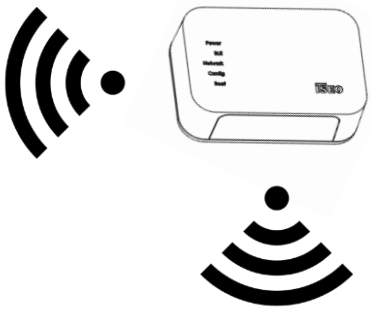
The unique limit is the distance between *Gateway* and devices that must not exceed on average about 10mt, which may vary depending on the environmental conditions: wall thickness, corners, electromagnetic noise around, *Gateway* installation place, position and height.

Gateway Installation example

Door with *ISEO Smart Devices* installed on it.

Bluetooth 5.0 range (about 10mt)

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



WiFi range

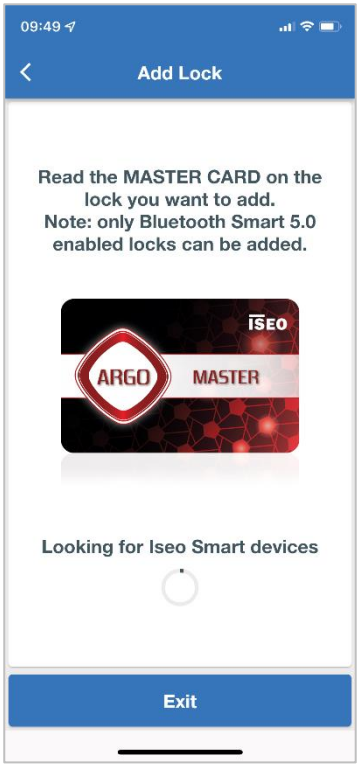
WiFi router

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

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

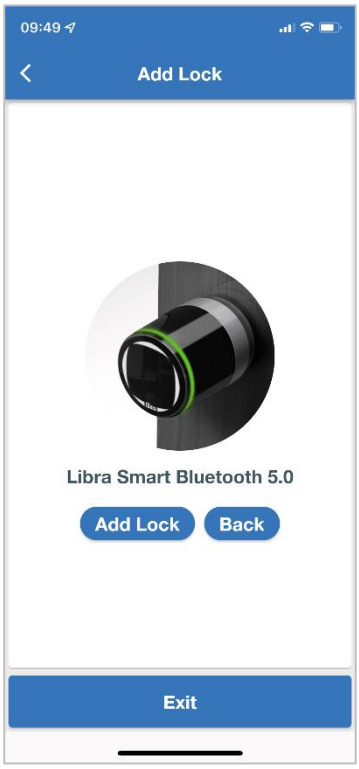
You can also add locks later, by the related menu reachable in the *Argo from Remote Home page*. To know more about the menu functions, go to *Advanced* chapter.

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



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

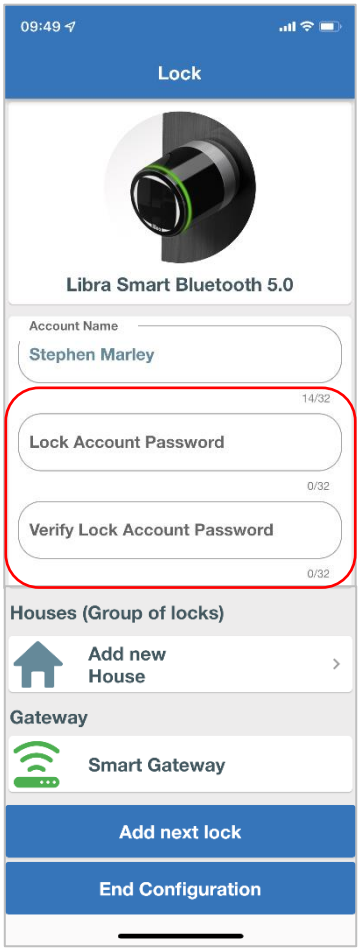
3. Tap **Add lock** to confirm and wait for the lock configuration.



The lock name is automatically taken by *Argo Local*.

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

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



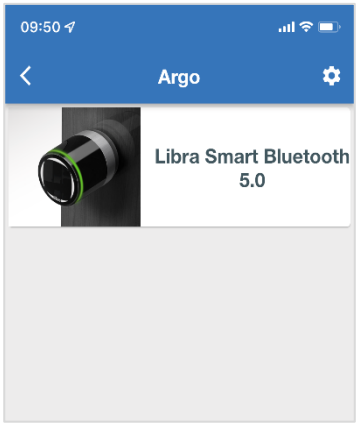
The password can be automatically associated to the smartphone biometric identifications (fingerprint or face-id), for the best user experience and convenience.

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

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

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

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



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

Connect to the lock from remote

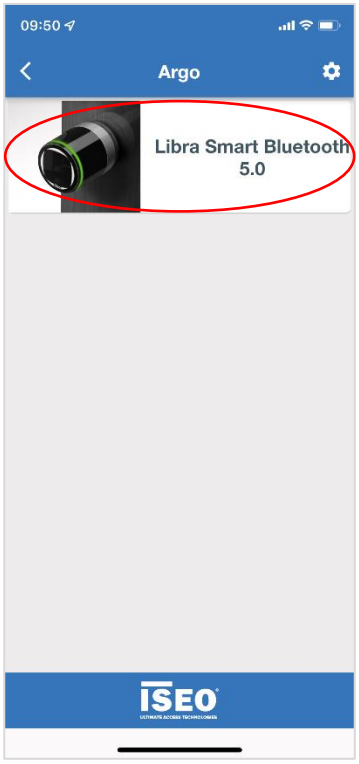
Once the *Argo Account* has been created, the *Smart Gateway* has been configured and the lock has been added to the system (see *Basics*), you can now connect from remote to the *ISEO Smart Device* to perform the next operations:

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

Open the lock from remote

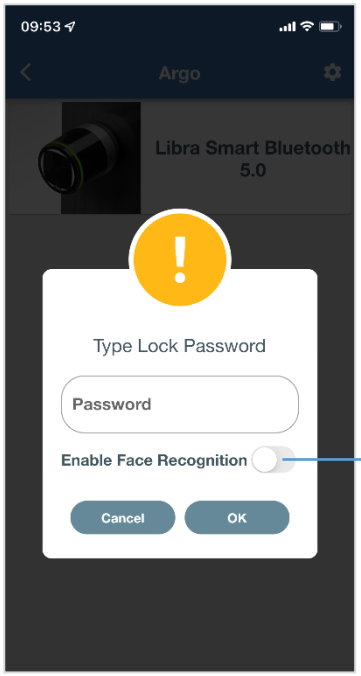
With *Argo 3.0* is possible to open a door from remote. This can be useful in case of specific needs or emergency, for example if you need to let someone enter the door when you are not inside or nearby. To do that *Login* to the *Argo Account* (see *Basics, Login to the Argo Account*) and follow the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

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



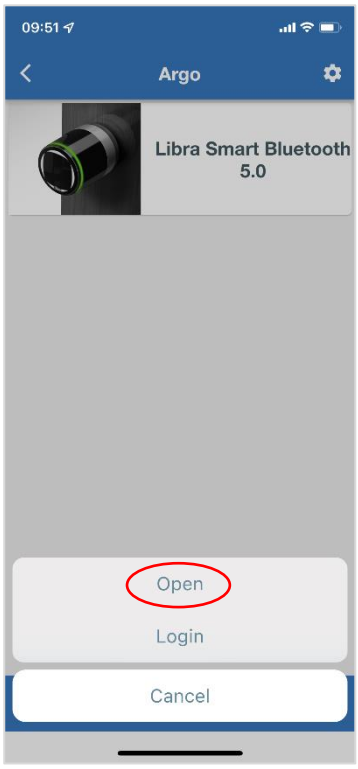
On *Argo from Remote* the *Tap & Hold* function used in *Argo Local* to show the additional functionalities, is not present. Whether you tap one time or tap & hold, the result is the same: the app always shows the enabled functions.

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



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

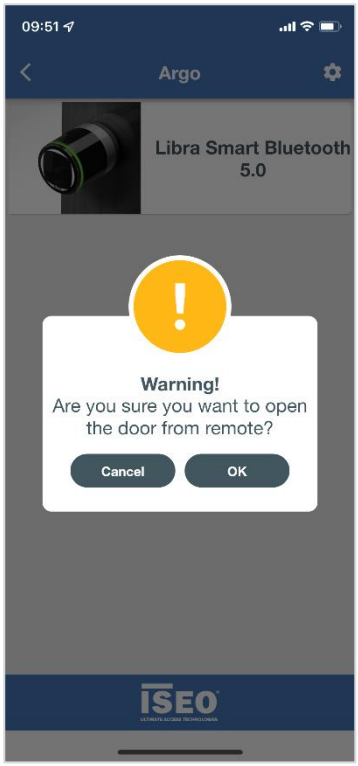
3. Tap **Open**.



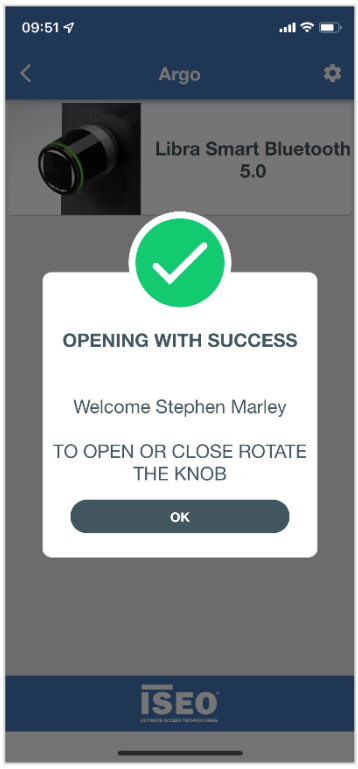
Login is always present by default because it is the basic requirement for the *Administrator* to manage the lock from remote.

The *Remote Owner Administrator* has the *Open* function by default.

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



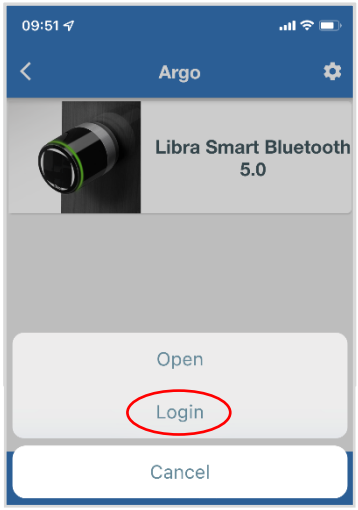
5. Wait for the opening successful message.



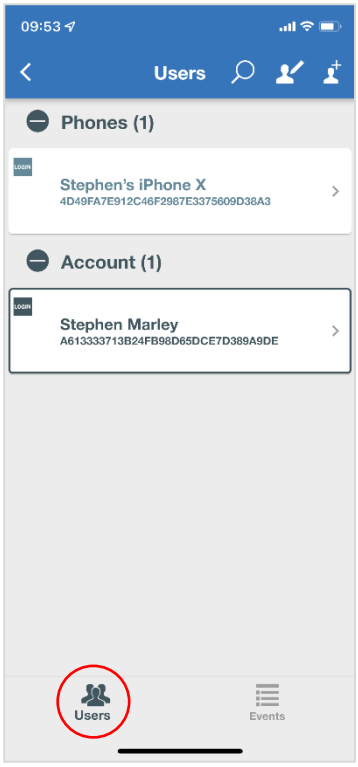
Login to the lock from remote

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

1. Tap **Login**



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



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

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

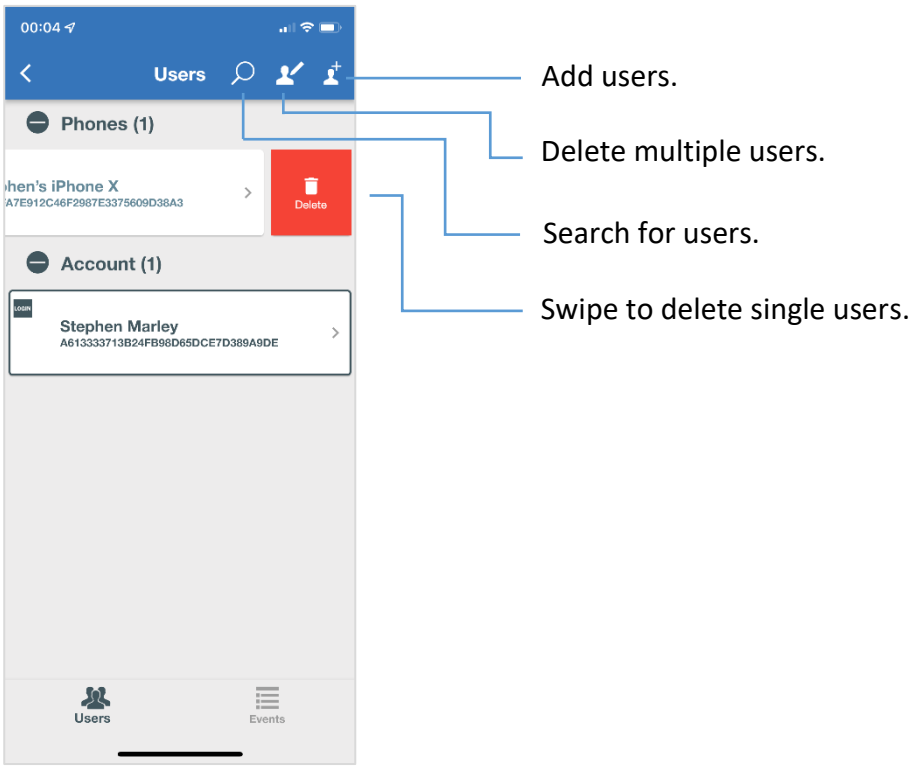
An *Administrator* can be only *Local* and not *Remote* or vice-versa; or he could have both identities, like in the above example. *Local Administrator* cannot login from remote and vice-versa.

After login you can:

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

Add, edit or delete Users

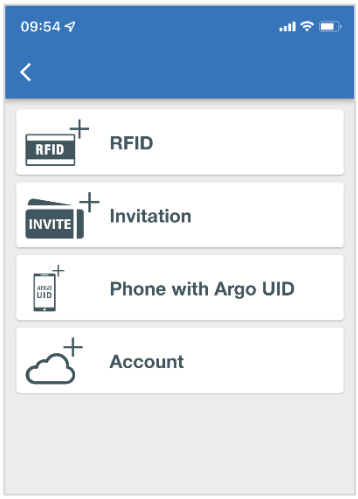
Like *Argo Local* you can search, add, edit or delete users but from remote.



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

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

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

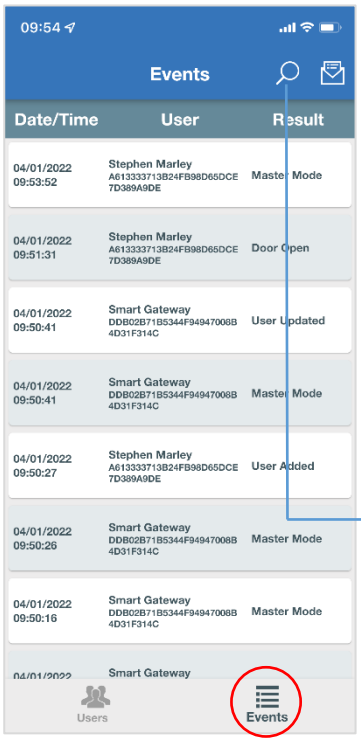


In this example the *ISEO Smart Device* is a Libra Smart, therefore we cannot add PIN codes.

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

Read the History events

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



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

Differently from *Argo Local* you cannot send all events in one shot, but just the ones pre-loaded in the phone memory.

Scroll down the event list to show more events. All the showed events can be sent via email.

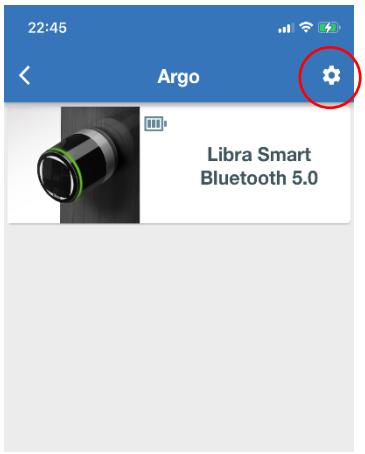
Tap to open the search box tool to search events by *Date/Time*, *User* or *Result*, even with just some letters or numbers (partial words).

Advanced

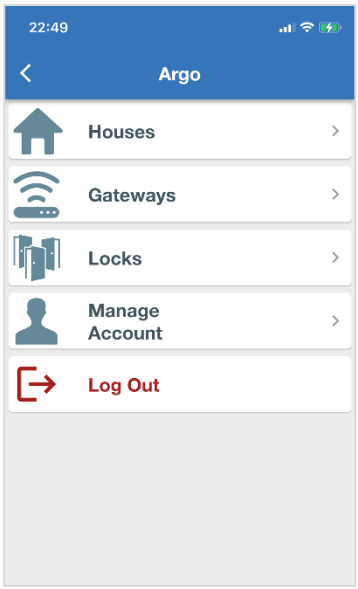
In this advanced section you can find the *Argo from Remote* menu explanation and all the related functions. After the menu overview, each function is also individually explained.

Argo from Remote menu overview

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



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



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

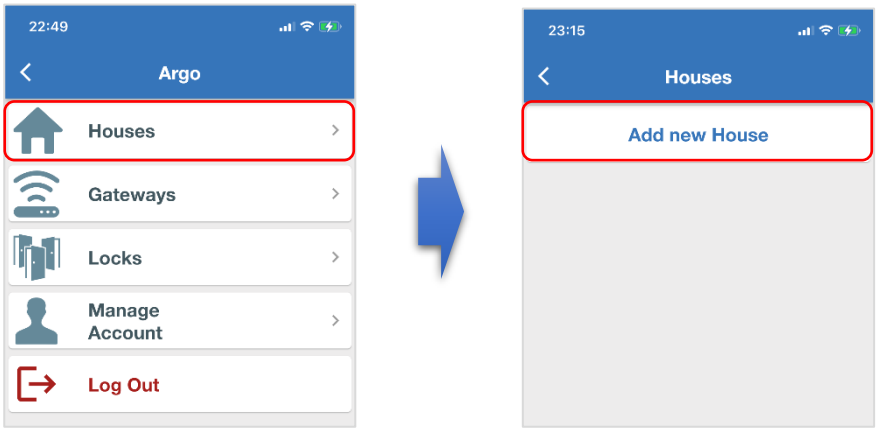
Account logout

Houses

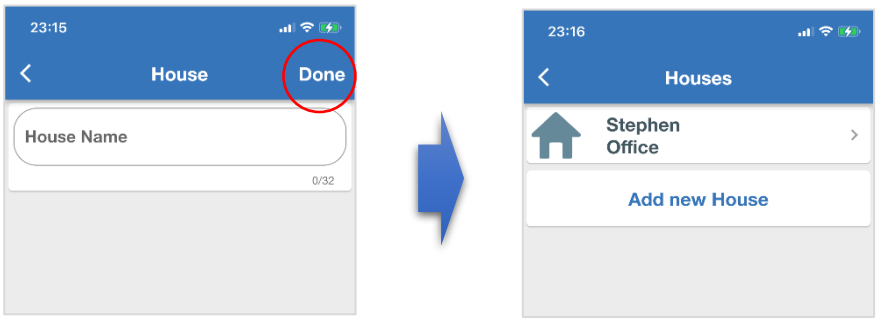
In this menu you can add a new *Houses* or manage the existing ones (delete or rename).

To add a new **House**:

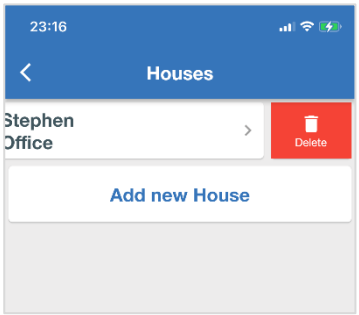
1. Tap **Houses** and then tap **Add new House**.



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



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



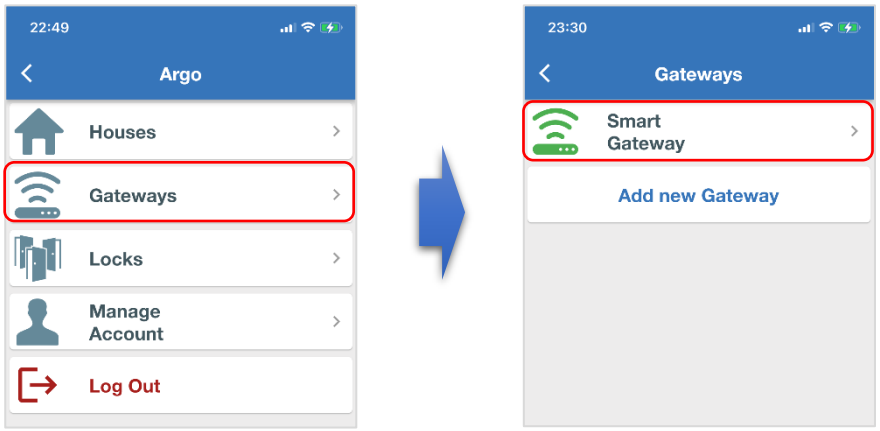
4. To rename a *House* simply tap on the *House* name to enter edit mode and rename it.

Gateways

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

To see **Gateway** info:

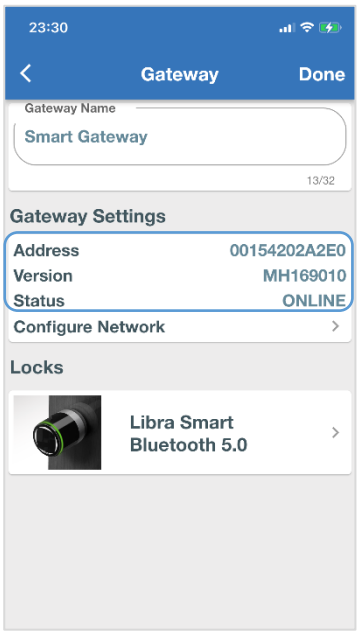
1. Tap **Gateways** and then tap on the gateway name.



A green coloured *Gateway* icon means that the *Gateway* is online. A red icon means *Gateway* offline (not connected to Internet).

Tap **Add a new Gateway** to start the wizard previously showed (go to *Basics*, *Configure the Smart Gateway*)

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



Tap to rename the gateway.

Gateway software information.

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

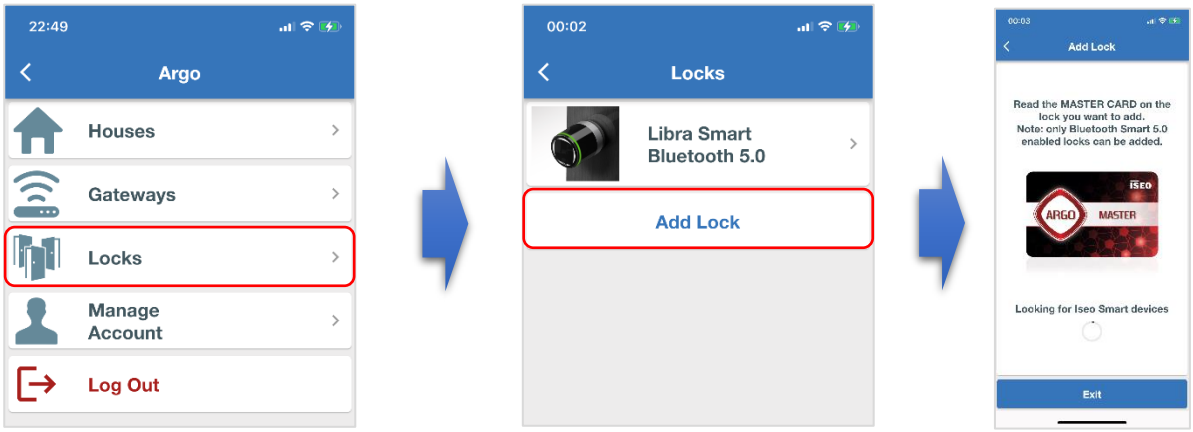
Lock connected to this Gateway. Tap the lock name and icon to directly enter the *Locks* menu, also reachable from the main menu (see *Locks*).

Locks

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

Add a new Lock

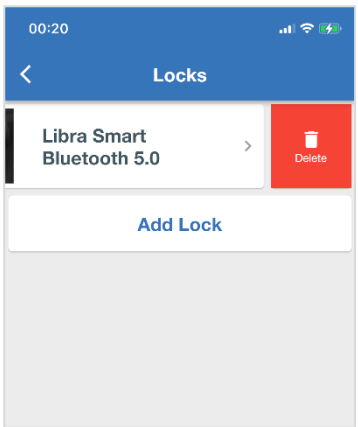
- Tap **Locks** and then tap **Add Lock**. It will start the same wizard previously described (go to *Basics*, *Add locks to the system*).



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

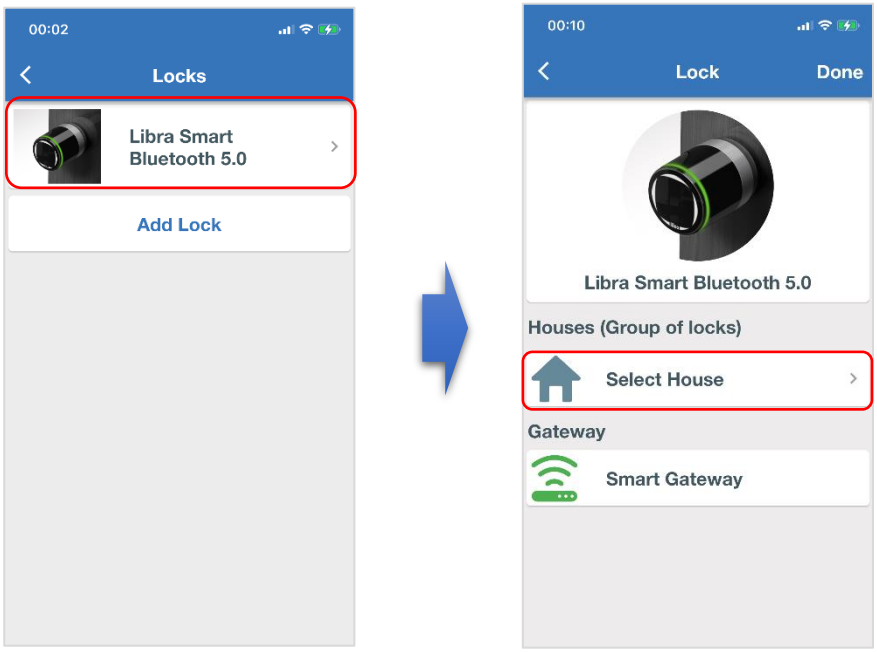
Delete a lock

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

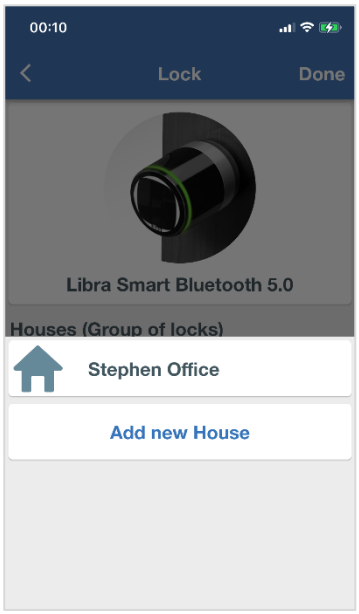


Assign locks to House

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



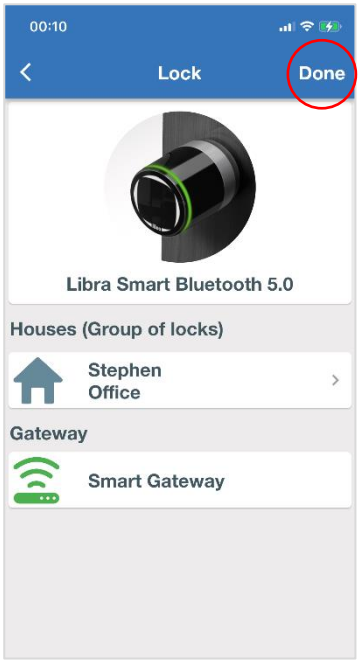
2. Choose the *House* to assign (i.e. Stephen Office) or **Add a new House** to create a new one.



House previously configured in the system.

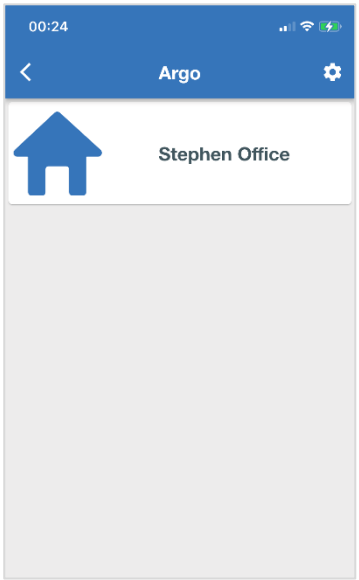
It is also possible to create Houses during the first system configuration (*Basics, Add locks to the system*), or directly in the *House* menu.

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



House assigned to this lock.

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

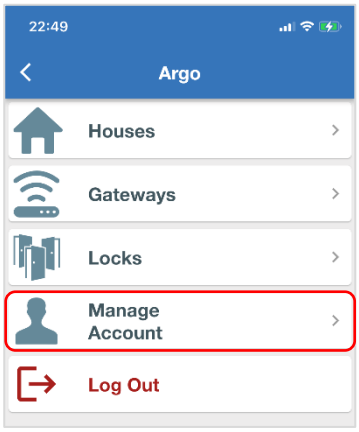


Home page: the lock now is "inside" the *House*. Tap the *House* name and icon to see the locks belonging to this house.

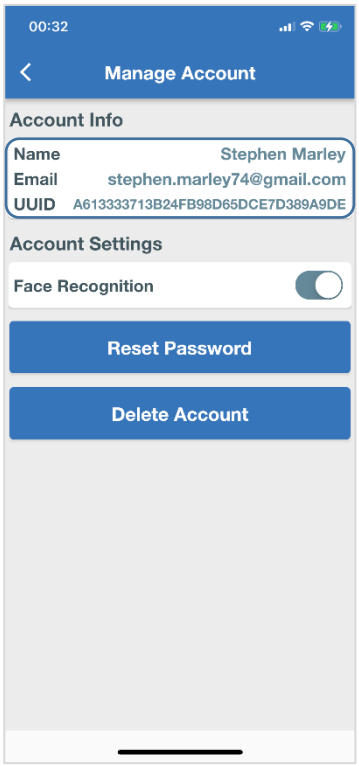
Manage Account

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

1. Tap **Manage Account**.



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



Account info.

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

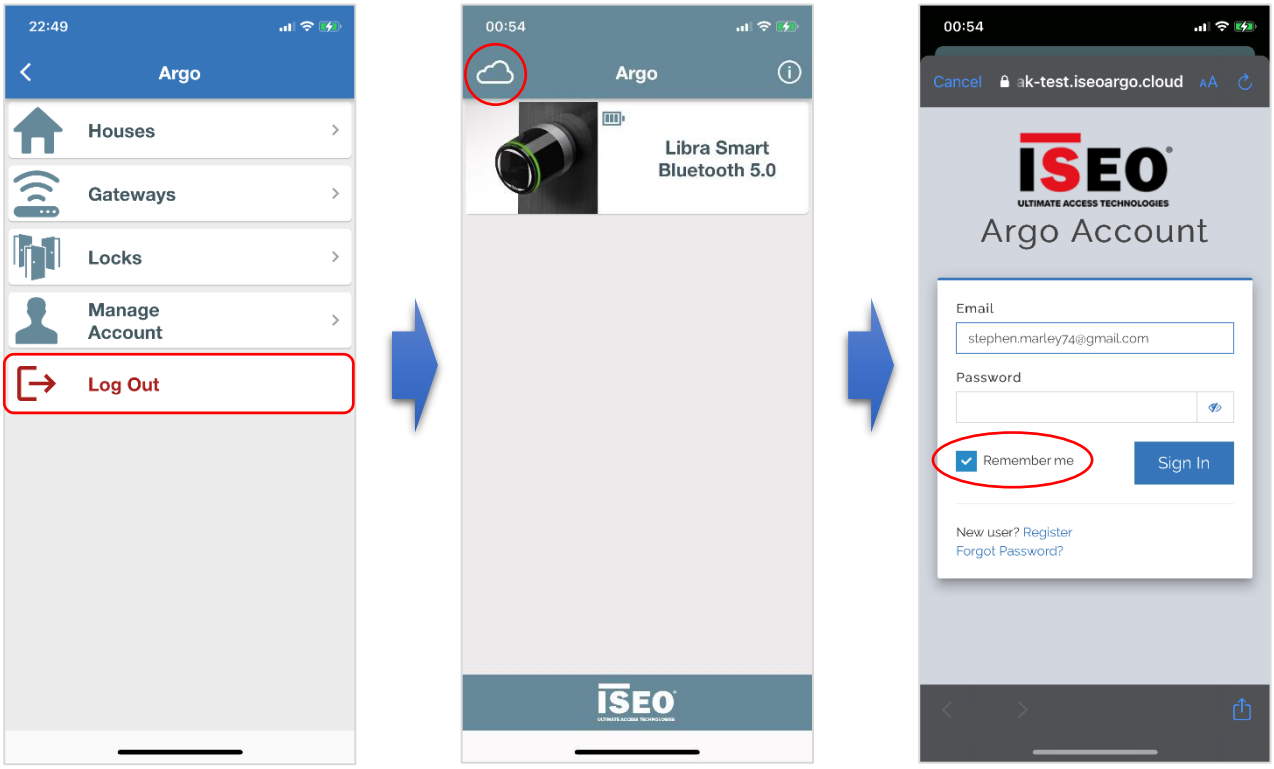
Tap to reset your account password, then follow the step-by-step instructions.

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

Log Out

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

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

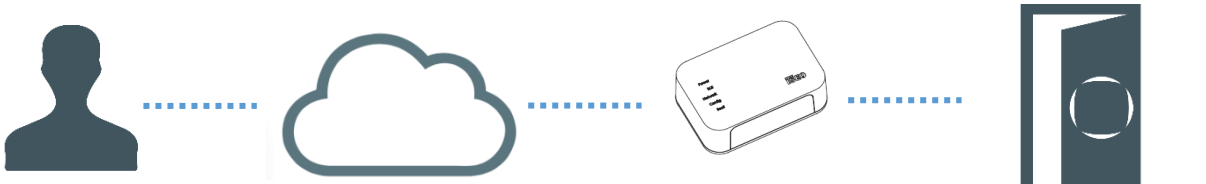


Log Out overrides the *Remember me* function; so it can be useful for security reasons to be sure nobody can enter your account even if someone gets hold of your phone.

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

Account user

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



Account User the Remote Administrator of the lock, also owner of the Smart Gateway

Argo Account in the ISEO Cloud

Smart Gateway configured in the Argo Account

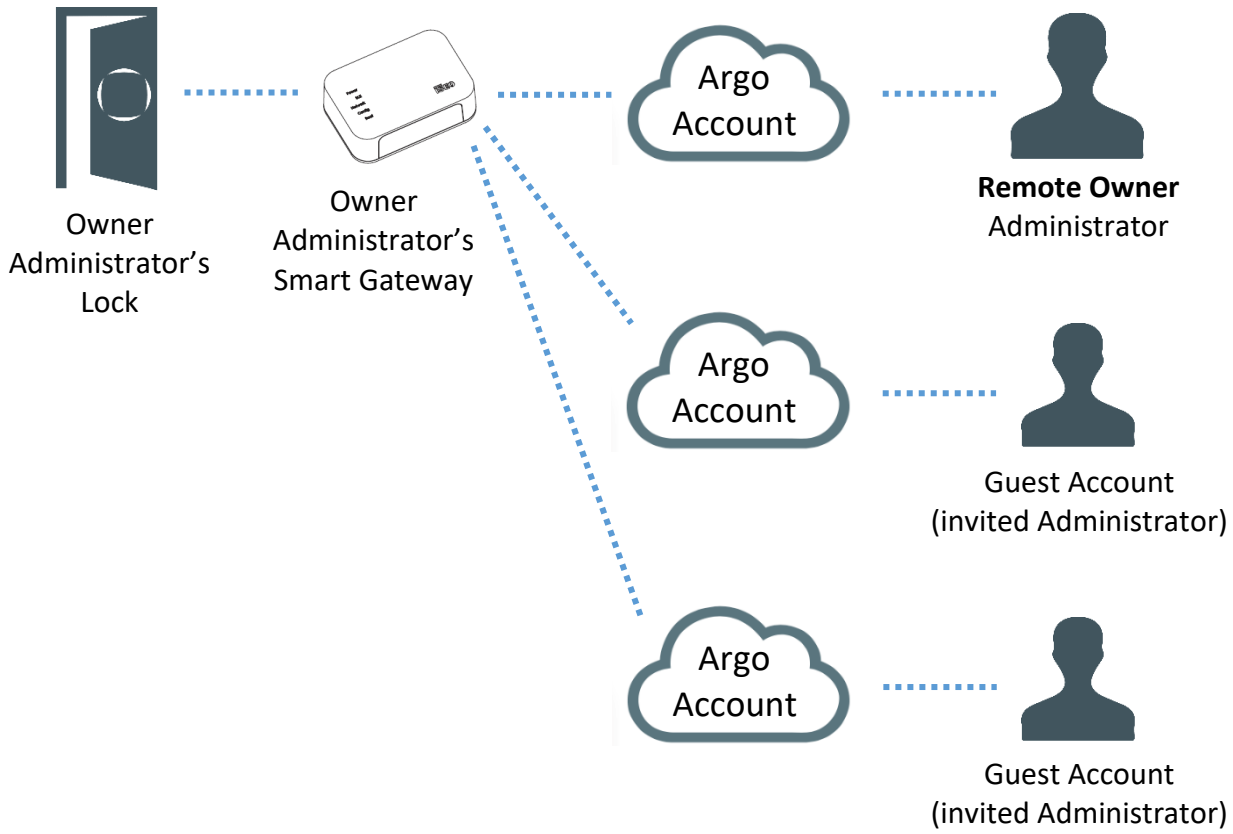
Door-lock added to the Argo Account

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

Guest Account

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

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



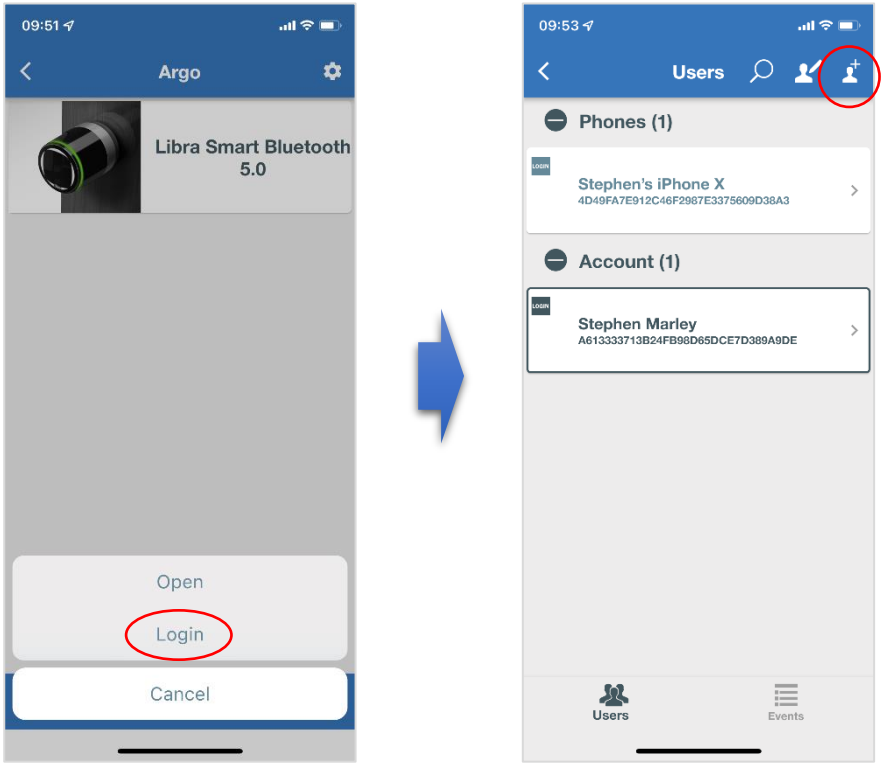
Argo from Remote, differently from *Argo Local*, gives the possibility to assign different *Administrator's permissions* to the *Guest Account* (to find out more go to *Add Account*).

Add Account (invite Remote Administrator)

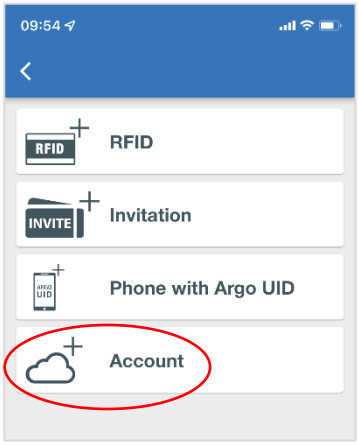
The *Remote Owner Administrator* can add one or more *Administrators* to help him managing the lock from remote. This function is called *Add Account* and allows to invite a new *Remote Administrator* called *Guest Account*. To add a *Guest Account* to the lock, proceed as follows.

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

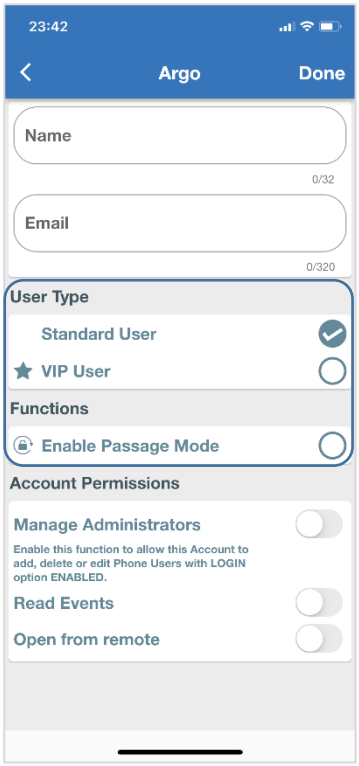
1. Login to the lock then tap **Add User**



2. Tap **Add Account**



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



Guest account name.

Guest account email address.

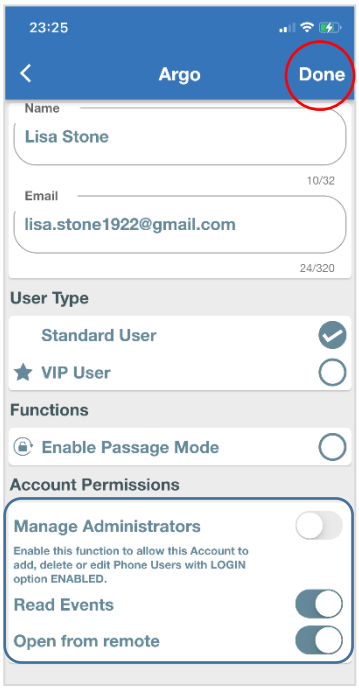
Standard Argo functionalities (to know more read the *Argo 2.7 User manuals* at *iseo.com*).

Go to *Manage Administrators* paragraph.

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

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

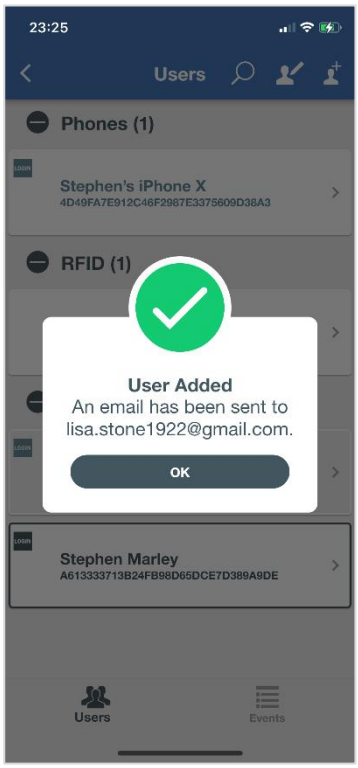
4. Tap **Done** at the end.



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

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

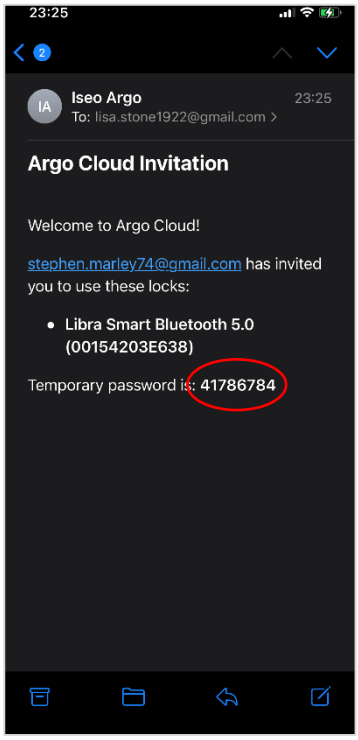
5. Wait the **User Added** confirmation message, then tap **OK**.



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

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

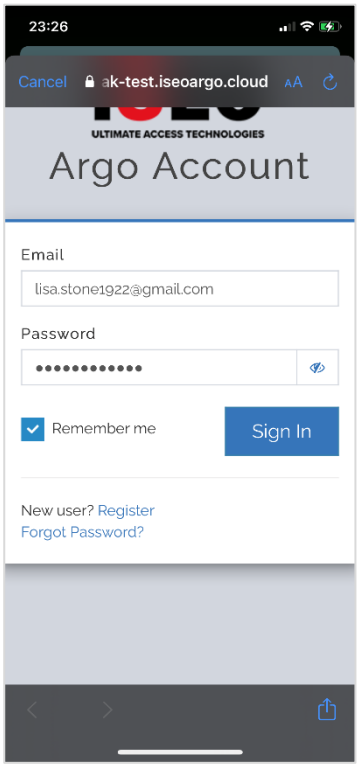
1. The *Invited Administrator* receives an email like the example below.



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

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

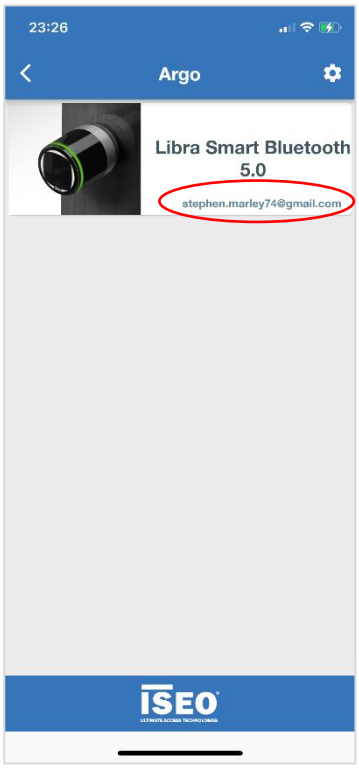
2. The *Invited Administrator* logins to its *Argo from Remote Account*.



The *Invited Administrator* must have a valid *Argo Account* in the *ISEO Cloud* otherwise he/she cannot be invited from the *Owner Administrator* (to find out how to set up a new Account go to *Basics, Create your Argo Account*).

It is possible to create an *Argo Account* without having any *Smart Gateway* and locks configured.

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

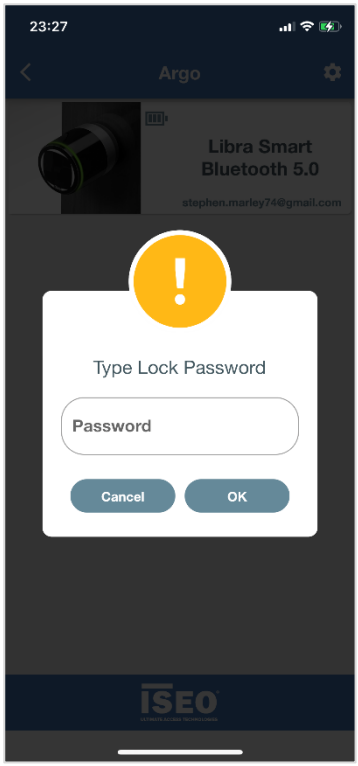


The new lock belonging to the *Owner administrator* Stephen Marley, now appearing in the Lisa Stone *Account home page*.

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

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

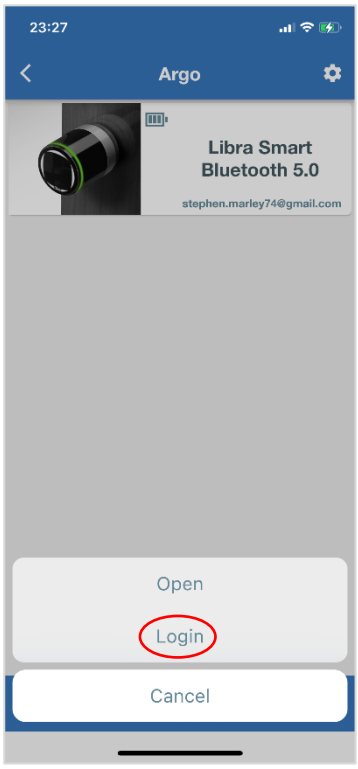
4. Tap the lock name and icon to start the communication. The temporary *Lock Account Password* is required to connect to the lock.



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

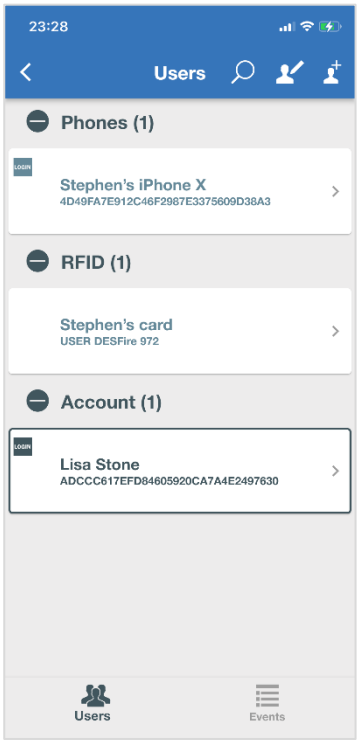
Enable *Face or Fingerprint* recognition in the *Manage Account* menu to associate the password to your phone biometric identification.

5. Tap **Login**.



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

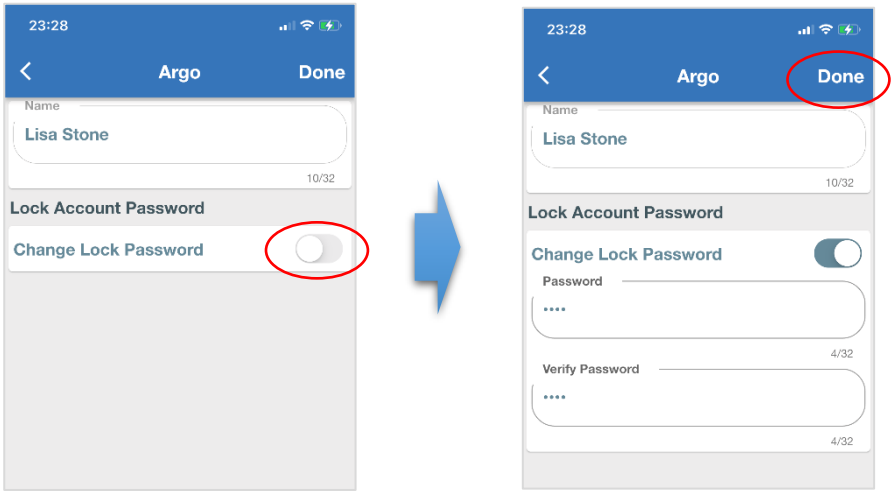
6. *Argo from Remote* **User List** appears.



Guest Account

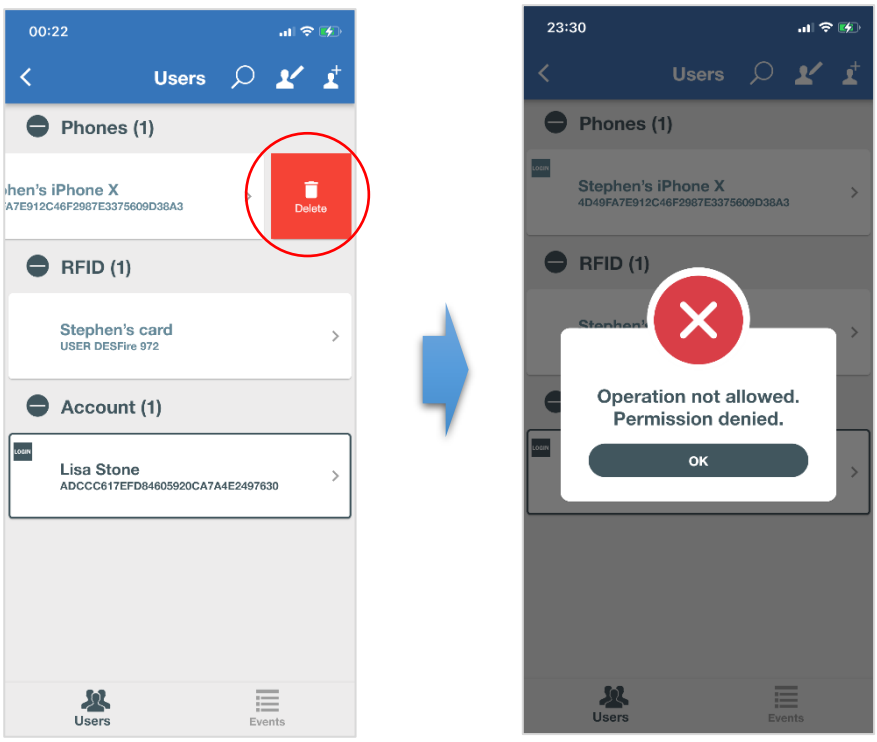
The *Owner Administrator* account is not visible from the *Guest Account*. The latter in fact cannot change any setting of the lock owner.

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



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

8. Considering the *Account Permissions* set by the *Owner Administrator*, Lisa Stone can *Open from Remote* and *Read Events*, but she cannot *Manage Administrators*. That means she cannot add, delete or edit *Phone Users* with login. For example: if Lisa Stone tries to delete the *Phone User Administrator Stephen's iPhone,* she will get the error message as per picture below, and the operation will not be completed.



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

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

Delete the Account

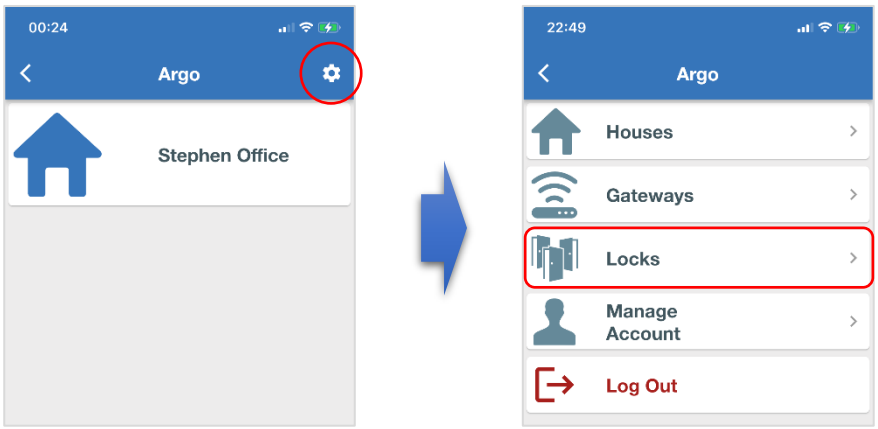
Delete an *Account* is a critical operation since it involves all configured *Gateways* and *Locks*. An *Account* might also have one or more *Guest Accounts* sharing some of its locks.
To summarize, before deleting an *Account*, we need to take into consideration:

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

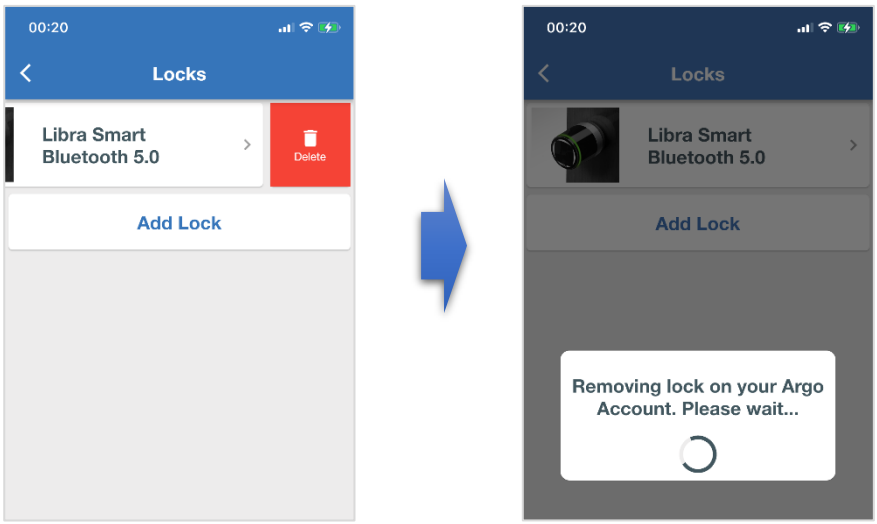
Only the *Owner Administrator* can delete his/her *Account* and the invited *Guest Accounts*. If the *Owner Administrator* deletes the *Account*, all the *Guest Accounts* belonging to it will be automatically deleted.

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

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



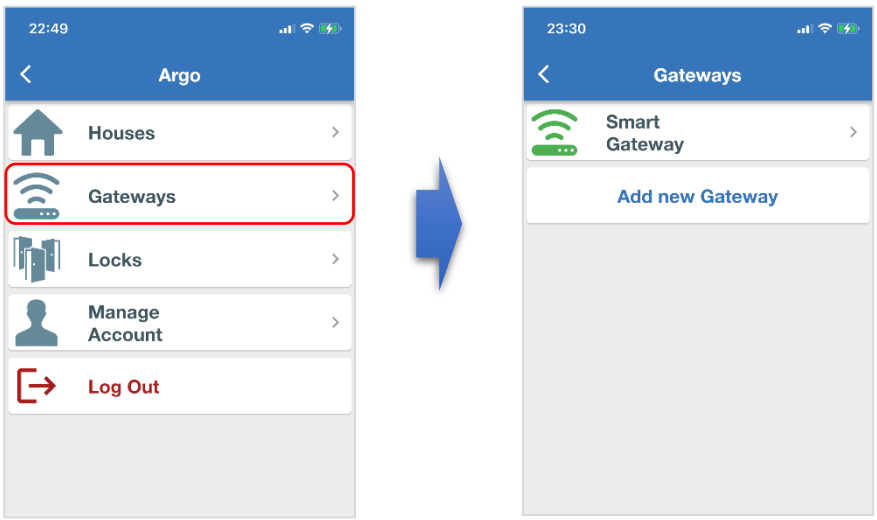
2. Delete all the **Locks** one by one, providing the lock password or by phone biometric identification.



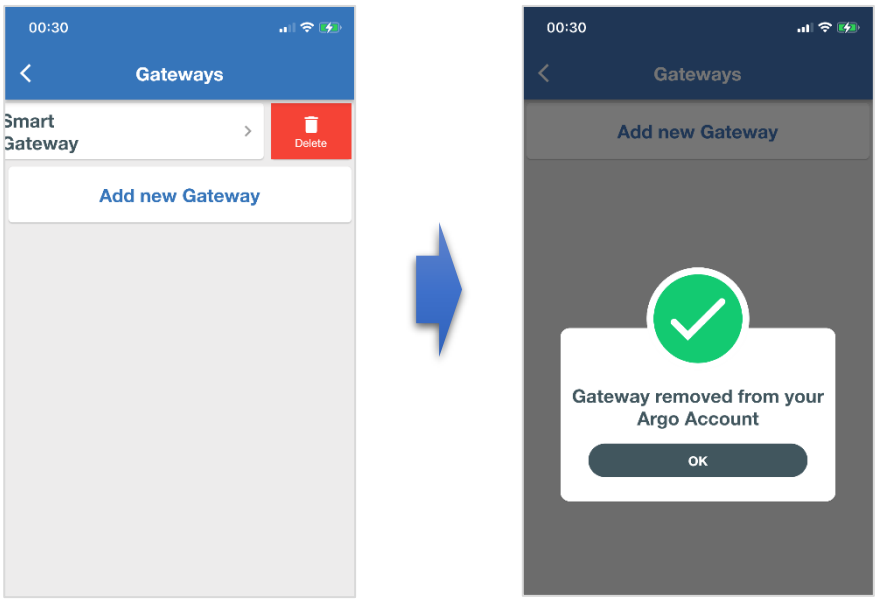
Removing a *Lock* from the *Owner Administrator Account*, the lock will be automatically removed from all the *Guest Account* invited, if any.

The same happens when the *Owner Administrator* deletes the *Guest Account* from the Lock.

3. Go back to the main menu, then tap **Gateways**.

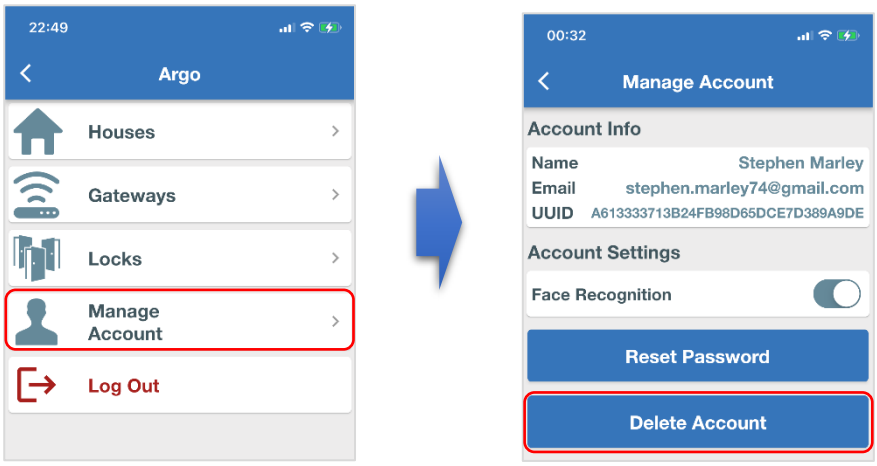


4. Delete the **Gateway**, always swiping from right to left, and confirm the message.

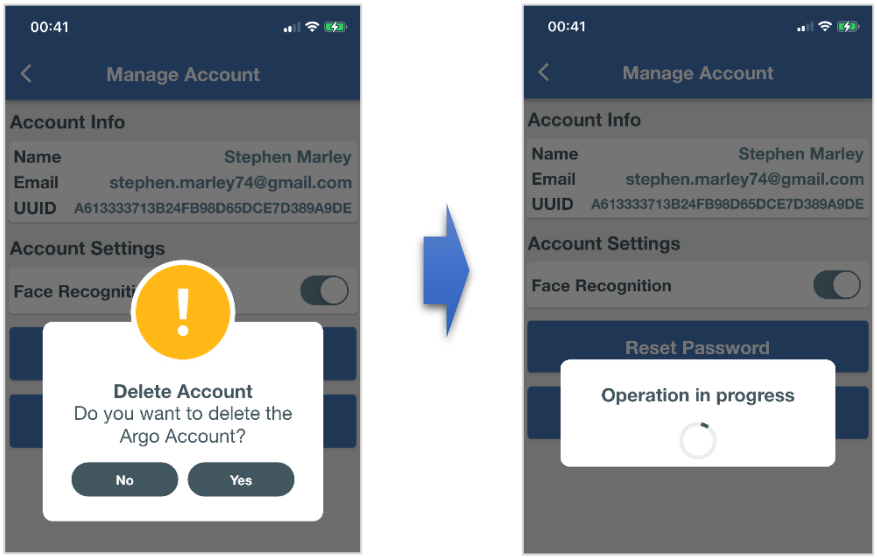


A **Gateway** connected to a *Lock* cannot be removed and the app will give an error message. Be sure all the *Locks* have been deleted before deleting a *Gateway* (for more info about errors go to *Troubleshooting*).

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



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



Any **Houses** will be automatically removed during the *Account* cancellation.

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

Questions & Answers

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

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

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

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

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

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

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

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

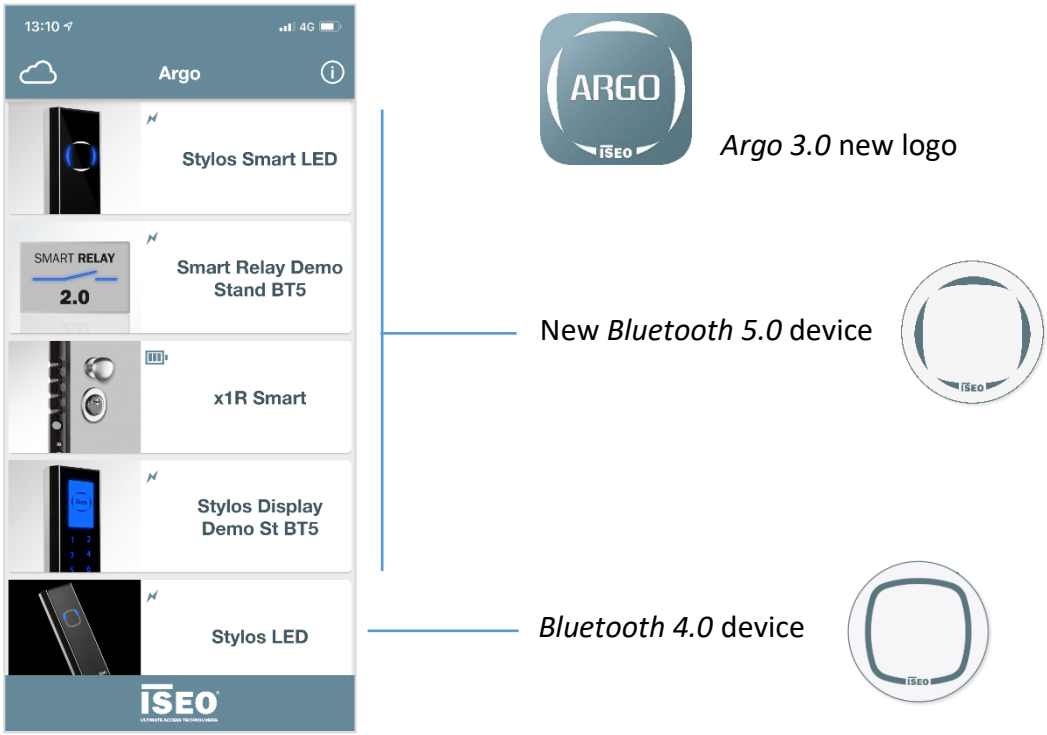
   Answer: yes, you can add more *Gateways* to your *Argo Account*, to reach different locks far away from each other.

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

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

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

   Answer: you can recognize it by the new logo design, aimed to show the *Bluetooth 5.0* technology evolution. The new logo is printed in all the *BLE 5 ISEO Smart Devices* aesthetic covers. It is also possible to recognize *Bluetooth 5.0 ISEO Smart Device* by the Argo app: the new devices come up in the *Home screen* with a new icon showing the new logo design.



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

   Answer: no, all the *Bluetooth 4.0 ISEO Smart Devices*, except *x1R Smart*, cannot be upgraded to *Bluetooth 5.0*. It is necessary to replace the entire device to manage it from remote. *x1R Smart* is the unique exception because this lock is composed by 2 devices: the mechanical lock inside the door and the credential reader, that embeds the *Bluetooth*, usually placed on the outside of the door. To upgrade *x1R Smart* to *Bluetooth 5*.0 you need to:

   - Replace the entire reader with a *Bluetooth 5*.0 version.
   - Upgrade the *x1R Smart* firmware by a service app called *ISEO App Tool.* Tutorial video available at link: https://www.youtube.com/watch?v=WOgmzzra0f8

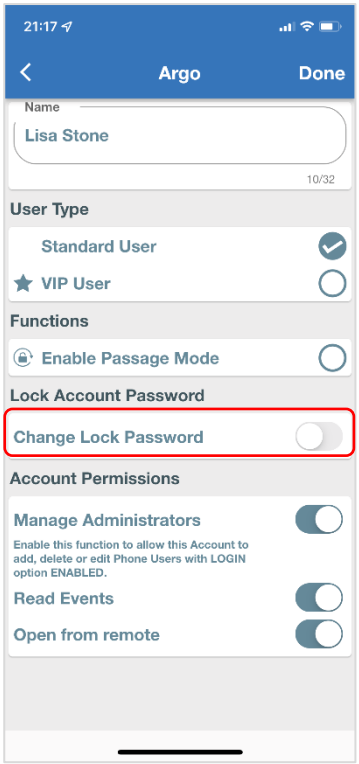
   This operation is only intended for competent and properly trained installers or staff.

8. *Argo Local* allows 300 *Users* to be memorized in the door-lock. What happens when I add a *Gateway* and the *Lock* in the *Argo Account*? Does it change the *Users* capability of the *Lock*? **Answer**: yes, during the configuration the *Gateway* and the *Owner Administrator Account* are registered in the *Lock* memory. These are considered 2 credentials: that's why the users' capability changes. For example: if 300 *Users* then becomes 298 *Users*. This is due to the principle of working of Argo called *data on device*. And this is also the strongness of Argo about security: the *Gateway* is just used as a tunnel; all the data are in the most secure place, inside the lock.

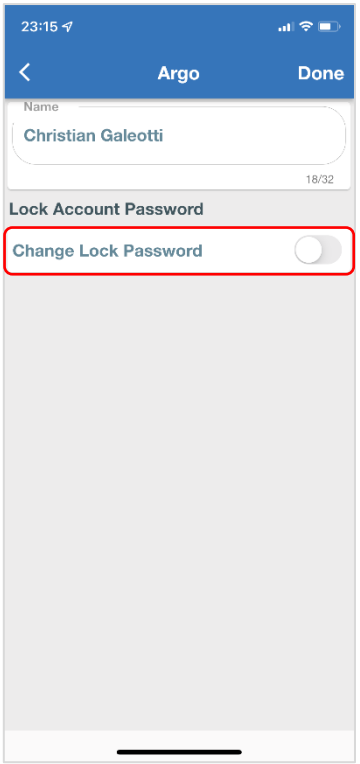
9. Where can I change the *Lock Account Password*? I cannot find it.

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

Lock Password - Owner Administrator Account setting



Lock Password - Guest Administrator Account setting



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

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

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

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

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

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

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

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

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

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

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

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

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

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

17. Can I change the lock name from remote?

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

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

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

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

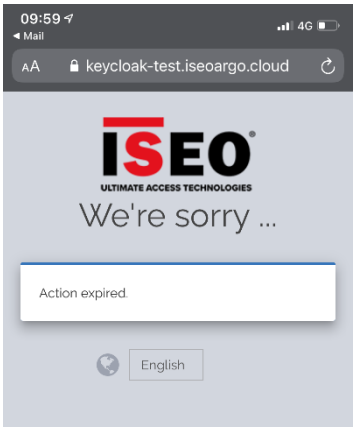
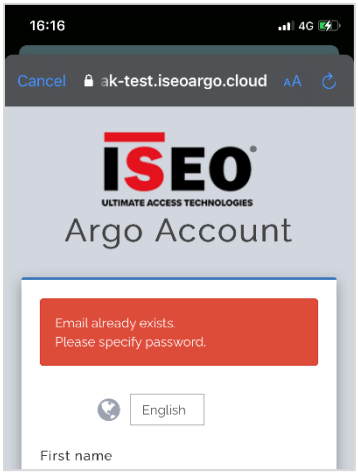
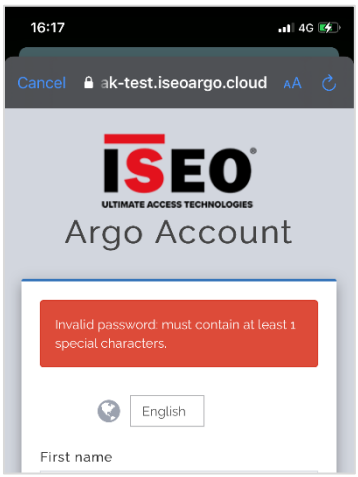
    Answer: yes, anyone can open an *Argo account*. It is just required a valid e-mail address and a free-choice password. For example: an administrator invited by the owner must necessarily register an *Argo account*, even if he does not own any system. This in order to be able to manage the lock to which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

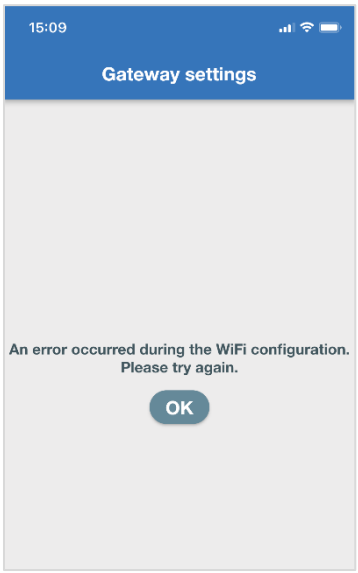
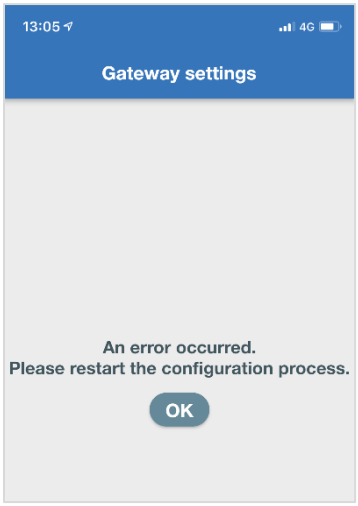
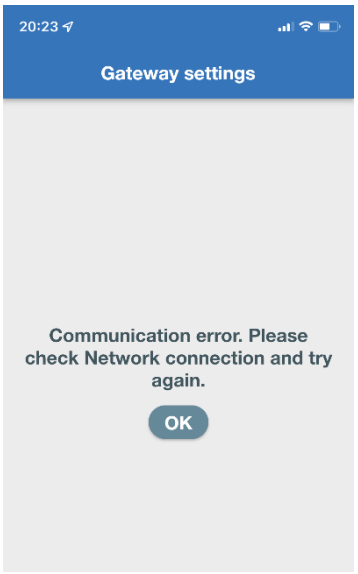
20. Is it possible to share the same *Gateway* between different *Argo accounts* owners with different system codes (*Master Card*)? This is the case, for example, of the common door of a condominium shared between the various apartments, where each apartment is a distinct Argo system.

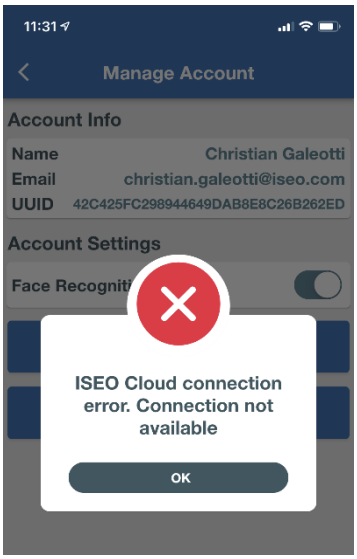
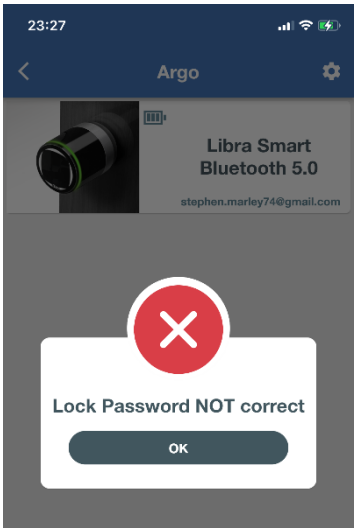
    Answer: no, for security and reliability reasons of the system and of the software structure, a *Gateway* is assigned to a single system and the owner administrator is unique. The owner administrator can still invite other administrators to manage the lock. In the case of the example of the common door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

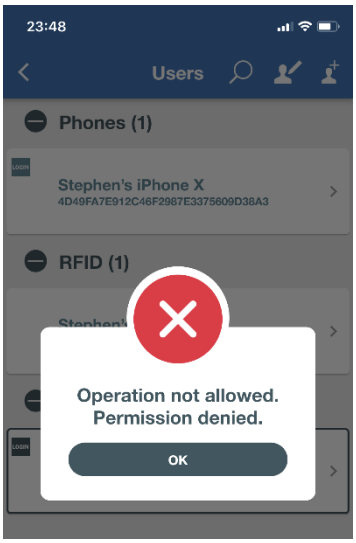
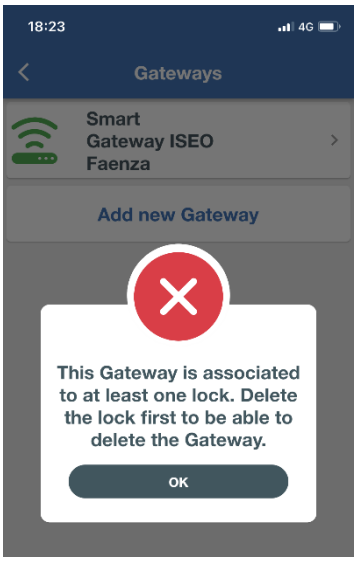
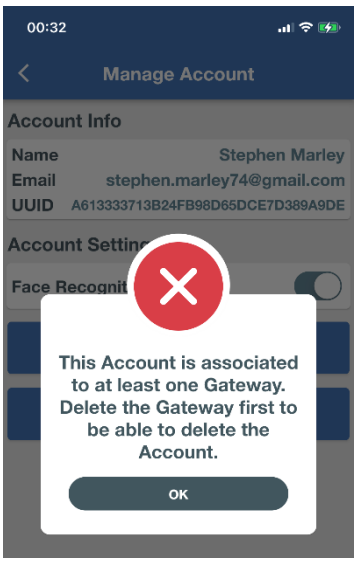
Troubleshooting

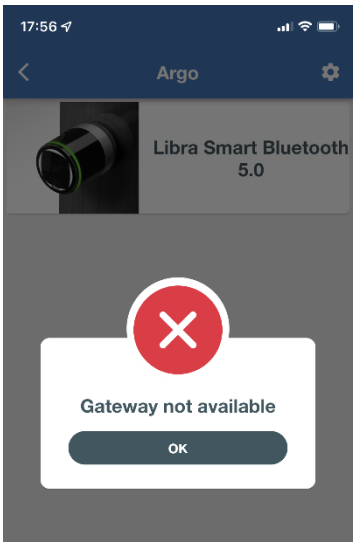
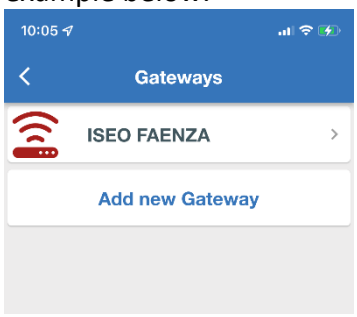
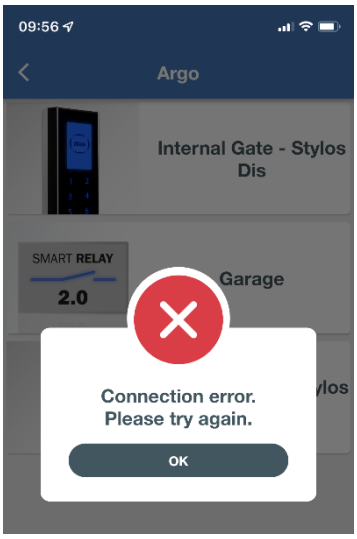
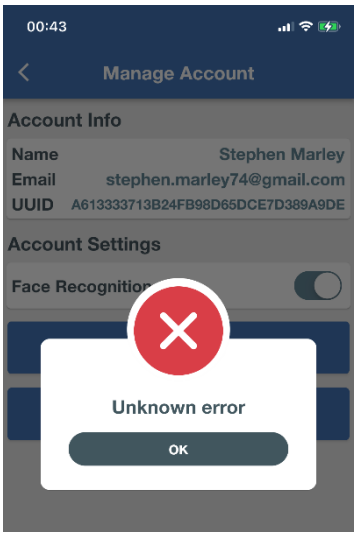
See below the most common errors messages and the related explanation.

Error	Meaning	What to do
	You took too much time to complete a step in the Account registration procedure. For security reason there is a time-out and once expired you get this error message.	Repeat the operation faster.
	You inserted an already existing email during the Argo Account registration.	Choose a different email address to register a new account or use the already existing one.
	You didn’t type a strong rule password.	Please type a password with at least 8 characters that contains 1 capital letter, 1 number and 1 special character.

Error	Meaning	What to do
	This error could happen during the Gateway configuration, at the 1st step, when the Gateway is trying to connect to the WiFi router. This usually means wrong router password inserted.	Tap OK to restart the process and try again. Take care to insert the correct router password. Use the password view function to double-check the password. If the problem persists check your WiFi router if reachable by any other device (PC, Smartphone, tablet). If the problem cannot be solved, please contact the *ISEO Service Operation Center* (go to *Technical Support*).
	This error could happen during the Gateway configuration, at the 1st step, when the Gateway is trying to connect to the WiFi router. The password is correct but for some reason, the router rejected the Gateway connection.	Tap OK to restart the process and try again. If the problem persists check your WiFi router if reachable by any other device (PC, Smartphone, tablet). If the problem cannot be solved, please contact the *ISEO Service Operation Center* (go to *Technical Support*).
	This error could happen during the Gateway configuration, at the 2nd step, when the Gateway is trying to connect to the ISEO Cloud, to be loaded in the Argo Account. For some reason the communication between Gateway and Cloud failed. This problem can be caused by different issues: 1. Slow Internet connection 2. Firewall blocking the communication 3. Error during data exchange	Tap OK to restart the process and try again. If the problem persists check your Internet connection: check if any other device like PC, Smartphone, can surf the web as usual. Perform an Internet speed test to check the communication performance. If the problem cannot be solved, please contact the *ISEO Service Operation Center* (go to *Technical Support*).

Error	Meaning	What to do
	1. Your Account has just been deleted 2. The ISEO Cloud is not reachable.	1. If you have just deleted your Argo Account this is a correct message. 2. Try again later and check your device Mobile or WiFi Internet connection. If the problem persists, please contact the *ISEO Service Operation Center* (go to *Technical Support*).
	This error could happen at the beginning of the Gateway configuration, during the QR-Code reading. The system warns you that this Gateway has already been registered in the ISEO Cloud.	1. Use a different Gateway since this has already been assigned to an Argo Account. 2. Delete this Gateway from the current Argo Account and then you can use it for another Account. **Note**: to connect the Gateway to another Argo Account you will need to reset it as showed in the configuration wizard.
	1. The Lock Account Password is not correct. 2. The Lock Account Password has been associated to the smartphone Biometric Identification, but later this password has been changed. The phone at the first attempt recalls from the memory the first associated password, that actually has changed: that's why it is no longer correct.	1. Insert the correct Lock Account Password. 2. Repeat the procedure: the app will ask to manually type the new password after the Biometric Identification failed 2 times.

Error	Meaning	What to do
	In this example a Guest Account was trying to delete a Phone User with Login (Local Administrator), without having the Manage Administrators permission enabled by the Owner Administrator. The same error happens every time the Guest Account try to make an operation not allowed by the Owner Administrator (i.e. Open Door, Read Events)	You cannot perform operations not authorized by the Owner Administrator. Ask the permission to the Owner Administrator.
	In this example the Owner Administrator is trying to delete the Gateway but there are locks configured in the system.	Delete all locks first, one by one, then at the end you can delete the Gateway.
	In this example the Owner Administrator is trying to delete the Argo Account but there is a Smart Gateway configured into the system.	Delete the Smart Gateway first (deleting all the locks before), and finally you can permanently delete the Argo Account.

Error	Meaning	What to do
	The Smart Gateway is not reachable. It could be OFF or for some reason not properly working. The icon in the Gateway menu is red like the example below. 	Check if: • The Gateway is ON with the Network led ON. • The Gateway is correctly installed to communicate to the router. • The router is properly working. If YES, all the above, restart the Gateway and check if it is now working. If the problem cannot be solved, please contact the *ISEO Service Operation Center* (go to *Technical Support*).
	A problem happened trying to connect to the locks from remote. The Gateway is available, but the locks cannot be reached.	• Check locally if the lock is properly working. • Replace the lock battery if empty. • Check the lock position if in the Gateway Bluetooth range.
	An unexpected and unknown error happened. This error has not been yet translated in the system. A numeric code inside square brackets might follow the text (software error code).	Try the operation again to check if it is a recurrence error. If the problem persists, please contact the *ISEO Service Operation Center* (go to *Technical Support*), providing the numeric code if present.

All Argo app functionalities

To explore all the *Argo Local* functions and features, read the *Argo 2.7 User Manual* available at *iseo.com*.

Technical Support

For technical support please contact the ISEO Support Service. You can find your country contact at:

https://www.iseo.com/

When you contact the *Service Operations Center* please provide the next information:

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

ISEO
ULTIMATE ACCESS TECHNOLOGIES

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.com