



# ISTRUZIONI DI MONTAGGIO



ARGO 3.0 FROM REMOTE  
MANUALE D'INSTALLAZIONE E D'USO

**ARGO 3.0 FROM REMOTE**  
**MANUALE UTENTE**

I T A L I A N O

**ISEO**<sup>®</sup>  
ULTIMATE ACCESS TECHNOLOGIES

# Informazioni sul manuale

Questo manuale parla di *Argo 3.0* e del nuovo sistema di gestione da remoto.

*Argo 3.0* è la nuova versione di *Argo*, aggiornamento della precedente (*Argo 2.7*) e introduce una nuova serie di *Dispositivi Smart di ISEO*, dotati dell'innovativa tecnologia *Bluetooth 5.0*. Grazie a questa tecnologia, *Argo 3.0* abbinato ai nuovi *Dispositivi Smart di ISEO*, permette di **gestire il sistema da remoto**. Questo è il motivo per cui *Argo 3.0* è chiamato **Argo From Remote**.

Per avere maggiori informazioni su *Argo*, tutte le funzionalità standard e i relativi menu, fare riferimento al *Manuale Utente Argo 2.7* disponibile sul sito *iseo.com* al seguente link:

[https://www.iseo.com/data/updati/manuali/ISEOZERO1ELECTRONICSOLUTIONS\\_SISTEMAARGO\\_ARGOAPPSISTEMADIGESTIONE/Argo%202.7\\_User%20Manual\\_EN\\_01\\_20200611.pdf](https://www.iseo.com/data/updati/manuali/ISEOZERO1ELECTRONICSOLUTIONS_SISTEMAARGO_ARGOAPPSISTEMADIGESTIONE/Argo%202.7_User%20Manual_EN_01_20200611.pdf)

Per tutta la restante documentazione, come leaflet, brochure e certificazioni, visitare la seguente pagina: <https://www.iseo.com/it/en/detail-product/argo-app--management-system>

**Nota:** in questo manuale viene illustrata la configurazione di *Argo 3.0* e le caratteristiche relative ai capitoli *Funzioni base* e *Funzioni avanzate*. La configurazione del *Gateway* è inoltre illustrata nel video *Argo 3.0 From Remote Quick Start* al seguente link: <https://youtu.be/bFrKiuZqZmE>

## Icone informative

Per una lettura più semplice del manuale, prendere nota delle seguenti icone:



**ATTENZIONE:** importanti informazioni riguardanti il corretto funzionamento del sistema.



**NOTE:** note, suggerimenti e ulteriori informazioni.



**IDEA:** note, suggerimenti e ulteriori informazioni.

## Come utilizzare questo manuale

### Sommario

#### Informazioni sul manuale

Icone informative	2
Come utilizzare questo manuale	3
Informazioni sul copyright	4
Marchi commerciali	4
Parole chiave	4

#### Argo da remoto

Principio di funzionamento	8
----------------------------	---

#### Smart Gateway

Modelli Smart Gateway	10
Dati tecnici di Smart Gateway	11

Nel *Sommario*, clicca sull'argomento o il numero di pagina per andare direttamente al paragrafo o al capitolo relativo.

## Argo da remoto

*Argo 3.0* abbinato alla nuova generazione di *Smart Device ISEO* dotati di *Bluetooth 5.0* e *Smart Gateway*, consente di gestire il sistema da remoto. Ciò significa che l'*amministratore* può connettersi alla serratura per aggiungere utenti o leggere eventi anche senza trovarsi nelle vicinanze della porta.

### Principio di funzionamento

Il telefono è in grado di raggiungere lo *Smart Gateway* tramite l'*account Argo personale* creato nel servizio gratuito di *Cloud ISEO*. Il telefono comunica con il *Cloud ISEO* tramite dati mobili o connessione WiFi, se disponibile. Il *Cloud ISEO* comunica con lo *Smart Gateway* attraverso una connessione Internet, tramite un router a cui è connesso il *gateway* (router domestico o aziendale — non fornito da ISEO). Il *gateway* deve essere configurato correttamente per raggiungere il router e, attraverso il router, l'*account Argo*. Il *gateway* deve essere posizionato vicino alla serratura, nel raggio di portata *Bluetooth*, per comunicare con la serratura tramite la tecnologia Bluetooth 5.0.

Da qualsiasi pagina, clicca *Sommario* per tornare alla pagina dell'indice.

## Informazioni sul copyright

- Nessuna parte di questa guida può essere riprodotta, distribuita, tradotta o trasmessa in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, compresi fotocopiatura o registrazione in qualsiasi sistema di memorizzazione e recupero dati, senza il previo consenso scritto di ISEO.
- ISEO si riserva il diritto di modificare le specifiche hardware e software descritti in questo manuale in qualsiasi momento e senza preavviso.
- ISEO non potrà essere ritenuto responsabile di eventuali danni derivanti dall'uso di questo prodotto.

## Marchi commerciali

- Il logo Apple, Apple™, iPhone™, iPad™ e App Store™ sono marchi registrati della APPLE Inc.
- Il logo Android, Google™, YouTube™, Google Play™ Store sono marchi registrati della Google Inc.
- Bluetooth® è un marchio registrato in tutto il mondo della Bluetooth SIG, Inc
- IOS è un marchio registrato della Cisco negli Stati Uniti ed altri paesi.
- MIFARE® è un marchio registrato della NXP B. V.
- Tutti gli altri marchi e diritti d'autore sono di proprietà dei loro rispettivi proprietari.

## Parole chiave

- **Argo Account:** è fondamentale per attivare il sistema *Argo 3.0 from Remote*. Viene creato per la prima volta durante la registrazione dell'utente al servizio *ISEO Cloud*. Permette di raggiungere lo *Smart Gateway* e di gestire il sistema da remoto. È gratuito ed è necessario inserire un indirizzo e-mail valido al momento della creazione dell'account.
- **Argo Local:** quando l'Amministratore o l'utente si connettono direttamente con il telefono, via *Bluetooth*, al *Dispositivo Smart di ISEO*. "Local" significa essere di fronte alla serratura, nel raggio del *Bluetooth*, in modo da "vedere" con lo smartphone la lista delle serrature vicine.
- **Argo from Remote:** quando l'Amministratore si connette con lo smartphone, ad un *Dispositivo Smart di ISEO*, utilizzando un *Account Argo*, per mezzo della connessione dati e attraverso lo *Smart Gateway* posto vicino alla serratura. "Remoto" significa che l'Amministratore si trova al di fuori della portata del *Bluetooth* della serratura, ma può lo stesso raggiungere e comunicare con la serratura grazie al servizio *ISEO Cloud*.
- **Bluetooth 5.0:** chiamato anche *BLE 5*, è una nuova tecnologia che aggiorna la precedente *Bluetooth 4.0* e permette una comunicazione multicanale. Ciò significa che, mentre il *BLE 4* può comunicare con un solo dispositivo alla volta (canale singolo), il *BLE 5* può comunicare con più dispositivi simultaneamente. Ad esempio: mentre qualcuno sta aprendo la serratura con lo smartphone, l'Amministratore può collegarsi da remoto attraverso lo *Smart Gateway* e la serratura sarà in grado di eseguire entrambe le richieste nello stesso momento.

- **Guest Account:** vedi *Amministratore Invitato da Remoto*.
- **Houses:** vengono mostrate nell'interfaccia utente di *Argo from Remote* e riferiscono ad un gruppo di serrature. Questa funzione permette di identificare meglio le serrature installate in diverse località o zone, al fine di organizzare e ordinare la *Home page di Argo from Remote*.
- **ISEO Cloud:** l'infrastruttura gratuita del servizio cloud su cui funziona *Argo from Remote*. Per connettersi a questo servizio è richiesto un *Argo Account*.
- **ISEO Smart Devices:** le serrature elettroniche di ISEO installate sulle porte dispongono ora della tecnologia *Bluetooth 5.0*. Anche chiamate serrature, è fondamentalmente lo stesso hardware usato nelle precedenti versioni di *Argo*, ma con il chip *Bluetooth 5.0* incorporato nella scheda elettronica. Anche il logo del prodotto è cambiato al fine di indentificare velocemente e facilmente la nuova tecnologia.
- **Local Administrator:** qualsiasi utente nella *Lista Utenti di Argo* con possibilità di LOGIN. Il login infatti fornisce automaticamente agli utenti i diritti di *Amministratore*. L'*Amministratore Locale* può quindi accedere alla serratura, ma solo nel raggio del *Bluetooth* (*Argo Local*).
- **Lock Account Password:** per comunicare con la serratura tramite l'*account Argo*, per aprire o eseguire il login, è necessaria una password chiamata *Lock Account Password*. Viene configurata durante la configurazione dell'*account Argo* quando viene aggiunta la serratura ed è creata per ogni singola serratura. Può anche essere associata all'identificazione biometrica dello smartphone, per una maggiore comodità dell'utente. Con la *Lock Account Password*, anche se qualcuno è in grado di accedere all'*account Argo* o ruba il telefono, non potrà aprire né accedere alla serratura da remoto poiché questa password è richiesta a ogni tentativo di comunicazione.
- **Remote Owner Administrator:** è l'*identità dell'account* ora presente nell'*elenco utenti di Argo from Remote* e corrisponde all'*amministratore* che per primo ha creato l'*account Argo* per gestire il sistema da remoto. Questo amministratore è il proprietario del sistema e dello *Smart Gateway* utilizzato per connettere le serrature al Cloud. Può invitare altri amministratori affinché lo aiutino a gestire la serratura da remoto (vedere *Remote Invited Administrator*).
- **Remote Invited Administrator (Guest Account):** è un altro tipo di *Account identity* nell'*elenco utenti di Argo from Remote*. È l'*amministratore* invitato da un *Remote Owner Administrator* per aiutare a gestire le serrature da remoto. Viene anche chiamato *Guest Account* perché è come un ospite che utilizza uno *Smart Gateway* per raggiungere serrature di proprietà di un altro amministratore: l'*Owner Administrator*. Si noti che l'*Invited Administrator* non può eliminare l'*Owner Administrator* e non può eliminarsi dalla serratura a cui è stato invitato. Deve chiedere all' *Owner Administrator* di farlo.
- **Smart Gateway:** il dispositivo elettronico ISEO è in grado di collegare gli *Smart Device ISEO* al *Cloud ISEO*. Dev'essere collegato a un router WiFi o PoE per raggiungere l'*account Argo* e comunica con le serrature delle porte tramite la tecnologia *Bluetooth 5.0*. Deve essere installato tra i dispositivi *Bluetooth* rilevati dalle serrature e funziona solo con gli *Smart Device ISEO* dotati di tecnologia *Bluetooth 5.0*. È disponibile in 2 modelli: in versione WiFi e PoE.



Per altre *Parole chiave di Argo*, leggere il *Manuale Utente Argo 2.7* disponibile su [iseo.com](http://iseo.com).

# Sommario

<b>Informazioni sul manuale</b>	<b>2</b>
Icane informative	2
Come utilizzare questo manuale	3
Informazioni sul copyright	4
Marchi commerciali	4
Parole chiave	4
<b>Argo da remoto</b>	<b>8</b>
Principio di funzionamento	8
<b>Smart Gateway</b>	<b>9</b>
Modelli Smart Gateway	10
Dati tecnici di Smart Gateway	11
<b>Smart Device ISEO con Bluetooth 5.0</b>	<b>12</b>
Nuova estetica del logo	12
<b>Funzioni base</b>	<b>14</b>
Creazione dell'account Argo	14
Login all'account Argo	19
Configurazione dello Smart Gateway	20
Aggiunta di serrature al sistema (è richiesta la Master Card)	25
<b>Connessione alla serratura da remoto</b>	<b>29</b>
Apertura della serratura da remoto	29
Login alla serratura da remoto	32

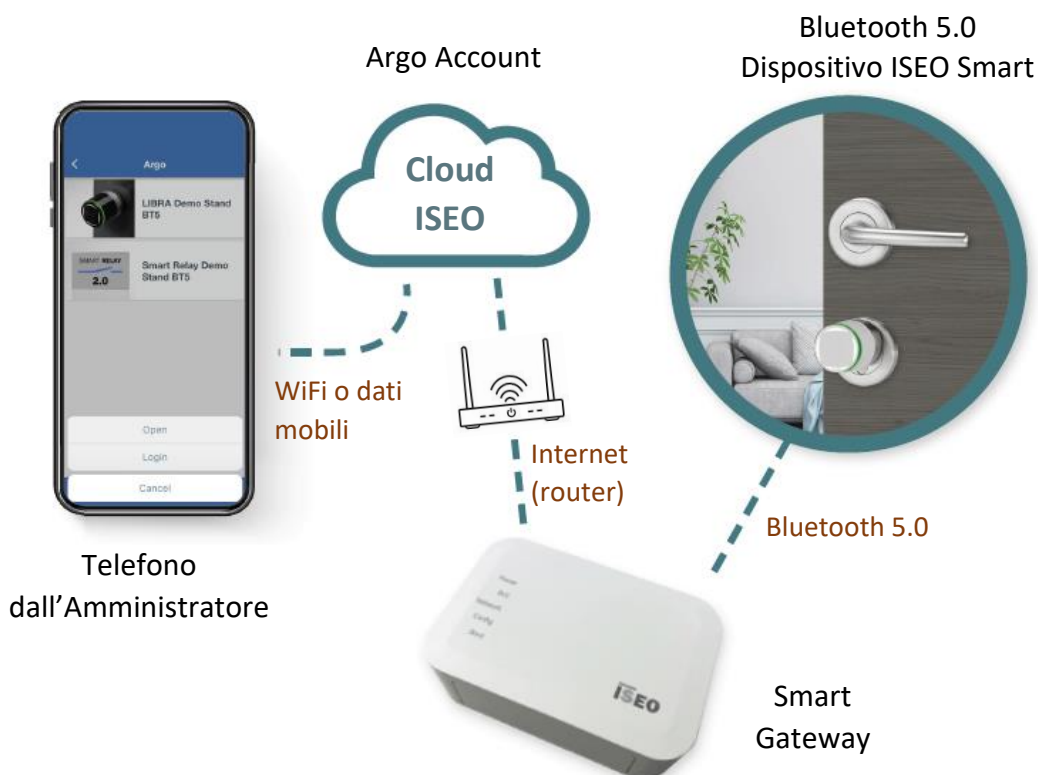
<b>Funzioni avanzate</b>	<b>35</b>
Panoramica del menu Argo from Remote	35
Houses	36
Gateways	37
Locks	38
Manage Account	41
Log Out	42
Account user	43
Guest Account	44
Aggiunta account (invito di un amministratore remoto)	45
Eliminazione dell'account	52
<b>Domande e risposte</b>	<b>55</b>
<b>Ricerca guasti</b>	<b>60</b>
Tutte le funzionalità dell'app Argo	65
Supporto tecnico	65

# Argo da remoto

*Argo 3.0* abbinato alla nuova generazione di *Smart Device ISEO* dotati di *Bluetooth 5.0* e *Smart Gateway*, consente di gestire il sistema da remoto. Ciò significa che l'*amministratore* può connettersi alla serratura per aggiungere utenti o leggere eventi anche senza trovarsi nelle vicinanze della porta.

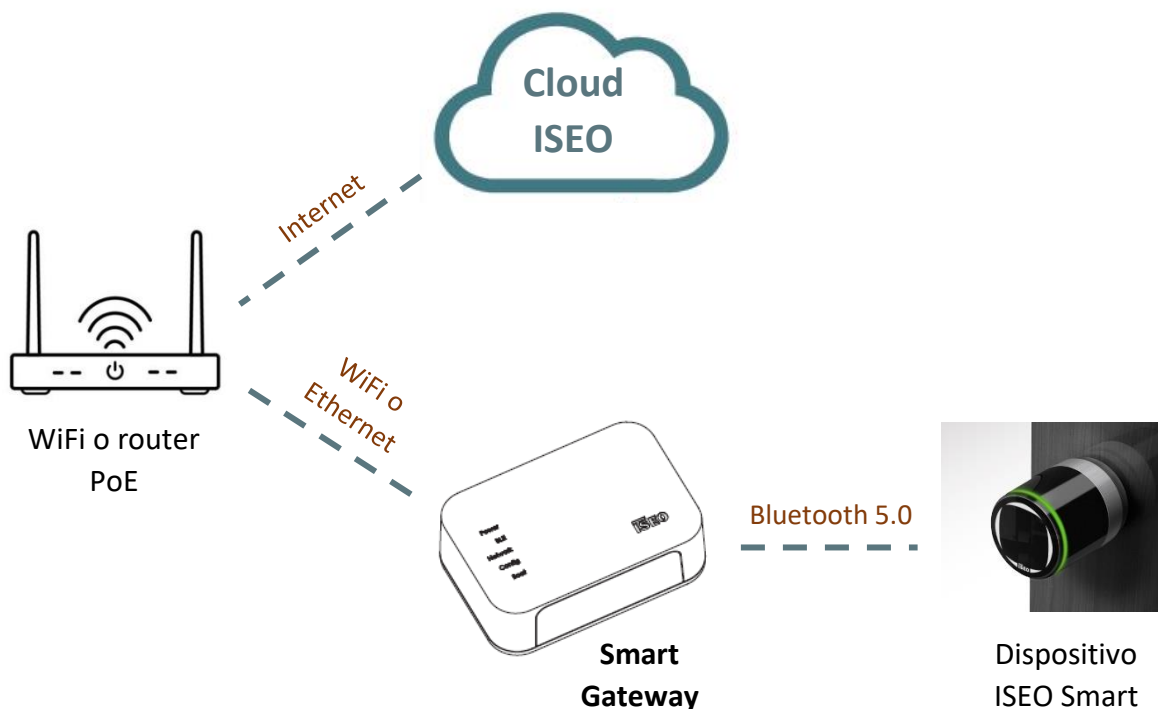
## Principio di funzionamento

Il telefono è in grado di raggiungere lo *Smart Gateway* tramite l'*account Argo personale* creato nel servizio gratuito di *Cloud ISEO*. Il telefono comunica con il *Cloud ISEO* tramite dati mobili o connessione WiFi, se disponibile. Il *Cloud ISEO* comunica con lo *Smart Gateway* attraverso una connessione Internet, tramite un router a cui è connesso il *gateway* (router domestico o aziendale — non fornito da ISEO). Il *gateway* deve essere configurato correttamente per raggiungere il router e, attraverso il router, l'*account Argo*. Il *gateway* deve essere posizionato vicino alla serratura, nel raggio di portata *Bluetooth*, per comunicare con la serratura tramite la tecnologia Bluetooth 5.0.



# Smart Gateway

Lo *Smart Gateway* collega il *Cloud ISEO* al *dispositivo ISEO Smart*. Comunica con il cloud via Internet tramite un router WiFi e con la serratura tramite *Bluetooth Smart 5.0*. Lo *Smart Gateway* può gestire tutti gli *Smart Device ISEO* nel raggio di portata *Bluetooth* (circa 10 metri, a seconda delle condizioni ambientali).



Il router non è fornito da ISEO.

In caso di più *Smart Device ISEO*, distanti più di 10 metri l'uno dall'altro, è possibile aggiungere altri gateway collegati allo stesso router.

*Smart Gateway* è un potente dispositivo Linux con un processore *ARM 7* ed estende le capacità di *Argo* anche a distanza, fornendo lo stesso livello di sicurezza garantita in locale. Consente un'architettura di sicurezza con connettività diretta alla serratura con crittografia end-to-end. Il *Cloud ISEO* è utilizzato solo come tunnel e non memorizza alcun dato sensibile per la serratura della porta.

Lo *Smart Gateway*, con *sistema operativo Linux* e delle *API* già fornite, può essere utilizzato dagli *ISEO Argo*

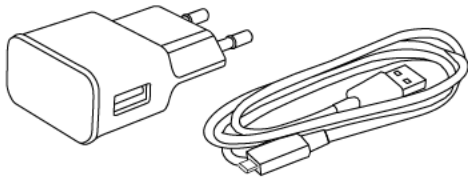
*Developers* (integratori) di *Argo SDK* per scrivere il loro software e la loro applicazione in modo efficiente e semplice. Inoltre, il *sistema operativo Linux* garantisce stabilità e maggiore sicurezza da minacce esterne o attacchi di virus.

## Modelli Smart Gateway

Lo *Smart Gateway* è disponibile in due modelli:

### Gateway WiFi

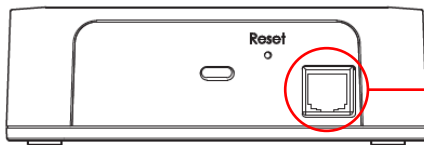
- Richiede un router WiFi.
- Deve essere alimentato da un alimentatore da 10W.



Trasformatore elettrico 5V  
CC – 2A Connettore USB C.

### Gateway PoE (alimentato tramite Ethernet)

- Richiede un router PoE.
- Deve essere collegato tramite cavo LAN alla porta PoE del router.



Il Gateway PoE è dotato di una  
porta Ethernet sul retro.

- In alternativa, può essere collegato tramite cavo LAN a un router standard (non con porta Ethernet PoE), ma in questo caso deve essere alimentato anche dall'alimentatore da 10W.



*Il Gateway PoE* richiede un router con **DHCP abilitato** per ricevere automaticamente un indirizzo IP valido.

Il cavo LAN non è fornito da ISEO.

L'alimentatore da 10 W deve essere ordinato separatamente. Non è incluso nella confezione *Smart Gateway*.

## Dati tecnici di Smart Gateway

Caratteristiche	WiFi	PoE (Power over Ethernet)
Funzionalità	<ul style="list-style-type: none"> <li>Converte da dati WIFI a BLE 5</li> <li>WIFI dual band a 2,4 GHz e 5 GHz</li> </ul>	<ul style="list-style-type: none"> <li>Converte da Ethernet a BLE 5</li> </ul>
Alimentazione	<ul style="list-style-type: none"> <li>Alimentato da USB C + 5V CC alimentazione in ingresso 2A (10W)</li> <li>Alimentatore non incluso (accessorio da ordinare)</li> </ul>	<ul style="list-style-type: none"> <li>PoE (Power over Ethernet)</li> <li>Richiede switch PoE IEEE 802.3af fino a 15,4 W</li> <li>Invio di dati e alimentazione tramite cavo ethernet Cat5e/Cat6.</li> <li>Consumo energetico massimo 10W</li> <li>Opzionalmente alimentato da USB C +5V CC alimentazione in ingresso 2A (10W)</li> <li>Alimentatore non incluso (accessorio da ordinare)</li> </ul>
Dimensioni	<ul style="list-style-type: none"> <li>125x40x85mm (LxPxA)</li> </ul>	<ul style="list-style-type: none"> <li>125x40x85mm (LxPxA)</li> </ul>
Condizioni di funzionamento	<ul style="list-style-type: none"> <li>Temperatura di funzionamento: -0 °C/+50 °C.</li> <li>Temperatura di immagazzinamento: -25 °C/+75 °C.</li> </ul>	<ul style="list-style-type: none"> <li>Temperatura di funzionamento: -0 °C/+50 °C.</li> <li>Temperatura di immagazzinamento: -25 °C/+75 °C.</li> </ul>
Installazione	<ul style="list-style-type: none"> <li>Desktop</li> <li>Opzione di fissaggio a parete (accessorio da ordinare)</li> </ul>	<ul style="list-style-type: none"> <li>Desktop</li> <li>Opzione di fissaggio a parete (accessorio da ordinare)</li> </ul>
Porte di connessione	<ul style="list-style-type: none"> <li>USB C femmina</li> </ul>	<ul style="list-style-type: none"> <li>USB C femmina</li> <li>Ethernet TCP/IP 10/100 baseT</li> </ul>
LED di segnalazione	<ul style="list-style-type: none"> <li>Alimentazione (bianco): ON = alimentatore collegato</li> <li>BLE (bianco): ON = trasmissione BLE in corso</li> <li>Rete (bianco) ON = Gateway connesso al Cloud</li> <li>Config. (bianco): ON = gateway da configurare</li> <li>Avvio (rosso): ON = avvio del gateway</li> </ul>	<ul style="list-style-type: none"> <li>Alimentazione (bianco): ON = alimentatore collegato</li> <li>BLE (bianco): ON = trasmissione BLE in corso</li> <li>Rete (bianco) ON = Gateway connesso al Cloud</li> <li>Config. (bianco): ON = gateway da configurare</li> <li>Avvio (rosso): ON = avvio del gateway</li> </ul>
CPU, memoria, sistema operativo	<ul style="list-style-type: none"> <li>Modulo CPU basato su ARM A7</li> <li>512 MB di RAM</li> <li>Memoria non volatile eMMC Flash da 8 GB</li> <li>Sistema operativo: Linux integrato</li> </ul>	<ul style="list-style-type: none"> <li>Modulo CPU basato su ARM A7</li> <li>512 MB di RAM</li> <li>Memoria non volatile eMMC Flash da 8 GB</li> <li>Sistema operativo: Linux integrato</li> </ul>
Pulsanti	<ul style="list-style-type: none"> <li>Reset (riavvio o stato modalità di fabbrica)</li> </ul>	<ul style="list-style-type: none"> <li>Reset (riavvio o stato modalità di fabbrica)</li> </ul>
Versione OEM	<ul style="list-style-type: none"> <li>Versione OEM disponibile per integratori Argo con SDK</li> </ul>	<ul style="list-style-type: none"> <li>Versione OEM disponibile per integratori Argo con SDK</li> </ul>

# Smart Device ISEO con Bluetooth 5.0

La nuova serie Smart Device ISEO sfrutta la tecnologia Bluetooth 5.0 (chiamata anche *BLE 5*). Questa tecnologia consente più connessioni contemporaneamente. Esempio: mentre qualcuno sta aprendo la serratura della porta con lo smartphone, l'*amministratore* può connettersi da remoto tramite lo *Smart Gateway* e la serratura sarà in grado di eseguire entrambe le attività contemporaneamente.

Dal punto di vista della forma e della meccanica, i nuovi *Smart Device ISEO* sono gli stessi rispetto ai precedenti, dotati di tecnologia *Bluetooth 4.0*. A cambiare e renderli diversi sono i seguenti aspetti:

- Chip *Bluetooth 5.0* integrato nella scheda elettronica.
- Nuovo design estetico del logo per identificare immediatamente la nuova tecnologia *Bluetooth 5.0*.

## Nuova estetica del logo

Il nuovo logo *Argo 3.0* è presente su tutti i nuovi *Smart Device ISEO* con tecnologia *Bluetooth 5.0* integrata. Il nuovo logo comunica l'evoluzione tecnologica del prodotto, dotato di caratteristiche e funzionalità nuove e uniche:

- migliori prestazioni di comunicazione degli *Smart Device ISEO*.
- Connettività multipla contemporanea.
- Gestione remota *Argo* tramite un nuovo dispositivo: lo *Smart Gateway*.

## Evoluzione del logo Argo degli Smart Device ISEO



Smart Device Argo 2.7 e  
Bluetooth 4.0



Smart Device Argo 3.0 e  
Bluetooth 5.0

## Evoluzione del logo dell'app da Argo 2.7 ad Argo 3.0



Argo 2.7 e  
Bluetooth 4.0



Argo 3.0 e  
Bluetooth 5.0



Nell'app *Argo 3.0* i nuovi dispositivi con *Bluetooth 5.0* sono identificati da una nuova icona (vedi *Impostazioni di base, Creazione dell'account Argo*).

## Esempi di evoluzione del logo degli Smart Device ISEO



Libra Smart  
Bluetooth 4.0



Libra Smart  
Bluetooth 5.0



Stylos Smart  
Bluetooth 4.0



Stylos Smart  
Bluetooth 5.0



Lettore smart X1r  
Bluetooth 4.0



Lettore smart X1r  
Bluetooth 5.0



Su *x1R Smart* la scheda elettronica *Bluetooth 5.0* è inserita nel lettore esterno, anch'esso dotato del nuovo logo.

# Funzioni base

Questa sezione spiega come configurare *Argo 3.0* per gestire il sistema da remoto.

Per configurare *Argo from Remote* occorre:

1. Creare l'*account Argo*.
2. Eseguire il login all'*account Argo*.
3. Configurare lo *Smart Gateway*.
4. Aggiungere serrature al sistema (è richiesta la *Master Card*).

## Creazione dell'*account Argo*

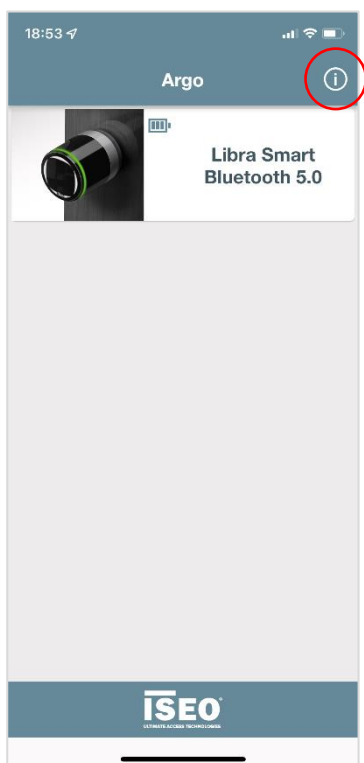
Alla prima configurazione del sistema, occorre creare il proprio *account Argo* utilizzando un indirizzo e-mail valido, raggiungibile dal telefono o tablet. A tal fine, seguire questi semplici passaggi.

1. Avviare **Argo 3.0**



Icona e logo *Argo 3.0* nuovi.

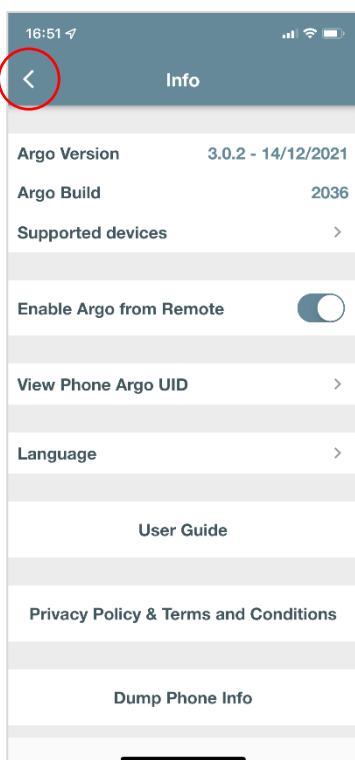
## 2. Toccare il menu **Info App**



Notare la nuova icona Libra per identificare immediatamente i dispositivi *Bluetooth 5.0*.

Tutti i nuovi dispositivi *BLE 5.0* presentano una nuova icona affinché possano essere riconosciuti facilmente dai modelli *BLE 4.0*.

## 3. Selezionare **Enable Argo From Remote**, poi tornare al menu principale.

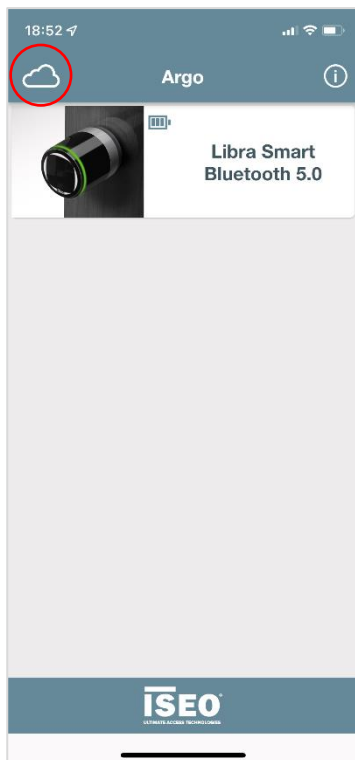


Argo from Remote abilitato

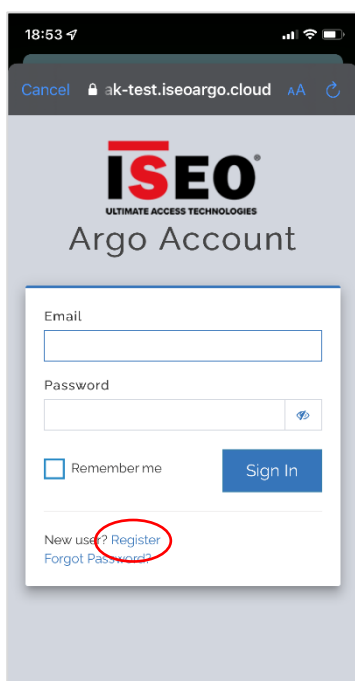


Viene visualizzato un messaggio di avviso che spiega le funzionalità e i requisiti di *Argo from Remote*. Leggere e accettare per continuare.

4. Dopo aver abilitato *Argo From Remote*, viene visualizzata un'icona del Cloud. Toccare l'**icona del Cloud**.

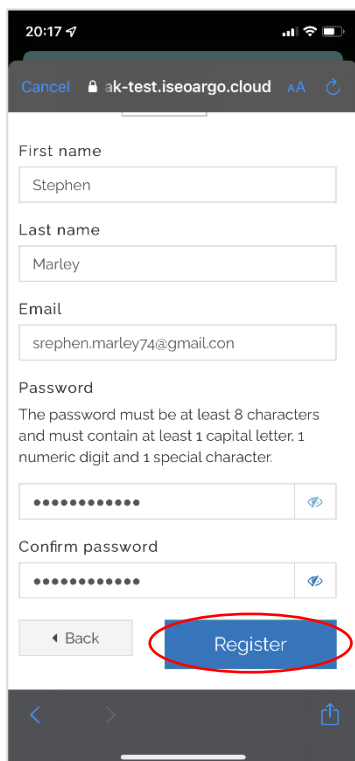


5. Toccare **Register** per avviare una nuova registrazione utente nel *Cloud ISEO*. Quindi, seguire la procedura dettagliata.



La registrazione dell'utente dev'essere eseguita solo alla prima configurazione, per creare l'*account Argo*.

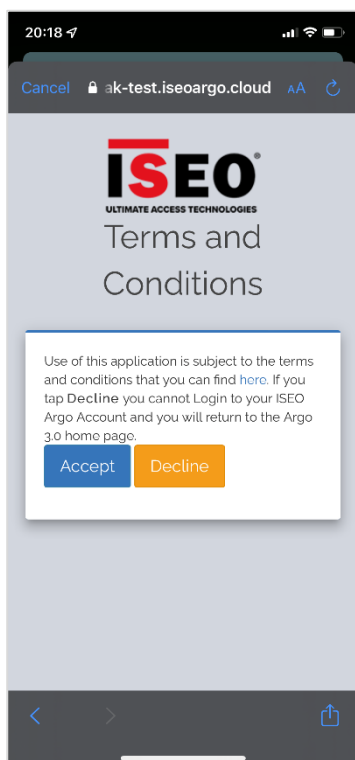
6. Inserire tutti i dati richiesti e toccare **Registra** alla fine.



— Inserire un indirizzo e-mail valido raggiungibile dal dispositivo da cui viene effettuata la registrazione.

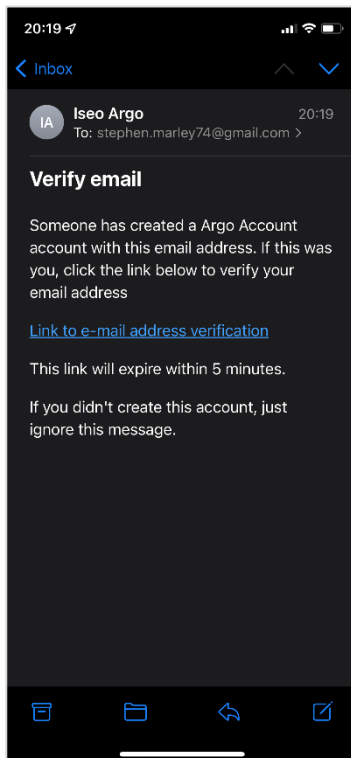
— È obbligatorio impostare una password forte.

7. **Accettare** i termini e le condizioni.



Se si tocca **Decline** si tonerà alla *home page* di Argo. Per tornare a questo passaggio, effettuare il login con l'e-mail e la password registrate nel passaggio precedente.

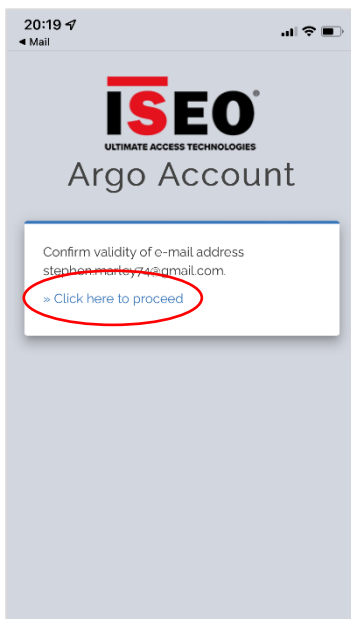
8. Attendere l'e-mail di verifica da parte del servizio del Cloud ISEO. Aprirla e toccare il link.



Toccare il link per confermare l'indirizzo e-mail.

9. Confermare la validità dell'indirizzo e-mail e attendere il messaggio di verifica.

Quindi, tornare alla *home page di Argo*.

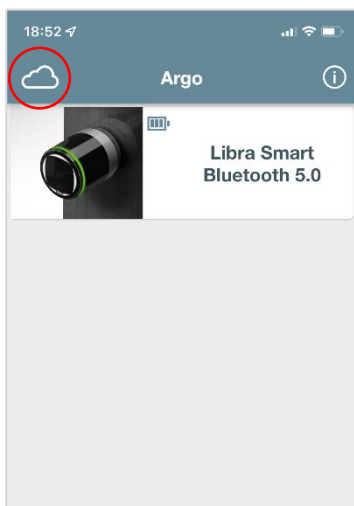


## Login all'account Argo

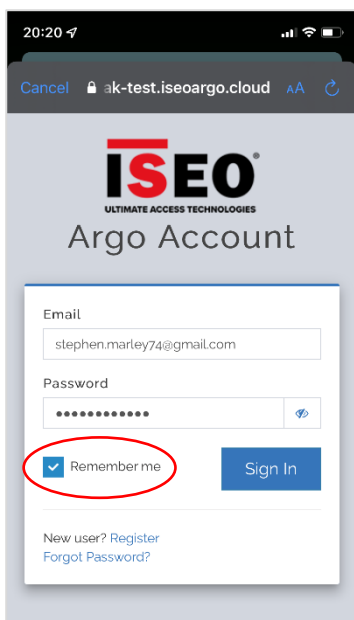
Una volta creato l'*account Argo* nel Cloud *ISEO*, è possibile effettuare il login.

Nella *home page di Argo 3.0*: g

1. Toccare l'icona del **Cloud**.



2. Accedere con l'indirizzo e-mail e la password scelti in precedenza durante la registrazione dell'*account Argo*.



Toccare **Sign In** per effettuare il login

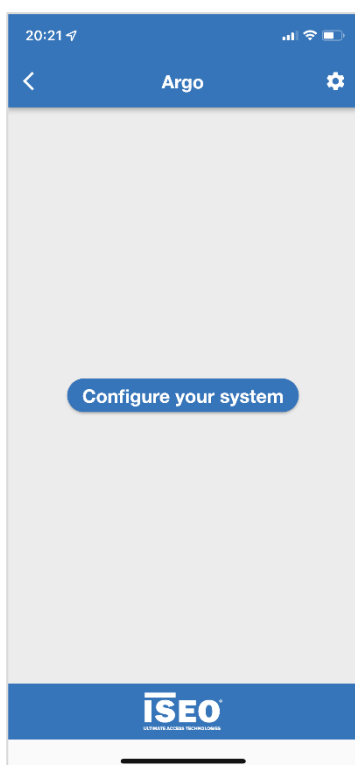


Selezionando *Remember me* non sarà necessario digitare l'e-mail e la password all'accesso successivo. Questo vale fino all'orario definito dall'app o fino a quando non ci si disconnette manualmente dall'account (per saperne di più sul logout, consultare il capitolo *Impostazioni avanzate*).

## Configurazione dello Smart Gateway

Quando si accede all'*account* *Argo* per la prima volta, è necessario configurare lo *Smart Gateway* per iniziare a utilizzare *Argo from Remote*. Lo *Smart Gateway* è lo “strumento”» che permette al telefono di “raggiungere” la serratura a distanza. Ecco perché non appena si apre *Argo from Remote* si riceve il messaggio: *Configure your system*.

### 1. Toccare **Configure your system**.



La barra menu superiore e inferiore ha un colore diverso da *Argo Local*. Questo indica che si è in ambiente remoto (*Argo from Remote*).

### 2. **Accendere** lo *Smart Gateway*, quindi seguire la procedura dettagliata integrata nell'app.



L'avvio dello *Smart Gateway* dura circa 1 minuto.



Procedura guidata di configurazione



Se la *spia di configurazione del gateway* NON è accesa, toccare **No** e l'app mostrerà come ripristinare il Gateway alla modalità di fabbrica.

3. Leggere il **QR-code** dello *Smart Gateway* utilizzando il proprio smartphone.



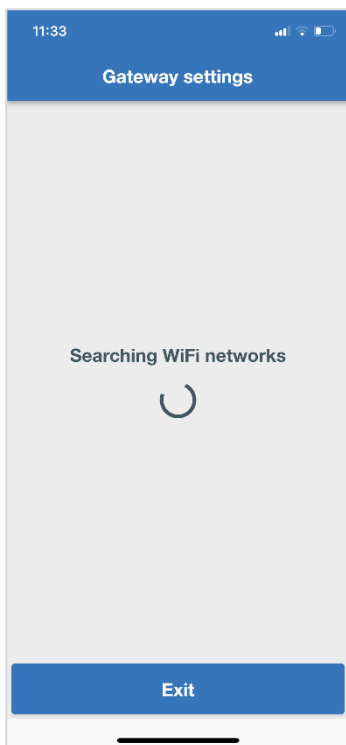
Sul retro del gateway sono presenti due *QR-Code*:

- Numero di serie del prodotto
- Codice di registrazione.

Argo legge automaticamente solo il codice corretto: il **codice di registrazione**.

In caso di problemi di lettura del *QR-code*, è possibile aggiungere manualmente il *codice di registrazione* toccando **Add manually**.

4. Una volta letto il *QR-code* con il *codice di registrazione*, la **procedura guidata** inizia a cercare le reti WiFi entro la portata del telefono.

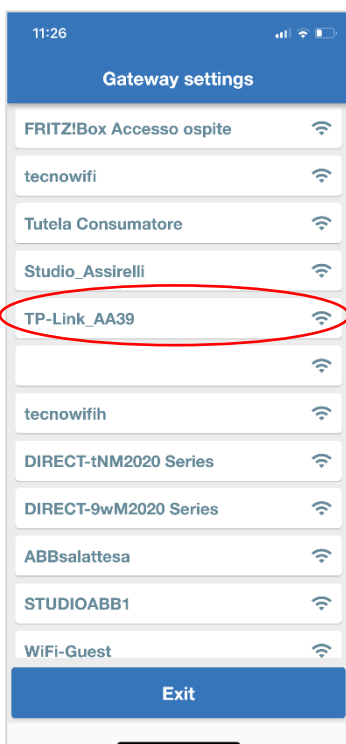


In caso di *Smart Gateway PoE*, andare al passaggio 7.

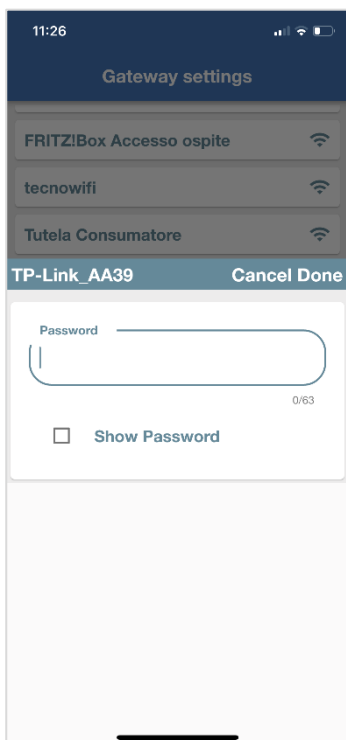
I passaggi 4, 5 e 6 sono validi solo per *Smart Gateway WiFi*.

Questo perché il *Gateway PoE* è collegato direttamente al router tramite cavo LAN e riceve automaticamente un indirizzo IP tramite il protocollo DHCP.

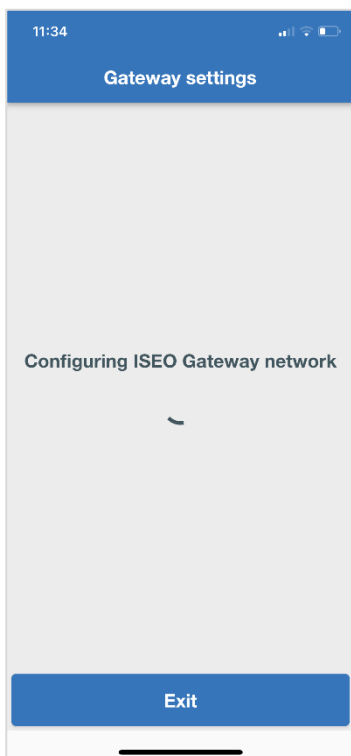
5. Scegliere e toccare la **rete WiFi** fornita dal router.



6. Inserire la password WiFi personale e toccare **Done**.



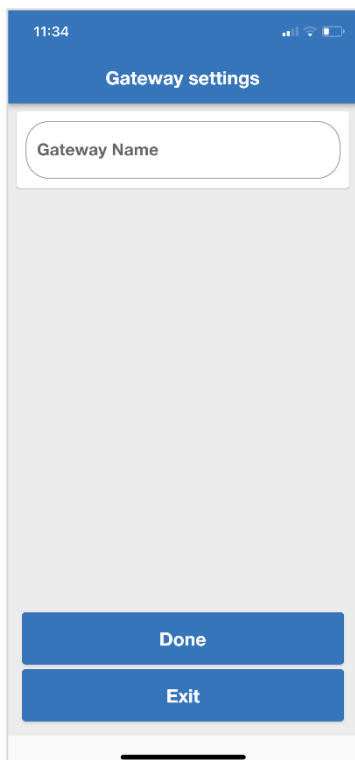
7. Attendere la configurazione automatica della rete dello *Smart Gateway*.



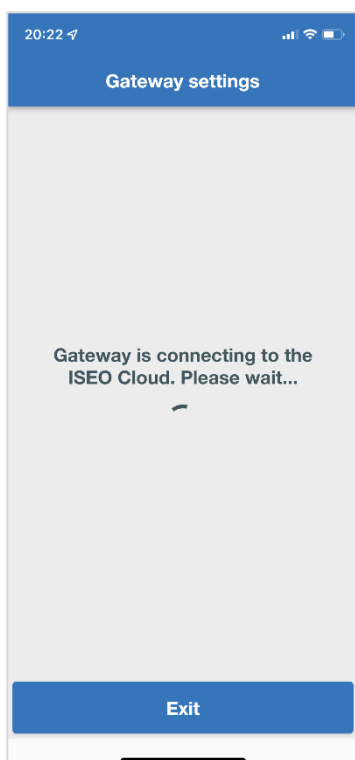
In questa fase il gateway si sta connettendo alla rete WiFi del router. Se si verifica un errore, ripetere il processo e ricontrollare la password del router.

Per ulteriori informazioni sui tipi di errore, andare al capitolo *Ricerca guasti*.

8. Non appena lo *Smart Gateway* si è connesso correttamente al router, è possibile assegnare un nome al gateway per identificarlo meglio. Quindi, toccare **Done**.



9. Attendere ora che lo *Smart Gateway* raggiunga e si connetta all'*account Argo* nel *Cloud ISEO*.



In questa fase il gateway si sta connettendo al *Cloud ISEO*. Se si verifica un errore, le cause possono essere molteplici:

- Nessuna connessione Internet.
- Connessione Internet lenta (latenza di rete).
- Errore di comunicazione dovuto alle impostazioni del router o al firewall.

Ripetere la procedura. Se il problema persiste, controllare il router e la connessione Internet.

Per ulteriori informazioni sui tipi di errore, leggere il capitolo *Ricerca guasti*.

10. Quando lo *Smart Gateway* si connette al *Cloud ISEO* viene visualizzato un messaggio di conferma:

**Smart Gateway is ONLINE.** Ora è possibile aggiungere serrature al sistema.



## Aggiunta di serrature al sistema (è richiesta la Master Card)

Aggiungere serrature al sistema significa connettere i propri *Smart Device ISEO* allo *Smart Gateway* configurato per poterle raggiungere da remoto attraverso l'*account Argo* creato nel *Cloud ISEO*.

Per comunicare con lo *Smart Gateway*, gli *Smart Device ISEO* devono essere:

- Versione *Bluetooth 5.0*.
- Posizionato entro il raggio Bluetooth dello *Smart Gateway*.

È possibile aggiungere tutti gli *Smart Device ISEO* desiderati, non esiste un limite definito. Il *gateway* si comporta come uno smartphone con *Argo*: è in grado di rilevare qualsiasi dispositivo entro il raggio di portata Bluetooth.

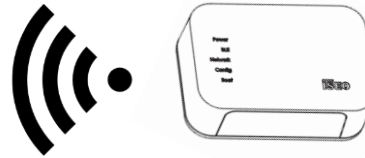
Il limite unico è la distanza tra il *gateway* e i dispositivi, che non deve superare, in media, i 10 metri circa. Il valore può variare a seconda delle condizioni ambientali: spessore della parete, angoli, rumore elettromagnetico intorno, luogo di installazione del *gateway*, posizione e altezza.

## Esempio di installazione del gateway



Porta con installato  
*Smart Device ISEO*

Portata Bluetooth 5.0  
(circa 10 metri)



*Smart Gateway* installato vicino alla porta e nel raggio di portata WiFi del router.



Portata WiFi



Router WiFi

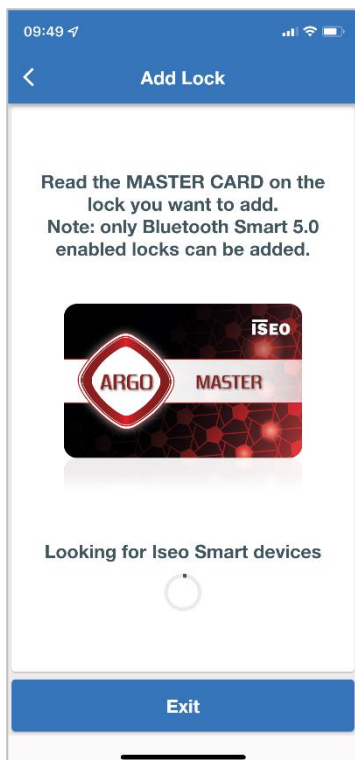
1. Toccare **Add new locks**, quindi seguire la procedura guidata di installazione. Assicurarsi di essere davanti alla serratura da aggiungere per presentare la *Master Card* quando richiesto dall'app.



Questa procedura **richiede la Master Card** e l'amministratore deve trovarsi davanti alla serratura.

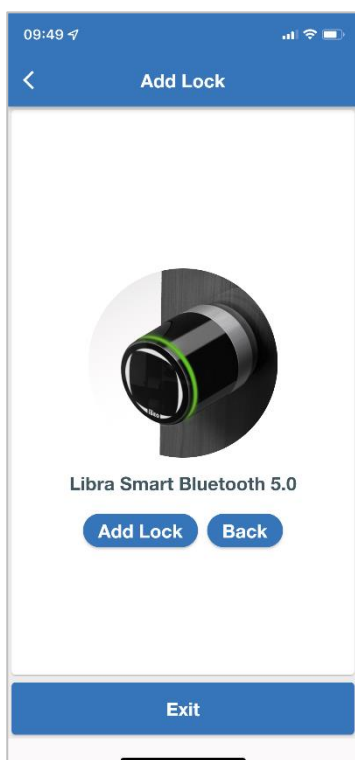
È inoltre possibile aggiungere serrature in un secondo momento utilizzando il menu apposito disponibile nella *home page di Argo from Remote*. Per ulteriori informazioni sulle funzioni del menu, leggere il capitolo *Impostazioni avanzate*.

- L'app inizia a cercare gli *Smart Device ISEO Bluetooth 5.0* nelle vicinanze. Non appena i dispositivi vengono trovati, seguire le istruzioni nell'app.



Presentare la **Master Card** con il codice di sistema univoco assegnato al proprio impianto.

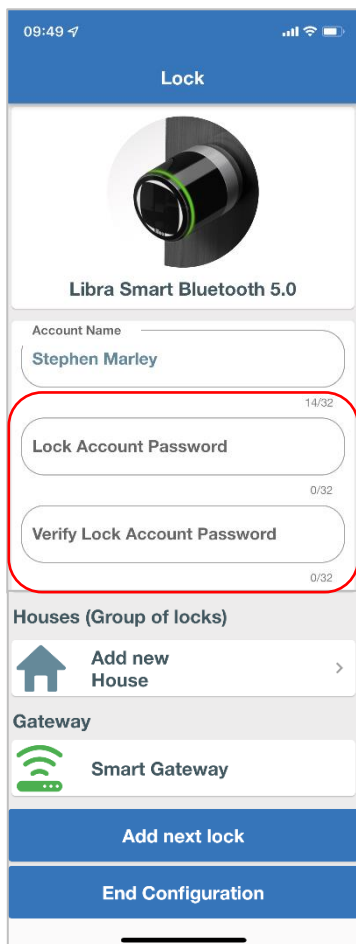
- Toccare **Add lock** per confermare e attendere la configurazione della serratura.



Il nome della serratura viene acquisito automaticamente da *Argo Local*.

Per cambiare il nome della serratura, modificarlo come al solito da *Argo Local* nel menu *Door Info*. Il nome della serratura viene aggiornato automaticamente in *Argo from Remote* al login successivo.

4. Scegliere la **Lock Account Password**. Questa password è una sicurezza aggiuntiva per proteggere la comunicazione verso la serratura e viene memorizzata nel posto più sicuro: all'interno della serratura.



La password può essere associata automaticamente alle identificazioni biometriche dello smartphone (impronta digitale o face-id), per una migliore esperienza utente e maggiore comodità.

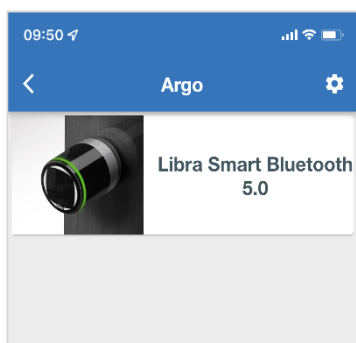
È possibile creare una *House* in cui posizionare la serratura. Per saperne di più sulla *House*, leggere al capitolo *Impostazioni avanzate*.

Questo è lo *Smart Gateway* collegato alla serratura, configurata in precedenza.



Per maggiori informazioni su *Argo From Remote*, consultare la scheda *Argo 3.0* disponibile su [iseo.com](http://iseo.com).

5. Attendere la fine della configurazione: la serratura, protetta dalla password scelta, verrà aggiunta all'*account Argo* nel *Cloud ISEO*. A operazione completata, compariranno l'icona della serratura e il pulsante nella *home page di Argo from Remote*.



La serratura aggiunta viene ora visualizzata nella *home page di Argo from Remote*.

# Connessione alla serratura da remoto

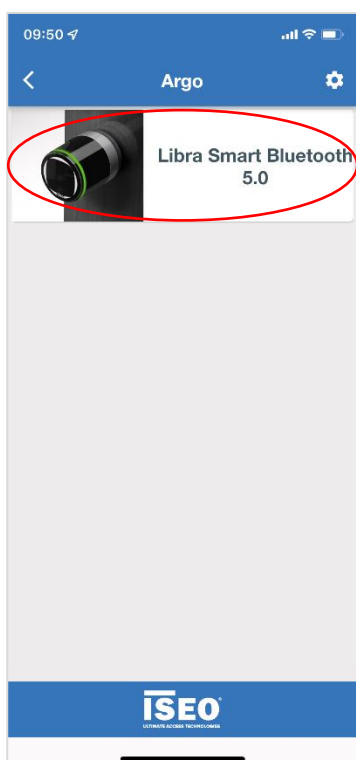
Una volta creato l'*account Argo*, configurato lo *Smart Gateway* e aggiunta la serratura al sistema (vedere il capitolo *Impostazioni di base*), è possibile connettersi da remoto allo *Smart Device ISEO* per eseguire le operazioni successive:

- Aprire la serratura da remoto.
- Eseguire il login alla serratura da remoto.

## Apertura della serratura da remoto

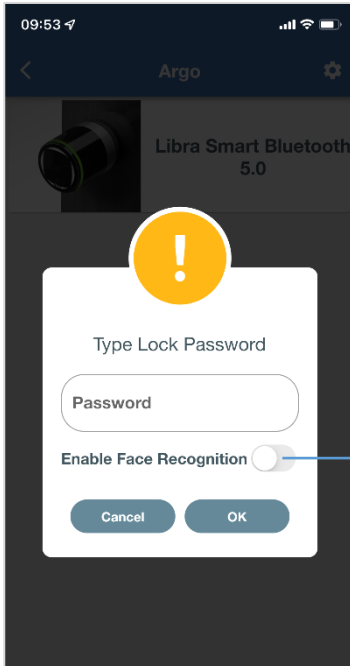
Con *Argo 3.0* è possibile aprire una serratura da remoto. Questo può essere utile in caso di esigenze specifiche o di emergenza, ad esempio se occorre far entrare qualcuno dalla porta quando non si è all'interno o nelle vicinanze. A tal fine, eseguire il *login* all'*account Argo* (vedere *Impostazioni di base*, *Login all'account Argo*) e seguire i passaggi successivi.

1. Toccare la serratura con il nome e l'icona della porta e attendere la connessione.



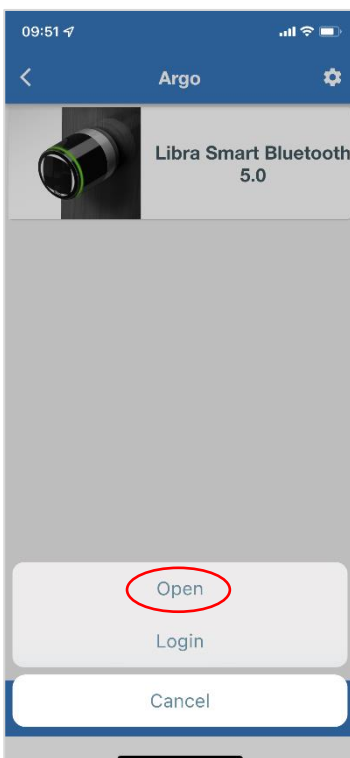
Su *Argo from Remote* non è presente la funzione *Tap & Hold* utilizzata in *Argo Local* per mostrare le funzionalità aggiuntive. Sia toccando una volta, sia toccando e tenendo premuto, il risultato è lo stesso: l'app mostra sempre le funzioni abilitate.

2. Digitare la **Lock Account Password** impostata in precedenza (*Impostazioni di base, Aggiunta di serrature al sistema*). Questa password garantisce la sicurezza del sistema e viene memorizzata nel posto più sicuro: all'interno della serratura.



Abilitare il riconoscimento del volto o dell'impronta digitale per associare questa password all'identificazione biometrica dello smartphone. In questo modo, per le operazioni successive non sarà necessario digitare nuovamente la password.

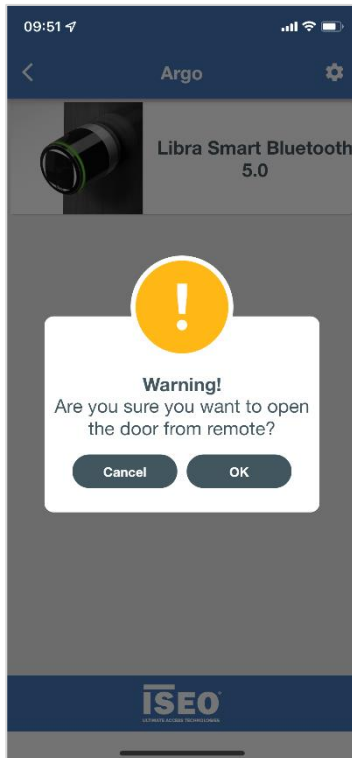
3. Toccare **Open**.



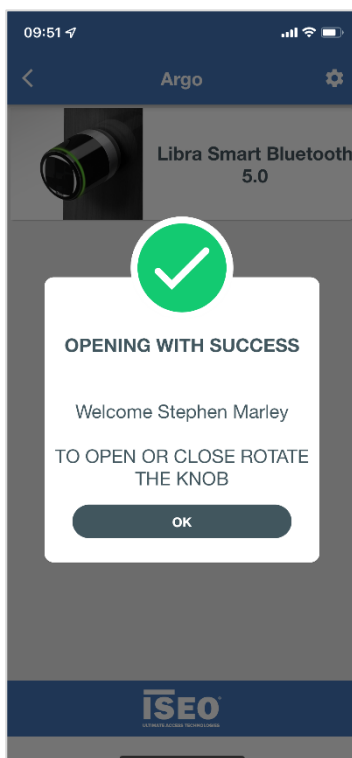
Il *login* è sempre presente per impostazione predefinita perché è il requisito di base affinché l'*amministratore* possa gestire la serratura da remoto.

Il *Remote Owner Administrator* ha la funzione *Open* per impostazione predefinita.

4. L'apertura di una porta da remoto è un'operazione critica perché non ci si trova davanti alla porta. Confermare l'operazione una seconda volta toccando **OK** nel messaggio di avviso.



5. Attendi il messaggio di apertura riuscito.

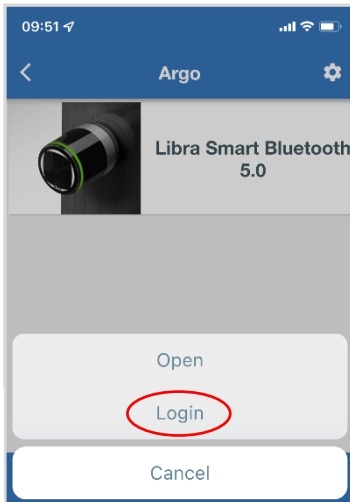


## Login alla serratura da remoto

Con *Argo 3.0* l'*amministratore* può accedere alla serratura da remoto per gestire l'elenco degli utenti o leggere gli eventi, senza la necessità di essere davanti alla porta, nel raggio di *azione Bluetooth*.

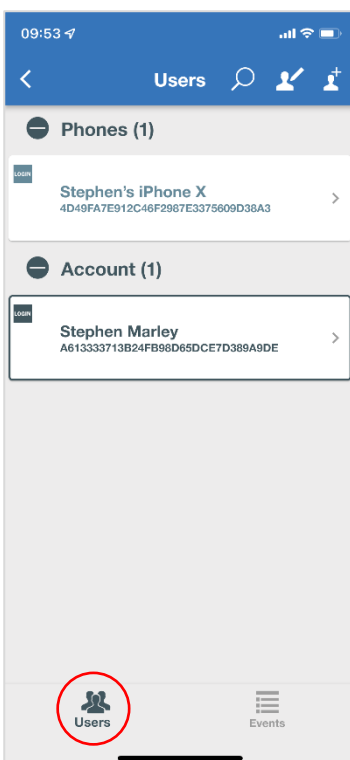
Per accedere da remoto:

### 1. Toccare **Login**



2. Digitare la **Lock Account Password** se non è ancora associata all'identificazione biometrica dello smartphone (vedere *Apertura della serratura da remoto, passaggio 2*).

3. Dopo il tempo di connessione si entrerà direttamente nell'*elenco degli utenti* della serratura da remoto.



Utente telefonico con funzionalità di login. È chiamato **Local Administrator**.

Account dell'amministratore. È chiamato **Remote Owner Administrator**.



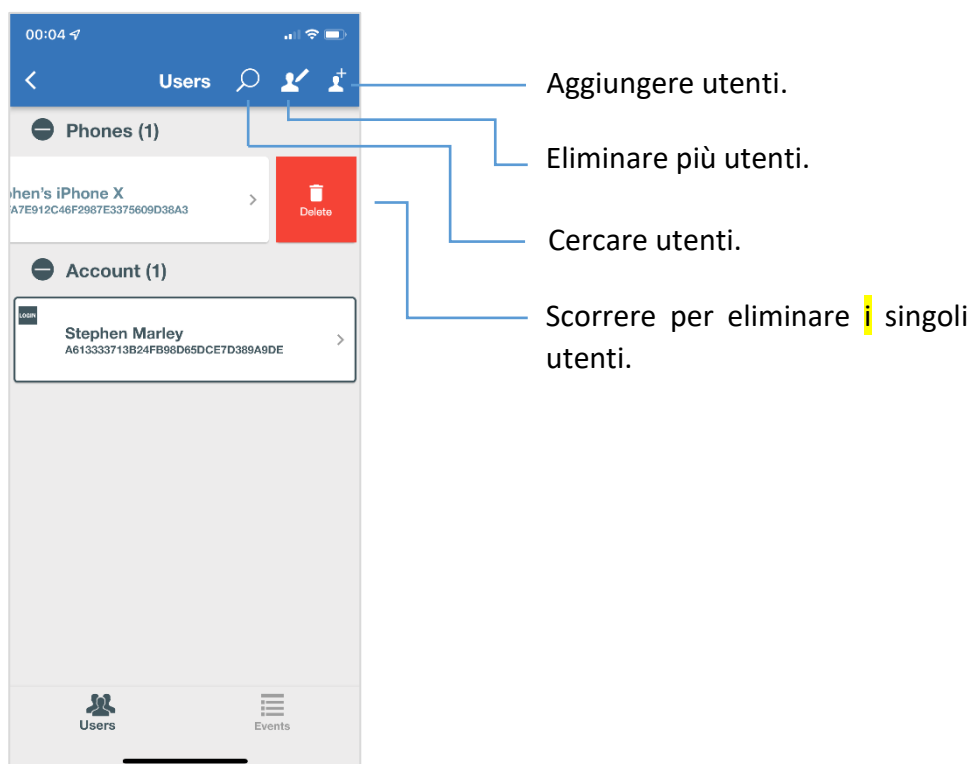
Un *amministratore* può essere solo *locale* e non *remoto* o viceversa, oppure può avere entrambe le identità, come nell'esempio precedente. Il *Local Administrator* non può eseguire il login da remoto e viceversa.

Dopo il login è possibile:

- Aggiungere, modificare o eliminare *Users*.
- Leggere lo storico degli *Events*.
- Aggiungere un *Guest Account* (questo argomento è trattato nel capitolo *Impostazioni avanzate*).


## Aggiunta, modifica o eliminazione di utenti

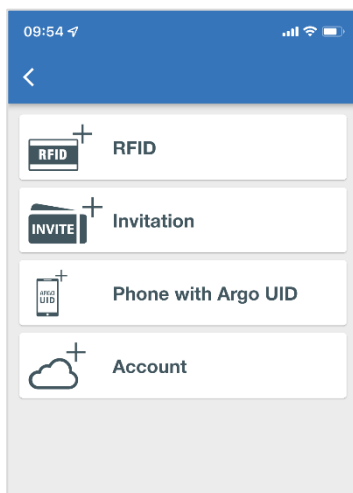
Come in *Argo Local*, è possibile cercare, aggiungere, modificare o eliminare utenti, ma da remoto.



L'interfaccia utente di *Argo from Remote* è la stessa di *Argo Local*: la logica, l'estetica, i pulsanti e le icone sono gli stessi. Questo consente di fornire la migliore esperienza utente e comodità d'uso: chi conosce *Argo Local* saprà anche usare *Argo From Remote* senza difficoltà.

Per maggiori informazioni su *Argo Local* leggere il *Manuale utente di Argo 2.7*.

Toccare l'icona **Add user**  per visualizzare le credenziali che possono essere aggiunte, a seconda del tipo di *Smart Device ISEO*. Le credenziali da aggiungere sono le stesse di *Argo Local*, oltre una nuova: *Account* (vedere il capitolo *Impostazioni avanzate*)

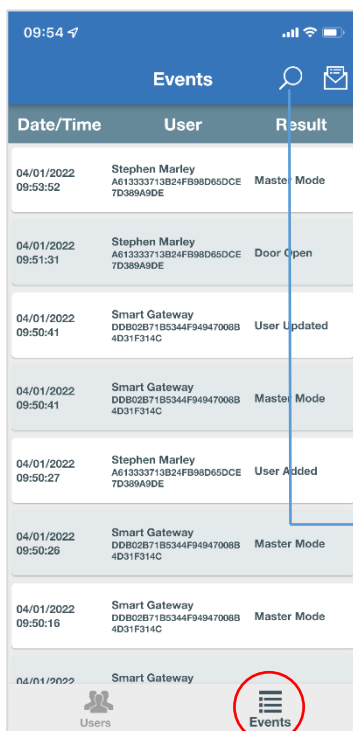


In questo esempio lo *Smart Device ISEO* è un *Libra Smart*, quindi non possiamo aggiungere codici PIN.

L'opzione *Add Fingerprint*, disponibile per *X1r Smart* su *Argo Local*, non è presente su *Argo from Remote*, a causa del tipo di procedura di registrazione che richiede la presenza in loco dell'utente.

## Letture dello storico degli eventi

Toccando il menu *Events*, è possibile vedere da remoto tutti gli eventi relativi alla serratura. Gli *Events* sono mostrati con la stessa interfaccia utente di *Argo Local* per fornire la migliore esperienza utente e praticità d'uso, seguendo sempre la filosofia di *Argo*: semplicità ed efficacia.



Toccare per inviare gli eventi visualizzati via e-mail o tramite qualsiasi altra app di comunicazione.

A differenza di *Argo Local* non è possibile inviare tutti gli eventi con un solo invio, ma solo quelli precaricati nella memoria del telefono.

Scorrere l'elenco degli eventi verso il basso per visualizzare altri eventi. Tutti gli eventi mostrati possono essere inviati via e-mail.

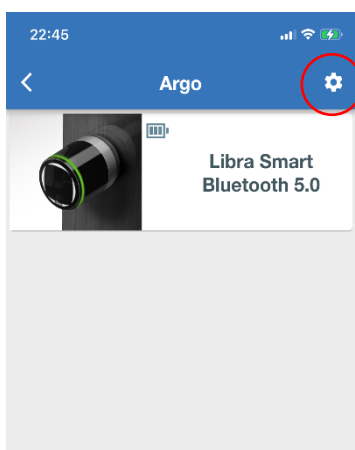
Toccare per aprire lo strumento di ricerca per cercare gli eventi per *Date/Time*, *User* o *Result*, anche solo con alcune lettere o numeri (parole parziali).

# Funzioni avanzate

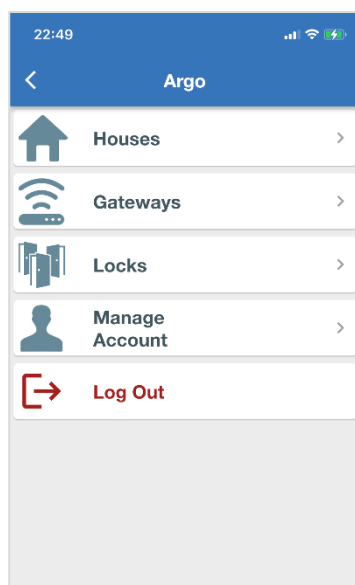
Questa sezione sulle impostazioni avanzate illustra il menu *Argo from Remote* e tutte le funzioni correlate. Dopo la panoramica del menu, ogni funzione verrà spiegata singolarmente.

## Panoramica del menu Argo from Remote

1. Eseguire il login al proprio **account Argo** e toccare l'icona del menu 



2. In questa pagina sono presenti tutti i sottomenu correlati.



Aggiunta, eliminazione, rinomina

Aggiunta, eliminazione, rinomina dei

Aggiunta, eliminazione, rinomina

- Informazioni sull'account
- Abilitazione del riconoscimento di volti o impronte digitali
- Reimpostazione password dell'account
- Eliminazione dell'account

Logout dall'account

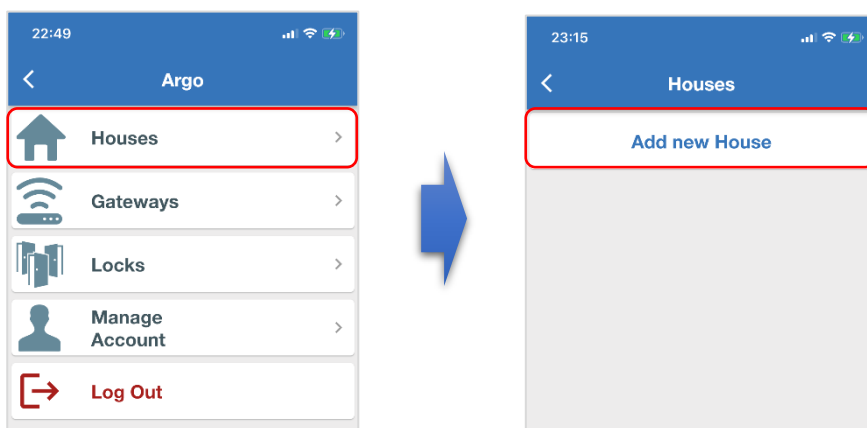
## Houses



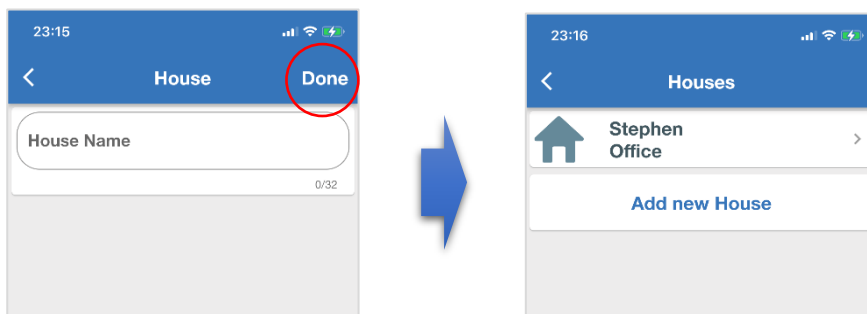
In questo menu è possibile aggiungere una nuova *House* o gestire le case esistenti (eliminare o rinominare).

Per aggiungere una nuova **casa**:

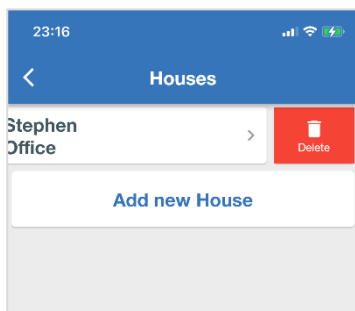
1. Toccare **Houses** e poi toccare **Add new House**.



2. Digitare l'**House Name** e quindi toccare **Done**. La *casa* viene quindi creata.



3. Per eliminare una *casa*, scorrere da destra a sinistra.



4. Per rinominare una *casa* è sufficiente toccarne il nome per entrare in modalità di modifica e rinominarla.

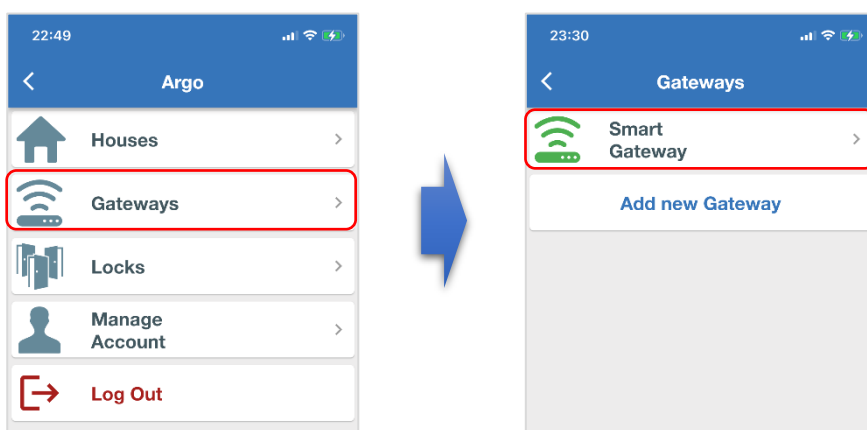
## Gateways



In questo menu è possibile aggiungere un nuovo *gateway* o gestire quelli esistenti: cancellare, rinominare e ottenere informazioni.

Per vedere le informazioni sui **gateway**:

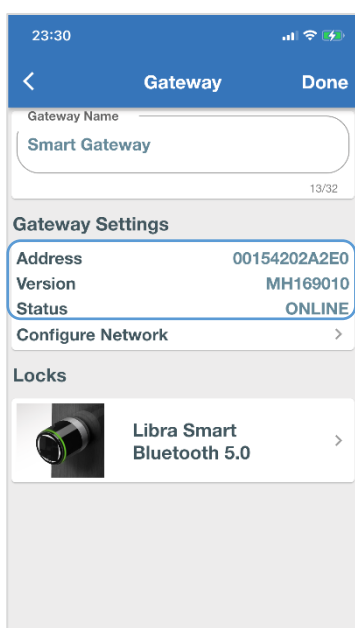
1. Tocca **Gateways**, quindi toccare il nome del gateway che interessa.



Un'icona del *gateway* di colore verde indica che il *gateway* è online. Un'icona rossa indica che il *gateway* è offline (non connesso a Internet).

Toccare **Add a new Gateway** per avviare la procedura guidata mostrata in precedenza (*Impostazioni di base, Configurazione dello Smart Gateway*)

2. In questa pagina è possibile vedere tutte le informazioni sul *gateway*.



Toccare per rinominare il gateway.

Informazioni sul software del gateway.

Toccare per riconfigurare il gateway WiFi. Ad esempio: può essere utile in caso di sostituzione del router.

Serratura collegata a questo gateway. Toccare il nome e l'icona della serratura per accedere direttamente al menu *Locks*, raggiungibile anche dal menu principale (vedere *Locks*).

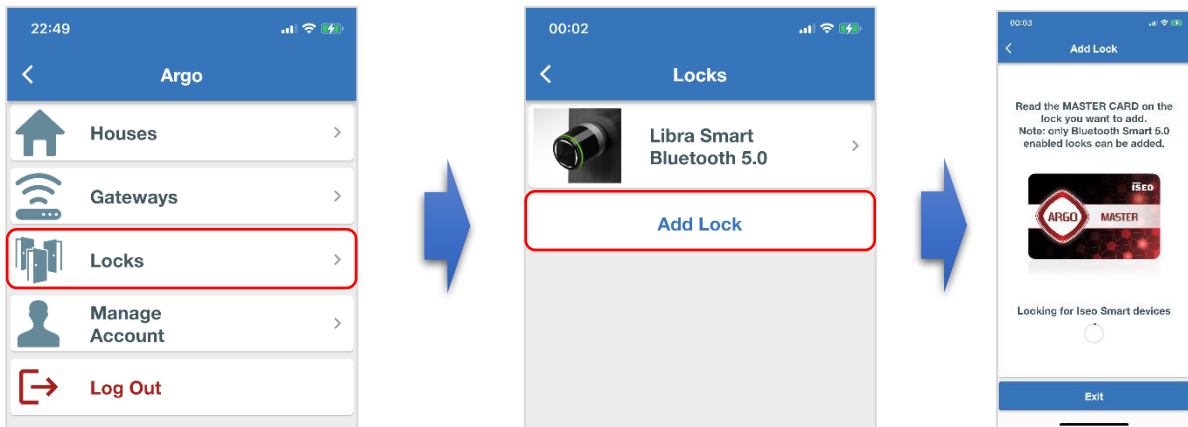
## Locks



In questo menu è possibile aggiungere ed eliminare *serrature* o assegnare e cambiare casa a quelle esistenti.

### Aggiunta di una nuova serratura

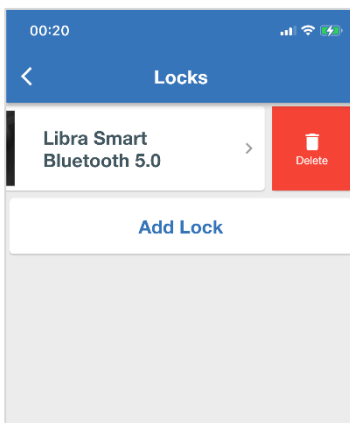
- Toccare **Locks**, quindi toccare **Add Lock**. Viene avviata la stessa procedura guidata descritta in precedenza (vedere *Impostazioni di base, Aggiunta di serrature al sistema*).



Per compiere questa operazione, l'amministratore deve trovarsi davanti alla serratura ed è necessaria la Master Card.

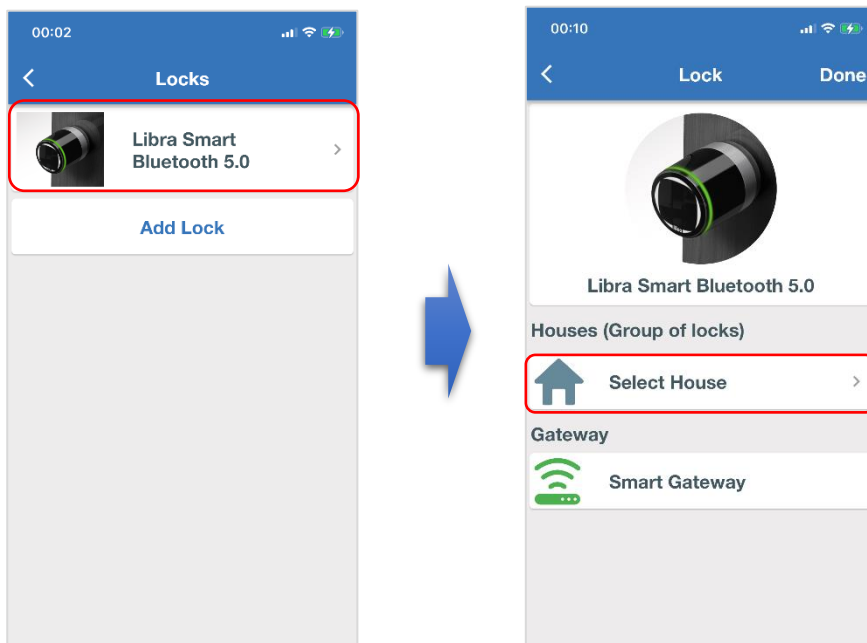
### Eliminazione di una serratura

- Toccare **Locks**, quindi scorrere per eliminare la serratura. Confermare il messaggio di avviso con OK.

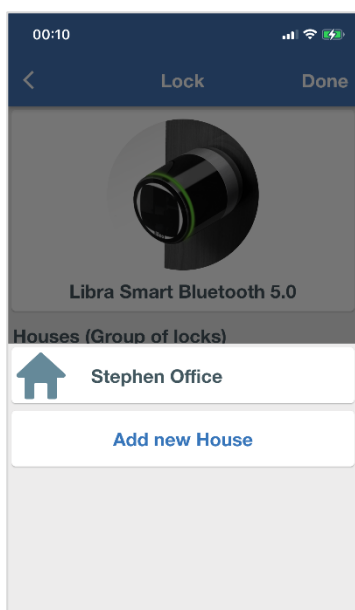


## Assegnazione di serrature a una casa

1. Nel menu *Locks* toccare il nome e l'icona del lucchetto, quindi toccare **Select House**.



2. Scegliere la *casa* da assegnare (es. Stephen Office) o **Add a new House** per crearne una nuova.

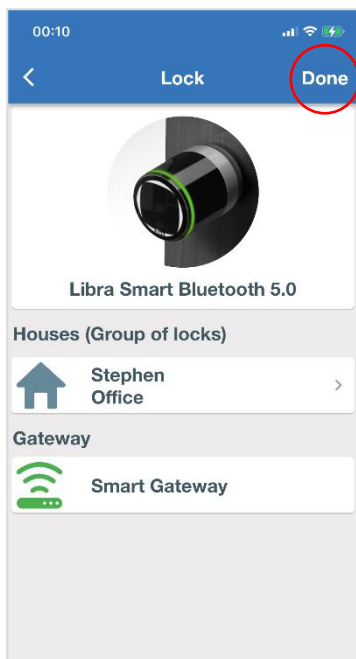


**Casa** precedentemente configurata nel sistema.



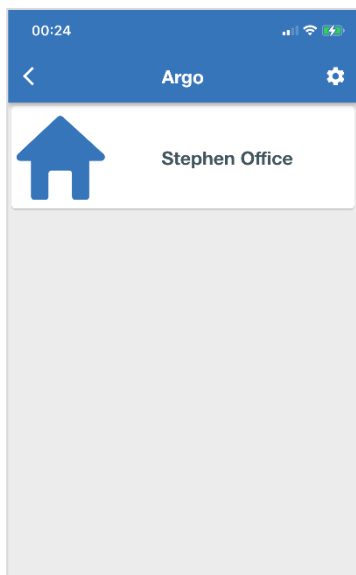
È anche possibile creare case durante la prima configurazione del sistema (*Impostazioni di base, Aggiunta di serrature al sistema*), o direttamente nel menu *House*.

3. Toccare **Done** alla fine per salvare la configurazione.



———— Casa assegnata a questa serratura.

4. Dopo che la *casa* è stata assegnata alla serratura, la *home page di Argo 3.0* cambia nel modo seguente:

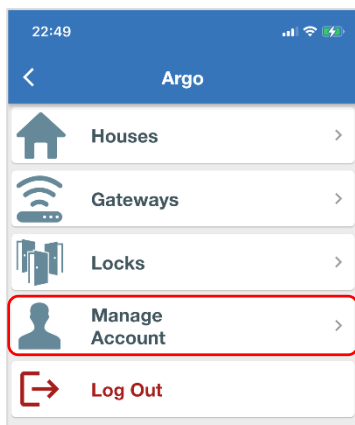


———— **Home page:** la serratura ora è “dentro” la *casa*. Toccare il nome e l'icona della *casa* per vedere le serrature che le appartengono.

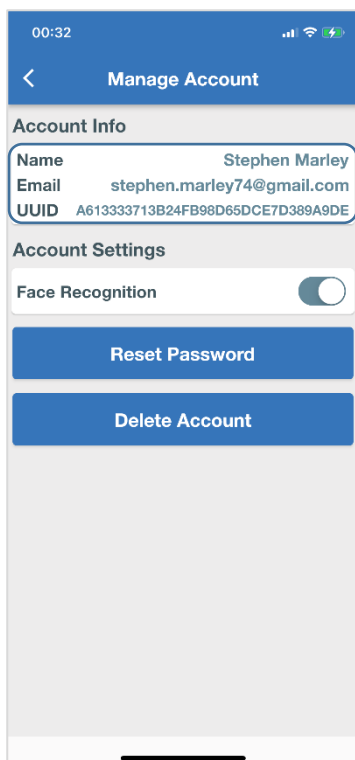
## Manage Account

In questo menu è possibile leggere le informazioni sull'*account* ed eseguire altre operazioni importanti, come mostrato di seguito.

### 1. Toccare **Manage Account**.



### 2. Nel menu **Manage Account** è possibile leggere le seguenti informazioni:



Informazioni sull'*account*.

Abilitare il riconoscimento del *volto* o dell'*impronta digitale* (a seconda della tecnologia dello smartphone), per associare la password della serratura alla propria identificazione biometrica, e così velocizzare il processo di connessione per migliorare l'esperienza utente e la comodità d'uso.

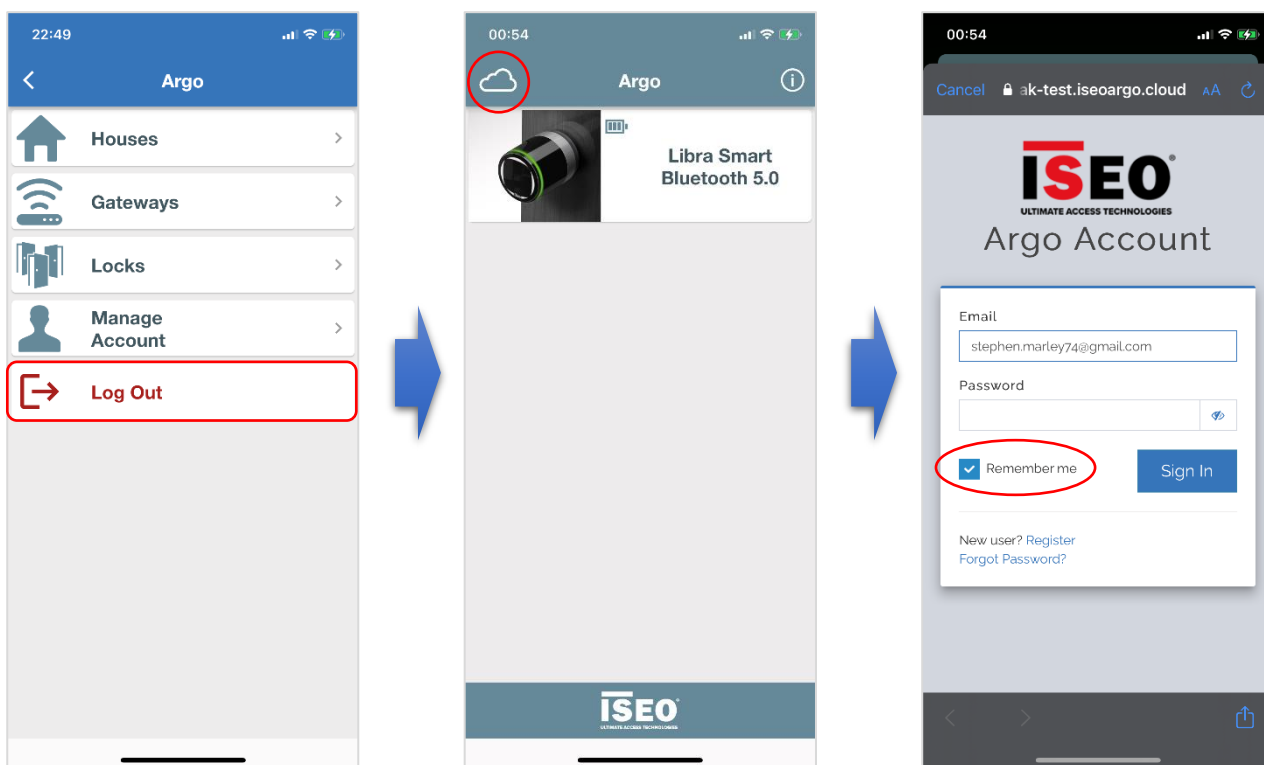
Toccare per reimpostare la password del tuo account, quindi seguire le istruzioni dettagliate.

Toccare per eliminare definitivamente il proprio *account*. Eliminare l'*account* è un'operazione critica se contiene dispositivi configurati (serrature e gateway). Per informazioni su come eliminare correttamente un account, leggere la sezione *Eliminazione dell'account dell'Owner Administrator*.

## Log Out

Toccando **Log Out**, l'*amministratore* viene immediatamente disconnesso dall'*account*. Per eseguire nuovamente il login, l'*amministratore* deve inserire la password dell'*account* personale. Per uscire dall'*account*:

1. Toccare **Log Out** per uscire da *Argo from Remote*. Tocca l'icona *Cloud* per accedere nuovamente.



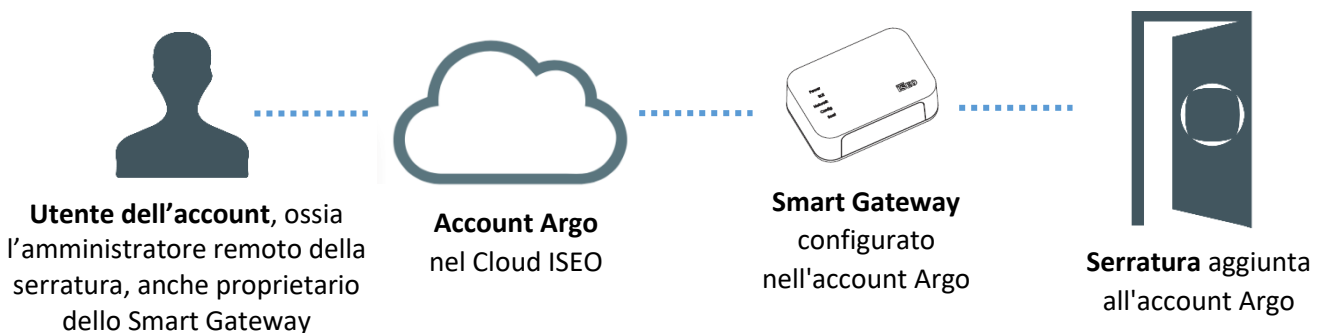
**Log Out** ha la precedenza sulla funzione *Remember me*; può quindi essere utile per motivi di sicurezza, per essere certi che nessuno possa accedere al proprio account anche entrando in possesso del telefono.

La funzione **Remember me** consente di accedere rapidamente all'*account* senza inserire nuovamente la password. La funzione resta attiva per un tempo limitato impostato automaticamente dall'app.

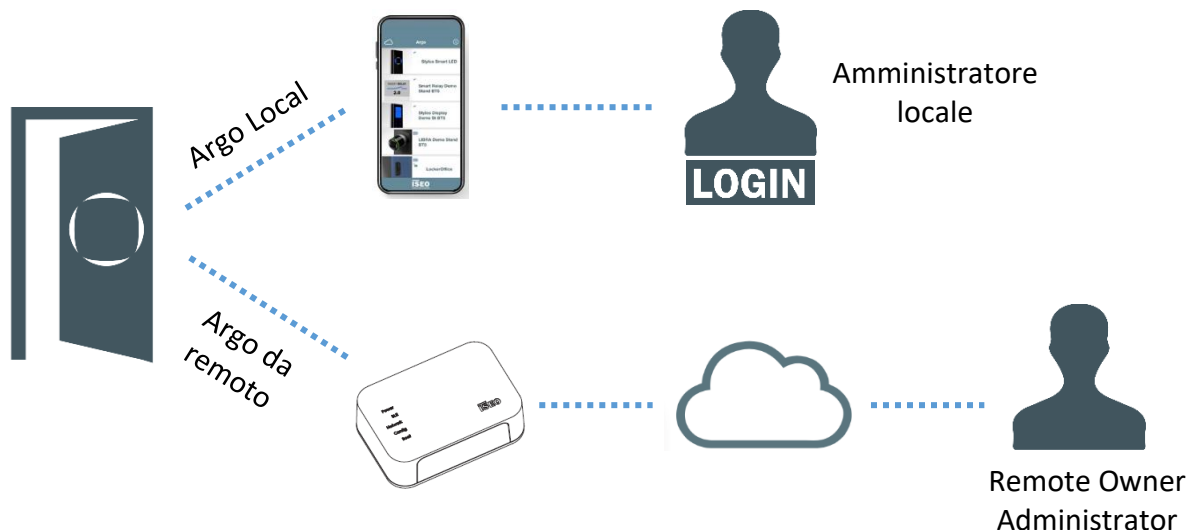
## Account user



L'*Account User* è una nuova identità strettamente correlata ad *Argo from Remote*. Fondamentalmente, si tratta di un *amministratore remoto*. L'*amministratore remoto* deve infatti avere un *account Argo* per esistere, uno spazio nel *Cloud ISEO*, per sfruttare *Argo da Remote*. Questo è fondamentale per raggiungere la serratura tramite uno *Smart Gateway*.



L'*amministratore remoto* non deve' essere confuso con l'*amministratore locale* (vedere *Parole chiave*). Si tratta di due identità diverse che possono coesistere anche nella stessa serratura. Un *amministratore locale* è ciò che abbiamo gestito finora con *Argo Local*: si tratta di qualsiasi utente di smartphone con funzionalità di login. *Argo* può avere molti *amministratori locali* per la stessa serratura, con gli stessi diritti di accesso. In effetti, *Argo Local* non ha diverse *autorizzazioni da amministratore*: tutti gli *amministratori* sono allo stesso livello gerarchico. Si noti che qualsiasi *amministratore locale* può iscrivere altri *amministratori* (con la funzione di *login* abilitata) senza alcuna limitazione: tramite *Master Card* o *su invito* oppure con le funzioni *Add Phone with Argo UID*.

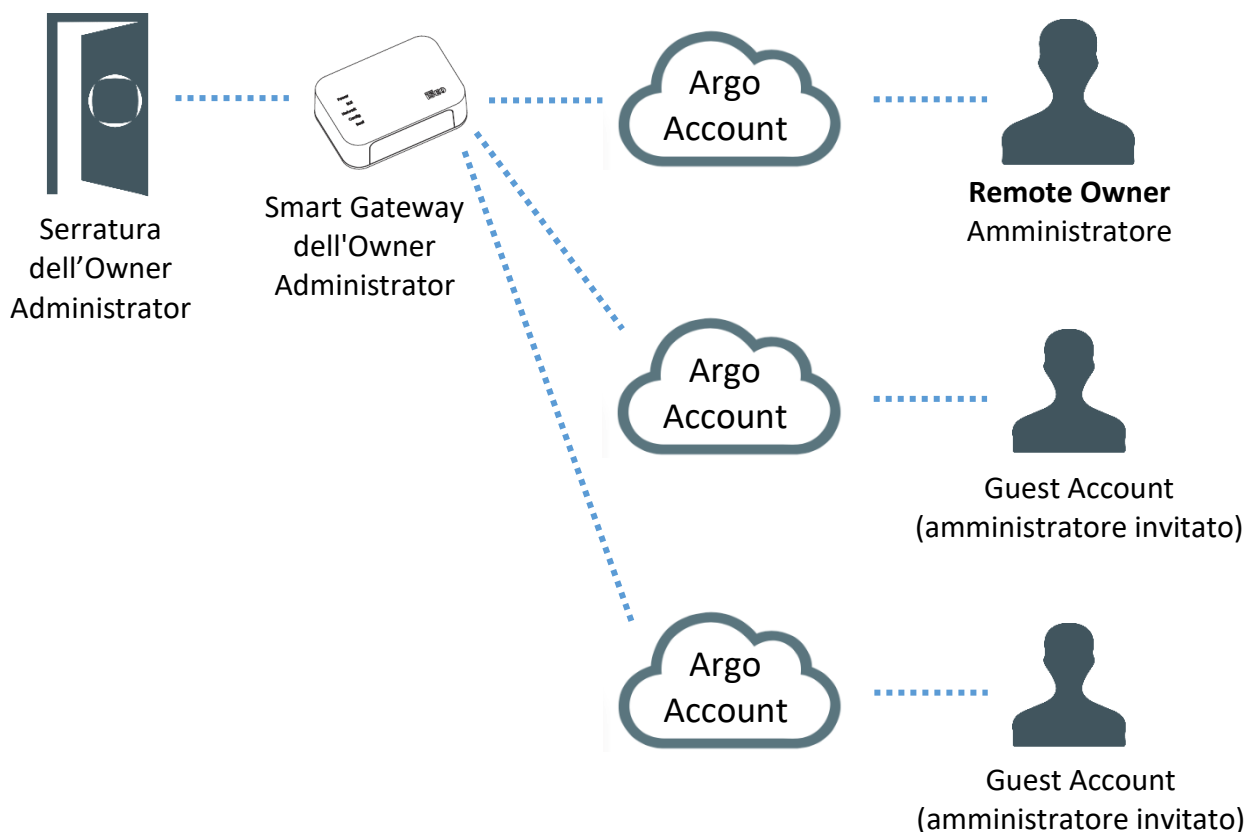


## Guest Account



L'*amministratore remoto*, il primo che ha creato l'*account Argo*, ha configurato lo *Smart Gateway* e aggiunto le serrature al sistema (vedere le *Informazioni di base*), è fondamentalmente il proprietario del Gateway, il proprietario di questo sistema, ecco perché si chiama *Remote Owner Administrator*. L'*Owner Administrator* può anche invitare altri *amministratori remoti*, affinché lo aiutino a gestire una serratura da remoto; ad esempio, per aprire la serratura in caso di situazioni di emergenza o per effettuare il login per aggiungere utenti o controllare eventi. Questi *amministratori remoti* invitati sono chiamati *Guest Account*.

Il *Guest Account* deve avere un *account Argo* valido per operare attraverso il *Cloud ISEO*, ma non ha bisogno di un *gateway* poiché userà il *Gateway dell'Owner Administrator* per comunicare con la serratura a cui sono stati invitati.



*Argo from Remote*, a differenza di *Argo Local*, dà la possibilità di assegnare diverse *autorizzazioni da amministratore* al *Guest Account* (per ulteriori informazioni leggere la sezione *Aggiunta account*).

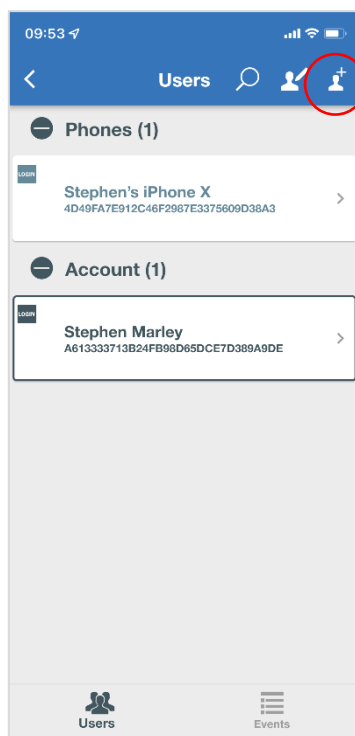
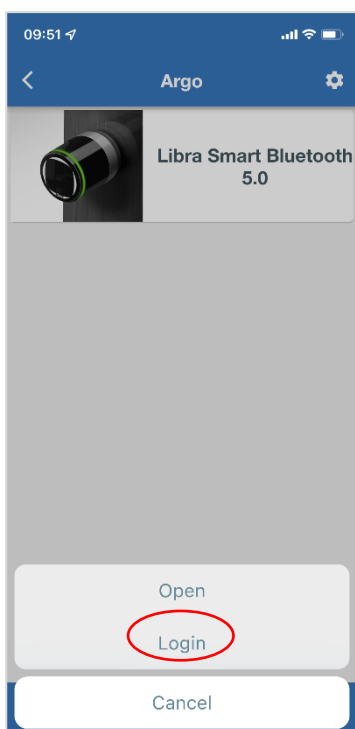
## Aggiunta account (invito di un amministratore remoto)



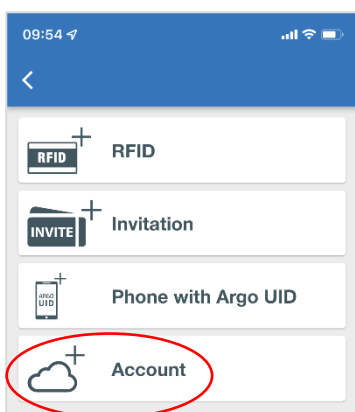
Il *Remote Owner Administrator* può aggiungere uno o più *amministratori* affinché lo aiutino a gestire la serratura da remoto. Questa funzione si chiama *Add Account* e consente di invitare un nuovo *amministratore remoto* chiamato *Guest Account*. Per aggiungere un *Guest Account* alla serratura, procedere come segue.

### 1a parte: l'Owner Administrator invia l'invito al Guest Account.

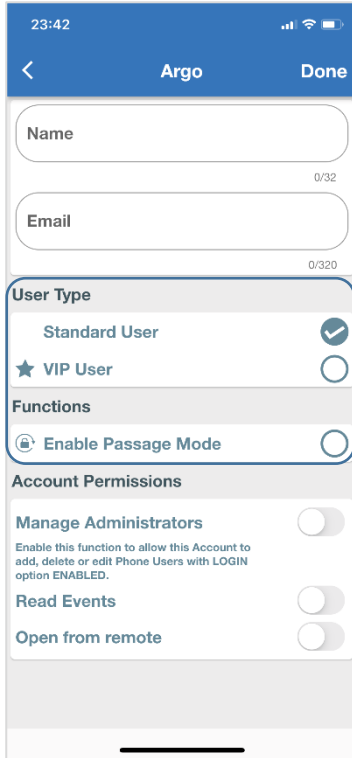
1. Effettuare il login alla serratura, quindi toccare **Add User** 



2. Toccare **Add Account** 



3. Digitare il **Nome** e l'indirizzo **e-mail** dell'*Account Administrator* da invitare. Abilitare le funzioni necessarie e i permessi autorizzati come mostrato nell'immagine di seguito.



Nome del *Guest account*.

Indirizzo e-mail del *Guest Account*.

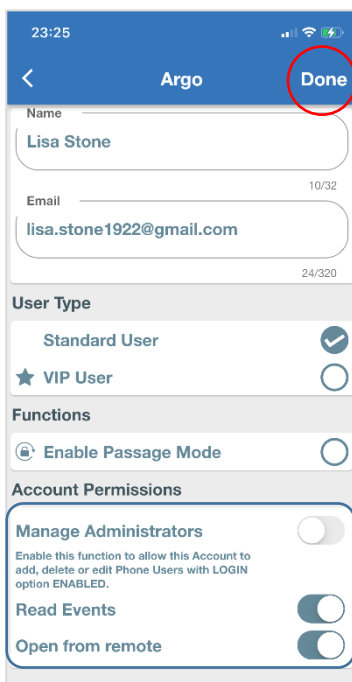
Funzionalità standard di Argo (per ulteriori informazioni, leggere i *manuali utente di Argo 2.7* su [iseo.com](http://iseo.com)).

Andare alla sezione *Manage Administrators*.

Abilitando questa funzione, il *Guest Account* avrà la possibilità di leggere gli *Eventi* relativi alla serratura.

Abilitando questa funzione, il *Guest Account* avrà la possibilità di aprire la serratura da remoto (serratura a cui è stato invitato).

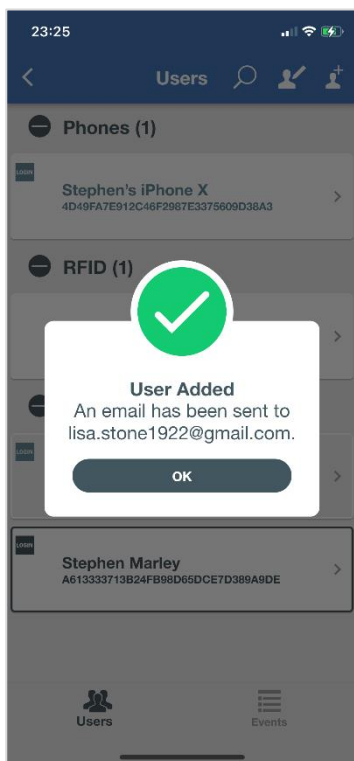
4. Al termine toccare **Done**.




L'*Invited Administrator* deve avere un *account Argo* valido già registrato nel *Cloud ISEO*, altrimenti non può essere aggiunto come *Guest Account* (si verifica un messaggio di errore; per ulteriori informazioni sugli errori leggere la sezione *Ricerca guasti*). È possibile creare un *account Argo* senza aver configurato *Smart Gateway* né serrature.

In questo esempio l'*Invited Administrator* può **leggere gli eventi** e **aprire da remoto** (*autorizzazioni account* abilitate).

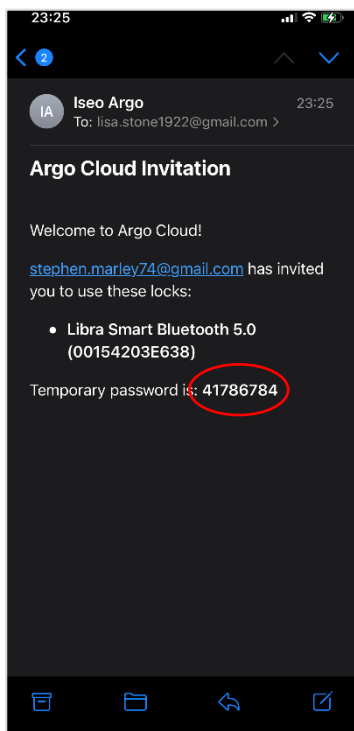
5. Attendere il messaggio di conferma **User Added**, quindi toccare **OK**.



Avvisare il *Guest Account*, che riceverà presto un'e-mail di invito.

## 2a parte: l'Invited Administrator (Guest Account) riceve l'e-mail.

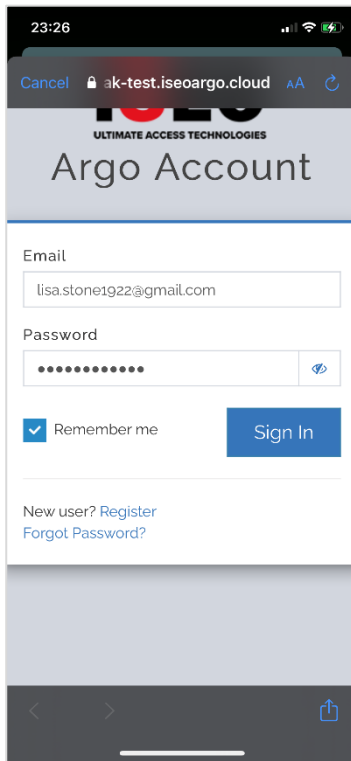
1. L'*Invited Administrator* riceve un'e-mail come nell'esempio riportato di seguito.



La *password temporanea* viene generata automaticamente nel messaggio di invito e sarà la *Account Lock Password*. È necessario affinché il *Guest Account* possa comunicare con la serratura (apertura e login).

Per motivi di sicurezza, una volta effettuato il login per la prima volta, il *Guest Account* dovrebbe cambiare la password temporanea digitandone una personale.

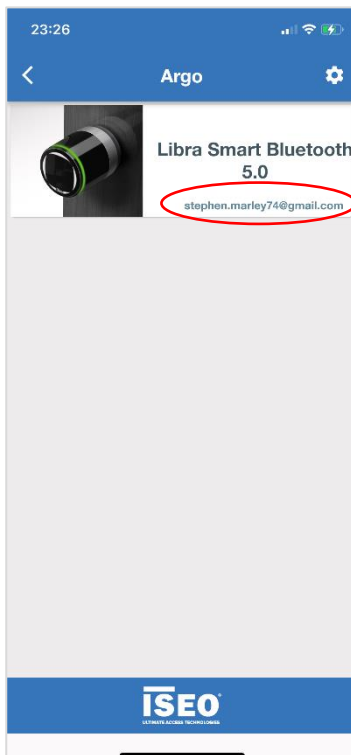
2. L'*Invited Administrator* accede al suo *account di Argo from Remote*.



L'*Invited Administrator* deve avere un *account Argo* valido nel *Cloud ISEO*, altrimenti non può essere invitato dall'*Owner Administrator* (per informazioni su come impostare un nuovo *account*, leggere la sezione *Impostazioni di base, Creazione dell'account Argo*).

È possibile creare un *account Argo* senza aver configurato alcuno *Smart Gateway* né serrature.

3. L'*Invited Administrator* troverà la serratura a cui è stato invitato nella *home page di Argo from Remote*.



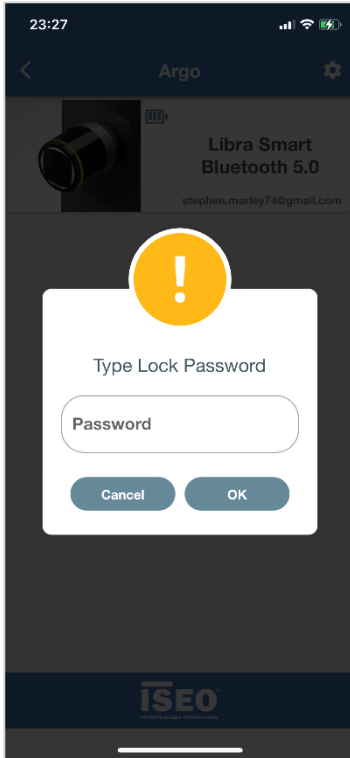
La nuova serratura che appartiene all'*Owner administrator* Stephen Marley ora appare nella *home page dell'account* di Lisa Stone.



Sotto il nome e l'icona della serratura viene riportato l'indirizzo e-mail dell'*Owner Administrator* per notificare immediatamente che questa serratura appartiene a un altro *account Argo*.

Il messaggio *Configure your system* non viene visualizzato perché questo *account* userà il *gateway* dell'*Owner Administrator* della serratura. Questo *account* può sempre aggiungere un proprio

4. Toccare il nome e l'icona della serratura per avviare la comunicazione. È necessaria la *Lock Account Password* per connettersi al blocco.

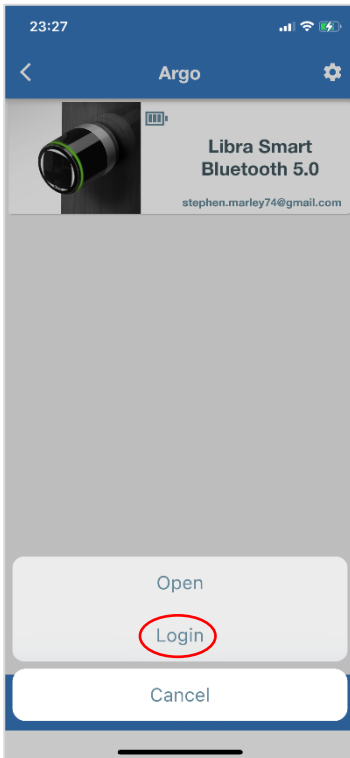


Digitare la *password della serratura* temporanea ricevuta nell'e-mail di invito.



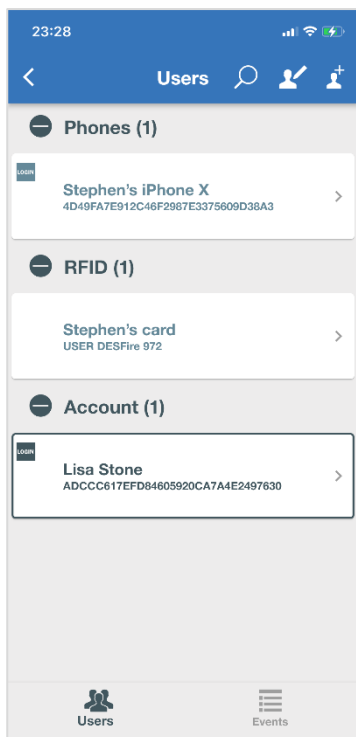
Abilitare il riconoscimento del *volto o dell'impronta digitale* nel menu *Manage Account* per associare la password all'identificazione biometrica del telefono.

5. Toccare **Login**.



Open è disponibile perché abilitato nell'*Account Permission* dall'*Owner Administrator*.

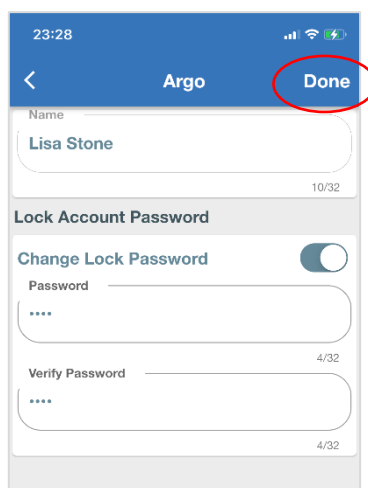
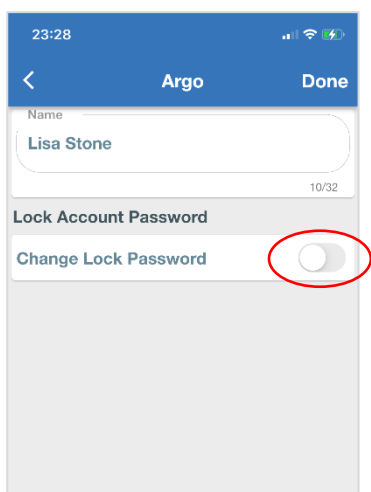
6. Viene visualizzato l'elenco utenti di Argo from Remote.



L'account dell'Owner Administrator non è visibile dal Guest Account. Quest'ultimo non può modificare alcuna impostazione del proprietario della serratura.

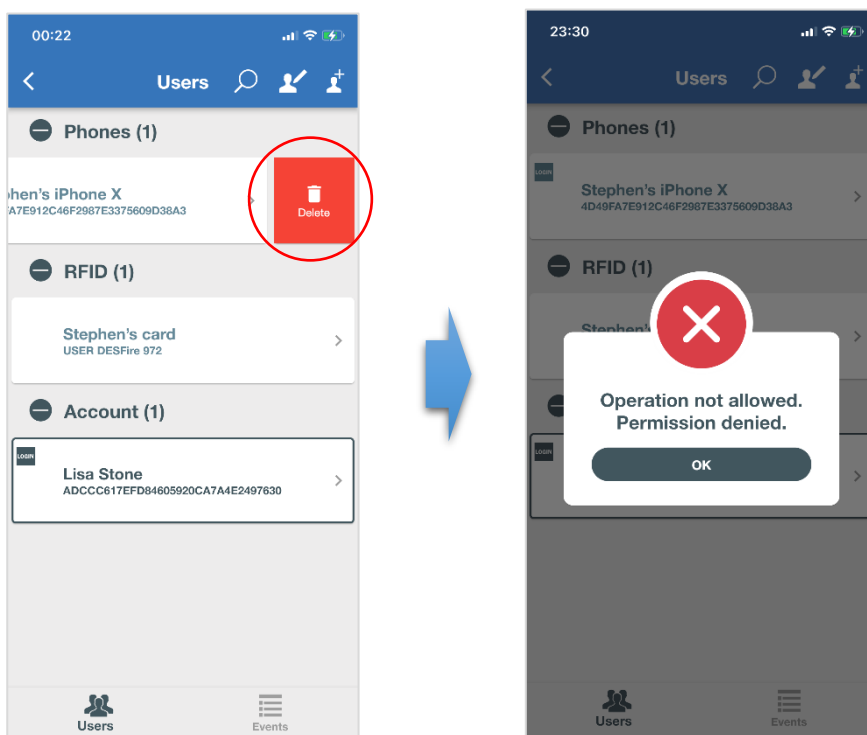
Guest Account

7. Toccando il suo account, Lisa Stone può solo modificare la password della serratura. Per motivi di sicurezza si consiglia vivamente di cambiare la password temporanea della serratura con una password personale. Per modificare la password, attivare il pulsante a scorrimento, digitare la nuova password e premere **Done**. Il sistema tornerà alla home page di Argo from Remote. Infine, toccare il nome e l'icona della serratura e inserire la nuova password per connettersi.

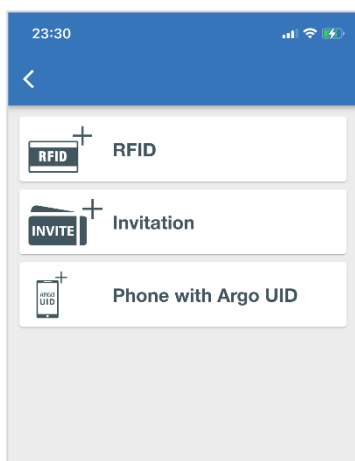


Abilitare il riconoscimento del volto o dell'impronta digitale nel menu Manage Account per associare la password all'identificazione biometrica del telefono.

8. Considerando le *autorizzazioni dell'account* impostate dall'*Owner Administrator*, Lisa Stone può *aprire da remoto e leggere eventi*, ma non può *gestire gli amministratori*. Ciò significa che non può aggiungere, eliminare o modificare *gli utenti del telefono* con il login. Esempio: se Lisa Stone tenta di eliminare l'*iPhone dell'amministratore utente del telefono Stephen*, riceverà il messaggio di errore illustrato nell'immagine qui sotto e l'operazione non sarà completata.



9. Lisa può effettuare il login, aggiungere, modificare o eliminare qualsiasi tipo di credenziale, poiché queste sono le operazioni di base e fondamentali che può svolgere qualsiasi *amministratore*. Non può aggiungere alcun *Guest Account* poiché non è la proprietaria della serratura.



Solo l'*Owner Administrator* può aggiungere *Guest Account* alla sua serratura (invitare altri amministratori).

## Eliminazione dell'account

L'eliminazione di un *account* è un'operazione critica poiché coinvolge tutti i *gateway* e le *serrature* configurati. Un *account* può avere anche uno o più *Guest Account* che condividono alcune delle sue serrature.


Per riassumere, prima di eliminare un *account*, occorre prendere in considerazione:

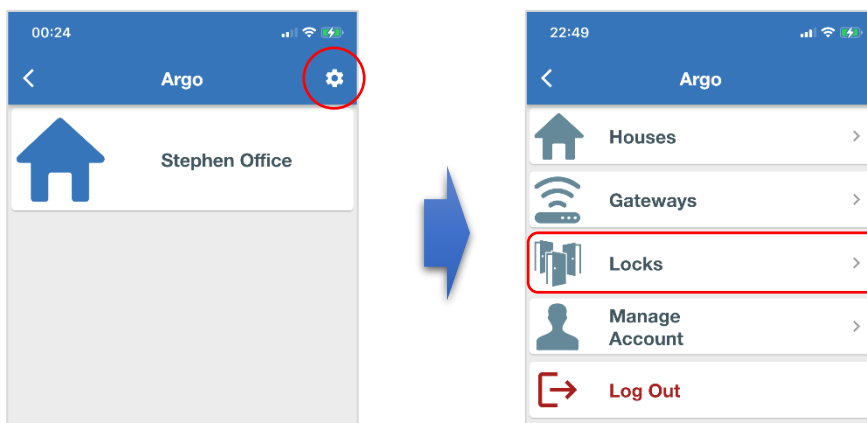
- Numero di **gateway** configurati nell'*account*.
- Numero di **serrature** collegate ai gateway.
- Qualsiasi **Guest Account** che condivide uno o più serrature.



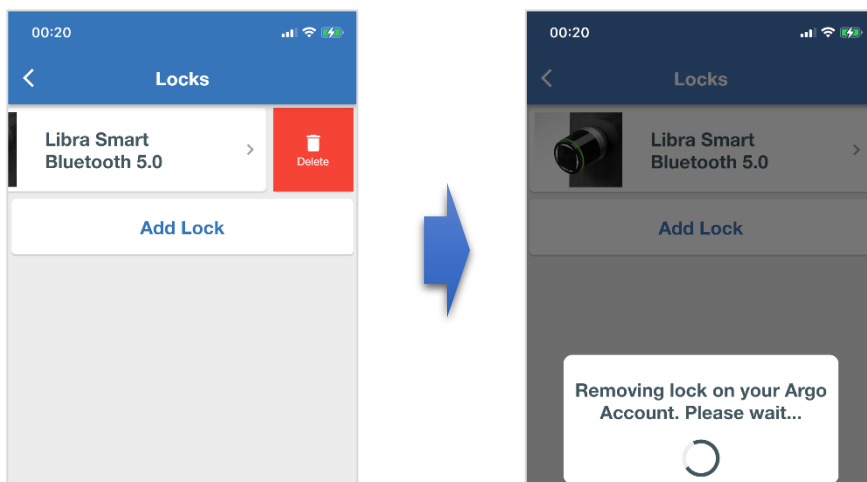
Solo l'*Owner Administrator* può cancellare il suo *account* e i *Guest Account* invitati. Se l'*Owner Administrator* cancella l'*account*, tutti i *Guest Account* che ne fanno parte verranno eliminati automaticamente.


Nel prossimo esempio elimineremo l'*account* creato in precedenza (*Impostazioni di base, Creazione dell'account Argo*).

1. Effettuare il login all'**account** e toccare l'icona del menu  , quindi toccare **Locks**.



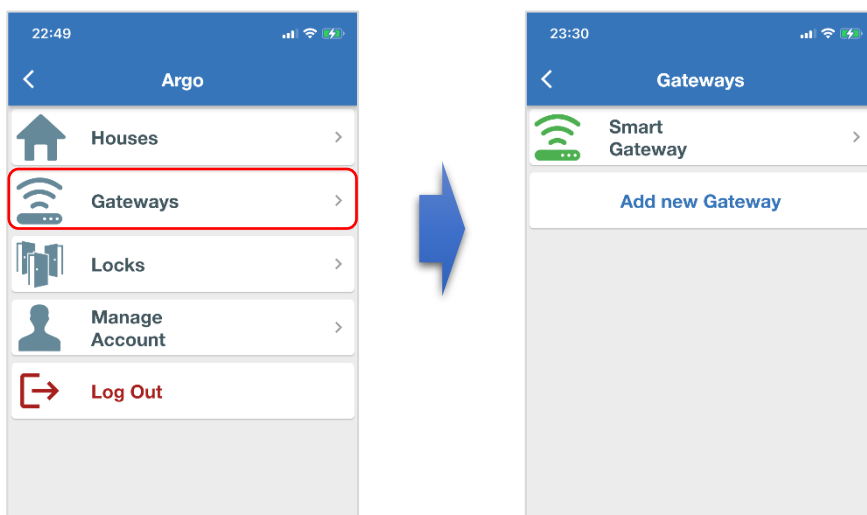
2. Elimina tutte le **serrature** una per una, forndo la password della serratura o l'identificazione biometrica del telefono.



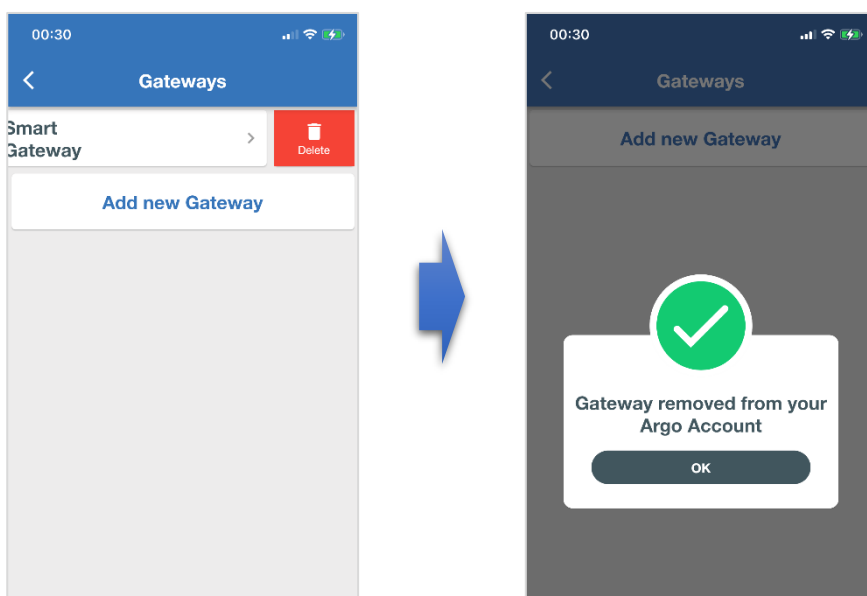
 Rimuovendo una *serratura* dall'*account dell'Owner Administrator*, la serratura sarà automaticamente rimossa da tutti i *Guest Account* invitati, se presenti.


Lo stesso accade quando l'*Owner Administrator* elimina il *Guest Account* dalla serratura.

3. Tornare al menu principale, quindi toccare **Gateways**.

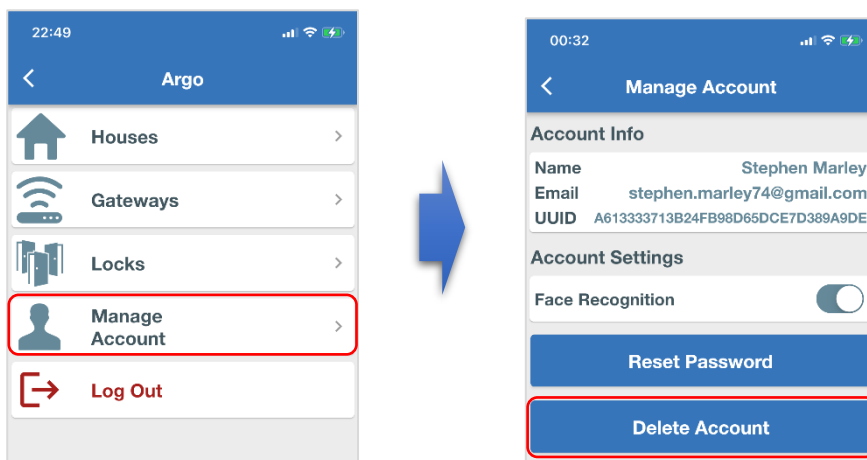


4. Eliminare il **gateway**, scorrendo sempre da destra a sinistra e confermare il messaggio.

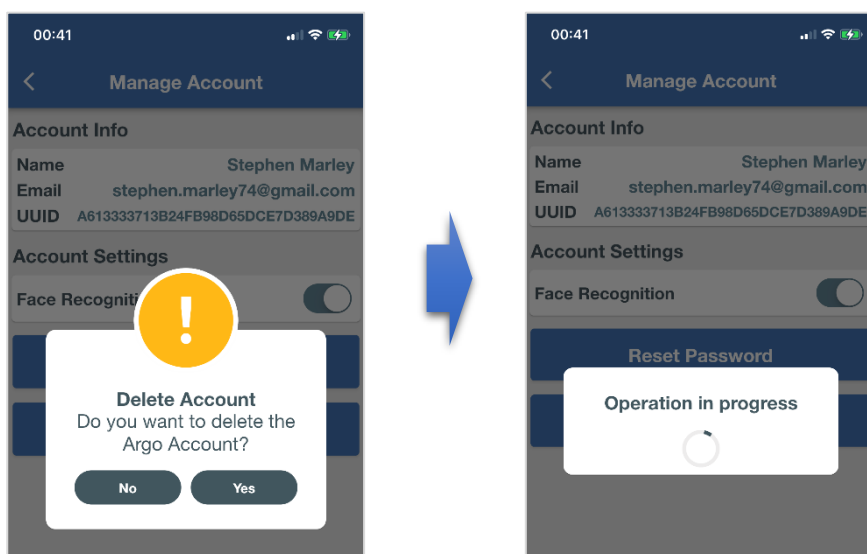


 Un **gateway** connesso a una *serratura* non può essere rimosso e l'app visualizzerà un messaggio di errore. Assicurarsi che tutte le *serrature* siano state eliminate prima di eliminare un *gateway* (per maggiori informazioni sugli errori, vedere la sezione *Ricerca guasti*).

5. Tornare al menu principale e toccare **Manage Account**, quindi toccare **Delete Account**.



6. Confermare con **Yes** al messaggio di avviso e attendere che l'*account* venga eliminato.



Tutte le **case** verranno rimosse automaticamente durante la cancellazione dell'*account*.

Se si tenta di accedere a un *account* eliminato, verrà visualizzato il messaggio: *Invalid username or password*. Il messaggio viene mostrato per motivi di sicurezza, per non rivelare account esistenti o non esistenti se qualcuno tenta di inserire un indirizzo e-mail a caso.

# Domande e risposte

Di seguito sono riportate alcune delle domande più comuni e le relative risposte.

1. L'*account Argo* è sicuro? Cosa succede se un hacker, in qualche modo, entra nel mio *account*?  
L'hacker può aprire la porta da remoto o eseguire altre operazioni?

**Risposta:** anche se qualcuno riesce ad accedere a un *account Argo*, l'hacker non può eseguire alcuna operazione sulla *serratura* poiché è richiesta la *password della serratura dell'account*. E questa password è memorizzata nel posto più sicuro: all'interno della serratura. L'*account* viene utilizzato solo come tunnel.

2. Il *gateway* è sicuro? Cosa succede se un hacker, in qualche modo, raggiunge e si connette al mio *gateway*? L'hacker può aprire la porta da remoto o eseguire altre operazioni?

**Risposta:** se qualcuno riesce a connettersi al *gateway*, l'hacker non può fare nulla poiché il *gateway* viene utilizzato solo come tunnel. Nessuna informazione viene memorizzata nel *gateway*. Il *gateway* è solo un tunnel utilizzato per raggiungere e comunicare con la *serratura*. Tutte le informazioni rilevanti si trovano nel posto più sicuro: all'interno della serratura e protette da password.

3. Quante serrature possono essere collegate a uno *Smart Gateway*?

**Risposta:** non esiste un numero definito. Lo *Smart Gateway* funziona come uno smartphone con *Argo*, quindi la risposta è: tutte le serrature all'interno del raggio di portata *Bluetooth* del *gateway*.

4. Cosa succede se ho diversi *Smart Device ISEO*, ma sono distanti più di 10 metri? È possibile configurare più di 1 *gateway* con lo stesso *account*, in modo che tutti gli smart device possano essere collegati e raggiunti?

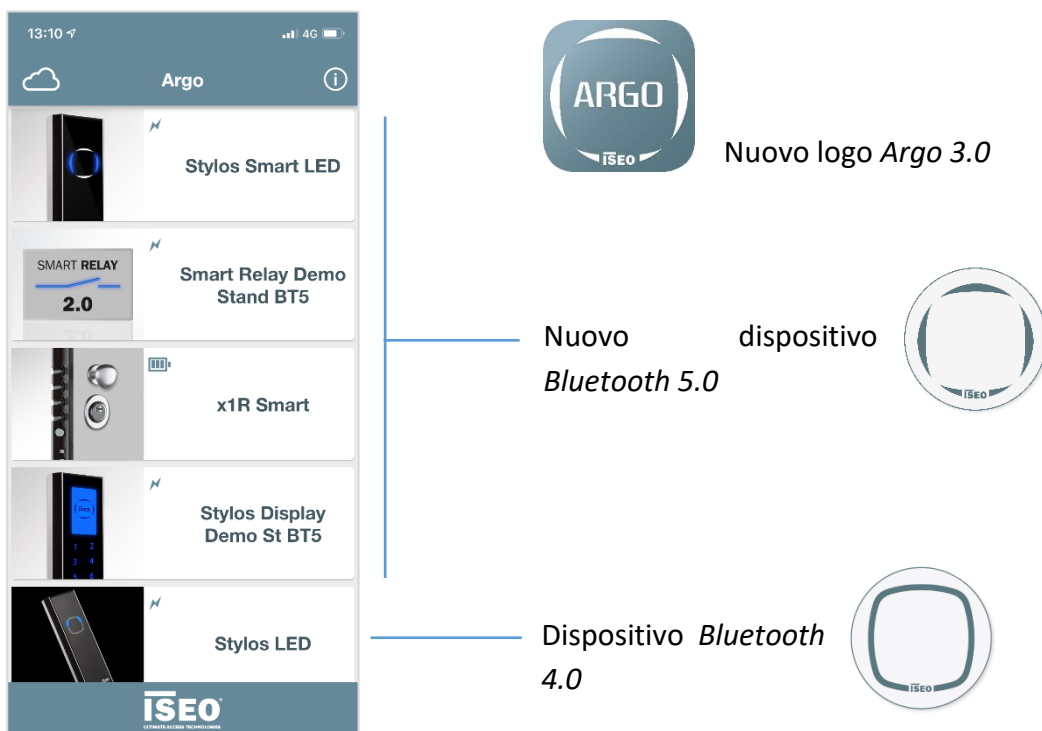
**Risposta:** sì, è possibile aggiungere altri *gateway* al proprio *account Argo* per raggiungere diverse serrature, lontane l'una dall'altra.

5. Posso collegare gli *Smart Device ISEO Bluetooth 4.0* al *gateway*? Il *gateway* funziona anche con la tecnologia *Bluetooth 4.0*?

**Risposta:** no, lo *Smart Gateway* è compatibile solo con gli *Smart Device ISEO Bluetooth 5.0* e funziona solo tramite la tecnologia *Bluetooth 5.0*. Questa tecnologia consente più connessioni contemporaneamente, il che è obbligatorio per lavorare con *Argo from Remote*.

## 6. Come faccio a riconoscere uno *Smart Device ISEO Bluetooth 5.0*?

**Risposta:** Lo si riconosce dal nuovo design del logo, che mostra l'evoluzione della tecnologia *Bluetooth 5.0*. Il nuovo logo è stampato su tutte le cover estetiche degli *Smart Device ISEO BLE 5*. È anche possibile riconoscere gli *Smart Device ISEO Bluetooth 5.0* dall'app Argo: i nuovi dispositivi vengono visualizzati nella *schermata della home page* con una nuova icona che mostra il nuovo design del logo.



## 7. Posso aggiornare gli *Smart Device ISEO Bluetooth 4.0* alla tecnologia *Bluetooth 5.0* per gestirli da remoto tramite uno *Smart Gateway*?

**Risposta:** no, gli *Smart Device ISEO Bluetooth 4.0*, tranne *X1r Smart*, non possono essere aggiornati a *Bluetooth 5.0*. È necessario sostituire l'intero dispositivo per gestirlo da remoto. *X1r Smart* è l'unica eccezione perché questa serratura è composta da 2 dispositivi: la serratura meccanica all'interno della porta e il lettore di credenziali, che incorpora il *Bluetooth*, solitamente posizionato all'esterno della porta. Per aggiornare *X1r Smart* a *Bluetooth 5.0* occorre:

- Sostituisci l'intero lettore con una versione *Bluetooth 5.0*.
- Aggiornare il firmware di *X1r Smart* con un'app di servizio chiamata *ISEO App Tool*. Video tutorial disponibile al link: <https://www.youtube.com/watch?v=W0gmzzra0f8>



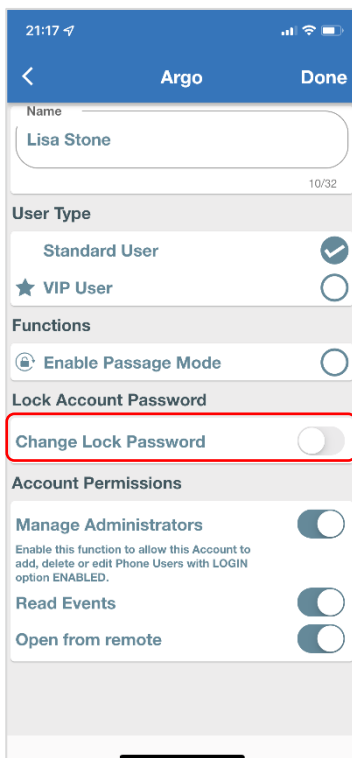
Questa operazione è destinata esclusivamente a installatori o personale competenti e adeguatamente formati.

8. *Argo Local* consente di memorizzare 300 *utenti* nella serratura della porta. Cosa succede quando aggiungo un *gateway* e la *serratura* nell'*account Argo*? Cambia la capacità di *utenti* della *serratura*? **Risposta:** sì, durante la configurazione il *gateway* e l'*account dell'Owner Administrator* sono registrati nella memoria della *serratura*. Queste sono considerate 2 credenziali: ecco perché la capacità degli utenti cambia. Ad esempio: 300 *utenti* diventano 298 *utenti*. Ciò è dovuto al principio di funzionamento di *Argo* chiamato *data on device*. È anche il punto di forza di *Argo* in termini di sicurezza: il *gateway* è infatti usato solo come tunnel e tutti i dati si trovano nel posto più sicuro, all'interno della serratura.

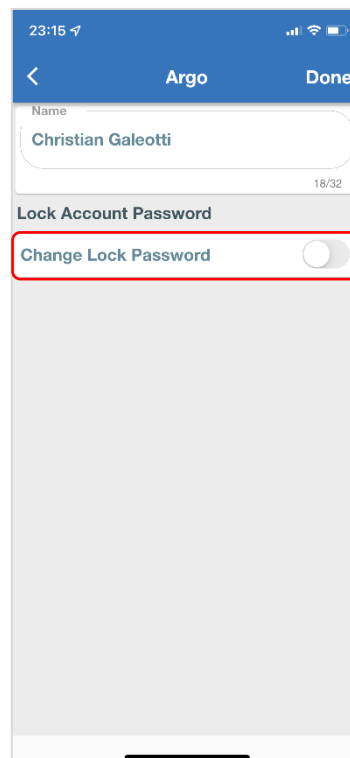
9. Dove posso cambiare la *Lock Account Password*? Non riesco a trovarlo.

**Risposta:** la *Lock Account Password* è memorizzata nel posto più sicuro, all'interno della serratura. È strettamente correlata a ciascuna serratura e può essere diversa da una serratura a un'altra, a seconda della scelta dell'amministratore. È diversa anche da *account* ad *account* quando diversi *amministratori remoti* gestiscono lo stesso blocco (*Account Guest*). Ecco perché per modificarla è necessario eseguire il *login* alla serratura specifica, inserire le impostazioni dell'*account dell'amministratore* e modificare la *Lock Account Password*.

Password della serratura - Impostazione dell'account dell'Owner Administrator



Password della serratura - Impostazione del Guest Account



10. Come posso scollegare una *serratura* da un *gateway*?

**Risposta:** nell'*account Argo*, andare al menu *Lock*, successivamente eliminare la *serratura* dall'*account* (semplicemente scorrendo da destra a sinistra). Si noti che: selezionando *Reset to Factory* per la serratura di *Argo Local*, anche la serratura verrà rimossa dall'*account*.

11. Il *gateway PoE* funziona anche tramite WiFi?

**Risposta:** no, il *gateway PoE* non ha il WiFi integrato; può essere collegato solo a una porta LAN del router tramite cavo Ethernet. Può essere alimentato sia dal router tramite una porta PoE sia da un alimentatore esterno, se il router non fornisce la porta PoE.

12. Non ricordo la *Lock Account Password*. Cosa posso fare?

**Risposta:** per motivi di sicurezza non è possibile recuperare la *Lock Account Password*. L'unica soluzione per l'*amministratore* è eliminare la *serratura* dall'*account* (vedere *Impostazioni avanzate, Locks, Eliminazione di una serratura*) e quindi aggiungerla nuovamente utilizzando la *Master Card* proprietaria (vedere *Impostazioni avanzate, Locks, Aggiunta di una serratura*).

13. Ci sono telefoni non compatibili con il *Bluetooth 5.0*?

**Risposta:** no, tutti i telefoni compatibili *Bluetooth 4* sono automaticamente compatibili con il *Bluetooth 5.0*.

14. Il *Bluetooth 5.0* è multicanale, ovvero permette più connessioni allo stesso momento. Ma quanti utenti possono collegarsi ad una serratura contemporaneamente?

**Risposta:** per preservare la performance ottimale del sistema e la fruibilità, evitando conflitti nelle operazioni, si possono collegare al massimo 2 utenti. Per esempio: un utente che apre la porta *da locale* e contemporaneamente un utente amministratore che *da remoto* effettua il LOGIN alla serratura. Questa è anche la situazione più comune e frequente.

15. È possibile aggiungere più Gateway allo stesso impianto? Come vengono gestiti dal sistema? Come fa la serratura a sapere a quale gateway riferire?

**Risposta:** sì, è possibile aggiungere più Gateway proprio perché le serrature potrebbero essere a una distanza superiore di 10mt tra loro. L'assegnazione Gateway-Serratura avviene durante il processo di configurazione ed è gestita dalla app Argo che automaticamente si collega al gateway più vicino (segnale più forte) e di conseguenza associa ad esso la serratura. Anche durante il collegamento da remoto il processo viene gestito automaticamente dalla app.

16. È possibile aprire la porta mentre un utente amministratore è collegato da remoto e sta effettuando operazioni sulla serratura?

**Risposta:** sì, è possibile perché il Bluetooth 5.0 è multicanale (vedi anche p.to 14).

17. Posso cambiare il nome della serratura da remoto?

**Risposta:** no, è possibile cambiare il nome della serratura solo da locale. In automatico verrà poi aggiornato anche da remoto al successivo login nell'*Argo Account*.

18. Posso aggiungere un'impronta digitale per x1R Smart da remoto?

**Risposta:** no, l'impronta digitale può essere aggiunta solo da locale. Questo per la necessità di interazione diretta dell'utente che è richiesta durante la registrazione dell'impronta. È possibile aggiungere da remoto codici PIN, credenziali con UID, telefoni e inviti.

19. Può aprire chiunque un *account Argo* anche se non ha serrature né *Gateway*?

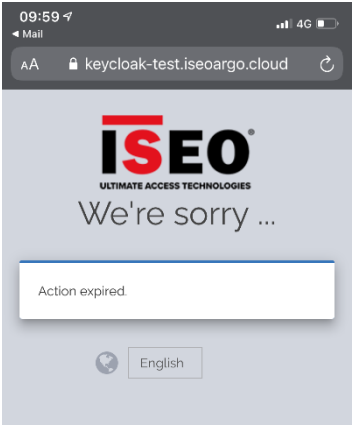
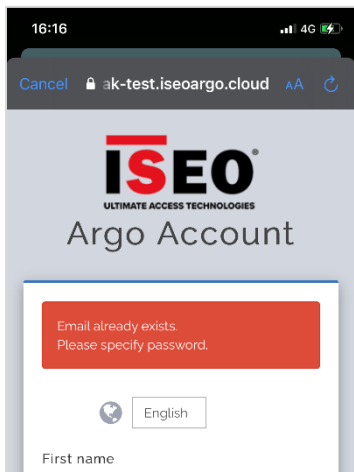
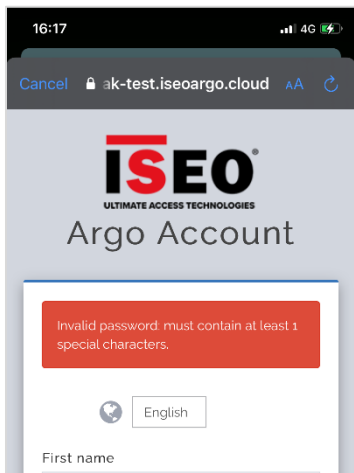
**Risposta:** sì, chiunque può aprire un *account Argo*, è sufficiente un indirizzo e-mail valido e una password a scelta. Per esempio: un amministratore invitato dal proprietario, dovrà necessariamente registrare un *account Argo*, anche se non proprietario di alcun impianto, per poter poi gestire la serratura alla quale è stato invitato.

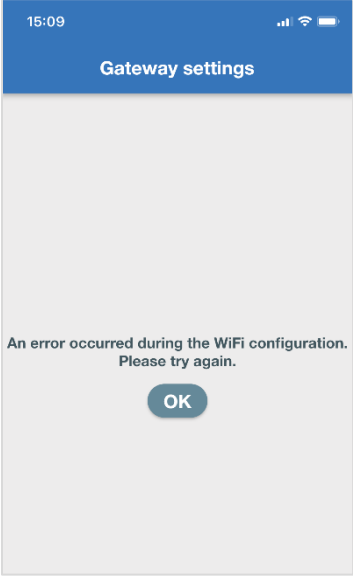
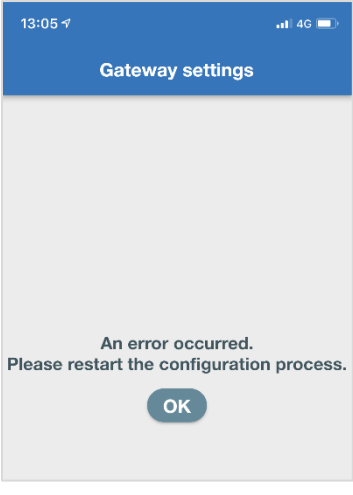
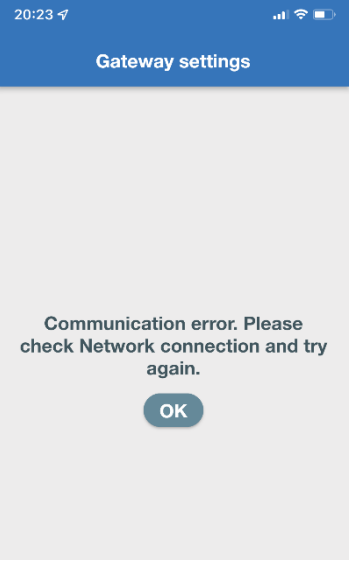
20. È possibile condividere lo stesso *Gateway* tra diversi *account Argo* proprietari con differenti codici impianto (*Master Card*)? È il caso, per esempio, della porta comune di un condominio condivisa tra i vari appartamenti, dove ogni appartamento è un impianto *Argo* distinto.

**Risposta:** no, per ragioni di sicurezza e affidabilità dell'impianto e della struttura software, un *Gateway* viene assegnato ad un unico impianto e l'amministratore proprietario è unico. L'amministratore proprietario può comunque invitare altri amministratori a gestire la serratura. Nel caso dell'esempio della porta comune del condominio, potrà essere gestita dall'amministratore condominiale che potrà garantire l'accesso ai condomini e dovrà gestire di conseguenza le autorizzazioni di accesso.

# Ricerca guasti

Di seguito sono riportati i messaggi di errore più comuni e la relativa spiegazione.

Errore	Significato	Cosa fare
	<p>Si è impiegato troppo tempo per completare un passaggio della procedura di registrazione dell'account. Per motivi di sicurezza esiste un time-out e una volta scaduto viene visualizzato questo messaggio di errore.</p>	<p>Ripetere l'operazione più velocemente.</p>
	<p>È stata inserita un'e-mail già esistente durante la registrazione dell'account Argo.</p>	<p>Scegliere un indirizzo e-mail diverso per registrare un nuovo account o utilizzare quello già esistente.</p>
	<p>Non è stata digitata una password abbastanza forte.</p>	<p>Digitare una password di almeno 8 caratteri che contenga 1 lettera maiuscola, 1 numero e 1 carattere speciale.</p>

Errore	Significato	Cosa fare
	<p>Questo errore potrebbe verificarsi durante la configurazione del gateway, al primo passaggio, quando il gateway sta tentando di connettersi al router WiFi. Di solito significa che è stata inserita una password del router errata.</p>	<p>Toccare OK per riavviare il processo e riprovare. Assicurarsi di inserire la password del router corretta. Utilizzare la funzione di visualizzazione della password per ricontrollarla.</p> <p>Se il problema persiste controllare il router WiFi verificando se è raggiungibile da un altro dispositivo (PC, smartphone, tablet).</p> <p>Se non è possibile risolvere il problema, contattare il <i>Service Operation Center ISEO</i> (vedere la sezione <i>Supporto tecnico</i>).</p>
	<p>Questo errore potrebbe verificarsi durante la configurazione del gateway, al primo passaggio, quando il gateway sta tentando di connettersi al router WiFi. La password è corretta ma, per qualche motivo, il router ha rifiutato la connessione con il gateway.</p>	<p>Toccare OK per riavviare il processo e riprovare.</p> <p>Se il problema persiste controllare il router WiFi verificando se è raggiungibile da un altro dispositivo (PC, smartphone, tablet).</p> <p>Se non è possibile risolvere il problema, contattare il <i>Service Operation Center ISEO</i> (vedere la sezione <i>Supporto tecnico</i>).</p>
	<p>Questo errore potrebbe verificarsi durante la configurazione del gateway, al secondo passaggio, quando il gateway tenta di connettersi al Cloud ISEO per essere caricato nell'account Argo. Per qualche motivo la comunicazione tra gateway e Cloud non è riuscita. Questo problema può essere causato da diversi problemi:</p> <ol style="list-style-type: none"> <li>1. Connessione Internet lenta</li> <li>2. Firewall che blocca la comunicazione</li> <li>3. Errore durante lo scambio di dati</li> </ol>	<p>Toccare OK per riavviare il processo e riprovare.</p> <p>Se il problema persiste, controllare la connessione Internet: controllare se altri dispositivi come PC, smartphone, riescono a navigare sul web come al solito. Eseguire un test della velocità di Internet per verificare le prestazioni della comunicazione.</p> <p>Se non è possibile risolvere il problema, contattare il <i>Service Operation Center ISEO</i> (vedere la sezione <i>Supporto tecnico</i>).</p>

Errore	Significato	Cosa fare
	<ol style="list-style-type: none"> <li>1. L'account è stato appena cancellato.</li> <li>2. Il Cloud ISEO non è raggiungibile.</li> </ol>	<ol style="list-style-type: none"> <li>1. Se si è appena eliminato l'account Argo, questo è un messaggio corretto.</li> <li>2. Riprovare più tardi e controllare la connessione Internet mobile o WiFi del dispositivo. Se il problema persiste, contattare il <i>Service Operation Center ISEO</i> (vedere la sezione <i>Supporto tecnico</i>).</li> </ol>
	<p>Questo errore potrebbe verificarsi all'inizio della configurazione del gateway, durante la lettura del QR-code. Il sistema avvisa che questo gateway è già stato registrato nel Cloud ISEO.</p>	<ol style="list-style-type: none"> <li>1. Utilizzare un gateway diverso poiché questo è già stato assegnato a un account Argo.</li> <li>2. Eliminare questo gateway dall'account Argo corrente, sarà quindi possibile usarlo per un altro account. <b>Nota:</b> per connettere il gateway a un altro account Argo si dovrà reimpostarlo come mostrato nella procedura guidata di configurazione.</li> </ol>
	<ol style="list-style-type: none"> <li>1. La Lock Account Password non è corretta.</li> <li>2. La Lock Account Password è stata associata all'identificazione biometrica dello smartphone, ma è stata successivamente modificata. Al primo tentativo il telefono richiama dalla memoria la prima password associata, che in realtà è cambiata: ecco perché non è più corretta.</li> </ol>	<ol style="list-style-type: none"> <li>1. Inserire la Lock Account Password corretta.</li> <li>2. Ripetere la procedura: l'app chiederà di digitare manualmente la nuova password dopo 2 volte in cui l'identificazione biometrica fallisce.</li> </ol>

Errore	Significato	Cosa fare
	<p>In questo esempio un Guest Account stava tentando di eliminare un utente del telefono con login (amministratore locale) senza che l'autorizzazione Manage Administrators fosse stata abilitata dall'Owner Administrator. Lo stesso errore si verifica ogni volta che il Guest Account tenta di eseguire un'operazione non consentita dall'Owner Administrator (ad esempio Open Door, Read Events)</p>	<p>Non è possibile eseguire operazioni non autorizzate dall'Owner Administrator. Chiedere l'autorizzazione all'Owner Administrator.</p>
	<p>In questo esempio l'Owner Administrator sta tentando di eliminare il gateway ma il sistema contiene serrature configurate.</p>	<p>Prima eliminare tutte le serrature, una ad una, e infine eliminare il gateway.</p>
	<p>In questo esempio l'Owner Administrator sta tentando di eliminare l'account Argo ma il sistema contiene uno Smart Gateway configurato.</p>	<p>Eliminare prima lo Smart Gateway (eliminando tutte le serrature), infine è possibile eliminare definitivamente l'account Argo.</p>

Errore	Significato	Cosa fare
	<p>Lo Smart Gateway non è raggiungibile. Potrebbe essere SPENTO o per qualche motivo non funzionare correttamente. L'icona nel menu Gateway è rossa come nell'esempio seguente.</p> 	<p>Verificare se:</p> <ul style="list-style-type: none"> <li>• Il gateway è acceso con il led di rete acceso.</li> <li>• Il gateway è installato correttamente per comunicare con il router.</li> <li>• Il router funziona correttamente.</li> </ul> <p>Se la risposta è Sì tutto quanto sopra, riavviare il gateway e verificare se ora funziona. Se non è possibile risolvere il problema, contattare il <i>Service Operation Center ISEO</i> (vedere la sezione <i>Supporto tecnico</i>).</p>
	<p>Si è verificato un problema durante il tentativo di connettersi alle serrature da remoto. Il gateway è disponibile, ma le serrature non possono essere raggiunte.</p>	<ul style="list-style-type: none"> <li>• Controllare localmente se la serratura funziona correttamente.</li> <li>• Sostituire la batteria della serratura se è scarica.</li> <li>• Controllare la posizione della serratura per verificare che si trovi nel raggio di portata Bluetooth del gateway.</li> </ul>
	<p>Si è verificato un errore imprevisto e sconosciuto. Questo errore non è stato ancora tradotto nel sistema. Un codice numerico all'interno di parentesi quadre potrebbe seguire il testo (codice di errore del software).</p>	<p>Ritentare l'operazione per verificare se si tratta di un errore ricorrente.</p> <p>Se il problema persiste, contattare il <i>Service Operation Center ISEO</i> (vedere la sezione <i>Supporto Tecnico</i>), fornendo il codice numerico, se presente.</p>

## Tutte le funzionalità dell'app Argo

Per esplorare tutte le funzioni e le caratteristiche di *Argo Local*, leggere il *Manuale utente di Argo 2.7* disponibile su [iseo.com](http://iseo.com).



## Supporto tecnico

Per assistenza tecnica si prega di contattare il *Service Operations Center ISEO*. Puoi trovare i contatti relativi alla tua nazione al sito:

<https://www.iseo.com/>

Quando si contatta il *Service Operations Center*, fornire le seguenti informazioni:

- Versione software dell'app *Argo*.
- Modello di smartphone e versione software.
- Dispositivo di controllo accessi, coinvolto nel problema, codice del prodotto e versione del software.
- Descrizione precisa e dettagliata del problema.



**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**