ARGO NUTZERHANDBUCH

USER MANUAL

ARGO 3.0

ISEO®

ULTIMATE ACCESS TECHNOLOGIES

Über diese Anleitung

Dieses Handbuch dreht sich um *Argo 3.0* und die Remote-Umgebung.

Bei *Argo 3.0* handelt es sich um die neue Argo-Version, den Nachfolger von Argo 2.7. *Argo 3.0* umfasst eine neue Produktserie von *ISEO Smart Geräten* mit der innovativen Technologie *Bluetooth 5.0*. Mit dieser Technologie kann *Argo 3.0* gemeinsam mit den neuen *ISEO Smart Geräten* **aus der Ferne verwaltet werden**. Daher wird *Argo 3.0* auch als **Argo Fernsteuerung** bezeichnet.

Weitere Informationen zu *Argo* und allen Standardfunktionen von *Argo* sowie zu den einzelnen Menüs finden Sie im *Argo 2.7 Nutzerhandbuch*, das unter *iseo.com* verfügbar ist:

https://www.iseo.com/data/updati/manuali/ISEOZERO1ELECTRONICSOLUTIONS_SISTEMAARGO_ARGOAPPSISTEMADIGESTIONE/DE/Argo%202.5_User%20Manual_DE_01_20190403.pdf

Alle weiteren Dokumente zum Produkt wie das Prospekt, die Broschüre oder Zertifizierungen finden Sie unter:

https://www.iseo.com/it/de/node/195/argo-app--zutrittssteuerungssystem

Dieses Handbuch erläutert die Einrichtung von *Argo 3.0* und die Funktionen der Kapitel *Grundlagen* und *Erweiterte Funktionen*. Für das Kapitel *Grundlagen* schauen Sie sich auch das Video *Argo 3.0 from Remote Basics* unter folgendem Link an:

https://youtu.be/bFrKiuZqZmE

Symbole

Zum besseren Verständnis dieser Anleitung machen Sie sich bitte mit den folgenden Symbolen vertraut:

WARNUNG: Wichtiger Hinweis, damit das System ordnungsgemäß funktioniert.

HINWEIS: Hinweise, Empfehlungen und Zusatzinformationen.

TIPP: Tipps und Tricks für einfachere und schnellere Bedienung.

Hinweise zur Nutzung

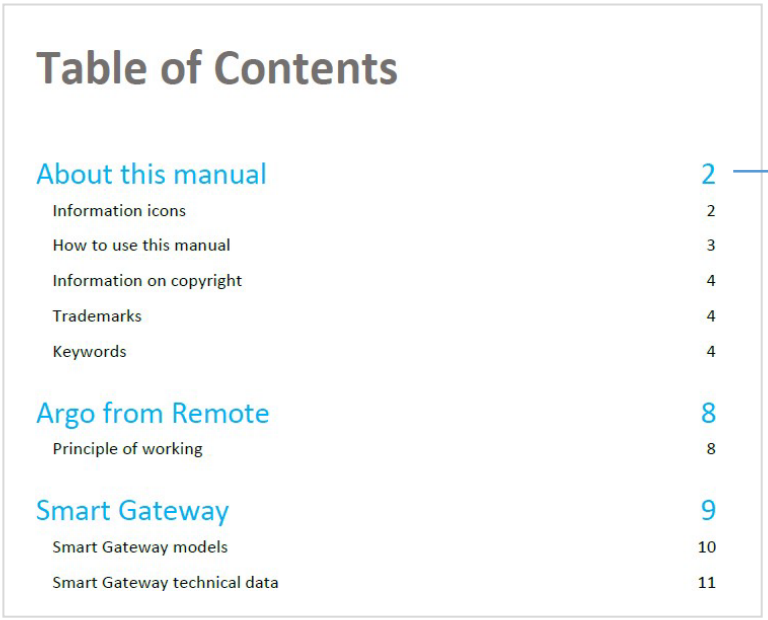
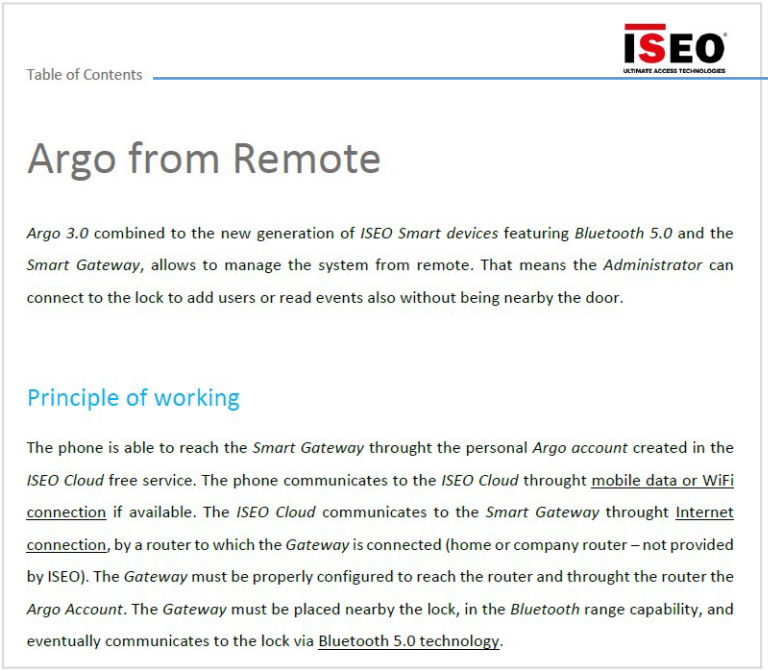


Table of Contents

Im *Inhaltsverzeichnis* können Sie durch Anklicken des Kapitels oder der Seitenzahl direkt zur entsprechenden Seite der Anleitung springen.



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.

Wenn Sie auf den Titel in der Kopfzeile der Seite klicken, gelangen Sie wieder zum Inhaltsverzeichnis.

Informationen zum Urheberrecht

- Die komplette oder teilweise Vervielfältigung, Verbreitung, Übersetzung oder Übertragung dieser Anleitung egal welcher Art ist ohne vorherige schriftliche Genehmigung von ISEO untersagt, das umfasst auch Fotokopie, Aufnahme oder die Speicherung in einem Speicher- und Datenabfragesystem.
- ISEO behält sich das Recht auf Änderungen der in dieser Anleitung beschriebenen Software und Hardware jederzeit und ohne vorherige Ankündigung vor.
- ISEO übernimmt keinerlei Haftung für Schäden, die durch die Nutzung der beschriebenen Produkte entstehen.

Markenzeichen

- Das Apple-Logo, Apple®, iPhone®, iPad®, Apple Watch® und App Store® sind Markenzeichen von APPLE Inc.
- Das Android™-Logo, Google™, Youtube™, Google Play™ Store sind Markenzeichen von Google ILLC.
- Bluetooth® ist ein eingetragenes Markenzeichen von Bluetooth SIG, Inc.
- iOS ist ein Markenzeichen oder eingetragenes Markenzeichen von Cisco in den USA und anderen Ländern.
- MIFARE® und MIFARE® DESFire® sind eingetragene Marken von NXP B. V.
- Alle anderen Markenzeichen und Copyrights sind Eigentum der jeweiligen Inhaber.

Glossar

- **Argo Fernsteuerung**: Wenn der Bediener per Smartphone über das *Argo-Konto* und das *Smart Gateway*, das in der Nähe des Schlosses installiert ist, eine Datenverbindung zum *ISEO Smart Gerät* herstellt. Remote oder aus der Ferne bedeutet, dass der *Administrator* außerhalb der *Bluetooth-Reichweite* des Schlosses ist, das Schloss aber immer noch über die *ISEO Clouddienste* erreichen und mit diesem kommunizieren kann.
- **Argo Local**: Wenn der Bediener oder der Endnutzer eine direkte Verbindung mit den *ISEO Smart Geräten* per Smartphone via Bluetooth herstellt. Lokal bedeutet, dass man sich vor dem Schloss und innerhalb der Bluetooth-Reichweite befindet, so dass die Türliste auf dem eigenen Smartphone angezeigt wird.
- **Argo-Konto**: Die Voraussetzung, um das System Argo-System mit Fernsteuerung in Betrieb zu nehmen. Es wird bei der Registrierung des Endnutzers bei den ISEO Cloudservices erstellt und ermöglicht es, das Smart Gateway und das System aus der Ferne zu erreichen bzw. zu verwalten. Das Konto ist kostenlos, für die Erstellung benötigt man eine gültige E-Mailadresse.
- **Bluetooth 5.0**: auch als BLE 5 bezeichnet, ist eine neue Technologie, die das vorige Bluetooth 4.0 verbessert und Multichannel-Kommunikation ermöglicht. Während BLE 4 zeitgleich nur mit einem Gerät kommunizieren kann (ein Kanal), kann *BLE 5* mit mehreren Geräten gleichzeitig kommunizieren. Beispiel: Während eine Person das Schloss per Smartphone öffnet, kann sich der *Bediener* aus der Ferne über das *Smart Gateway* verbinden. Das Schloss kann beide Vorgänge gleichzeitig ausführen.

- **Gast-Konto**: siehe *Remote-Bediener*.
- **Gerätepasswort**: Es bedarf eines Passworts, um mit dem Schloss über das Argo-Konto zu kommunizieren, es zu öffnen oder sich anzumelden, das sogenannte Gerätepasswort. Es wird während der Einrichtung des Argo-Kontos vergeben, wenn das Schloss hinzugefügt wird. Für jedes einzelne Schloss muss ein Passwort vergeben werden. Für höchste Bedienerfreundlichkeit kann das Passwort mit der biometrischen Identifizierung des Smartphones verknüpft werden. Durch das Gerätepasswort ist sichergestellt, dass eine Person, auch wenn sie auf das Argo-Konto zugreifen kann oder das Smartphone gestohlen hat, das Schloss nicht aus der Ferne öffnen oder sich anmelden kann, da das Passwort bei jeder Kommunikation benötigt wird.
- **Häuser**: werden in der Benutzeroberfläche der *Argo Fernsteuerung* angezeigt. Hier handelt es sich um Schlossgruppen, die es vereinfachen, Schlösser verschiedener Standorte zu organisieren und damit die *Startseite* von *Argo Fernsteuerung* übersichtlich zu gestalten.
- **ISEO Cloud**: Die kostenlose Cloudservice-Infrastruktur, auf der die *Argo Fernsteuerung* läuft. Um auf diesen Service zuzugreifen, wird ein *Argo-Konto* benötigt.
- **ISEO Smart Geräte**: Die elektronischen Schlösser von ISEO, die an den Türen installiert werden, verfügen nun über *Bluetooth 5.0*. Sie werden auch als Schlösser bezeichnet, es handelt sich im Prinzip um dieselbe Hardware wie in den vorigen *Argo*-Versionen, aber mit einem *Bluetooth 5.0-Chip* auf der Elektronikplatine. Das Produktlogo wurde angepasst, um die neue Technologie schnell zu identifizieren.
- **Lokaler Bediener**: Jeder Smartphone-Nutzer mit Zugriff auf den Programmier-Modus in der Argo-Nutzerliste. Dadurch erhalten Nutzer automatisch *Bedienerr*echte. Der *Lokale Bediener* kann sich daher an der Tür anmelden, sofern er sich innerhalb der Bluetooth-Reichweite befindet (*Argo Local*).
- **Remote-Bediener (Gast-Konto)**: Es handelt sich um eine andere *Rolle* in der *Nutzerliste* der *Argo Fernsteuerung*. Dabei handelt es sich um den Bediener, der vom *Remote-Hauptbediener* eingeladen wurde, um die Schlösser aus der Ferne zu verwalten. Es wird auch als *Gast-Konto* bezeichnet, da auch hier eine Art Gast ein *Smart Gateway* verwendet, um auf Schlösser zuzugreifen, die einem anderen Bediener gehören: dem *Hauptbediener*. Bitte beachten Sie, dass der eingeladene *Bediener* weder den *Hauptbediener* noch sich selbst vom Schloss entfernen kann, zu dem er eingeladen worden ist. Dafür muss der *Hauptbediener* kontaktiert werden.
- **Remote-Hauptbediener**: Eine neue *Rolle*, die nun in der *Nutzerliste* der *Argo Fernsteuerung* vorhanden ist. Es handelt sich um den *Bediener*, der zuerst ein *Argo-Konto* für die Systemverwaltung von unterwegs eingerichtet hat. Der Bediener ist Besitzer des Systems und des *Smart Gateways*, das verwendet wird, um die Schlösser an die Cloud anzubinden. Er kann andere Bediener einladen, um das Schloss ebenfalls aus der Ferne zu verwalten (siehe dazu *Remote-Bediener*).
- **Smart Gateway**: Das elektronische Gerät von ISEO ist in der Lage, *ISEO Smart Geräte* mit der *ISEO Cloud* zu verbinden. Es muss per WLAN oder PoE mit einem Router verbunden sein, um das *Argo-Konto* zu erreichen; mit den Türschlössern kommuniziert es über *Bluetooth 5.0*. Es muss innerhalb der *Bluetooth*-Reichweite der Schlösser installiert werden und funktioniert nur mit *ISEO Smart Geräten* mit *Bluetooth 5.0*. Es sind zwei Modelle verfügbar: Ausführung mit WLAN und PoE

Weitere *Argo spezifische Bezeichnungen* finden Sie im *Argo 2.7 Nutzerhandbuch*, verfügbar unter *iseo.com*.

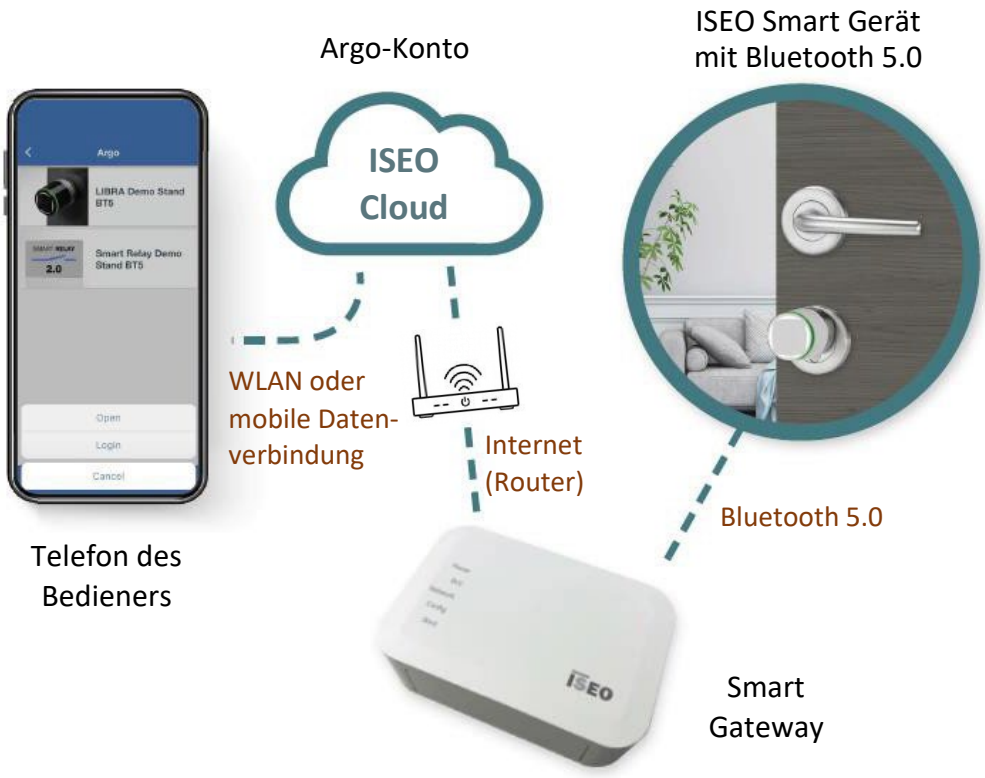
Inhaltsverzeichnis

Argo Fernsteuerung

Mit *Argo 3.0*, der neuen Generation der *ISEO Smart Geräte* mit *Bluetooth 5.0* und dem *Smart Gateway* kann das System auch aus der Ferne verwaltet werden. Das heißt, der *Bediener* kann auf das Schloss zugreifen, um Nutzer hinzuzufügen oder Ereignisse auszulesen, ohne in der Nähe des Schlosses sein zu müssen.

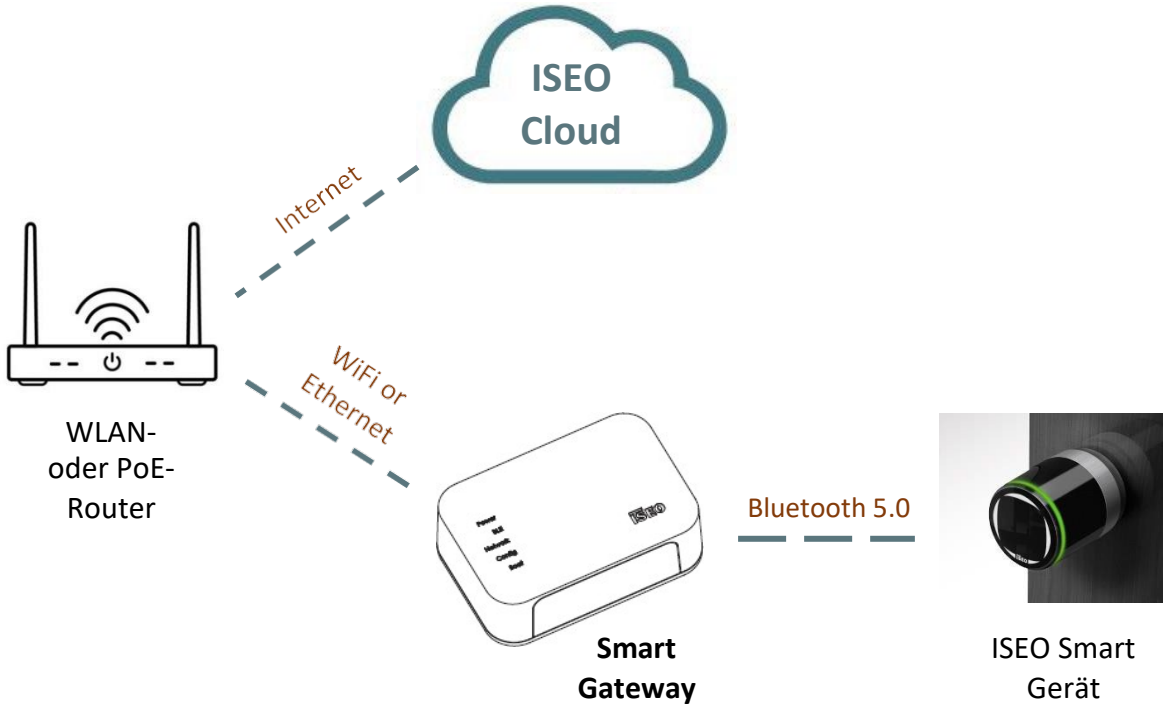
Funktionsprinzip

Das Smartphone kann das *Smart Gateway* über das persönliche Argo-Konto erreichen, das in der kostenlosen *ISEO Cloud* erstellt wurde. Das Smartphone kommuniziert mit der *ISEO Cloud* über eine mobile Daten- oder WLAN-Verbindung, sofern diese verfügbar ist. Die *ISEO Cloud* kommuniziert mit dem *Smart Gateway* über eine Internetverbindung und einen Router, mit dem es verbunden ist (privater oder Firmenrouter – nicht im Lieferumfang enthalten). Das *Gateway* muss ordnungsgemäß eingerichtet sein, um den Router zu erreichen und über diesen auf das *Argo-Konto* zuzugreifen. Das *Gateway* muss in der Nähe des Schlosses innerhalb der *Bluetooth*-Reichweite installiert werden; es kommuniziert mittels Bluetooth 5.0 mit dem Schloss.



Smart Gateway

Das *Smart Gateway* verbindet die ISEO Cloud und das I*SEO Smart Gerät*. Es kommuniziert mit der Cloud über eine Internetverbindung mittels WLAN-Router und mit dem Türschloss über *Bluetooth Smart 5.0*. Mit dem Smart Gateway können alle *ISEO Smart Geräte* innerhalb der *Bluetooth-Reichweite* (ca. 10 Meter je nach Umgebungsbedingungen) verwaltet werden.



Der Router ist nicht im Lieferumfang enthalten.
Sofern mehrere ISEO Smart Geräte mit einem Abstand von mehr als 10 Metern installiert wurden, können weitere Gateways mit demselben Router verbunden werden.

Beim Smart Gateway handelt es sich um ein leistungsstarkes Linux-Gerät mit ARM 7 Prozessor. Der Funktionsumfang von Argo wird damit auf Remote-Anwendungen mit demselben Sicherheitsniveau wie bei lokaler Verwendung erweitert. Das Smart Gateway ermöglicht eine Sicherheitsarchitektur mit direkter Verbindung zum Schloss mit End-zu-End-Verschlüsselung. Die ISEO Cloud fungiert nur als Tunnel, es werden keinerlei sensible Daten des Türschlosses gespeichert.

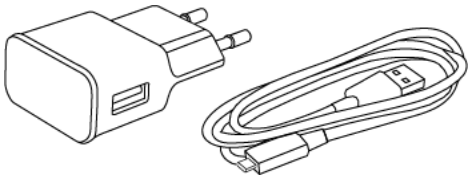
Das Smart Gateway mit dem Betriebssystem Linux und den APIs kann über ISEO Argo verwendet werden. Entwickler (Integratoren) können das *Argo SDK* nutzen, um ihre Software und Anwendung einfach und effizient zu programmieren. Darüber hinaus sorgt *Linux* für Stabilität und besseren Schutz vor externen Angriffen oder Virenangriffen.

Smart Gateway Modelle

Es sind zwei *Smart Gateway* Modelle erhältlich:

Smart Gateway WLAN

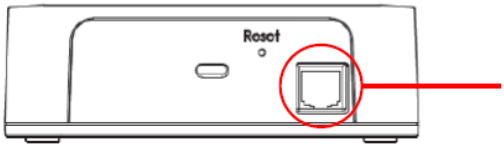
- Erfordert einen WLAN-Router.
- Es wird über ein 10 W Netzteil mit Strom versorgt.



5 VDC – 2 A Netzteil
USB C-Schnittstelle

Smart Gateway PoE (Powered over Ethernet)

- Erfordert einen PoE-Router.
- Es muss an den PoE-Port des Routers mittels LAN-Kabel angeschlossen werden.



Das Gateway PoE verfügt auf der Rückseite über einen Ethernetanschluss.

- Alternativ kann es auch mittels LAN-Kabel an einen normalen Router (ohne PoE-Port) angeschlossen werden, dann wird für die Stromversorgung allerdings das 10 W Netzteil benötigt.

Das *Gateway PoE* erfordert einen Router mit **aktiviertem DHCP**, um automatisch eine gültige IP-Adresse zu erhalten.

Das LAN-Kabel ist nicht im Lieferumfang enthalten.

Das 10 W Netzteil muss separat bestellt werden. Es ist nicht im Lieferumfang des *Smart Gateways* enthalten.

Technische Daten Smart Gateway

Eigenschaft	WLAN	PoE (Power over Ethernet)
Funktionsweise	▪ Konvertiert WLAN-Daten in BLE 5 ▪ Dual Band WLAN mit 2,4 GHz u. 5 GHz	▪ Konvertiert Ethernet in BLE 5
Netzteil	▪ Stromversorgung über USB C + 5 VDC Eingangsspannung 2 A (10 W) ▪ Netzteil NICHT im Lieferumfang enthalten (separat zu bestellen)	▪ PoE (Power over Ethernet) ▪ Benötigt PoE Switch IEEE 802.3af mit bis zu 15,4 W ▪ Daten- und Stromversorgung über Ethernetkabel CAT5e/CAT6. ▪ Maximaler Stromverbrauch 10 W ▪ Stromversorgung optional auch über USB C + 5 VDC Eingangsspannung 2 A (10 W) ▪ Netzteil NICHT im Lieferumfang enthalten (separat zu bestellen)
Abmessungen	▪ 125x40x85 mm (LxBxH)	▪ 125x40x85 mm (LxBxH)
Betriebs-bedingungen	▪ Betriebstemperatur: 0° C/+50° C ▪ Lagertemperatur: -25° C/+75° C	▪ Betriebstemperatur: 0° C/+50° C ▪ Lagertemperatur: -25° C/+75° C
Installation	▪ Tisch ▪ Wandmontage möglich (Zubehör separat zu bestellen)	▪ Tisch ▪ Wandmontage möglich (Zubehör separat zu bestellen)
Anschlüsse	▪ USB C female	▪ USB C female ▪ Ethernet TCP/IP 10/100 baseT
Signal-LEDs	▪ Stromversorgung (weiß): AN = Stromversorgung vorhanden ▪ BLE (weiß): AN = BLE-Übertragung läuft ▪ Netzwerk (weiß) AN = Gateway mit Cloud verbunden ▪ Config (weiß): AN = Einrichtung Gateway erforderlich ▪ Boot (rot): AN = Gateway fährt hoch	▪ Stromversorgung (weiß): AN = Stromversorgung vorhanden ▪ BLE (weiß): AN = BLE-Übertragung läuft ▪ Netzwerk (weiß) AN = Gateway mit Cloud verbunden ▪ Config (weiß): AN = Einrichtung Gateway erforderlich ▪ Boot (rot): AN = Gateway fährt hoch
CPU, Speicher, Betriebssystem	▪ CPU der ARM A7-Serie ▪ 512 MB RAM ▪ 8 GB Flash eMMC nicht volatiler Speicher ▪ Betriebssystem: integriertes Linux	▪ CPU der ARM A7-Serie ▪ 512 MB RAM ▪ 8 GB Flash eMMC nicht volatiler Speicher ▪ Betriebssystem: integriertes Linux
Tasten	▪ Reset (Neustart oder Zurücksetzen)	▪ Reset (Neustart oder Zurücksetzen)
OEM-Ausführung	▪ OEM-Ausführung für Argo-Integratoren mit SDK verfügbar	▪ OEM-Ausführung für Argo-Integratoren mit SDK verfügbar

ISEO Smart Devices mit Bluetooth 5.0

Die *ISEO Smart Geräte* der neuen Generation verwenden *Bluetooth 5.0* (auch als BLE 5 bezeichnet). Diese Technologie ermöglicht mehrere Verbindungen gleichzeitig.
Beispiel: Während eine Person das Schloss per Smartphone öffnet, kann sich der *Bediener* aus der Ferne über das *Smart Gateway* verbinden. Das Schloss kann beide Vorgänge gleichzeitig ausführen.

Bei der Form und Mechanik der neuen *ISEO Smart Geräte* gibt es keine Änderungen zu den vorigen Geräten mit Bluetooth 4.0. Die beiden Serien unterscheiden sich in folgenden Punkten:

- Bluetooth 5.0 Chip auf der Platine,
- Neues Logo, um Bluetooth 5.0 auf den ersten Blick erkennen zu können.

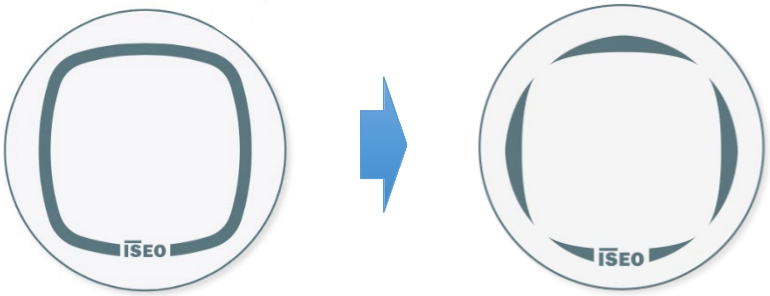
Neues Logo

Das neue *Argo 3.0* Logo befindet sich auf allen *ISEO Smart Geräten* mit *Bluetooth 5.0*.

Es kennzeichnet die technologische Entwicklung des Produktes, das nun neue und einzigartige Funktionen aufweist:

- Verbesserte Kommunikation der *ISEO Smart Geräte*.
- Mehrere Verbindungen gleichzeitig.
- Verwaltung aus der Ferne über *Argo* dank des neuen *Smart Gateways*.

Neues Logo für Argo & ISEO Smart Geräte



Smart Geräte
Argo 2.7 & Bluetooth 4.0

Smart Geräte
Argo 3.0 & Bluetooth 5.0

Neues Logo für Argo 3.0

Argo 2.7 &
Bluetooth 4.0

Argo 3.0 &
Bluetooth 5.0

In der *Argo 3.0*-App werden die neuen Geräte mit *Bluetooth 5.0* mit einem neuen Icon dargestellt (s. *Grundlagen, Argo-Konto erstellen*).

Neues Logo bei ISEO Smart Geräten

Libra Smart
Bluetooth 4.0

Libra Smart
Bluetooth 5.0

Stylos Smart
Bluetooth 4.0

Stylos Smart
Bluetooth 5.0

Lesegerät
x1R Smart

Lesegerät
x1R Smart

Beim *x1R Smart* befindet sich die *Bluetooth 5.0* Platine im externen Lesegerät, das nun auch über das neue Logo verfügt.

Grundlagen

In diesem Abschnitt wird erläutert, wie man Argo 3.0 konfiguriert, um das System aus der Ferne verwalten zu können.

Um die Argo Fernsteuerung einzurichten, müssen Sie:

1. Ihr *Argo-Konto* erstellen.
2. Sich beim *Argo-Konto* anmelden.
3. Das *Smart Gateway* einrichten.
4. Schlösser zum System hinzufügen (Masterkarte erforderlich).

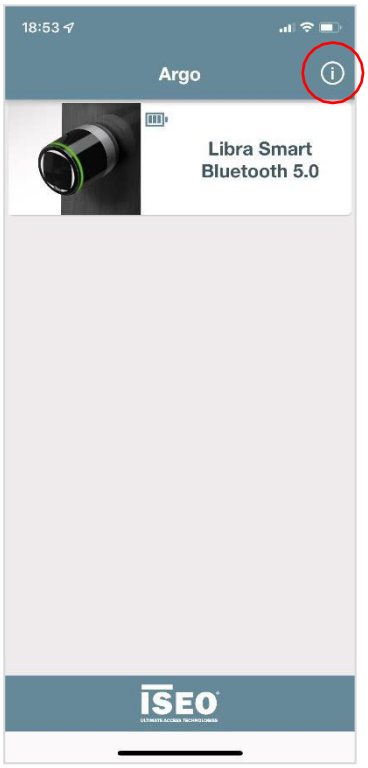
Argo-Konto erstellen

Bei der ersten Systemkonfiguration müssen Sie ein *Argo-Konto* erstellen. Dafür benötigen Sie eine gültige E-Mailadresse, auf die Sie von Ihrem Smartphone oder Tablet zugreifen können. Folgen Sie dazu den nächsten Schritten.

1. Starten Sie **Argo 3.0**.

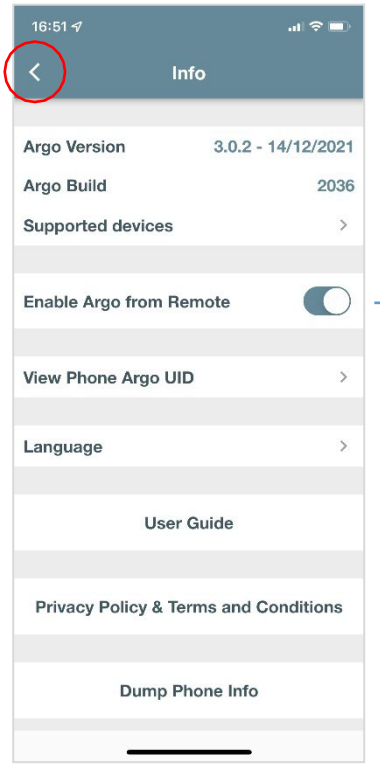
Neues Design und Logo von *Argo 3.0.*

2. Tippen Sie in der App auf das **Info-Menü**.



Beachten Sie das neue Libra-Icon, um sofort Geräte mit *Bluetooth 5.0* zu erkennen.
Alle neuen Geräte mit *BLE 5.0* werden mit dem neuen Logo dargestellt, um sie von Modellen mit *BLE 4.0* zu unterscheiden.

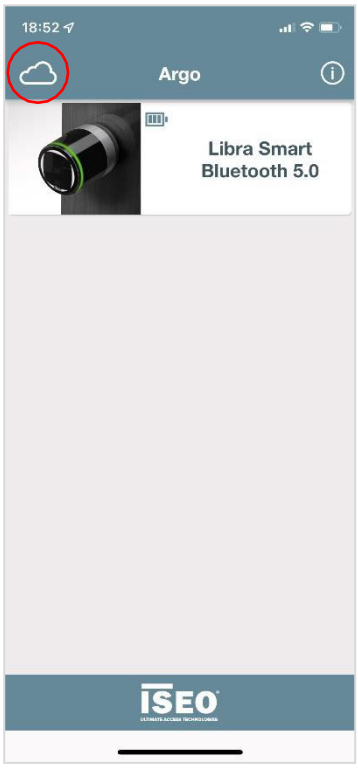
3. Aktivieren Sie **Argo Cloud aktivieren** und kehren Sie dann ins Hauptmenü zurück.



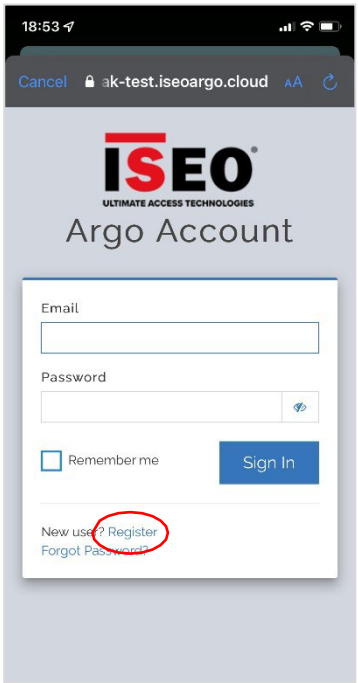
Argo Cloud aktivieren.

Ein Hinweis erscheint, in dem die Funktionen und Anforderungen der *Argo Fernsteuerung* erläutert werden. Lesen Sie diesen und tippen Sie auf Akzeptieren, um fortzufahren.

4. Nach der Aktivierung erscheint eine Wolke. Tippen Sie auf das **Cloud-Symbol**.

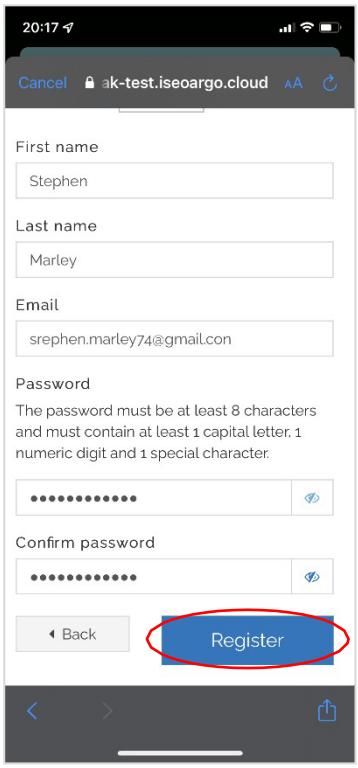


5. Tippen Sie auf **Registrieren**, um sich als Nutzer bei der *ISEO Cloud* zu registrieren. Folgen Sie dann einfach den einzelnen Schritten.



Die Nutzerregistrierung ist nur bei der Ersteinrichtung erforderlich, um das *Argo-Konto* zu erstellen.

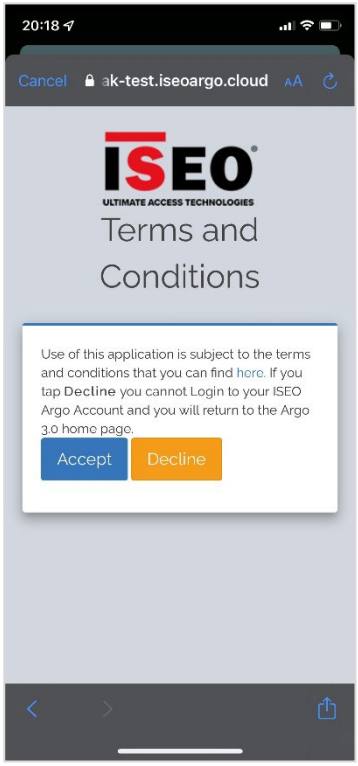
6. Geben Sie alle erforderlichen Daten ein und tippen Sie am Ende auf **Registrieren**.



Geben Sie eine gültige E-Mailadresse ein, auf die Sie von dem Gerät, mit dem Sie die Registrierung vornehmen, zugreifen können.

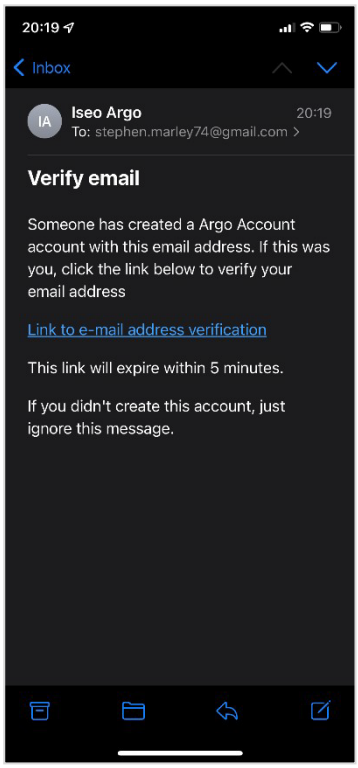
Es muss ein starkes Passwort eingegeben werden.

7. **Akzeptieren** Sie die allgemeinen Geschäftsbedingungen.



Wenn Sie auf **Ablehnen** tippen, werden Sie automatisch auf die Argo-*Startseite* weitergeleitet. Melden Sie sich mit Ihrer E-Mailadresse und Ihrem Passwort an, um hier fortzufahren.

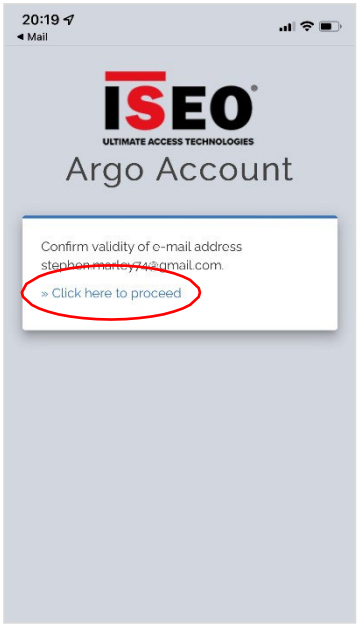
8. Warten Sie auf die E-Mailbestätigung vom *ISEO Cloudservice*. Öffnen Sie die Mail und tippen Sie auf den **Link**.



Tippen Sie auf den Link, um Ihre E-Mailadresse zu bestätigen.

9. Bestätigen Sie die E-Mailadresse und warten Sie auf die Bestätigungsnachricht.

   Kehren Sie dann zur *Argo-Startseite* zurück.

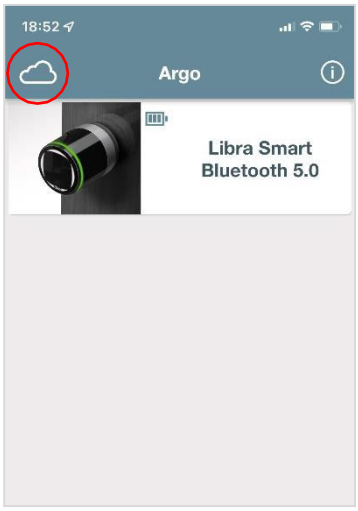


Beim Argo-Konto anmelden

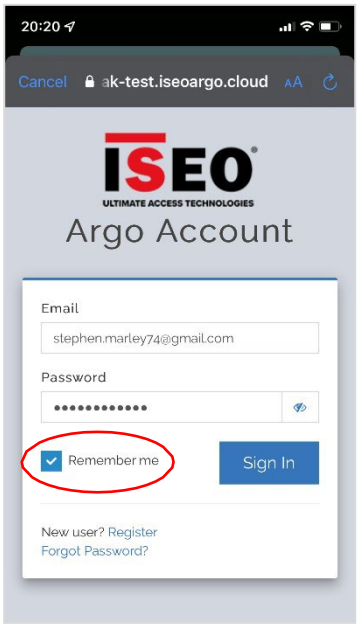
Sobald Ihr *Argo-Konto* in der *ISEO Cloud* erstellt wurde, können Sie sich anmelden.

Auf der *Argo 3.0 Startseite*:

1. Tippen Sie auf das **Cloud**-Symbol.



2 Melden Sie sich mit Ihrer E-Mailadresse und dem Passwort an, die Sie bei der Registrierung des *Argo-Kontos* verwendet haben.



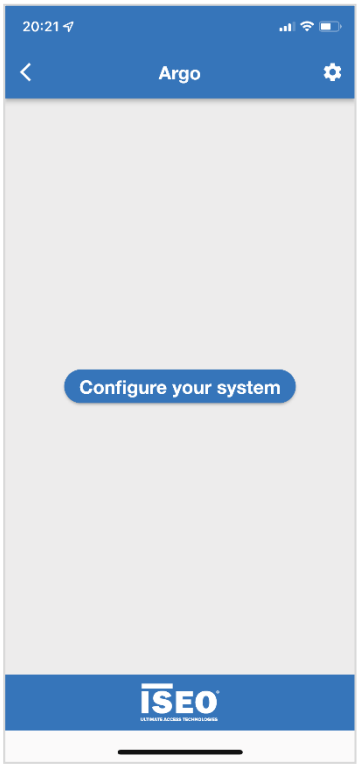
Tippen Sie auf **Anmelden**, um sich anzumelden.

Wählen Sie *Angemeldet bleiben*, wenn Sie Ihre E-Mailadresse und Ihr Passwort bei der nächsten Anmeldung nicht erneut eingeben wollen. Das gilt für einen bestimmten durch die App definierten Zeitraum oder bis die automatische Abmeldung vom Konto erfolgt (weitere Informationen zur Abmeldung finden Sie unter *Erweiterte Funktionen*).

Smart Gateway einrichten

Wenn Sie sich zum ersten Mal bei Ihrem *Argo-Konto* anmelden, müssen Sie zunächst das *Smart Gateway* einrichten, um die *Argo Fernsteuerung* verwenden zu können. Das *Smart Gateway* ist im Prinzip das Werkzeug, mit dem Ihr Smartphone das Schloss aus der Ferne erreichen kann. Daher erhalten Sie beim Öffnen mit der *Argo Fernsteuerung* folgende Nachricht: *System konfigurieren.*

1. Tippen Sie auf **System konfigurieren**.



Die Balken oben und unten haben eine andere Farbe als bei *Argo Local*. Damit wird die Remote-Umgebung (*Argo Fernsteuerung*) gekennzeichnet.

2. Schließen Sie das *Smart Gateway* an den Strom an und folgen Sie den einzelnen Schritten, die in der App erläutert werden.

Das Hochfahren des *Smart Gateways* dauert rund 1 Minute.

Einrichtungsassistent

Falls die *Config-LED des Gateways* NICHT LEUCHTET, tippen Sie auf **Nein**. Ihnen wird in der App angezeigt, wie Sie das Gateway auf Werkseinstellungen zurücksetzen.

3. Lesen Sie den **QR-Code** des *Smart Gateways* mit Ihrem Smartphone.

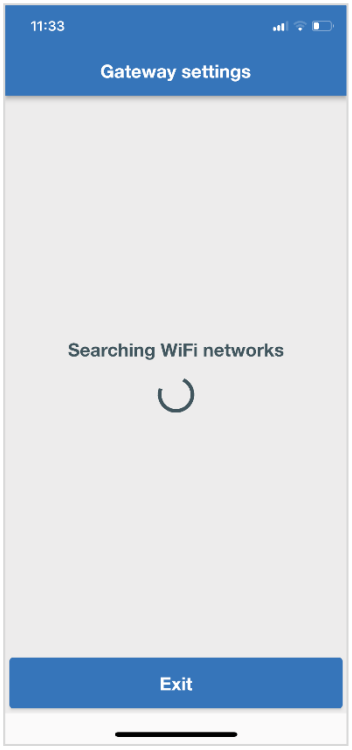
Auf der Rückseite des Smart Gateways befinden sich zwei *QR-Codes*:

- Seriennummer
- Registrierungscode

Argo liest automatisch nur den richtigen Code, den **Registrierungscode**.

Falls es Probleme beim Lesen des *QR-Codes* gibt, kann der *Registrierungscode* auch manuell hinzugefügt werden, indem man auf **Manuell hinzufügen** tippt.

4. Sobald der *QR-Code* des *Registrierungscodes* gelesen wurde, sucht der **Assistent** automatisch nach WLAN-Netzwerken in Reichweite.

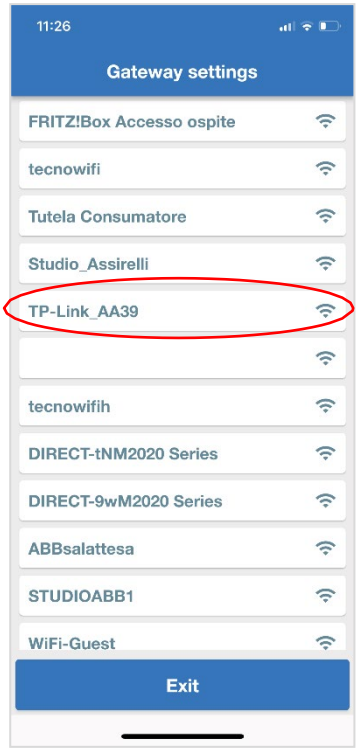


Falls Sie ein *Smart Gateway PoE* verwenden, gehen Sie direkt zu Schritt 7.

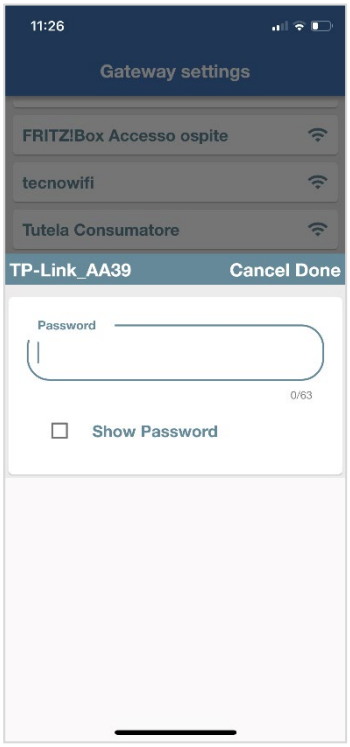
Die Schritte 4, 5 und 6 sind nur für das *Smart Gateway WLAN* erforderlich.

Das Gateway PoE wird per LAN-Kabel direkt mit dem Router verbunden und erhält über DHCP-Protokoll automatisch eine IP-Adresse.

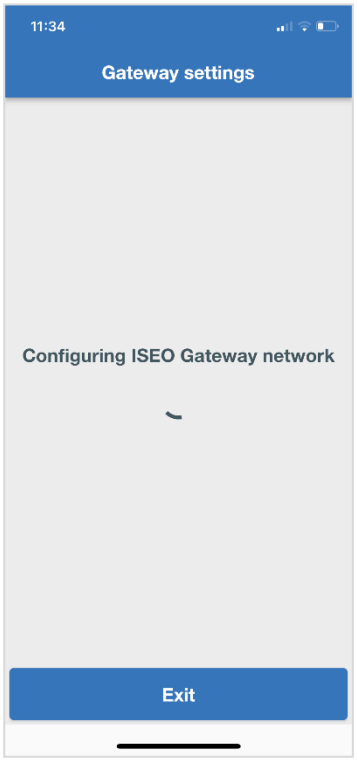
5. Wählen Sie das WLAN-Netzwerk Ihres Routers.



6. Geben Sie Ihr WLAN-Passwort ein und tippen Sie auf **Fertig**.



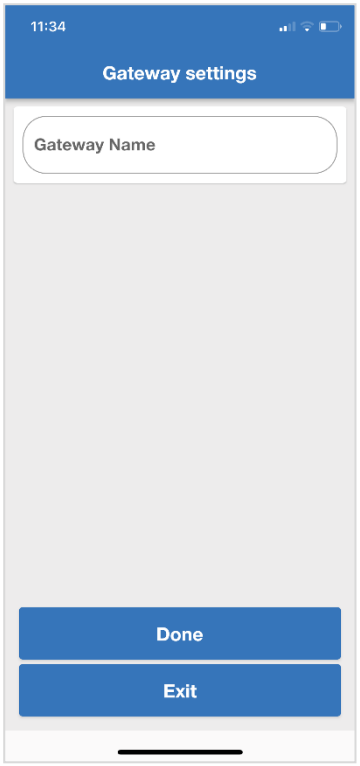
7. Warten Sie, bis das *Smart Gateway* konfiguriert ist.



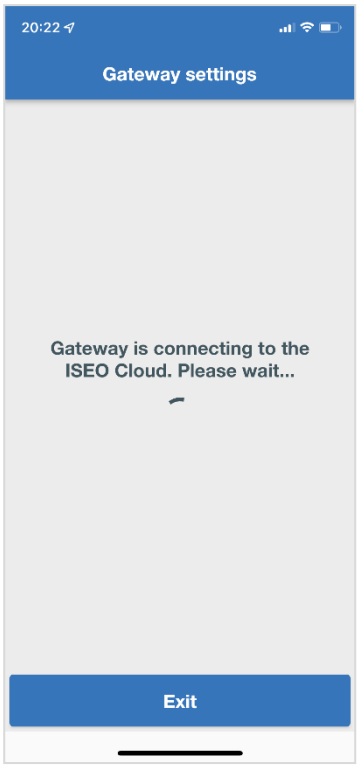
Jetzt verbindet sich das Gateway mit dem WLAN-Netzwerk Ihres Routers. Falls ein Fehler auftritt, wiederholen Sie den Vorgang und prüfen Sie das Netzwerkpasswort.

Weitere Informationen zu möglichen Fehlern finden Sie im Kapitel *Problembehebung*.

8. Sobald sich das *Smart Gateway* erfolgreich mit dem Router verbunden hat, können Sie dem Gateway einen Namen zuweisen. Tippen Sie dann auf **Fertig**.



9. Warten Sie nun, bis das *Smart Gateway* Ihr *Argo-Konto* in der *ISEO Cloud* erreicht und eine Verbindung hergestellt hat.



Jetzt verbindet sich das Gateway mit der *ISEO Cloud*. Falls ein Fehler auftritt, kann das verschiedene Ursachen haben:

- Keine Internetverbindung.
- Langsame Internetverbindung (Netzwerklatenz).
- Kommunikationsfehler aufgrund von Routereinstellungen oder der Firewall.

Bitte wiederholen Sie den Vorgang. Sollte das Problem weiterhin bestehen, prüfen Sie den Router und Ihre Internetverbindung.

Weitere Informationen zu möglichen Fehlern finden Sie im Kapitel *Problembehebung*.

10. Sobald die Verbindung zwischen *Smart Gateway* und *ISEO Cloud* erfolgreich hergestellt wurde, erscheint folgende Nachricht:

Schlösser zum System hinzufügen (Masterkarte erforderlich)

Schlösser zum System hinzuzufügen bedeutet, Ihre *ISEO Smart Geräte* mit dem eingerichteten *Smart Gateway* zu verbinden, um sie dann aus der Ferne über das in der *ISEO Cloud* erstellte *Argo-Konto* zu erreichen.

Um mit dem *Smart Gateway* zu kommunizieren, muss das *ISEO Smart Gerät*:

- Über *Bluetooth 5.0* verfügen.
- Sich innerhalb der Bluetooth-Reichweite des *Smart Gateways* befinden.

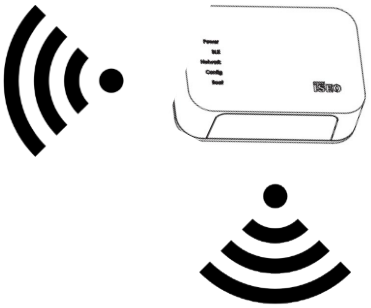
Sie können beliebig viele *ISEO Smart Geräte* hinzufügen, es gibt keine Obergrenze. Das *Gateway* verhält sich wie ein Smartphone, auf dem Argo läuft: Es kann jedes Gerät innerhalb der Bluetooth-Reichweite erkennen.

Die einzige Einschränkung besteht in der Entfernung zwischen *Gateway* und den Geräten, die nicht mehr als 10 Meter betragen sollte, aber je nach Umgebungsbedingungen auch geringer sein muss: Wandstärke, Ecken, weitere elektromagnetische Felder, Installationsort des *Gateways*, Position und Höhe.

Installationsbeispiel Smart Gateway

Tür mit installiertem *ISEO Smart Gerät*

Reichweite Bluetooth 5.0



Das *Smart Gateway* wurde nahe der Tür und innerhalb der WLAN-Reichweite des Routers installiert.

WLAN-Reichweite

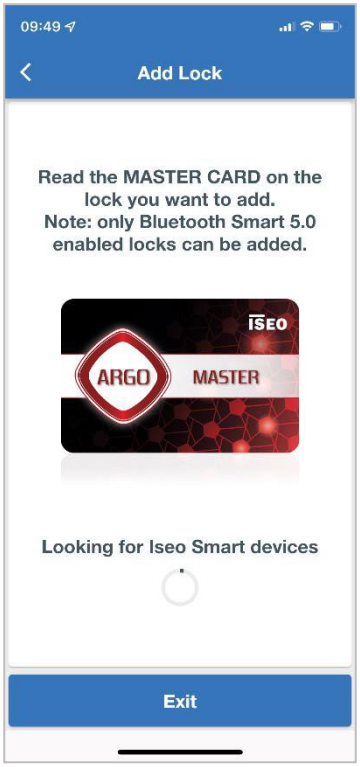
WLAN-Router

1. Tippen Sie auf **Neue Schlösser hinzufügen** und folgen Sie dann den Anweisungen. Stellen Sie sicher, dass Sie sich vor dem Schloss befinden, das Sie hinzufügen wollen, damit Sie die *Master*-Karte vorhalten können, sobald dies erforderlich ist.

Dieser Vorgang **erfordert die Master-Karte** und der Bediener muss sich vor dem Schloss befinden.

Sie können auch später über das von der *Startseite* der *Argo Fernsteuerung* erreichbare Menü Schlösser hinzufügen. Weitere Informationen zu den Menüs finden Sie im Kapitel *Erweiterte Funktionen*.

2. Die App sucht nach *ISEO Smart Geräten* mit *Bluetooth 5.0*. Folgen Sie den Anweisungen der App, sobald Geräte gefunden wurden.



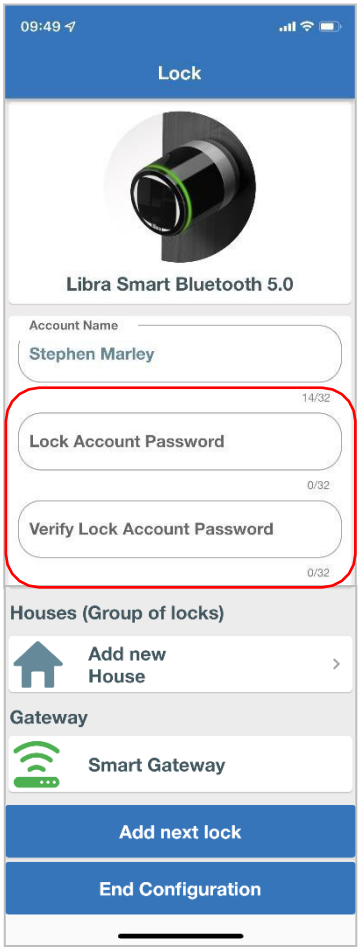
Halten Sie die **Master-Karte** mit dem zu Ihrer Anlage gehörigen Systemcode vor das Schloss.

3. Tippen Sie zur Bestätigung auf **Schloss hinzufügen** und warten Sie, bis Sie das Schloss einrichten können.

Die Schlossbezeichnung wird automatisch von *Argo Local* übernommen.

Um die Bezeichnung zu ändern, müssen Sie den Namen wie gehabt über *Argo Local* im Menü *Tür-Info* ändern. Der Schlossname wird bei der nächsten Anmeldung bei der *Argo Fernsteuerung* aktualisiert.

4. Wählen Sie das **Gerätepasswort**. Dieses Passwort erhöht die Sicherheit und dient dazu, die Kommunikation mit dem Schloss zu schützen. Es wird am sichersten Ort gespeichert: im Schloss.



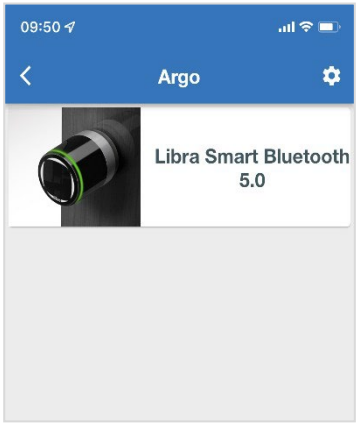
Für höchste Bedienerfreundlichkeit kann das Passwort mit der biometrischen Identifizierung des Smartphones (Fingerabdruck, Gesichtserkennung) verknüpft werden.

Sie können ein *Haus* erstellen und diesem das Schloss zuordnen. Weitere Informationen zum *Haus* finden Sie im Kapitel *Erweiterte Funktionen*.

Das ist das mit dem zuvor eingerichteten Schloss verbundene *Smart Gateway*.

Weitere Informationen zur Sicherheit der *Argo Fernsteuerung* finden Sie in der *Argo 3.0 Broschüre* unter *iseo.com*.

5. Warten Sie, bis die Konfiguration abgeschlossen ist. Das mit dem gewählten Passwort geschützte Schloss wird zum *Argo-Konto* in der *ISEO Cloud* hinzugefügt. Sobald das erfolgt ist, erscheinen das Schlossicon und die Schaltfläche auf der *Startseite* der *Argo Fernsteuerung*.



Das hinzugefügte Schloss erscheint nun auf der *Startseite* der *Argo Fernsteuerung*.

Verbindung zum Schloss aus der Ferne herstellen

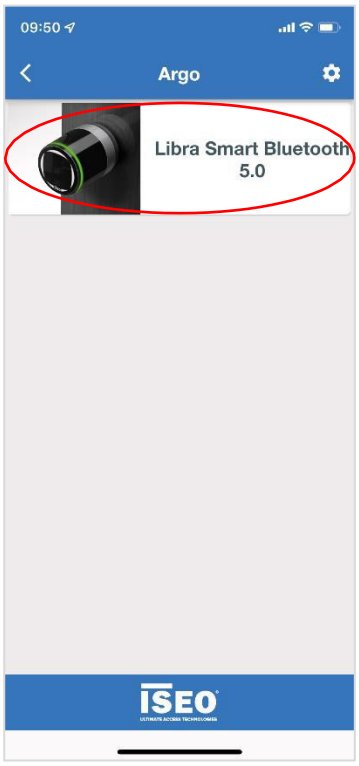
Sobald das *Argo-Konto* erstellt, das *Smart Gateway* eingerichtet und das Schloss zum System hinzugefügt wurde (s. *Grundlagen*), können Sie sich aus der Ferne mit dem *ISEO Smart Gerät* verbinden und Folgendes tun:

- Schloss aus der Ferne öffnen.
- Aus der Ferne am Schloss anmelden.

Schloss aus der Ferne öffnen

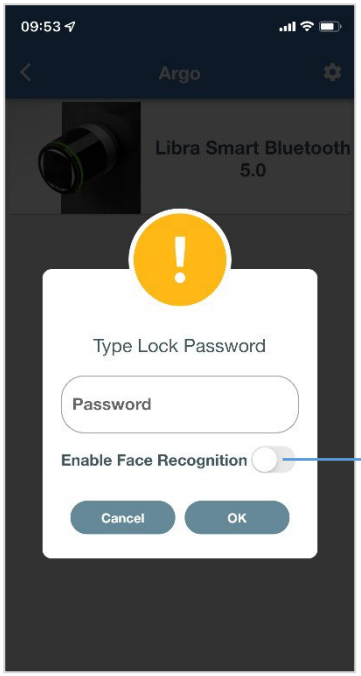
Mit *Argo 3.0* können Türen aus der Ferne geöffnet werden. Das kann in bestimmten Situationen oder Notfällen hilfreich sein, z. B. wenn Sie jemanden hereinlassen wollen, wenn Sie nicht da oder in der Nähe sind. Melden Sie sich dafür am *Argo-Konto* an (s. *Grundlagen, Beim Argo-Konto anmelden*) und folgen Sie den folgenden Schritten.

1. Tippen Sie auf das Schloss mit dem Namen und Icon und warten Sie, bis die Verbindung hergestellt wurde.



Die Funktion *Tap & Hold* von *Argo Local*, um weitere Funktionen anzuzeigen, existiert in der *Argo Fernsteuerung* nicht. Unabhängig davon, ob Sie einmal tippen oder tippen und halten, zeigt Ihnen die App immer die verfügbaren Funktionen.

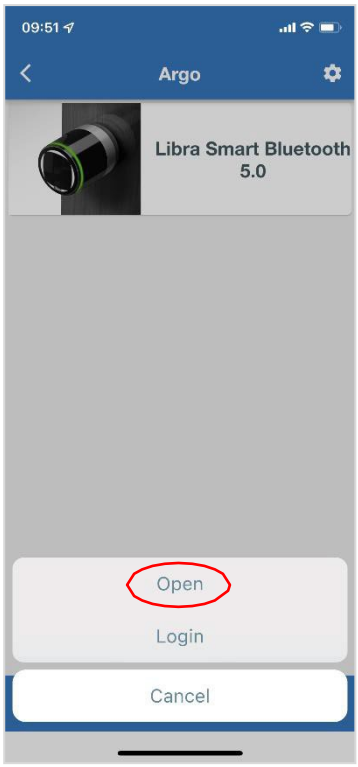
2. Geben Sie das zuvor definierte **Gerätepasswort** ein (*Grundlagen, Schlösser zum System hinzufügen*). Dieses Passwort garantiert die Systemsicherheit und wird am sichersten Ort gespeichert: im Schloss.



Aktivieren Sie die Gesichtserkennung und Fingerabdruck, um das Passwort mit der biometrischen Identifizierung Ihres Smartphones zu verknüpfen.

Dadurch müssen Sie bei den nächsten Vorgängen Ihr Passwort nicht erneut eingeben.

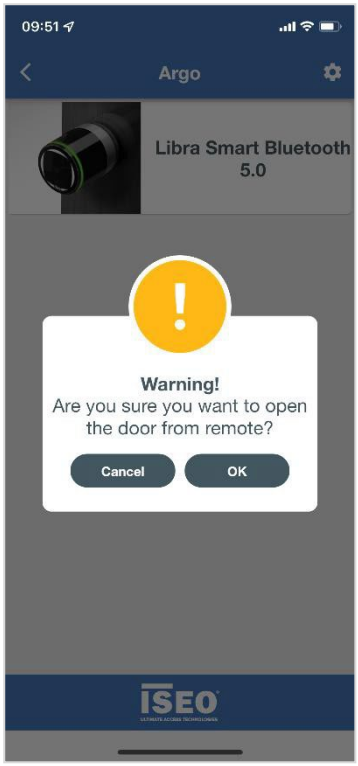
3. Tippen Sie



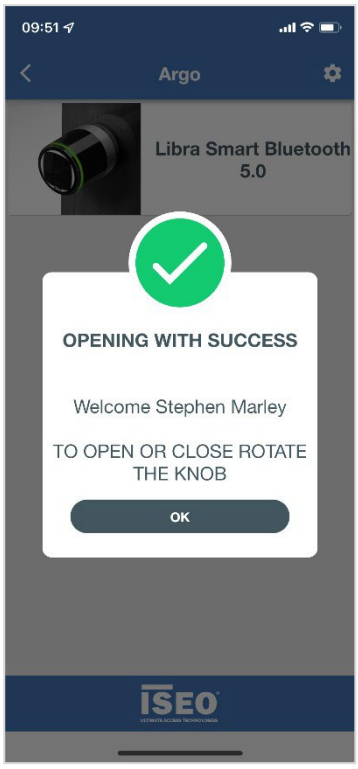
Die Funktion *Programmier-Modus* ist standardmäßig verfügbar, da es sich um die Voraussetzung handelt, damit der *Bediener* das Schloss aus der Ferne verwalten kann.

Der *Remote-Hauptbediener* verfügt standardmäßig über die Funktion *Öffnen*.

4. Eine Tür aus der Ferne zu öffnen, ist ein kritischer Vorgang, da Sie nicht vor der Tür stehen. Bestätigen Sie den Vorgang ein zweites Mal, in dem Sie auf **OK** unter dem Hinweistext tippen.



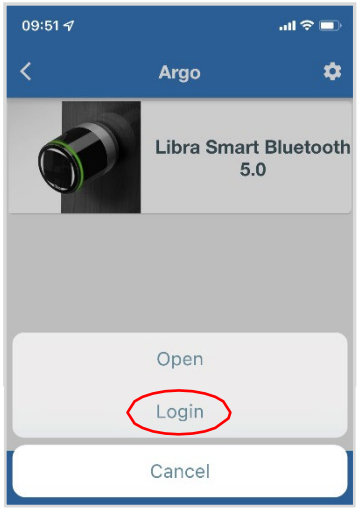
5. Warten Sie auf die Meldung der erfolgten Öffnung.



Programmier-Modus aus der Ferne starten

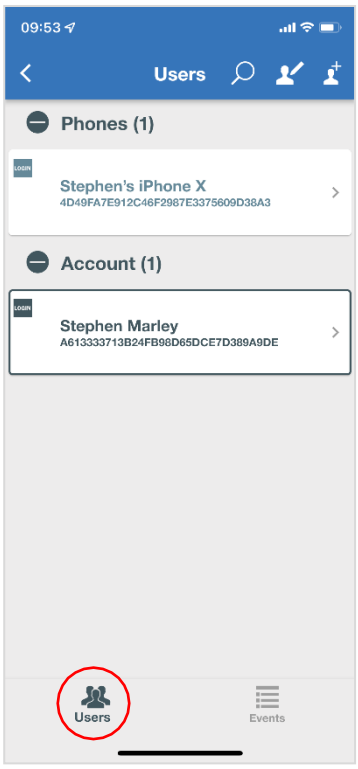
Mit *Argo 3.0* kann der *Bediener* den Programmier-Modus aus der Ferne starten, um die Nutzerliste zu verwalten oder Ereignisse einzusehen. Dafür muss er sich nicht vor dem Schloss oder innerhalb der *Bluetooth*-Reichweite befinden. Um sich aus der Ferne anzumelden:

1. Tippen Sie auf **Programmier-Modus**.



2. Geben Sie das Gerätepasswort ein, sofern keine Verknüpfung mit der Identifizierung am Smartphone besteht (s. *Schloss aus der Ferne öffnen*, *Schritt 2*).

3. Nachdem die Verbindung hergestellt wurde, können Sie direkt remote auf die *Nutzerliste* des Schlosses zugreifen.



Smartphone-Nutzer mit Zugriff auf den Programmier-Modus. Er wird als **Lokaler Bediener** bezeichnet.

Bedienerkonto. Es wird als **Remote-Hauptbediener** bezeichnet.

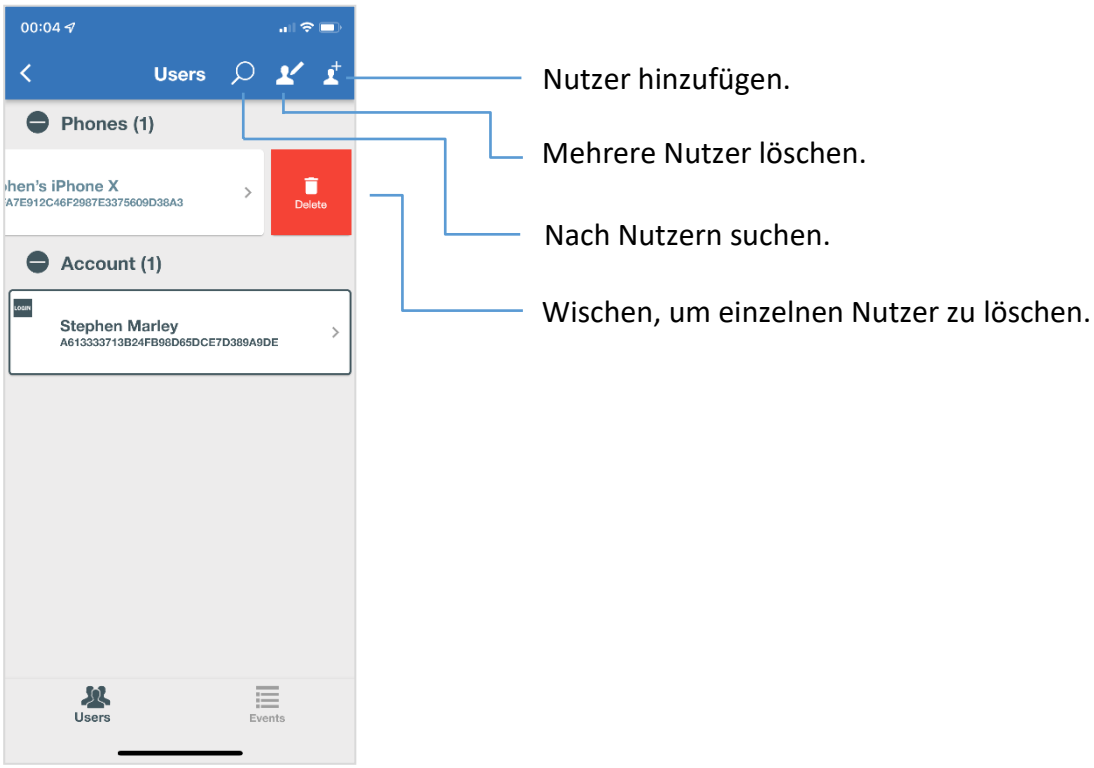
Bei einem *Bediener* kann es sich um einen *lokalen* oder einen *Remote-Bediener* handeln oder aber er verfügt wie im obigen Beispiel über beide Rollen. *Lokale Bediener* können sich nicht remote anmelden, *Remote-Bediener* nicht lokal.

Nach dem Starten des Programmier-Modus können Sie:

- *Nutzer* hinzufügen, bearbeiten oder löschen.
- Die *Ereignisse* auslesen.
- Ein *Gastkonto* hinzufügen (Informationen dazu finden Sie im Kapitel *Erweiterte Funktionen*).

Nutzer hinzufügen, bearbeiten oder löschen

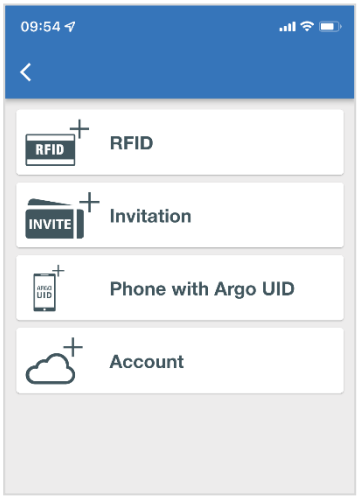
Wie bei *Argo Local* können Sie remote nach Nutzern suchen, Nutzer hinzufügen, bearbeiten oder löschen.



Die Benutzeroberfläche der *Argo Fernsteuerung* ist mit der von *Argo Local* identisch: gleiche Logik, gleiches Aussehen, dieselben Schaltflächen und Symbole. Dies dient dazu, die beste Nutzererfahrung und Bedienerfreundlichkeit zu ermöglichen: Wer *Argo Local* kennt, weiß direkt, wie er die *Argo Fernsteuerung* verwendet.

Weitere Informationen zu *Argo Local* finden Sie im *Argo 2.7 Nutzerhandbuch*, verfügbar unter *iseo.com*.

Tippen Sie auf das Symbol **Nutzer hinzufügen** , um die Identmedien zu sehen, die je nach *ISEO Smart Gerät* hinzugefügt werden können. Es können dieselben Identmedien wie bei *Argo Local* hinzugefügt werden, zudem ein weiteres: *Account* (s. Kapitel *Erweiterte Funktionen*).

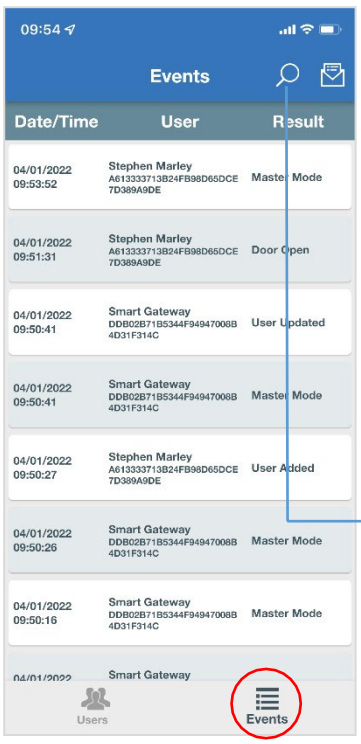


Das *ISEO Smart Gerät* im Beispiel ist Libra Smart, daher können wir keinen PIN-Code hinzufügen.

Die Option *Fingerabdruck hinzufügen* für *x1R Smart* bei *Argo Local* ist bei der *Argo Fernsteuerung* aufgrund des Registrierungsvorgangs, bei dem der Nutzer anwesend sein muss, nicht verfügbar.

Ereignisse auslesen

Wenn Sie auf das Menü *Ereignisse* tippen, können Sie aus der Ferne alle Ereignisse sehen. Die *Ereignisse* werden wie bei *Argo Local* dargestellt, um die beste Nutzererfahrung und Bedienerfreundlichkeit zu ermöglichen und der Devise von Einfachheit und Effektivität von *Argo* gerecht zu werden.



Tippen Sie, um die angezeigten Ereignisse per E-Mail oder anderer Kommunikationsapp zu versenden.
Anders als bei *Argo Local* können Sie nicht alle Ereignisse auf einmal versenden, sondern nur die auf dem Smartphone bereits geladenen Ereignisse.
Scrollen Sie in der Ereignisliste weiter nach unten, um weitere Ereignisse anzuzeigen. Alle dargestellten Ereignisse können per E-Mail verschickt werden.

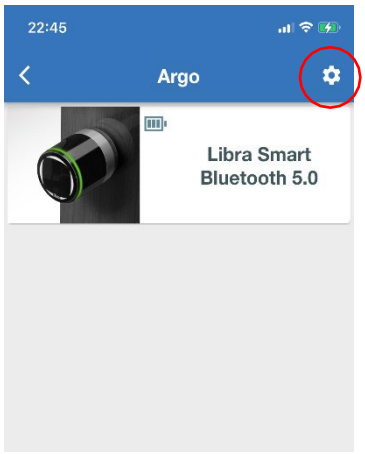
Tippen Sie, um die Suche zu öffnen und nach *Datum/Uhrzeit*, *Nutzer* oder *Ergebnis* zu filtern; es reicht, wenn Sie dafür nur einige Zeichen eingeben.

Erweiterte Funktionen

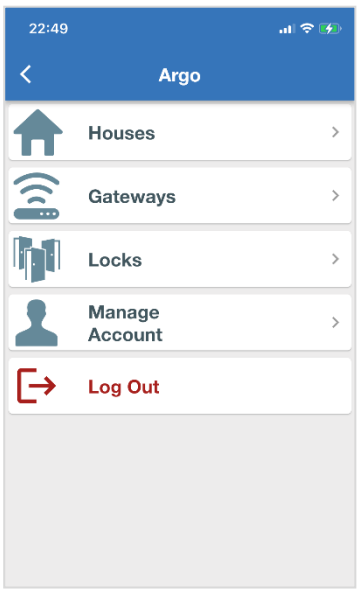
In diesem Abschnitt finden Sie weitere Erläuterungen zu Menüs in der *Argo Fernsteuerung* sowie den zugehörigen Funktionen. Nach der Menüübersicht wird jede Funktion einzeln erklärt.

Menüübersicht Argo Fernsteuerung

1. Melden Sie sich bei Ihrem **Argo-Konto** an und tippen Sie auf das Menü-Symbol .



2. Auf dieser Seite finden Sie alle zugehörigen Untermenüs.



Häuser hinzufügen, löschen oder umbenennen.

Gateways hinzufügen, löschen oder umbenennen.

Türschlösser hinzufügen, löschen oder umbenennen.

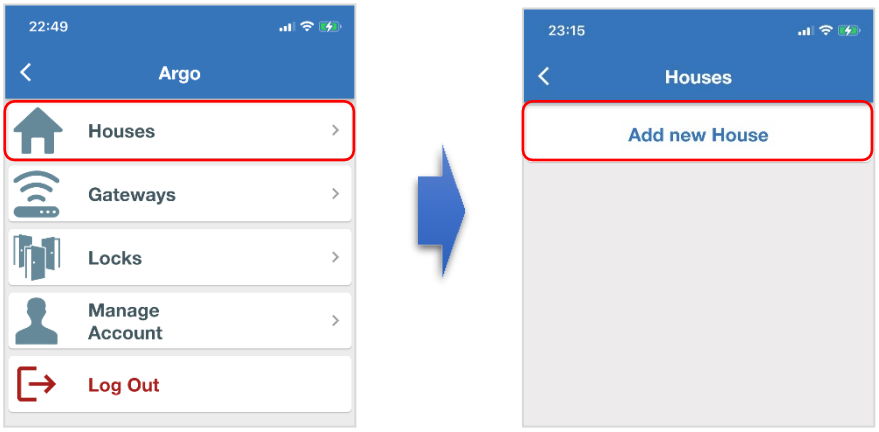
- Konto-Informationen
- Gesichtserkennung oder
- Fingerabdruck aktivieren
- Kontopasswort zurücksetzen

Abmelden

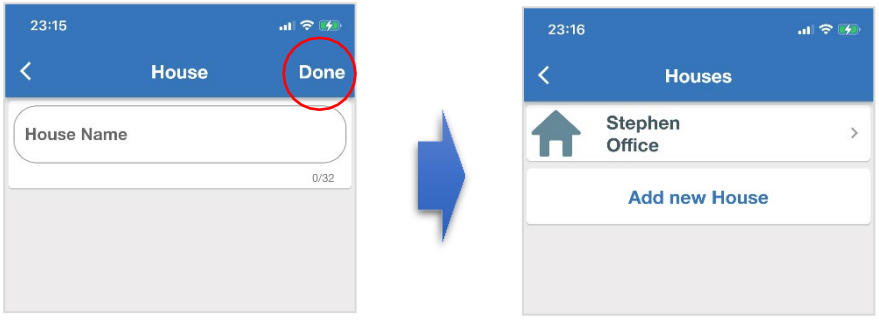
Häuser

In diesem Menü können Sie neue *Häuser* erstellen oder bestehende verwalten (löschen oder umbenennen).
Um ein neues **Haus** hinzuzufügen:

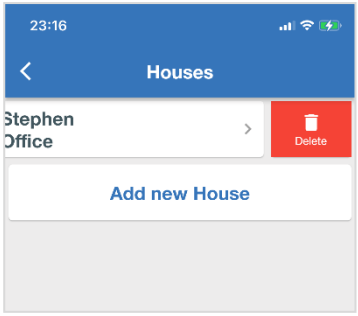
1. Tippen Sie auf **Häuser** und dann auf **Neues Haus hinzufügen**.



2. Geben Sie den **Namen des Hauses** ein und tippen Sie dann auf **Fertig**. Das *Haus* wird erstellt.



3. Um ein *Haus* zu löschen, wischen Sie von rechts nach links.



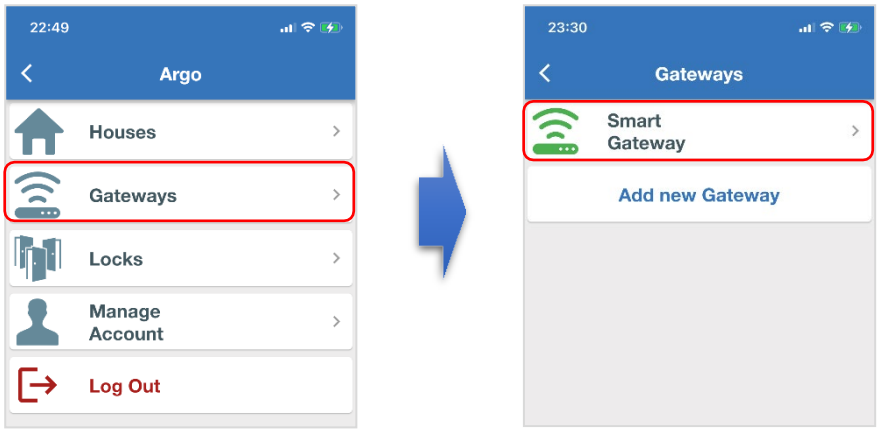
4. Um ein *Haus* umzubenennen, tippen Sie auf den Hausnamen, um ihn zu bearbeiten.

Gateways

In diesem Menü können Sie neue *Gateways* erstellen oder bestehende verwalten: löschen, umbenennen und Informationen einsehen.

Um die **Gateway**-Informationen einzusehen:

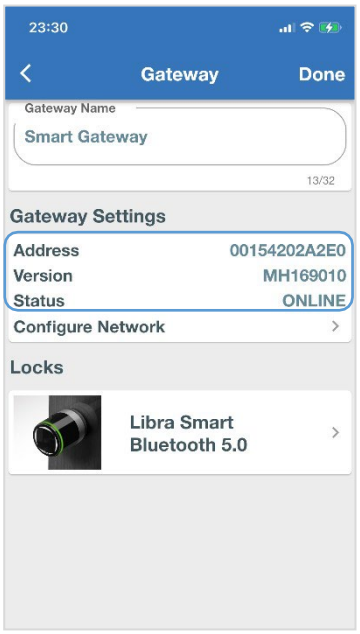
1. Tippen Sie auf **Gateways** und dann auf den Namen des *Gateways*.



Ein grünes *Gateway*-Symbol bedeutet, dass das *Gateway* online ist. Ein rotes *Gateway*-Symbol bedeutet, dass das *Gateway* offline ist (keine Internetverbindung).

Tippen Sie auf **Neues Gateway hinzufügen**, um den bereits erläuterten Assistenten zu starten (s. *Grundlagen*, *Smart Gateway einrichten*).

2. Auf dieser Seite können Sie alle Informationen des Gateways einsehen.



Tippen Sie, um den Namen des Gateways zu ändern.

Softwareinformationen des Gateways.

Tippen Sie, um das WLAN des Gateways neu einzurichten. Das kann z. B. beim Routeraustausch sinnvoll sein.

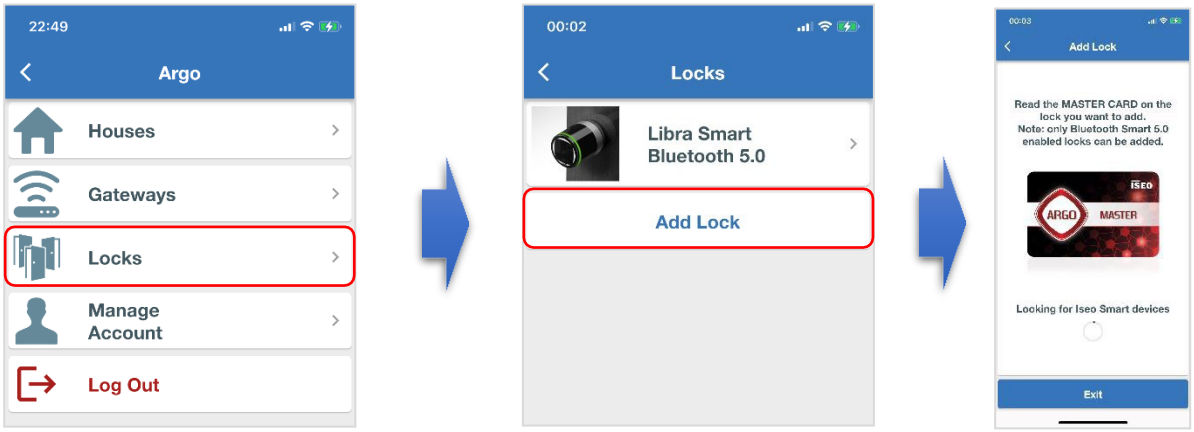
Mit dem Gateway verbundenes Schloss. Tippen Sie auf den Schlossnamen und das Symbol, um direkt ins Schlossmenü zu gelangen, das auch über das Hauptmenü aufgerufen werden kann (s. *Schlösser*).

Schlösser

In diesem Menü können Sie *Schlösser* hinzufügen oder löschen oder die Zuweisung zu Häusern vornehmen oder ändern.

Neues Schloss hinzufügen

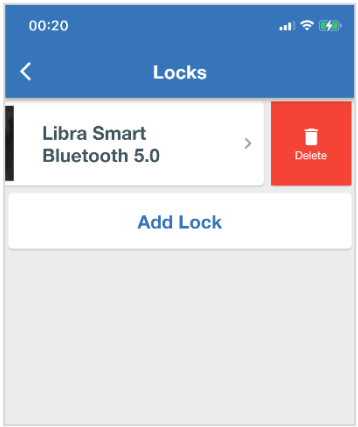
- Tippen Sie auf **Schlösser** und dann auf **Schloss hinzufügen**. Damit starten Sie den bereits erläuterten Assistenten (s. *Grundlagen*, *Schlösser zum System hinzufügen*).



Für diesen Vorgang muss sich der Bediener vor dem Schloss befinden und er erfordert die Master-Karte.

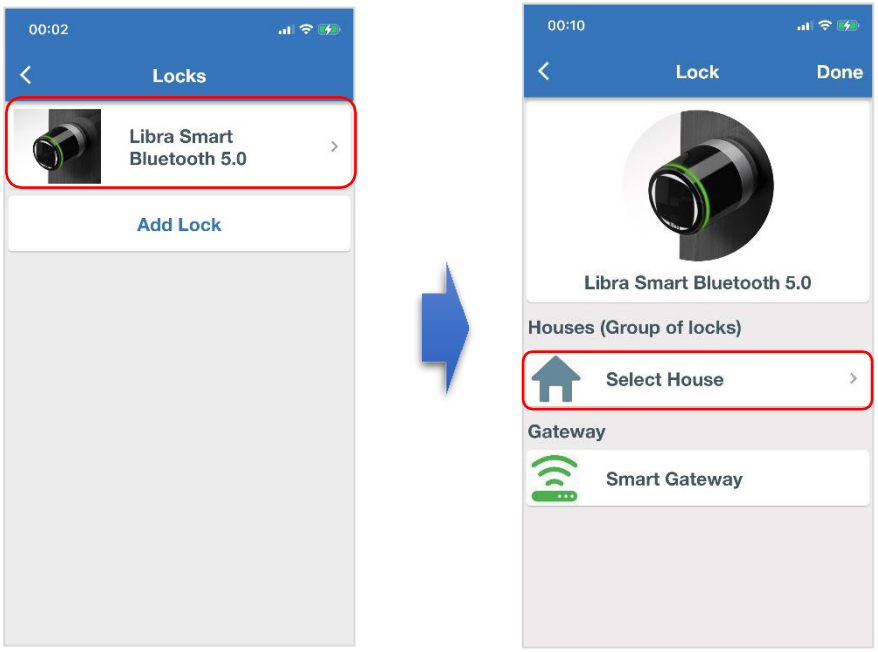
Schloss löschen

- Tippen Sie auf **Schlösser** und löschen Sie ein Schloss mit der Wischgeste. Bestätigen Sie die Warnung mit OK.

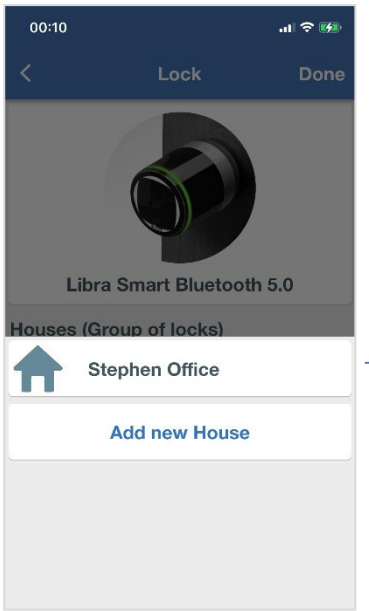


Schlösser einem Haus zuweisen

1. Tippen Sie im Schlossmenü auf den Schlossnamen und das Symbol und dann auf **Haus wählen**.



2. Wählen Sie das *Haus*, dem Sie das Schloss zuordnen wollen (z. B. Büro Stephen), oder tippen Sie auf **Neues Haus hinzufügen**, um ein neues zu erstellen.



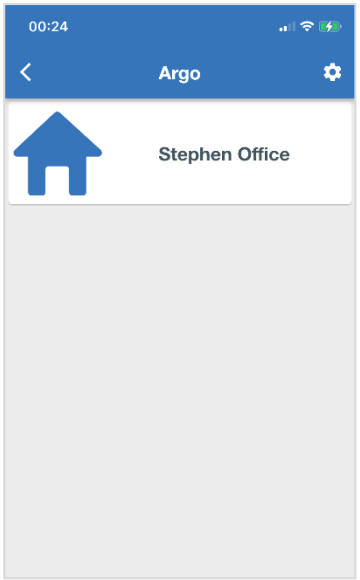
Ein zuvor im System eingerichtetes Haus.

Sie können Häuser bei der ersten Systemeinrichtung erstellen (*Grundlagen*, *Schlösser zum System hinzufügen*) oder direkt im Menü Häuser.

3. Tippen Sie am Ende auf **Fertig**, um die Änderungen zu speichern.

Dem Schloss zugeordnetes **Haus**.

4. Nachdem dem Schloss ein Haus zugewiesene wurde, ändert sich die *Argo 3.0 Startseite*:

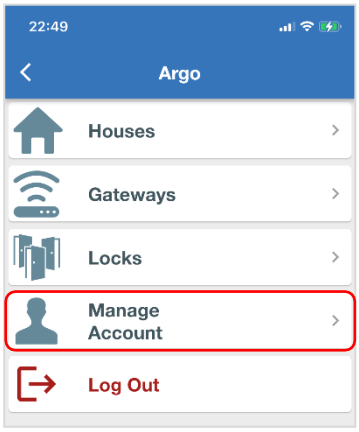


Startseite: Das Schloss ist nun „im“ *Haus*. Tippen Sie auf den Namen des *Hauses* und das Symbol, um die Schlösser anzuzeigen, die zum Haus gehören.

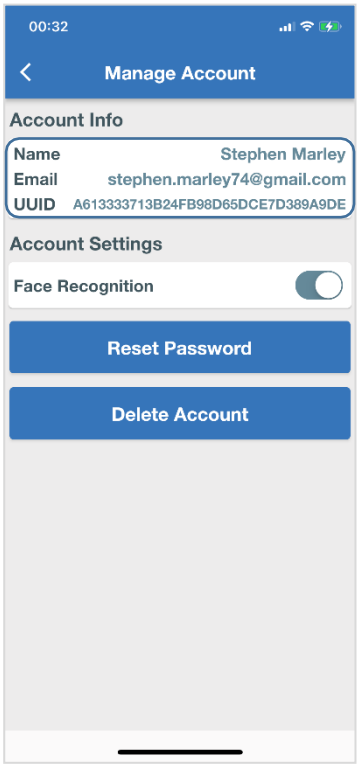
Konto verwalten

In diesem Menü sehen Sie die Konto-Informationen und können die im Folgenden erläuterten Vorgänge vornehmen.

1. Tippen Sie auf **Account verwalten**.



2. Im Menü **Account verwalten** finden Sie die folgenden Informationen:



Konto-Informationen.

Gesichtserkennung oder Fingerabdruck aktivieren (abhängig von den Funktionen Ihres Smartphones), um das Gerätepasswort mit Ihrer biometrischen Identifizierung zu verknüpfen und damit den Verbindungsvorgang für beste Nutzererfahrung und Bediener-freundlichkeit zu beschleunigen.

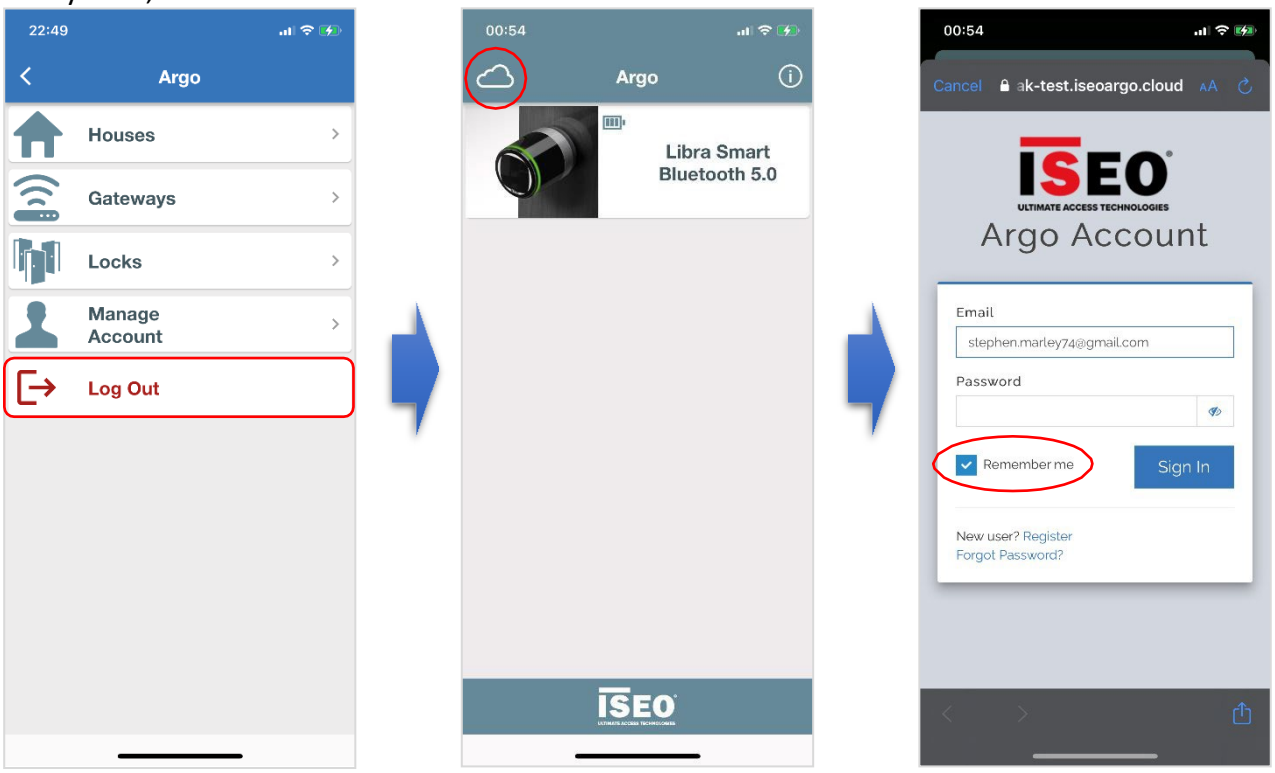
Tippen Sie, um das Account-Passwort zurücksetzen und folgen Sie dann den Anweisungen.

Tippen Sie hier, um Ihr *Konto* dauerhaft zu löschen.
Das Löschen des Kontos ist ein kritischer Vorgang, sofern es eingerichtete Geräte enthält (Schlösser und Gateways). Wie Sie zum Löschen Ihres Kontos am besten vorgehen, erfahren Sie unter *Konto des Hauptbedieners löschen*.

Abmelden

Wenn Sie auf **Abmelden** tippen, wird der *Bediener* sofort vom *Konto* abgemeldet. Um sich wieder als *Bediener* anzumelden, muss das Passwort eingegeben werden. Um sich vom *Konto* abzumelden:

1. Tippen Sie auf **Abmelden**, um die *Argo Fernsteuerung* zu verlassen. Tippen Sie auf das *Cloud*-Symbol, um sich wieder anzumelden.

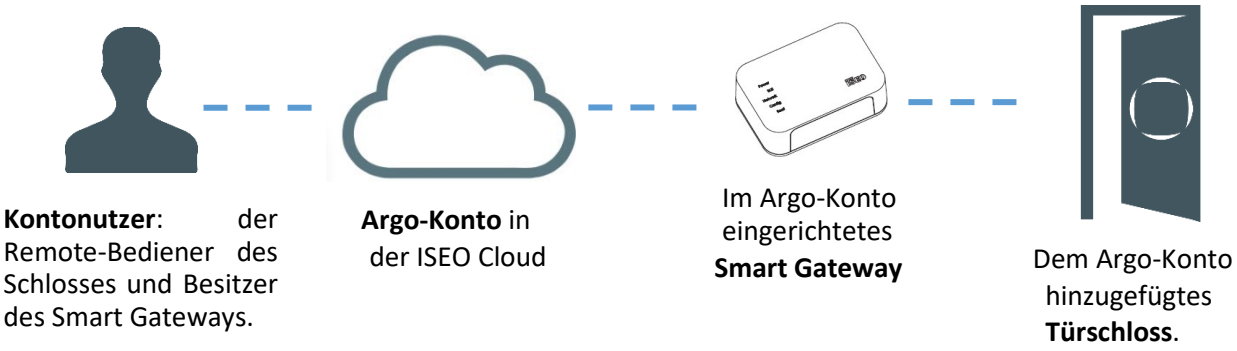


Durch das **Abmelden** wird die Funktion *Angemeldet bleiben* überschrieben. Es kann also aus Sicherheitsgründen verwendet werden, um sicherzustellen, dass niemand auf das Konto zugreifen kann, selbst wenn er Ihr Smartphone hat.

Die Funktion **Angemeldet bleiben** ermöglicht das schnelle Anmelden beim *Konto* ohne erneute Eingabe des Passworts. Das gilt für einen von der App definierten Zeitraum.

Kontonutzer

Die Rolle *Kontonutzer* ist eine neue Rolle bei der *Argo Fernsteuerung*. Es handelt sich im Prinzip um den *Remote-Bediener*. Der *Remote-Bediener* muss über ein *Argo-Konto* verfügen, einen Ort in der *ISEO Cloud*, um die *Argo Fernsteuerung* zu verwenden. Das ist die Voraussetzung, um ein Schloss über ein *Smart Gateway* zu erreichen.



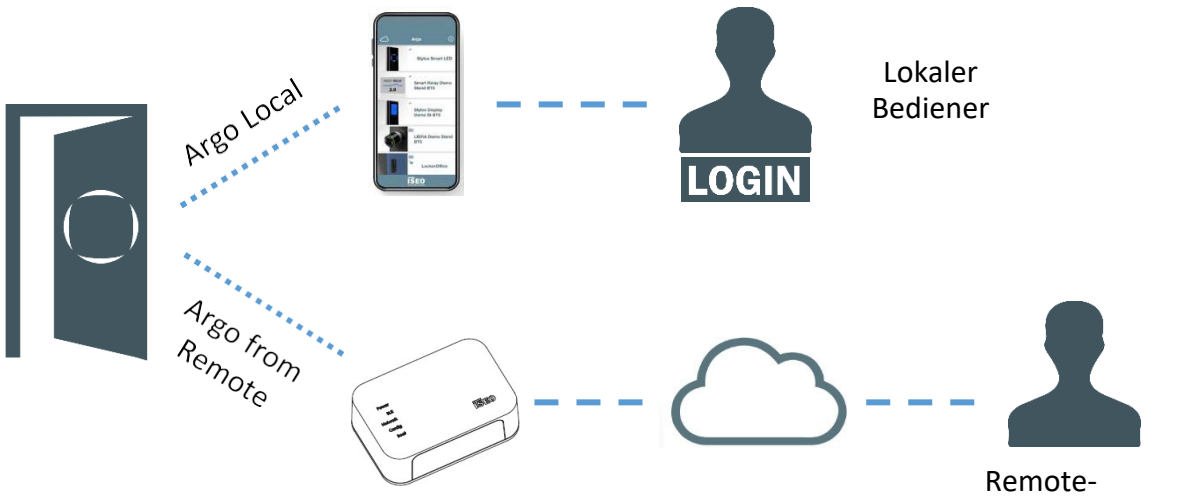
Kontonutzer: der Remote-Bediener des Schlosses und Besitzer des Smart Gateways.

Argo-Konto in der ISEO Cloud

Im Argo-Konto eingerichtetes **Smart Gateway**

Dem Argo-Konto hinzugefügtes **Türschloss**.

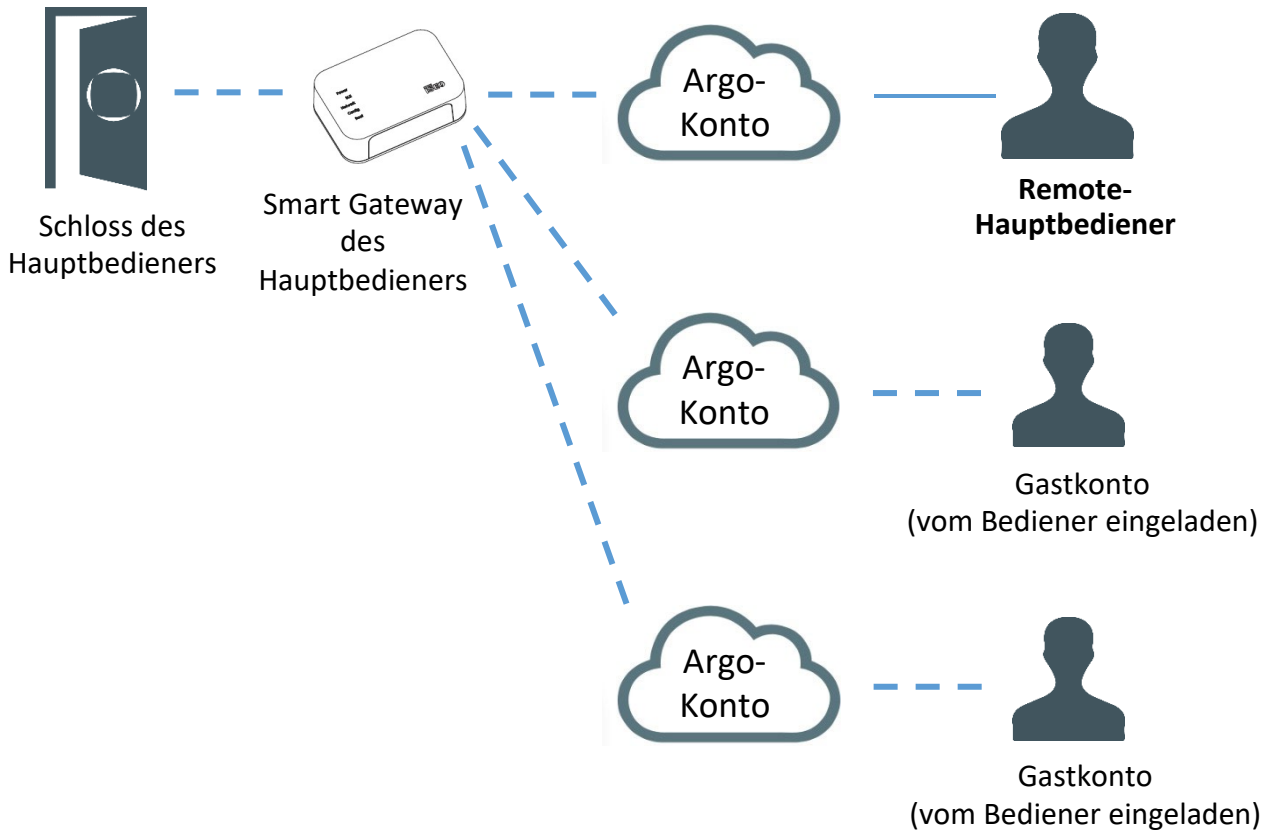
Der *Remote-Bediener* darf nicht mit dem *lokalen Bediener* verwechselt werden (s. *Glossar*). Es handelt sich um zwei verschiedene Rollen, die auch zusammen in einem Schloss auftreten können. Ein *lokaler Bediener* ist das, was bisher mit *Argo Local* verwaltet wurde: jeder Smartphone-Nutzer mit Zugriff auf den Programmier-Modus. *Argo* kann über viele *lokale Bediener* für ein Schloss mit denselben Zutrittsrechten verfügen. Bei *Argo Local* bestehen de facto keine unterschiedlichen *Bedienerberechtigungen*: Jeder *Bediener* ist hierarchisch auf derselben Ebene. Beachten Sie, dass jeder *lokale Bediener* unbegrenzt andere *Bediener* registrieren kann (sofern der *Programmier-Modus* aktiviert ist): über die *Master*-Karte, mittels *Einladung* oder über *Smartphone mittels Argo-UID hinzufügen*.



Gastkonto

Der *Remote-Bediener*, der zuerst das *Argo-Konto* erstellt, das *Smart Gateway* eingerichtet und die Schlösser zum System hinzugefügt hat (s. *Grundlagen*), ist der Inhaber des Gateways, des Systems, und wird daher auch als *Remote-Hauptbediener* bezeichnet.
Der *Hauptbediener* kann auch andere *Remote-Bediener* einladen, um das Schloss mit ihnen aus der Ferne zu verwalten, zum Beispiel, um die Tür im Notfall zu öffnen, Nutzer hinzuzufügen oder Ereignisse zu prüfen. Diese eingeladenen *Remote-Bediener* werden als *Gastkonto* bezeichnet.

Ein Gastkonto muss über ein aktives *Argo-Konto* verfügen, um über die *ISEO Cloud* eine Verbindung herzustellen. Es wird aber kein Gateway benötigt, da auf das *Gateway des Hauptbedieners* für die Kommunikation mit dem Schloss zurückgegriffen wird.



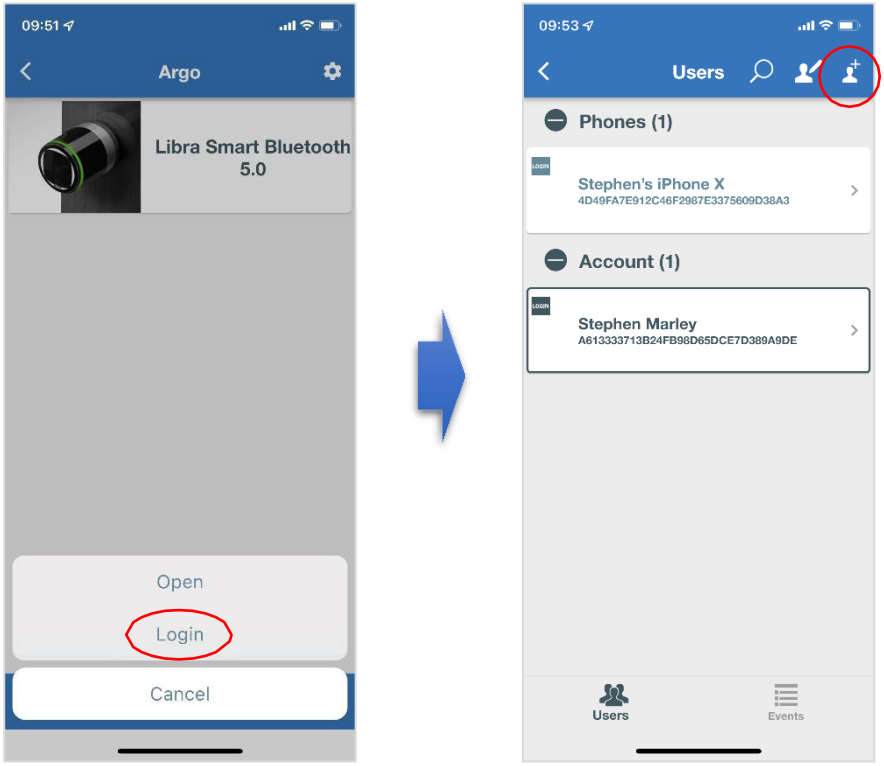
Im Gegensatz zu *Argo Local* gibt es bei der *Argo Fernsteuerung* die Möglichkeit, dem *Gastkonto* verschiedene *Bedienerrechte* zuzuweisen (weitere Informationen finden Sie unter *Konto hinzufügen*).

Konto hinzufügen (Remote-Bediener einladen)

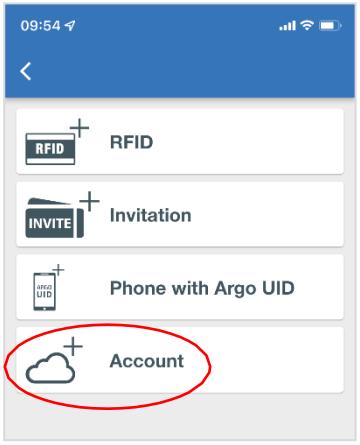
Der *Remote-Hauptbediener* kann einen oder mehrere *Bediener* hinzufügen, um das Schloss aus der Ferne zu verwalten. Diese Funktion heißt *Konto hinzufügen* und ermöglicht es, neue *Remote-Bediener*, auch bezeichnet als *Gastkonto*, einzuladen. Um dem Schloss ein *Gastkonto* hinzuzufügen, gehen Sie wie folgt vor:

Erster Teil: Der Hauptbediener schickt dem Gastkonto eine Einladung.

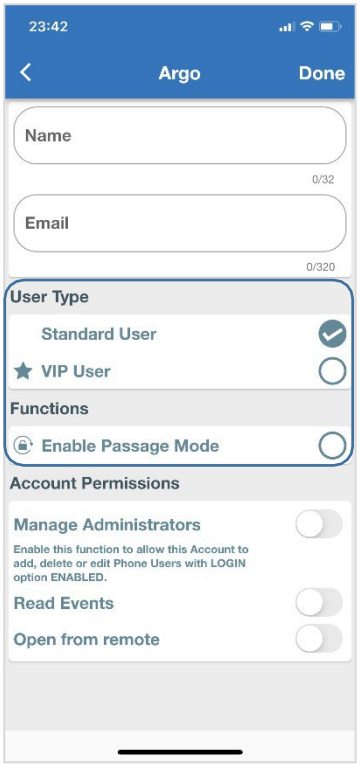
1. Melden Sie sich am Schloss an und tippen Sie auf **Nutzer hinzufügen** .



2. Tippen Sie auf **Konto hinzufügen** .



3. Geben Sie den **Namen** und die **E-Mailadresse** des *Bedieners* ein, den Sie einladen wollen. Aktivieren Sie die erforderlichen Funktionen und Berechtigungen, die unten erläutert werden.



Name des *Gastkontos*.

E-Mailadresse des *Gastkontos*.

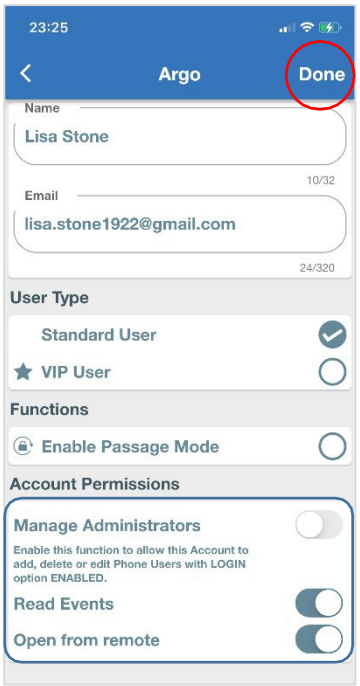
Standard-Argofunktionen (weitere Informationen finden Sie im *Argo 2.7 Nutzerhandbuch*, verfügbar unter *iseo.com*).

Siehe *Verwaltung von Bedienern*.

Wenn Sie diese Funktion aktivieren, kann mit dem *Gastkonto* die *Ereignisliste* des Schlosses gelesen werden.

Wenn Sie diese Funktion aktivieren, kann mit dem *Gastkonto* das Schloss aus der Ferne geöffnet werden (das Schloss, zu dem es eingeladen wurde).

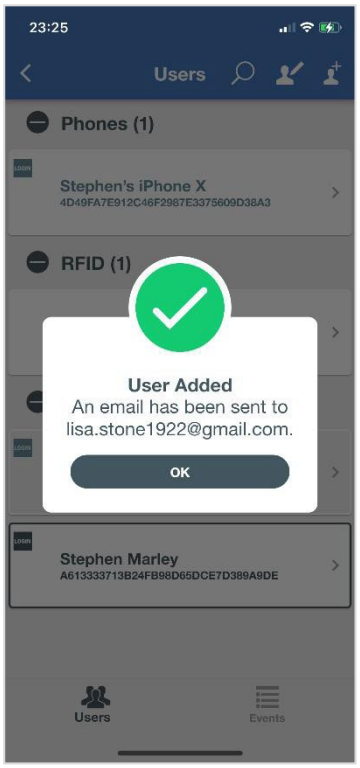
4. Tippen Sie am Ende auf **Fertig**.



Der *einzuladende Bediener* muss bereits über ein aktives *Argo-Konto* verfügen, das in der *ISEO Cloud* registriert ist, sonst kann er nicht als *Gastkonto* hinzugefügt werden (eine Fehlermeldung erscheint; weitere Informationen zu Fehlermeldungen finden Sie unter *Problembehebung*). Es ist möglich, ein *Argo-Konto* zu erstellen, ohne *Smart Gateways* oder *Schlösser* eingerichtet zu haben.

Im Beispiel hier kann der *eingeladene Bediener* die **Ereignisse lesen** und **Aus der Ferne öffnen** (aktivierte *Berechtigungen*).

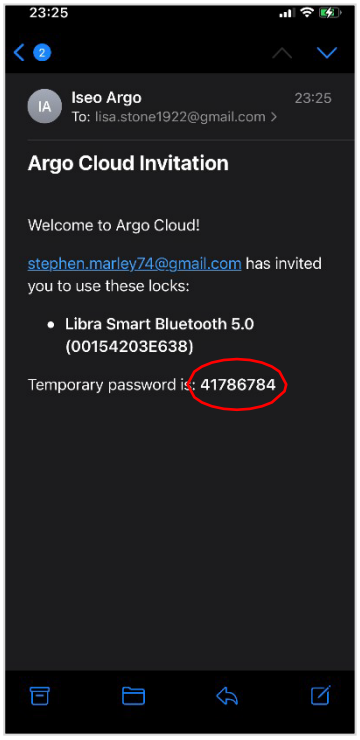
5. Warten Sie, bis der Vorgang **Nutzer hinzufügen** bestätigt wird und tippen Sie **OK**.



Das Gastkonto wird informiert und erhält demnächst eine Einladung per E-Mail.

Zweiter Teil: Der eingeladene Bediener (Gastkonto) erhält die E-Mail.

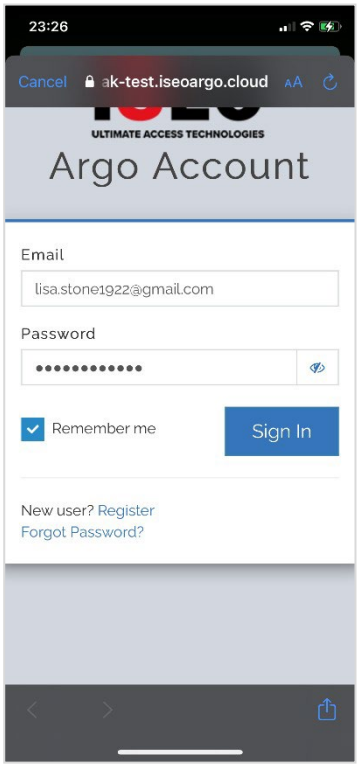
1. Der eingeladene *Bediener* erhält eine E-Mail wie im Beispiel unten.



Das *temporäre Passwort* wird automatisch mit der Einladung generiert und ist das *Gerätepasswort*. Das *Gastkonto* benötigt das Passwort, um mit dem Schloss zu kommunizieren (Öffnung und Programmier-Funktion).

Aus Sicherheitsgründen sollte das *Gastkonto* das Passwort nach der ersten Anmeldung durch ein persönliches Passwort ersetzen.

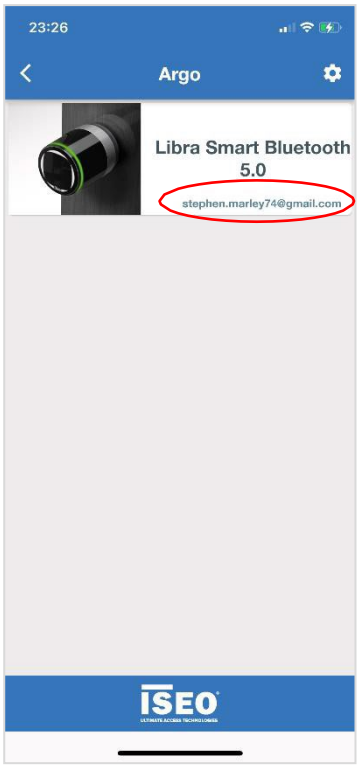
2. Der eingeladene *Bediener* meldet sich bei seinem *Argo-Konto* an.



Der *einzuladende Bediener* muss über ein aktives *Argo-Konto* in der *ISEO Cloud* verfügen, sonst kann er nicht vom Hauptbediener eingeladen werden (Informationen zum Einrichten eines neuen Kontos finden Sie unter *Grundlagen*, *Argo-Konto erstellen*).

Es ist möglich, ein *Argo-Konto* zu erstellen, ohne *Smart Gateways* oder *Schlösser* eingerichtet zu haben.

3. Der eingeladene *Bediener* findet das Schloss, zu dem er eingeladen wurde, auf der *Startseite* von der *Argo Fernsteuerung*.

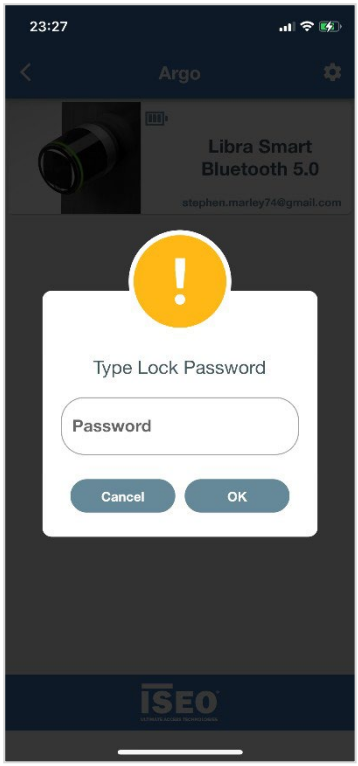


Das neue Schloss, das dem *Hauptbediener* Stephen Marley gehört, erscheint nun auf der *Startseite* des *Kontos* von Lisa Stone.

Unter dem Schlossnamen und Symbol steht die E-Mailadresse des *Hauptbedieners*. Damit lässt sich direkt erkennen, dass das Schloss einem anderen *Argo-Konto* zugeordnet ist.

Die Nachricht *System konfigurieren* erscheint nicht, da das *Konto* auf das *Gateway* des *Hauptbedieners* des Schlosses zugreift. Dem *Konto* kann jederzeit ein eigenes Gateway im Menü *Gateways* hinzugefügt werden.

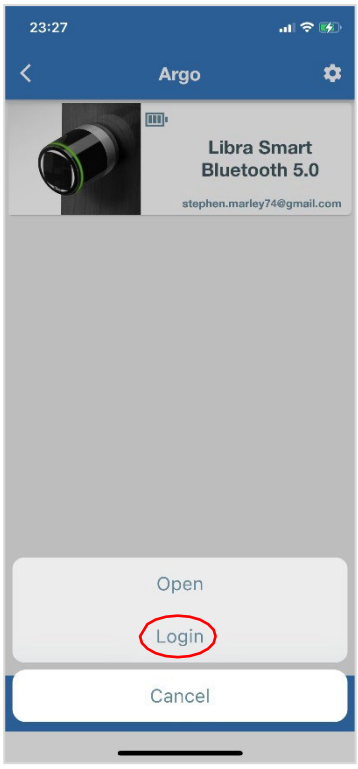
4. Tippen Sie auf den Schlossnamen, um die Kommunikation zu beginnen. Das temporäre *Gerätepasswort* ist für die Verbindung erforderlich.



Geben Sie das temporäre *Gerätepasswort* ein, das Sie in der Einladungsmail erhalten haben.

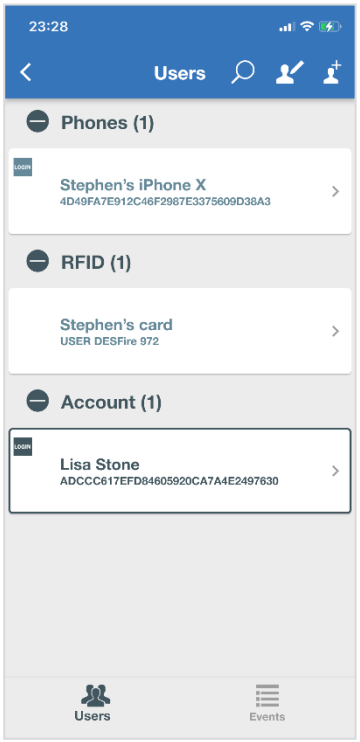
Aktivieren Sie die *Gesichtserkennung und Fingerabdruck* im Menü *Konto verwalten*, um das Passwort mit der biometrischen Identifizierung Ihres Smartphones zu verknüpfen.

5. Tippen Sie auf **Programmier-Modus**.



Funktion *Öffnen* verfügbar, da sie vom *Hauptbediener* freigegeben wurde.

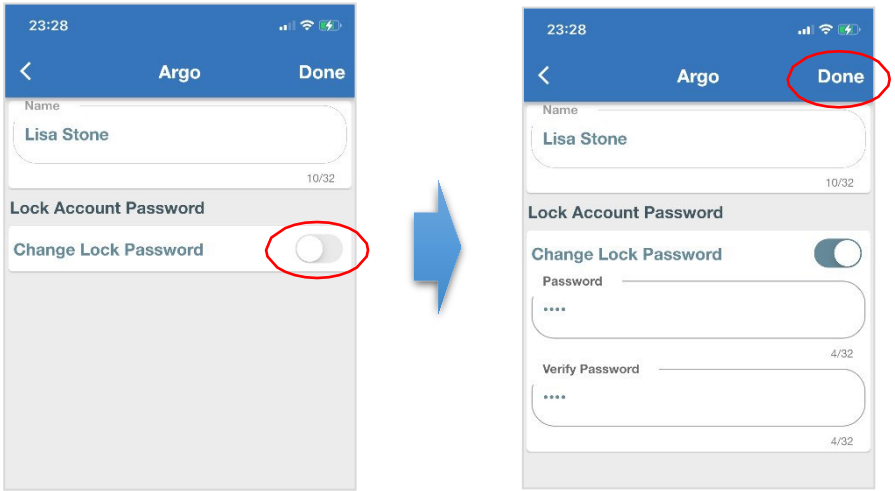
6. Die **Nutzerliste** der *Argo Fernsteuerung* erscheint.



Auf das Konto des *Hauptbedieners* kann vom *Gastkonto* aus nicht zugegriffen werden. Über das Gastkonto können keinerlei Einstellungen des Schlossinhabers geändert werden.

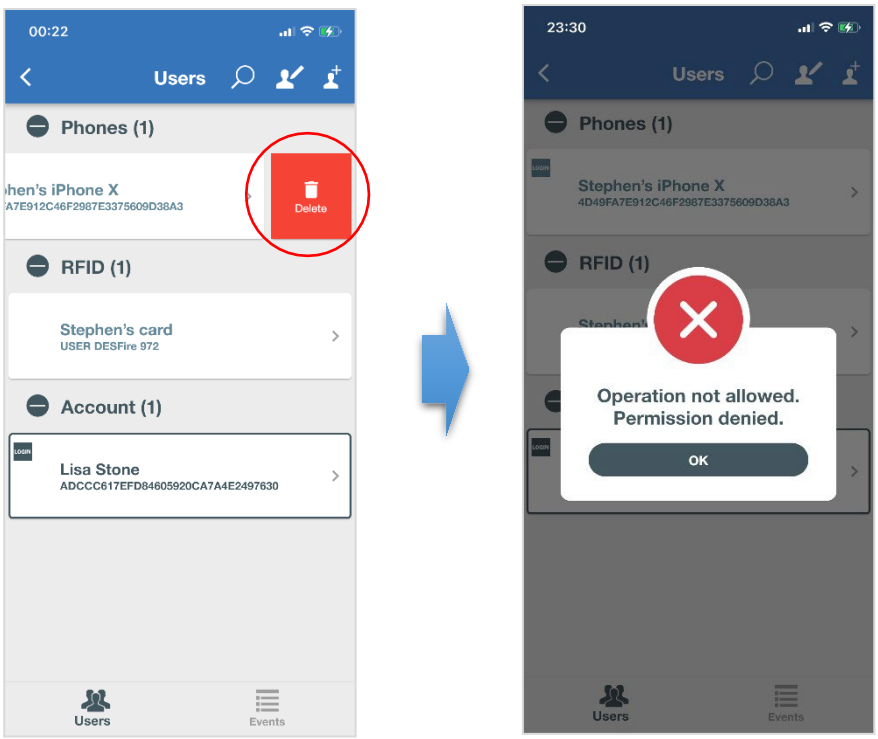
Gastkonto

7. Wenn Lisa Stone auf ihr *Konto* tippt, kann sie ausschließlich das *Gerätepasswort* ändern. Aus Sicherheitsgründen wird ausdrücklich empfohlen, das temporäre Gerätepasswort durch ein persönliches Passwort zu ersetzen. Um das Passwort zu ändern, aktivieren Sie die Schaltfläche, geben Sie das neue Passwort ein und tippen Sie **Fertig**. Sie werden automatisch auf die *Startseite* von der *Argo Fernsteuerung* weitergeleitet. Tippen Sie dann auf den Schlossnamen und das Symbol und geben Sie das Passwort ein, um eine Verbindung herzustellen.



Aktivieren Sie die *Gesichtserkennung und Fingerabdruck* im Menü *Konto verwalten*, um das Passwort mit der biometrischen Identifizierung Ihres Smartphones zu verknüpfen.

8. Entsprechend der *Kontoberechtigungen*, die von *Hauptbediener* definiert wurden, kann Lisa Stone *Aus der Ferne Öffnen* und *Ereignisse anzeigen*, aber nicht *Bediener verwalten*. Das bedeutet, dass sie weder *Smartphone-Nutzer* mit Zugriff auf den Programmier-Modus hinzufügen, löschen oder bearbeiten kann.
   Beispiel: Wenn Lisa Stone versucht, den *Smartphone-Nutzer Stephens iPhone* zu löschen, erhält sie eine Fehlermeldung wie unten dargestellt und der Vorgang wird nicht ausgeführt.



9. Lisa kann jede Art von Identmedien registrieren, hinzufügen, bearbeiten oder löschen, da es sich dabei um die Grundfunktionen für *Bediener* handelt. Sie kann aber kein *Gastkonto* hinzufügen, da sie nicht Inhaberin des Schlosses ist.

Nur der *Hauptbediener* kann ein *Gastkonto* zum Schloss hinzufügen (andere Bediener einladen).

Konto löschen

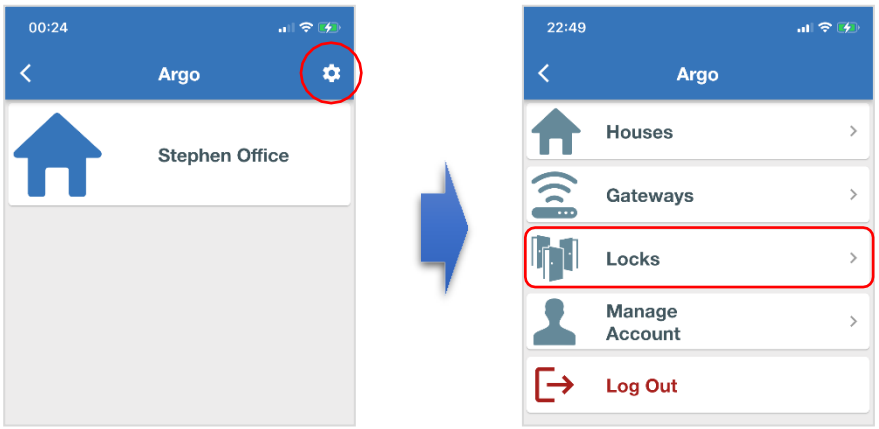
Das Löschen eines Kontos ist ein kritischer Vorgang, da er alle eingerichteten *Gateways* und *Schlösser* betrifft. Ein *Konto* kann auch mit einem oder mehreren *Gast-Konten* verknüpft sein, um einige Schlösser gemeinsam zu verwalten. Zusammenfassend bedeutet das: Bevor Sie ein *Konto* löschen, müssen wir Folgendes berücksichtigen:

- Anzahl der im Konto eingerichteten **Gateways**.
- Anzahl der mit den Gateways verbundenen **Schlösser**.
- Alle **Gast-Konten**, die auf ein oder mehrere Schlösser zugreifen können.

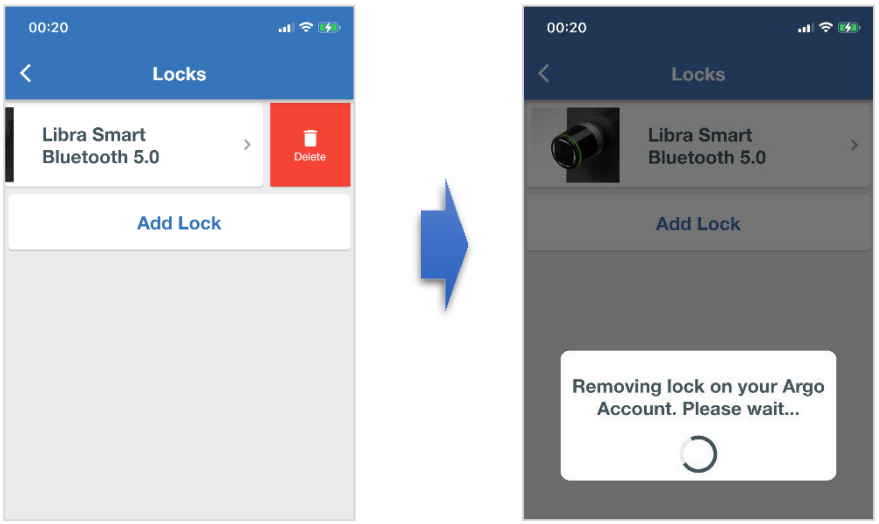
Nur der *Hauptbediener* kann sein Konto und die zugehörigen *Gast-Konten* löschen. Wenn der *Hauptbediener* das *Konto* löscht, werden alle zugehörigen *Gast-Konten* automatisch gelöscht.

Im folgenden Beispiel löschen wir das zuvor erstellte *Konto* (*Grundlagen*, *Argo-Konto erstellen*).

1. Melden Sie sich beim **Konto** an und tippen Sie auf das Menü-Symbol , tippen Sie dann auf **Schlösser**.



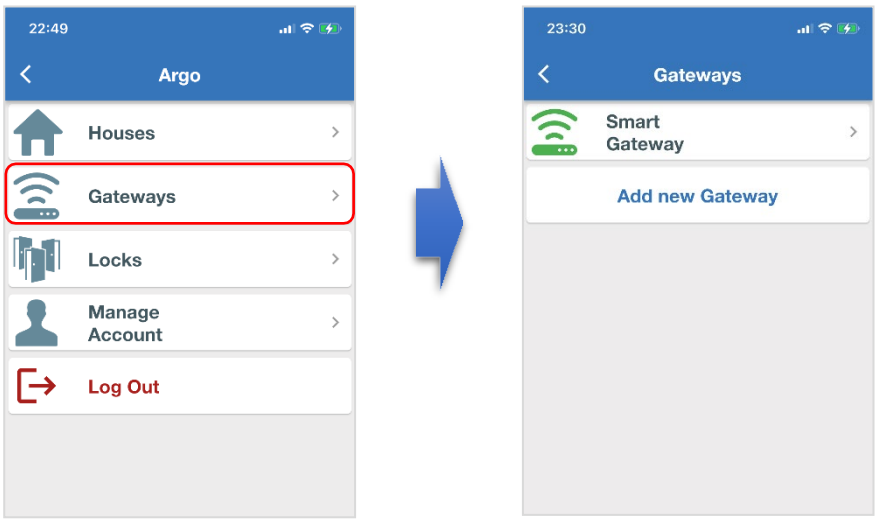
2. Löschen Sie alle **Schlösser** nacheinander, geben Sie dafür das Gerätepasswort ein oder verwenden Sie die biometrische Identifizierung Ihres Smartphones.



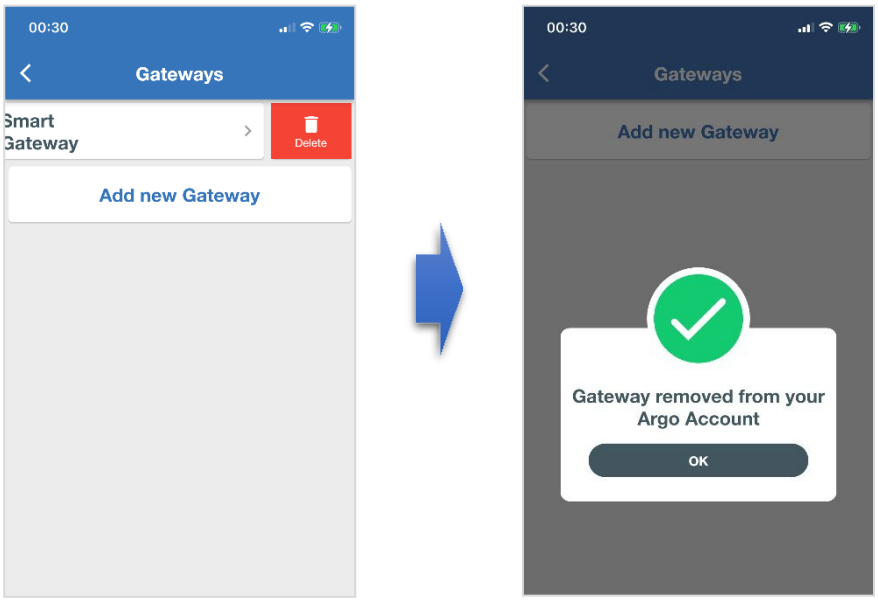
Wenn ein *Schloss* vom *Konto* des *Hauptbedieners* entfernt wird, wird es auch automatisch von allen *Gast-Konten* gelöscht, sofern diese bestehen.

Dasselbe passiert, wenn der *Hauptbediener* das *Gast-Konto* vom Schloss löscht.

3. Gehen Sie zurück ins Hauptmenü und tippen Sie auf **Gateways**.

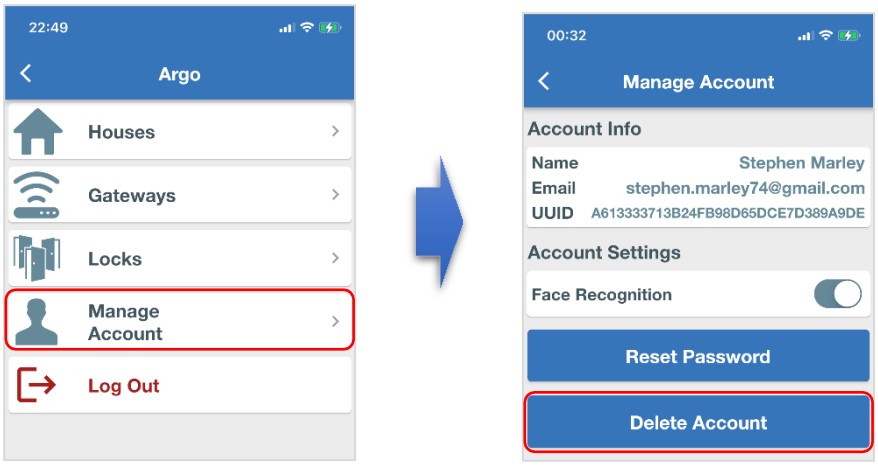


4. Löschen Sie das **Gateway**, indem Sie von rechts nach links wischen, und bestätigen Sie den Hinweis.

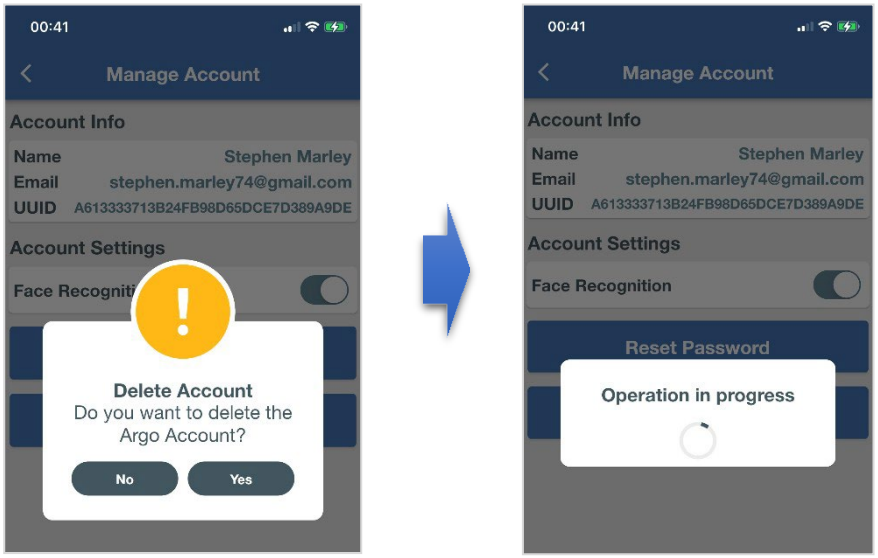


Ein mit einem *Schloss* verbundenes **Gateway** kann nicht gelöscht werden und in der App erscheint eine Fehlermeldung. Stellen Sie sicher, dass Sie alle *Schlösser* entfernt haben, bevor Sie ein *Gateway* löschen (weitere Informationen zu Fehlern finden Sie unter *Problembehebung*).

5. Gehen Sie zurück ins Hauptmenü und tippen Sie auf **Konto verwalten**, dann auf **Konto löschen**.



6. Bestätigen Sie den Hinweis mit **Ja** und warten Sie, bis das *Konto* gelöscht wurde.



Alle **Häuser** werden bei der Kontolöschung automatisch entfernt.

Wenn Sie versuchen, sich bei einem gelöschten *Konto* anzumelden, erscheint folgende Meldung: *Ungültiger Nutzername oder Passwort*. Diese Meldung erscheint aus Sicherheitsgründen, damit nicht erkennbar ist, ob es sich um bestehende Konten handelt, wenn man zufällige E-Mailadressen eingibt.

Fragen & Antworten

Im Folgenden finden Sie einige häufig gestellte Fragen und die entsprechenden Antworten:

1. Ist *das Argo-Konto* sicher? Was passiert, sollte ein Hacker irgendwie auf mein *Konto* zugreifen können? Kann der Hacker die Tür aus der Ferne öffnen oder einen anderen Vorgang ausführen?

   Antwort: Selbst wenn jemand Zugriff auf Ihr *Argo-Konto* hat, kann er keine Vorgänge beim *Schloss* ausführen, da dafür das *Gerätepasswort* erforderlich ist. Und dieses Passwort wird am sichersten Ort gespeichert: im Schloss. Das Konto dient lediglich als Tunnel.

2. Ist das *Gateway* sicher? Was passiert, sollte ein Hacker irgendwie mein *Gateway* erreichen und sich damit verbinden? Kann der Hacker die Tür aus der Ferne öffnen oder einen anderen Vorgang ausführen?

   Antwort: Sollte sich jemand mit dem *Gateway* verbinden, kann er keinen Vorgang ausführen, da das *Gateway* lediglich als Tunnel dient. Im *Gateway* werden keinerlei Informationen gespeichert. Das *Gateway* dient nur als Tunnel, um das *Schloss* zu erreichen und mit diesem zu kommunizieren. Alle relevanten Informationen werden am sichersten Ort gespeichert, im Schloss, und sind mit einem Passwort geschützt.

3. Wie viele Schlösser können mit einem *Smart Gateway* verbunden werden?

   Antwort: Es gibt keine Beschränkung. Das *Smart Gateway* funktioniert wie ein Smartphone mit Argo. Daher können alle Schlösser innerhalb der *Bluetooth*-Reichweite mit dem *Gateway* verbunden werden.

4. Was passiert, wenn ich verschiedene *ISEO Smart Geräte* habe, diese aber mehr als 10 Meter entfernt sind? Kann man mehr als ein *Gateway* mit demselben *Konto* verknüpfen, damit alle Smart Geräte eingebunden werden können?

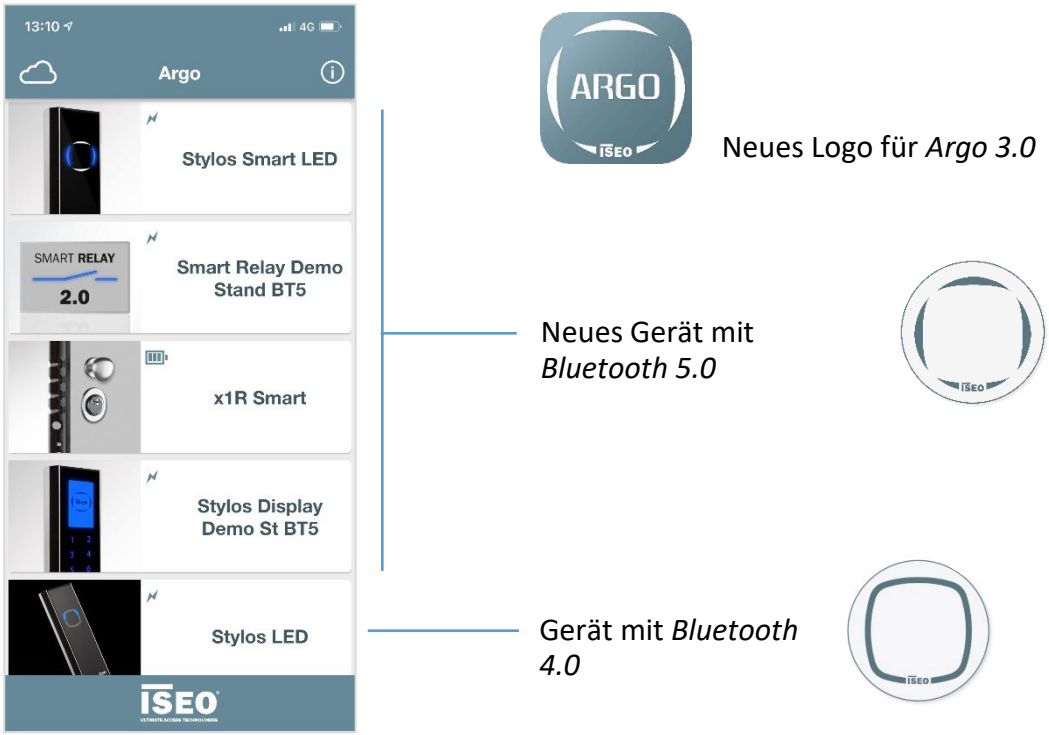
   Antwort: Ja, Sie können mehrere *Gateways* mit Ihrem *Argo-Konto* verknüpfen, um verschiedene Schlösser zu erreichen.

5. Kann ich *ISEO Smart Geräte* mit *Bluetooth 4.0* mit einem *Gateway* verbinden? Funktioniert das *Gateway* auch mit *Bluetooth 4.0*?

   Antwort: Nein, das *Smart Gateway* ist ausschließlich mit *ISEO Smart Geräten* mit *Bluetooth 5.0* kompatibel und funktioniert nur mit *Bluetooth 5.0*. Diese Technologie ermöglicht mehrere Verbindungen gleichzeitig, eine Voraussetzung für die *Argo Fernsteuerung*.

6. Wie erkenne ich *ISEO Smart Geräte* mit *Bluetooth 5.0*?

   Antwort: Sie erkennen Sie anhand des neuen Logos, das auf *Bluetooth 5.0* hinweist. Das neue Logo befindet sich auf allen *ISEO Smart Geräten* mit *BLE 5*. Sie können die *ISEO Smart Geräte* mit *Bluetooth 5.0* auch in der Argo-App erkennen: Die neuen Geräte erscheinen auf der *Startseite* mit einem neuen Symbol und dem neuen Logo.



7. Kann ich *ISEO Smart Geräte* mit *Bluetooth 4.0* auf *Bluetooth 5.0* aufrüsten, um sie mittels *Smart Gateway* auch aus der Ferne zu verwalten?

   Antwort: Nein die *ISEO Smart Geräte* mit *Bluetooth 4.0*, mit Ausnahme von *x1R Smart*, können nicht auf *Bluetooth 5.0* aufgerüstet werden. Das komplette Gerät muss getauscht werden, um es aus der Ferne zu steuern. *x1R Smart* bildet hier eine Ausnahme, weil das Schloss aus zwei Geräten besteht: dem mechanischen Schloss auf der Türinnenseite und dem Identmedienlesegerät, das über *Bluetooth* verfügt, das sich in der Regel außen an der Tür befindet. Um ein *x1R Smart* auf *Bluetooth 5.0* aufzurüsten, müssen Sie:

   - Das Lesegerät mit einem Gerät ersetzen, das über *Bluetooth 5.0* verfügt.
   - Die *x1R Smart* Firmware mit der App *ISEO App Tool* aktualisieren. Einführungsvideo verfügbar unter: https://www.youtube.com/watch?v=WOgmzzra0f8

   Dieser Vorgang sollte nur von kompetentem und geschultem Personal vorgenommen werden.

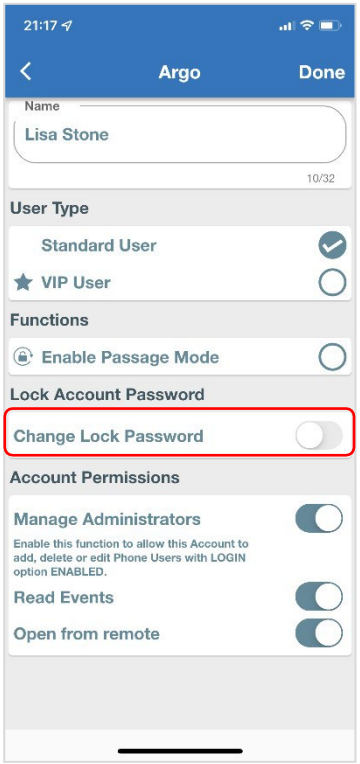
8. Mit *Argo Local* können bis zu 300 *Nutzer* im Schloss gespeichert werden. Was passiert, wenn ich ein *Gateway* und das *Schloss* zum *Argo-Konto* hinzufüge? Beeinflusst das die Anzahl der *Nutzer*, die im Schloss gespeichert werden können?

   Antwort: Ja, bei der Einrichtung werden das *Gateway* und das *Hauptbediener-Konto* im Schlossspeicher registriert. Diese werden als zwei verschiedene Identmedien behandelt, dadurch ändert sich die Nutzerzahl.
   Beispiel: Statt 300 möglicher *Nutzer* sind noch 298 verfügbar. Das liegt am Funktionsprinzip von Argo, nämlich *Data on Device*. Gleichzeitig ist das die Stärke von Argo hinsichtlich Sicherheit: Das *Gateway* dient lediglich als Tunnel; alle Daten werden am sichersten Ort gespeichert: im Schloss.

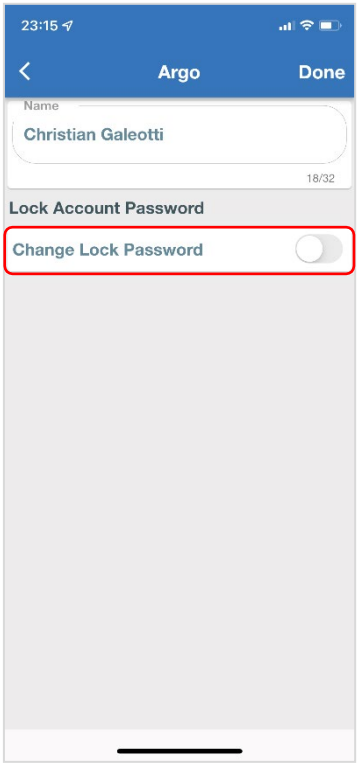
9. Wie kann ich das *Gerätepasswort* ändern? Ich kann die Option nicht finden.

   Antwort: Das *Gerätepasswort* wird am sichersten Ort gespeichert: im Schloss. Es ist ganz klar einem Schloss zugeordnet und kann sich von Schloss zu Schloss unterscheiden, abhängig vom Bediener. Es unterscheidet sich auch von *Konto* zu *Konto*, wenn verschiedene *Remote-Bediener* dasselbe Schloss verwalten (*Gast-Konten*). Daher müssen Sie sich bei dem speziellen Schloss anmelden, dessen Passwort Sie ändern wollen, auf die Einstellungen des *Bediener-Kontos* zugreifen und das *Gerätepasswort* ändern.

Gerätepasswort - Inhaber
Einstellungen Bediener-Konto



Gerätepasswort - Gast
Einstellungen Bediener-Konto



10. Wie kann ich ein *Schloss* von einem *Gateway* entfernen?

    Antwort: Gehen Sie im *Argo-Konto* in das Menü *Schlösser* und löschen Sie dort das *Schloss* vom *Konto* (wischen Sie dafür einfach von rechts nach links). Bitte beachten Sie: Wenn Sie das Schloss mit *Argo Local auf Werkseinstellungen zurücksetzen*, wird es auch automatisch vom *Konto* entfernt.

11. Funktioniert das *Gateway PoE* auch mit WLAN?

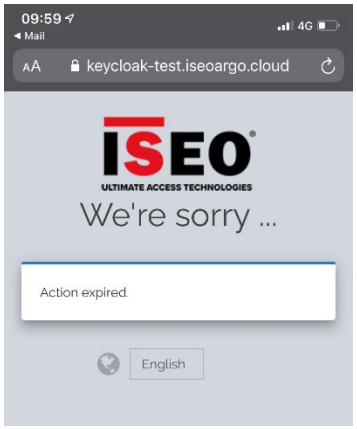
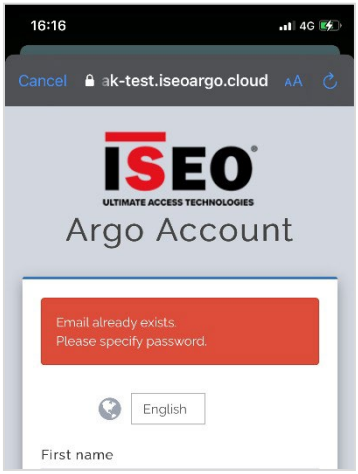
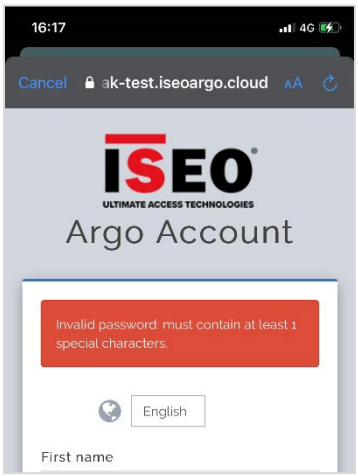
    Antwort: Nein, das *Gateway PoE* verfügt nicht über WLAN; es kann mit dem Router nur per LAN- oder Ethernet-Kabel verbunden werden. Es kann über den Router und PoE oder durch ein externes Netzteil mit Strom versorgt werden, falls der Router über keinen PoE-Port verfügt.

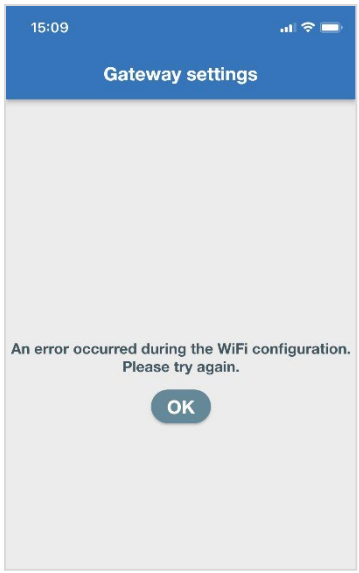
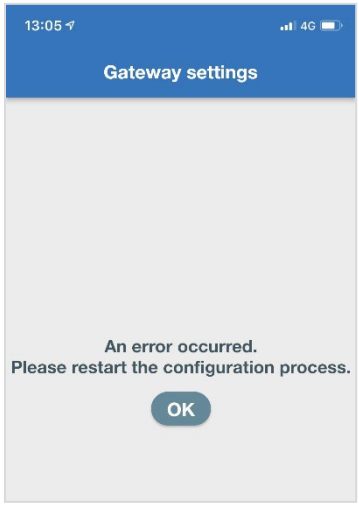
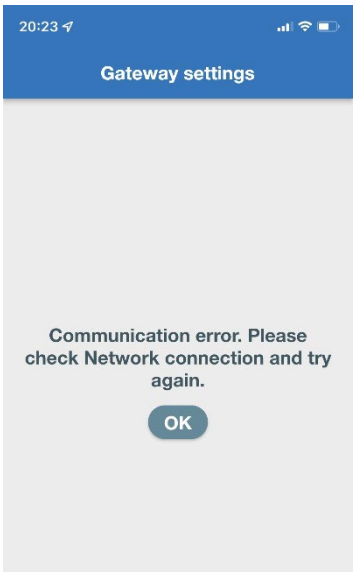
12. Ich habe das *Gerätepasswort* vergessen. Was mache ich jetzt?

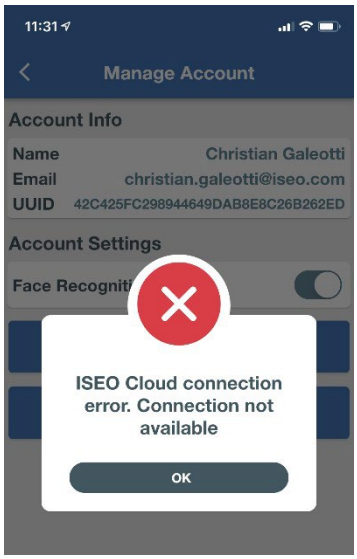
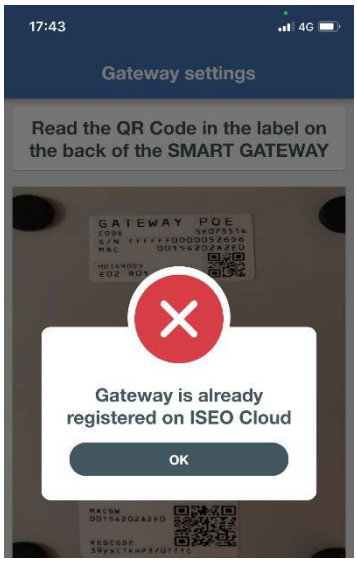
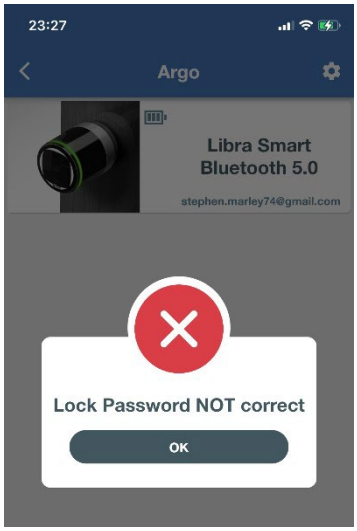
    Antwort: Aus Sicherheitsgründen gibt es keine Möglichkeit, das *Gerätepasswort* zurückzusetzen. Die einzige Lösung für den *Bediener* besteht darin, das *Schloss* vom *Konto* zu löschen (s. *Erweiterte Funktionen*, *Schlösser*, *Schloss löschen*) und es dann mit der *Master-Karte* hinzuzufügen (s. *Erweiterte Funktionen*, *Schlösser*, *Schloss hinzufügen*).

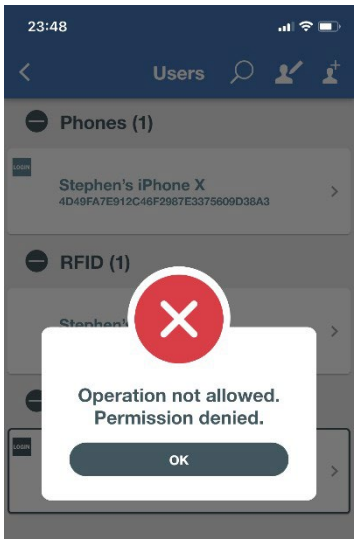
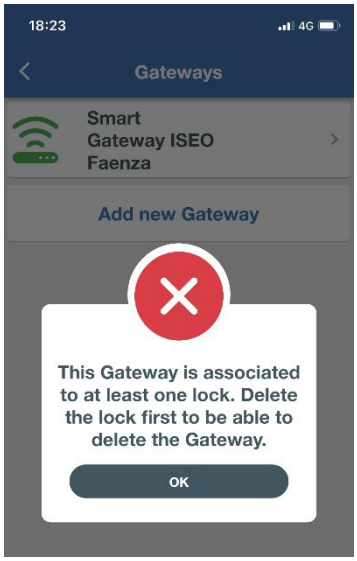
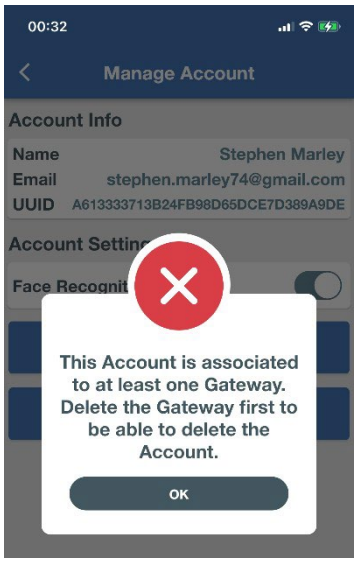
Problembehebung

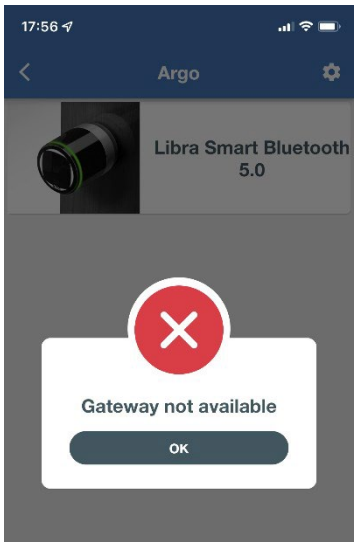
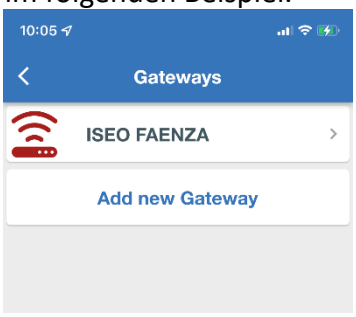
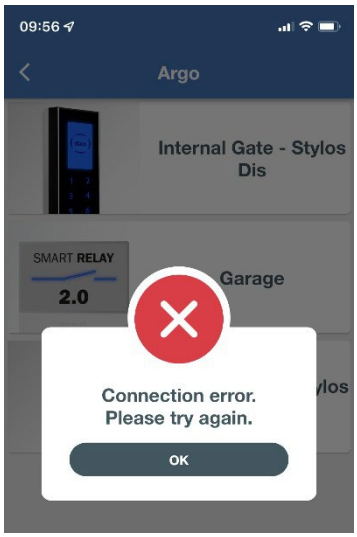
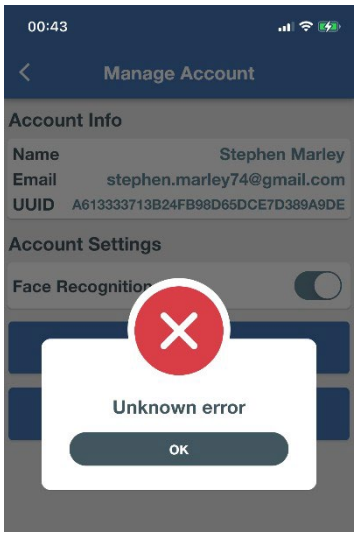
Unten finden Sie eine Übersicht über die häufigsten Fehlermeldungen und deren Ursachen.

Fehler	Bedeutung	Maßnahmen
	Ein Schritt bei der Registrierung des Kontos hat zu lange gedauert. Aus Sicherheitsgründen erhalten Sie nach Überschreitung einer bestimmten Zeit diese Fehlermeldung.	Bitte wiederholen Sie den Vorgang und gehen Sie schneller vor.
	Sie haben eine bereits registrierte E-Mailadresse bei der Registrierung des Argo-Konto verwendet.	Wählen Sie eine andere E-Mailadresse, um ein neues Konto anzulegen oder verwenden Sie das bestehende Konto.
	Das eingegebene Passwort ist nicht komplex genug.	Bitte geben Sie ein Passwort mit mindestens 8 Zeichen ein, darunter ein Großbuchstabe, eine Zahl und ein Sonderzeichen.

Fehler	Bedeutung	Maßnahmen
	Dieser Fehler kann bei der Einrichtung des Gateways bei Schritt 1 auftreten, wenn das Gateway versucht, die Verbindung mit dem WLAN-Router herzustellen. Normalerweise ist das eingegebene Netzwerkpasswort falsch.	Bestätigen Sie mit OK und beginnen Sie von vorn. Achten Sie darauf, das korrekte Netzwerkpasswort einzugeben. Verwenden Sie die Funktion Passwort anzeigen, um das Passwort zu prüfen. Sollte das Problem weiterhin bestehen, prüfen Sie, ob Ihr WLAN-Router von anderen Geräten erreicht werden kann (PC, Smartphone, Tablet). Sollten Sie das Problem nicht lösen können, wenden Sie sich an ISEO (s. *Technischer Support*).
	Dieser Fehler kann bei der Einrichtung des Gateways bei Schritt 1 auftreten, wenn das Gateway versucht, die Verbindung mit dem WLAN-Router herzustellen. Das Passwort ist korrekt, aber der Router lässt die Verbindung des Gateways nicht zu.	Bestätigen Sie mit OK und beginnen Sie von vorn. Sollte das Problem weiterhin bestehen, prüfen Sie, ob Ihr WLAN-Router von anderen Geräten erreicht werden kann (PC, Smartphone, Tablet). Sollten Sie das Problem nicht lösen können, wenden Sie sich an ISEO (s. *Technischer Support*).
	Dieser Fehler kann bei der Einrichtung des Gateways bei Schritt 2 auftreten, wenn das Gateway versucht, die Verbindung mit der ISEO Cloud und dem Argo-Konto herzustellen. Die Kommunikation zwischen Gateway und Cloud ist fehlgeschlagen. Dieses Problem kann verschiedene Ursachen haben: 1. Langsame Internetverbindung 2. Firewall, die die Kommunikation verhindert 3. Fehler beim Datenaustausch	Bestätigen Sie mit OK und beginnen Sie von vorn. Sollte das Problem weiterhin bestehen, prüfen Sie Ihre Internetverbindung: Prüfen Sie, ob andere Geräte wie PC oder Smartphone über eine Internetverbindung verfügen. Testen Sie die Internetgeschwindigkeit, um die Leistung zu prüfen. Sollten Sie das Problem nicht lösen können, wenden Sie sich an ISEO (s. *Technischer Support*).

Fehler	Bedeutung	Maßnahmen
	1. Ihr Konto wurde gelöscht. 2. Die ISEO Cloud ist nicht erreichbar.	1. Wenn Sie Ihr Argo-Konto gelöscht haben, ist dieser Hinweis korrekt. 2. Versuchen Sie es später erneut und prüfen Sie die mobile oder WLAN-Internetverbindung. Sollten Sie das Problem nicht lösen können, wenden Sie sich an ISEO (s. *Technischer Support*).
	Dieser Fehler kann zu Beginn der Einrichtung des Gateways auftreten, wenn der QR-Code gelesen wird. Das System warnt, dass dieses Gateway bereits in der ISEO Cloud registriert ist.	1. Verwenden Sie ein anderes Gateway, da dieses bereits einem Argo-Konto zugewiesen wurde. 2. Löschen Sie das Gateway vom aktuellen Argo-Konto, dann können Sie es einem anderen Konto zuordnen. **Hinweis**: Um das Gateway mit einem anderen Argo-Konto zu verknüpfen, müssen Sie es zurücksetzen. Befolgen Sie dafür die Anweisungen im Einrichtungsassistenten.
	1. Das Gerätepasswort ist falsch. 2. Das Gerätepasswort wurde mit der biometrischen Identifizierung des Smartphones verknüpft, aber später geändert. Das Smartphone greift auf das zuerst mit dem Schloss verknüpfte Passwort zurück, das geändert wurde: Daher ist das Passwort nicht mehr gültig.	1. Geben Sie das aktuell gültige Gerätepasswort ein. 2. Wiederholen Sie den Vorgang: Die App fordert Sie auf, das Passwort einzugeben, wenn die biometrische Identifizierung zwei Mal fehlgeschlagen ist.

Fehler	Bedeutung	Maßnahmen
	In diesem Beispiel wurde mit einem *Gast-Konto* versucht, einen Smartphone-Nutzer mit Login (lokaler Bediener) zu löschen, obwohl es nicht über die Berechtigung zum Verwalten von Bedienern verfügt, die der Hauptbediener zuweisen kann. Der gleiche Fehler tritt auf, wenn mit dem Gast-Konto ein Vorgang vorgenommen werden soll, für den der Hauptbediener keine Berechtigungen erteilt hat (z. B. Tür öffnen, Ereignisse anzeigen).	Sie können keine Vorgänge ausführen, für die Sie der Hauptbediener nicht berechtigt hat. Wenden Sie sich für diese Rechte an den Hauptbediener.
	In diesem Beispiel versucht der Hauptbediener, das Gateway zu löschen, aber im System sind noch Schlösser hinterlegt.	Löschen Sie zunächst nacheinander alle Schlösser, dann können Sie das Gateway löschen.
	In diesem Beispiel versucht der Hauptbediener, das Argo-Konto zu löschen, aber im System ist noch ein Smart Gateway hinterlegt.	Löschen Sie zunächst das Smart Gateway (zuvor müssen alle Schlösser gelöscht werden), dann können Sie das Argo-Konto löschen.

Fehler	Bedeutung	Maßnahmen
	Das Smart Gateway ist nicht erreichbar. Es kann ausgeschaltet sein oder nicht korrekt arbeiten. Das Symbol im Gateway-Menü ist rot wie im folgenden Beispiel. 	Prüfen Sie Folgendes: • Das Gateway ist eingeschaltet und die Netzwerk-LED leuchtet. • Das Gateway ist korrekt eingerichtet und kann mit dem Router kommunizieren. • Der Router funktioniert korrekt. Falls alles davon zutrifft, starten Sie das Gateway neu und prüfen Sie, ob es funktioniert. Sollten Sie das Problem nicht lösen können, wenden Sie sich an ISEO (s. *Technischer Support*).
	Die Verbindung zum Schloss konnte aus der Ferne nicht hergestellt werden. Das Gateway ist verfügbar, das Schloss nicht.	• Prüfen Sie vor Ort, ob das Schloss korrekt funktioniert. • Ersetzen Sie die Schlossbatterie, falls sie leer ist. • Prüfen Sie, ob das Schloss innerhalb des Bluetooth-Reichweite des Gateways liegt.
	Es ist ein unbekannter Fehler aufgetreten. Dieser Fehler wird im System noch nicht abgebildet. Neben dem Text erscheint ggf. ein Code in eckigen Klammern (Softwarefehlercode).	Versuchen Sie es erneut und prüfen Sie, ob der Fehler wieder auftritt. Sollte das Problem weiterhin bestehen, wenden Sie sich an ISEO (s. *Technischer Support*) und geben Sie den Fehlercode an, sofern dieser angezeigt wird.

Alle Funktionen der Argo-App

Um alle Funktionen von *Argo Local* zu entdecken, nutzen Sie das *Argo 2.7 Nutzerhandbuch* verfügbar unter *iseo.com*.

Technischer Support

Bitte kontaktieren Sie uns für technischen Support: Die Kontaktdaten für Ihr Land finden Sie unter:

https://www.iseo.com/

Wenn Sie *ISEO* kontaktieren, halten Sie bitte folgende Informationen bereit:

- Softwareversion der Argo-
- Smartphonemodell und Softwareversion.
- Gerät für die Zutrittskontrolle, das den Fehler verursacht, Produktcode und Softwareversion.
- Eine genaue Beschreibung des Problems.

Iseo Serrature s.p.a.
Via San Girolamo, 13
25055 Pisogne BS, Italy
T. +39 0364 8821
Fax +39 0364 882263
iseo@iseo.com

iseo.com