AIO-KEY

StandAlone

INSTALLER MANUAL

IM_ENG_REV0125_AIO-KEY STANDALONE

1.INDEX

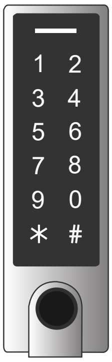
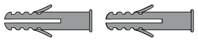
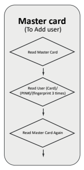
2.INTRODUCTION

Manual for the installation of the AIO-KEY reader in standalone operation. The possible identifications are: proximity, PIN, fingerprint and smartphone via TUYA APP.

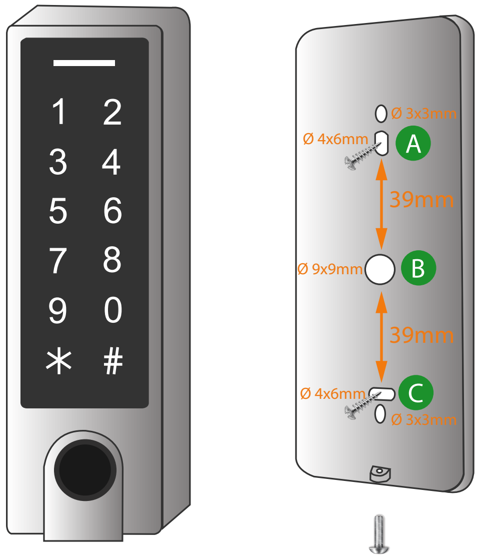
3.SPECIFICATIONS

Material	Zinc alloy and black ABS plastic
Protection degree	IP-66
Input voltage	12/18Vdc
Current	Standby: ≤ 60mA / Active: ≤ 150mA
Capacity	Reader registration: 1000 users (users with fingerprint: 100, users with card or PIN: 888) Registration in APP TUYA: 500 users. Event registration in APP TUYA: unlimited.
Comunication	WiFi
PIN	12 keys (PIN 4-6 digits)
Reading frequency	Mifare 13.56MHz and 125KHz EM
Reading range	2-6cm
Relay	NO, NC, common (2A max.)
Transmission format	Wiegand 26
Connectivity	WiFi
Support	Tuya APP
Dimension (Height x Width x Depth):	43,5(W) x 148(H) x 22(D)mm

4.PRODUCT CONTENT

 AIO-KEY reader		Diode.
		Fixing blocks.
		Screws.
		Allen key for fastening screws.
	 	MASTER programming card.

5.INSTALLATION



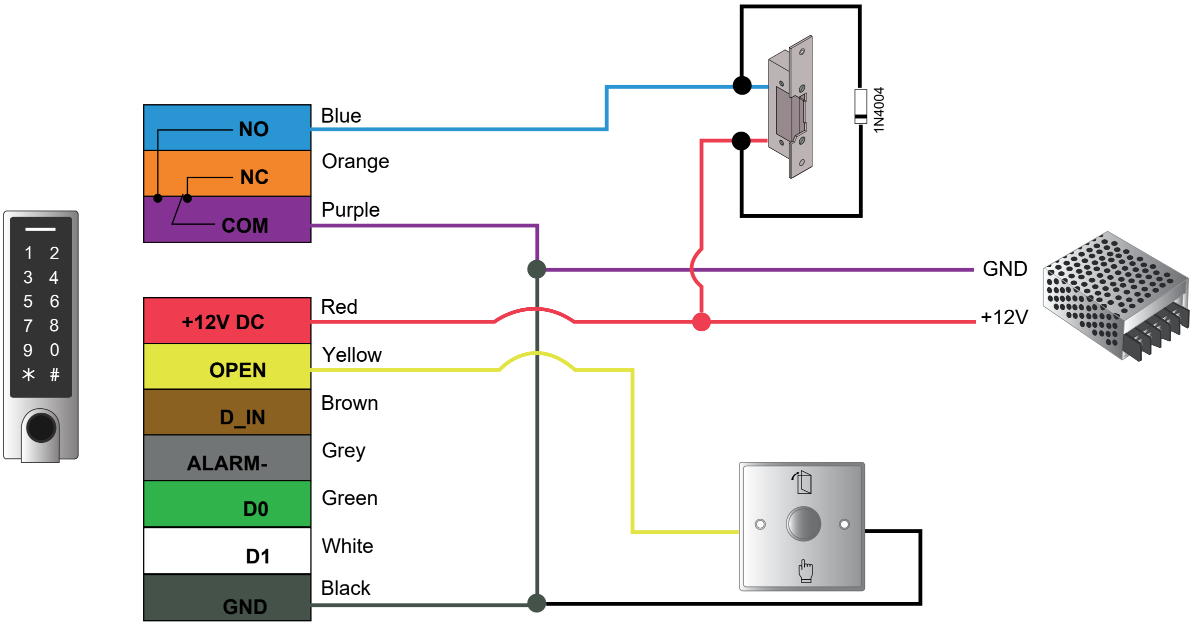
1. Unfasten the screw at the bottom and remove the reader from the base.
2. Drill a pair of holes in the wall (A,C) for the fixing blocks and another for the cables.
3. Place the fixing blocks in the holes (A,C).
4. Pass the cable through the hole (B).
5. Fasten the base to the wall with the screws provided.
6. Fit the reader into the base and secure both parts with the screw at the bottom.

IMPORTANT: The reader is equipped with an anti-tampering LDR sensor on the rear side: .
It is light-sensitive, so if light shines on the sensor after placing the reader, the tamper alarm will be triggered.

6.CONNECTION

WIRE COLOUR	FUNCTION	DESCRIPTION
Red	12Vcc	Input 12-18VDC current
Black	GND	GND
Blue	NO	Normally open relay output
Purple	Common	Common contact for relay output
Orange	NC	Normally closed relay output
Yellow	Opening	Exit pushbutton
Green	D0	Wiegand Data 0 output
White	D1	Wiegand Data 1 output
Grey	Alarm output	Negative alarm contact
Brown	Input contact	Door contact input (NC)

7.STANDALONE CONNECTION DIAGRAM

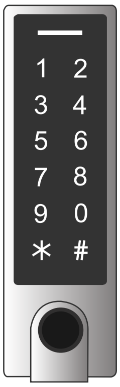


IMPORTANT: do not forget to connect the supplied diode (1N4004) in parallel to the lock release to protect the equipment.

USERS MANAGEMENT

8.USERS MANAGEMENT

User registrations can be made on the reader or on the smartphone through the Tuya APP:



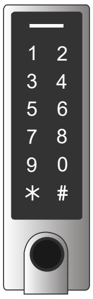
Through the reader

Through mobile phone via the APP Tuya

IMPORTANT: before proceeding with user registration, please note that users can't be transferred from the reader to the Tuya APP or vice versa.

8.1. USER MANAGEMENT IN READER

The management of users in the reader, as you illustrate below, can be carried out in a basic (8.1.1.Basic user management in reader) or advanced (8.1.2.Advanced user management in reader) way.



Registration in reader

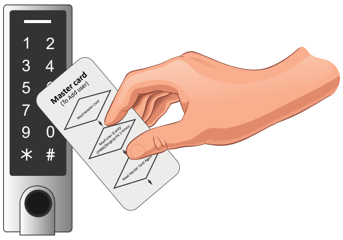
In case to choose the last option (APP registration), continue with the manual in section"8.2. User management in APP Tuya".

8.1.1.BASIC USER MANAGEMENT IN READER

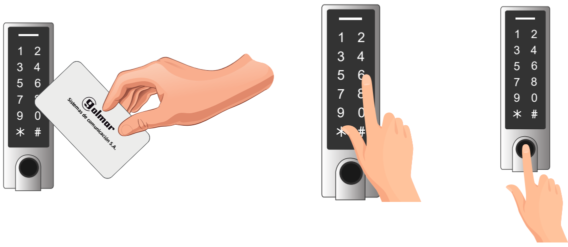
Basic programming (user registration/deletion) using the "Master Card" supplied with the product.

8.1.1.1.USER REGISTRATION

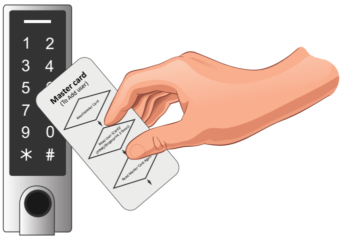
1) Approach the "Master Card" card to the reader.



2) Approach the card or enter the PIN or fingerprint to be registered.
*For PIN enter PIN of 4 to 6 digits plus #.
*For fingerprint, place fingerprint 3 times on the reader.

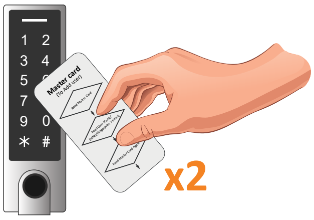


3) Approach the "Master Card" card to the reader.

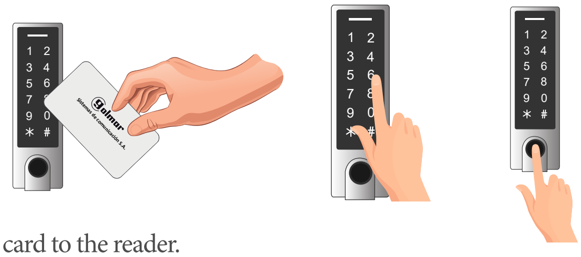


8.1.1.2.DELETE USER

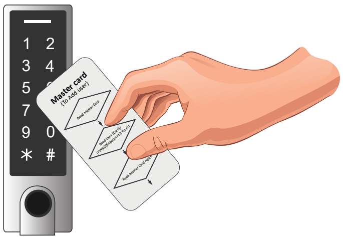
1) Approach the “Master Card” card to the reader 2 times at an interval of less than 5 seconds.



2) Approach the card or enter the PIN or fingerprint to be registered.
*For PIN enter PIN of 4 to 6 digits plus #.
*For fingerprint, place fingerprint 1 time on the reader.



3) Approach the “Master Card” card to the reader.



NOTE: in case of loss the MASTER CARD it is possible to create one by following the procedure described in section “10.6.Reset to factory settings”. It is possible to create a MASTER fingerprint, see section “10.7.Master fingerprint registration”.

8.1.2.ADVANCED USER MANAGEMENT IN READER

The following actions require to enter programming, it is possible to access programming as follows:

Enter administrator mode		
*	MASTER CODE (Por defecto: 123456)	#

The reader will indicate access to programming when the “green” LED lights up and then the LED will flash “red”. At the start of the programming sequence (function to be programmed) the led will be shown in “orange”.
To exit programming, press “*” and the reader will go to standby mode, status LED will be shown in “steady red”. In the case that no key presses are made, the reader automatically exits programming after 30 seconds.

Once in programming, carry out the desired programming sequence. The different system programming sequences are detailed below.

8.1.2.1.CHANGE MASTER CODE

It is advisable to modify the master code for this purpose:

Enter administrator mode		
*	MASTER CODE	#

0	NEW MASTER CODE (6 DIGITS)	#	NEW MASTER CODE (6 DIGITS)	#

Example: * 123456 # 0 987654 # 987654 #

8.1.2.2.CARD REGISTRATION (AUTO ID)

Card registration with automatic recording.

Enter administrator mode		
*	MASTER CODE	#

1	APPROACH CARD

Example: * 987654 # 1 APPROACH CARD

8.1.2.3.CARD REGISTRATION (SPECIFIC ID)

Maximum number of records is 888. User IDs from 100 to 987.

Enter administrator mode		
*	MASTER CODE	#

1	USER ID (100-987)	#	APPROACH CARD

Example: * 987654 # 1 105 # APPROACH CARD

IMPORTANT: do not enter user IDs with zeros before the ID value.

8.1.2.4.PIN REGISTRATION (AUTO ID)

PIN registration with automatic recording.

Enter administrator mode					
*	MASTER CODE	#	1	PIN	#

Example: * 987654 # 1 4543 #

8.1.2.5.PIN REGISTRATION (SPECIFIC ID)

Maximum number of records is 888. User IDs from 100 to 987.

Enter administrator mode							
*	MASTER CODE	#	1	USER ID (100-987)	#	PIN	#

Example: * 987654 # 1 110 # 5678 #

IMPORTANT: do not enter user IDs with zeros before the ID value.

8.1.2.6.FINGERPRINT REGISTRATION (AUTO ID)

Automatic fingerprint registration.

Enter administrator mode				
*	MASTER CODE	#	1	Place fingerprint 3 times

Example: * 987654 # 1 FINGERPRINT FINGERPRINT FINGERPRINT

8.1.2.7.FINGERPRINT REGISTRATION (SPECIFIC ID)

Maximum number of records is 99. User IDs from 0 to 98.

Enter administrator mode						
*	MASTER CODE	#	1	USER ID (0-98)	#	Place fingerprint 3 times

Example: * 987654 # 1 5 # FINGERPRINT FINGERPRINT FINGERPRINT

IMPORTANT: do not enter user IDs with zeros before the ID value.

8.1.2.8.DELETE PIN

PIN deletion by introducing the PIN to be deleted.

Enter administrator mode					
*	MASTER CODE	#	2	INTRODUCE PIN	#

Example: * 987654 # 2 4543 #

8.1.2.9.DELETE CARDS

Erasing cards by approaching the card to be deleted.

Enter administrator mode				
*	MASTER CODE	#	2	APPROACH CARD

Example: * 987654 # 2 APPROACH CARD

8.1.2.10.DELETE FINGERPRINTS

Erasing of fingerprints by placing the fingerprint to be deleted.

Enter administrator mode				
*	MASTER CODE	#	2	Place fingerprint

Example: * 987654 # 2 FINGERPRINT

8.1.2.11.DELETE USERS (SPECIFIC ID)

Enter the ID corresponding to the user to be deleted.

Enter administrator mode					
*	MASTER CODE	#	2	USER ID (0-987)	#

Example: * 987654 # 2 5 #

8.2. USER MANAGEMENT IN APP TUYA

This equipment has WiFi communication which allows the use of the APP Tuya.

NOTA: below is detailed information for the configuration of the TUYA APP. Please refer to the quick guide "QGI_ENG_REV0124_ CONFIG-APP-TUYA" for a more simplified version of this information.

8.2.1.TUYA APP INSTALLATION

Install the "TUYA" application on your smartphone.
It can be downloaded from Google Play or Apple Store depending on the operating system of the smartphone.

Play Store QR
(Android)

Apple Store QR
(IOS)

IMPORTANT:
- Golmar is not the developer of the Tuya APP, Tuya is a cloud platform that allows the management of IoT devices, Golmar offers the possibility to make use of the reader with Tuya technology.
- The APP is supported by smartphones with iOS (7.0 or higher) or Android (4.3 or higher) version.

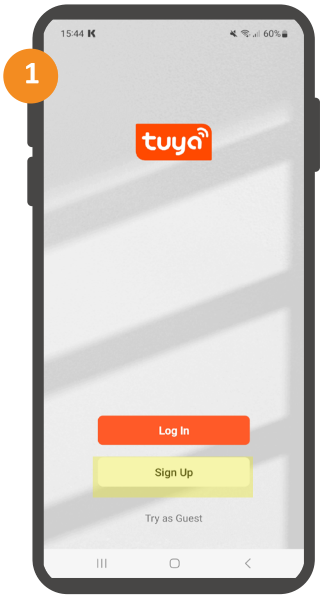
8.2.2.REGISTRATION AND LOGIN

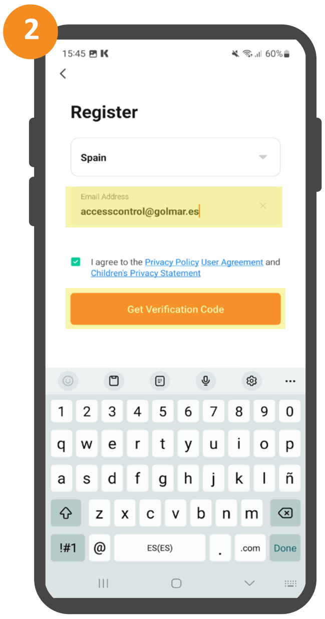
1 - Press the "Create new account" option on the initial screen.

2 - Enter the e-mail address of the "super administrator" of the installation. Then press "Get verification code".

3 - Enter the verification code that you will have received at the e-mail address provided.

4 - Set a password.



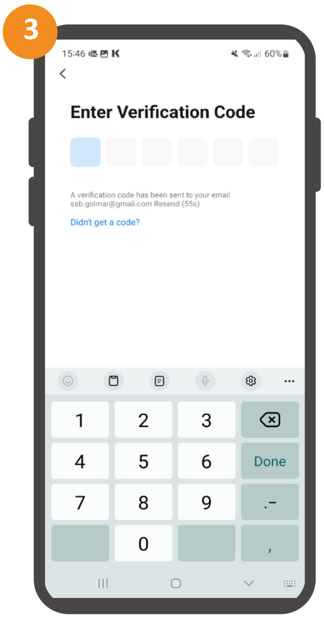


Register

Spain

Email Address: accesscontrol@golmar.es

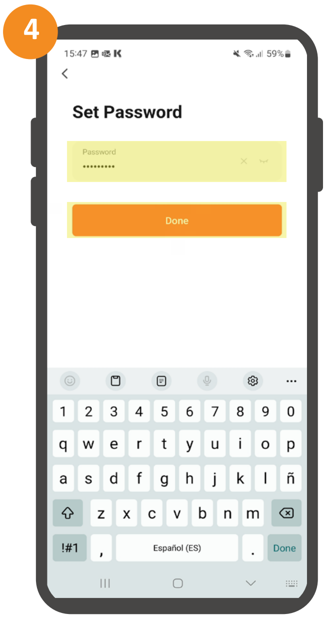
☑ I agree to the Privacy Policy User Agreement and Children's Privacy Statement



Enter Verification Code

A verification code has been sent to your email ssb.golmar@gmail.com Resend (55s)

Didn't get a code?



Set Password

Password: ••••••••

NOTE: after these steps probably a window will appear indicating "We need the following permissions to offer you better services", these permissions are not necessary to make use of the application, it is up to you to decline or accept them.

8.2.3.ADD READER

Once the above steps have been completed, the account will be created and with the session started, the APP wizard will suggest to add device. Proceed as follows:

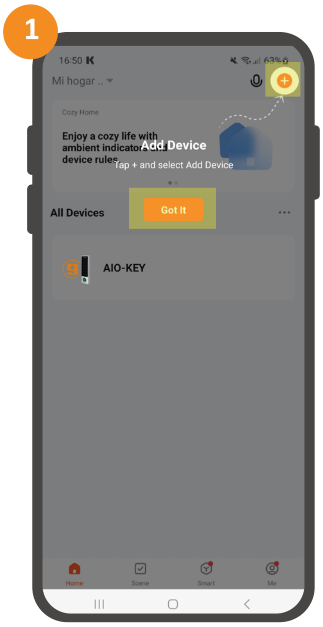
1 - Press the "got it" option and then the "+" or "add device" symbol.

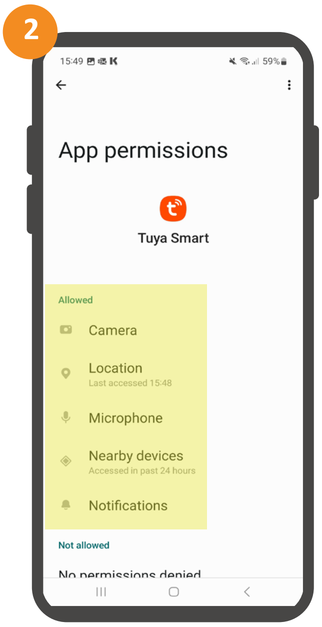
2 - Grant permission to the APP to make use of different smartphone features (camera, microphone, location, ...).

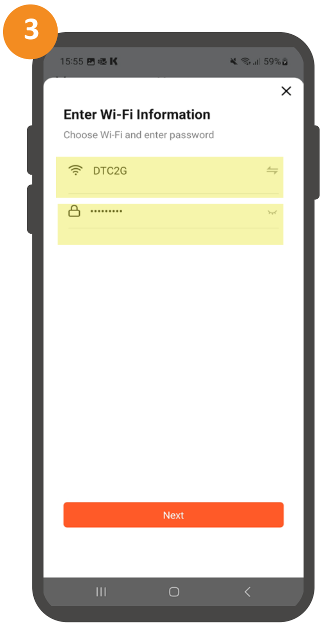
3 - Then bring the smartphone close to the reader (Bluetooth must be enabled as it is required during pairing).

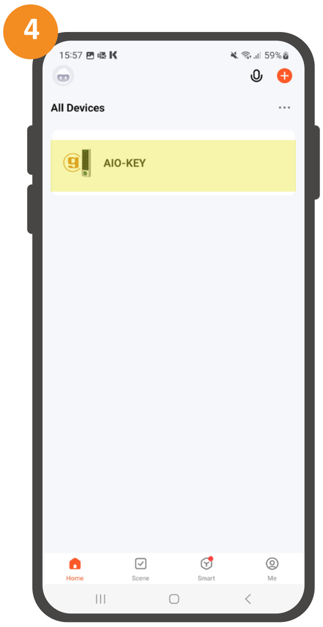
Then select and set the password of the WiFi connection to which the reader will connect to have internet access.

4 - Reader will be added.


1
16:50
Mi hogar
Cozy Home
Enjoy a cozy life with ambient indicator and device rules
Add Device
Tap + and select Add Device
Got It
All Devices
AIO-KEY
Home
Scene
Smart
Me







IMPORTANT

- The WiFi network to which the reader is connected must be 2.4GHz frequency.
- In case the reader is not detected automatically, perform the following sequence on the reader:

* master code # 9 master code #

The connectivity will be reset, perform this sequence only in case the device is not detected.

8.2.4.SHARE DEVICE

The user who initially adds the reader is by default "administrator", this user can manage the following:

FUNCTION	ADMINISTRATOR
DOOR OPENING	YES
ADMINISTRATOR AND USER MANAGEMENT	YES
USER MANAGEMENT	YES
DEFINE USERS AS ADMIN	YES
VIEW ALL LOGS	YES
SET RELAY TIMES	YES

This user can share the installation with other users who can be "administrators" or "users" (ordinary members). The users (ordinary members) will be able to manage the following:

FUNCTION	ADMINISTRATOR	USER (ordinary member)
DOOR OPENING	YES	YES
ADMINISTRATOR AND USER MANAGEMENT	YES	NO
USER MANAGEMENT	YES	NO
DEFINE USERS AS ADMIN	NO	NO
VIEW ALL LOGS	YES	NO
SET RELAY TIMES	YES	NO

1 - Press on the “Member manage” option located at the bottom of the main screen of the reader.

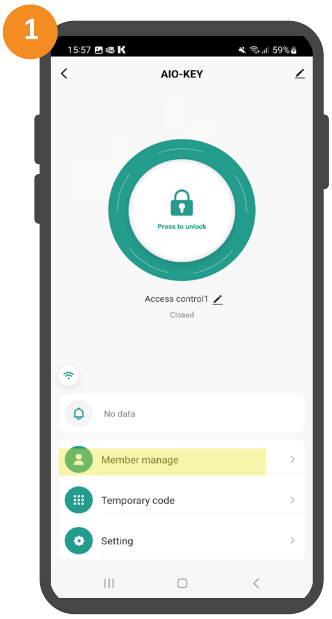
2 - Then press the “ordinary member” tab and then “+”.

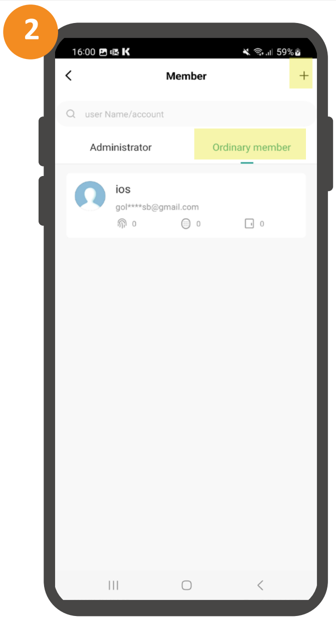
3 - Enter an identifiable name in the “user name” field and enter the email address of the TUYA user in “user account”, uncheck the “administrator” box, then click “next”.

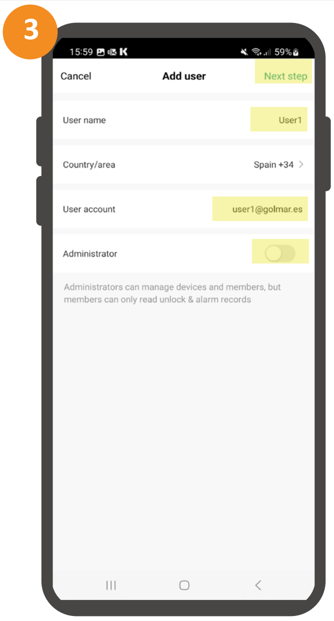
4 - The device will be shared. As soon as the user accepts the invitation the user will be able to start using the device.

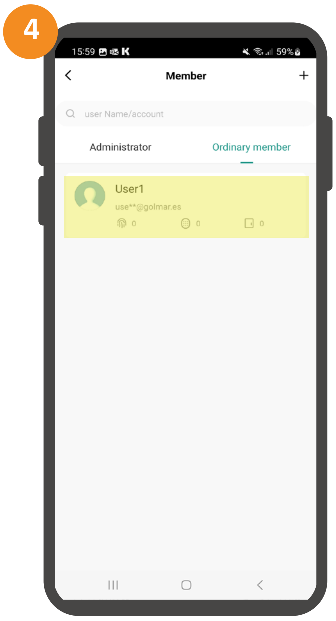
IMPORTANT

The user to whom the installation is shared must have an account (registered in the APP, section “8.2.2.Registration and login”).









NOTES

1 - The user will now be able to open with the smartphone, to grant other access methods see point number 8.2.8.

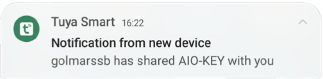
2 - In case more users are to be added, repeat the process.

3 - In case it is desired to delete a user, access the list (screen step 2), select the user and then press the option “delete member”.

4 - In case it is desired to add the user with “administrator” rights, do not uncheck the “administrator” checkbox in step 3.

8.2.5. USERS

1 - The user will receive a push notification that a new device has been shared:



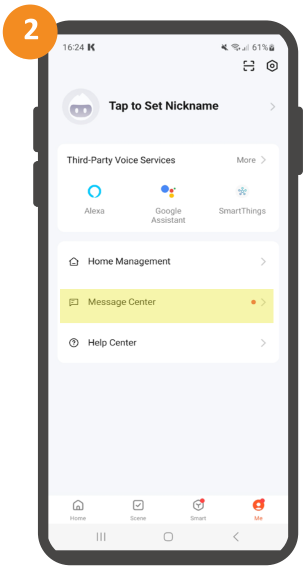
Tuya Smart 16:22

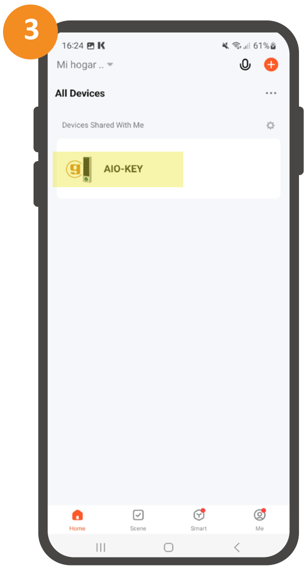
Notification from new device

golmarssb has shared AIO-KEY with you

2 - This can be checked from the “message center” (“me” tab of the main screen).

3 - The device will appear on the main screen as “ devices shared with me ”.

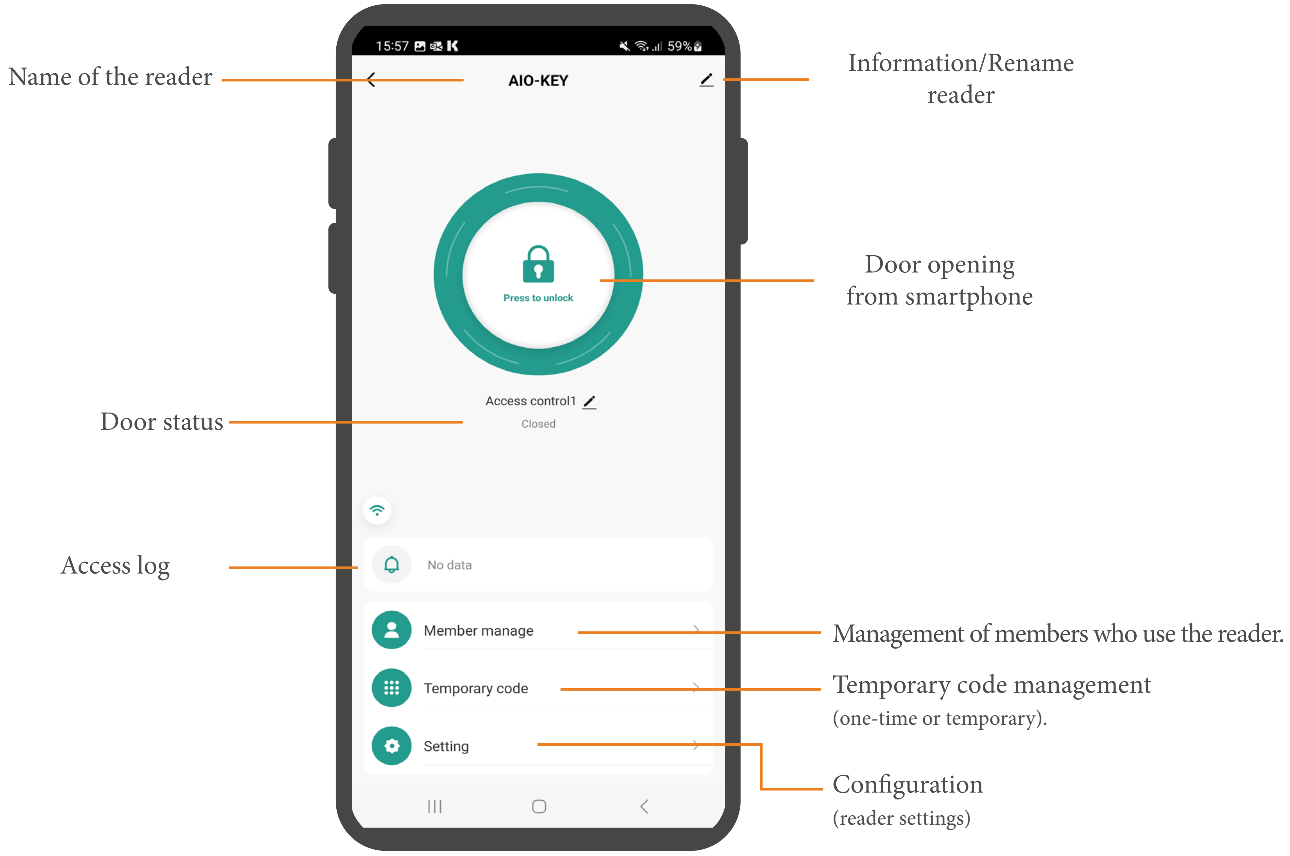




NOTE: push notifications may vary depending on the smartphone operating system.

8.2.6. MAIN READER SCREEN

The main screen of the reader is described below:


15:57
59%
AIO-KEY
Press to unlock
Access control1
Closed
No data
Member manage
Temporary code
Setting
Name of the reader
Information/Rename reader
Door opening from smartphone
Door status
Access log
Management of members who use the reader.
Temporary code management (one-time or temporary).
Configuration (reader settings)

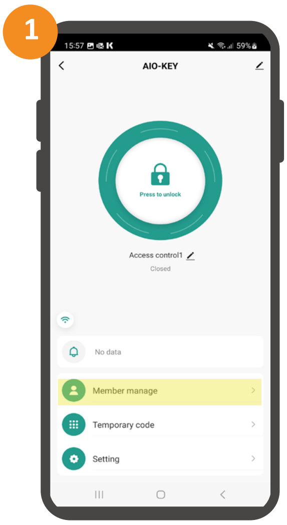
NOTE: ordinary members (users) will not be able to use the "Member Management", "Temporary Code" and "Configuration" functions.

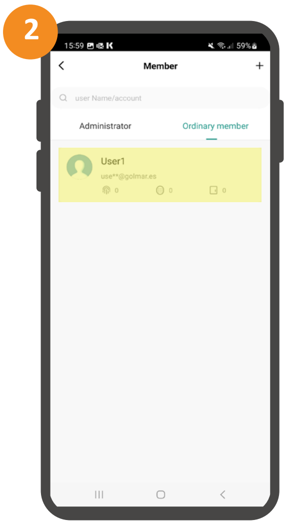
8.2.7. IDENTIFICATIONS

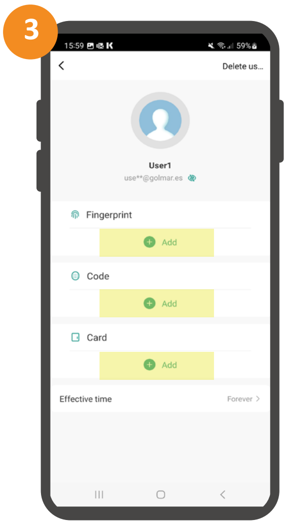
Before proceeding with the access credentials, please note that the user performing this procedure must be an "administrator".

8.2.8. REGISTRATION OF IDENTIFICATIONS

1 - In the main screen of the reader, click on "Member manage".
2 - Select the user to register the credential.
3 - Press "Add" on the type of identification to register (fingerprint, code or card).



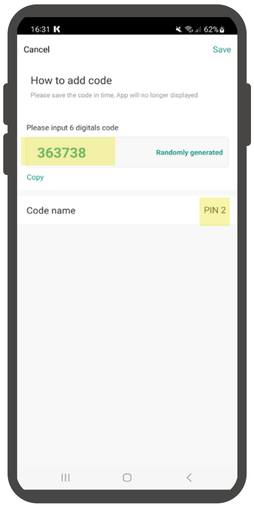




Below is a description of the registration process for the different types of identification:

8.2.9. PIN REGISTRATION

Set a 6-digit PIN and a name to identify the registered PIN, then press “save”.



How to add code

Please save the code in time, App will no longer displayed

Please input 6 digitals code

363738

Code name PIN 2

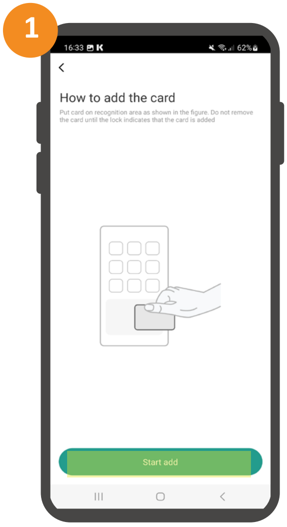
8.2.10. CARD REGISTRATION

1 - Press on the “Start add” option.

2 - Approach the card to be registered on the reader.

3 - Enter a name to identify the registered card.

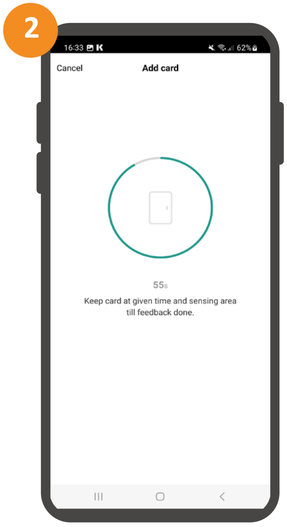
1



How to add the card

Put card on recognition area as shown in the figure. Do not remove the card until the lock indicates that the card is added

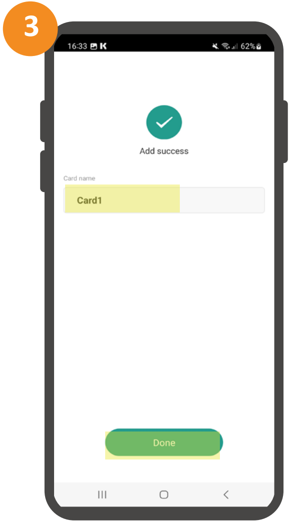
2



55s

Keep card at given time and sensing area till feedback done.

3



Add success

Card name

Card1

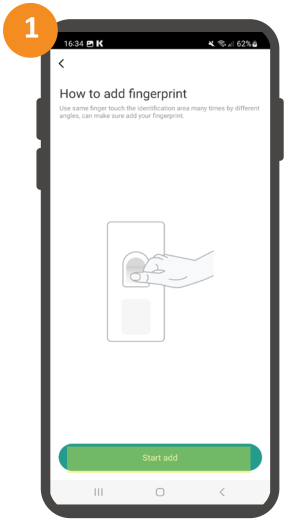
8.2.11. FINGERPRINT REGISTRATION

1 - Press on the “Start add” option.

2 - Place and remove the fingerprint to be enrolled in the reader 3 times.

3 - Enter a name to identify the enrolled fingerprint.

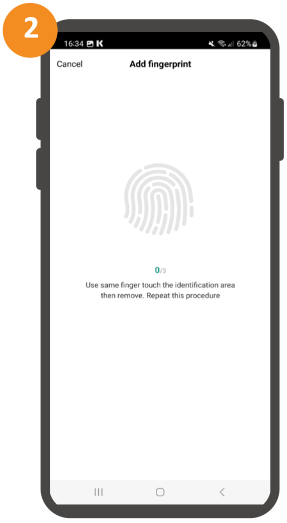
1



How to add fingerprint

Use same finger touch the identification area many times by different angles, can make sure add your fingerprint.

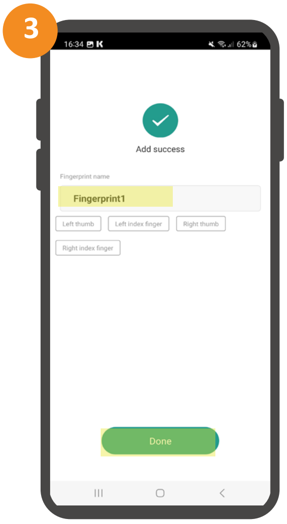
2



0/3

Use same finger touch the identification area then remove. Repeat this procedure

3



Add success

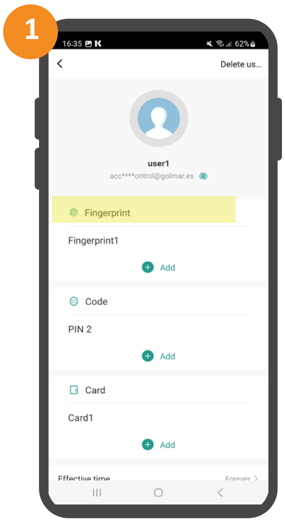
Fingerprint name

Fingerprint1

8.2.12. DELETE IDENTIFICATION

1 - Select the access credential of the user to be deleted.
2 - Press the “delete” option highlighted in red.
3 - Press “confirm” to complete the deletion process.

1



Delete us...

user1
acc****ontrol@golmar.es

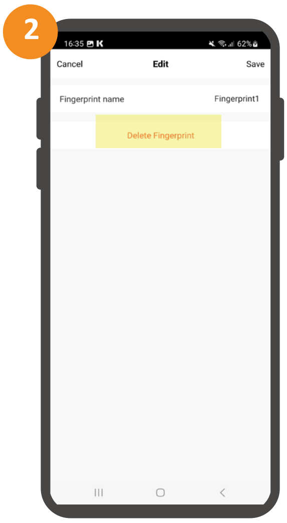
Fingerprint
Fingerprint1
Add

Code
PIN 2
Add

Card
Card1
Add

Effective time — Forever

2

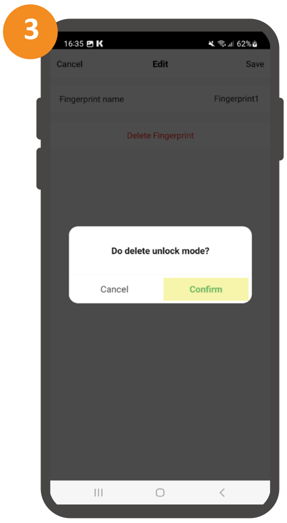


Cancel — Edit — Save

Fingerprint name — Fingerprint1

Delete Fingerprint

3



Do delete unlock mode?

Cancel — Confirm

9.TUYA APP ADDITIONAL FUNCTIONS

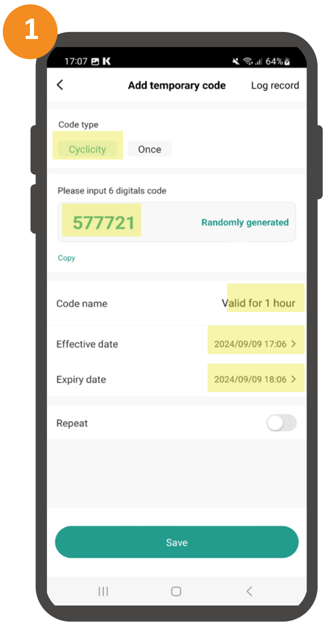
9.1. TEMPORAL CODE PER TIME PERIOD

Press on the “temporary code” option located at the bottom of the device management screen.
1 - Fill in the following temporary code generation fields:
- Select “Temporary” code type.
- Enter the 6-digit code that will allow the opening or press on the “Randomly generated” option.
- Name the temporary access you are about to generate.
- Define the validity period of the access.

2 - Confirmation of the generated temporary access will be displayed.

3 - Press share and select the method by which to send the activation code. In case it does not appear in the visible options, press on the “more” option.

1



Add temporary code — Log record

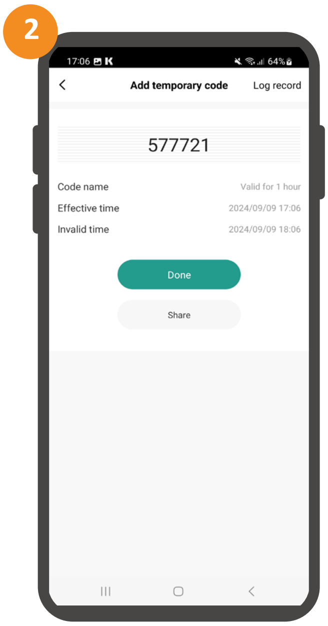
Code type: Cyclicity — Once

Please input 6 digitals code
577721 — Randomly generated
Copy

Code name — Valid for 1 hour
Effective date — 2024/09/09 17:06
Expiry date — 2024/09/09 18:06
Repeat

Save

2



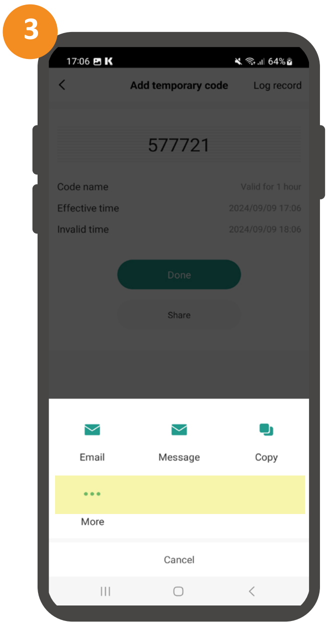
Add temporary code — Log record

577721

Code name — Valid for 1 hour
Effective time — 2024/09/09 17:06
Invalid time — 2024/09/09 18:06

Done
Share

3



Email — Message — Copy
More
Cancel

9.2. ONE-TIME USE TEMPORARY CODE

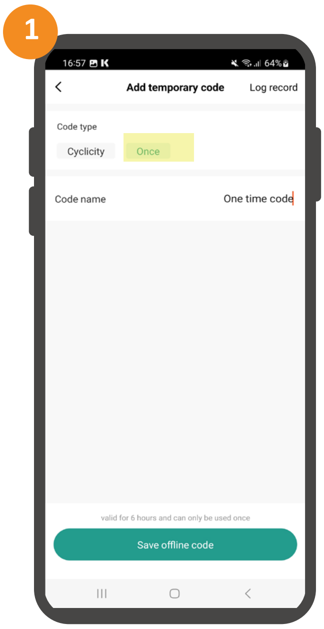
Press on the “temporary code” option located at the bottom of the device management screen.

1 - Select “One time” code type.

- Name the temporary access you are about to generate.

2 - Confirmation of the generated temporary access will be displayed. In case it is desired to share the code, follow step 3 described in the previous point.

1



16:57 64%

Add temporary code | Log record

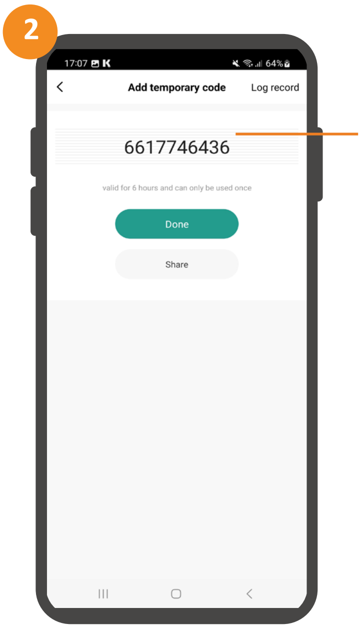
Code type: Cyclicity | Once

Code name: One time code

valid for 6 hours and can only be used once

Save offline code

2



17:07 64%

Add temporary code | Log record

6617746436

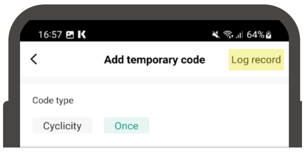
valid for 6 hours and can only be used once

Done

Share

The code will be valid for 6 hours from its generation.

NOTE: it is possible to check the generated temporary codes from the “log record” option of the “temporary code” menu:



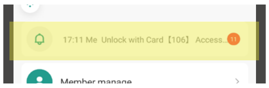
16:57 64%

Add temporary code | Log record

Code type: Cyclicity | Once

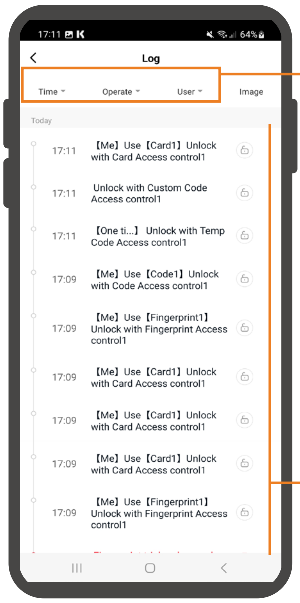
9.3. LOGS (EVENT LOG)

Press on the “access log” option on the reader’s main screen to monitor accesses:



17:11 Me Unlock with Card【106】 Access... 11

Member manage



17:11 64%

Log

Time | Operate | User | Image

Today

17:11 【Me】Use【Card1】Unlock with Card Access control1

17:11 Unlock with Custom Code Access control1

17:11 【One ti...】 Unlock with Temp Code Access control1

17:09 【Me】Use【Code1】Unlock with Code Access control1

17:09 【Me】Use【Fingerprint1】Unlock with Fingerprint Access control1

17:09 【Me】Use【Card1】Unlock with Card Access control1

17:09 【Me】Use【Card1】Unlock with Card Access control1

17:09 【Me】Use【Card1】Unlock with Card Access control1

17:09 【Me】Use【Fingerprint1】Unlock with Fingerprint Access control1

Filters:

TIME: show all events “All tiem”, those of the last 3 days “Nearly three days”, last 7 days “Nearly seven days”, last month “Nearly a month” or define the desired time range “Custom”.

OPERATE: shows all accesses “All records”, only authorized accesses “Door opening record” or only denied accesses “Alarm record”.

USER: displays all users “All user” or it is possible to select specific user/s to be displayed.

Records:

🔓 Records of authorized access.

⚠ Records of unauthorized access.

The record lines include date and time of the record, as well as identifying data of the recorded event: user, type of identification and name of the credential.

9.4.VALIDITY OF THE USER CREDENTIALS

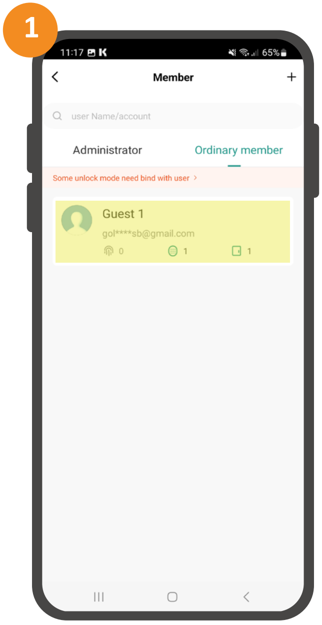
For temporary access management, it is recommended to use the “temporal code per time period” option explained in section “9.1” of this manual, however, the application allows the validity of the user’s credentials to be established as follows:

1 - From “Member manage” select the user for whom you wish to limit the period of time of use.

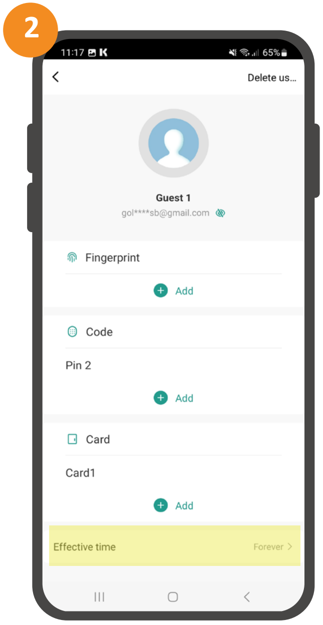
2 - Click on the option “Effective time”.

3 - Activate the “Customize” option, then set the start and end date of validity, complete the configuration by clicking on “Save”.

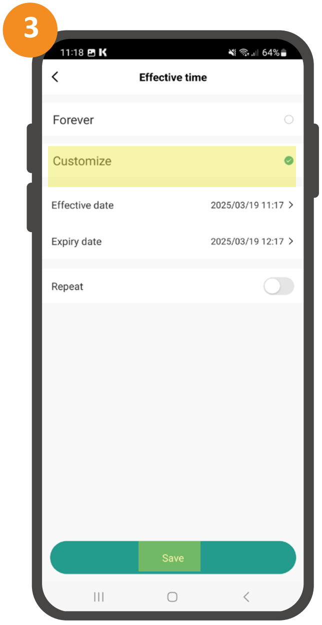
4 - The setting will be completed and the user will only be able to identify himself as valid for the set period of time.



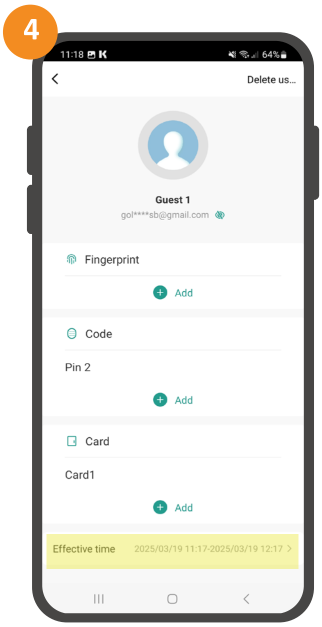
Guest 1
gol****sb@gmail.com
0 1 1



Guest 1
gol****sb@gmail.com
Pin 2
Card1
Effective time Forever ›



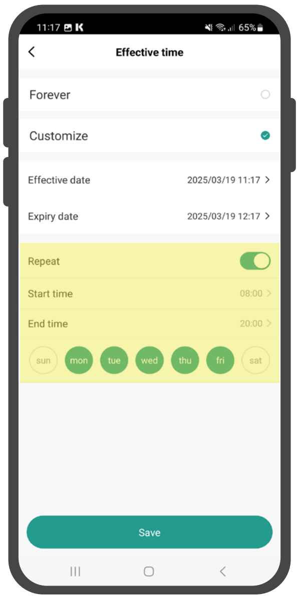
Forever ○
Customize ✓
Effective date 2025/03/19 11:17 ›
Expiry date 2025/03/19 12:17 ›
Repeat



Guest 1
gol****sb@gmail.com
Pin 2
Card1
Effective time 2025/03/19 11:17-2025/03/19 12:17 ›

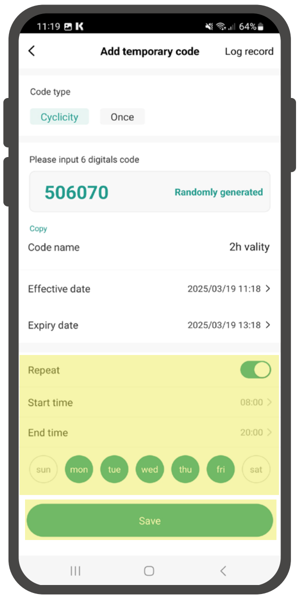
9.5.SCHEDULES

To the “validity of the user credentials” as well as to “temporaral code per time period” a usage schedule may be applied:



Forever ○
Customize ✓
Effective date 2025/03/19 11:17 ›
Expiry date 2025/03/19 12:17 ›
Repeat ●
Start time 08:00 ›
End time 20:00 ›
sun mon tue wed thu fri sat

Schedule configuration in “validity of the user credentials”



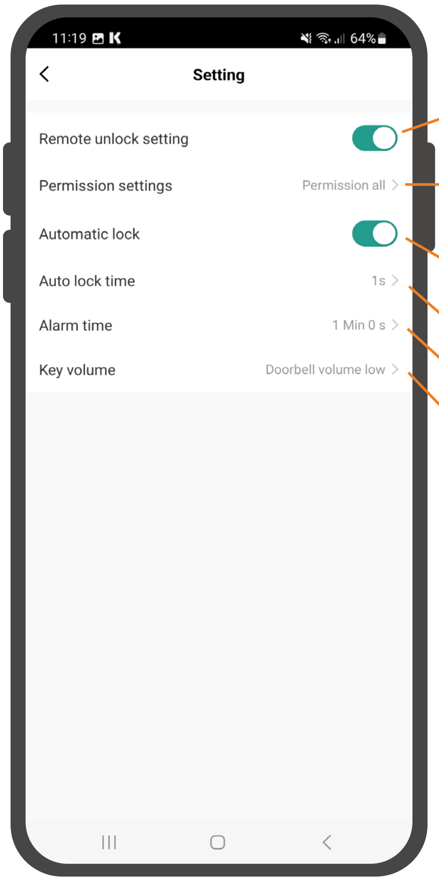
Code type
Cyclicity Once
Please input 6 digitals code
506070 Randomly generated
Code name 2h vality
Effective date 2025/03/19 11:18 ›
Expiry date 2025/03/19 13:18 ›
Repeat ●
Start time 08:00 ›
End time 20:00 ›
sun mon tue wed thu fri sat

Schedule configuration in “temporaral code per time period”

As it can be seen, the schedule setting allows to establish which days and in which time interval the access will be possible.

9.6. SETTINGS FROM THE APP

By pressing the “Configuration” menu on the main page of the device, the following settings can be made:



11:19

Setting

Remote unlock setting

Permission settings: Permission all

Automatic lock

Auto lock time: 1s

Alarm time: 1 Min 0 s

Key volume: Doorbell volume low

Active, allows to activate the relay contact via APP.

Permission admin, ordinary members cannot activate the relay contact via APP.

Permission all, All users can activate the relay contact via APP.

* In case certain users are not required to use the APP, choose not to register the e-mail address when adding them.

Automatic lock active, pulse mode.

Automatic lock deactived, latched mode.

Auto lock time, adjustable in pulse mode (1-100 seconds).

Alarm time, alarm for failed attempts, open door,... (1-180 seconds).

Key volume, confirmation beep volume when pressing remote control keys.

READER CONFIGURATION

10.OTHER SETTINGS

10.1. IDENTIFICATION MODE

Identification by fingerprint

Enter administrator mode				
*	MASTER CODE	#	40	#

Example: * 987654 # 40 #

Identification by card

Enter administrator mode				
*	MASTER CODE	#	41	#

Example: * 987654 # 41 #

Identification by PIN

Enter administrator mode				
*	MASTER CODE	#	42	#

Example: * 987654 # 42 #

Multi identification

The reader will open when there has been identification (in a short time interval) with several credentials (min.2, max.9).

Enter administrator mode				
*	MASTER CODE	#	43 + (2-9)	#

Example: * 987654 # 432 #

NOTE: in the example the reader would have been configured to validate the opening when two valid credentials are identified.

Identification by fingerprint, card or PIN (factory setting)

Enter administrator mode				
*	MASTER CODE	#	44	#

Example: * 987654 # 44 #

10.2. RELAY SETTINGS

PULSE MODE

Enter administrator mode					
*	MASTER CODE	#	3	1-99	#

Example: * 987654 # 3 15 #

The pulse can be active from 1 to 99 seconds. In the example, the value 15 has been entered, so it would be active for 15 seconds.
Factory setting: 5 seconds.

LATCHING MODE

Enter administrator mode					
*	MASTER CODE	#	3	0	#

Example: * 987654 # 3 0 #

The relay is becomes to ON/OFF mode.

10.3. ALARM SETTINGS (TAMPER)

Enter administrator mode				
*	MASTER CODE	#	5(0-3)	#

Example: * 987654 # 52 #

The tamper alarm activation time is from 0 to 3 minutes. In the example, the value 52 has been entered, so it would be active for 2 minutes. Default setting: 51 (1 minute).

10.4. LOCKOUT ALARM (UNSUCCESSFUL ATTEMPTS)

The lockout alarm will be activated after 10 unsuccessful attempts. The factory default is OFF, but can be set to deny access for 10 minutes or to activate the alarm after it is triggered.

Lockout disabled (factory setting)

Enter administrator mode				
*	MASTER CODE	#	60	#

Example: * 987654 # 60 #

10-minute access code

Enter administrator mode				
*	MASTER CODE	#	61	#

Example: * 987654 # 61 #

The LED will start blinking and the equipment will be blocked for 10 minutes. To return to the normal state, wait 10 minutes or restart the reader.

Alarm

Enter administrator mode				
*	MASTER CODE	#	62	#

Example: * 987654 # 62 #

In case of identification with a valid user or MASTER credential, the alarm will stop.

10.5. ACOUSTIC AND VISUAL FEEDBACK

Deactivate sound

Enter administrator mode				
*	MASTER CODE	#	70	#

Example: * 987654 # 70 #

Activate sound (factory setting)

Enter administrator mode				
*	MASTER CODE	#	71	#

Example: * 987654 # 71 #

Deactivate led

Enter administrator mode				
*	MASTER CODE	#	72	#

Example: * 987654 # 72 #

Activate led (factory setting)

Enter administrator mode				
*	MASTER CODE	#	73	#

Example: * 987654 # 73 #

Keyboard backlighting always off

Enter administrator mode				
*	MASTER CODE	#	74	#

Example: * 987654 # 74 #

Backlit keyboard always on

Enter administrator mode				
*	MASTER CODE	#	75	#

Example: * 987654 # 75 #

Keyboard backlighting automatically deactivated (factory setting)

Enter administrator mode				
*	MASTER CODE	#	76	#

Example: * 987654 # 76 #

- Automatic shutdown after 20 seconds. It will be turned on by pressing any key (this key will not be taken into consideration).

10.6. RESET TO FACTORY SETTINGS

The reset restores the reader to factory defaults, clearing the configuration and the master code. User information will be retained.

1. Turn off the power.
2. Press and hold the exit button*.
3. Turn on the power.
4. When 2 beeps are heard, release the output button*.
5. The LED will light up yellow.
6. Approach a13.56MHz to the reader
7. The light will illuminate red and the equipment will be reset to factory settings.

**It requires to have connected the output push button, the yellow (OPEN) and the black wire (GND).

NOTE
- This process generates a Master card replacing the previous one.
- In case it is not desired to replace the current master card, press the * button instead of step 6 to finalise the reset.

10.7. MASTER FINGERPRINT REGISTRATION

Enter administrator mode					
*	MASTER CODE	#	1	ID 99	Place fingerprint 3 times

Example: * 987654 # 1 99 # FINGERPRINT FINGERPRINT FINGERPRINT

10.8. DELETE ALL THE USERS

Enter administrator mode					
*	MASTER CODE	#	2	MASTER CODE	#

Example: * 987654 # 2 987654 #

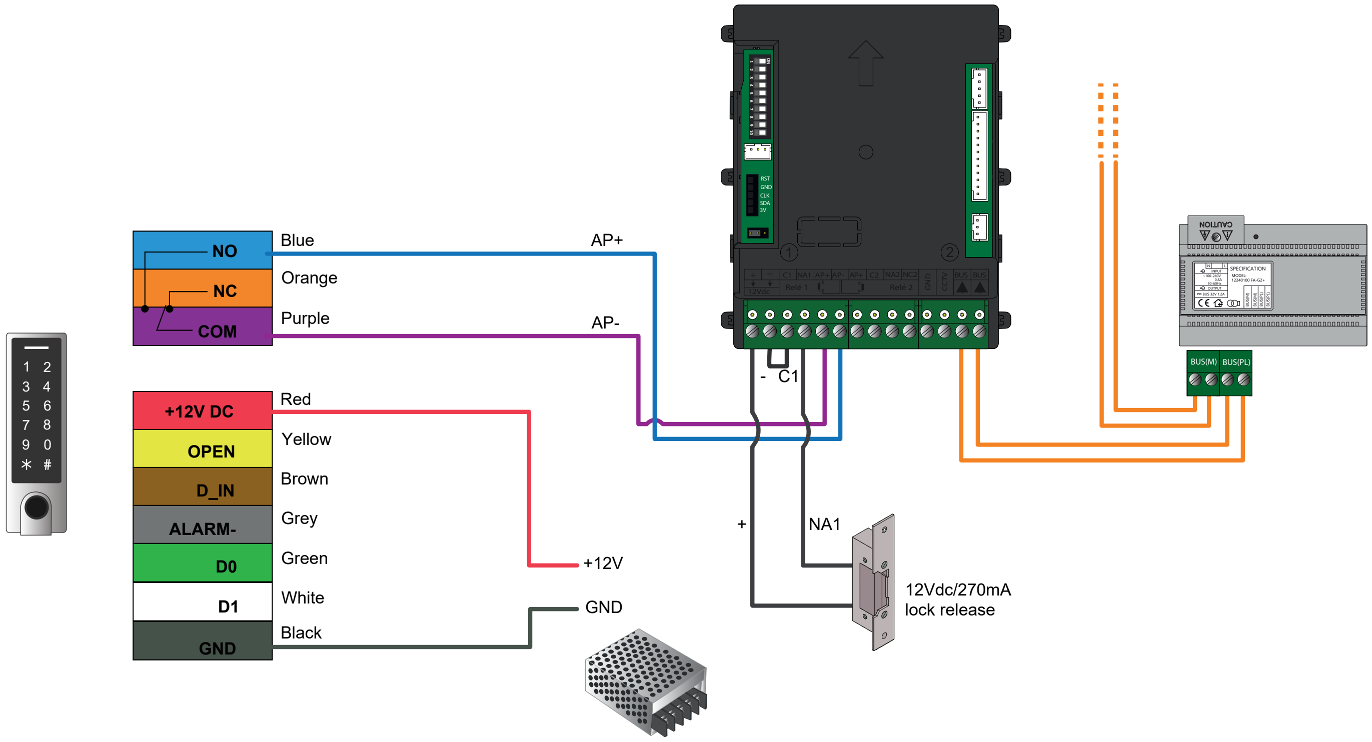
IMPORTANT: Before performing this function, make sure that it is OK to REMOVE all previously registered users.

11.STATUS DISPLAYS

OPERATING STATUS	COLOUR LED	BUZZER
Stand by	Red	-
Enter programming mode	Flashing red	Short beep
In programming mode	Orange	Short beep
Operation error	-	3 beeps
Exit programming mode	Red	Short beep
Door open	Green	Short beep
Alarm	Flashing red	Beeps

12.OTHER CONNECTION DIAGRAMS

12.1.CONNECTION DIAGRAM WITH INTERCOM



NOTE: The AP (door release) of the intercom does not activate the door opener until the pulse of the AIO-KEY reader has finished. To avoid opening delays, set the minimum pulse to 1 second on the reader:

Enter administrator mode					
*	MASTER CODE	#	3	1	#

13.ANNEX

13.1.SHARED DEVICE IS NOT DISPLAYED ON MAIN PAGE

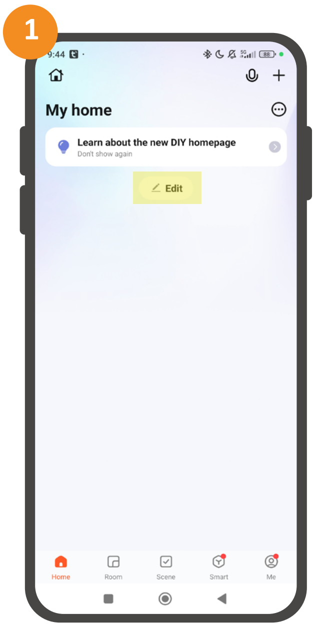
In some cases when the administrator shares the device with another user the application may not directly display the device on the guest user's home page. In this case the guest should proceed as shown below:

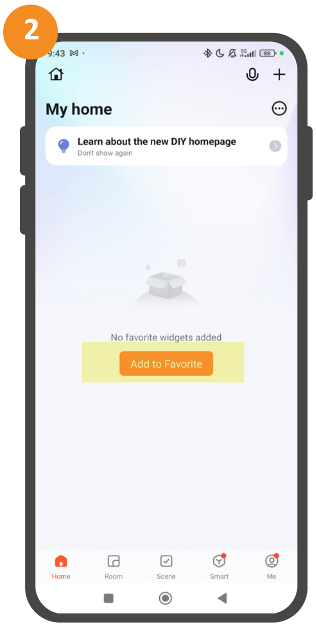
1 - Click on the "Edit" option located on the "My Home" page.

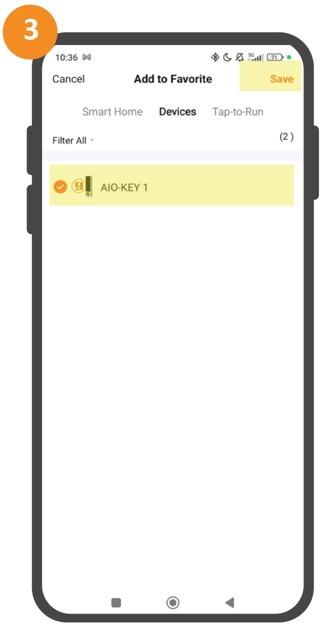
2 - Click on the "Add to favorites" option below.

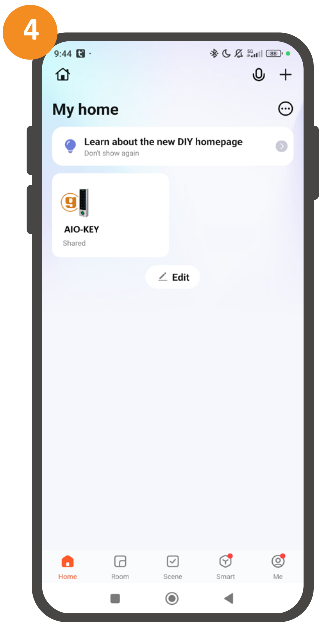
3 - Select the "AIO-KEY" reader and then click on "Save".

4 - The reader will be added.









13.2.CONNECTIVITY WITH THE READER

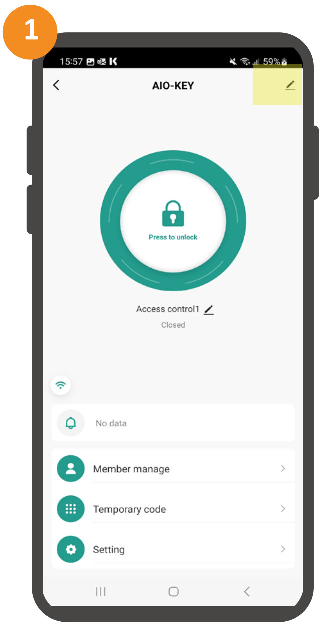
Below is indicated how to proceed in case of experiencing different connectivity cases:

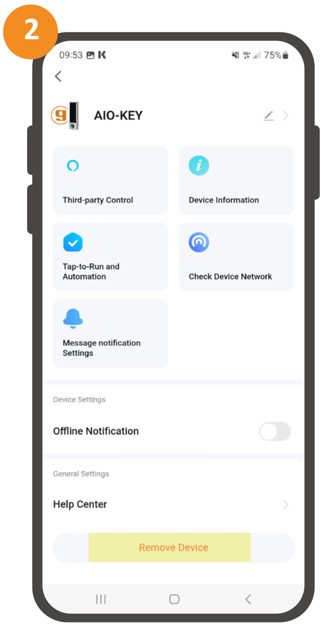
1) Difficulties to link the reader, try performing the following sequence:

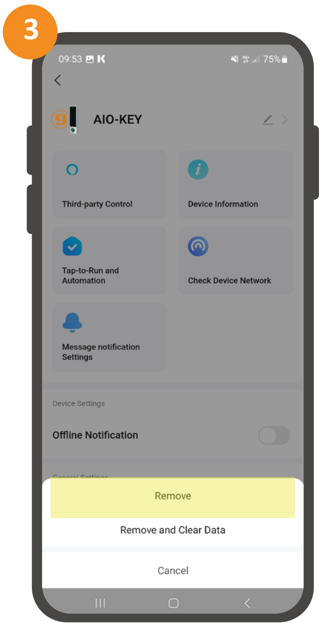
* master code # 9 master code #

This will reset the reader's connectivity. Remember that the WiFi network to which the reader is connected must be 2.4GHz frequency.

2) Administrator problems to perform the management in the APP, press on the "pencil" icon on the main screen of the device and then on the "Remove device" option.







This will unlink the administrator from the device (it does not delete the information).

IMPORTANT: in case of pressing on the option "Remove and Clear data" the reader will be unlinked and all the information will be lost. Use this other option only in case of needing to reset everything done in the APP.

golmar
Sistemas de comunicación S.A.

C/ Silici 13. Poligon Industrial Famadas
08940 – Cornellà del llobregat – Spain
golmar@golmar.es
Tel: 93 480 06 96
www.golmar.es
www.golmar-seguridad.es

Golmar deserves the right for any modification without prior notice.