WCONTROL

INSTALLER MANUAL

IM_ENG_REV0226_WCONTROL

1.TABLE OF CONTENTS

2.INTRODUCTION

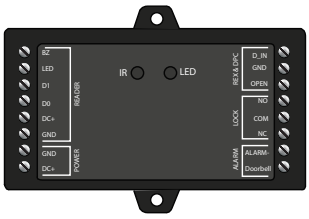
Installation manual for the WControl device. This can act as a smart relay and allow the activation of the relay contact by means of the TUYA APP, as well as act as a controller by connecting a Wiegand reader to control proximity and keypad identifications.

Golmar guarantees the proper operation when a reader is connected, as long as the following models are used: CODEPROX-N, KEYBUS SE, KEYDUPROX, DUPROX and BLE-S.

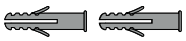
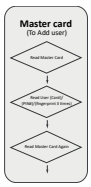
3.SPECIFICATIONS

Material	Black ABS plastic
Input voltage	12Vdc
Current	Standby: ≤ 100mA / Active: ≤ 150mA
Capacity	Hardware use: 1000 users / TUYA APP use: 500 users
Relay	NO, NC, common (2A max.)
Supported identifications	Card, PIN, remote via APP TUYA
Supported Wiegand formats	Wiegand 26-44, 56 and 58 bits
Supported keypad output bit formats	4 bits or 8bits (ASCII)
Dimension (Height x Width x Depth):	91(H) x 48(W) x 20(D)mm
Working humidity range:	0-90% (non-condensing)

4.PRODUCT CONTENT



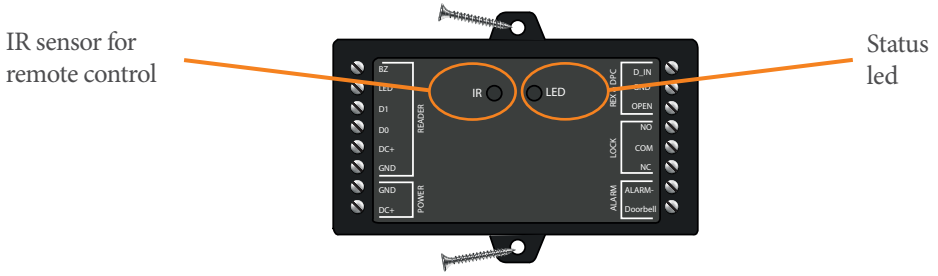
WControl controller

	Diode.
	Varistors.
	Fixing blocks.
	Screws.
	Screwdriver
	Remote control for programming.
	MASTER programming card.

IMPORTANT:
Once the controller has been programmed, keep the master card and the remote control in a safe place for future programming.

5.INSTALLATION

Place the controller in a protected room or a protected box and secure it with the screws provided. Before placing the controller, keep in mind that in case of using the Tuya APP, the controller must receive WiFi coverage from the router of the installation.



6.CONNECTION

LEFT TERMINALS	DESCRIPTION
BZ	Buzzer control
LED	Led control
D1	Wiegand Data 0 input
D0	Wiegand Data 1 input
DC+	Positive power output
GND	Negative power output
GND	Negative power input
DC+	Positive power input

RIGHT TERMINALS	DESCRIPTION
D_IN	Door status detection
GND	Door and exit contact negative
OPEN	Exit pushbutton
NO	Normally open relay output
COM	Common contact for relay output
NC	Normally closed relay output
ALARM-	Alarm negative
DOOR BELL	External doorbell

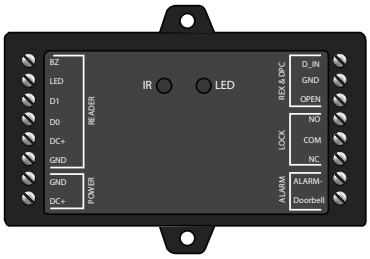
7.STATUS DISPLAYS

OPERATING STATUS	LED COLOUR	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

USERS MANAGEMENT

8.USERS MANAGEMENT

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



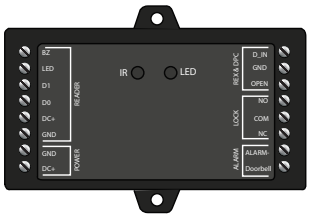
Through controller

Through smartphone via the APP Tuya

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

8.1. USER MANAGEMENT THROUGH CONTROLLER

The management of users in the controller, as it is illustrate below, can be carried out in a basic (**8.1.1.Basic user progamming**), by collection (**8.1.2.Progamming by card collection**) or advanced (**8.1.3.Advanced programming**) way.



Registration in controller

In case to choose APP registration continue with the manual in section "**8.2. User management through APP**".

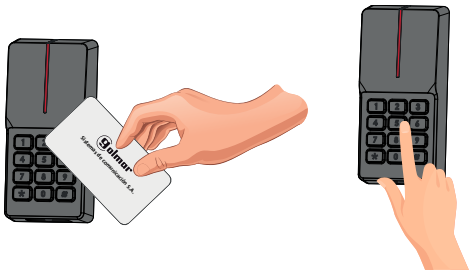
8.1.1.BASIC USER PROGRAMMING

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

USER REGISTRATION

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

2) Approach the "Master card" or enter PIN to be registered.
For code enter PIN from 4 to 6 digits plus #.

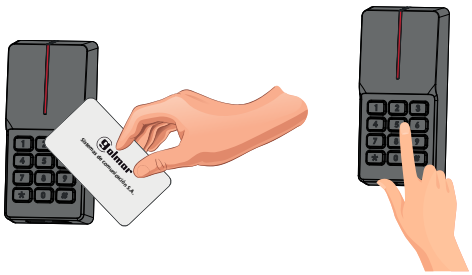


3) Approach the "Master Card" card to the reader.

DELETE USER

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

2) Approach the "Master card" or enter PIN to be deleted.



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

NOTE: In case of loss of the MASTER CARD, it is possible to create one by following the procedure described in section "10.4.Reset to factory defaults".

8.1.2.PROGRAMMING BY CARD COLLECTION

The controller supports card programming in pick-up mode. This means that once activated, any card approaching the reader will open the door and will be programmed, once the pick-up mode is deactivated, the programming will be completed (new cards will not open the door and will not be encoded).

COLLECTION MODE ON

* (MASTER CODE) # 93

DOOR IS UNLOCKED

USER IS REGISTERED

COLLECTION MODE OFF

* (MASTER CODE) # 92

CARD COLLECTION MODE DEACTIVATED (factory default)

Enter administrator mode				
*	MASTER CODE	#	92	#

Example: * 987654 # 92 #

CARD COLLECTION MODE ACTIVATED

Enter administrator mode				
*	MASTER CODE	#	93	#

Example: * 987654 # 93 #

This mode is intended for installers as it simplifies the work, as they can deliver the credentials to the installation administrator and deactivate the collection mode after a few days (once all the delivered credentials have been used).

8.1.3.ADVANCED PROGRAMMING

Advanced programming will require the use of the remote control:

- Remove the protective plastic from the battery before starting to use the remote control.
- Use the remote control in a position close to the controller and pointing at the LED (infrared receiver is located next to the LED).

Perform the following sequence to enter programming:

Enter administrator mode		
*	MASTER CODE (By default: 123456)	#

IMPORTANT

The controller 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 controller will go to standby mode, status LED will be shown in "steady red". In the case that no key presses are made, the controller automatically exits programming after 30 seconds.

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

8.1.3.1.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 #

8.1.3.2.CARD REGISTRATION (AUTO ID)

Registration of cards with automatic registration.

Enter administrator mode				
*	MASTER CODE	#	1	APPROACH CARD

Example: * 987654 # 1 APPROACH CARD

8.1.3.3.CARD REGISTRATION (SPECIFIC ID)

Maximum number of records is 990. Users IDs from 0 to 989.

Enter administrator mode						
*	MASTER CODE	#	1	USER ID (0-989)	#	APPROACH CARD

Example: * 987654 # 1 1 # APPROACH CARD

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

8.1.3.4.PIN REGISTRATION (AUTO ID)

PIN registration with automatic recording.

Enter administrator mode					
*	MASTER CODE	#	1	PIN	#

Example: * 987654 # 1 4543 #

8.1.3.5.PIN REGISTRATION (SPECIFIC ID)

Maximum number of records is 990. User IDs from 0 to 989.

Enter administrator mode							
*	MASTER CODE	#	1	USER ID (0-989)	#	PIN	#

Example: * 987654 # 1 1 # 4543 #

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

8.1.3.6.PIN DELETION

PIN deletion by introducing the PIN to be deleted.

Enter administrator mode					
*	MASTER CODE	#	2	INTRODUCE PIN	#

Example: * 987654 # 2 4543 #

8.1.3.7.CARD DELETION

Erasing cards by approaching the card to be deleted.

Enter administrator mode				
*	MASTER CODE	#	2	APPROACH CARD

Example: * 987654 # 2 APPROACH CARD

8.1.3.8.DELETING CARDS OR PIN (SPECIFIC ID)

Enter the ID corresponding to the user to be deleted.

Enter administrator mode					
*	MASTER CODE	#	2	USER ID (0-989)	#

Example: * 987654 # 2 1 #

8.2. USER MANAGEMENT IN APP TUYA

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

NOTE: below is detailed information for the configuration of the TUYA APP. Please refer to the quick guide "QGI_ENG_REV0125_APP-TUYA-WCONTROL" 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

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 controller with Tuya technology.
- The APP is supported by smartphones with iOS (7.0 or higher) or Android (4.3 or higher) version.

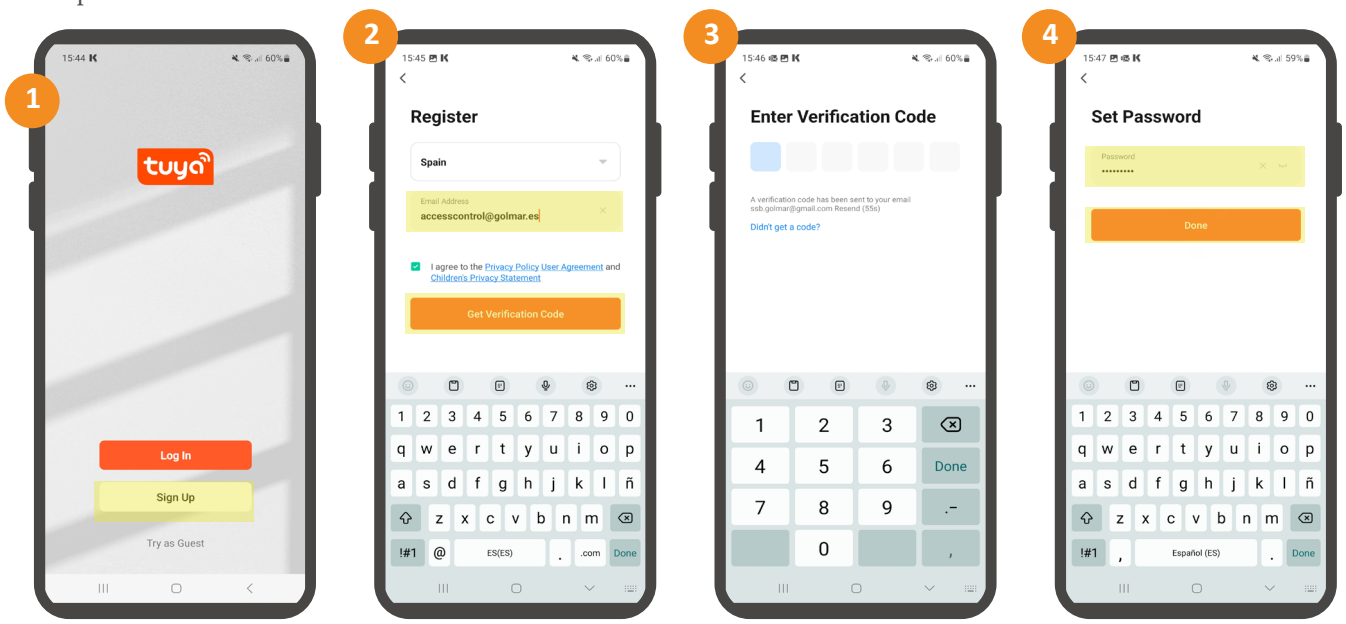
8.2.2.REGISTRATION AND LOGIN

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.



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 CONTROLLER

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:

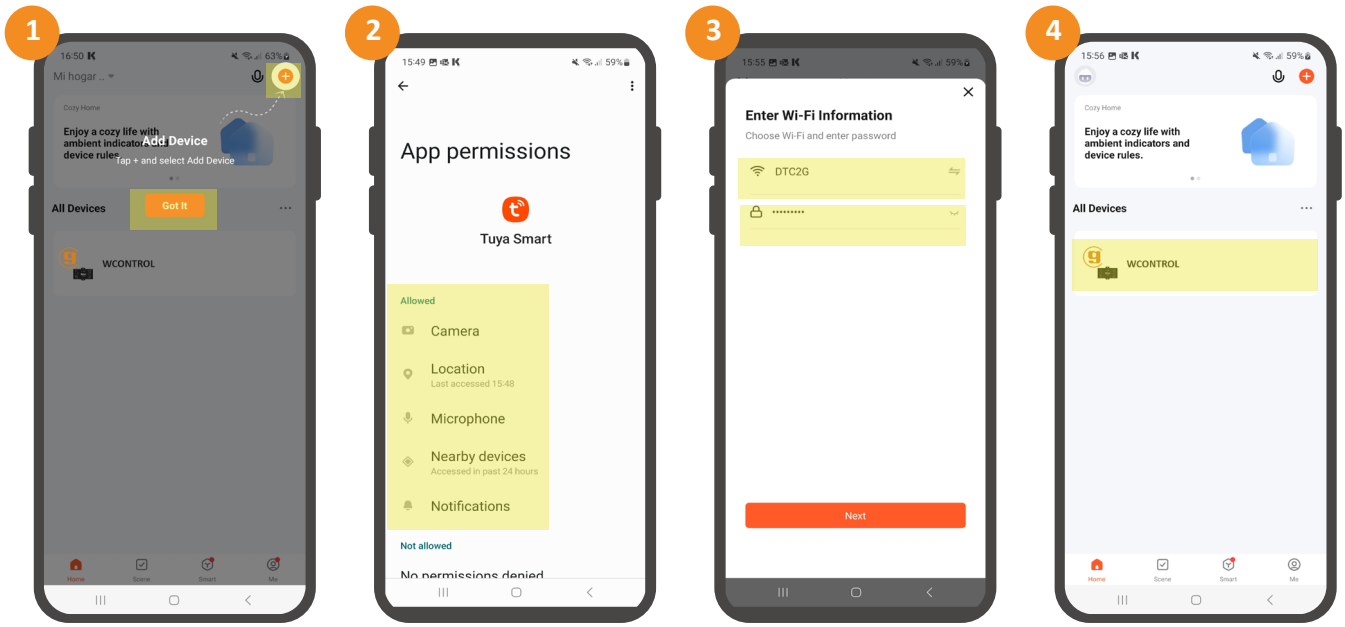
1 - Press the "got it" option and then the "+" or "add device" symbol.

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

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

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

4 - Controller will be added.



IMPORTANT

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

* 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 controller is by default "administrator", this user can manage the following:

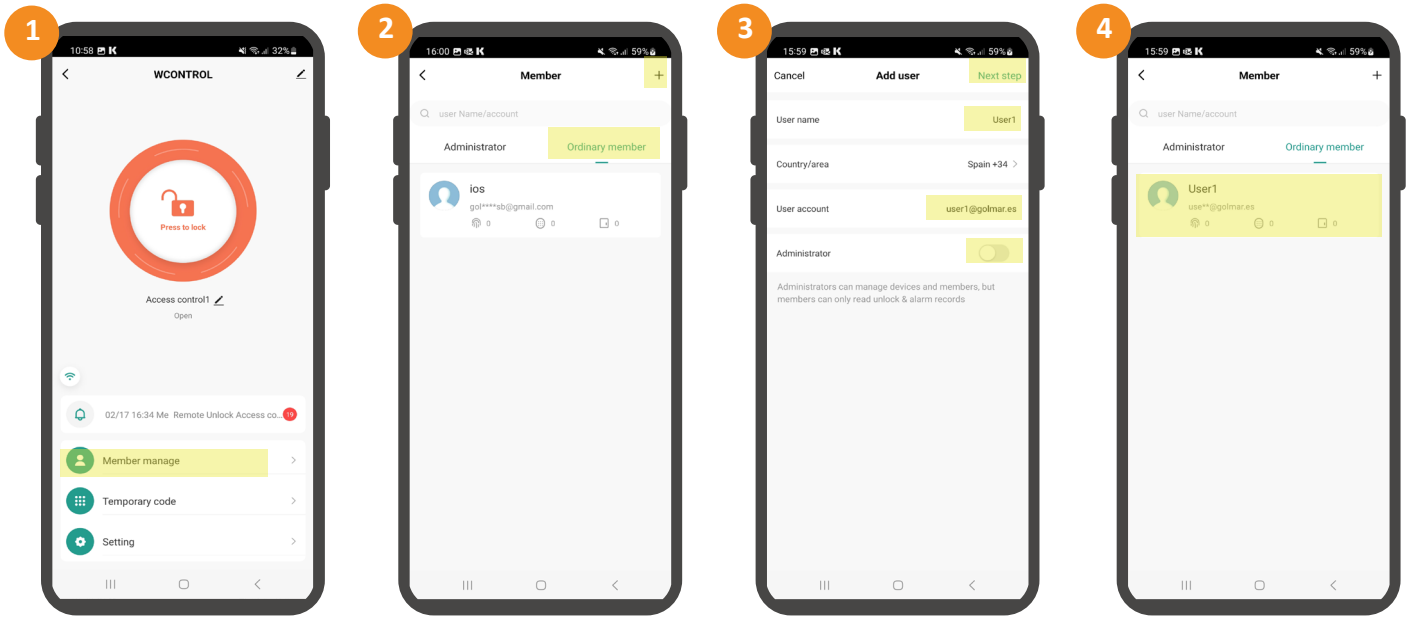
FUNCTION	ADMINISTRATOR
DOOR OPENING	YES
ADMINISTRATOR AND USER MANAGEMENT	YES
USER MANAGEMENT	YES
DEFINE USERS AS ADMIN	YES
VIEW ALL LOGS	YES
SET RELAY TIMES	YES

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 controller.
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.

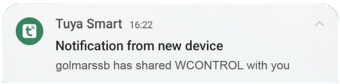
IMPORTANT
The user to whom the installation is shared must have an account (registered in the APP, section “8.2.2.Registration and login”).



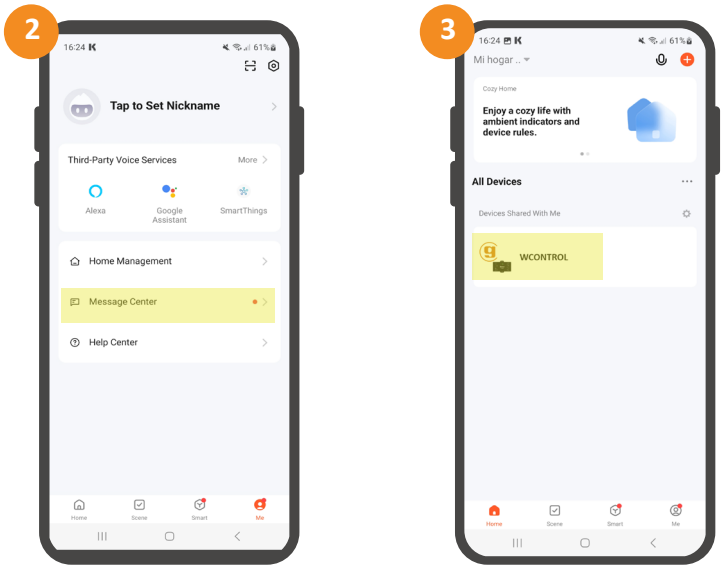
NOTES
1 - The user will now be able to open with the smartphone, to grant other access methods see point number 9.2.8.
2 - In case more users are to be added, repeat the process.
3 - In case it is desired to delete a user, access the list (screen step 2), select the user and then press the option “delete 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:



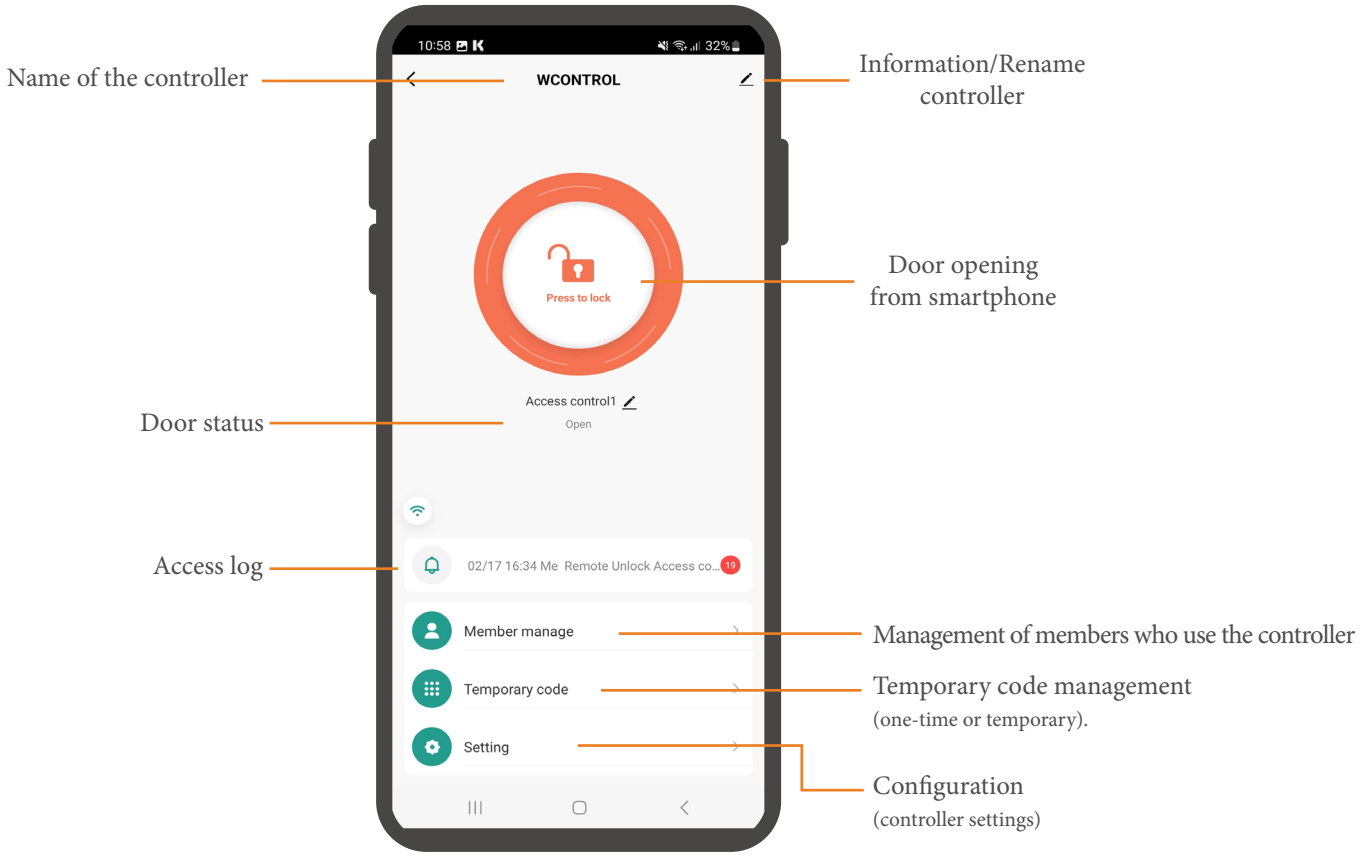
2 - This can be checked from the “message center” (“me” tab of the main screen).
3 - The device will appear on the main screen as “ devices shared with me ”.



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

8.2.6.MAIN CONTROLLER SCREEN

The main screen of the controller is described below:



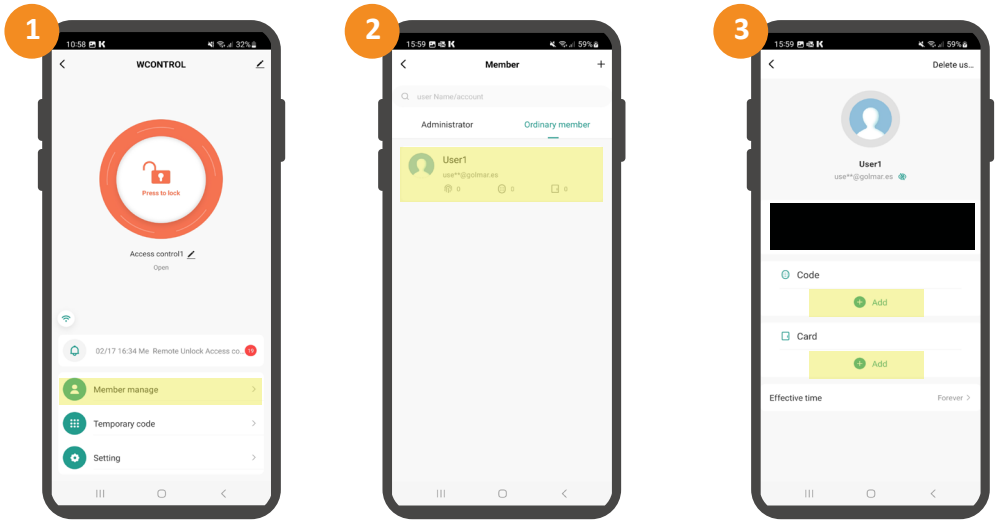
NOTE: ordinary members (users) will not be able to use the “Member Management”, “Temporary Code” and “Configuration” functions.

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

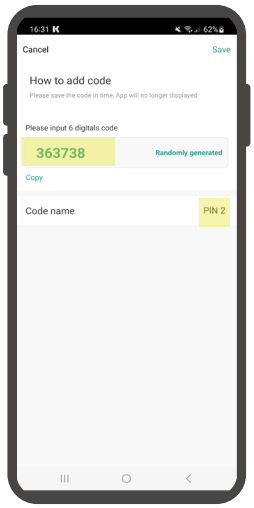
1 - In the main screen of the controller, press on “Member manage”.
2 - Select the user to register the credential.
3 - Press “Add” on the type of identification to register code or card).



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

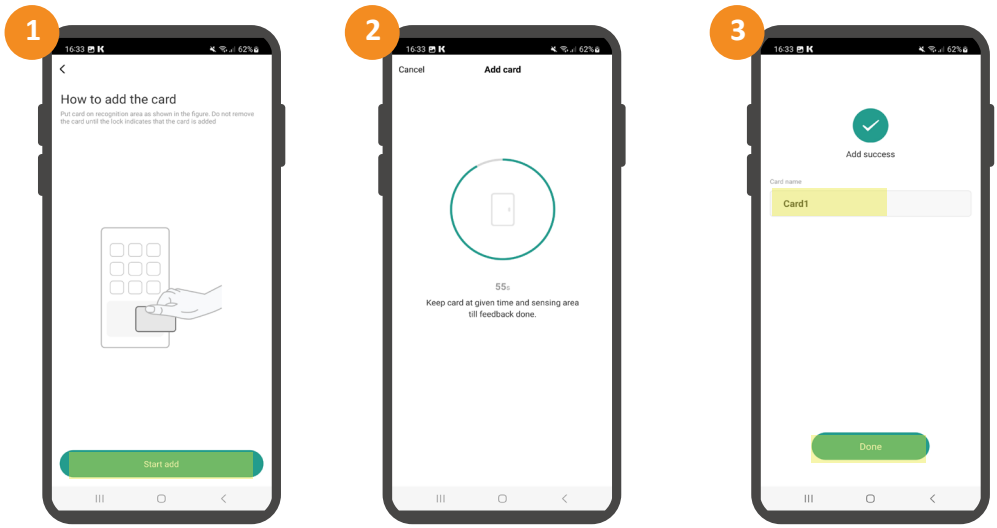
8.2.9.PIN REGISTRATION

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



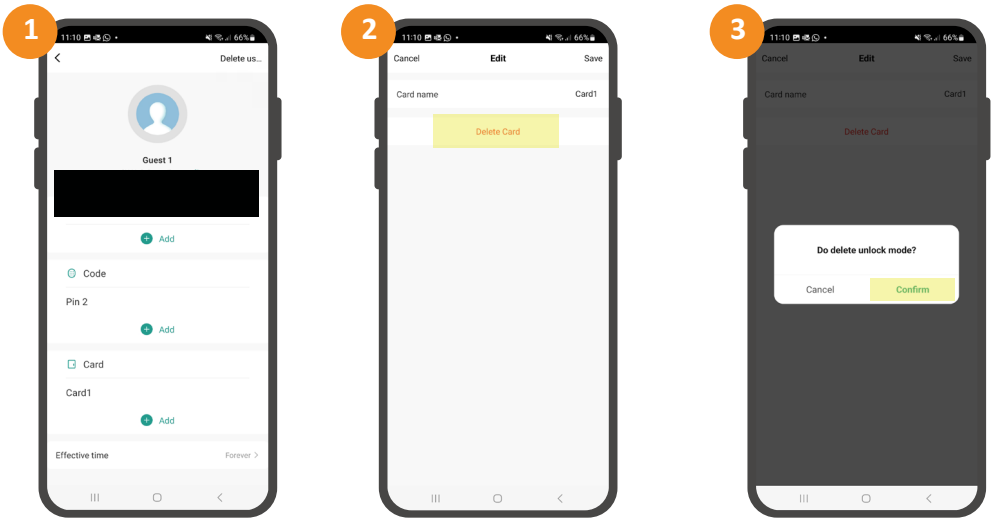
8.2.10.CARD REGISTRATION

1 - Press on the “Start add” option.
2 - Approach the card to be registered on the reader connected.
3 - Enter a name to identify the registered card.



8.2.11.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.



9.TUYA APP ADDITIONAL FUNCTIONS

9.1. TEMPORAL CODE PER TIME PERIOD

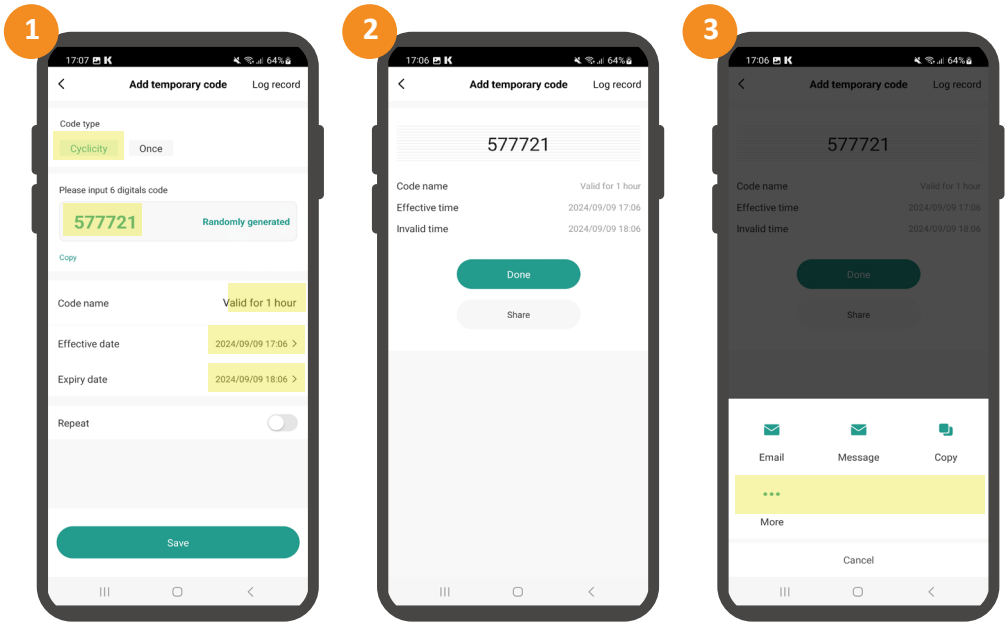
Press on the "temporary code" option located at the bottom of the device management screen.

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.



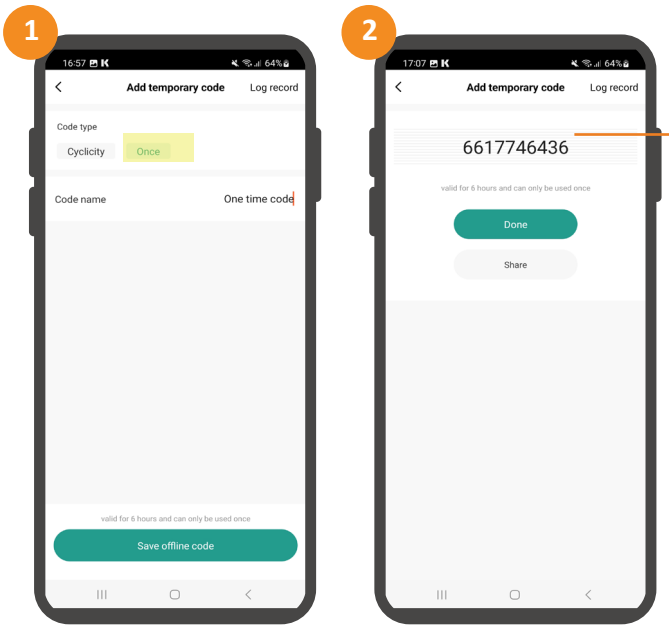
9.2. ONE-TIME USE TEMPORARY CODE

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

1 - Select "One time" code type.

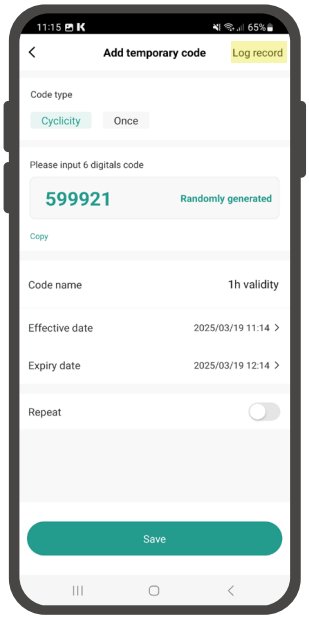
- Name the temporary access you are about to generate.

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.



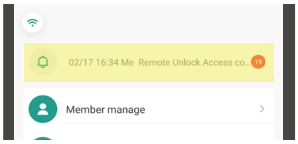
The code will be valid for 6 hours from its generation.

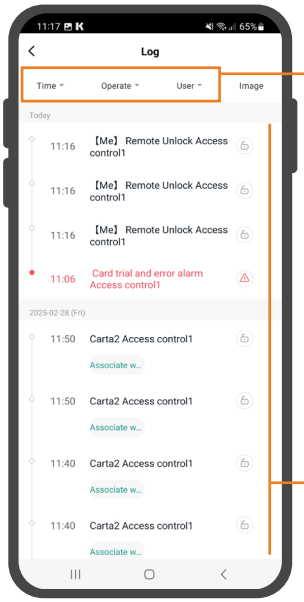
NOTE: it is possible to check the generated temporary codes from the “log record” option of the “temporary code” menu:



9.3. LOGS (EVENT LOG)

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





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

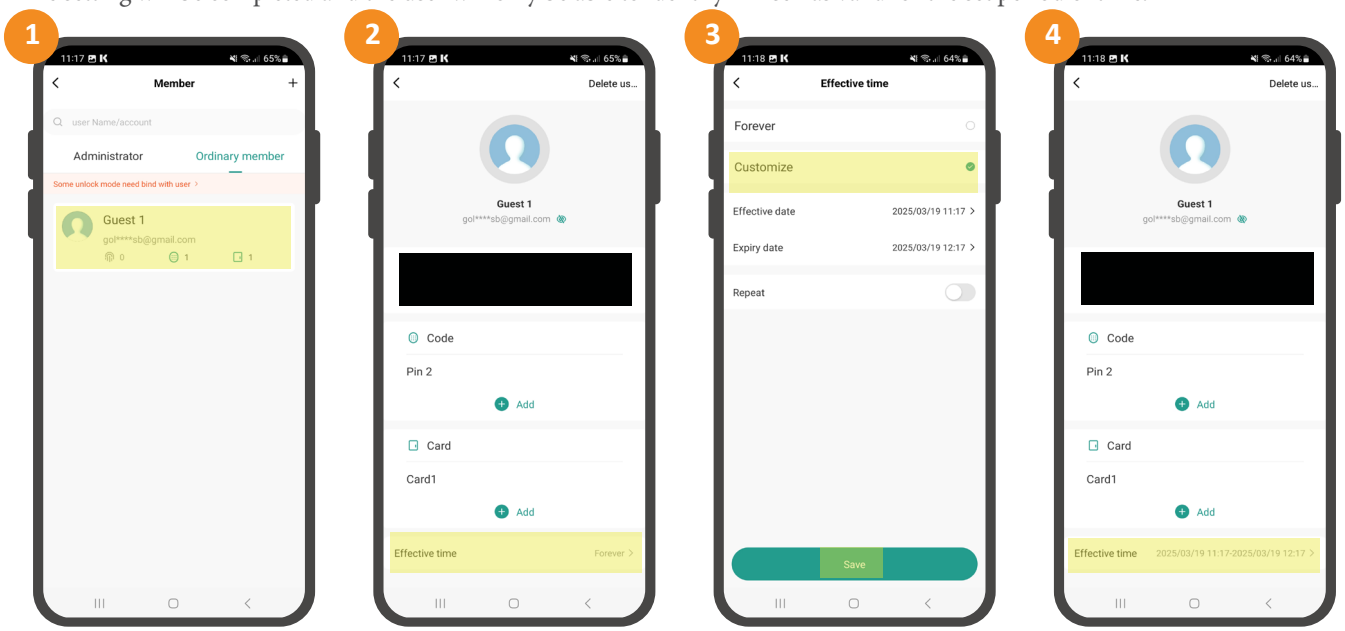
For temporary access management, it is recommended to use the "temporal code per time period" option explained in section "10.1" of this manual, however, the application allows the validity of the user's credentials to be established as follows:

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".

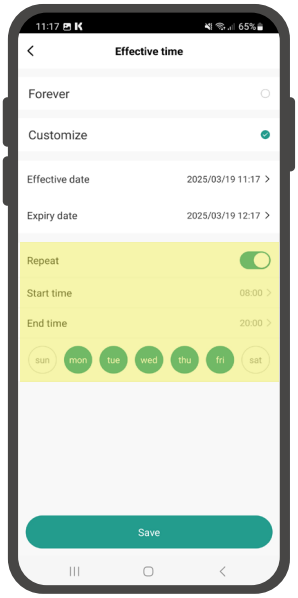
3 - Activate the "Customize" option, then set the start and end date of validity, complete the configuration by clicking on "Save".

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

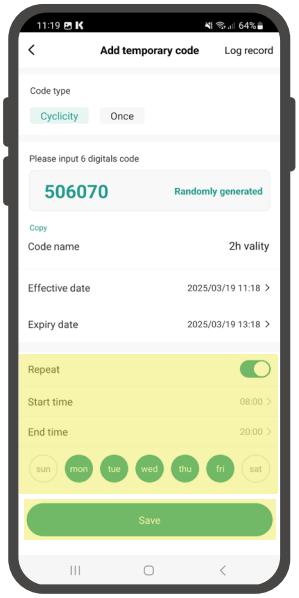


9.5.SCHEDULES

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



Schedule configuration in "validity of the user credentials"

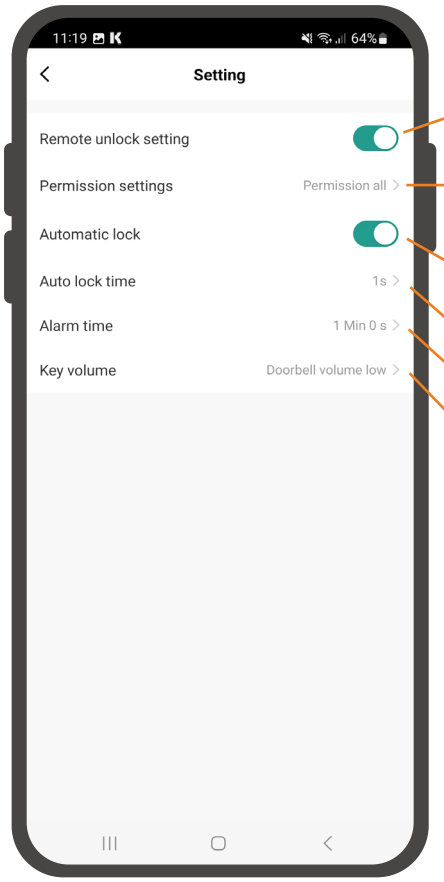


Schedule configuration in "temporaral code per time period"

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:



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.

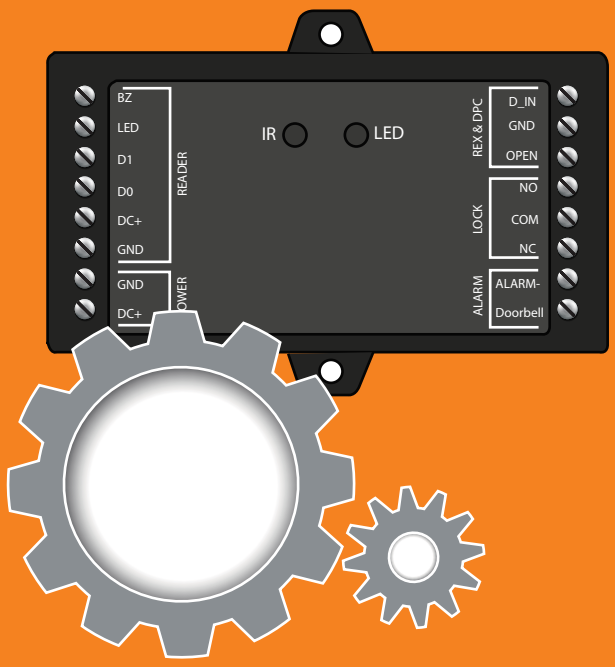
Automatic lock deactived, latched mode.

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.

CONTROLLER CONFIGURATION



10.OTHER SETTINGS

10.1. IDENTIFICATION MODE

10.1.1.IDENTIFICATION BY CARD OR PIN

Enter administrator mode				
*	MASTER CODE	#	43 (factory setting)	#

Example: * 987654 # 43 #

10.1.2.IDENTIFICATION BY PIN

Enter administrator mode				
*	MASTER CODE	#	41	#

Example: * 987654 # 41 #

10.1.3.IDENTIFICATION BY CARD

Enter administrator mode				
*	MASTER CODE	#	40	#

Example: * 987654 # 40 #

10.2. ALARM SETTINGS (TAMPER)

10.2.1.ACTIVATE 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.
Factory setting: 51 (1 minute).

10.3. RELAY SETTINGS

10.3.1.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.

10.3.2.LATCHING MODE

Enter administrator mode					
*	MASTER CODE	#	3	0	#

Example: * 987654 # 3 0 #

The relay becomes to operate in an ON/OFF mode.

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.

10.4.1.BLOCKING DEACTIVATED

Enter administrator mode				
*	MASTER CODE	#	60 (factory setting)	#

Example: * 987654 # 60 #

10.4.2.10-MINUTE ACCESS BLOCKING

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 controller.

10.4.3.ALARM

Enter administrator mode		
*	MASTER CODE	#

62	#

Example: * 987654 # 62 #

The alarm will be activated, in case of 10 unsuccessful attempts the alarm will sound for the time defined in chapter "11.2. ALARM SETTINGS (TAMPER)". In case to approach a user card, enter user PIN code or approach MASTER card, the alarm will stop.

10.5. OPEN DOOR DETECTION

It is recommended to connect a door contact in the device. Otherwise, in the mobile APP the door status will always be shown as 'ON'. Connect the door contact to terminals 'D_IN' and 'GND'.

10.5.1.OPEN DOOR DETECTION ACTIVATED

Enter administrator mode		
*	MASTER CODE	#

64	#

Example: * 987654 # 64 #

10.5.2.OPEN DOOR DETECTION DEACTIVATED

Enter administrator mode		
*	MASTER CODE	#

63 (factory setting)	#

Example: * 987654 # 63 #

10.6. ACOUSTIC AND VISUAL FEEDBACK

10.6.1.BUZZER ACTIVE

Enter administrator mode		
*	MASTER CODE	#

71 (factory setting)	#

Example: * 987654 # 71 #

10.6.2.BUZZER DEACTIVATED

Enter administrator mode		
*	MASTER CODE	#

70	#

Example: * 987654 # 70 #

10.6.3.LED ACTIVE

Enter administrator mode		
*	MASTER CODE	#

73 (factory setting)	#

Example: * 987654 # 73 #

10.6.4.LED DEACTIVATED

Enter administrator mode		
*	MASTER CODE	#

72	#

Example: * 987654 # 72 #

10.7. RESET TO FACTORY SETTINGS

The reset restores the controller 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 a card through the reader (the type of card must be recognisable by the connected 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.

10.8. DELETE ALL THE USERS

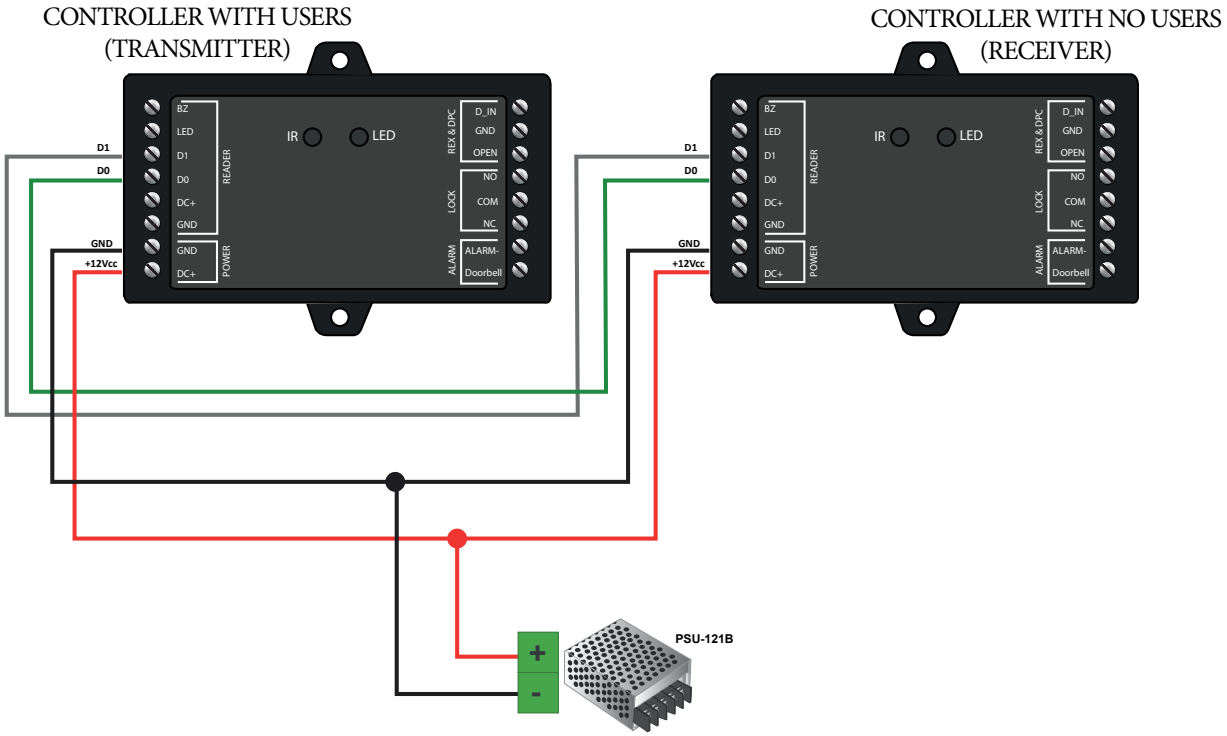
Enter administrator mode					
*	MASTER CODE	#	2	MASTER CODE	#

Example: * 987654 # 2 987654 #

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

11.TRANSFER USER INFORMATION

It is possible to transfer registered user information from one unit to another. To do this, make the following connection between controllers:



Then perform the following sequence on the controller that contains the registered users (transmitter):

Enter administrator mode				
*	MASTER CODE	#	98	#

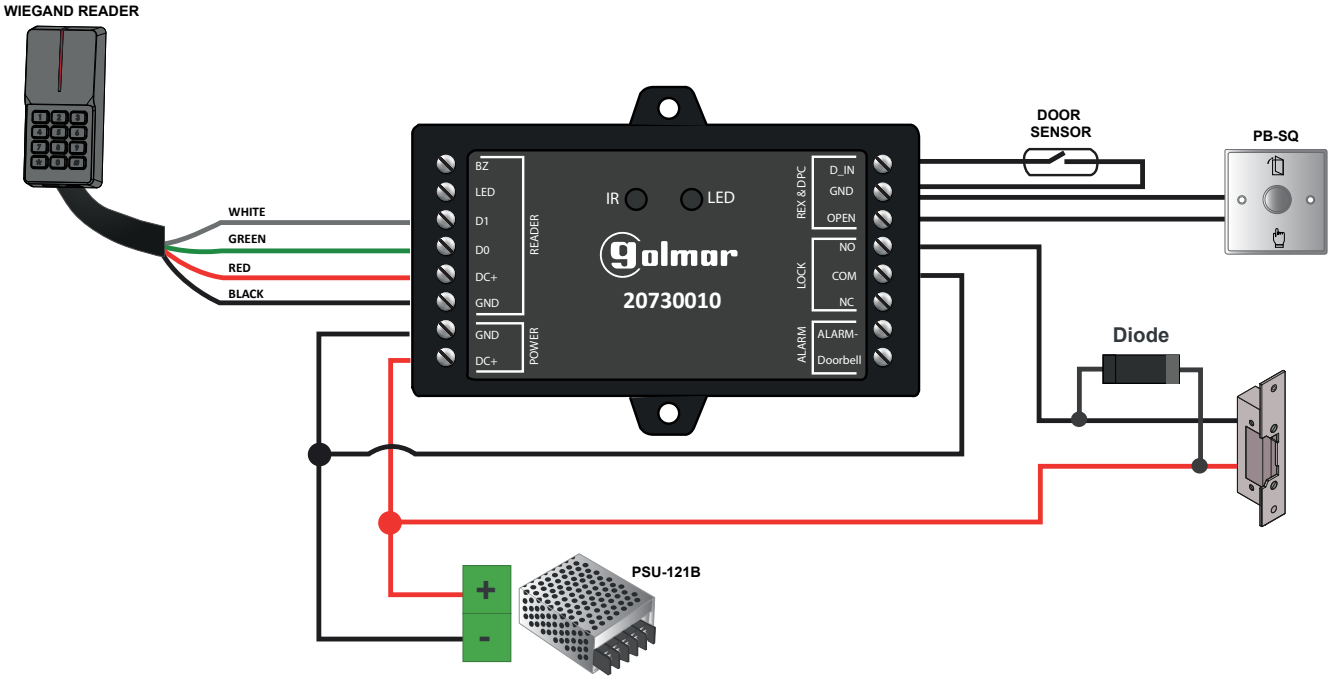
Example: * 987654 # 98 #

At an interval of 30 seconds, the green led flashes, after a beep, the led will turn red, which means that the user information has been transferred successfully. Once the transfer is completed press "*" or wait for the controller to return to the standby state.

IMPORTANT: The master code set in the sending and receiving controllers has to be the same. In case the receiving controller has registered users, these will be deleted.

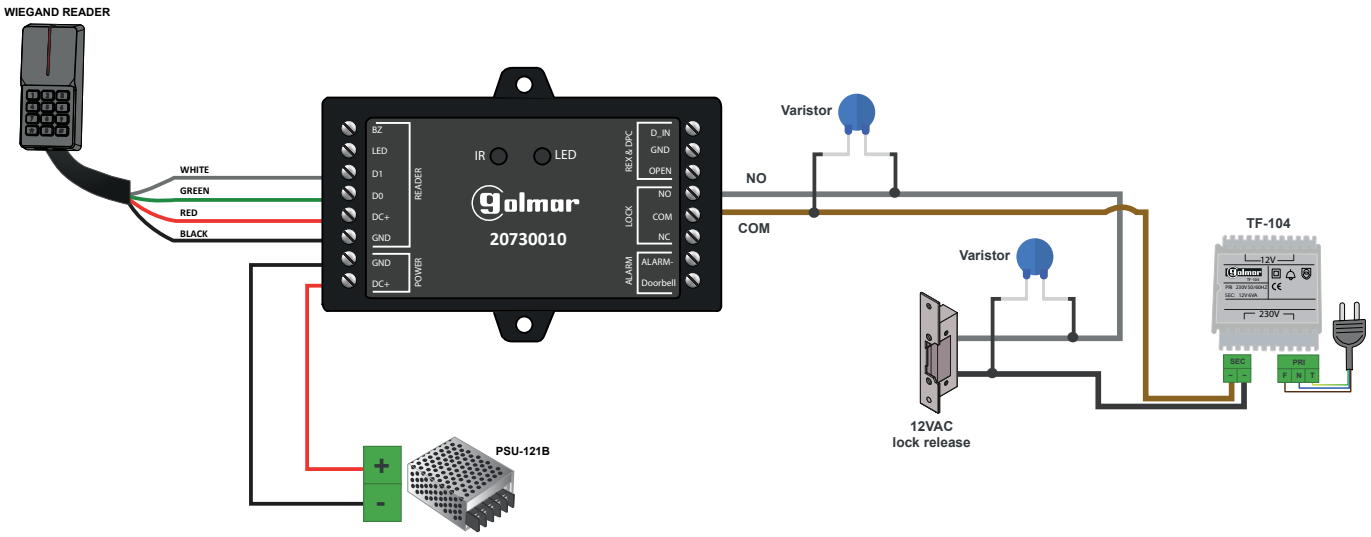
12.CONNECTION DIAGRAMS

12.1.CONNECTION DIAGRAM WITH DC LOCK RELEASE



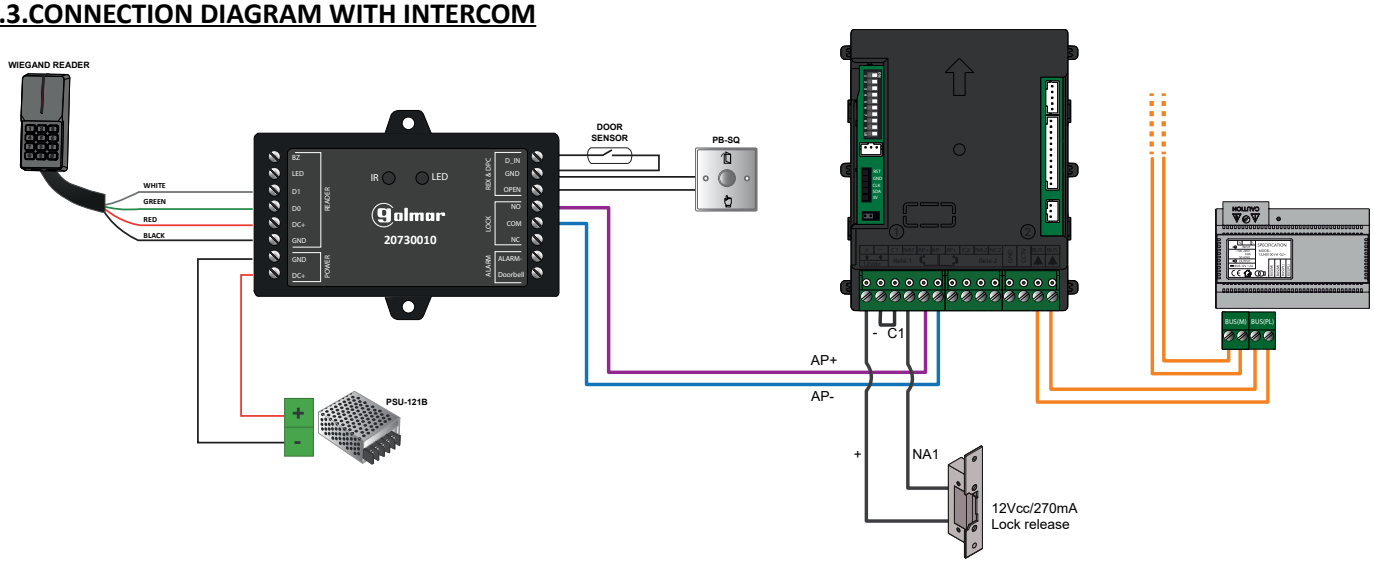
IMPORTANT: Do not forget to connect the supplied diode in parallel to the lock release to protect the equipment.

12.2.CONNECTION DIAGRAM WITH AC LOCK RELEASE



IMPORTANT: Golmar recommends using DC lock releases, as connecting an AC lock release may cause high voltage spikes that could damage the device or cause it to malfunction. However, in the event the AC lock release is used, protect the equipment by fitting a varistor to the relay contact output and another in parallel with the lock release.

12.3.CONNECTION DIAGRAM WITH INTERCOM

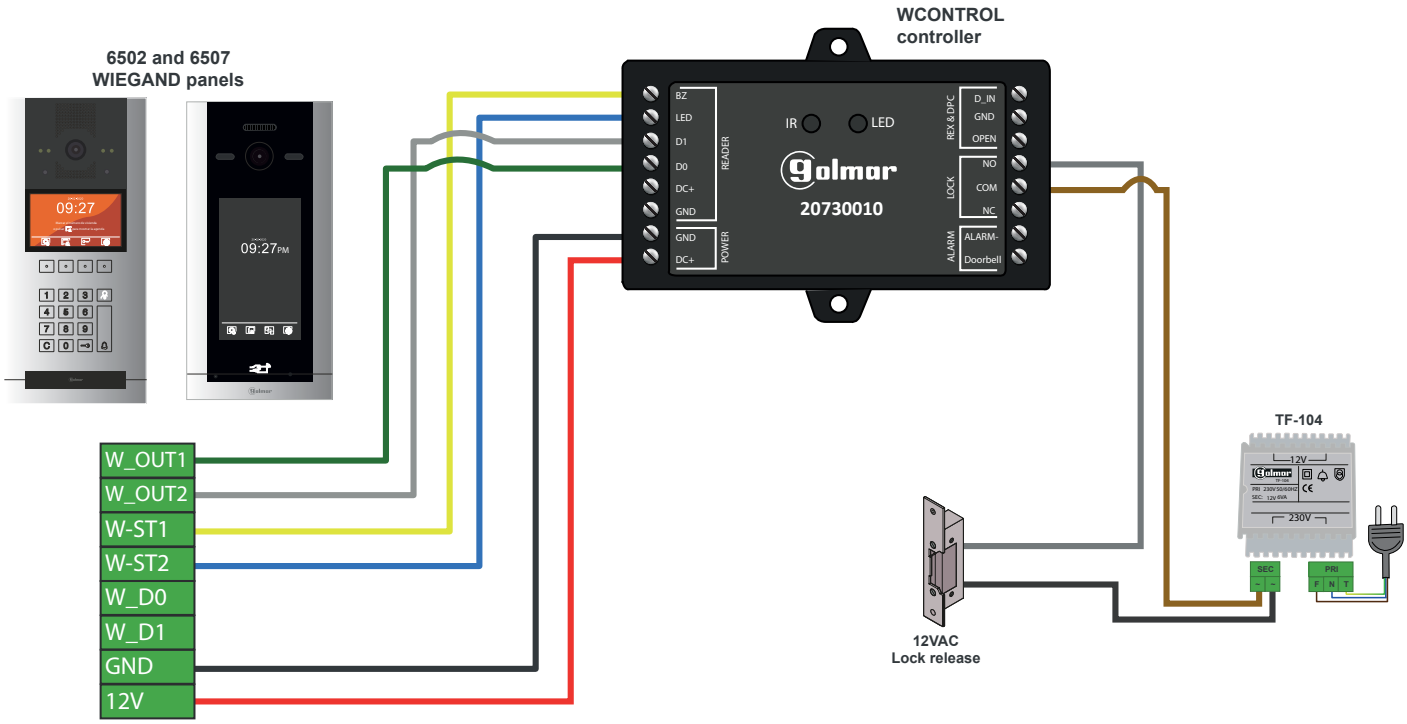


NOTE: The AP (door release) of the intercom does not activate the lock release until the pulse provided by the controller has finished. To avoid opening delays, set the minimum pulse time to 1 second at the controller:

Enter administrator mode					
*	MASTER CODE	#	3	1	#

12.4.CONNECTION DIAGRAM WITH SIXTY PANELS

It allows the management of proximity cards and PIN codes identifications with Wiegand technology in WCONTROL.



NOTE: It is advisable to connect W-ST1 and W-ST2 so that the "door open" warning is aligned with Wiegand operation.

13.ANNEX

13.1.SHARED DEVICE IS NOT DISPLAYED ON MAIN PAGE

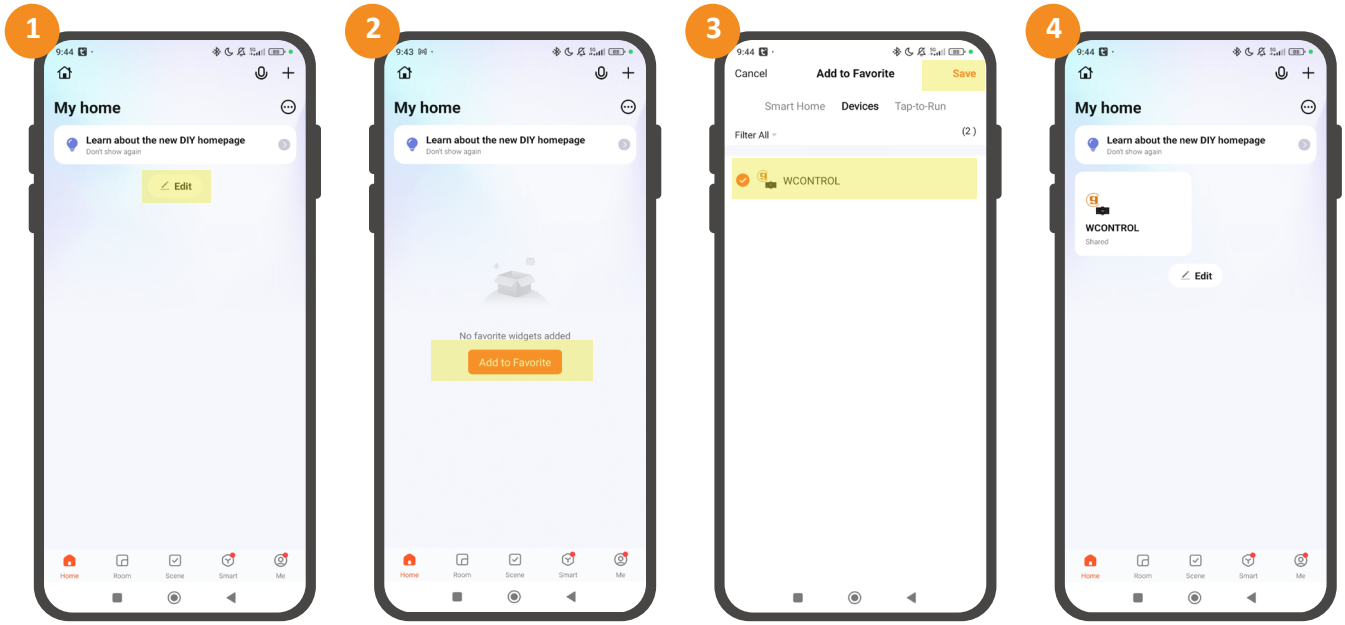
In some cases when the administrator shares the device with another user the application may not directly display the device on the guest user's home page. In this case the guest should proceed as shown below:

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

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

3 - Select the "WCONTROL" controller and then press on "Save".

4 - The controller will be added.



13.2.CONNECTIVITY WITH THE CONTROLLER

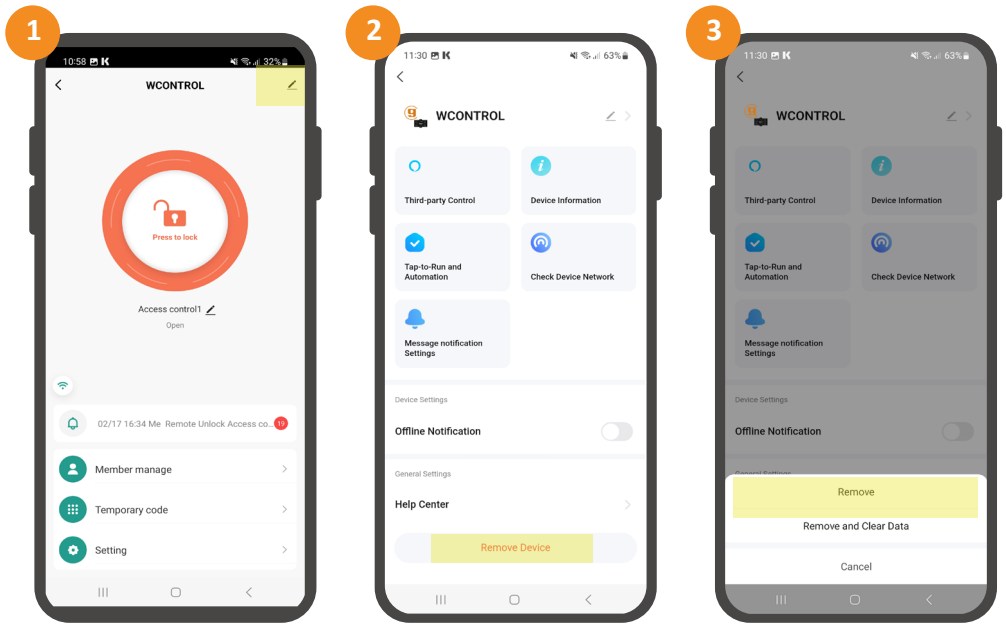
Below is indicated how to proceed in case of experiencing different connectivity cases:

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

* master code # 9 master code #

This will reset the controller´s connectivity. Remember that the WiFi network to which the controller must be connected must be 2.4GHz.

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 controller 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.

NOTES

NOTES

NOTES

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