golmar

BIO-N

INSTALLER MANUAL

IM_ENG_REV0122_BIO-N

1.INDEX

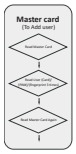
2.INTRODUCTION

Installation manual for BIO-N reader. Proximity and fingerprint reader for stand-alone and slave operation.

3.SPECIFICATIONS

Material	Stainless steel and black ABS plastic
Protection degree	IP-66
Input voltage	12/18Vdc
Current	Standby current: ≤ 30mA / Active: ≤ 120mA
Capacity	989 users (890 cards and 99 fingerprints)
Fingerprint reader	Resolution: 500DPI Id time: <1s FAR: <0.01% FRR: <0.1%
Reading frequency	EM 125KHz
Reading range	0-6cm
Relay	NO, NC, common 2A max.
Transmission format	Wiegand 26
Dimension (H x W x D):	Electronics: 48(W) x 62(H) x 25(D)mm. Electronics plus front cover: 86(W) x 86(H) x 25(D)mm
Working temperature range:	-25 ~60° C
Working humidity range:	0-98% (non-condensing)

4.PRODUCT CONTENT

		Diode.
		Fixing blocks.
		Screws.
		Screw cover labels.
		Remote control for programming.
		MASTER programming card.

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

5.INSTALLATION

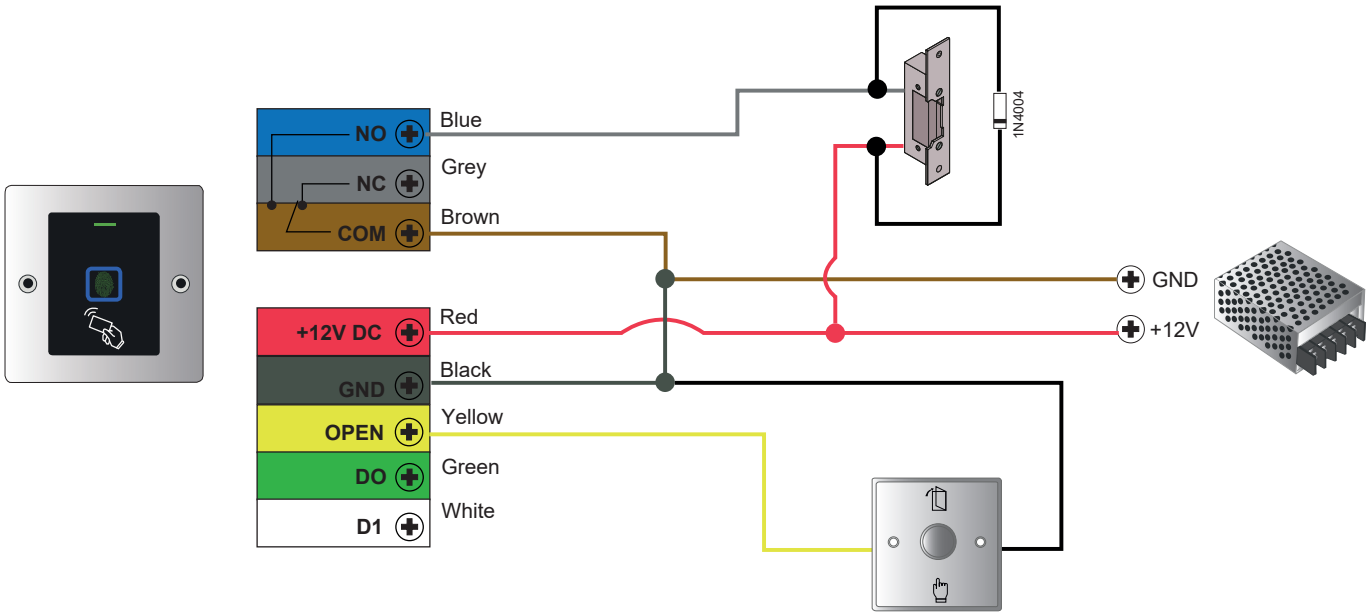
This reader is intended for mounting/integration in Nexa panels, which requires the use of an adapter module.
However, it can also be mounted independently on a specific embedding box (universal embedding box is not valid).

See chapter “14. TYPES OF INSTALLATION” to proceed.

6.CONNECTION

WIRE COLOUR	FUNCIÓN	DESCRIPCIÓN
Red	12Vdc	Input 12-18V DC current
Black	GND	GND
Blue	NO	Normally open relay output
Brown	Common	Common contact for relay output
Grey	NC	Normally closed relay output
Yellow	Opening	Exit pushbutton
Green	D0	Wiegand Data 0 output
White	D1	Wiegand Data 1 output

7.STANDALONE CONNECTION DIAGRAM



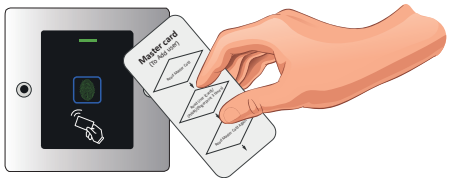
IMPORTANT: Do not forget to connect the supplied diode (1N4004) in parallel to the lock release to protect the equipment.

8.BASIC PROGRAMMING

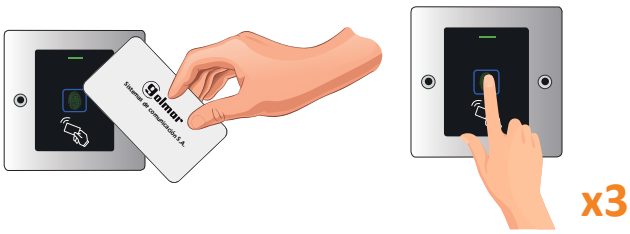
Basic programming (user registration/deletion) using the "Master Card" supplied with the product.

8.1. USER REGISTRATION

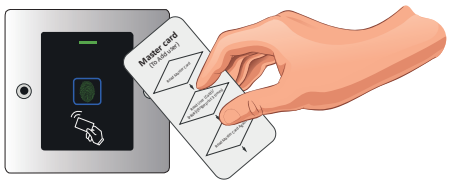
1) Approach the "Master Card" card to the reader.



2) Approach the card or fingerprint of the user to be registered.
*For the fingerprint, insert and remove your finger 3



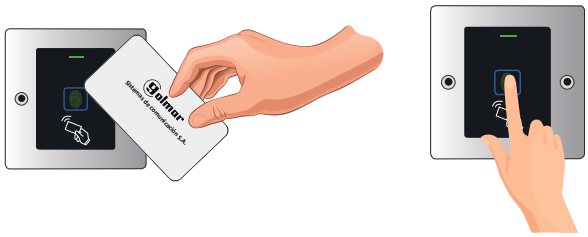
3) Approach the "Master Card" card to the reader.



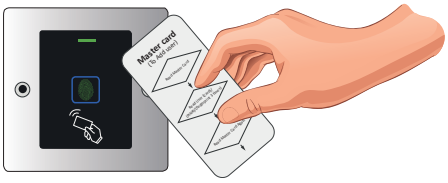
8.2. USER DELETION

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

2) Approach the card or fingerprint of the user to be deleted.



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



NOTE
In case of loss of the MASTER CARD you can create one by performing the process described in section "10.4.Reset to factory settings". This same process also allows you to create fingerprint as MASTER.

9.ADVANCED PROGRAMMING

For advanced programming it will be necessary to use 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 reader and pointing to the

9.1. PROGRAMMING

Perform the following sequence to enter programming:

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

IMPORTANT
The reader will indicate the access to programming with the "green" lighting up and then the flashing LED in "red" . At the start of the programming sequence (function to be programmed) the led will be "orange".
To exit programming, press "*" and the reader will go to standby, the status LED will be "steady red". If you do not press anything, after 30 seconds the reader will also automatically exit programming.

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

9.1.1.CHANGE MASTER CODE

It is highly recommended to modify the master code:

Enter administrator mode		
*	MASTER CODE	#

0	NEW MASTER CODE (6 DIGITS)	#

NEW MASTER CODE (6 DIGITS)	#

Example: * 123456 # 0 987654 # 987654 #

9.1.2.CARD REGISTRATION (AUTO ID)

Card registration with automatic registration.

Enter administrator mode				
*	MASTER CODE	#	1	APPROACH CARD

Example: * 987654 # 1 APPROACH CARD

9.1.3.CARD REGISTRATION (specific ID)

Maximum number of records is 890. User IDs from 100 to 989.

Enter administrator mode						
*	MASTER CODE	#	1	USER ID (100-989)	#	APPROACH CARD

Example: * 987654 # 1 1 # APPROACH CARD

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

9.1.4.FINGERPRINT REGISTRATION (AUTO ID)

PIN registration with automatic recording position.

Enter administrator mode				
*	MASTER CODE	#	1	FINGERPRINT (3 times)

Example: * 987654 # 1 ENTER FINGERPRINT x3

9.1.5.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)	#	FINGERPRINT (3 times)

Example: * 987654 # 1 1 # FINGERPRINT x3

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

9.1.6.FINGERPRINT DELETION (by fingerprint reading)

Fingerprint deletion by entering the fingerprint to be deleted.

Enter administrator mode				
*	MASTER CODE	#	2	FINGERPRINT

Example: * 987654 # 2 ENTER FINGERPRINT

9.1.7.CARD DELETION (by card reading)

Deletion of cards by approaching the card to be deleted.

Enter administrator mode				
*	MASTER CODE	#	2	APPROACH CARD

Example: * 987654 # 2 APPROACH CARD

9.1.8. FINGERPRINT OR CARD DELETION (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 #

10.OTHER SETTINGS

10.1. IDENTIFICATION MODE

10.1.1.IDENTIFICATION BY CARD OR FINGERPRINT (default value)

Enter administrator mode				
*	MASTER CODE	#	30	#

Example: * 987654 # 30 #

10.1.2.IDENTIFICATION BY FINGERPRINT ONLY

Enter administrator mode				
*	MASTER CODE	#	31	#

Example: * 987654 # 31 #

10.1.3.IDENTIFICATION BY CARD ONLY

Enter administrator mode				
*	MASTER CODE	#	32	#

Example: * 987654 # 32 #

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.
Default value: 51 (1 minute).

10.3. RELAY SETTINGS

10.3.1.PULSE MODE

Enter administrator mode					
*	MASTER CODE	#	4	1-99	#

Example: * 987654 # 4 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.
Default value: 5 seconds.

10.3.2.LATCHING MODE

Enter administrator mode					
*	MASTER CODE	#	4	0	#

Example: * 987654 # 4 0 #

The relay switches to ON/OFF mode.

10.4. LOCKOUT ALARM (FAILED ATTEMPTS)

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

10.4.1.LOCKOUT DISABLED (default value)

Enter administrator mode				
*	MASTER CODE	#	60	#

Example: * 987654 # 60 #

10.4.2.10-MINUTE ACCESS LOCKOUT

Enter administrator mode				
*	MASTER CODE	#	61	#

Example: * 987654 # 61 #

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

10.4.3.ALARM

Enter administrator mode				
*	MASTER CODE	#	62	#

Example: * 987654 # 62 #

In case a valid user card or MASTER card is approached, the alarm will stop.

10.4. RESET TO FACTORY DEFAULTS

The reset returns the reader to factory defaults. Restoring the configuration and the master code. User information will be kept.

1. Turn off the power.
2. Press and hold the exit button*.
3. Turn on the power.
4. When you hear 2 beeps, release the output button*.
5. The LED will light up yellow.
6. Approach a 125KHz card through the reader and a fingerprint 3 times.
7. The light will illuminate red and the equipment will be reset to factory defaults.

*Requires exit push button, yellow wire (OPEN) and black wire (GND) to be connected.

NOTE

- This process generates a MASTER card/fingerprint replacing the previous one.
- In case you do not wish to replace the current master card/fingerprint, press the * button instead of step 6 to finalise the reset.

10.5. DELETION OF ALL USERS

Enter administrator mode					
*	MASTER CODE	#	2	0000	#

Example: * 987654 # 2 0000 #

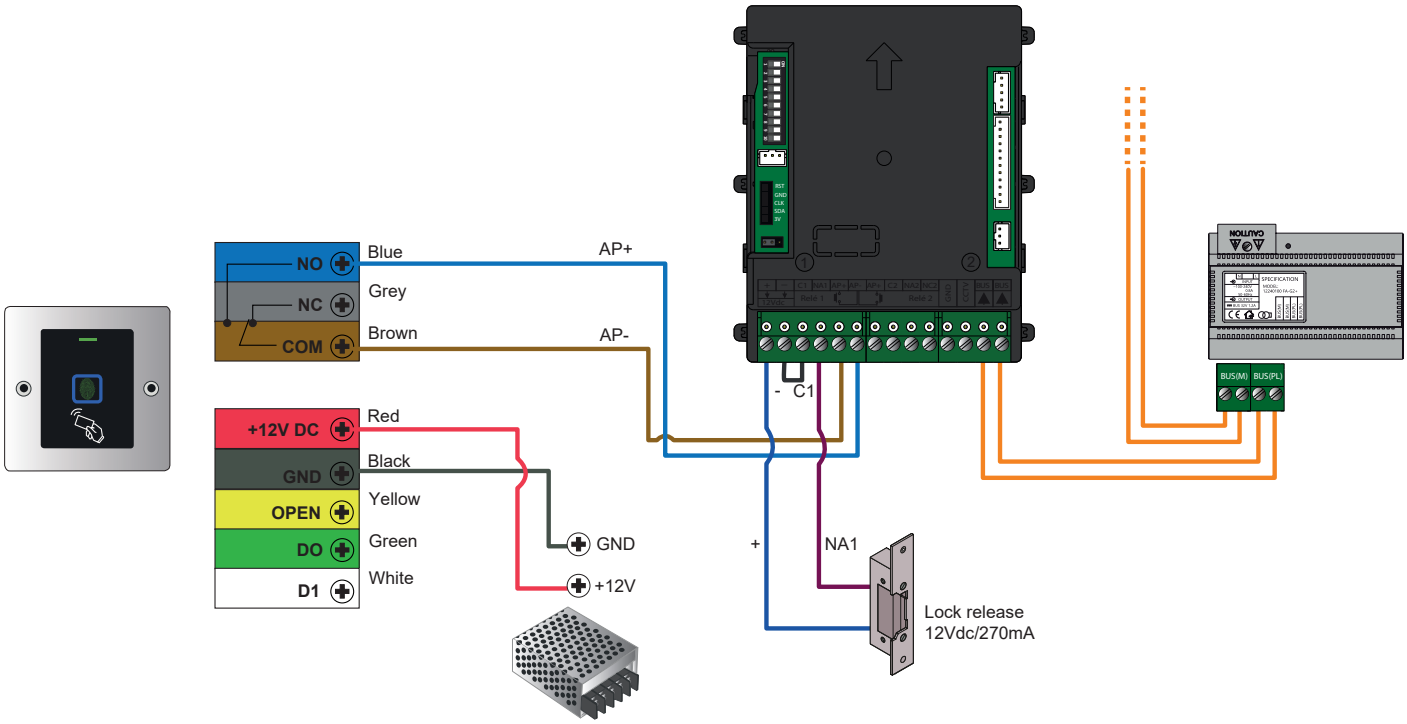
IMPORTANT:

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

11.STATUS DISPLAYS

OPERATION 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.CONNECTION DIAGRAM WITH VIDEO DOOR SYSTEM



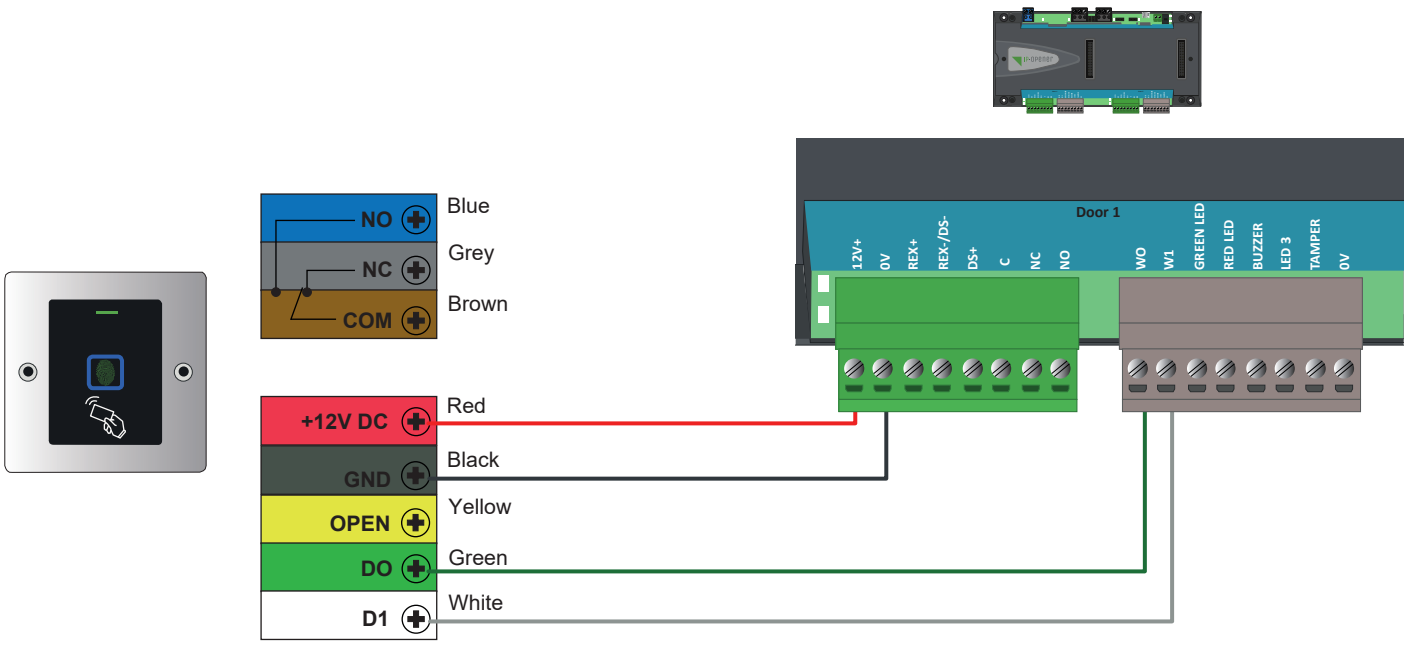
NOTE: The door opener (AP) does not activate the lock release until the pulse on the BIO-N reader has been finished. To avoid opening delays set the minimum pulse time to 1 second at the reader:

Enter administrator mode					
*	MASTER CODE	#	4	1	#

13.WIEGAND

The following chapter describes how to use the BIO-N reader in an iP Opener system with a Wiegand controller.

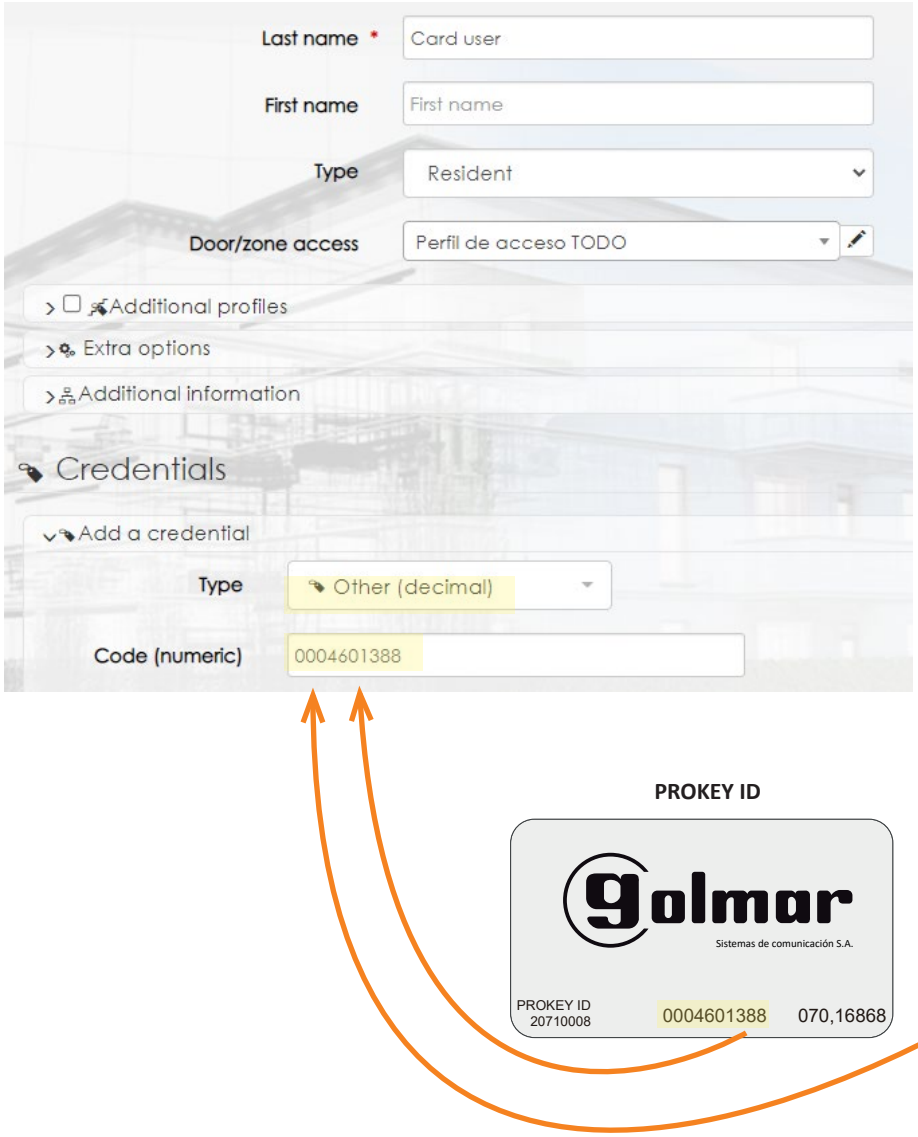
13.1. CONNECTION DIAGRAM



13.2. PROGRAMMING

13.2.1.PROGRAMMING CARD

Generate a user with credential type “Other (decimal)” and enter in the field “code” the ID of the card or key fob:



At this point the card or key fob will be registered in iP Opener and the access will be granted:

Fecha / Hora	Evento	Elemento	Informaciones	Dirección de la persona	Grupo	Login
2022-06-28 12:31:30	Acceso autorizado	2P WIEGAND - Puerta 0001 Lector 0001 Secu	Usuario Tarjeta	--	--	0004601388

Fecha / Hora	Evento	Elemento	Informaciones	Dirección de la persona	Grupo	Login
2022-06-28 12:32:24	Acceso autorizado	2P WIEGAND - Puerta 0001 Lector 0001 Secu	Usuario Llavero	--	--	0009701804

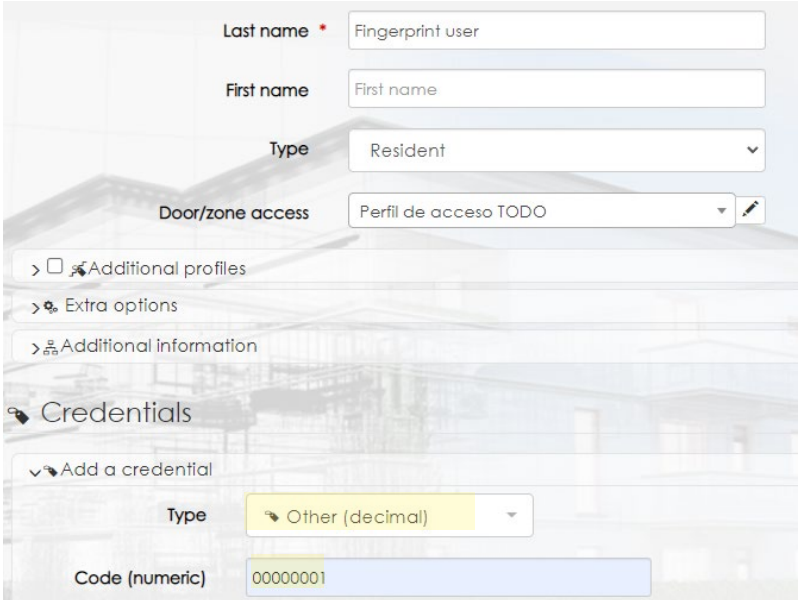
13.2.2.PROGRAMMING FINGERPRINT

Register the fingerprint in the reader:

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

Example: * 987654 # 1 1 # FINGERPRINT x3

NOTE
Do not use ID 0. Register in this case the fingerprint from ID 1 (ID 1 to 98, ID 0 is not interpreted by iP Opener).
Generate a user with credential type "Other (decimal)" and with the user ID value registered in the reader:



At this point the fingerprint will be registered in iP Opener and the access will be granted:

Fecha / Hora	Evento	Elemento	Informaciones	Login
2021-12-28 15:55:36	Acceso autorizado	2P WIEG - Puerta 0002 Lector 0002 Perfil de acceso TODO	Usuario huella	00000001

IMPORTANT
- The value to be entered in decimal must contain 8 digits. For this reason, the value 00000001 has been registered in this case.
- The reader can register 99 fingerprints (ID 1 - 98).
- For a correct management/use of the users, follow the programming dynamics described in the following table:

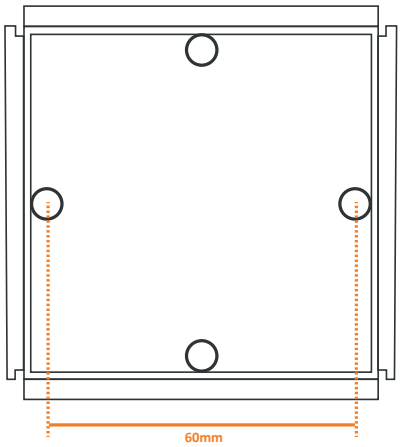
FINGERPRINT USER ID	iP OPENER CODE (Other decimal)
1	00000001
2	00000002
...	...
97	00000097
98	00000098

NOTE
The use of the reader integrated in the iP Opener system implies the loss of the buzzer and led states (there will be no visual and audible confirmation on the reader of validated or denied accesses).

14.TYPES OF INSTALLATION

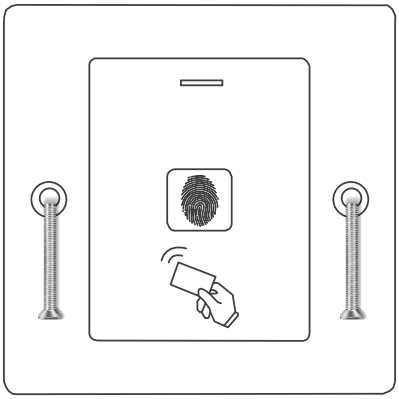
14.1. STAND-ALONE INSTALLATION

As briefly mentioned in section "5.INSTALLATION", the installation of these readers is designed to be integrated in Nexa panels. However, you can choose to install the reader independently on a embedding box. In this case, follow the steps below:



1

Place a embedding box AP-1 (20363401).



2

Attach the reader to the box with the metric screws supplied. Then cover the screws with the supplied screw cover labels.

IMPORTANTE: The reader incorporates an anti-tamper LDR sensor on the back of the reader  .
It is light-sensitive, so if light shines on the sensor after placing the reader, the tamper alarm will be triggered.

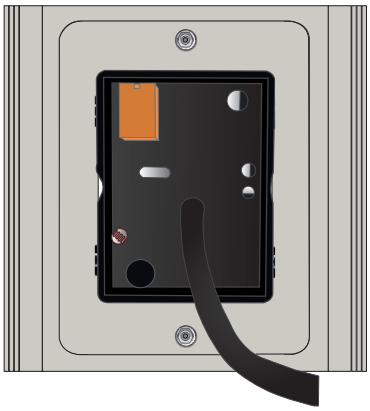
14.2. INSTALLATION ON NEXA PANEL

The integration of the reader on the Nexa panel requires the use of the reader in kit format:

N3000/BIO-N (20700015), kit for BIO-N reader mounting on Nexa Aluminium.
NX3000/BIO-N (20700016), kit for BIO-N reader mounting on Nexa Inox.

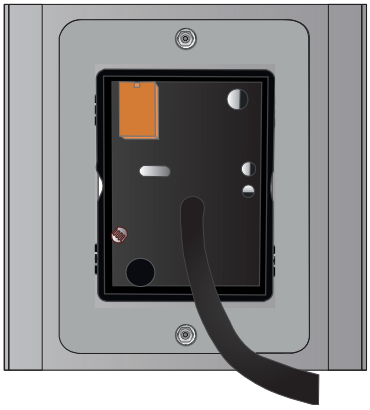
Due to the fact that the kit is supplied with the reader assembled in a special Nexa cover:

Front view of Nexa Aluminium cover panel with reader



Back view of Nexa Aluminium cover panel with reader

Front view of Nexa Inox cover panel with reader



Back view of Nexa Inox cover panel with reader

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-seguridad.es