BIO100

Installer manual

Table of contents

1 Description

BIO100 is a Wiegand biometric reader for access control applications. It offers storage up to 100 fingerprints and programable Wiegand Output (8 to 128 bits).

Configuration of the readers and fingerprint enrollment is done through CONTROL PC Software.

Connection between the biometric readers is RS485 and it is used for fingerprint transfer and configuration.

The tamper switch output can trigger the alarm system, if an attempt is made to open or remove the unit from the wall.

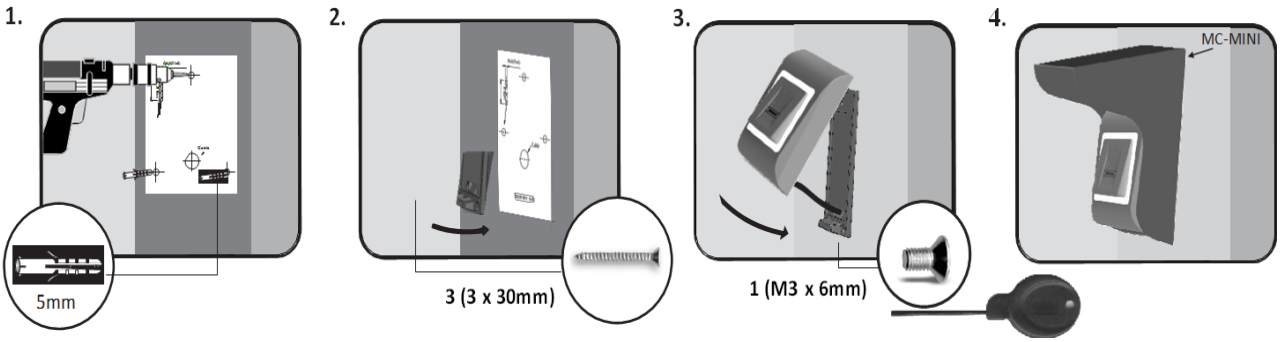
The sensor incorporates dedicated sensing hardware to facilitate the detection of “spoofing” attacks based on fake fingers. This data is embedded into the image data stream, and is processed on the processor. The system is capable of detecting and defeating well-known fake finger mechanisms, such as molded “gummy” fingers.

The coating on the surface of the TouchChip sensor provides protection from scratching and abrasion due to normal contact with fingertips and any incidental contact with fingernails.

2 Specifications

Fingerprint capacity	up to 100 fingerprints
Technology	Biometry (capacitive sliding sensor)
Use	internal
Authentication	Finger
Interface	Wiegand de 8 a 128 bits (26 bits por defecto)
Protocol programming	By CONTROL software
Max. wires length	50m
1:1000 identification time	970 msec, including feature extraction time
Fingerprint enrolment	On the reader or from the USB desktop reader
Panel connection	Wires, 1m
Green and Red LED	Externally Controlled
Orange LED	Idle mode
Buzzer ON/OFF	Yes
Backlight ON/OFF	Yes
Manual control	Yes
Consumption	100mA
IP Rating	IP65
Power supply	9-14VDC
Operating Temperature	-20°C to +50°C
Dimensions (mm)	80 x 80 x 9
Storage/Operating Humidity	5% to 93% RH without condensation

3 Mounting



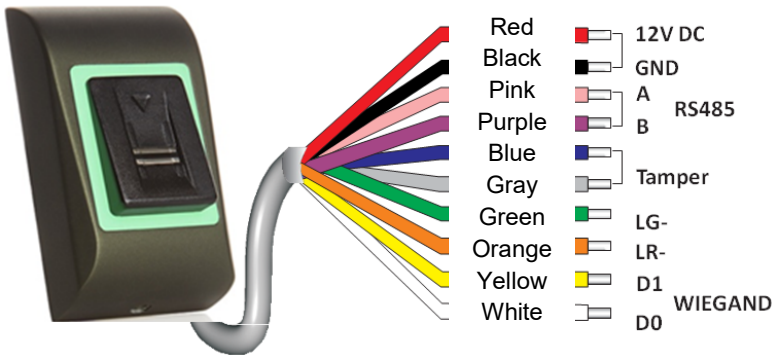
If the biometric reader is installed and used outdoor, the reader MUST be fitted with the MC-MINI metal cover available in our accessories in order to protect the sensor from direct rainfall. The operating temperature of the product is between -20ºC - + 50ºC.

If the reader is installed in an environment where the temperature can drop below -10ºC or/and if the sensor could only be exposed to direct sunlight, it is strongly recommended to install the reader inside a third party sealed wall mount box (fitted with additional heater if very low temperature) to keep a constant sensor level performance.

JCM cannot guarantee the functionality of the product if measures and advice before are not followed.

It is also strongly recommended to use double technology biometric readers when use outdoor to offer first higher security but also the possibility to use different readers depending on users.

4 Wiring

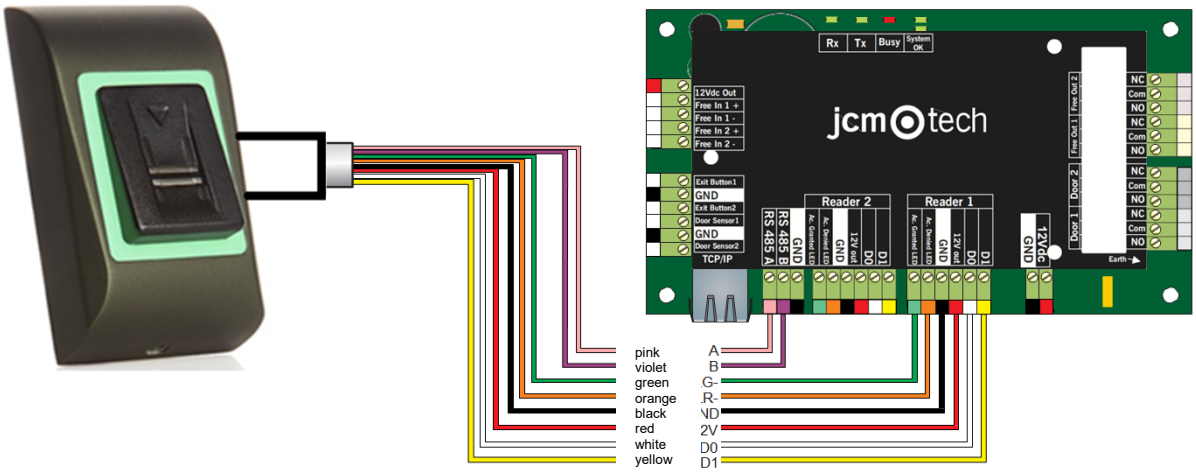


12V DC	9-14V DC
GND	ground
A	RS485 A
B	RS485 B
LR-	Red LED -
LG-	Green LED -
D1	Data 1
D0	Data 0
Tamper	Tamper Switch(NO)
Tamper	Tamper Switch(NO)

5 Connecting to C2P controller

The Biometric readers can't work independently. They must be connected to virtually a C2P controller by the Wiegand inputs (standard 26bit or self-defined).

- The lines D0 and D1 are the Wiegand lines and the Wiegand Number is sent through them.
- The RS485 line (A, B) is used for fingerprint transfer and reader settings.
- The Biometric readers must be powered from the controller.
- If you use different power supply for the biometric reader, connect the GND from the both devices to ensure correct transfer of the wiegand signal.
- When you have connected the reader and powered on, the LED should flash in orange light + 2 beeps. This lets you know it's on and ready for use.
- Fingerprint enrollment is done from the PC Software. Connection between the Biometric readers and the PC must be established.

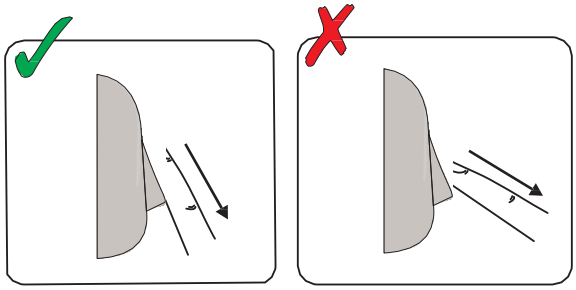


- If the distance Reader-Controller is high (50meters) and if the communication with the reader can not be established, then terminate the RS485 network by closing the jumper in the C2P Controller or as described in chapter 4.

6 Enrollment

Follow the below instructions for correct finger swiping.

Starting from the first finger joint, place the selected finger on the swipe sensor and move it evenly towards oneself in one steady movement.



Result:

- **For a valid swipe:** Tricolour Status LED turns green + OK Beep(short + long beep)
- **For an invalid or misread swipe:** Tricolour Status LED turns red + Error Beep (3 short beeps)

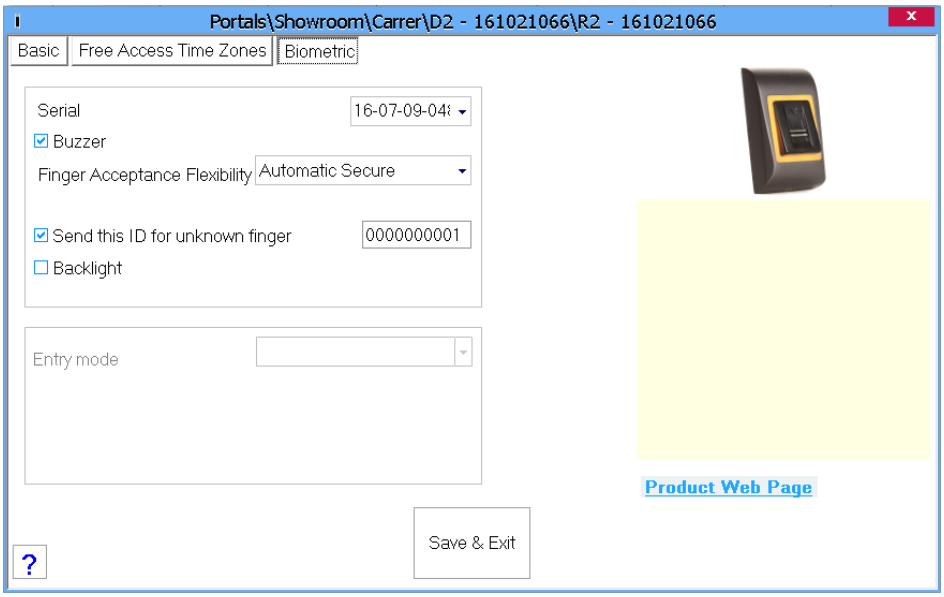
7 Configurating in Control software

7.1 Adding biometric reader

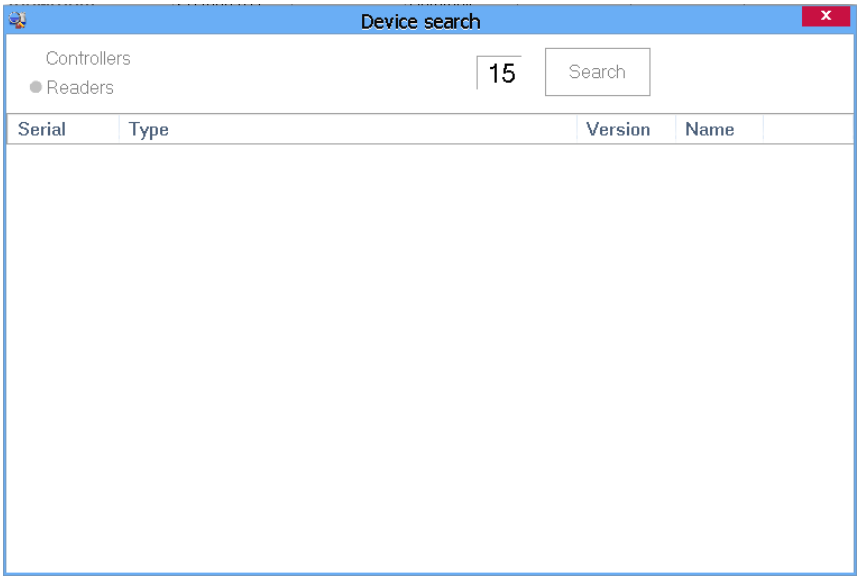
1. Expand the Door item to view the readers
2. Right click on the reader and select properties

3. In the Basic tab, for “Type” of the Reader select “BIO100”.

4. After selecting the type, a third tab will appear “Biometric”. Go to that tab and put the serial number of the Biometric Reader.



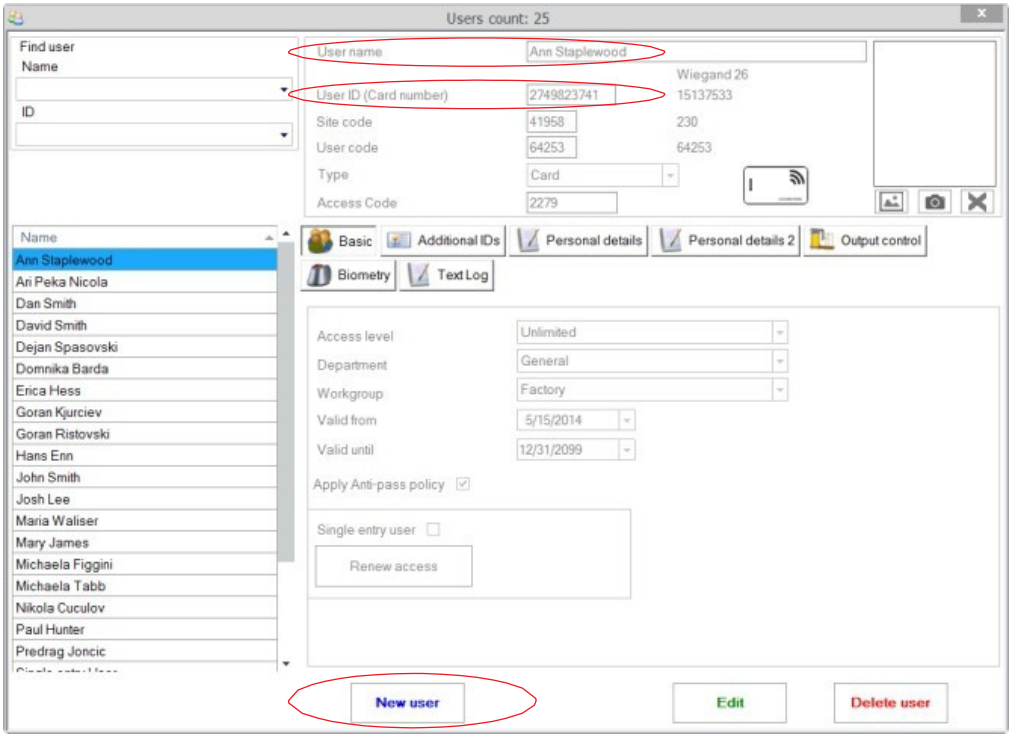
Important Note: The serial number of the reader can be found on a sticker inside the reader, on the packaging box and it can be search from the software (right click on the portal/search devices/readers).



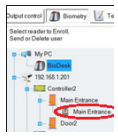
To check if the reader is On Line, right click on the reader and select “Check version”. In the Event Window a message should appear “Device ON Line, Type: BIO100”

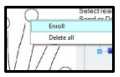
7.2 Enrolling fingerprints from a reader

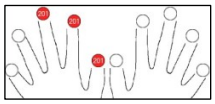
1. Open the Users Window and create a new user. Click on “New User”, put a name and ID(card number).



2. Go to the “Biometric” Tab. Select the reader (with left click) from which the enrollment will be done.
3. Right click on the fingertip and select enroll.
4. In the next 25 seconds, physically swipe the finger on the selected reader minimum 5 times and the finger tip will turn red; the fingertip in the screen will become red, indicating the register percentage, while the reader will blink in orange.





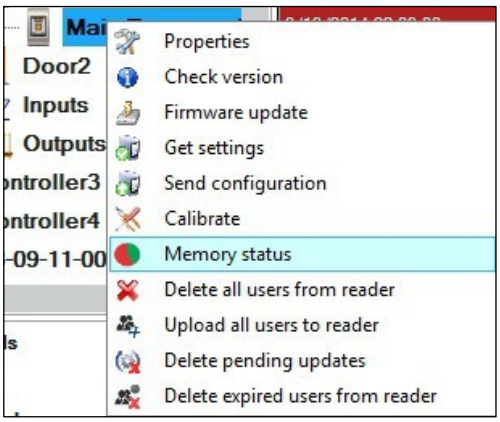


5. Repeat points 3 & 4 for each finger that should be enrolled.
6. Click on “Save New” and the fingerprint will be sent automatically to all Biometric Readers where that user has access, i.e. to all the readers according to the Access Level assign to that user.

Example:

If the user has “Unlimited” Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

Note: To check if all the fingerprints are sent to the reader, right click on the reader and select “Memory Status”.



In the event window a line will appear indicating the number of fingerprints stored in the reader.

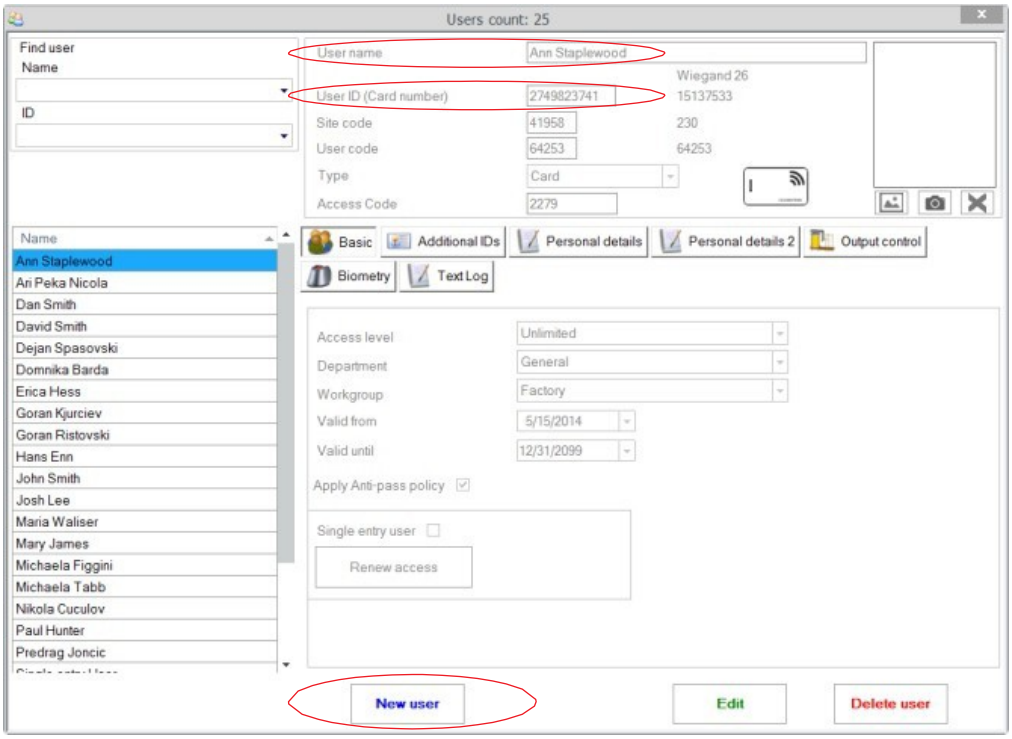
Reader	Door	Event
BIO100		Enrolled fingers : 3

Note: If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).

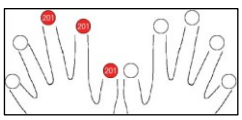
7.3 Enrolling fingerprints from desktop readers

Plug the Swipe Desktop Reader in the PC. If the device is not installed automatically use the drivers located on the CD provided with the Biometric reader. It is installed in the same way as a USB Device. When the desktop reader has been installed it will automatically appear in the Software.

1. Open the Users Window and create a new user. Click on “New User”, put a name and ID (card number).



2. Go to the “Biometric” Tab and select the USB Swipe desktop Reader (with left click).
3. Right click on the fingertip and select Enroll.
4. In the next 25 seconds, physically swipe the finger on the selected reader minimum 5 times and the finger tip will turn red; the fingertip in the screen will become red, indicating the register percentage, while the reader will blink in orange.



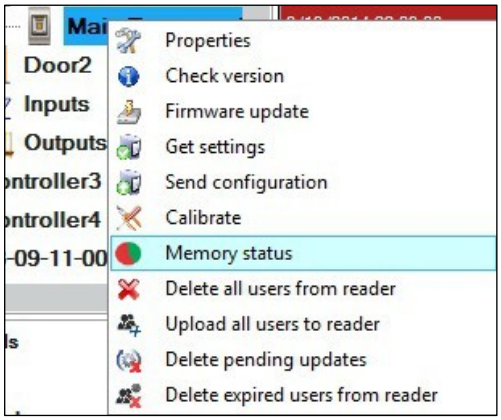
5. Repeat points 3 & 4 for each finger that should be enrolled.
6. Click on “Save New” and the fingerprint will be sent automatically to all Biometric Readers where that user has access, i.e. to all the readers according to the Access Level assign to that user.

If the reader is offline, fingers will be sent when the connection between CONTROL server and the readers is established. No further registration or action is required. Fingerprints will be sent as soon as the communication is established.

Example:

If the user has “Unlimited” Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

Note: To check if all the fingerprints are sent to the reader, right click on the reader and select “Memory Status”.



In the event window a line will appear indicating the number of fingerprints stored in the reader.

Reader	Door	Event
BIO100		Enrolled fingers : 3

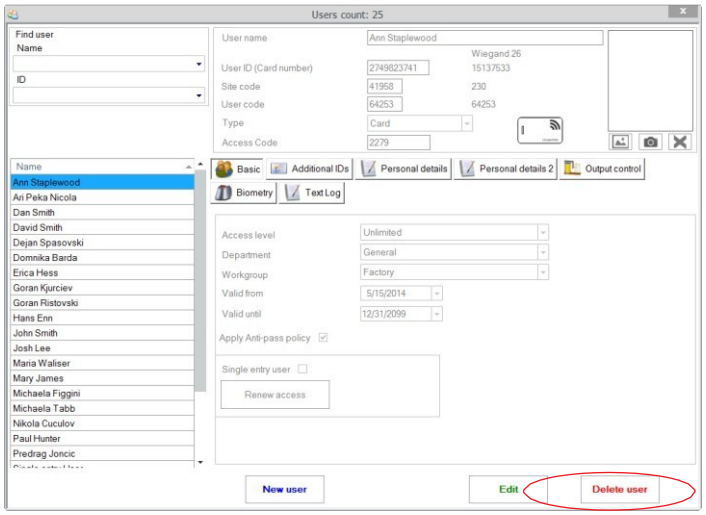
Note: If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID (card Number).

7.4 Deleting fingerprints

In general, the fingerprints are stored in the Biometric reader and in the Software. Deleting can be done only in the readers or from both places.

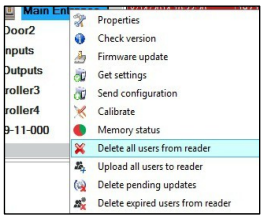
Deleting one user from the biometric reader

Select the User and click on “Delete User”. The User together with its fingerprints will be deleted from both the software and the fingerprint readers.



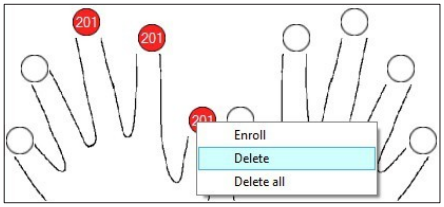
Deleting all users from the biometric reader

Right click on the reader and select “Delete all users from reader”.



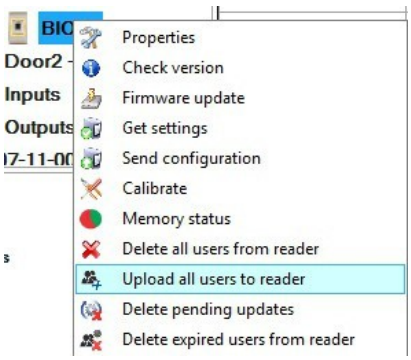
Deleting one or more fingerprints

Select the User and open the “Biometric” tab. Go to the fingertip that needs to be deleted, right click and select ”Delete” for one finger or “Delete All” for all fingers of the User. Click “Save Changes”.



7.5 Uploading the fingerprints to the biometric readers

Right click on the biometric reader and select “Upload all users to reader”.



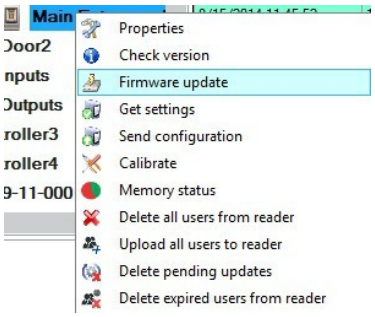
While receiving the fingerprints the reader will blink in orange.

Nota: Use this feature when you change or add a reader, if pending tasks are deleted in the software or if there are doubts that fingerprints in the reader memory are not synchronized with the software database.

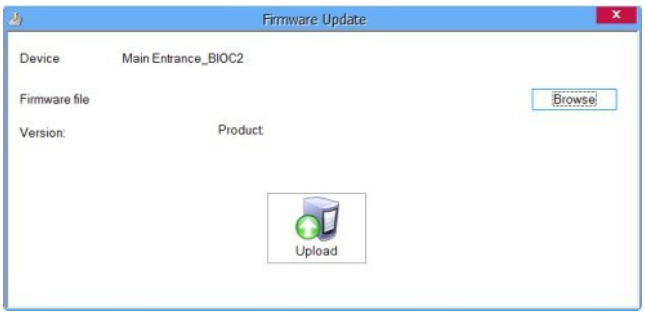
In normal usage, the fingerprints are sent automatically and this feature is not used.

7.6 Firmware update

Right-click on the reader and select Firmware update menu.

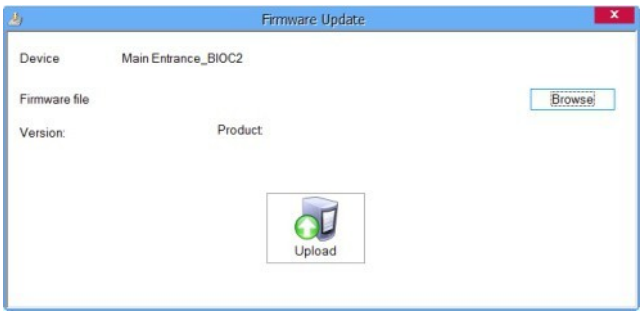


On the Firmware update window, click on the Browse button.



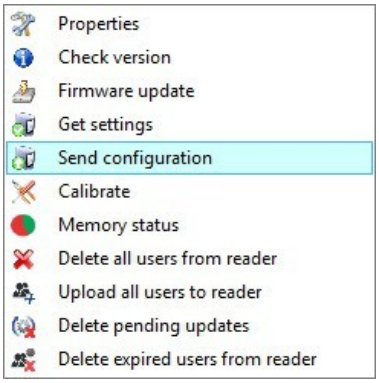
The default location of the firmware files installed with CONTROL is in the folder "Firmware". Select the firmware file with a "xhc" extension. Click on the Upload button.

Important: Wait for the update end message. Do not turn off the reader, the software or any communication device in between during the entire process.



7.7 Send configuration to a receiver

Right-click on the reader and select the Send configuration menu.



See the events panel to check the configuration flow.

Note: The biometric reader gets its settings automatically. This function is used if the reader was off line while making the changes.

7.8 Advanced settings

Send ID for Unknown Finger: sends the desired ID when an unknown finger is applied.

Backlight: ON or OFF

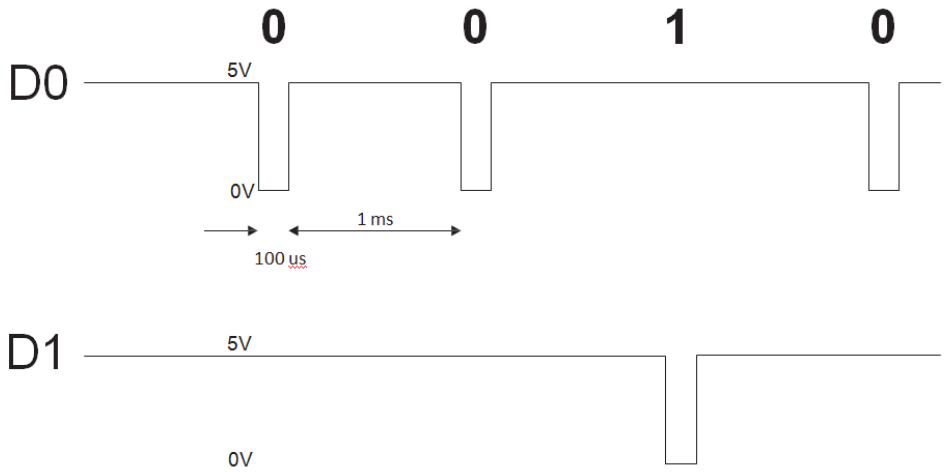
Buzzer: ON or OFF

Finger Acceptance Flexibility: Accepted tolerance. The recommended value is “Automatic Secure”.

8 Wiegand protocol description

The data is sent over the lines DATA 0 for the logic “0” and DATA 1 for the logic “1”. Both lines use inverted logic, meaning that a pulse low on DATA 0 indicates a “0” and a pulse low on DATA 1 indicates a “1”.When the lines are high, no data is being sent. Only 1 of the 2 lines (DATA 0 / DATA 1) can pulse at the same time.

Example: data 0010...

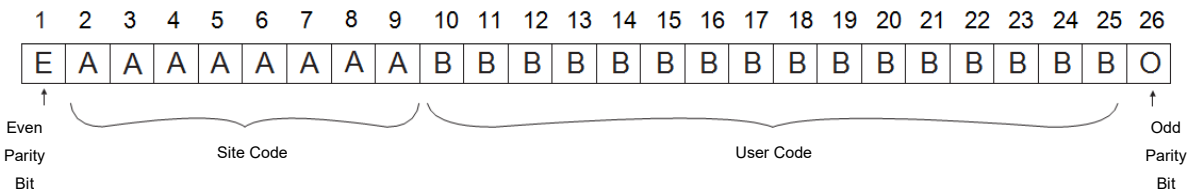


Data bit 0 = approximately 100 us (microseconds)
Data bit 1 = approximately 100 us (microseconds)

Time between two data bits: approximately 1 ms (millisecond). Both data lines (D0 and D1) are high.

Description for the 26 bits Wiegand format

Each data block consists of a first parity bit P1, a fixed 8 bits header, 16 bits of user code and a 2nd parity bit P2. Such a data block is shown bellow:



Note: Parity bits are calculated as follows:

P1 = even parity calculated over the bits 2 to 13
P2 = odd parity calculated over the bits 14 to 25

Ejemplo:	170	31527	
PP	**Site code**	**User code**	**PI**
1	**10101010**	**01111011 00100111**	0

9 Safety instructions

- Do not install the device in a place subject to direct sun light without protective cover.
- Do not install the device and cabling closeto a source of strongelectro-magnetic fieldslike radio-transmitting antenna. Do not placethe device near or above heating equipments.
- If cleaning,do not spray or splash water or other cleaning liquids but wipe it out with smooth cloth or towel.
- Do not let children touch the device without supervision.
- Note that if the sensor is cleaned by detergent,benzene or thinner,the surface will be da maged and the fingerprint can't be entered.

10 Regulatory data

Use of the system

This equipment is designed for applications with automated garage door. It is not guaranteed for the direct activation of devices other than those specified.

The manufacturer reserves the right to change the equipment specifications without prior notice.

11 UE Declaration of conformity

JCM Technologies S.A., hereby declares that the product BIO100 complies with the relevant fundamental requirements of the Directives 2014/30/EU on electromagnetic compatibility and with the 2011/65/EU RoHS Directive, as long as its use is foreseen.

See web page www.jcm-tech.com/es/declaraciones

JCM TECHNOLOGIES, SA
BISBE MORGADES, 46 BAIXOS
08500 VIC (BARCELONA)
ESPAÑA