

BIO9500

Installer manual



Contents

1. DESCRIPTION	3
2. SPECIFICATIONS	4
3. MOUNTING.....	5
4. WIRING.....	5
5. CONNECTING TO C2P CONTROLLER	6
6. ENROLLMENT	7
7. CONFIGURATING THE CONTROL SOFTWARE.....	8
7.1 ADDING BIOMETRIC READER.....	8
7.2 ENROLLING FINGERPRINTS FROM A READER	10
7.3 ENROLLING FINGERPRINTS FROM A DESKTOP READER	12
7.4 DELETING FINGERPRINTS	14
7.5 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS	15
7.6 FIRMWARE UPDATE.....	16
7.7 SENSOR CALIBRATION	16
7.8 SEND CONFIGURATION TO A RECEIVER	17
7.9 ADVANCED SETTINGS.....	17
8. WIEGAND PROTOCOL DESCRIPTION	18
9. SAFETY INSTRUCTIONS	19
10. TROUBLESHOOTING.....	19
11. REGULATORY DATA	20
12. UE DECLARATION OF CONFORMITY	20

1 Description

BIO9500 is a biometric reader for indoor access control applications. It offers storage up to 9500 fingerprints and programmable Wiegand output (8 to 128 bits).

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

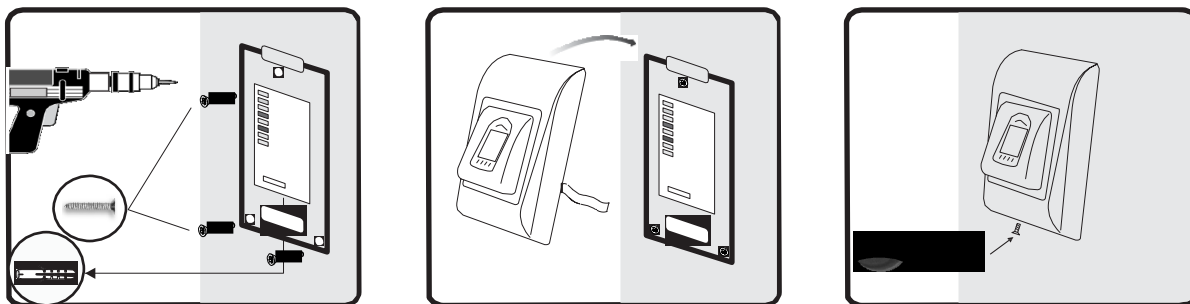
Connection between the biometric readers is RS485 and it is used for fingerprint transfer and configuration.

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

2 Specifications

Fingerprint capacity	up to 9500 fingerprints
Technology	Biometry (capacitive sensor)
Use	Indoor
Authentication	Finger
Interface	Wiegand 8 to 128 bits; Default: Wiegand 26bit
Protocol programming	By CONTROL software
Maximum cable distance	50m
1:1000 identification time	970 msec, including feature extraction time
Fingerprint enrolment	On the reader or from the USB desktop reader (BIOE)
Panel Connection	Wires, 1m
Green and Red LED	Externally Controlled
Orange LED	Idle mode
Buzzer	Yes
Backlight ON/OFF	Yes
Control manual	Manual control
Consumption	100mA
IP Rating	IP54
Power supply	9-14VDC
Operating Temperature	0°C to +40°C
Dimensions (mm)	92 x 51 x 25
Housing	Moulded Aluminium

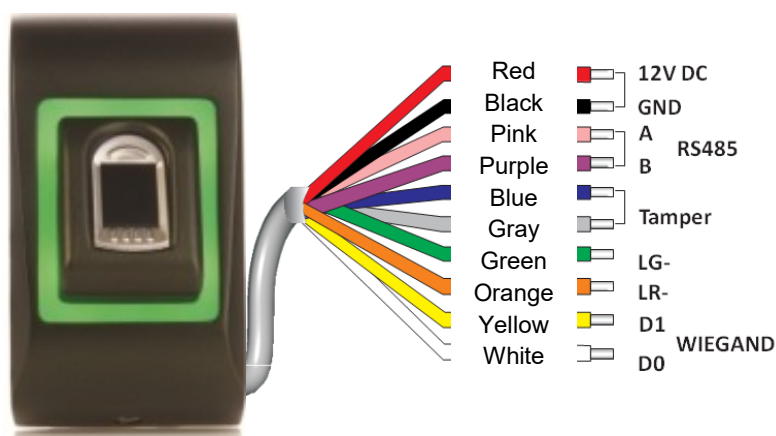
3 Mounting



If the reader is installed in an environment where the temperature may drop below 0°C and /or if the sensor can only be exposed to direct sunlight, it is strongly recommended that it be installed inside a sealed wall-mounted enclosure (equipped with additional heating in case of a very low temperature) to maintain its level of performance constant.

JCM can not guarantee the functionality of the product if the measures and the advice given are not respected.

4 Wiring

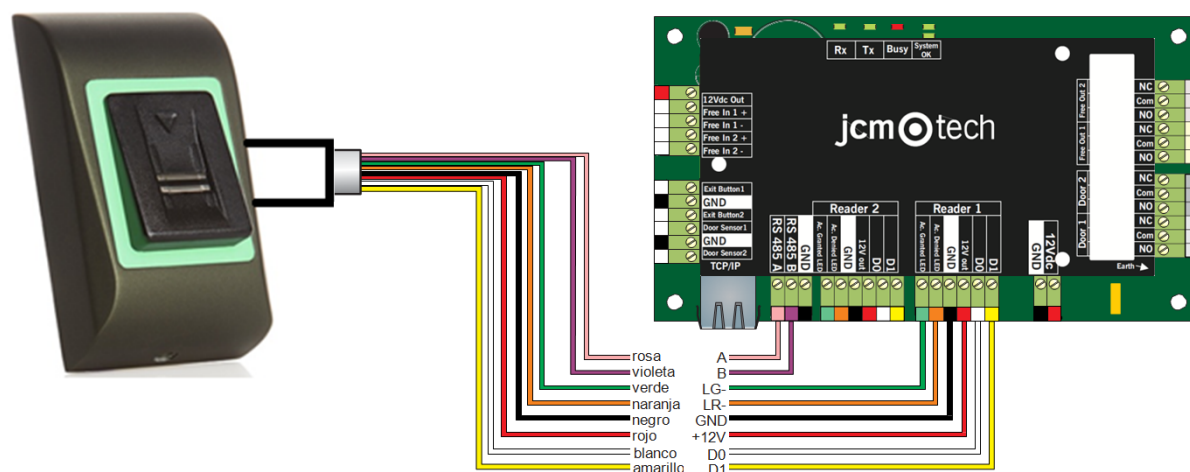


12V DC	9-14V DC
GND	ground
A	RS485 A
B	RS485 B
LR-	Red LED -
LG-	Green LED -
D1	Data 1
D0	Data 0
Tamper	Tamper Switch(NO)
Tamper	Tamper Switch(NO)

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).

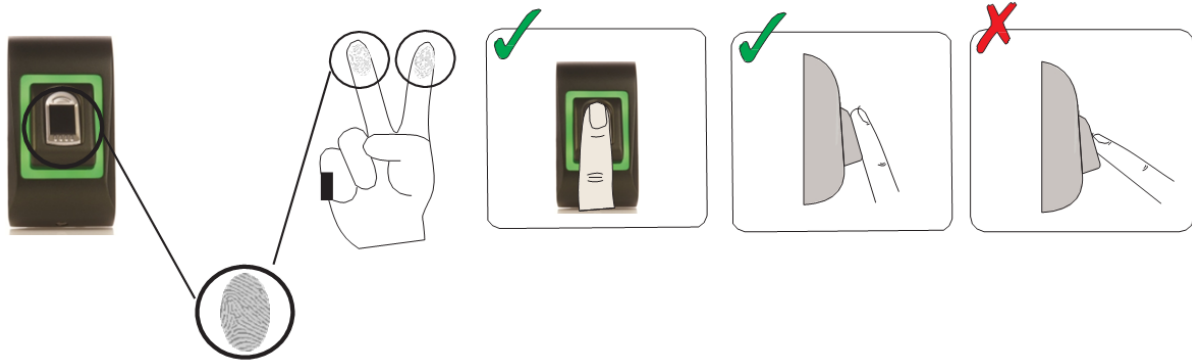
- The lines D0 and D1 are the Wiegand lines and the Wiegand Number is sent through them.
- The RS485 line (A, B) is used for fingerprint transfer and reader settings.
- The Biometric readers must be powered from the controller. If using another power supply for the biometric reader, connect the ground (GND) from both sources to ensure correct transfer of the Wiegand signal.
- Connect the lines D0, D1, Gnd, +12V, A and B to C2P controller.
- When the reader is connected and turned on, the LED will blink orange and emit two beeps. This indicates that it is 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 Reader-Controller distance is large (50 meters) and if communication with the reader can not be established, terminate the RS485 bus by closing the bridge on the C2P Controller.

6 Enrollment

Follow the below instructions for correct finger swiping. Place the selected finger on the sensor.



Result:

- **Valid reading:** The three-color status LED lights green + OK beep (one short beep plus one long beep).
- **Incorrect recording or reading:** The three-color status LED lights up in red + error beep (3 short beeps).

7 Configuring the 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 "BIO9500".



Portales\Showroom\Carrer\D1 - 161021066\R1 - 161021066

Básico Zonas horarias de libre acceso Biométrico

Lector 1

Nombre R1 - 161021066

Tipo BIO9500

Puerta D1 - 161021066

Tipo de Wiegand Wiegand34

Habilitar acceso por zonas horarias ☐

Omitir anti-passback ☐

Salida de Inside

Entrada a Inside

Tiempo de restablecimiento de anti-passback 00:00

Acceso libre ininterrumpido ☐

Si se producen 0 intentos no válidos, deshabilitar durante 0 minutos

Número requerido de usuarios con acceso válido 1

Guardar y salir

Vaya a la pestaña "Biométrico"
Introduzca el número de serie del
Lector Biométrico

[Página web del producto](#)

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

Portales\Showroom\Carrer\D1 - 161021066\R1 - 161021066

Básico Zonas horarias de libre acceso Biométrico

Serie 11-11-11-11

☒ Buzzer

Flexibilidad de aceptación de Automático (seguro)

Sensibilidad (0 = valor más bajo) 7

☒ Enviar este Id. para huella desconocida 0000000001

☐ Backlight

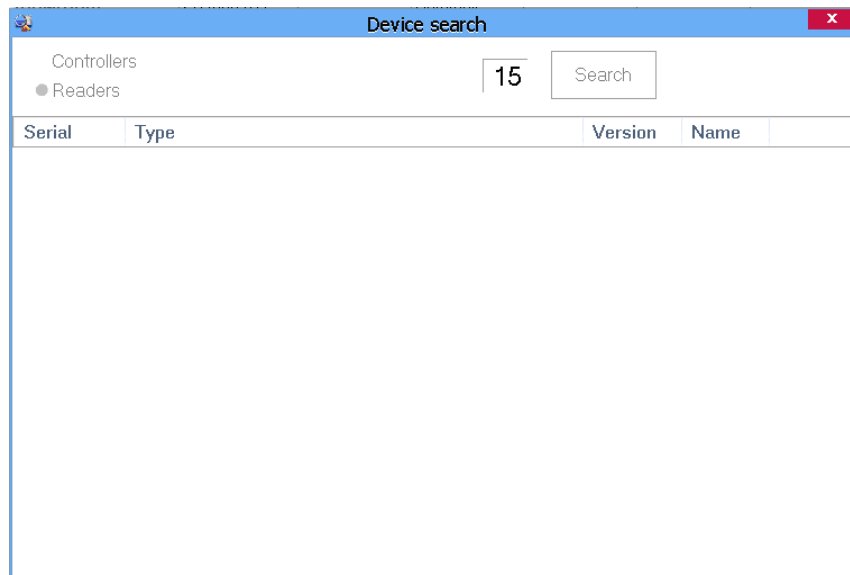
Modo de entrada

Guardar y salir

Vaya a la pestaña "Biométrico"
Introduzca el número de serie del
Lector Biométrico

[Página web del producto](#)

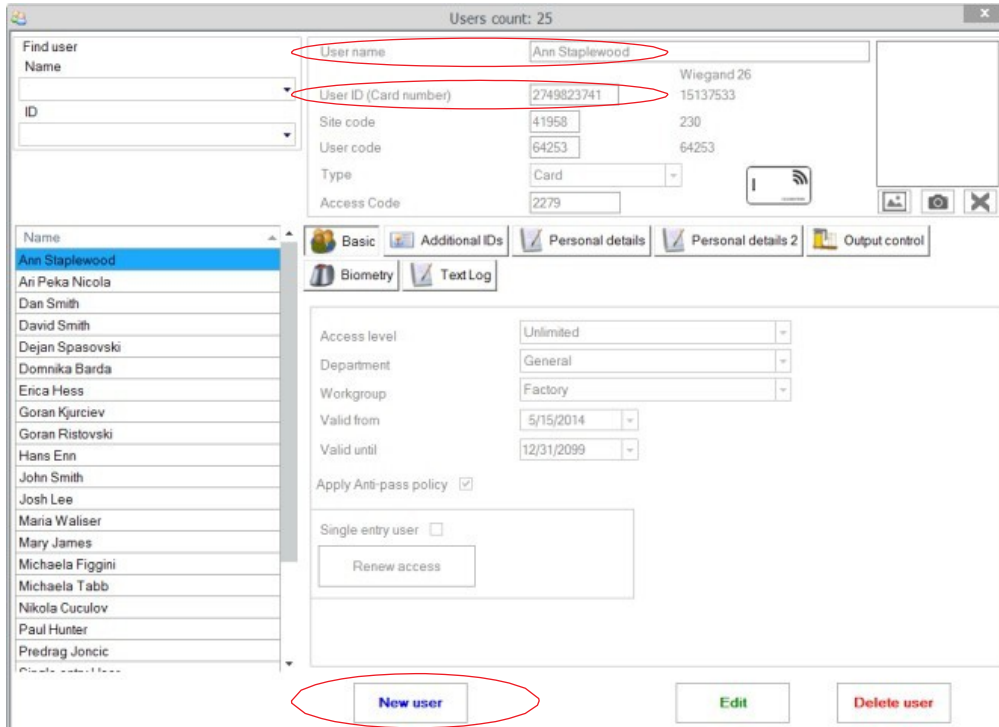
Important Note: The serial number of the reader can be found on a sticker inside the reader, on the packaging box and it can be search from the software (right click on the portal/search devices/readers).



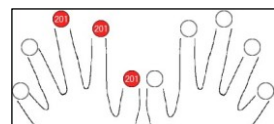
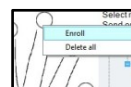
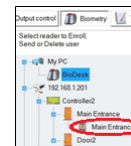
To check if the reader is On Line, right click on the reader and select “Check version”. In the Event Window a message should appear “Device ON Line, Type: BIO9500”

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).



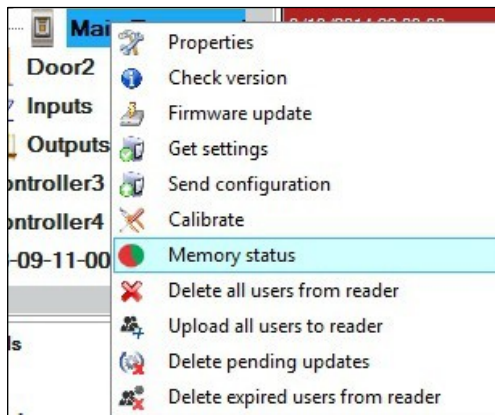
2. Go to the “Biometric” Tab. Select the reader (with left click) from which the enrollment will be done.
3. Right click on the fingertip and select enroll.
4. In the next 25 seconds, physically place the finger on the selected reader; the fingertip in the screen will become red, indicating the register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

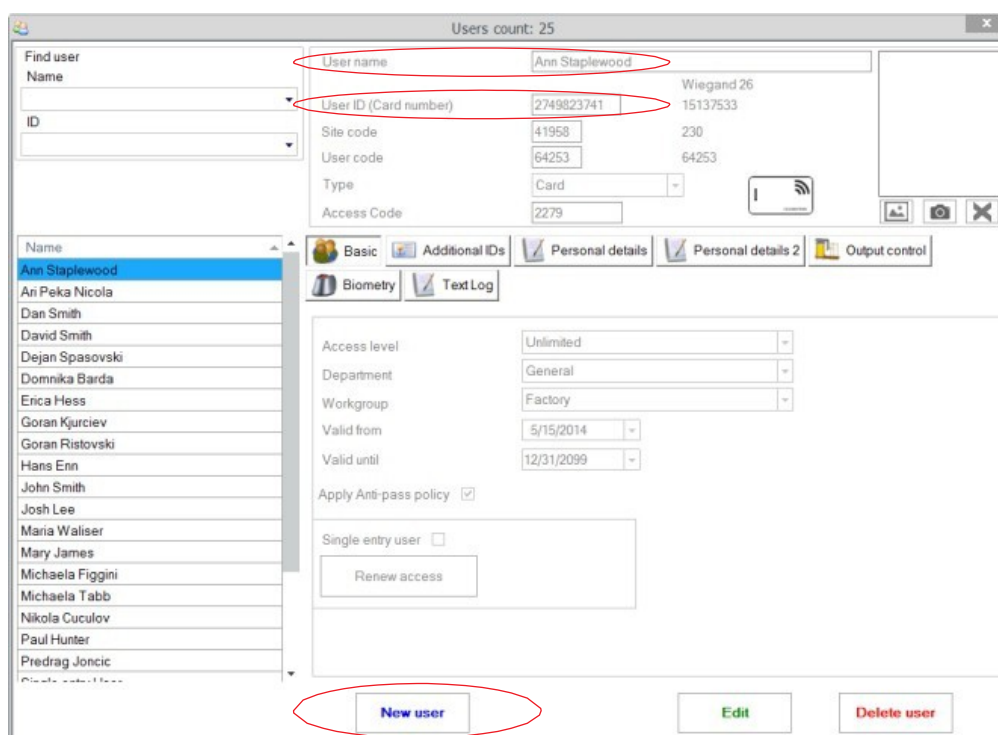
Reader	Door	Event
BIO9500		Enrolled fingers : 3

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).

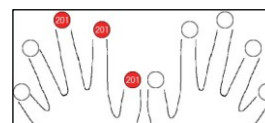
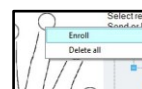
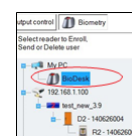
7.3 Enrolling fingerprints from a desktop reader

Plug the desktop reader in the PC. If the device does not install automatically, use the drivers included on the web <https://www.jcm-tech.com/JCM/control/>. 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 place the finger on the selected reader; 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.

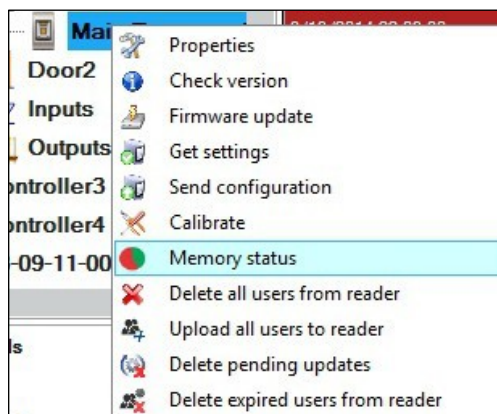


If the reader is offline, fingers will be sent when the connection between CONTROL server and the readers is established. No further registration or action is required. Fingerprints will be sent as soon as the communication is established.

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
BIO9500		Enrolled fingers : 3

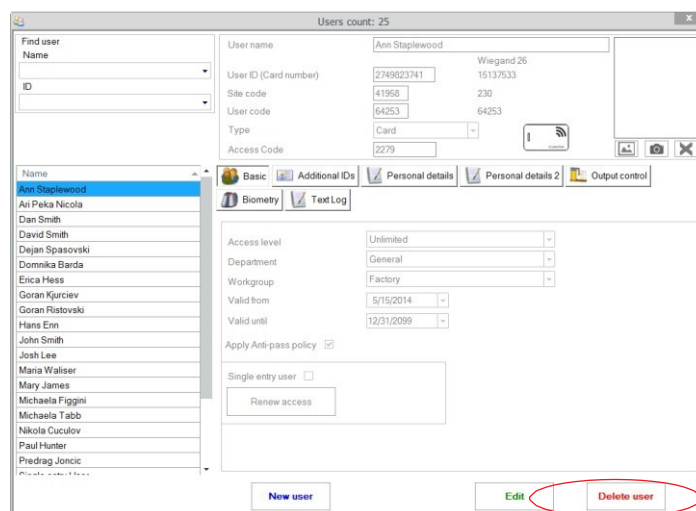
Note: If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID (card Number).

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.

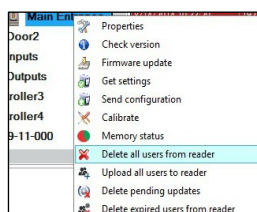
Deleting one user from the biometric reader

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.



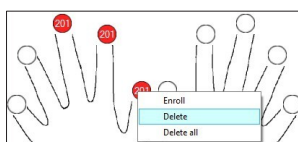
Deleting all users from the biometric reader

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



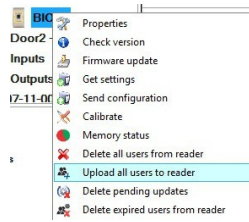
Deleting one or more fingerprints from reader and software

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”.



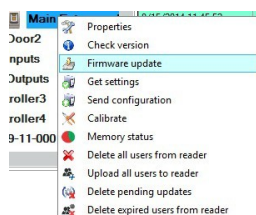
While receiving the fingerprints the reader will blink in orange.

Note: 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.

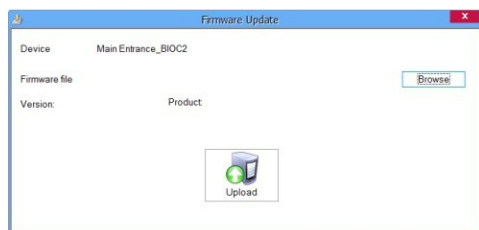
In normal usage, the fingerprints are sent automatically and this feature is not used.

7.6 Firmware update

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



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

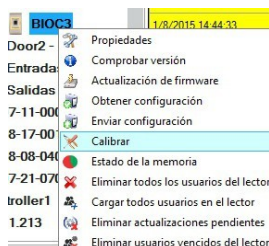


The default location of the firmware files installed with CONTROL is in the folder "Firmware". Select the firmware file with a "xhc" extension. Click on the Upload button.

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 Sensor calibration

Right click on the biometric reader and select "Calibrate" and wait for confirmation message.

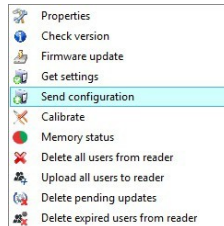


Note: It is recommended to do a calibration while commissioning the reader and in cases when there are problems with reading the fingers.

7.8 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.

7.9 Advanced settings

Buzzer: ON or OFF

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

Sensitivity: Bio-sensor sensitivity, the recommended value is 7, most sensitive.

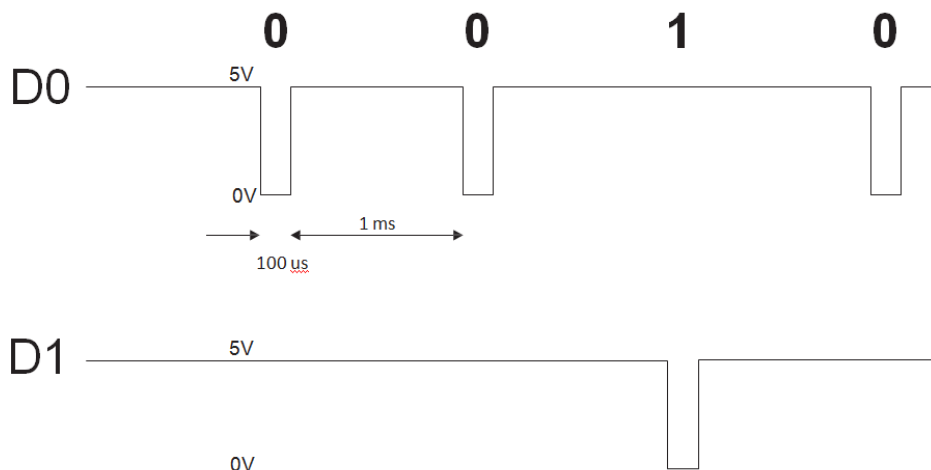
Send This ID for: Unknown Finger sends the desired Wiegand when an unknown finger is applied.

Backlight: ON or OFF

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...



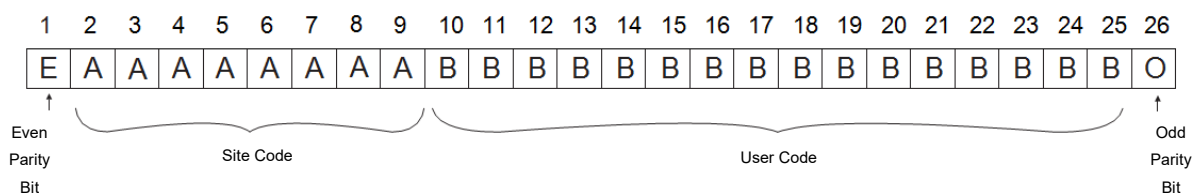
Bit de datos 0 = aproximadamente 100 µs (microsegundos)

Bit de datos 1 = aproximadamente 100 µs (microsegundos)

Tiempo entre dos bits de datos: aproximadamente 1 ms (milisegundo). Ambas líneas de datos (D0 y D1) están altas.

Descripción para el formato Wiegand de 26 bits

Cada bloque de datos consta de un primer bit de paridad P1, un encabezado fijo de 8 bits (A), 16 bits de código de usuario (B) y un 2º bit de paridad P2.



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

Example:

	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 close to a source of strong electro-magnetic fields like radio-transmitting antenna. Do not place the 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 damaged and the fingerprint can't be entered.

10 Troubleshooting

The red LED on the biometric reader blinks all the time	15 authentication attempts (fingerprint or PIN) have been made. The red LED will turn off when a fingerprint or PIN code is accepted.
Enrollment can be done from the desktop reader, but fingerprints are not sent to all biometric readers in the network.	<ul style="list-style-type: none"> • Check the serial number of the readers. • Check if the termination is correct, as described. • Check if the communication cables (A and B) are correctly connected to the reader.
The biometric reader does not turn on. The tricolor LED is off.	Check the power supply (red and black wire).
The fingerprint (or a PIN code) is recognized (the tricolor LED is green), but the controller sends another ID number and access is denied.	<ul style="list-style-type: none"> • If the user has not been deleted from the reader and the same user is re-registered with a new ID, the reader will recognize the fingerprint with the first ID. To solve the problem, delete all users from the reader and return to load them. • Check the Wiegand bus (yellow and white wire) Check if the ground of the controller and biometric reader is the same. • Check if the length between the biometric reader and the controller is less than 50 m.
Electrostatic discharges affect the reading of the fingerprint.	Connect the biometric reader housing to the ground wire.
The reading performance of the reader has decreased.	Check if the fingerprint reading area is dirty. Do not clean the device with any liquid. Use only a soft, dry cloth. The reading area is damaged. If the damage is minor, try to calibrate the sensor.
The fingerprint is not recognized in the normal way.	Try again when you have removed the moisture from your finger. If your finger is too dry, touch your forehead and try again. If you have a cut on your finger, register another fingerprint.

11 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.

12 UE Declaration of conformity

JCM Technologies S.A., hereby declares that the product BIO9500 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.

web page swww.jcm-tech.com/es/declaraciones

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