

# BIOPROX-MF V1

EN

Biometric Mifare Reader



USER'S MANUAL

# CONTENTS

<u>1. DESCRIPTION</u> .....	3
<u>2. SPECIFICATIONS</u> .....	3
<u>3. MOUNTING</u> .....	4
<u>4. WIRING</u> .....	4
<u>5. CONNECTING BIOMETRIC READERS TO EWS CONTROLLER</u> .....	5
5.1 CONNECTING BIOMETRIC READERS IN SAME RS-485 LINE WITH THE EWS CONTROLLERS.....	5
5.2 CONNECTING BIOMETRIC READERS WHEN ALL THE CONTROLLERS HAVE TCP/IP COMMUNICATION .....	6
5.3 RS-485 TUNING .....	6
<u>6. CONNECTING BIOMETRIC READERS TO 3RD PARTY CONTROLLER</u> .....	7
6.1 CONVERTERS PIN DESCRIPTION .....	7
<u>7. ENROLLMENT</u> .....	7
<u>8. CONFIGURING THE BIOMETRIC READERS IN PROS SOFTWARE</u> .....	8
8.1 ADDING BIOMETRIC READER .....	8
8.2 ENROLLING FINGERPRINTS FROM A READER .....	9
8.3 ENROLLING FINGERPRINTS FROM DESKTOP READER .....	10
8.4 DELETING FINGERPRINTS .....	11
8.5 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS .....	11
8.6 FIRMWARE UPDATE .....	12
8.7 ENTRY MODE .....	12
8.7.1 CARD OR FINGER .....	12
8.7.2 CARD AND FINGER .....	12
8.7.3 FINGER ONLY .....	12
8.7.4 FINGER ON CARD .....	13
8.8 SENSOR CALIBRATION .....	14
8.9 SEND CONFIGURATION .....	14
8.10 ADVANCED SETTING .....	14
<u>9. CONFIGURING THE BIOMETRIC READERS IN BIOMANAGER</u> .....	15
9.1 ADD PORTAL .....	15
9.2 ADD READER .....	15
9.3 EDIT READER .....	16
9.4 DELETE READER .....	16
9.5 ADD USER .....	17
9.6 DELETE FINGERPRINTS .....	18
9.7 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS .....	18
9.8 CUSTOM WIEGAND .....	19
<u>10. WIEGAND PROTOCOL DESCRIPTION</u> .....	20
<u>11. SAFETY PRECAUTIONS</u> .....	20

## 1. DESCRIPTION

BIOPROX-MF V1 is a Wiegand biometric and proximity reader for access control applications with programmable wiegand output. It offers storage of up to 9500 fingerprints, it reads cards/tags and has a progrMifare Classic 1K & 4K, Ultralight, Desfire ammable Wiegand Output (8 to 128 bits).

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

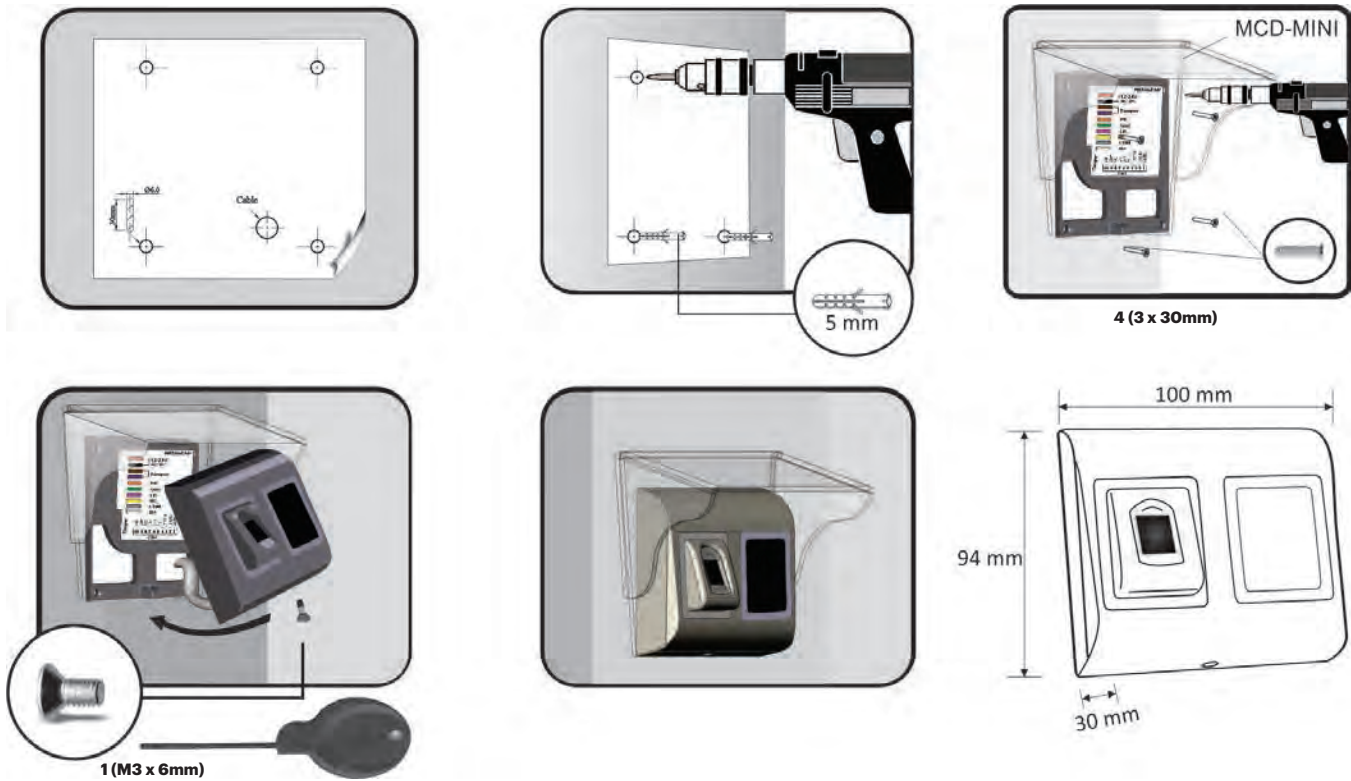
Configuration of the readers and fingerprint enrollment is done through PC Software.

Connection between the biometric readers is RS-485 and it is used for fingerprint transfer and configuration. When used with third party controllers, the connection between the Biometric readers and the PC is done through a converter (CNV200-RS-485 to USB or CNV1000-RS-485 to TCP/IP). Only one converter is needed per system (one converter for 1, 2, 3...30, 31 Biometric readers).

## 2. SPECIFICATIONS

<b>Fingerprint capacity</b>	up to 9500 fingerprints; unlimited in Finger on Card mode
<b>Technology</b>	Biometry and Mifare (13,56Mz)
<b>Authentication</b>	Finger, Card, Finger or/and Card, Finger on Card
<b>Fingerprints per user</b>	1-10 fingerprints
<b>Proximity reading type</b>	Mifare Classic 1K & 4K, Ultralight, Desfire; Finger on Card (Classic and Desfire)
<b>Reading distance</b>	1.5 to 5.5cm
<b>Interface</b>	Wiegand 8 to 128 bits; Default: Wiegand 26bit
<b>Protocol programming</b>	By PROS CS software (EWS system) and BIOMANAGER CS (all access control systems)
<b>Cable distance</b>	150m
<b>Fingerprint Sensor Type</b>	Capacitive
<b>1:1000 identification time</b>	970 msec, including feature extraction time
<b>Fingerprint enrolment</b>	On the reader or from the USB desktop reader
<b>Panel Connection</b>	Cable, 0.5m
<b>Green and Red LED</b>	Externally Controlled
<b>Buzzer</b>	Yes
<b>Buzzer</b>	Yes, by software settings
<b>Tamper</b>	Yes
<b>Consumption</b>	Max. 160mA
<b>IP Rating</b>	65
<b>Power supply</b>	9-14V DC
<b>Operating Temperature</b>	-15°C to +50°C, non-condensing
<b>Dimensions (mm)</b>	100 x 94 x 30
<b>Housing</b>	ABS

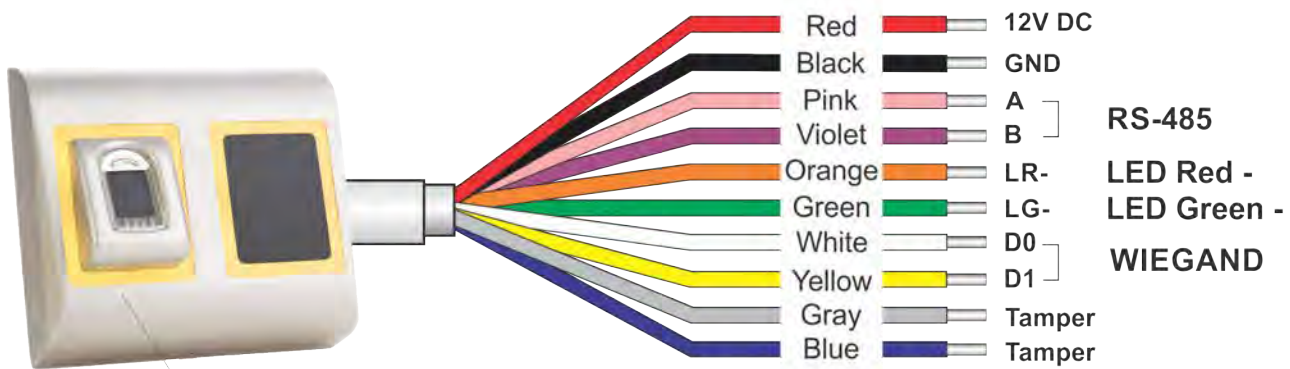
### 3. MOUNTING



If the biometric reader is installed and used outdoor, the reader **MUST** be fitted with MCD-MINI cover available in our accessories in order to protect the sensor from direct rainfall. The operating temperature of the product is between -15°C - + 50°C. If the reader is installed in an environment where the temperature can drop below -10°C 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. XPR™ 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



Tricolor LED (Red, Green, Orange)

#### DIP Switch



2 - not used

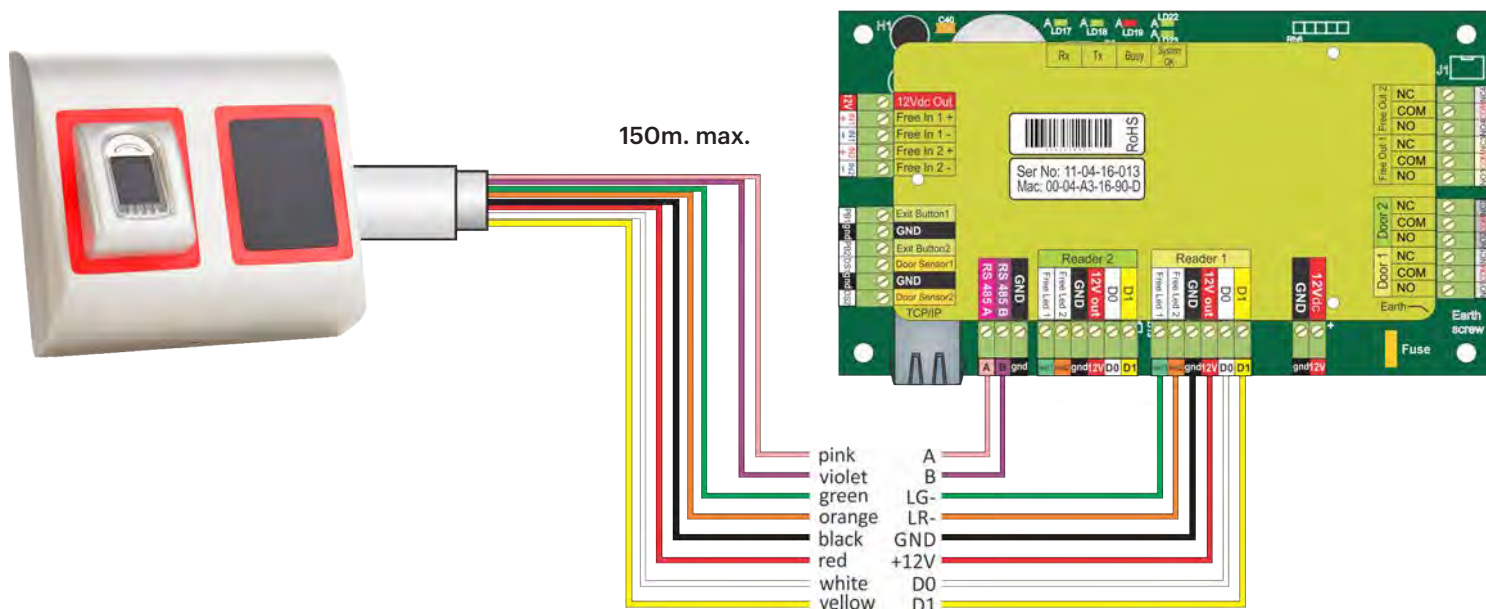
1 - Convert 7byte UID to 4byte UID

12V DC	9-14V DC
GND	ground
A	RS-485 A
B	RS-485 B
LR-	Red LED -
LG-	Green LED -
D1	Data 1
D0	Data 0
Tamper	Tamper Switch(NO)
Tamper	Tamper Switch(NO)

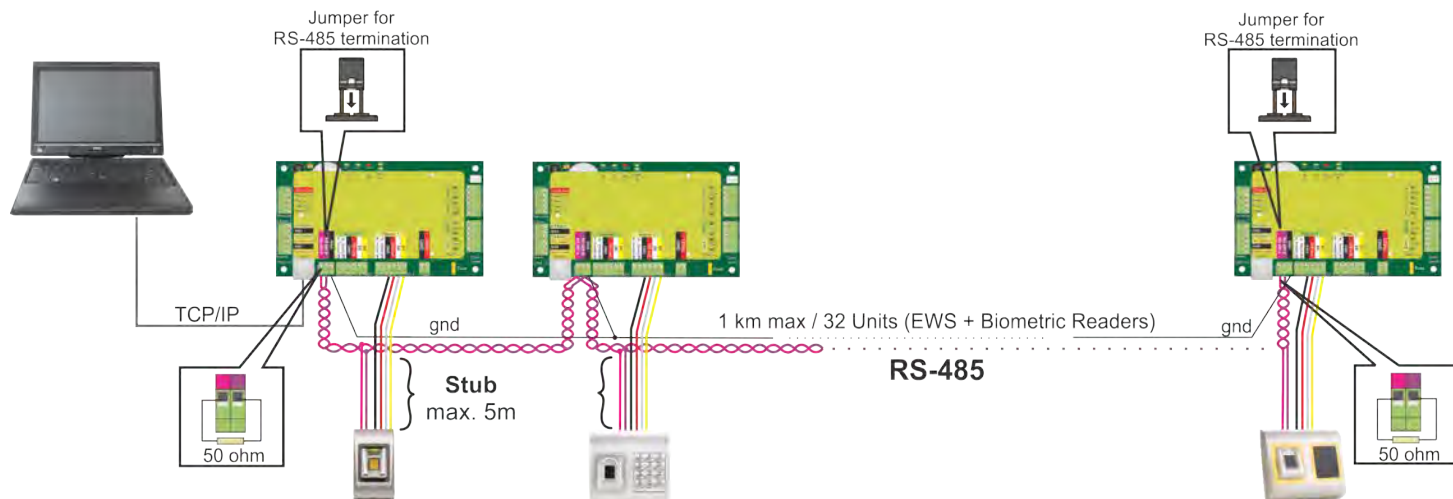
**Note:** The conversion from 7byte ID to 4 byte ID is only possible with cards that have 7 byte ID Number. Those are: Mifare plus, Desfire and Ultralight. The number is converted according to NXP algorithm. It corresponds to the number obtained by the USB desktop reader.

## 5. CONNECTING BIOMETRIC READERS TO EWS CONTROLLER

- The Biometric readers can be connected to virtually any controller that conforms to Wiegand format standards (standard Wiegand 26bit or self-defined Wiegand).
- The lines D0 and D1 are the Wiegand lines and the Wiegand Number is sent through them.
- The RS-485 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.

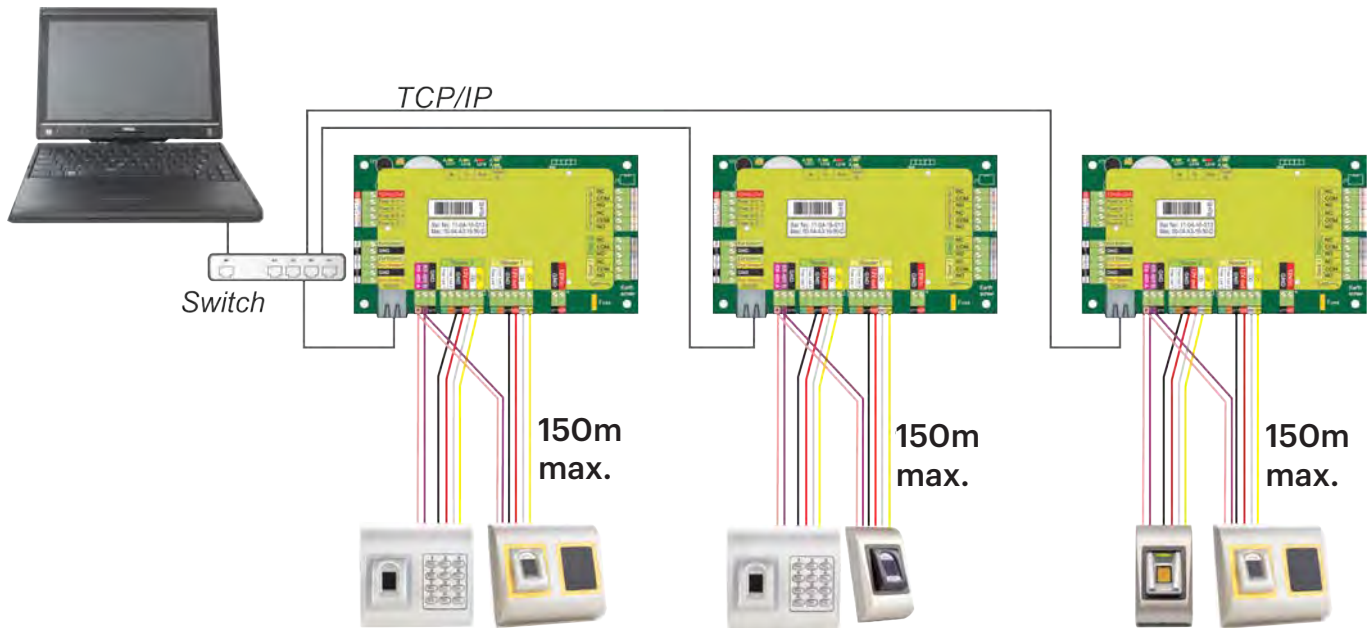


### 5.1 CONNECTING BIOMETRIC READERS IN SAME RS-485 LINE WITH THE EWS CONTROLLERS



- The Biometric readers are connected through RS-485 bus. The same RS-485 bus that the EWS controllers are connected to.
- Maximum units in one network (EWS + Biometric readers) is 32.
- If there are more than 32 units in one network, please utilize RS-485 HUB to connect.
- The RS-485 Line should be configured in the form of a daisy chain, NOT in a form of a star. If star must be used in some points, keep the stubs from the RS-485 backbone as short as possible. Maximum length of the stub is dependant of the installation (total number of devices in RS-485 line (total cable length, termination, cable type...)) so recommendation is to keep stubs shorter than 5 meters, keeping in mind that this can be possible reason for errors in communication with PC software
- The cable must be twisted and shielded with a min. 0.2 mm<sup>2</sup> cross section.
- Connect the ground (0V) of each unit in the RS-485 Line using a third wire in the same cable.
- The shield of the communication cable between two devices must be connected to the EARTH from ONE side of the RS-485 Line. Use the side that has earth connection to the building's grounding network.

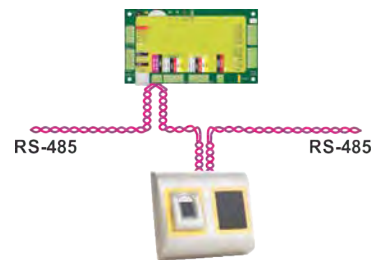
## 5.2 CONNECTING BIOMETRIC READERS WHEN ALL THE CONTROLLERS HAVE TCP/IP COMMUNICATION



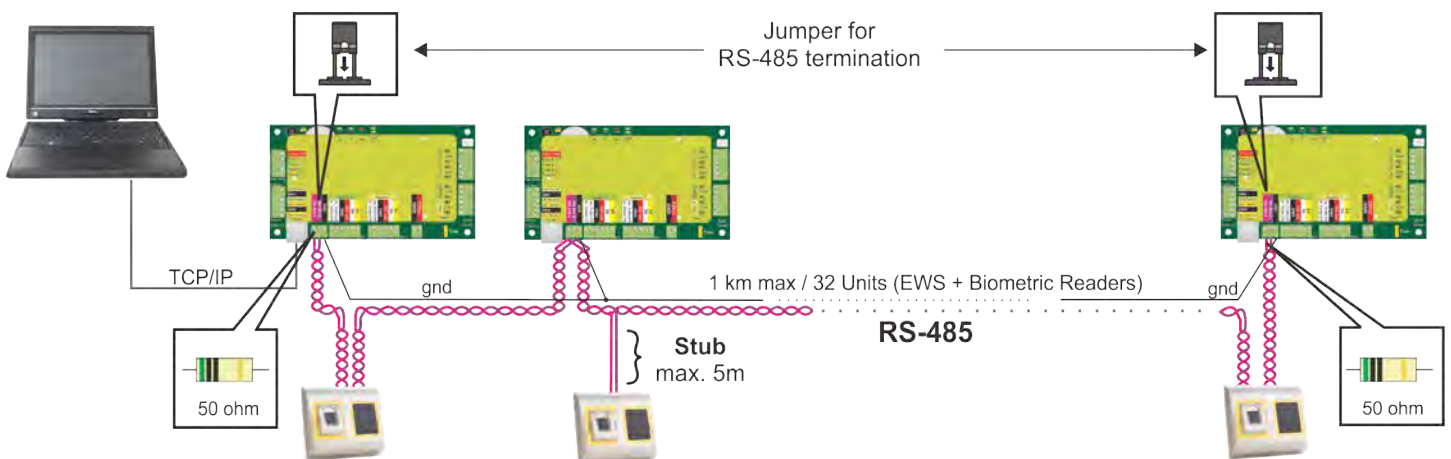
- When all the controllers are connected via TCP/IP, then the RS-485 network becomes local (from Reader 1 to the Controller then to the Reader 2).
- Connect the readers directly to the RS-485 terminals in each controller.
- If the distance Reader-Controller is high (50meters) and if the communication with the reader can not be established, then terminate the RS-485 network by closing the jumper in the EWS Controller or as described in chapter 5.1.

**NOTE: This is recommended configuration when you have multiple biometric readers in the same network. In this configuration, NO TERMINATION resistors are required.**

When all the controllers have TCP/IP communication the biometric readers are easily wired. When the controllers have RS-485 communication, it is difficult to maintain the daisy chain of the RS-485 network. Wiring the biometric readers in that formation is a challenge. See the schematic diagram below.



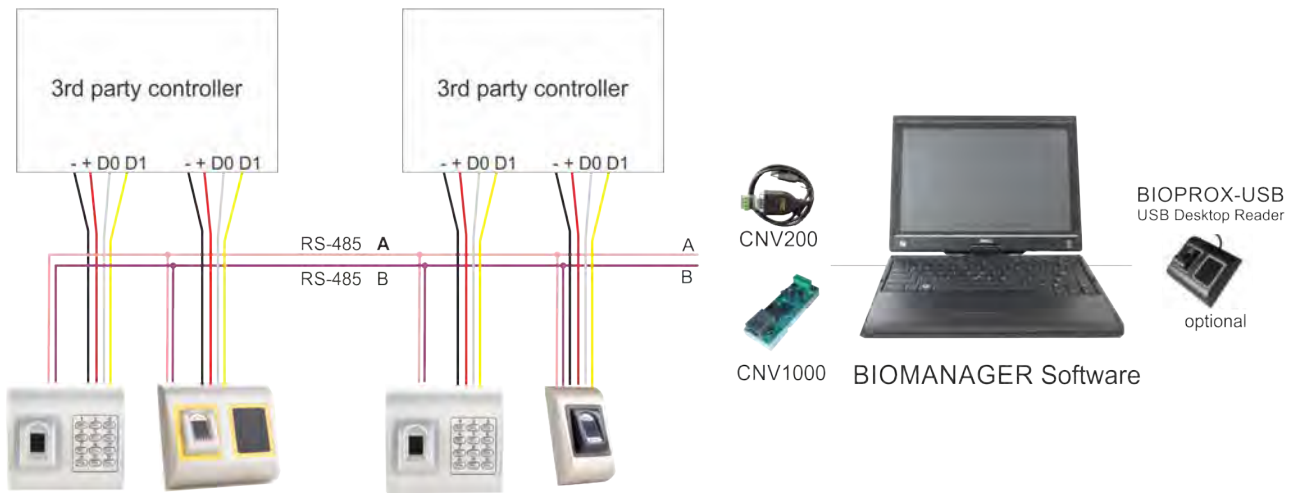
## 5.3 RS-485 TUNING



### RS-485 Termination resistors:

- Terminate both ends of the line with 120 Ohm resistor. If end of line is EWS, use built in resistor (120 ohm) by closing the jumper.
  - If the communication is not established and stable, use the external resistors provided in the hardware kit.
- When using CAT 5 compatible cable, in most of the cases, termination made with 50 Ohm external resistor or combination of 50 Ohm external and termination resistor from the EWS (120 Ohm) should be the solution.

## 6. CONNECTING BIOMETRIC READERS TO THIRD PARTY CONTROLLERS



- Connect the lines D0, D1, Gnd and +12V to the third party controller.
- Connect the RS-485 Line (A, B) to the converter. Connect the converter in the PC.
- Fingerprint enrollment is done from the PC Software. Connection between the Biometric readers and the PC must be established.
- The Biometric readers communicate with each other with a RS-485 and with the PC Software through a Converter.
- The RS-485 Line should be configured in the form of a daisy chain, NOT in a form of a star. Keep the stubs from the RS-485 backbone as short as possible (not more than 5 meters)
- Only one converter per installation is needed, not per reader.

### 6.1 CONVERTERS PIN DESCRIPTION



#### CNV200

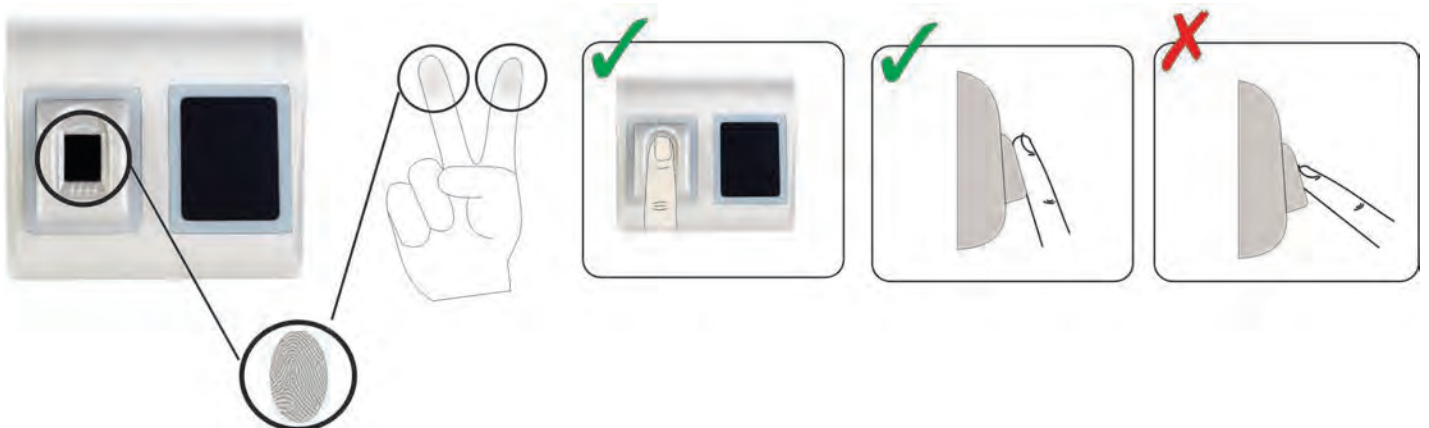
Converter RS-485 to USB  
Requires installation as USB serial device (refer to CNV200 Manual). The Drivers are located on the web site.

#### CNV1000

Converter RS-485 to TCP/IP  
Does not require installation. IP address set through Internet Browser

Biometric Reader	Converter
RS-485 A	PIN 1 (RS-485 +)
RS-485 B	PIN 2 (RS-485 -)

## 7. ENROLLMENT



## 8. CONFIGURING THE BIOMETRIC READERS IN PROS CS SOFTWARE

### 8.1 ADDING BIOMETRIC READER

1. Expand the Door item to view the readers
2. Right click on the reader and select properties (8.1)
3. In the Basic tab, for "Type" of the Reader select "BIOPROX-MF". (8.2)
4. After selecting the type, a third tab will appear "Biometric". Go to that tab and put the serial number of the Biometric Reader. (8.3)

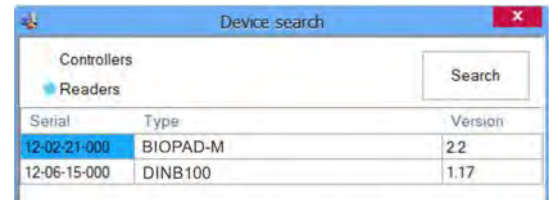
**Important Note:** The serial number of the reader can be found on a sticker inside the reader, on the packaging box and it can be search from the software (right click on the portal/search devices/readers). (8.4 & 8.5)  
To check if the reader is On Line, right click on the reader and select "Check version". In the Event Window a message should appear "Device ON Line, Type: BIOPROX-MF" (8.6)



8.1

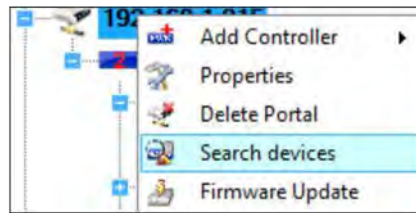
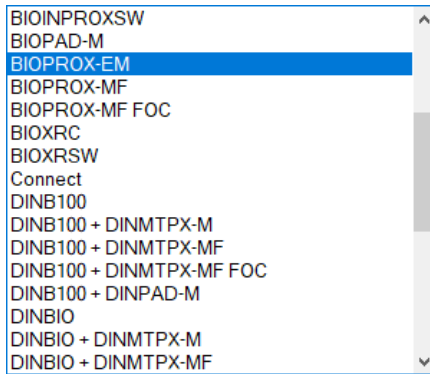


8.3

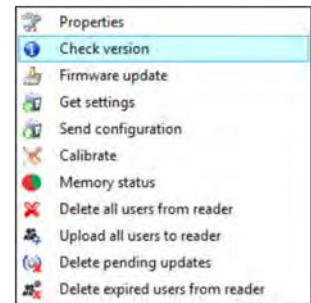


Serial	Type	Version
12-02-21-000	BIOPAD-M	2.2
12-06-15-000	DINB100	1.17

8.5



8.4



8.6

## 8.2 ENROLLING FINGERPRINTS FROM A READER

1. Open the Users Window and create a new user.  
Click on "New User", put a name, ID(card number). (8.7)
2. Go to the "Biometric" Tab
3. Select the reader(with left click) from which the enrollment will be done. (8.8)
4. Right click on the fingertip and select enroll. (8.9)
5. In the next 25 sec. present the finger on the selected reader and the finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip. (8.10)  
In these 25 sec. the reader will continuously blink in orange.
6. Repeat point 4&5 for each finger that should be enrolled.
7. 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:

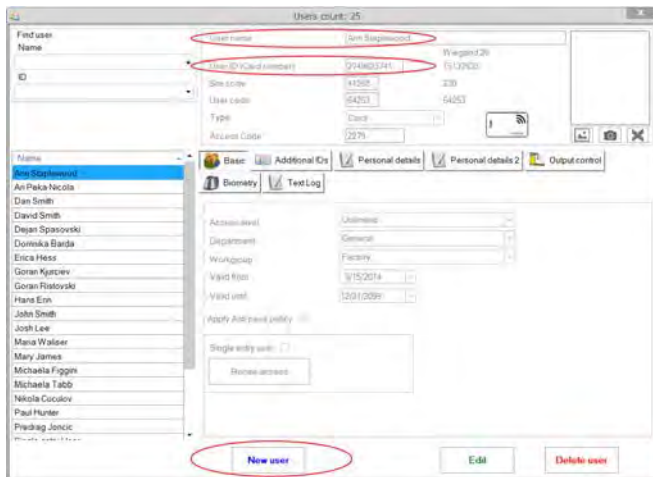
If the user has "Unlimited" Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

### Note:

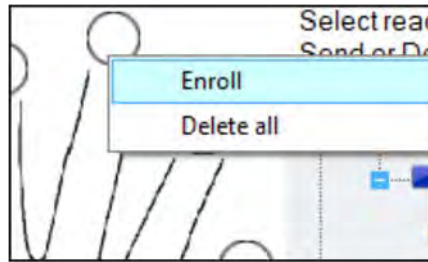
To check if all the fingerprints are sent to the reader, right click on the reader and select "Memory Status". (8.11)  
In the event window a line will appear indicating the number of fingerprints stored in the reader. (8.12)

### Note:

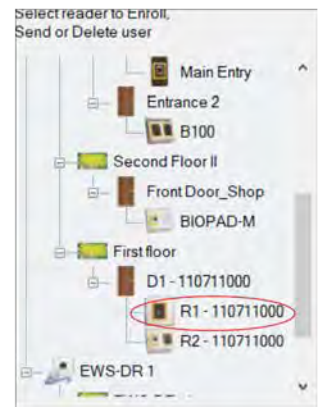
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



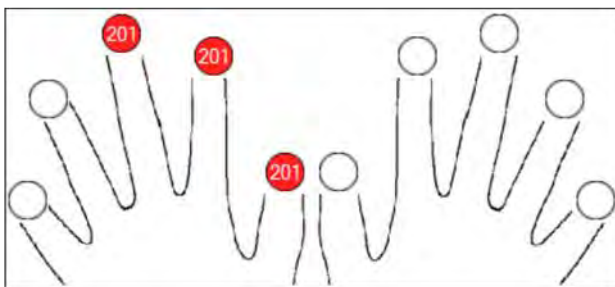
8.7



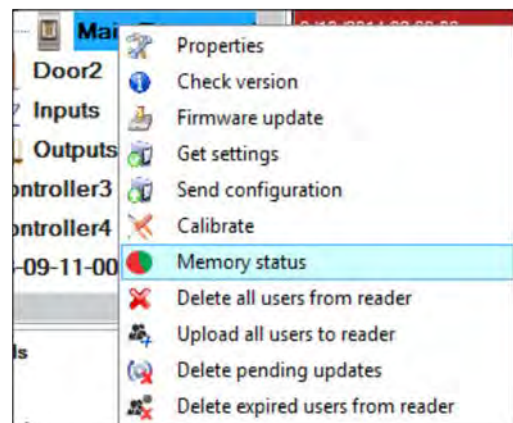
8.9



8.8



8.10



8.11

Reader	Door	Event
B100		Enrolled fingers : 3

8.12

### 8.3 ENROLLING FINGERPRINTS FROM DESKTOP READER

Plug the Desktop Reader in the PC. 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. (8.13)

1. Open the Users Window and create a new user. Click on "New User", put a name, ID(card number). ( 8.7)
  2. Go to the "Biometric" Tab
  3. Select the USB desktop Reader (with left click). (8.8)
  4. Place the finger on the BIOPROX-USB, right click on the fingertip and select enroll. (8.9)
  5. The finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip. (8.10)
  6. Repeat point 5 for each finger that should be enrolled.
  7. 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 off line, the fingers will be sent upon the connection is established between PROS server and the reader. No need for additional enrollment or actions. The fingerprints will be sent as soon as communication is established.

**Example:**

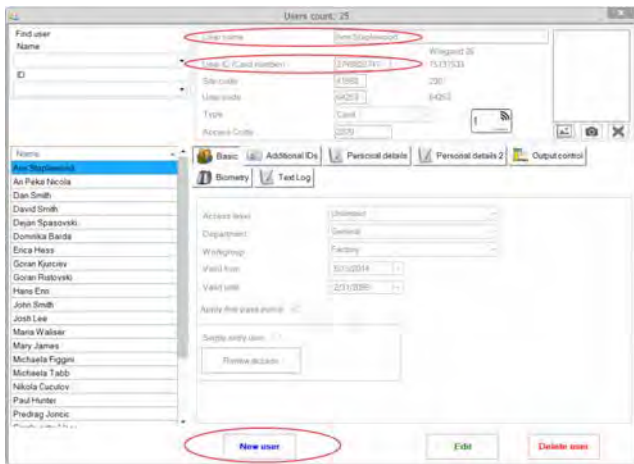
If the user has "Unlimited" Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

**Note:**

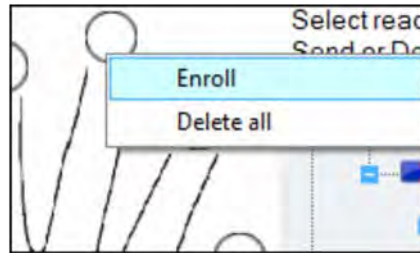
To check if all the fingerprints are sent to the reader, right click on the reader and select "Memory Status". (8.11)  
In the event window a line will appear indicating the number of fingerprints stored in the reader. (8.12)

**Note:**

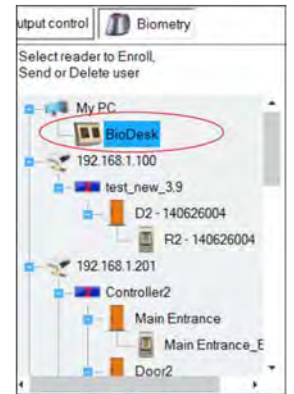
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



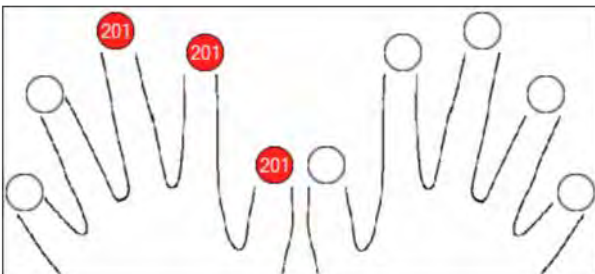
8.7



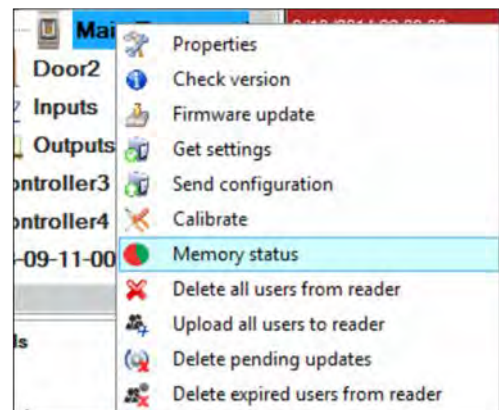
8.9



8.13



8.10



8.11

Reader	Door	Event
BIOC3		Enrolled fingers :28

8.12

## 8.4 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

Click on "Delete User". The User together with its fingerprints will be deleted from both the software and the fingerprint readers. (8.14)

### Deleting all users from the biometric reader

Right click on the reader and select "Delete all users from reader" (8.15)

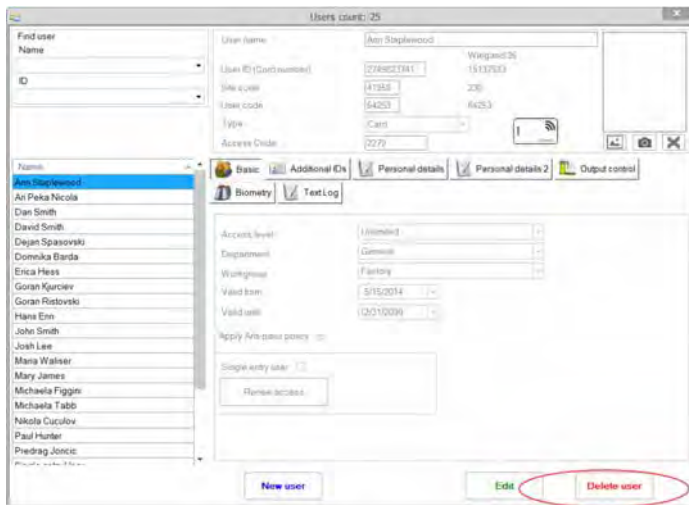
### Delete one or more fingerprints

Select the User and open the "Biometric" tab

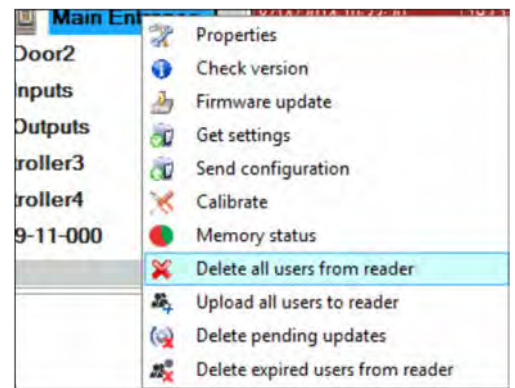
Go to the fingertip that needs to be deleted, right click and select "Delete" for one finger or "Delete All" for all fingers of the User.

Click "Save Changes".

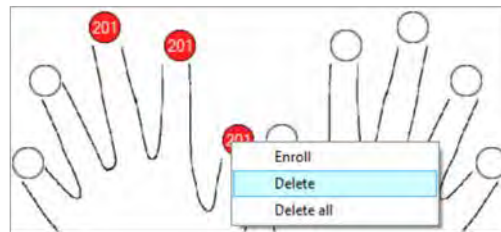
With this procedure the User's fingerprints are deleted from the software and from the reader. (8.16)



8.14



8.15



8.16

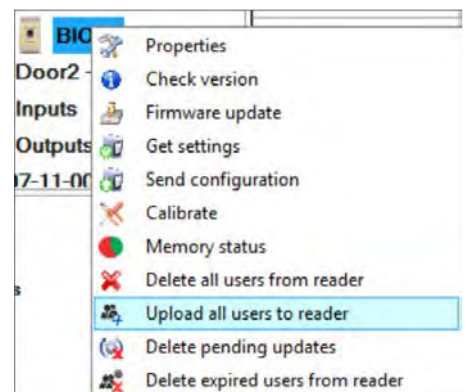
## 8.5 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS

Right click on the biometric reader

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.



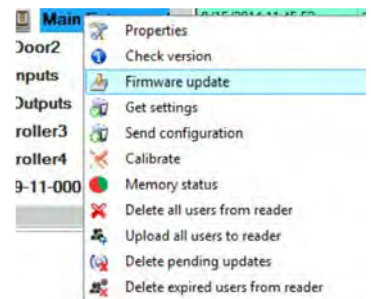
8.17

## 8.6 FIRMWARE UPDATE

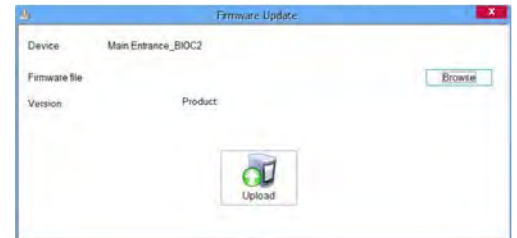
Right-click on the reader and select Firmware update menu (8.18)

On the Firmware update window, click on the Browse button (8.19). The default location of the firmware files installed with PROS CS 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.



8.18



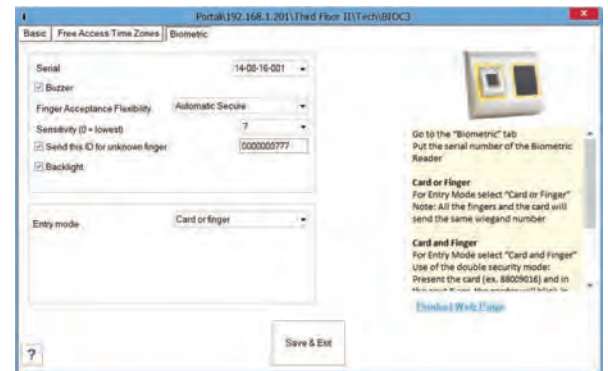
8.19

## 8.7 ENTRY MODE

### 8.7.1 CARD OR FINGER

Right click on the biometric reader  
Select "Properties" and go to the "Biometric" tab  
For Entry Mode select "Card or Finger" (8.20)

**Note:** All the fingers and the card will send the same wiegand number (8.23)

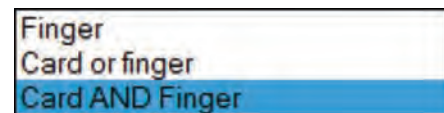


8.20

### 8.7.2 CARD AND FINGER

Right click on the biometric reader  
Select "Properties" and go to the "Biometric" tab  
For Entry Mode select "Card and Finger" (8.21)

Use of the double security mode:  
Present the card (ex. 88009016), in the next 8 sec. the reader will blink in orange waiting for the finger. Present the finger



8.21

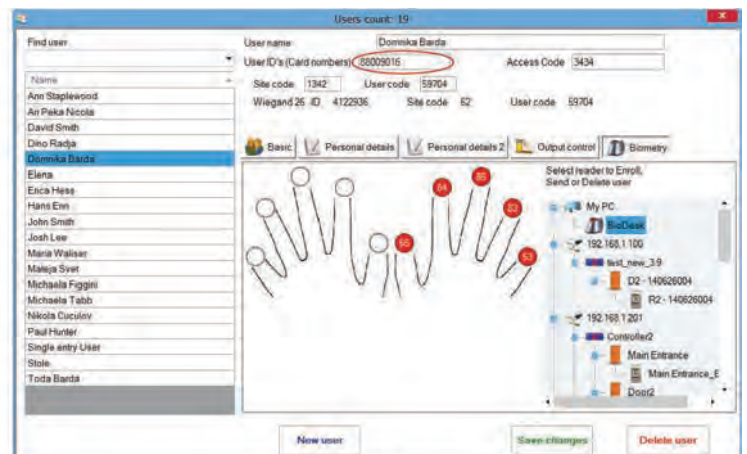
### 8.7.3 FINGER ONLY

Right click on the biometric reader  
Select "Properties" and go to the "Biometric" tab  
For Entry Mode select "Finger" (8.22)

**Note:**  
In this mode the proximity reader will become inactive.



8.22



8.21

## 8.7.4 FINGER ON CARD

Right click on the biometric reader

Select "Properties"

For "type" of the reader select "BIOPROX-MF FOC" (8.30)

### Writing Template on the card

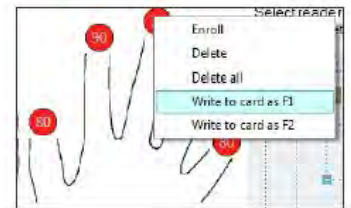
1. Open Users window
2. Select existing user or create new one
3. Enroll 1 or 2 fingers using BIOPROX-USB Desktop Biometric Reader
4. Place the user card on the BIOPROX-USB
5. Right click on the fingertip and select "Write to Card as F1" (8.31)
6. To put the second finger in the card, go to another fingertip and select "Write to Card as F2"
7. If the fingerprints are not to be stored in the software database, right click on the fingertip and select "Delete all"
8. If some user data other than fingerprints is edited or the fingerprints should be saved in the software database, click Save, otherwise go to another user or close the window if no other user management is required.

### Note:

Depending on the Mifare Card, 1 or maximum 2 fingers can be written. 1k Cards can store 1 fingerprint, 4K cards can store 2 fingerprints.



8.30



8.31

### To use the "Finger on Card" mode:

Present the mifare card with written fingerprints in it, the reader will beep and blink.

Present the finger on the Biometric Reader

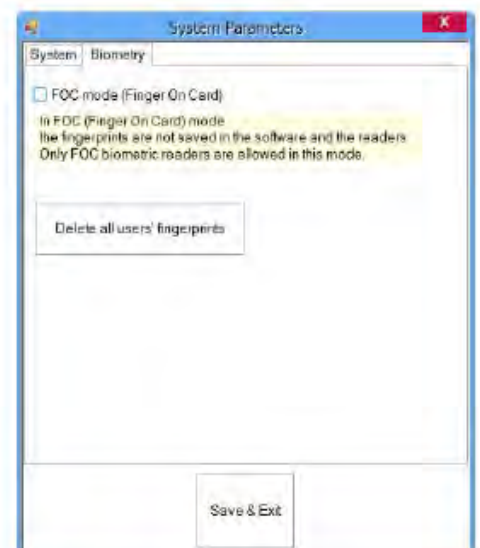
### Note:

In "Finger on Card" mode, there is NO LIMIT on the capacity of the fingerprints, since the fingerprints are stored in the user's card, not in the biometric reader.

### Note:

In "Finger on Card" Mode (FOC), the fingerprints are stored in the card and in the software's database.

If you want the fingerprints not to be stored in the database, then tick the checkbox in: Settings/System Parameters (8.32)

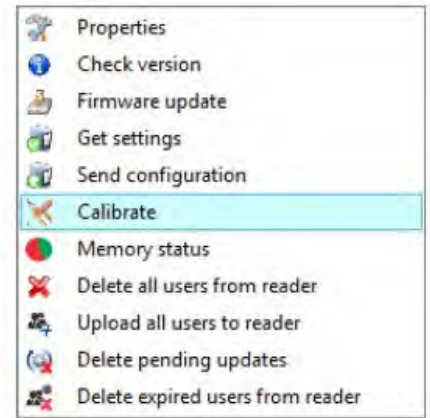


8.32

## 8.8 SENSOR CALIBRATION

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

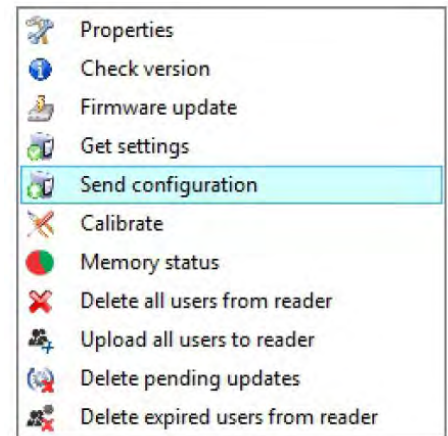
**Note:** It is recommended to do a calibration while commissioning the reader and in cases when there are problems with reading the fingers



## 8.9 SEND CONFIGURATION

- 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.



## 8.10 ADVANCED SETTINGS

### Send This ID for:

Unknown Finger sends the desired Wiegand when an unknown finger is applied.

### Backlight:

Backlight of the device (ON or OFF)

### Buzzer:

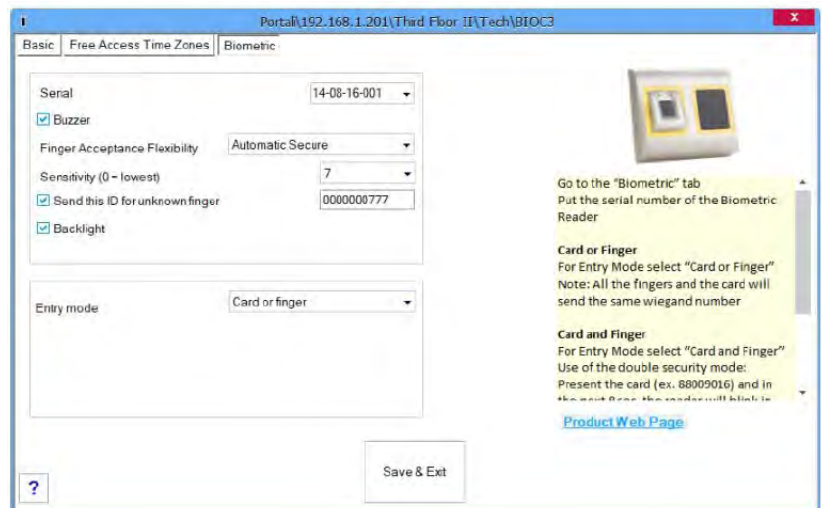
Buzzer of the device (ON or OFF)

### Finger Acceptance Flexibility:

Accepted tolerance. The recommended value is “Automatic Secure”.

### Sensitivity:

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



## 9. CONFIGURING THE BIOMETRIC READERS IN BIOMANAGER CS

BIOMANAGER CS is software for fingerprint management of XPR Biometric readers, when used with third party access controllers.

### Main functions:

#### - Fingerprint Enrollment

It can be done by ANY Biometric reader in the network or by Desktop (USB) Biometric reader.

#### - Fingerprint Transfer

Finger templates can be sent to any Reader in the Network. Different Users can be sent to different Biometric readers.

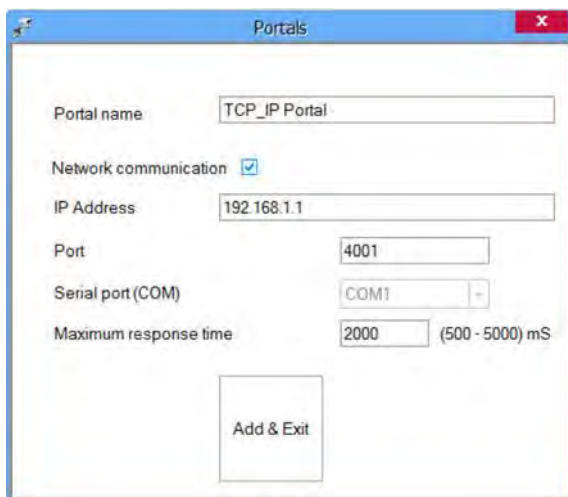
#### - PIN Codes management and transfer

PIN Code length configuration (1 to 8 digits) and PIN Code transfer.

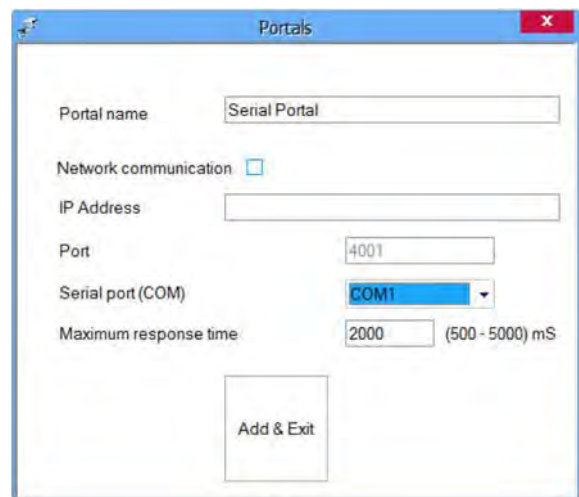
#### - Wiegand Output Configuration

The Wiegand output of the Biometric reader can be customized bitwise.

### 9.1 ADD PORTAL



9.1



9.2

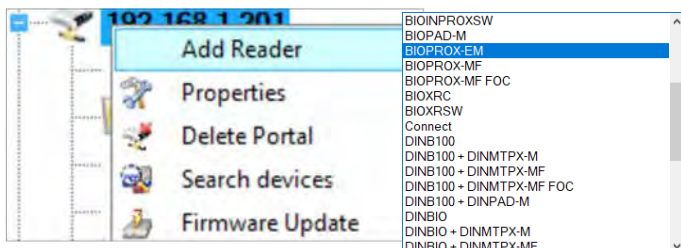
Right-click on "Portal" and select "Add Portal".

If the converter used for the Biometric Readers is RS-485 to TCP/IP converter, then create Portal by adding the IP Address of the converter.(9.1)

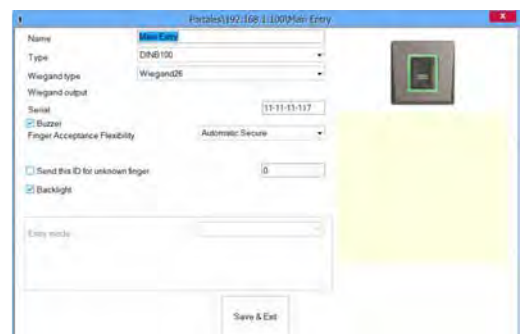
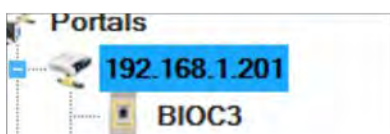
If the converter used for the Biometric Readers is RS-485 to USB converter, then create ID Portal by adding the COM port of the converter.(9.2)

### 9.2 ADD READER

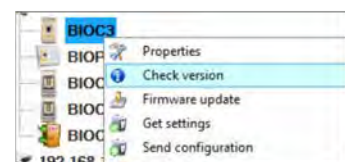
Right-click on the portal connected to the reader and select **Add reader**



Click on **Save** and the reader icon appears under the selected portal



Fill the **Reader** form



Right-click on reader and select **Check Version**

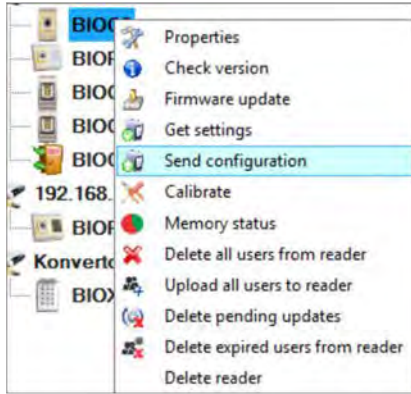
If reader is online, new line is added on top of the event table

Time	Portal	Controller	Reader	Door	Event	User
8/6/2015 12:57:03	192.168.1.201		BIOC3		Device online	Type: BIOC3 Version: 1.11

If reader is not online, following line is added on top of the event table

Time	Portal	Controller	Reader	Door	Event	User
8/6/2015 12:58:42	192.168.1.215		BIOPROX-EM		No response	

If reader is online, right click on reader and select **Upload configuration**

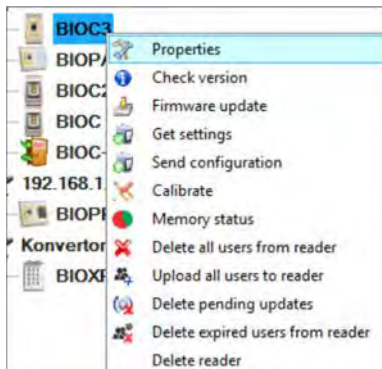


Check at event table if configuration was successful

Time	Portal	Controller	Reader	Door	Event	User
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure wiegand	Success
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure Sensitivity2	Success
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure Sensitivity	Success
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure flexibility level2	Success
8/6/2015 12:59:45	192.168.1.201		BIOC3		Configure flexibility level	Success
8/6/2015 12:59:45	192.168.1.201		BIOC3		Configure parameters	Success

### 9.3 EDIT READER

Right-click on the reader and select **Properties**



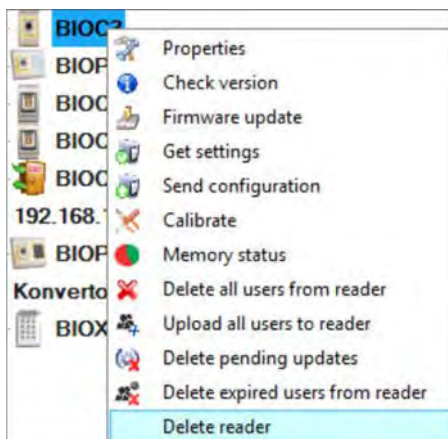
Check at event table if configuration was successful

Time	Portal	Controller	Reader	Door	Event	User
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure wiegand	Success
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure Sensitivity2	Success
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure Sensitivity	Success
8/6/2015 12:59:46	192.168.1.201		BIOC3		Configure flexibility level2	Success
8/6/2015 12:59:45	192.168.1.201		BIOC3		Configure flexibility level	Success
8/6/2015 12:59:45	192.168.1.201		BIOC3		Configure parameters	Success

Edit reader properties and click **Save** button

### 9.4 DELETE READER

Right-click on the reader and select **Delete reader**



Time	Portal	Controller	Reader	Door	Event
10/28/2015 14:27:19	Konvertor_192.168.		asfdasd		Reader deleted

## 9.5 ADD USER

1. Open the Users Window and create a new user.  
Click on "New User", put a name, ID(card number). (8.7)
2. Go to the "Biometric" Tab
3. Select the reader(with left click) from which the enrollment will be done. (8.8)
4. Right click on the fingertip and select enroll. (8.9)
5. In the next 25 sec. present the finger on the selected reader and the finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip. (8.10)  
In these 25 sec. the reader will continuously blink in orange.
6. Repeat point 4&5 for each finger that should be enrolled.
7. 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:

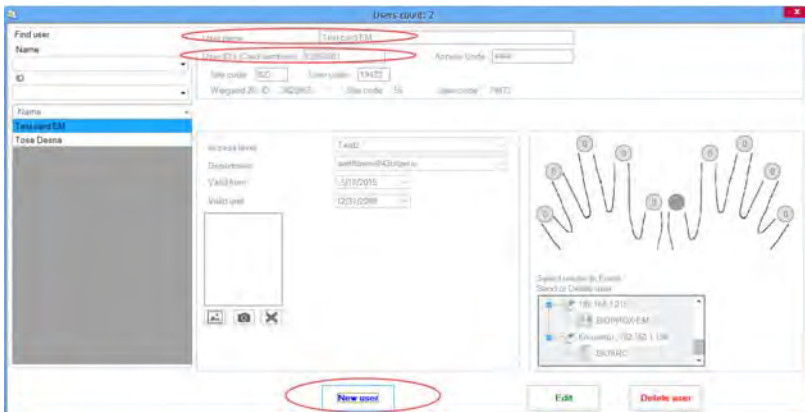
If the user has "Unlimited" Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

### Note:

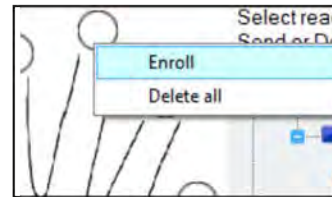
To check if all the fingerprints are sent to the reader, right click on the reader and select "Memory Status". (8.11)  
In the event window a line will appear indicating the number of fingerprints stored in the reader. (8.12)

### Note:

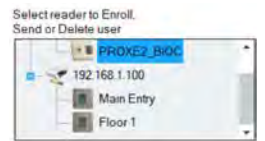
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



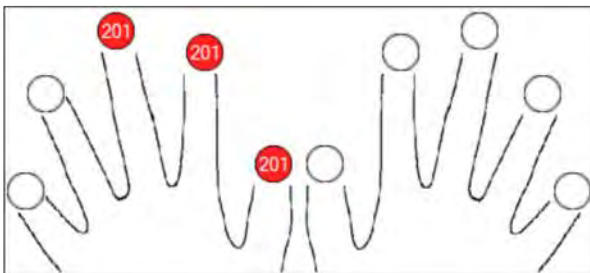
8.7



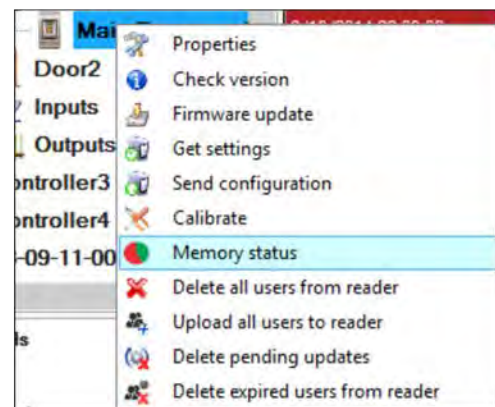
8.9



8.8



8.10



8.11

Reader	Door	Event
B100		Enrolled fingers - 3

8.12

## 9.6 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  
Click on “Delete User”. The User together with its fingerprints will be deleted from both the software and the fingerprint readers. (8.14)

### Deleting all users from the biometric reader

Right click on the reader and select “Delete all users from reader” (8.15)

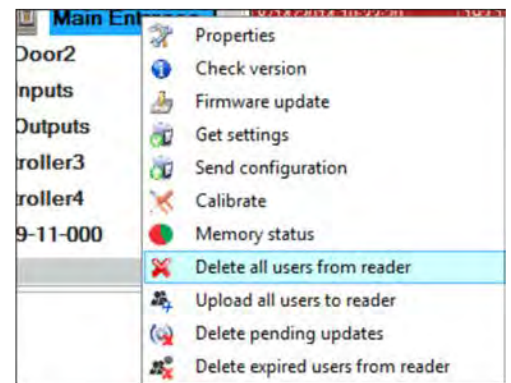
### Delete one or more fingerprints

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”.

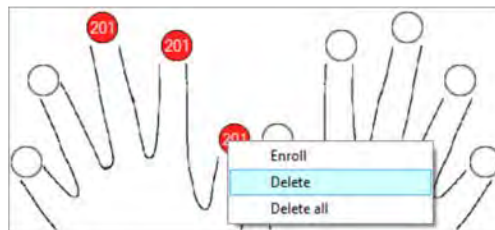
With this procedure the User’s fingerprints are deleted from the software and from the reader. (8.16)



8.14



8.15

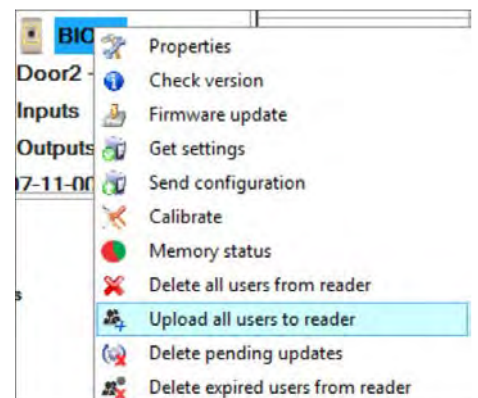


8.16

## 9.7 UPLOADING THE FINGERPRINTS TO THE BIOMETRIC READERS

Right click on the biometric reader  
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.

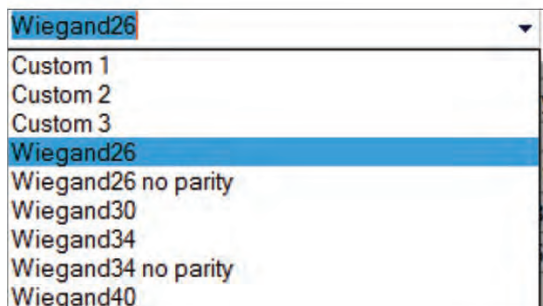
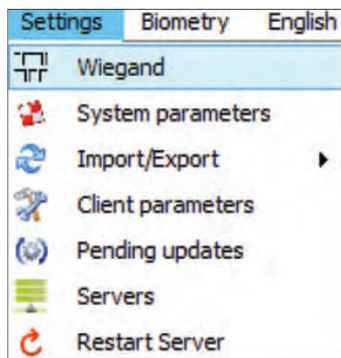


8.17

## 9.8 CUSTOM WIEGAND

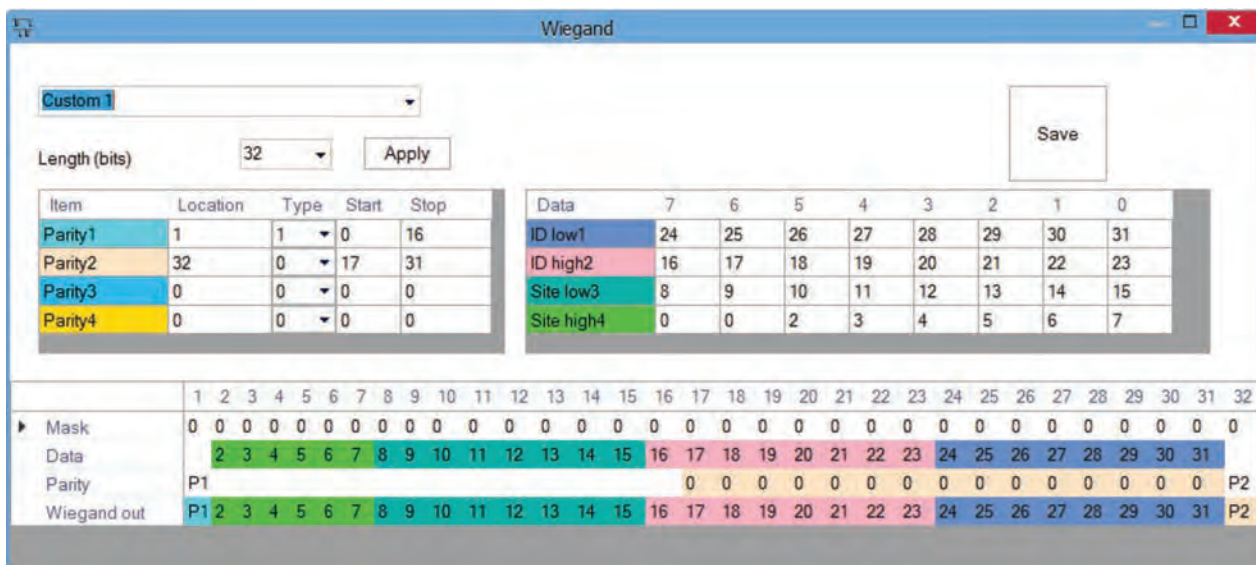
BIOMANAGER CS has defined Wiegand 26, 30, 34, 40 bit as standard options and other 3 Wiegand settings as user definable.

To setup custom Wiegand format  
Select **Wiegand** menu from **Settings**



At Wiegand setup window select one from customs Wiegand

Set Wiegand parameter



Click on **Save button**

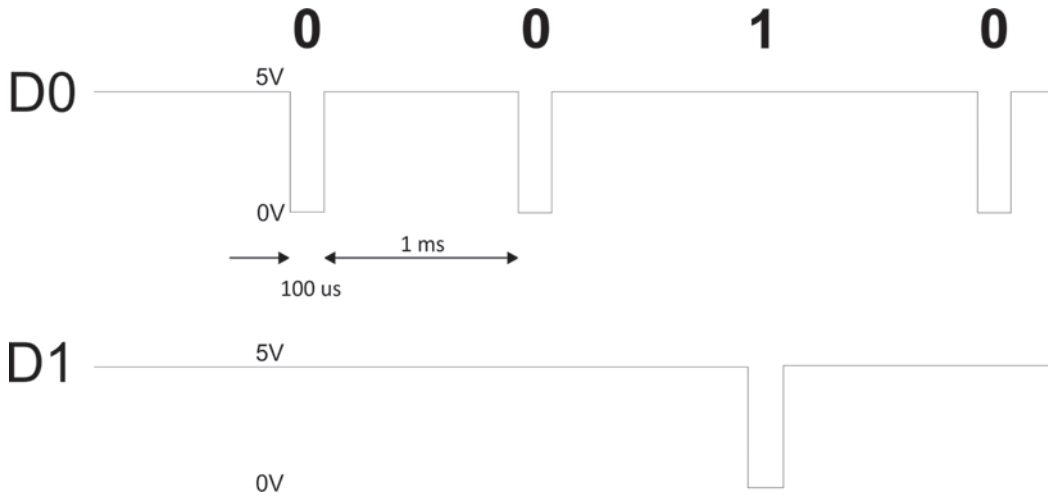
**Note:**  
Wiegand settings are out of scope for common end user. Please ask your installer to set the parameters and do not change it later.

For more information please refer to **BIOMANAGER CS User Manual**

## 10. 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:

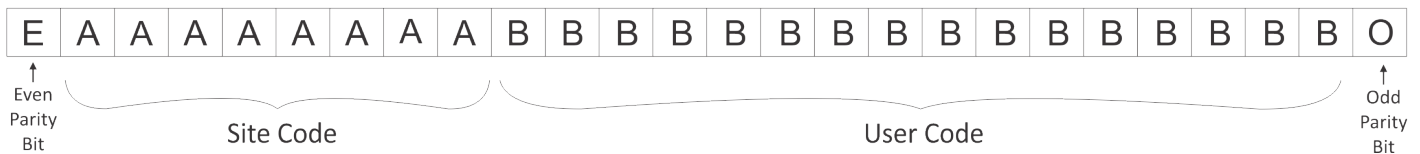
Parity bit (bit 1) + 8 bits header + 16 bits user code = 2 bytes + Parity bit (bit 26)

	P1	XXXXXXXX	XXXXYYYY	YYYYYYYY	P2
Example:	1	170	31527		0
		10101010	0111101100100111		

**Note:** Parity bits are calculated as follows:

P1 = even parity calculated over the bits 2 to 13 (X)

P2 = odd parity calculated over the bits 14 to 25 (Y)



## 11. SAFETY PRECAUTIONS

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.