



# BIOPAD-M Biometric Keypad Reader

## User's Manual

# **Contents**

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| <b><u>1. DESCRIPTION</u></b>                                                        | 3  |
| <b><u>2. SPECIFICATIONS</u></b>                                                     | 3  |
| <b><u>3. MOUNTING</u></b>                                                           | 4  |
| <b><u>4. WIRING</u></b>                                                             | 5  |
| <b><u>5. CONNECTING BIOMETRIC READERS TO EWS CONTROLLER</u></b>                     | 5  |
| 5.1 CONNECTING BIOMETRIC READERS IN SAME RS485 LINE WITH THE EWS CONTROLLERS        | 6  |
| 5.2 CONNECTING BIOMETRIC READERS WHEN ALL THE CONTROLLERS HAVE TCP/IP COMMUNICATION | 6  |
| <b><u>6. CONNECTING BIOMETRIC READERS TO 3RD PARTY CONTROLLER</u></b>               | 7  |
| 6.1 CONVERTERS PIN DESCRIPTION                                                      | 7  |
| <b><u>7. ENROLLMENT</u></b>                                                         | 8  |
| <b><u>8. CONFIGURING THE BIOMETRIC READERS IN PROS SOFTWARE</u></b>                 | 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                             | 12 |
| 8.6 FIRMWARE UPDATE                                                                 | 12 |
| 8.7 ENTRY MODE                                                                      | 13 |
| 8.7.1 Finger or PIN Code                                                            | 13 |
| 8.7.2 Finger and PIN Code                                                           | 13 |
| 8.7.3 Finger Only                                                                   | 13 |
| 8.8 CHANGE PIN CODE LENGTH                                                          | 14 |
| 8.9 SENSOR CALIBRATION                                                              | 15 |
| 8.10 SEND CONFIGURATION                                                             | 15 |
| 8.11 ADVANCED SETTING                                                               | 15 |
| <b><u>9. CONFIGURING THE BIOMETRIC READERS IN BIOMANAGER</u></b>                    | 16 |
| 9.1 ADD READER                                                                      | 16 |
| 9.2 EDIT READER                                                                     | 17 |
| 9.3 DELETE READER                                                                   | 18 |
| 9.4 CALIBRATE SENSOR                                                                | 18 |
| 9.5 ADD USER                                                                        | 18 |
| 9.6 EDIT USER                                                                       | 18 |
| 9.7 DELETE USERS                                                                    | 19 |
| 9.8 ENROLL FINGERS                                                                  | 19 |
| 9.9 UPLOAD FINGERPRINTS TO READER                                                   | 19 |
| 9.10 DELETE FINGERPRINTS                                                            | 20 |
| 9.10.1 Deleting one user from the biometric reader                                  | 20 |
| 9.10.2 Deleting all users from the biometric reader                                 | 20 |
| 9.11 COMPLEX USER UPLOAD                                                            | 20 |
| 9.12 CUSTOM WIEGAND                                                                 | 21 |
| <b><u>10. WIEGAND PROTOCOL DESCRIPTION</u></b>                                      | 22 |
| <b><u>11. SAFETY PRECAUTIONS</u></b>                                                | 23 |
| <b><u>12. TROUBLESHOOTING</u></b>                                                   | 23 |

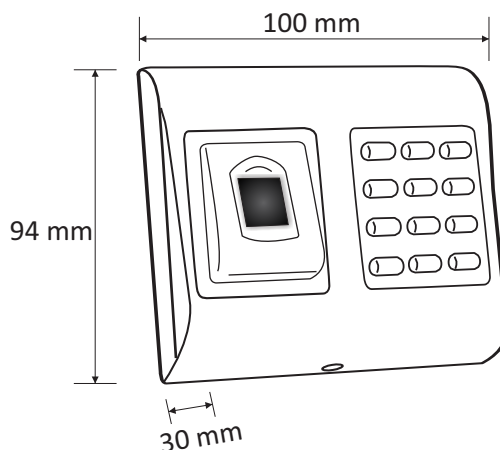
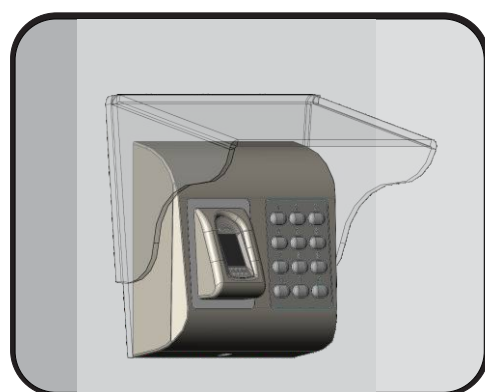
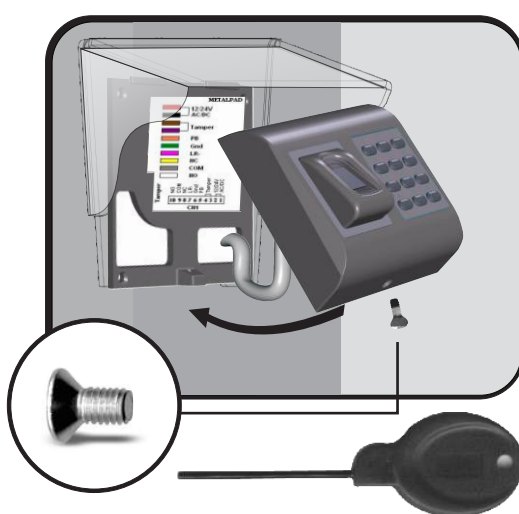
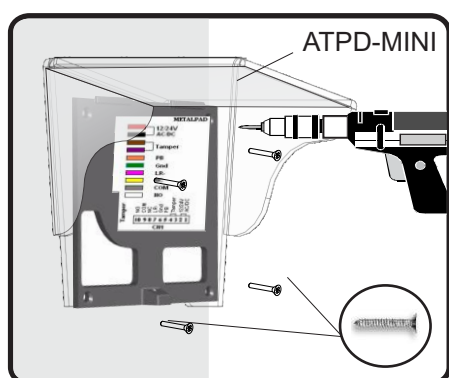
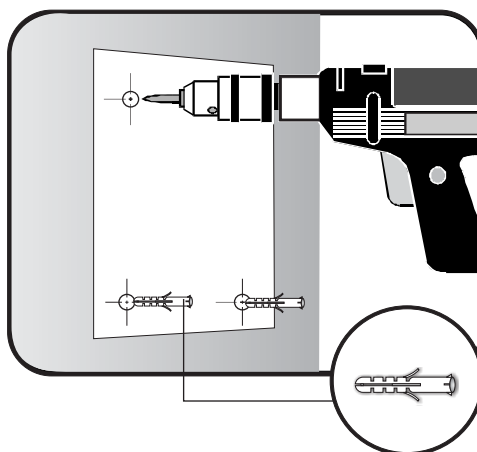
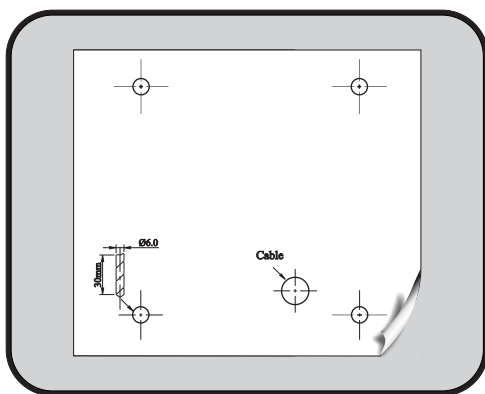
## 1. DESCRIPTION

BIOPAD-M is a Wiegand biometric keypad for access control applications with backlit keys and programmable wiegand output. It offers storage up to 9500 fingerprints, programmable Wiegand Output (8 to 128 bits) and selectable PIN Code length. 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

|                                   |                                                                           |
|-----------------------------------|---------------------------------------------------------------------------|
| <b>Fingerprint capacity</b>       | up to 9500 fingerprints                                                   |
| <b>Technology</b>                 | Biometry and Keypad                                                       |
| <b>Authentication</b>             | Finger, PIN Code, Finger or/and PIN Code                                  |
| <b>Fingerprints per user</b>      | 1-10 fingerprints                                                         |
| <b>PIN Code Length</b>            | 1- 8 Digits                                                               |
| <b>Interface</b>                  | Wiegand 8 to 128 bits; Default: Wiegand 26bit                             |
| <b>Protocol programming</b>       | By PROS software (EWS system) and BIOMANAGER (all access control systems) |
| <b>Cable distance</b>             | 50m                                                                       |
| <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 (BIOE)                       |
| <b>Panel Connection</b>           | Cable, 1m                                                                 |
| <b>Green and Red LED</b>          | Externally Controlled                                                     |
| <b>Orange LED</b>                 | Idle mode                                                                 |
| <b>Buzzer</b>                     | Yes                                                                       |
| <b>Backlight ON/OFF</b>           | Yes, by software settings                                                 |
| <b>Tamper</b>                     | Yes                                                                       |
| <b>Consumption</b>                | Max. 130mA                                                                |
| <b>IP Rating</b>                  | 65                                                                        |
| <b>Power supply</b>               | 9-14V DC                                                                  |
| <b>Operating Temperature</b>      | -15°C to +60°C                                                            |
| <b>Dimensions (mm)</b>            | 100 x 94 x 30                                                             |
| <b>Housing</b>                    | Moulded Aluminium                                                         |
| <b>Colour</b>                     | Silver, Red, Green, Dark Grey, Blue, White                                |

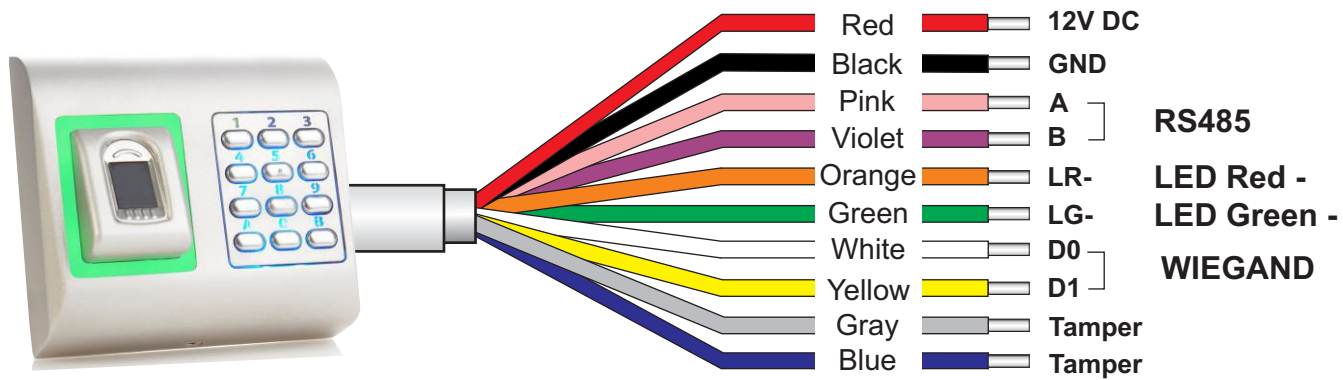
### 3. MOUNTING



If the biometric reader is installed and used outdoor, the reader **MUST** be fitted with the ATPD-MINI polycarbonate cover available in our accessories in order to protect the sensor from direct rainfall. The operating temperature of the product is between -15°C - + 60°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



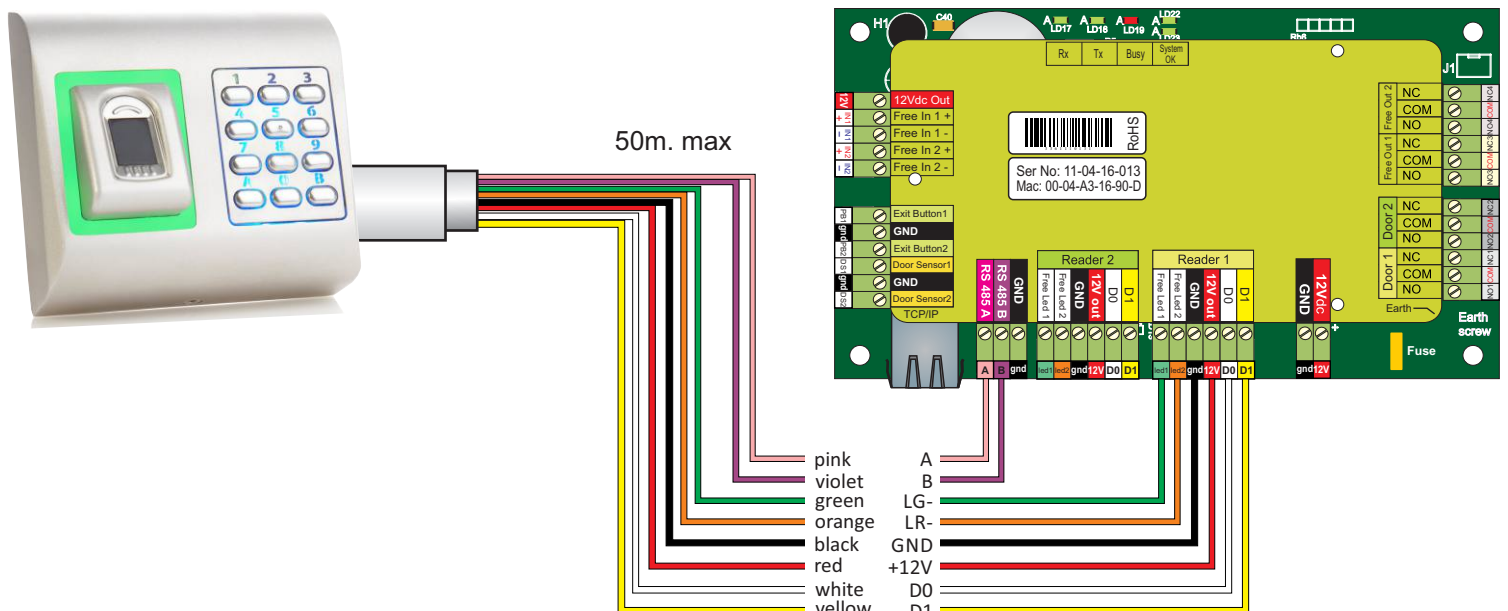
Tricolor LED (Red, Green, Orange)



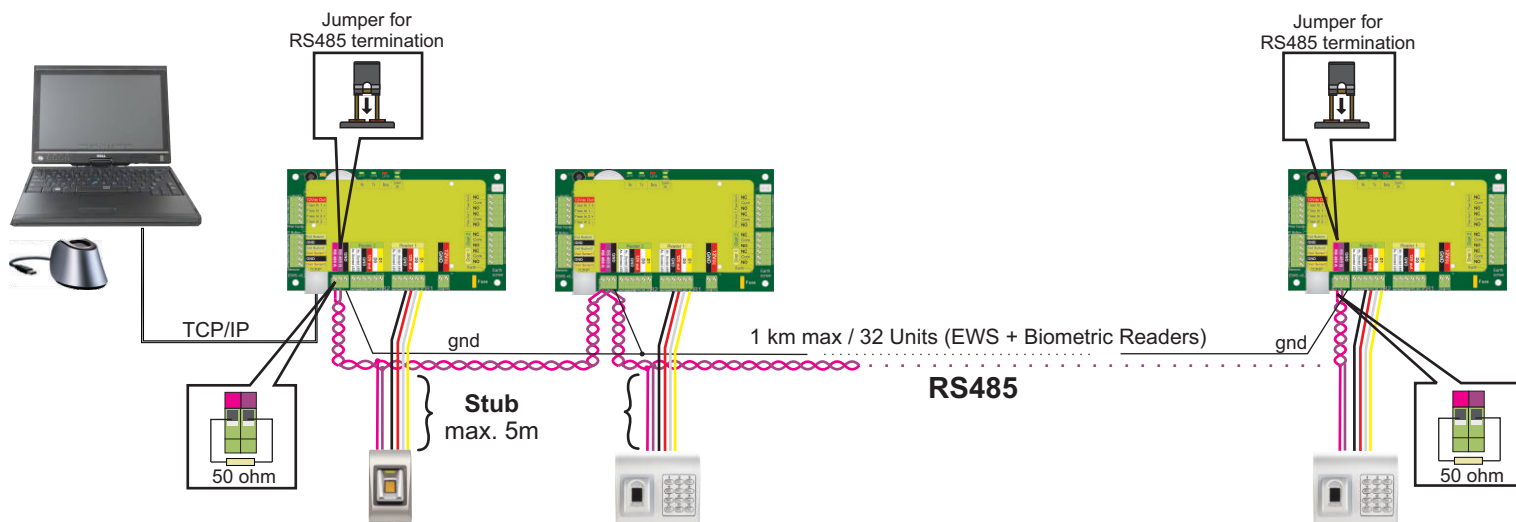
| 12V DC | 9-14V DC          |
|--------|-------------------|
| GND    | ground            |
| A      | RS485 A           |
| B      | RS485 B           |
| LR-    | Red LED -         |
| LG-    | Green LED -       |
| D1     | Data 1            |
| D0     | Data 0            |
| Tamper | Tamper Switch(NO)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

## 5. CONNECTING 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 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.

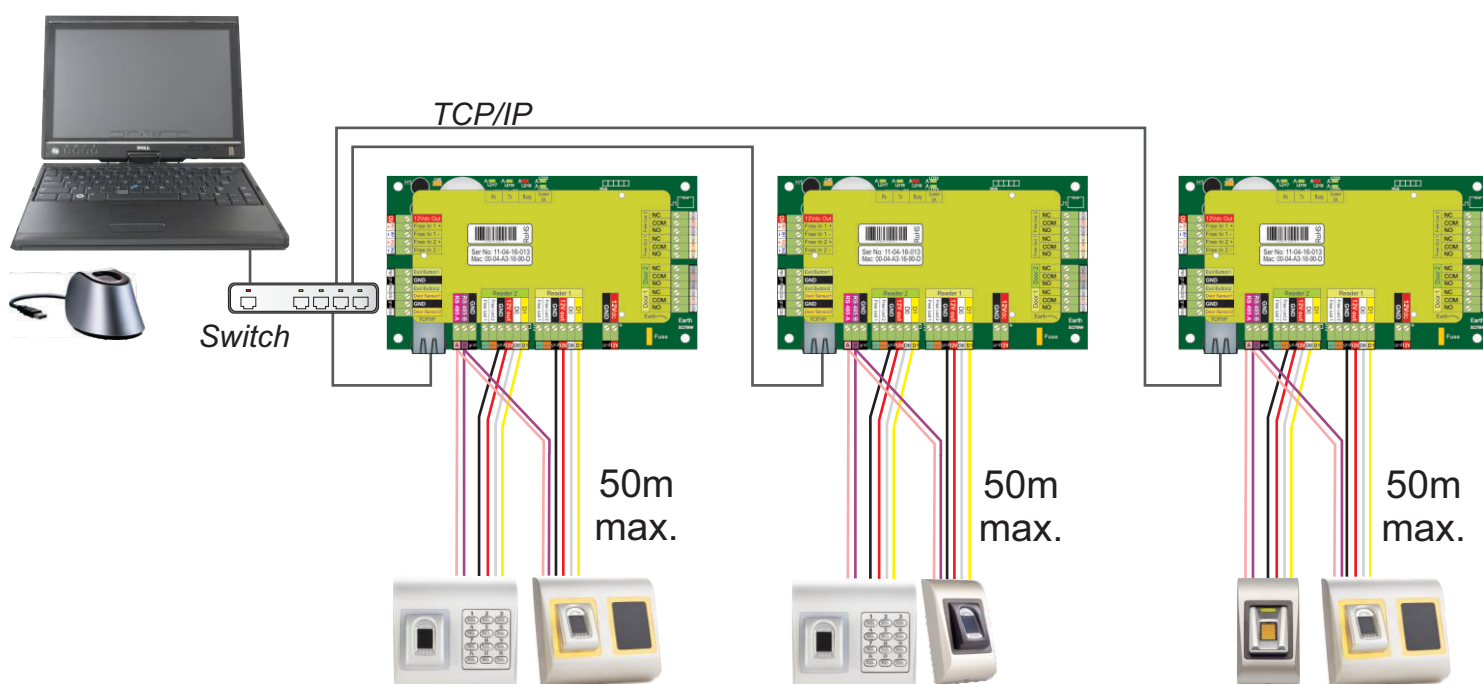


## 5.1 CONNECTING BIOMETRIC READERS IN SAME RS485 LINE WITH THE EWS CONTROLLERS



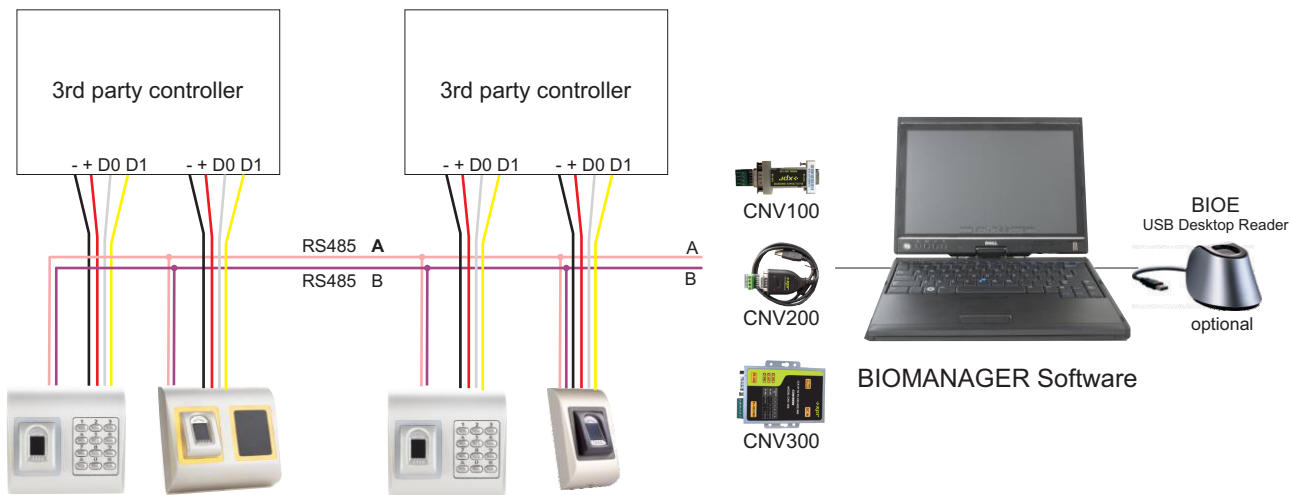
- The Biometric readers are connected through RS485 bus. The same RS485 bus that the EWS controllers are connected to.
- Maximum units in one network (EWS + Biometric readers) is 32.
- If there are more than 32 units in one network, please utilize RS 485 HUB to connect.
- The RS485 Line should be configured 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 RS485 backbone as short as possible. Maximum length of the stub is dependant of the installation (total number of devices in RS485 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



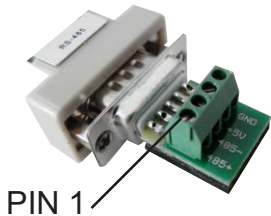
- When all the controllers are connected via TCP/IP, then the RS485 network becomes local (from Reader 1 to the Controller then to the Reader 2).
- Connect the readers directly to the Rs485 terminals in each controller.
- If the distance Reader-Controller is high (50meters) and if the communication with the reader can not be established, then terminate the RS485 network by closing the jumper in the EWS Controller or as described in chapter 4.

6. CONNECTING BIOMETRIC READERS TO THIRD PARTY CONTROLLERS

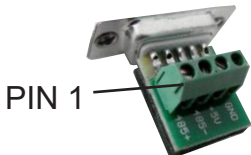


- Connect the lines D0, D1, Gnd and +12V to the third party controller.
- Connect the RS485 Line (A, B) to the converter. Connect the converter in the PC.
- Fingerprint enrollment is done from the PC Software. Connection between the Biometric readers and the PC must be established.
- The Biometric readers communicate with each other with a RS485 and with the PC Software through a Converter.
- The RS485 Line should be configured in the form of a daisy chain, NOT in a form of a star. Keep the stubs from the RS485 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



**CNV100**  
Converter RS485 to RS232  
Does not requires installation



**CNV200**  
Converter RS485 to USB  
Requires installation as USB serial device (refer to CNV200 Manual). The Drivers are located on the CD.

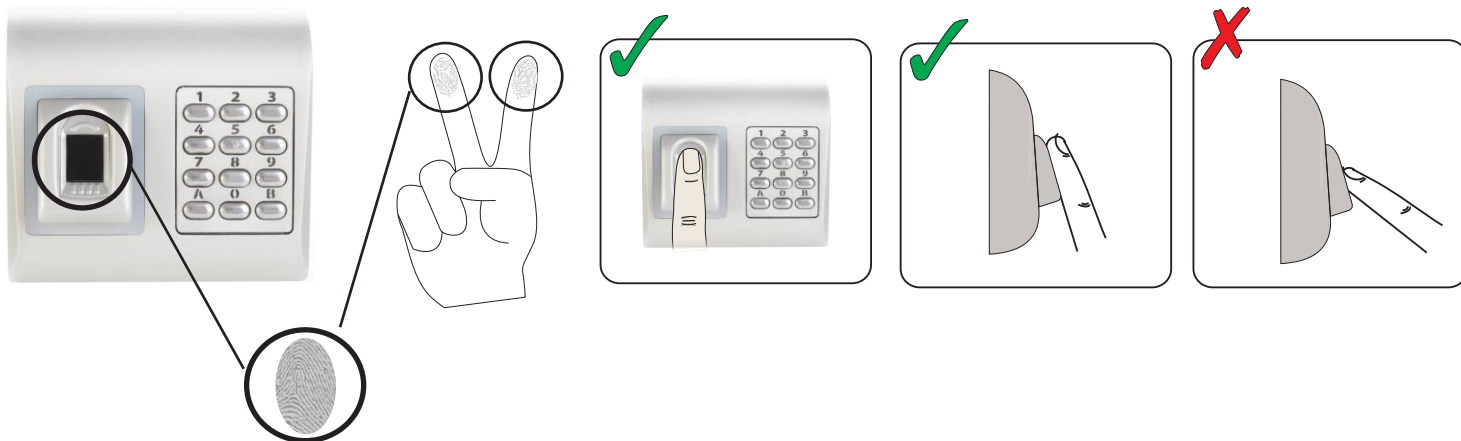


**CNV300**  
Converter RS485 to TCP/IP  
Does not require installation. IP address set through Internet Browser(refer to CNV300 Manual)

| 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

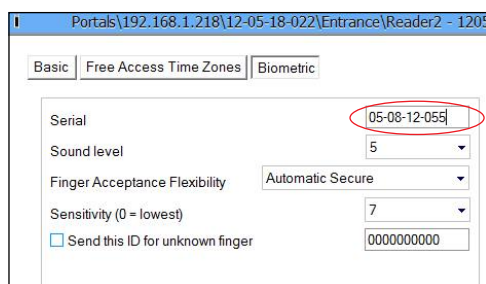
1. Expand the Door item to view the readers
2. Right click on the reader and select properties (8.1)
3. In the Basic tab, for "Type" of the Reader select "BIOPAD-M". (8.2)
4. After selecting the type, a third tab will appear "Biometric". Go to that tab and put the serial number of the Biometric Reader.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

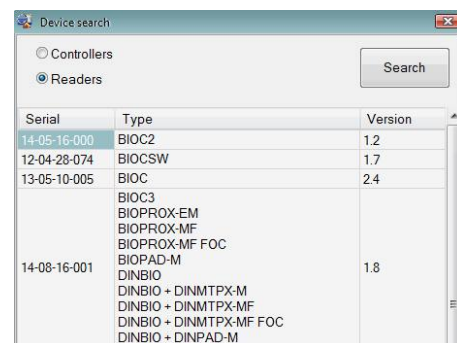
To check if the reader is On Line, right click on the reader and select "Check version". In the Event Window a message should appear "Device ON Line, Type: "BIOPAD-M" (8.6)



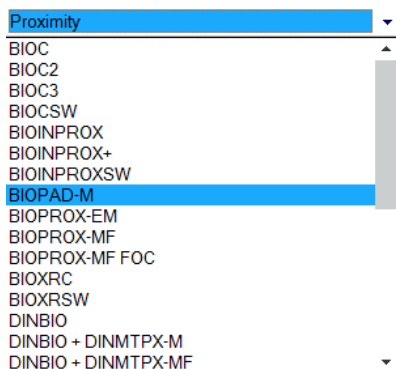
8.1



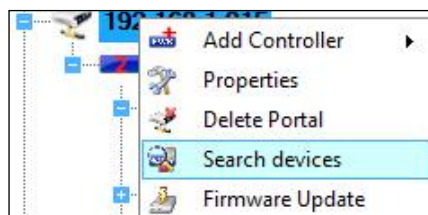
8.3



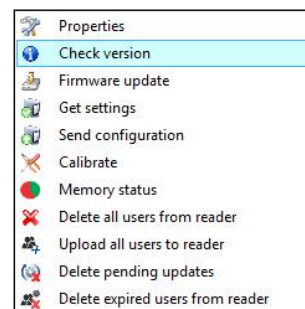
8.5



8.2



8.4



8.6



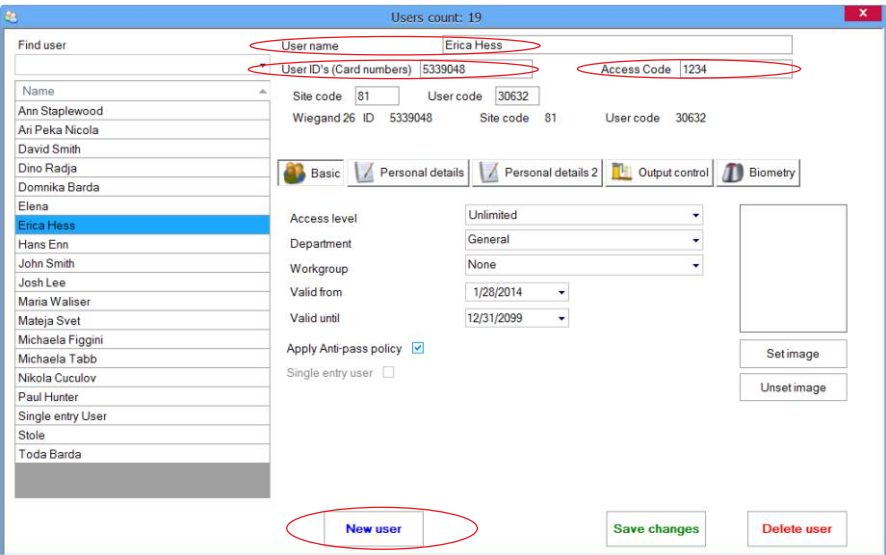
8.2 ENROLLING FINGERPRINTS FROM A READER

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

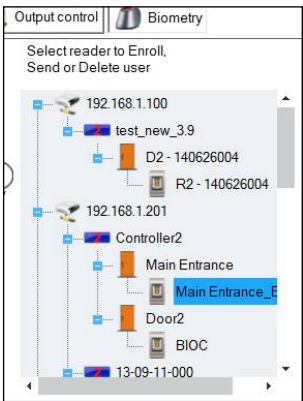
**Example:**  
If the user has “Unlimited” Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

**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)

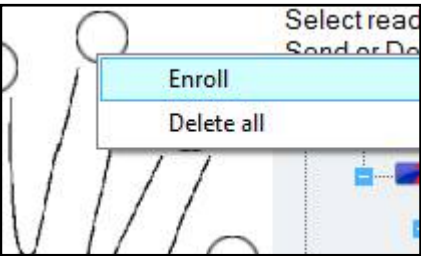
**Note:**  
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



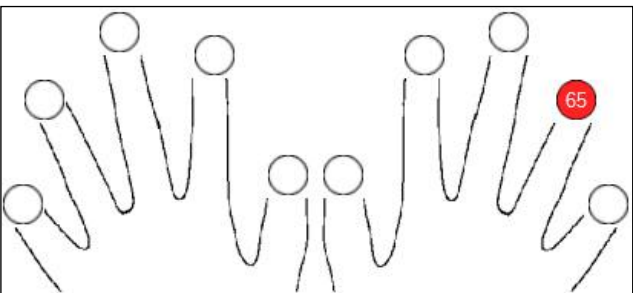
8.7



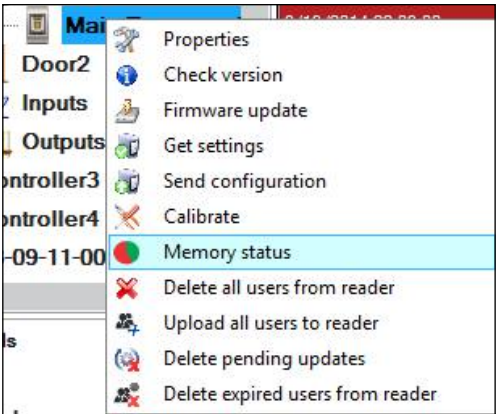
8.8



8.9



8.10



8.11

| Reader              | Door | Event                 |
|---------------------|------|-----------------------|
| Main Entrance_BIOC2 |      | Enrolled fingers : 29 |

8.12

8.3 ENROLLING FINGERPRINTS FROM DESKTOP READER

Plug the Desktop Reader (BIOE) 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. (8.13)

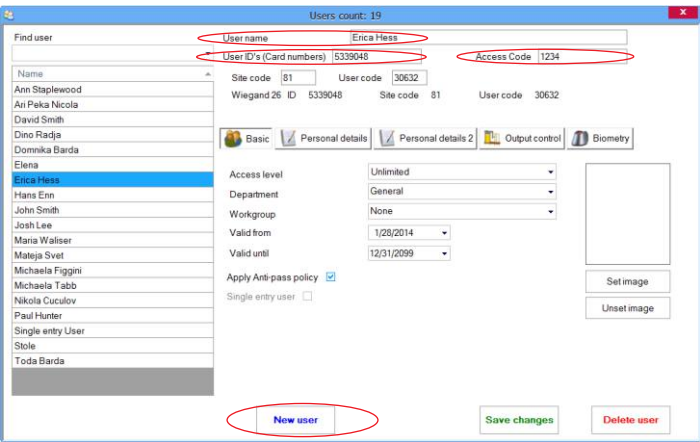
- 1. Open the Users Window and create a new user.  
Click on “New User”, put a name, ID(card number) and Access Code. (8.7)
- 2. Go to the “Biometric” Tab
- 3. Select the USB desktop Reader (with left click).
- 4. Place the finger on the BIOE, right click on the fingertip and select enroll. (8.9)
- 5. 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 CS server and the reader. No need for additional enrollment or actions. The fingerprints will be sent as soon as communication is established.

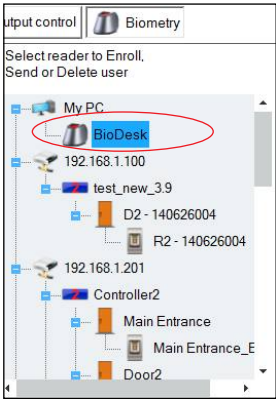
**Example:**  
If the user has “Unlimited” Access level then the fingerprints will be sent to all readers, if the user has Access level only for Reader1 and Reader 3 then the fingerprints will be sent only to those two readers.

**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)

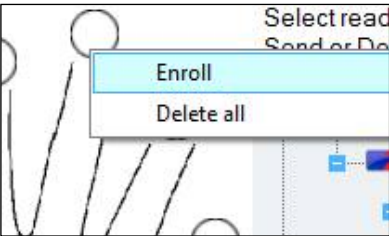
**Note:**  
If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller, the one written in the field User ID(card Number).



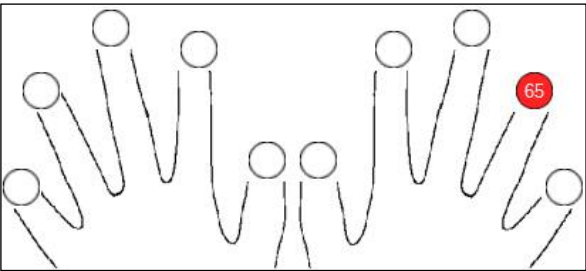
8.7



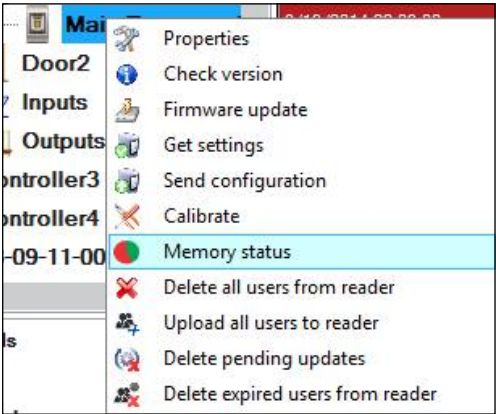
8.13



8.9



8.10



8.11

| Reader              | Door | Event                 |
|---------------------|------|-----------------------|
| Main Entrance_BIOC2 |      | Enrolled fingers - 29 |

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)

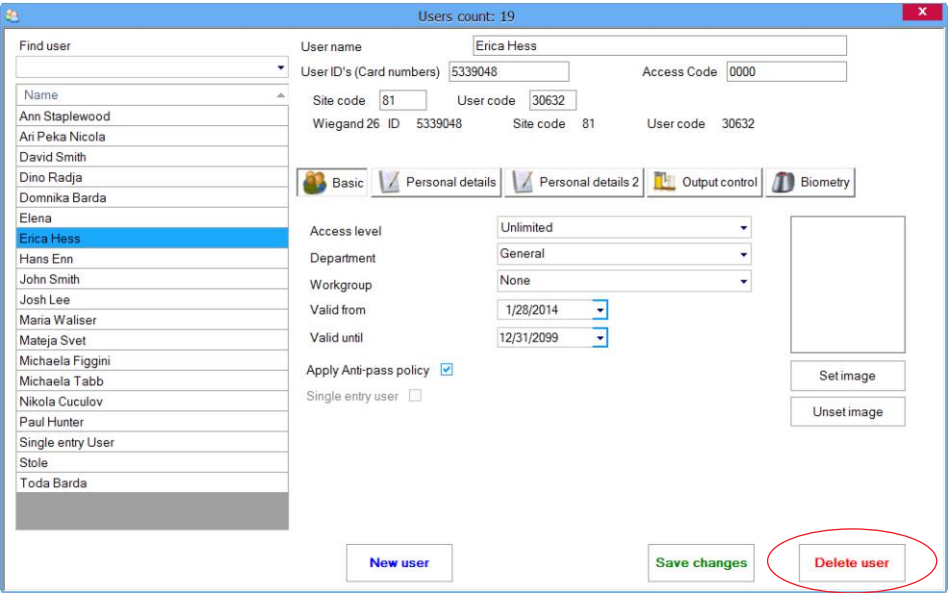
Deleting all users from the biometric reader

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

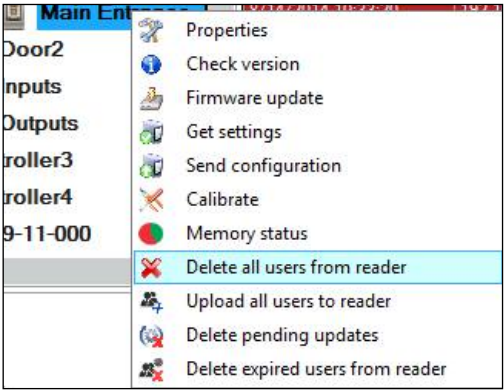
Delete one or more fingerprints

- 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".

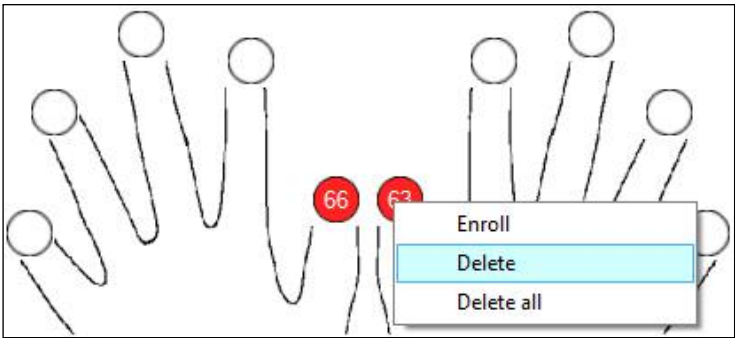
With this procedure the User's fingerprints are deleted from the software and from the reader. (8.16)



8.14



8.15

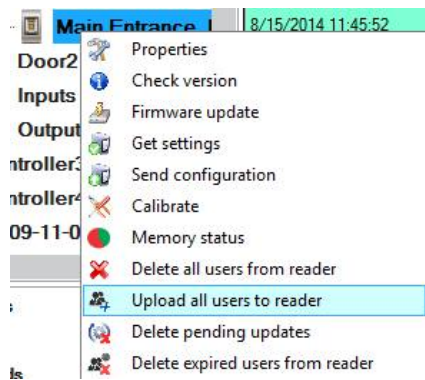


8.16

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.

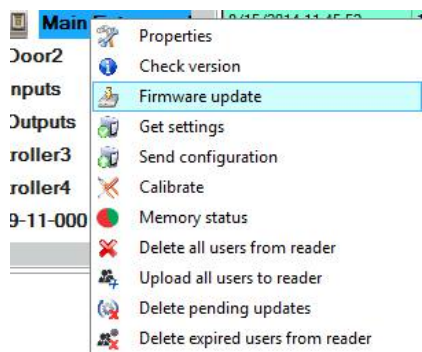
**Note:** Use this feature when you change or add a reader, if pending tasks are deleted in the software or if there are doubts that fingerprints in the reader memory are not synchronized with the software database.  
In normal usage, the fingerprints are sent automatically and this feature is not used.



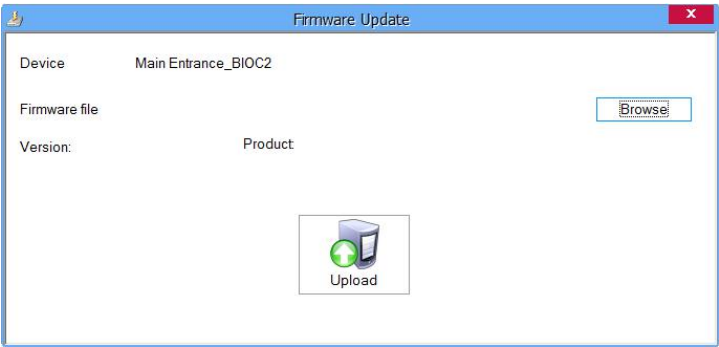
8.17

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

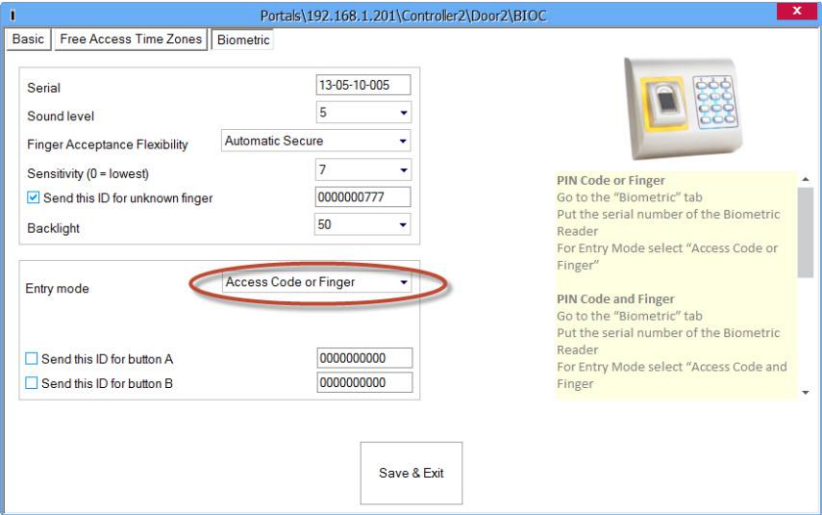


8.19

8.7 ENTRY MODE

8.7.1 Finger or PIN Code

Right click on the biometric reader  
Select “Properties” and go to the “Biometric” tab  
For Entry Mode select “Access Code or Finger” (8.20)

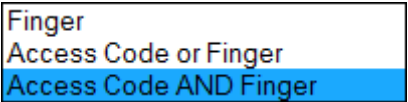


8.20

8.7.2 Finger and PIN Code

Right click on the biometric reader  
Select “Properties” and go to the “Biometric” tab  
For Entry Mode select “Access Code and Finger” (8.21)

Use of the double security mode:  
Type the PIN Code (ex. 3434), in the next 8 sec. the  
reader will blink in orange waiting for the finger.  
Present the finger.

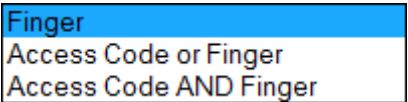


8.21

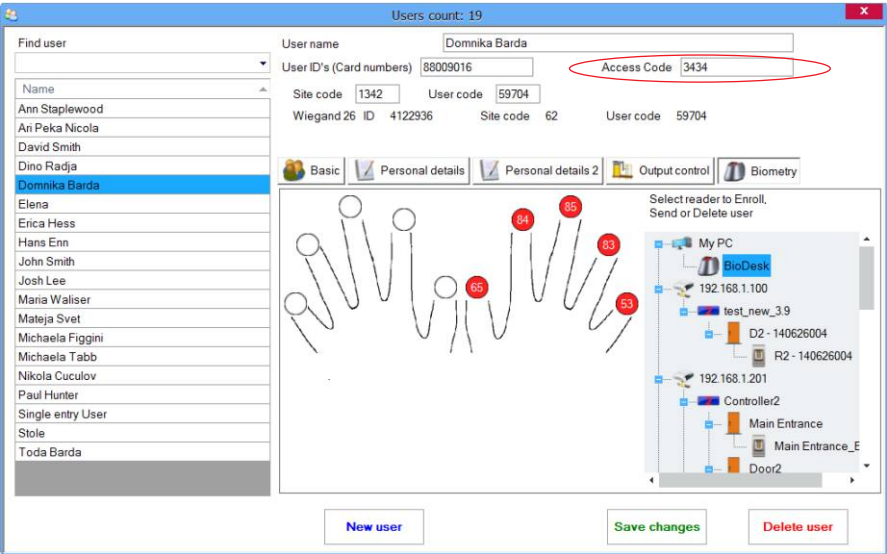
8.7.3 Finger Only

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 keypad will become inactive.



8.22



8.21

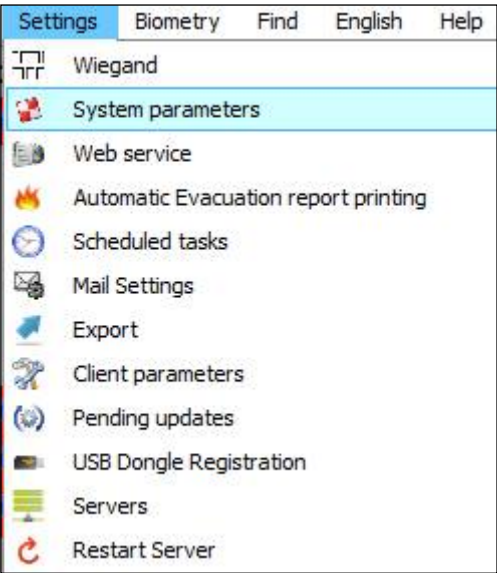


8.8 CHANGE PIN CODE LENGTH

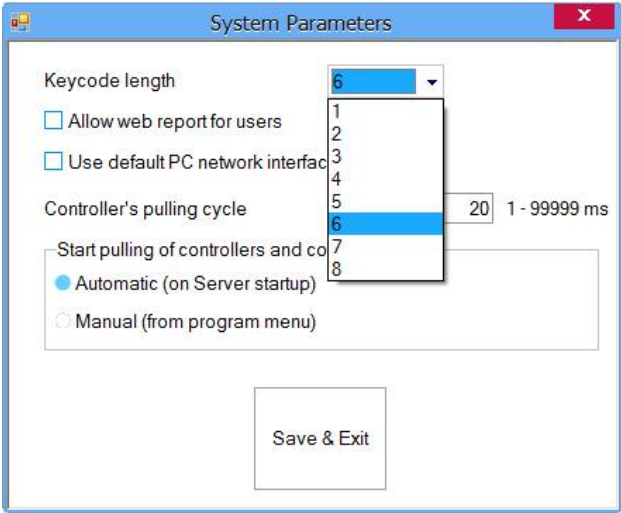
Go to Settings/ System parameters. (8.24)  
Select the desired length and click “Save&Exit”. (8.25)  
All the readers in the network will automatically receive the change

**Note:** It is recommended to do this setting immediately after installing the software, as this parameter will set the available number of PIN Code digits in the user form.

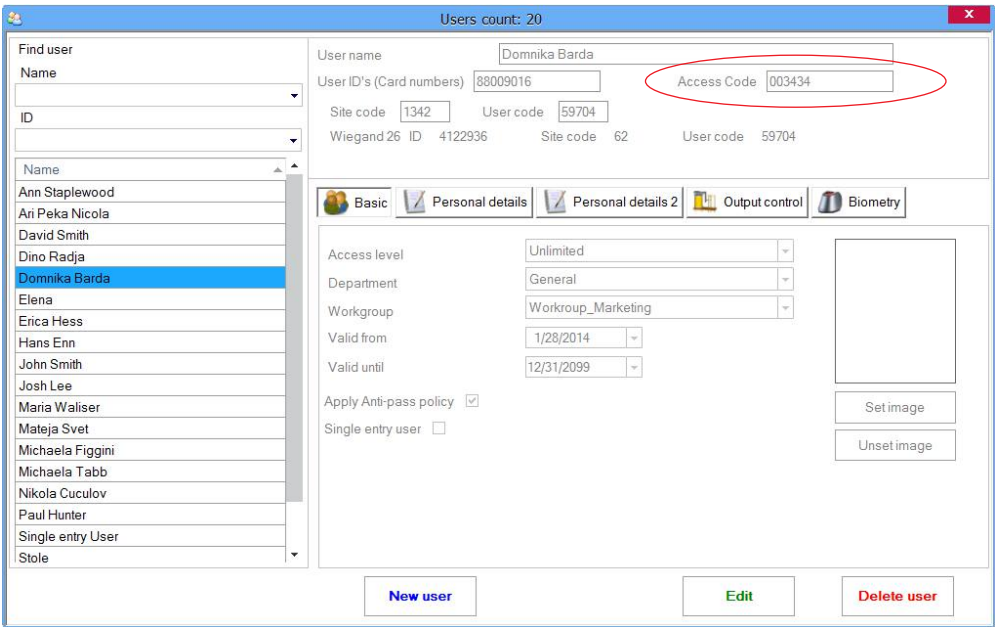
**Example:** If the PIN code length is set to 6 digits, then in the Users Window, the PIN Code will require 6 digits entry. (8.26)



8.24



8.25

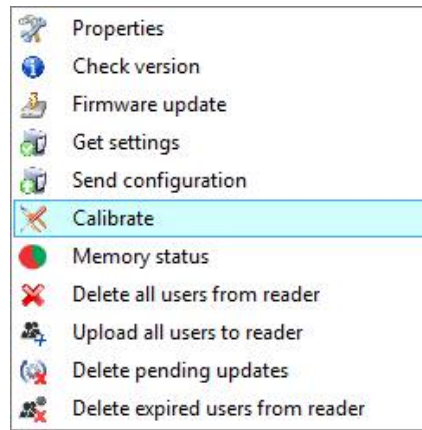


8.26

## 8.9 SENSOR CALIBRATION

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

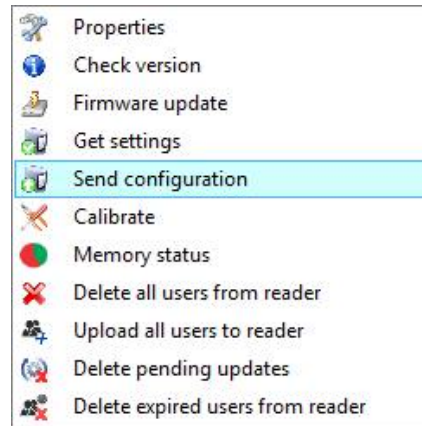
**Note:** It is recommended to do a calibration while commissioning the reader and in cases when there are problems with reading the fingers



## 8.10 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.



## 8.11 ADVANCED SETTINGS

### Send This ID for:

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

**Unknown PIN** sends the desired Wiegand when an unknown Pin Code is applied.

**Button “A” Pressed** sends the desired Wiegand when button “A” is pressed.

**Button “B” Pressed** sends the desired Wiegand when button “B” is pressed.

Click on the Save & Exit button

### Sound level:

Sound level 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.

| Basic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Free Access Time Zones | Biometric |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-----------|
| <div>Serial <input type="text" value="13-05-10-005"/></div> <div>Sound level <input type="text" value="5"/></div> <div>Finger Acceptance Flexibility <input type="text" value="Automatic Secure"/></div> <div>Sensitivity (0 = lowest) <input type="text" value="7"/></div> <div><input checked="" type="checkbox"/> Send this ID for unknown finger <input type="text" value="0000000777"/></div> <div>Backlight <input type="text" value="50"/></div> <div>Entry mode <input type="text" value="Access Code or Finger"/></div> <div><input type="checkbox"/> Send this ID for button A <input type="text" value="0000000000"/></div> <div><input type="checkbox"/> Send this ID for button B <input type="text" value="0000000000"/></div> <div>Save &amp; Exit</div> |                        |           |



## 9 CONFIGURING THE BIOMETRIC READERS IN BIOMANAGER

BioManager 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.

Note: The Desktop Biometric reader BIOE is only compatible to Biometric readers with capacitive sensor, not with the ones with thermal sensor.

- 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

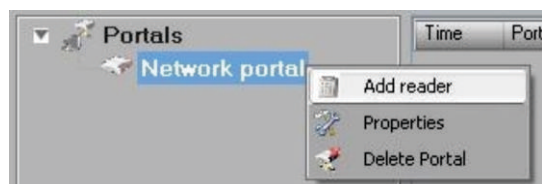
PIN Code length configuration (1 to 8 digits) and PIN Code transfer.

- Wiegand Output Configuration

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

### 9.1 ADD READER

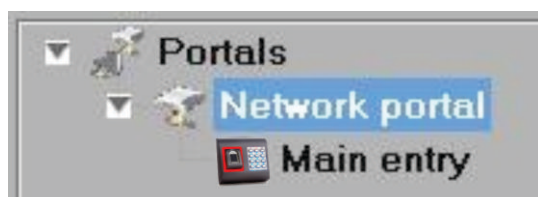
Right-click on the portal connected to the reader and select Add reader



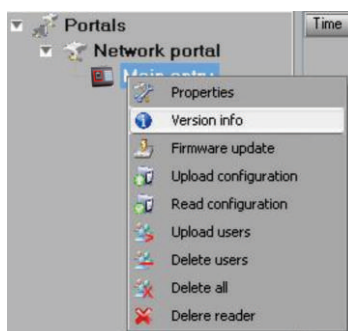
Fill the Reader form

A screenshot of the 'Reader properties' dialog box. It contains several fields and checkboxes. The fields are: 'Name' (text box), 'Serial number' (text box with dashes), 'Type' (dropdown menu), 'Wiegand type' (dropdown menu with 'Wiegand26' selected), 'Sound level' (text box with '5' selected), 'Finger acceptance flexibility' (dropdown menu with 'Automatic More Secure' selected), and 'Entry mode' (dropdown menu with 'Finger' selected). Below these are four checkboxes: 'Wrong finger ID', 'Wrong code ID', 'Send this ID for button A', and 'Send this ID for button B'. To the right of each checkbox is a text box containing '0000000000'. At the bottom is a 'Save' button.

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



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



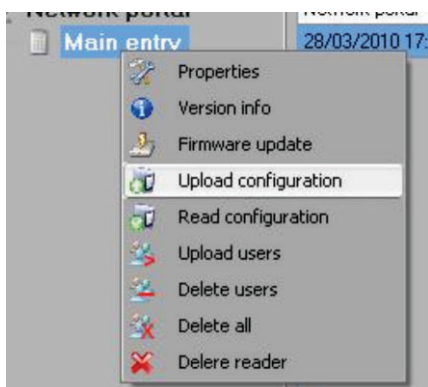
If reader is online, new line is added on top of the event table

| Time                | Portal         | Reader     | Event         | User                      |
|---------------------|----------------|------------|---------------|---------------------------|
| 28/03/2010 17:41:30 | Network portal | Main entry | Device online | Type: BioXr Version: 1.22 |

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

| Time           | Portal     | Reader      | Event | User |
|----------------|------------|-------------|-------|------|
| Network portal | Main entry | No response |       |      |

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

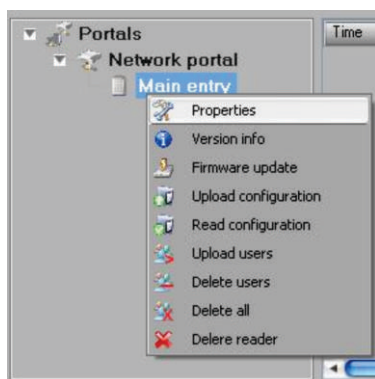


Check at event table if configuration was successful

| Time                | Portal         | Reader     | Event                       | User   |
|---------------------|----------------|------------|-----------------------------|--------|
| 28/03/2010 17:58:16 | Network portal | Main entry | Configure Wiegand           | Succes |
| 28/03/2010 17:58:15 | Network portal | Main entry | Configure Flexibility Level | Succes |
| 28/03/2010 17:58:15 | Network portal | Main entry | Save Flexibility Level      | Succes |
| 28/03/2010 17:58:15 | Network portal | Main entry | Configure parameters        | Succes |

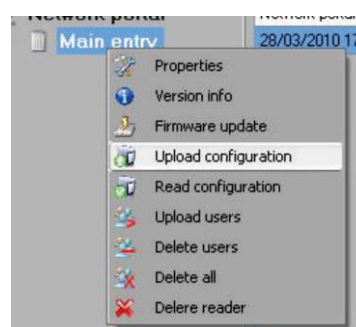
## 9.2 EDIT READER

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



Edit reader properties and click **Save** button

Right click on the reader and select **Upload configuration**

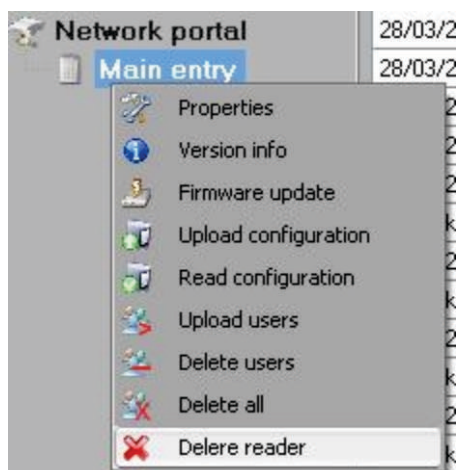


Check at event table if configuration was successful

| Time                | Portal         | Reader     | Event                       | User   |
|---------------------|----------------|------------|-----------------------------|--------|
| 28/03/2010 17:58:16 | Network portal | Main entry | Configure Wiegand           | Succes |
| 28/03/2010 17:58:15 | Network portal | Main entry | Configure Flexibility Level | Succes |
| 28/03/2010 17:58:15 | Network portal | Main entry | Save Flexibility Level      | Succes |
| 28/03/2010 17:58:15 | Network portal | Main entry | Configure parameters        | Succes |

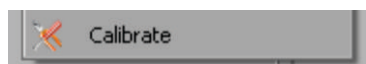
### 9.3 DELETE READER

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



### 9.4 CALIBRATE SENSOR

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



See the events panel to check the calibration flow

It is recommended to do sensor calibration once after reader is mounted. Clean the fingerprint sensor before calibration.

### 9.5 ADD USER

At user table, click on the last empty user field and enter user name

| # | User      | ID (User code) | PIN code |
|---|-----------|----------------|----------|
|   | Tom Smith | 12345          | 1111     |
|   |           | 0              | 0        |

Click on ID (User code) field and enter ID number. This number will be sent by the reader to the access controller when user finger is recognized by the reader

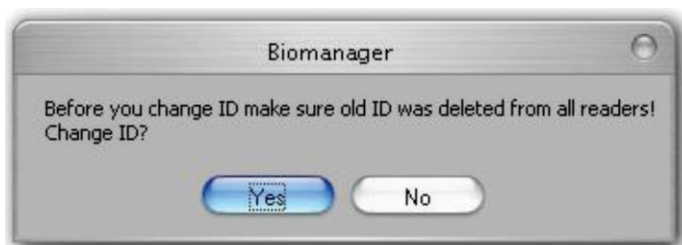
Click on PIN code field and enter the PIN. PIN code is used at readers with keypad. When PIN code is typed at reader, User ID will be sent to the access controller

### 9.6 EDIT USER

- Find the user at user table to edit
- Click on the user field for edit (Name, ID or PIN)
- Type new value
- Press Enter on the keyboard

#### Important:

**When ID is changed, warning message is displayed reminding that if ID exist in some reader, should be deleted from reader prior to change.**



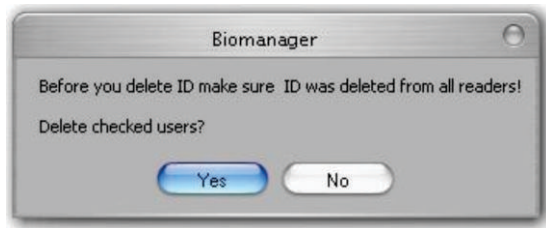
## 9.7 DELETE USERS

- Check the users to be deleted
- Right-click on the users table
- Click on **Delete checked users** menu

|                                     |         |     |      |
|-------------------------------------|---------|-----|------|
| <input checked="" type="checkbox"/> | John Do | 567 | 0067 |
| <input type="checkbox"/>            | Lane Ly |     | 0000 |
| <input type="checkbox"/>            |         |     | 0    |

Delete checked users  
Select all  
Clear all

Confirm warning message



## 9.8 ENROLL FINGERS



- Select the User in the User Column, not the check box (the check box is for sending the fingerprints) and the User name cell will turn blue
- Select the Biometric reader or Desktop reader BIOE from where the enrollment will be done

| #                        | User      | ID (User code) | PIN code |
|--------------------------|-----------|----------------|----------|
| <input type="checkbox"/> | Tom Smith | 12345          | 1111     |
| <input type="checkbox"/> | John Do   | 567            | 0067     |
| <input type="checkbox"/> | Lane Ly   | 456            | 0000     |
| <input type="checkbox"/> |           | n              | n        |

A diagram showing a finger being swiped on a reader. A context menu is open with options: "Enroll", "Delete", and "Delete all".

Right click on the fingertip and select **Enroll**



Swipe the finger on the Reader and the finger tip will become blue, with percentage of successful enrollment given right beside the fingertip

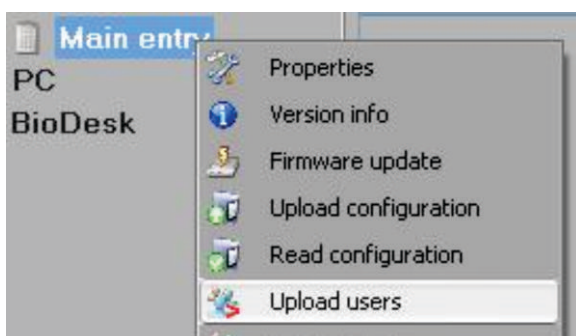
**Note:** If more fingerprints are added for one user, all fingerprints will send the same Wiegand Code to the controller.

## 9.9 UPLOAD FINGERPRINTS TO READER

Check the users which fingerprints will be sent to the Reader

| #                                   | User      |
|-------------------------------------|-----------|
| <input checked="" type="checkbox"/> | Tom Smith |
| <input checked="" type="checkbox"/> | John Do   |
| <input checked="" type="checkbox"/> | Lane Ly   |

Right-click on the Biometric reader those users should be sent and select **Upload users**



As each user is being sent, the checkbox will become unchecked indicating that the user is successfully sent. In the same time the orange LED of the Biometric reader blinks

Note: Average time for transferring one finger template is 0,6 sec.

Note: The PIN Codes are also being sent, if there are any.

9.10 DELETE FINGERPRINTS

After the transfer, the fingerprint are stored in the Biometric reader and in the PC.

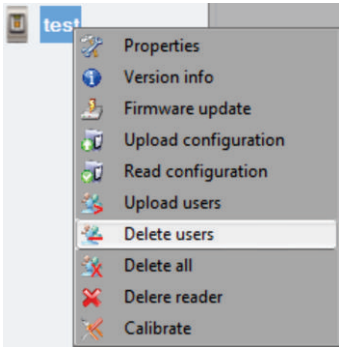
Deleting can be done only in the software, only in the readers or from the both places.

9.10.1 Deleting one user from the biometric reader

Select the users checkbox.

| #                                   | User      |
|-------------------------------------|-----------|
| <input checked="" type="checkbox"/> | Tom Smith |
| <input checked="" type="checkbox"/> | John Do   |
| <input checked="" type="checkbox"/> | Lane Ly   |

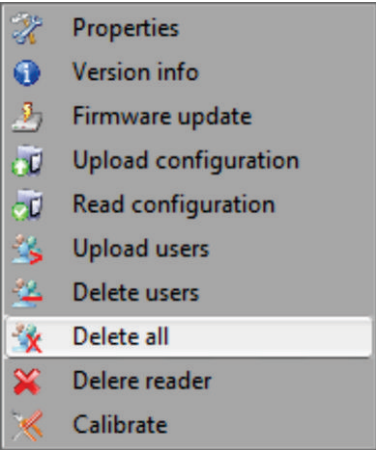
Right click on the Reader and select **Delete Users**



The user is deleted from the reader, but his fingerprints are still in the software's database. They can be sent ones again without the need of re enrollment.

9.10.2 Deleting all users from the biometric reader

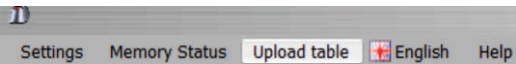
Right click on the Reader and select **Delete all**



9.11 COMPLEX USER UPLOAD

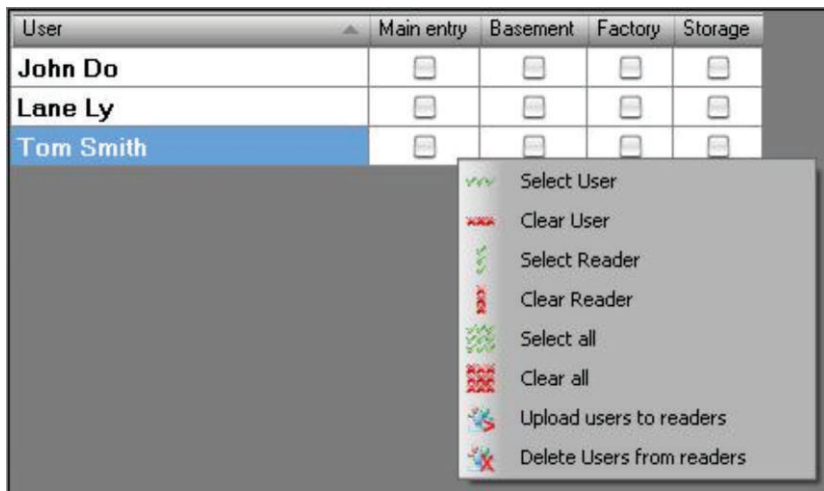
Complex user upload is used to sent multiply user selection to more readers

Click on **Upload table** at main menu





Use mouse click to select the combination you need or use right-click to check or clear entire row or column



Select **Upload Users to readers** or **Delete Users from readers** at right-click menu

As upload is progressing, check boxes are cleared mining appropriate combination was successfully done

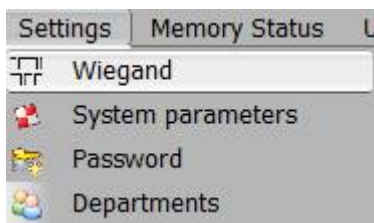
When upload is over, if there are still checked items, repeat the upload command

## 9.12 CUSTOM WIEGAND

BioManager has defined Wiegand 26 and 34 bit as standard options and other 3 Wiegand settings as user definable.

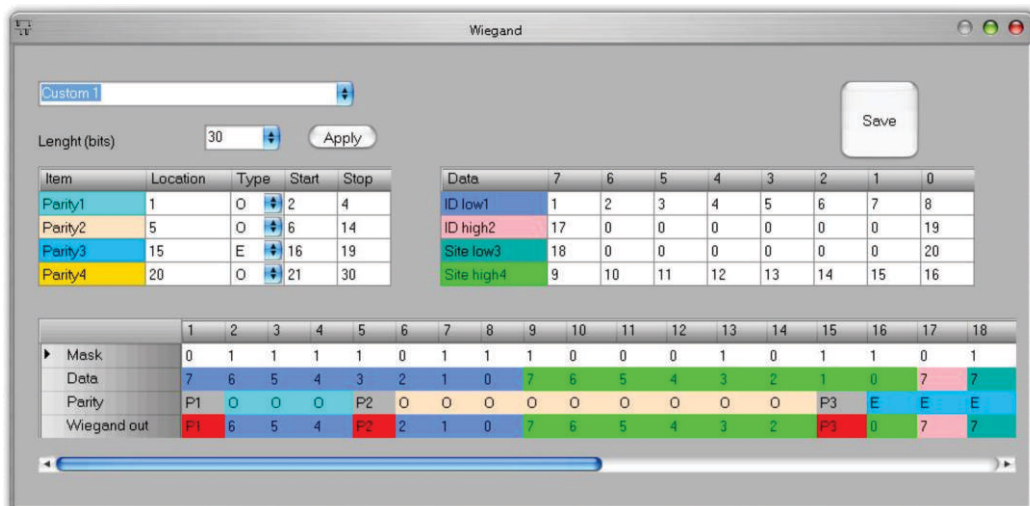
To setup custom Wiegand format

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.

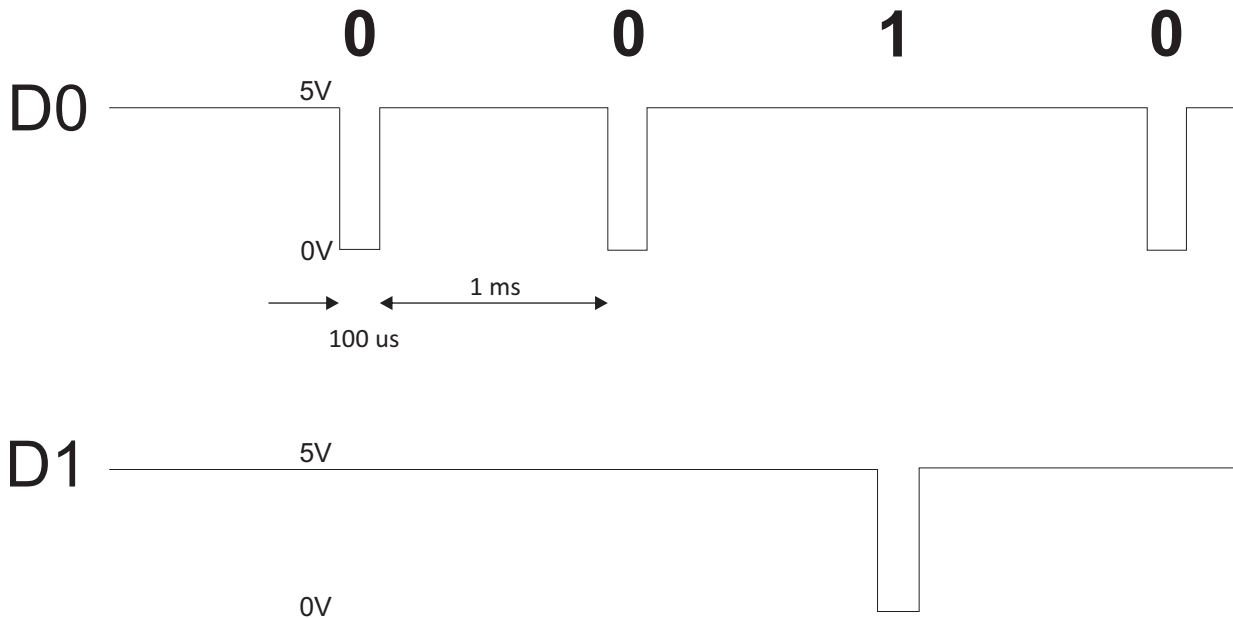
**For more information please refer to BioManager User Manual**



## 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

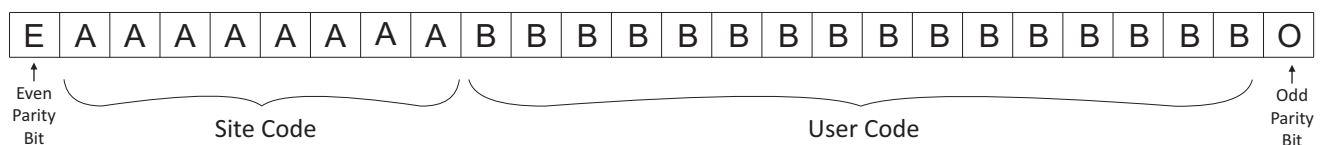
Each data block consists of a first parity bit P1, a fixed 8 bits header, 16 bits of user code and a 2nd parity bit P2. Such a data block is shown bellow:

|          |                                    |   |                             |   |                     |
|----------|------------------------------------|---|-----------------------------|---|---------------------|
|          | Parity bit (bit 1) + 8 bits header | + | 16 bits user code = 2 bytes | + | Parity bit (bit 26) |
|          | P1                                 |   | XXXXXXXX                    |   | P2                  |
| Example: |                                    |   | 170                         |   | 31527               |
|          | 1                                  |   | 10101010                    |   | 01111011 00100111   |
|          |                                    |   |                             |   | 0                   |

**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.

## 12. TROUBLESHOOTING

|                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Red Led on the Biometric Reader is blinking all the time                                                                             | There were 15 unsuccessful attempts of authentication (Finger or PIN). The Red LED will turn off after the first accepted finger or PIN.                                                                                                                                                                                                                                                                                                                                                                                 |
| The keypad of the Biometric Reader is not working                                                                                        | The operation Mode of the Biometric Reader is set as "Finger". Please select "Keycode OR Finger" mode                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Enrollment from desktop reader can be done, but the Fingerprints are not sent to all Biometric Readers in the network                    | <ul style="list-style-type: none"><li>·Check the Ser.No of the Readers.</li><li>·Check if proper termination is done as described before</li></ul> Check if the Communication wires (A & B) are properly connected to the reader                                                                                                                                                                                                                                                                                         |
| The Biometric Reader is not powered ON.<br>The tricolour LED is OFF.                                                                     | Check the power Supply (red & black wire)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Fingerprint (or PIN Code) is recognized (the tricolor LED is green), but the controller reports other ID number and the access is denied | <ul style="list-style-type: none"><li>·If the user is not deleted from the reader and the same user is enrolled again with new ID, the reader will recognize the finger with the first ID. To resolve this, delete all users from the reader and upload all users to the reader</li><li>·Check the Wiegand Bus (yellow &amp; white wire)</li><li>·Check if the ground of the controller and the Biometric Reader is the same</li></ul> Check if the length between Biometric Reader and the controller is less than 50 m |
| Electro static discharge influences the Fingerprint Scan.                                                                                | Connect the housing of the Biometric Reader to the earth wire                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| PIN Codes are working correctly, finger scan does not work.<br>The triocolour LED is OFF.                                                | <ul style="list-style-type: none"><li>·Fingerprint Sensor malfunction</li><li>·Check the Sensor position and its physical condition</li></ul> Reset the system. Contact your installer                                                                                                                                                                                                                                                                                                                                   |
| Reader reading performance is decreased                                                                                                  | <ul style="list-style-type: none"><li>·<b>Check if fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use soft and dry cloth only</b></li></ul> Reading area is damaged. If the damage is minor, try to calibrate the sensor                                                                                                                                                                                                                                                            |
| Fingerprint is not recognized normally                                                                                                   | <ul style="list-style-type: none"><li>·Retry after drying the wetness of your finger</li><li>·When your finger is too dry, touch your forehead and try again</li></ul> When you have a cut on your registered finger, register another fingerprint                                                                                                                                                                                                                                                                       |



This product herewith complies with requirements of EMC directive 2014/30/EU. In addition it complies with RoHS directive EN50581:2012



**Visual Plus Corporation, s.a.**

*Drève Richelle 161  
WOP G - Bte 34  
1410 Waterloo - Belgium*



a Visual **Plus** Corporation Company