Reader Scoria Bio and Bio SW

Scoria Bio SW is a compact and stylish biometric reader for outdoor environment. The reader is equipped with the latest in biometric technology, which means that Scoria Bio SW has a capacitive silicon sensor that is tamper proof.

Biometric Reader

1 *Scoria Bio*

2 *Scoria Bio SW*

Content

1 Product concept

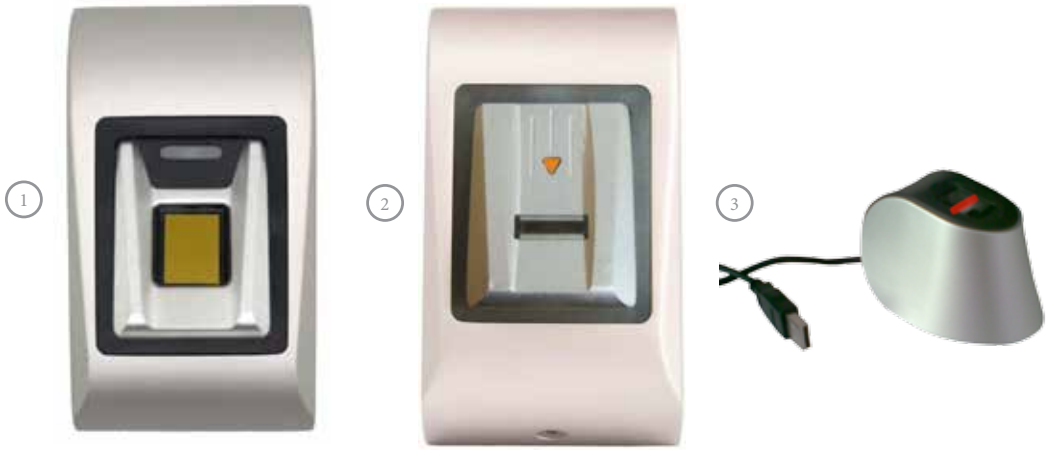
- Bio and Bio SW, is a Biometric reader with adjustable Wiegand Output and can be connected to most Access Controllers with Wiegand interface.
- BioE is a desktop USB biometric reader used for fingerprint enrollment.
- Bio and Bio SW is a surface mount product.
- Bio and BIOSW operate with fingerprint only.
- Connection between the biometric readers is RS485 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 (CNV100-RS485 to RS232 or CNV200-RS485 to USB or CNV300-RS485 to TCP/IP). Only one converter is needed per system (one converter for 1, 2, 3...30, 31 Biometric readers).
- Configuration of the readers and fingerprint enrollment is done through PC Software.
- The Biometric Readers can be used with EX8 as standalone access control system, or as readers with access control panels.

Biometric Readers

1 *Bio*

2 *Bio SW*

3 *BioE*



2 Product Description

2.1 Bio and Bio SW

Features

- Surface mount biometric reader with capacitive sensor, Bio SW has got a swipe sensor.
- Adjustable Wiegand protocol (8 to 128-bit) is utilized in the biometry reader which makes it compatible with other controllers with a Wiegand interface.
- Only fingerprint operation.
- Storage capacity: 9000 fingerprints.
- Configuring the system and Fingerprint enrollment is done through PC, locally or remotely.
- Enrollment can be also done from a Desktop Reader BioE.
- Buzzer sound level adjustment through PC.
- Two free tension LED.
- Wiegand Protocol adjustment is done through PC.
- Separate BioManager Software available free when used with third party controllers.
- The Fingerprints are stored in the reader and a backup copy is kept in the software.
- Elegant aluminium housing in different colours.

Technical Specifications

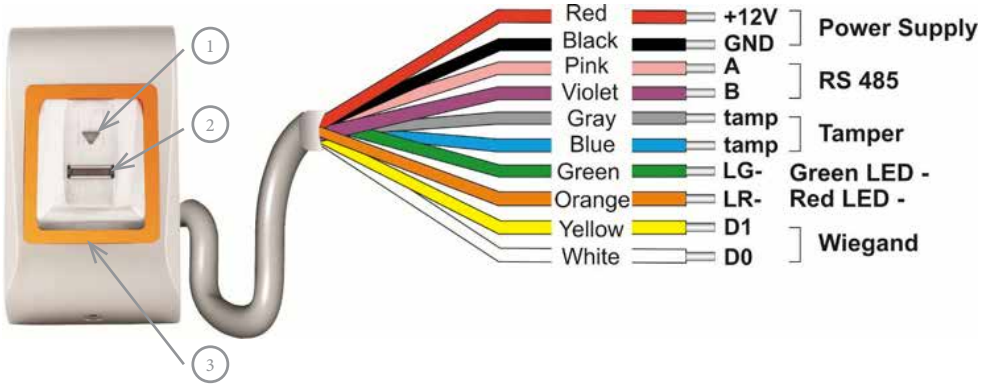
- Authentication: Finger
- Template capacity: 9000
- Finger enrollment time: < 1 second for each finger
- Recognition and matching time: < 1 second for each finger
- Number of templates for each user: 1-10 Templates (Fingers)
- Output: Wiegand (8-128bit), default: Wiegand 26bit
- Communication: RS485
- Power Supply: 12Vdc
- Consumption: 70mA max.
- Weight: 200g
- IP factor: Bio – IP 44, Bio SW - IP 65
- Operating temperature: –20°C – +50°C

Bio SW

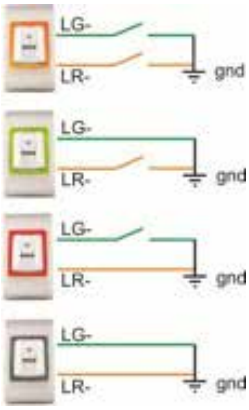
1 *Tricolour LED (idle mode – orange, finger not accepted – red and finger accepted – green).*

2 *Fingerprint Capacitive swipe Sensor.*

3 *Free Tension LED (Red/Green).*



In idle mode the free tension LED is orange.
When access is granted the free tension LED is Green.
When Access is denied the free tension LED is red.



Orange (Idle Mode): LG- and LR- not connected
Green: LG-(green wire) connected to GND
Red: LR-(orange wire) connected to GND
No light: LG-(green wire) and LR-(orange wire) connected to GND

Note: There are no terminal blocks in EX8 for the free tension LED. When Bio SW is connected to EX8, the tricolour triangle LED gives the access status.

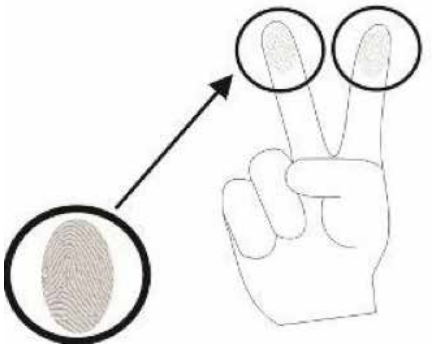
2.2 BioE

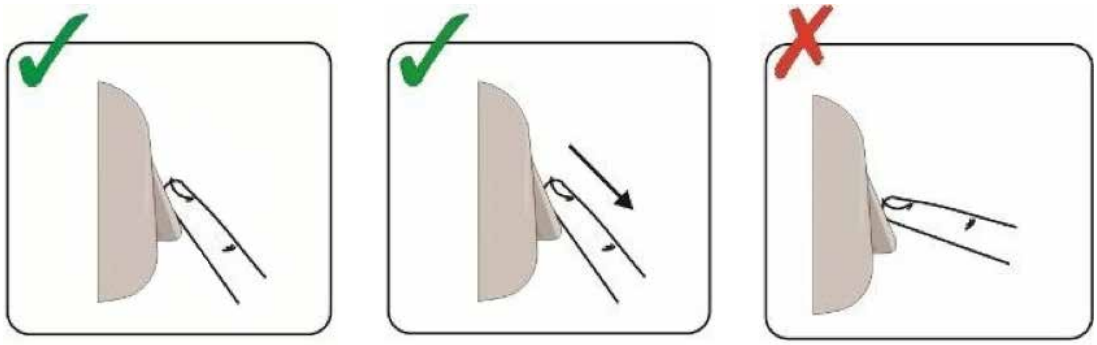
Features

- Desktop Biometric reader.
- USB powered.
- Used only for fingerprint enrollment.
- BioE is used when the enrollment needs to be done from somebody's desk. It is not necessary to have BioE in the system. The enrollment can be done from any installed biometric reader.

BioE

3 Enrollment





4 Authentication

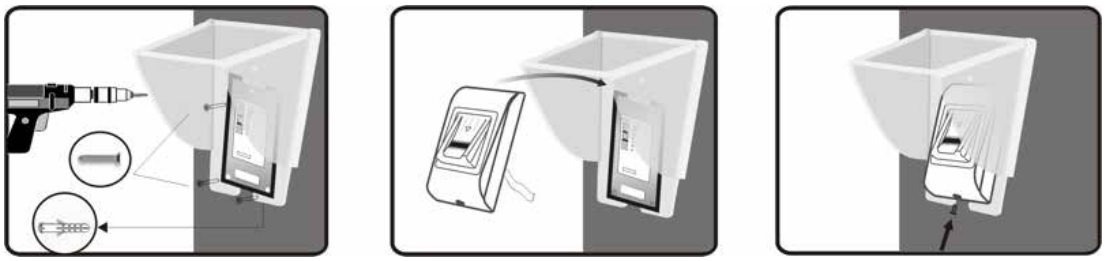
The tricolour LED has three colour statuses; Orange, Green & Red. It operates only on fingerprint enrollment and stays in an orange state before authentication.

Important Note: During user authentication the finger must be swiped in the same way as it was during the enrollment process. This increases the chance of a successful authentication.

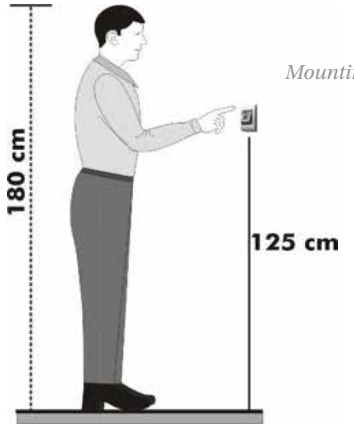
4.1 Authentication of a user by a fingerprint

When swiping a finger, the tricolour LED turns green for one second and beeps twice if the user is valid. For an invalid user or a misread authentication for a valid user, the tricolour LED turns red for three seconds together with multiple beeps.

5 Mounting

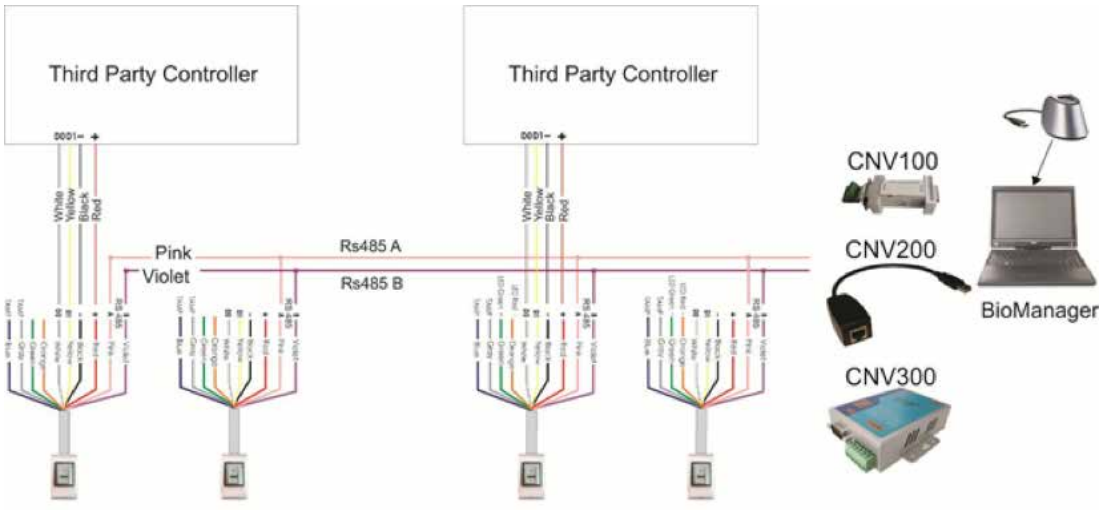


Note: The protective plastic cover is recommended for all outdoor installations!



Mounting

6 Connecting Biometric Readers to Third Party Controller

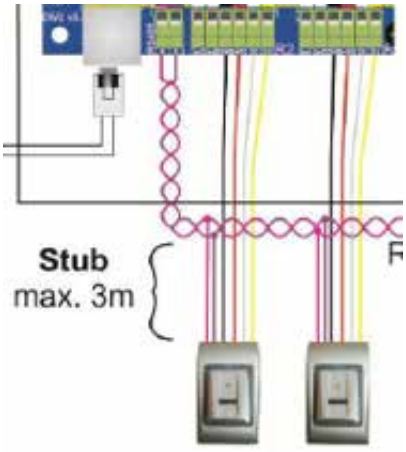


Connect the lines D0, D1, Gnd and +12V to the third party controller.
Connect the RS485 Line (A, B) to the converter. Connect the converter in the PC.

Fingerprint enrollment is done from the PC Software. Connection between the Biometric readers and the PC must be established.

Note: The Biometric reader must be powered from the controller or make common ground for the controller and the Biometric reader.

6.1 Communication chain RS485



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 3 meters).

Converter Types:

- CNV100 – Rs485 to Rs232
- CNV200 – Rs485 to USB
- CNV300 – Rs485 to TCP/IP

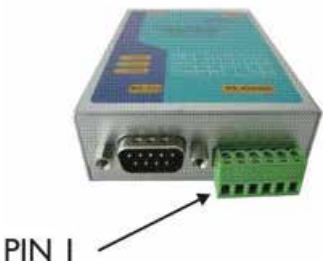
Wiring Configuration (applies to all converters)

Bio and Bio SW	→	Converter
RS 485 A	→	PIN 1 (RS 485 +)
RS 485 B	→	PIN 2 (RS 485 –)

7 Konverters PIN beskrivning

CNV100
Converter RS485 to RS232.
Does not require 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.
No installation. IP address set through Internet Browser (refer to CNV300 Manual).

8 Configuring the Biometric Readers in BioManager

- BioManager is software for fingerprint management of PAS Card Biometric readers, when used with third party access controllers.

Features

- 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

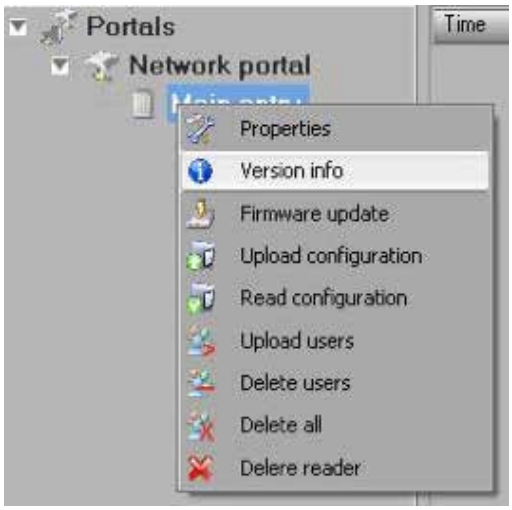
8.1 Add Reader

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

- Fill the Reader form.

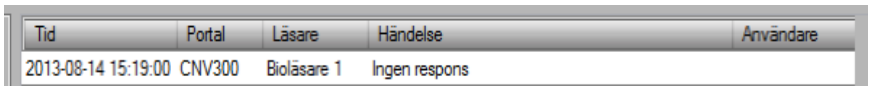
- Click on **Save** and the reader icon appears under the selected portal.

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

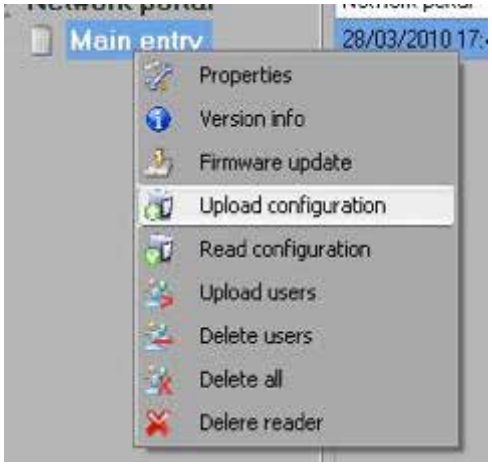


- If reader is online, new line is added on top of the event table.

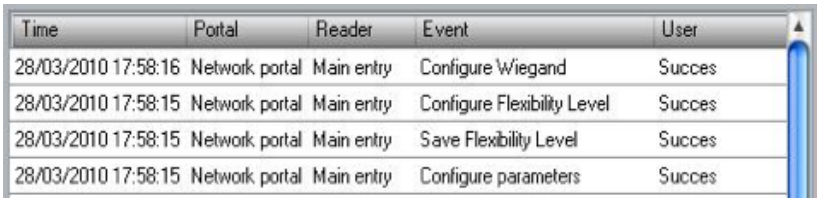
- If reader is not online, following line is added on top of the event table.



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



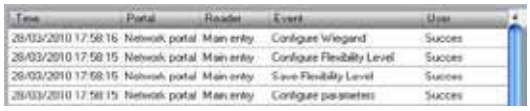
- Check at event table if configuration was successful.



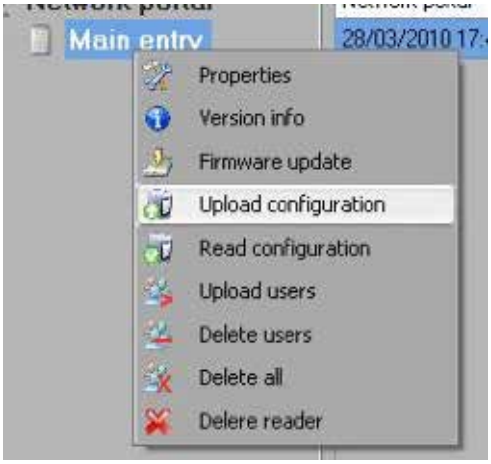
8.2 Edit Reader

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

- Check at event table if the configuration was successful.

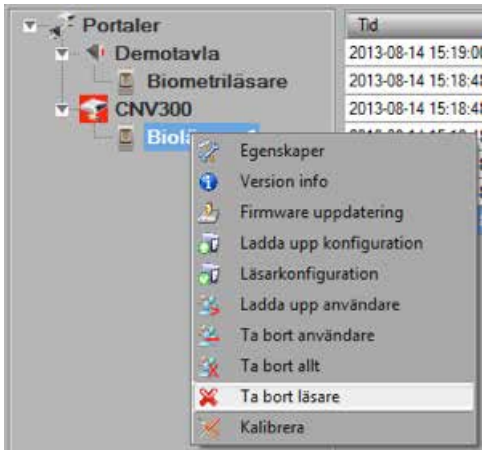


- Edit reader properties and click **Save** button.
- Right click on the reader and select **Upload configuration**.



8.3 Delete Reader

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



8.4 Calibrate sensor

- Right-click on the reader and select Calibrate.
- See events panel to check Calibration flow.

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

8.5 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.

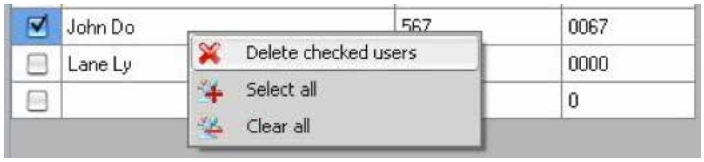
8.6 Edit user

- Find 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, a warning message is displayed reminding that if ID exists in some readers, it should be deleted from reader prior to change.

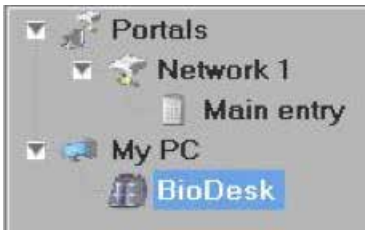
8.7 Delete users

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



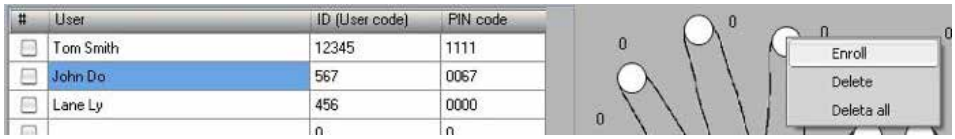
- Confirm warning message.

8.8 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.

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

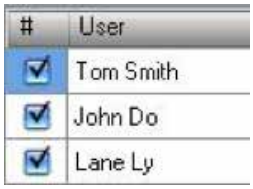


- Swipe the finger on the Reader and the fingertip will become blue, with percentage of successful enrollment given right beside the fingertip.

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

8.9 Ladda registrerat fingertemplat till läsare

- Check the users which fingerprints will be sent to the Reader.



- 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.

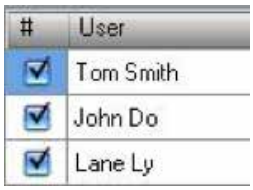
Note: Average time for transferring one finger template is 0,6 sec. The PIN Codes are also being sent, if there are any.

8.10 Delete fingerprints

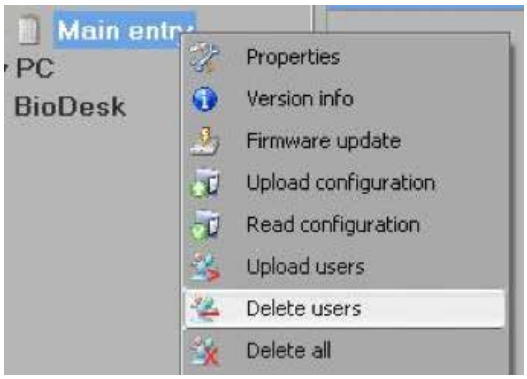
- After transferring, the fingerprint is stored in the Biometric reader and in the PC.
- Deleting can be done only in the software, only in the readers or from the both places.

8.11 Deleting one user from the biometric reader

- Select the user's checkbox.



- 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 reenrollment.

8.12 Deleting all users from the biometric reader

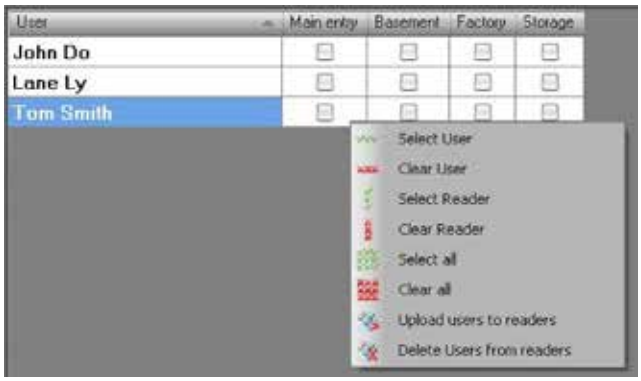
- Right click on the Reader and select **Delete all**.

8.13 Complex user upload

Complex user upload is used to send 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.

8.14 Custom Wiegand

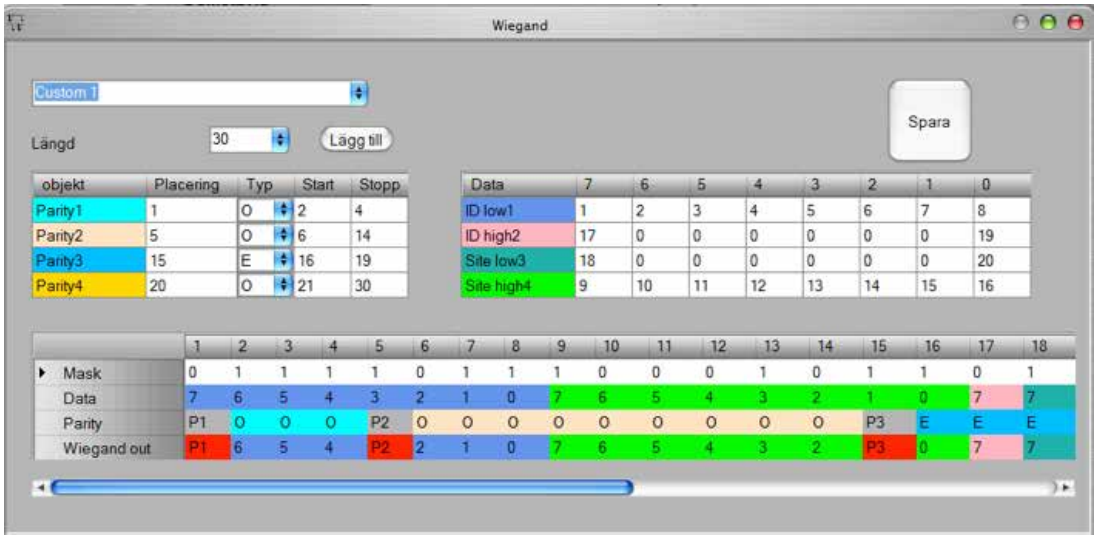
BioManager has defined Wiegand 26 and 34 bit as standard options and three other Wiegand settings as user definable.

To setup custom Wiegand format:

- Select **Wiegand** menu from **Settings**.

- At Wiegand setup window select one from customs Wiegand.

- Set Wiegand parameters.

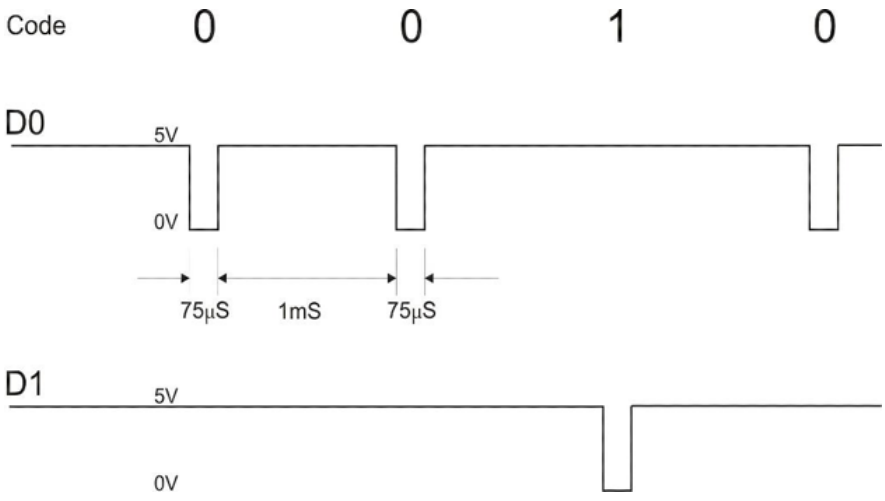


- Click on **Save** button.

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.

9 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 75 us (microseconds)
Data bit 1 = approximately 75 us (microseconds)

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

9.1 Description for the 26 bits Wiegand format

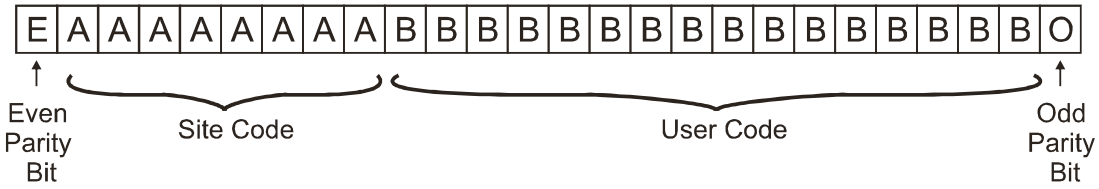
Each data block consists of a first parity bit P1, a fixed 8 bits header, 16 bits of user code and a 2nd parity bit P2. Such a data block is shown below:

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

Note: Parity bits are calculated as follows:

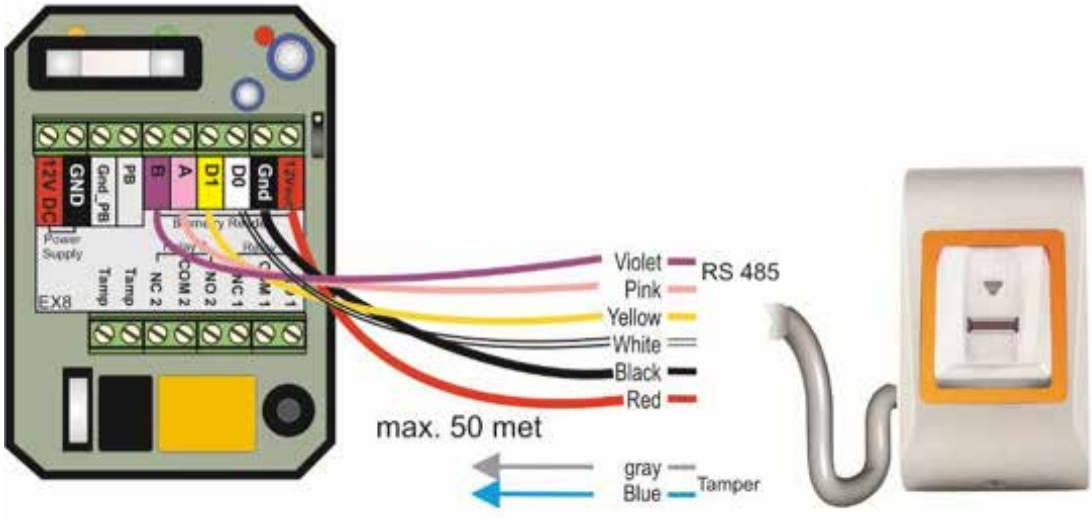
P1 = even parity calculated over the bits 2 to 13 (X)

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



10 Connecting the Biometric readers with EX8 controller

When connected with EX8 controller, the Biometric Readers are becoming Standalone Biometric readers. The Biometric Reader becomes known to the EX8 controller as soon as they are linked. No further configuration is required.



Maximum cable length between EX8 and reader is 50 meters.

For programming please refer to EX8 User Manual.

11 Safety precautions

- Do not install the device in a place subject to direct sun light, humidity or dust.
- When the device is mounted outside, use the protective plastic cover (ref.: ATP; ATP-MINI).
- 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 equipment's.
- Do not clean the device with any form of liquid. Use soft and dry cloth only.
- Be careful not to let liquid like water, drinks or chemicals leak inside the device.
- 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

Observation	Action
The orange Led on the Biometric Reader is blinking all the time.	There were 15 unsuccessful attempts of authentication (Finger or PIN). The orange 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 "Key code OR Finger" mode.
The finger scan in Bio SW works, but the proximity does not work.	The operation Mode of the Biometric Reader is set as "Finger". Please select "Card OR Finger" mode.
Enrollment from desktop reader can be done, but the Fingerprints are not sent to all Biometric Readers in the network.	Check the serial number of the readers. Check if proper termination is done as described In 6.2. Check if the communication wires (A and B) are properly connected to the reader.
The Biometric Reader is not powered ON. The tricolour LED is OFF.	Check the power supply (red and black wire).
Fingerprint (or PIN Code) is recognized (the tricolour LED is green), but the controller reports other ID number and the access is denied.	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. Check the Wiegand Bus (yellow and white wire). Check if the ground of the controller and the Biometric Reader is the same. 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. The tricolour LED is OFF.	Fingerprint sensor malfunction. Check the sensor position and its physical condition Reset the system. Contact your installer.
Reader reading performance is decreased.	Check if fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use soft and dry cloth only. Reading area is damaged. If the damage is minor, try to calibrate the sensor.
Fingerprint is not recognized normally.	Retry after drying the wetness of your finger. When your finger is too dry, touch your forehead and try again. When you have a cut on your registered finger, register another fingerprint.