



# BioSafe™ Fingerprint Recognition System

---

## Installation Guide

Version 2.4

---

This publication contains proprietary information of the BioGuard Company and is provided for customer use only. No other uses are authorized without the express written permission of BioGuard.

### **Warranty**

BioGuard provides this publication “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or suitability for any particular purpose.

BioGuard reserves the right to revise this publication, and to make changes in the content hereof from time to time without notification. There are some countries, as well as some states in the US, that do not allow a disclaimer of express or implied warranties in certain transactions; if you are a resident of such a country or state, this statement may not apply to you.

This publication may include technical inaccuracies or typographical errors. Changes are made periodically to the information herein; these changes will be incorporated in new editions of the publication. BioGuard may make improvements and/or changes in the products and/or the software described in this publication at any time.

### **Notice to User**

This User Guide should not be construed as a representation or warranty with respect to the hardware or software named herein. *Occasionally, changes or variations exist in the hardware or software that is not reflected in the manual.* Generally, if such changes or variations are known to exist and to affect the product significantly, a release note or “read me” file will accompany the User Guide and/or the distributed hardware or software.

### **Publication**

The descriptions, specifications, design and procedures contained in this User Guide were effective at the time of publication of this document. BioGuard reserves the right to modify any of the above at any time without notice and without incurring obligations.

### **Trademarks**

All trademarks are the property of their respective holders and are hereby acknowledged.

## TABLE OF CONTENTS

WARRANTY.....	2
NOTICE TO USER.....	2
PUBLICATION.....	2
TRADEMARKS.....	2
TABLE OF CONTENTS.....	3
TABLE OF FIGURES.....	5
<b>1 INSTALLATION &amp; CONNECTION.....</b>	<b>6</b>
1.1 Mounting the AC-02 Unit Box.....	6
1.2 Connecting the AC-02 unit.....	7
1.3 Mounting the sensor unit.....	16
1.4 Connecting the sensor unit at the sensor end.....	16
1.5 Connecting the sensor unit to the AC-02.....	18
1.6 Connecting the proximity cable to the AC-02 WIEGAND 'Data In' connector.....	19
<b>2 USER REGISTRATION.....</b>	<b>20</b>
2.1 Proximity Cards, Keypads and IDs.....	21
2.2 Shadow IDs.....	21
2.2.1 Group Shadow IDs.....	21
2.2.2 Individual Shadow IDs.....	22
2.3 Administrators and other User IDs and their functions.....	22
2.4 Creating a Standard Enroll Permission ID (SE ID).....	23
2.5 Creating an Enroll Administrator ID (EA ID).....	23
2.6 Creating an Administrator ID (AID).....	23
2.7 Registering a User (fingerprint-based access) by using an Enroll ID (EID).....	24
2.8 Registering a User (fingerprint-based access) by using an Administrator ID (AID) and fingerprint.....	24

<b>2.9</b>	<b>Registering and configuring a User for access by using only a User ID .....</b>	<b>25</b>
<b>2.10</b>	<b>Creating a Standard Delete Permission ID (SD ID) .....</b>	<b>26</b>
<b>2.11</b>	<b>Creating an Enroll Administrator with Delete Permission ID (EAD ID).....</b>	<b>26</b>
<b>2.12</b>	<b>Creating an Administrator with Delete Permission ID (AD ID).....</b>	<b>27</b>
<b>2.13</b>	<b>Deleting an ID including an Administrator with Delete Permission ID (AD ID) by using a Standard Delete Permission ID (SD ID) .....</b>	<b>27</b>
<b>2.14</b>	<b>Deleting an ID by using an Administrator with Delete Permission ID (AD ID) fingerprint .....</b>	<b>28</b>
<b>2.15</b>	<b>Basic Operation .....</b>	<b>29</b>

## **TABLE OF FIGURES**

<b><u>Figure</u></b>		<b><u>Page</u></b>
<b>Figure 1</b>	<b>The Series I &amp; II AC-02 Units</b>	<b>6</b>
<b>Figure 2</b>	<b>Mounting the Series I &amp; II AC-02 back-boxes</b>	<b>6</b>
<b>Figure 3</b>	<b>The connections and layout of the H2PCCI V2 interface board (top side view)</b>	<b>8</b>
<b>Figure 4</b>	<b>The connections and layout of the H2PCCI V3 interface board (top side view)</b>	<b>9</b>
<b>Figure 5</b>	<b>REX button connector and mode jumpers</b>	<b>10</b>
<b>Figure 6</b>	<b>12V DC Input socket</b>	<b>10</b>
<b>Figure 7</b>	<b>TCP/IP and RS-232 selector switch</b>	<b>11</b>
<b>Figure 8</b>	<b>RS282 / TCP/IP / RS-485 connection selector switch (V3 board)</b>	<b>12</b>
<b>Figure 9</b>	<b>Connecting via the RS-232 interface</b>	<b>13</b>
<b>Figure 10</b>	<b>12V DC Output connector</b>	<b>13</b>
<b>Figure 11</b>	<b>Relay (dry contact)</b>	<b>14</b>
<b>Figure 12</b>	<b>WIEGAND Protocol Interface</b>	<b>14</b>
<b>Figure 13</b>	<b>RS-485 Connector (V3 board only)</b>	<b>15</b>
<b>Figure 14</b>	<b>Series I &amp; II sensors and their fixing holes</b>	<b>16</b>
<b>Figure 15</b>	<b>Circuit board and connector locations on Series I &amp; II sensors</b>	<b>16</b>
<b>Figure 16</b>	<b>Cables correctly connected to sensors</b>	<b>17</b>
<b>Figure 17</b>	<b>Cables incorrectly connected to sensors</b>	<b>18</b>
<b>Figure 18</b>	<b>Sensor cable correctly connected to AC-02 board</b>	<b>18</b>
<b>Figure 19</b>	<b>Cable connection sequence for the built-in proximity sensor</b>	<b>19</b>

# 1 INSTALLATION & CONNECTION

---

## 1.1 Mounting the AC-02 Unit Box

There are two types of AC-02 Unit boxes currently available. The Series I box is a mostly metal case with rear and side cable access. The Series II box is a high-quality plastic case that is available in various colors and has cable access from the rear and sides.



Figure 1. The Series I AC-02 unit (left) & the Series II AC-02 unit (right)

Mount the empty box on the wall (see Figure 2 below), in a convenient and preferably concealed place, such as above the door, above a false ceiling, inside a communication case, etc. Ensure that adequate access is available to the appropriate cable entry holes in the case.

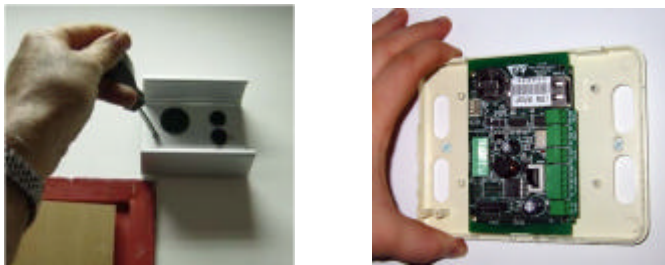


Figure 2. Mounting the Series I AC-02 (left) & the Series II AC-02 (right) box onto a wall

## 1.2 Connecting the AC-02 unit

The complete AC-02 unit consists of two boards in a dual board assembly; the Biometric Processing Engine (BPE Unit), with the H2 power controller and communication interface (H2PCCI) placed on top of the BPE.

There are currently two versions of the H2PCCI boards available. These are V2 and V3.

The main differences between the two boards with regards to connectivity abilities are shown in the following comparison table:

Interface	H2PCCI V2	H2PCCI V3
TCP/IP*	●	●
RS-232*	●	●
RS-485**		●
12V DC Output	●	●
Relay (Dry Contact)	●	●
WIEGAND IN	●	●
WIEGAND OUT		●
REX (Request for Exit)		●

\* Optional depending on the version ordered

\*\* Available August 2006

The illustrations on the following pages show the layout and connectivity of the H2PCCI V2 and V3 boards.

The H2PCCI V2 interface board

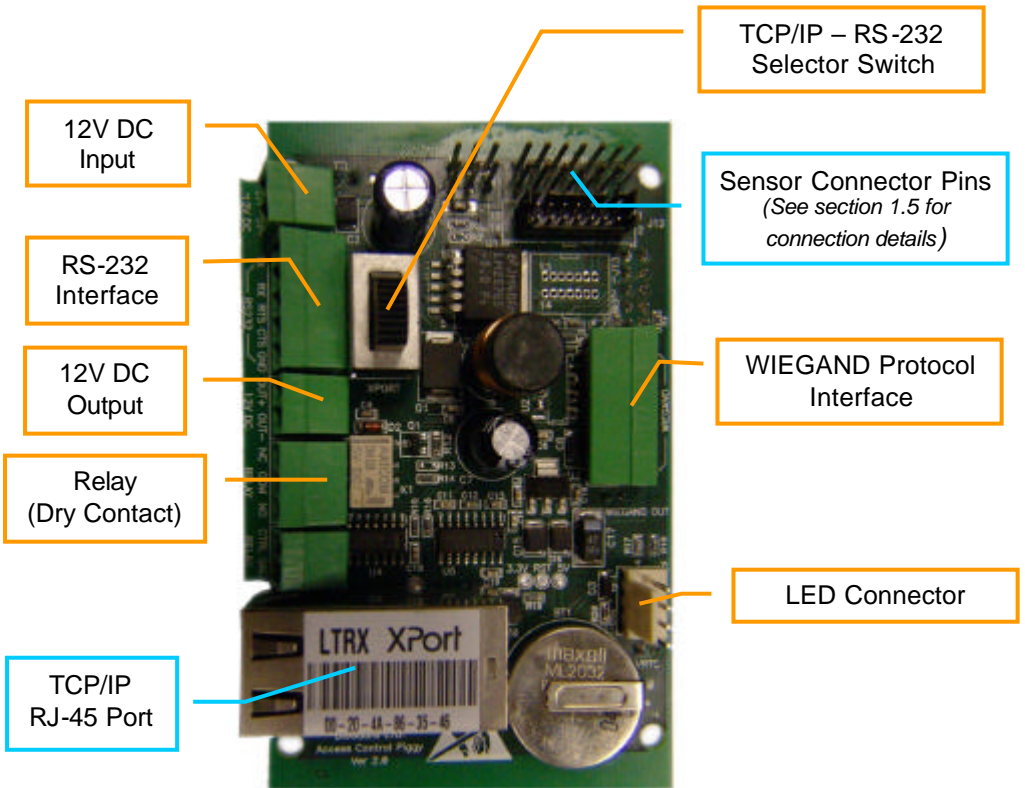


Figure 3. The connections and layout of the H2PCCI interface board V2



Tip: The details of each connector/interface are printed on the circuit board next to each connector/interface.

The H2PCCI V3 interface board

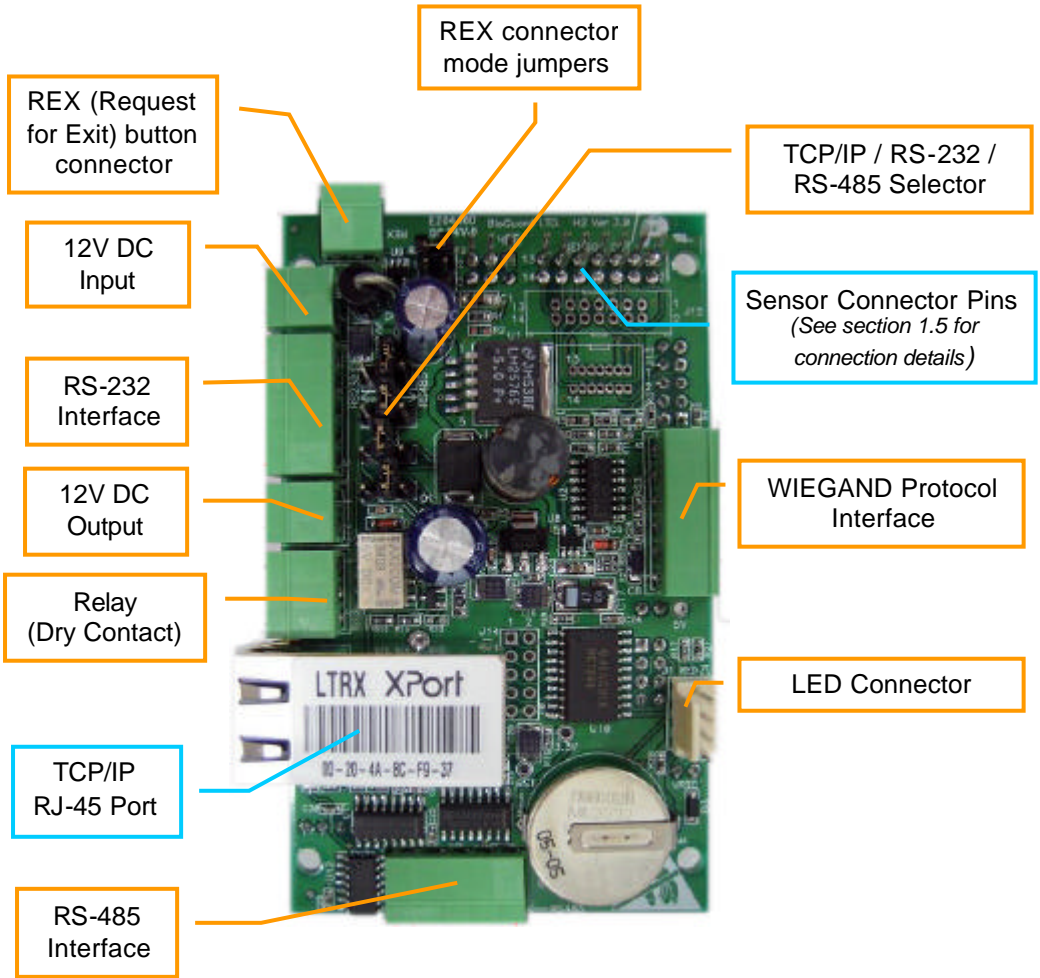


Figure 4. The connections and layout of the H2PCCI Interface board V3



Tip: The details of each connector/interface are printed on the circuit board next or behind each connector/interface.

**REX (Request for Exit) button connector and REX mode jumpers**

**\*\*V3 ONLY\*\***

The REX connector allows the connection of a push type switch, which when pressed will release the relay for the preset duration configured on the BioSafe unit. This would typically be used for an exit button for the door controlled by the BioSafe unit.

The mode jumpers determine if the REX button to be used is in a normally open or normally closed state.

Note: This will only release the relay on the unit, and will not provide an output on the WIEGAND or any other port.

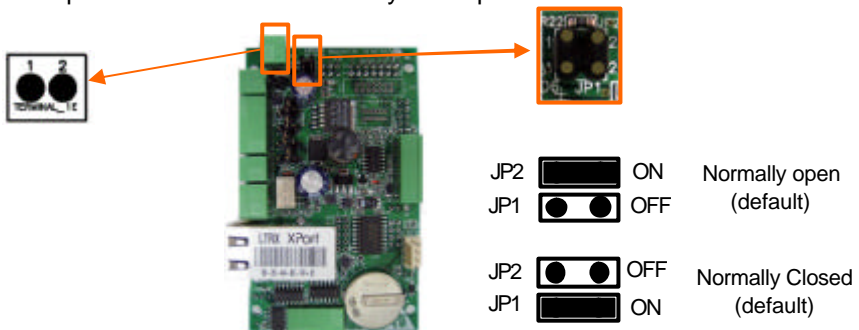


Figure 5. REX Button connector and mode jumpers (V3 board)

**12V DC Input: Connection to the 12V DC AC-02 power supply**

Figure 4 shows where to connect the main power supply to the AC-02. Either the power supply *supplied* with the unit or an alternative supply rated at 12 Volt DC, 2A Output can be used for this purpose.

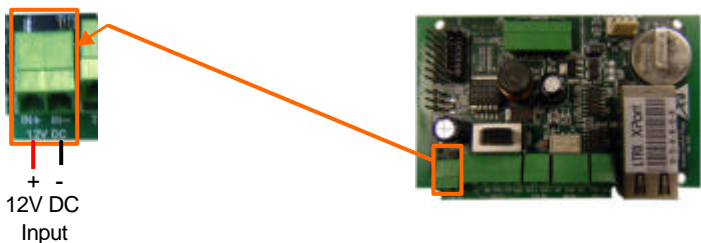


Figure 6. 12V DC input socket (V2 board shown)

**Selector switch: Select between RS-232 or TCP/IP**  
**\*\*V2 ONLY\*\***

There are two ways of connecting the AC-02 to a PC or Network:

- Via RS-232 connection – also identified as ‘Terminal’ on the board
- Via TCP/IP (LAN) connection – also identified as ‘Xport’ on the board

To specify the type of connection, set the switch to the appropriate position as shown in Figure 5 below:



Figure 7. RS-232 /TCP/IP connection selector switch (V2 board)

**!** Note: Selection between RS-232 and TCP/IP is exclusive.

**Selector switch: Select between RS-232, TCP/IP or RS-485**  
**\*\*V3 ONLY\*\***

On the V3 H2PCCI board There are three ways of connecting to the unit from a PC, the LAN or another device:

- RS-232 connection
- TCP/IP (LAN) connection
- RS-485 connection

To specify the type of connection required, set the jumpers to the appropriate position as shown below:

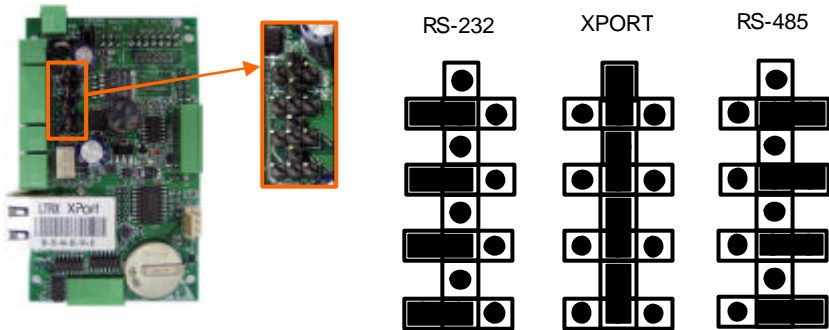


Figure 8. RS-232 / TCP/IP / RS-485 connection selector switch (V3 board)

**!** Note: Selection between RS-232, TCP/IP or RS-485 is exclusive.

**RS-232 Connection: connect to a PC via RS-232 connection**

Figure 6 shows the connections and the connection selector switch for RS-232:

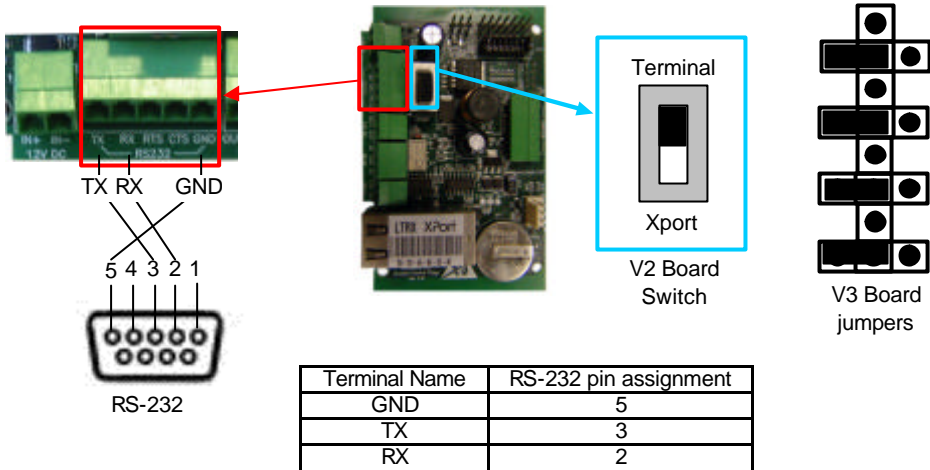


Figure 9. Connecting via the RS-232 interface (V2 board shown)

**12V DC Output**

This can be connected to provide 12V DC to an electrical device, e.g. electric lock, etc. (see Figure 7 below).

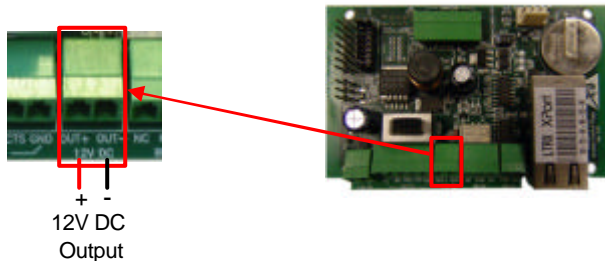


Figure 10. 12V DC Output connector (V2 board shown)

**Relay (Dry Contact)**

Standard dry contact relay, configurable in normally open (NO) and/or normally closed (NC) (see Figure 8 below).

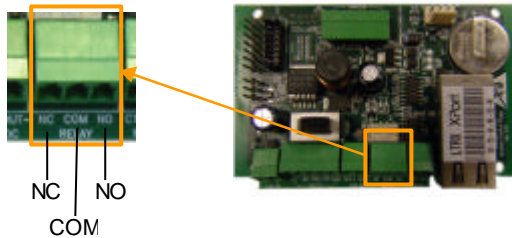


Figure 11. Relay (Dry Contact) – (V2 board shown)

**WIEGAND protocol interface**

The WIEGAND protocol interface is provided via a connector (see Figure 9 below) that enables the connection and powering (5V DC if required) of a WIEGAND-based device (proximity reader, card reader or a keypad) to the AC-02 unit. In addition to this, the AC-02 can be configured to send an output (the ID of the User) over the WIEGAND ‘Data Out’ link when a User is verified. Details of connecting the proximity reader built into the BioSafe sensor can be found in section 1.6.

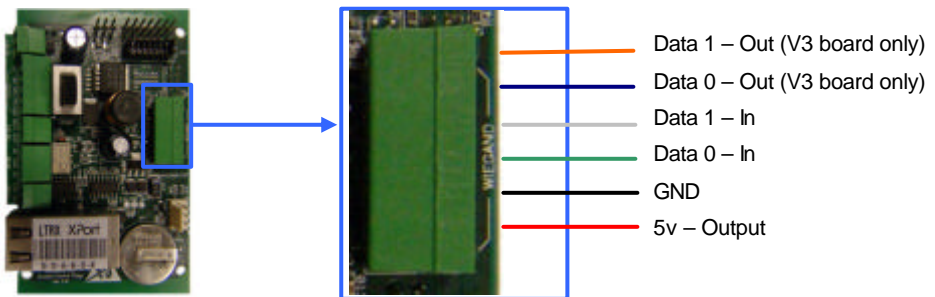


Figure 12. WIEGAND Protocol Interface (V2 board shown)

**!** Note (V2 only): The functionality of the ‘Data Out’ link is only available as standard on the V3 H2 board. Should you require it on a V2 board, this **must be specified as a requirement when the unit is ordered**. If you are not sure whether or not your unit has the WIEGAND ‘Out’ feature, please contact BioGuard Technical Support.

**RS-485 Connector \*\*V3 Only\*\***

The RS-485 connector enables the BioSafe unit to be connected to other devices that utilize a RS-485 port.

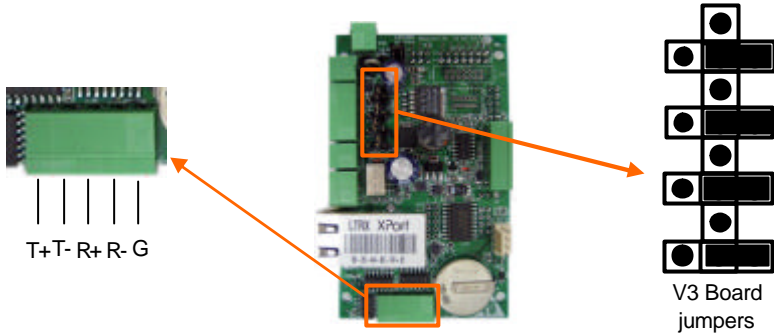


Figure 13. RS-485 Connector (V3 board only)

**LED Connector**

The LED connector on the circuit board serves to connect to the LEDs located on the front face of the AC-02's casing. When lit ('On'), the red LED indicates "Power On" and the green LED indicates when the relay has been triggered.

### 1.3 Mounting the sensor unit

Two standard casing styles are currently used for the AC-02 unit (see Figure 10). The Series I sensor is cased in plastic casing and the Series II sensor is cased in high quality plastic casing (available in different colors).



Figure 14. Series I Sensor (left) and Series II Sensor (right) and locations of relevant fixing holes

To mount the sensor on a wall, pass the 14 wire sensor cable and the 4 wire proximity cable that protrude from the wall through the opening in the sensor case base. Mount the sensor case base on the wall by using four screws.

### 1.4 Connecting the sensor unit at the sensor end

The sensor cable and the proximity cable must be connected to the appropriate sockets via their 14 pin and 4 pin connectors respectively, as shown in Figure 15 below.

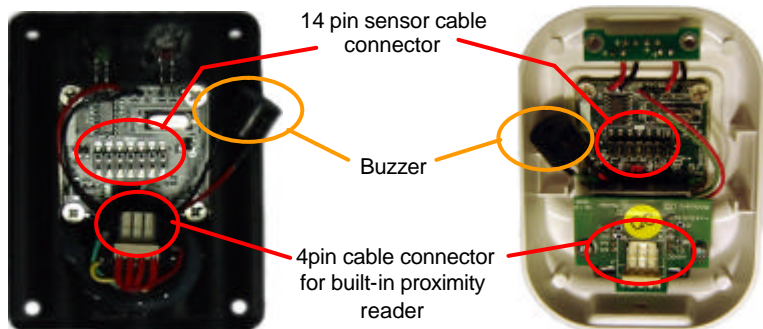


Figure 15. Circuit board and connector locations on Series I (left) & Series II (right) sensors

Although slight variations from the basic design might be found in the component layout, the connection is made according to the rule stated above

**!** Note: Connecting the built-in proximity reader and / or the WIEGAND connection is not mandatory, since the BioSafe system is designed to operate autonomously. The WIEGAND connection has been provided as a feature that assists in helping to connect devices such as proximity readers, keypads or card readers, used for registering or deleting fingers on a standalone unit. Such a device can also be used to provide authentication using a proximity card or keyed-in code only, or proximity card or keyed code and a fingerprint together.

Connect the cables to the sensor as shown below:

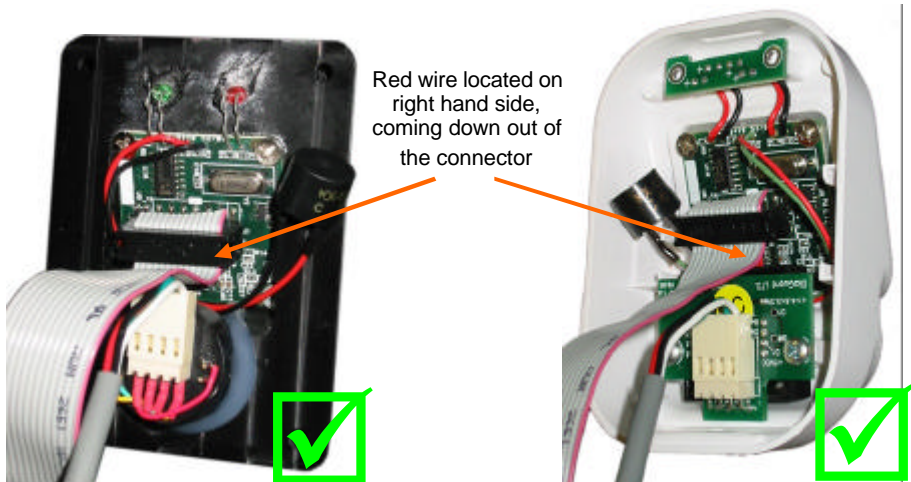


Figure 16. Cables correctly connected to sensors (Series I on left, Series II on right)

Note that the red line must be positioned to the right of the unit (when viewed from the inside of the sensor covering case with the LEDs at the top). Connecting the cable in the wrong way may permanently damage the unit.

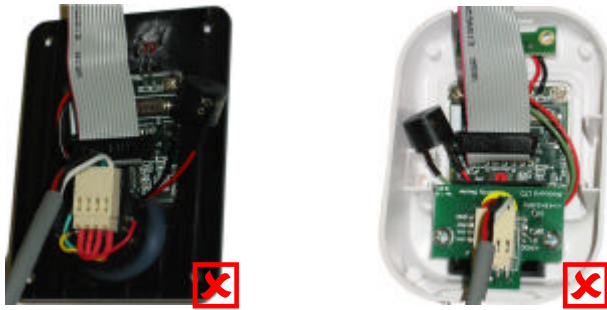


Figure 17. Cables incorrectly connected to sensors (Series I on left, Series II on right)

Once the cables are correctly connected, carefully secure the sensor onto the sensor base.

### 1.5 Connecting the sensor unit to the AC-02

To connect the sensor unit to the AC-02, locate the AC-02 sensor connector pins on the main AC-02 circuit board (see Figure 3).

Connect the 14 wire sensor cable via the 14 pin connector to the connector pins on the AC-02. Please observe the correct positioning of the red mark on the 14 wire flat cable (see Figure 14 below).

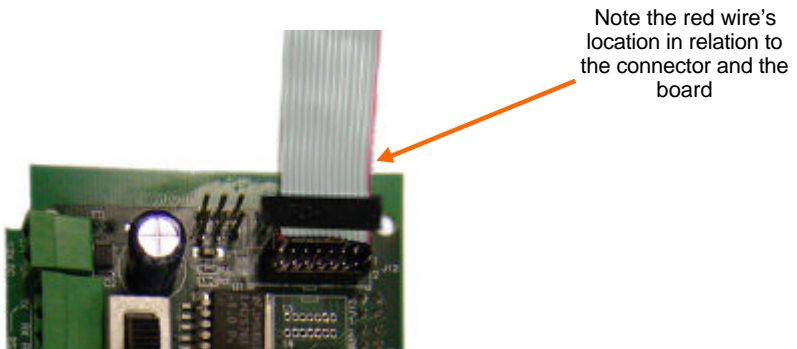


Figure 18. Sensor cable correctly connected to H2 board (V2 board shown)

**!** Note: Flat cables, particularly at the plug joints into the connector are particularly sensitive to being bent at sharp angles, sometimes resulting in unsafe or even interrupted connection.

### 1.6 Connecting the proximity cable to the AC-02 WIEGAND 'Data In' connector

To connect the proximity sensor built into the BioSafe sensor to the AC-02 unit, locate the WIEGAND Protocol Interface on the AC-02 board (see Figure 3).

The proximity sensor built into the BioSafe sensor only requires the use of the WIEGAND 'Data In' connection, in addition to the power supply. Connect the 4 wire cable into the appropriate terminals on the AC-02 board taking particular notice of matching the colors of the cable wires to the appropriate terminal on the board. See Figure 19 below for the correct color matching.

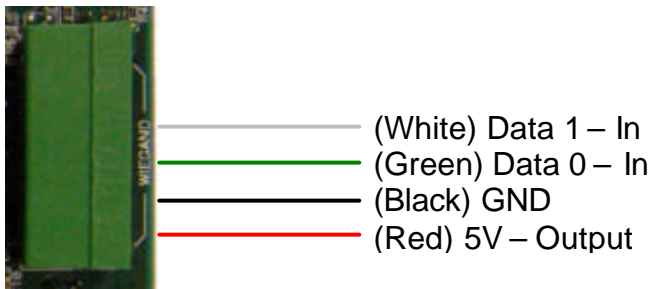


Figure 19. Cable connection sequence for the built-in BioSafe proximity sensor

**⚠ Note:** The proximity reader supplied with the BioSafe unit is compatible with **26bit proximity cards or tokens that operate at 125 MHz**. For more information, please contact BioGuard technical support.

## 2 USER REGISTRATION


---


The following registration instructions apply primarily to standalone installations where the AC-02 unit is not connected to a computer or where enrollment, as described in this section, is specifically required by the administrator.

If connected to a computer, registration and template management is usually carried out using the BioManage software available from BioGuard.

It is advised, however, to configure some functionalities of the AC-02 unit using the BioManage software **before** installation, in particular, entering Administrator and other IDs in the WIEGAND interface settings section.

Users can be registered by using either a proximity card (by default), or a keypad (optional – requires connection of the keyboard to the WIEGAND Protocol Interface instead of the proximity card). **This card, token or code is referred to in this section as an 'ID'**

 **Note:** The two registration methods of using a keypad and proximity sensor / card reader cannot be combined or used simultaneously, nor is it recommended that you connect two devices onto the same WIEGAND 'Data In' port.

 **Tip:** When the sensor unit is not in use, by default a constant green light (not flashing) indicates the unit is 'Idle' and waiting for a finger to be placed on the sensor.

## **2.1 Proximity Cards, Keypads and IDs**

A standalone BioSafe unit uses inputs from a device other than a fingerprint sensor in order to register Users or additional administrators into the unit. These input devices come in various shapes and forms, including proximity card sensors, keypads and swipe card readers. These devices can be connected via the WIEGAND Protocol Interface to the AC-02 unit.

The input device provides the AC-02 unit with a unique code or 'ID'. Depending on what rights or functions, if any, have been associated with this ID, the AC-02 unit will determine the corresponding action for the AC-02 unit to perform.

## **2.2 Shadow IDs**

A *Shadow ID* is the term used in this document to refer to an ID that is used to register a person into a BioSafe unit, with the ID not being required for normal access. This Shadow ID may have the form of a card, token or code and is initially presented to the system when a User is being registered into the unit.

The Shadow ID is only used when enrolling (registering), verifying or deleting the User or Users associated with that ID. During the regular use of BioSafe, a normal User uses his/her registered fingerprint(s) for normal access authentication, while the Shadow ID is filed as associated with the particular User(s).

### **2.2.1 Group Shadow IDs**

A group Shadow ID can be used when registering a group of Users for which no individual management is required. When being enrolled into the system, this same ID is presented as the User ID for each person in the group. As this ID is associated with a number of different Users' fingerprints, it is important to remember that the removal of a Group Shadow ID will remove ALL associated group fingerprints from the system.

A group shadow ID could be particularly useful when temporary access is required for a specific group of people. If individual Shadow ID management is required (i.e. the ability to be able to remove one User at a time) then Individual Shadow IDs should be used for each User.

### 2.2.2 Individual Shadow IDs

Individual Shadow IDs are used when the management of each individual User is required. An example is when there is a need to enroll and delete Users on the standalone BioSafe unit individually.

### 2.3 Administrators and other User IDs and their functions

In order for a User to be enrolled in the system, whether it is a Shadow ID or a User ID, they must be enrolled by a person who has been authenticated by using an Enroll ID or an Administrator ID.

An Enroll Administrator ID (EA ID) exists that is used to enroll Administrators, who in turn acquire the permission to add Users to the system by using only their Administrator ID and fingerprint.

The same principles that correspond to Enroll Administrator IDs also apply to IDs used for deleting Users.

The table below shows the different Administrators and Users, as well as their rights pertaining to enrollment and authentication in the system:

ID Type \ Function	Enroll / Delete Admin	Enroll User	Finger-print Auth.	ID Auth.	Delete User
Standard Enroll Permission ID (SE ID)	-	●	-	-	-
Enroll Administrator ID (EA ID)	● (Enroll)	-	-	-	-
Administrator ID (AID)	-	●	●	-	-
User* (Fingerprint Only)	-	-	●	-	-
User ID**	-	-	(●)	●	-
Standard Delete Permission ID (SD ID)	● (Delete)	-	-	-	●
Enroll Administrator with Delete Permission ID (EAD ID)	● (Delete)	-	-	-	-
Administrator with Delete Permission ID (AD ID)	-	-	-	-	●

\* The ID used for the User(s) during enrollment may be a Shadow ID (Individual or Group)

\*\* User IDs are used for getting access without a fingerprint

## **2.4 Creating a Standard Enroll Permission ID (SE ID)**

Each unit is delivered as standard with a pre-configured Standard Enroll Permission ID (SE ID) in the form of a proximity card or token. This is normally labeled as 'Enroll', and is used for registering standard Users using just this single SE ID and the new Users' ID and fingerprint. This applies to registrations using Shadow or Individual IDs (see section 2.7 for details on enrolling a User using an SE ID).

Within the unit, the code associated with this EID (card or token) had been previously entered into the relevant settings area of the AC-02 to define the ID as an Enroll ID.

If a different EID is required, for example a code from a keypad, changing an EID or adding a new EID can be done by using the BioManage software package from BioGuard.

(For more information on configuring a Standard Enroll ID please see 'BioManage Software User Guide')

## **2.5 Creating an Enroll Administrator ID (EA ID)**

An Enroll Administrator ID (EA ID) is used to create Administrator IDs. As with the SE ID (see section 2.4) defining an EA ID in the AC-02 requires the use of the BioManage software package from BioGuard. A pre-configured EA ID is not supplied as standard with a BioSafe unit.

(For more information on configuring an Enroll Administrator ID please see 'BioManage Software User Guide')

## **2.6 Creating an Administrator ID (AID)**

An Administrator ID (AID) is used to enroll Users into the BioSafe unit. The AID is not predefined in the AC-02 unit and therefore the ID to be enrolled can be provided by any compatible ID (card, token or code as applicable). The AID is created as it follows:

- 2.6.1 Present an Enroll Administrator ID. The red LED will flash for 5 seconds.
- 2.6.2 While the red LED is flashing, present the designated Administrator ID. Both the red and green LED will be lit.
- 2.6.3 While the two LEDs are lit, place finger of the would-

be administrator on the sensor.

- 2.6.4 Hold finger on the sensor until both LEDs flash, then remove finger.

Successful (confirmed) enrollment: Both LEDs will be lit and the buzzer will produce a sound. The unit then returns to idle mode (green LED 'On'). Enrollment is completed.

Failed (rejected) enrollment: Red LED flashes with no sound and the unit then returns to idle mode (green LED 'On'). Repeat the enrollment process.

## **2.7 Registering a User (fingerprint-based access) by using an Enroll ID (EID)**

To register a User by using an Enroll ID that not requires authentication via fingerprint, follow these steps:

- 2.7.1 Present an Enroll ID. The red LED will flash for 5 seconds.
- 2.7.2 While the red LED is flashing, present a Group Shadow ID or Individual User/Shadow ID.
- 2.7.3 Both the red and green LEDs will be lit for 5 seconds.
- 2.7.4 While the two LEDs are lit, place the User's Finger on the sensor.
- 2.7.5 Hold finger on the sensor until both LEDs flash, then remove finger.

Successful (confirmed) enrollment: Both LEDs will be lit and the buzzer will produce a sound. The unit then returns to idle mode (green LED 'On'). Enrollment is completed.

Failed (rejected) registration: Red LED flashes with no sound. The unit then returns to idle mode (green LED 'On'). Repeat the User registration process.

## **2.8 Registering a User (fingerprint-based access) by using an Administrator ID (AID) and fingerprint**

To register a User (using an Administrator ID) that requires authentication using their fingerprint, follow these steps:

- 2.8.1 Present an Administrator ID. Both the red and green LEDs will light.
- 2.8.2 While the two LEDs are lit, place the Administrator's

- enrolled finger on the sensor.
- 2.8.3 Hold finger on the sensor until both LEDs flash, then remove finger.
- 2.8.4 If properly identified, both LEDs will be lit and the buzzer will produce a sound, followed by the red LED flashing for 5 seconds.
- 2.8.5 While the red LED is flashing, present a Group Shadow ID or Individual User/Shadow ID.
- 2.8.6 Both the red and green LEDs will be lit for 5 seconds.
- 2.8.7 While the two LEDs are lit, place the User's finger on the sensor.
- 2.8.8 Hold finger on the sensor until both LEDs flash, then remove finger.

Successful (confirmed) registration: Both LEDs will be lit and the buzzer will produce a sound. The unit then returns to idle mode (green LED 'On'). Enrollment is completed.

Failed (rejected) registration: Red LED flashes with no sound. The unit then returns to idle mode (green LED 'On'). Repeat the User registration process.

## **2.9 Registering and configuring a User for access by using only a User ID**

Should it be required, a User ID can be configured so that when used, the access is granted (verified) based only on a User ID, with no need for a fingerprint. For example, this might be the case if a User has no fingerprints or if access to the system without the use of a fingerprint is required for some other reason.

To configure a User ID so that it will be verified without the use of a fingerprint, the AC-02 should be properly configured via the BioManage software package from BioGuard. The software requires that the User ID belongs to the range of the "WIEGAND IDs Interval" parameters.

(Please see the "BioManage Software Guide" for more details regarding configuration of WIEGAND IDs Interval parameters).

Once the User ID has been configured within the unit's settings, the User can be enrolled in the same way as other Users, however, when it is required for a fingerprint to be presented, the Administrator must present his/her fingerprint. This fingerprint must not be one already existing in the unit and must not be used for authentication of the

Administrator in the future. That finger can, however, be used again in the future for assisting in the enrollment of any other User IDs that are being configured for ID only access.

**!** **Note:** When registering individuals using IDs, User templates within the unit will be associated with the appropriate card. With this in mind, please be aware that when a card is deleted ALL USERS ASSOCIATED WITH THAT ID WILL BE REMOVED. This particularly applies to Group Shadow ID's

**!** **Note:** The number configured on a proximity card can be read, set, changed and removed only via computer software not supplied by BioGuard.

**!** **Note:** A code can be any number between 1 - 65535 and can be made up of 1, 2, 3, 4 & 5 digit numbers. Numbers under 5 digits must be flowed by the # key or press 0 before the number. For example if the number 442 is required then you can enter 442# or enter 00442. If number 5542 is required then enter 5542# or 05542. 5-digit codes are valid and accepted provided they do not exceed the value of 65535.

## **2.10 Creating a Standard Delete Permission ID (SD ID)**

Each unit is delivered with a pre-configured Standard Delete Permission ID (SD ID) contained in a proximity card or token, normally labeled as 'Delete.' This is used for removing Users using just this one SD ID and the ID to be deleted. This ID could be a Group Shadow ID or an Individual Shadow ID (see section 2.13 for details on deleting a User using a SD ID).

Within the unit, the code associated with this SD ID had been pre-entered into the relevant settings area of the AC-02 to define the ID as a WIEGAND Delete ID.

If a different SD ID is required, a SD ID can be changed, or a new SD ID can be added only by using the BioManage software from BioGuard.

(For more information on configuring a Standard Delete Permission ID please see 'BioManage Software User Guide'.)

## **2.11 Creating an Enroll Administrator with Delete Permission ID (EAD ID)**

An Enroll Administrator with Delete Permission ID (EAD ID) is used to

create Administrator with Delete Permission IDs (AD IDs). As with the SD ID (see section 2.10) an EAD ID can be defined on the AC-02 only by using the BioManage software package from BioGuard. A pre-configured EAD ID is not supplied as standard with a BioSafe unit.

(For more information on configuring an Enroll Administrator ID with Delete Permission ID please see 'BioManage Software User Guide'.)

## **2.12 Creating an Administrator with Delete Permission ID (AD ID)**

An Administrator with Delete Permission ID (AD ID) is used to enroll Users into the BioSafe unit. The AD ID is not predefined in the AC-02 unit, therefore the ID to be enrolled can be on any compatible ID support (card, token or code as applicable). The AD ID is created by as follows:

- 2.12.1 Present an Enroll Administrator with Delete Permission ID (EAD ID). The red LED will flash for 5 seconds.
- 2.12.2 While the red LED is flashing, present the designated Administrator with Delete Permission ID (AD ID). Both the red and green LEDs will be lit.
- 2.12.3 While the two LEDs are lit, place the AD's finger on the sensor.
- 2.12.4 Hold finger on the sensor until both LEDs flash, then remove finger.

Successful (confirmed) enrollment: Both LEDs will be lit and the buzzer will produce a sound. The unit then returns to idle mode (green LED 'On'). Enrollment is completed.

Failed (rejected) enrollment: Red LED flashes with no sound. The unit then returns to idle mode (green LED 'On'). Repeat the enrollment process.

## **2.13 Deleting an ID including an Administrator with Delete Permission ID (AD ID) by using a Standard Delete Permission ID (SD ID)**

- 2.13.1 Present a Standard Delete Permission ID (SD ID). The red LED will flash for 5 seconds.
- 2.13.2 While the red LED is flashing, present the ID you wish to delete

Successful (confirmed) deletion: Both LEDs will be lit and the buzzer will produce a sound. The unit then returns to idle mode (green LED 'On'). Deletion is completed.

Failed deletion: Red LED flashes with no sound. The unit then returns to idle mode (green LED 'On'). Repeat the deletion process.

## **2.14 Deleting an ID by using an Administrator with Delete Permission ID (AD ID) fingerprint**

To delete an ID by using an Administrator with Delete Permission ID (AD ID) fingerprint, follow these steps:

- 2.14.1 Present an AD ID. Both the red and green LEDs will be lit.
- 2.14.2 While the two LEDs are lit, place the AD's enrolled finger on the sensor.
- 2.14.3 Hold finger on the sensor until both LEDs flash, then remove finger.
- 2.14.4 If finger is properly identified, both LEDs will be lit and the buzzer will sound, followed by the red LED flashing for 5 seconds.
- 2.14.5 While the red LED is flashing, present the ID that is to be deleted.

Successful (confirmed) deletion: Both LEDs will be lit and the buzzer will produce a sound. The unit then returns to idle mode (green LED 'On'). Deletion is completed.

Failed deletion: Red LED flashes with no sound. The unit then returns to idle mode (green LED 'On'). Repeat the deletion process and check that the correct ID is being presented for deletion.

**!** **Note:** When a card is deleted: ALL USERS ASSOCIATED WITH THAT CARD WILL BE DELETED.

**!** **Note:** Standard Delete Permission ID's and Enroll Administrator with Delete Permission ID's can only be removed from a unit using the BioManage software package from BioGuard.

## **2.15 Basic Operation**

- 2.15.1 Make sure the green LED is 'On'.
  - 2.15.2 Place a finger on the sensor. The green LED will turn off while the unit attempts to identify the finger. Both LEDs flash once the unit has completed reading the finger.
  - 2.15.3 Lift the finger. If properly identified, the green LED will flash and the buzzer will sound. If connected to a device such as an electric door lock, its latch will be released / activated for a predetermined delay (3 seconds by default, however this be changed by using the computer software).
  - 2.15.4 If not properly identified, the red LED will flash and the buzzer will produce no sound.
  - 2.15.5 Identification failure means that the system failed to identify the fingerprint. This could be due to one of the following:
    - A finger different than the one originally enrolled was used. Try again using the correct finger.
    - The reader did not accurately read the fingerprint on this occasion – try again.
    - The User is not registered in the system – contact the Administrator for advice on being registered onto the unit.
-

**For further questions or assistance, please contact  
BioGuard Components & Technologies Ltd:**



**Israel Office (Head Office):**

BioGuard Components and  
Technologies Ltd  
Beleres House, Suite 7  
11 Ha'Avoda St.  
Rosh Ha'Ain  
Mail: P.O. Box 1418  
ISRAEL 48017

Tel: +972 (3) 902 5902  
Fax: +972 (3) 902 1808

Email:  
info@bio-guard.net

**European Office:**

BioGuard (UK) Ltd  
  
Fairgate House  
205 Kings Road  
Tyseley  
Birmingham  
B11 2AA  
UNITED KINGDOM

Tel: +44 (0) 121 708 5457  
Fax: +44 (0) 121 708 5465

Email:  
info.europe@bio-guard.net

[www.bio-guard.net](http://www.bio-guard.net)