smart i™
Smart identification Solutions

USER MANUAL & WARRANTY CERTIFICATE

BIOtrak

Fingerprint & Card Based Attendance Terminal
For Multi-location Attendance Management.

Model No: SBNG0330 *series*

Preface

Congratulations on purchasing your new ***BIOtrak*** and thank you for the confidence you have shown in us. You have chosen a high-quality product that has been manufactured, tested and packed with care.

Please familiarize yourself with these instructions, before attempting to install the ***BIOtrak.*** Because prolonged reliable and trouble-free operation will only be ensured if it is fitted properly. We hope your new ***BIOtrak*** will bring you lasting safety and effective operations for your employee attendance.

BIOtrak series are Cost effective Biometric System with rugged design & Touchscreen keypad. It boasts of compact aesthetics and strong design with flawless fingerprint optical sensor.

Disclaimer:

- *Please handle the equipment with care. Physical Damage to the system is not covered under warranty.*
- *Do not power on the system without reading this manual. Ensure proper power supply with Earthing.*
- *Note down the serial number and model no. of the device for future reference and quote in all support and service requests.*
- *To connect or interface the Card reader to the **'BIOtrak'** unit please refer to the Hardware Installation Guide or Manual and carefully follow the instructions. A trained technician must make the connections.*
- *Any negligence on your part may damage the Card reader interface on the BIOtrak terminal.*
- *Mounting the unit in strong sunlight may affect user visibility of the LCD. Ensure that the LCD and LED's are clearly visible in all lighting conditions.*
- *The fingerprint sensor glass may periodically require cleaning - use suitable glass cleaner.*
- *Never insert objects of any kind into the unit or through the cabinet slots as they may touch voltage points and/or short circuit parts possibly resulting in fire or electric shock. Never spill liquid of any kind on the unit.*
- *When connecting up the BIOtrak ensure that the mains power supply is safely isolated. Power up the controller only when installation is complete.*

As this product is regularly updated, we cannot guarantee exact consistency between this product and the information provided in these instructions. We will hear no disputes that arise due to differences between the actual product and the contents of these instructions, and you may not be informed of **changes in advance.**

Table of Contents

Fire Safety and accountability Notice

When connecting card or Biometric readers to any emergency entry, exit door, barrier or elevator must provide an alternative exit in accordance with all fire and life safety codes pertinent to the installation. These fire and safety codes vary from city to city and you must get approval from local fire officials whenever using an electronic product to control a door or other barrier.

Imperative Directives

- Take the backup of the finger prints of all the users after enrolment, through the Template Upload/Download Option in Software (Refer User Manual of Software for taking finger prints backup and uploading the backup finger prints back to the BIOtrak devices.)

- Care should be taken identifying the wires. Improper wiring may render permanent damage to the device or personal injury.

- Refer the colour code on the Reader to connect the external Wiegand reader on the controller.

- Check the earthing at the site before installing the controllers. Normally the earthing should be between 1V to 2V only. Earthing on the higher side may damage the controller or its various other components.

The Contained in This Manual are Subject To Change without Notice at Any Time. It is Smart I's goal to supply accurate and reliable documentation. If you discover a discrepancy in this document or Need Help, please e-mail your comments to **support@smartisystems.com**

USER MANUAL
BIOtrak
Version: 1.0

SMART-I ELECTRONICS SYSTEMS PVT. LTD.

An ISO 9001:2008 certified company

Units No 250 to 252, Second Floor, Building No D-7, Bhumi World,
Pimplas Village, Bhiwandi, Thane-421302, Maharashtra. INDIA.
Web: www.smartisystems.com

Warning & Caution

- Please handle the equipment with care. Physical Damage to the system is not covered under warranty.
- Do not power on the system without reading this manual. Ensure proper power supply with Earthing.
- Note down the serial number and model no. of the device for future reference and quote in all support and service requests.
- To connect or interface the Card reader to the 'BIOtrak' unit please refer to the Hardware Installation Guide or Manual and carefully follow the instructions. A trained technician must make the connections.
- Any negligence on your part may damage the Card reader interface on the BIOtrak terminal.
- Mounting the unit in strong sunlight may affect user visibility of the LCD. Ensure that the LCD and LED's are clearly visible in all lighting conditions.
- The fingerprint sensor glass may periodically require cleaning - use suitable glass cleaner.
- Do not use this unit near water.
- Never insert objects of any kind into the unit or through the cabinet slots as they may touch voltage points and/or short circuit parts possibly resulting in fire or electric shock. Never spill liquid of any kind on the unit.
- When connecting up the BIOtrak Access Controller ensure that the mains power supply is safely isolated. Power up the controller only when installation is complete.

Get started with Biotrak

Included items:

Product	Image	Qty	Use
Biotrak		1	Attendance System
Power Supply		1	Supplying power for the Biometric Unit
Software CD	http://www.smartisystems.com/Software.html	1	For Device Configuration/ Management & For Data Downloading
Installation Guide & Test Report		1	For referring functions keys for programming the device by keypad & Other Installation Details

Power Supply Specification:

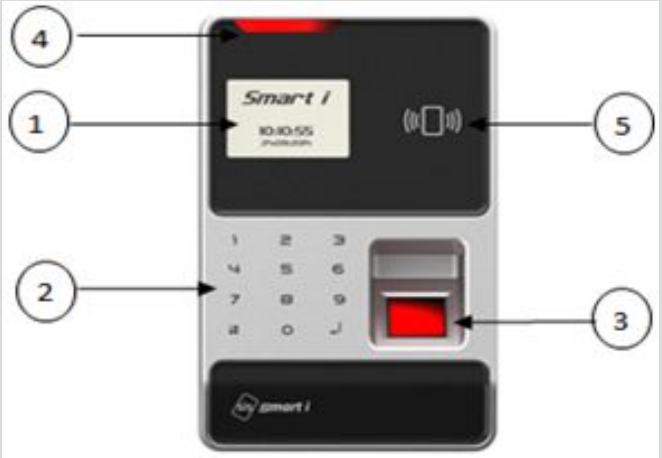
In case you do not have the required power supply included in the package and intends to buy your own power supply use these specifications. Below given specifications should be strictly adhered to.

Device	Application	Power Supply	Input	Output
Biotrak	Attendance & Access (Lock Voltage)	Universal AC Adapter Isolated i/o	110 to 230 VAC	12 V DC/ 2A (Min)

Introduction

The new **BIOTRAK**blends loads of innovative features to streamline installation and administration for small, medium or, large business enterprises for standalone door access control deployment. **BIOTRAK**brings the high speed, accuracy, flexibility and user friendly interactivity. It provides intuitive and aesthetic GUI on graphical LCD with easy-to-use touch sense keypad.

Description of keys & other parts



① LCDGraphical LCD

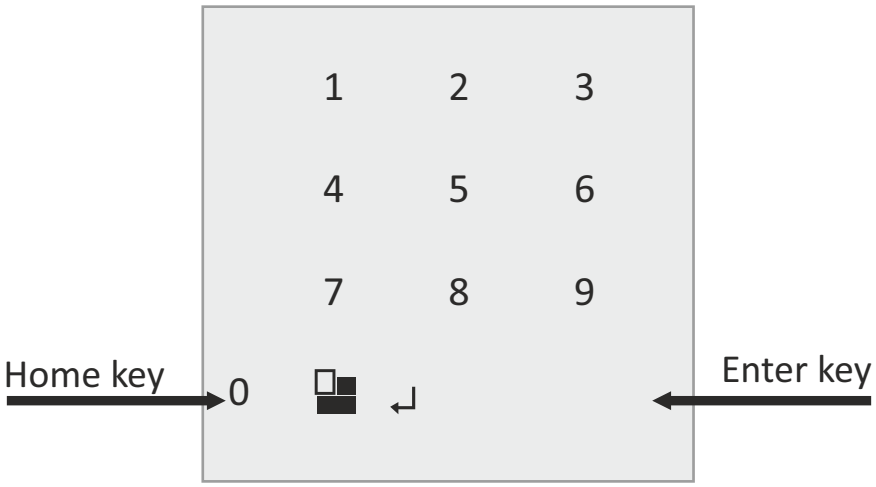
② KeypadCapacitive Touch Keypad

③ Bio sensor Optical sensor

④ LEDTricolor LED Bar

⑤ RFID card reader

Operational keys:



keys	Description
Numeric keys(0-9)	To access keypad functions& to enter UID for verification
Keys 2 & 8	Scroll keys to select menu after admin login.
Keys 4 & 6	Scroll keys to select options
Home screen key	To go to the home screen
Enter key	Entering into menu parameter and set the values for parameter

Specification

Hardware Specification:

Particulars	Description
CPU	32 Bit RISC Arm
Memory	Upto Flash 8 MB
Events/Transactions	50000
No. of templates in sensor	3000
No. of Users	7500
Operation Modes	Finger + Card + Pin
Sensor	High Quality Scratch Resistance Optical Sensor.
Communications Port	TCP/IP, weigand, Rs485
Baud Rate	9600bps (Default)
Controller ID	Max 9999
LCD	Graphical LCD
Keypad	Capacitive Touch Keypad
LED	Tricolor LED Bar
Language	English
Power Supply	12 V DC/ 2A (Min)
Enclosure	ABS Plastic
Color	Silver & Black
Dimension (H X W X D) in mm	167 x105 x 45
Mounting	Wall Mounting

Sensor Specification:

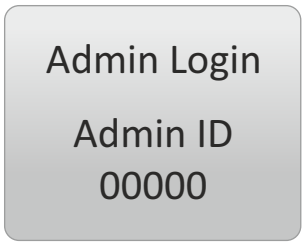
Particulars	Description
Type	Optical Finger print Sensor
Image Resolution	500 dpi
Enrollment Time	<1 sec
Verification Time	<1 sec
Authentication / Identification	Upto 1000 1:N & Up to 3000 1:N (User Groups facility for faster verification)
Identification Time	1 sec
Template Size	496 bytes
EER/FAR/FRR	FAR<0.001%(Security level 3),FRR<0.1% (Security level 3)
Image Size (Pixels)	242*266 pixel
Sensing Area (mm)	18*22mm

Display & keypad Interface

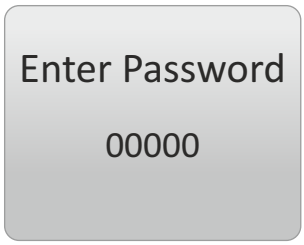
Home Screen

After power on the unit, the unit shows the below home screen.

Login Screen

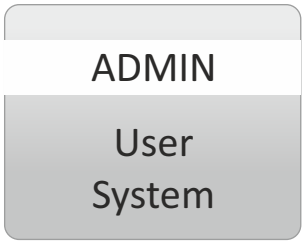


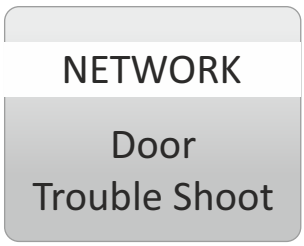
Press home key from keypad, you get Login screen. Enter admin ID i.e 11111 (default) &press 'enter' key from keypad.



Then enter password i.e. 12345 (default)

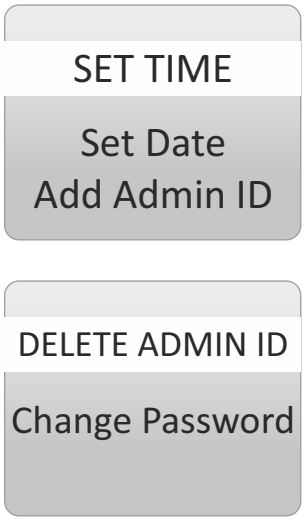
Main Menu Screen





If admin ID & password is right then you get menu screen.

Admin

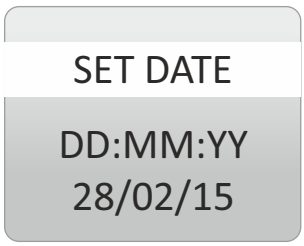


This mode is used to set time and date, add/del/change admin users and to change its password.
Select Admin by moving cursor using keys 2 & 8. Then press enter key.

Set Time

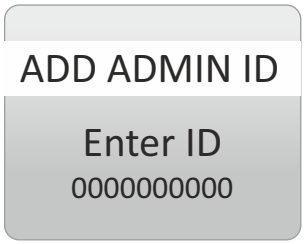
In this menu user can change the time format & time according to user's requirement using the keypad. After selecting time format press enter then set time, press enter to set it.

Set Date



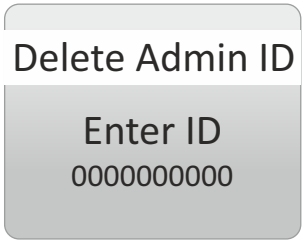
User can edit the date according to his requirement using keypad. After editing the date press enter to set it successfully.

Add Admin ID



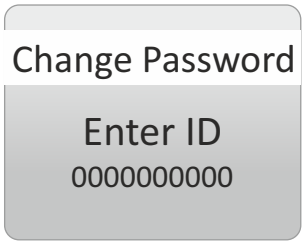
In this mode, enter the Admin id and password and press enter to go back to the submenu
User can create Admin ID by entering ID and password. With the added admin ID user can log in, but depending upon the authentication level set, user can access selected features..

Delete Admin ID



In this mode, user can Enter the admin ID and password and press enter to delete the created admin ID.

Change Password

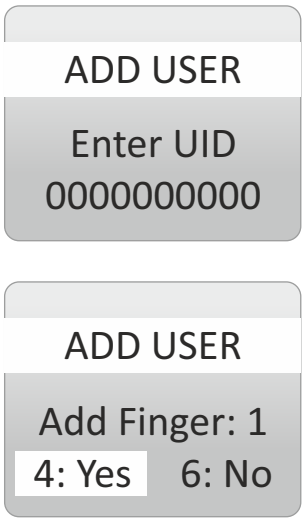


In this mode enter the admin ID or shows card, press enter key then system ask for old password, enter old password & press enter after then system ask new password , enter new password and then press enter to set the change password successfully.

User

This mode is used to access all different parameters related to the user such as add user, delete user, search user, bulk add card, change pin, add user data, and facility code.

Add User

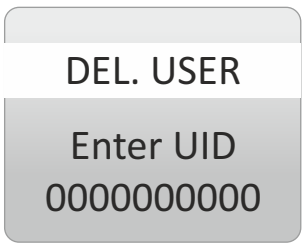


In this menu enter the UID or show the card and press enter and select finger addition YES No option by 4 & 6 keys. Select YES option to enroll the finger or select NO to add only card or UID.

If you select YES then it ask to place New finger with sensor ON follow the instruction displayed on screen . After finger gets added it shows finger Added & then asks for 2nd finger.

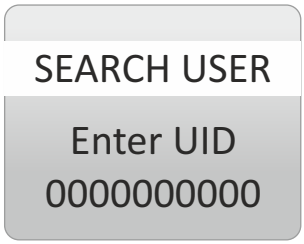
If you want to add 2nd finger then press key 4.
To add more fingers you can use 'Add fing. to ID' menu.

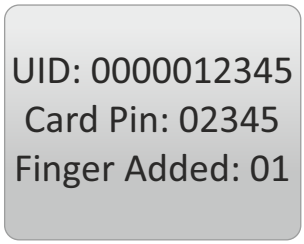
Delete User



In this menu, enter the UID no. or show card and press enter to delete that user and its fingers.

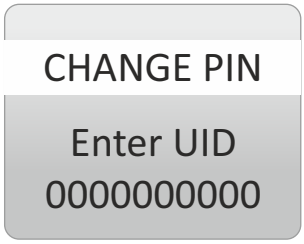
Search User

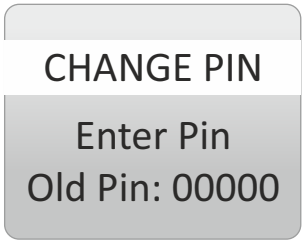


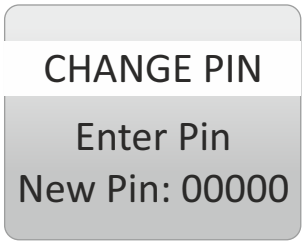


In this menu enter the UID or shows card and press enter to displays card pin and enrolled fingers no.

Change Pin

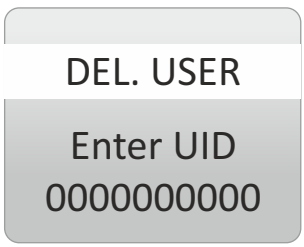






Enter the UID or show card then it will ask for old pin and then for new Pin and press enter to set the new added pin for particular UID successfully.

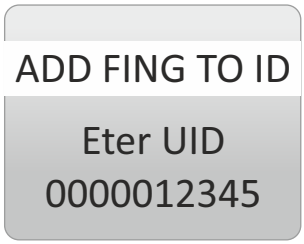
Add User Data

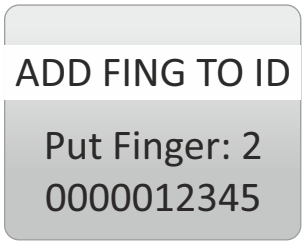


In this menu, Enter the UID or show card for which you want to add the data and press enter. And select the following card types according to user:

1. UID/Card+Finger
2. UID/Card only
3. Card+Finger
4. Card Only
5. UID/CARD+F+ PIN
6. Finger only
7. Card & finger
8. Press enter to set it successfully.

Add Finger to ID

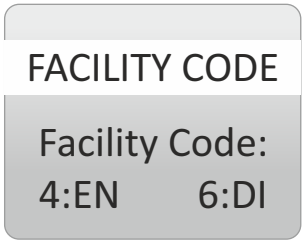




After selecting **Add Fing to ID** enter the UID no. or show card and press enter, sensor get ON to add fingers for that particular UID with score.

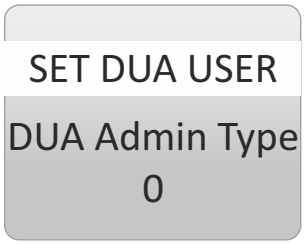
Note: Only added user can enroll finger by this menu.

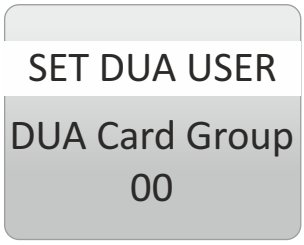
Facility Code



By using the keys 4 and 6 user can enable and disable the facility code. After enabling the facility code it will ask for the location, set the location & press enter then show card to get facility code from that card and after getting facility code press enter.
You can set 8 different facility codes.

Set DUA user





To set dual authetication as per user enter in this menu. Enter UID or shows card & press enter key. Then enter master type & then select group. If you want duress check for perticuler user then enter 1 to enable duress for that card.

Please refer annexure C.

Set DUA User

DURESS CHK
0

System

Set Slave ID

Set Controller No
Sensor

This mode is used to select the different parameters of the unit like set slave ID, controller no, controller type, weigand bits etc. by using the 2-8 keys we can select the require option.

Controller Type

Weigand Out
Display

DualAuth EN/DI

Keypad EN/DI
Sound EN/DI

Set Slave ID

Set Slave ID

Set Controller No
000

Select an option and press enter to go in slave id menu, in this menu enter the desired slave ID and press enter to update it. Default slave ID isWe can set max 128 slave IDs to device.by using the 2-8 keys we can select the require option.

Set Controller ID

Set Controller ID

Controller No:
00000

We can set unique controller no. using this menu. After entering the controller no. press enter to update it. We can set max 10000 controller nos. to device.

Sensor

Identify Mode

Sensor Security
Verifying DB EN/DI

From this menu you can set sensor mode, security levels.

Identify Mode

Identify Mode

Normal
Identify By Key
Auto Identify

By using keys 2-8 select the mode and set press enter to set it.

In Normal mode, after showing card + enter or entering UID+ enter, sensor gets ON.

In Identify By key mode, when # key is pressed sensor gets ON.

In Auto Identify mode, Sensor remains continue ON (If single Template is present in Device).

Sensor Security

SENSOR SECURITY

Level: 04
Level: 05
Level: 06
Level: 07

SENSOR SECURITY

Level: 08
Auto Normal 09
Auto Secure 10
AutoMSecure 11

In this menu security level specifies the false acceptance ratio.

User can set sensor security according to the level defined in menu. Max 12 levels are specified but the Default level is 6. Using keys 2-8 select the level and press enter to set it.

Refer annexure B.

Verify Finger DB EN/DI

Verfy FngrDB EN/DI

Verify Finger DB
4:YES6:NO

This is used to verify finger DB at the time of enrollment. Normally it is enable to check same finger but as template data goes on increasing then it will take more time to enroll finger. To reduce this time press 6:NO i.e. to do not check same finger.

Controller Type

Controller Type

Bio Access
Bio Access 2RD
Bio Att.
Bio Att. 2RD

Controller Type

Bio Att. No Chk
Bio Att No Chk 2RD
Bio Att. SCNoChk
Bio Att. SCNoChk 2RD

Controller Type

Deny List
Bio No Check
Deny List Bio No Chek

In this menu user can set total 12 different controller type. Depending upon the controller type unit will give access to the user, default controller type is Bio Access. After selecting the controller type On/Off the system.

For controller mode set bio access or Bio Attendance mode.

For reader mode set bio attendance no check or deny mode.

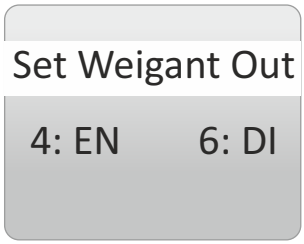
Weigand Out Reader

Set Weigand Out

Weigand Bits

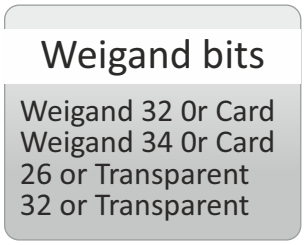
Use this menu when device set as a reader with another controller.

Set Weigand Out



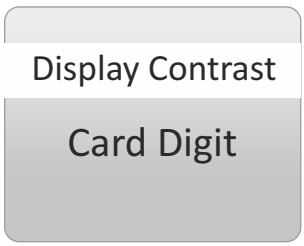
To enable weigand reader mode press 4 to disable& press 6.

Weigand Bits

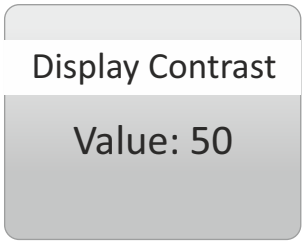


In this menu, user can select the six different type of weigand formats. Select itand press enter to set it. Default is 32 or transparent.

Display

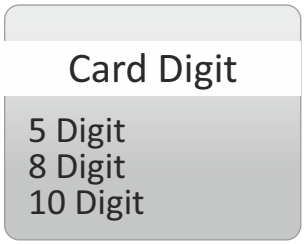


Display Contrast



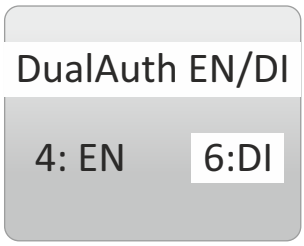
In this menu you can set display contrast as per your requiment.

Card Digit



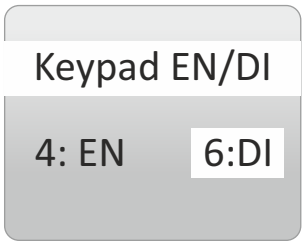
In this menu, user can set the three types of card digit display. We can set it as 5-digit,8-digit,10-digit depending upon the user requirement. User can select it using 2 & 8 keys and press enter to set it successfully.

Dual Auth EN/DI



To enable dual user authentication.
Press 4 to enable & press 6 to disable this functionality.

Keypad EN/DI



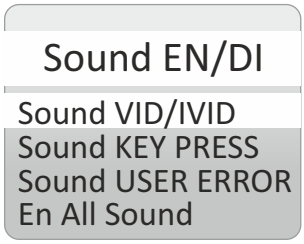
To avoid uanwanted user's access of keypadthen disable itso no one can access keypad menus.

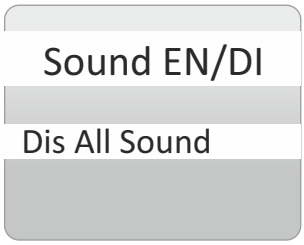
Press 4 to enable & press 6 to disable this functionality.

To enable keypad press Home key for 5 times within 5secs.

Note : After logout keypad get disable again so do above to enable keypad.

Sound EN/DI





Sound VID/ IVID

Enable sound on for valid & invalid user.

Sound Key Press

Enable sound for key press

Enable All sound

Enable all sound like for valid/invalid card, key press, access error for card.

Disable All sound

Disable all above sound.

Network

Network Setting

EnDisTCPPush
Server Auth

In this mode we can change the network setting according to user network settings. We can also disable and enable the MAC security to secure download the transaction.

Network Setting

Network Setting

IP Address:
192.168.000.200

In this menu user can edit the various parameters such as, unit IP address, subnet mask, default gateway, server IP address …..etc.
User have to set various parameters such as,
IP Address
Subnet mask
Gateway
Server IP Address
Local port No
Push Server1 IP
Push Server1 Port
Push Server2 IP
Push Server2 Port
UDP IP Address
UDP Port No
DNS Server IP
HB Server IP
HB Port No
HB Time in Min
UDP Server Port
Enter the proper value and press enter to set other parameters After setting all parameters need to restart the device.

EnDis TCP Push

EnDis TCP Push

4:EN6:DI

To enable TCP push functionality. For TCP push works need to set server IP address & port no by Network setting menu.

Server Authentication

EN/DI ServerCHK

4:EN6:DI

To enable Server authentication functionality.

For this functionality need to set server IP address & port no by Network setting menu.

This functionality is used where user authentication done by server.

AuthSvr1 IPAddr

IP Address:
192.168.000.3

AuthSvr1 Port No.

Port No.
3001

AuthSvr1 IPAddr

IP Address:
192.168.000.3

AuthSvr1 IPAddr

Port No.
3001

Door

Door Open Time

Reader In/Out
Fire-TAMPER EnDs

This mode is used to set the door open time, reader in/out setting, FIRE-TAMPER EnDs

Door Open Time

Door Open Time

Enter Time:
005

In this menu user can set the door time from 1 to 98secs as on his requirement.
Enter the door open time and press enter to set it.
Default door open time is 5sec.
Scroll Down for Door open time Min/Sec.

Reader IN/OUT

Reader In/Out

Reader Normal
Reader In
Reader Out
RdrInOut Toggle

In this menu user can set different bio-metric reader type.
Default reader type is Reader normal.

I. Reader normal

ii. Reader IN – It shows IN entry on display

iii. Reader OUT – It shows OUT entry on display

Reader IN/OUT Toggle – IN OUT entry can toggle using 0 key.

FIRE-TAMPER EnDs

Reader In/Out

DISABLE ALL
ENABLE FIRE
ENABLE TAMPER
EN FIRE-TAMPER

In this menu user can enable disable fire and tamper by selecting the particular option by keys 2 & 8 and press enter to set it successfully.

Troubleshoot

Initialize System

Weigand Display
Network test

In this mode, we can initialise the system,test the network and weigand display. We can initialise the particular parameter like transaction, system info,facility code, time zone error etc.

Initialize System

Del Transaction
Del All Users
Set All Default

In this menu user can initialize the system according to different parameters.
Use 2 & 8 key to select particular menu.
After selection press enter. It shows yes & no option.
Press 4 to YES& 6 to NO.

Delete Sys Info

Del Time Zone
Del Holiday

Del Facility Code

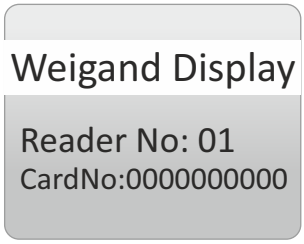
Del Door info
Del Admin IDs

Rest System

Del Cards Only
Del All Fingers

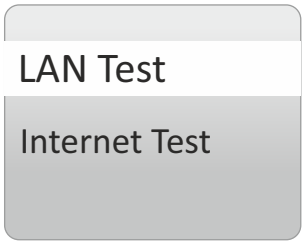
Delete All Data

Weigand Display



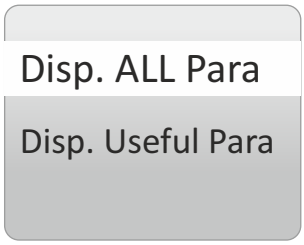
In this menu, card information is displayed after showing card on reader such as,
Card No , Reader No
Weigand Bits
Parity chk
Weigand Raw data
Extra data

Network Test



In this menu,we can test the LAN test and Internet test. If N/W settings are proper then you get TEST OK message for each.

Device Info



In this mode, we can see the all the information related to the product specification and features.

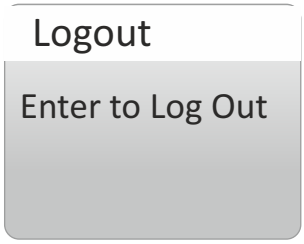
Display All Parameter

Select the option and press enter to go in display all parameter. In this menu, user can see all the parameters related to the product setting like terminal ID, IP address, net mask, gateway, server IP but user cannot edit it.

Display Useful Parameter

In this menu user can see the product related information like, model no., used card buffer, firmware version….. etc. by pressing enter key.

Logout mode



In this mode we can log out from the log in admin ID by pressing the Enter key.
Press enter key.

Annexure A

Security level setting

Security level specifies FAR (False Acceptance Ratio). If it is set to “Level 2” i.e. 1/100,000, it means that the probability of accepting false fingerprints is 1/100,000.

The following table shows the relationships between the automatic security levels and the number of enrolled templates. For example, when the security level is Automatic Secure and the number of enrolled templates is 500, the actual FAR for identification will be 1/10,000,000. The security level for verification is not changed.

Automatic Level	Verification (1:1)	Identification (1:N)			
		1 ~ 9	10 ~ 99	100 ~ 999	1000 ~
Normal	1/10,000	1/10,000	1/1,00,000	1/10,00,000	1/10,00,000
Secure	1/1,00,000	1/1,00,000	1/10,00,000	1/1,00,00,000	1/1,00,00,000
More Secure	1/10,00,000	1/10,00,000	1/1,00,00,000	1/10,00,00,000	1/10,00,00,000

Annexure B

Network setting

Sr. No.	Network Setting Parameters	Description
1.	IP Addres	Set IP address to device for TCP/IP communication
2.	Subnet Mask	As per your network.
3.	Gateway	As per your network.
4.	Local TCP Port	For device identification and communication
5.	Local UDP Port	For device identification and communication
6.	Server IP	Set Server IP Address, it is used when MAC security feature is Enable.
7.	PUSH Server1 IP	Set Server IP Address where we want to push transaction data using TCP.
8.	PUSH Server1 Port	Set Server IP Address where we want to push transaction data using TCP.
9.	PUSH Server2 IP	NA
10.	PUSH Server2 Port	NA
11.	UDP PushServer IP	Set Server IP Address where we want to push transaction data using UDP.
12.	UDP PushServer Port	Set Server IP Address where we want to push transaction data using UDP.
13.	HB Server IP	Set Server IP Address where we want to push Heart Beat data. Device sendsall important information to this server.
14.	HB Server Port	Set Server Port Address where we want to push Heart Beat data.
15.	HB Time	Set Heart Beat Time, this is time delay after which controller send Device Information to HB Server IP.

Annexure C

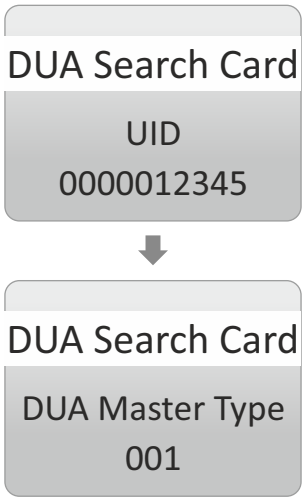
Procedure for configuring users for Dual Authentication

1) Firstly You have to LoginPress Home key press " 11111"Press Enter Password "12345"Press Enter.

2) Enroll the finger for Users from User menu.
Go in User menu Enter in Add user Show card or Enter UID press enter Press 4=YES Press Enter Sensor get ON Place Finger it will Display Finger Added with ...%.

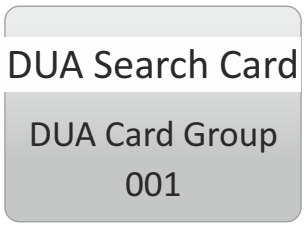
3) Repeat Step no.2 for Number of Users to added in Unit.

4) Now to config dual user go in User menu & select 'DUA Search Card'.
Show card or enter UID.

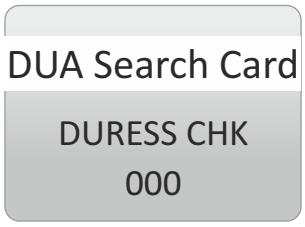


Press Enter.

Now enter 01 for Master & 00 for normal user. Press Enter.

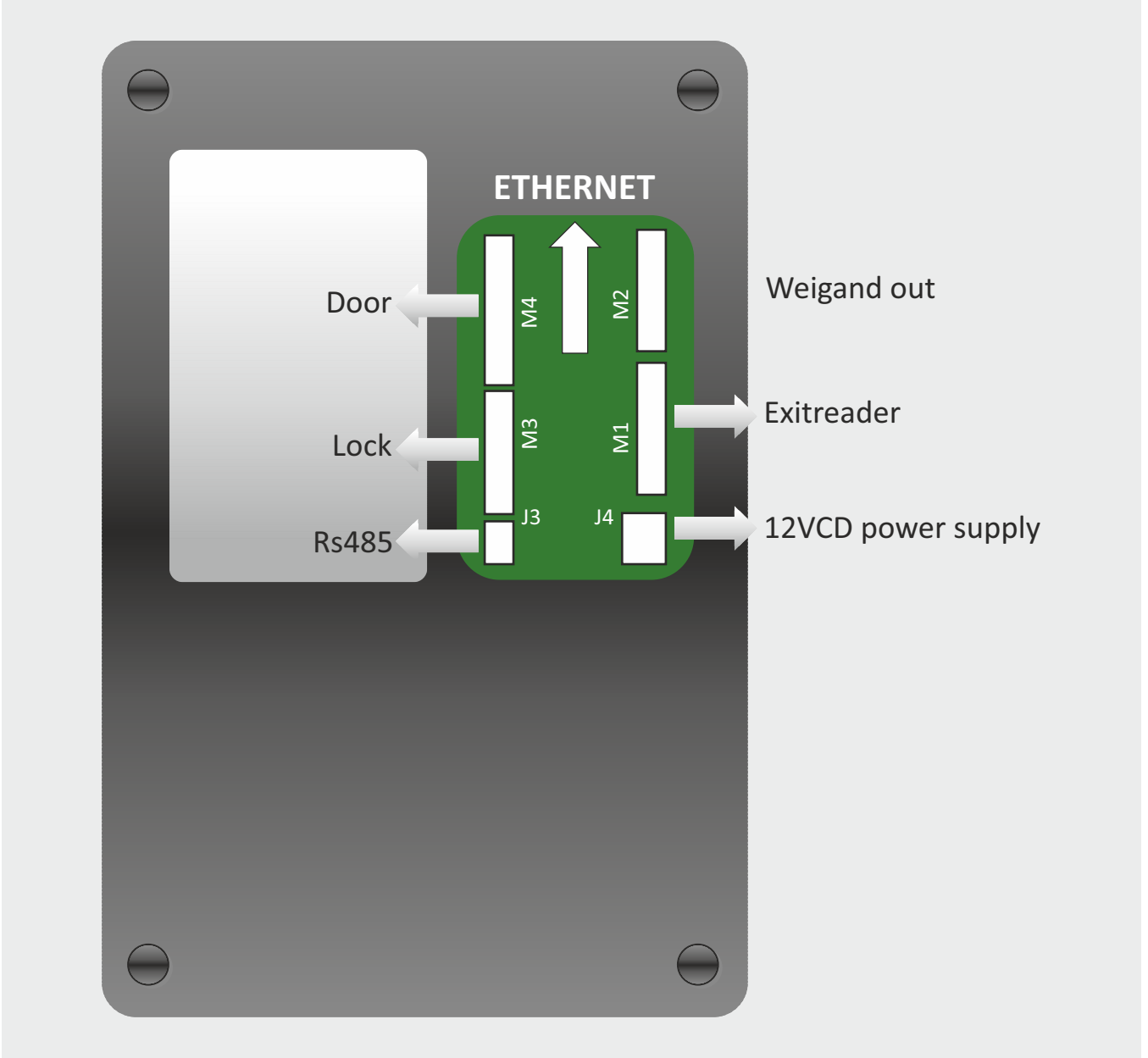


Assign Group no. Press Enter.



Press "01" to enable Duress & Press "00" to Disable Duress
Press enter (it will go for next card number)

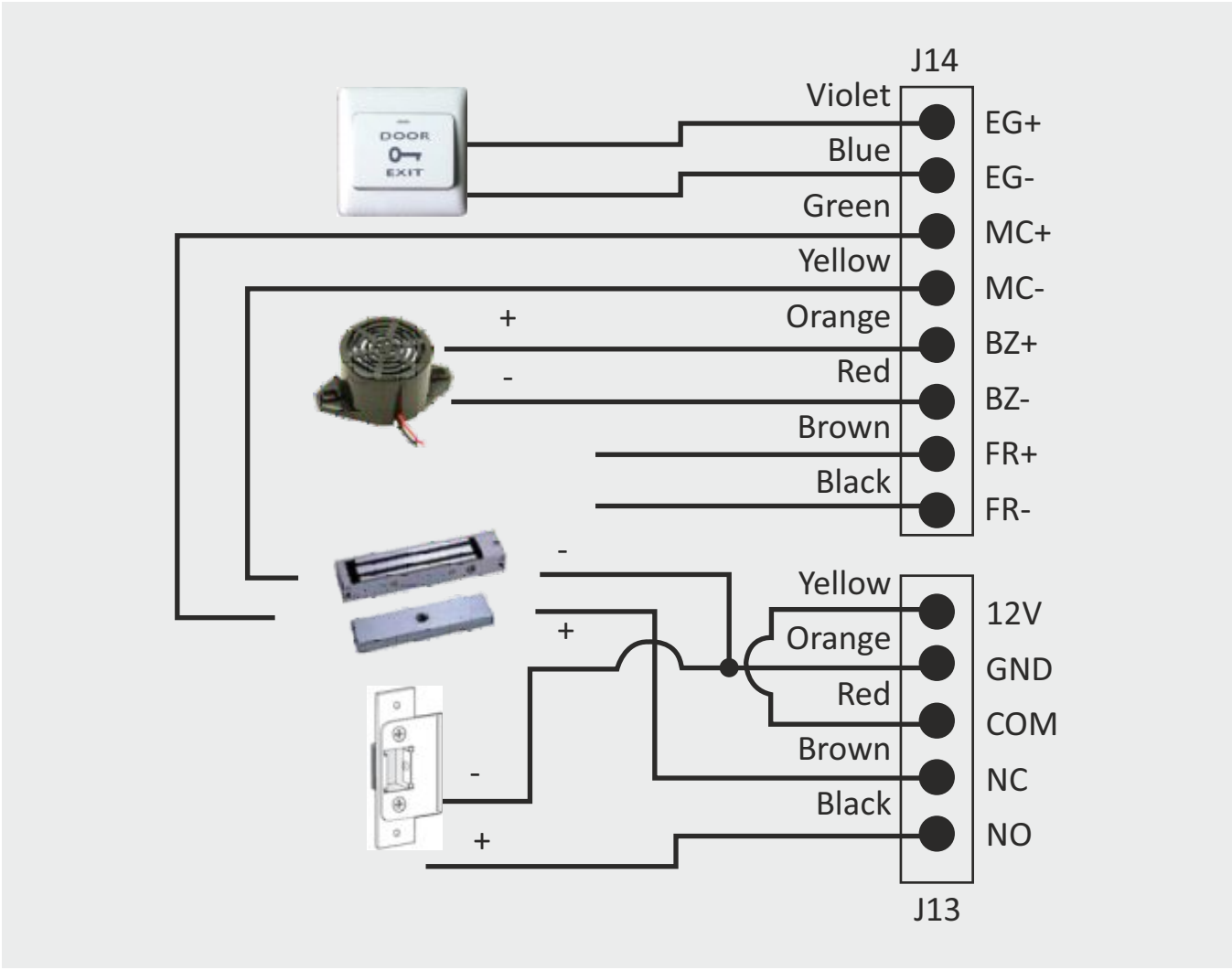
Biotrak connection details



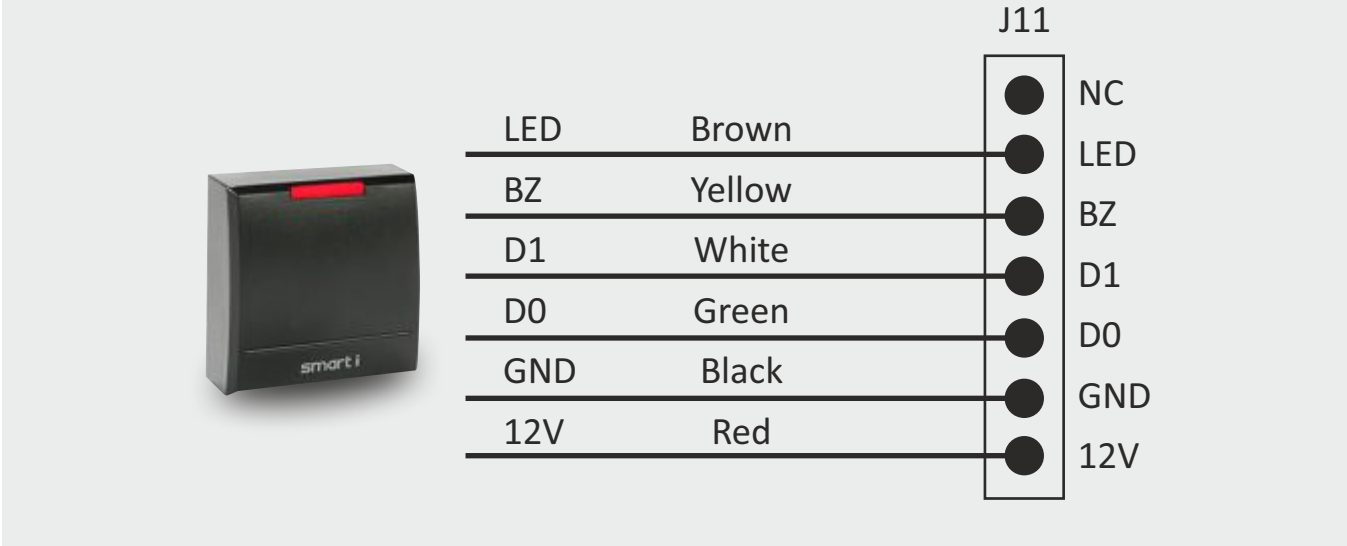
Power Supply connection:

12DC power supply

Door connection

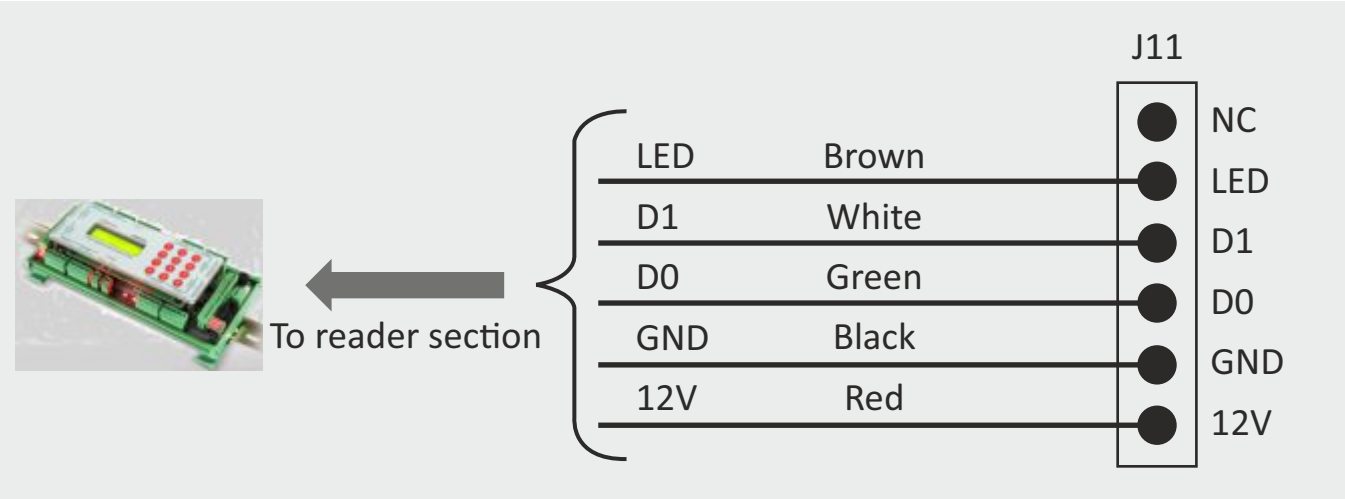


Exit reader connection:



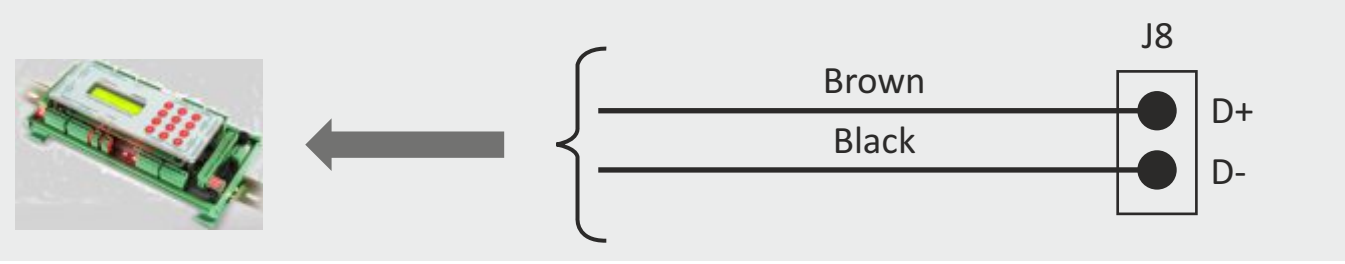
Weigand OUT connection

In weigand out mode need to use this connection to connect with controller at it's reader section.



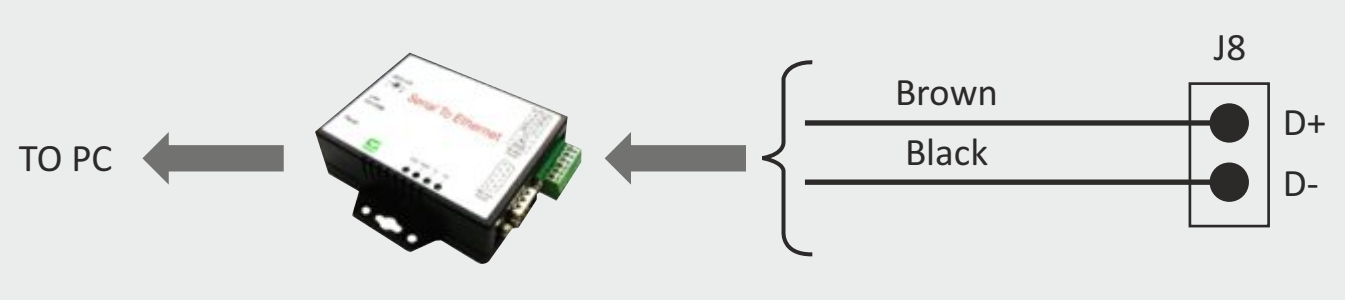
Rs485 connection:

To controller for template management by TCP/IP comm.

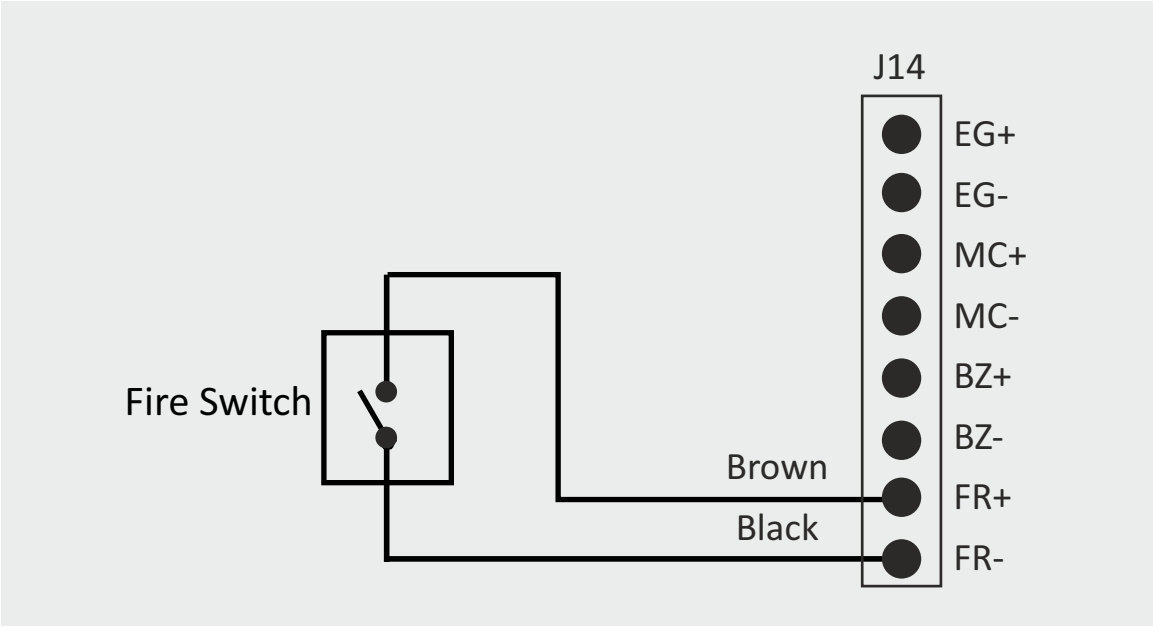


OR

To RS485 converter for serial communication.

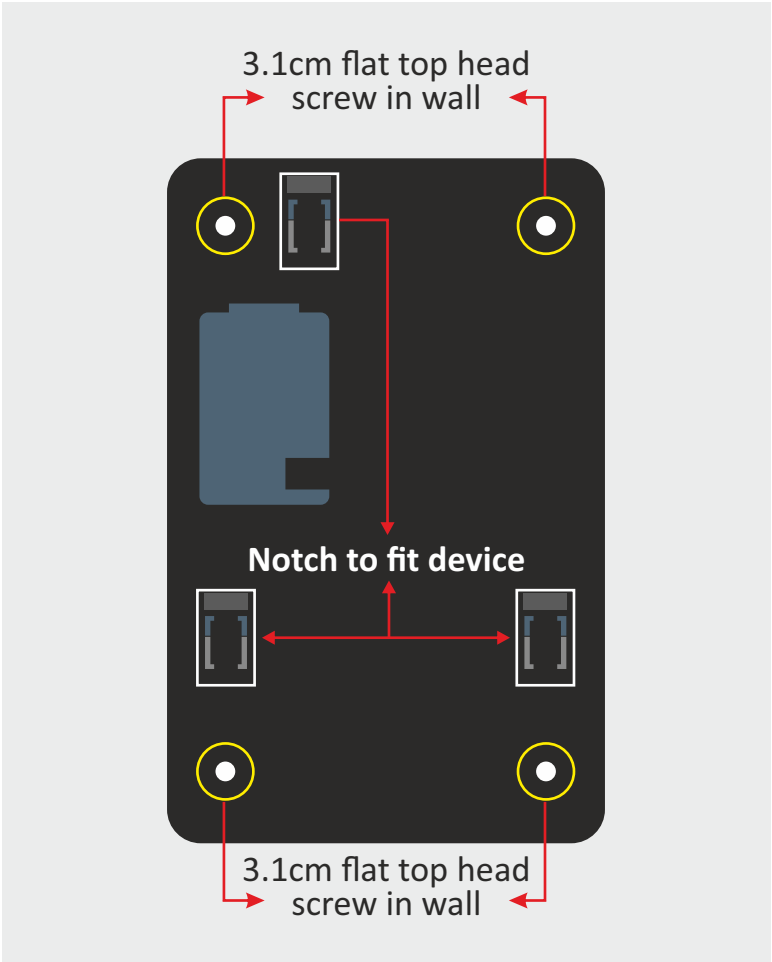


Fire Panel connection

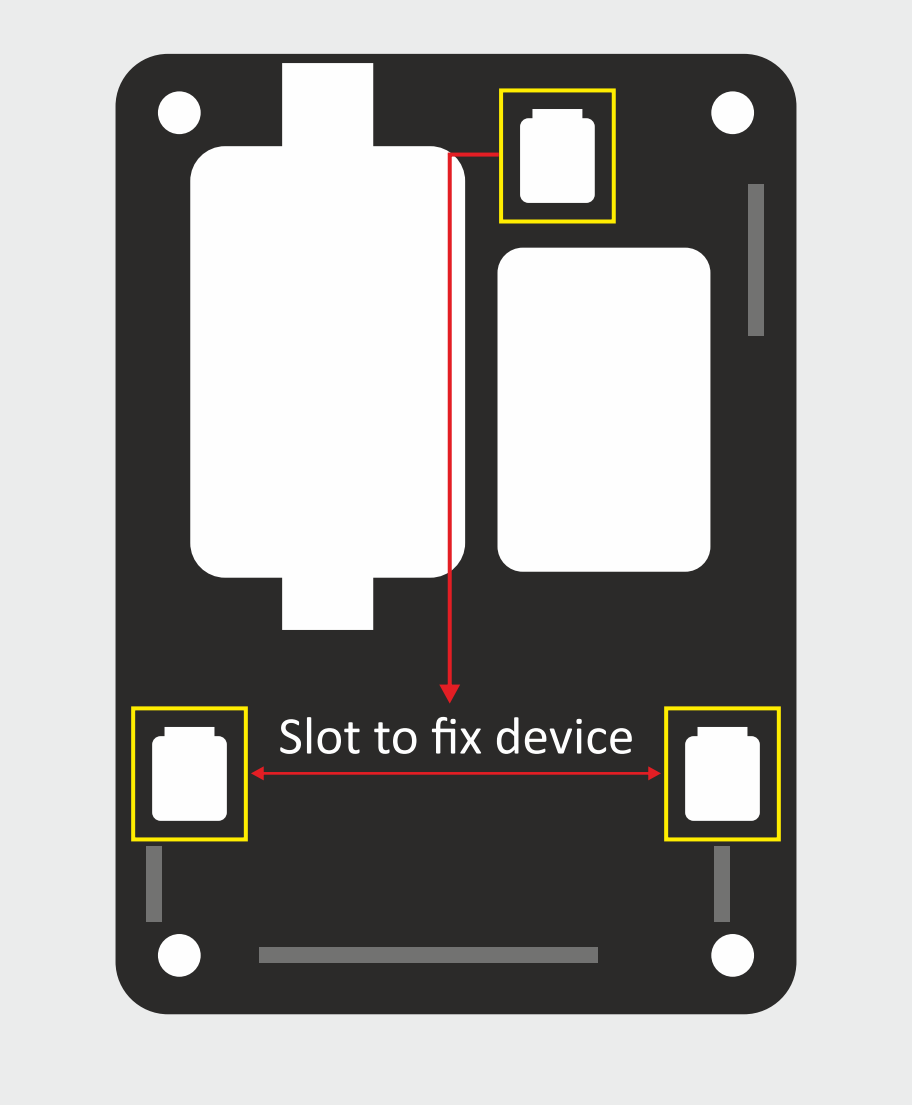


Mounting of unit on the wall

In weigand out mode need to use this connection to connect with controller at it's reader Fit the wall mounting plate on the wall as shown and screw the plate on the wall using the drill machine and 3.1cm screws as shown below:



1. Fit device on back plate by fixing the slots given at the back cover of device.



Connecting To Host Computer

The Biotrak can be connect to the computer by TCP/IP (Ethernet).

*Note: Use proper manually crimped**CAT5**cable, Refer bellow images,*

Manually Crimped RJ-45

ReadymadeRJ-45

The Biotrak series can be connected on the LOCAL AREA NETWORK (LAN) Or Wide Area Network (WAN) as under:

Connecting single controller directly to a PC Using TCP/IP (CAT5) Network Cable

Step 1

Use the crossover network cable, with one end connected to the Biotrak TCP/IP port, and the other end to your PC network adapter.

Step 2

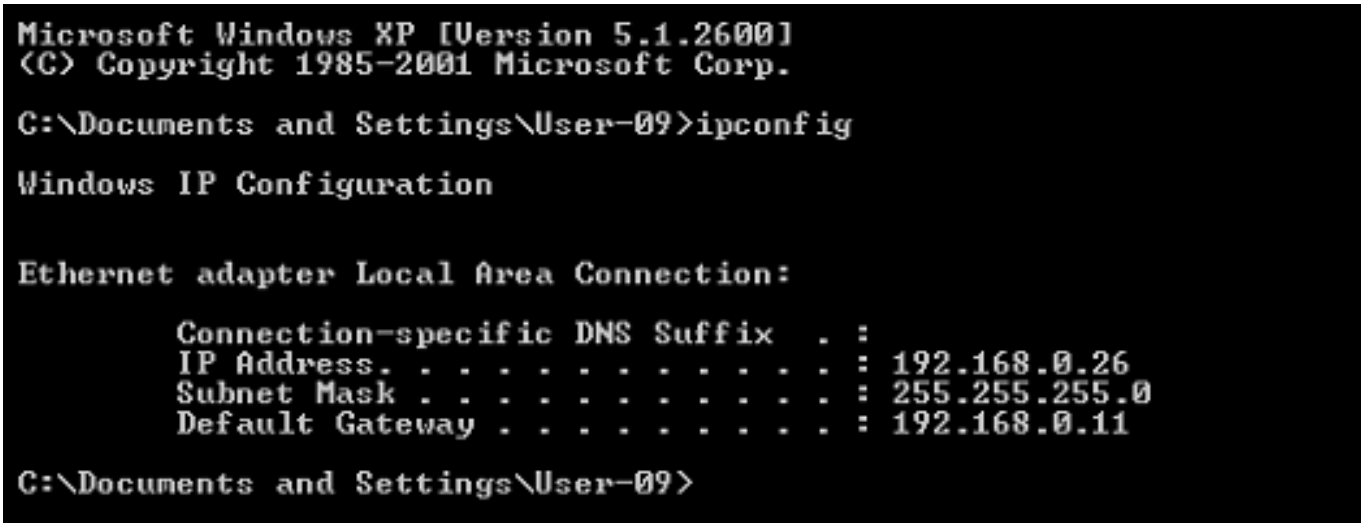
To check your PC's IP Address Settings, find out the IP address of the network. To do so, go to a PC in the network presently, press Start -> Run -> Type “command” and click on 'OK'.

Step 3

Type “ipconfig” and press 'Enter'.

Step 4

Note the IP Address displayed, following is an example.



Step 5

To Check the IP Address of controller press HOME KEY enter user id (11111) then Enter Password (12345) press ↵ then select network call which will display the Current IP Address to Controller, make a note of it. (Default IP of the controller is 192.168.000.200)

Step 6

To change the IP Address in Controller unit. Refer Configuration of Biotrak (port is default 01234 no need to change)

Testing the Connection

Once the configuration is complete, it is recommended that the connection be tested. To test the connection following is the under mentioned steps

Step 1

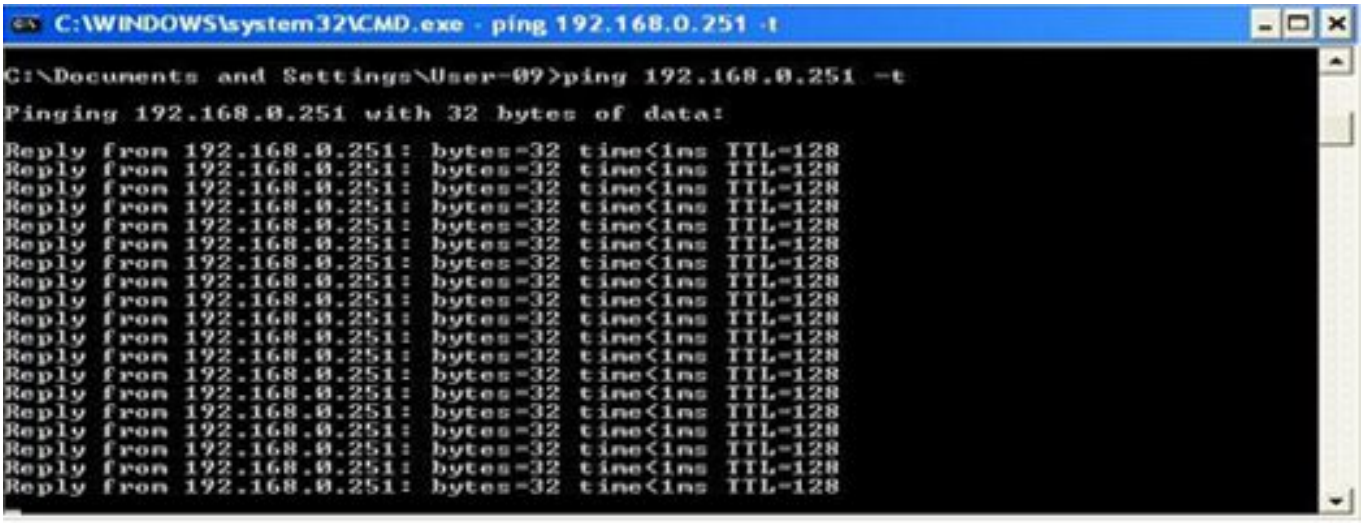
At the PC, Click Start -> Run -> Type “command” and press 'OK'.

Step 2

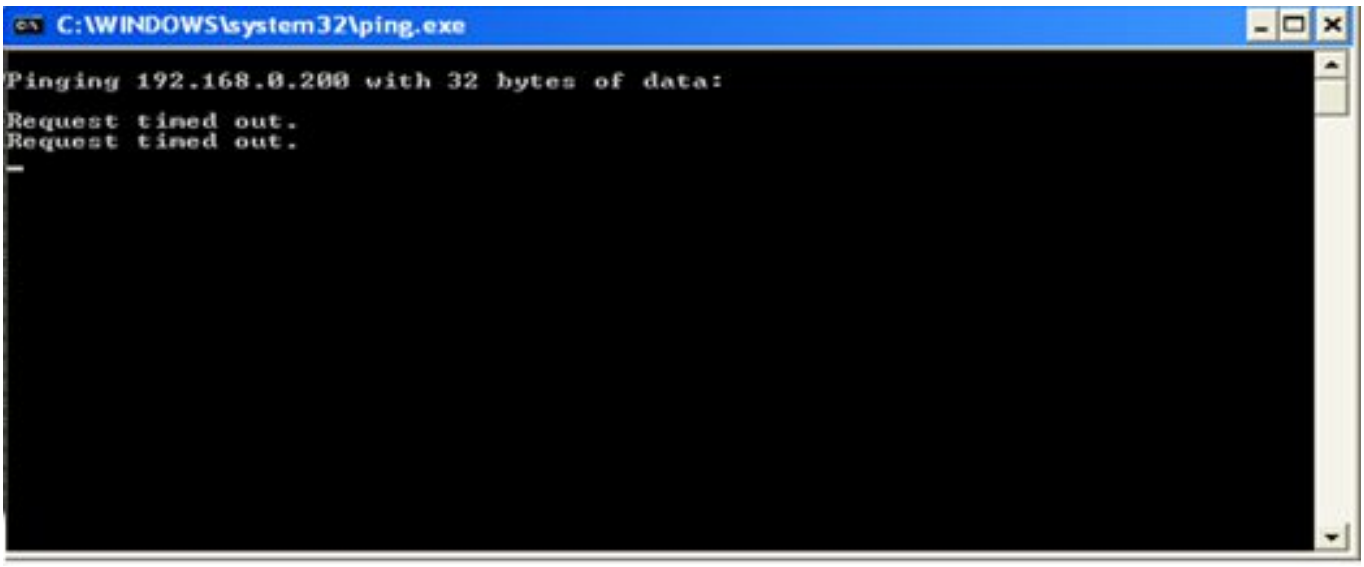
Type “Ping 192.168.0.251 -t”
(The IP Address should reflect that of your Biotrak unit)

Note: - If unsuccessful, either “Destination Host Unreachable” or “Request Timed Out” will be displayed, please follow the above steps carefully and test the connection.
Type “ipconfig” and press 'Enter'.

Successful Connectivity



Unsuccessful connectivity

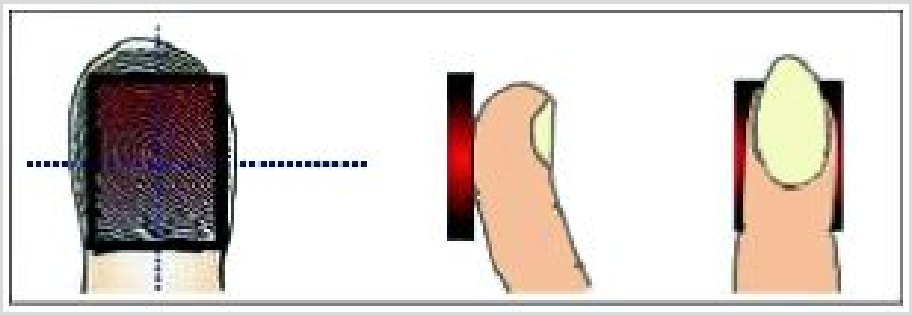


Using Biotrak

The user enrollment process is performed in one of the 'Biotrak' Unit OR through the administrator's computer, and the biometric data is distributed to other readers over the 'Biotrak' Network.

I Proper Finger Presentation.

When it is necessary to place your finger on the fingerprint sensor, gently place the last segment of the finger used during enrollment squarely & firmly on the fingerprint sensor.



II Keep finger on fingerprint sensor until the unit responds in one of the following ways.

If the LED lights up in green, the authentication is successful

LED STATUS	BUZZER STATUS	DESCRIPTION
LED FLASHES RED	SHORT BEEP	USER NOT FOUND
LED FLASHSES GREEN	LONG BEEP	ACCESS GRANTED

Trouble Shooting

No Communication from Biometric Controller to PC

- There are a few points that can be checked to fix it:
- Make sure the network cable is functional; sometimes a damaged cable may be the cause of all problems. To check if it is functional, make sure there are no loose ends and the jack is properly attached to the cable.
- Check that the IP Address Assignment matches the network settings of the corporate LAN or the PC being used.
- Make sure no IP has clashed and that there are no two identical IP addresses in the network.

Fingerprint sensor not activate in Identify mode

- To Enter into Admin Mode refer the manual
- Check for Identification mode by Using Key functions.
- Select an option and press enter to go in Identify menu. In this menu user Can set different types of identify mode like normal mode, identify by key, auto sense etc. by using keys 2-8 select the mode and set press enter to set it.

LCD screen of the Biometric completely blank

- Check whether the power supply is working or not
- The output voltage generated by the power supply is 12V DC. Check this voltage using multi meter if possible
- Check 12V-Gpower connector properly inserted into a socket.

Is it possible to connect two locks or two readers on single connector?

- NO, do not connect 2 locks or 2 readers together on a single connector. A single lock connector can safely drive 600mA current.
- If load current increases beyond 1A, that may cause hardware problems.

"Time out" is displayed after the sensor went on the state of "Light-up".

- The state of your fingerprint is dry. So, the sensor may not scan the image of your fingerprint in time.
- You have to check if the strength of pushing when your finger pressed on the sensor is strong or not.
- You have to keep being proper strength when your finger pressed on the sensor.
- You have to check if your finger departs from the sensor before capturing the image.
- Your fingerprint doesn't have to depart from the sensor before capturing image.

When finger is placed on sensor in display show “User Unauthorized”

- To Enter into Admin Mode & search user finger refer keypad functions.
- If user is added then it will show card no and fingers enrolled.
- The state of your fingerprint is dry. So, the sensor cannot scan the image of your fingerprint in time.
- You have to place your finger squarely and firmly on the sensor for proper scanning of the fingerprint image.

Continues Beep & Door Force Open

- Checkfor lock magnetic contact (MC+/ MC-), it should be short if not in used.(Refer connection Diagram)

Admin User: User/Password Fail

- If the System/Unit is initializing then password will not match. In this case RESET the System i.e. power off and then power on the system then enter Admin Id and password.

Is it possible to connect Biotrak as weigand reader then what will be to step follow-up?

- Enable as weigand out mode by menu System Weigand Out
- Change weigand bit in transparent mode by menu System Weigand Bits
- All changes done by using key function.

WARRANTY CERTIFICATE

Valid in India

We, **SMART-I ELECTRONICS SYSTEMS PVT. LTD**. (herein after referred as "Company"), Hereby gives a warranty for a period of 12 months from the date of purchase to the first purchaser. The warranty assures that the Company will repair or replace, without charges, any part or parts of the product (all hereinafter collectively referred to as the "product") sold and identified by the Company to be defective in material or workmanship under normal use. The Foregoing Warranty is Company's sole and exclusive warranty. The Company makes no other warranties of any kind, either express or implied. This warranty is subject to the following limitations:

Limitations of Warranty

1 This warranty is confined of the first purchaser of the Product only.

2 This warranty does not cover damage(s) caused to the Product by reason of misuse, alteration, normal were and tear, physical damage, accident, any acts of god, erratic power supply or failure to follow instructions issued by the company of proper usage of the product(s).

3 The Company is not liable for any incidental or consequential losses, costs, damages expenses or liability incurred by the customer caused due to fire, intrusion, theft, smoke etc. as a result of any defects in the Product sold or any of its parts requiring field repair, installation, or any other reason. The liability of the Company shall be restricted only to repair or replacement as mentioned above. This warranty assures free repair or replacement only of the defective Product and does not warrant the intended use of the Product.

4 The Company / its authorized representatives reserves the right to either repair or replace the Product at their discretion. If the required repairs can be carried out at the customer's place then the Company's authorized engineer will visit the customer's place and carry out repairs there. However, it the Product requires to be repaired at the Company's premises, then the Company's engineer is authorized to bring back the product or any of its part(s) for repair / replacement at the company's authorized service center.

5 If at any stage it is found that the Product has been unauthorized tampered, in that case this warranty shall lapse immediately and there upon the Company shall stand absolved from all its obligations under this warranty.

6 The Company does not represent that the service it offers and the product it provides may not be compromised or circumvented, and that the product will prevent any personal illness or loss of health by infection, or otherwise, or that the product in any case provides accurate warning or protection. Customer understand and fully aware that a properly installed and maintained electronic screening system may only reduce the risk of infection, illness, or other events which may occur without such systems and screening, but is not an insurance or a guarantee or an assurance of prevention, or any assurance that such a situation will not occur or that there will be no personal illness or loss to health as a result of any such situation.

7 If the customer has defaulted in payments of any of its dues to the Company, then this warranty shall stand suspended till the time the customer clears all his defaults, and such period shall be counted in calculating the total period of warranty. In such circumstances the Company reserves the right to carry out repair / replacement under this warranty at its own discretion.

8 In the event of repairs / replacement of any of the Product or part(s) thereof, this warranty will thereafter continue and remain in force only for the unexpired period of the warranty. Moreover the time taken for repair / replacement and in-transit whether under the warranty or otherwise shall not be excluded from the warranty.

9 The Company is not liable for any delay in servicing due o reasons beyond the control of the Company or any of its Authorized Service Centers.

10 If the Product is given on rent or allowed to be used by any person other than the first customer without the prior written approval of the Company, then this warranty shall not remain in force and shall lapse with immediate effect.

11 If the Product is removed from the place where it was installed by the Company without prior approval of the Company, then the Company shall not be liable to honor this warranty.

12 In case after installation of the Product, the location of the place where the Product is installed is to be changed, then at least one week before the date of change, intimation is to be given to the Company or its Authorized Service Centre so that the warranty obligation for the remaining part of the warranty can be transferred to the new location of the first purchaser. in such a case,

if services of the Company's technicians are required, separate service charged(s) will be levied by the Company depending upon the type and extent of the service(s) required.

13 Damage(s) to the Product or any of its part(s) caused during shifting or transportation is not covered under this warranty, unless such shifting or transportation is done by the Company itself.

14 Although the Company will make every effort to carry out repair / replacement under this warranty as soon as possible, the Company shall not be liable to do so within any specified time.

15 This warranty shall terminate on expiry of the warranty period for which it is given irrespective of whether the Product was in use or not.

16 The Company / its Authorized Service Centres reserves the right to retain any part(s) of Component replaced at its discretion in the event of a defect noticed in the Product during the warranty period.

17 The Company's employees or authorized representatives have no authority to vary any of he terms of this warranty.

18 This Warranty is issued in lieu of all other conditions expressed or implied by law or by any person purposing to act on behalf of the Company and excluded every condition not herein expressly set out19 This Warranty is issued at Mumbai and Courts at Mumbai shall have exclusive jurisdiction on matters covered by or arising out of this warranty. If a customer wants repair / replacement to be carried out to the Product or any of its part(s) etc., under this warranty, he should contact any of the contact details as given below.

20 The Company has currently launched the Product in 67 cities of India as per the list given overleaf. The Company will give warranty support to the customer in the geographical vicinity of these cities only.

Customer:_____ Dealer:_____

Addres:_____
_____
_____

Date of Purchase: ____/ ____/ _____

Product Name: _____ Item Code: _____

Serial No: _____

Franchisee Details

Name: _____ Date: ____/ ____/ _____

Addres:_____
_____
_____

Stamp

List of Cities for company's Warranty Support

1. Agra
2. Ahmedabad
3. Ajmer
4. Akola
5. Allahabad
6. Anand
7. Aurangabad
8. Bangalore
9. Baroda
10 Belgaum1
1. Bhavnagar
12.Bhilai
13.Bhopa
14.Bhubaneshwar /Cuttack
15.Calicut
16.Chandigarh
17.Chennai
18.Coimbatore
19.Delhi /NCRF
20.Durgapur
21.Goa/Punjim & Madgaon only
22.Guwahati
23.Hubli/Dharwad
24.Hydrebad
25.Indore
26.Jabalpur
27.Jaipur
28.Jalandhar
29.Jammu
30.Jodhpur
31.Kanpur
32.Kochi
33.Kolhapur
34.Kolkata
35.Kottayam
36.Lucknow
37.Ludhiana
38.Madurai
39.Mangalore/Udupi
40.Mehsana
41.Mumbai
42.Mysore
43.Nagpur
44.Nasik
45.Navasari
46.Panipat
47.Patiala
48.Patna
49.Pondicherry
50.Pune
51.Raipur
52.Rajkot
53.Ranchi
54.Rourkela
55.Salem
56.Sangli
57.Silliguri
58Sonipat
59.Surat
60.Tatanagar
61.Thrissur
62.Trichy
63.Trivandrum
64.Udaipur
65.Ujjain
66.Vapi
67.Vizag

- The Service Contract option will be extended to these 67 cities only
- The proposed contract is a National Service Contract which can be transferred to any of the 67 cities to which we would cater
- As we go forward we plan to extend it to other locations as well.

Fill in your details and post this portion of the warranty certificate to **"Manager - Service, Smart-i Electronics Systems Pvt. Ltd, Bhumi World, Pimplas, Bhiwandi, Thane, Maharashtra-421302.INDIA"** or hand over to **"SMART-I Representative",** The warranty will not be valid if the following portion is not sent within 15 days of purchase.

Customer:_____ Retailer/DSA/Franchisee:_____

Address:_____

Date of Purchase:_____

Invoice No:_____ Product Name:_____

Model No:_____ Serial No:_____

Contact Person:_____ Phone No:_____

Email ID:_____ Warranty Expiry:_____

Customer Industry Type: (please tick relevant)
Retail / Media Entertainment / Mall & Multiplexes/ Healthcare / IT&ITES
Education / BFSI / Manufacturing / Pharmaceutical / Tourism & Hotel

Environment: (please tick relevant)
Direct Sunlight / Air-Conditioned / Dusty / Humid

All Functions working properly: Yes/No
Whether device/s are connected to UPS: Yes/No

The system has been installed satisfactorily. I have read warranty conditions mentioned above.

Customer Sign:_____ Engineer Sign:_____

Customer Stamp:_____ Dealer/Distributor Stamp/Sign

SMART-I Electronics Systems Pvt. LTd.

smart i™

Smart identification Solutions

Regd Off:

Smart-i Electronics Systems Pvt. Ltd.

Bhumi World, Pimplas, Bhiwandi, Thane, Maharashtra-421302.INDIA

Call: +91-02522-661521/500 or email us at service@smartisystems.com