smart i™
Smart identification Solutions

USER MANUAL
BIOSLIM

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. Contact:- (+91) 7039047042 , (+91) 02522-661518

Web: www.smartisystems.com E-mail: enquiry@smartisystems.com

Preface

Congratulations on purchasing your new ***BIOSLIM*** 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 ***BIOSLIM.*** Because prolonged reliable and trouble-free operation will only be ensured if it is fitted properly. We hope your new ***BIOSLIM*** will bring you lasting safety and effective operations for your employee attendance.

BIOSLIM series are Cost effective ***BIOSLIM*** 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 **'BIOSLIM'** 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 **BIOSLIM** 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 **BIOSLIM** 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

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**

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.
- 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.

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.

Important Instructions

- Take the backup of the finger prints of all the users after enrollment, 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 Bioslim devices.)

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

- Refer the color code on the Reader to connect the external weigand 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.

Get started with Bioslim

Included items:

Product	Image	Qty	Use
Bioslim		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
Bioslim	Access (Lock Voltage)	Universal AC Adapter Isolated i/o	110 to 230 VAC	12 V DC/ 2A (Min)

Specification

Hardware Specification:

Particulars	Description
CPU	32 Bit RISC Arm
Memory	Upto Flash 8 MB
Events/Transactions	1,00,000
No. of templates in sensor	1900/19000
No. of Users	7500
Operation Modes	UID/Card + Finger UID/Card only Card + Finger Card Only UID/CARD+F+ PIN UID /card +pin Card only + pin UID only +pin Finger only Card & finger
Sensor	High Quality Scratch Resistance Optical Sensor.
Communications Port	TCP/IP, weigand, Rs485
Baud Rate	9600bps (Default)
Controller ID	Max 9999
Display	TFT colour display
Keypad	Capacitive Touch sense Keypad
LED	Tricolor LED Bar
Language	English
Power Supply	12 V DC/ 2A (Min)
Enclosure	IP65 ABS Plastic
Color	Silver & Black
Dimension (H X W X D) in mm	(209 x 57 x 47.02)in mm
Mounting	Wall Mounting

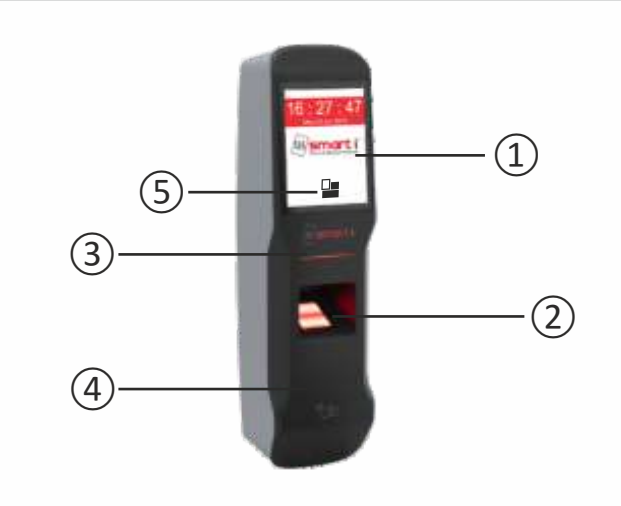
Sensor Specification:

Particulars	Description
Type	Optical
Image Resolution	500 dpi
Enrollment Time	<1 sec
Verification Time	<1 sec
Identification Time	1 sec
Template Size	384 bytes
EER/FAR/FRR	<0.1%/0.001%/0.1%
Image Size (Pixels)	272 X 320
Sensing Area (mm)	16X19

Introduction

The new **BIOSLIM** blends loads of innovative features to streamline installation and administration for small, medium or, large business enterprises for standalone door access control deployment. **BIOSLIM** 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 TFT touch Screen display

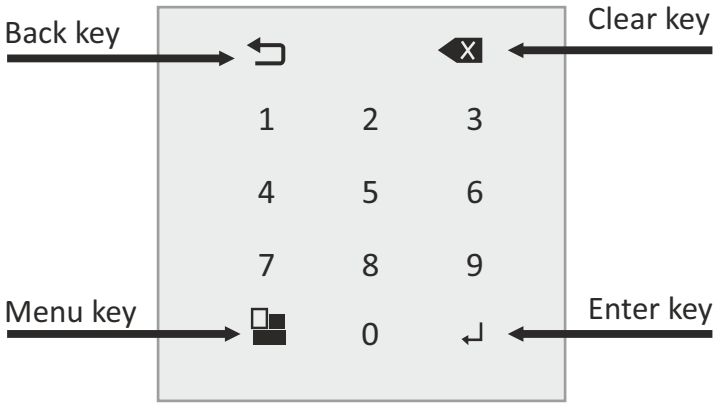
② Biometric Sensor

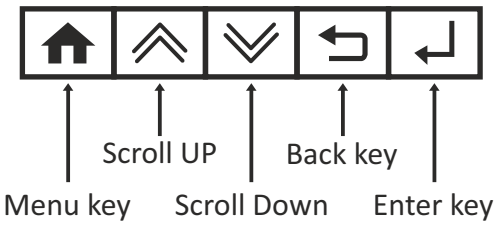
③ Tricolour LED Bar

④ RFID card reader

⑤ Menu Key

Operational keys:



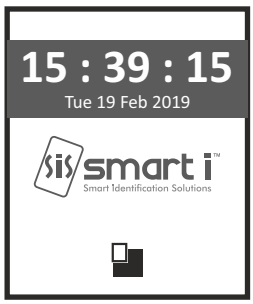


keys	Description
Numeric Keys (0-9)	To access keypad functions& to enter UID for verification
⌃ ⌄	Scroll keys to select menu after admin login.
⮌	Back key to go back on previous screen
⌂	To go to the home screen
↵	Entering into menu parameter and set the values for parameter

How to Use:

Step 1.: Enrollment Process

1. Do Admin login



i Press on menu key

ii Enter admin id >> 11111(Default admin id) > press Enter .

iii Enter password >>12345(Default password) > press Enter .

2. ADD User

After Admin Login Success

I. Press on USER icon

ii. Add User by Showing card on reader or Enter UID > Enter >

iii. Add Finger 1 (across UID)> Press Yes>(Place Finger Twice)

iv. Add Finger 2 > Press YES or NO > Enter >

v. Logout

Step 2.: Verification Process

i. Show Card / Enter UID and Place finger

ii. For Authorized Swipe, authorized message will be displayed along with logo and long Beep and Led will turn Green

iii. For Unauthorized Swipe, User authorized message will be displayed along with logo and two buzzer beep and Led will turn Red.

Power OFF >ON and check point (i) again.

Step 1.: Enrollment Process

1. Press on Network icon

2. Select Network Setting > Enter

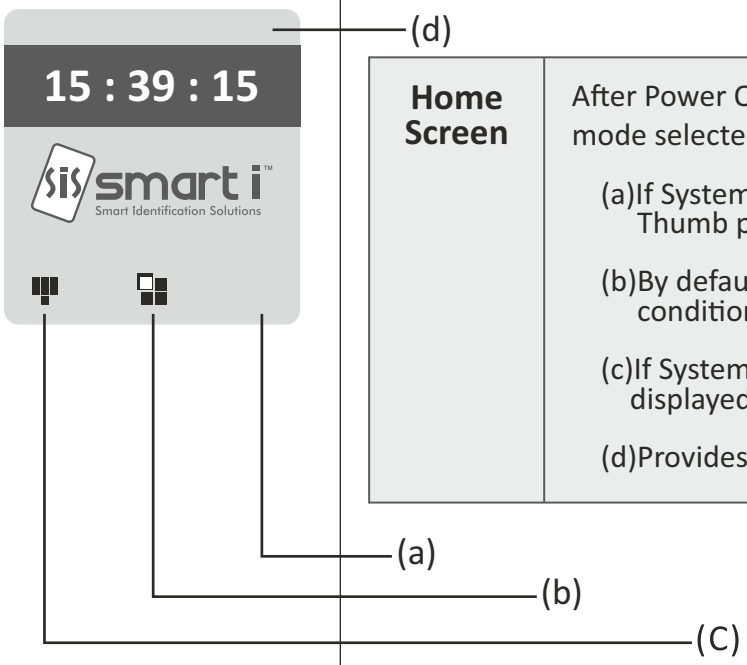
3. In this menu user can edit the various parameters such as, unit IP address, subnet mask, default gateway, server IP address .....etc.

   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

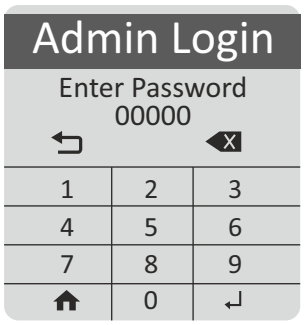
4. Enter>> Reset the Device.

HOME SCREEN



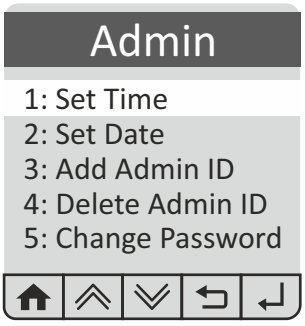
Home Screen	After Power ON , these screen will be displayed as per mode selected (a)If System>>Sensor>>Identify mode>> Enable> Thumb print symbol will be Displayed (b)By default only Home key is displayed in normal condition (c)If System>>Allow UID by Key >> Enable> Fig C will be displayed (d)Provides information of LAN connectivity

LOGIN SCREEN



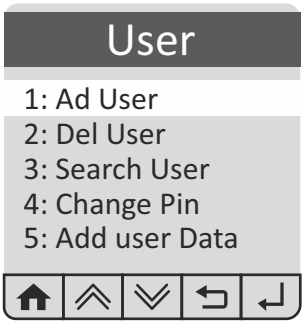
Login Screen	On pressing home key, Login screen will be displayed. Enter Admin ID .: 11111 and Press Enter. Then enter Password .: 12345

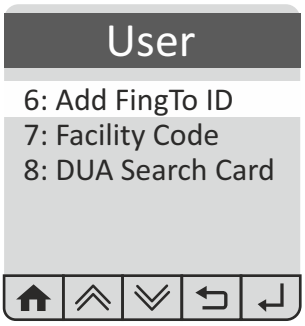
ADMIN



ADMIN		
1. Set Time	Select option press enter key	1)Will allow to set Time as require i. hh:mm:ss ii. hh:mm 2)Try to set invalid TIME> It will not allow to set
2. Set Date	Select option press enter key	1)Will allow to set Time as require 2)Try to set invalid DATE> It will not allow to set
3. Add Admin ID	1) Select option press Enter key 2) Add Admin ID & Password 3) Try to Add more than its capacity.	1)Admin ID should get added properly 2)Should Memory Full message if buffer is full.
4. Delete Admin ID	1) Select option press Enter key 2) Enter Admin ID & Password 3) Try to Delete un added admin ID.	1)Admin ID should get deleted and should get logged in. 2)It Should show user search fail.
5. Change Password		System should ask for old and new password

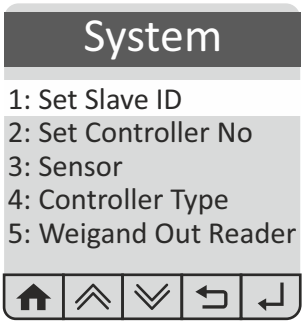
USER





USER		
1. Add User	1)Enter User ID & presenter. It will ask for finger 2)If finger is already added>Display finger exist. 3)Make card memory full & then add the card.	1) User to get added properly with proper Pin number and finger. 2) ON memory full it should show "memory full" message
2. Del User	1)Enter user ID to delete press enter. 2)Try to delete unadded UID.	1) User should get deleted proper along with finger 2) "User Not Found" message should be displayed for deleting Unadded UID.
3. Search User	1)Search added card 2)Search unadded card	1) Will show card number and Pin of that card 2) It will show "User Search Fail" for unadded card
4. Change Pin	1)Enter UID press# 2)Enter OLD PIN press# 3)Enter NEW PIN Press enter	properly Pin should be shown 1) Pin should get change properly 2) After searching that same card,
5. Add User Data	1)Enter UID press# 2)Select option from UID/Card + Finger UID/Card only Card + Finger Card Only UID/CARD+F+ PIN UID /card +pin Card only + pin UID only + pin Finger only Card & finger	Should work as per function mention 1.UID/Card + Finger 2.UID/Card only 3.Card+Finger 4.Card Only 5.UID/CARD+F+ PIN.: If finger is place it ask for pin and access 6.UID /card +pin 7. Card only +pin 8.UID only +pin 9.Finger only 10.Card & finger : both are compulsory
6. AddFing To ID	1)Enter UID press enter 2)Place finger on sensor	proper Finger should get added and score should be shown
7. Facility Code	1)Facility En/DI 2)Show card or enter UID 3)Update facility code	Proper Facility code should be shown according to card digit.
8.DUA Search Card	1)Show Card/ Enter UID 2)Enter 0/1 EN/DI Duress 3)If **Dual authentication** is ON I. Enter card number ii. Select Admin Type iii. Enter Group NO. iv. Duress Check	If Duress is ON across any UID then Duress event is generated and access is granted **Refer Annexure C**

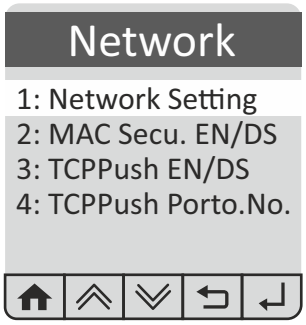
SYSTEM



SYSTEM		
1. Set Slave ID	1) Enter Slave No from 1 to 128.	Proper Slave ID should be set with "slave ID Updated" message
2: Set Controller No	1) Controller Number from 0 to9999	Proper controller number should beset with "controller number Updated" message
3.Sensor 3.1 Sensor Security Level	1) On selecting this option will see 12 different levels. 2) Select any one out of 12 levels.	Level should get set proper as per requirement **Refer Annexure A**
3.2. Identity Mode	1) On selecting this option will see 3 different option 1=Normal 2=Identify by Key 3=Auto Identify	1=Show card sensor will get enable 2=Press ((O)) key Sensor will get enable 3=Sensor will be ON continuously
3.3.Set Finger DB verify		
4. Controller Type	1) Select any one out of 11 option 1=Bio Access 2=Bio Access 2RD 3=Bio Attn 4=Bio Att 2rd 5=Bio Attn No chk 6=Bio Att No chk2rd 7=Bio Att SCNO chk 8=Bio Attn NO Chk3RD 9=Deny List 10=Bio no Chk 11=Deny list bio no chk	controller should set properly and should function accordingly. 1=Bio access= Relay trigger()single reader 2=Bio Access 2RD= 3=Bio Attn= relay won't trigger 4=Bio Att 2rd 5=Bio Attn No chk=don't Checkholidays 6=Deny List=Access transaction

5. Weigand Bits	**1) Select any one option out of 7option 1=Weigand 26 2=Weigand 32 3=Weigand 34 4=Weigand 26 or card 5=Weigand 32 orcard6=Weigand 26 or transparent 7=Weigand 32 or transparent**	**This applicable only in weigand out. The bit will send to controller according bit set.**
6.Displayi. Disp Brightness	To vary the brightness level from zero to 10	To set display brightness Min value - 0Max value - 10
ii. Disp. Sleep EN/DI	1.Enable 2.Disable	Given to enable/disable auto display sleep (i.e. brightness level set to 0) after settable time in sec.
iii. Set Disp Sleep Time	After Setting the Time the display brightness will change to Zero	Display will get to brightness level 0 And after single touch on display or Card swipe or finger swipe the brightness of display will get to its set value
iv. Card Digit Display	1) Select any one out of 3 option 5Digit / 8Digit / 10Digit	Card Number will be displayed accordingly for 5, 8 or 10 digit.
v. Display User Name Type	1) Select any one out of 3 option a. UID only b. Name only c. UID and Name	On showing card, Card details will be displayed as per selection.
7.Allow UID by Key	1.Enable 2.Disable	If Enable then Menu will be displayed on Home screen.
8.Sound EN/DIS	1.Sound VID/IVID 2.Keypress 3.USER Error 4.All Sound	1.Only sound of authorised and unauthorized user will be played. 2.Only sound of keypad will be played 3.Only for any error sound will be played 4.All Sound EN 5.All Sound DIS
9.Dual auth EN/DI	Enable / Disable option for Dual authentication	To Use the system in dual auth mode enable dual auth and configure using **dua search card option.**

NETWORK



NETWORK		
1. Network Setting	**1) Select accordingly to make changes i. Ip address ii. Subnet mask iii. Gateway iv. Local server port no. v. Push Server IP vi.Push Server Port**	**All network should get set properly check after off/on unit. Refer Annexure B**
2.Mac Secu. EN/DS	Enable MAC Security	Only Device with set MAC address can download the transaction.
3.TCP Push EN/DIS	Enable MAC Security	Enable TCP push to download transaction on register ip address
4.TCP Push Protocal number		As per selection transaction will be pushed and Del.

DOOR

DOOR		
1. Door Open Time	1)Set Door Open time. By default will set to 5sec	We can enter the desire door open time and it shows saved message
2. Shared DOTL	1)En/Dis Share DOTL Reader no:1 ReaderNO:2 Reader no: All	**By Default Shared DOTL is not in used**
3. Reader In/Out	1)Reader Normal 1=Reader In 2=Reader Out 3=Reader IN/ OUTToggle 4=Scheduled INOUT 5=As weigand out	1.Reader Works as Normal 2.For reader in or reader out we require 2 different controller. 3.Reader IN/OUT N.A. 4.Schedule reader 5.As weigand
4. Fire TAMPER EnDS	1)Disable All 2)Enable Fire 3) Enable Tamper 4)En Fire Tamper 5)En Intrusion 6)En Fire Intrusion 7)En Intrusion, Tamper	5) En Intrusion =NA 6) En Fire Intrusion =NA 7) En Intrusion, Tamper =NA
5. Set APB En/DiS	1) Set APB En/Dis	Anti pass back will be enable.

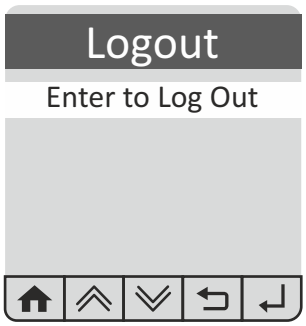
TROUBLE SHOOT

TROUBLESHOOT		
1. Initialize System	00 Delete all data 01 Delete Transaction 02Delete All Users 03Set All Default 04Delete Sys. Info 05Delete Time Zone 06Delete Holiday 07Delete Facility Code 08Delete Door info 09Delete Admin Ids 10Reset System 11Delete Cards Only 12Delete all fingers 13Delete all expt N/W 14Initialize Update	Should have show all message properly on display.
2. Weigand Display	Select option Press enter key	It shows Reader No, Weigand Bits of particular card
3. Network Test	1) Gateway/LAN Test 2) Internet Test	Check the device is connected to network or not

DEVICE INFO

DEVICE INFO		
Display All Parameter		Shows All parameter related to system.
Disp Useful Parameter	Model Number Unit ID Controller No Card Buffer Used Card Buffer Bal. Card Buffer Trans Buffer Used Trans Buff Bal. Trans Buff Templates supp. Used Templates Bal. Template Serial No Manufacturing Date FW Compile Date Firmware Version Hardware Version Controller Type Reader Type MAC address	It shows Reader No, Weigand Bits of particular card

LOGOUT



LOGOUT	Press enter	after pressing enter system should log out

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**

(NOTE: The values of FAR in Security level are suggested by Suprema)

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 Login → Press Home key → Enter Admin ID " 11111" → Press Enter → Password "12345" → Press Enter.

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

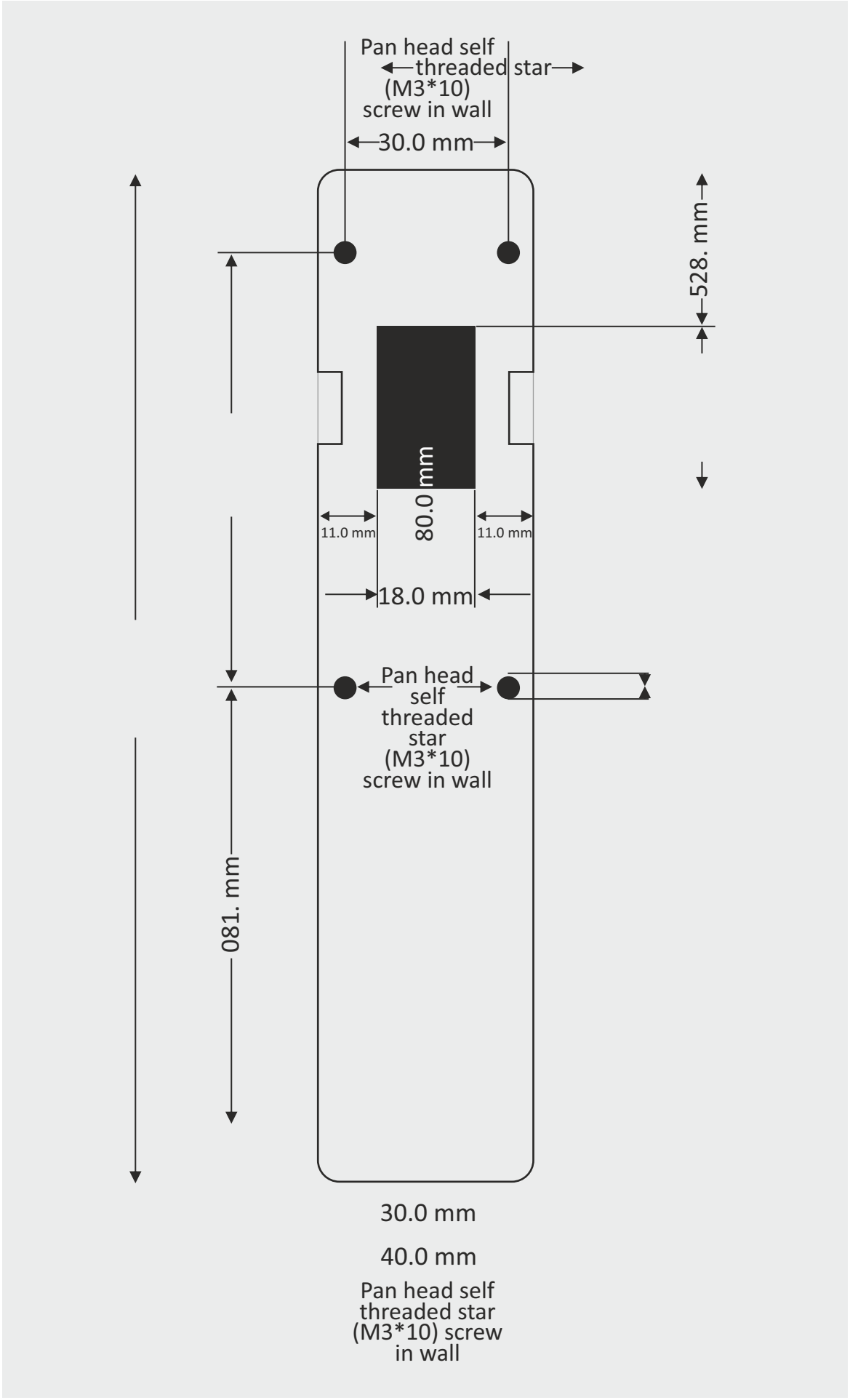
3) Repeat Step no.2 for Number of Users to added in Unit.

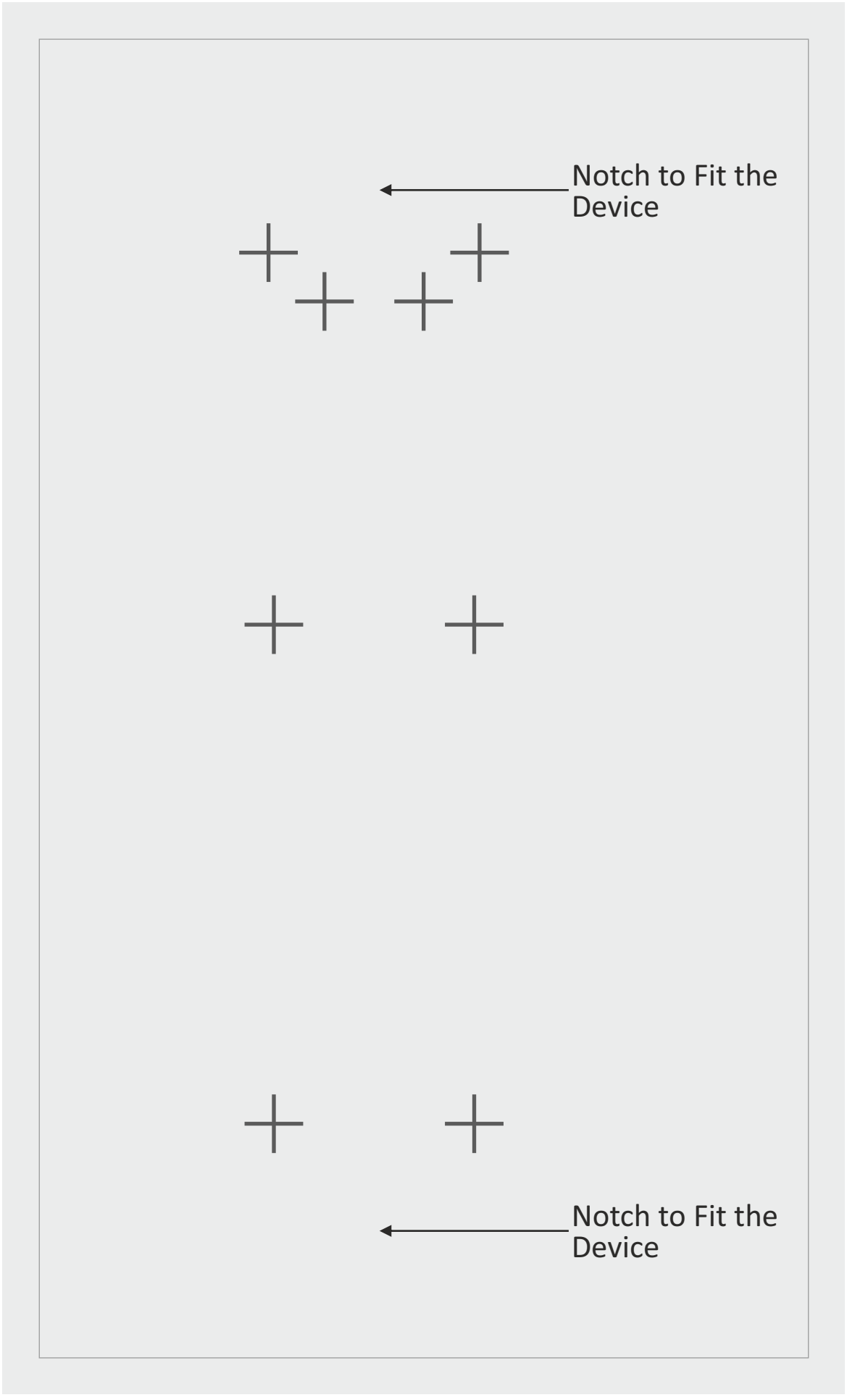
4) Now to config dual user go in User menu & select „DUA Search Card".
Show card or enter UID → Press Enter.(Make sure Dual authentication is ON)

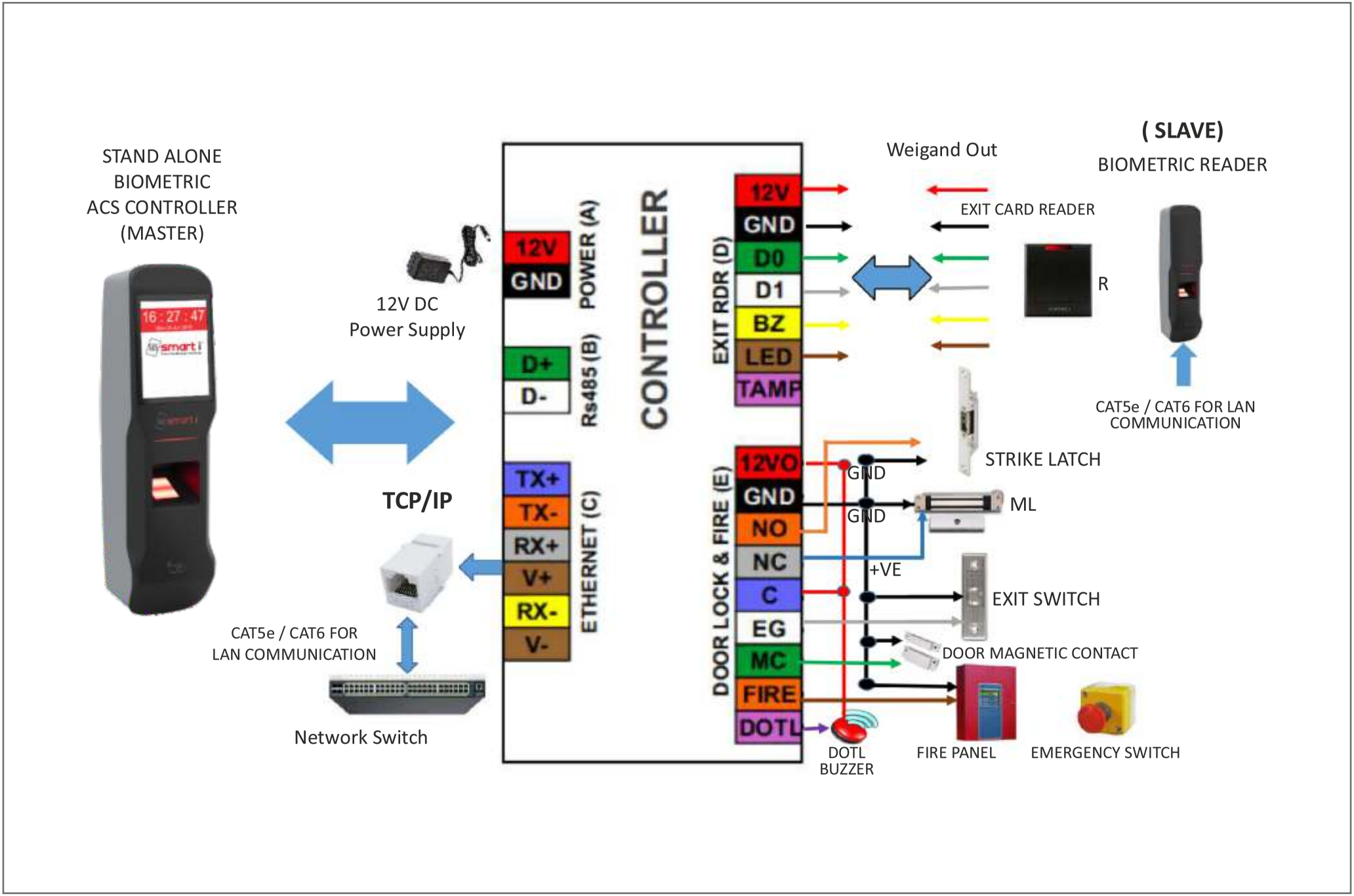
5) Now enter 01 for Master & 00 for normal user. Press Enter. Assign Group no. Press Enter.

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

Mounting Plate Details




Notch to Fit the Device
Notch to Fit the Device


STAND ALONE
BIOMETRIC
ACS CONTROLLER
(MASTER)
12V DC
Power Supply
TCP/IP
CAT5e / CAT6 FOR
LAN COMMUNICATION
Network Switch
CONTROLLER
POWER (A)
12V
GND
Rs485 (B)
D+
D-
ETHERNET (C)
TX+
TX-
RX+
V+
RX-
V-
EXIT RDR (D)
12V
GND
D0
D1
BZ
LED
TAMP
DOOR LOCK & FIRE (E)
12VO
GND
NO
NC
C
EG
MC
FIRE
DOTL
Weigand Out
EXIT CARD READER
R
(SLAVE)
BIOMETRIC READER
CAT5e / CAT6 FOR LAN
COMMUNICATION
STRIKE LATCH
GND
GND
ML
+VE
EXIT SWITCH
DOOR MAGNETIC CONTACT
DOTL
BUZZER
FIRE PANEL
EMERGENCY SWITCH

Bioslim Connector WIRE details

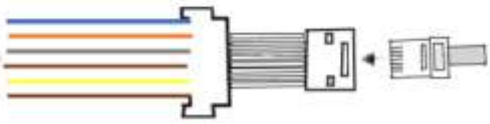
A Power

PIN	PIN DESCRIPTION	WIRE
1	POWER + (12Vdc)	RED
2	POWER -	BLACK

B Rs485

PIN	PIN DESCRIPTION	WIRE
1	D+	GREEN
2	D-	WHITE

C Ethernet

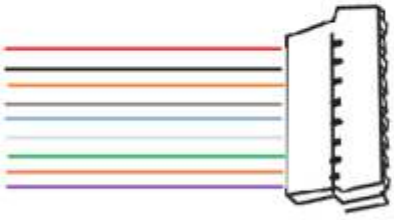


PIN	PIN DESCRIPTION	WIRE
1	TX+	BLUE
2	TX-	ORANGE
3	RX+	GREY
4	V+	BROWN
5	R-	YELLOW
6	V-	BROWN

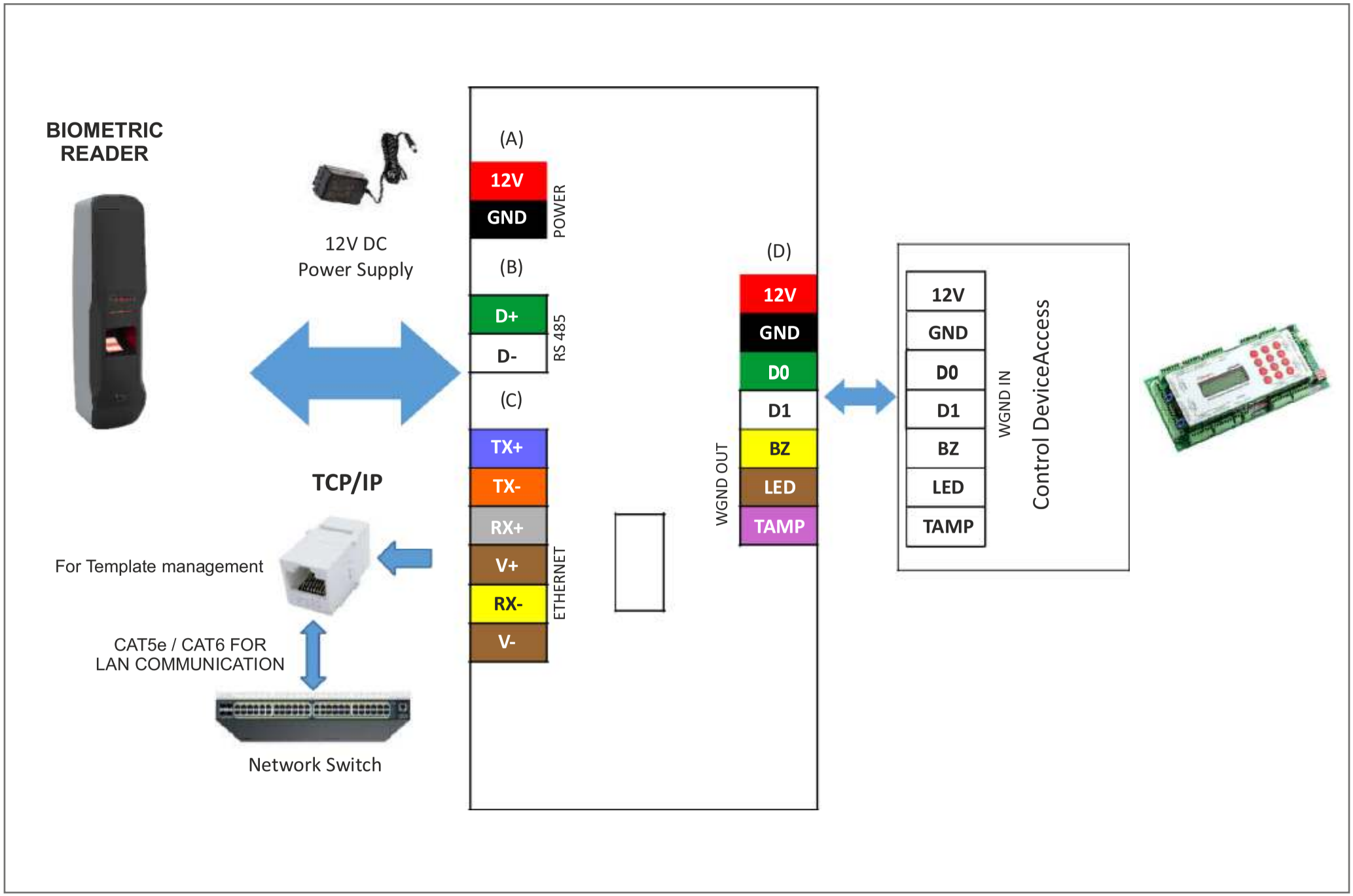
D Exit Reader

PIN	PIN DESCRIPTION	WIRE
1	12V	RED
2	GND	BLACK
3	DO	GREEN
4	D1	WHITE
5	BUZZER	YELLOW
6	LED	BROWN
7	TAMP	VOILET

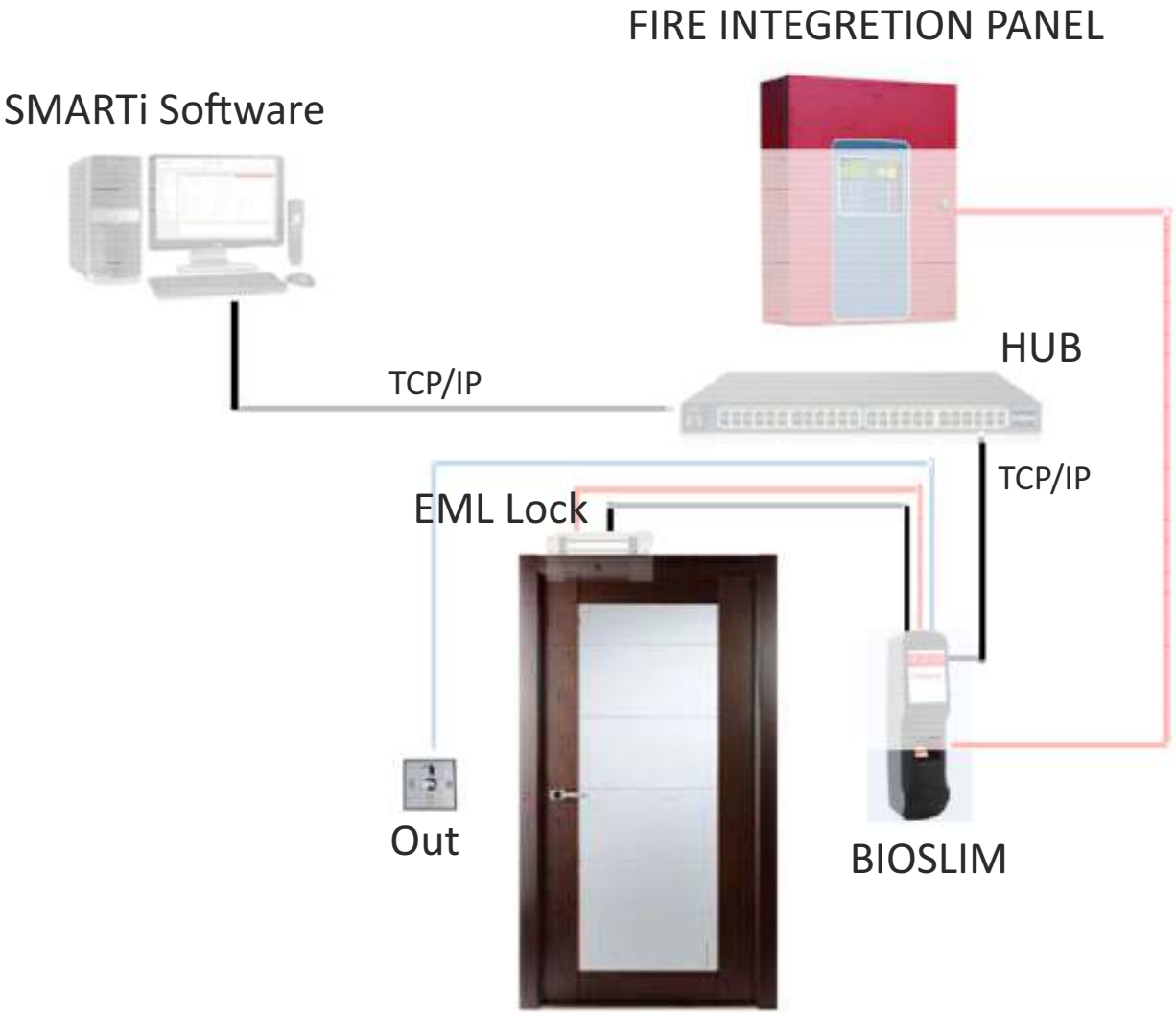
E Door & Lock



PIN	PIN DESCRIPTION	WIRE
1	12V	RED
2	GND	BLACK
3	NO	ORANGE
4	NC	GREY
5	C	BLUE
6	EG	WHITE
7	MC	GREEN
8	FIRE	ORANGE
9	DOTL	VOILET


BIOMETRIC READER
12V DC Power Supply
(A)
12V
GND
POWER
(B)
D+
D-
RS 485
(C)
TX+
TX-
RX+
V+
RX-
V-
ETHERNET
(D)
12V
GND
D0
D1
BZ
LED
TAMP
WGND OUT
12V
GND
D0
D1
BZ
LED
TAMP
WGND IN
Control DeviceAccess
TCP/IP
For Template management
CAT5e / CAT6 FOR LAN COMMUNICATION
Network Switch

STANDALONE BIOSLIM CONFIGURATION

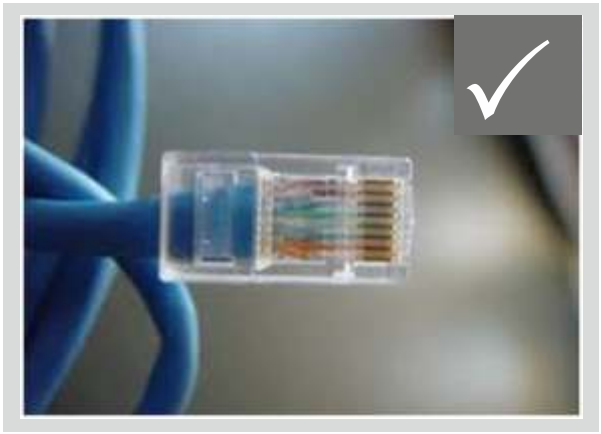


Connecting To Host Computer

The Bioslim 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 Bioslim 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

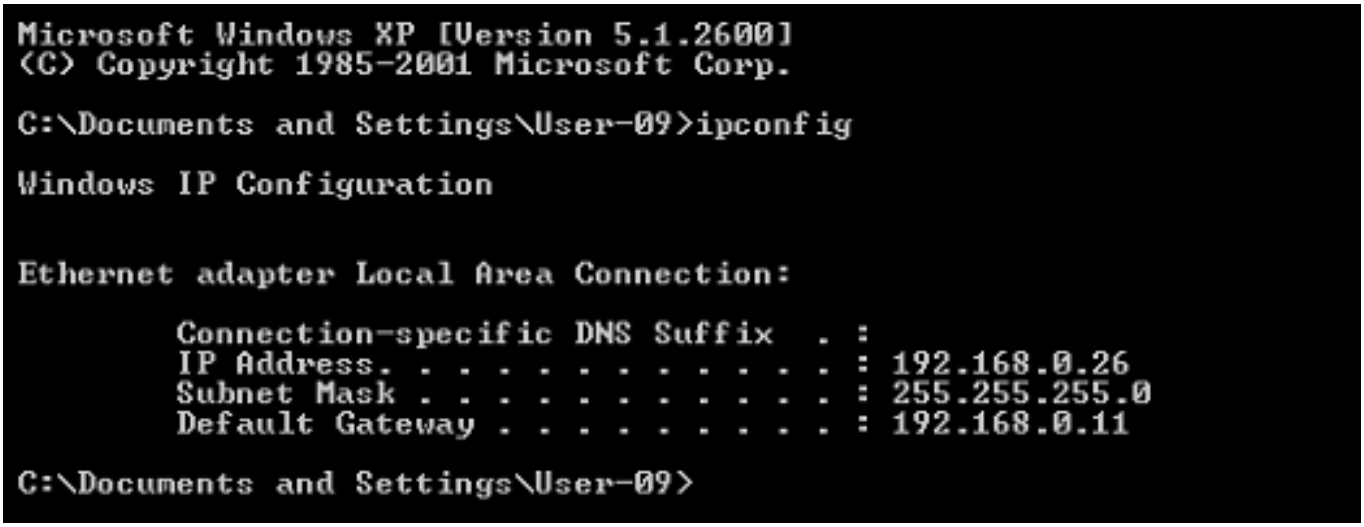
To check your PC's IP Address Settings, find out the IP address of the network. To do so, go to a PC in the network presently, press Start -> Run -> Type “command” and click on 'OK'.

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

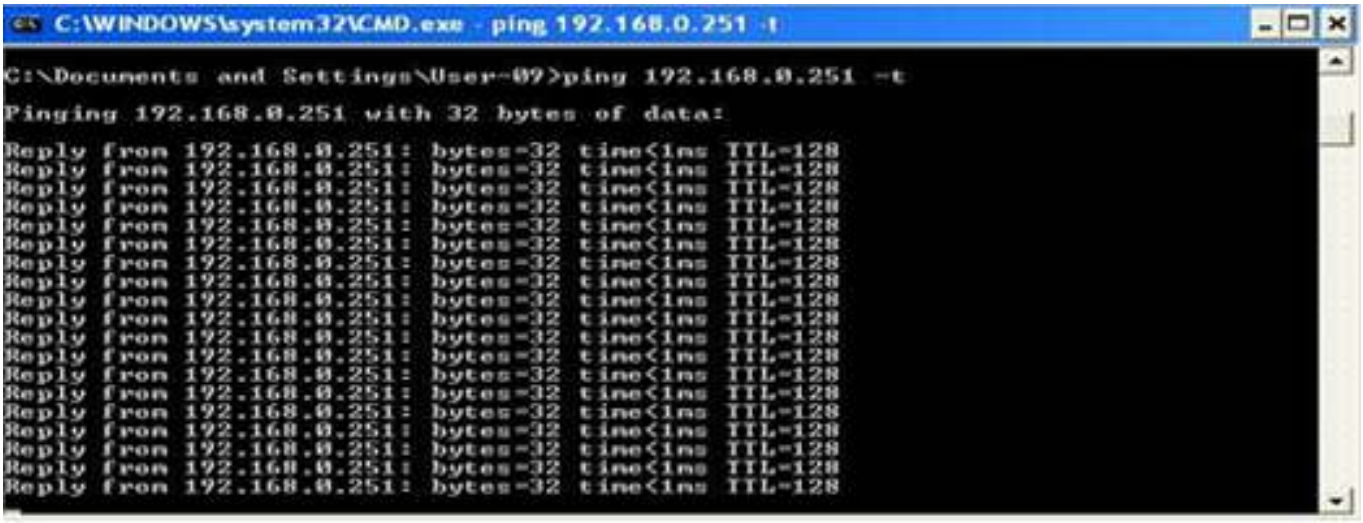
At the PC, Click Start -> Run -> Type “command” and press 'OK'.

Step 2

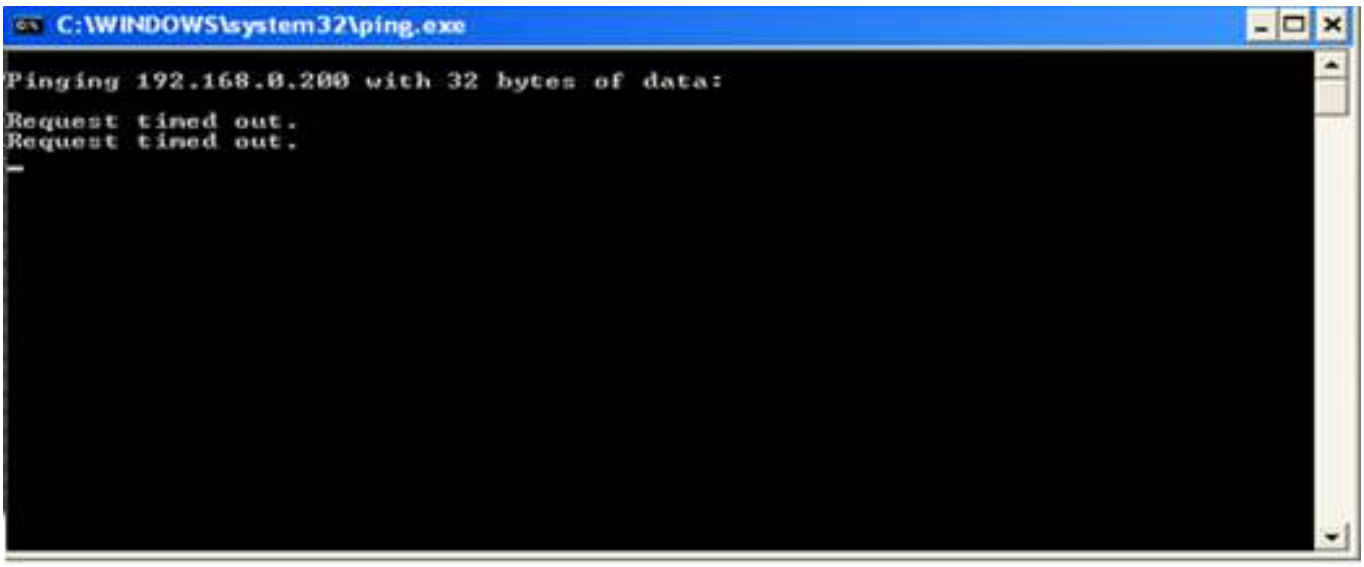
Type “Ping 192.168.0.251 -t”
(The IP Address should reflect that of your Biotrak unit)

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

Successful Connectivity



Unsuccessful connectivity



Testing the Connection

To test the connection following is the under mentioned steps

Step 1

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

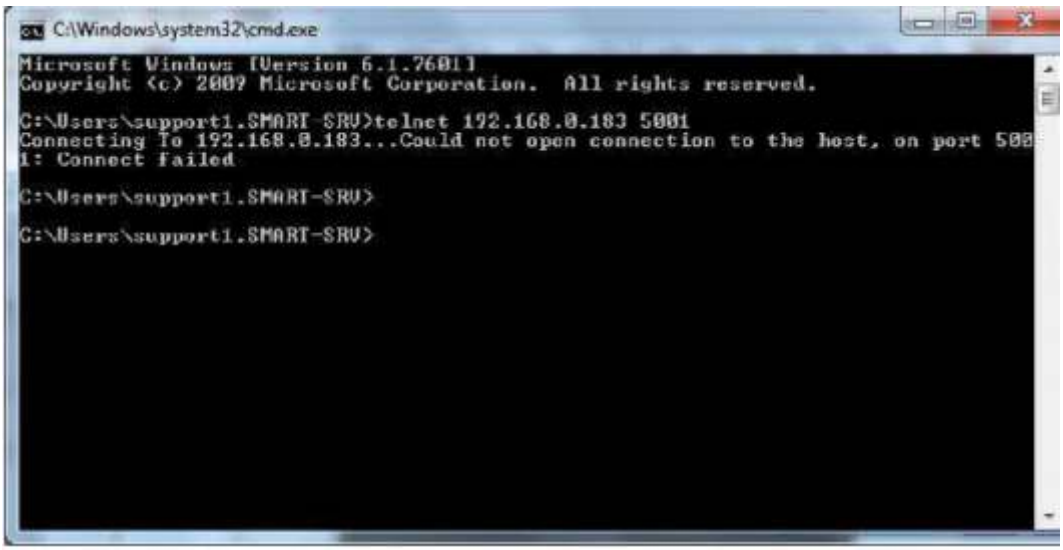
Step 2

Type “telnet ipaddress port"
(The IP Address should reflect that of your Bioslim unit)

Note: - If unsuccessful, either “Connect failed will be displayed, please follow the above steps carefully and test the connection.

Successful Connectivity

Unsuccessful connectivity

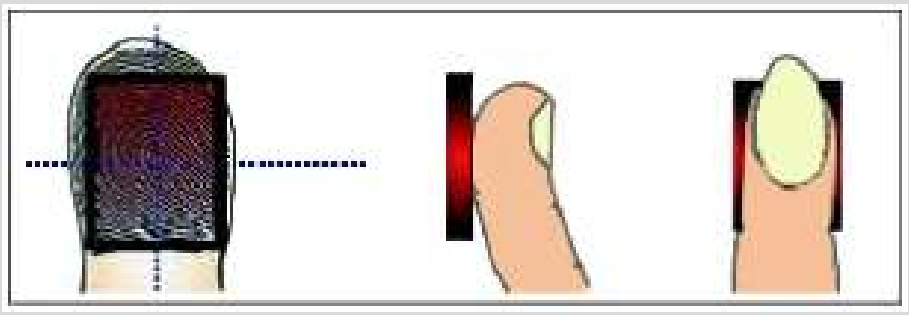


Using Biotrak

The user enrollment process is performed in one of the **'Bioslim'** Unit OR through the administrator's computer, and the biometric data is distributed to other readers over the **'Bioslim'** 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 Bioslim as weigand reader then what will be to step follow-up?

- No Not possible to connect Bioslim as weigand reader on Site

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