USER MANUAL

NGBIOLITE

SMART-IELECTRONICS SYSTEMS PVT. LTD.(An ISO 9001:2008 certified company)
Corporate Office: A-308, Puranik Capital, Ghodbander Road, Opp hypercity, KasarVadavali, Thane (W) 400607

R&D, Training & Customer Support Center:
First Floor, Arihant Plaza Phase II, Village-Ovala, Ghodbander Road, Thane (W) 400607
Tel: + 91-22-6566 6555
Web site: www.smartisystems.com

PRESENCE : MUMBAI - DELHI - BANGALORE – KOLKATA - CHENNAI - AHMEDABAD – PUNE - HYDERABAD

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

- Ø Please handle the equipment with care. Physical Damage to the system is not covered under warranty.
- Ø Do not power on the system without reading this manual. Ensure proper power supply with Earthing.
- Ø Note down the serial number and model no. of the device for future reference and quote in all support and service requests.
- Ø To connect or interface the Card reader to the 'NG Bio-lite' unit please refer to the Hardware Installation Guide or Manual and carefully follow the instructions. A trained technician must make the connections.
- Ø Any negligence on your part may damage the Card reader interface on the NG Bio-lite terminal.
- Ø 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.
- Ø The fingerprint sensor glass may periodically require cleaning - use suitable glass cleaner.
- Ø Do not use this unit near water.
- Ø 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.
- Ø When connecting up the NG Bio-lite 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 the SmartEngine (Refer User Manual of SmartEngine for taking finger prints backup and uploading the backup finger prints back to the NG Biolite 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 NG biolite

Included items:

Product	Image	Qty	Use
NG Biolite		1	Attendance System
Power Supply		1	Supplying power forthe 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
NG Biolite	Attendance &Access (Lock Voltage)	Universal AC Adapter Isolated i/o	110 to 230 VAC	12 V DC/ 2A (Min)

Introduction

The new **NG BIOLITE** blends loads of innovative features to streamline installation and administration for small, medium or, large business enterprises for standalone door access control deployment. **NG BIOLITE** 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

①LCD→Graphical LCD

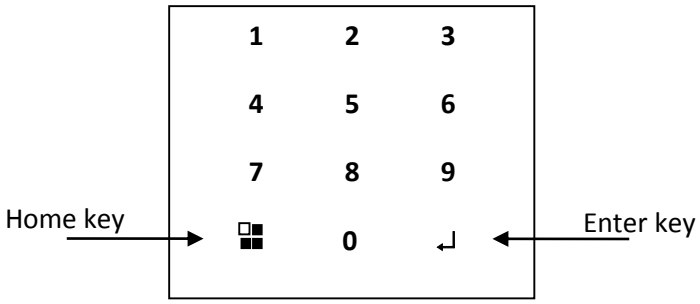
②Keypad→Capacitive Touch Keypad

③Bio sensor →Optical sensor

④LED→Tricolor LED Bar

⑤RFID 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:

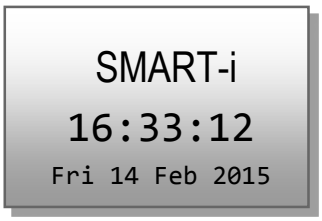
Particulars	Description
CPU	32 Bit RISC Arm
Memory	Upto Flash 8 MB
Events/Transactions	1,00,000
No. of templates in sensor	19000
No. of Users	75000
Operation Modes	Card Only, UID + Finger, Card + Finger, Finger Only, UID only
Sensor	High Quality Scratch Resistance Optical Sensor.
Communications Port	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 x 105 x 45
Mounting	Wall Mounting

Sensor specification:

Particulars	Description
Type	Optical
Image Resolution	500 dpi
Enrollment Time	<1 sec
Verification Time	<1sec
Authentication / Identification	1:1& 1:N (User Groups facility for faster verification)
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)	16 X 19

Keypad Function Details

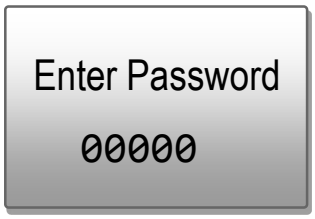
Home screen



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

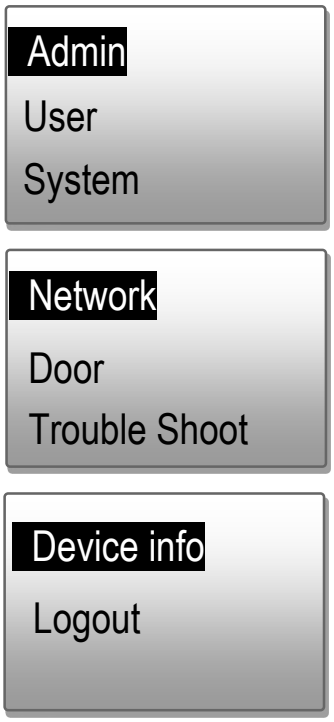
Login Screen

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



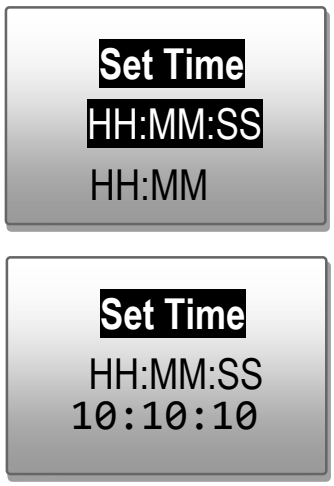
If admin ID & password is right then you get menu screen.

Admin

This mode is used to set time and date, add/del/change admin users and to change its password.

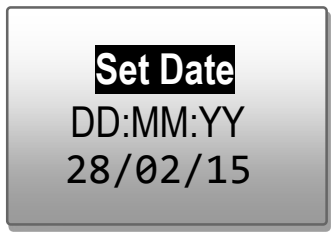
Select Admin by moving cursor using keys 2 & 8.Then press enter key.

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

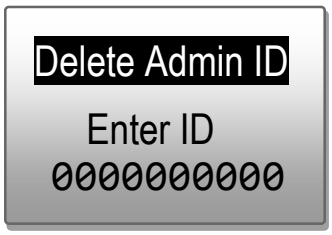


User can edit the date according to his requirement using keypad. After editing the date press enter to set it successfully.

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.

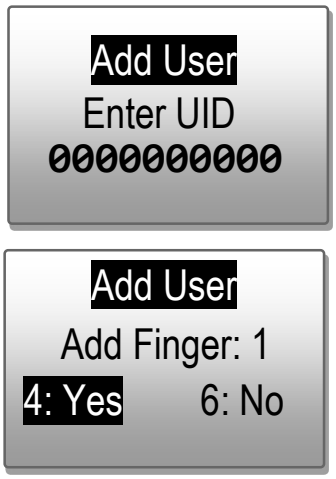
Change Password

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 finger 1with sensor ON. After finger gets added it shows score of finger & 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.

Note: Per user you can add 8 fingers only.

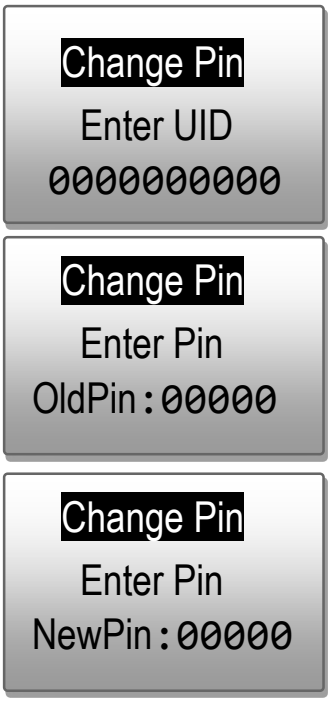
Delete User

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

Search User

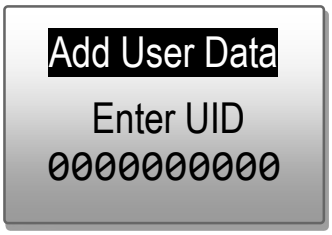
In this menu enter the UID or shows card and press enter to displays card pin and enrolled fingers no.

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



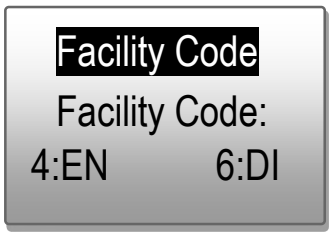
In this menu, Enter the UID or show card for which you want to add the data and press enter.
And select the following card types according to user:
UID/Card + F
UID/Card Only
Card + Finger
Card Only
Key/Card + Pin
And press enter to set it successfully.

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.

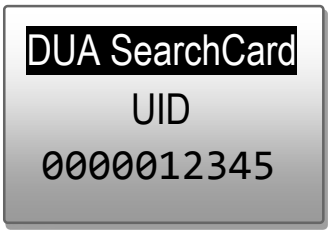
Note: Only added user can enroll finger by this menu.

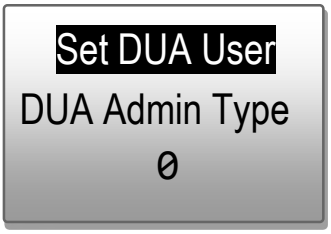
Facility Code

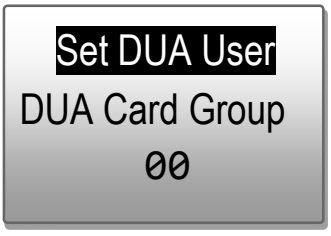


By using the keys 4 and 6 user can enable and disable the facility code. After enabling the facility code it will ask for the location, set the location & press enter then show card to get facility code from that card and after getting facility code press enter.
You can set 8 different facility codes.

Set DUA user

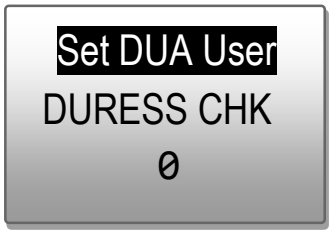




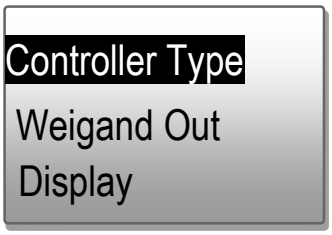
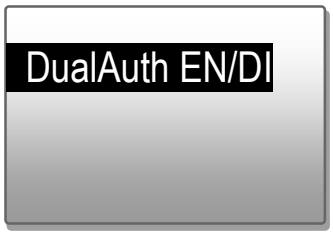


To set dual authetication as per user enter in this menu. Enter UID or shows card & press enter key. Then enter master type & then select group. If you want duress check for perticuler user then enter 1 to enable duress for that card.

Please refer annexure C.

System

  	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.

Set Slave ID

	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.

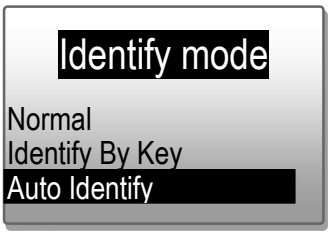
Set Controller ID

	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

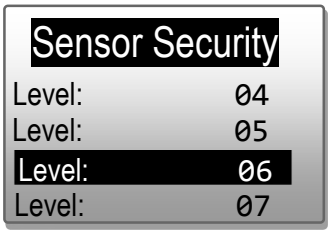
From this menu you can set sensor mode, security levels.

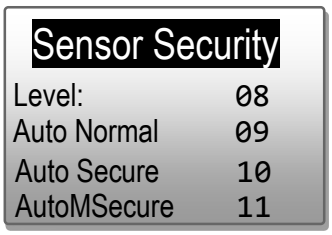
Identify Mode



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.

Sensor Security



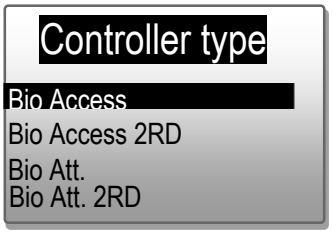


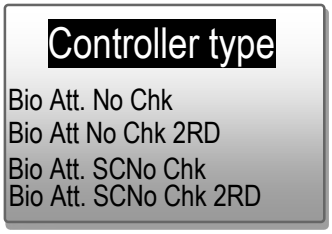
In this menu security level specifies the false acceptance ratio.
User can set sensor security according to the level defined in menu. Max 12 levels are specified but the Default level is 6. Using keys 2-8 select the level and press enter to set it.
Refer annexure B.

Verify Finger DB EN/DI

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





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.

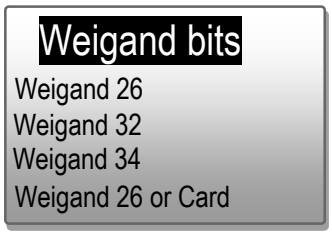
Weigand Out Reader

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

Set Weigand Out

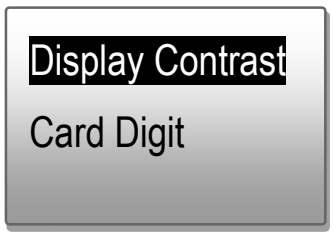
To enable weigand reader mode press 4 to disable & press 6.

Weigand Bits

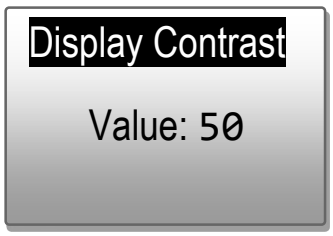


In this menu, user can select the six different type of weigand formats. Select itand press enter to set it. Default is 32 or transparent.

Display

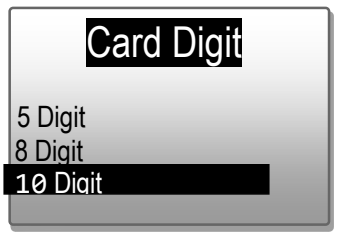


Display Contrast



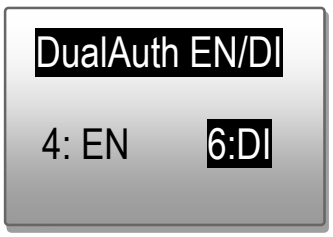
In this menu you can set display contrast as per your requiment.

Card Digit



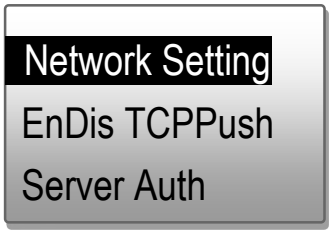
In this menu, user can set the three types of card digit display. We can set it as 5-digit,8-digit,10-digit depending upon the user requirement. User can select it using 2 & 8 keys and press enter to set it successfully.

Dual Auth EN/DI



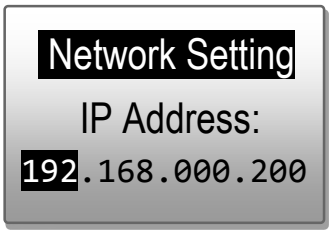
To enable dual user authentication.
Press 4 to enable & press 6 to disable this functionality.

Network



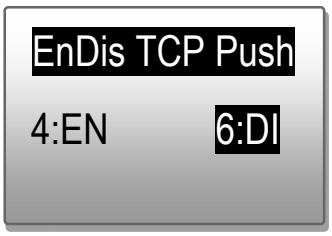
In this mode we can change the network setting according to user network settings. We can also disable and enable the MAC security to secure download the transaction.

Network Setting



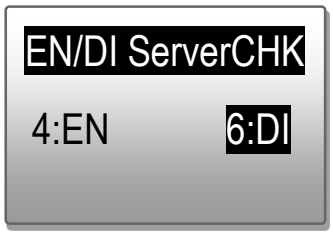
In this menu user can edit the various parameters such as, unit IP address, subnet mask, default gateway, server IP address …..etc.
User have to set various parameters such as,
IP Address
Subnet mask
Gateway
Server IP Address
Local port No
Push Server1 IP
Push Server1 Port
Push Server2 IP
Push Server2 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.

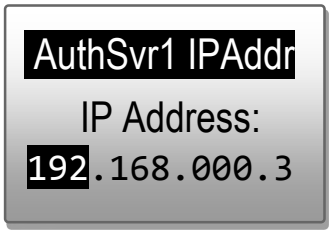
EnDis TCP Push

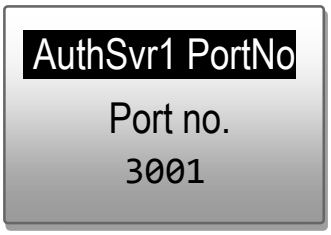


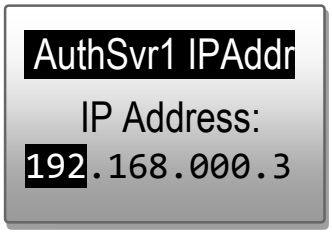
To enable TCP push functionality. For TCP push works need to set server IP address & port no by Network setting menu.

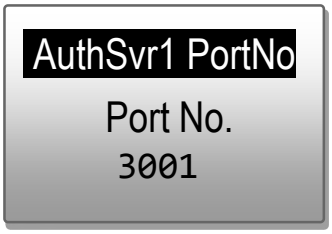
Server Authentication











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.

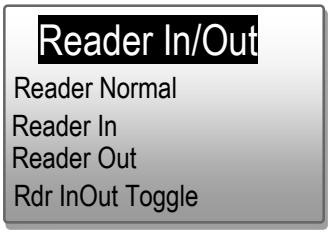
Door

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

Door Open Time

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.

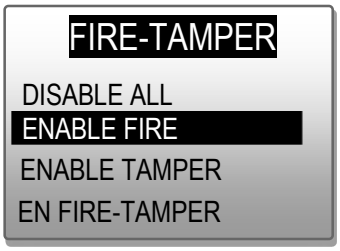
Reader IN/OUT



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

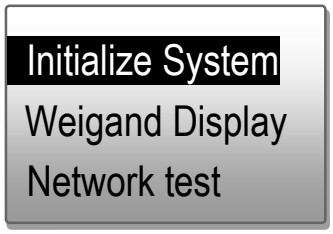
i. Reader normal
ii. Reader IN – It shows IN entrey on display
iii. Reader OUT – It shows OUT entry on display
iv. Reader IN/OUT Toggle – IN OUT entry can toggle using 0 key.

FIRE-TAMPER EnDs



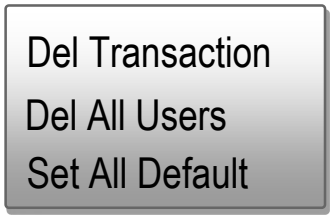
In this menu user can enable disable fire and tamper by selecting the particular option by keys 2 & 8 and press enter to set it successfully.

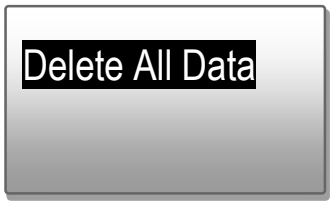
Troubleshoot



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.

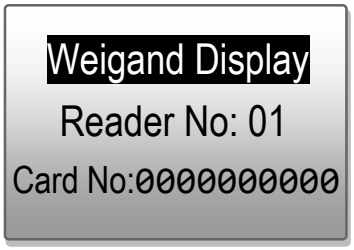
Initialize system





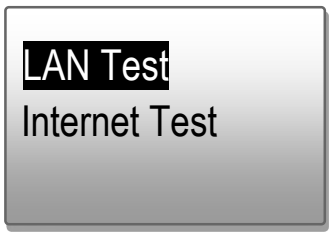
In this menu user can initialize the system according to different parameters.
Use 2 & 8 key to select perticuler menu.
After selection press enter. It shows yes & no option. Press 4 to YES & 6 to NO.

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	1/1,00,00,000
Secure	1/1,00,000	1/1,00,000	1/10,00,000	1/1,00,00,000	1/10,00,00,000
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)

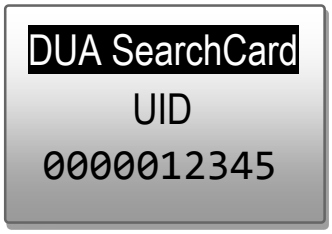
Annexure B

Network setting

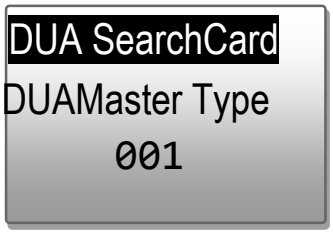
Sr. No.	Network Setting Parameters	Description
1.	**IP Addres**	Set IP address to device for TCP/IP communication
2.	**Subnet Mask**	As per your network.
3.	**Gateway**	As per your network.
4.	**Local TCP Port**	For device indentification and communication
5.	**Local UDP Port**	For device indentification 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 Port Address where we want to push transactiondata 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 Port Address where we want to push transactiondata 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 →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 add in Unit.
4) Now to config dual user go in User menu & select ‘DUA Search Card’.
   Show card or enter UID.

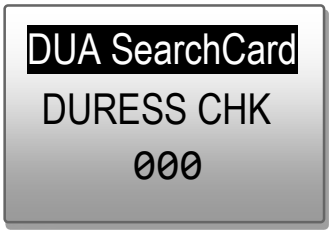


Press Enter.



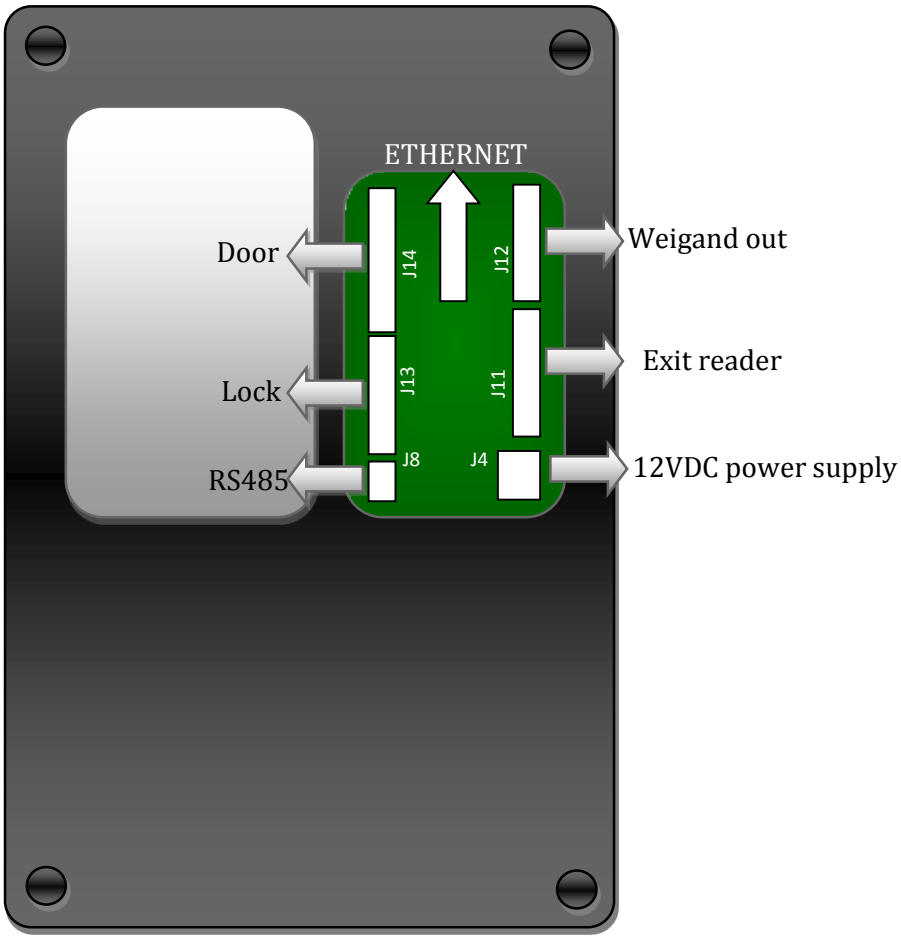
Now enter 01 for Master & 00 for normal user. Press Enter.

Assign Group no. Press Enter.

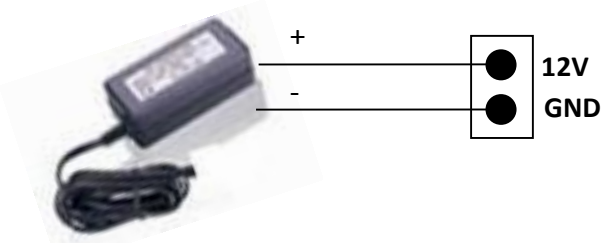


Press “01”→ to enable Duress & Press “00”→ to Disable Duress
Press enter (it will go for next card number)

NG biolite connection details

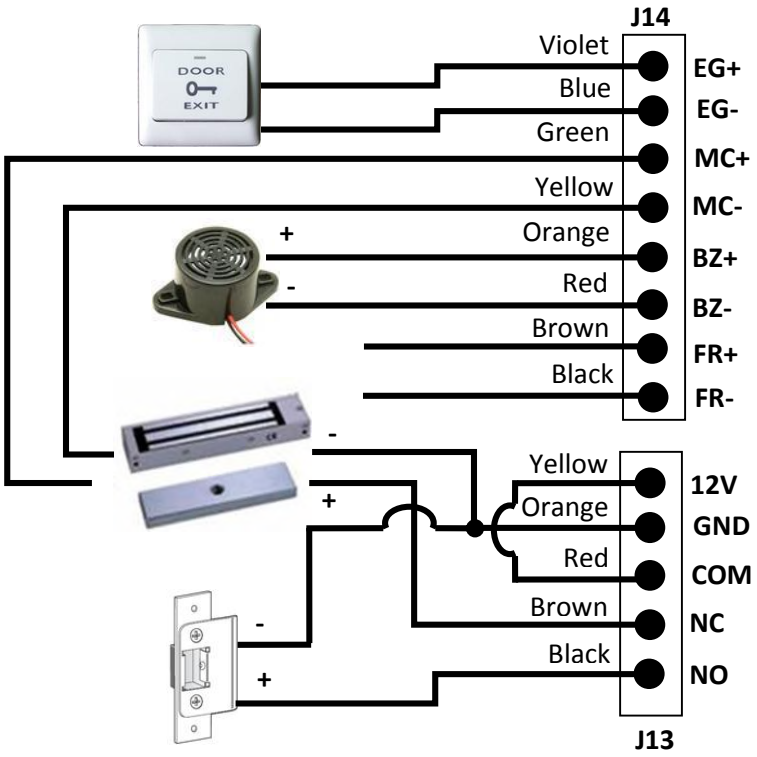


Power Supply connection:



12DC power supply

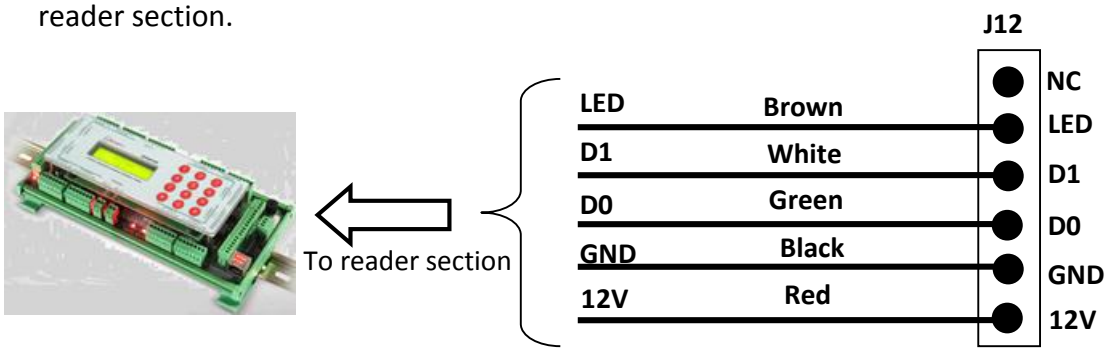
Door connection:



Exit reader connection:

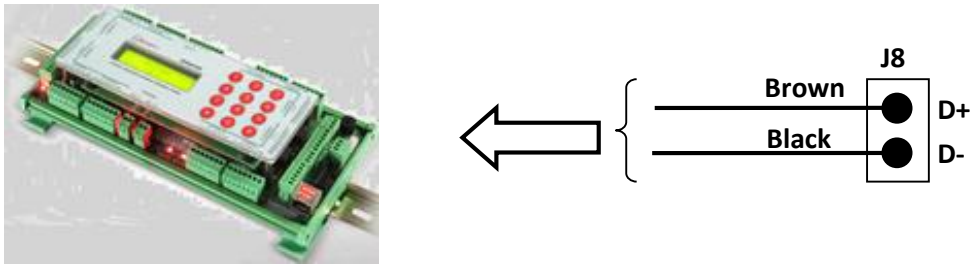
Weigand OUT connection:

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



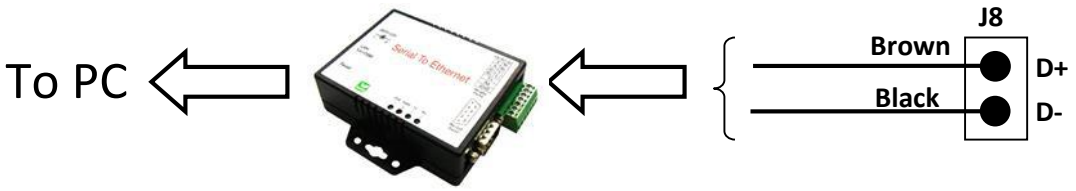
RS485 connection:

To controller for template management by TCP/IP comm.

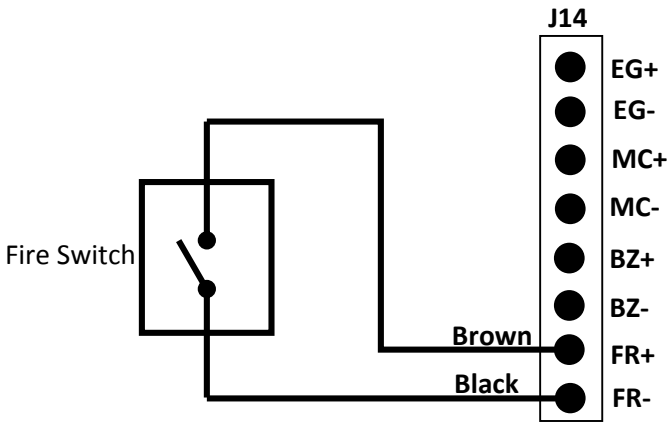


OR

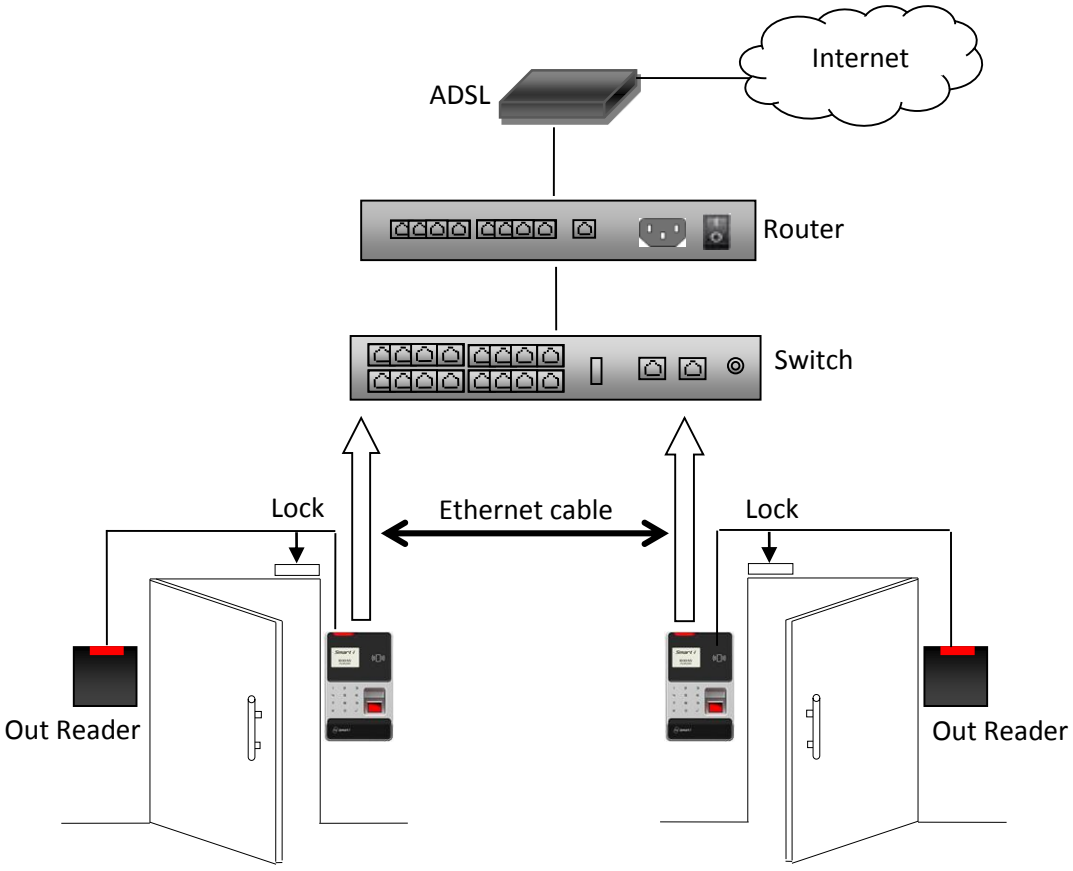
To RS485 converter for serial communication.



Fire Panel connection:



Device configuration



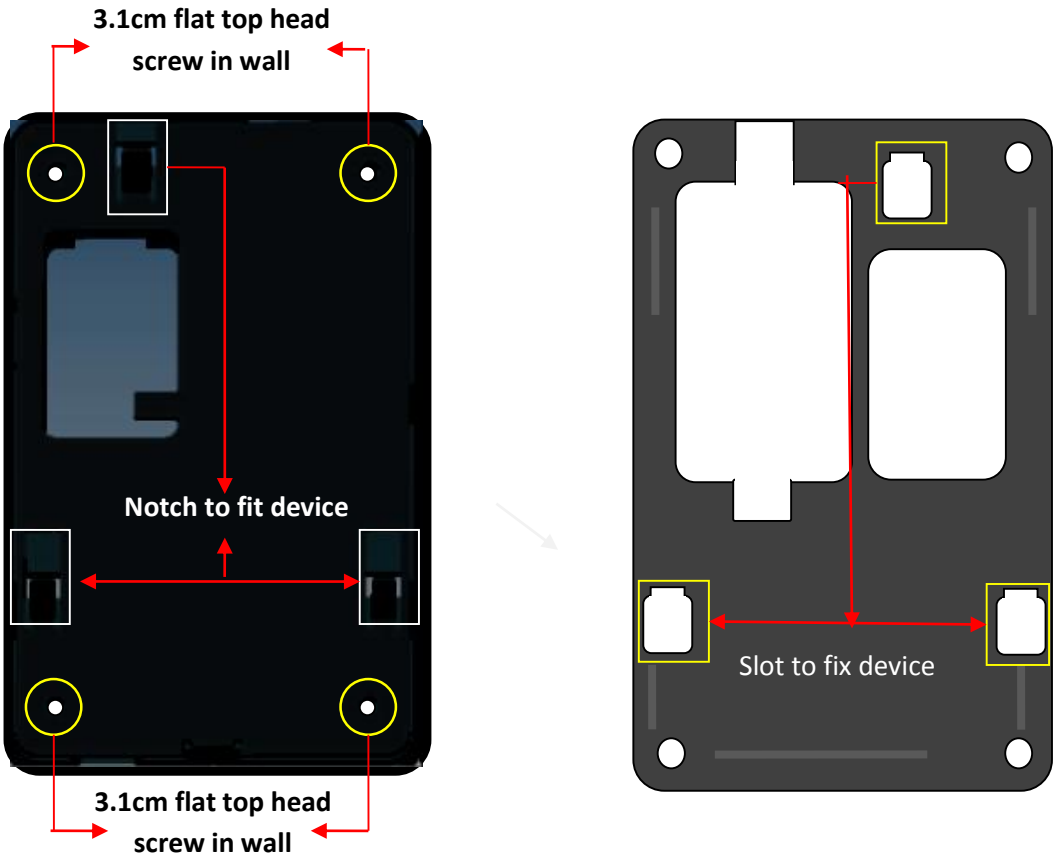
Recommended Cable specification

Type	Particular	Cable Spec	Distance
A	Reader (Weigand)	22AWG; 6 core; shielded Cable	Up to 25 meter
B	Egress switch, Magnetic contact	22 AWG;2 core; shielded Cable	Up to 10Ft.
C	Lock	16 AWG; 2 core; shielded Cable	Up to 10 Ft.
D	Unit to Power Supply	22AWG; 2 Core shielded Cable	Up to 10 Ft.
E	LAN Cable	24AWG; CAT5 / CAT6 (4 pair)	Up to 100 meter

Mounting of unit on the wall

Img1. 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:

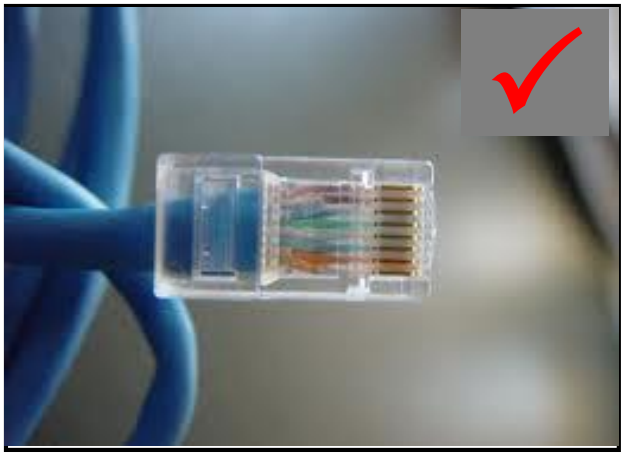
Img2. Fit device on back plate by fixing the slots given at the back cover of device.



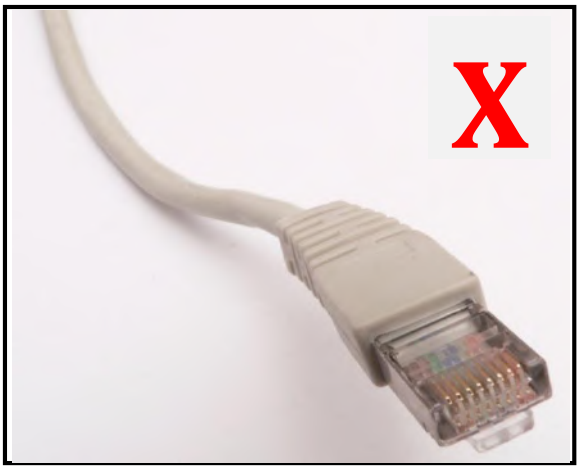
Connecting To Host Computer

The NG biolite can be connect to the computer by TCP/IP (Ethernet).
Note: Use proper manually crimped **CAT5** cable, Refer bellow images,

Manually Cramped RJ-45



Readymade RJ-45



The NG Biolite 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 NGBiolite 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.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\User-09>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.26
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.11

C:\Documents and Settings\User-09>
```

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 NGBiolite (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'.

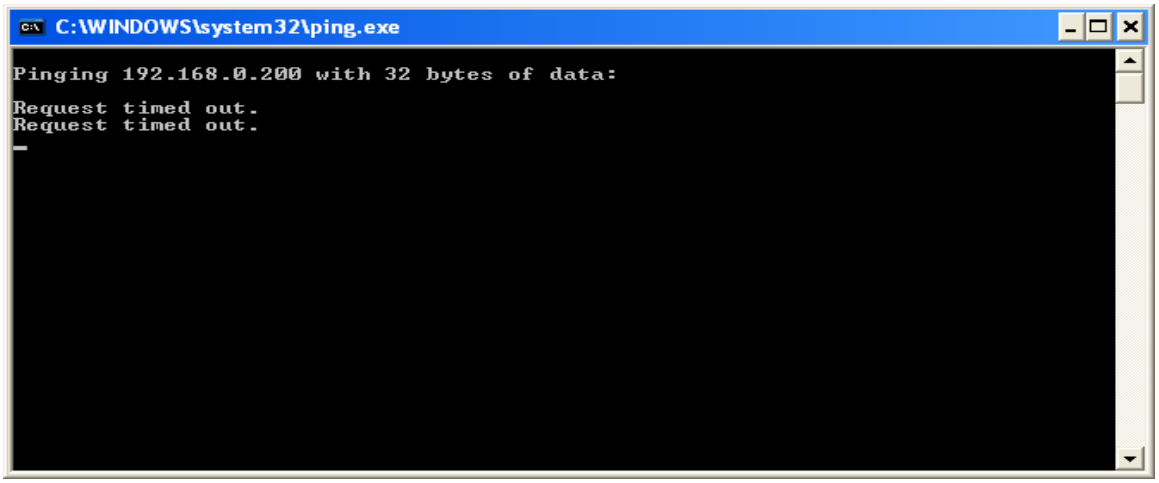
Step 2

Type "Ping 192.168.0.251 -t"
(The IP Address should reflect that of your NG Biolite 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



Using NG Biolite

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

I Proper Finger Presentation.

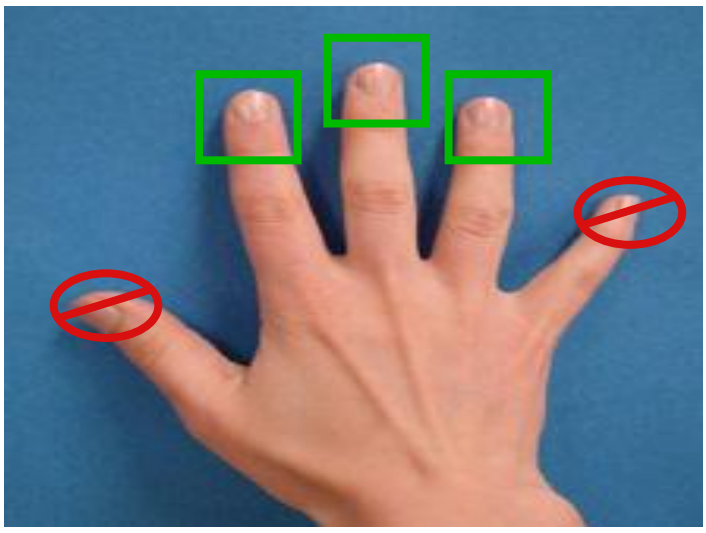
When it is necessary to place your finger on the fingerprint sensor, gently place the last segment of the finger used during enrollment squarely & firmly on the fingerprint sensor.

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

Suggested Use of Finger Print Sensor



Suggested Fingers:

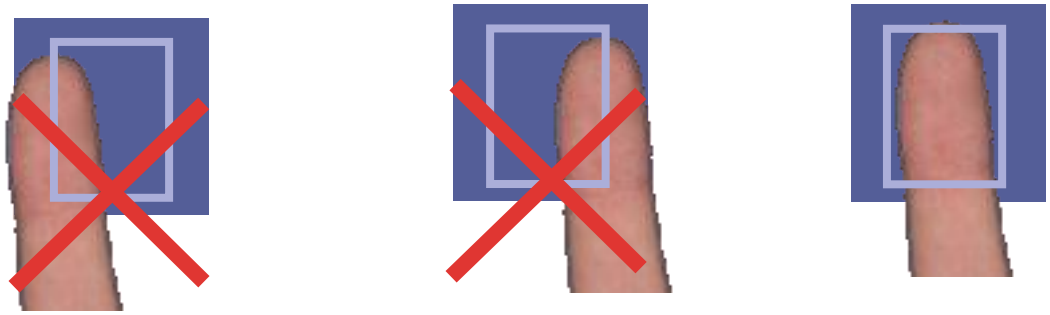
Index, middle or ring fingers. Avoid using thumb and small fingers since they are typically awkward to position consistently on the sensor.

When enrolling, place the finger on the sensor where the entire core can clearly be seen in the Fingerprint Image window.

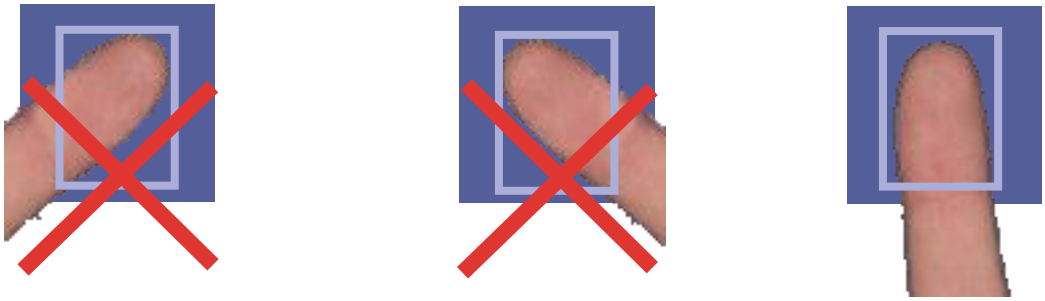
Do not enroll thumbs unless it is too difficult to capture a good image from one of the suggested fingers.

Finger Placement:
Completely covering the entire area of the sensor with the fingerprint will provide the best performance. Touching the sensor as if pressing a button creates an image that lacks information-rich fingerprint data.

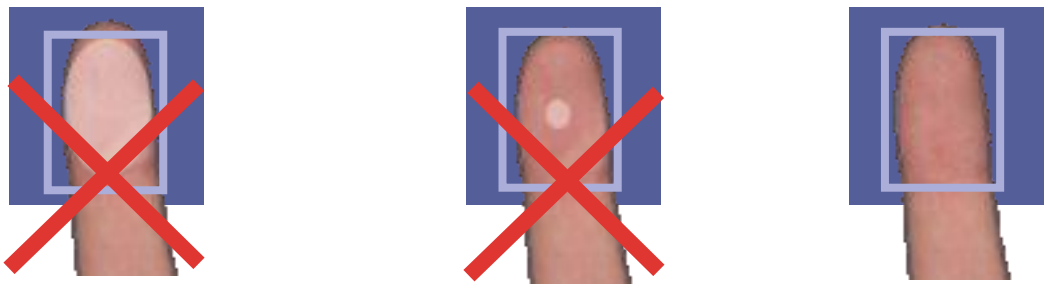
Position: - Placing your finger far from the center position of the sensor will increase the rejection rate.



Rotation: - Finger rotation should be kept minimal during enrollment and verification.



Pressure: - Apply moderate pressure when making contact with the sensor. Too much pressure may cause smudging of the fingerprint. Too little pressure may not allow the sensor to recognize the presence of a finger.



Finger Conditions: Wet or Dry

Image of Very wet finger

- **Wipe finger with a piece of cloth or paper towel**

Image of Very dry finger

- **Users can increase the finger pressure**
- **or use small amount of skin-moisturizing lotion.**

Image of Normal finger

Improving the Image Quality at the time of Registration

How to Improve the Image Quality

- Clean the sensor and the finger
- Keep the finger on the sensor for several seconds prior to the enrollment
- Change the finger

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 multimeter if possible
- Check 12V-G power 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 NG Biolite 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.