eSSL®

Security at Fingertips

QUICK START GUIDE

2.4 Inch TFT WiFi Access Control Terminal

www.esslsecurity.com

Safety Precautions

Before installation, please read the following safety precautions for user safety and to prevent product damage.

Do not install the device in a place subject to direct sun light, humidity, dust or soot.

Do not place a magnet near the product. Magnetic objects such as magnet, CRT, TV, monitor or speaker may damage the device.

Do not place the device next to heating equipment.

Do not to let liquid like water, drinks or chemicals leak inside the device.

Do not let children touch the device without supervision.

Do not drop or damage the device.

Do not disassemble, repair or alter the device.

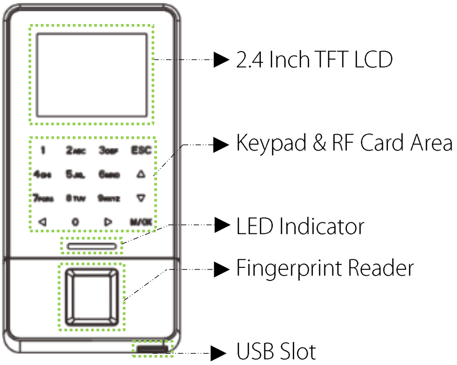
Do not use the device for any purpose other than those specified.

Clean the device often to remove dust on it. In cleaning, do not splash water on the device but wipe it out with smooth cloth or towel.

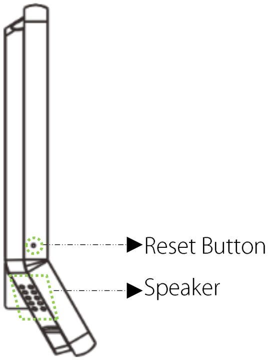
Contact your supplier in case of a problem!

Device Overview

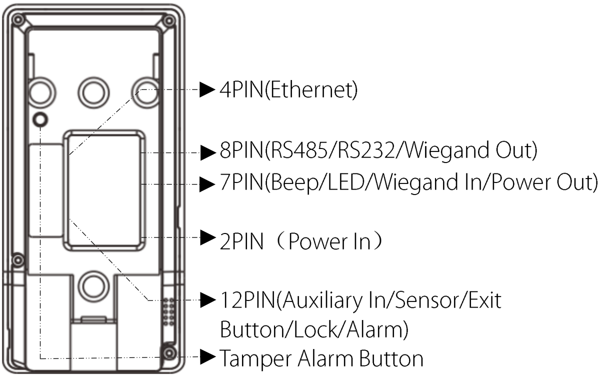
Front



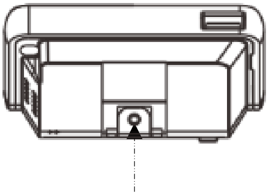
Side



Back

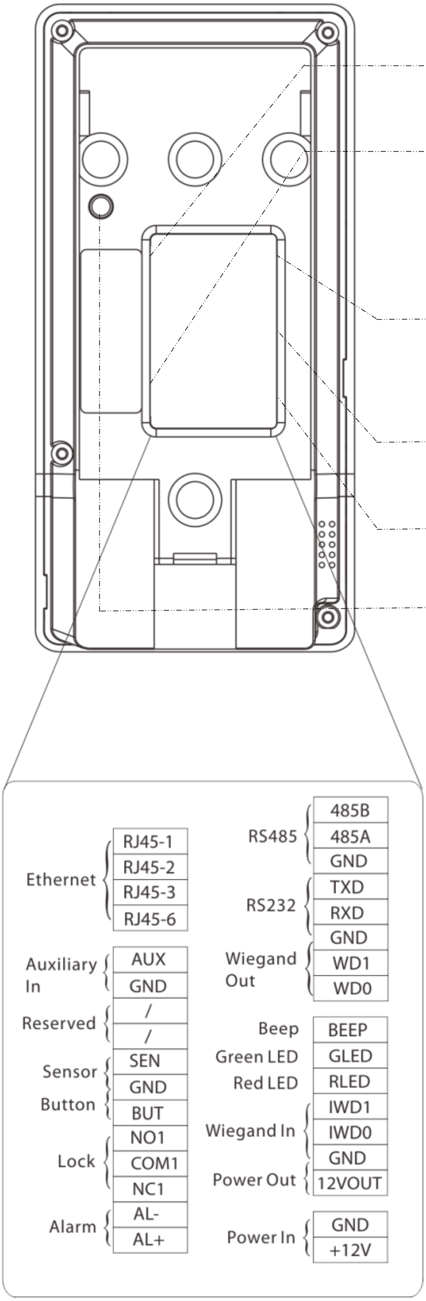

4PIN(Ethernet)
8PIN(RS485/RS232/Wiegand Out)
7PIN(Beep/LED/Wiegand In/Power Out)
2PIN（Power In）
12PIN(Auxiliary In/Sensor/Exit Button/Lock/Alarm)
Tamper Alarm Button

Bottom



Star-shaped screw hole for fixing device to back plate

Device Overview



4 Pin Cable Connectors Ethernet (TCP/IP)

12 Pin Cable Connectors
- Auxiliary In
- Reserved
- Sensor
- Button
- Lock
- Alarm

8 Pin Cable Connectors
- RS485
- RS232
- Wiegand Out

7 Pin Cable Connectors
- LED, Beep
- Wiegand In
- Power Out

2 Pin Cable Connectors
- Power In

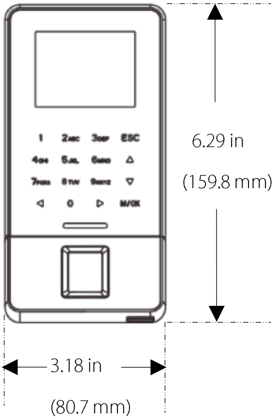
Tamper Alarm Button

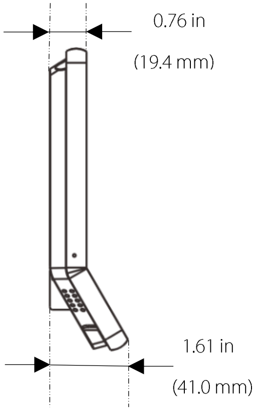
Ethernet	RJ45-1
	RJ45-2
	RJ45-3
	RJ45-6
Auxiliary In	AUX
	GND
Reserved	/
	/
Sensor	SEN
	GND
Button	BUT
Lock	NO1
	COM1
	NC1
Alarm	AL-
	AL+

RS485	485B
	485A
	GND
RS232	TXD
	RXD
	GND
Wiegand Out	WD1
	WD0
Beep	BEEP
Green LED	GLED
Red LED	RLED
Wiegand In	IWD1
	IWD0
	GND
Power Out	12VOUT
Power In	GND
	+12V

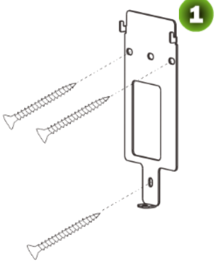
Device Dimensions & Installation

Product Dimensions



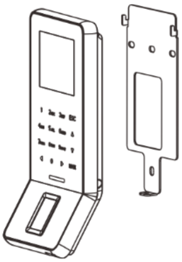


Mounting the Device on Wall

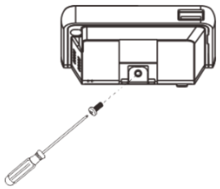


1 Fix the back plate onto the wall using wall mounting screws.

Note: We recommend drilling the mounting plate screws into solid wood (i.e. stud/beam). If a stud/beam cannot be found, use supplied drywall plastic anchors.



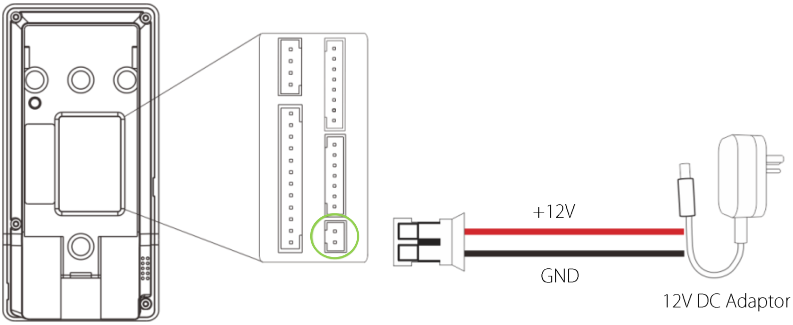
2 Insert the device to back plate.



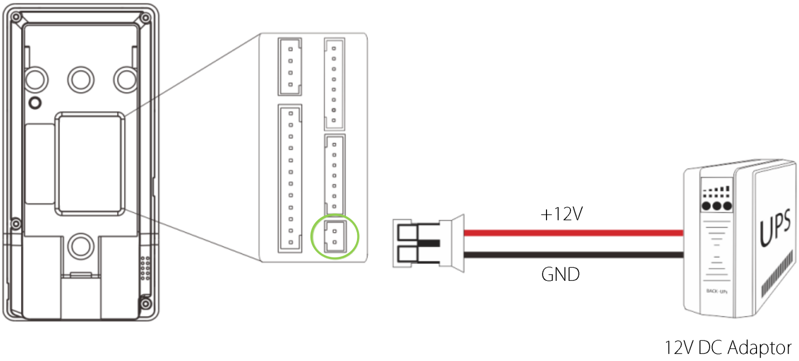
3 Use security screws to fasten the device to back plate.

Power Connection

❖ Without UPS



❖ With UPS (Optional)

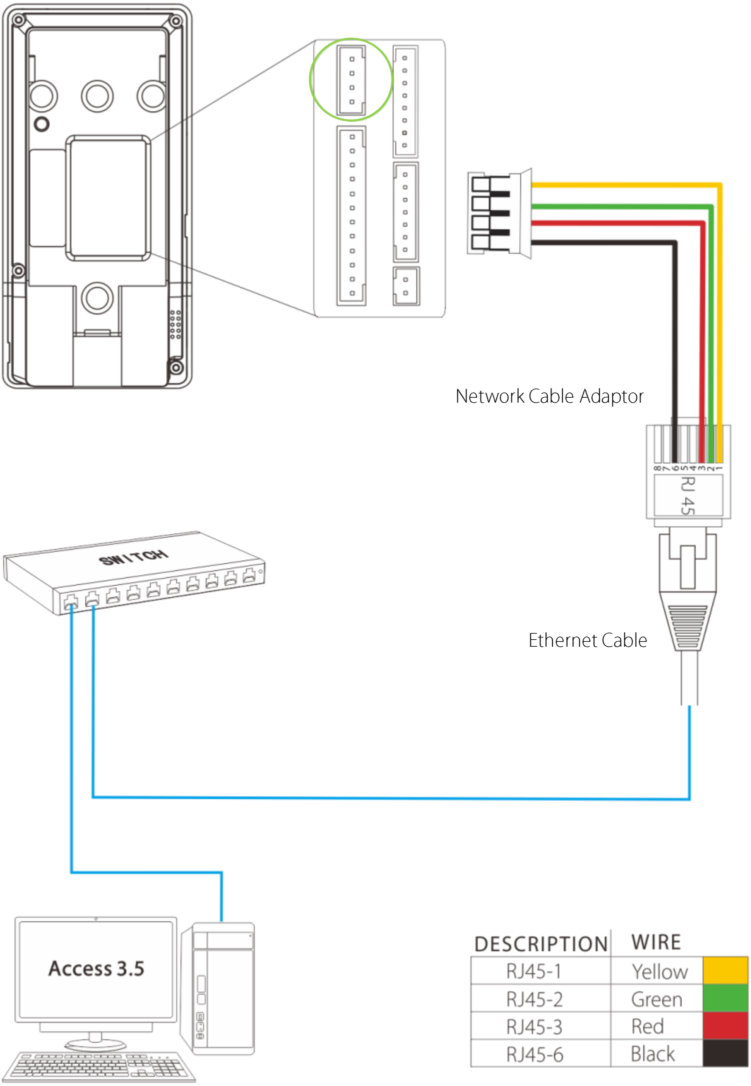


❖ Recommended Power Supply

- 12V±10%, at least 500MA.
- To share the power with other devices, use a power supply with higher current ratings.

Ethernet Connection

❖ LAN Connection



DESCRIPTION	WIRE	
RJ45-1	Yellow	🟨
RJ45-2	Green	🟩
RJ45-3	Red	🟥
RJ45-6	Black	⬛

Note: The device can be connected to PC directly by Ethernet cable.

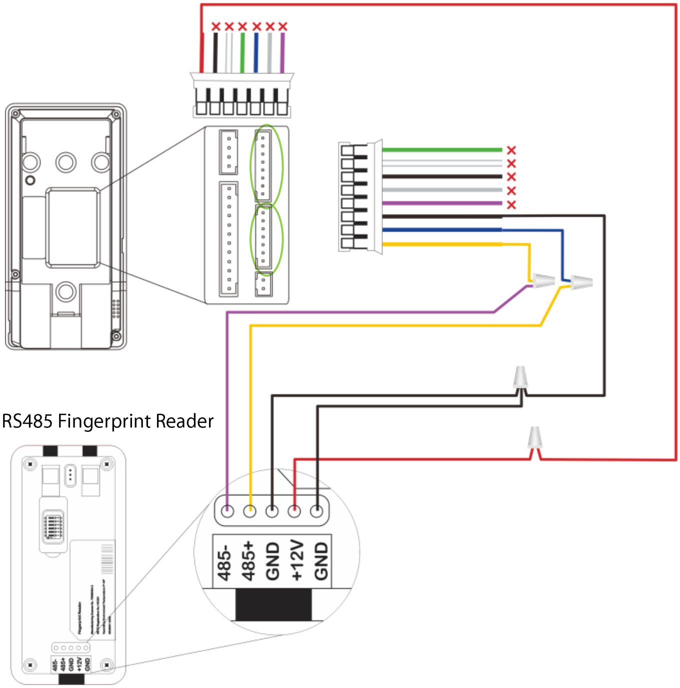
RS485 Connection

❖ RS485 Fingerprint Reader Connection

DESCRIPTION		WIRE	
BEEP	✖	Purple	🟪
GLED	✖	Gray	▨
RLED	✖	Blue	🟦
IWD1	✖	Green	🟩
IWD0	✖	White	⬜
GND	✖	Black	⬛
+12V		Red	🟥

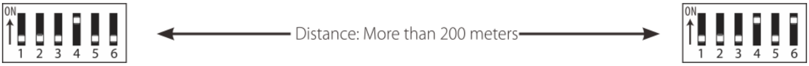
✖ Do not use

DESCRIPTION		WIRE	
485B		Yellow	🟨
485A		Blue	🟦
GND		Black	⬛
TXD	✖	Purple	🟪
RXD	✖	Gray	▨
GND	✖	Black	⬛
WD1	✖	White	⬜
WD0	✖	Green	🟩



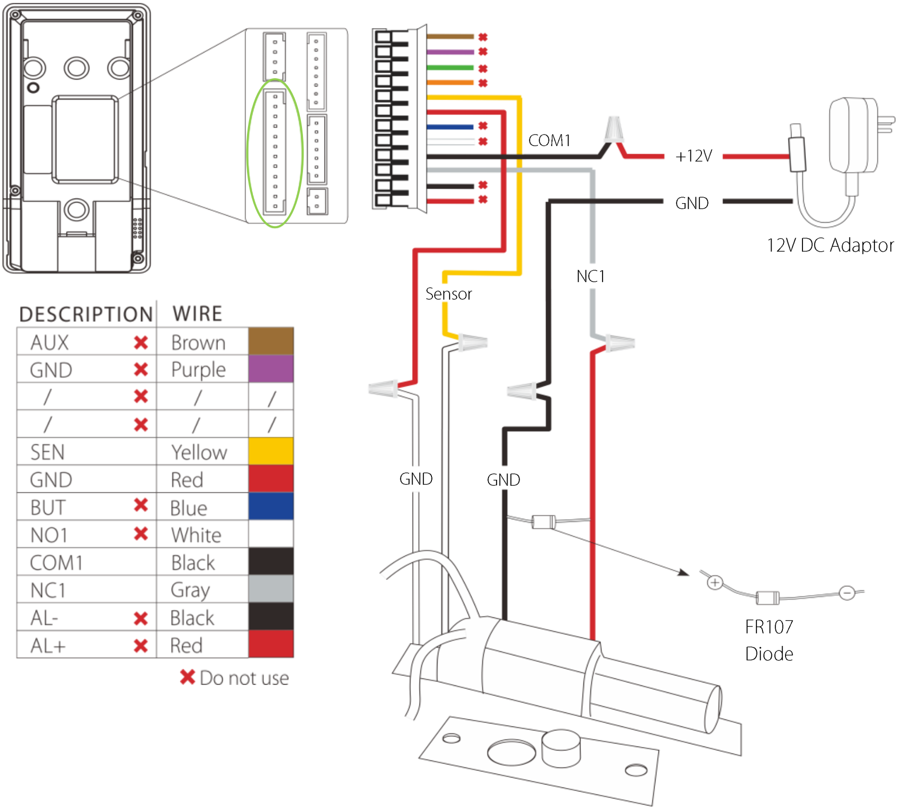
❖ DIP Settings

- ❖ There are six DIP switches on the back of RS485 fingerprint reader, switches 1-4 are for RS485 address, switch 5 is reserved, switch 6 is for reducing noise on long RS485 cable.
- ❖ If RS485 fingerprint reader is powered from the terminal, the length of wire should be less than 100 meters or 330 ft.
- ❖ If the cable length is more than 200 meters or 600 ft., the number 6 switch should be ON as below.



Lock Relay Connection

❖ Device Not Sharing Power with the Lock



DESCRIPTION		WIRE	
AUX	✖	Brown	🟫
GND	✖	Purple	🟪
/	✖	/	/
/	✖	/	/
SEN		Yellow	🟨
GND		Red	🟥
BUT	✖	Blue	🟦
NO1	✖	White	⬜
COM1		Black	⬛
NC1		Gray	▒
AL-	✖	Black	⬛
AL+	✖	Red	🟥

✖ Do not use

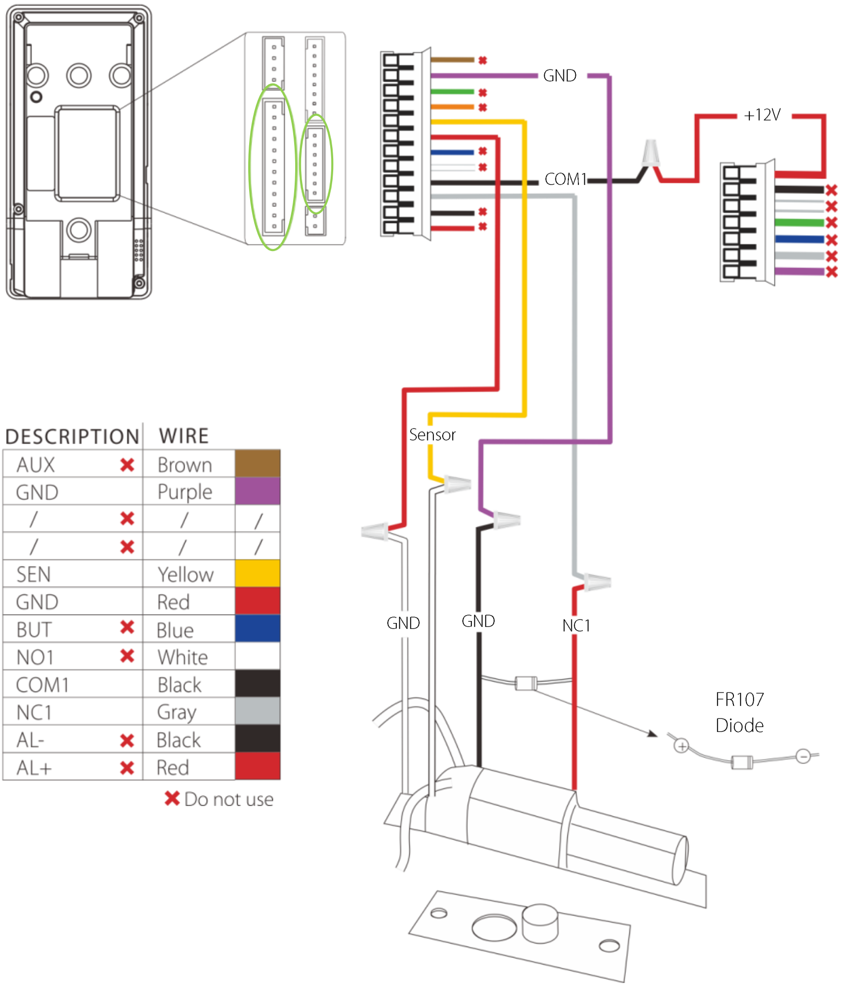
Normally Closed Lock

Notes:

1. The system supports **NO LOCK** and **NC LOCK**. For example the **NO LOCK** (normally opened at power on) is connected with '**NO1**' and '**COM1**' terminals, and the **NC LOCK** (normally closed at power on) is connected with '**NC1**'and '**COM1**' terminals.
2. When electrical lock is connected to the Access Control System, you must parallel one FR107 diode (equipped in the package) to prevent the self-inductance EMF from affecting the system.
   ⚠Do not reverse the polarities.

Lock Relay Connection

❖ Device Sharing Power with the Lock

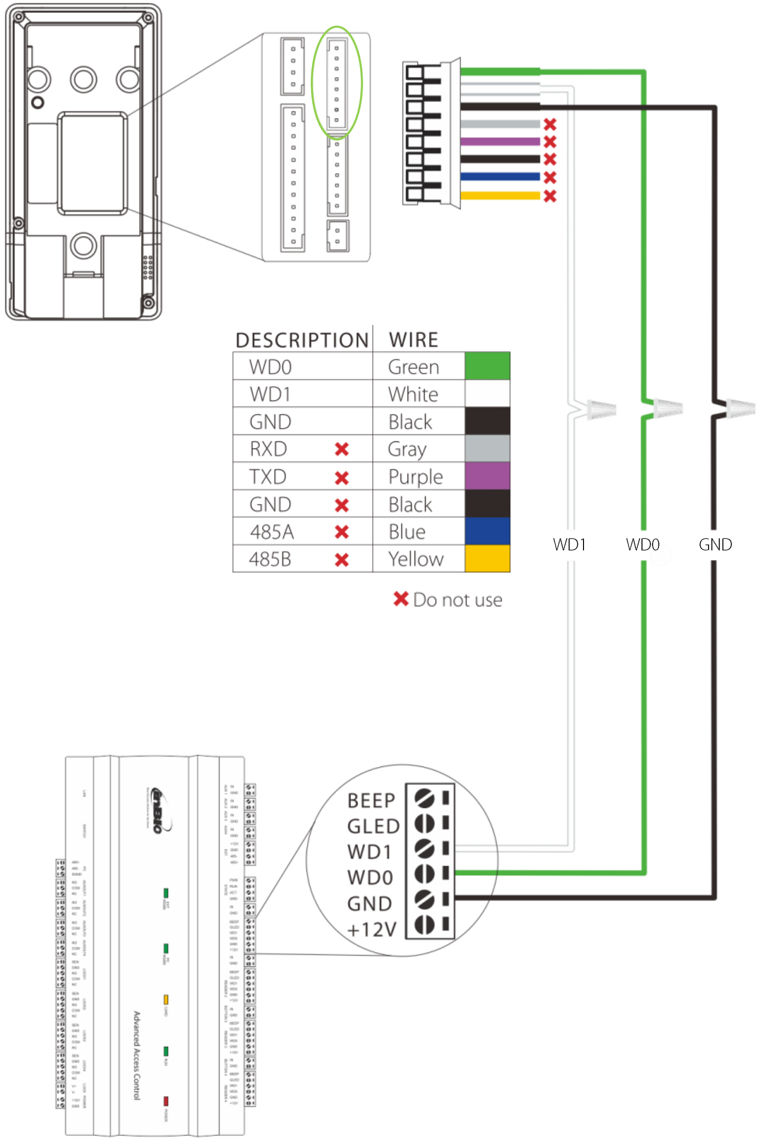


DESCRIPTION		WIRE	
AUX	✖	Brown	🟫
GND		Purple	🟪
/	✖	/	/
/	✖	/	/
SEN		Yellow	🟨
GND		Red	🟥
BUT	✖	Blue	🟦
NO1	✖	White	⬜
COM1		Black	⬛
NC1		Gray	▨
AL-	✖	Black	⬛
AL+	✖	Red	🟥

✖ Do not use

Normally Closed Lock

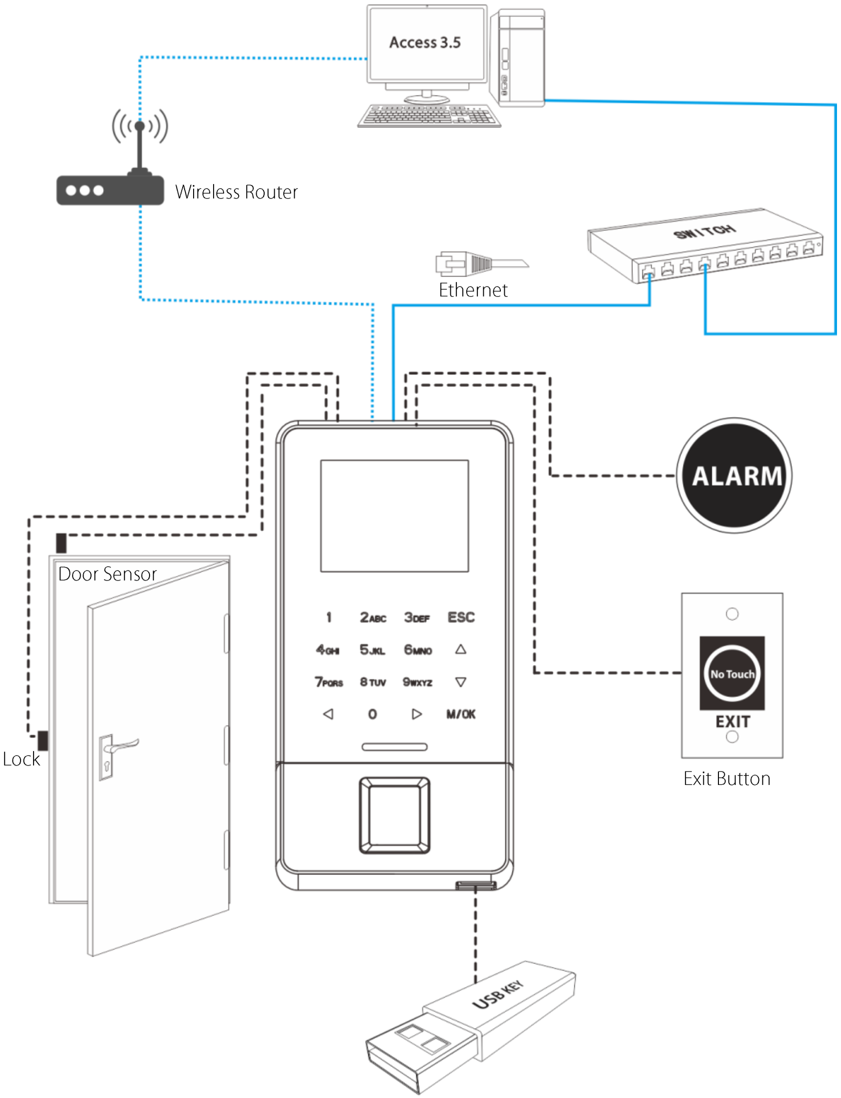
Wiegand Output Connection



DESCRIPTION		WIRE	
WD0		Green	🟩
WD1		White	□
GND		Black	■
RXD	✖	Gray	▨
TXD	✖	Purple	🟪
GND	✖	Black	■
485A	✖	Blue	🟦
485B	✖	Yellow	🟨

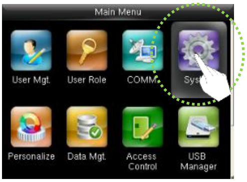
✖ Do not use

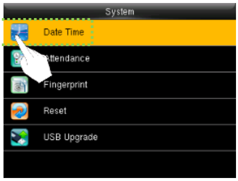
Standalone Installation

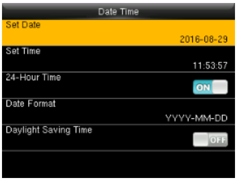


Device Operation

❖ Date / Time Settings






Date Time

Set Date 2016-08-29

Set Time 11:53:57

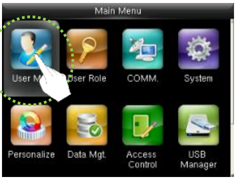
24-Hour Time ON

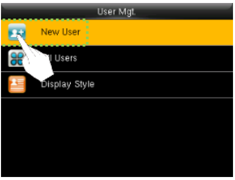
Date Format YYYY-MM-DD

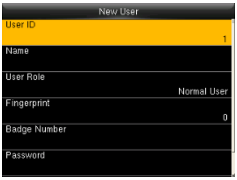
Daylight Saving Time OFF

Press **M/OK** icon to enter the main menu> System > Date Time to set date and time.

❖ Adding User






New User

User ID 1

Name

User Role Normal User

Fingerprint 0

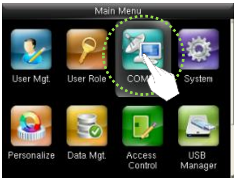
Badge Number

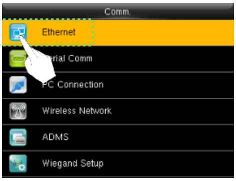
Password

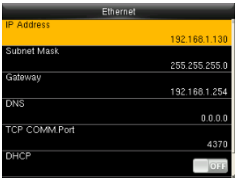
Press **M/OK** icon to enter the main menu> User Mgt. > New User to enter the adding New User interface.

Settings include inputting user ID, user name, choosing user role (Super Admin / Normal User), registering FP / badge number★ / password, and setting access control role.

❖ Ethernet Settings






Ethernet

IP Address 192.168.1.130

Subnet Mask 255.255.255.0

Gateway 192.168.1.254

DNS 0.0.0.0

TCP COMM.Port 4370

DHCP OFF

Press **M/OK** icon to enter the main menu > Comm. > Ethernet.

The Parameters below are the factory default values. Please adjust them according to the actual network.

IP Address: 192.168.1.201

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

DNS: 0.0.0.0

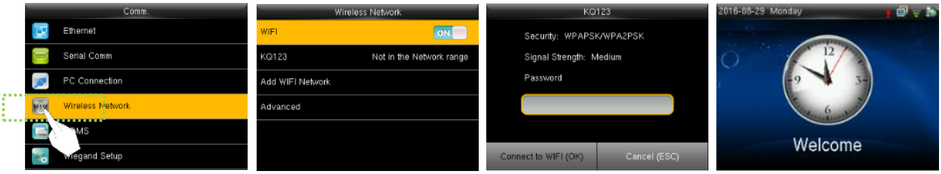
TCP COMM. Port: 4370

DHCP: Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server. If DHCP is enabled, IP cannot be set manually.

Display in Status Bar: To set whether to display the network icon , on the status bar.

Device Operation

❖ WIFI Settings



WIFI ON

KQ123 Not in the Network range

Security: WPAPSK/WPA2PSK

Signal Strength: Medium

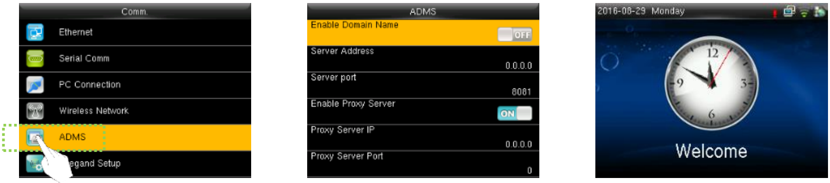
1. Press **M/OK** icon to enter the main menu > Comm. > Wireless Network;

2. Press **M/OK** icon to open WIFI, and search for available WIFI within the network;

3. Select an available WIFI, press **M/OK** icon to input the password;

4.When the Webserver is connected successfully, the initial interface will display the 📶 logo.

❖ ADMS Settings★



Enable Domain Name OFF

Server Address 0.0.0.0

Server port 8081

Enable Proxy Server ON

Proxy Server IP 0.0.0.0

Proxy Server Port 0

Press **M/OK** icon to enter the main menu > Comm. > ADMS, to set the parameters which are used for connecting with the ADMS server.

When the Webserver is connected successfully, the initial interface will display the 🖧 logo.

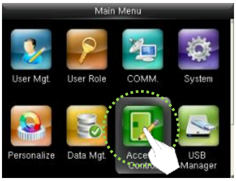
Enable Domain Name: When this function is turned on, the domain name mode "http://... " will be used, such as http://www.XXX.com. XXX denotes the domain name when this mode is on; when this mode is off, enter the IP address format in XXX.

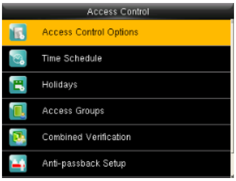
Server Address: IP address of the ADMS server.

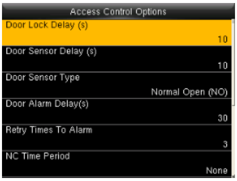
Server Port: Port used by the ADMS server.

Enable Proxy Server: Method of enabling proxy. To enable proxy, please set the IP address and port number of the proxy server. Entering proxy IP and server address will be the same.

❖ Access Control Settings






Access Control Options

Door Lock Delay (s) 10

Door Sensor Delay (s) 10

Door Sensor Type Normal Open (NO)

Door Alarm Delay(s) 30

Retry Times To Alarm 3

NC Time Period None

Press **M/OK** icon to enter the main menu > Access Control to enter Access Control setting interface.

To gain access, the registered user must meet the following conditions:

1. User's access time falls within either user's personal time zone or group time zone.
2. User's group must be in the access combo (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

Access Control Options: To set parameters of the lock and other related devices.

Time Schedule: It is the minimum unit of access control option.

Holidays: Set some days as holidays, and then set Time Schedule of those days.

Access Groups: Grouping is to manage employees in groups. Employee in groups use group time zone by default. Group members can also set user time zone.

Combined Verification: Make various groups into different access controls to achieve multi-verification and improve security.

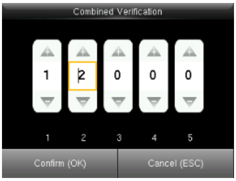
Anti-Passback Setup: To prevent someone following the employee into the company.

Duress Options: The device will open the door as usual, but the alarm signal will be sent to backstage alarm when employee comes across duress.

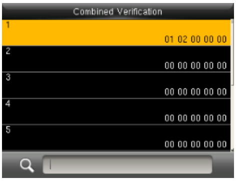
➢ Access Control Combination Settings

E.g.: Add an access control combination which requires 2 persons' verification from both group 1 (set in User Management) and group 2.

1



2


Combined Verification

1 01 02 00 00 00

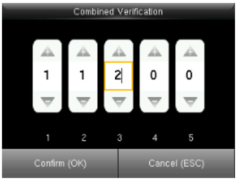
2 00 00 00 00 00

3 00 00 00 00 00

4 00 00 00 00 00

5 00 00 00 00 00

3



1.In "Combined Verification" List, click the desired combination to modify, and enter the interface(as shown in figure 1).

2.Click"+/-" to change the number, and click"Confirm" to save and back to "Combined Verification" (as shown in figure 2).

Note:

1. A single Access Control Combination can consist of a maximum of 5 user groups (in order to open door, verification of all 5 users is required).
2. If the combination is set as shown in figure 3, a user from access group 2 must obtain verification of two users from access group 1 in order to open door.
3. Set all group number to zero to reset access control combination.

Troubleshooting

1.Fingerprint can not be read or it takes too long?

- Check whether a finger or fingerprint sensor is stained with sweat, water, or dust.
- Retry after wiping off finger and fingerprint sensor with dry paper tissue or a mildly wet cloth.
- If a fingerprint is too dry, blow on the finger and retry.

2. “Invalid time zone” is displayed after verification?

- Contact Administrator to check if the user has the privilege to gain access within that time zone.

3. Verification succeeds but the user cannot gain access?

- Check whether the user privilege is set correctly.
- Check whether the lock wiring is correct.

4. The Tamper Alarm rings?

- When the device is tampered, the device will send a signal to the speaker then the icon ⚠ is displayed on the top right corner and the speaker is ringing. Only the [Speaker Alarm] (Access Control >Access Control Options>Speaker Alarm)is [ON] can user heard the ringing.

  Please install the device properly.

#24,Shambavi Building, 23rd Main, Marenahalli,
JP Nagar 2nd Phase, Bangalore - 560078
Phone : 91-8026090500 | Email : sales@esslsecurity.com
www.esslsecurity.com