Quick Start Guide

ZKTeco
ZKBioSecurity 3.0
✓ Easy to configure and use
✓ Door management
✓ Linkage settings
✓ Real time monitoring
✓ Maps, reports and maintenance
✓ SDK available for third party integration

inPulse & inPulse+
+
ZKBioSecurity 3.0

CONTENT

Safety Precautions........................3
Device Overview........................4
Product Dimensions & Installation........................6
Power Connection........................7
Ethernet Connection........................8
Lock Relay Connection........................9
Wiegand Output Connection........................11
Standalone Installation........................12
Third Party Controller........................13
How does inPulse/inPulse+ works........................14
Registration and Verification........................15
Device Operation........................16

ZKBioSecurity 3.0

Downloading........................20
Installation........................21
Adding Device........................23
Creating a Time Zone........................25
Creating an Access Level........................26
Enrolling Personnel........................27
Wiegand Format........................29
Add & Delete Personnel to Access Level........................30
Real -Time Monitoring........................31
Exporting Reports........................32

ZKBioSecurity Software

Installation and Setup starts at Page 20

Safety Precautions

The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

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

Do not place a magnet near the product. Magnetic objects such as magnets, CRTs, TVs, monitors or speakers may damage the device.

Do not place the device next to heating equipment.

Be careful 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 other purpose than specified.

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

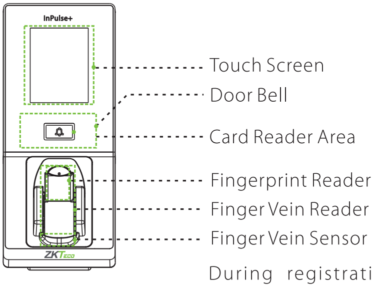
Contact your supplier in case of a problem.

Device Overview

★ Not all products have fingerprint and finger vein functions.

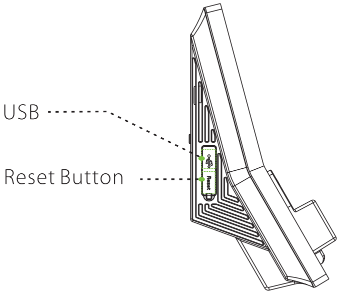
inPulse+

Front View



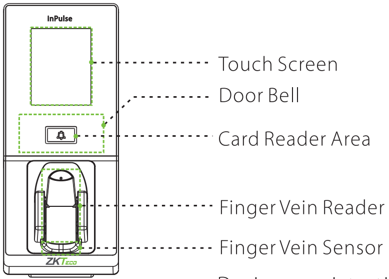
During registration, after finger touches the sensor, device begins collecting and verifying fingerprint and finger vein.

Left Side View



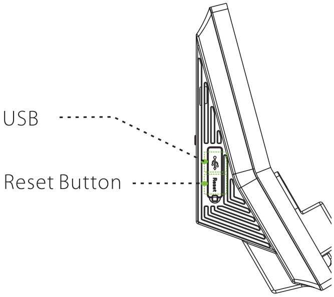
inPulse

Front View

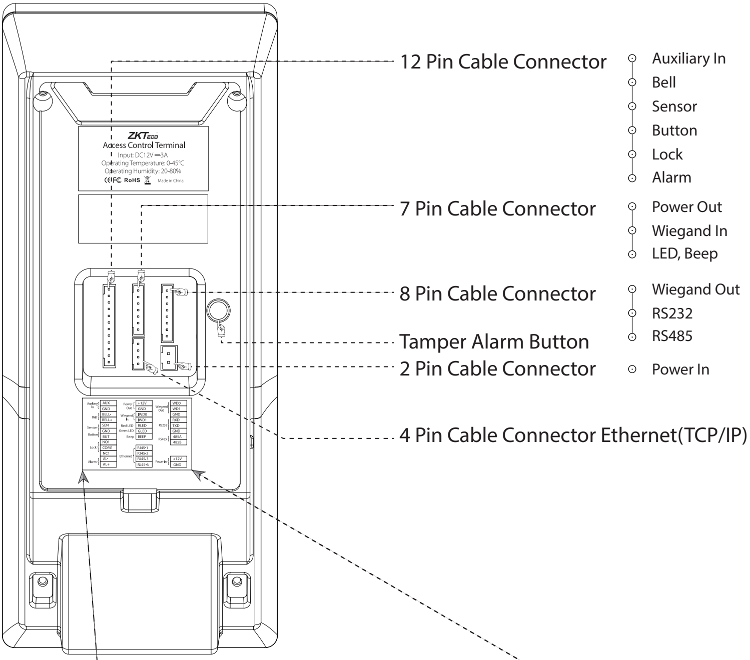


During registration, after finger touches the sensor, device begins collecting and verifying finger vein.

Left Side View



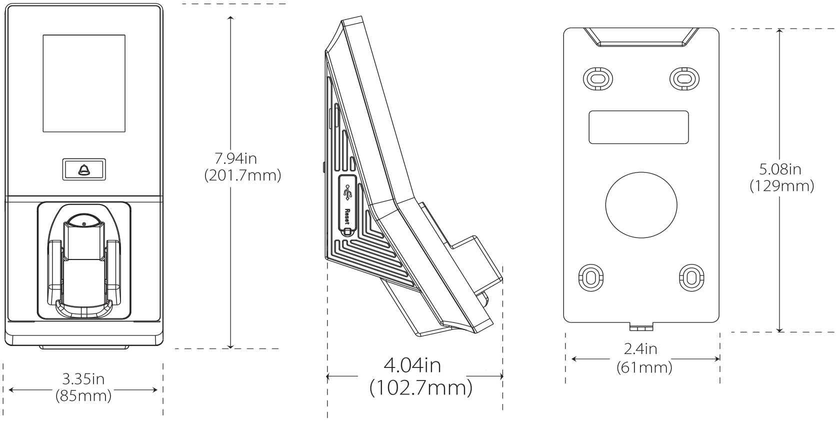
Device Overview



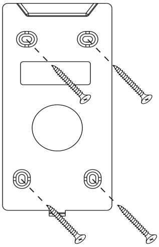
Auxiliary In	AUX	Power Out	+12V	Wiegand Out	WD0
	GND		GND		WD1
Bell	BELL-	Wiegand In	IWD0		GND
	BELL+		IWD1	RS232	RXD
Sensor	SEN	Red LED	RLED		TXD
Button	GND	Green LED	GLED		GND
	BUT	Beep	BEEP	RS485	485A
Lock	NO1				485B
	COM1	Ethernet	RJ45-1		
	NC1		RJ45-2		
Alarm	AL-		RJ45-3	Power In	+12V
	AL+		RJ45-6		GND

Product Dimensions & Installation

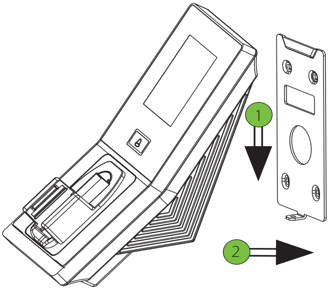
Product Dimensions



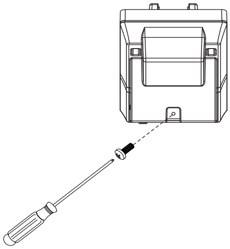
Mounting the Device on the Wall



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.



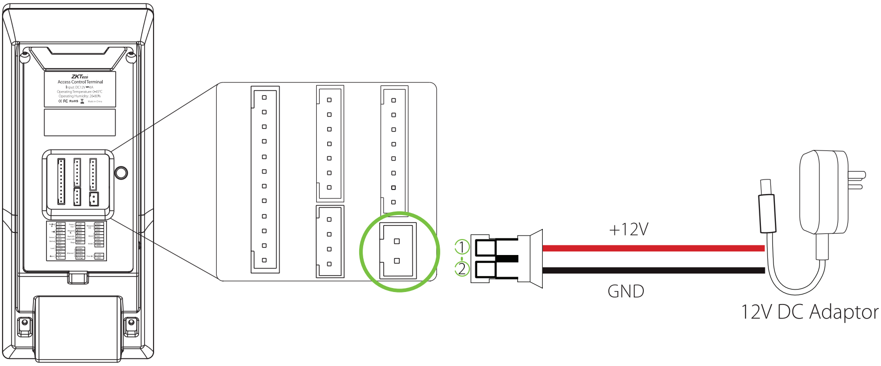
2. Insert the device to back plate.



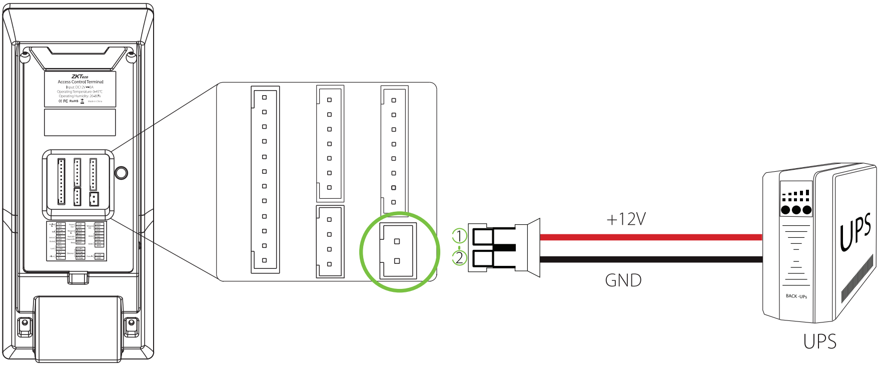
3. Use security screws to fasten the device to back plate.

Power Connection

Without UPS



With UPS (Optional)

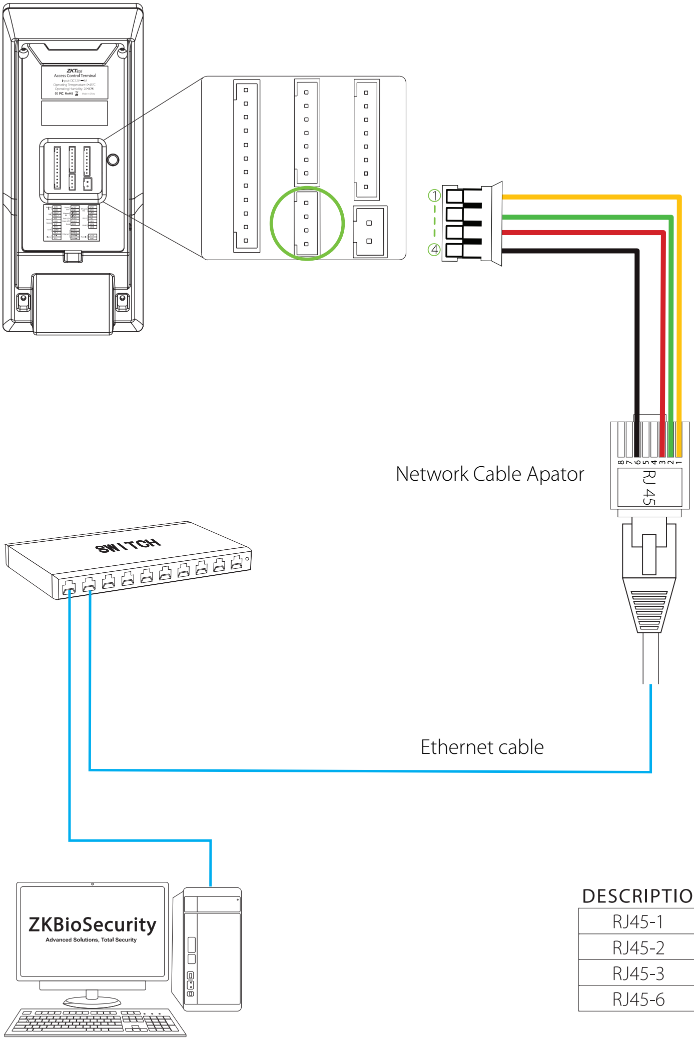


Recommended Power Supply

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

Ethernet Connection

LAN Connection

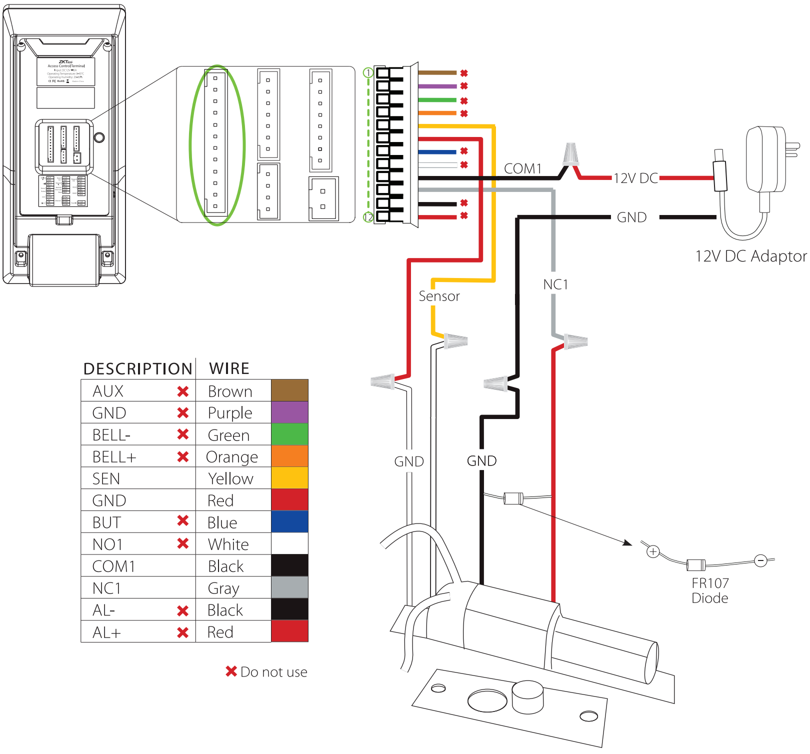


DESCRIPTION	WIRE	
RJ45-1	Yellow	🟨
RJ45-2	Green	🟩
RJ45-3	Red	🟥
RJ45-6	Black	⬛

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

Lock Relay Connection

Device Not Sharing Power with the Lock



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

✖ Do not use

Normally Closed Lock

Notes:

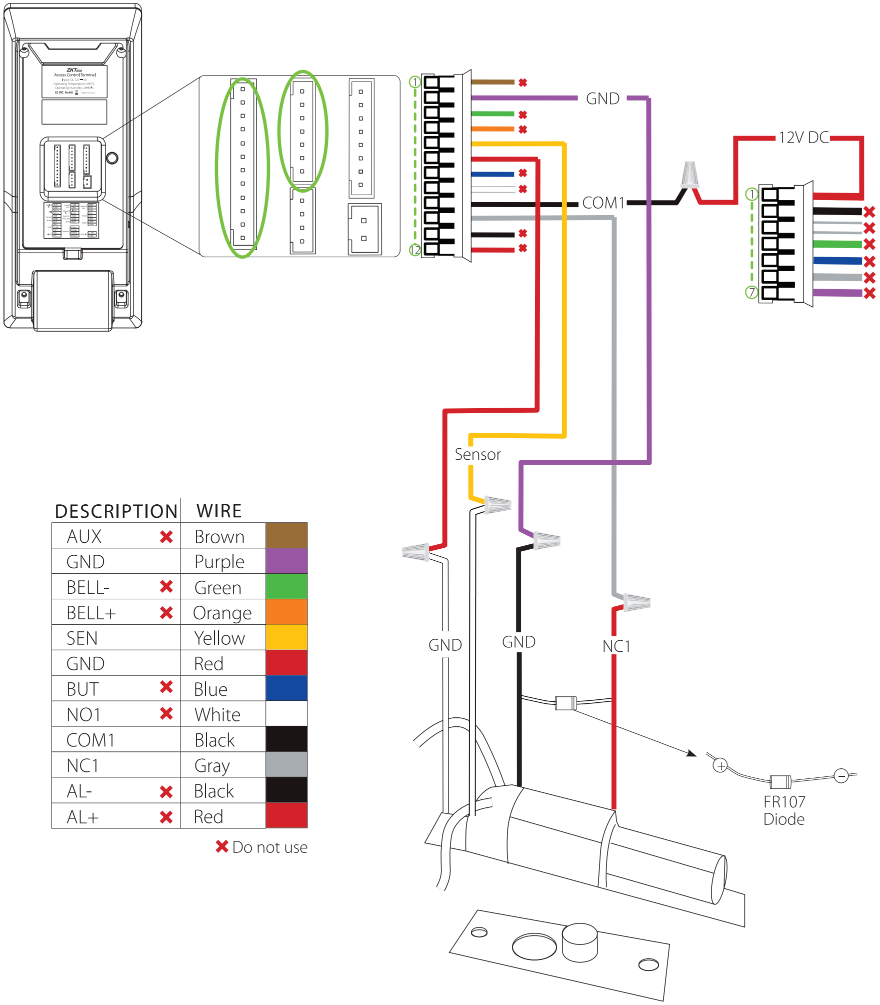
1. The system supports **NO LOCK** and **NC LOCK**. For example the **NO LOCK** (normally opened at power on) is connected with '**NO1**' and '**COM1**' terminals, and the **NC LOCK** (normally closed at power on) is connected with '**NC1**'and '**COM1**' terminals.

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

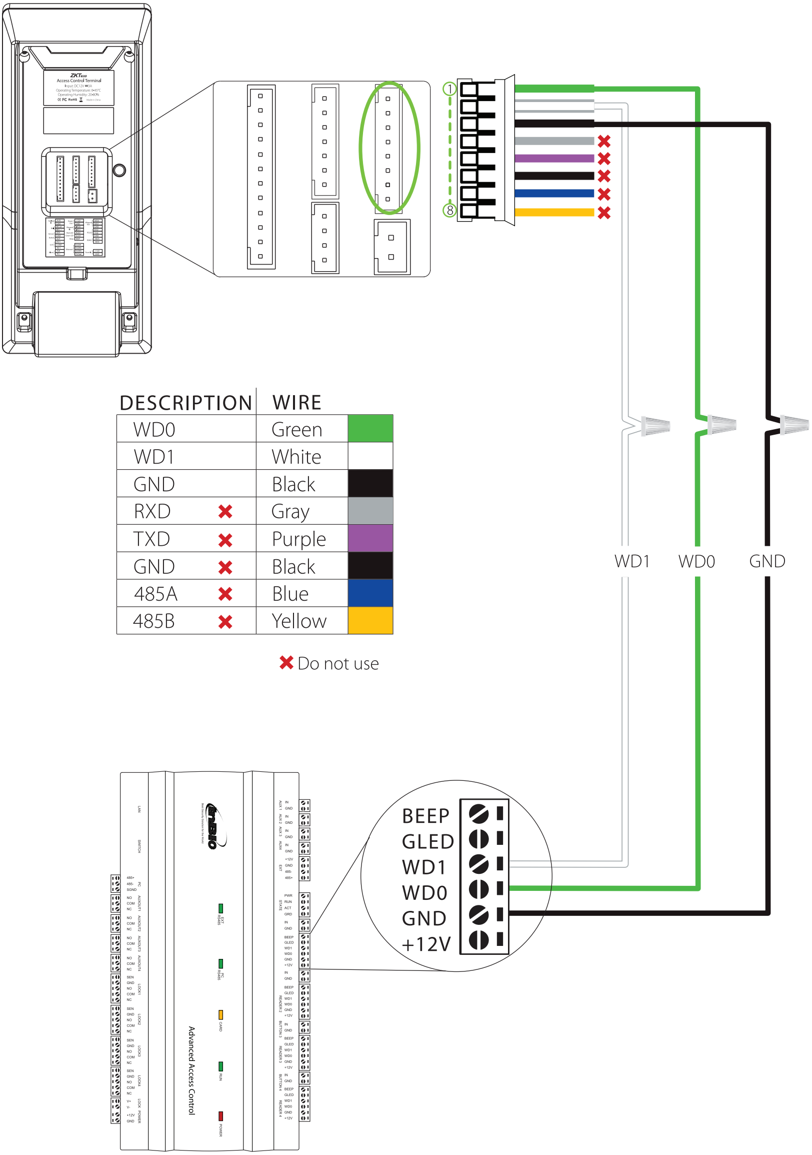


DESCRIPTION		WIRE	
AUX	✖	Brown	🟫
GND		Purple	🟪
BELL-	✖	Green	🟩
BELL+	✖	Orange	🟧
SEN		Yellow	🟨
GND		Red	🟥
BUT	✖	Blue	🟦
NO1	✖	White	⬜
COM1		Black	⬛
NC1		Gray	▨
AL-	✖	Black	⬛
AL+	✖	Red	🟥

✖ Do not use

Normally Closed Lock

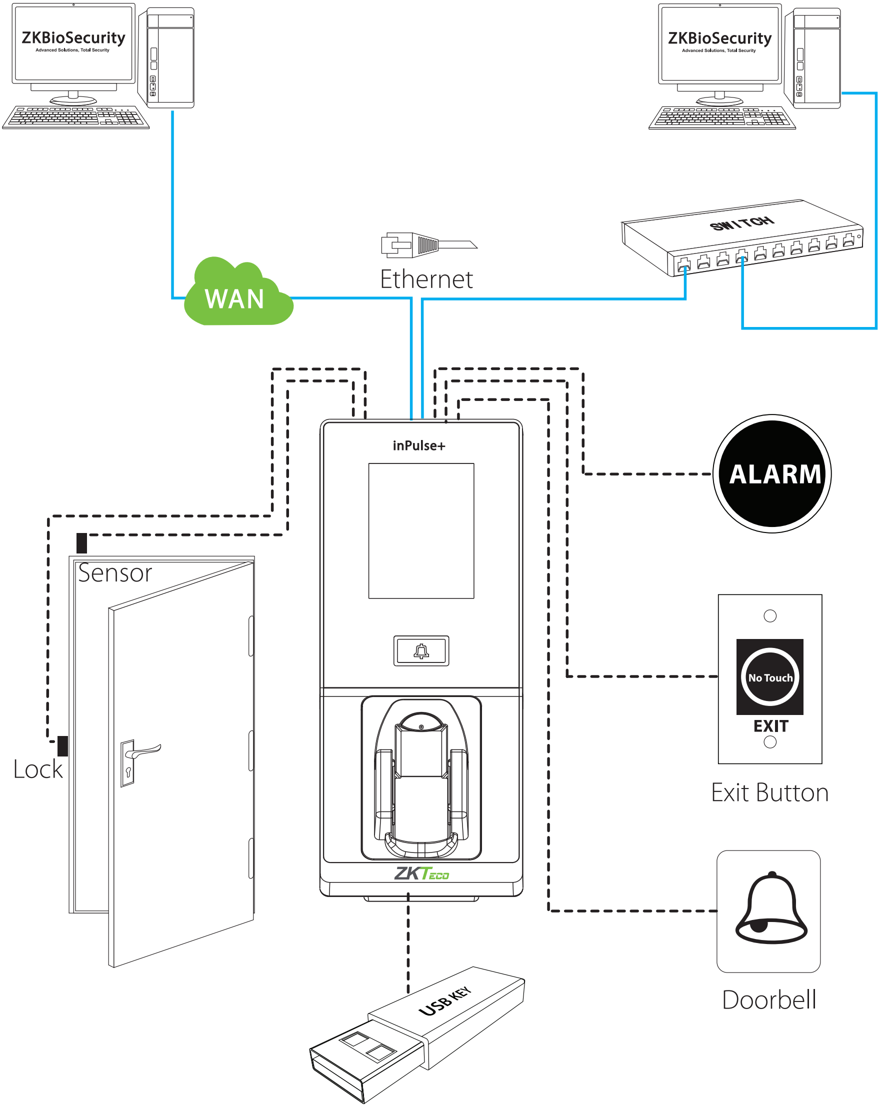
Wiegand Output Connection



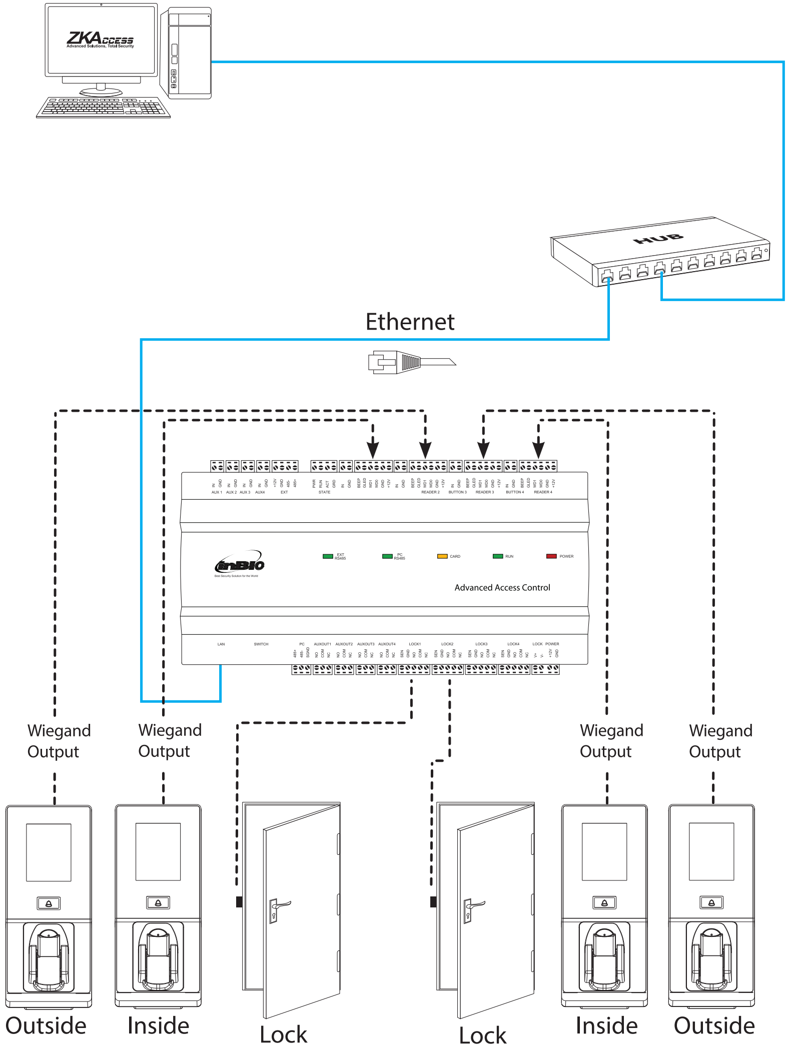
DESCRIPTION		WIRE	
WD0		Green	🟩
WD1		White	⬜
GND		Black	⬛
RXD	❌	Gray	▨
TXD	❌	Purple	🟪
GND	❌	Black	⬛
485A	❌	Blue	🟦
485B	❌	Yellow	🟨

❌ Do not use

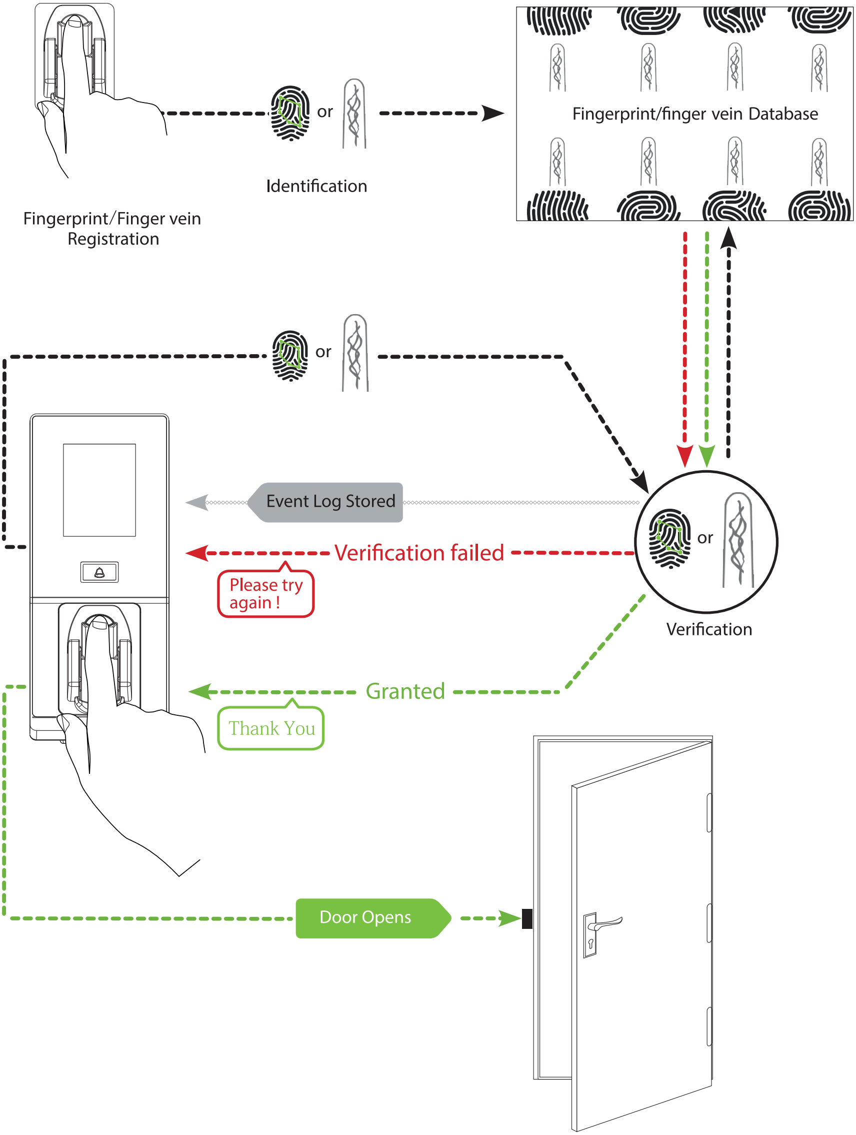
Standalone Installation



Wiegand Output Connection



How does inPulse/inPulse+ works

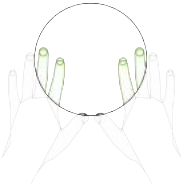


Registration and Verification

Note: During finger vein registration process, fingerprint of the selected finger is also registered

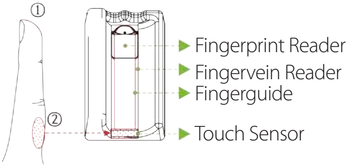
Select a finger to enroll

- It is recommended to use an index finger or a middle finger.
- Thumb, ring or little finger are relatively difficult to place in the correct position.

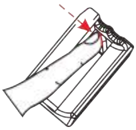
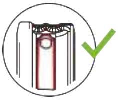
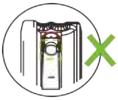
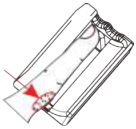
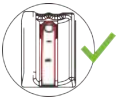
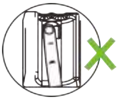
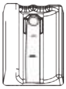
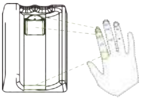


Fingerprint Placement Position

- In order to read your fingerprint and finger vein data touch the front side of finger vein reader with fingertip.
- The device starts collecting data once the finger root touches the finger vein reader



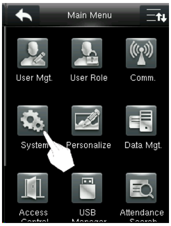
Verification Steps

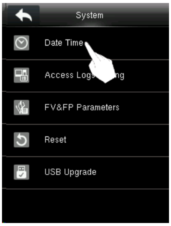
1 		
Touch the front side of finger vein reader with fingertip, then press your finger upon the finger vein reader.	Place the finger according to the finger guide.	Finger-tip must touch the front of finger vein reader in order to properly collect fingerprint and finger vein images.
2 		
Touch the reader with finger root.		Improper positioning of finger will affect the proper collection of fingerprint and finger vein images.
3 		The device starts collecting data once the finger root touches the finger vein reader. Remove finger after "beep" sound.

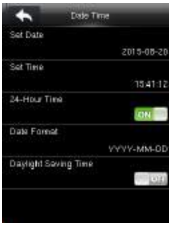
Note: Maintain the natural hand gesture.
Do not bend your fingers.
Do not exert finger to press the reader

Device Operation

Date/Time Settings



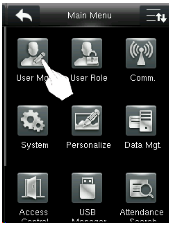


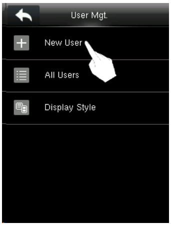


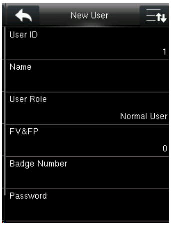
Set Date 2015-08-20
Set Time 15:41:12
24-Hour Time ON
Date Format YYYY-MM-DD
Daylight Saving Time OFF

Press ▦ icon to enter the Main Menu > System > Date Time to set date and time.

Adding User



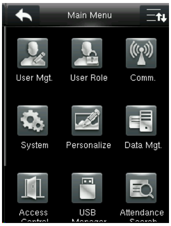


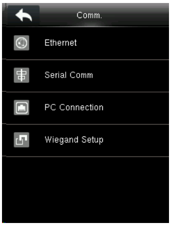


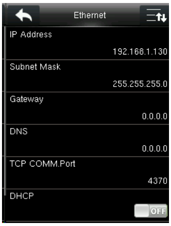
User ID 1
Name
User Role Normal User
FV&FP 0
Badge Number
Password

Press ▦ icon to enter the Main Menu > User Mgt. > New User to enter the New User adding interface. Settings include entering user ID, user role, choosing user role (Super Admin / Normal User), registering fingerprint & Fingervein★ / badge number★ / password, and setting access control role.

Ethernet Settings







IP Address 192.168.1.130
Subnet Mask 255.255.255.0
Gateway 0.0.0.0
DNS 0.0.0.0
TCP COMM.Port 4370
DHCP OFF

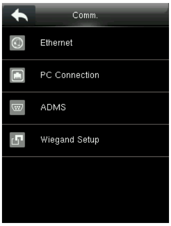
Press ▦ icon to enter the Main Menu > Comm. > Ethernet.

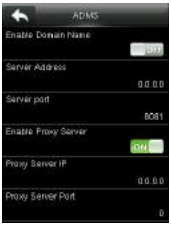
The parameters below are the system default values. Please adjust them according to the actual network.

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 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.

ADMS Settings




ADMS
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 ▦ 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.XYZ.com. XYZ denotes the domain name when this mode is on; when this mode is off, enter the IP address format in XYZ.

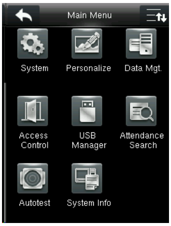
Server Address: Enter IP address of the ADMS server.

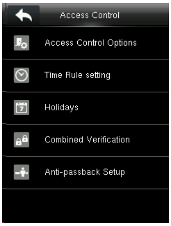
Server Port: Enter the port number used by the ADMS server.

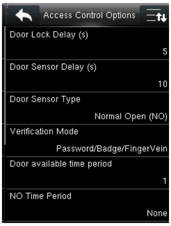
Enable Proxy Server: Method of enabling proxy. To enable proxy, please set the IP address and port number of the proxy server. Entering proxy IP and server address will be the same.

Note: To connect the device to ZKBioSecurity software, Ethernet and ADMS options must be set correctly.

Access Control Settings






Access Control Options
Door Lock Delay (s) 5
Door Sensor Delay (s) 10
Door Sensor Type Normal Open (NO)
Verification Mode Password/Badge/FingerVein
Door available time period 1
NO Time Period None

Press ▦ icon to enter the Main Menu, press > and ∨ to select Access Control.

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

1. User's access time must fall 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 Rule Setting: To set a maximum of 50 time rules. Each time rule consists of 10 spaces (7 spaces for one week and 3 holiday spaces), each space consists of 3 time periods.

Holidays: To set dates of holiday and the access control time zone for that holiday.

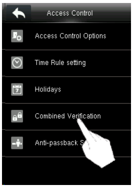
Combined Verification: To set access control combinations. A combination consists of a maximum of 5 access control groups.

Anti-Passback Setup: To prevent passing back which causes risks to security. Once this function is enabled, entry and exit records must be matched in order to open door. In Anti-Passback, Out Anti-Passback and In/Out Anti-Passback functions are available.

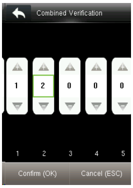
Access Control Combination Settings

E.g. : Add an access control combination which requires 2 person's verification from both Access Control Group 1 (set in User Management) and Access Control Group 2.

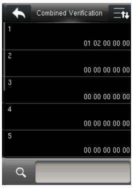
1



2



3



1 01 02 00 00 00

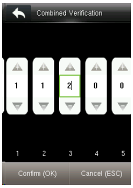
2 00 00 00 00 00

3 00 00 00 00 00

4 00 00 00 00 00

5 00 00 00 00 00

4



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:

A. 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).

B. If the combination is set as shown in figure 3, a user from access control group 2 must obtain verification of 2 users from access control group 1 in order to open door.

C. Set all group number to zero to reset access control combination.

Troubleshooting

1. "Invalid time zone" is displayed after verification?
   - ➪ Contact Administrator to check if the user has the privilege to gain access within that time zone.

2. Verification succeeds but the user cannot gain access?
   - ➪ Check whether the user privilege is set correctly.
   - ➪ Check whether the lock wiring is correct.

3. The Tamper Alarm rings?
   - ➪ To cancel the triggered alarm mode, carefully check whether the device and back plate are securely connected to each other, and reinstall the device properly if necessary.

ZKBioSecurity 3.0

It is recommended to install software version 3.0.3.0 or above

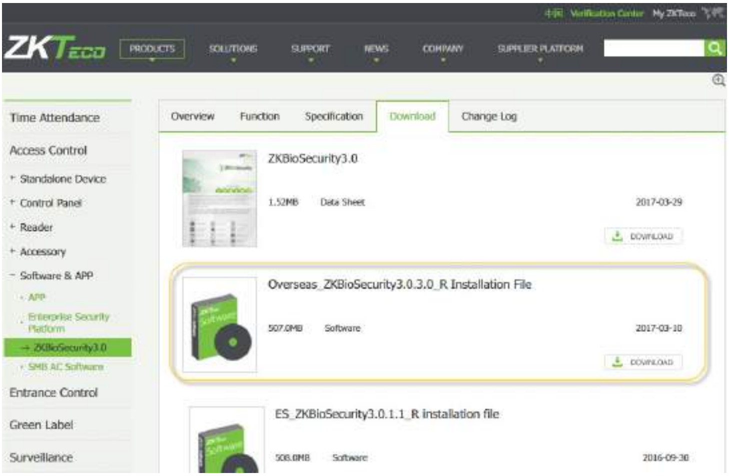
ZKTeco
ZKBioSecurity 3.0
✓ Easy to configure and use
✓ Door management
✓ Linkage settings
✓ Real time monitoring
✓ Maps, reports and maintenance
✓ SDK available for third-party integration

Installation & Setup

Downloading....................20
Installation....................21
Adding Device....................23
Creating a Time Zone....................25
Creating an Access Level....................26
Enrolling Personnel....................27
Wiegand Format....................29
Add & Delete Personnel to Access Level....................30
Real -Time Monitoring....................31
Exporting Reports....................32

Downloading

1. Go to http://www.zkteco.com/product/ZKBioSecurity3.0_421.html
2. Download the latest software and related files as required.



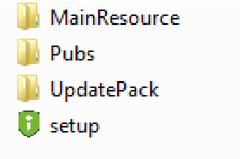
ZKBioSecurity3.0 — 1.52MB — Data Sheet — 2017-03-29

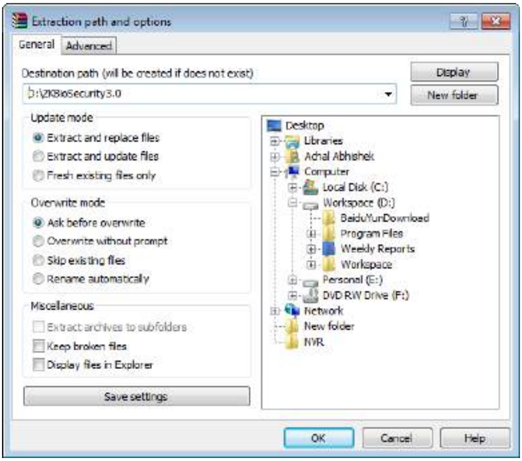
Overseas_ZKBioSecurity3.0.3.0_R Installation File — 507.0MB — Software — 2017-03-10

ES_ZKBioSecurity3.0.1.1_R installation file — 508.0MB — Software — 2016-09-30

3. Once downloaded, extract the .rar file to a new folder.

4. Click on setup to begin installstion.





Destination path (will be created if does not exist)

D:\ZKBioSecurity3.0

Update mode

- ● Extract and replace files
- ○ Extract and update files
- ○ Fresh existing files only

Overwrite mode

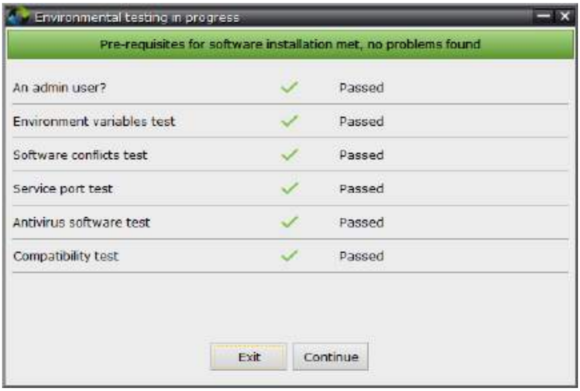
- ● Ask before overwrite
- ○ Overwrite without prompt
- ○ Skip existing files
- ○ Rename automatically

Miscellaneous

- □ Extract archives to subfolders
- □ Keep broken files
- □ Display files in Explorer

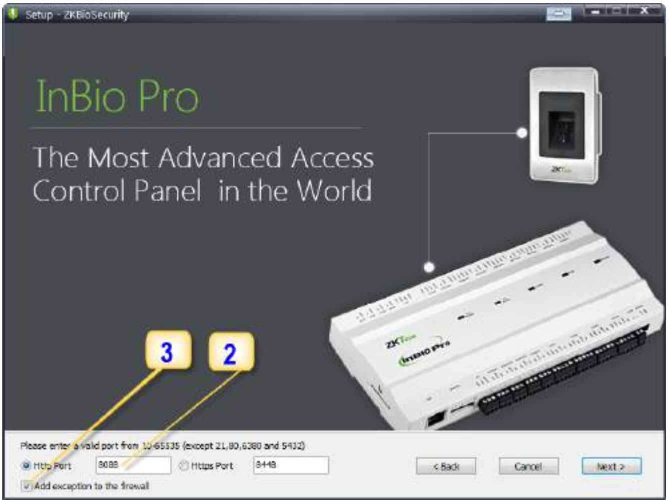
Installation

1. System will check the requirements to install the software. Click *Continue* if all tests are passed, else check the issues and re-test.



Pre-requisites for software installation met, no problems found

An admin user?	✓	Passed
Environment variables test	✓	Passed
Software conflicts test	✓	Passed
Service port test	✓	Passed
Antivirus software test	✓	Passed
Compatibility test	✓	Passed



Please enter a valid port from 10-65535 (except 21,80,6380 and 5432)

● Http Port 8088 ○ Https Port 8443

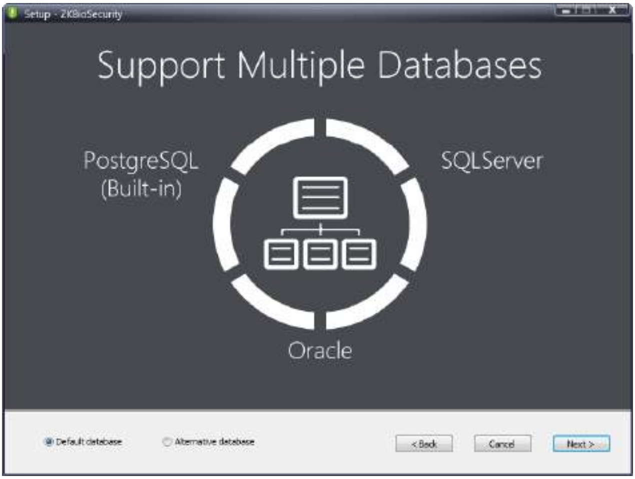
☑ Add exception to the firewall

2. Add an open port (Default 8088) or ask a network administrator for an open port.
   Note: Stanalone device doesn't support https.

3. Click the check box to add firewall exception for this port.

Installation

4. Select the mode of database. The default will be PostgreSQL, if you want to select any other database, then select *Alternative database*.

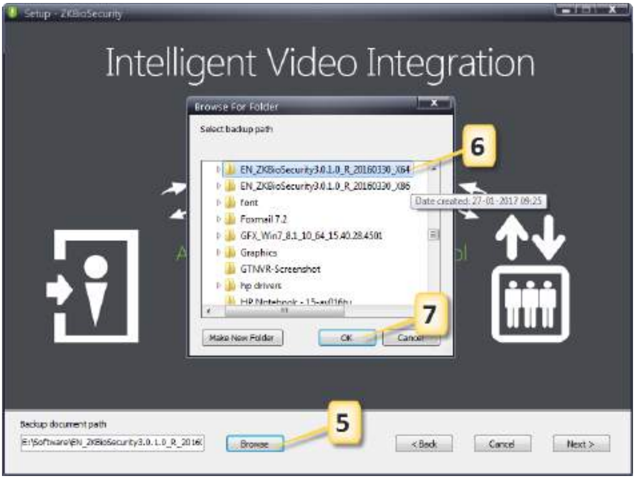


● Default database ○ Alternative database

5. Click Browse and choose or create a folder to store your backup files.

6. Select/Create the required folder.

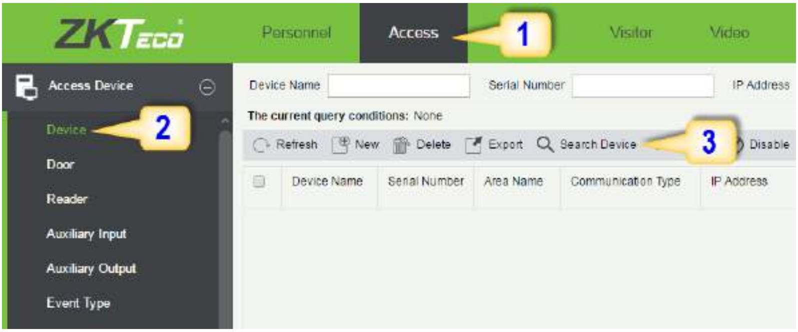
7. Click OK.



Backup document path: E:\Software\EN_ZKBioSecurity3.0.1.0_R_2016(

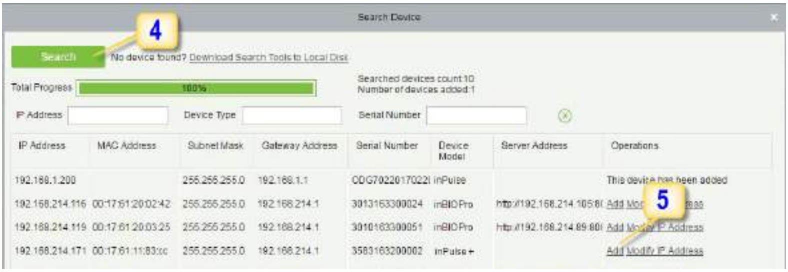
Adding Device

1. Click on *Access* to get below interface of Access Module of the software.



2. Click on *Device.*

3. Click on *Search Device.*



No device found? Download Search Tools to Local Disk

Total Progress 100%

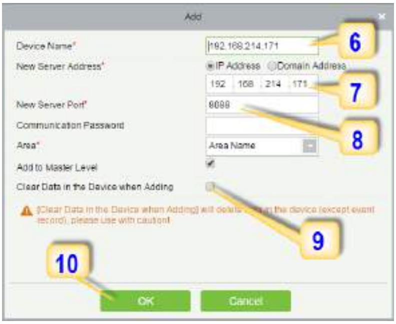
Searched devices count:10
Number of devices added:1

IP Address | Device Type | Serial Number

IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Device Model	Server Address	Operations
192.168.1.200		255.255.255.0	192.168.1.1	ODG7022017022I	inPulse		This device has been added
192.168.214.116	00:17:61:20:02:42	255.255.255.0	192.168.214.1	3013163300024	inBIOPro	http://192.168.214.105:8(	Add Mo[illegible]ess
192.168.214.119	00:17:61:20:03:25	255.255.255.0	192.168.214.1	3010163300051	inBIOPro	http://192.168.214.89:80(	Add Modify IP Address
192.168.214.171	00:17:61:11:83:cc	255.255.255.0	192.168.214.1	3583163200002	inPulse+		Add Modify IP Address

4. Click *Search* to search all the sandalone devices on the network.

5. From the list, click *Add* to add the required device.



Device Name* 192.168.214.171

New Server Address* ● IP Address ○ Domain Address

192 . 168 . 214 . 171

New Server Port* 8088

Communication Password

Area* Area Name

Add to Master Level ☑

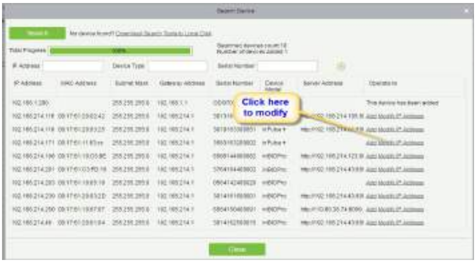
Clear Data in the Device when Adding □

⚠ [Clear Data in the Device when Adding] will delete [illegible] in the device (except event record), please use with caution!

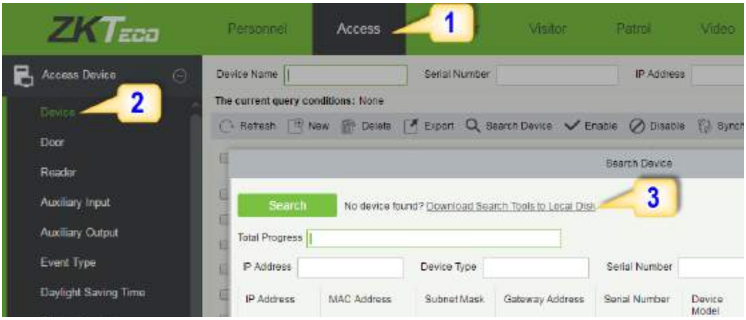
Adding Device

6. Enter a unique name.
7. Enter the IP address of current system (PC).
8. Enter the access point of system.
9. Click on this option, after adding device, the system will clear all data in the device (except the event logs).
10. Click OK to finish.

The default IP address may conflict with the device IP of other devices. In order to avoid that problem, modify the IP address as shown below:



When the device is not in the same network with server, customers should download the tool and search the device as shown below:



Device Name | Serial Number | IP Address

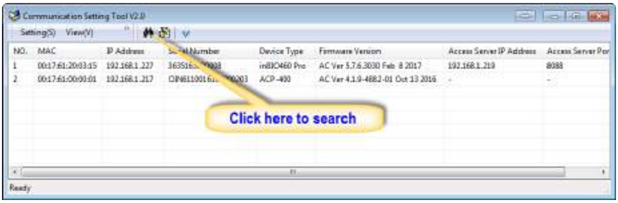
The current query conditions: None

No device found? Download Search Tools to Local Disk

Total Progress

IP Address | Device Type | Serial Number

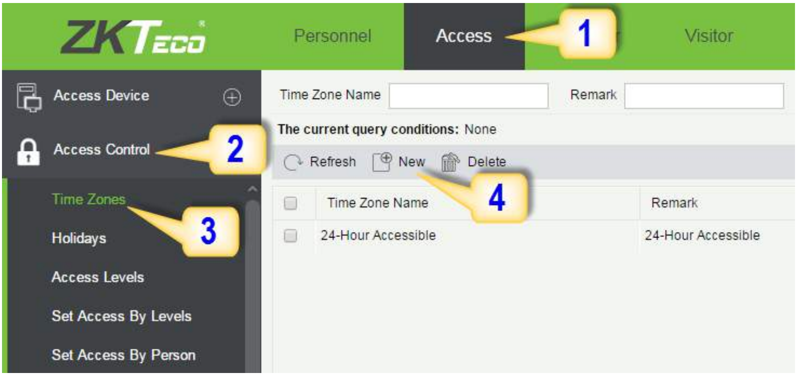
IP Address | MAC Address | Subnet Mask | Gateway Address | Serial Number | Device Model



NO.	MAC	IP Address	Serial Number	Device Type	Firmware Version	Access Server IP Address	Access Server Por
1	00:17:61:20:03:15	192.168.1.227	363516[illegible]0008	inBIO460 Pro	AC Ver 5.7.6.3030 Feb 8 2017	192.168.1.219	8088
2	00:17:61:00:00:01	192.168.1.217	OIN611001612[illegible]00203	ACP-400	AC Ver 4.1.9-4882-01 Oct 13 2016	-	-

Creating a Time Zone

Click Access Control > Time Zones > Add to access the time zone.

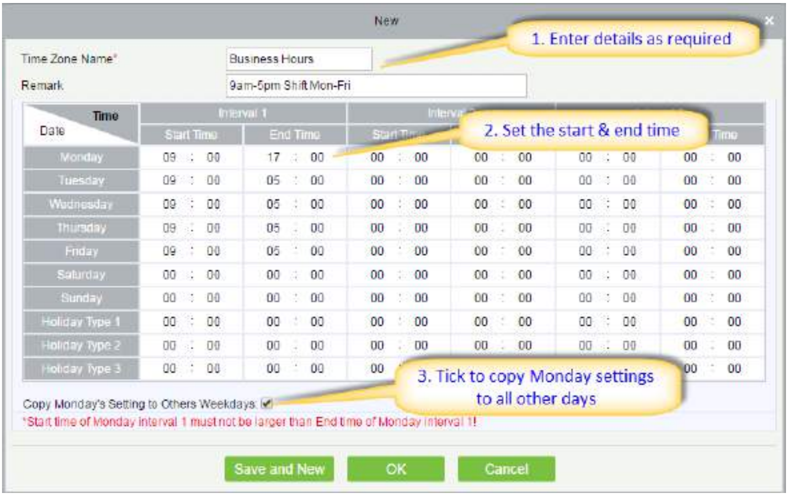


Time Zone Name | Remark

The current query conditions: None

□	Time Zone Name	Remark
□	24-Hour Accessible	24-Hour Accessible

After setting the time zone, click *OK* to save, and the time zone will appear in the list.


New
1. Enter details as required
2. Set the start & end time
3. Tick to copy Monday settings to all other days
Save and New
OK
Cancel

Time Zone Name* Business Hours

Remark 9am-5pm Shift Mon-Fri

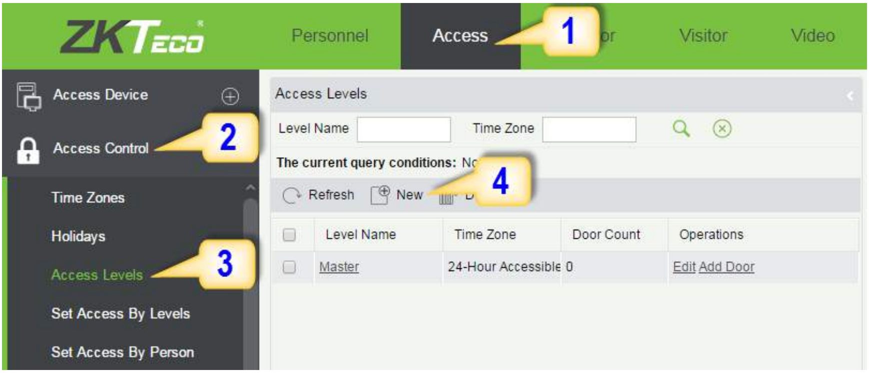
Time / Date	Interval 1		Interva			
	Start Time	End Time	Start T			Time
Monday	09 : 00	17 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Tuesday	09 : 00	05 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Wednesday	09 : 00	05 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Thursday	09 : 00	05 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Friday	09 : 00	05 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Saturday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Sunday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 1	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 2	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 3	00 : 00	00 : 00	00			00 : 00

Copy Monday's Setting to Others Weekdays: ☑

*Start time of Monday interval 1 must not be larger than End time of Monday interval 1!

Creating an Access Level

1. Click Access **2.** Click Access Control **3.** Click Access Levels **4.** Click New.



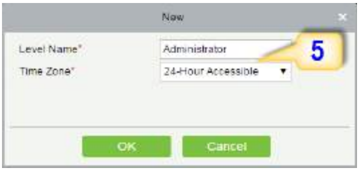
Access Levels

Level Name Time Zone

The current query conditions: No

□	Level Name	Time Zone	Door Count	Operations
□	Master	24-Hour Accessible	0	Edit Add Door

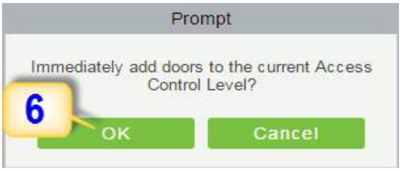
5. Enter the details and click *OK.*



Level Name* Administrator

Time Zone* 24-Hour Accessible

6. You need to add doors to the access levels.

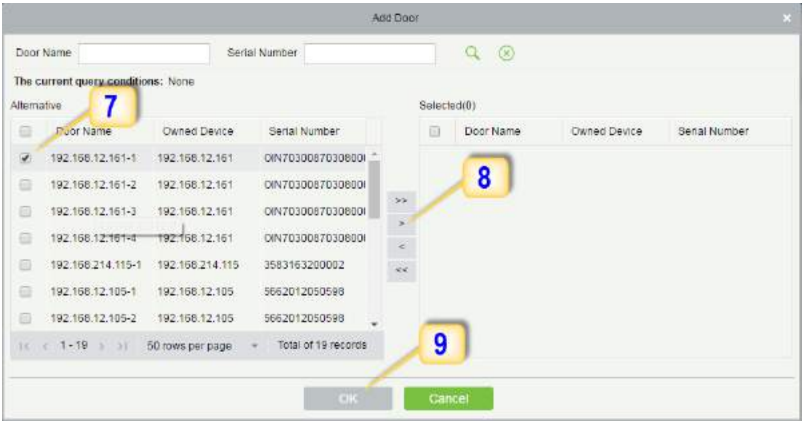


Immediately add doors to the current Access Control Level?

7. Select the required door(s).

8. Move the selected door(s).

9. Click *OK* to finish adding doors.



Door Name Serial Number

The current query conditions: None

Alternative

□	Door Name	Owned Device	Serial Number
☑	192.168.12.161-1	192.168.12.161	OIN7030087030800(
□	192.168.12.161-2	192.168.12.161	OIN7030087030800(
□	192.168.12.161-3	192.168.12.161	OIN7030087030800(
□	192.168.12.161-4	192.168.12.161	OIN7030087030800(
□	192.168.214.115-1	192.168.214.115	3583163200002
□	192.168.12.105-1	192.168.12.105	5662012050598
□	192.168.12.105-2	192.168.12.105	5662012050598

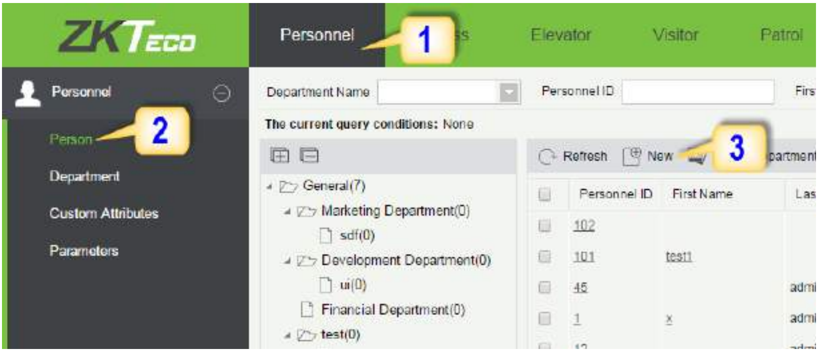
1 - 19 50 rows per page Total of 19 records

Selected(0)

□	Door Name	Owned Device	Serial Number

Enrolling Personnel

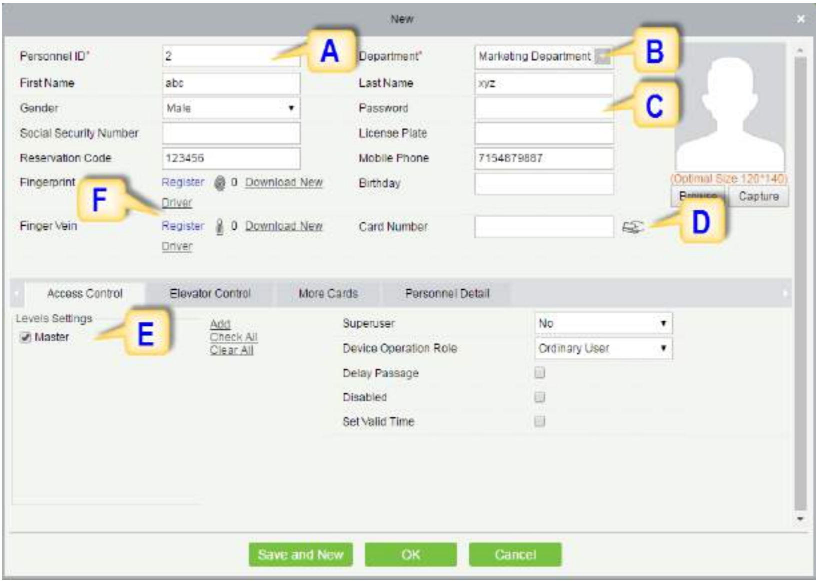
1. Click Personnel **2.** Click Person **3.** Click *New* to add personnel.



The current query conditions: None

- General(7)
  - Marketing Department(0)
    - sdf(0)
  - Development Department(0)
    - ui(0)
  - Financial Department(0)
  - test(0)

□	Personnel ID	First Name	Las
□	102		
□	101	test1	
□	45		admi
□	1	x	admi



Personnel ID*	2	Department*	Marketing Department
First Name	abc	Last Name	xyz
Gender	Male	Password	
Social Security Number		License Plate	
Reservation Code	123456	Mobile Phone	7154879887
Fingerprint	Register 0 Download New Driver	Birthday	
Finger Vein	Register 0 Download New Driver	Card Number	

Levels Settings
☑ Master
Add
Check All
Clear All

Superuser	No
Device Operation Role	Ordinary User
Delay Passage	□
Disabled	□
Set Valid Time	□

A. Personnel ID: It must be a unique 9 characters length with the valid range of 1-79999999. It can be configured based on actual conditions. The Personnel No. contains only numbers by default but may also include letters after setting parameters.

Enrolling Personnel

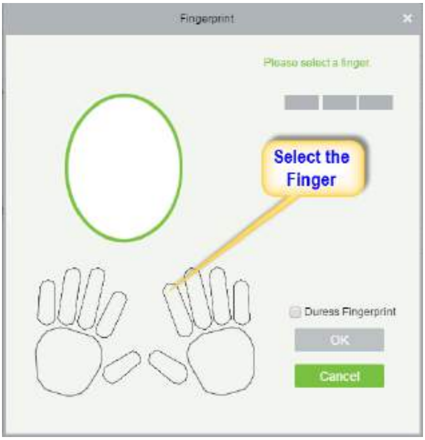
B. Department: Select from the pull-down menu and click *OK*. If the department was not set previously, you can only select the default [Company Name] department.

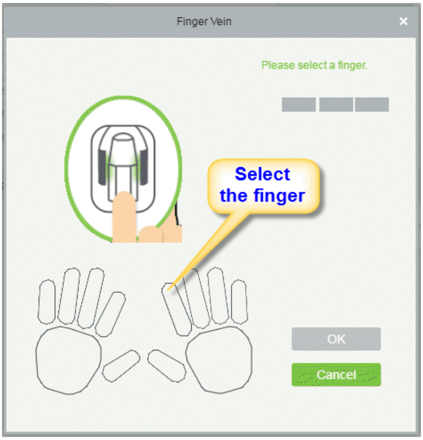
C. Password: Set personnel password. It only supports 6-digit passwords. If password exceeds the specified length, the system will truncate it automatically. It can't be same with duress or other passwords.

D. Card Number: You can add a card number through manual entry or a card issuer. For issuing through issuer, click on the card icon directly. For issuing card manually, you must enter both the card number and the site code, then the software converts the numbers to the card number for access control system verification.

E. Access Control: Here you will get all the access levels created by you and by default. Tick the required box.

F. Fingerprint/Fingervein: Enroll the Personnel Fingerprint/Fingervein or Duress Fingerprint. Duress Fingerprint is to trigger the alarm and send the signal to the system in case of emergency.

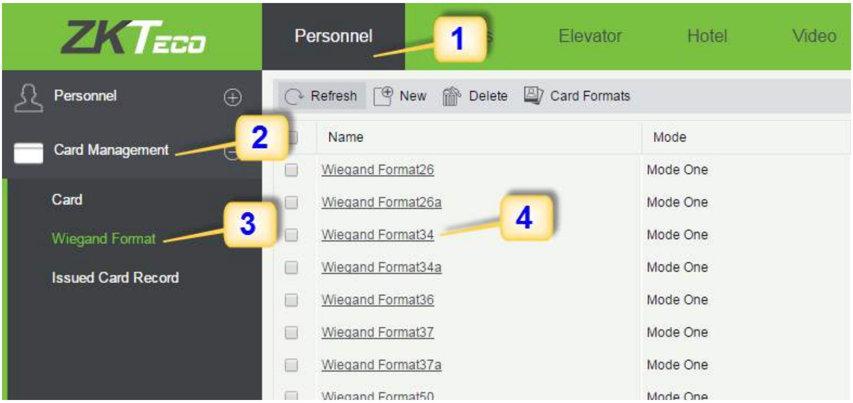




Wiegand Format

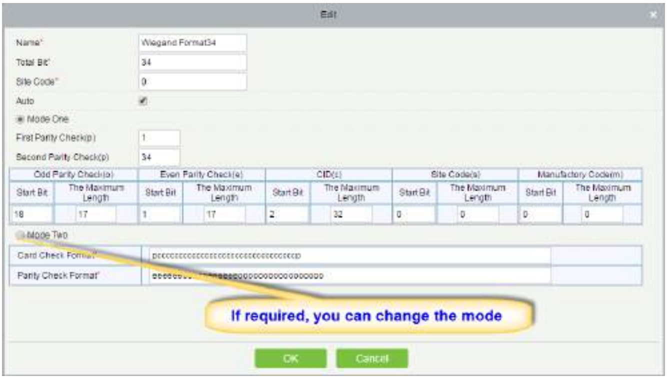
Wiegand Format is the card format that can be identified by Wiegand reader. The software is embedded with 10 Wiegand formats. You may set the Wiegand card format as required.

1. Click Personnel **2.** Click Card Management **3.** Click Wiegand Format.
4. Taking Wiegnad Format34 as an example. Click to edit.



Name	Mode
Wiegand Format26	Mode One
Wiegand Format26a	Mode One
Wiegand Format34	Mode One
Wiegand Format34a	Mode One
Wiegand Format36	Mode One
Wiegand Format37	Mode One
Wiegand Format37a	Mode One
Wiegand Format50	Mode One

This software supports two modes for adding Wiegand Format, if mode 1 does not meet your setting requirement, switch to mode 2.



Name*	Wiegand Format34
Total Bit*	34
Site Code*	0
Auto	☑

● Mode One

First Parity Check(p)	1
Second Parity Check(p)	34

Odd Parity Check(o)		Even Parity Check(e)		CID(c)		Site Code(s)		Manufactory Code(m)	
Start Bit	The Maximum Length	Start Bit	The Maximum Length	Start Bit	The Maximum Length	Start Bit	The Maximum Length	Start Bit	The Maximum Length
18	17	1	17	2	32	0	0	0	0

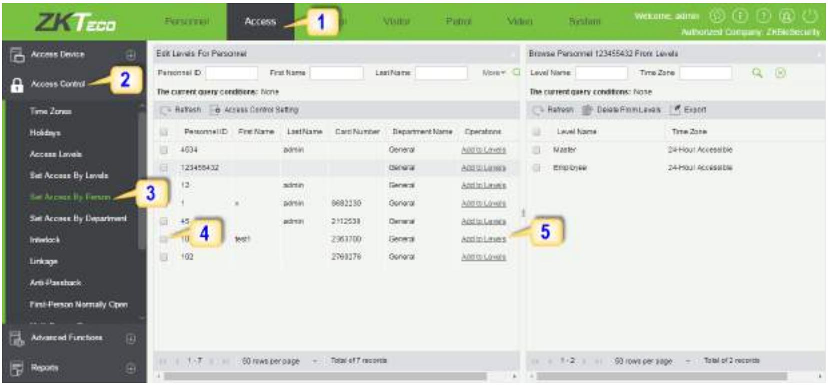
○ Mode Two

Card Check Format*	pccccccccccccccccccccccccccccccccp
Parity Check Format*	eeeeee[illegible]eeeeoooooooooooooooooo

p indicates Parity Position, s indicates Site Code, c indicates Cardholder ID, f indicates Facility Code, m indicates Manufactory Code, e indicates Even Parity, O indicates Odd Parity, b indicates both odd check and even check, x indicates parity bits no check.

Add & Delete Personnel to Access Level

1. Click Access **2.** Access Control **3.** Set Access by Person **4.** Click on the required employee **5.** Click Add to Levels.



Edit Levels For Personnel

Personnel ID: First Name: Last Name: More▾

The current query conditions: None

□	Personnel ID	First Name	Last Name	Card Number	Department Name	Operations
□	4634		admin		General	Add to Levels
□	123456432				General	Add to Levels
□	12		admin		General	Add to Levels
□	1	x	admin	8682230	General	Add to Levels
□	45		admin	2112538	General	Add to Levels
□	10	test1		2363700	General	Add to Levels
□	102			2769276	General	Add to Levels

1-7 50 rows per page Total of 7 records

Browse Personnel 123455432 From Levels

Level Name: Time Zone:

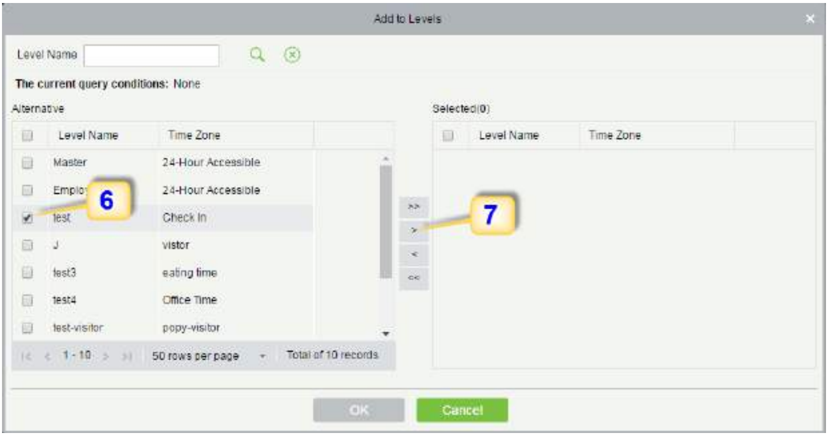
The current query conditions: None

□	Level Name	Time Zone
□	Master	24-Hour Accessible
□	Employee	24-Hour Accessible

1-2 50 rows per page Total of 2 records

6. Select Level(s).

7. Click to move the selected level(s) to the right, and then click OK to complete adding. The added level(s) will appear in the list on to the right side.



Add to Levels

Level Name

The current query conditions: None

Alternative

□	Level Name	Time Zone
□	Master	24-Hour Accessible
□	Emplo	24-Hour Accessible
☑	test	Check In
□	J	vistor
□	test3	eating time
□	test4	Office Time
□	test-visitor	popy-visitor

1-10 50 rows per page Total of 10 records

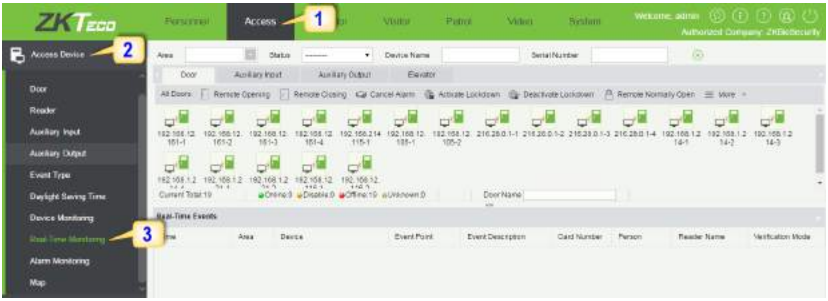
Selected(0)

□	Level Name	Time Zone

Real -Time Monitoring

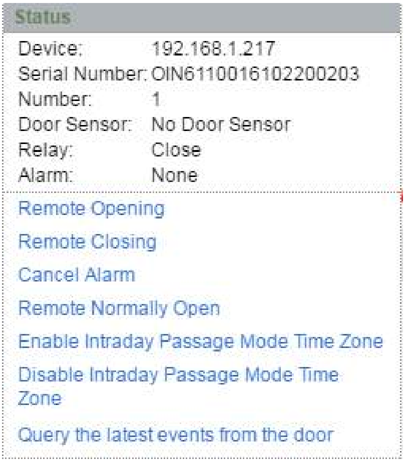
1. Click Access **2.** Click Access Device **3.** Click Real-Time Monitoring

Real-time monitor the status and real-time events of standalone in the system, including normal events and abnormal events (including alarm events) device transactions.



You can also filter by Area, device name, Serial number to check a specific device transactions or all at once.

Hover over a door icon to open pop up menu as shown below and click Remote Closing, Remote Opening, or Cancel Alarm and more.



Status

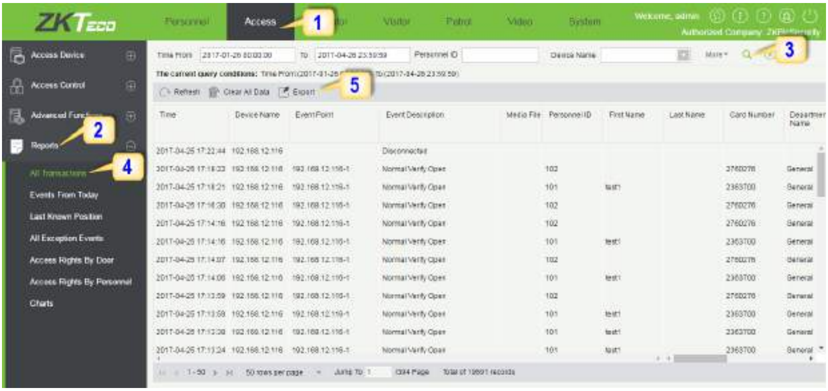
Device: 192.168.1.217
Serial Number: OIN6110016102200203
Number: 1
Door Sensor: No Door Sensor
Relay: Close
Alarm: None

Remote Opening
Remote Closing
Cancel Alarm
Remote Normally Open
Enable Intraday Passage Mode Time Zone
Disable Intraday Passage Mode Time Zone
Query the latest events from the door

Exporting Reports

Access Module:

1. Click Access **2.** Click Reports **3.** Filter the data (time, Personnel ID, Device Name and more) if required and click on search **4.** Click All transactions or as required.



Time From 2017-01-26 00:00:00 To 2017-04-26 23:59:59 Personnel ID Device Name

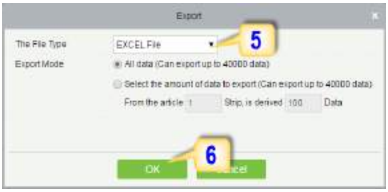
The current query conditions: Time From(2017-01-26 ... To(2017-04-26 23:59:59)

Time	Device Name	Event Point	Event Description	Media File	Personnel ID	First Name	Last Name	Card Number	Department Name
2017-04-25 17:22:44	192.168.12.116		Disconnected						
2017-04-25 17:18:33	192.168.12.116	192.168.12.116-1	Normal Verify Open		102			2760276	General
2017-04-25 17:18:21	192.168.12.116	192.168.12.116-1	Normal Verify Open		101	test1		2363700	General
2017-04-25 17:16:30	192.168.12.116	192.168.12.116-1	Normal Verify Open		102			2760276	General
2017-04-25 17:14:18	192.168.12.116	192.168.12.116-1	Normal Verify Open		102			2760276	General
2017-04-25 17:14:16	192.168.12.116	192.168.12.116-1	Normal Verify Open		101	test1		2363700	General
2017-04-25 17:14:07	192.168.12.116	192.168.12.116-1	Normal Verify Open		102			2760276	General
2017-04-25 17:14:06	192.168.12.116	192.168.12.116-1	Normal Verify Open		101	test1		2363700	General
2017-04-25 17:13:59	192.168.12.116	192.168.12.116-1	Normal Verify Open		102			2760276	General
2017-04-25 17:13:58	192.168.12.116	192.168.12.116-1	Normal Verify Open		101	test1		2363700	General
2017-04-25 17:13:30	192.168.12.116	192.168.12.116-1	Normal Verify Open		101	test1		2363700	General
2017-04-25 17:13:24	192.168.12.116	192.168.12.116-1	Normal Verify Open		101	test1		2363700	General

1-50 50 rows per page Jump To 1 /394 Page Total of 19691 records

5. Click on *Export* to get the list.

6. Click OK.

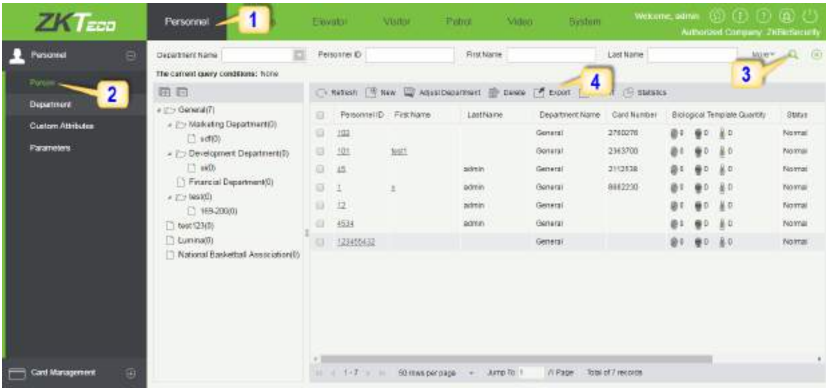


The File Type: EXCEL File

Export Mode:
● All data (Can export up to 40000 data)
○ Select the amount of data to export (Can export up to 40000 data)
From the article 1 Strip, is derived 100 Data

Personnel Module:

1. Click Personnel **2.** Click Person **3.** Filter the data (Department, Personnel ID, and more) if required and click on search **4.** Click on Export to get the list.



Department Name Personnel ID First Name Last Name

The current query conditions: none

□	Personnel ID	First Name	Last Name	Department Name	Card Number	Biological Template Quantity	Status
□	102			General	2760276	1 0 0	Normal
□	101	test1		General	2363700	1 0 0	Normal
□	15		admin	General	2112538	1 0 0	Normal
□	1	1	admin	General	8882230	1 0 0	Normal
□	12		admin	General		1 0 0	Normal
□	4534		admin	General		1 0 0	Normal
□	123455432			General		1 0 0	Normal

1-7 50 rows per page Jump To 1 /1 Page Total of 7 records

6 Kingsbridge Road, Suite 8
Fairfield, NJ 07004
T: +1 862 505 2101
sales@zkaccess.com
www.zkaccess.com

ZKAccess-division of ZKTeco