User Manual

ProRF

Version: 1.1

Date: April 2024

Green Label

Copyright © 2024 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect,

special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **ProRF**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Contents

1 Overview 1

1.1 Appearance 1

1.2 Terminal Description 2

1.3 Wiring Description 3

1.3.1 Power Connection 3

1.3.2 Ethernet Connection 3

1.3.3 Lock Relay Connection 4

1.3.4 Door Sensor, Exit Button, Bell & Alarm Connection 5

1.3.5 RS485 Connection 5

1.3.6 RS232 Connection (Optional) 6

1.3.7 Wiegand Output Connection 6

1.3.8 Wiegand Input Connection 6

1.4 Installation 7

2 Connect to Webserver 8

2.1 Login Webserver 8

2.2 Forgot Password 9

2.3 Device 9

2.4 Device Setup 10

2.4.1 Communication Settings 10

2.4.2 Cloud Service Setup 11

2.4.3 System Settings 12

2.4.4 Date Setup 12

2.4.5 Wiegand Setup 13

2.5 Device Management 15

2.5.1 Device Management 15

2.5.2 Updata Firmware 16

2.5.3 Change Password 17

2.5.4 Operation Log 17

3 Connect to ZKBio CVSecurity Software 18

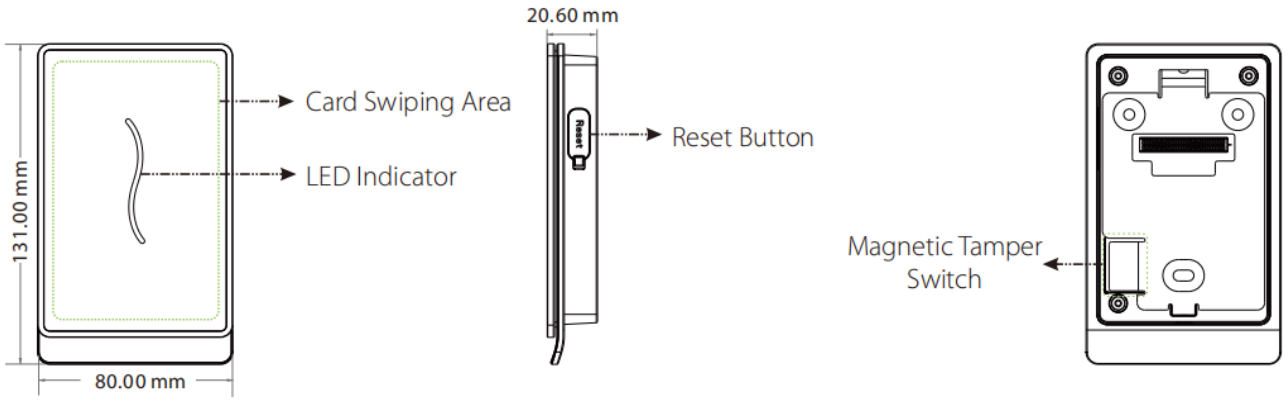
3.1 Set the Communication Address 18
3.2 Add Device on the Software 19
3.3 Add Personnel on the Software and Card Registration 20
3.4 Set Access Levels 21
3.5 Set Access by Levels 24
3.6 Synchronize All Data to Devices 26
3.7 Real-Time Monitoring 28
CE Note 29
FCC Warning 30
Eco-friendly Operation 31

1 Overview

ProRF is an elegantly designed RFID access control terminal. Its IP67 water-proof & dust-proof level enables direct outdoor installation, and is even able to normally operate under extreme weather conditions in a temperature range of -20°C~65°C.

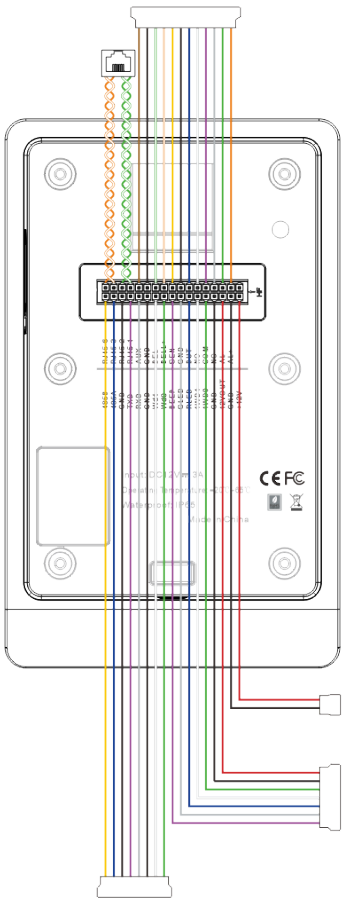
As an advanced terminal, ProRF is equipped with 2 relays of lock, alarm control, SRB for enhanced security, and auxiliary smoke detection input for fire security linkage. Its large storage capacity of up to 100,000 users/cards and 600,000 transactions is perfectly applicable to mega-size enterprise.

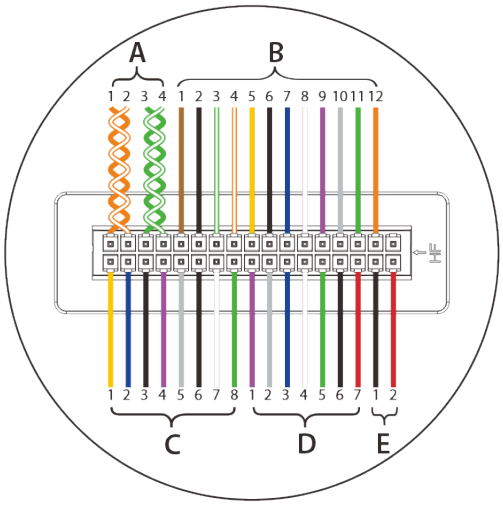
1.1 Appearance



Name	Description
LED Indicator	• Green flashes once in a second: standby status. • Green glows continuously for 2 seconds: authentication success • Red glows continuously for 2 seconds: authentication failure
Reset	Reboot the device: press the reset button and hold it for 3 seconds.
Magnetic Tamper Switch	• Restore factory settings • Tamper Switch: keep the magnetic tamper switch on the back plate, or it will trigger the tamper alarm.

1.2 Terminal Description





PIN	DESCRIPTION	WIRE
D1	BEEP	Purple
D2	GLED	Gray
D3	RLED	Blue
D4	IWD1	White
D5	IWD0	Green
D6	GND	Black
D7	12VOUT	Red
E1	GND	Black
E2	+12V	Red

PIN	DESCRIPTION	WIRE
A1	RJ45-6	Orange
A2	RJ45-3	Orange+White
A3	RJ45-2	Green
A4	RJ45-1	Green+White
B1	AUX	Brown
B2	GND	Black
B3	BELL-	Green+White
B4	BELL+	Orange+White
B5	SEN	Yellow
B6	GND	Black
B7	BUT	Blue
B8	NO	White
B9	COM	Purple
B10	NC	Gray
B11	AL-	Green
B12	AL+	Orange
C1	485B	Yellow
C2	485A	Blue
C3	GND	Black
C4	TXD	Purple
C5	RXD	Gray
C6	GND	Black
C7	WD1	White
C8	WD0	Green

1.3 Wiring Description

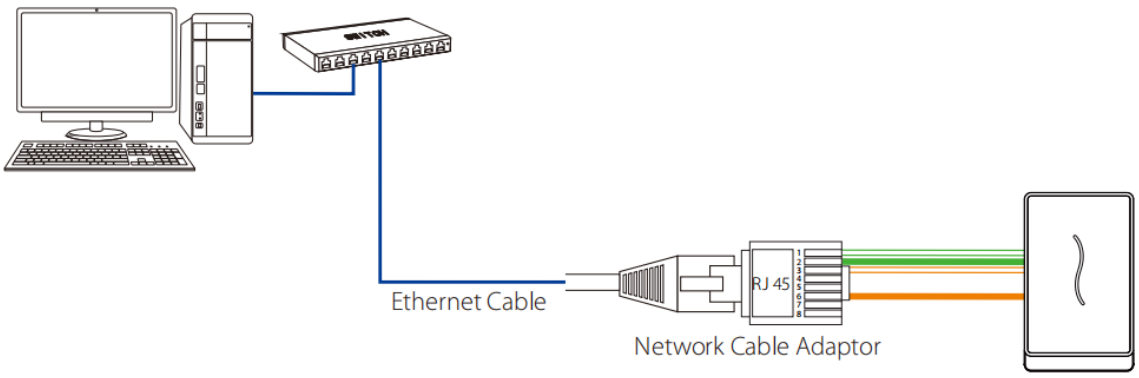
1.3.1 Power Connection

Recommended power supply

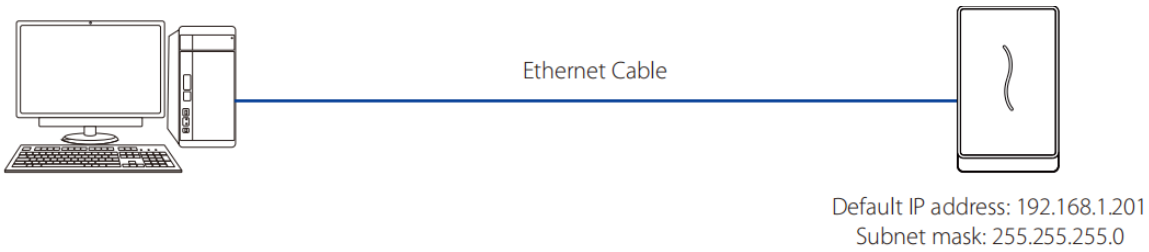
- 12V ± 10%, at least 3000mA.
- To share the device's power with other devices, use a power supply with higher current ratings.

1.3.2 Ethernet Connection

1) The device connects to the computer over an Ethernet through a switch.



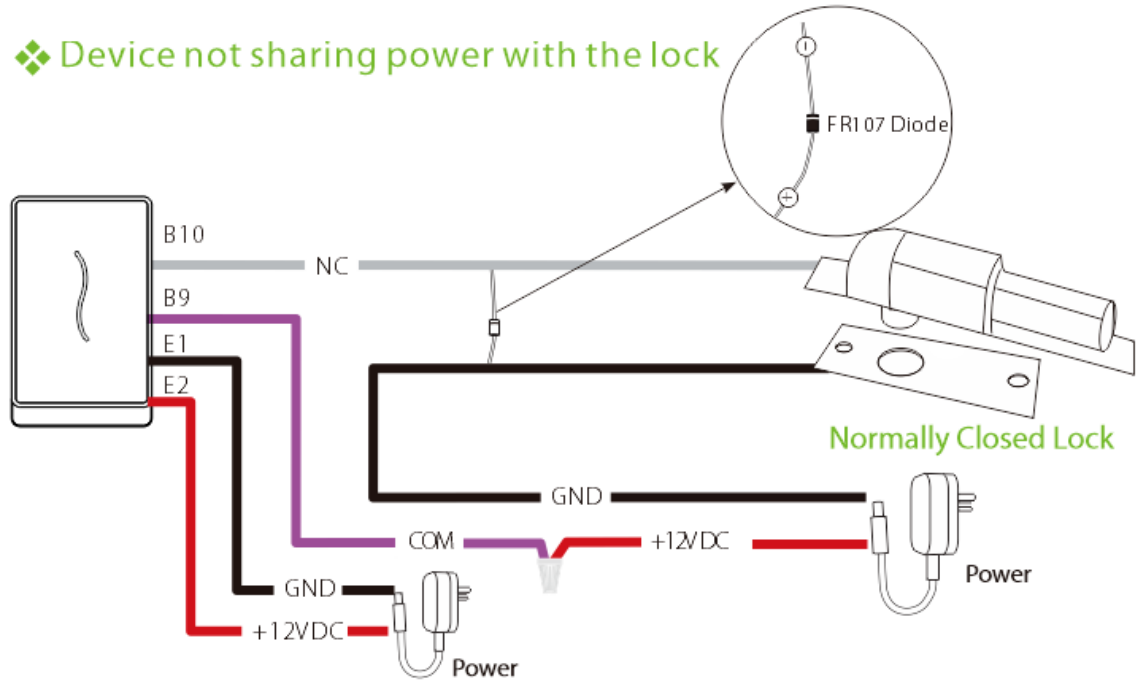
2) The device directly connects to the computer.

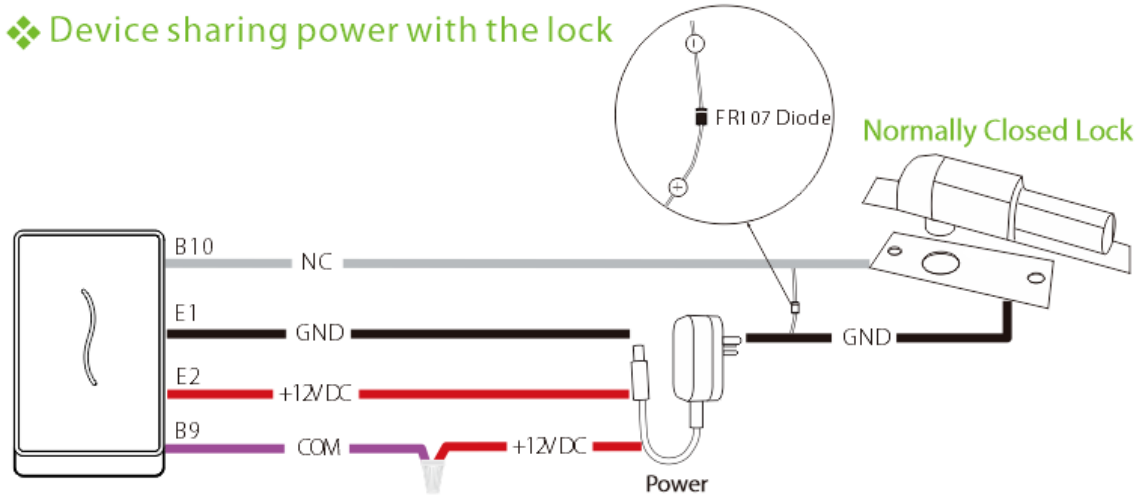


1.3.3 Lock Relay Connection

The system supports Normally Opened Lock and Normally Closed Lock.

Take Normally Closed Lock as an example below:





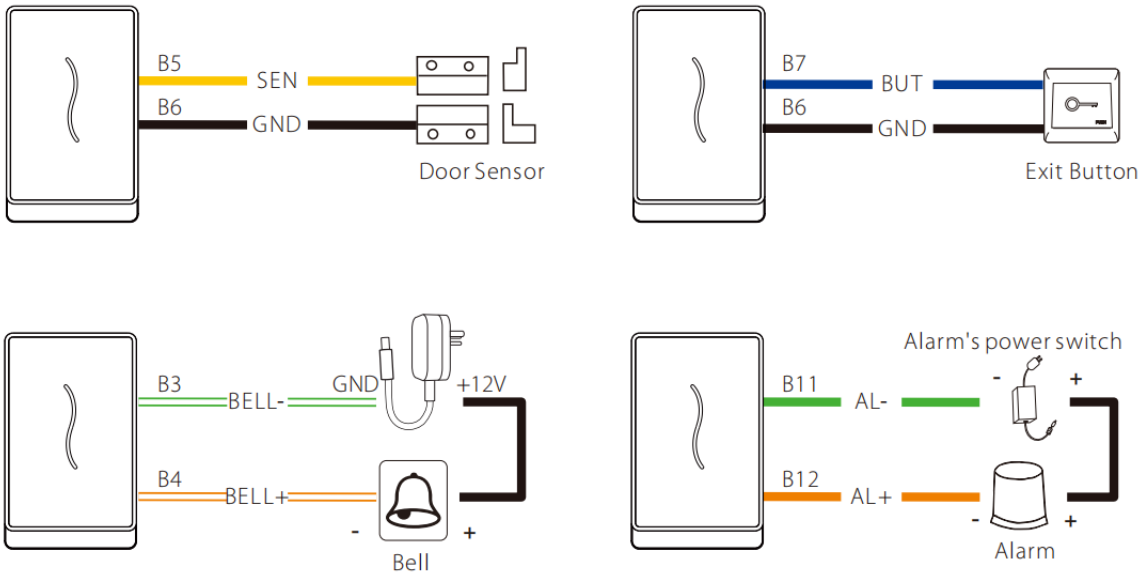
Notes:

1. The system supports Normally Opened Lock and Normally Closed Lock. The NO LOCK (normally

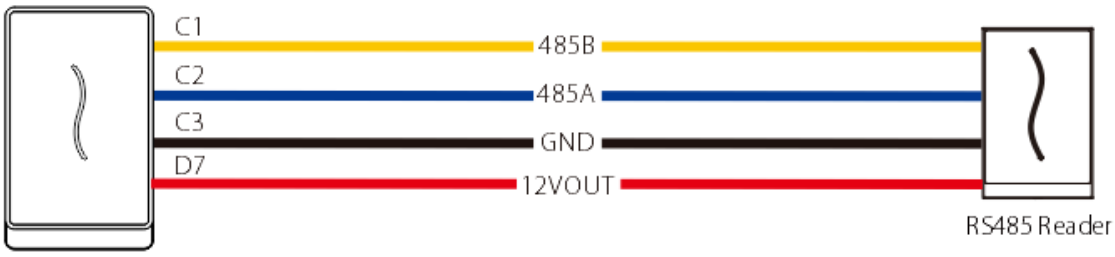
opened at power on) is connected with 'NO' and 'COM' terminals, and the NC LOCK (normally closed at power on) is connected with 'NC' and 'COM' terminals.

2. When electrical lock is connected to the Access Control System, you must add one FR107 diode in parallel (equipped in the package) to prevent the self-inductance EMF from affecting the system.
3. If you want the device and the lock to share a common power, split the power into two sets of wires out, one connecting to the device and one connecting to the lock.
4. The 12VOUT terminal of the device is only used to power the reader or SRB, not the lock.

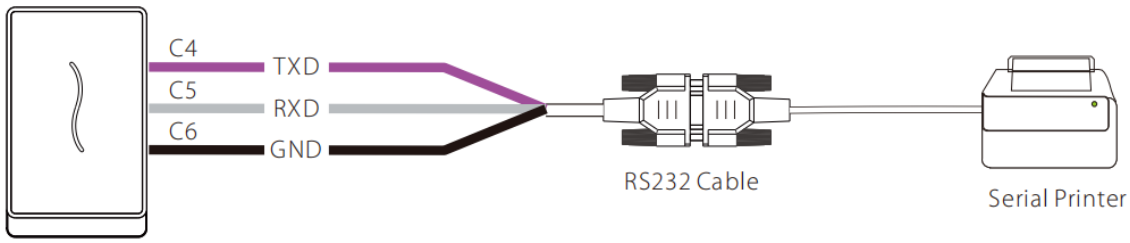
1.3.4 Door Sensor, Exit Button, Bell & Alarm Connection



1.3.5 RS485 Connection

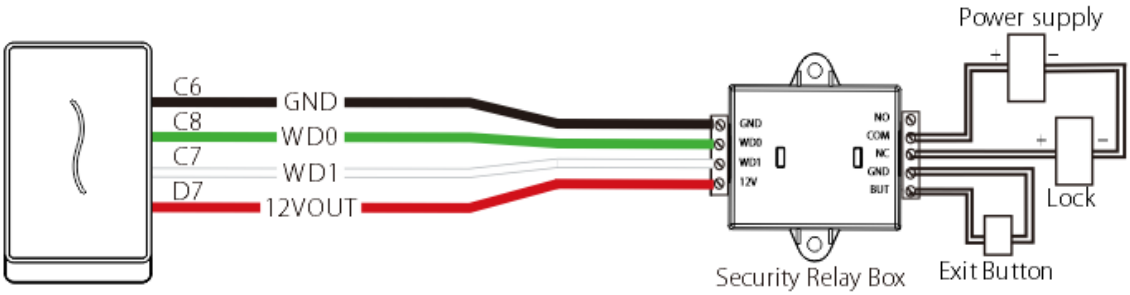


1.3.6 RS232 Connection (Optional)

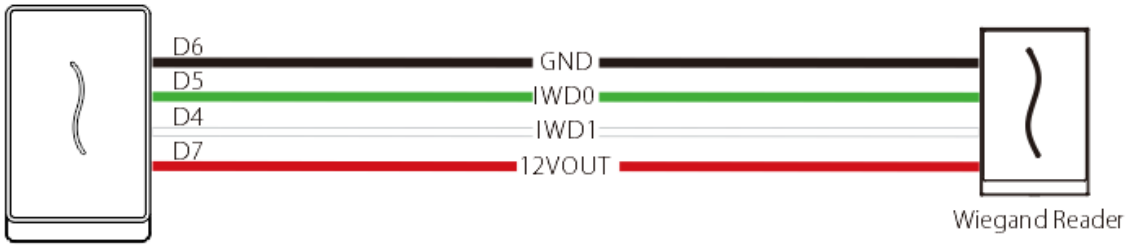


1.3.7 Wiegand Output Connection

After a successful verification, the device will send Wiegand signals to the SRB access controller, then the SRB will output relay signals to trigger the relay to unlock the door.

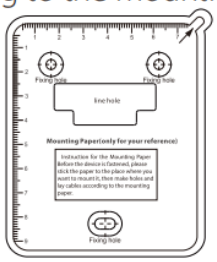


1.3.8 Wiegand Input Connection

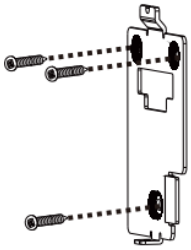


1.4 Installation

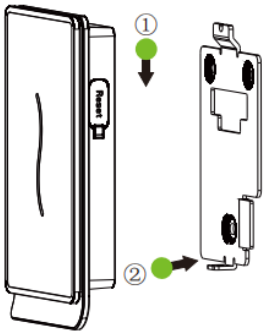
1) Paste the mounting template sticker on the wall, and drill holes according to the mounting paper.



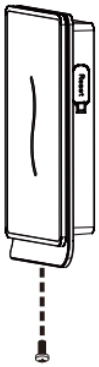
2) Fix the back plate on the wall using wall mounting screws.



3) Attach the device to the back plate.



4) Fix the device to the back plate with a security screw.



2 Connect to Webserver

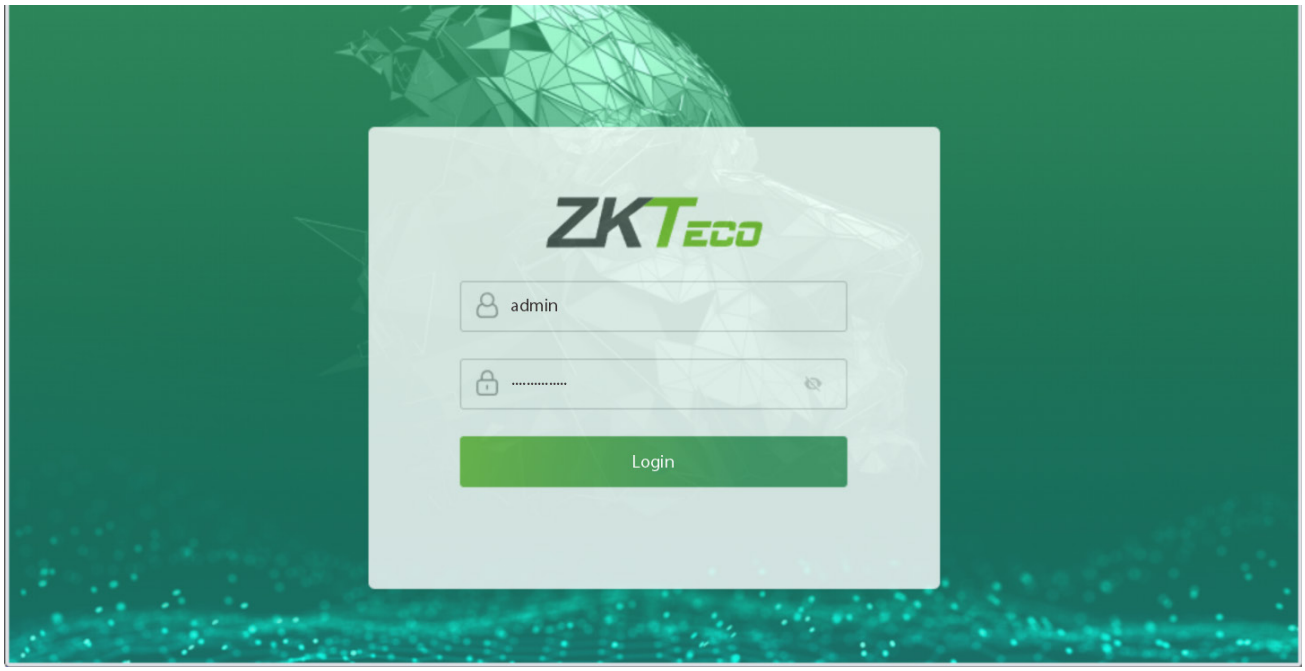
2.1 Login Webserver

A user can open the web application to set the relevant parameters of the device.

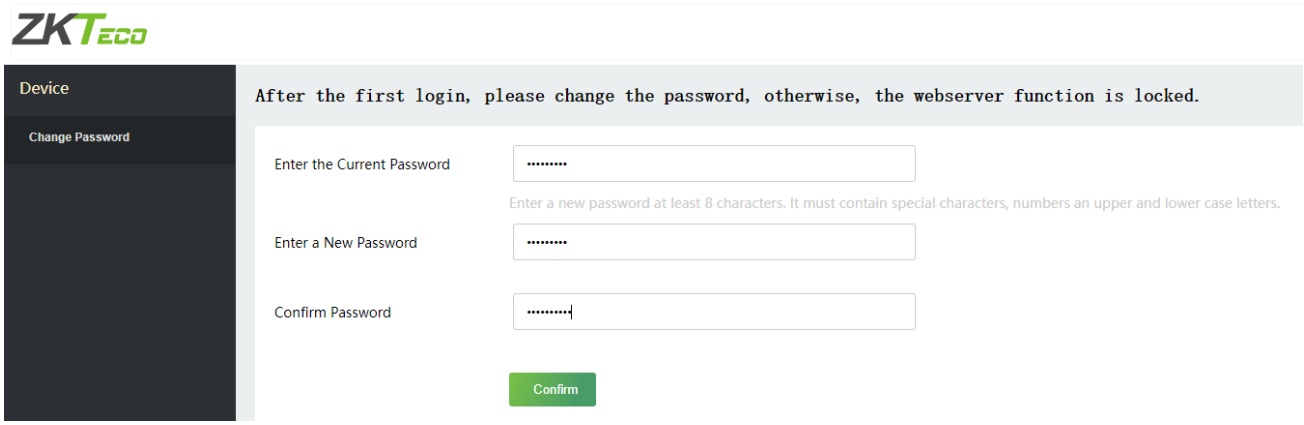
1. Open a browser to enter the address to log in to the WebServer, the address is **https:// Serial IP Address**. For example: **https://192.168.1.201.**

Note: The Serial IP Address of the device for communication can be modified, for details please refer to Communication Settings.

2. Enter the WebServer account and password, the default account is: **admin**, password: **admin@123**.



Note: After logging in for the first time, users need to change their original password and log in again before they can use it.



2.2 Forgot Password

You can use the magnetic tamper switch to restore factory settings.

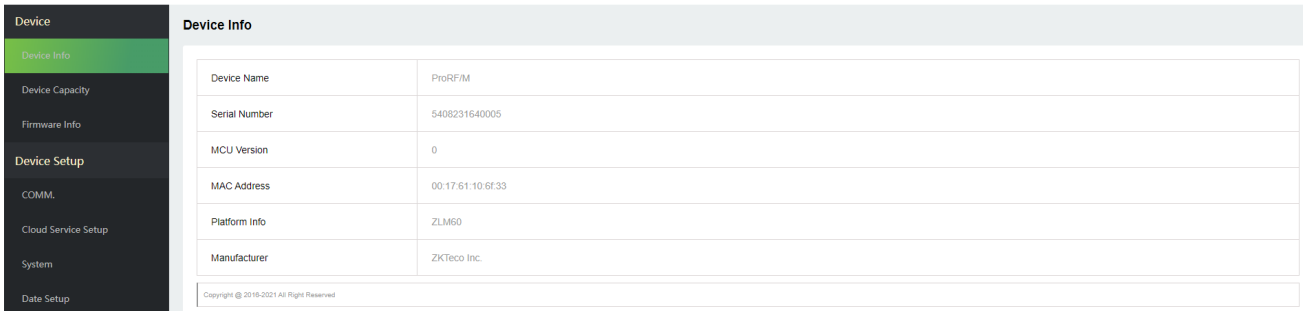
First remove the back plate of the device and power on the device. Put the magnet on the tamper switch three times after you hear the tamper alarm sound for 30 seconds but no more than 60 seconds. Then the device will short beeps for a while, indicating that it is restoring. After it is restored successfully, the device will restart automatically (the indicator glows yellow continuously and the device makes a long beep).

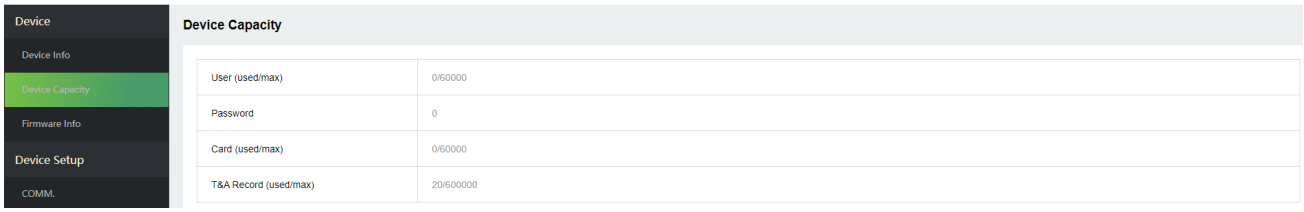
Notes:

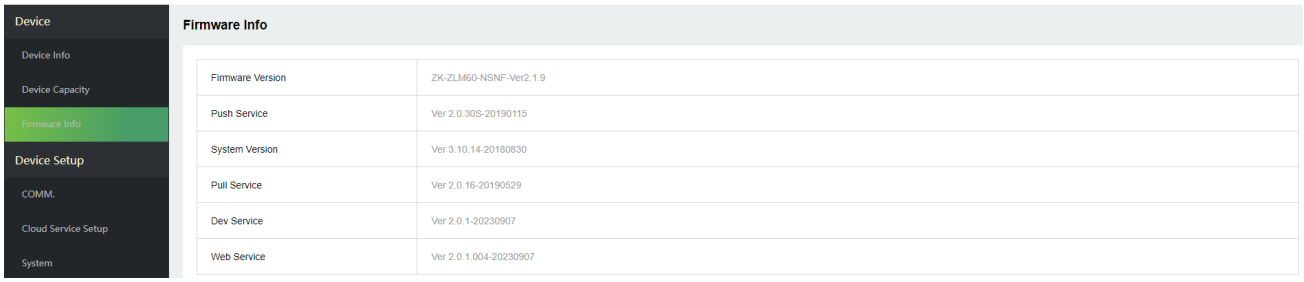
- The password of Webserver is restored to default (admin@123), and the IP of the device is restored to the original 192.168.1.201.
- The registered user data will not be cleared, but the access levels of the users need to be re-synchronized through the software.

2.3 Device

Click **Device Info / Device Capacity / Firmware Info** on the WebServer, you can view the data capacity, device and firmware information of the current device.







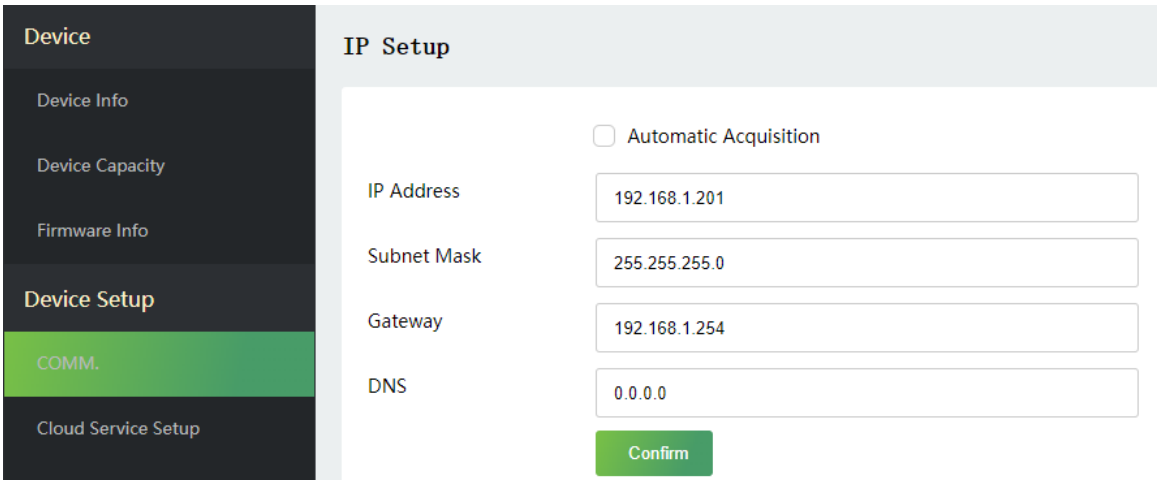
Function Name	Description
Device Info	Displays the device's name, serial number, MCU version, MAC address, platform and manufacturer information.
Device Capacity	Displays the current device's user storage, password, card storage and T&A records.
Firmware Info	Displays the firmware version and other version information of the device.

2.4 Device Setup

2.4.1 Communication Settings

Click **COMM.** on the WebServer.

Change the IP address of the device as needed, click **Confirm** to save, and the device will automatically synchronize the IP information.



Function Name	Description
Automatic Acquisition	Select whether to obtain the IP Address by automatically.
IP Address	The default IP address is 192.168.1.201. It can be modified according to network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to network availability.

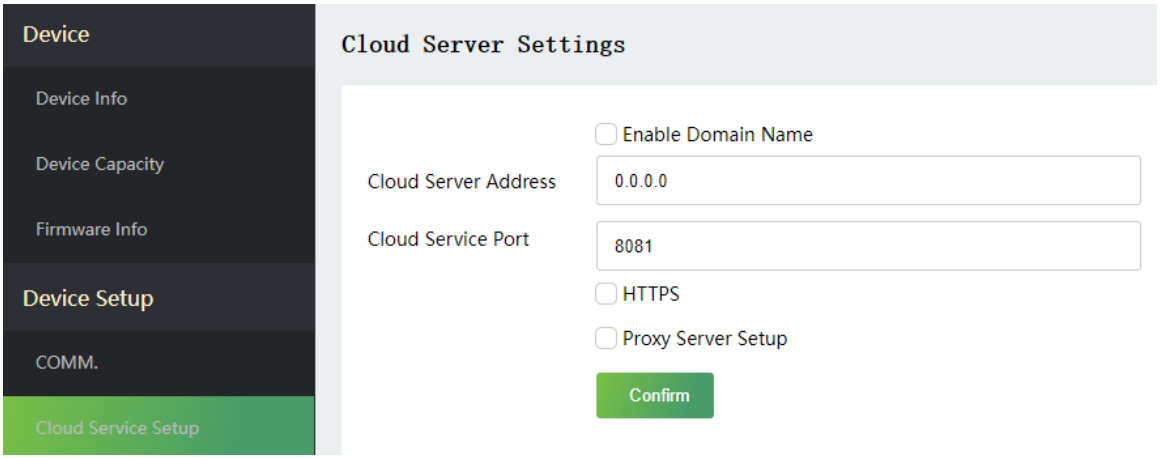
DNS	The default DNS address is 0.0.0.0. It can be modified according to network availability.

Note: After the IP address of the device is changed successfully, you need to log out of the currently WebServer and log in again to the IP address you just changed to connect to the device. For WebServer login details, please refer to Login WebServer.

2.4.2 Cloud Service Setup

Click **Cloud Service Setup** on the WebServer.

Cloud Server Setup was used to connect to the ZKBio CVSecurity software, please refer to 3.1 Set the Communication Address.

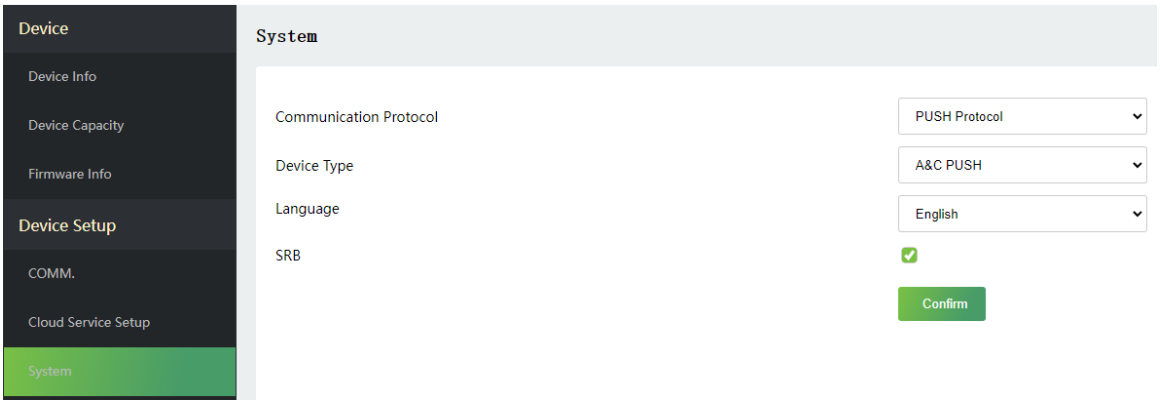


Function Name		Description
Enable Domain Name	**Cloud Server Address**	Once this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name (when this mode is turned **ON**).
Disable Domain Name	**Cloud Server Address**	IP address of the ADMS server.
	Cloud Server Port	Port used by the ADMS server.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.
Proxy Server Setup		When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

2.4.3 System Settings

Click **System** on the WebServer.

It helps to set related system parameters to optimize the accessibility of the device.

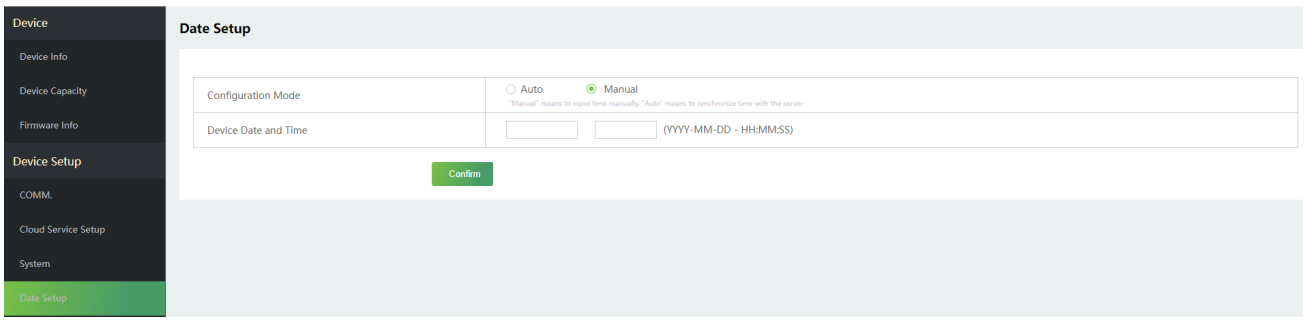


Function Name	Description
Communication Protocol	Set the communication protocol of the device. Currently only supports PUSH Protocol.
Device Type	Set the device as an access control terminal or attendance terminal. ***Note:*** After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.
Language	Select the language of the WebServer and device. Currently only supports English.
SRB	Select whether to enable the SRB function.

2.4.4 Date Setup

Click **Date Setup** on the WebServer.

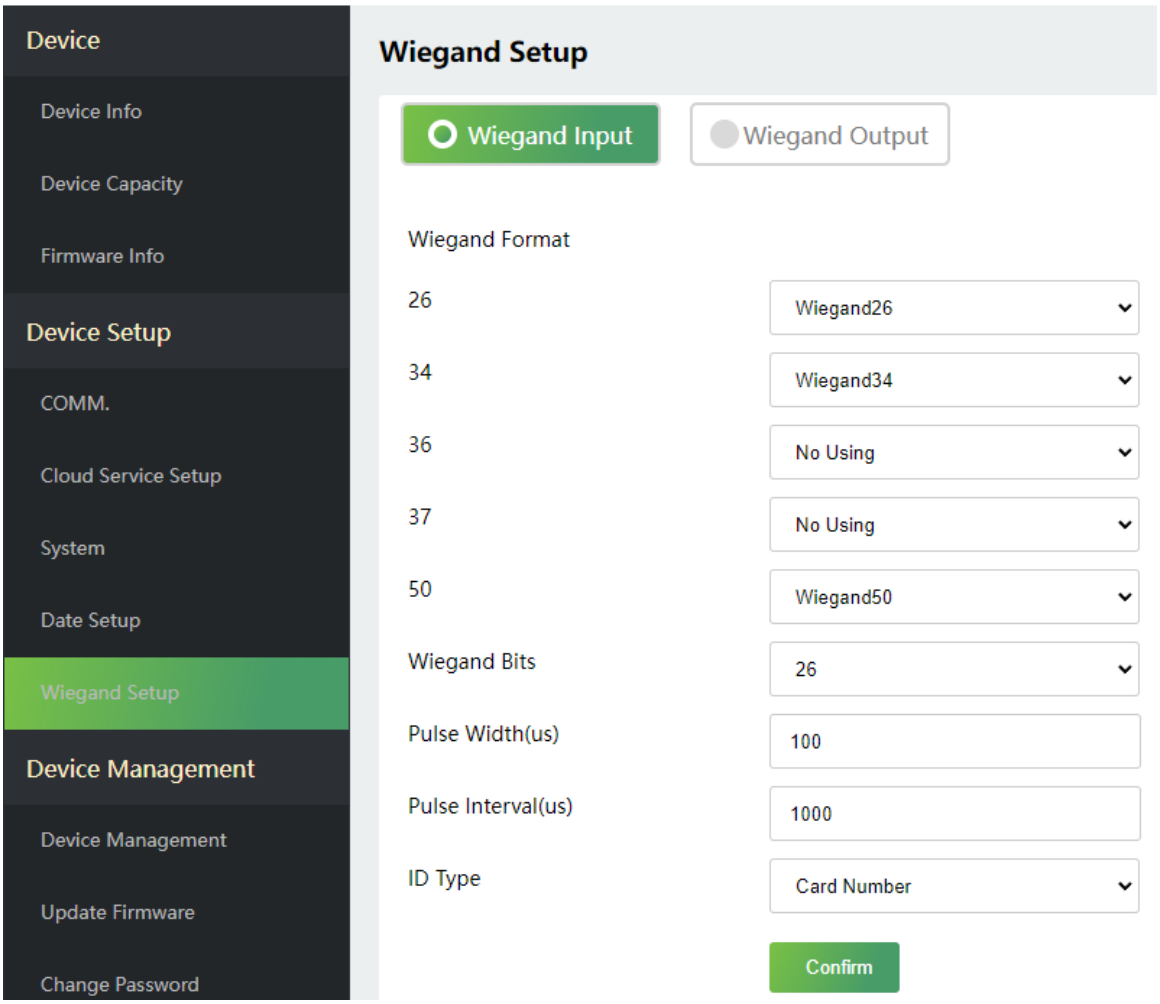
- Click **Manual** to manually set the date and time and click **Confirm** to save.

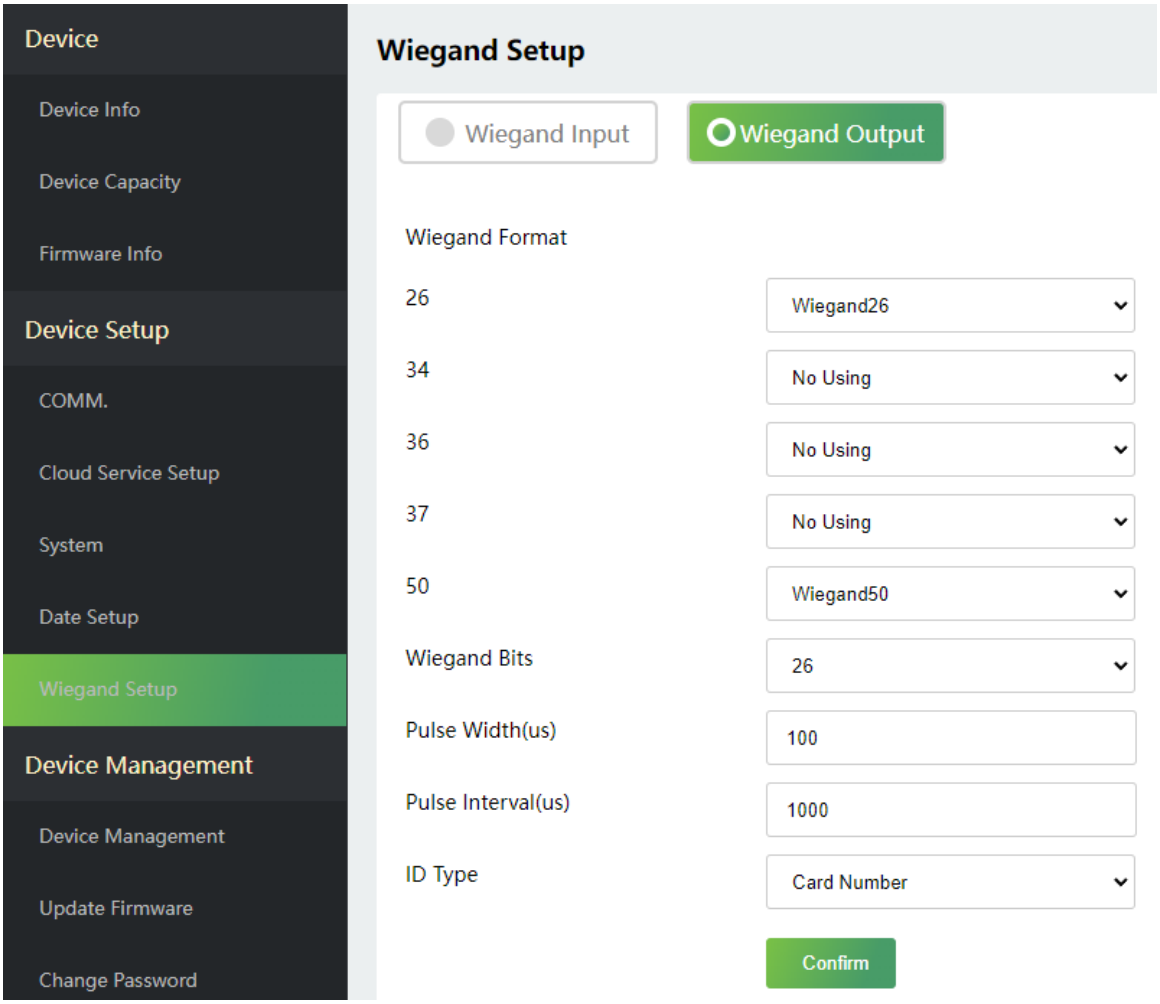


2.4.5 Wiegand Setup

Click **Wiegand Setup** on the WebServer.

It is used to set the Wiegand input and output parameters.



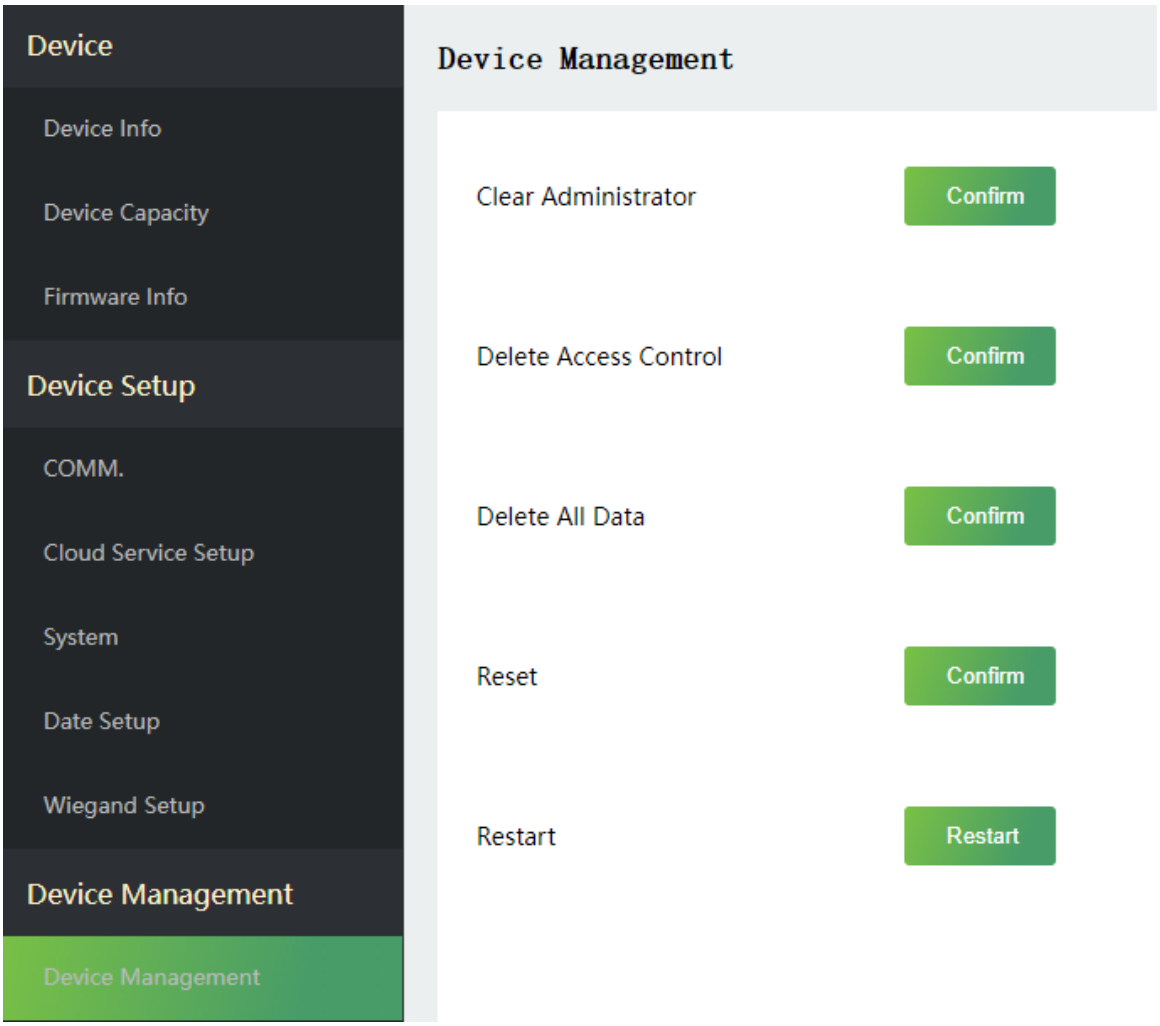


Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits and 50 bits.
Wiegand Bits	The number of bits of the Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds and can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and card number.

2.5 Device Management

2.5.1 Device Management

Click **Device Management** on the WebServer.



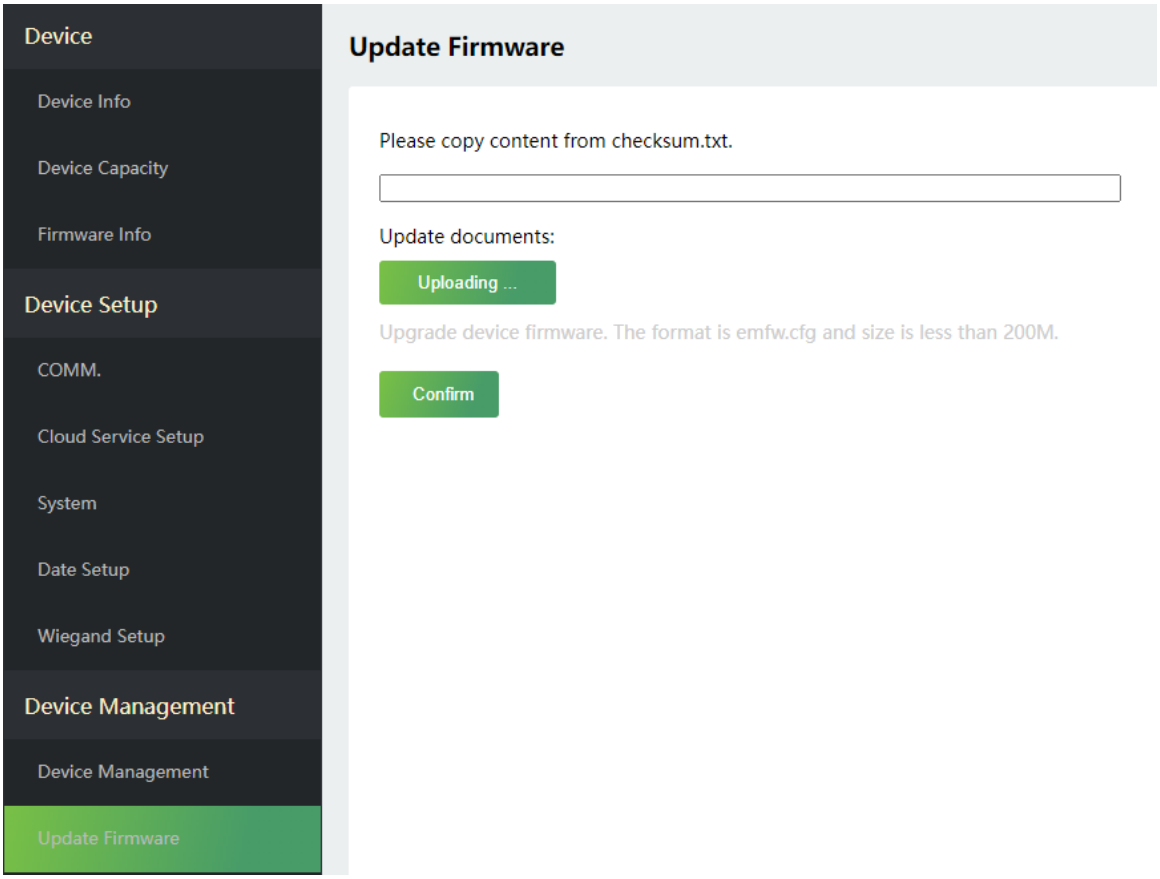
Function Name	Description
Clear Administrator	Choose whether to change the super administrator into a normal user.
Delete Access Control	To delete the access control data from the device.
Delete All Data	To delete the information and attendance logs/access records of all registered users.
Reset	The Reset function restores the device settings such as communication and system

	settings to the default factory settings (this function does not clear registered user data, but the access levels of the users need to be re-synchronized through the software). ***Note:*** After reset, the device will reboot, the password of Webserver is restored to default, and the IP of the device is restored to the original 192.168.1.201, please refer to 2.4.1 Communication Settings to modify the IP.
Restart	Choose whether to restart the device.

2.5.2 Updata Firmware

Click **Updata Firmware** on the WebServer.

Select an upgrade file and click **Confirm** to complete firmware upgrade operation.

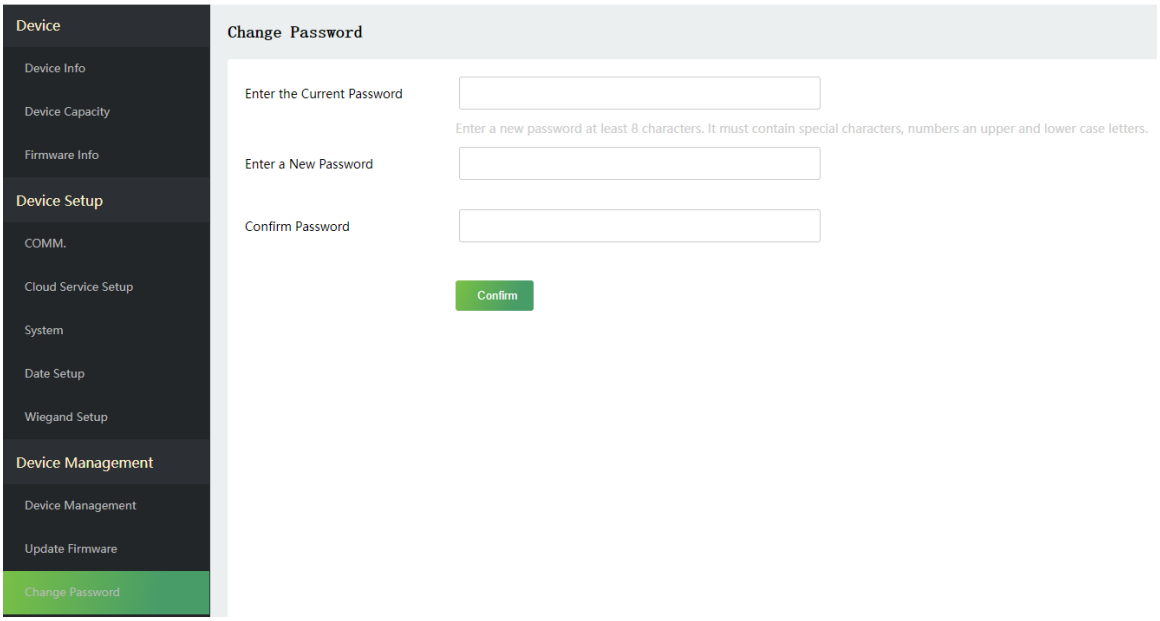


Note: If the upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.

2.5.3 Change Password

Click **Change Password** on the WebServer.

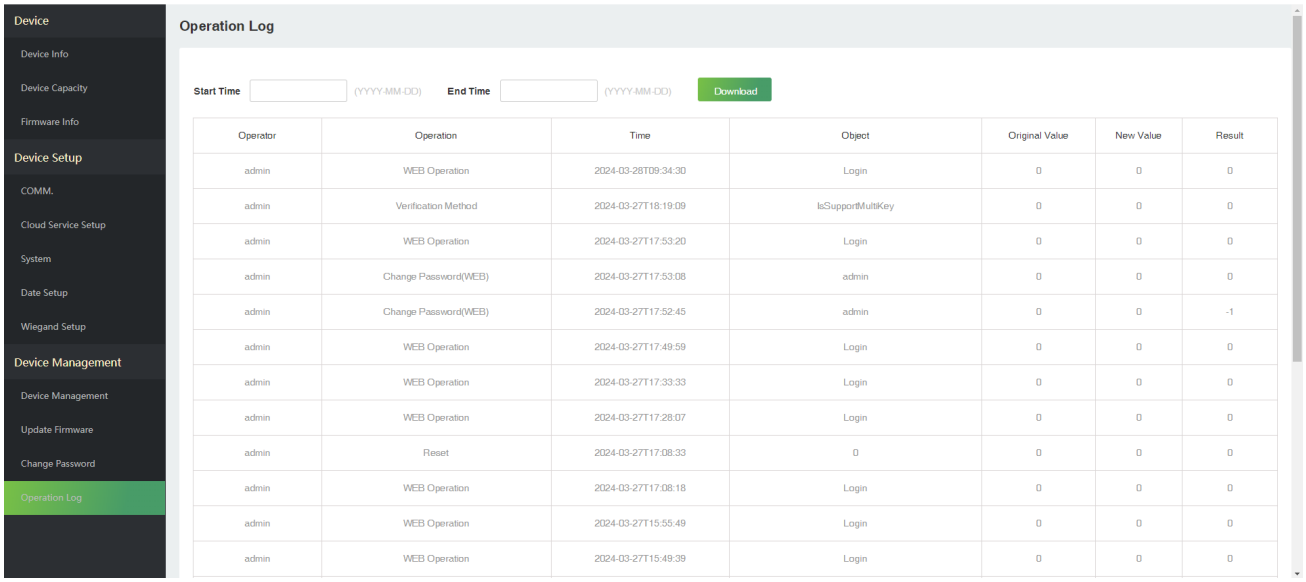
In this interface, you can change the password of WebServer.



2.5.4 Operation Log

Click **Operation Log** on the WebServer.

All the user's operation records on the device or WebServer are saved. Users can search and download these logs by time.



3 Connect to ZKBio CVSecurity Software

3.1 Set the Communication Address

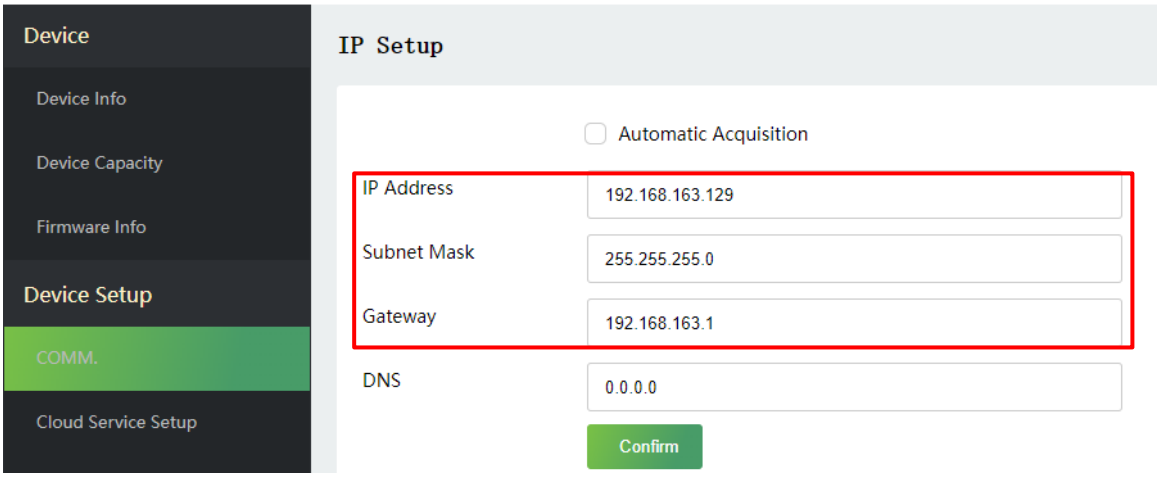
1. Click **COMM.** in the WebServer to set the IP address and gateway of the device.

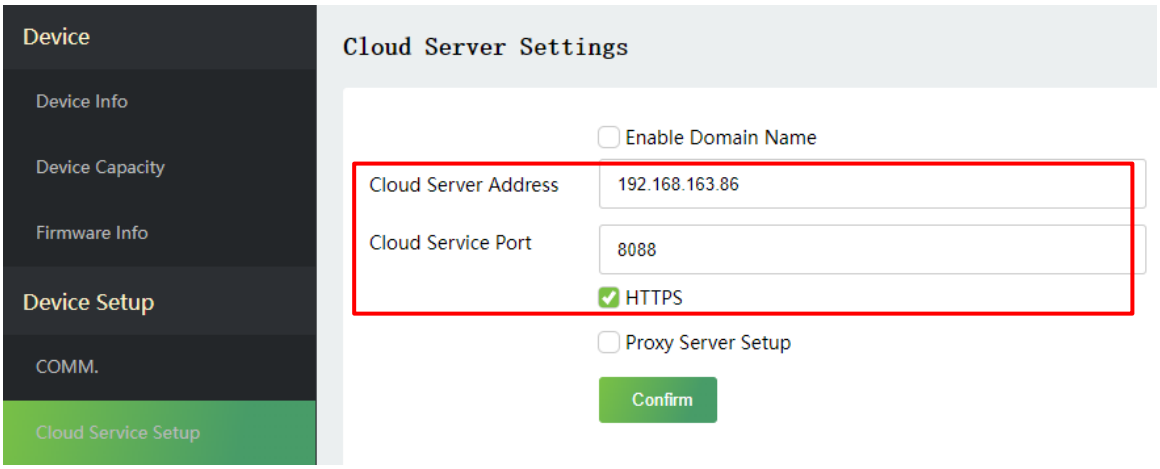
   (***Note:*** The IP address should be able to communicate with the ZKBio CVSecurity server, preferably in the same network segment with the server address)

2. In the WebServer, click **Cloud Server Setup** to set the server address and server port.

   Server address: Set the IP address as of ZKBio CVSecurity server.

   Server port: Set the server port as of ZKBio CVSecurity (the default is 8088).

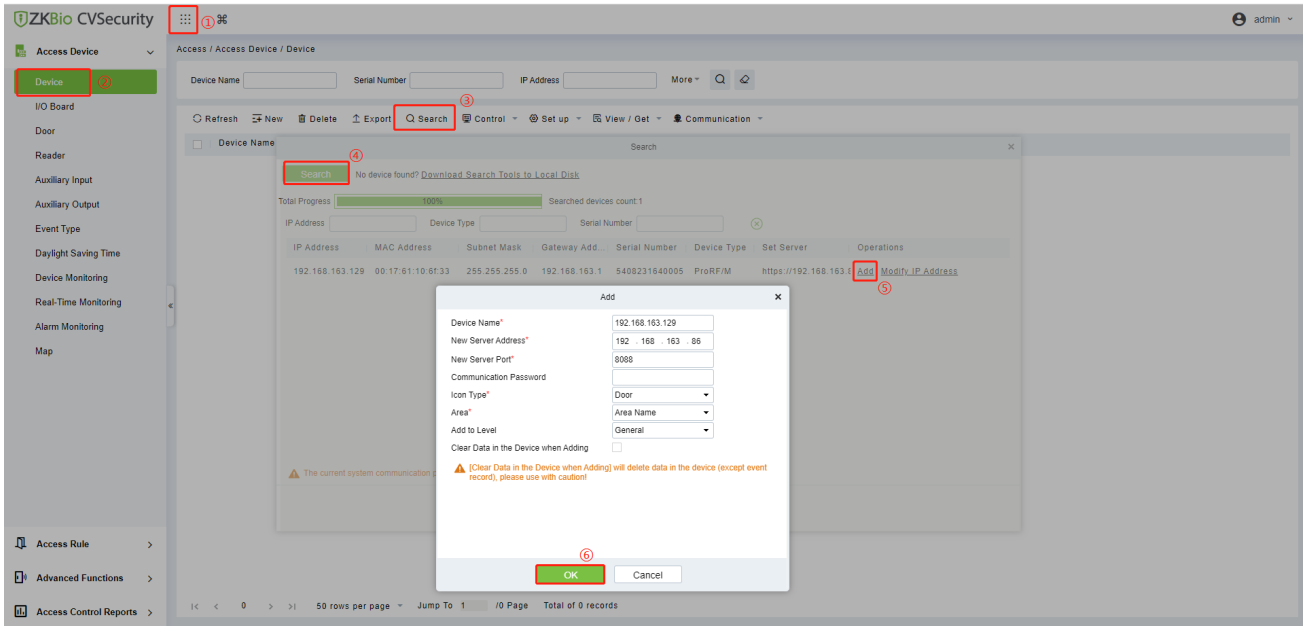




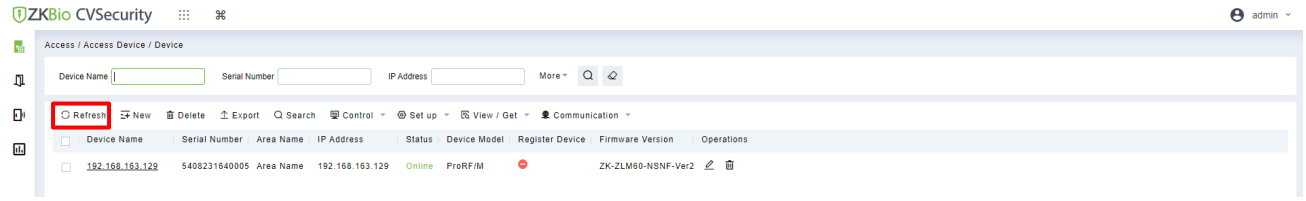
3.2 Add Device on the Software

Add the device by searching. The process is as follows:

1. Click **Access** > **Device** > **Search**, to open the Search interface in the software.
2. Click **Search**, and it will prompt [**Searching……**].
3. After searching, the list and total number of access controllers will be displayed.

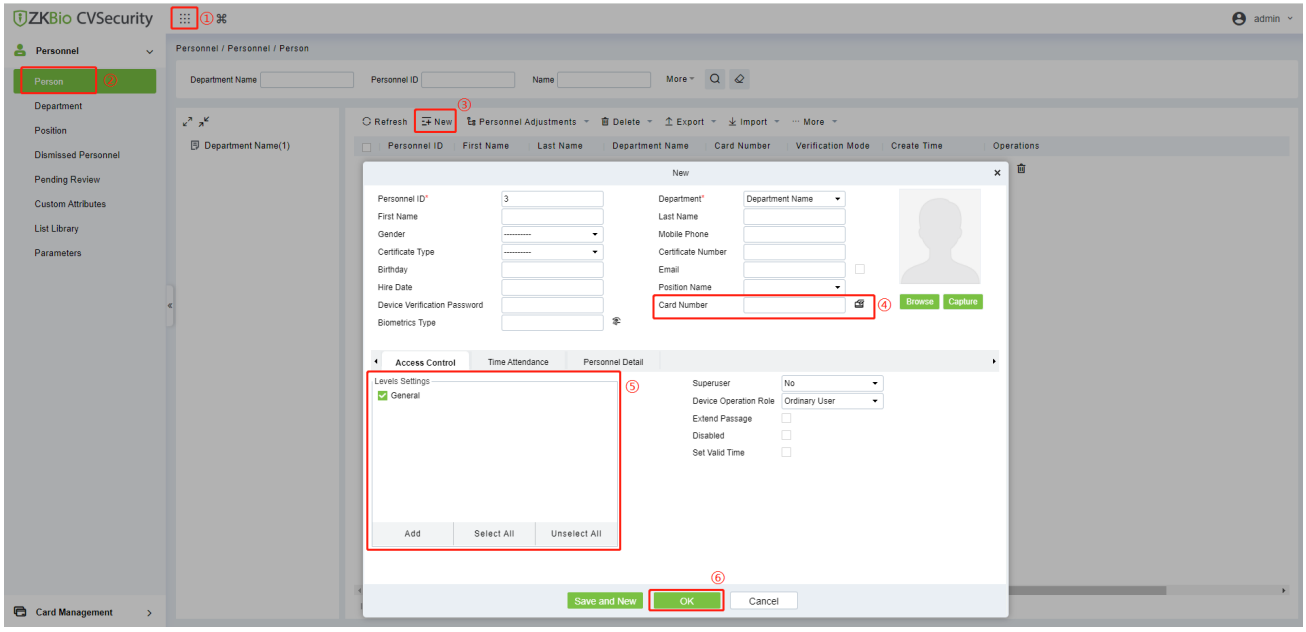


4. Click **Add** in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click **OK** to add the device.
5. After the addition is successful, click **Refresh**, the device will be displayed in the device list.



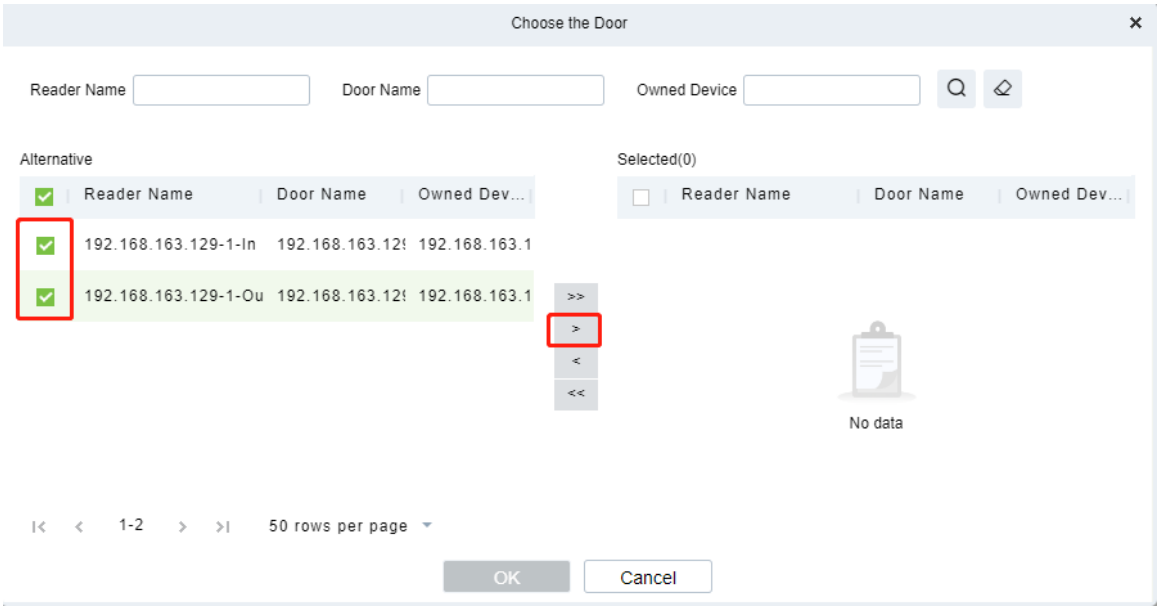
3.3 Add Personnel on the Software and Card Registration

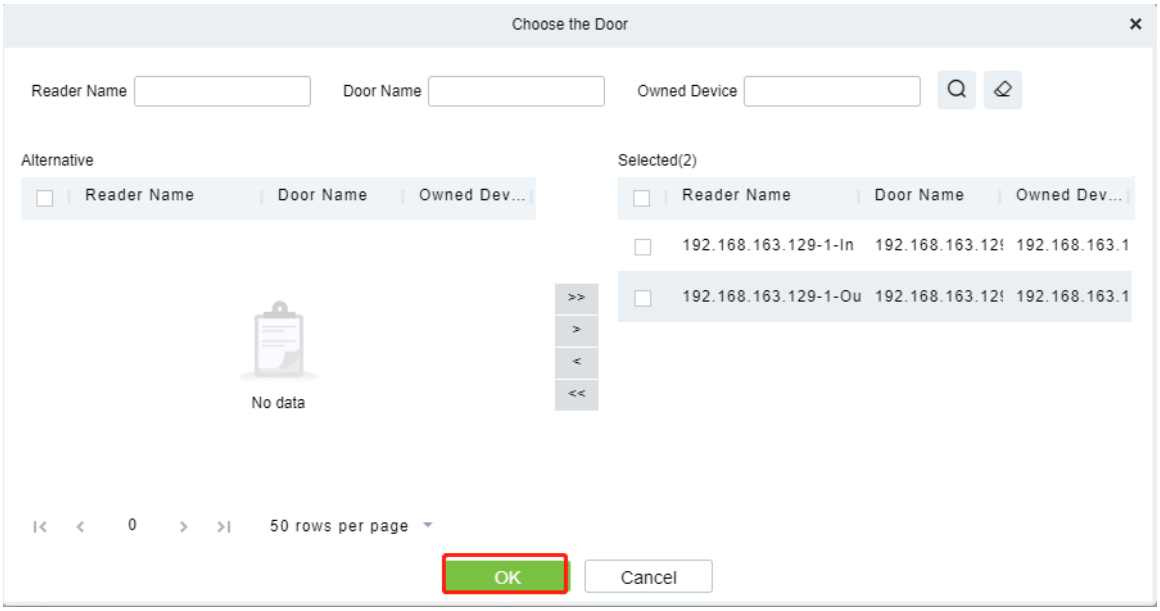
1. Click **Personnel** > **Person** > **New**:



2. Fill in the related information of the user.

3. **Register card number:** You can fill in the card number manually or click the icon to issue card from device. Select the device which you just added on the software, and click the icon and click **OK**. Then you can swipe your card on the ProRF, the card number will be displayed automatically in the box.

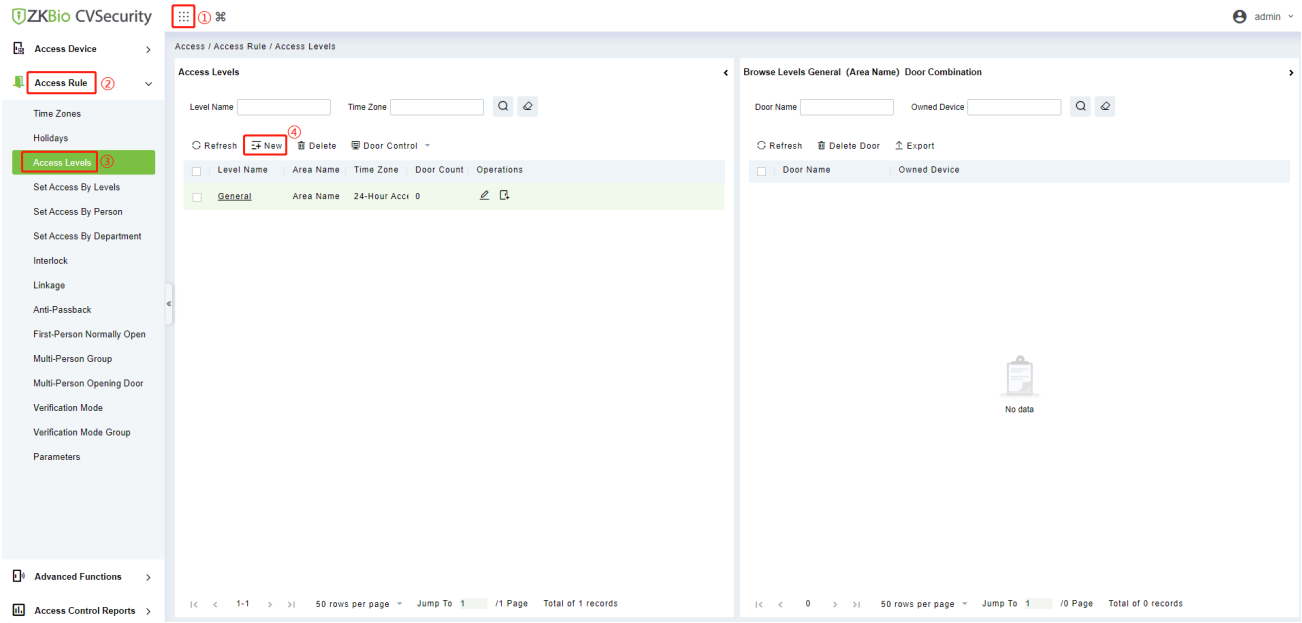




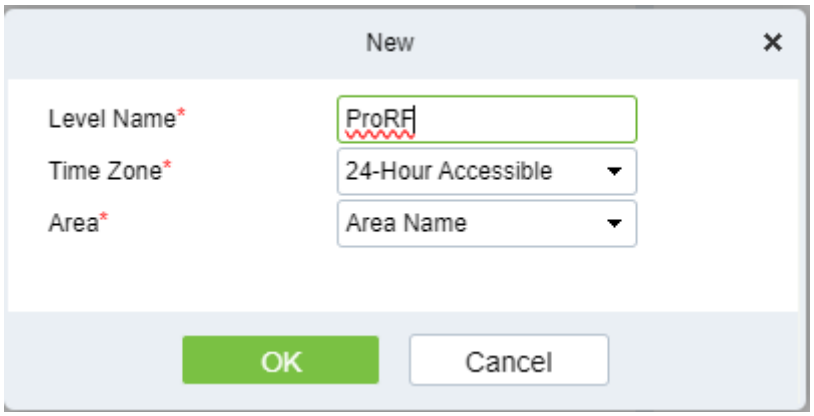
4. Select the access level of the user, and set the related permissions. (For the setting of access levels, please refer to 3.4 Set Access Levels)
5. Click **OK** to save the user.

3.4 Set Access Levels

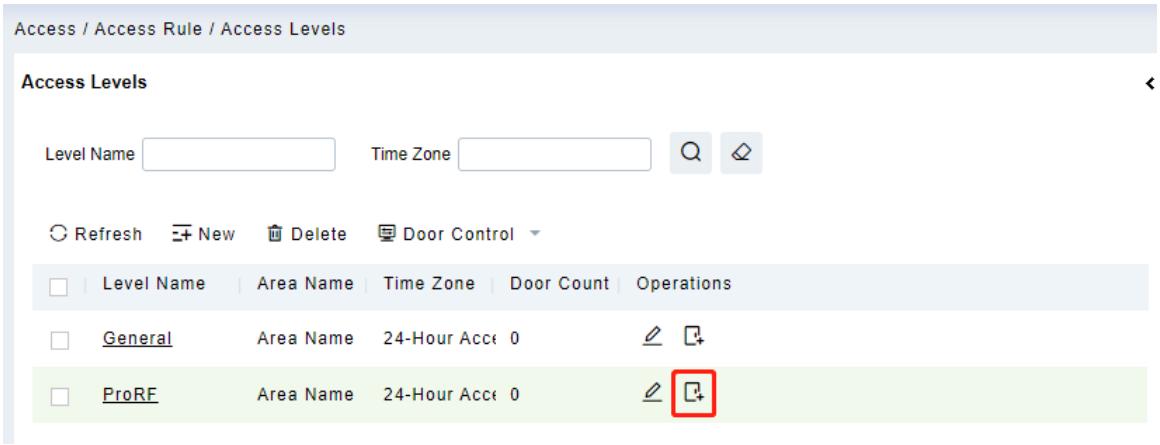
1. Click **Access > Access Rule > Access Levels > New** to add access level.



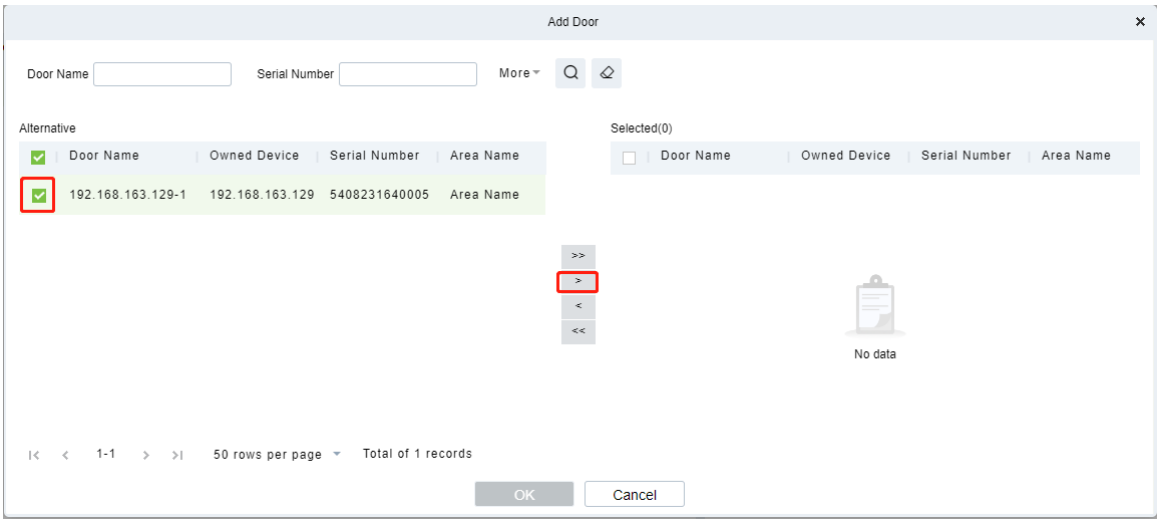
2. Fill in the level name, select the time zone and area and click **OK**.

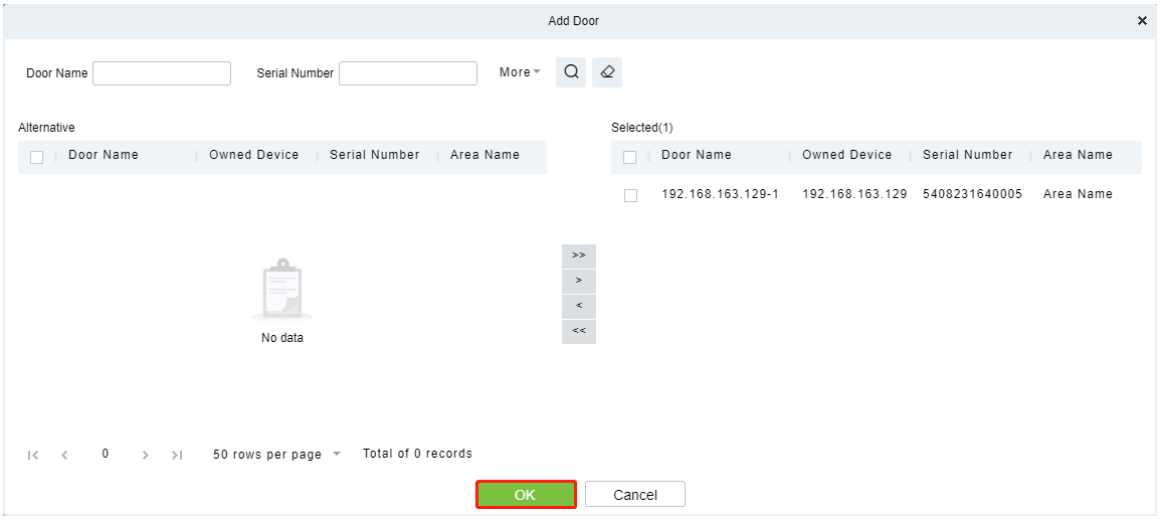


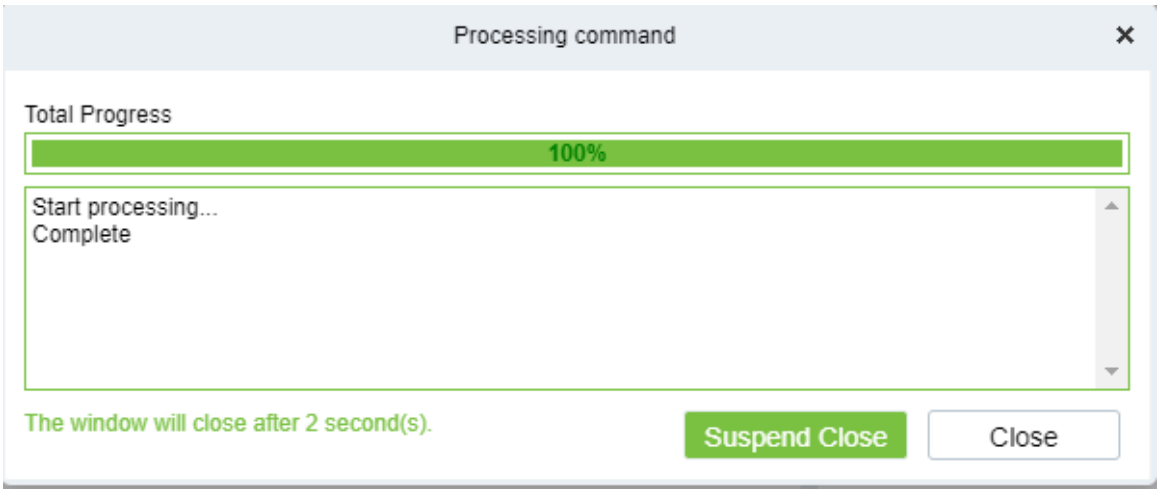
3. Click the icon behind the access level you want to add door.



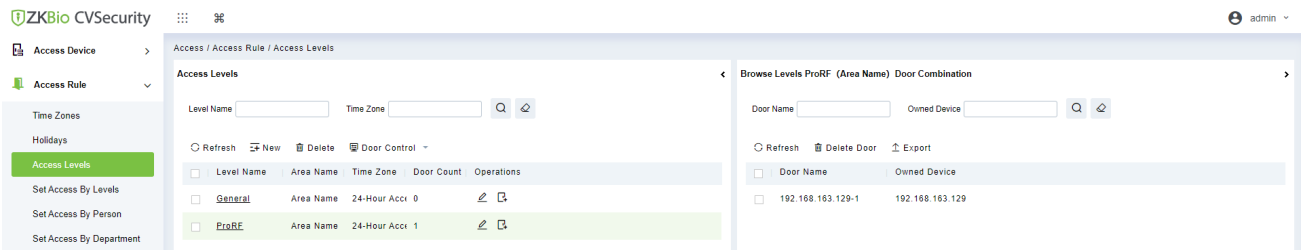
4. Select the door which is corresponding to the device, click the icon and click **OK**.





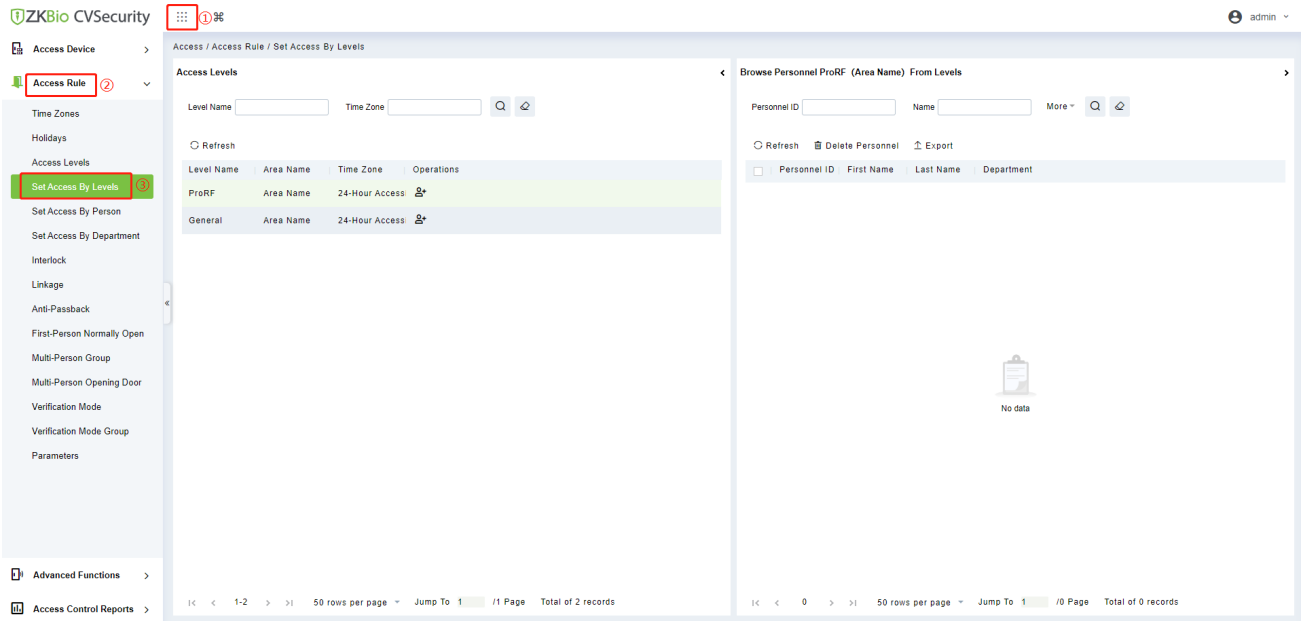


5. After the process is complete, the door will be displayed in the right of the interface.

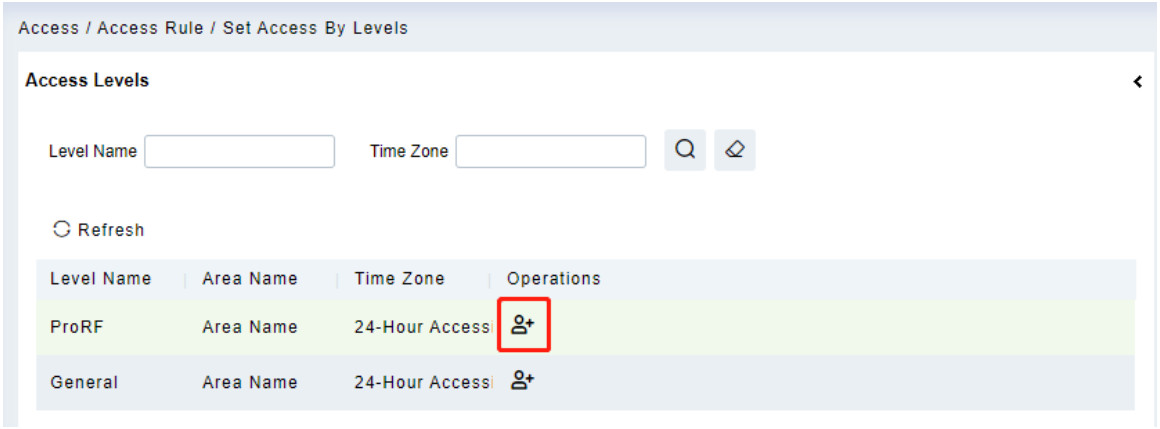


3.5 Set Access by Levels

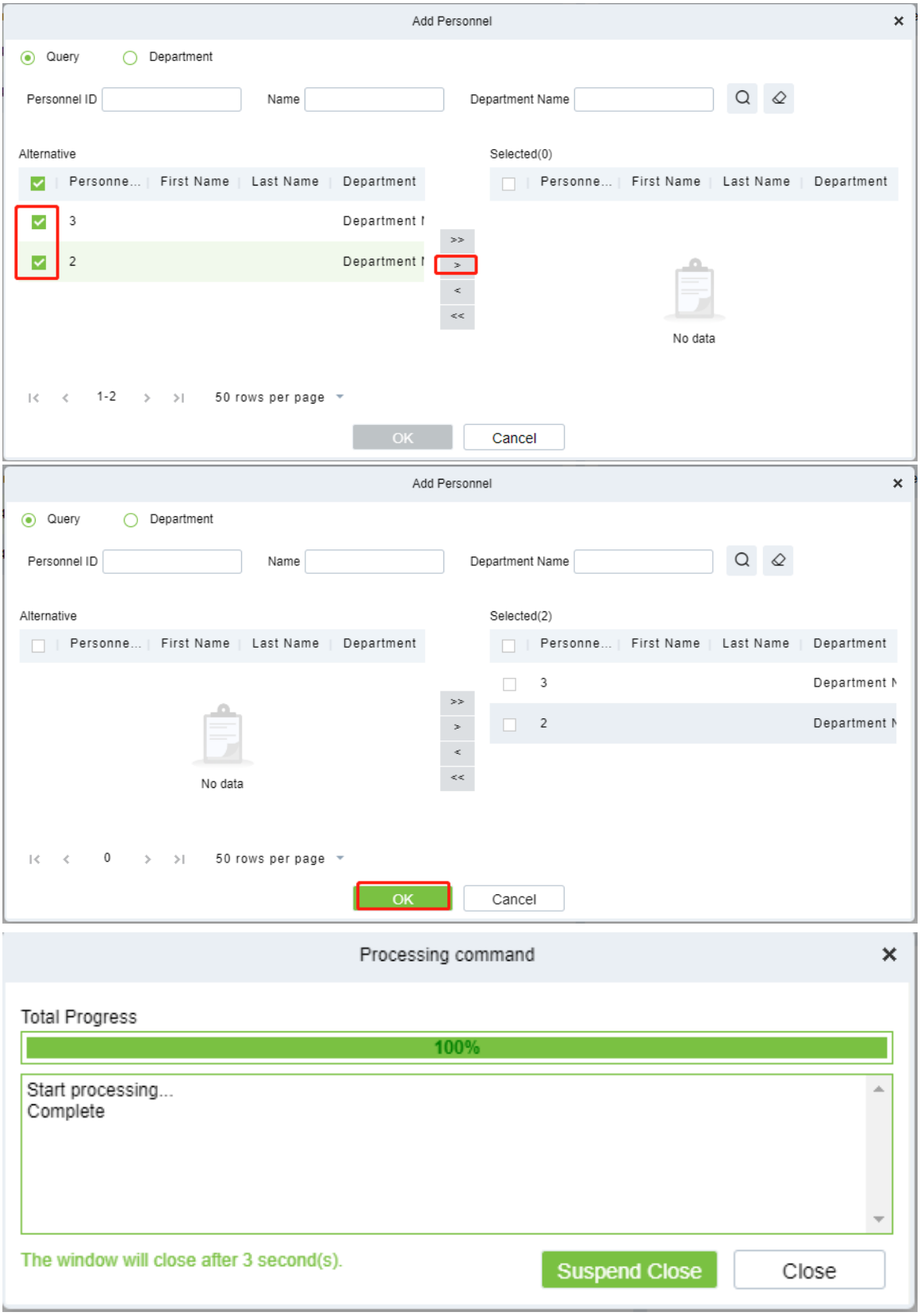
1. Click **Access > Access Rule > Access Levels > Set Access by Levels**.



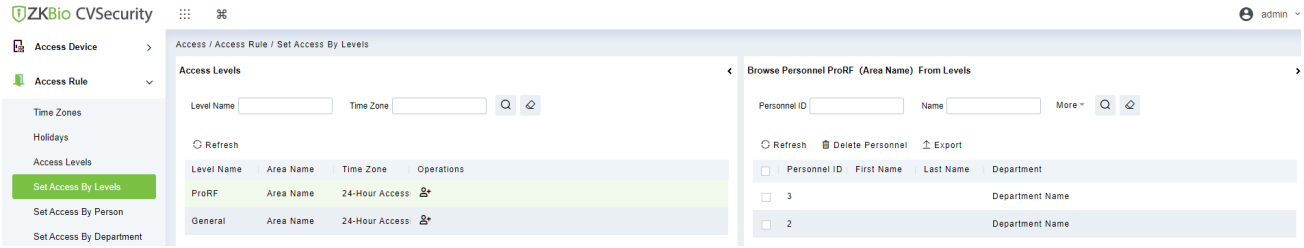
2. Click the icon behind the access level you want to add personnel.



3. Select the personnel who need to be assigned to the access level, click the icon and click **OK**.



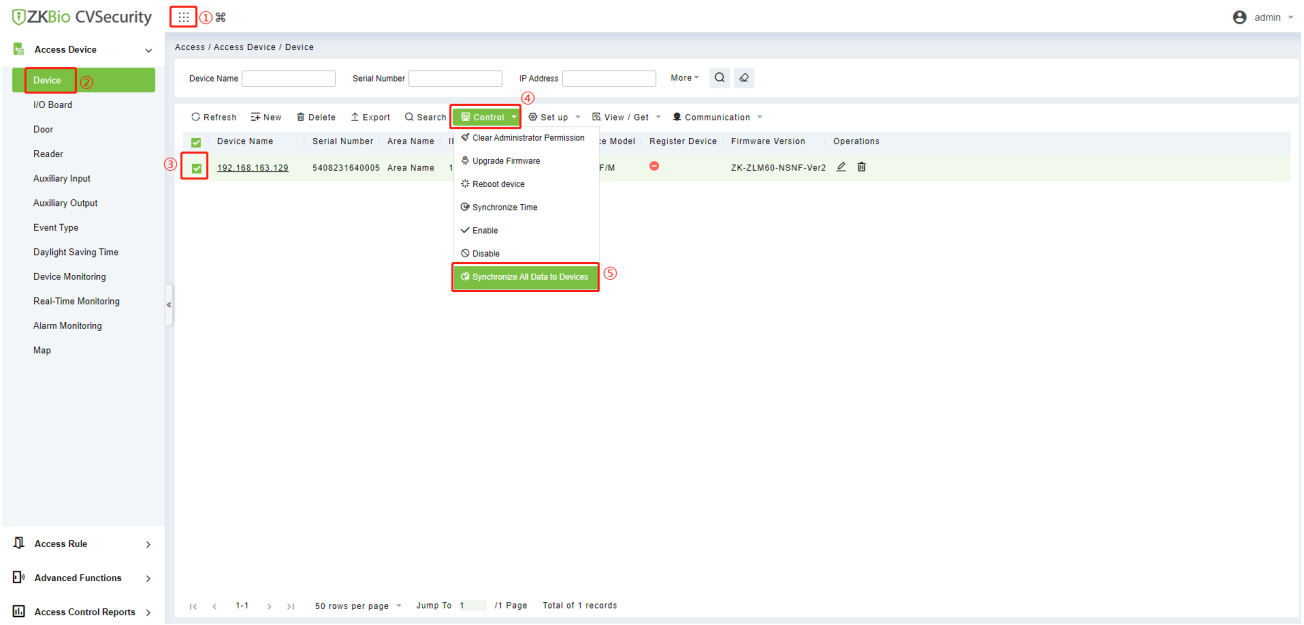
4. After the process is complete, the personnel will be displayed in the right of the interface.



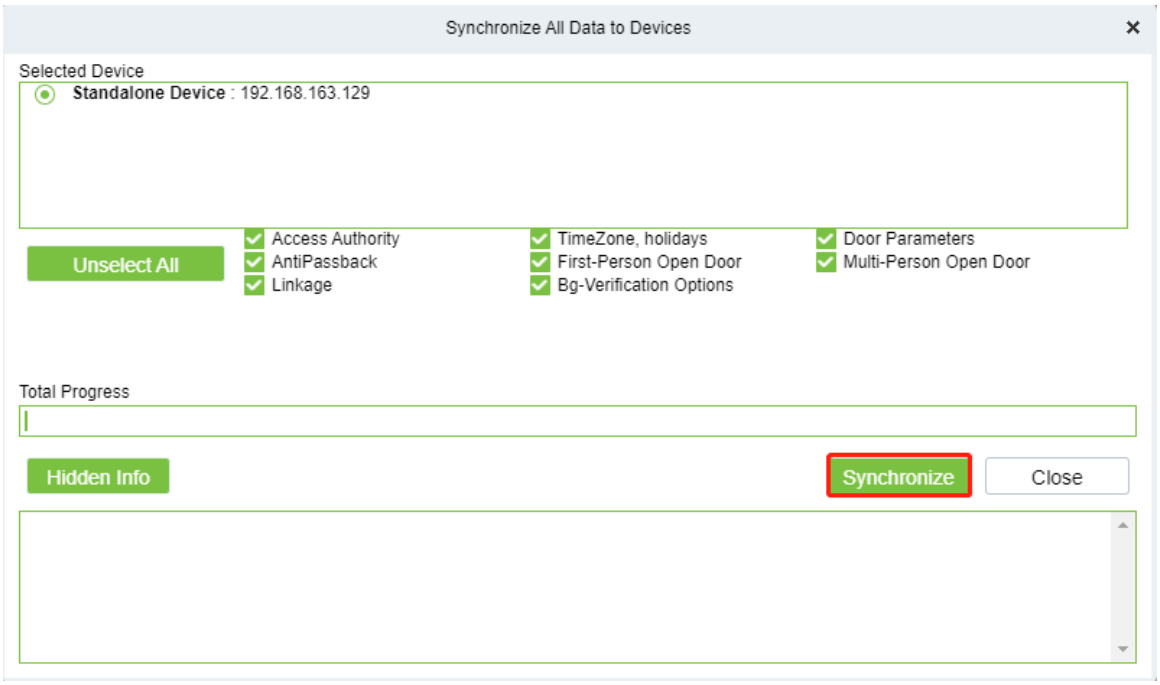
Note: The user can also set access by person or by department. For other access control settings, please refer the *ZKBio CVSecurity User Manual*.

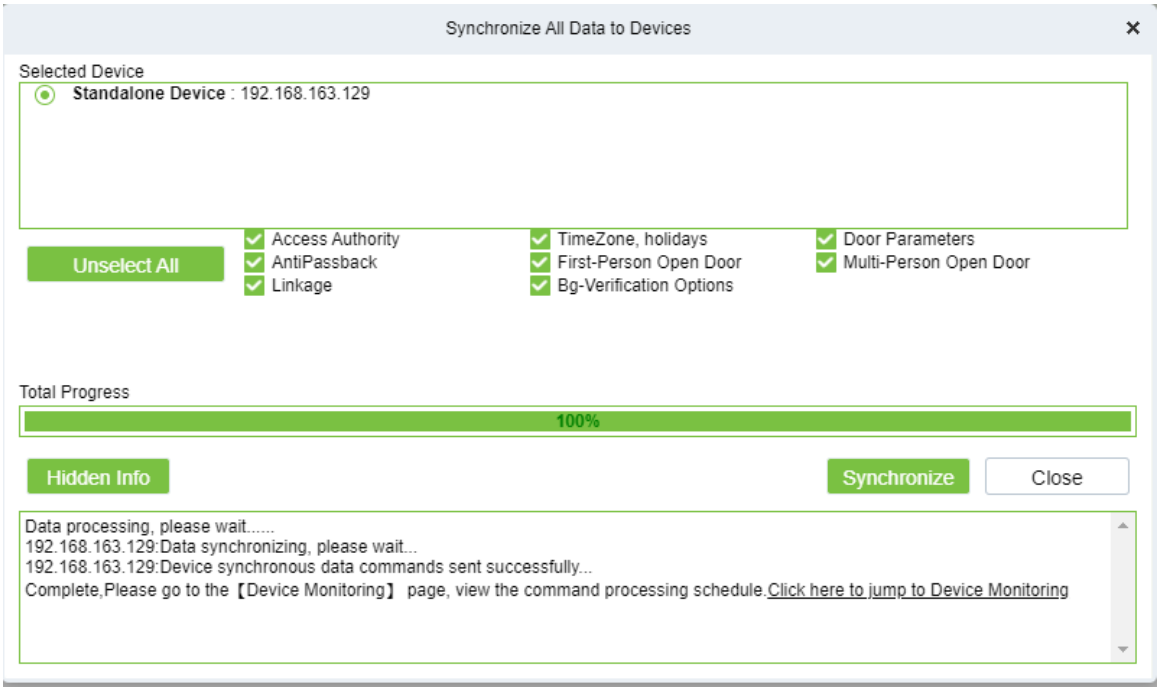
3.6 Synchronize All Data to Devices

1. Click **Access** > **Device**, check the device you want to operate and click **Control** > **Synchronize All Data to Devices**.



2. Click **Synchronize** to synchronize all the data to the device including the new users.

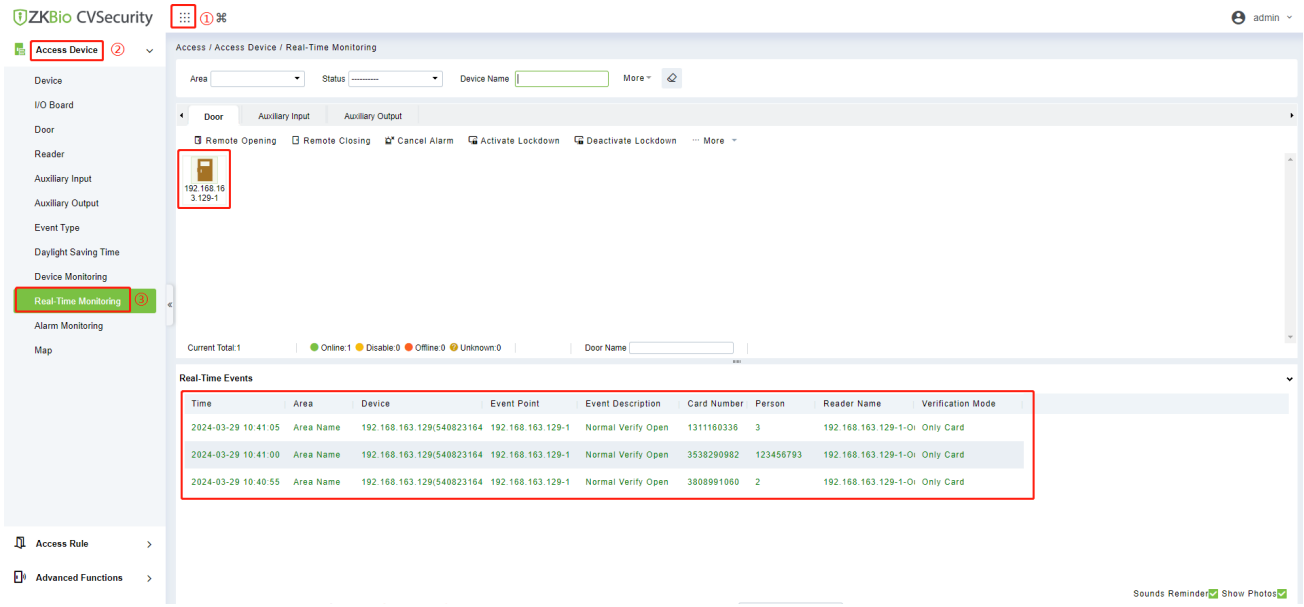




3. After the process is complete, the users who registered cards can verify on the ProRF.

3.7 Real-Time Monitoring

Click **Access > Real-Time Monitoring**, the user can view the status of the door and the real-time events of the device.



Note: For other specific operations, please refer the *ZKBio CVSecurity User Manual*.

CE Note

Manufacturer: ZKTECO CO., LTD.

Address: No.32, Industrial Road, Tangxia Town, Dongguan City, Guangdong Province, China 523728

Hereby, ZKTECO CO., LTD. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

Importers: ZKTECO EUROPE SL

Address: Carretera de Fuencarral, 44 Edificio 1, Planta 2, 28108 Alcobendas, Madrid- Spain

A copy of the declaration of conformity can be obtained with this user manual; this product is not restricted in the EU.

The wireless operation frequency

RFID: 13.56MHz; Max H-Field Strength: -15.78dBuA/m at 10m

Or 125kHz; Max H-Field Strength: 20.13 dBuA/m at 10m

The device has been evaluated to meet CE general RF exposure requirement. The device can be used without restriction.

FCC Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the separation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate this equipment.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure Statement

The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.

Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

Green Label

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone: +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com

Copyright © 2024 ZKTECO CO., LTD. All Rights Reserved.