User Manual

KF1100 Pro / KF1200 Pro

Date: August 2024

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

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 have 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 **KF1100 Pro / KF1200 Pro**.

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 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.

Table of Contents

1 Overview

1.1 Introduction

ZKTeco's KF1100 Pro & KF1200 Pro is a sophisticated visible light facial authentication and RFID reader. This series can operate either as a biometric readers or as standalone access control devices, offering you the flexibility to choose the mode that best suits your needs.

Designed to integrate seamlessly with the inBio Pro Plus controllers, the KF1100 Pro & KF1200 Pro can capture and convert face images into face templates as small as 512 bytes. The face templates will then be transmitted to the inBio Pro Plus controllers via RS-485 for authentication. The KF1100 Pro & KF1200 Pro are equipped with TCP/IP port, allows for fast data synchronization with the controllers, raising the bar for stable and precise facial authentication capabilities.

Also, KF1100 Pro & 1200 Pro showcase its versatility when deployed as a visible light facial authentication standalone access control device with a DM10 (door lock extension panel). KF1100 Pro & 1200 Pro is compatible with the ZKBio CVSecurity through ZKTeco A&C PUSH protocol.

1.2 Features

Biometric Reader Mode (via RS-485)

- Dedicated to InBio Pro Plus controller to adopt facial authentication technology. (A maximum of face template capacity: 3,000; user capacity: 100,000).
- Fully compatible with ZKBio CVSecurity (V6.3.0).
- Support high-speed communication ports including TCP/IP, Wi-Fi (IEEE 802.11 a/g/n).

- Capture and convert face images into face templates of just 512 bytes.

Visible Light Facial Authentication Standalone Device Mode (with DM10)

- Support a maximum of 1,500 face template / 30,000 cards / 100,000 transactions.
- Support high-speed communication ports including TCP/IP and Wi-Fi (IEEE 802.11 a/g/n).
- Fully compatible with ZKBio CVSecurity (V6.3.0).
- Support wall-mount and it is compatible with Asian gang-box (KF1100 Pro); compatible with Single gang-box (KF1200 Pro).
- User friendly on-board web server for quick system configuration.
- Advance protection standard fully compliant with ZKCSBL (ZKTeco Cyber Security Base Line).

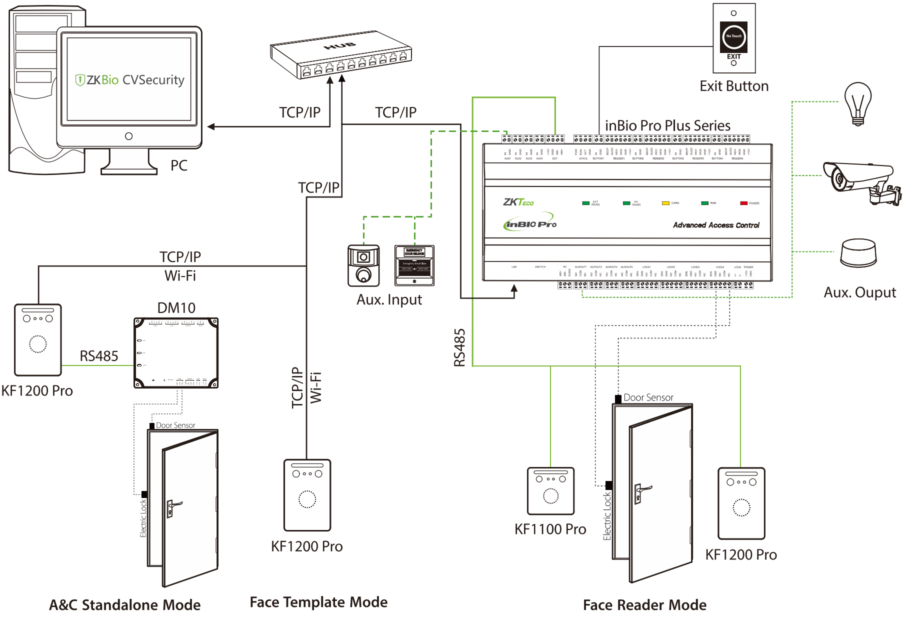
1.3 Specifications

Model	KF1100 Pro	KF1200 Pro
Display	N/A	
Camera	Dual Camera @ 2MP	
Operation System	Linux OS	
Hardware	CPU:1.2GHz Dual Core RAM: 256MB; ROM:512MB	
Authentication Method	Face/Card	
Fingerprint Template Capacity	N/A	
Face Template Capacity	Face Reader Mode: 3,000 Store in InBio Pro Plus(Default) A&C Standalone Mode:1,500 (1:N) (with DM10) (Optional)	

Palm Template Capacity	N/A
Card Capacity	Face Reader Mode:100,000 Store in InBio Pro Plus(Default) A&C Standalone Mode:30,000 (1:N) (with DM10) (Optional)
User Capacity	Face Reader Mode:100,000 Store in InBio Pro Plus (Default) A&C Standalone Mode:30,000 (1:N) (with DM10) (Optional)
Transaction Capacity	Face Reader Mode:500,000 Store in InBio Pro Plus (Default) A&C Standalone Mode:100,000 (1:N) (with DM10) (Optional)
Biometric Authentication Speed	less than 0.3 sec (Facial Recognition)
Touchless Biometric Authentication Distance	30cm to 50cm (FacialRecognition)
Touchless Biometric Operating Lighting Environment	≤2,000 lux @Face
False Acceptance Rate(FAR)%	FAR≤0.01%
False Rejection Rate(FRR)%	FRR≤0.02%
Biometric Algorithm	ZKLiveface 3.5/4
Card Type	IDCard@125 kHz(Standard) IC Card@13.56 MHz(Optional)
Communication	Face Reader Mode:ZKTeco RS485*1 A&C Standalone Mode / Face Template Mode:TCP/IP*1 Wi-Fi(IEEE802.11a/g/n) @2.4 GHz (Optional)
Mobile Communication	N/A
Standard Functions	Face Reader Mode (with InBio Pro Plus) A&C Standalone Mode (with DM10) Face Template Mode (Default)

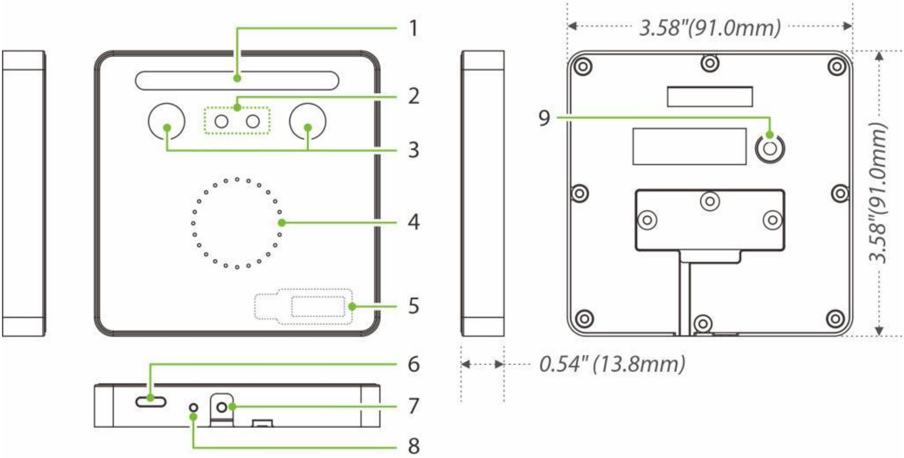
Optional Functions	IC Card@13.56 MHz(Optional) Wi-Fi(IEEE802.11a/g/n) @2.4 GHz (Optional)	
Access Control Interface	A&C Standalone Mode(with DM10)	
Power Supply	DC 12V 3A	
Operating Temperature	-10°C to 50°C	
Operating Humidity	10% to 90% RH (Non-condensing)	
Dimensions	91 mm*91 mm*13.8 mm (L*W*H)	121mm*80mm*13.8mm (L*W*H)
Gross Weight	0.36 Kg	
Net Weight	0.27Kg	
Supported Software	ZKBio CVSecurity	
Installation	Wall-mount (Compatible with Asian Gang Box)	Wall-mount (Compatible with Single Gang Box)
Housing Material	Aluminium Alloy	Aluminium Alloy
Ingress Protection Rating	N/A	
Certifications	ISO14001, ISO9001, CE, FCC, RoHS	
FactoryID	AC01-VL06H-P17	AC01-VL07H-P17

1.4 Configuration

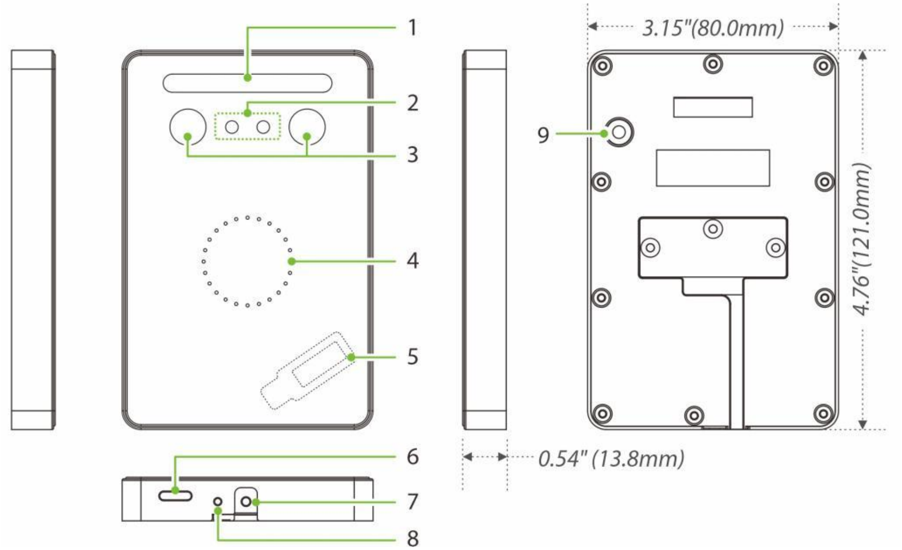


1.5 Appearance

KF1100 Pro



KF1200 Pro



Back Plate

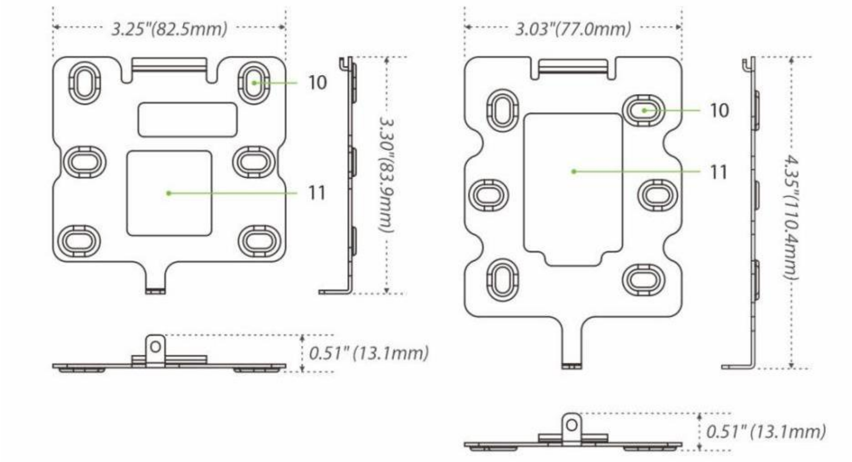


Figure 1-1 KF1100 Pro & KF1200 Pro Appearance

Table 1-1 Description

No.	Description
1	Flash
2	Camera
3	Near-Infrared Flash
4	LED Indicator
5	Receive Antenna / Card Reading Area
6	Speaker
7	Tamper Switch
8	Restart Button
9	Reset Button
10	Mounting Hole
11	Wiring Hole

Remarks:

- *If you forget the WebServer password, you can restore the factory settings by pressing and holding the* ***Reset Button*** *for* ***5*** *seconds, and then logging in again with the initial password. This function does not have any clear registered user data.*

- *The KF1000 Pro series reader supports tamper alarm function in both encryption and unencrypted modes of 485 communication. When the reader is illegal tampering, it will send a tamper signal to the controller via 485, and the controller will report to the software to form a tamper alarm event. Users can configure the alarm linkage on the software side and connect the alarm to the auxiliary output.*

2 Installation Set-up

2.1 Safety Precautions

- Make sure the device in the package is in good condition and all the assembly parts are included.
- Make sure that the operating voltage is the same one labelled on the attendance device.
- Make sure all the related equipment is power-off during the installation.
- Keep the device away from water or dampness. Prevent water or moisture from entering the chassis of the attendance device.
- Do not place the device on an unstable case or desk. The device might be damaged severely in case of a fall.
- Do not open the chassis when the attendance device is operating or when electrical hazards are present to avoid electrical shocks.

2.2 Installation Site

The device must be installed indoors adequate clearance is reserved at the air inlet/exhaust vents for heat dissipation.

2.3 Installation Steps

Make sure that the device is installed as per the installation instructions. Otherwise, you will bear any consequence resulting from your actions.

Step 1: Attach the mounting template sticker to the wall, and drill holes according to the mounting paper.

Step 2: Fix the back plate on the wall using wall mounting screws.

Step 3: After passing the wires through the wiring hole and connecting them to the device, and then attach the device to the back plate from top to bottom.

Step 4: Fasten the device to the back plate with a security screw.

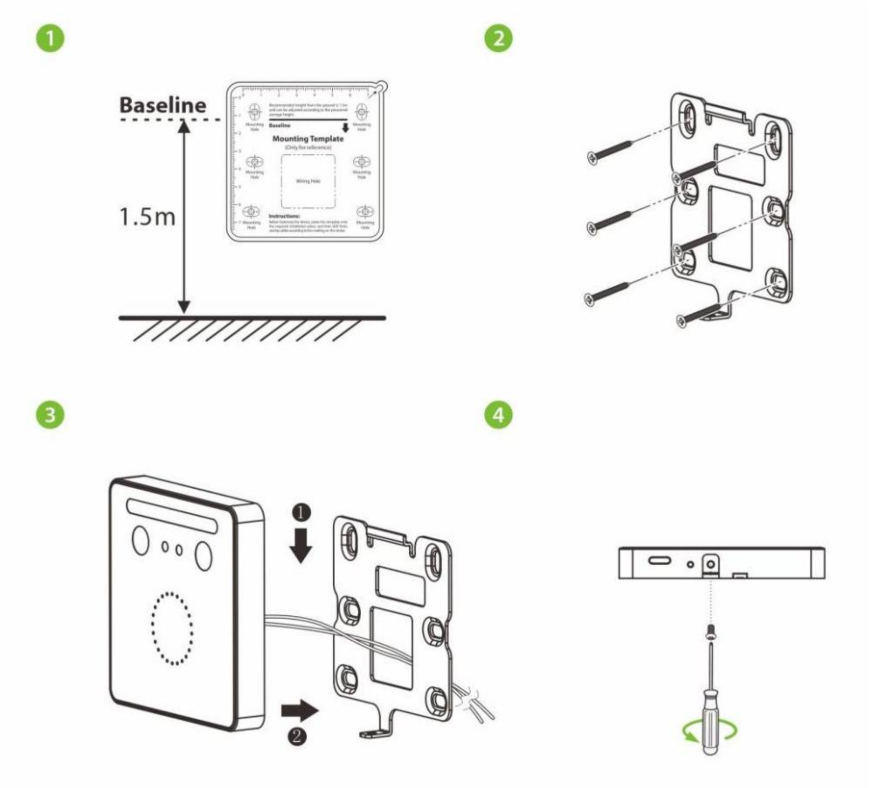


Figure2-1 KF1000 Pro Series Installation

Notes:

- *The installation method of KF1200 Pro is the same as that of KF1100 Pro. Only KF1100 Pro is used as an example, and will not be repeated here again.*
- *The KF1100 Pro series is compatible with the Asian gang box, and the KF1200 Pro series is compatible with the Single Gang box.*

3 Terminal and Wiring Description

3.1 Terminal Description

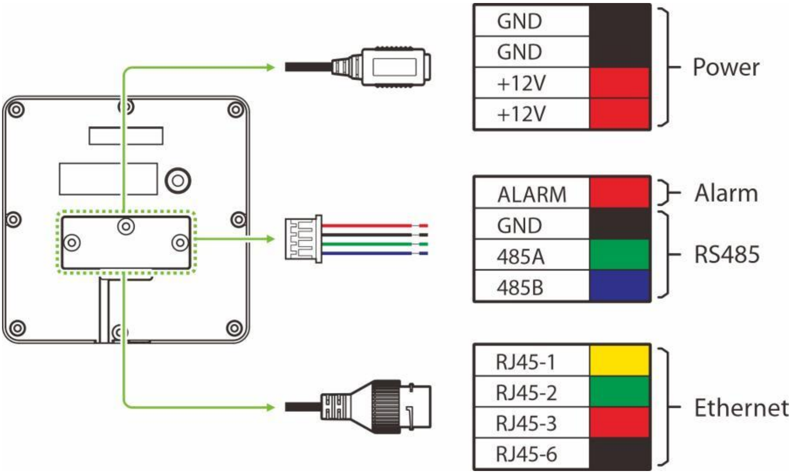


Figure 3-1 Terminal Description

Table 3-1 Description of Terminal and Interfaces

Name	Interface	Description
Power	GND	12V DC Input ***Note:*** *Minimum AC adapter:**12V, 1.5A**,* *Recommended AC adapter:**12V, 3A***.
	GND	
	+12V	
	+12V	
Alarm	ALARM	Alarm Input

Name	Interface	Description
RS485	GND	Grounding
	485A	RS485 Communication Interface For connecting to DM10/inBio Pro Plus Series. ***Note:*** *User need to enable the DM10 function on the WebServer to access it.*
	485B	
Ethernet	LAN	Network Interface

3.2 Power Wiring

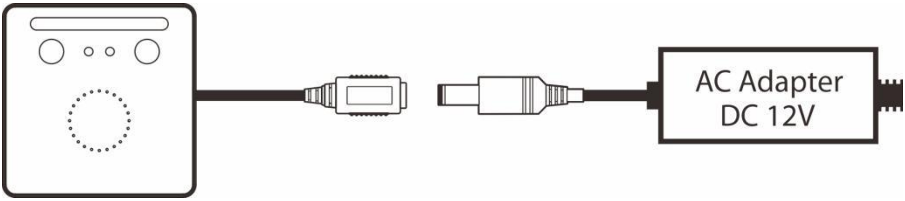


Figure 3-2 Power Wiring

Notes:

- *Minimum AC adapter:**12V,1.5A**, Recommended AC adapter:**12V, 3A**.*
- *To share the power with other devices, use an AC adapter with higher current ratings.*
- *Users need to configure their own suitable power adapter according to the product power specifications.*

3.3 Network Wiring

Establish the connection between the device and the software using an Ethernet cable. An illustrative example is provided below:

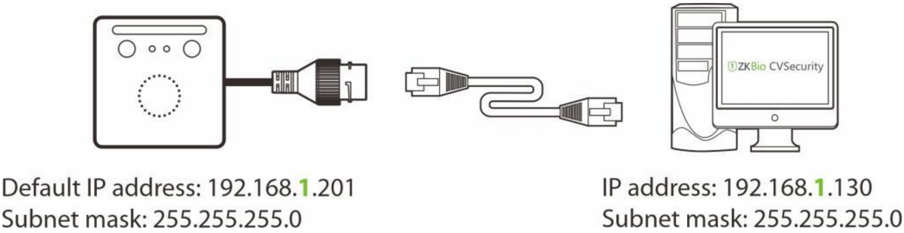

ZKBio CVSecurity
Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0
IP address: 192.168.1.130
Subnet mask: 255.255.255.0

Figure 3-3 Network Wiring

Notes:

- *On the WebServer page, click [**Advanced Settings**] > [**COMM.**] > [**IP Address**] to change the IP address and then click [**Confirm**].*
- *In LAN, the IP addresses of the server (PC) and the device must be in the same network segment while connecting to the ZKBio CVSecurity software.*

4 Device Operating Mode

The KF1000 Pro series has three device operating modes: Standalone Mode, Reader Background Identifying Mode and Face Server Mode.

4.1 Standalone Mode

In the standalone mode, the KF1000 Pro series can be used as an standalone to connect with the DM10 as shown in the wiring diagram below.

4.1.1 Wiring Diagram

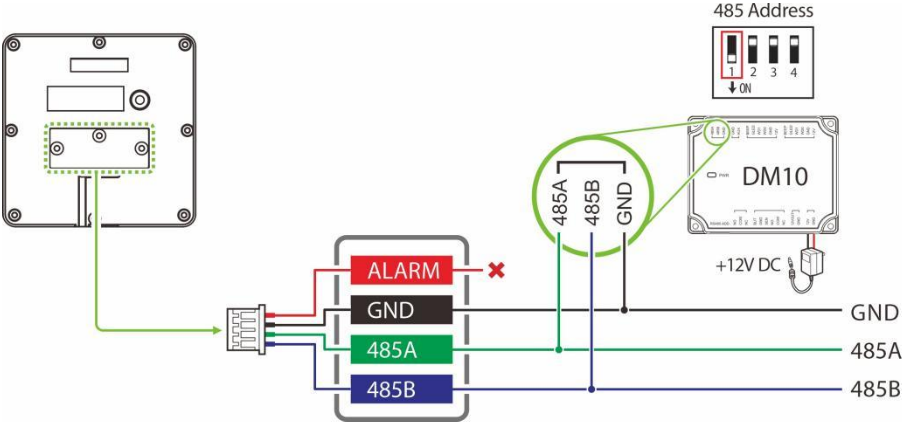


Figure 4-1 Wiring Diagram of KF1000 Pro Series and DM10

Notes:

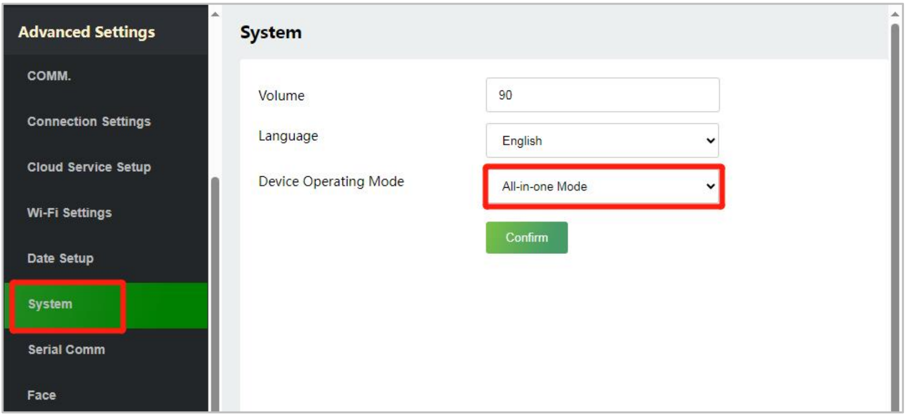
- *The DM10 can only be used in software if it is connected to the KF1000 Pro series via RS485.*
- *You need to switch the device operating mode to standalone mode on the*

WebServer and then enable the DM10 function manually to access it. For details, see 4.1.2.

- *Set the 485 address of DM10 to 1.*
- *A KF1000 Pro series only supports connecting one DM10.*
- *Each device requires a separate power supply.*
- *The DM10 can be extended to connect the smoke detector, Wiegand Reader, Door Sensor, Exit Button and Alarm.*

4.1.2 Parameter Configurations on the WebServer

1. Log in to the WebServer of the KF1000 Pro Series, see 5.1 Login to the WebServer for details.
2. Click [**Advanced Settings**] > [**System**] > [**Device Operating Mode**] > [**Standalone Mode**] to switch the device operating mode to standalone mode. After clicking [**Confirm**], the device will reboot to take effect.



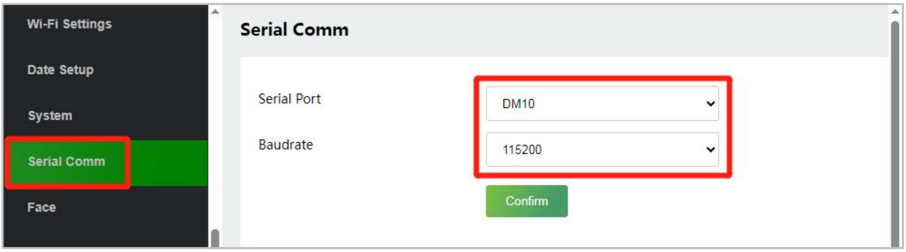
System

Volume: 90

Language: English

Device Operating Mode: All-in-one Mode

3. And then you need to manually enable the DM10 function on the WebServer to access. Click [**Advanced Settings**] > [**Serial Comm**] > [**Serial Port**] > [**DM10**] to set.The baudrate is set accordingly to **115200**.



Serial Comm

Serial Port: DM10

Baudrate: 115200

4.2 Reader Background Identifying Mode

In reader background identifying mode, the KF1000 Pro Series can communicate with the inBio Pro Plus controller via RS485. The wiring diagram is shown below.

4.2.1 Wiring Diagram

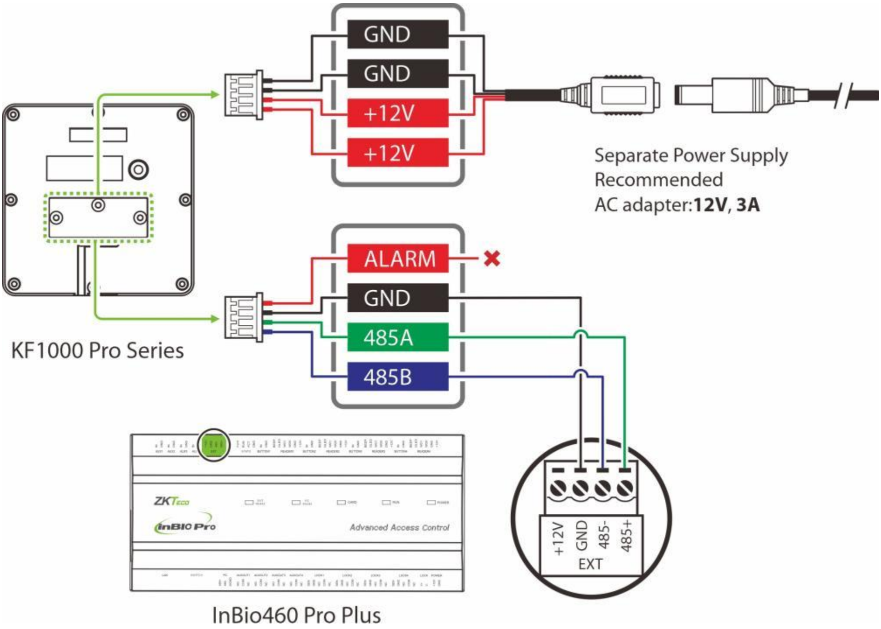


Figure 4-2 Wiring Diagram of KF1000 Pro Series and InBio460 Pro Plus

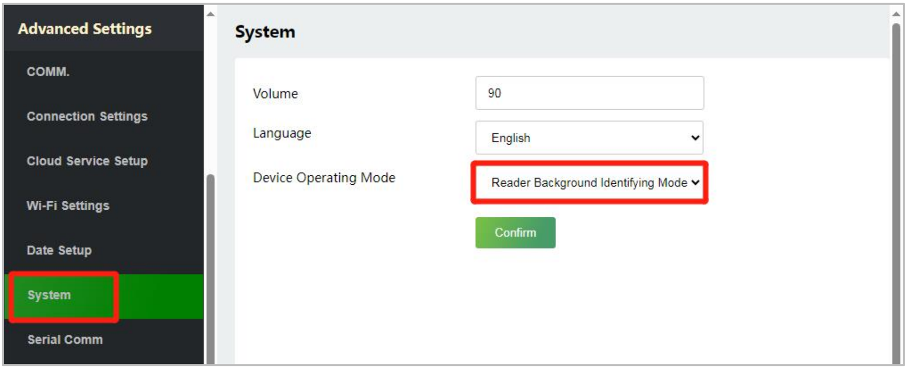
Notes:

- *The KF1000 Pro series requires a separate power supply.*
- *After the KF1000 Pro is wired according to normal RS485 wiring and the reader is configured in the software, it can communicate normally with the InBio Pro Plus controller, and the user verifies on the reader side, which supports the extraction of card number information and user face template information, and then transmits it to the back-end controller through 485 communication for verification and opens the door according to the user's authority.*

4.2.2 Parameter Configurations on the WebServer

1. Log in to the WebServerof the KF1000 Pro Series, see 5.1 Login to the WebServer for details.

2. Click [**Advanced Settings**] > [**System**] > [**Device Operating Mode**] > [**Reader Background Identifying Mode**] to switch the device operating mode to Reader Background Identifying Mode. After clicking [**Confirm**], the device reboots to take effect.



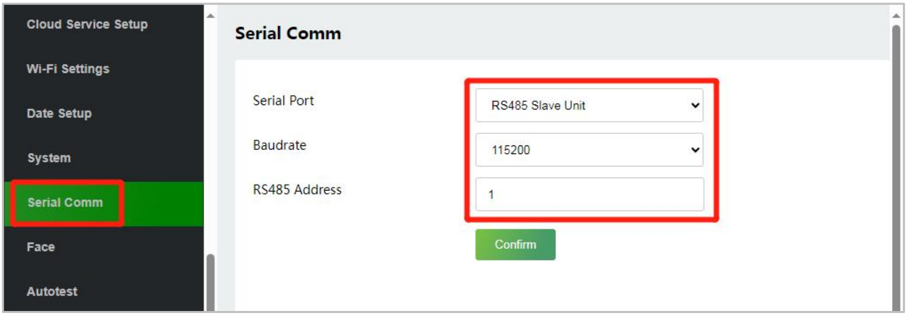
System

Volume: 90

Language: English

Device Operating Mode: Reader Background Identifying Mode

3. Click [**Serial Comm**] > [**Serial Port**] to set the serial port to [**RS485 Slave Unit**]. And then set the baud rate and enter the 485 address of the reader.



Serial Comm

Serial Port: RS485 Slave Unit

Baudrate: 115200

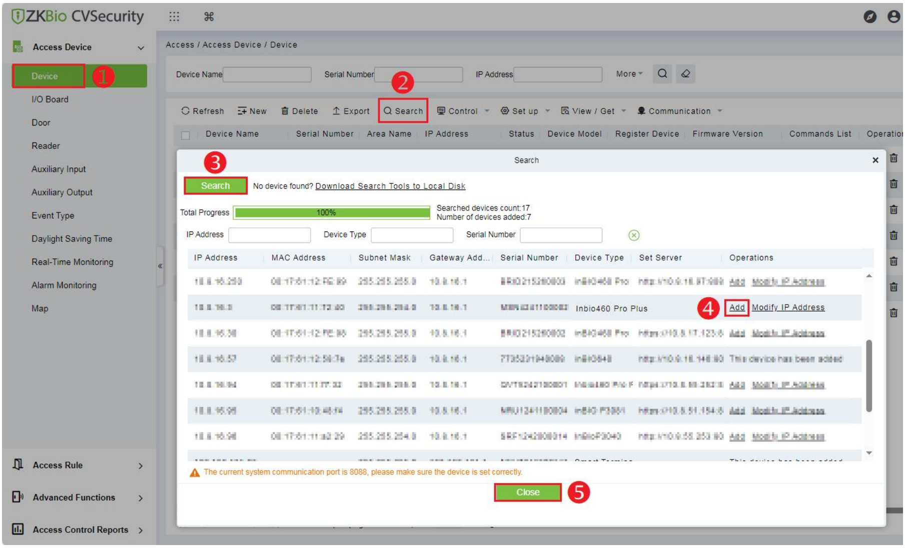
RS485 Address: 1

- **Serial Port:** Set to **RS485 Slave Unit.**
- **Baudrate:** The default is 115200, which is set according to the actual configuration of the controller.
- **RS485 address:** The 485 address of KF1000 Pro series reader.

4.2.3 Parameter Configurations on the Software

1. **Add Controller on the Software**

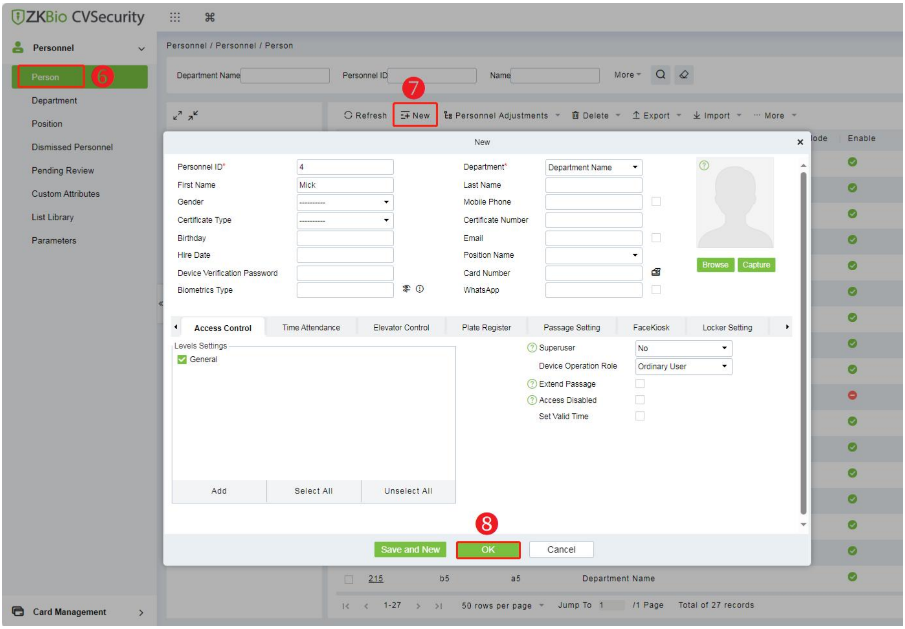
   1) Click [**Access**] **>** [**Access Device**] **>** [**Device**] **>** [**Search**], to open the Search interface in the software.
   2) Click [**Search**], and it will prompt [**Searching**……].
   3) After searching, the list and total number of access controllers will be displayed.
   4) Click [**Add**] 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) Click [**Personnel**] > [**Person**] > [**New**] to register a new user.
   6) Then click [**Access Device**] > [**Device**] > [**Control**] > [**Synchronize All Data to Devices**] to synchronize all the data to the device including the new users.



No device found? Download Search Tools to Local Disk

Searched devices count:17
Number of devices added:7

The current system communication port is 8088, please make sure the device is set correctly.



Personnel ID* 4

First Name Mick

Gender ---------

Certificate Type ---------

Birthday

Hire Date

Device Verification Password

Biometrics Type

Department* Department Name

Last Name

Mobile Phone

Certificate Number

Email

Position Name

Card Number

WhatsApp

☑ General

Superuser No

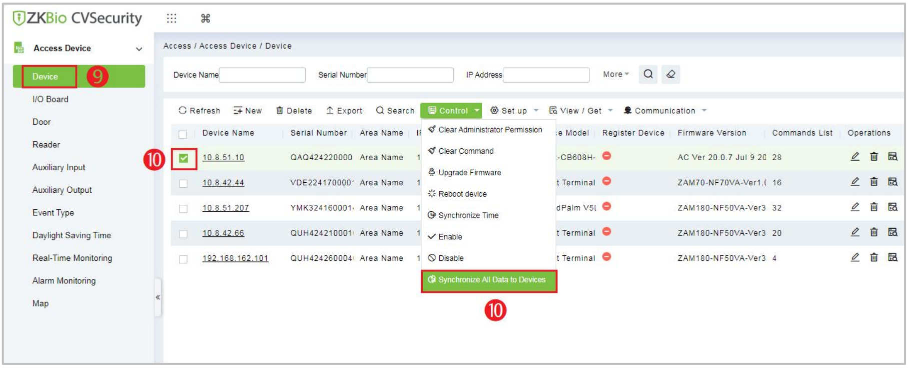
Device Operation Role Ordinary User

Extend Passage □

Access Disabled □

Set Valid Time □

215 b5 a5 Department Name



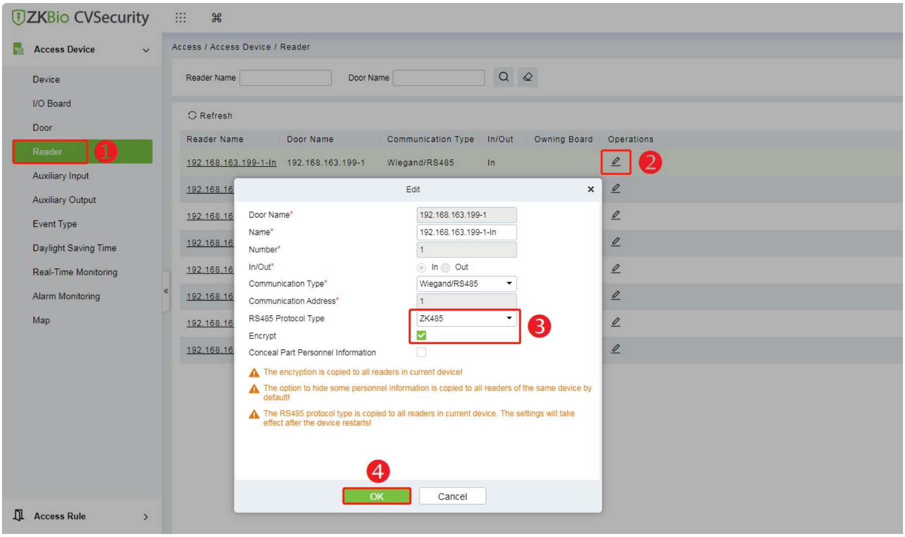
☐	Device Name	Serial Number	Area Name	IF	e Model	Register Device	Firmware Version	Commands List	Operations
☑	10.8.51.10	QAQ424220000	Area Name	1	-CB608H-	⛔	AC Ver 20.0.7 Jul 9 20	28	
☐	10.8.42.44	VDE224170000	Area Name	1	t Terminal	⛔	ZAM70-NF70VA-Ver1.(	16	
☐	10.8.51.207	YMK324160001	Area Name	1	dPalm V5L	⛔	ZAM180-NF50VA-Ver3	32	
☐	10.8.42.66	QUH424210001	Area Name	1	t Terminal	⛔	ZAM180-NF50VA-Ver3	20	
☐	192.168.162.101	QUH424260004	Area Name	1	t Terminal	⛔	ZAM180-NF50VA-Ver3	4	

2. Add Reader and Set the RS485 Protocol Type to ZK485

1) Click [**Access**] > [**Access Device**] > [**Reader**] to to enter the setting interface.

2) Then select the reader and click [**Edit**] icon ✎ behind it to enter the editing screen.

3) Change the RS485 Protocol Type to **ZK485** and check **Encrypt**.



Reader Name	Door Name	Communication Type	In/Out	Owning Board	Operations
192.168.163.199-1-In	192.168.163.199-1	Wiegand/RS485	In		✎

Edit

- Door Name*: 192.168.163.199-1
- Name*: 192.168.163.199-1-In
- Number*: 1
- In/Out*: ● In ○ Out
- Communication Type*: Wiegand/RS485
- Communication Address*: 1
- RS485 Protocol Type: ZK485
- Encrypt: ☑
- Conceal Part Personnel Information: ☐

⚠ The encryption is copied to all readers in current device!

⚠ The option to hide some personnel information is copied to all readers of the same device by default!

⚠ The RS485 protocol type is copied to all readers in current device. The settings will take effect after the device restarts!

4.2.4 Verification of Registered Users

When the KF1000 Pro reader completes the above RS485 wiring and parameter configuration, it can communicate normally with the InBio Pro Plus controller, and the user will be authenticated at the reader side, which supports extracting the card number information and the user's face template information, and then transmits them to the back-end controller for authentication and opening the door according to the user's authority through 485 communication.

Note:

- *For more details, please refer to the InBio Pro Plus User Manual and ZKBio CVSecurity User Manual.*

4.3 Face Server Mode

How to obtain the facial template information of personnel in the controller?

You need to configure the address of the face template extraction server in the personnel management of the software side, and add users and face photos in the place of face registration after configuration. Then the software will find the face template extraction server, send the face photo, after the server converts the template, it will send the face template back to the software, and then set the access control authority group on the software side, send the user data with the face template to the InBio Pro Plus controller. The operation steps are shown below.

4.3.1 Wiring Diagram

When multiple KF1000 Pro readers are connected to the InBio Pro Plus controller, the wiring is shown below. You can select any one of the readers as the converter, plug in the network cable to it, enable the face template extraction function, and set the address of the face template extraction server.

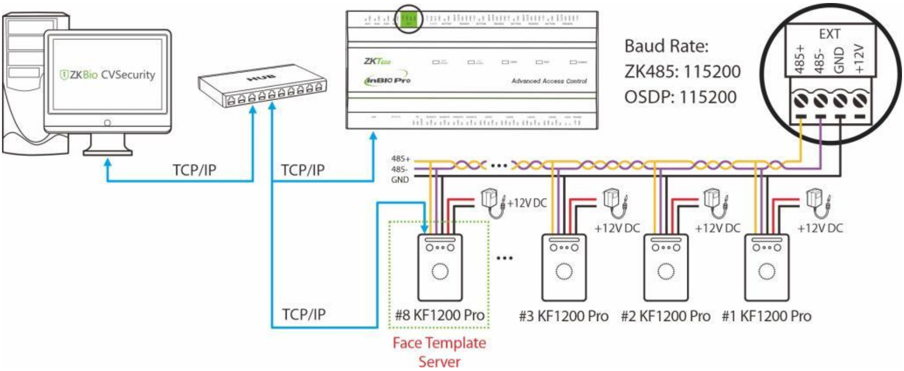


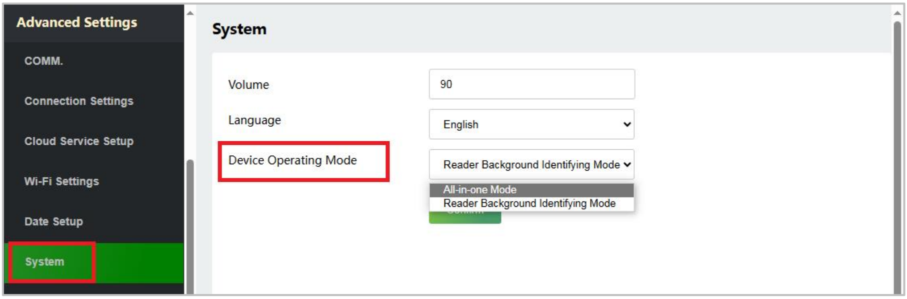
Figure 4-3 Wiring Diagram of Multiple Readers and Controller

Notes:

- *Each device requires a separate power supply.*
- *Select any one of these readers as a converter and plug in the network cable for it.*

4.3.2 Parameter Configurations on the WebServer

1. Log in to the WebServerof the KF1000 Pro Series, see 5.1 Login to the WebServer for details.
2. Click [**Advanced Settings**] > [**System**] > [**Device Operating Mode**] to switch the device operating mode. After clicking [**Confirm**], the device reboots to take effect. Set up according to actual needs. This is set to Reader Background Identifying Mode. **Note:** Face template extraction can be enabled for both device operating modes.
3. Then click [**Advanced Settings**] > [**Serial Comm**] > [**Serial Port**] to set the appropriate serial port according to the actual situation.



System

Volume: 90

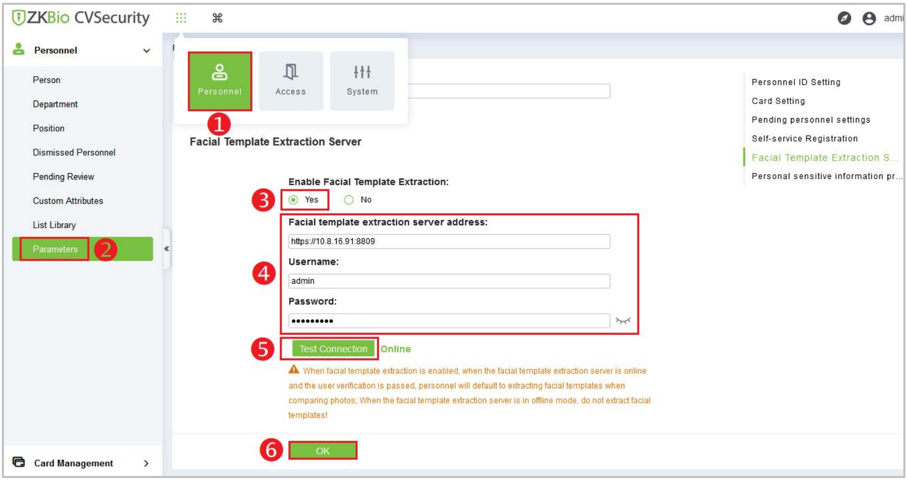
Language: English

Device Operating Mode: Reader Background Identifying Mode

4.3.3 Parameter Configurations on the Software

1. Setting the Facial Template Extraction Server

Log in to the ZKBio CVSecurity software and click [**Personnel**] > [**Personnel**] > [**Parameters**] to enable facial template extraction.



Facial Template Extraction Server

Enable Facial Template Extraction: ● Yes ○ No

Facial template extraction server address: https://10.8.16.91:8809

Username: admin

Password: •••••••••

Online

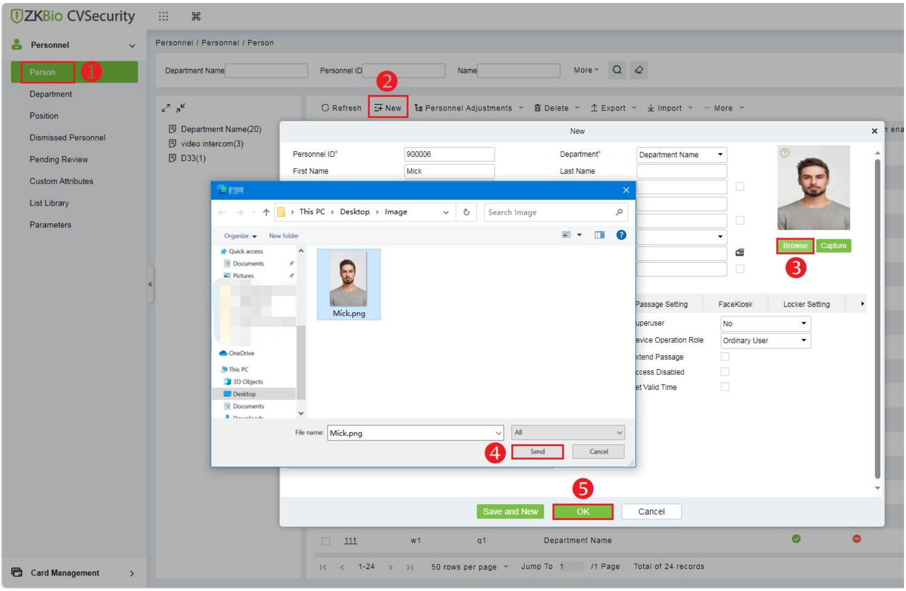
⚠ When facial template extraction is enabled, when the facial template extraction server is online and the user verification is passed, personnel will default to extracting facial templates when comparing photos; When the facial template extraction server is in offline mode, do not extract facial templates!

- **Facial template extraction server address:** Enter the server address, the default port number is **8809**.
- **Username:** Enter the Webserver user name for the KF1000 Pro series reader.
- **Password:** Enter the Webserver password for the KF1000 Pro series reader.

2. Adding Photos to the Software

Upload a photo for the person to use to capture the face template.

1) Click [**Personnel**] > [**Person**] > [**New]** > [**Browse**] to find the photo you need to upload.
2) Then click [**Send**] to comfirm and follow the prompts.
3) After entering the person's information, click [**OK**] to save and exit.



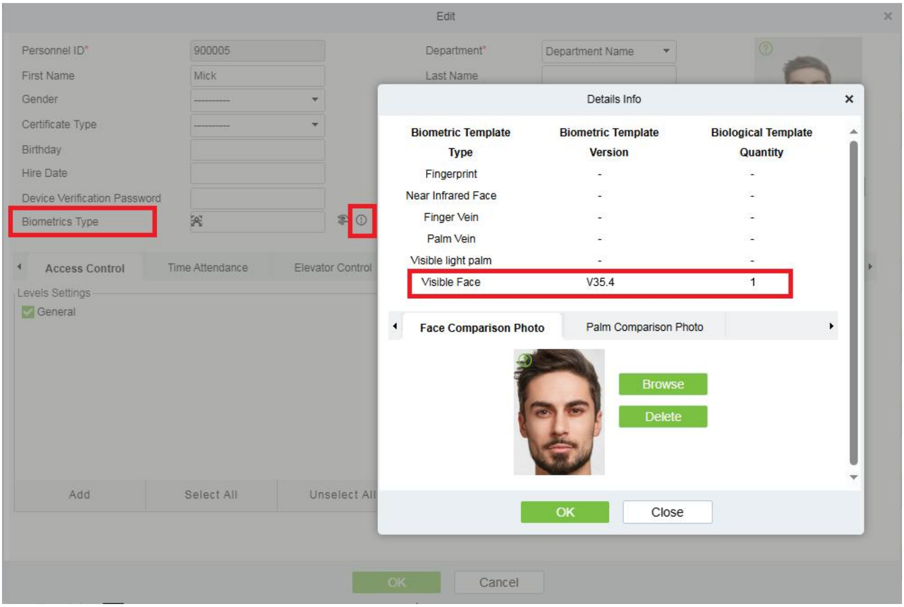
Personnel ID*: 900006
First Name: Mick
Department*: Department Name
Last Name:
Superuser: No
Device Operation Role: Ordinary User
Extend Passage □
Access Disabled □
Set Valid Time □
File name: Mick.png
All

111 w1 q1 Department Name

1-24 50 rows per page Jump To 1 /1 Page Total of 24 records

Note: *For better verification results, please make sure the photos are clear and avoid over-retouching.*

4) After the Face Template Extraction Server has converted the photo conversion to a template, click the ⓘ icon after Biometrics Type to view the template information for the person, as shown in the following figure.



Edit

Personnel ID* 900005

First Name Mick

Gender ----------

Certificate Type ----------

Birthday

Hire Date

Device Verification Password

Biometrics Type

Department* Department Name

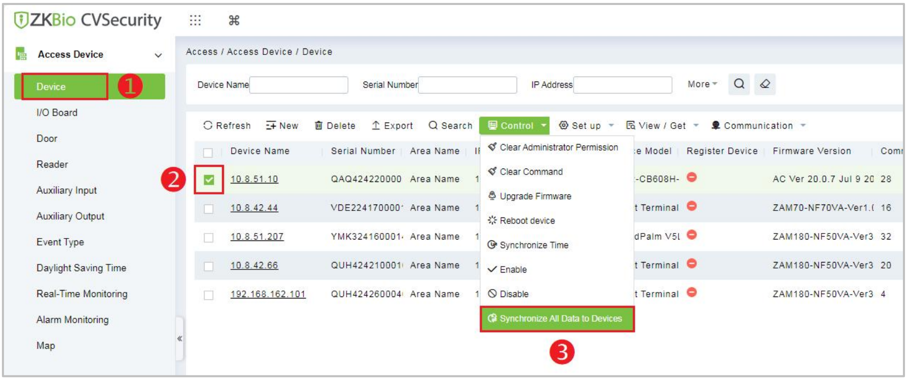
Last Name

Details Info

Biometric Template Type	Biometric Template Version	Biological Template Quantity
Fingerprint	-	-
Near Infrared Face	-	-
Finger Vein	-	-
Palm Vein	-	-
Visible light palm	-	-
Visible Face	V35.4	1

3. Synchronize All Data to Devices

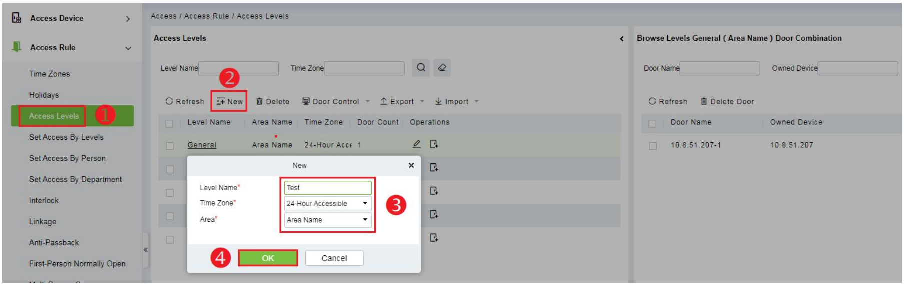
Then click [**Access Device**] > [**Device**] > [**Control**] > [**Synchronize All Data to Devices**] to synchronize all the data to the device including the new users.



☐	Device Name	Serial Number	Area Name	IF	e Model	Register Device	Firmware Version	Com
☑	10.8.51.10	QAQ424220000	Area Name	1	-CB608H-	⛔	AC Ver 20.0.7 Jul 9 20	28
☐	10.8.42.44	VDE224170000	Area Name	1	t Terminal	⛔	ZAM70-NF70VA-Ver1.(	16
☐	10.8.51.207	YMK324160001	Area Name	1	dPalm V5L	⛔	ZAM180-NF50VA-Ver3	32
☐	10.8.42.66	QUH424210001	Area Name	1	t Terminal	⛔	ZAM180-NF50VA-Ver3	20
☐	192.168.162.101	QUH424260004	Area Name	1	t Terminal	⛔	ZAM180-NF50VA-Ver3	4

4. Set Access Levels Group

1) Click [**Access**] > [**Access Rule**] > [**Access Levels**] to enter the setting interface.
2) Click [**New**] to add a new access level group.
3) Enter the level name, time zones and setting area, then click [**OK**] to confirm and exit.



Level Name	Area Name	Time Zone	Door Count
General	Area Name	24-Hour Acce	1

Door Name	Owned Device
10.8.51.207-1	10.8.51.207

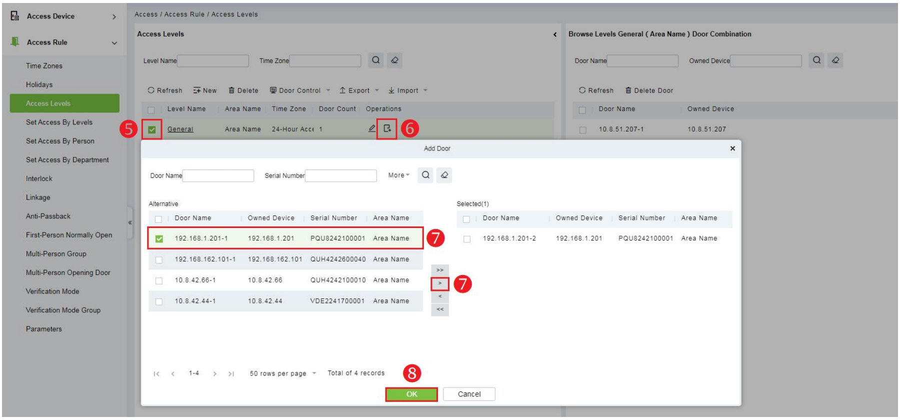
New

Level Name* Test

Time Zone* 24-Hour Accessible

Area* Area Name

4) After adding successfully, check the levels group.
5) Click [**Add Door**] icon in the levels group bar to open the settings window.
6) Select the door and then click > to move it to the selected column on the right.
7) Click [**OK**] to confirm and exit.



	Level Name	Area Name	Time Zone	Door Count	Operations
☑	General	Area Name	24-Hour Acce	1	

	Door Name	Owned Device
□	10.8.51.207-1	10.8.51.207

Alternative

	Door Name	Owned Device	Serial Number	Area Name
☑	192.168.1.201-1	192.168.1.201	PQU8242100001	Area Name
□	192.168.162.101-1	192.168.162.101	QUH4242600040	Area Name
□	10.8.42.66-1	10.8.42.66	QUH4242100010	Area Name
□	10.8.42.44-1	10.8.42.44	VDE2241700001	Area Name

Selected(1)

	Door Name	Owned Device	Serial Number	Area Name
□	192.168.1.201-2	192.168.1.201	PQU8242100001	Area Name

5. Set Access By Levels

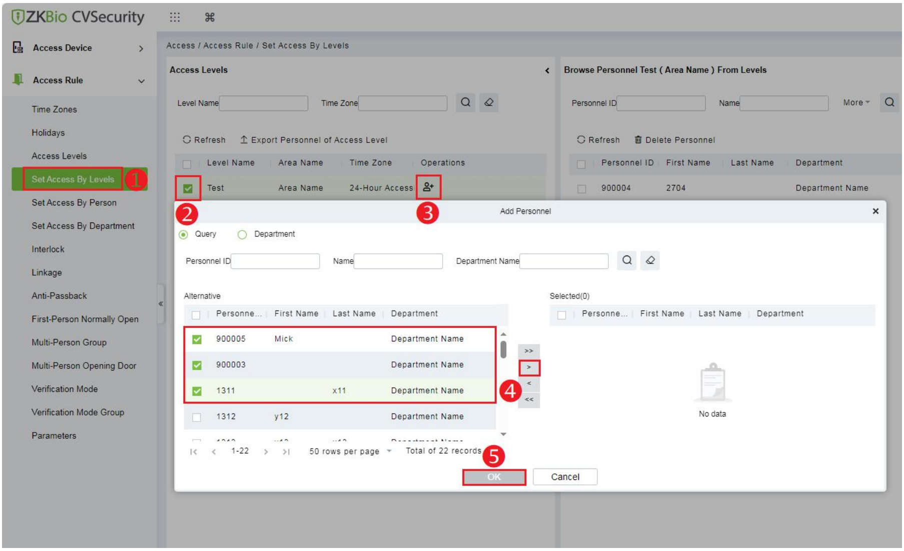
Add personnel to the elevator control level group.

1) Click [**Access**] > [**Access Rule**] > [**Set Access By Levels**] to enter the setting interface.

2) Check the levels group and click the 👤+ [**Add Personnel**] icon in its bar to open the settings window.

3) Select the person and then click > to move it to the selected column on the right.

4) Click [**OK**] to confirm and exit.



Level Name	Area Name	Time Zone	Operations
Test	Area Name	24-Hour Access	

Personnel ID	First Name	Last Name	Department
900004	2704		Department Name

Alternative

Personne...	First Name	Last Name	Department
☑ 900005	Mick		Department Name
☑ 900003			Department Name
☑ 1311		x11	Department Name
□ 1312	y12		Department Name

Selected(0)

Personne...	First Name	Last Name	Department

6. Set Access By Person

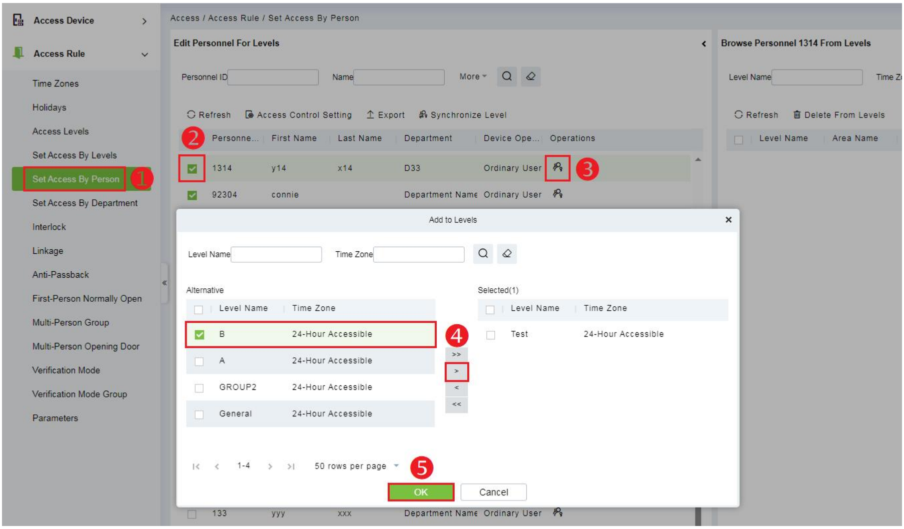
Edit the access level group for personnel.

1) Click [**Access**] > [**Access Rule**] > [**Set Access By Person**] to enter the setting interface.

2) Check the levels group and click the [**Add to Levels**] icon in its bar to open the settings window.

3) Select the levels group and then click > to move it to the selected column on the right.

4) Click [**OK**] to confirm and exit.



Personne...	First Name	Last Name	Department	Device Ope...	Operations
☑ 1314	y14	x14	D33	Ordinary User	
☑ 92304	connie		Department Name	Ordinary User	
□ 133	yyy	xxx	Department Name	Ordinary User	

Alternative

Level Name	Time Zone
☑ B	24-Hour Accessible
□ A	24-Hour Accessible
□ GROUP2	24-Hour Accessible
□ General	24-Hour Accessible

Selected(1)

Level Name	Time Zone
□ Test	24-Hour Accessible

7. Set Access By Department

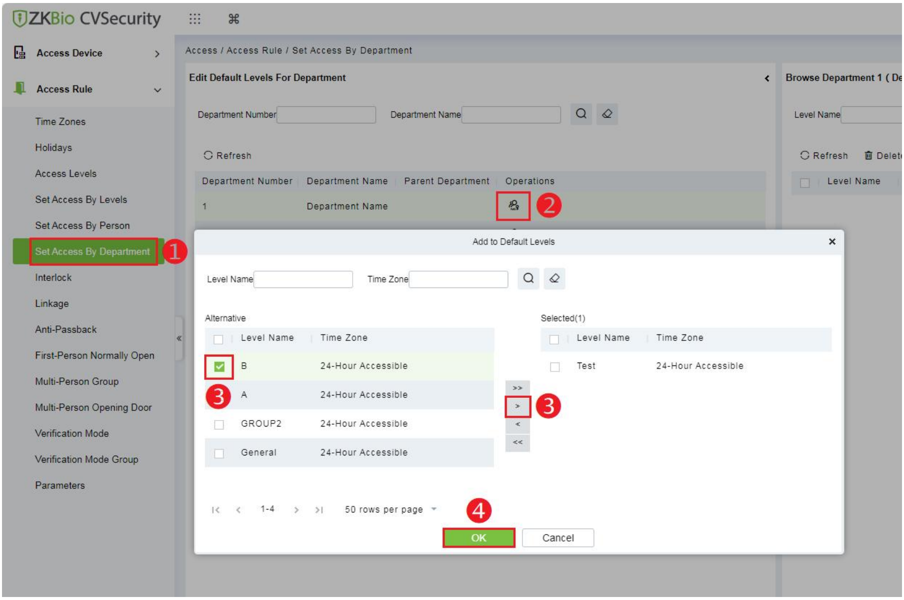
Edit the elevator control level group for the department.

1) Click [**Access**] > [**Access Rule**] > [**Set Access By Department**] to enter the setting interface.

2) Check the department and click the [**Add to Default Levels**] icon in its bar to open the settings window.

3) Select the levels group and then click > to move it to the selected column on the right.

4) Click [**OK**] to confirm and exit.



Department Number	Department Name	Parent Department	Operations
1	Department Name		

Alternative

	Level Name	Time Zone
☑	B	24-Hour Accessible
□	A	24-Hour Accessible
□	GROUP2	24-Hour Accessible
□	General	24-Hour Accessible

Selected(1)

	Level Name	Time Zone
□	Test	24-Hour Accessible

4.3.4 Facial Recognition Matching

After completing all the parameter settings, the device completes the operation of face matching verification through the following steps.

Acquisition: The KF1000 Pro converter extracts template information from photos sent by the software and saves it to the software, which then sends it to the controller.

Comparison: KF1000 Pro collects the compared face templates directly from the camera and transmits them to the controller via 485 for comparison.

5 Configuration via WebServer

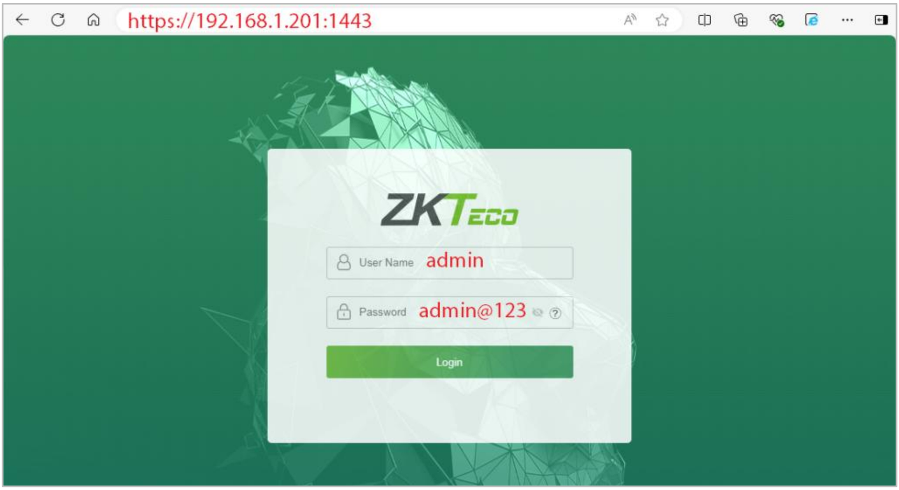
5.1 Login to the WebServer

After the device is powered on, connect the device using a network cable. Then open the recommended browser and input the IP address and server port in the address bar. The IP address is set as: https://device IP address: Port (for example: https://192.168.1.201:1443).

- **Device IP address: 192.168.1.201** is the default. You can modify the address on the WebServer through the following path: [**Advanced Settings**] > [**COMM.**] > [**IP Address**].
- **Port: 1443** is the default.

Login to the WebServer

After opening the webserver login page. You may input the username which is [**Admin**] by default. And the default password for the new user is [**admin@123**].



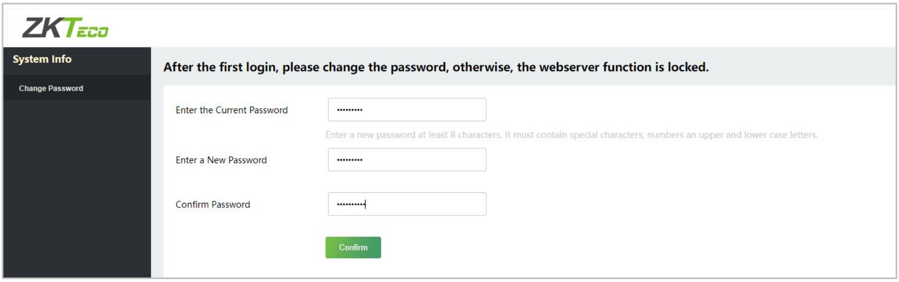
https://192.168.1.201:1443

User Name admin

Password admin@123

Change the Password

After the first login, please change the password; otherwise, the webserver function will be locked.



After the first login, please change the password, otherwise, the webserver function is locked.

Enter the Current Password: •••••••••

Enter a new password at least 8 characters. It must contain special characters, numbers an upper and lower case letters.

Enter a New Password: •••••••••

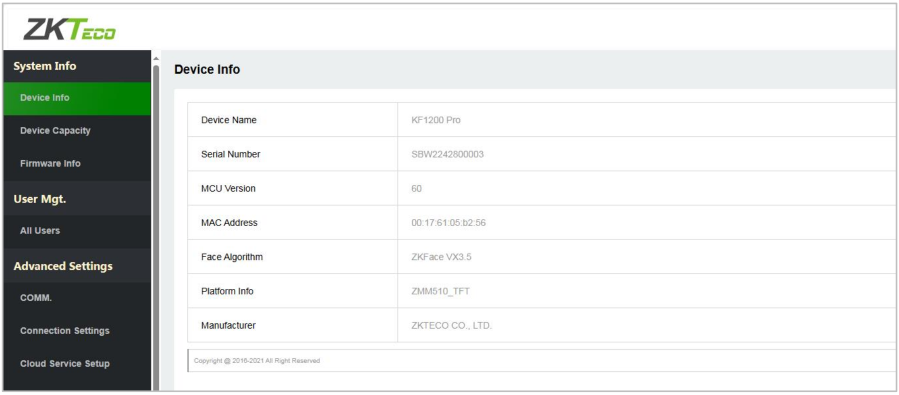
Confirm Password: ••••••••••

5.2 System Information

The System Information includes the device, device capacity and firmware information.

5.2.1 Device Information

The Device Information displays the Device Name, Serial Number, MCU Version, MAC Address, Face Algorithm, Platform Information Manufacturer, and Manufacture Date.



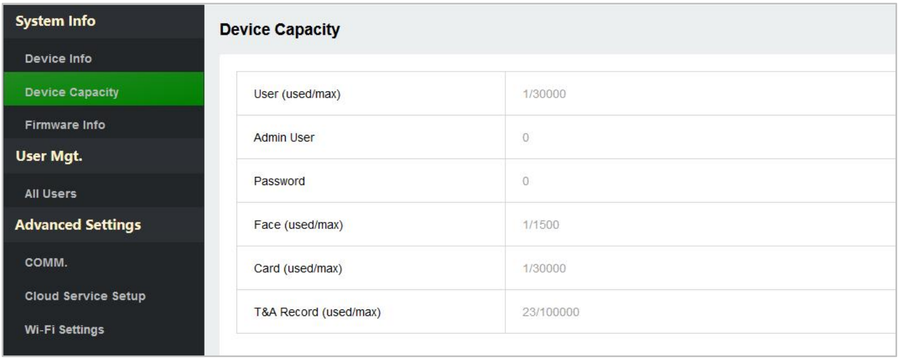
Device Info

Device Name	KF1200 Pro
Serial Number	SBW2242800003
MCU Version	60
MAC Address	00:17:61:05:b2:56
Face Algorithm	ZKFace VX3.5
Platform Info	ZMM510_TFT
Manufacturer	ZKTECO CO., LTD.

Copyright @ 2016-2021 All Right Reserved

5.2.2 Device Capacity

The Device Capacity displays the User Capacity, Admin User, Password, the used/max capacity of Face, the used/max capacity of Card, and the used/max capacity of T&A Record.

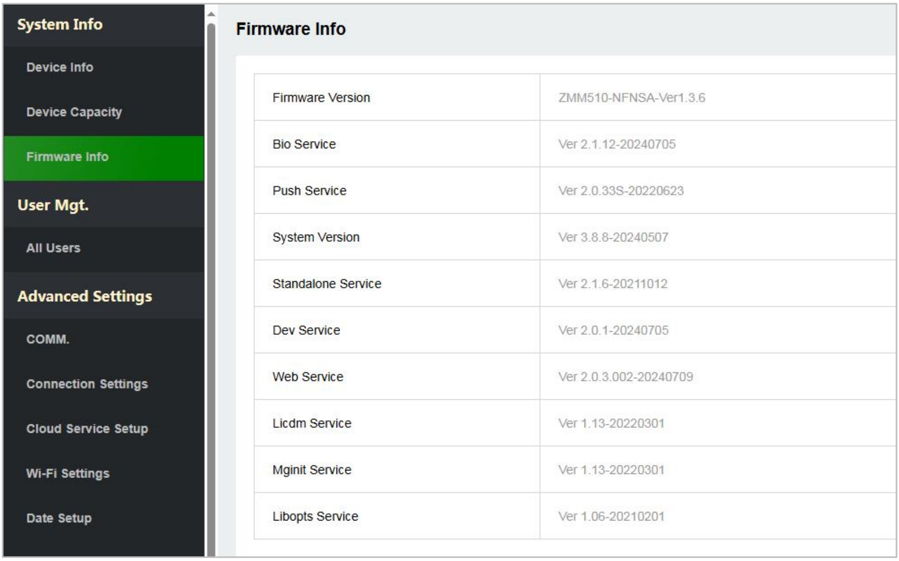


Device Capacity

User (used/max)	1/30000
Admin User	0
Password	0
Face (used/max)	1/1500
Card (used/max)	1/30000
T&A Record (used/max)	23/100000

5.2.3 Firmware Information

Displays the firmware version and other version information of the device.

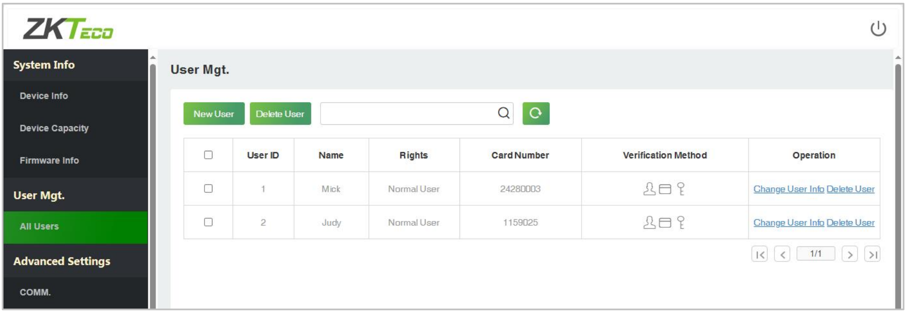


Firmware Info

Firmware Version	ZMM510-NFNSA-Ver1.3.6
Bio Service	Ver 2.1.12-20240705
Push Service	Ver 2.0.33S-20220623
System Version	Ver 3.8.8-20240507
Standalone Service	Ver 2.1.6-20211012
Dev Service	Ver 2.0.1-20240705
Web Service	Ver 2.0.3.002-20240709
Licdm Service	Ver 1.13-20220301
Mginit Service	Ver 1.13-20220301
Libopts Service	Ver 1.06-20210201

5.3 User Management

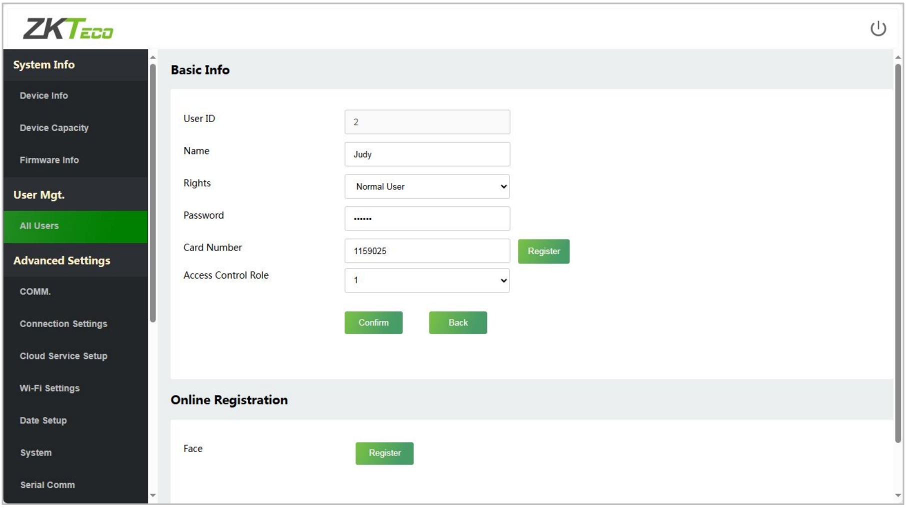
You can manage the basic information of the registered users, including User ID, Name, Rights, Card Number, and Verification Mode in the User Management.



□	User ID	Name	Rights	Card Number	Verification Method	Operation
□	1	Mick	Normal User	24280003		Change User Info Delete User
□	2	Judy	Normal User	1159025		Change User Info Delete User

5.3.1 Add User

1. Click [**User Mgt.**] > [**All Users**] > [**New User**]to register a new user.



User ID	2
Name	Judy
Rights	Normal User
Password	······
Card Number	1159025
Access Control Role	1
Face	

2. Enter the User ID, Name, Password, Card, setting user role and access control role.

3. Click [**Register**] on the card number bar and then place the card in the card induction area to register. After successful registration, the card number will be displayed on the input field.

4. After entering the basic information, click [**Confirm**] to save and then the interface will pop up a "**Enrolled Successfully!**" prompt.

5. Select **Face** on the **Online Registration** window and click [**Register**] to enter the face registration mode. Then users need to face the camera and adjust the position of the face according to the prompt of the LED indicator of the device, so that all the important features of the face can be captured by the camera. Then stay still for a while during face registration until registration is successful and the LED indicator turns green.

5.3.2 Search for Users

Select the **All Users** option in the **User Mgt.** Then enter the retrieval keyword in the search bar of the user list (keyword may be an ID, surname, or full name). The system will search for the users related to the entered information.

5.3.3 Edit User

Choose a user from the list and select **Change User Info** to enter the edit user interface.

Note:

- *The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user's detail.*

5.3.4 Deleting Users

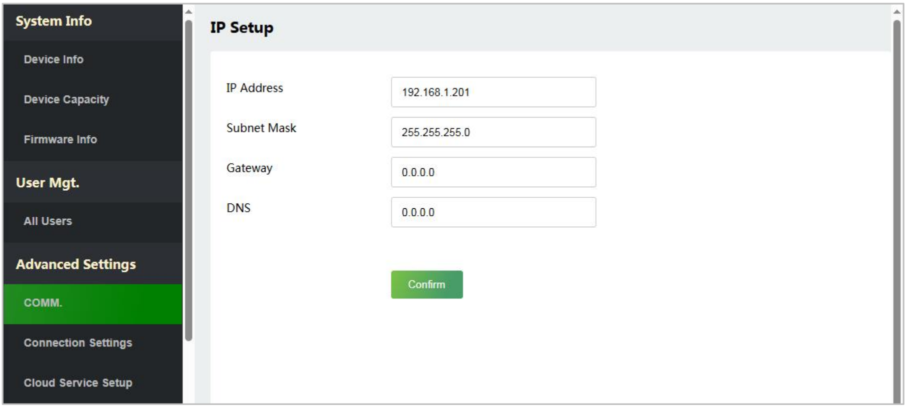
Choose a user from the list and select **Delete User**, all information of the user will be deleted.

5.4 Advanced Settings

On the advanced setting interface to set the relevant parameters as required. It includes options like Communication Settings, Connection Settings, Cloud Server Setup, Wireless Network, Data Setup, System Settings, Serial Comm, Face Setting, Autotest, and Wiegand Setup.

5.4.1 Communication Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.



IP Setup

IP Address: 192.168.1.201

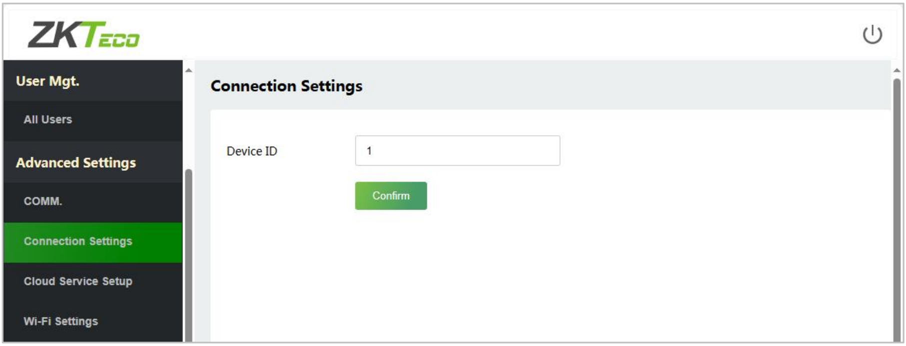
Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

DNS: 0.0.0.0

- **IP Address:** The default value is 192.168.1.201, it can be modified according to the available network parameters.
- **Subnet Mask:** The default value is 255.255.255.0, it can be modified according to the available network parameters.
- **Gateway:** The default value is 0.0.0.0, it can be modified according to the available network parameters.
- **DNS:** The default value is 0.0.0.0. Please set them according to the actual network situation.

5.4.2 Connection Settings



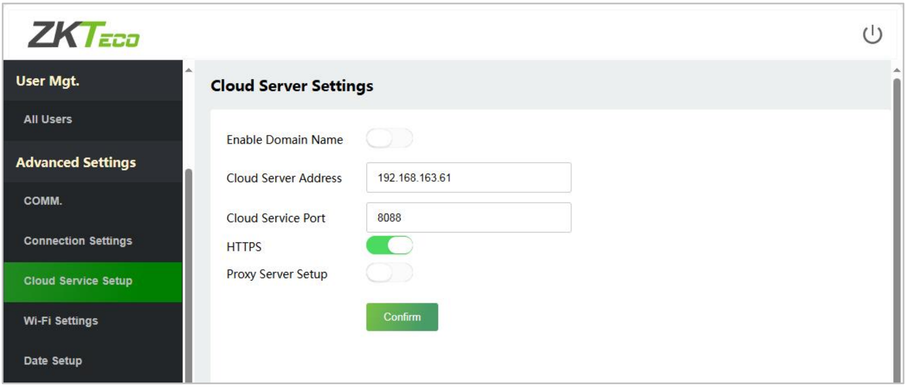
Connection Settings

Device ID: 1

- **Device ID:** Identity number of the device, which ranges between 1 and 254. If the communication method is RS485, you need to input this device ID in the software communication interface.

5.4.3 Cloud Server Setting

The Cloud Server setting option helps to set different configurations used for connecting with the ADMS server.



Cloud Server Settings

Enable Domain Name: off

Cloud Server Address: 192.168.163.61

Cloud Service Port: 8088

HTTPS: on

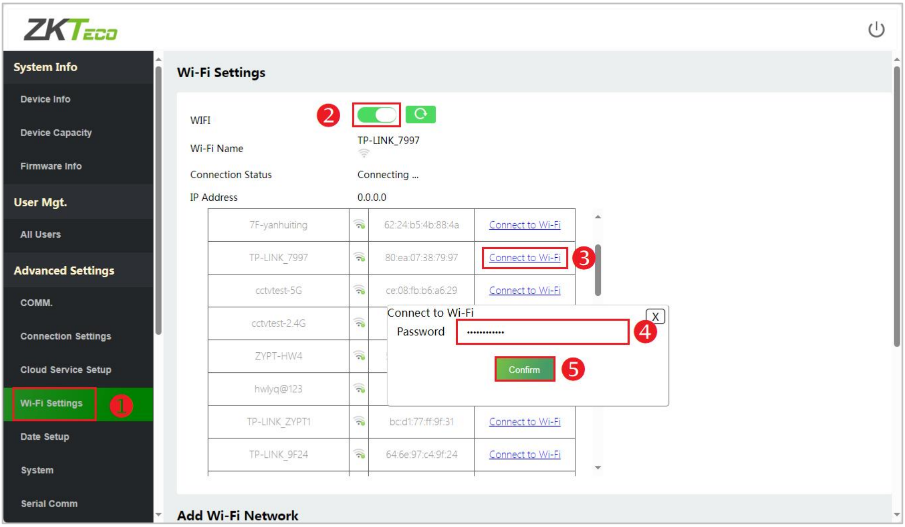
Proxy Server Setup: off

- **Enable Domain Name:** When this function is enabled, the domain name mode “http://...” is used, such as http://www.XYZ.com (XYZ denotes the domain name). When this mode is turned OFF, you need to enter the IP address and port to connect to the WebServer.

- **Cloud Server Address:** IP address of the ADMS server is required.
- **Cloud Server Port:** Port used by the ADMS server is required.
- **HTTPS:** It is an HTTP channel with security as its goal. Based on HTTP, transmission encryption and identity authentication ensure the security of the data transmission process.
- **Proxy Server Setup:** When a proxy is enabled, you need to set the IP address and port number of the proxy server.

5.4.4 Wireless Network★

The device supports the Wi-Fi module, which is built-in within the hardware, to enable data transmission via Wi-Fi and establish a wireless network environment. By default, the Wi-Fi is turned off. The user needs to enable and set the related parameters on the WebServer.



Wi-Fi Settings

WIFI

Wi-Fi Name TP-LINK_7997

Connection Status Connecting ...

IP Address 0.0.0.0

7F-yanhuiting		62:24:b5:4b:88:4a	Connect to Wi-Fi
TP-LINK_7997		80:ea:07:38:79:97	Connect to Wi-Fi
cctvtest-5G		ce:08:fb:b6:a6:29	Connect to Wi-Fi
cctvtest-2.4G			
ZYPT-HW4			
hwlyq@123			
TP-LINK_ZYPT1		bc:d1:77:ff:9f:31	Connect to Wi-Fi
TP-LINK_9F24		64:6e:97:c4:9f:24	Connect to Wi-Fi

Connect to Wi-Fi X

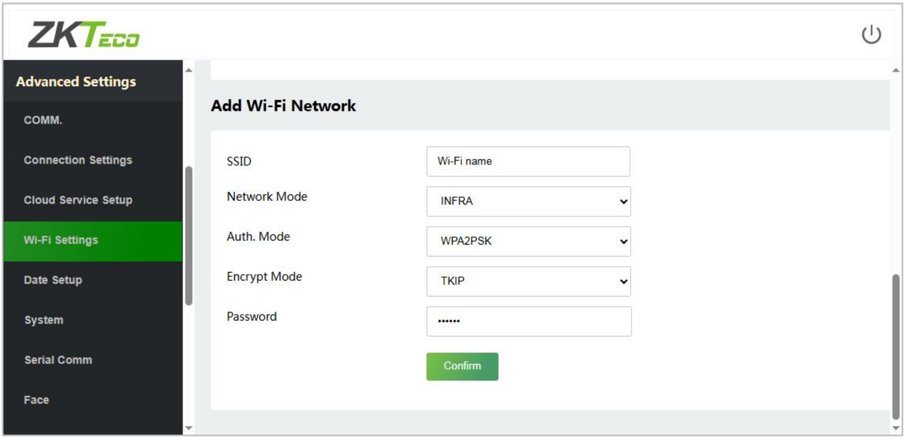
Password ············

Confirm

- Click the button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Click the required Wi-Fi in the Wi-Fi list and enter the correct password in the pop-up password screen, then click [**Confirm**] to connect.
- After successful verification, the connection status will display "**Connected**".

Adding Wi-Fi Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list. On the Add Wi-Fi Network screen, enter the parameters of the added Wi-Fi network. (The added network must exist.)



Add Wi-Fi Network

SSID: Wi-Fi name

Network Mode: INFRA

Auth. Mode: WPA2PSK

Encrypt Mode: TKIP

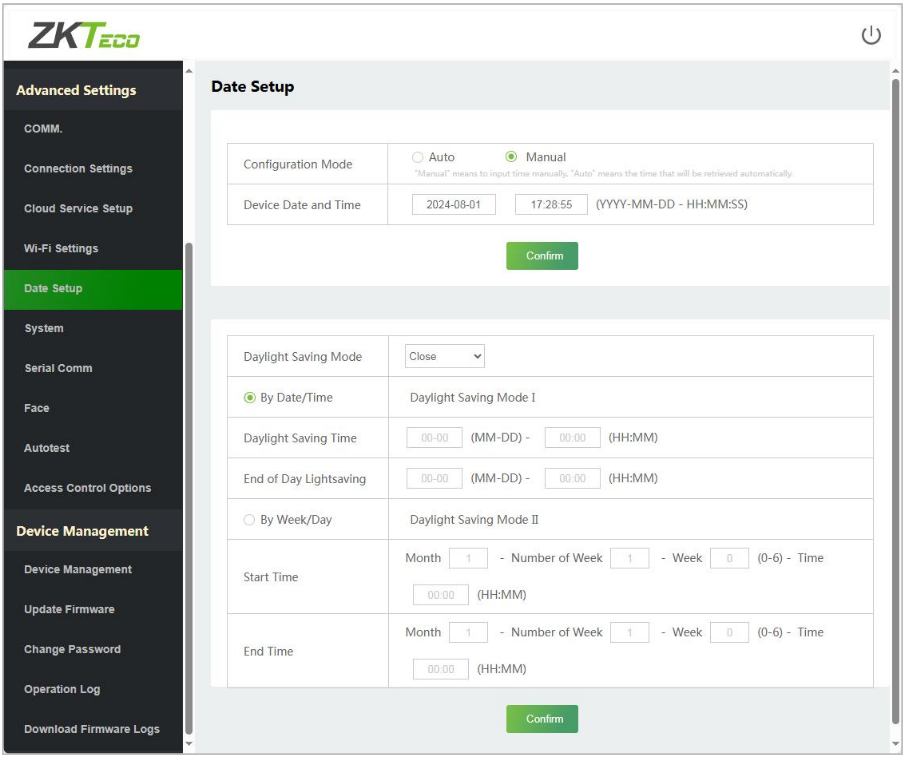
Password: ••••••

Confirm

Note:

- *After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name.*

5.4.5 Data/Time Settings



Date Setup

Configuration Mode	○ Auto ● Manual "Manual" means to input time manually, "Auto" means the time that will be retrieved automatically.
Device Date and Time	2024-08-01 17:28:55 (YYYY-MM-DD - HH:MM:SS)

Daylight Saving Mode	Close
● By Date/Time	Daylight Saving Mode I
Daylight Saving Time	00-00 (MM-DD) - 00:00 (HH:MM)
End of Day Lightsaving	00-00 (MM-DD) - 00:00 (HH:MM)
○ By Week/Day	Daylight Saving Mode II
Start Time	Month 1 - Number of Week 1 - Week 0 (0-6) - Time 00:00 (HH:MM)
End Time	Month 1 - Number of Week 1 - Week 0 (0-6) - Time 00:00 (HH:MM)

- **Configuration Mode:** To configure data and time, including automatic input and manual input. When Manual is selected, the date and time of the device can be entered manually.

- **Daylight Saving Mode:** Enable or disable the Daylight Saving Time Mode, by date/time mode and by week/day mode for selection.

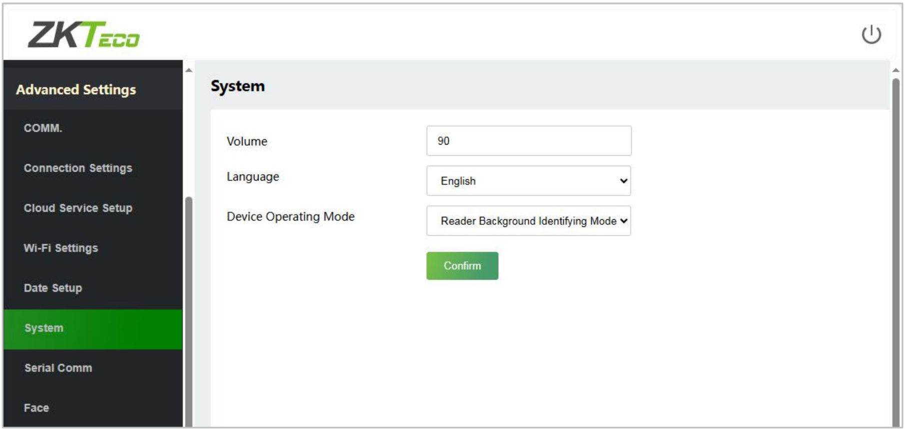
Notes:

- *DST, which is also called **Daylight Saving Time**, is a system adjusting local time to save energy. The time adopted during the set dates is called "DST". Usually, the time will be one hour forward in summer. This enables users to* *sleep or get up earlier, and also reduce device's lighting to save power. In autumn, the time will resume the standard time. Regulations are different in different countries. At present, nearly 110 countries adopt DST.*

- *To meet the demand of DST, a special option can be customized. Make the time one hour forward at XX (hour) XX (day) XX (month), and make the time one hour backward at XX (hour) XX (day) XX (month)*
- ***How to set the Daylight Saving Time?***

  For example, adjust the clock forward one hour at 08: 00 on April 1 and backward one hour at 08: 00 on October 1 (the system turns back to the original time).

5.4.6 System Settings



Volume: 90

Language: English

Device Operating Mode: Reader Background Identifying Mode

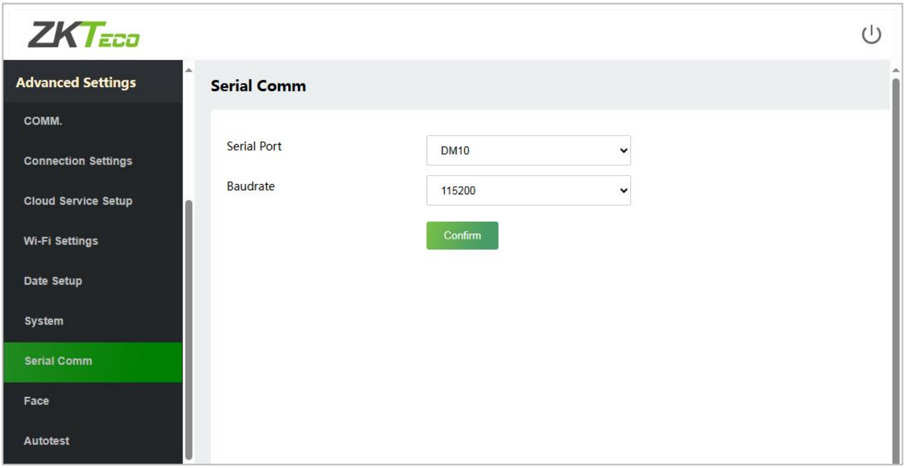
- **Volume:** Adjust the volume of device. The valid value ranges from 0 to 100.
- **Language:** To select the language of the device.
- **Device Operating Mode:** Used to switch the device operating mode, including: Standalone Mode and Reader Background Identifying Mode. The device reboots after the mode switch.

- ✧ **Standalone Mode:** Used in configuration with the DM10 to connect to the software via TCP or Wi-Fi.
- ✧ **Reader Background Identifying Mode:** In this mode, the InBio pro Plus controller can be connected via 485.

5.4.7 Serial Comm. Settings

Serial Comm function facilitates to establish communication with the device through a serial port (RS485).

When the device operation mode is switched to the **Standalone Mode**, the corresponding serial communication parameters are shown below.



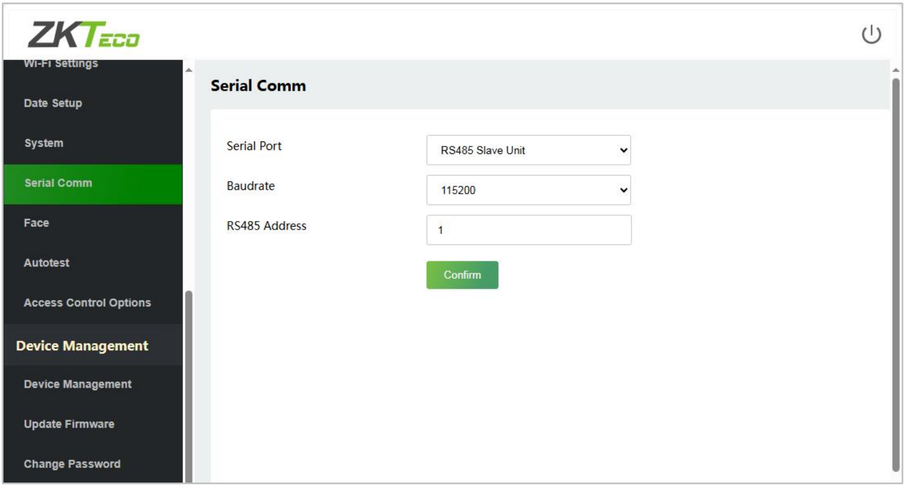
Serial Comm

Serial Port: DM10

Baudrate: 115200

- **Serial Port:** To connect the DM10.
- **Baudrate:** The rate of the communication with DM10; there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200 and 9600. The higher is the baud rate, the faster is the communication speed, but also the less reliable. In general, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.

When the device operation mode is switched to the **Reader Background Identifying Mode**, the corresponding serial communication parameters are shown below.



Serial Comm

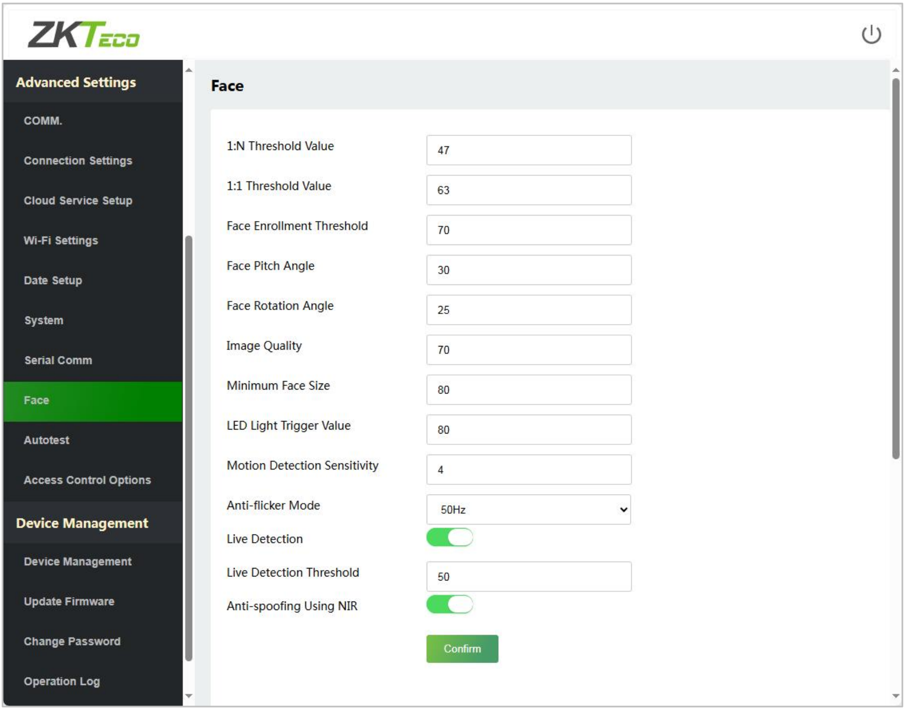
Serial Port: RS485 Slave Unit

Baudrate: 115200

RS485 Address: 1

- **Serial Port:** To connect the InBio Pro Plus controller via RS485.
- **Baudrate:** The rate of the communication with InBio Pro Plus; there are 5 options of baud rate: 115200 (default), 57600, 38400, 19200 and 9600. The higher is the baud rate, the faster is the communication speed, but also the less reliable. In general, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.
- **RS485 Address:** The 485 address of the reader.

5.4.8 Face Parameters



Face

1:N Threshold Value: 47
1:1 Threshold Value: 63
Face Enrollment Threshold: 70
Face Pitch Angle: 30
Face Rotation Angle: 25
Image Quality: 70
Minimum Face Size: 80
LED Light Trigger Value: 80
Motion Detection Sensitivity: 4
Anti-flicker Mode: 50Hz
Live Detection: On
Live Detection Threshold: 50
Anti-spoofing Using NIR: On

- **1:N Threshold Value:** Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value.

  The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgment rate and higher the rejection rate, and vice versa. The default value of 47 is recommended.

- **1:1 Threshold Value:** Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value.

The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgment rate and higher the rejection rate, and vice versa. The default value of 63 is recommended.

- **Face Enrollment Threshold:** During face enrollment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than the set threshold, it indicates that the face has already been registered.
- **Face Pitch Angle:** It is the pitch angle tolerance of a face for facial template registration and comparison. If a face's pitch angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
- **Face Rotation Angle:** It is the rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds the set value, it will be filtered by the algorithm, i.e., ignored by the terminal thus no registration and comparison interface will be triggered.
- **Image Quality:** It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
- **Minimum Face Size:** It sets the minimum face size required for facial registration and comparison.

  If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face.

  This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.

- **LED Light Trigger Value:** This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.

- **Motion Detection Sensitivity:** It sets the value for the amount of change in a camera's field of view known as potential motion detection that wakes up the terminal from standby to the comparison interface.

  The larger the value, the more sensitive the system would be, i.e., if a larger value is set, the comparison interface activates with much ease, and the motion detection is frequently triggered.

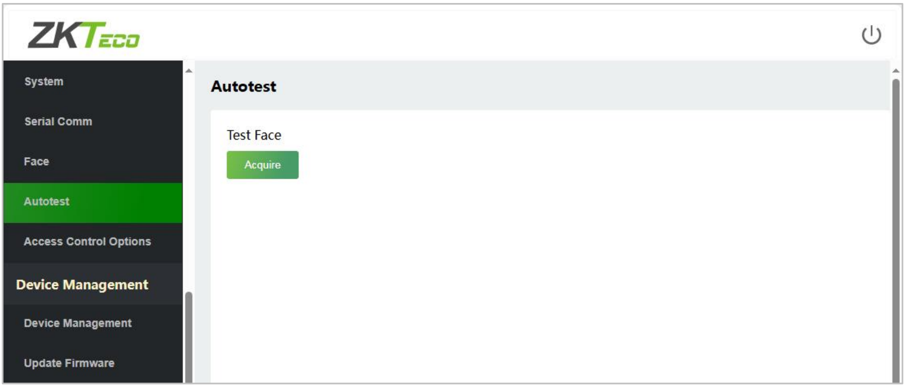
- **Anti-flicker Mode:** It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.

- **Live Detection:** It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.

- **Live Detection Threshold:** It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.

- **Anti-spoofing Using NIR:** Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.

5.4.9 Autotest

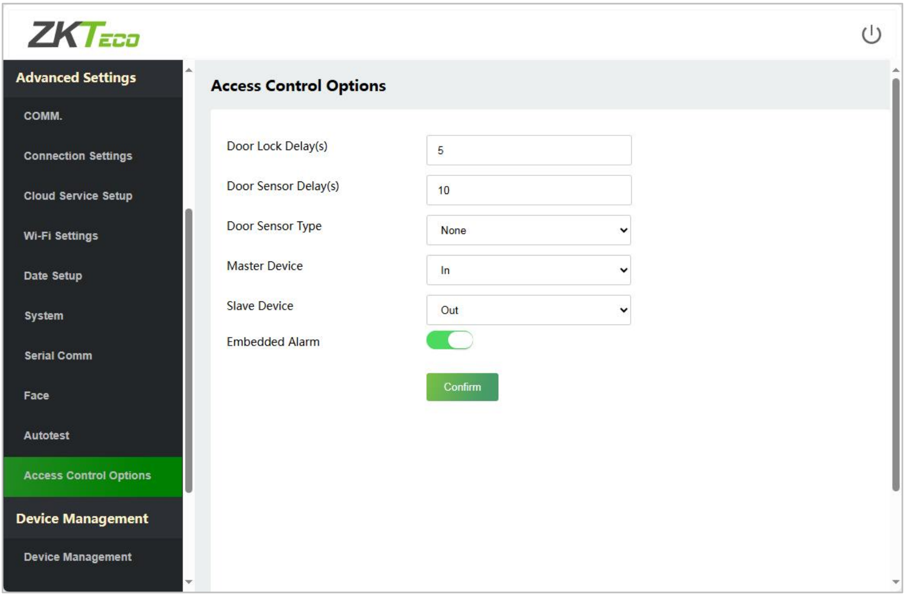


Autotest

Test Face

- **Test Face:** To test if the camera functions properly by checking the pictures taken to see if they are clear enough.

5.4.10 Access Control Options



Access Control Options

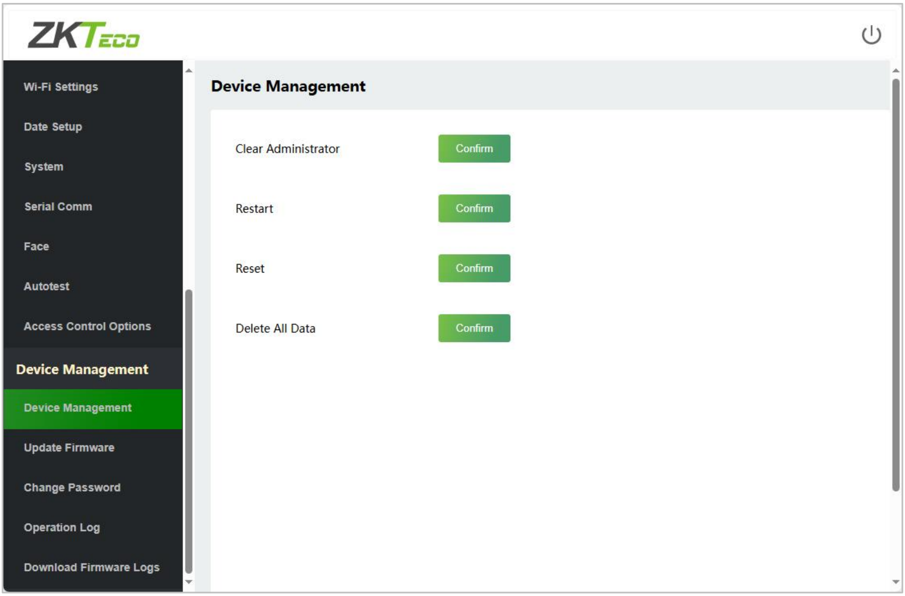
Door Lock Delay(s)	5
Door Sensor Delay(s)	10
Door Sensor Type	None
Master Device	In
Slave Device	Out
Embedded Alarm	●

- **Door Lock Delay (s):** The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.
- **Door Sensor Delay (s):** If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
- **Door Sensor Type:** There are three Sensor types: None, Normal Open, and Normal Close.
  - ✧ **None:** It means the door sensor is not in use.
  - ✧ **Normal Open(NO):** It means the door is always left open when electric power is on.
  - ✧ **Normal Closed(NC):** It means the door is always left closed when electric power is on.
- **Master Device:** While configuring the master and slave devices, you may set the state of the master as **Out** or **In**.
  - ✧ **Out:** A record of verification on the master device is a check-out record.
  - ✧ **In:** A record of verification on the master device is a check-in record.
- **Slave Device:** While configuring the master and slave devices, you may set the state of the slave as **Out** or **In**.
  - ✧ **Out:** A record of verification on the slave device is a check-out record.
  - ✧ **In:** A record of verification on the slave device is a check-in record.
- **Embedded Alarm:** It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.

5.5 Device Management

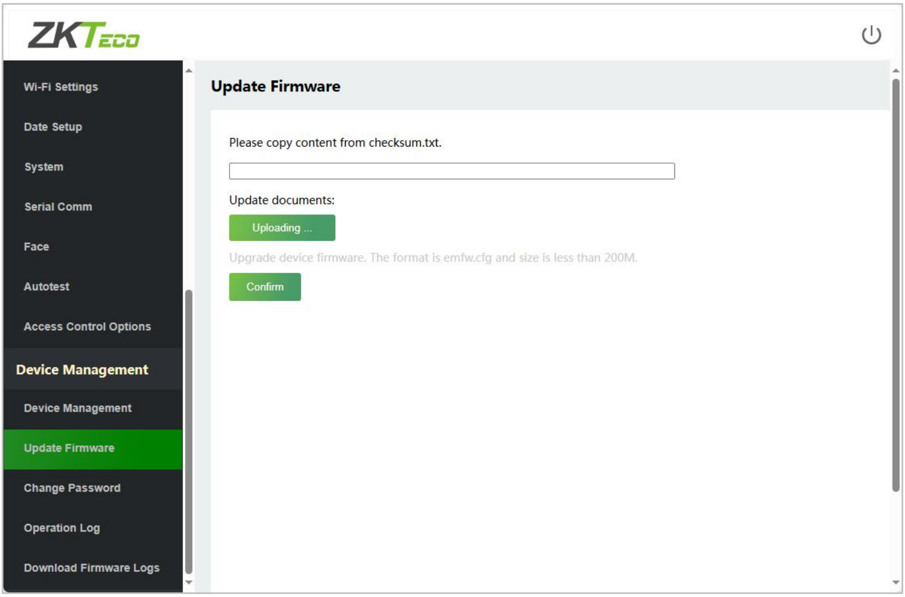
It helps to set related system parameters to optimize the performance and usability of the device.

5.5.1 Device Management



- **Clear Administrator:** To delete all the administrator.
- **Restart:** To restart the device.
- **Reset:** The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).
- **Delete All Data:** To delete information and access records of all registered users.

5.5.2 Update Firmware



Update Firmware

Please copy content from checksum.txt.

Update documents:

Uploading ...

Upgrade device firmware. The format is emfw.cfg and size is less than 200M.

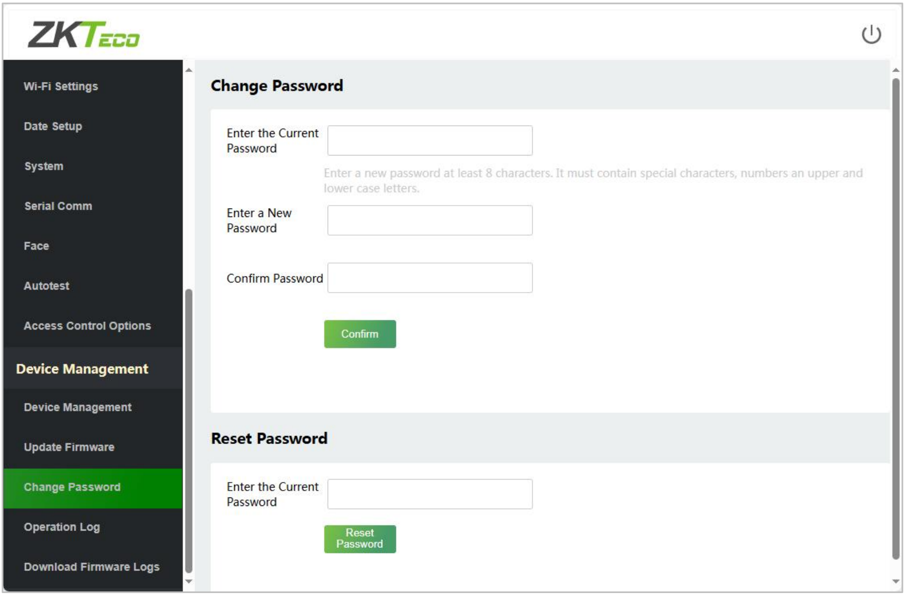
Confirm

- Click [**Uploading...**] to upload the upgrade file in emfw.cfg format. And then click [**Confirm**] to upgrade firmware.

Notes:

- *Make sure the size of the upgrade file is less than 200M.*
- *If an upgrade file is needed, please contact our technical support. Deny firmware upgrade under normal circumstances.*
- *Do not power off during the upgrade process.*

5.5.3 Change Password



Change Password

Enter the Current Password

Enter a new password at least 8 characters. It must contain special characters, numbers an upper and lower case letters.

Enter a New Password

Confirm Password

Confirm

Reset Password

Enter the Current Password

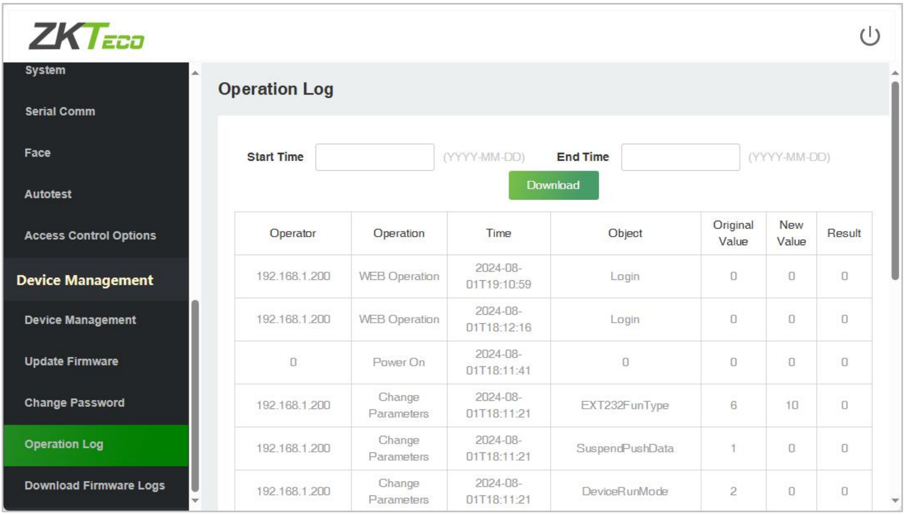
Reset Password

- When the user needs to change the password, he can set it on the Change Password window.
- The user can enter the current password in the Reset Password window and click [**Reset Password**] to restore the device to the factory password.

Note:

- *The password must be no less than 8 characters, and must contain special characters, numbers an upper and lower case letters.*

5.5.4 Operation Log



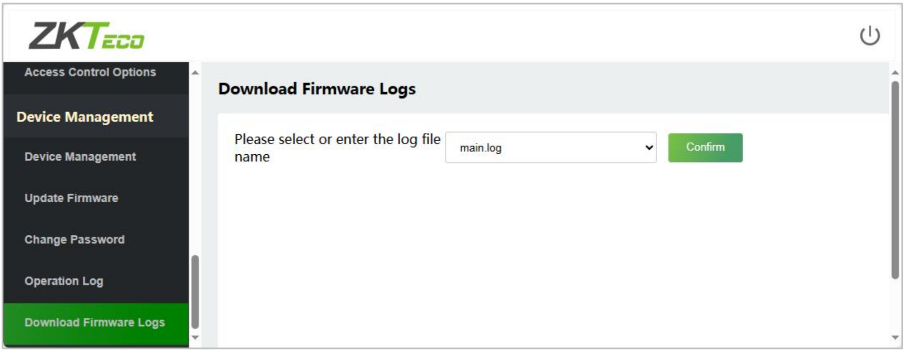
Operation Log

Start Time (YYYY-MM-DD) End Time (YYYY-MM-DD)

Operator	Operation	Time	Object	Original Value	New Value	Result
192.168.1.200	WEB Operation	2024-08-01T19:10:59	Login	0	0	0
192.168.1.200	WEB Operation	2024-08-01T18:12:16	Login	0	0	0
0	Power On	2024-08-01T18:11:41	0	0	0	0
192.168.1.200	Change Parameters	2024-08-01T18:11:21	EXT232FunType	6	10	0
192.168.1.200	Change Parameters	2024-08-01T18:11:21	SuspendPushData	1	0	0
192.168.1.200	Change Parameters	2024-08-01T18:11:21	DeviceRunMode	2	0	0

- After entering the start time and end time, the user can view the Operation Logs on the page and click [**Download**] to download the operation logs.

5.5.5 Download Firmware Logs



Download Firmware Logs

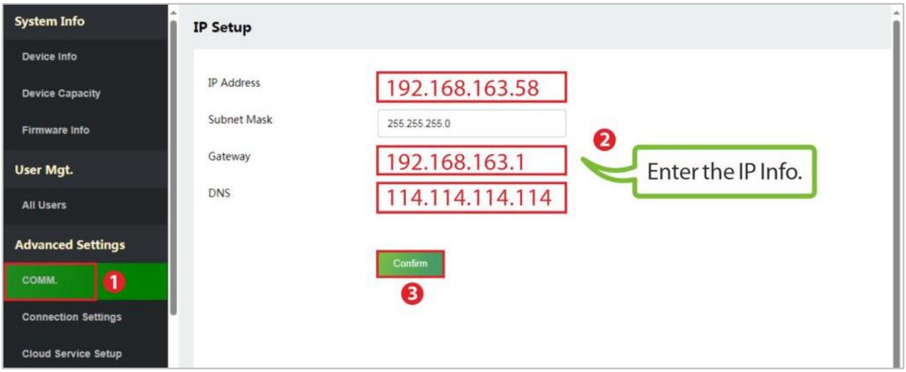
Please select or enter the log file name: main.log

- Users can download firmware logs here, including main.log, biometric.log and devs.log.

6 Connect to ZKBio CVSecurity Software

6.1 Set the Communication Address

Click [**Advanced Settings**] > [**COMM.**] > [**IP Address**] to set the IP address and then click [**Advanced Settings**] > [**Cloud Service Setup**] to set cloud service address on the WebServer. As shown in the figure below.



IP Setup

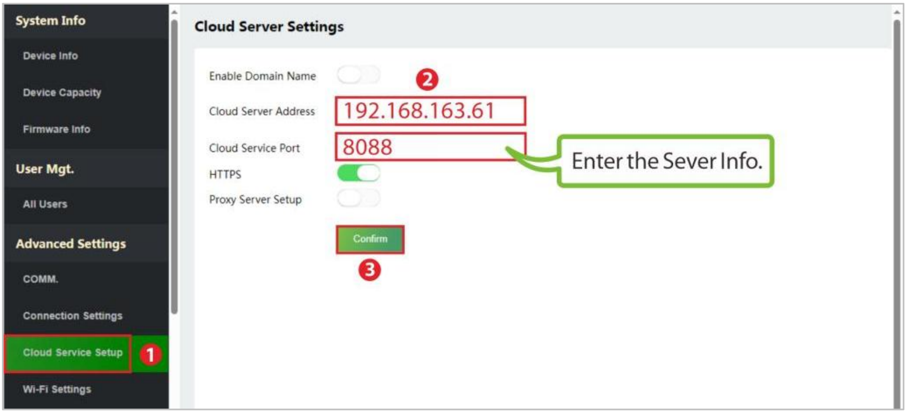
IP Address: 192.168.163.58

Subnet Mask: 255.255.255.0

Gateway: 192.168.163.1

DNS: 114.114.114.114

Enter the IP Info.



Cloud Server Settings

Enable Domain Name: ○

Cloud Server Address: 192.168.163.61

Cloud Service Port: 8088

HTTPS: ●

Proxy Server Setup: ○

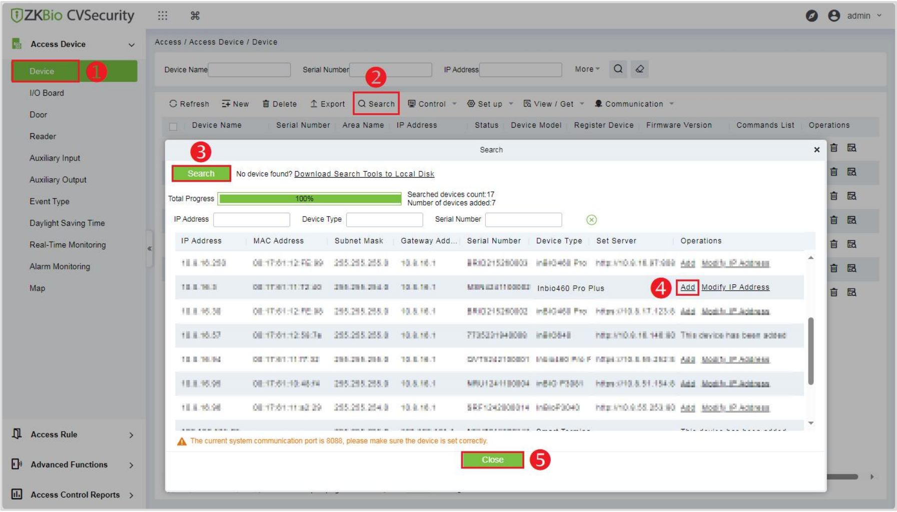
Enter the Sever Info.

- **Cloud Server Address:** This is the IP address after the software installation.
- **Cloud Service Port:** Default is **8088**.

6.2 Add Device on the Software

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

1. Click [**Access**] > [**Access Device**] > [**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.



No device found? Download Search Tools to Local Disk

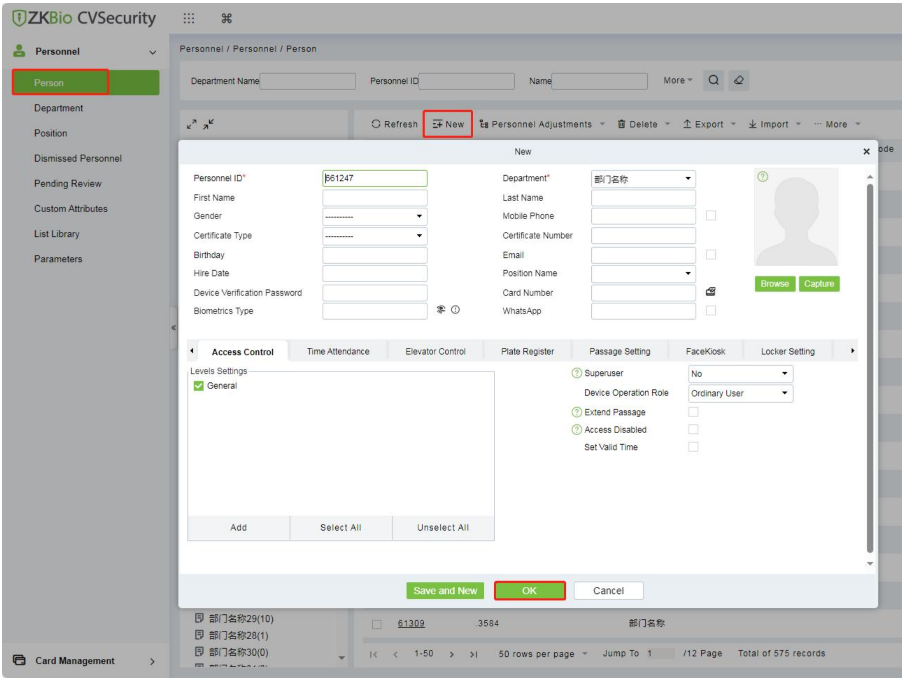
Searched devices count:17
Number of devices added:7

IP Address	MAC Address	Subnet Mask	Gateway Add...	Serial Number	Device Type	Set Server	Operations
[illegible]	[illegible]	255.255.255.0	10.8.16.1	[illegible]	inBIO460 Pro	[illegible]	Add Modify IP Address
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Inbio460 Pro Plus		Add Modify IP Address
[illegible]	[illegible]	255.255.255.0	10.8.16.1	[illegible]	inBIO460 Pro	[illegible]	Add Modify IP Address
[illegible]	[illegible]	255.255.255.0	10.8.16.1	[illegible]	inBIO848	[illegible]	This device has been added
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Add Modify IP Address
[illegible]	[illegible]	255.255.255.0	10.8.16.1	[illegible]	[illegible]	[illegible]	Add Modify IP Address
[illegible]	[illegible]	255.255.254.0	10.8.16.1	[illegible]	InBioP3040	[illegible]	Add Modify IP Address

⚠ The current system communication port is 8088, please make sure the device is set correctly.

6.3 Add Personnel on the Software

Click [**Personnel**] > [**Person**] > [**New**] to register a new user.



New

Personnel ID* 561247

Department* 部门名称

First Name

Last Name

Gender ----------

Mobile Phone

Certificate Type ----------

Certificate Number

Birthday

Email

Hire Date

Position Name

Device Verification Password

Card Number

Biometrics Type

WhatsApp

Levels Settings

☑ General

Superuser No

Device Operation Role Ordinary User

Extend Passage □

Access Disabled □

Set Valid Time □

部门名称29(10)
部门名称28(1)
部门名称30(0)

61309 .3584 部门名称

1-50 50 rows per page Jump To 1 /12 Page Total of 575 records

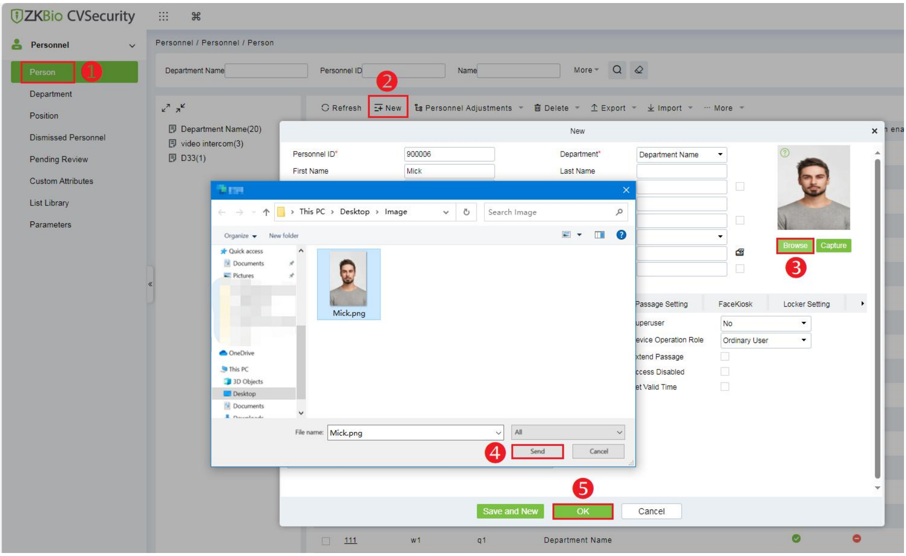
6.4 Adding Photos to the Software

Upload a photo for the person to use to capture the face template.

1) Click [**Personnel**] > [**Person**] > [**New**] > [**Browse**] to find the photo you need to upload.

2) Then click [**Send**] to comfirm and follow the prompts.

3) After entering the person's information, click [**OK**] to save and exit.



Personnel ID* 900006

First Name Mick

Department* Department Name

Last Name

File name: Mick.png

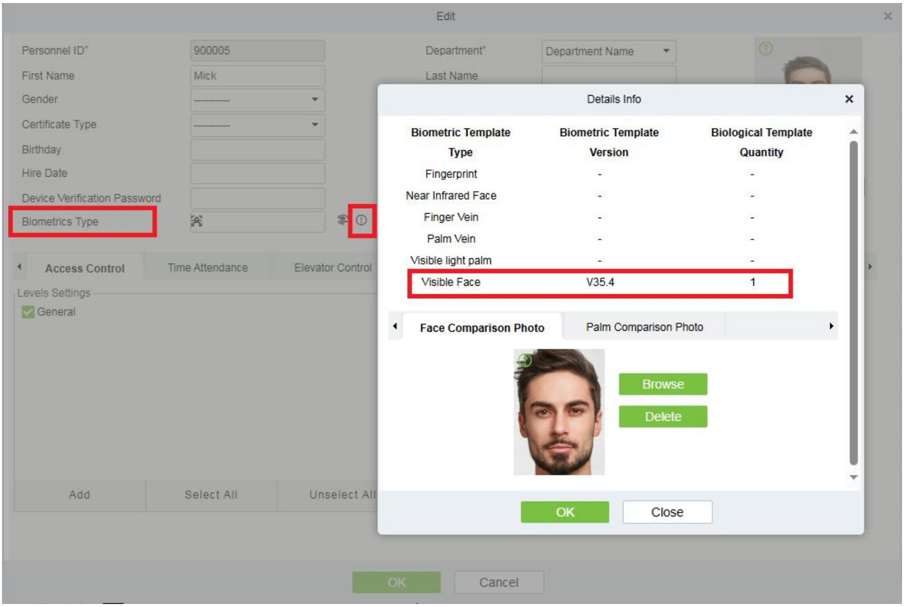
Superuser No

Device Operation Role Ordinary User

111 w1 q1 Department Name

Note: *For better verification results, please make sure the photos are clear and avoid over-retouching.*

4) After the Face Template Extraction Server has converted the photo conversion to a template, click the (!) icon after Biometrics Type to view the template information for the person, as shown in the following figure.



Biometric Template Type	Biometric Template Version	Biological Template Quantity
Fingerprint	-	-
Near Infrared Face	-	-
Finger Vein	-	-
Palm Vein	-	-
Visible light palm	-	-
Visible Face	V35.4	1

5) Click [**Access**] > [**Device**] > [**Device**] > [**Control**] > [**Synchronize All Data to Devices**] to synchronize all the data to the device including the new users.

For more details, please refer to the ZKBio CVSecurity User Manual.

ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.
Phone : +86 769 - 82109991
Fax : +86 755 - 89602394
www.zkteco.com