

User Manual

SpeedFace-V3L(Lite)

Date: May 2023

Doc Version: 1.1

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 © 2023 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 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 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 (Card, 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 Card 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 **SpeedFace-V3L(Lite)**.

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.


Table of Contents

1 SAFETY MEASURES	7
2 ELECTRICAL SAFETY	8
3 OPERATION SAFETY	9
4 INSTRUCTION FOR USE	10
4.1 STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE	10
4.2 FACE REGISTRATION	11
4.3 STANDBY INTERFACE	12
4.4 VIRTUAL KEYBOARD	14
4.5 VERIFICATION MODE	15
4.5.1 FACIAL VERIFICATION	15
4.5.2 CARD VERIFICATION	17
4.5.3 PASSWORD VERIFICATION	19
4.5.4 COMBINED VERIFICATION	21
5 MAIN MENU	23
6 USER MANAGEMENT	25
6.1 USER REGISTRATION	25
6.1.1 REGISTER A USER ID AND NAME	25
6.1.2 USER ROLE	26
6.1.3 FACE	27
6.1.4 CARD	27
6.1.5 PASSWORD	28
6.2 SEARCH USER	29
6.3 EDIT USER	29
6.4 DELETE USER	30
6.5 DISPLAY STYLE	31
7 USER ROLE	33
8 COMMUNICATION SETTINGS	35
8.1 NETWORK SETTINGS	35
8.2 PC CONNECTION	36
8.3 WI-FI SETTINGS	37
8.4 CLOUD SERVER SETTING	41
8.5 NETWORK DIAGNOSIS	42
9 SYSTEM SETTINGS	43
9.1 DATE AND TIME	43

9.2 ACCESS LOGS SETTINGS	45
9.3 FACE PARAMETERS	46
9.4 VIDEO INTERCOM PARAMETERS	49
9.5 DEVICE TYPE SETTINGS	50
9.6 SECURITY SETTINGS	51
9.7 FACTORY RESET	52
10 PERSONALIZE SETTINGS	53
10.1 INTERFACE SETTINGS	53
10.2 VOICE SETTINGS	55
10.3 BELL SCHEDULES	55
11 DATA MANAGEMENT	57
11.1 DELETE DATA	58
12 ACCESS CONTROL	59
12.1 ACCESS CONTROL OPTIONS	60
12.2 TIME SCHEDULE	63
12.3 HOLIDAYS	64
12.4 COMBINED VERIFICATION	66
13 ATTENDANCE SEARCH	68
14 AUTOTEST	69
15 SYSTEM INFORMATION	71
16 CONNECT TO ZKBIOACCESS SOFTWARE	72
16.1 SET THE COMMUNICATION ADDRESS	72
16.2 ADD DEVICE ON THE SOFTWARE	73
16.3 ADD PERSONNEL ON THE SOFTWARE	74
17 CONNECTING TO ZKBIO TALK SOFTWARE	75
18 CONNECTING TO ZSMART APP★	79
18.1 ADDING DEVICE ON THE ZSMART APP	79
18.2 VIDEO PHONE CONNECTION	80
19 CONNECTING TO SIP★	82
19.1 LOCAL AREA NETWORK USE	83
19.2 SIP SERVER	90

1 Safety Measures

The below instructions intend to ensure that the user can use the product correctly to avoid danger or property loss. The following precautions are to keep users safe and prevent any damage. Please read carefully before installation.

 Noncompliance with instructions could lead to product damage or physical injury (may even cause death).

1. **Read, follow, and retain instructions** – All safety and operational instructions must be properly read and followed before bringing the device into service.
2. **Do not ignore warnings** – Adhere to all warnings on the unit and in the operating instructions.
3. **Accessories** – Use only manufacturer-recommended or product-sold accessories. Please do not use any other components other than manufacturer suggested materials.
4. **Precautions for the installation** – Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.
5. **Service** – Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.
6. **Damage requiring service** – Disconnect the system from the Mains AC or DC power source and refer service personnel under the following conditions:
 - When cord or connection control is affected.
 - When the liquid spilled, or an item dropped into the system.
 - If exposed to water or due to inclement weather (rain, snow, and more).
 - If the system is not operating normally, under operating instructions.

Just change controls defined in operating instructions. Improper adjustment of the controls may result in damage and involve a qualified technician to return the device to normal operation.

And do not connect multiple devices to one power adapter as adapter overload can cause over-heat or fire hazard.

7. **Replacement parts** – When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in a burn, shock, or other hazards.
8. **Safety check** – On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the device.
9. **Power sources** – Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.
10. **Lightning** – Can install external lightning conductors to protect against electrical storms. It stops power-ups from destroying the system.

Recommended installing the devices in areas with limited access.

2 Electrical Safety

- Before connecting an external cable to the device, complete grounding properly, and set up surge protection; otherwise, static electricity will damage the mainboard.
- Make sure that the power has been disconnected before you wire, install, or dismantle the device.
- Ensure that the signal connected to the device is a weak-current (switch) signal; otherwise, components of the device will get damaged.
- Ensure that the standard voltage applicable in your country or region is applied. If you are not sure about the endorsed standard voltage, please consult your local electric power company. Power mismatch may cause a short circuit or device damage.
- In the case of power supply damage, return the device to the professional technical personnel or your dealer for handling.
- To avoid interference, keep the device far from high electromagnetic radiation devices, such as generators (including electric generators), radios, televisions, (especially CRT) monitors, or speakers.

3 Operation Safety

- If smoke, odour, or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service centre.
- Transportation and other unpredictable causes may damage the device hardware. Check whether the device has any intense damage before installation.
- If the device has major defects that you cannot solve, contact your dealer as soon as possible.
- Dust, moisture, and abrupt temperature changes can affect the device's service life. You are advised not to keep the device under such conditions.
- Do not keep the device in a place that vibrates. Handle the device with care. Do not place heavy objects on top of the device.
- Do not apply rosin, alcohol, benzene, pesticides, and other volatile substances that may damage the device enclosure. Clean the device accessories with a piece of soft cloth or a small amount of cleaning agent.
- If you have any technical questions regarding usage, contact certified or experienced technical personnel.

Note:

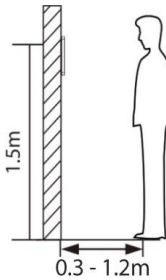
- 1) Make sure whether the positive polarity and negative polarity of the DC 12V power supply is connected correctly. A reverse connection may damage the device. It is not advisable to connect the AC 24V power supply to the DC 12V input port.
- 2) Make sure to connect the wires following the positive polarity and negative polarity shown on the device's nameplate.
- 3) The warranty service does not cover accidental damage, damage caused by mis-operation, and damage due to independent installation or repair of the product by the user.

4 Instruction for Use

Before getting into the device features and functions, it is recommended to be familiar with the below fundamentals.

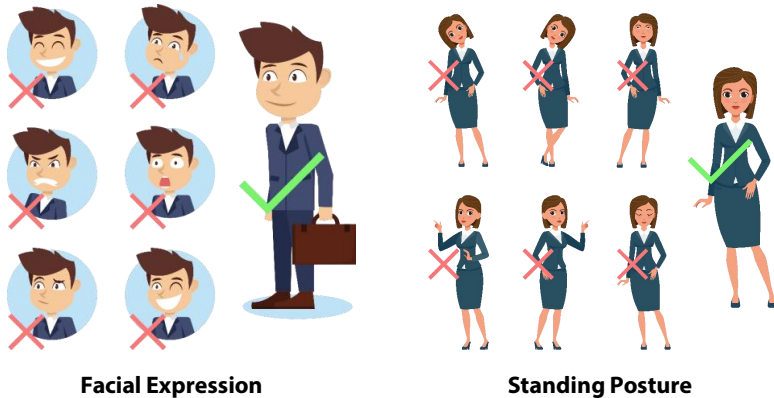
4.1 Standing Position, Facial Expression and Standing Posture

➤ The recommended distance



For indoor use, the distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 1.2m. Users may slightly move forward or backward to improve the character of facial images captured.

➤ Recommended standing posture and facial expression



Note:

Please keep your facial expression and standing posture natural while enrolment or verification.

4.2 Face Registration

Try to keep the face in the centre of the screen during registration. Please face the camera and stay still during face registration. The screen looks like this:



Correct face registration and authentication method

➤ Recommendation for registering a face

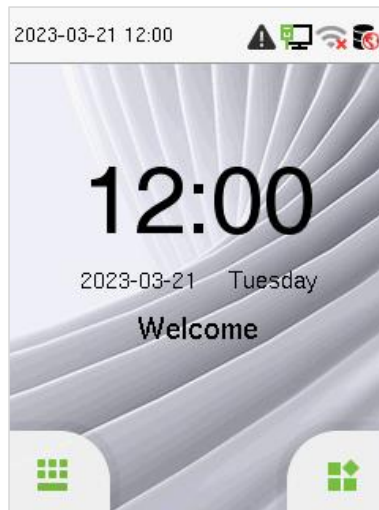
- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful to keep your facial expression natural and not to change. (smiling face, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take longer or may fail.
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses or eyeglasses.
- Be careful not to display two faces on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.



➤ Recommendation for authenticating a face

- Ensure that the face appears inside the guideline displayed on the screen of the device.
- Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

4.3 Standby Interface

After connecting the power supply, the following standby interface is displayed:

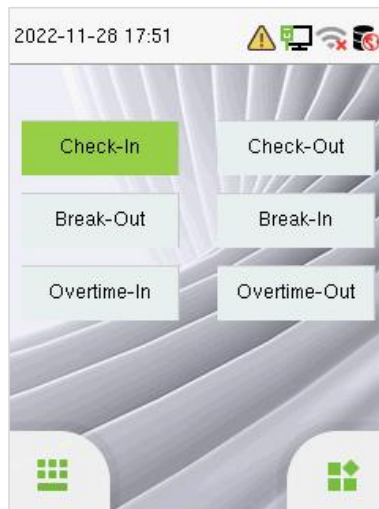


- Tap  to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap  to go to the menu.
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.

**Note:**

For the security of the device, it is recommended to register a super administrator the first time you use the device.

- The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:



- Press the corresponding punch state key to select your current punch state, which is displayed in green. Please refer to "Shortcut Key Mappings" for the specific operation method.

Note:


The punch state options are off by default and need to select other mode options in the "**Personalize > Punch State Option**" to get the punch state options on the standby screen.

4.4 Virtual Keyboard



Note:

The device supports the input in English language, numbers, and symbols.

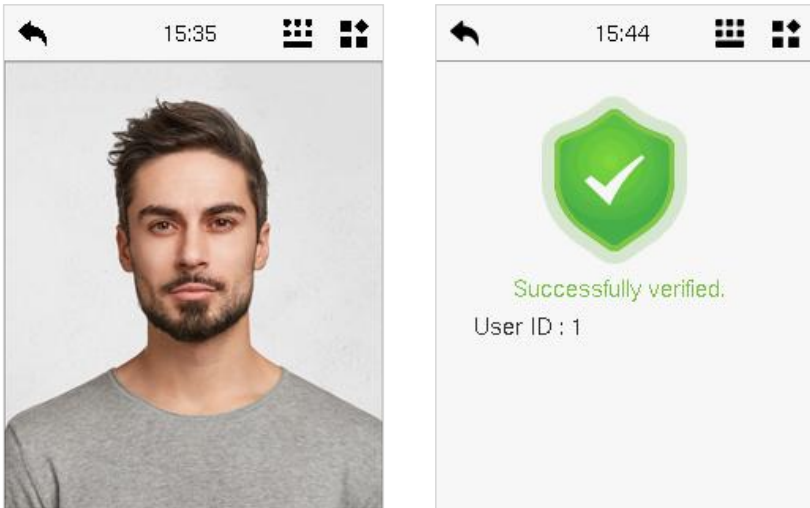
- Tap [**EN**] to switch to the numeric keyboard.
- Press [**123**] to switch to the symbolic keyboard.
- Tap [**@#&**] to return to the English keyboard.
- Tap [] to exit the virtual keyboard.

4.5 Verification Mode

4.5.1 Facial Verification


➤ **1:N Facial Verification Mode**

It compares the acquired facial images with all face data registered in the device. The following is the pop-up prompt box of comparison results.




➤ **1:1 Facial Verification Mode**

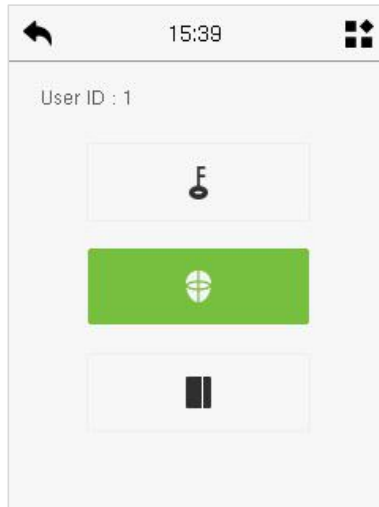
Compare the face captured by the camera with the facial template related to the entered user ID.

Press  on the main interface and enter the 1:1 facial verification mode.

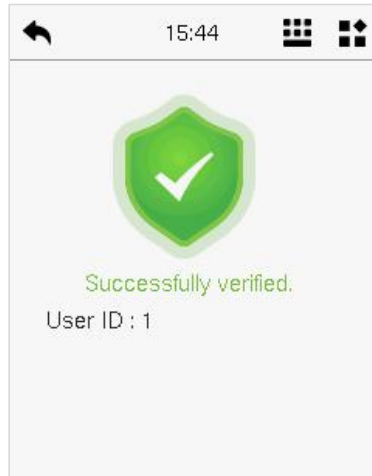
Enter the user ID and click **[OK]**.



If an employee registers password and card in addition to the face, the following screen will appear. Select the  icon to enter face verification mode.



After successful verification, the prompt box displays "**Successfully Verified.**", as shown below:

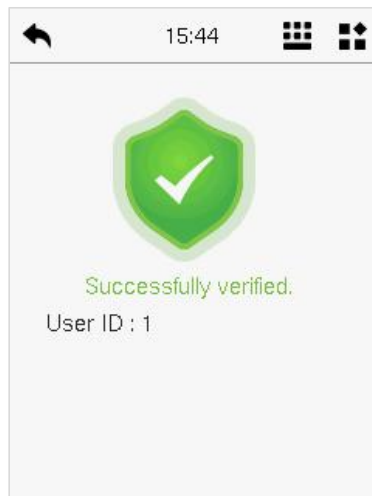


If the verification is failed, it prompts "**Please adjust your position!**".

4.5.2 Card Verification


➤ 1: N Card Verification Mode

The 1: N Card Verification mode compares the card number in the card induction area with all the card number data registered in the device; The following is the card verification screen.




➤ 1:1 Card Verification Mode

The 1:1 Card Verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

Press  on the main interface and enter the 1:1 card verification mode.

Enter the user ID and click **[OK]**.




If an employee registers face and password in addition to the card, the following screen will appear. Select the  icon to enter card verification mode.




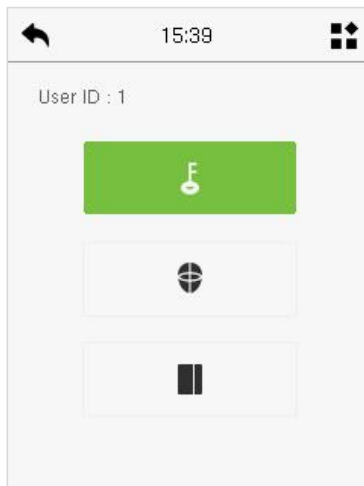
4.5.3 Password Verification

The device compares the entered password with the registered password of the given User ID.

Tap the  button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press [OK].



If an employee registers face and card in addition to the password, the following screen will appear. Select the  icon to enter password verification mode.

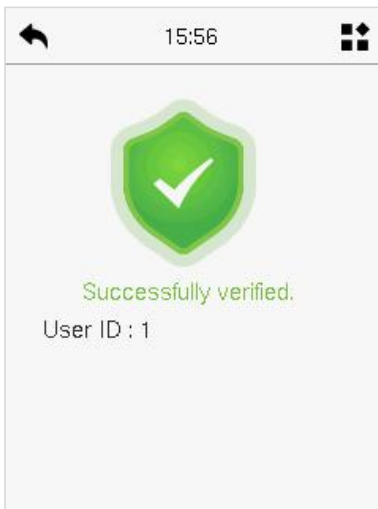


Input the password and press [OK].

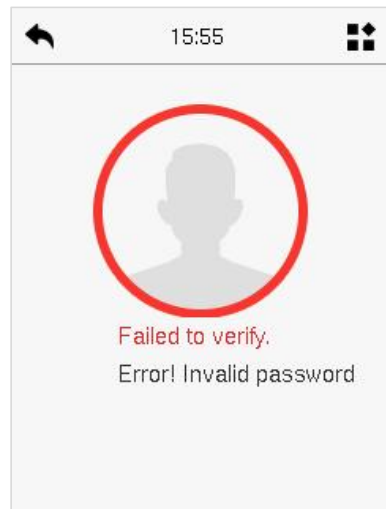


Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:



Verification is failed:



4.5.4 Combined Verification

This device allows you to use a variety of verification methods to increase security. There are a total of 9 distinct verification combinations that can be implemented, as listed below:

➤ Combined Verification Symbol Definition

Symbol	Definition	Explanation
/	or	This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device.
+	and	This method compares the entered verification of a person with all the verification templates previously stored to that Personnel ID in the Device.

← Verification Mode
↕

Password/Card/Face

User ID Only

Password

Card Only

Password+Card

← Verification Mode
↕

Password+Card

Password/Card

Face Only

Face+Password


Face+Card

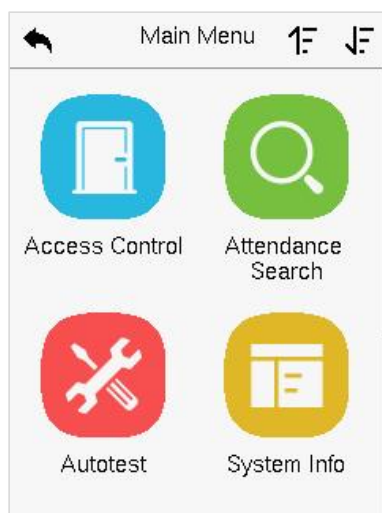
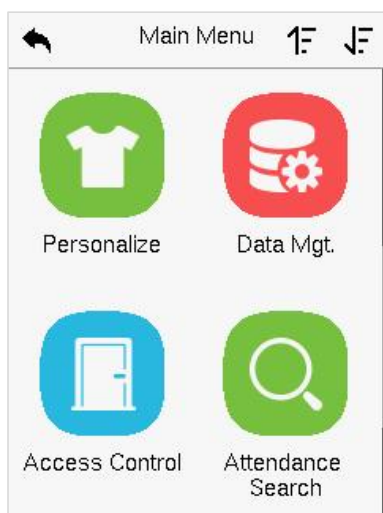
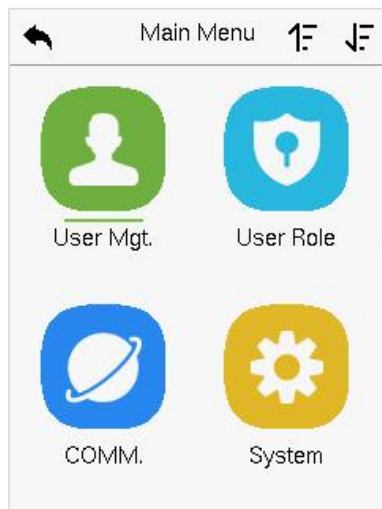
➤ Procedure to set for Combined Verification Mode

- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.

- For instance, when an employee has registered only for the face data, but the Device verification mode is set as "Face + Password", the employee will not be able to complete the verification process successfully.
- This is because the Device compares the face template of the person with the registered verification template (both the Face and the Password) previously stored to that Personnel ID in the Device.
- But as the employee has registered only the Face but not the Password, the verification will not get completed and the Device displays "Verification Failed".

5 Main Menu

Press  on the initial interface to enter the main menu, as shown below:



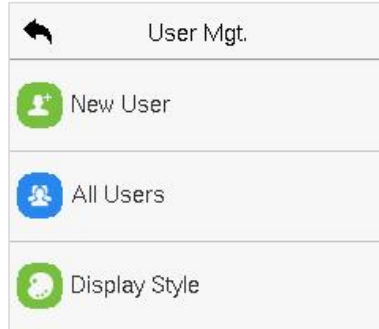
Function Description

Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Network, PC Connection, Wi-Fi, Cloud Server and Network Diagnosis.
System	To set parameters related to the system, including Date & Time, access logs settings, face parameters, video intercom parameters, monitoring settings ★ , device type settings, security settings and resetting to factory settings.
Personalize	To customize settings of User Interface, Voice and Bell Schedules.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock and the relevant access control device.
Attendance Search	To query the specified Event logs.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Microphone, Camera, and Real-Time Clock.
System Info	To view Device Capacity, Device information, Firmware information and Privacy Policy.

6 User Management

6.1 User Registration

Tap **User Mgt.** on the main menu.



6.1.1 Register a User ID and Name

Tap **New User** and enter the **User ID** and **Name**.

	New User	
User ID		2
Name		Mick
User Role		Normal User
Verification Mode		Password/Card/Face
Face		0

	New User	
User Role		Normal User
Verification Mode		Password/Card/Face
Face		0
Card Number		
Password		

Note:

- 1) A name can take up to 36 characters.
- 2) The user ID may contain 1-14 digits by default, support number and alphabetic.
- 3) During the initial registration, you can modify your ID but not after the registration.
- 4) If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

6.1.2 User Role

On the New User interface, tap on **User Role** to set the user's duty as either **Normal User** or **Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentic verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with User Defined Role. The user can be permitted to access several menu options as required.

	User Role
<input checked="" type="radio"/>	Normal User
<input type="radio"/>	Super Admin

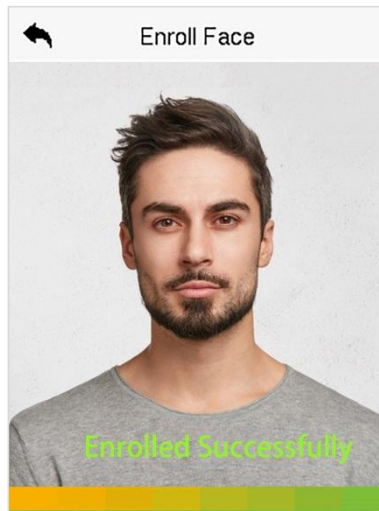
Note:

If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

6.1.3 Face

Tap **Face** in the **New User** interface to enter the face registration page.

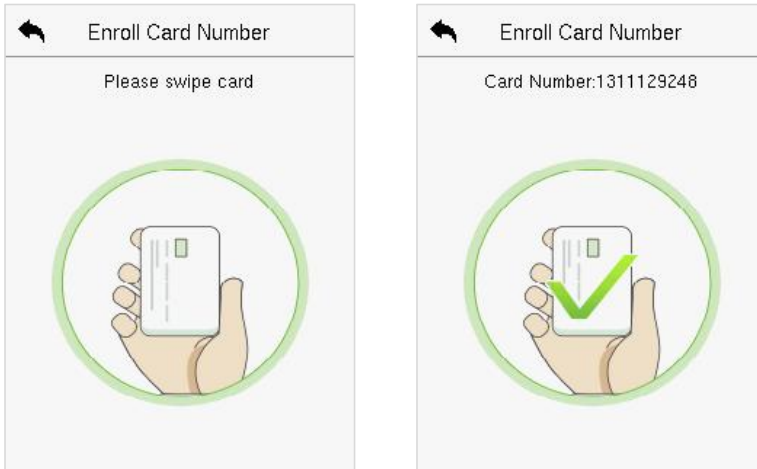
- Please face towards the camera and place yourself in such a way that your face image fits inside the white guiding box and stays still during face registration.
- A progress bar shows up while registering the face and then "**Enrolled Successfully**" message is displayed as the progress bar completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:



6.1.4 Card

Tap **Card** in the **New User** interface to enter the card registration page.

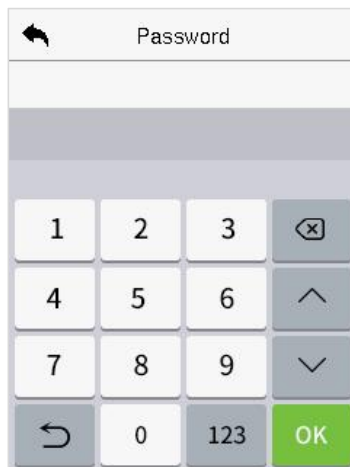
- Swipe the card underneath the card reading area on the Card interface. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface looks like this:



6.1.5 Password

Tap **Password** in the **New User** interface to enter the password registration page.

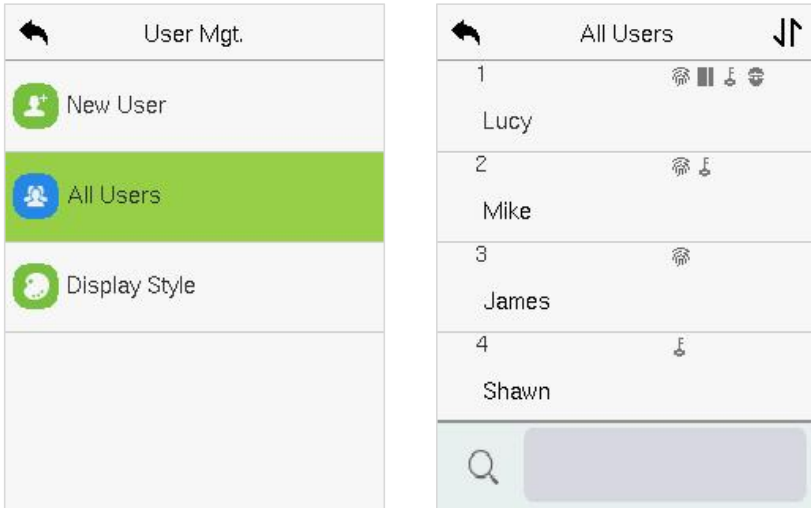
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password does not match!**", where the user needs to re-confirm the password again.
- The password may contain 6 to 8 digits by default.



6.2 Search User

On the **Main Menu**, tap **User Mgt.**, and then tap **All Users** to search a User.

- On the **All-Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.



6.3 Edit User

On the **All-Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.

User : 1 Lucy	
Edit	
Delete	

Edit : 1 Lucy	
User ID	1
Name	Lucy
User Role	Normal User
Verification Mode	Password/Card/Face
Face	1

Note:

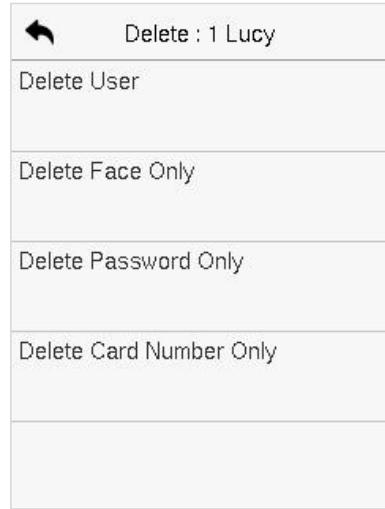
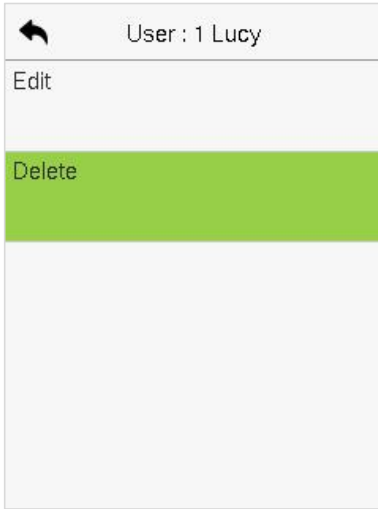
The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "6.1 User Registration".

6.4 Delete User

On the **All-Users** interface, tap on the required user from the list and tap **Delete** to delete the user or specific user information from the device. On the **Delete** interface, tap on the required operation, and then tap **OK** to confirm the deletion.

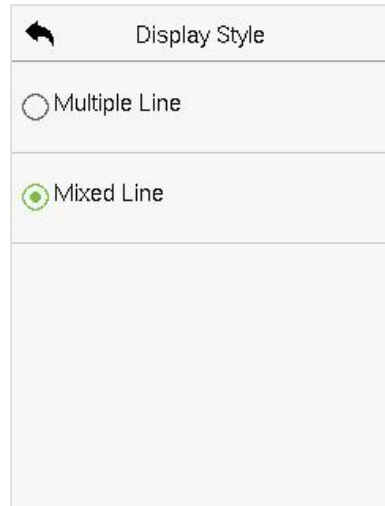
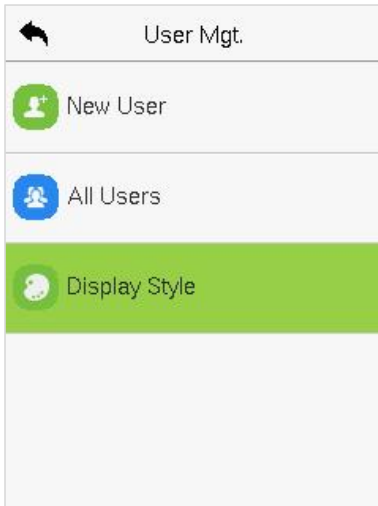
➤ Delete Operations

- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete Face Only:** Deletes the face information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Number Only:** Deletes the card information of the selected user.



6.5 Display Style

On the **Main Menu**, tap **User Mgt.**, and then tap **Display Style** to enter Display Style setting interface.



All the Display Styles are shown as below:

Multiple Line:

All Users	
1	Lucy
2	Mike
3	James
4	Shawn

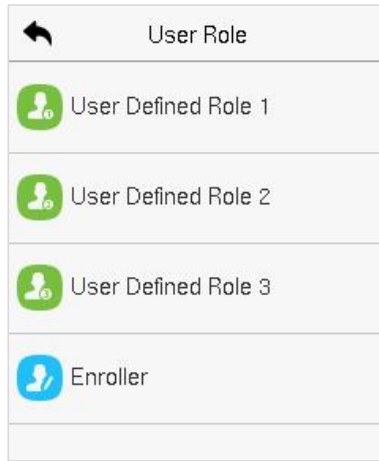
Mixed Line:

All Users	
1	Lucy
2	Mike
3	James
4	Shawn

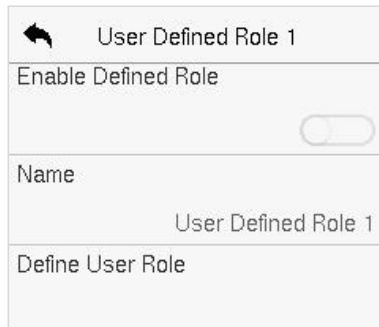
7 User Role

User Role facilitates to assign some specific permissions to certain users, based on the requirement.

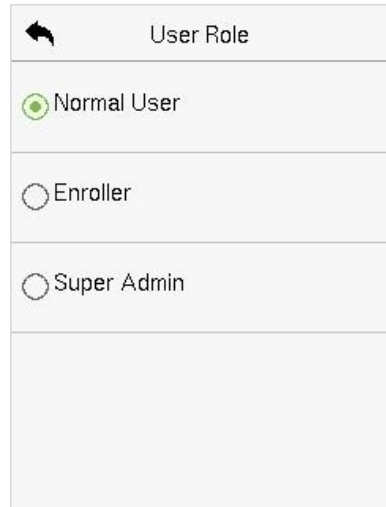
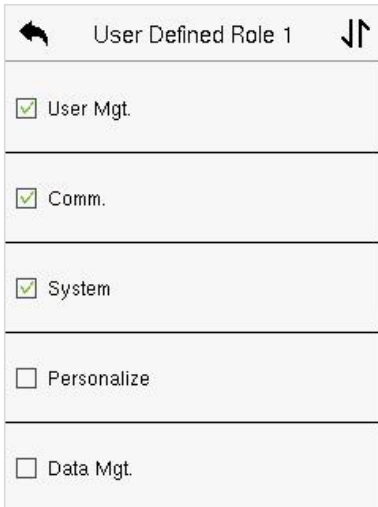
- On the **Main** menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.



- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



- Then, by tapping on Define User Role, select the required privileges for the new role, and then press the Return button.
- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required **Main Menu** function name, and then select its required sub-menus from the list.



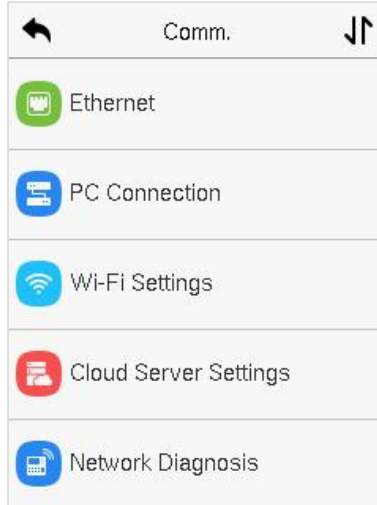
Note:

If the User Role is enabled for the Device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role function.

8 Communication Settings

Communication Settings are used to set the parameters of the relevant parameters of Network, PC Connection, Wi-Fi, Cloud Server and Network Diagnosis.

Tap **COMM.** on the main menu.



8.1 Network 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 connect to the same network segment.

Tap **Ethernet** on the **COMM.** Settings interface to configure the settings.

Ethernet	
IP Address	192.168.163.99
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
TCP COMM.Port	4370

Function Description

Function Name	Description
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.
TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.

8.2 PC Connection

Comm Key facilitates to improve the security of the data by setting up the communication between the device and the PC. Once the Comm Key is set, a password is required to connect the device to the PC software.

Tap **PC Connection** on the **Comm.** Settings interface to configure the communication settings.

Function Description

Function Name	Description
Comm Key	The default password is 0 and can be changed. The Comm Key can contain 1-6 digits.
Device ID	It is the identification number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

8.3 Wi-Fi Settings


The device provides a Wi-Fi module, which can be built-in within the device module.

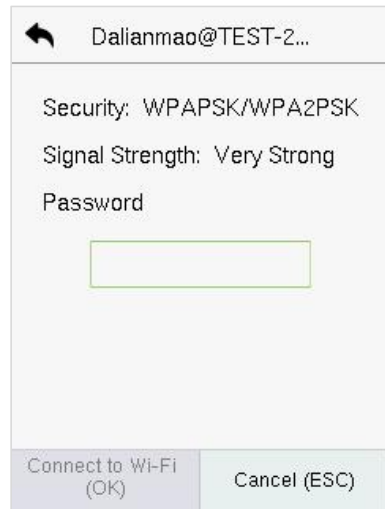
The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

Tap **Wi-Fi Settings** on the **Comm.** Settings interface to configure the Wi-Fi settings.




➤ Searching the Wi-Fi Network

- Wi-Fi is enabled in the device by default. Toggle 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.
- Tap on the required Wi-Fi name from the available list and input the correct password in the password interface, and then tap **Connect to Wi-Fi (OK)**.



Wi-Fi Enabled: Tap on the required network from the searched network list.

Tap on the password field to enter the password and tap on **Connect to Wi-Fi (OK)**.

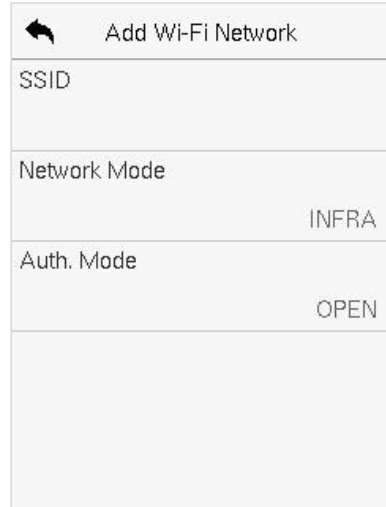
- When the Wi-Fi is connected successfully, the initial interface will display the Wi-Fi  logo.

➤ Adding Wi-Fi Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.



Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.



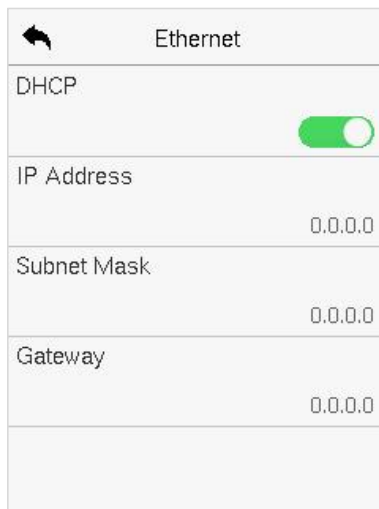
On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

Note:

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

➤ Advanced Setting

On the **Wi-Fi Settings** interface, tap on **Advanced** to set the relevant parameters as required.

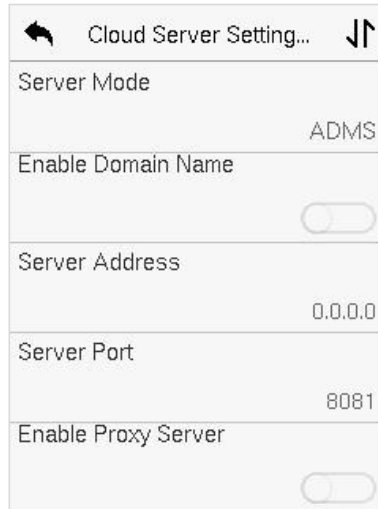


Function Description

Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	The IP address for the Wi-Fi network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the Wi-Fi network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The Default Gateway address is 0.0.0.0. It can be modified according to the network availability.

8.4 Cloud Server Setting

Tap **Cloud Server Setting** on the **Comm.** Settings interface to connect with the ADMS server.



Cloud Server Setting...	
Server Mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server Port	8081
Enable Proxy Server	<input type="checkbox"/>

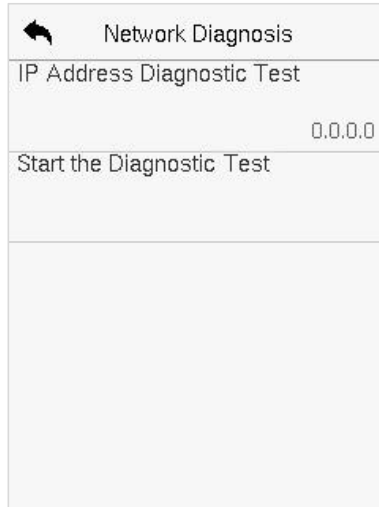
Function Description

Function Name		Description
Enable Domain Name	Server Address	Once this mode is turned ON, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	Server Address	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		The IP address and the port number of the proxy server is set manually when the proxy is enabled.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensures the security of the transmission process.

8.5 Network Diagnosis

It helps to set the network diagnosis parameters.

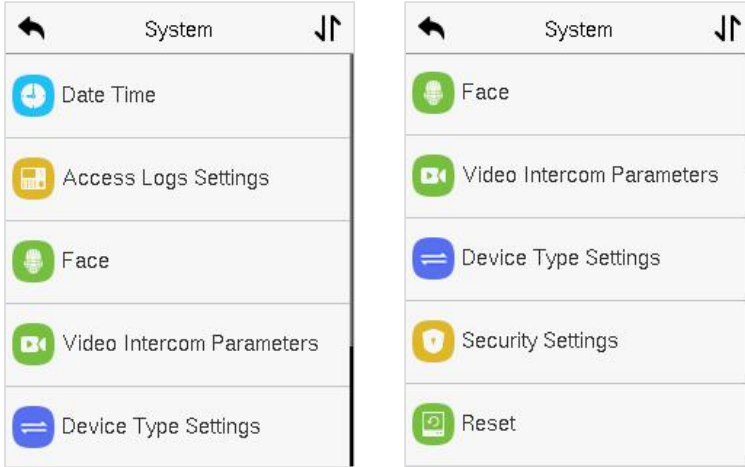
Tap **Network Diagnosis** on the **Comm.** Settings interface. Enter the IP address that needs to be diagnosed and tap **Start the Diagnostic Test** to check whether the network can connect to the device.



9 System Settings

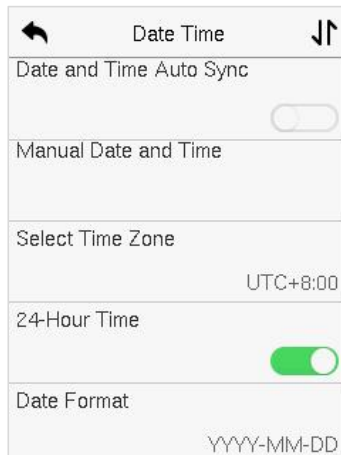
It helps to set related system parameters to optimize the accessibility of the device.

Tap **System** on the **Main Menu** interface to get into its menu options.



9.1 Date and Time

Tap **Date Time** on the **System** interface to set the date and time.



- Tap **Date and Time Auto Sync** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap to **Confirm** and save.
- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then select the **Date Format** to set the date.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch time.

Daylight Saving Setup	
Start Month	1
Start Week	1
Start Day	Sunday
Start Time	00:00
End Month	1

Week Mode

Daylight Saving Setup	
Start Date	00-00
Start Time	00:00
End Date	00-00
End Time	00:00

Date Mode

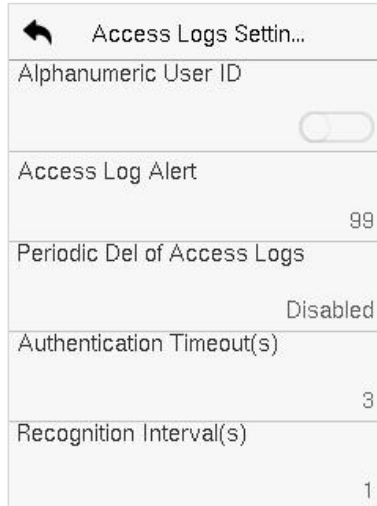
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

Note:

For example, if a user sets the time of the device (18:35 on March 15, 2021) to 18:30 on January 1, 2022. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2022.

9.2 Access Logs Settings

Tap **Access Logs Settings** on the **System** interface.



Access Logs Setting...	
Alphanumeric User ID	<input type="checkbox"/>
Access Log Alert	99
Periodic Del of Access Logs	Disabled
Authentication Timeout(s)	3
Recognition Interval(s)	1

Function Description

Function Name	Description
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	When the record space of the attendance access reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The time interval for which the "Successful Verification" message displays. Valid value: 1~9 seconds.

Recognition Interval(s)

To set the time interval for facial template matching as required.

Valid value: 0~9 seconds.

9.3 Face Parameters

Tap **Face** on the **System** interface to go to the Face parameter settings.

←	Face	↕
1:N Threshold		47
1:1 Threshold		63
Face Enrollment Threshold		70
Face Pitch Angle		30
Face Rotation Angle		25

←	Face	↕
Image Quality		70
Minimum Face Size		80
LED Light Trigger Value		80
Motion Detection Sensitivity		4
Live Detection		<input type="checkbox"/>

←	Face	↕
Live Detection Threshold		70
Anti-spoofing Using NIR		<input checked="" type="checkbox"/>
Anti-flicker Mode		50HZ
Face Algorithm		
Save Photo as Template		<input checked="" type="checkbox"/>

Function Description

Function Name	Description
<p>1:N Threshold</p>	<p>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.</p> <p>The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 47.</p>
<p>1:1 Threshold</p>	<p>Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value.</p> <p>The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.</p>
<p>Face Enrollment Threshold</p>	<p>During face enrollment, 1:N comparison is used to determine whether the user has already registered before.</p> <p>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.</p>
<p>Face Pitch Angle</p>	<p>It is the pitch angle tolerance of a face for facial template registration and comparison.</p> <p>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.</p>

<p>Face Rotation Angle</p>	<p>It is the rotation angle tolerance of a face for facial template registration and comparison.</p> <p>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.</p>
<p>Image Quality</p>	<p>It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.</p>
<p>Minimum Face Size</p>	<p>It sets the minimum face size required for facial registration and comparison.</p> <p>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.</p> <p>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.</p>
<p>LED Light Trigger Threshold</p>	<p>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.</p>
<p>Motion Detection Sensitivity</p>	<p>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.</p> <p>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.</p>

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.
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.
Face algorithm	It has facial algorithm related information and pause the facial template update.
Save Photo as Template	After disable this function, face re-registration is required after an algorithm upgrade.

9.4 Video Intercom Parameters

Click **Video Intercom Parameters** on the **System** interface.

←
Video Intercom Para...

QR Code Binding

Intercom Server Settings

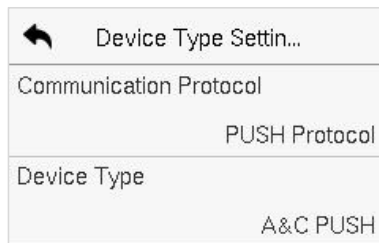
Calling Timeout(s) 20

Function Description

Function Name	Description
QR Code Binding	After downloading and installing the ZSmart APP on the phone. Open it and scan the QR code to add the device for the video door phone connection.
Intercom Server Setting	Set the IP address and port number of the intercom server. Server Address: Enter the sever installation IP address. Server Port: It is the service port set during installation (not the ADMS port).
Calling Timeout (s)	If the call is not answered within a specified time, it exits to the main interface.

9.5 Device Type Settings

Click **Device Type Settings** on the **System** interface.

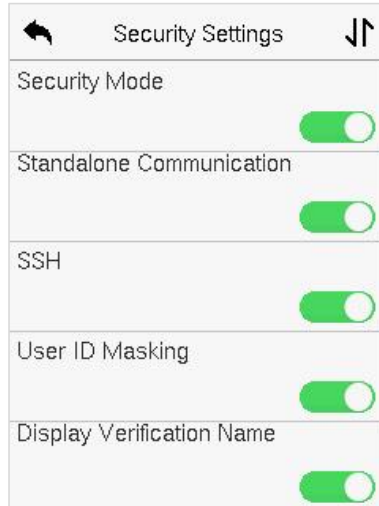


Function Description

Function Name	Description
Communication Protocol	Set the communication protocol to PUSH protocol.
Device Type	Set the device as T&A PUSH or A&C PUSH.

9.6 Security Settings

Tap **Security Settings** on the **System** interface to go to the Security settings.



Function Description

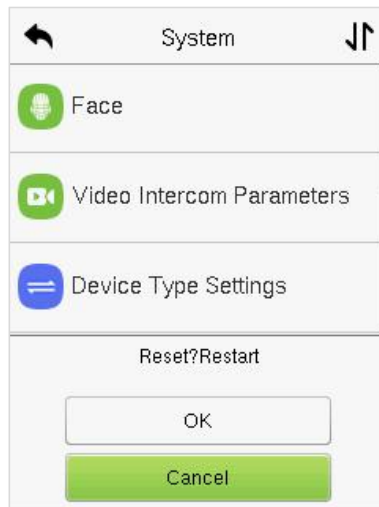
Function Name	Description
Security Mode	Select whether to enable the security mode to protect the device and the user's personal information. You can set the device to work offline and hide the user's personal information to prevent leakage during user verification.
Standalone Communication	To avoid being unable to use when the device is offline, you can download the C/S software (such as ZKAccess 3.5) on your computer in advance for offline use.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.

Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification result interface.

9.7 Factory Reset

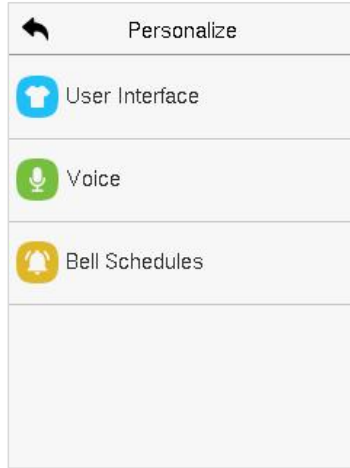
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



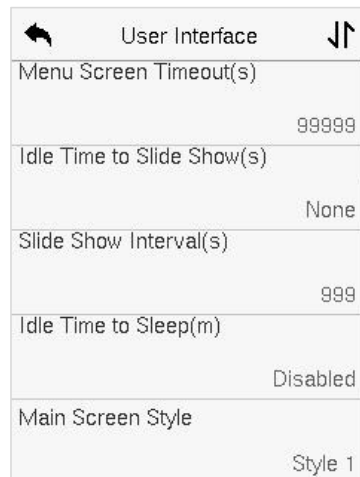
10 Personalize Settings

Tap **Personalize** the **Main Menu** interface to customize interface settings, voice, bell, punch state options, and shortcut key mappings.



10.1 Interface Settings

Tap **User Interface** on the **Personalize** interface to customize the display style of the main interface.

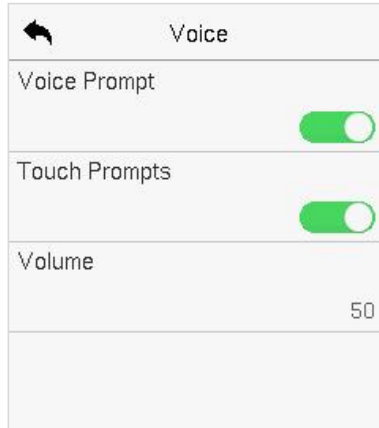


Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Timeout (s)	<p>When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface.</p> <p>The function can either be disabled or set the required value between 60 and 99999 seconds.</p>
Idle Time to Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show is displayed. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	<p>If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode.</p> <p>This function can be disabled or set a value within 1-999 minutes.</p>
Main Screen Style	The style of the main screen can be selected according to the user preference.

10.2 Voice Settings

Tap **Voice** on the **Personalize** interface to configure the voice settings.

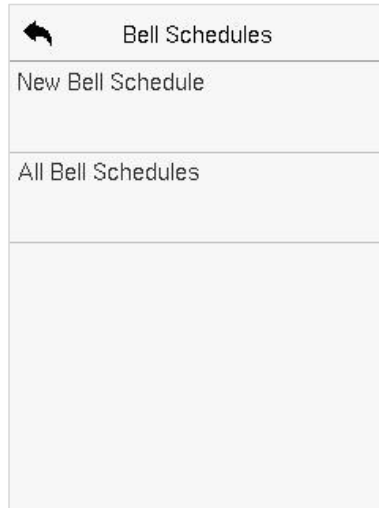


Function Description

Function Name	Description
Voice Prompt	Toggle to enable or disable the voice prompts during function operations.
Touch Prompt	Toggle to enable or disable the keypad sounds.
Volume	Adjust the volume of the device which can be set between 0-100.

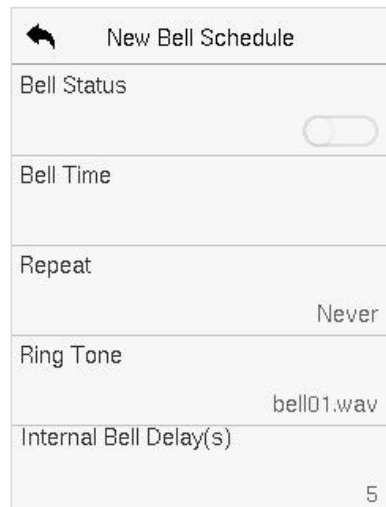
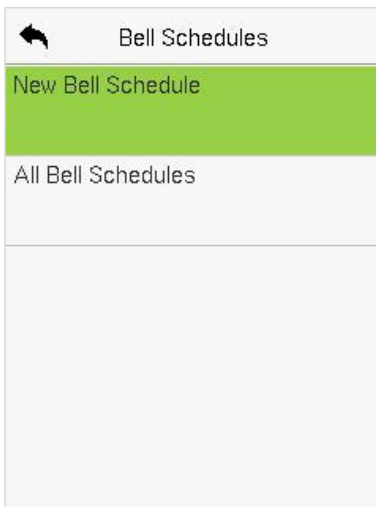
10.3 Bell Schedules

Tap **Bell Schedules** on the **Personalize** interface to configure the Bell settings.



➤ New Bell Schedule

Tap **New Bell Schedule** on the **Bell Schedule** interface to add a new bell schedule.



Function Description

Function Name	Description
Bell Status	Toggle to enable or disable the bell status.
Bell Time	Once the required time is set, the device automatically triggers to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ringtone.
Internal Bell Delay(s)	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

➤ **All Bell Schedules**

Once the bell is scheduled, on the **Bell Schedules** interface, tap **All Bell Schedules** to view the newly scheduled bell.

➤ **Edit the Scheduled Bell**

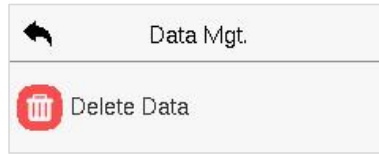
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

➤ **Delete a Bell**

On the **All Bell Schedules** interface, tap the required bell schedule, tap **Delete**, and then tap **Yes** to delete the selected bell.

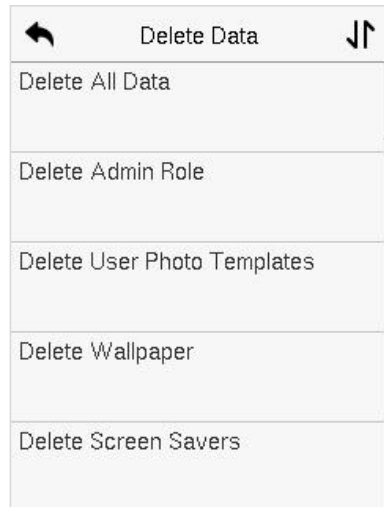
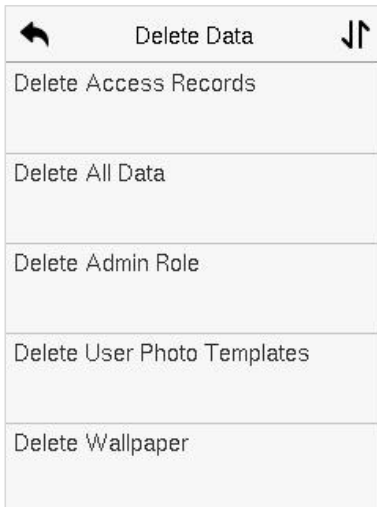
11 Data Management

On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.



11.1 Delete Data

Tap **Delete Data** on the **Data Mgt.** interface to delete the required data.

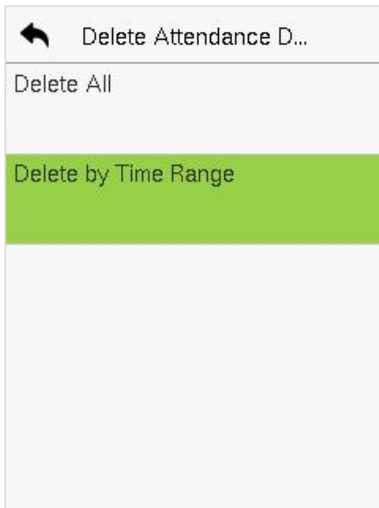


Function Description

Function Name	Description
Delete Access Records	To delete attendance data/access records conditionally.
Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete User Photo Templates	To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "Face re-registration is required after"

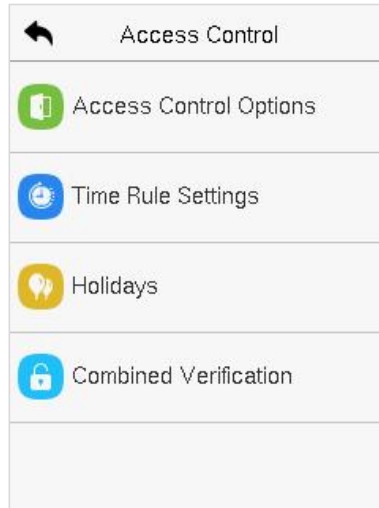
	an algorithm upgrade.”
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete all the screen savers in the device.

The user may select **Delete All** or **Delete by Time Range** when deleting the access records, attendance photos or block listed photos. Selecting **Delete by Time Range**, you need to set a specific time range to delete all data within a specific period.



12 Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.

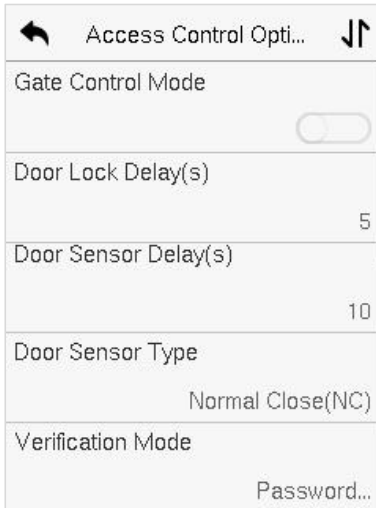


To gain access, the registered user must meet the following conditions:

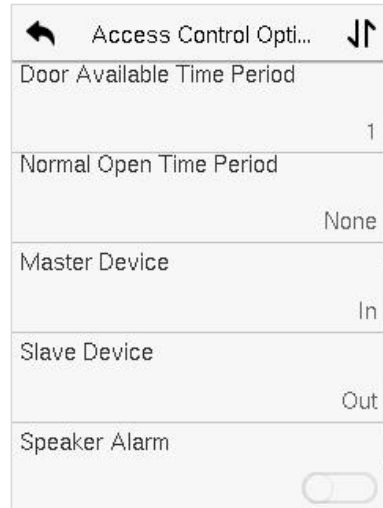
1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those group's members is also required to unlock the door).
3. In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

12.1 Access Control Options

Tap **Access Control Options** on the **Access Control** interface to set the parameters of the control lock of the terminal and related equipment.



Gate Control Mode	<input type="checkbox"/>
Door Lock Delay(s)	5
Door Sensor Delay(s)	10
Door Sensor Type	Normal Close(NC)
Verification Mode	Password...



Door Available Time Period	1
Normal Open Time Period	None
Master Device	In
Slave Device	Out
Speaker Alarm	<input type="checkbox"/>

Function Description

Function Name	Description
Gate Control Mode	It toggles between ON or OFF switch to get into gate control mode or not. When set to ON , the interface removes the Door lock relay, Door sensor relay, and Door sensor type options.
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.

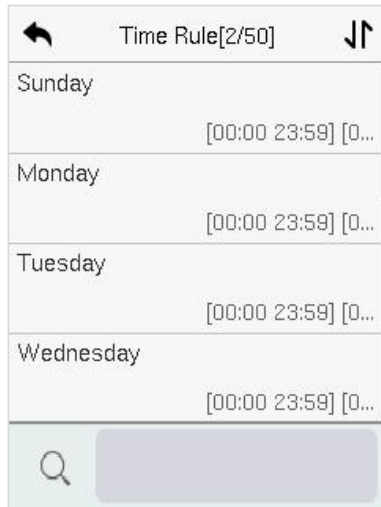
Verification Mode	The supported verification mode includes Password/Card/Face, User ID Only, Password, Card Only, Password + Card, Password/Card, Face Only, Face + Password, Face + Card.
Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Master Device	<p>While configuring the master and slave devices, you may set the state of the master as Out or In.</p> <p>Out: A record of verification on the master device is a check-out record.</p> <p>In: A record of verification on the master device is a check-in record.</p>
Slave Device	<p>While configuring the master and slave devices, you may set the state of the slave as Out or In.</p> <p>Out: A record of verification on the slave device is a check-out record.</p> <p>In: A record of verification on the slave device is a check-in record.</p>
Speaker 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.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

12.2 Time Schedule

Tap **Time Rule Settings** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).



On the selected Time Zone number interface, tap on the required day (that is Monday, Tuesday, etc.) to set the time.

Time Period 1

00:00 23:59

▲	▲	▲	▲
00	00	23	59
▼	▼	▼	▼
HH	MM	HH	MM

Confirm (OK) Cancel (ESC)

Specify the start and the end time, and then tap **OK**.

Note:

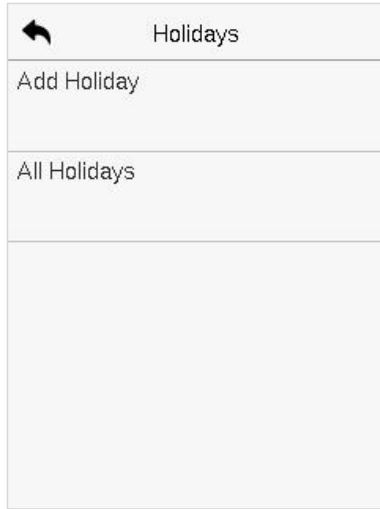
- The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57~23:56**).
- It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00~23:59**).
- The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).

The default Time Zone 1 indicates that the door is open all day long.

12.3 Holidays

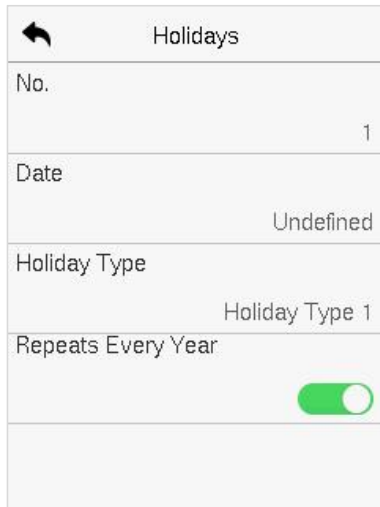
Whenever there is a holiday, you may need a distinct access time; but changing everyone's access time one by one is extremely cumbersome, so a holiday access time can be set that applies to all employees and the user will be able to open the door during the holidays.

Tap **Holidays** on the **Access Control** interface to set the Holiday access.



➤ **Add a New Holiday**

Tap **Add Holiday** on the **Holidays** interface and set the holiday parameters.



➤ **Edit a Holiday**

On the **Holidays** interface, select a holiday item to be modified. Tap **Edit** to modify holiday parameters.

➤ Delete a Holiday

On the **Holidays** interface, select a holiday item to be deleted and tap **Delete**. Press **OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

12.4 Combined Verification

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen security.

In a door-unlocking combination, the range of the combined number N is $0 \leq N \leq 5$ and the number of members N may all belong to one access group or may belong to five different access groups.

Tap **Combined Verification on** the **Access Control** interface to configure the combined verification setting.



On the combined verification interface, tap the Door-unlock combination to be set, and tap the **up** and **down** arrows to input the combination number, and then press **OK**.

For Example:

- If the **Door-unlock combination 1** is set as **(01 03 05 06 08)**. It indicates that the

unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.

- If the **Door-unlock combination 2** is set as **(02 02 04 04 07)**. It indicates that the unlock combination 2 consists of 5 people; the first two are from AC Group 2, the next two are from AC Group 4, and the last person is from AC Group 7.
- If the **Door-unlock combination 3** is set as **(09 09 09 09 09)**. It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as **(03 05 08 00 00)**. It indicates that the unlock combination 4 consists of only three people. The first person is from AC Group 3, the second person is from AC Group 5, and the third person is from AC Group 8.

Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

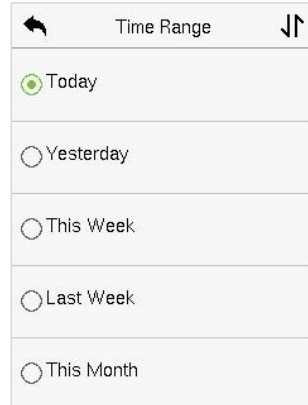
13 Attendance Search

Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

Select **Attendance Search** on the **Main Menu** interface to search for the required event Logs.



1. Enter the user ID to be searched and tap **OK**. If you want to search for records of all users, tap **OK** without entering any user ID.



2. Select the time range in which the records need to be searched.

Date	User ID	Time
05-09	04	
	0	09:10 09:10 09:10
		09:10
05-07	08	
	0	11:58 11:58 11:52
		11:52 11:52 11:52
		11:52 11:52
05-06	04	
	0	09:03 09:03 09:03
		09:03
05-05	131	
	0	18:02 18:02 16:32
		16:32 16:30 16:30

Once the record search completes. Tap the record highlighted in green to view its details.

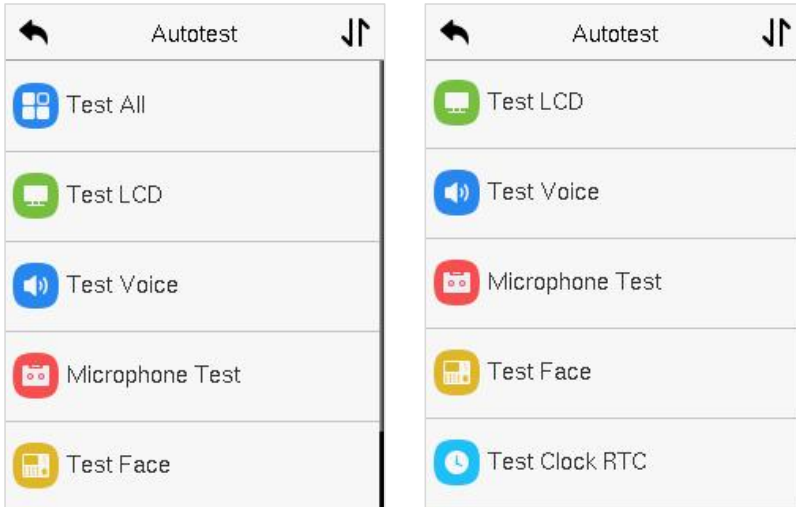
User ID	Name	Time
0		05-09 09:10
0		05-09 09:10
0		05-09 09:10
0		05-09 09:10

Verification Mode : Other
Status : 2

The figure shows the details of the selected record.

14 Autotest

Select **Main Menu**, tap **Autotest**. It enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Microphone, Camera and Real-Time Clock (RTC).



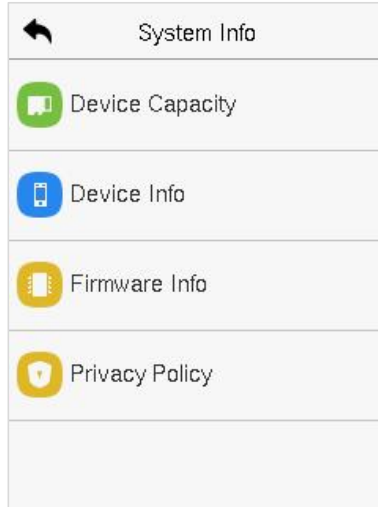
Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Voice, Microphone, Card, Camera and Real-Time Clock (RTC) are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.

Microphone test	To test if the microphone is working properly by speaking into the microphone.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

15 System Information

On the **Main Menu**, tap **System Info** to view the storage status, the version information of the device, firmware information and the privacy policy.



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, card, password and face storage, administrators and T&A records.
Device Info	Displays the device's name, serial number, MAC address, face algorithm, platform information, MCU Version, Manufacturer, and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	Display the device's privacy policy.

16 Connect to ZKBioAccess Software

16.1 Set the Communication Address

➤ Device side

1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

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

2. In the main menu, click **COMM.** > **Cloud Server Setting** to set the server address and server port.

Server address: Set the IP address as of ZKBioAccess server.

Server port: Set the server port as of ZKBioAccess (The default is 8088).

Ethernet		Cloud Server Setting	
IP Address	192.168.163.201	Server Mode	ADMS
Subnet Mask	255.255.255.0	Enable Domain Name	<input type="checkbox"/>
Gateway	192.168.163.1	Server Address	0.0.0.0
DNS	114.114.114.114	Server Port	8081
TCP COMM.Port	4370	Enable Proxy Server	<input type="checkbox"/>
DHCP	<input type="checkbox"/>	HTTPS	<input type="checkbox"/>

➤ Software side

Login to ZKBioAccess software, click **System** > **Communication** > **Communication Monitor** to set the ADMS service port, as shown in the figure below:

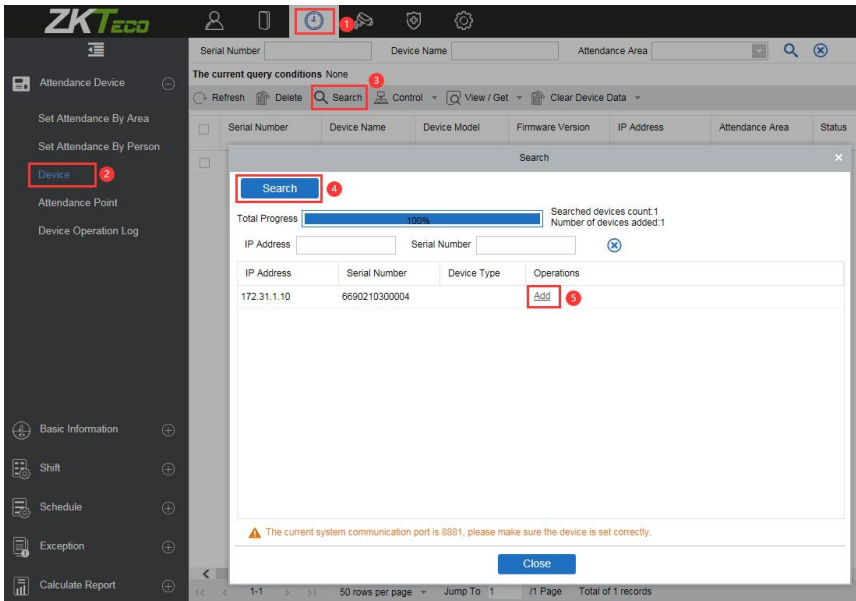
The screenshot shows the ZKTECO software interface. The left sidebar has a menu with 'Communication Monitor' highlighted. The main content area is titled 'Adms Service Settings' and contains the following information:

- Adms Service Port:** 8081
- Warning:** The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port.
- Allow external network access:** Radio buttons for 'No' (selected) and 'Yes'.

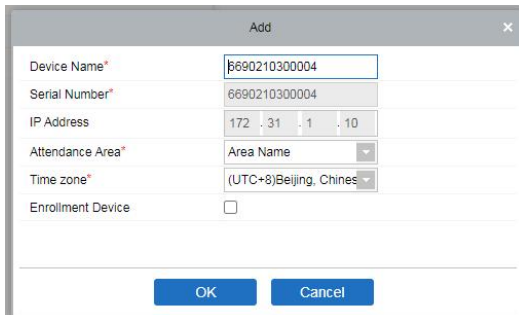
16.2 Add Device on the Software

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

1. Click **Attendance > Attendance 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 Attendance Area and Time zone from each dropdowns and click **OK** to add the device.



16.3 Add Personnel on the Software

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

The screenshot shows a 'New' personnel registration window. It features a top section with input fields for 'Personnel ID*', 'Department*' (set to 'Ban Giam Đock'), 'First Name', 'Last Name', 'Gender', 'Mobile Phone', 'Certificate Type', 'Certificate Number', 'Birthday', 'Email', 'Device Verification Password', and 'Card Number'. A 'Biometrics Type' field is present with 'Browse' and 'Capture' buttons. Below this is a 'Personnel Detail' section with a 'Levels Settings' list (General, Test, office, a) and a 'Personnel Detail' table with fields for 'Superuser', 'Device Operation Role', 'Disabled', and 'Set Valid Time'. At the bottom are 'Save and New', 'OK', and 'Cancel' buttons.

2. Fill in all the required fields and click **OK** to register a new user.


3. Click **Attendance > Attendance Device > Device > Control > Synchronize Software Data to the Device** to synchronize all the data to the device including the new users.

For more details, please refer to the ZKBioAccess User Manual.


17 Connecting to ZKBio Talk Software

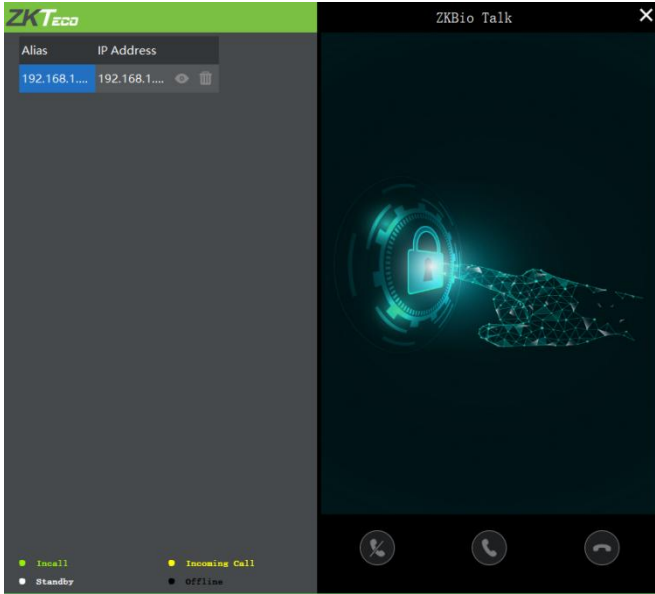
Download and install the ZKBio Talk software. The following are the steps to connect ZKBio Talk to the SpeedFace-V3L(Lite):



1. Firstly, change the parameter on the SpeedFace-V3L(Lite).

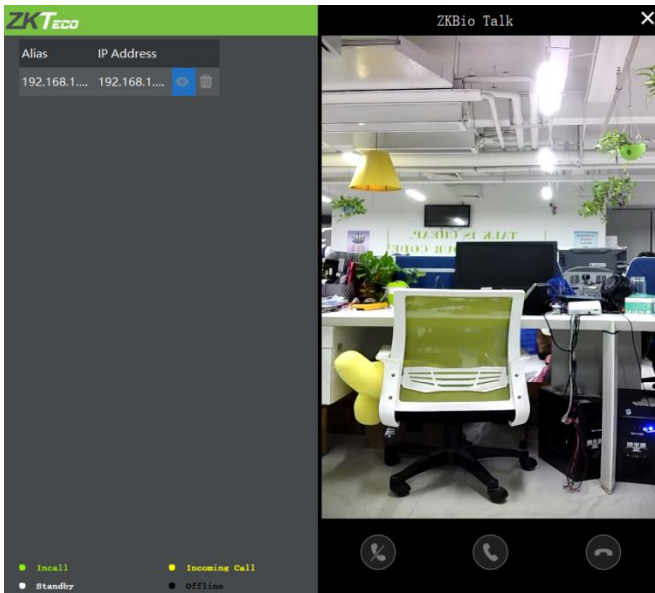
Tap  on the initial interface > **System** > **Video Intercom Parameters** > **Intercom Server Settings** on the device to change the server address and server port, as shown in the following figure.


Intercom Server Set...	
Server Address	192.168.163.61
Server Port	25550

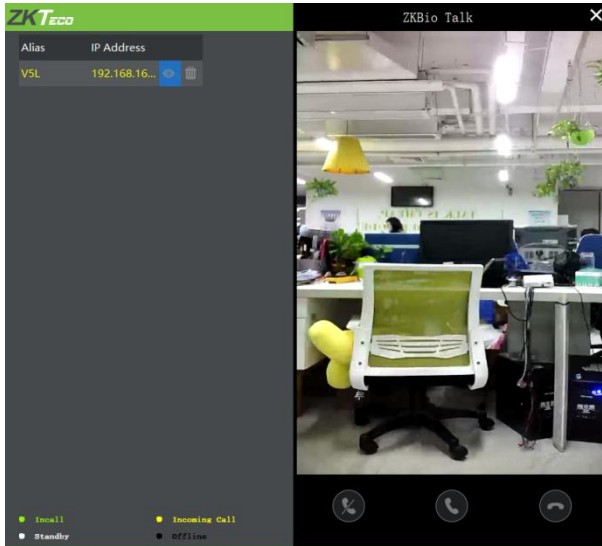
- **Server Address:** Enter the current server IP address, i.e., the IP address of the server after the software is installed.
 - **Server Port:** The default server port is **25550**.
2. Double click the  icon to open the ZKBio Talk software. When the device-side video intercom parameters are set correctly, the device automatically pushes the device list on the left, as shown in following figure.




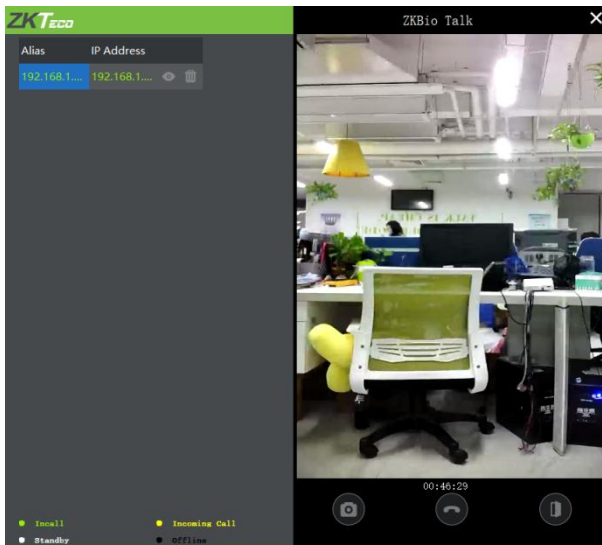
- 3. Users can click on  to preview the video on the right. Click  icon to close the preview screen.





- 4. When a user clicks the  **Doorbell Button** on the device to make a call, the software interface displays the IP address of the calling device in yellow.



- 5. When the user clicks the  icon to answer the call, the IP address is displayed in green while on the call. The call duration is also displayed just above the icon.



Function Description:


Menu	Description
	This is the Snapshot key, used to take a snapshot.
	This is the Remote open key, used to open the door remotely. The default lock drive time is 5 seconds

Note: Only the offline devices can be removed.

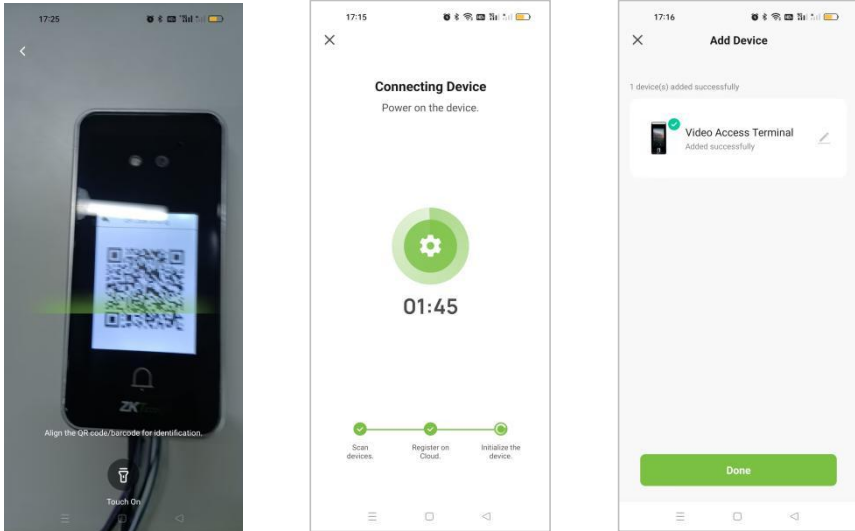
18 Connecting to ZSmart APP★

18.1 Adding Device on the ZSmart APP



After downloading and installing the ZSmart APP on your phone, create a User account initially with your Email ID. After creating the User account, log in to the APP, and click **Add Device** or **+** icon on the top right corner of the screen to add a device. The process is as follows:

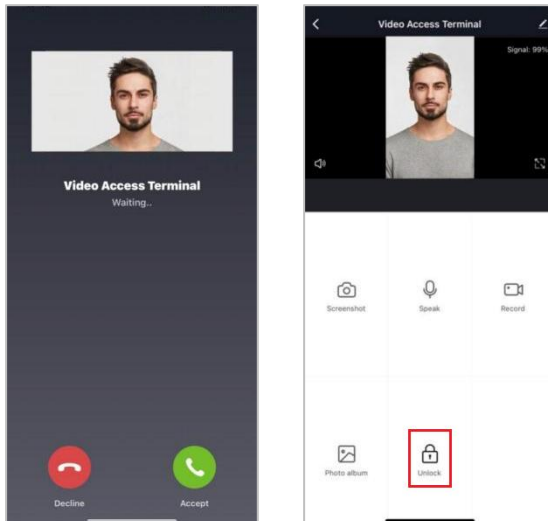
1. Click **Add Device** on the Home page.
2. Tap on **System > Video Intercom Parameters > QR Code Binding** to show the QR code of the device.
3. Click the  icon in the upper right corner.





18.2 Video Phone Connection

Visitors press the  **Doorbell Button** on the device to make a call and the phone will ring. The user can accept or decline the call. After the user accepts the call, it will open the video door phone interface. And then click  icon to unlock the door.



Function Description:

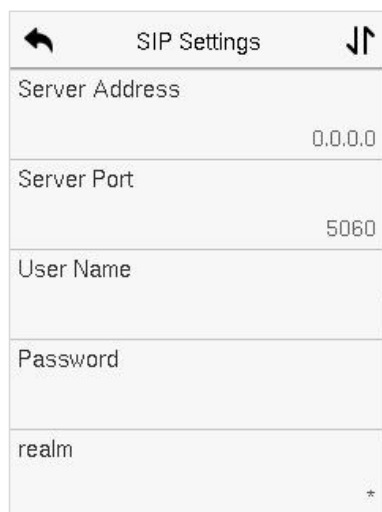
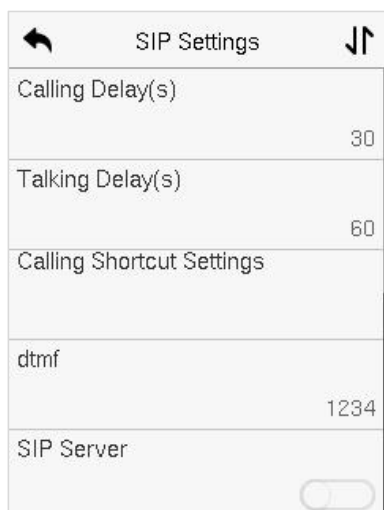
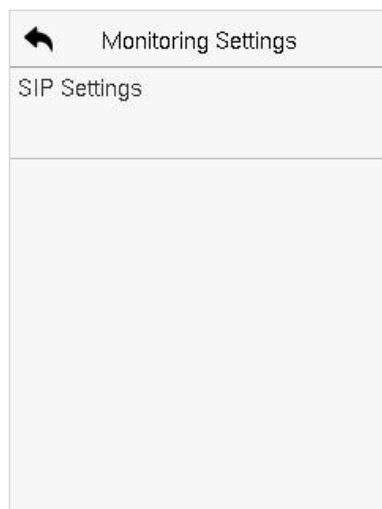
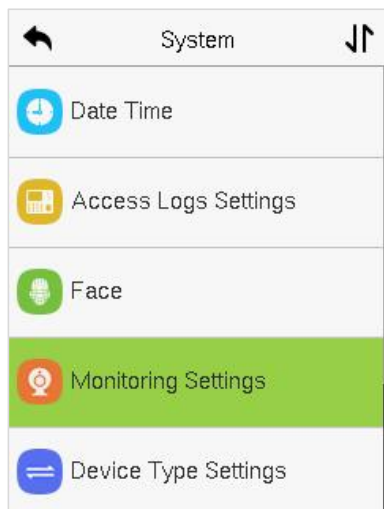
Parameter	Description
Screenshot	Click to take a screenshot.
Speak	The icon becomes blue when click it, and you can talk to the device at this time.
Record	Click to make a record video.
Photo album	View and delete screenshots and recorded videos.
Unlock	Click to open the door remotely. The unlocking record is saved in Me > Message Center .

Note: For other specific operations, please refer to the ZSmartAPP User Manual.

19 Connecting to SIP★

Tap **Monitoring Settings** > **SIP Settings** on the System interface to enter the SIP parameter setting interface.

Note: This function needs to be used with the indoor station **Vpad A2**.



Function Description

Function Name	Description
Calling Delay(s)	Set the time of call, valid value 30 to 60 seconds.
Talking Delay(s)	Set the time of intercom, valid value 60 to 120 seconds.
Calling Shortcut Settings	You can set a shortcut key to call the indoor station quickly without entering the IP address of the indoor unit each time.
dtmf	The value of WebServer is the same as the value of DMTF in the device in order to unlock it.
SIP Server	Select whether to enable the server address. Once you have connected to the server, you can call it by entering the username of the indoor station.
Server Address	The SIP server address.
Server Port	The SIP server port.
User Name	User name of the server, required field, user definable.
Password	The password of the SIP server. Users need to get the password from the distributor.
realm	The realm of server.

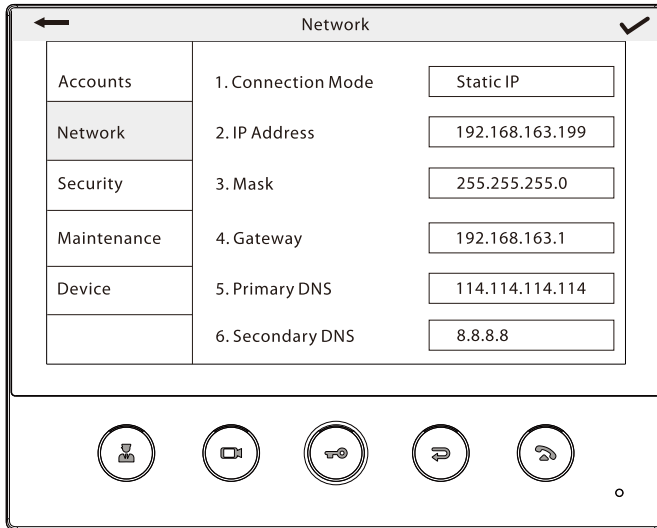
The SpeedFace-V3L(Lite) and the indoor station to achieve video intercom there are two modes, respectively, the LAN and SIP server.

Note: SIP is an optional feature, when users need to enable the SIP server, they need to purchase the server address and password from the distributor.

19.1 Local Area Network Use

Set the IP address on the indoor station, Tap **Menu > Advanced > Network > 1. Network > 1. IPv4.**

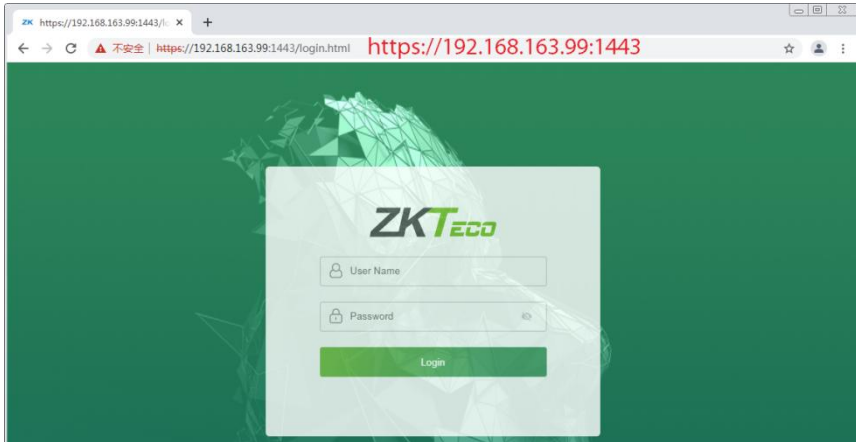
Note: In LAN, the IP addresses of the indoor station and the SpeedFace-V3L(Lite) must be in the same network segment.



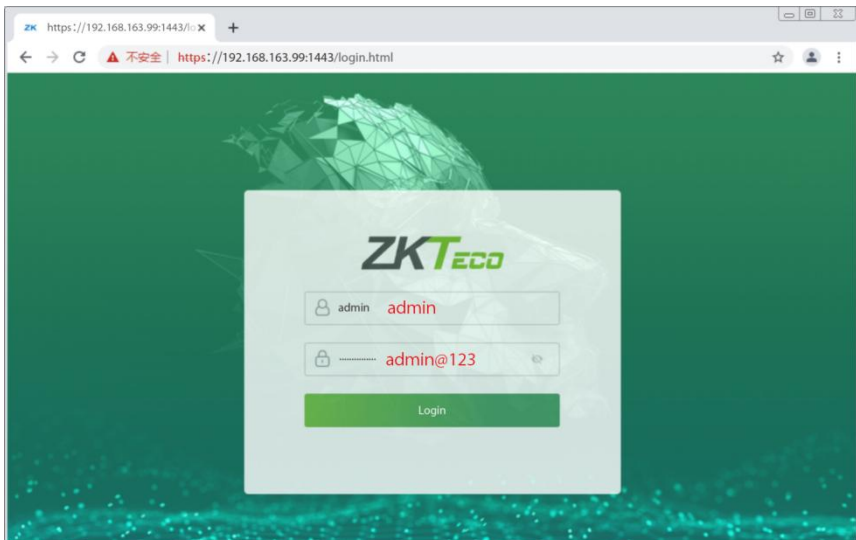
● Custom the Punch Status Options

1. Use your browser to enter the address to log into WebSever, the address is the Serial IP Address:**1443**, for example: <https://192.168.163.99:1443>.

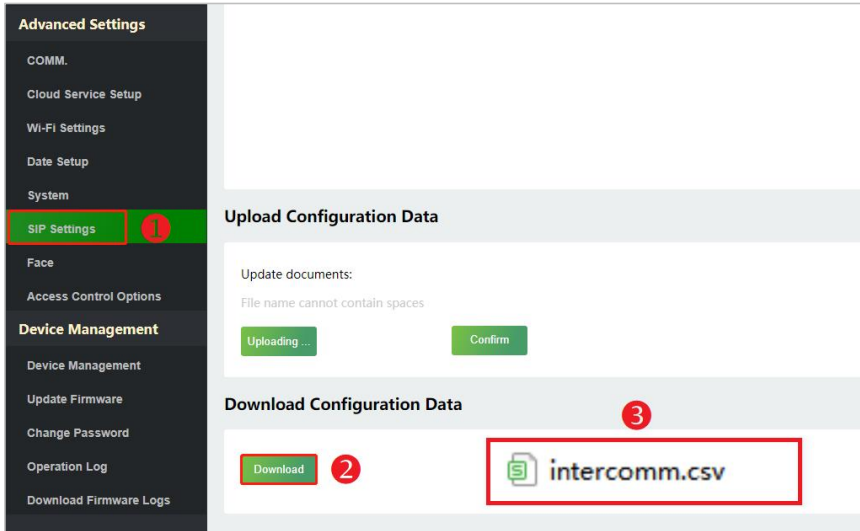




2. Enter the WebSever account and password, the initial account is: **admin**, password: **admin@123**.



3. After logging into the interface, click **Advanced Settings** > **SIP Settings** > **Download Configuration Data** to download an **intercomm.csv** file.



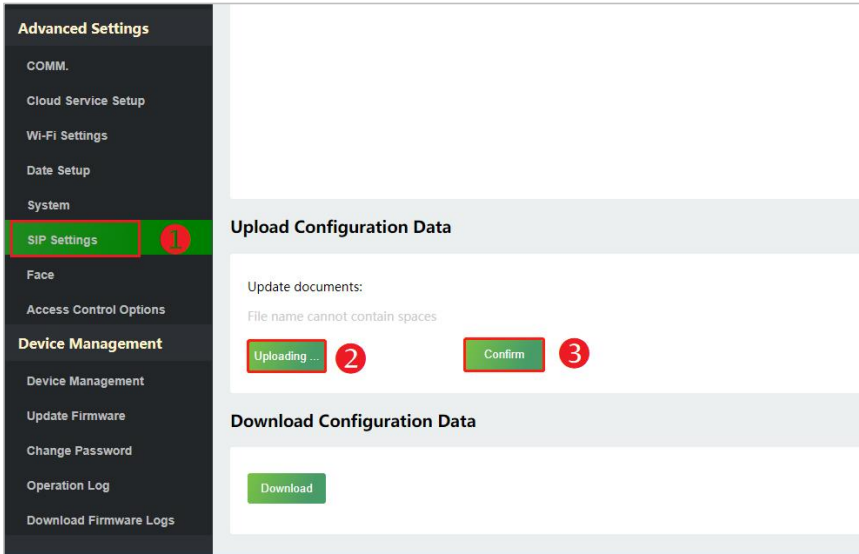
4. Enter the indoor station's communication address and device number in the downloadable form.

	A	B	C	D
1	IP Address	Subnet Mask	Gateway	Dialing Number
2	192.168.163.199	255.255.255.0	192.168.163.1	9
3	192.168.163.205	255.255.255.0	192.168.163.1	3
4	192.168.163.103	255.255.255.0	192.168.163.1	4
5	192.168.163.104	255.255.255.0	192.168.163.1	5
6	192.168.163.105	255.255.255.0	192.168.163.1	6
7				

IP Address/Subnet Mask/Gateway: Must be the same as the indoor station to be connected.

Dialing Number: Customize the number of the indoor station, you can enter the value on SpeedFace-V3L(Lite) to call the indoor station quickly for video intercom.

5. Once the form is set up and saved, upload the configuration form in WebServer.



6. On SpeedFace-V3L(Lite), tap **Calling Shortcut Settings**, select any item except admin, and enter the form information you just uploaded.




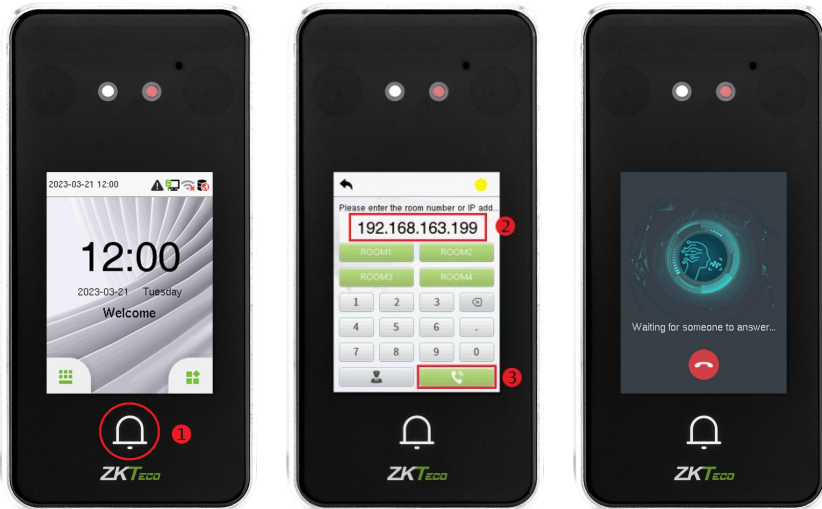
Function Description

Function Name	Description
Name	You can customize any character (support Chinese, English, numbers, symbols, etc.) that will be displayed on the call page.

Device Number	It is the dialing number in the configuration data, you can enter the value on SpeedFace-V3L(Lite) to call the indoor station quickly for video intercom.
IP Address	After entering the dialing number, the corresponding IP address in the configuration data will be automatically paired.

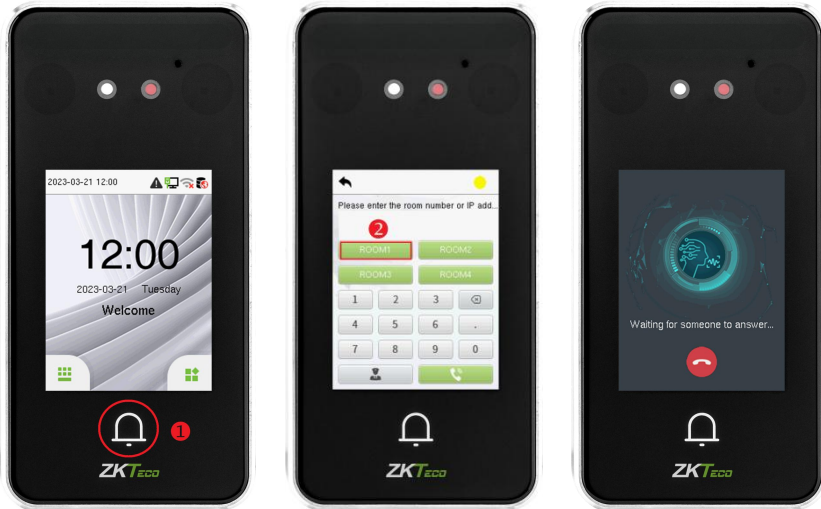
● **Directly Enter the IP Address of the Indoor Station**

Once the indoor station is configured with the network, the video intercom function can be realized by tap the  **Doorbell Button** on the SpeedFace-V3L(Lite) and entering the IP address of the indoor station in the jumping interface.



● **Name**

You can then tap **ROOM1** on the punch status options to directly implement the video intercom.



● **Device Number**

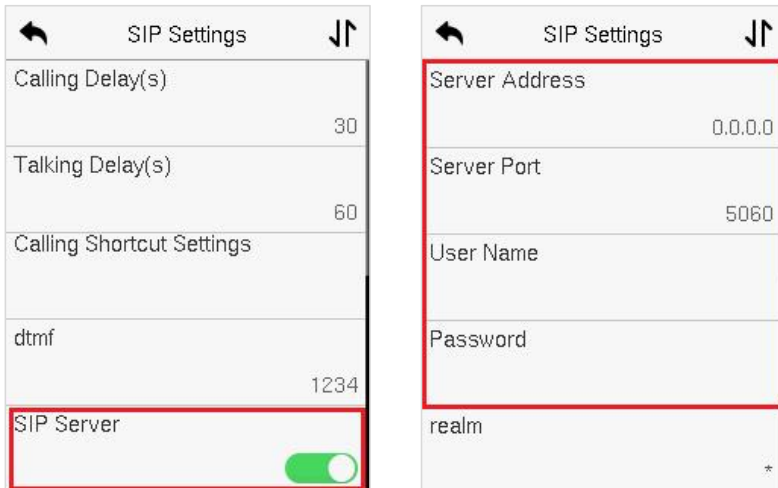
Enter the device number in the call screen.



19.2 SIP Server

1. On SpeedFace-V3L(Lite), enable the **SIP Server**, after the device is rebooted, enter the server-related parameters.

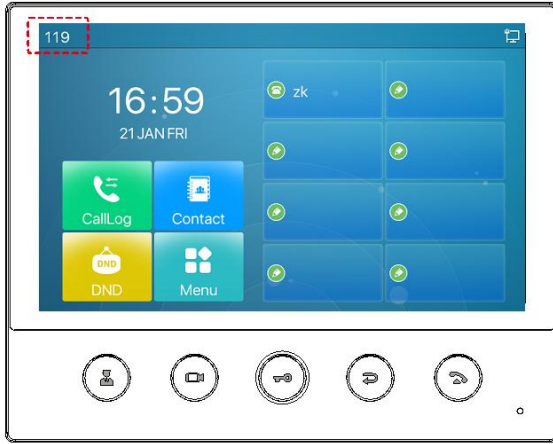
Note: SIP is an optional feature, users need to purchase the server address and password from the distributor, the user name is required fields can be customized.



2. Once the SIP is set up correctly, a green dot will appear in the upper right corner of the call page to indicate that the SpeedFace-V3L(Lite) is connected to the server.



- 3. Check the account number under the indoor station menu.



- 4. Just enter the account number of the indoor station in the call screen of SpeedFace-V3L(Lite) and then click the call icon.



For details on the operation and use of the indoor station, please refer to the *indoor station user manual*.

ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone: +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com



Copyright © 2023 ZKTECO CO., LTD. All Rights reserved.