User Manual

IN710

Date: January 2023

Doc Version: 1.2

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

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

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

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

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

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

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

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

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

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

ZKTeco Headquarters

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

Phone +86 769 - 82109991

Fax +86 755 - 89602394

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

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

About the Company

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

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

About the Manual

This manual introduces the operations of the **IN710**.

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

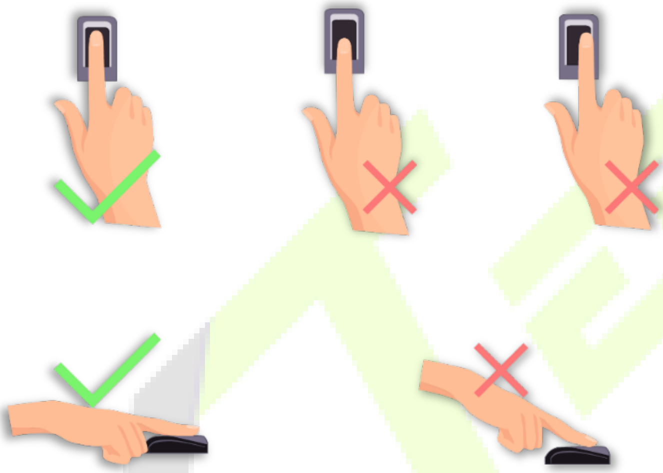
1 Instruction for Use

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

1.1 Finger Placement

Recommended fingers: Index, middle, or ring fingers.

Avoid using the thumb or pinky finger, as they are difficult to accurately tap onto the fingerprint reader.



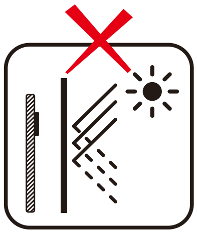
Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification.

1.2 Installation

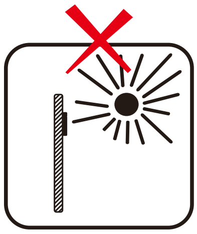
1.2.1 Use Environment

Please refer to the following recommendations for installation.

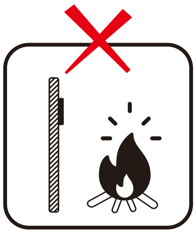
INSTALL INDOORS
ONLY



AVOID INSTALLATION
NEAR
GLASS WINDOWS



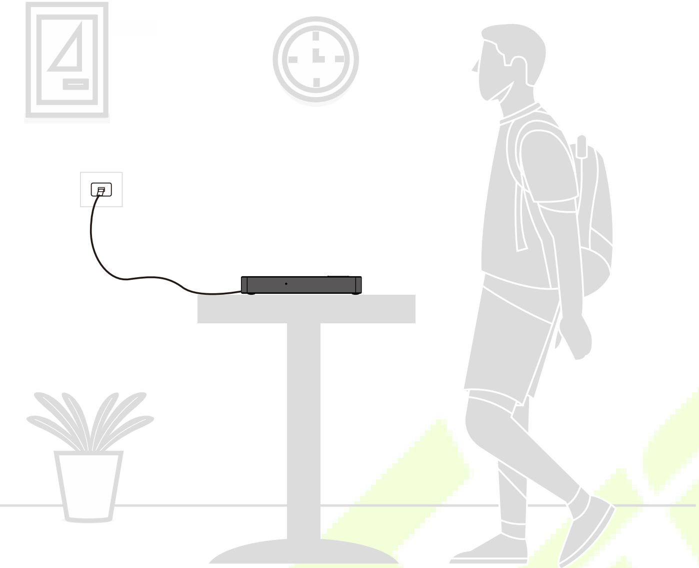
AVOID DIRECT
SUNLIGHT
AND EXPOSURE



AVOID USE OF ANY
HEAT SOURCE
NEAR THE DEVICE

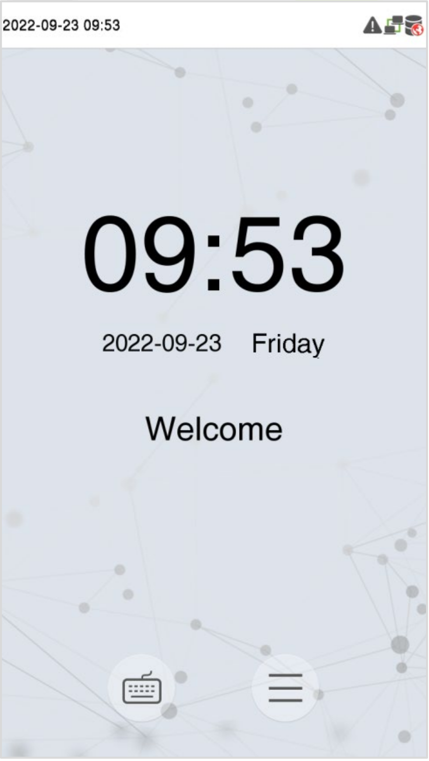
1.2.2 Device Installation

The IN710 requires no complicated installation, just fix the device on a flat table.



1.3 Standby Interface

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



2022-09-23 09:53

09:53

2022-09-23 Friday

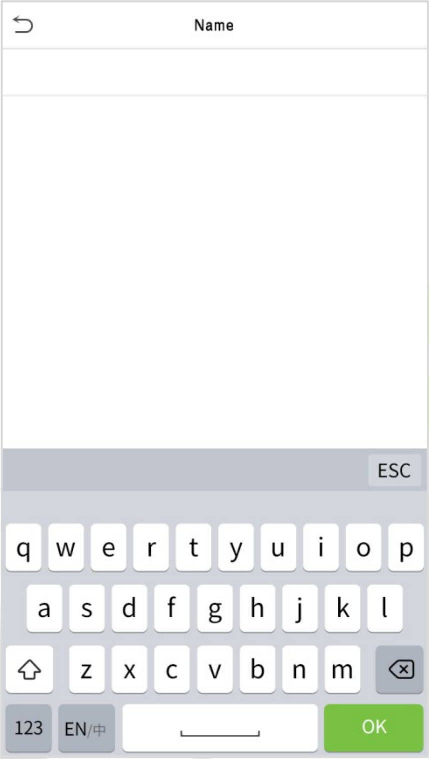
Welcome

- Tap ⌨ button to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap ☰ button 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.

1.4 Virtual Keyboard



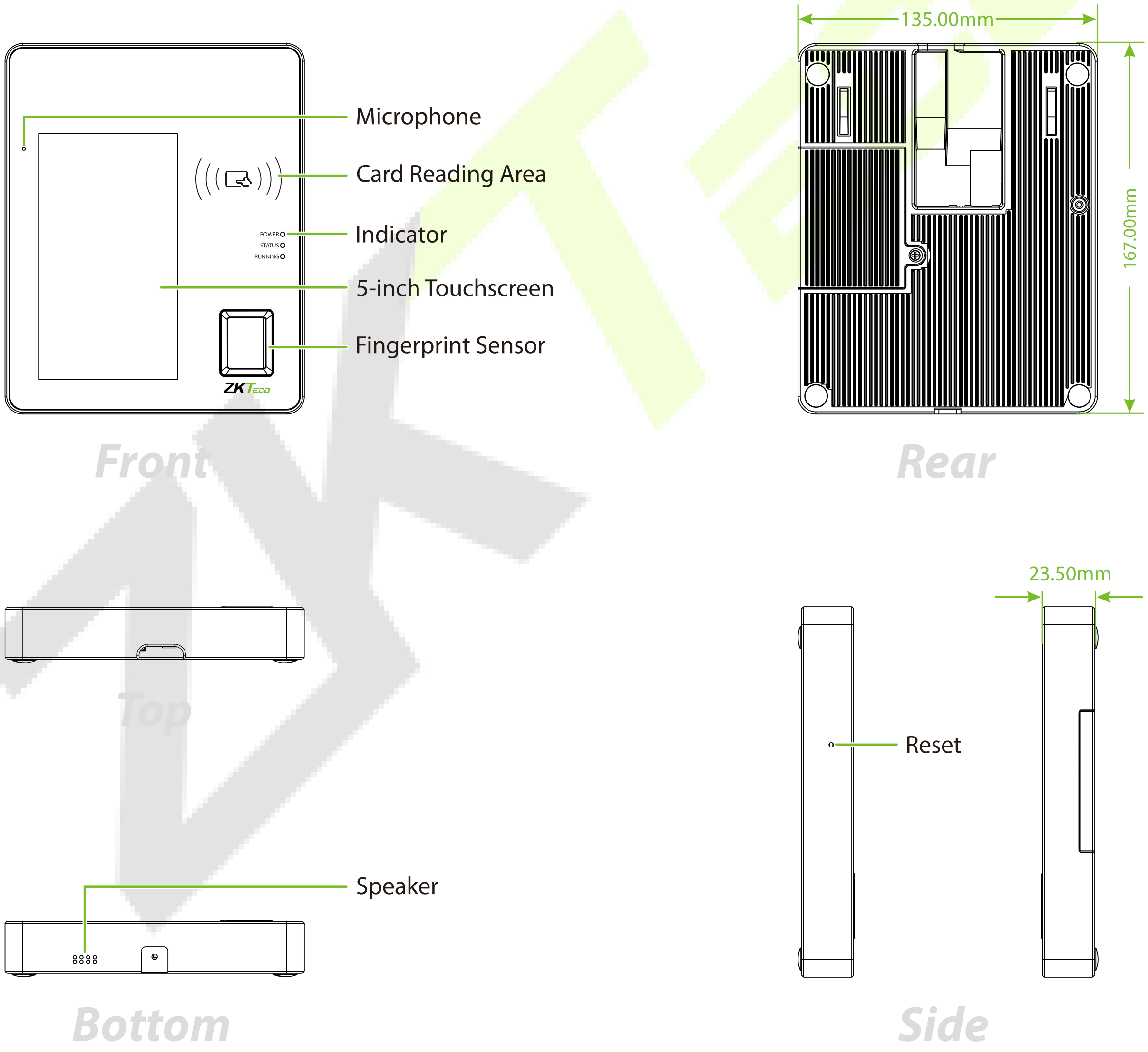
Note: The device supports the input in English language, numbers, and symbols.

- Tap [**En**] to switch to the English keyboard.
- Press [**123**] to switch to the numeric and symbolic keyboard.
- Tap [**ABC**] to return to the alphabetic keyboard.
- Tap the input box, a virtual keyboard appears.
- Tap [**ESC**] to exit the virtual keyboard.

2 Overview

ZKTeco developed the IN710, it is a well-designed and powerful personal verification and reader for Indonesian ID cards. The device features a 5-inch HD touch screen, speakers and mass storage for a fully upgraded body authentication terminal. Integrated smart card module and fingerprint module, support ISO/IEC 19794-2:2011 fingerprint template, maximum compatibility to read Indonesian ID card information, verify the validity of ID card and cardholder fingerprint. In addition, it also supports attendance access control. Applicable to government, banking, education, finance and other industries.

2.1 Appearance



2.2 Features

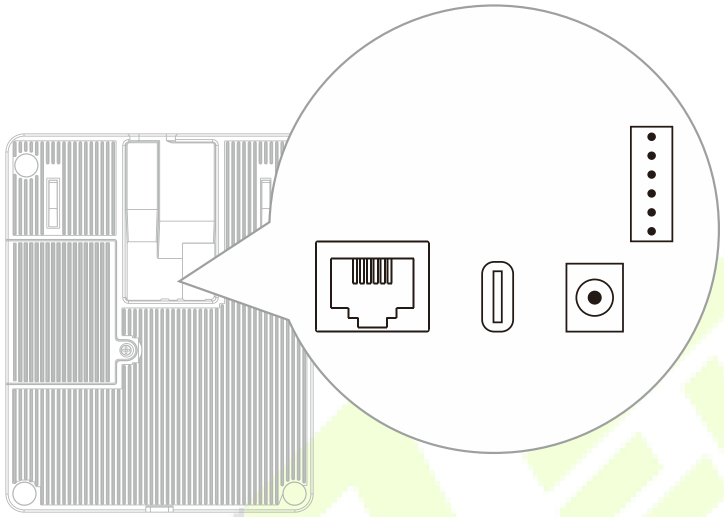
- The USB 2.0 interface has stable communication and unified integration.
- Read card information selectively.
- The new tamper-proof mechanism and unique identity protocol ensure data security.
- Equipped with 5-inch HD touchscreen.
- Strong anti-interference ability.
- Mass storage.
- Multiple Verifications: Fingerprint / Card / Password.

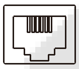
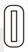
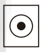
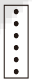
2.3 Technical Specifications

Model Name	IN710
Operating System	Linux
CPU	ARM Cortex-A53 Dual Core CPU @1.0GHz
Memory	RAM 8GB; ROM 8GB
Display	5-inch HD Touchscreen
Card Type	Indonesian ID Card
Card Reading Time	7s (Reading All Information)
Card Reading Distance	Up to 2cm
Fingerprint Module	Optical Fingerprint Module
Fingerprint Image Resolution	500 dpi
Fingerprint Image Size	300 * 400 pixels
Communication	TCP/IP
Interface	USB2.0
Power Supply	12V/3A
Standard Functions	T9 Input, Record Query, Access Levels, Tamper Switch Alarm, Multiple Verify Modes
Access Control Interface	Door Sensor, 3rd Party Electric Lock, Exit Button
Operating Humidity	20% to 80% RH

Operating Temperature	0°C to 45°C
Dimensions (L*M*H)	135.00*167.00*23.50(mm)

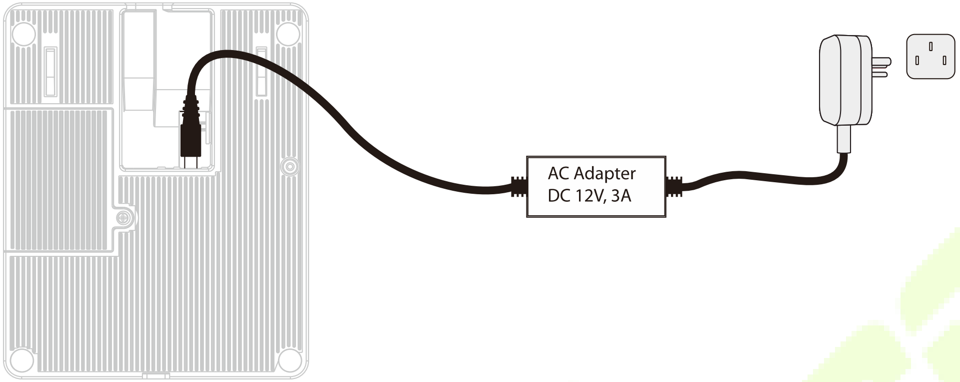
2.4 Terminal Description



Interface	Description	
	Network Interface	
	Type-C	
	12V Power In	
	NC	Lock
	COM	
	NO	
	SEN	Door Sensor
	GND	
	BUT	Exit Button

2.5 Wiring Description

2.5.1 Power Connection

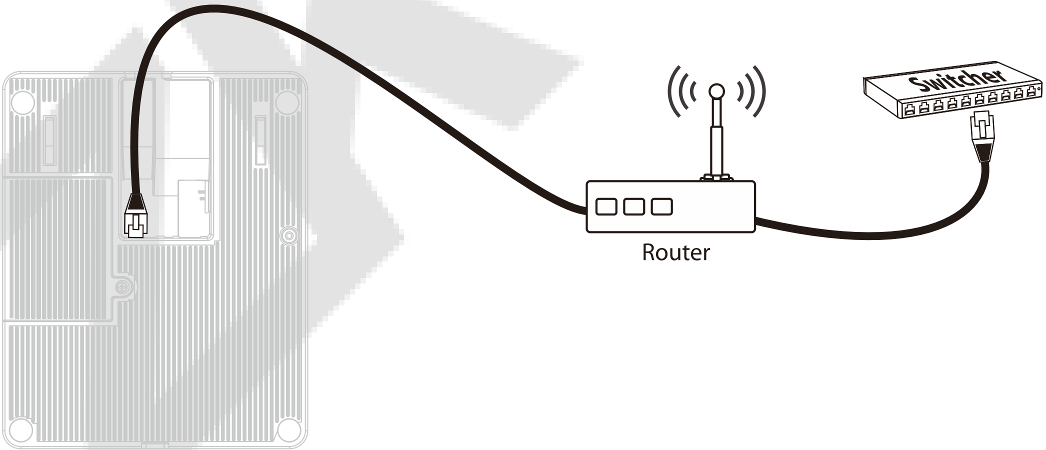


Recommended power supply

- Rating of 12V and 3A
- To share the device's power with other devices, use a power supply with higher current ratings.

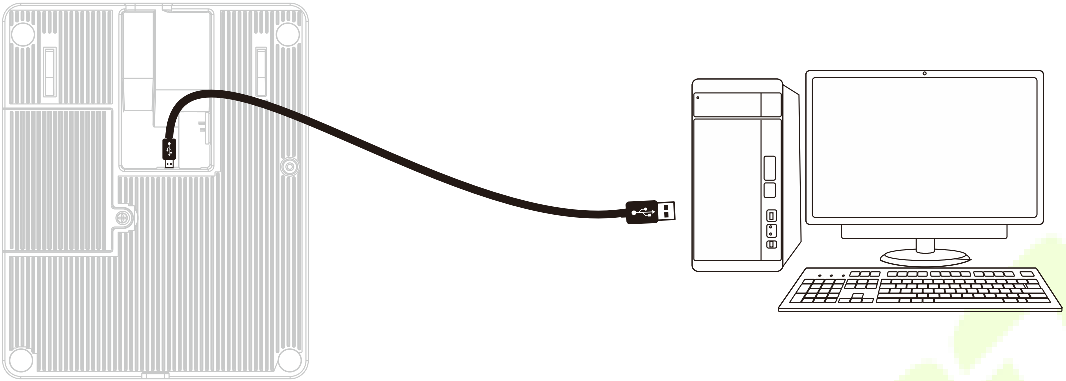
2.5.2 Ethernet Connection

After the device is powered on, connect the network connector via the Ethernet cable.

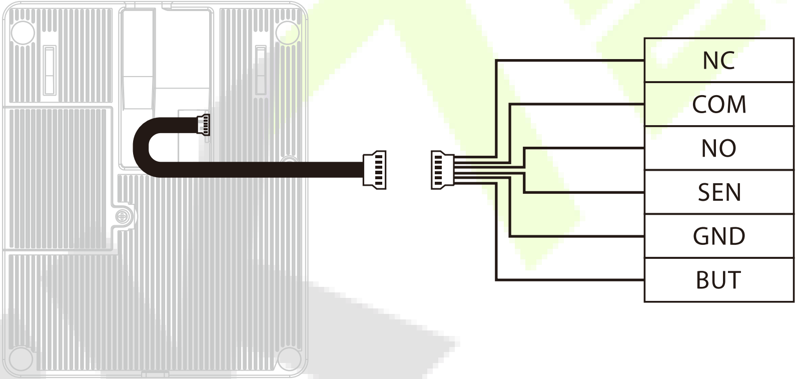


2.5.3 Type-C Connection

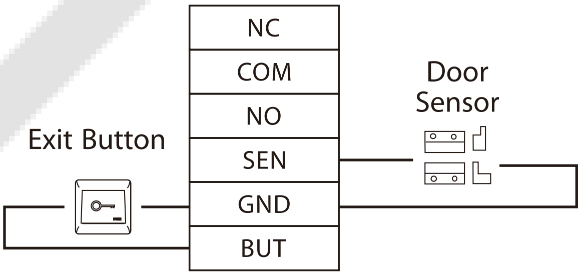
Connect the device and computer via Type-C cable.



2.5.4 Door Sensor, Exit Button and Lock Relay Connection

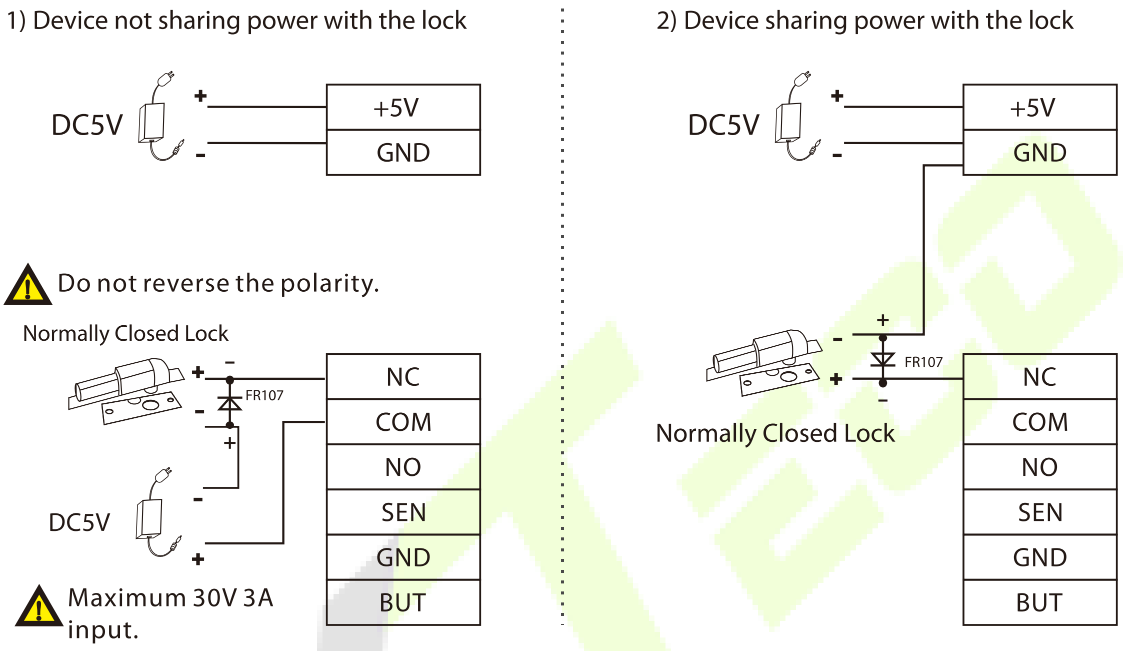


Door Sensor and Exit Button:



Lock Relay:

The system supports both Normally Opened Lock and Normally Closed Lock. The NO Lock (normally opened when power ON) is connected to 'NO1' and 'COM1' terminals, and the NC Lock (normally closed when power ON) is connected to 'NC1' and 'COM1' terminals. The power can be shared with the lock or used separately for the lock, as shown in the example with NC Lock below:


1) Device not sharing power with the lock

2) Device sharing power with the lock

3 Verification Mode

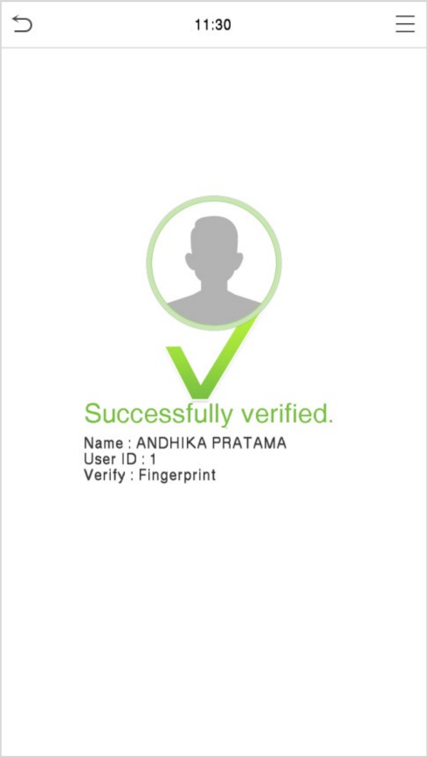
3.1 Fingerprint Verification

- **1:N Fingerprint Verification Mode:**

Compares the fingerprint pressed on the fingerprint reader to all the fingerprint data saved in the device.

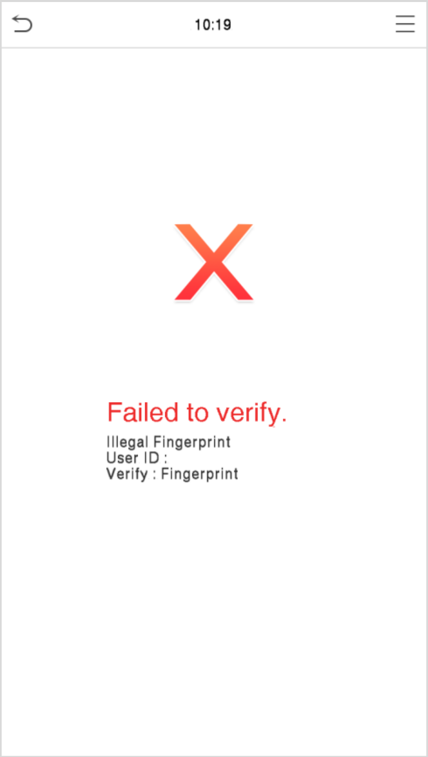
The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

Please follow the correct way to place your finger onto the sensor. For details, please refer to 1.1 Finger Placement section.



Successfully verified.

Name : ANDHIKA PRATAMA
User ID : 1
Verify : Fingerprint



Failed to verify.

Illegal Fingerprint
User ID :
Verify : Fingerprint

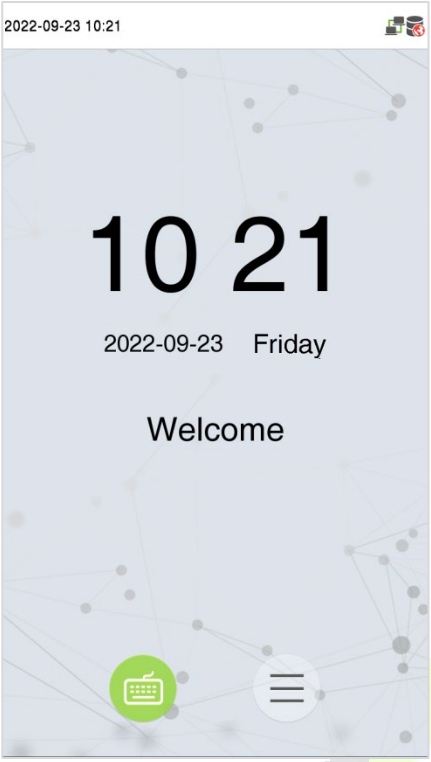
- **1:1 Fingerprint Verification Mode:**

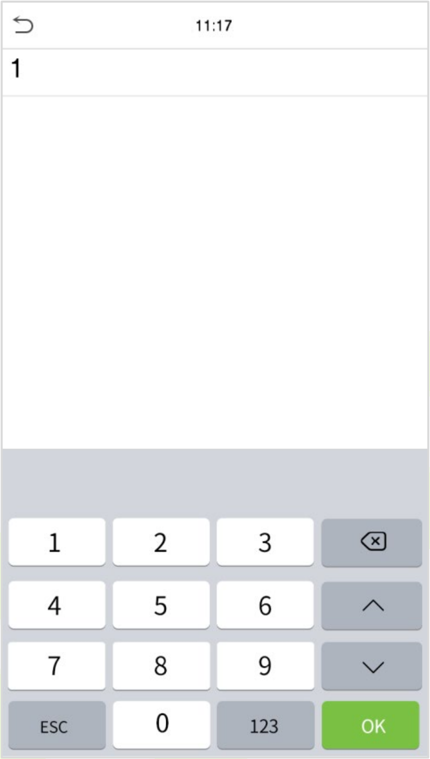
Compares the fingerprint pressed on the fingerprint reader to the fingerprints linked to User ID input via the virtual keyboard.

Users may verify their identities with 1:1 verification mode when they cannot gain access with 1: N authentication method.

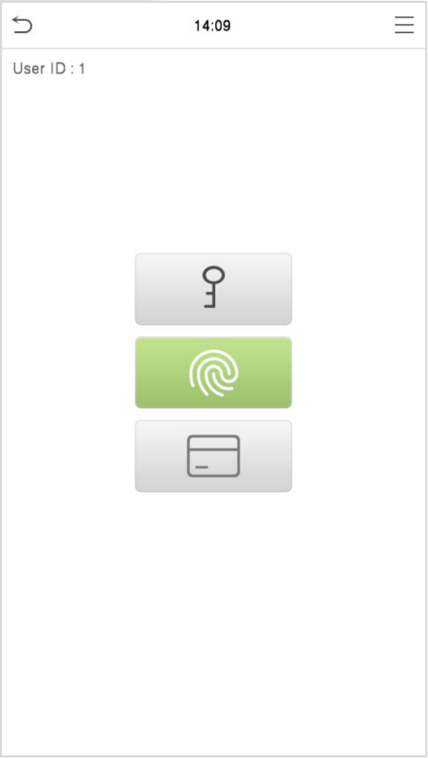
Click the ⌨ button on the main screen to enter 1:1 fingerprint verification mode.

Input the user ID and press [**OK**].

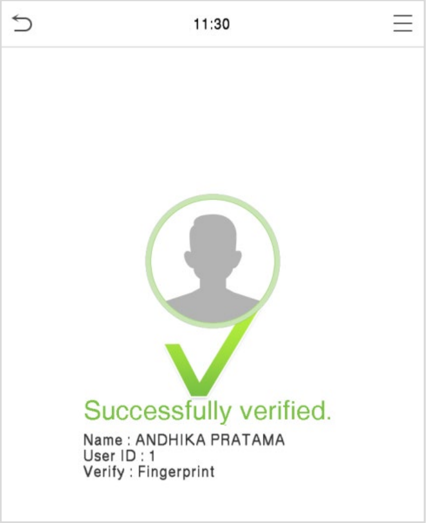




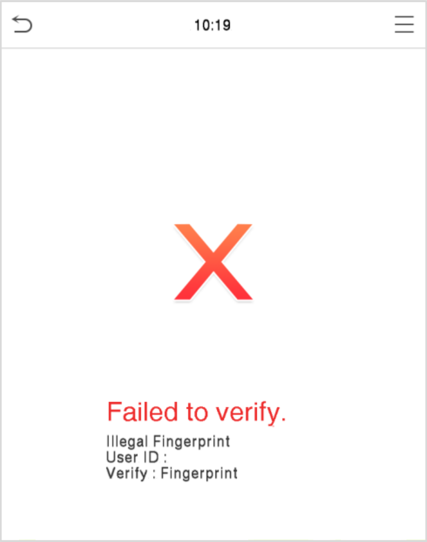
If the user has registered a password and a card in addition to his/her fingerprints and the verification method is set to Password/Fingerprint/Card verification, the following screen will appear. To enter fingerprint verification mode, press the fingerprint icon.



Press the fingerprint to verify.



Successfully verified.
Name : ANDHIKA PRATAMA
User ID : 1
Verify : Fingerprint



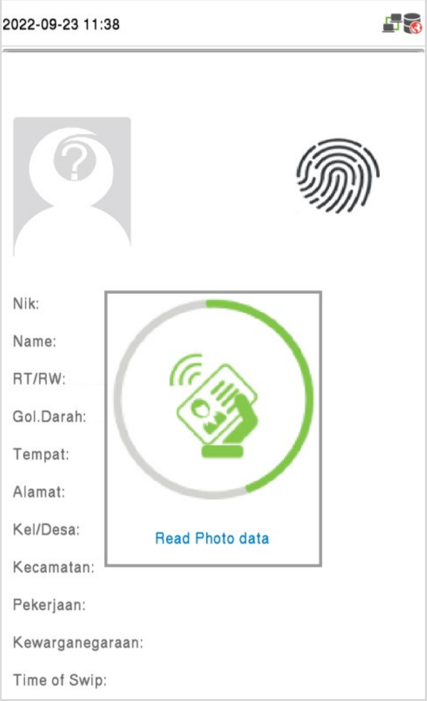
Failed to verify.
Illegal Fingerprint
User ID :
Verify : Fingerprint

3.2 Card Verification

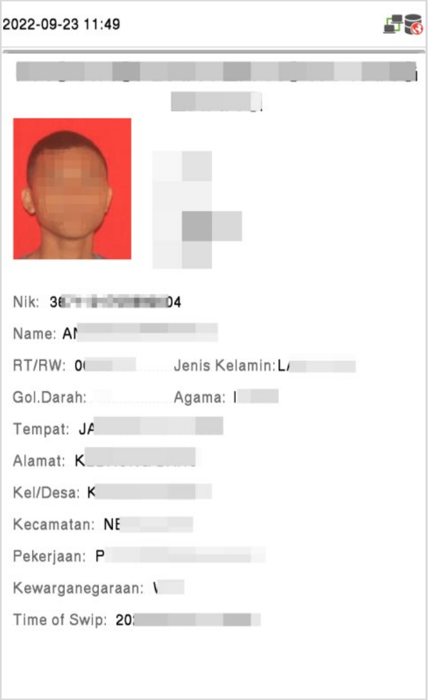
The Card Verification mode compares the card number in the card induction area with all the card number data registered in the device; the card verification screen is as follows

- **1: N Card Verification Mode:**

1:N Card Verification mode, place the ID card into the card induction area, the device automatically opens the identity verification, reading the ID card number, photo, comparing fingerprints and signatures, etc.


2022-09-23 11:38

Nik:
Name:
RT/RW:
Gol.Darah:
Tempat:
Alamat:
Kel/Desa:
Kecamatan:
Pekerjaan:
Kewarganegaraan:
Time of Swip:


2022-09-23 11:49

[redacted]

Nik: [redacted]
Name: [redacted]
RT/RW: [redacted] Jenis Kelamin: [redacted]
Gol.Darah: Agama: [redacted]
Tempat: [redacted]
Alamat: [redacted]
Kel/Desa: [redacted]
Kecamatan: [redacted]
Pekerjaan: [redacted]
Kewarganegaraan: [redacted]
Time of Swip: [redacted]

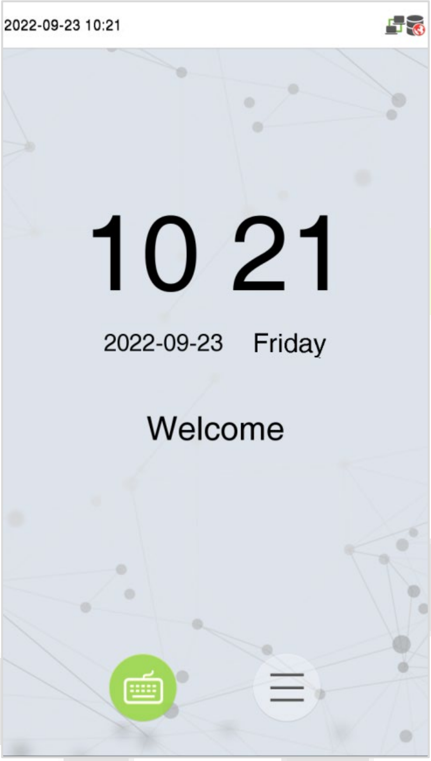
Note: The record of 1: N Card Verification mode will be recorded in the identity verification.

- **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 the ⌨ button on the main interface and enter the 1:1 card verification mode.

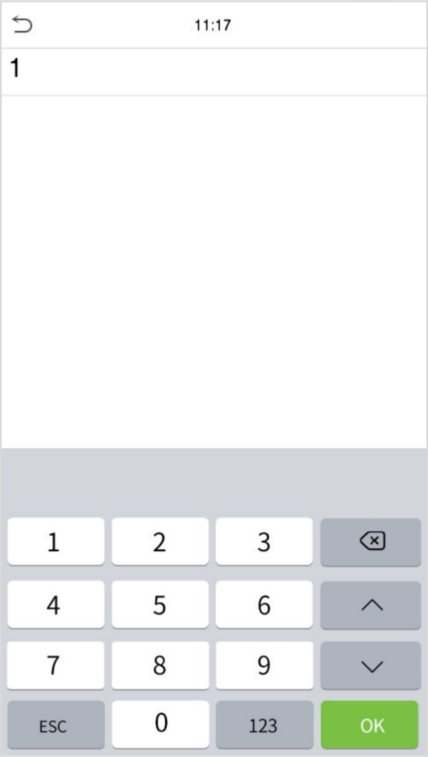
Enter the user ID and click [**OK**].


2022-09-23 10:21

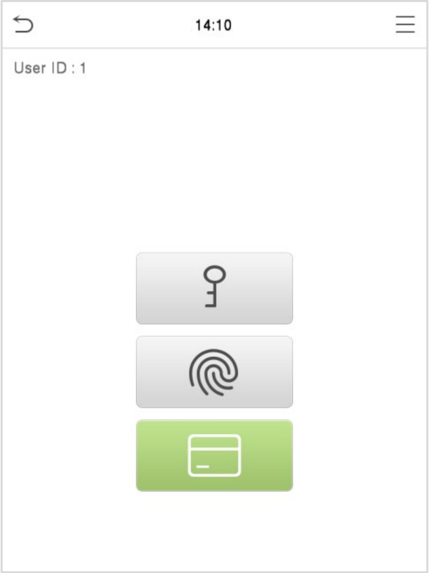
10 21

2022-09-23 Friday

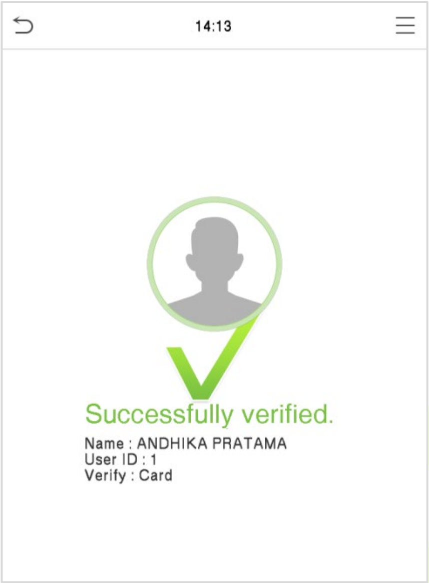
Welcome



If the user has registered a password and a fingerprint in addition to his/her card and the verification method is set to Password/Fingerprint/Card verification, the following screen will appear. To enter card verification mode, press the 💳 icon.



User ID : 1



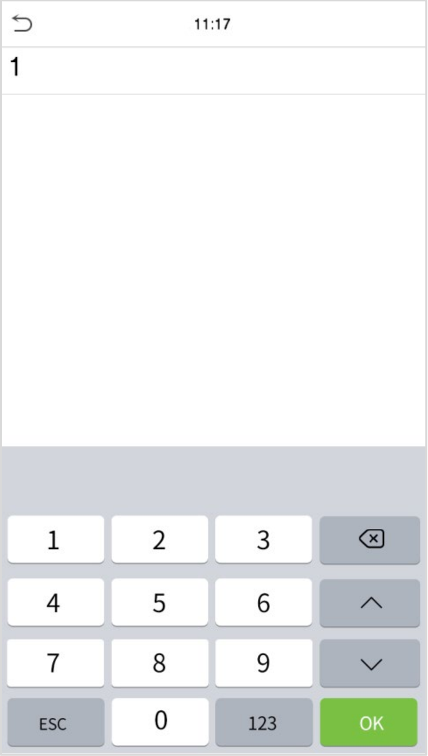
Successfully verified.
Name : ANDHIKA PRATAMA
User ID : 1
Verify : Card

Note: The record of 1: 1 Card Verification mode will be recorded in the attendance.

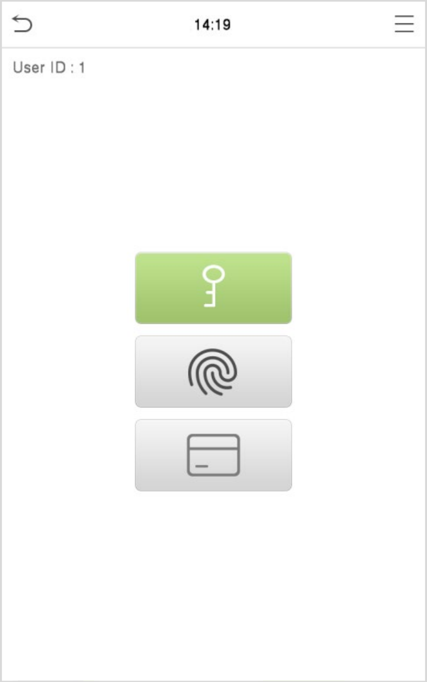
3.3 Password Verification

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

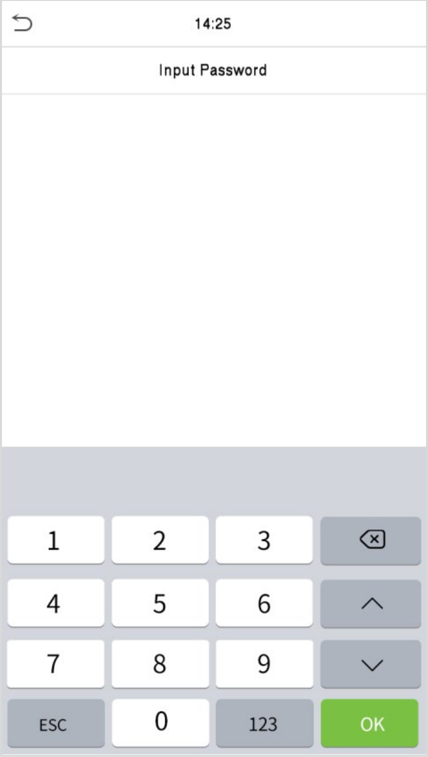
Tap the button on the main screen to enter the 1:1 password verification mode. Then, input the user ID and press [**OK**].



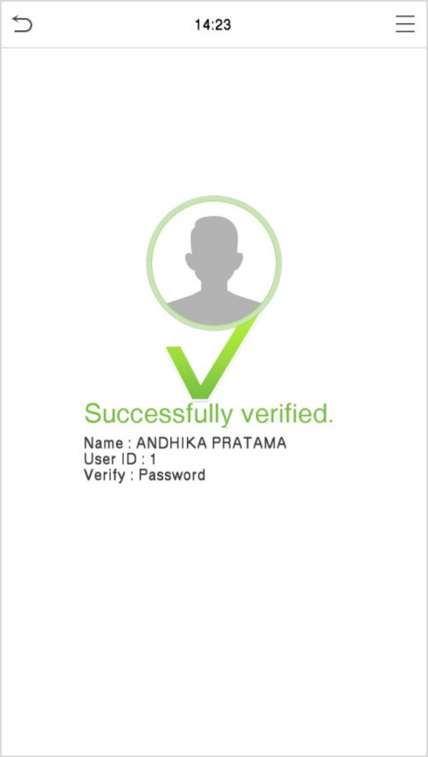
If the user has registered a fingerprint and a card in addition to his/her password and the verification method is set to Password/Fingerprint/Card verification, the following screen will appear. To enter the password verification mode, press on the 🔑 icon.



Input the password and press [**OK**].

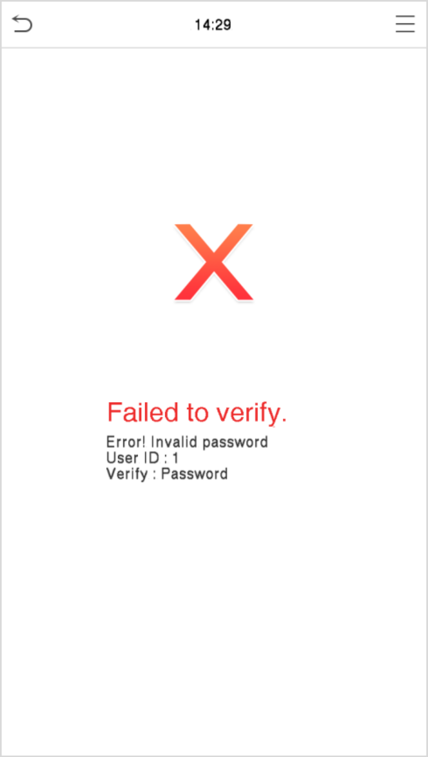


Below are the display screens after entering a correct password and a wrong password, respectively.



Successfully verified.

Name : ANDHIKA PRATAMA
User ID : 1
Verify : Password



Failed to verify.

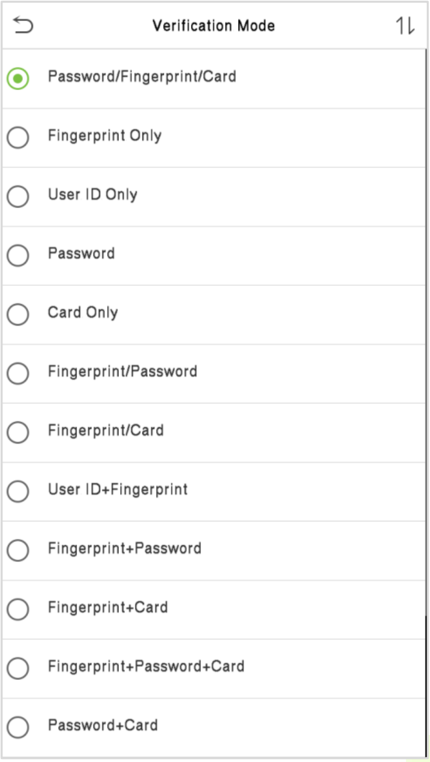
Error! Invalid password
User ID : 1
Verify : Password

3.4 Combined Verification

This device allows you to use a different types of verification methods to increase security. There are a total of 15 different verification combinations that can be implemented, as listed below:

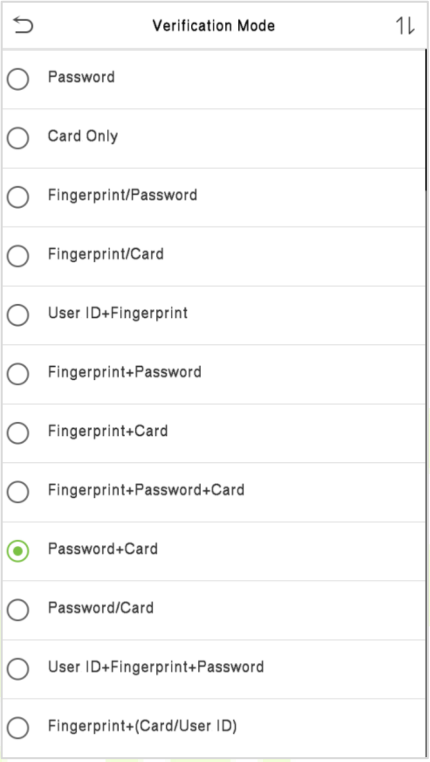
Combined Verification Symbol Definition

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/Fingerprint/Card
- ○ Fingerprint Only
- ○ User ID Only
- ○ Password
- ○ Card Only
- ○ Fingerprint/Password
- ○ Fingerprint/Card
- ○ User ID+Fingerprint
- ○ Fingerprint+Password
- ○ Fingerprint+Card
- ○ Fingerprint+Password+Card
- ○ Password+Card



Verification Mode

- ○ Password
- ○ Card Only
- ○ Fingerprint/Password
- ○ Fingerprint/Card
- ○ User ID+Fingerprint
- ○ Fingerprint+Password
- ○ Fingerprint+Card
- ○ Fingerprint+Password+Card
- ● Password+Card
- ○ Password/Card
- ○ User ID+Fingerprint+Password
- ○ Fingerprint+(Card/User ID)

Combined Verification Mode set up procedure:

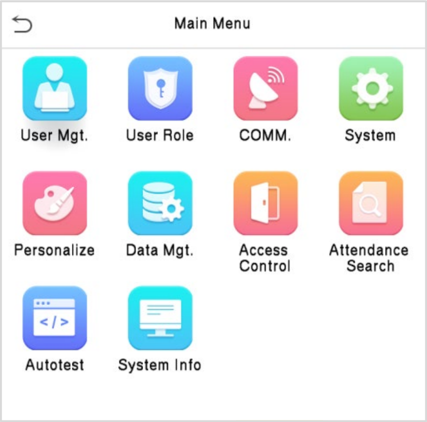
- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.
- For example, if a user just registered for their fingerprint data but the device verification mode is set to "Fingerprint + Password," users will not be able to successfully complete the verification process.

Reason:

- This is because the Device compares the person's fingerprint template to the previously stored verification template (both the Fingerprint and the Password) for that Personnel ID in the Device.
- But, since the user has just registered their fingerprint and not a password, the verification process will not be successful, and the device will show "Verification Failed."

4 Main Menu

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

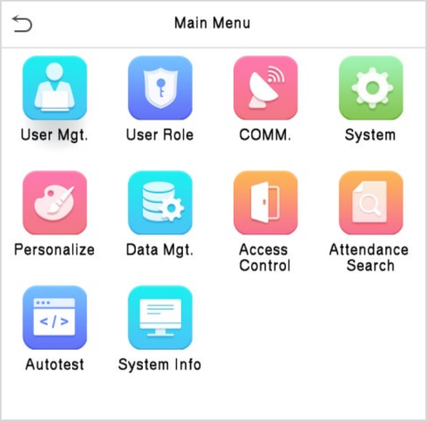


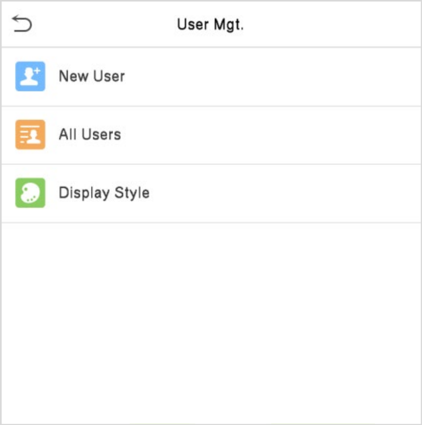
Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User.
User Role	To set the permission, scope of the custom role and enroller for the users, for example the system's operating rights..
COMM.	To set the relevant parameters of Network, PC Connection, Cloud Server Setting and Network Diagnosis.
System	To set parameters related to the system, including Date Time, Identity Verification, Fingerprint, Identity Verification Info options, Key Programming, Security and Reset.
Personalize	To customize settings of User Interface and Voice.
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, check Attendance Record, Identity Verification Record and Upload Serial Port Data.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Fingerprint Sensor, and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

5 User Management

5.1 New User Registration

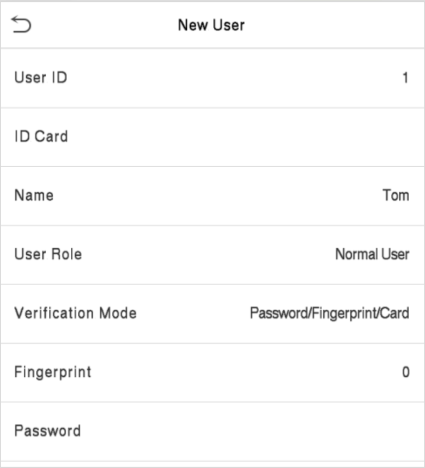
Tap **User Mgt.** on the main menu.





5.1.1 Register a User ID and Name

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



New User

User ID	1
ID Card	
Name	Tom
User Role	Normal User
Verification Mode	Password/Fingerprint/Card
Fingerprint	0
Password	

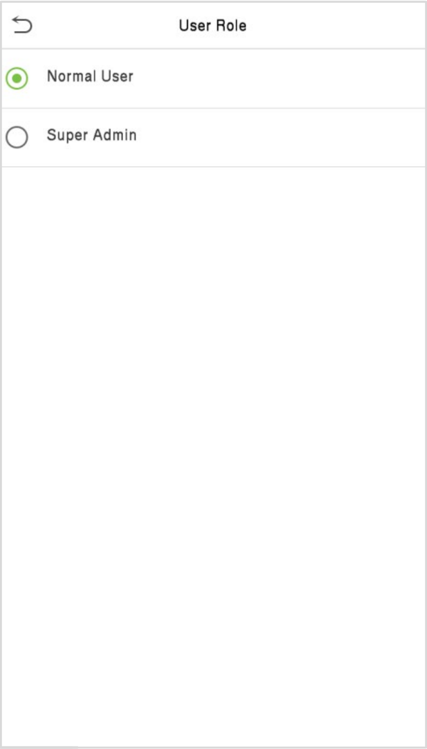
Note:

- A name can have up to 34 characters.
- By default, the user ID can have 1 to 9 digits.
- During the initial registration, you can modify your ID, but not after the registration.
- If the message "**Duplicated!**" appears, you must choose a different User ID because the one you entered already exists.

5.1.2 User Role

On the **New User** interface, tap on **User Role** to set the user's role 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.



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.

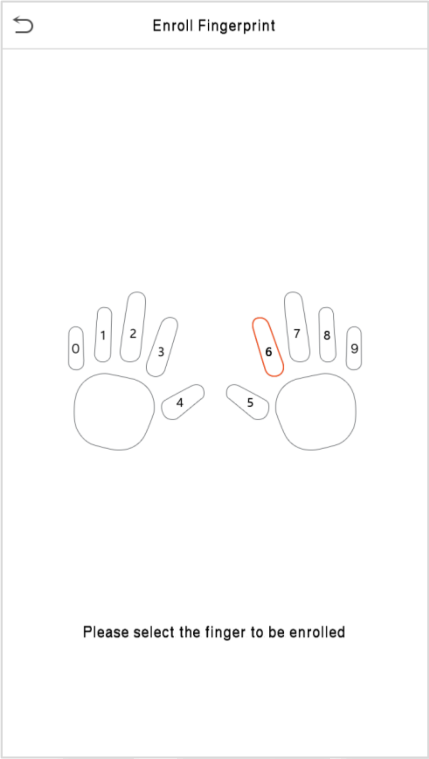
5.1.3 Verification Mode

On the **New User** interface, tap on **Verification Mode** to set mode of user verification, there are 15 types of verification mode to choose, please refer to 3.4 Combined Verification.

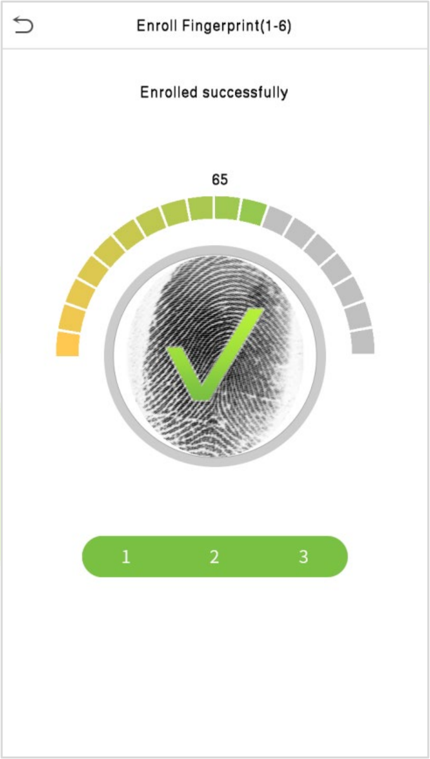
5.1.4 Fingerprint

Tap **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

- Click **Fingerprint** to enter the fingerprint registration page. Select the finger to be enrolled.
- Press the same finger on the fingerprint reader three times. Green indicates that the fingerprint was successfully enrolled.



Please select the finger to be enrolled

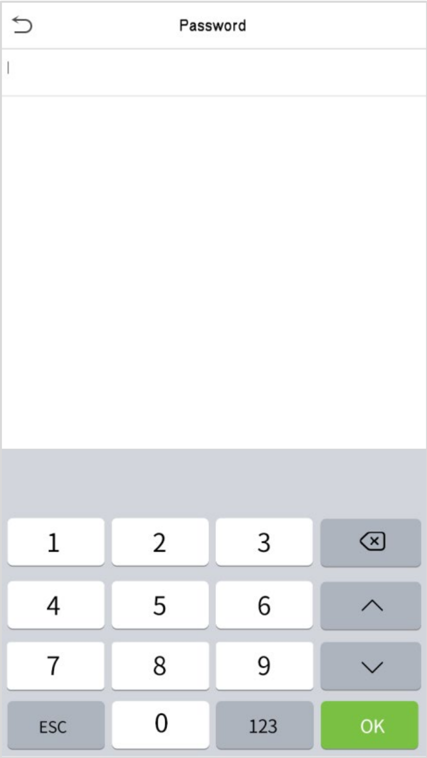


Enrolled successfully

5.1.5 Password

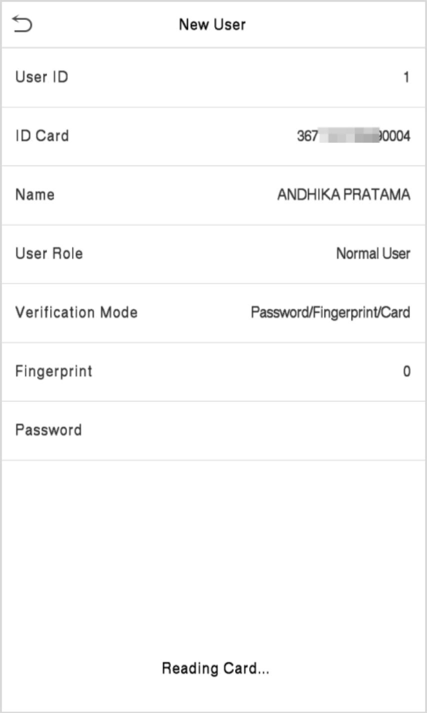
Tap **Password** in the **New User** interface to enter the password registration page.

- 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 first entered password, then the device prompts the message as "**Password does not match**!", where the user needs to re-confirm the password again.
- By default, the password can have 6 to 8 digits.



5.1.6 ID Card

In the interface of **New User**, place the ID card on the card induction area of the device, the device will read the ID card information and automatically fill in the **ID Card Number** and **Name** of the user.


New User

User ID 1

ID Card 367[redacted]0004

Name ANDHIKA PRATAMA

User Role Normal User

Verification Mode Password/Fingerprint/Card

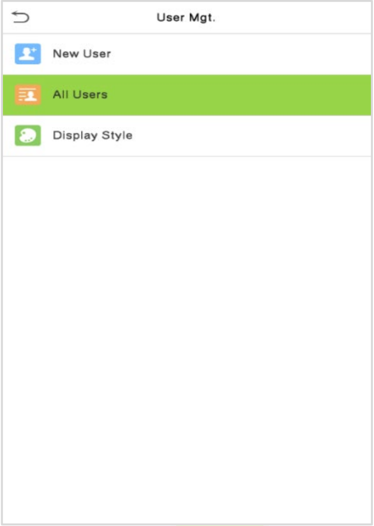
Fingerprint 0

Password

Reading Card...

5.2 All User

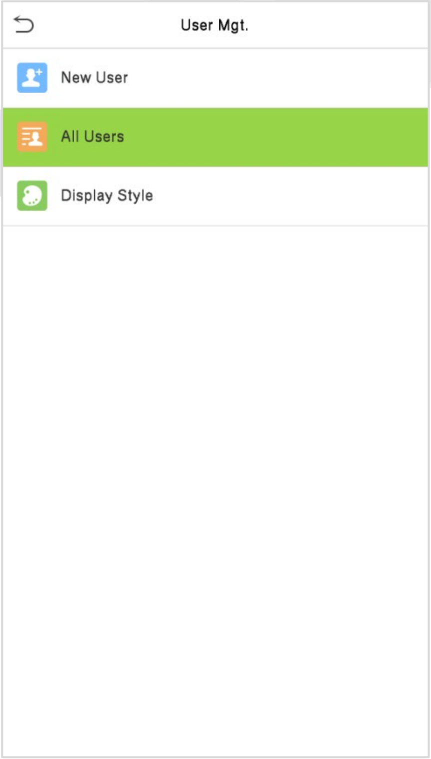
On the **Main Menu**, tap **User Mgt.**, and then tap **All Users.**

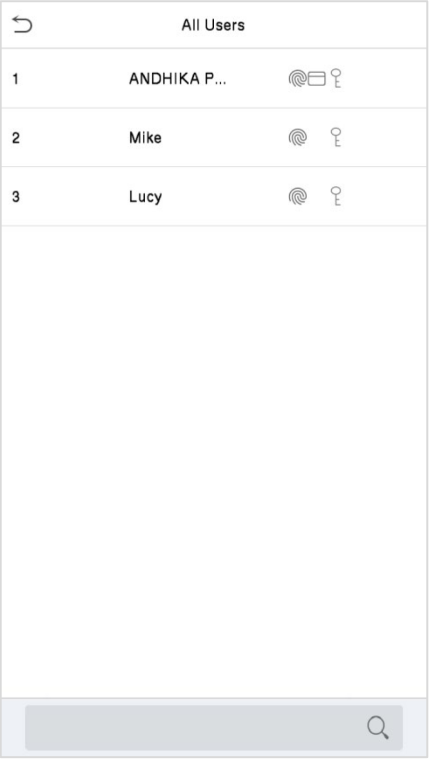


5.2.1 Search User

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.

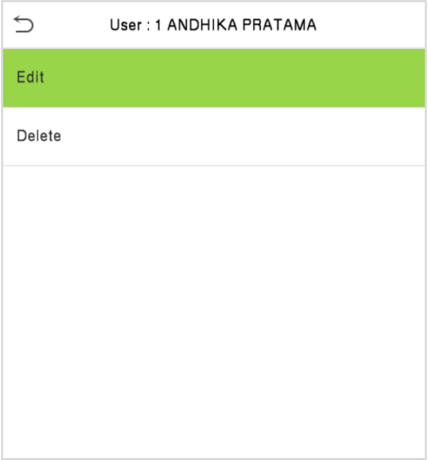




1	ANDHIKA P...
2	Mike
3	Lucy

5.2.2 Edit User

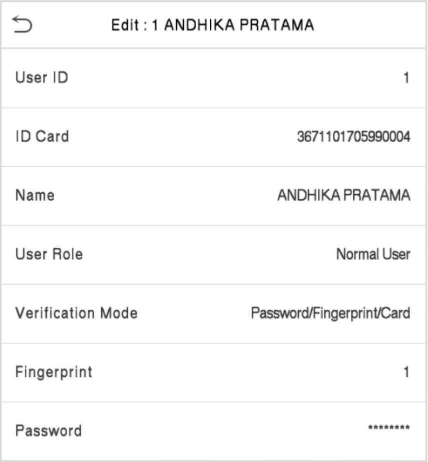
On the **All Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.



User : 1 ANDHIKA PRATAMA

Edit

Delete



Edit : 1 ANDHIKA PRATAMA

User ID	1
ID Card	3671101705990004
Name	ANDHIKA PRATAMA
User Role	Normal User
Verification Mode	Password/Fingerprint/Card
Fingerprint	1
Password	********

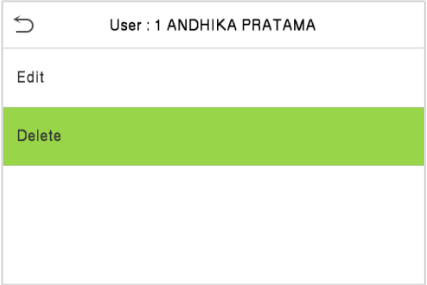
Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to 5.1 User Registration.

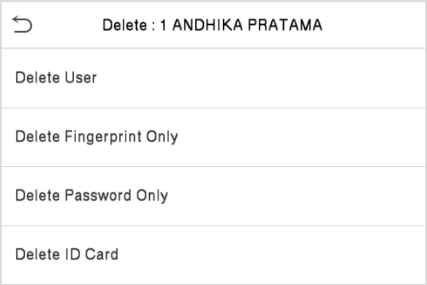
5.2.3 Delete User

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

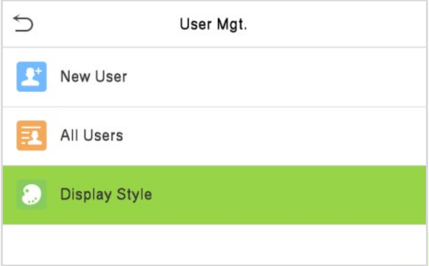
- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete ID Card:**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

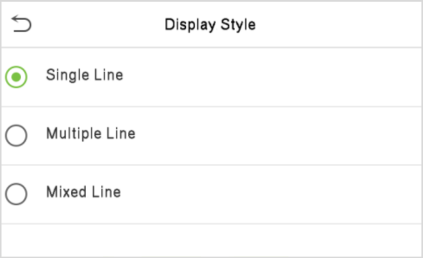




5.3 Display Style

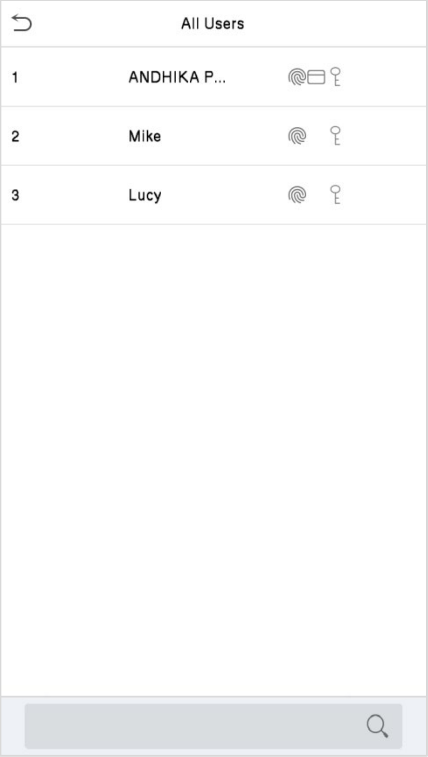
On the **Main Menu**, tap **User Mgt.**, and then tap **Display Style** to select Display Style setting interface.



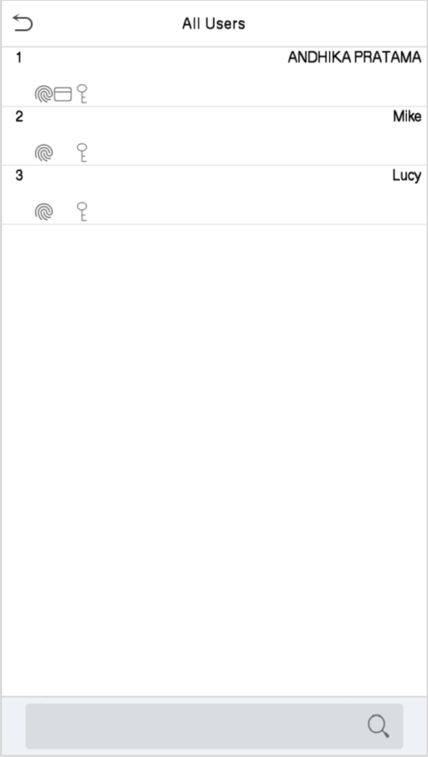


All the Display Styles are shown as below:

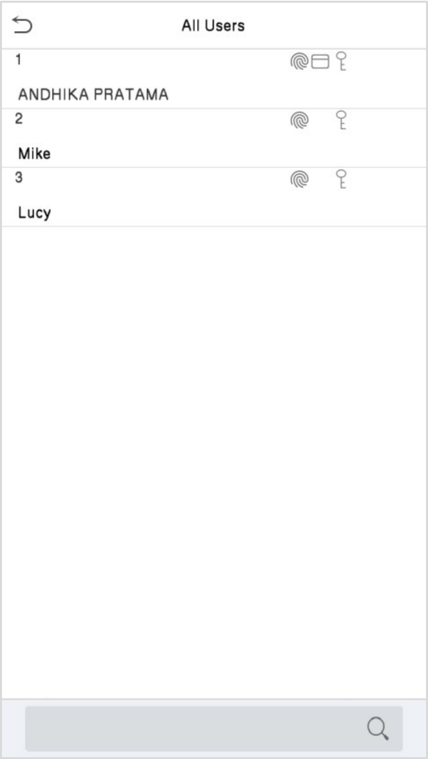
Single Line:



Multiple Line:



Mixed Line:



All Users

1
ANDHIKA PRATAMA

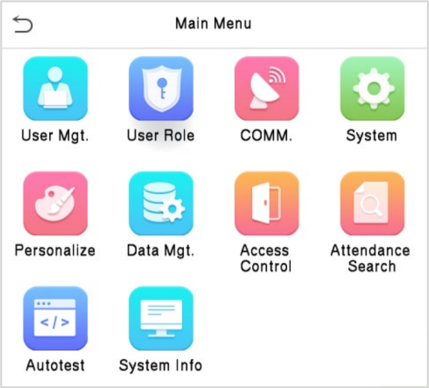
2
Mike

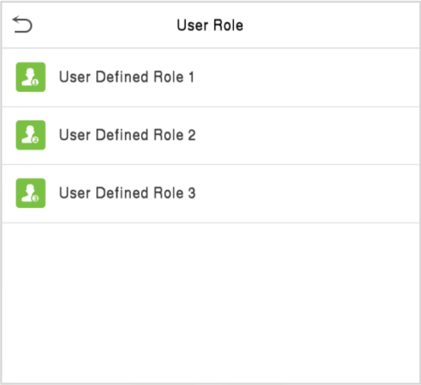
3
Lucy

6 User Role

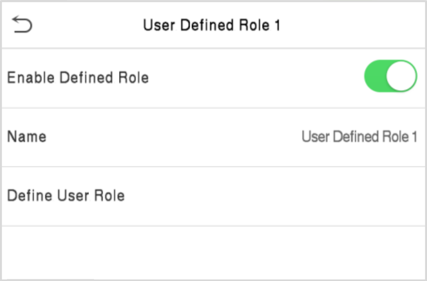
User Role allows you to assign specific permissions to certain users based on their requirements.

- 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.





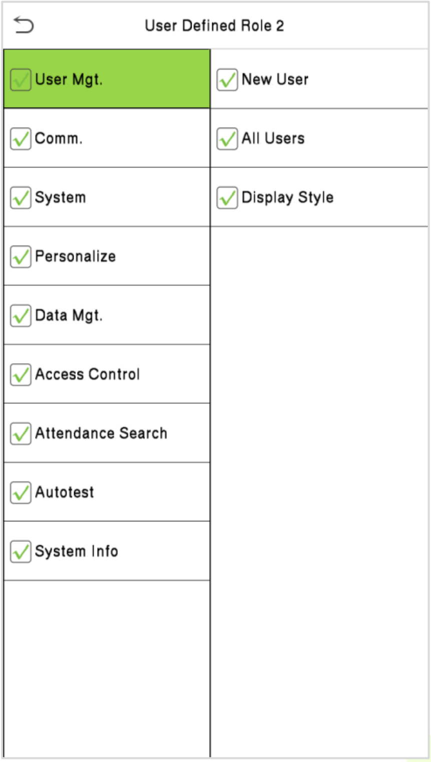
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



Enable Defined Role ●

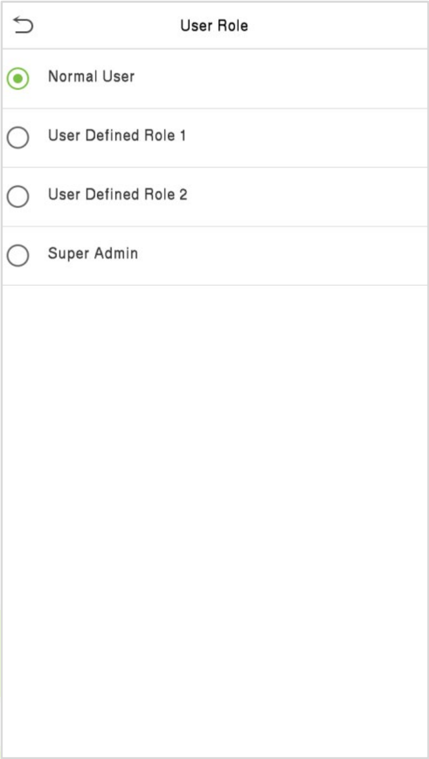
Name User Defined Role 1

- Then, by selecting on Define User Role, select the required privileges for the new role, and then press the Return button.
- When assigning privileges, the main menu's 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.



User Defined Role 2

☑ User Mgt.	☑ New User
☑ Comm.	☑ All Users
☑ System	☑ Display Style
☑ Personalize	
☑ Data Mgt.	
☑ Access Control	
☑ Attendance Search	
☑ Autotest	
☑ System Info	



User Role

● Normal User

○ User Defined Role 1

○ User Defined Role 2

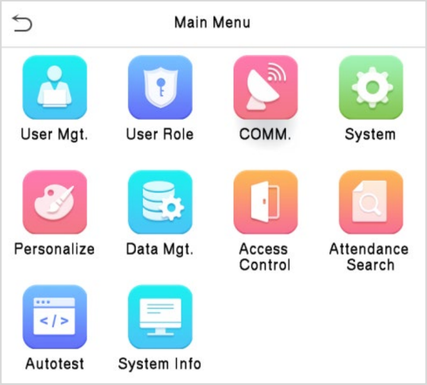
○ Super Admin

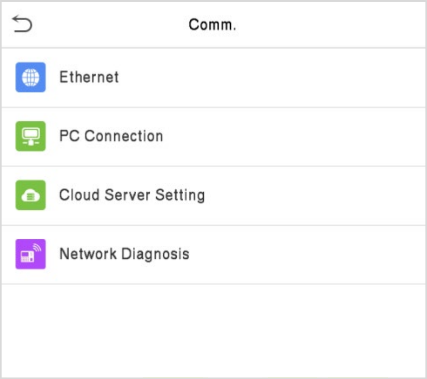
Note: If the User Role is enabled for the Device, tap on **User Mgt.** > **New User** > **User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the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

7 Communication

To set the relevant parameters of Network, PC Connection, Cloud Server Setting and Network Diagnosis.

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

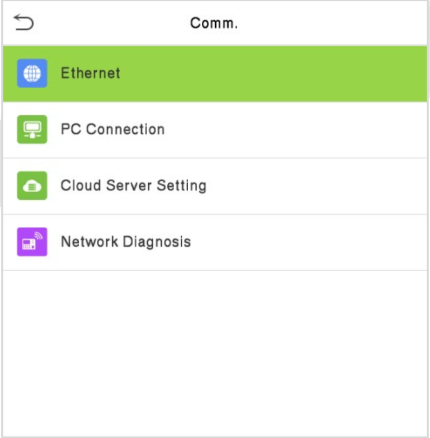


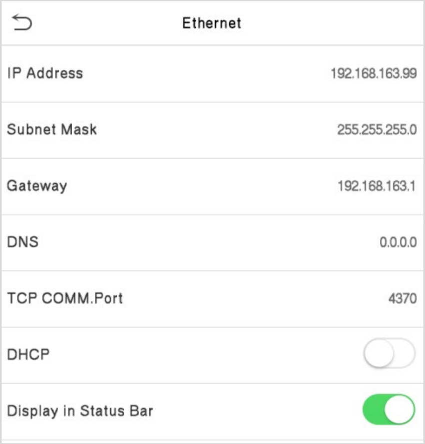


7.1 Ethernet

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and make sure that the device and the PC connect to the same network segment.

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





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

DHCP ○

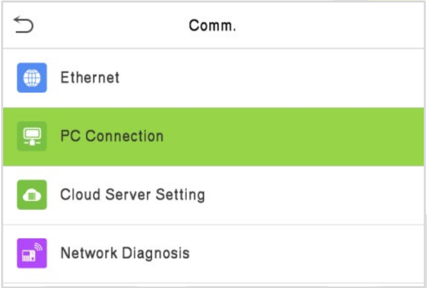
Display in Status Bar ●

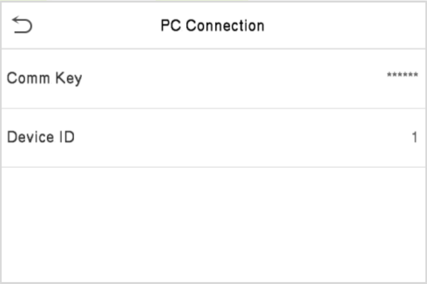
Function Name	Description
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.

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.
DHCP	Dynamic Host Configuration Protocol dynamically allocates IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

7.2 PC Connection

Comm Key helps 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.





Comm Key ******

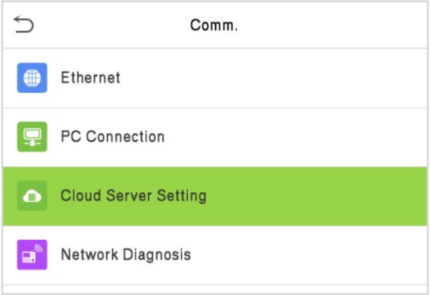
Device ID 1

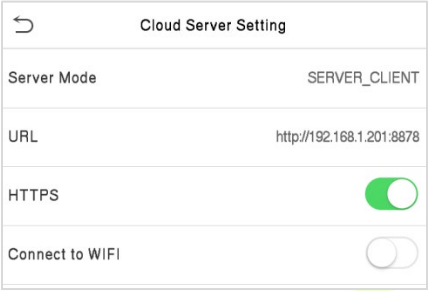
Tap **PC Connection** on the **Comm.** Settings interface to configure the communication settings.

Function Name	Description
Comm Key	The default password is 0 and can be changed. The Comm Key can contain 1 to 6 digits.
Device ID	It is the identification 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.

7.3 Cloud Server Setting

Tap **Cloud Server Setting** on the **Comm.** Settings interface to connect with the SERVER_CLIENT or SERVER_ZK server.




Cloud Server Setting

Server Mode SERVER_CLIENT

URL http://192.168.1.201:8878

HTTPS ●

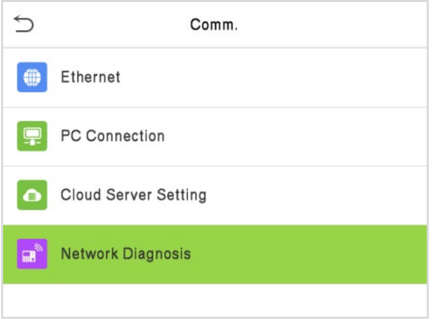
Connect to WIFI ○

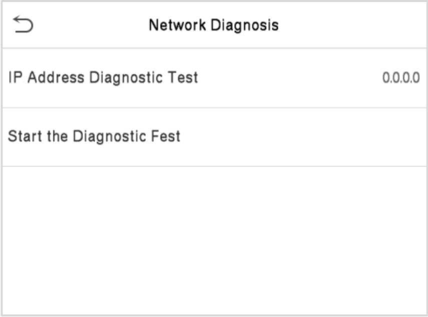
Function Name	Description
Server Mode	Select the type of server, SERVER_CLIENT or SERVER_ZK?
URL	Enter the IP address of the selected server.
HTTPS	Based on HTTP, transmission encryption and identity authentication, make sure that the security of the transmission process.
Connect to WIFI	Connecting to the server.

7.4 Network Diagnosis

To set the network diagnosis parameters.

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




Network Diagnosis

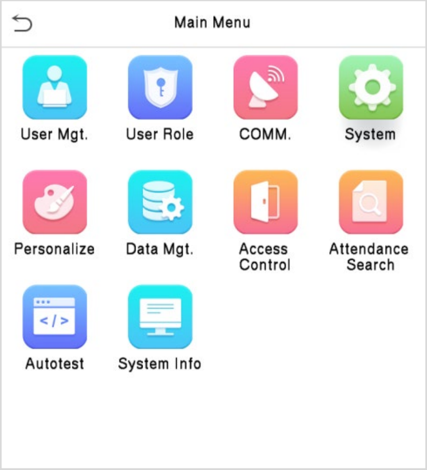
IP Address Diagnostic Test 0.0.0.0

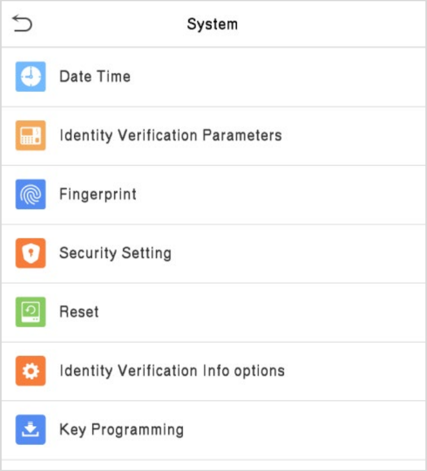
Start the Diagnostic Fest

8 System

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

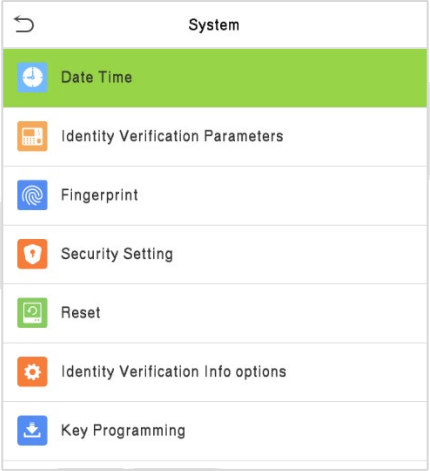
Tap **System** on the **Main Menu** interface to get into its menu options.

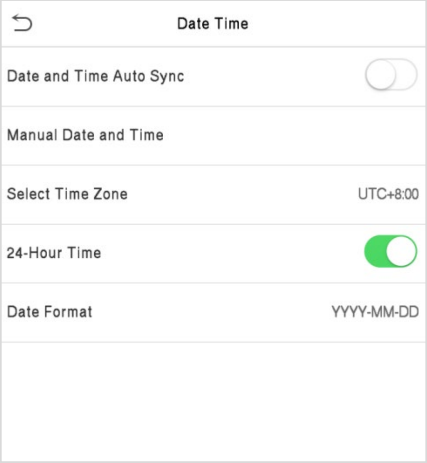



System
Date Time
Identity Verification Parameters
Fingerprint
Security Setting
Reset
Identity Verification Info options
Key Programming

8.1 Date and Time

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


System
Date Time
Identity Verification Parameters
Fingerprint
Security Setting
Reset
Identity Verification Info options
Key Programming


Date Time

Date and Time Auto Sync

Manual Date and Time

Select Time Zone UTC+8:00

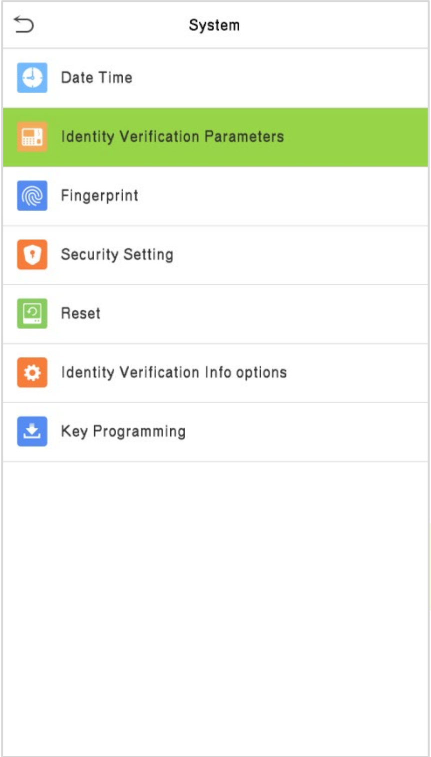
24-Hour Time

Date Format YYYY-MM-DD

- 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.

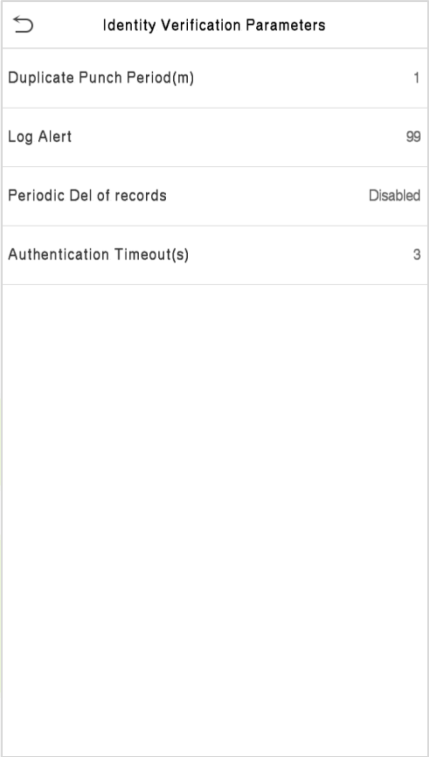
8.2 Identity Verification Parameters

Tap **Identity Verification Parameters** on the **System** interface to set the identity verification parameter.



System

- Date Time
- Identity Verification Parameters
- Fingerprint
- Security Setting
- Reset
- Identity Verification Info options
- Key Programming



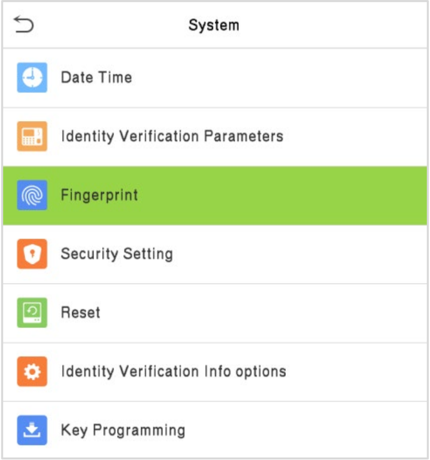
Identity Verification Parameters

Duplicate Punch Period(m)	1
Log Alert	99
Periodic Del of records	Disabled
Authentication Timeout(s)	3

Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Log Alert	When the record space of the attendance 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 records	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value:1 to 9 seconds.

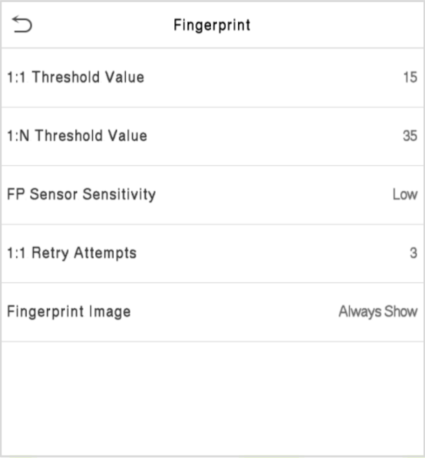
8.3 Fingerprint

Tap **Fingerprint** on the **System** interface to set the Fingerprint.



System

- Date Time
- Identity Verification Parameters
- Fingerprint
- Security Setting
- Reset
- Identity Verification Info options
- Key Programming



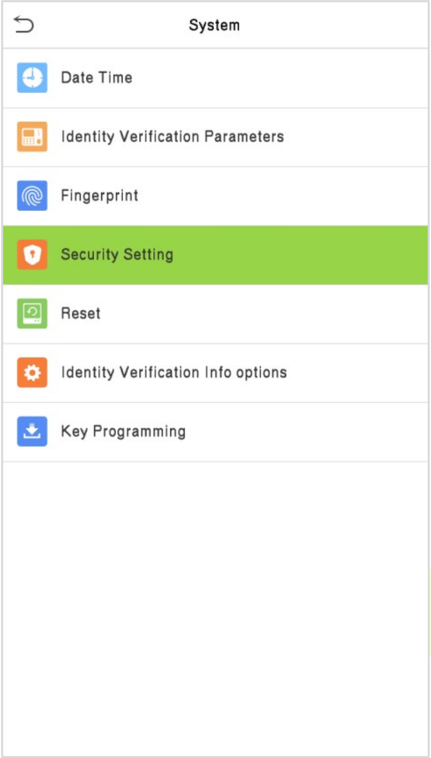
Fingerprint

1:1 Threshold Value	15
1:N Threshold Value	35
FP Sensor Sensitivity	Low
1:1 Retry Attempts	3
Fingerprint Image	Always Show

Function Name	Description
1:1 Threshold Value	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold Value	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Attempts	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: **Show for Enroll:** To display the fingerprint image on the screen only during enrollment. **Show for Match:** To display the fingerprint image on the screen only during verification. **Always Show:** To display the fingerprint image on screen during enrollment and verification. **None:** Not to display the fingerprint image.

8.4 Security Setting

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



System

Date Time

Identity Verification Parameters

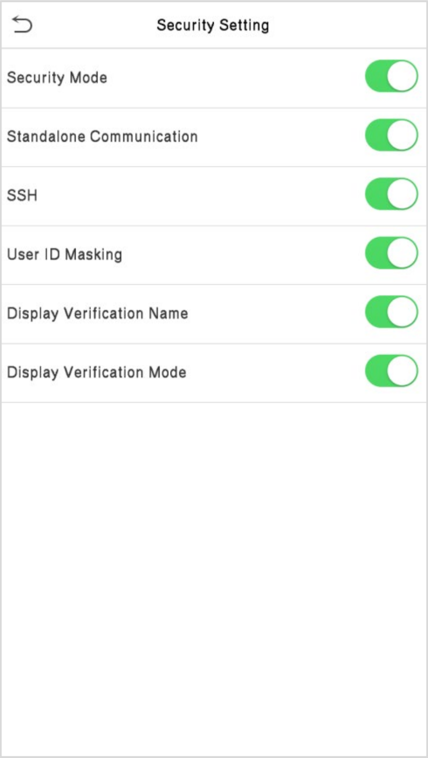
Fingerprint

Security Setting

Reset

Identity Verification Info options

Key Programming



Security Setting

Security Mode

Standalone Communication

SSH

User ID Masking

Display Verification Name

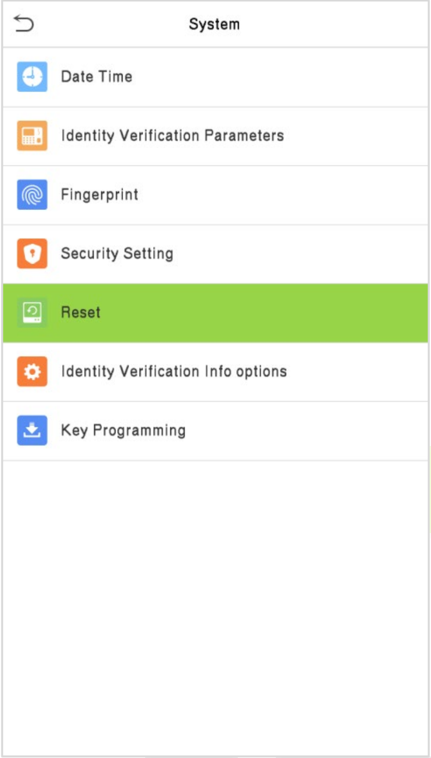
Display Verification Mode

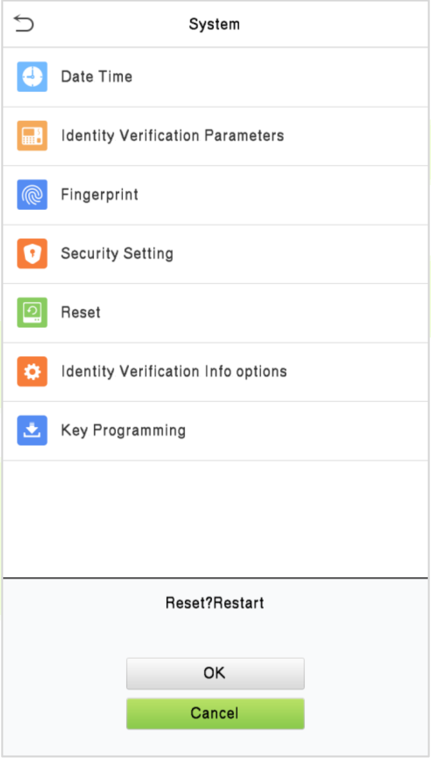
Function Name	Description
Security Mode	Select whether to enable the security mode to protect the device and the user's personal information. You can set the device to work offline and hide the user's personal information to prevent leakage during user verification.
Standalone Communication	To avoid 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.

8.5 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.

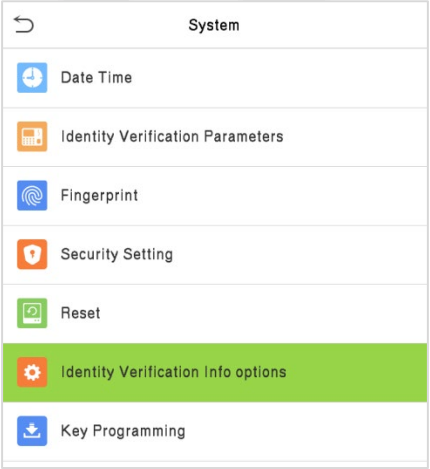

System
Date Time
Identity Verification Parameters
Fingerprint
Security Setting
Reset
Identity Verification Info options
Key Programming



Reset?Restart

8.6 Identity Verification Info Options

Tap **Identity Verification Info Options** on the **System** interface to select the content displayed during identity verification as needed.


System
Date Time
Identity Verification Parameters
Fingerprint
Security Setting
Reset
Identity Verification Info options
Key Programming

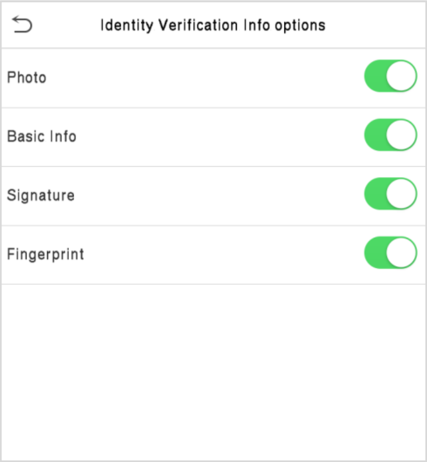
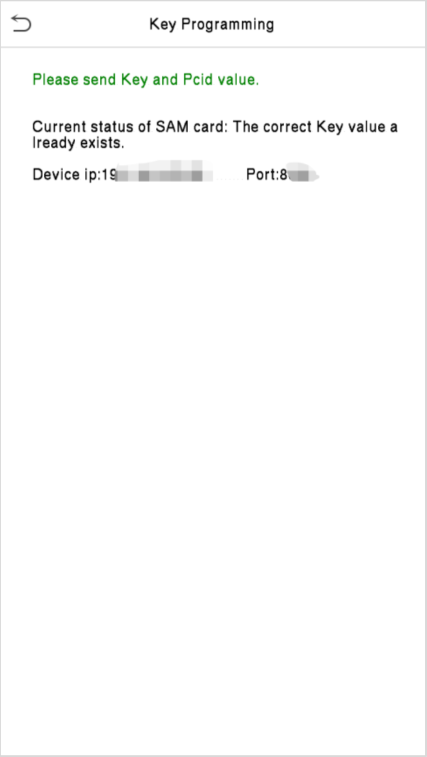


Photo ●
Basic Info ●
Signature ●
Fingerprint ●

8.7 Key Programming

It is a protection device for the device to prevent being dismantled and tampering with the device and data. It is forbidden to dismantle or damage the device, otherwise the ID card information cannot be read normally. The device is factory configured with Key value, if have any problem, please contact our after-sales staff.

Tap **Key Programming** on the **System** interface.



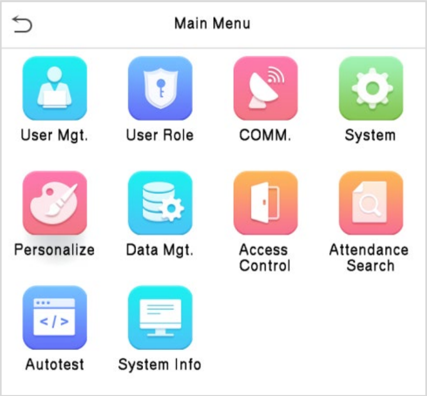
Please send Key and Pcid value.

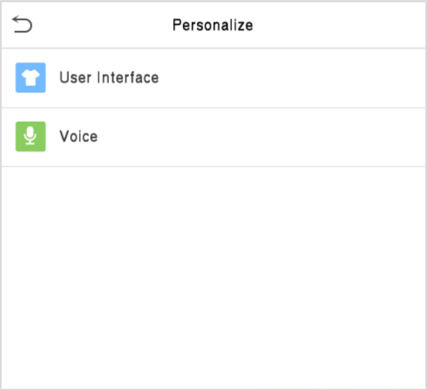
Current status of SAM card: The correct Key value a lready exists.

Device ip:19[redacted] Port:8[redacted]

9 Personalize

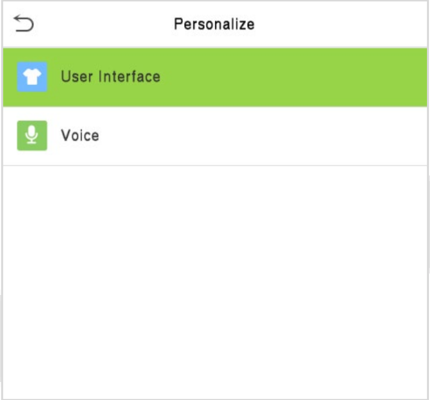
Tap **Personalize** the **Main Menu** interface to customize interface settings and voice.

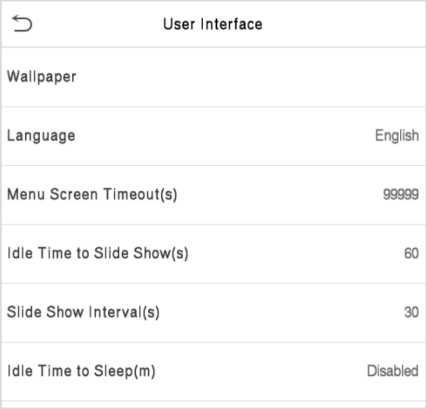




9.1 User Interface

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





Wallpaper

Language English

Menu Screen Timeout(s) 99999

Idle Time to Slide Show(s) 60

Slide Show Interval(s) 30

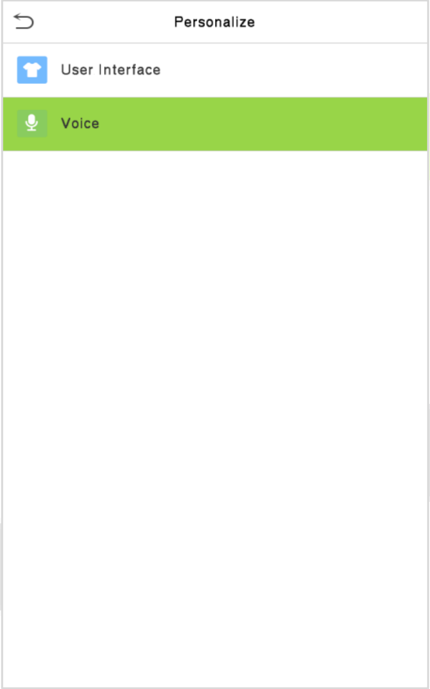
Idle Time to Sleep(m) Disabled

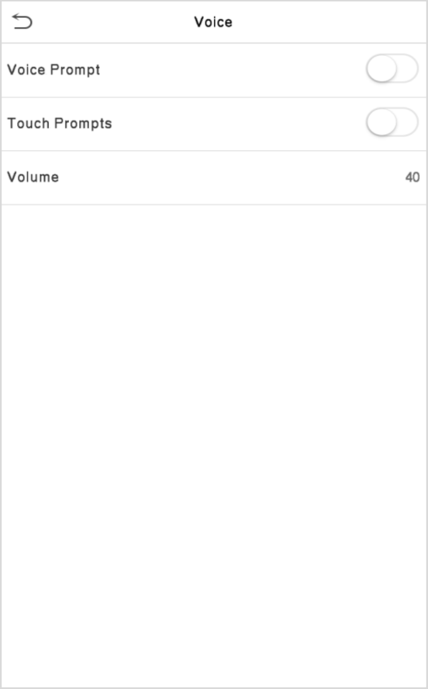
Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface. The function can either be disabled or set the required value between 60 and 99999 seconds.

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)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1-999 minutes.

9.2 Voice

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




Voice

Voice Prompt ○

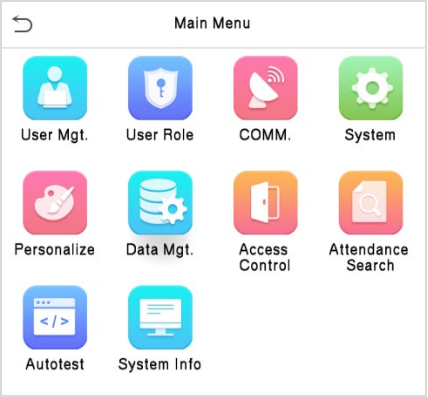
Touch Prompts ○

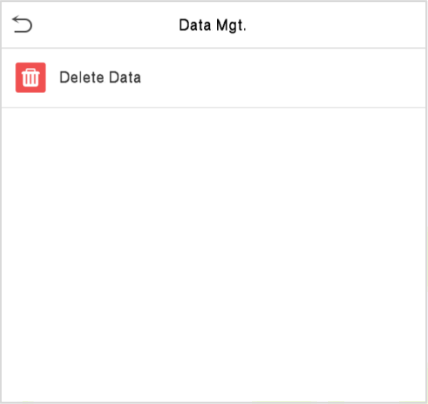
Volume 40

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 to100.

10 Data Management

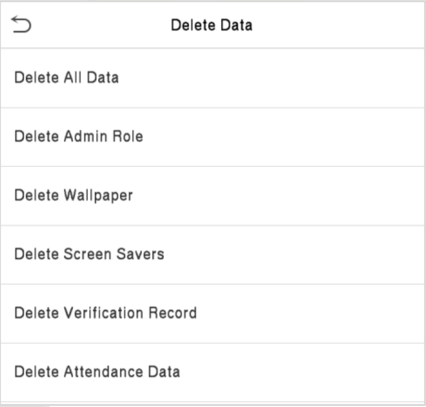
On the **Main Menu**, tap **Data Mgt.** to delete the relevant data in the device.





10.1 Delete Data

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

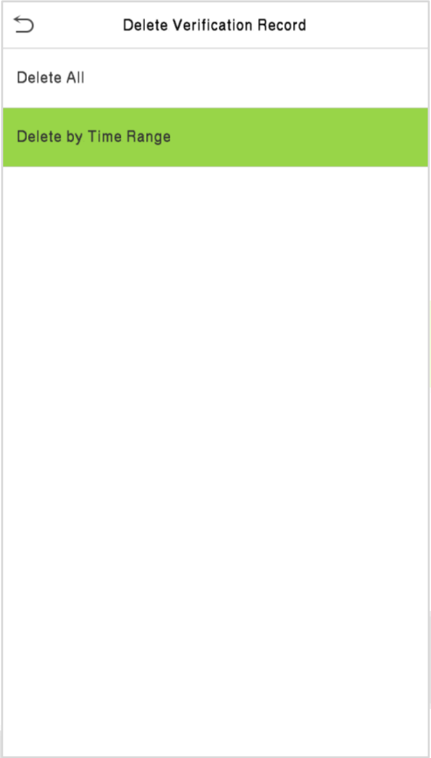


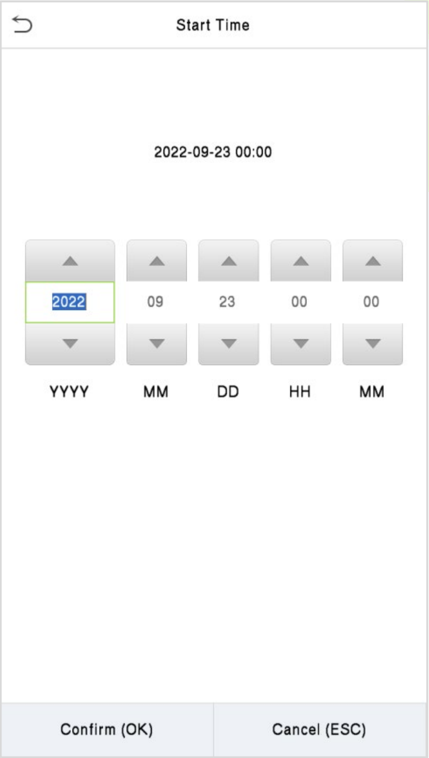
Function Name	Description
Delete All Data	To delete the information and attendance data of all registered users.
Delete Admin Role	To remove all the administrator privileges.
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete all the screen savers in the device.
Delete Verification Record	To delete all the verification record in the device.

Delete Attendance Data	To delete all the attendance data in the device.

Delete Verification Record:

The user may select **Delete All** or **Delete by Time Range** when deleting the verification record and attendance data. Selecting **Delete by Time Range**, you need to set a specific time range to delete all data within a specific period.



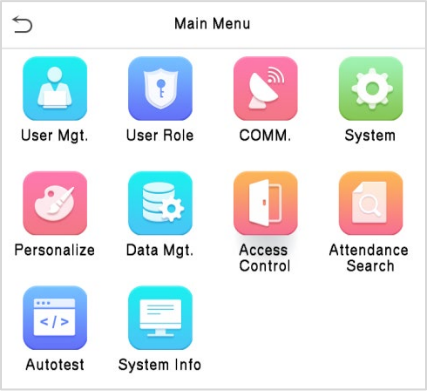


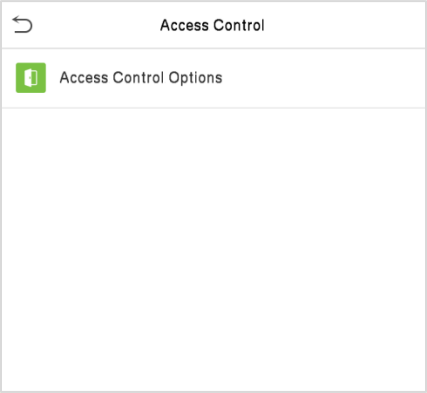
2022-09-23 00:00

YYYY	MM	DD	HH	MM
2022	09	23	00	00

11 Access Control

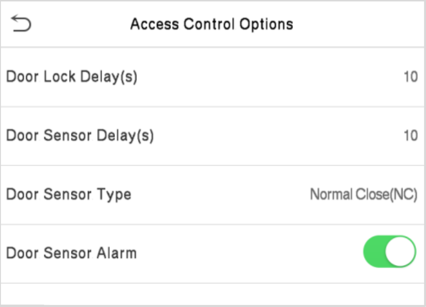
On the **Main Menu**, tap **Access Control** to set the parameters of the lock and the relevant access control device.





11.1 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.


Access Control Options

Door Lock Delay(s) 10

Door Sensor Delay(s) 10

Door Sensor Type Normal Close(NC)

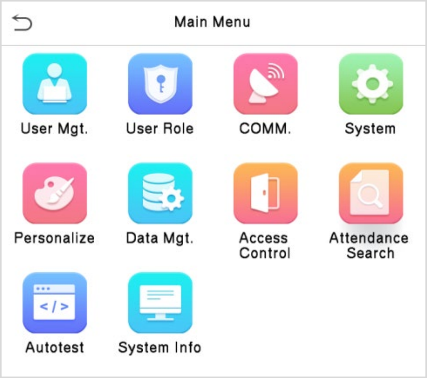
Door Sensor Alarm ●

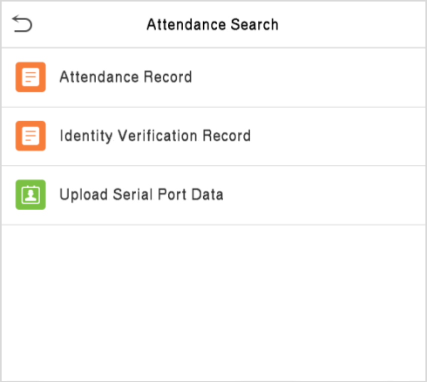
Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1to 10 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The 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 Closed. **Normally Open(NO):** It means the door is always left open when electric power is on. **Normally Closed(NC):** It means the door is always left closed when electric power is on. **None:** It means the door sensor is not in use.
Door Sensor 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.

12 Attendance Search

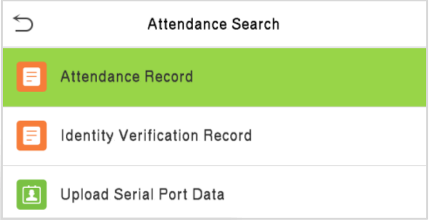
Once the identity of a user is verified, the attendance and identity verification record is saved in the device. This function enables users to check their event logs.

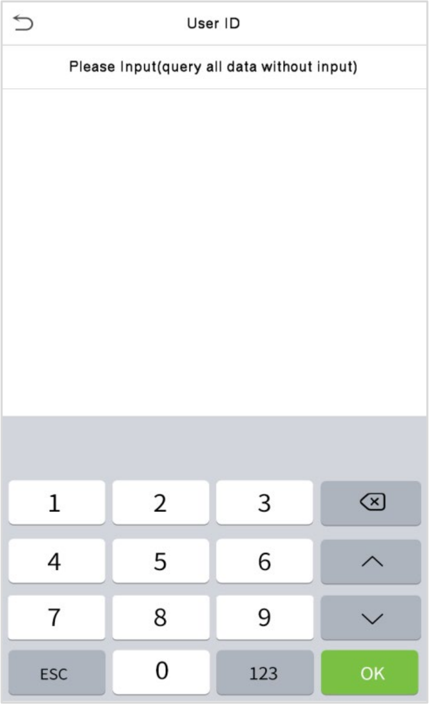




12.1 Attendance Record

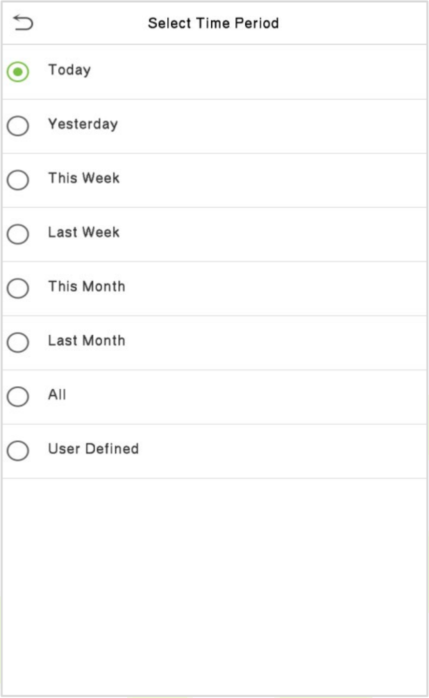
Select **Attendance Record** on the **Attendance Record** interface to search for the required attendance logs.





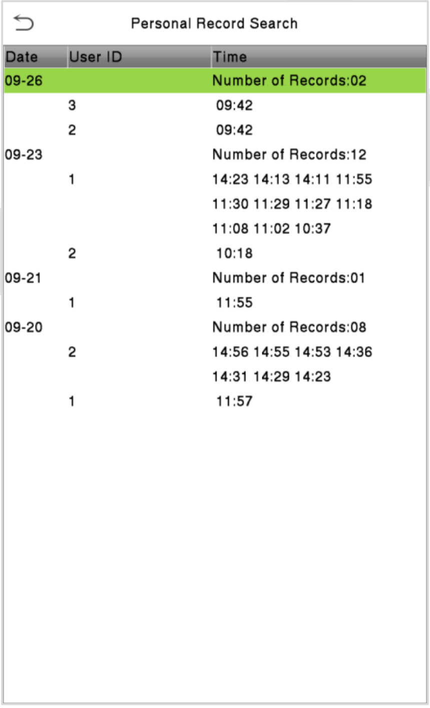
Please Input(query all data without input)

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.


Select Time Period

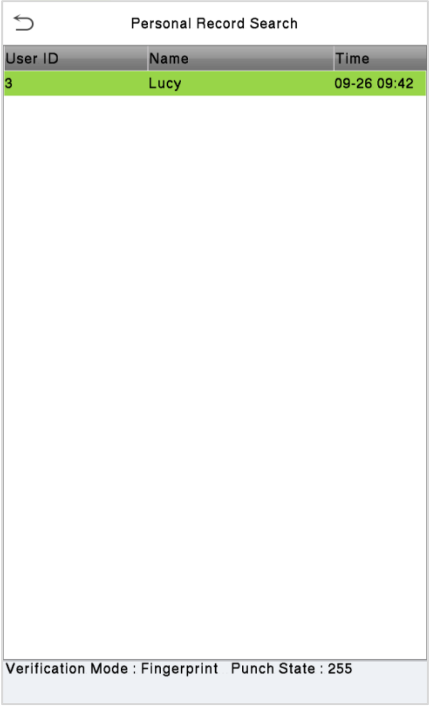
- ● Today
- ○ Yesterday
- ○ This Week
- ○ Last Week
- ○ This Month
- ○ Last Month
- ○ All
- ○ User Defined

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


Personal Record Search

Date	User ID	Time
09-26		Number of Records:02
	3	09:42
	2	09:42
09-23		Number of Records:12
	1	14:23 14:13 14:11 11:55 11:30 11:29 11:27 11:18 11:08 11:02 10:37
	2	10:18
09-21		Number of Records:01
	1	11:55
09-20		Number of Records:08
	2	14:56 14:55 14:53 14:36 14:31 14:29 14:23
	1	11:57

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


Personal Record Search

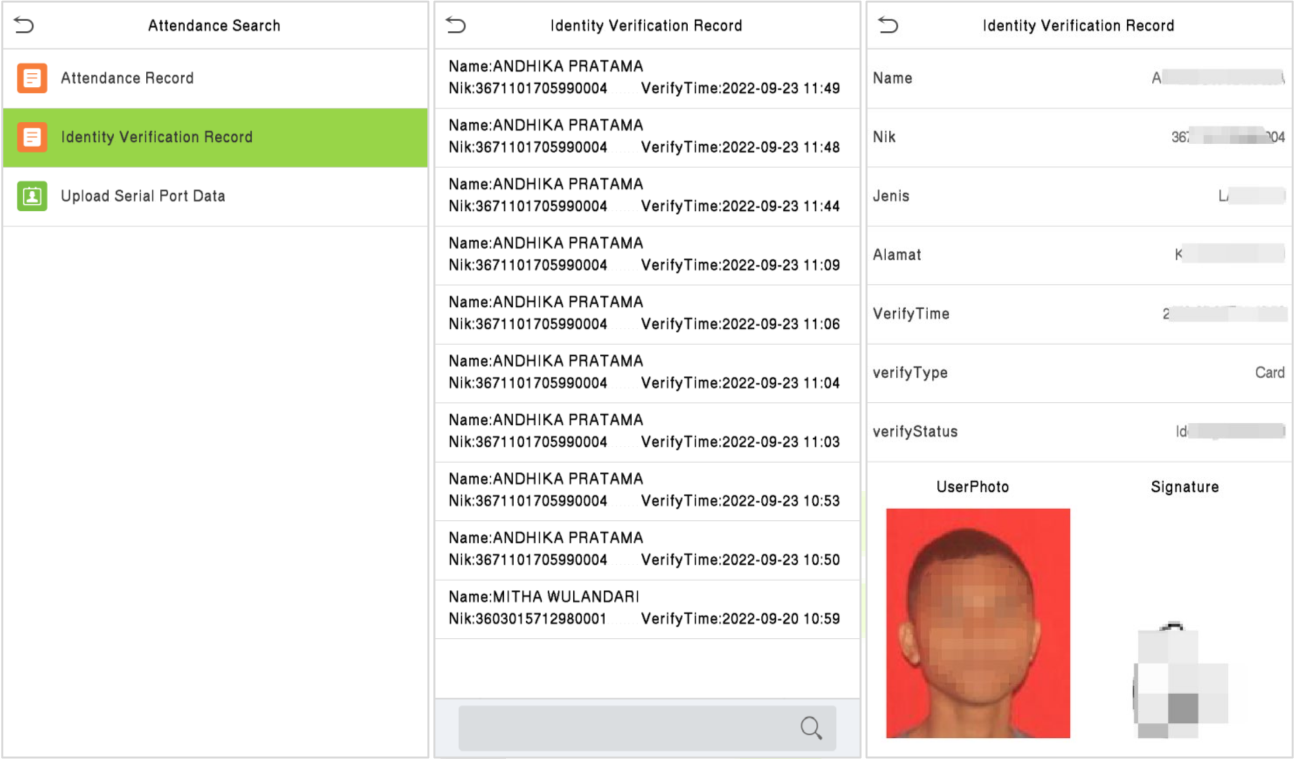
User ID	Name	Time
3	Lucy	09-26 09:42

Verification Mode : Fingerprint Punch State : 255

4. The figure shows the details of the selected record.

12.2 Identity Verification Record

Select **Identity Verification Record** on the **Attendance Record** interface to search for the required identity verification logs.



Attendance Search

- Attendance Record
- Identity Verification Record
- Upload Serial Port Data

Identity Verification Record

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:49

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:48

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:44

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:09

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:06

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:04

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 11:03

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 10:53

Name:ANDHIKA PRATAMA
Nik:3671101705990004 VerifyTime:2022-09-23 10:50

Name:MITHA WULANDARI
Nik:3603015712980001 VerifyTime:2022-09-20 10:59

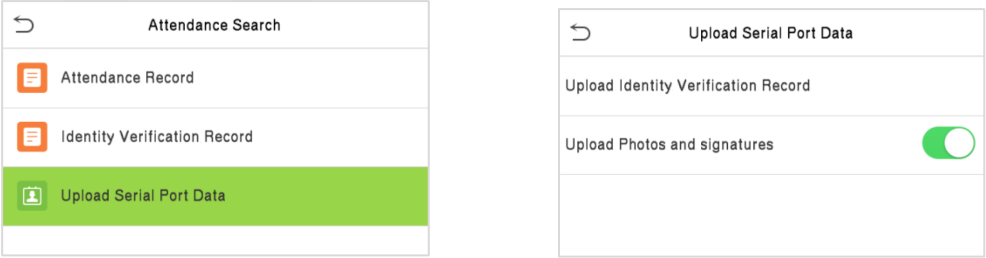
Identity Verification Record

Name	[redacted]
Nik	[redacted]
Jenis	[redacted]
Alamat	[redacted]
VerifyTime	[redacted]
verifyType	Card
verifyStatus	[redacted]

12.3 Upload Serial Port Data

The device supports uploading identity verification records to the computer via USB, while the device retains the uploaded recorded events.

Select **Upload Serial Port Data** on the **Attendance Record** interface to uploading, querying and setting up uploads for identity verification (photos and signatures)

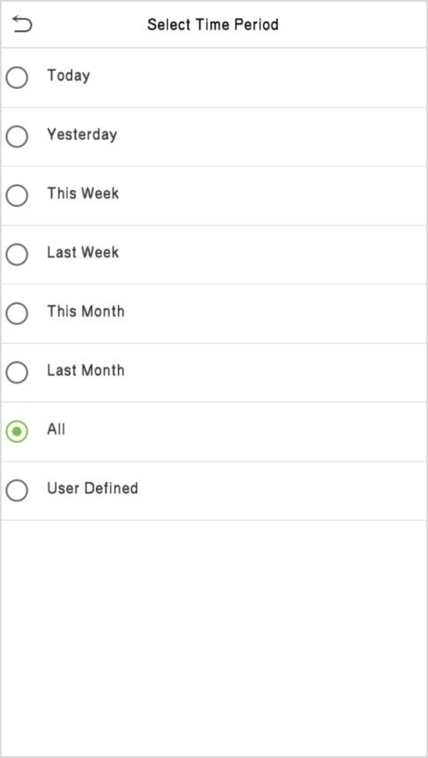


Attendance Search

- Attendance Record
- Identity Verification Record
- Upload Serial Port Data

Upload Serial Port Data

- Upload Identity Verification Record
- Upload Photos and signatures ●



Select Time Period

○ Today

○ Yesterday

○ This Week

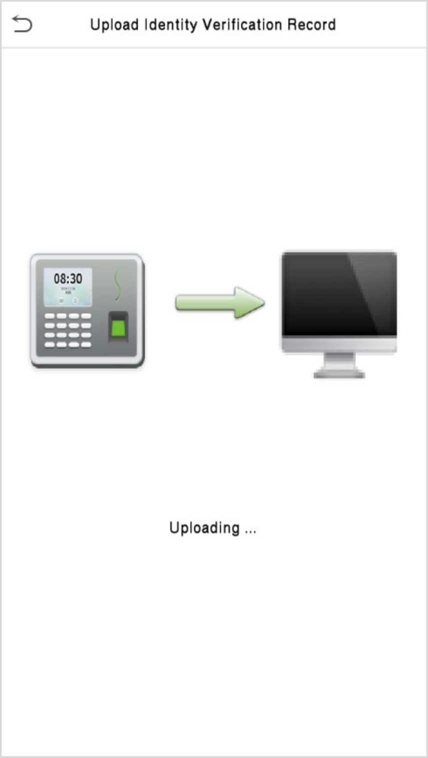
○ Last Week

○ This Month

○ Last Month

● All

○ User Defined

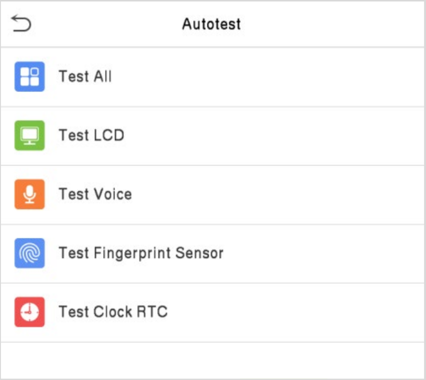


Upload Identity Verification Record

Uploading ...

13 Autotest

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


Autotest

Test All

Test LCD

Test Voice

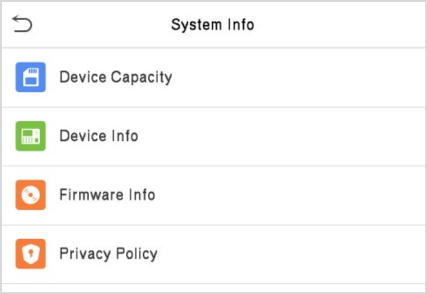
Test Fingerprint Sensor

Test Clock RTC

Function Name	Description
Test All	To automatically test whether the LCD, Voice, fingerprint sensor 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.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
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.

14 System Information

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



Function Name	Description
Device Capacity	Displays the current device's user storage, fingerprint, password, and card storage, administrators, attendance and identity verification record.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, platform information, and manufacturer and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy policy	The privacy policy control will appear when the gadget turns on for the first time. After tapping "**I have read it**," the customer can use the product regularly. Tap **System Info** -> **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. ***Note:*** The current privacy policy's text is only available in Simplified Chinese/English/Indonesia. However, translation of other multi-language content is underway, with more iterations.

Appendix 1

Privacy Policy

Notice:

To help you better use the products and services of ZKTeco (hereinafter referred as “we”, “our”, or “us”) a smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. <u>If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.</u>

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the**

Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/en/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com