USER MANUAL

2.8-inch Linux Visible Light Product

Version: 1.0

Date: June 2019

Important Statement

Thank you for choosing our product. Before using this product, please read this user manual carefully to avoid risks of danger to the users of this product or those nearby and damaging the device. Follow these instructions to ensure that your product functions properly and completes verifications in a timely manner.

Unless authorized by our company, no group or individual shall take excerpts of or copy all or part of these instructions nor transmit the contents of these instructions by any means.

The products described in this manual may include software that is copyrighted by our company and its possible licensors. No one may copy, publish, edit, take excerpts of, decompile, decode, reverse-engineer, rent, transfer, sublicense, or otherwise infringe upon the software's copyright unless authorized by the copyright holder(s). This is subject to relevant laws prohibiting such restrictions.

As this product is regularly updated, we cannot guarantee exact consistency between the actual product and the written information in this manual. Our company claims no responsibility for any disputes that arise due to differences between the actual technical parameters and the descriptions in this document. The manual is subject to change without prior notice.

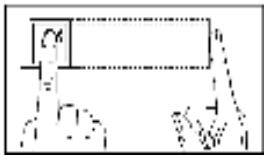
Contents

1 Notice for Use

1.1 Method of Pressing Fingerprint

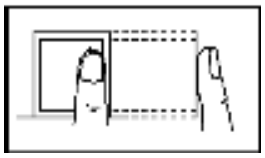
Recommended fingers: index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately press onto the fingerprint reader.

- Diagram of how to correctly press your fingers onto the fingerprint reader.

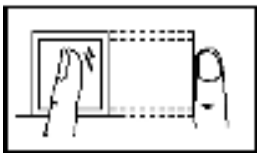


Press your finger onto the fingerprint reader.
Ensure that the center of your finger is aligned with the center of the fingerprint reader.

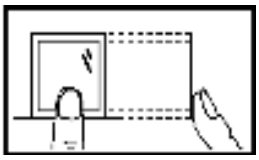
- Incorrect ways of pressing your fingers onto the fingerprint reader.



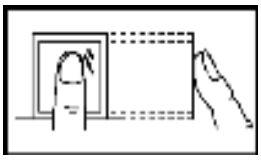
Off-center



Not the fingerprint's center



Off-center

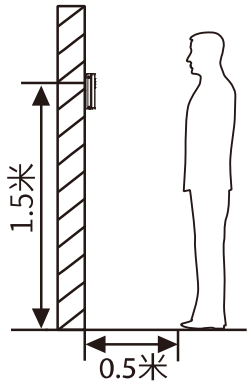


Not the fingerprint's center

Note: Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company will assume no liability for recognition issues that may result from incorrect usage of the product. We reserve the right of final interpretation and modification concerning this point.

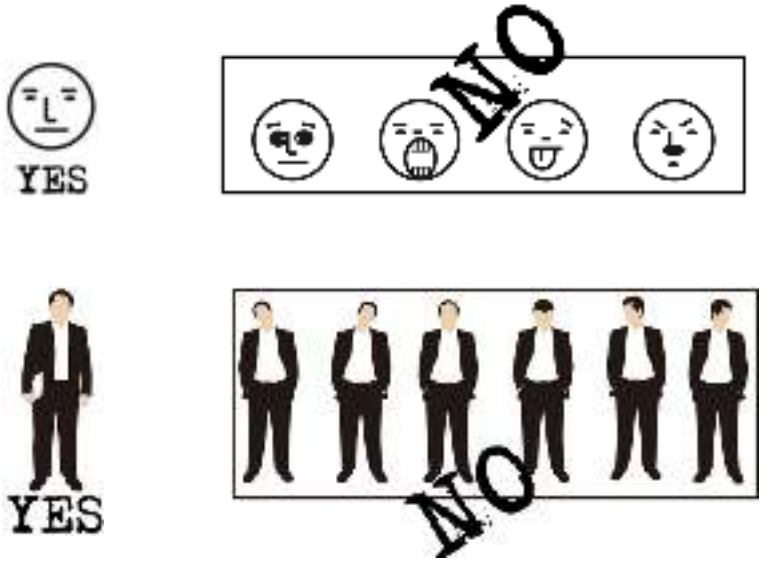
1.2 Standing Position, Facial Expression and Standing Posture

- **The recommended distance**



The distance between the device and a user whose height is within 1.55m-1.85m is recommended to be 0.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

- **Facial expression and standing posture**



Note: During enrolment and verification, please remain natural facial expression and standing posture.

1.3 Face Registration

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

1.4 Verification Mode

1.4.1 Password Verification

Compare the entered password with the registered User ID and password.

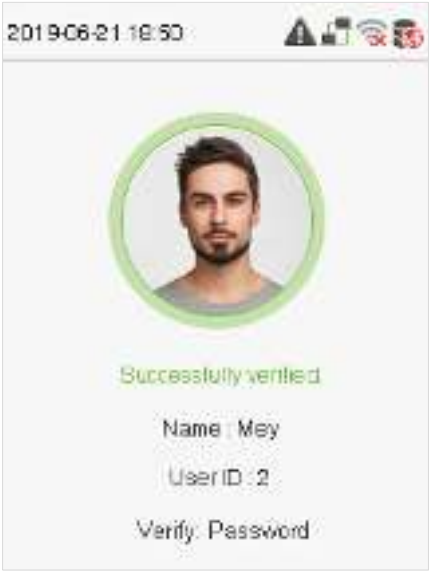
Enter the User ID on the main screen to enter the 1:1 password verification mode.

1. Enter the user ID and press **M/OK**.

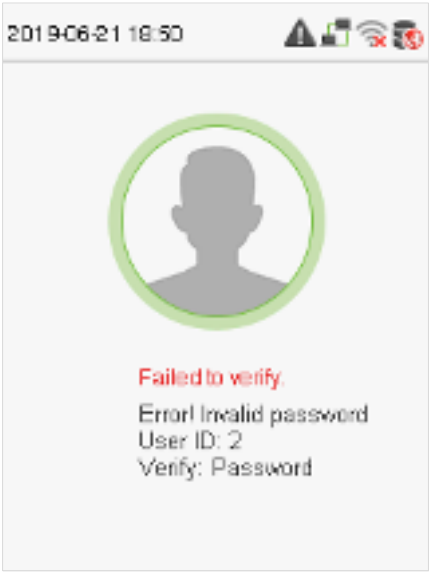
If the user registers face and fingerprint in addition to password, the following screen will appear. Select the Password icon to enter password verification mode.

2. Input the password and press **M/OK**.

Verification is successful.



Verification is failed.



1.4.2 Fingerprint Verification

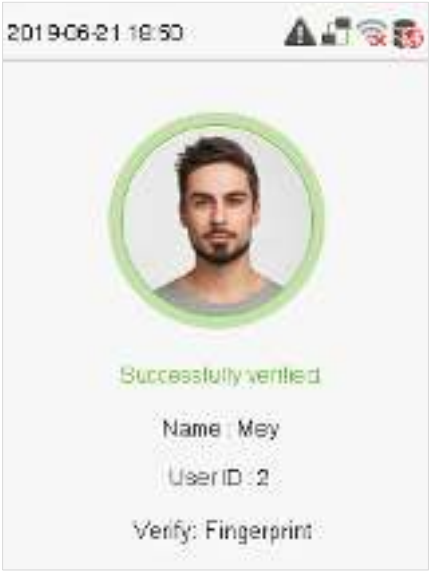
- **1:N fingerprint verification**

Compare the fingerprint that is being pressed onto the fingerprint reader with all of the fingerprint data that is stored in the device.

To enter fingerprint verification mode, simply press your finger on the fingerprint reader.

Make sure that you correctly press your fingerprint onto the fingerprint reader.

Successful verification:



Verification is failed:

- **1:1 fingerprint verification**

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to Employee ID input via the virtual keyboard. This method can be used when the system has trouble recognizing an employee's fingerprints.

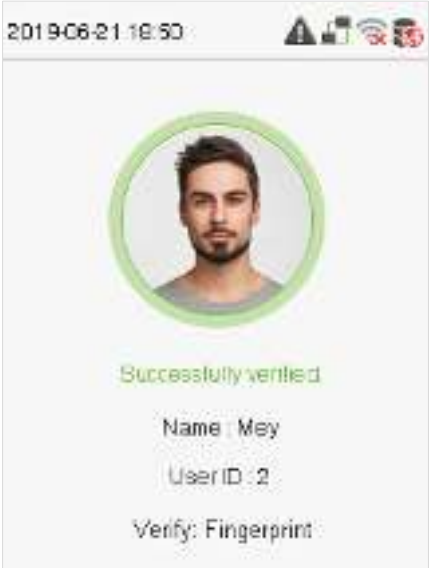
Enter the User ID on the main screen to enter 1:1 fingerprint verification mode:

1. Enter the User ID and press **M/OK**.

If the user has registered a face, a password and badge★ in addition to his/her fingerprints and the verification method is set to password/ fingerprint/ badge★/ face verification, the following screen will appear. Select the fingerprint icon to enter fingerprint verification mode:

2. Press the finger on the fingerprint reader to proceed with verification.

3. Successfully verified.

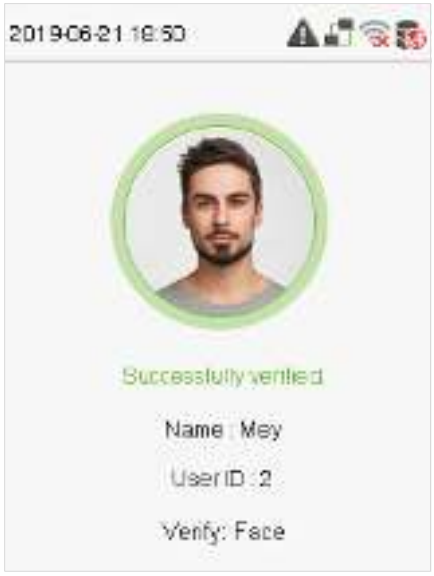


4. Verification is failed.

1.4.3 Facial Verification

- **1:N face verification**

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



- **1:1 face verification**

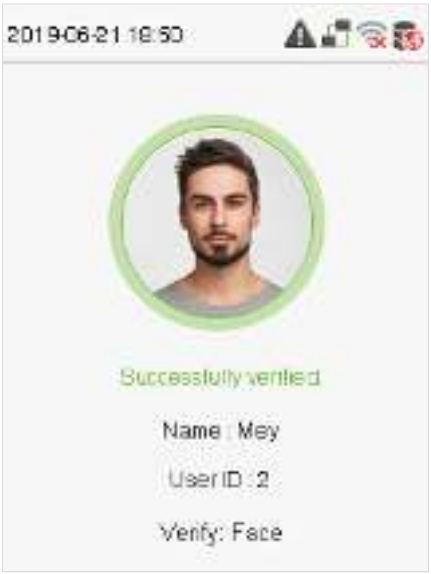
Compare the face captured by the camera with the facial template related to the entered user ID.

Enter the User ID on the main interface and enter the 1:1 facial verification mode.

1. Enter the user ID and select **M/OK**.

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

After successful verification, the prompt box "Successfully verified" will appear.



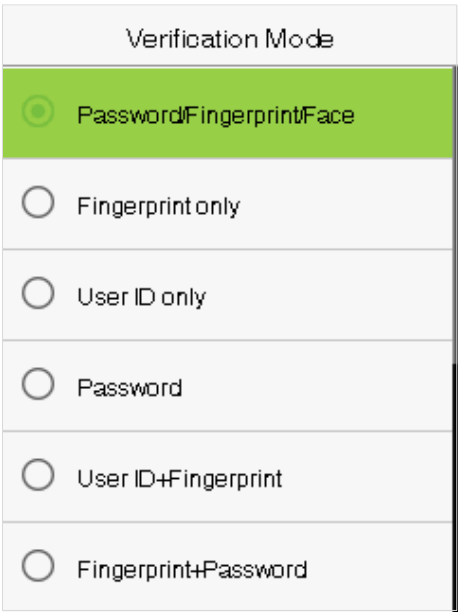
1.4.4 Card Verification★

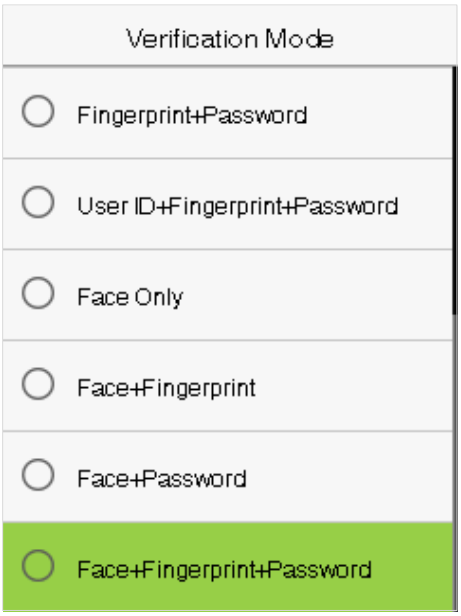
Only the product with the card module offers the card verification function.

Please place the registered card on the card reader.

1.4.5 Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 5 different verification combinations can be used, as shown below:





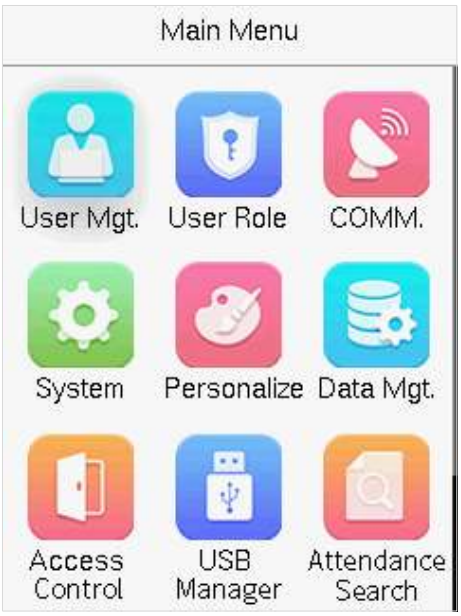
Notes:

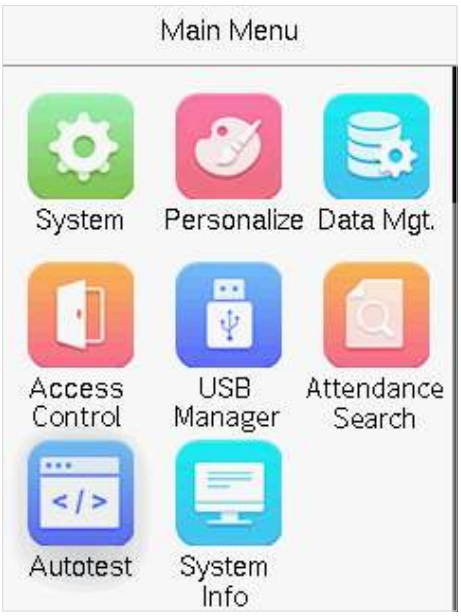
1) "/" means "or", and "+" means "and".

2) You must register the required verification information before using the combination verification mode, otherwise the verification may fail. For example, if a user uses Face Registration but the verification mode is Face + Password, this user will never pass verification.

2 Main Menu

Click **M/OK** on the initial interface to enter the main menu, as shown below:



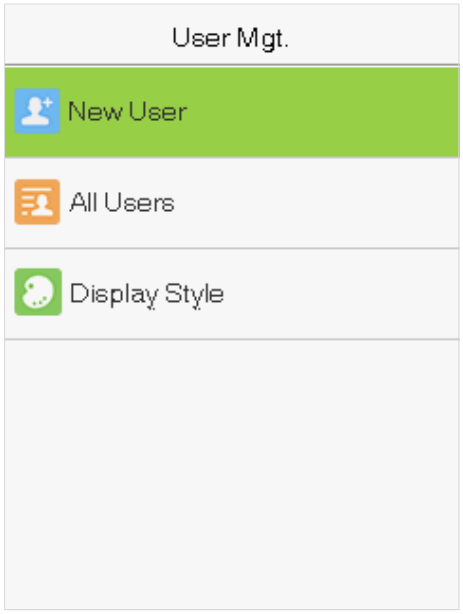


Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Ethernet, PC connection, Wireless network, cloud server setting.
System	To set parameters related to the system, including date & time, attendance, face, fingerprint, reset, USB upgrade.
Personalize	To customize settings of interface display, including user interface, voice, punch state options and shortcut key mappings.
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.
USB Manager	To transfer data such as user data and attendance logs from the USB disk to the supporting software or other devices.
Attendance Search	Query the specified access record, check attendance photos and blacklist photos.
Autotest	To automatically test whether each module functions properly, including the screen, audio, camera and real-time clock.
System Info	To view data capacity, device and firmware information of the current device.

3 User Management

3.1 Adding Users

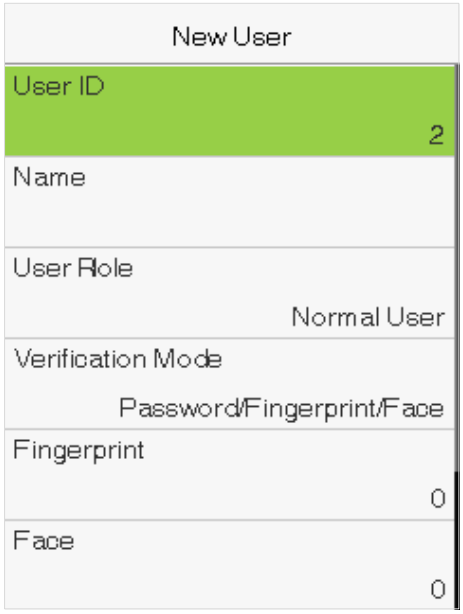
Select **User Mgt.** on the main menu.



Select **New User**.

- **Register a User ID and Name**

Enter the user ID and name.



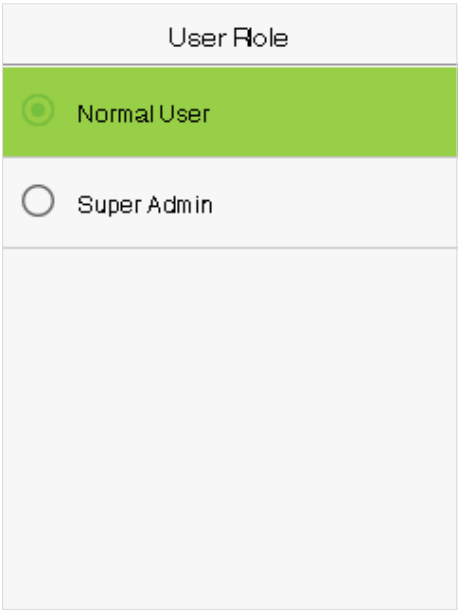
Notes:

1) A user name may contain 17 characters.
2) The user ID may contain 1-9 digits by default.
3) During the initial registration, you can modify your ID, which cannot be modified after registration.
4) User ID cannot be repeated. If there is a voice prompt, you must choose another ID.

- **Setting the User Role**

There are two types of user accounts: the **normal users** and the **super admin**. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The administrator owns all management privileges. If a custom role is set, you can also select **custom role** permissions for the user.

Select **User Role** to set Normal User or Super Admin.

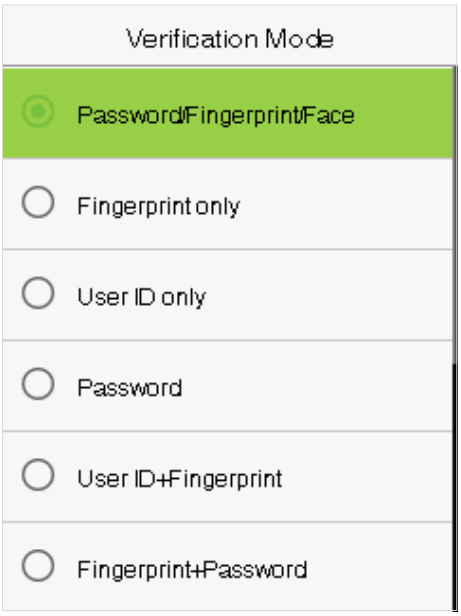


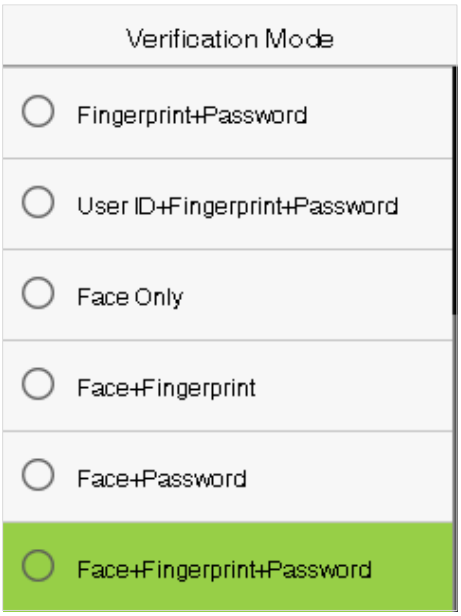
Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

- **Setting the Verification Mode**

Including password/fingerprint/face, fingerprint only, user ID only, password, user ID + fingerprint, fingerprint + password, user ID + fingerprint + password, face only, face + fingerprint, face + password, face + fingerprint + password.

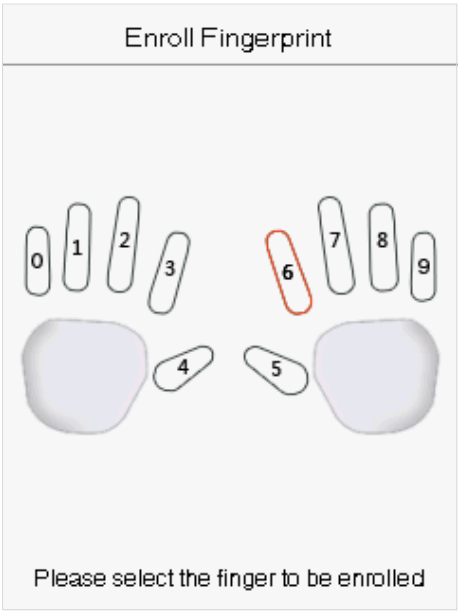
Select **Verification Mode** to set Individual verification mode of the user. Select **M/OK** to save and return to the New User interface.





- **Register fingerprint**

Select **Fingerprint** to enter the enroll fingerprint page. User can choose one or more fingerprint(s) to enroll. Press the finger horizontally onto the fingerprint sensor. The registration interface is as follows:

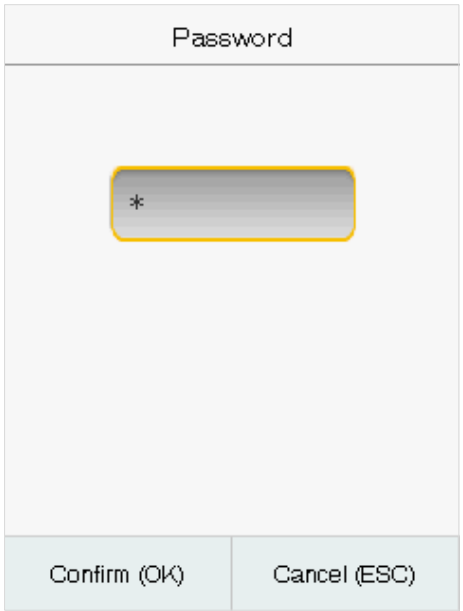


- **Register face**

Select **Face** to enter the face registration page. Please face the camera and stay still during face registration. The registration interface is as follows:

- **Register password**

Select **Password** to enter the password registration page. Enter a password and re-enter it. Select **M/OK**. If the two entered passwords are same, the system will return to the New User interface.



Note: The password may contain one to eight digits by default.

- **Register user photo**

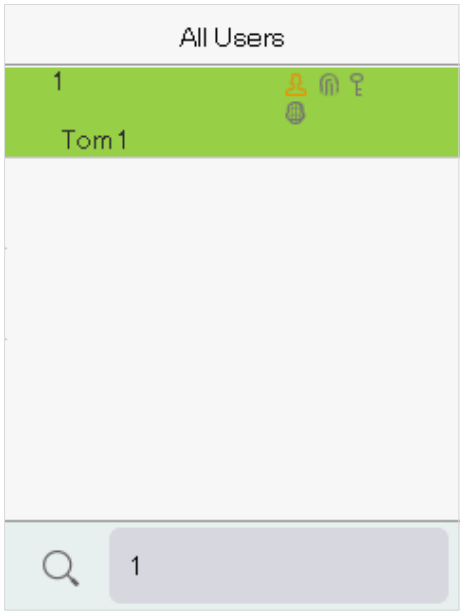
When a user registered with a photo passes the authentication, the registered photo will be displayed.

Select **User Photo**, Select **M/OK** to take a photo. Then Select **ESC** to exit and return to the New User interface.

Note: While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

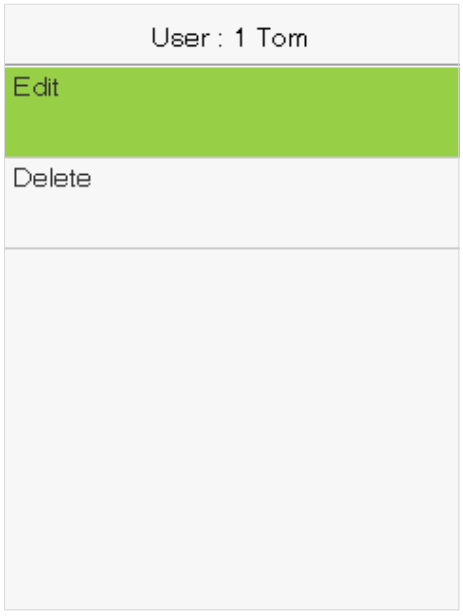
3.2 Search for Users

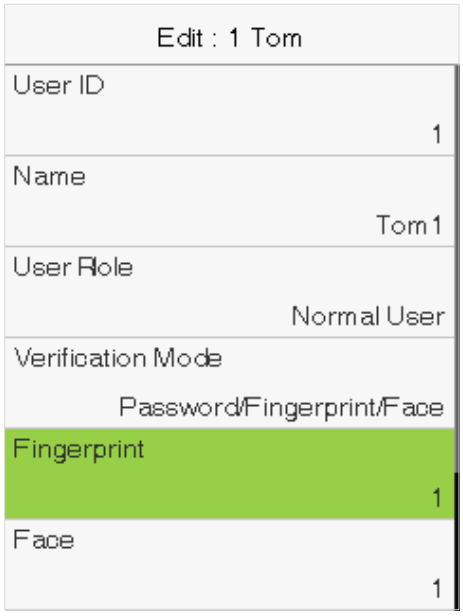
Enter the retrieval keyword on the user list (The keyword may be an ID, surname or full name.). The system will search for the users related to the information.



3.3 Edit Users

Choose a user from the list and select **Edit** to enter the edit user interface:

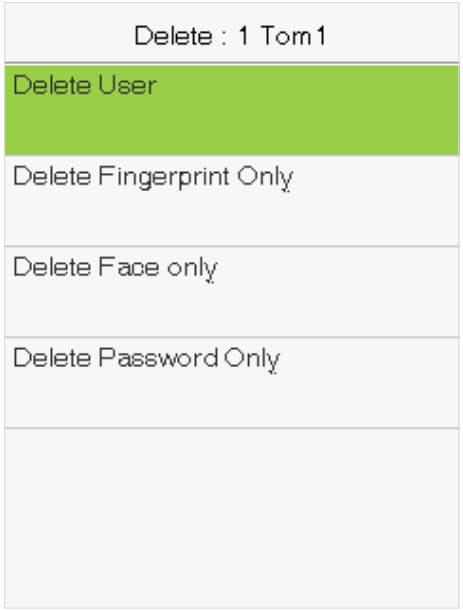




Note: The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user.

3.4 Deleting Users

Choose a user from the list and select **Delete** to enter the delete user interface. Select the user information to be deleted and click **M/OK**.



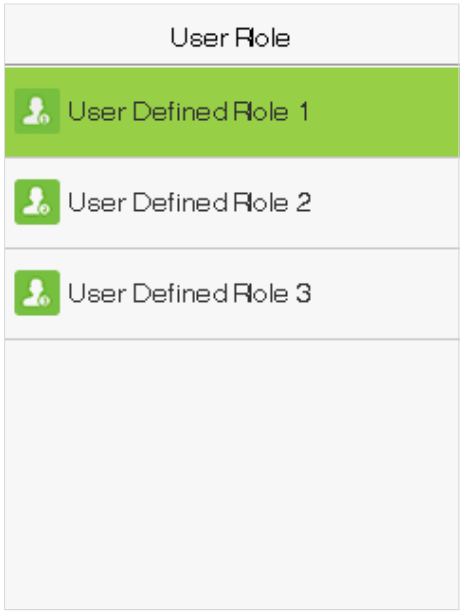
Note: If you select **Delete User**, all information of the user will be deleted.

4 User Role

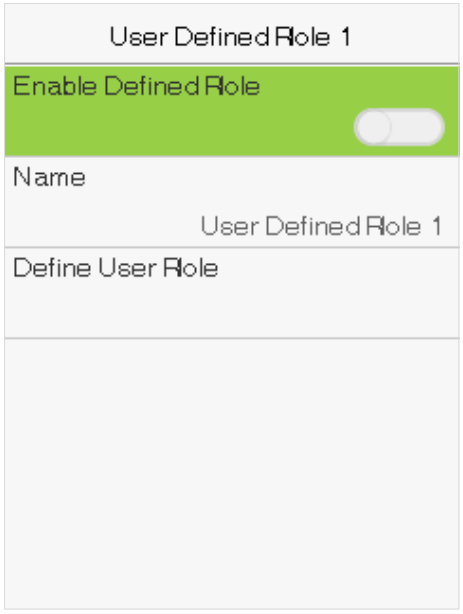
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

You may set the permission scope of the custom role (up to 3 roles) and enroller, that is, the permission scope of the operation menu.

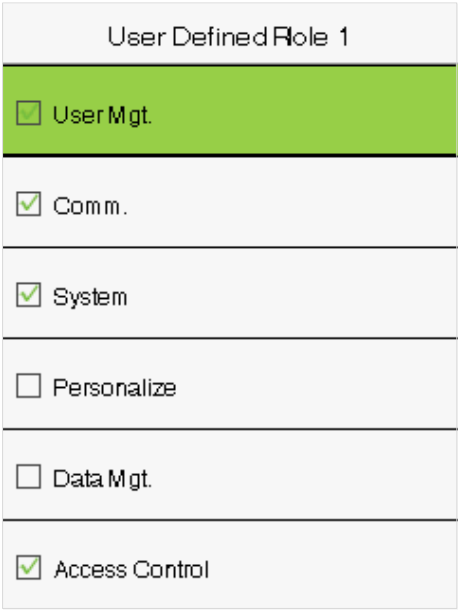
Select **User Role** on the main menu interface.



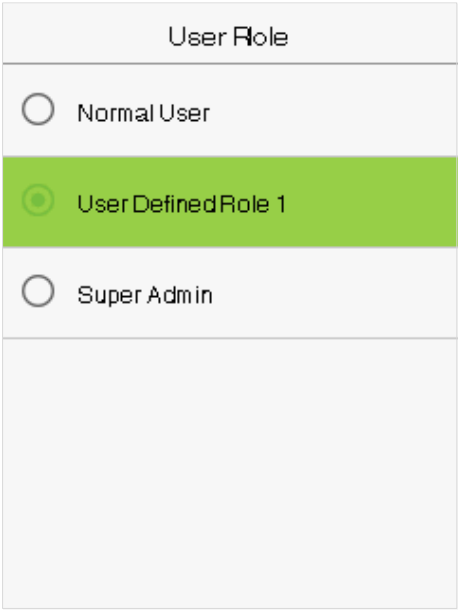
1. Select any item to set a defined role. Select the row of **Enable Defined Role** to enable this defined role. Select **Name** and enter the name of the role.



2. Select **Define User Role** to assign the privileges to the role. The privilege assignment is completed. Click **ESC** to save and return.



Note: You need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by selecting User Mgt. > New User > User Role.

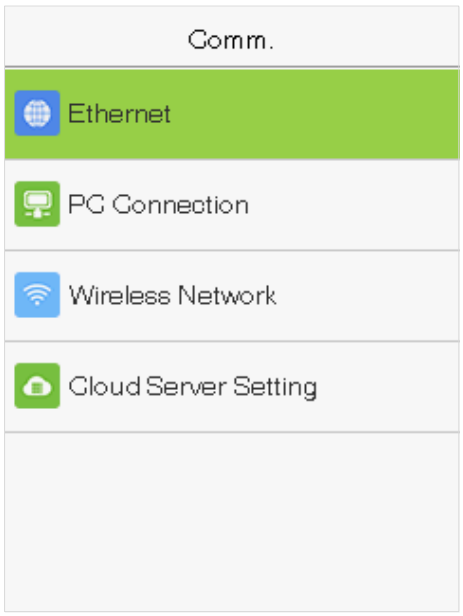


If no super administrator is registered, the device will prompt "Please register super administrator user first!" after Selecting the enable bar.

5 Communication Settings

Set parameters of the network, PC connection, WIFI and cloud server.

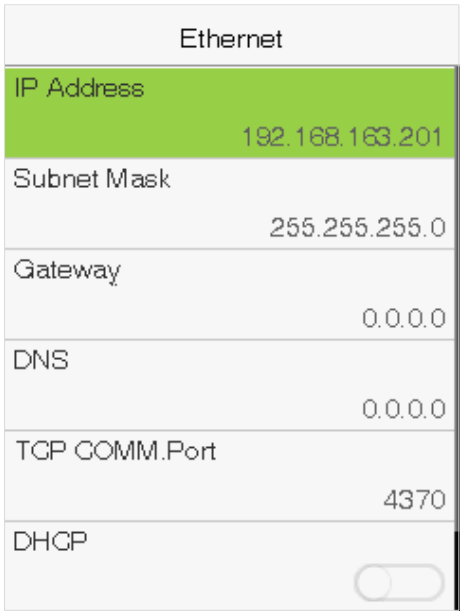
Select **COMM.** on the main menu.



5.1 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 are connecting to the same network segment.

Select **Ethernet** on the Comm. Settings interface.



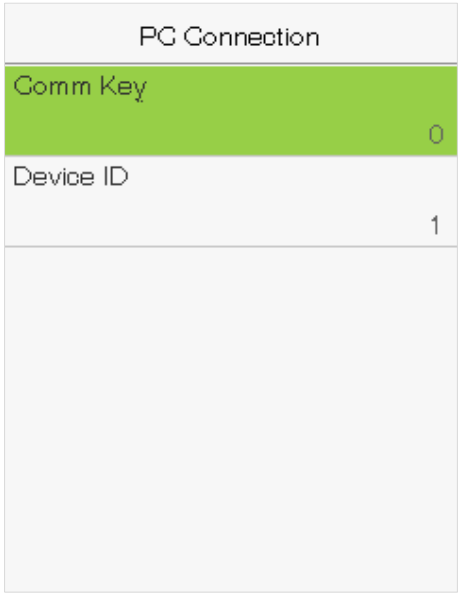
Item	Descriptions
IP Address	The factory default value is 192.168.1.201. Please adjust them according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0. Please adjust them according to the actual network situation.
DNS	The factory default address is 0.0.0.0. Please adjust them according to the actual network situation.
TCP COMM. Port	The factory default value is 4370. Please adjust them according to the actual network situation.
DHCP	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
Display in Status Bar	To set whether to display the network icon on the status bar.

5.2 PC Connection

To improve the security of data, please set a Comm Key for communication between the device and the PC.

If a Comm Key is set, this connection password must be entered before the device can be connected to the PC software.

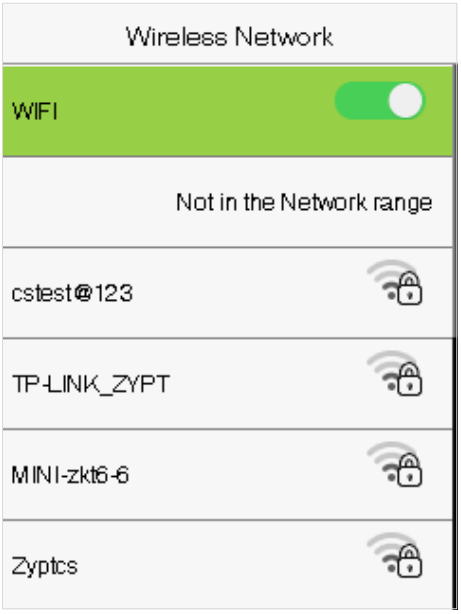
Select **PC Connection** on the Comm. Settings interface.



Item	Descriptions
Comm Key	The default password is 0, which can changed. The Comm Key may contain1-6 digits.
Device ID	Identity 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.

5.3 WIFI Setting

Select **Wireless Network** on the Comm. Settings interface.

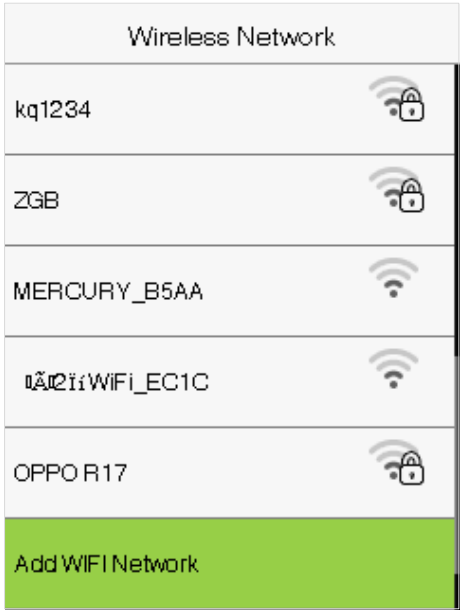


When WIFI is enabled, select the searched network. Enter the password, and select Connect to WIFI (OK). The connection succeeds, with icon displayed on the status bar.

➢ **Adding WIFI Network**

If the desired Wi-Fi network is not in on the list, you can add the Wi-Fi network manually.

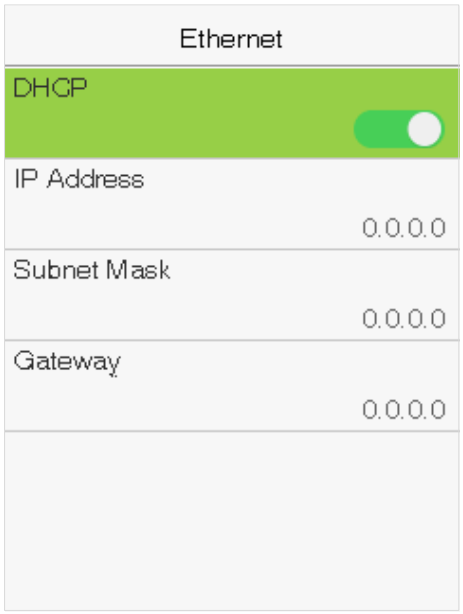
Select Add WIFI Network. Enter the parameters of the Wi-Fi network. (The added network must exist.)



After adding, find the newly added Wi-Fi network in list and connect to it in the above way.

➢ **Advanced**

This is used to set Wi-Fi network parameters.

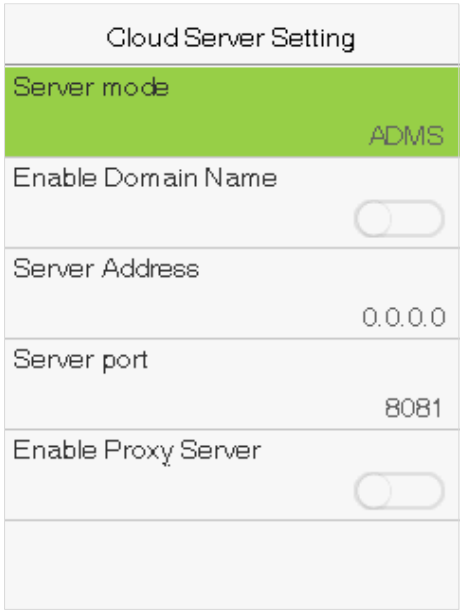


Item	Description
DHCP	Short for Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway	Gateway address of the Wi-Fi network.

5.4 Cloud Server Setting

This represents settings used for connecting with the ADMS server.

Select **Cloud Server Setting** on the Comm. Settings interface.

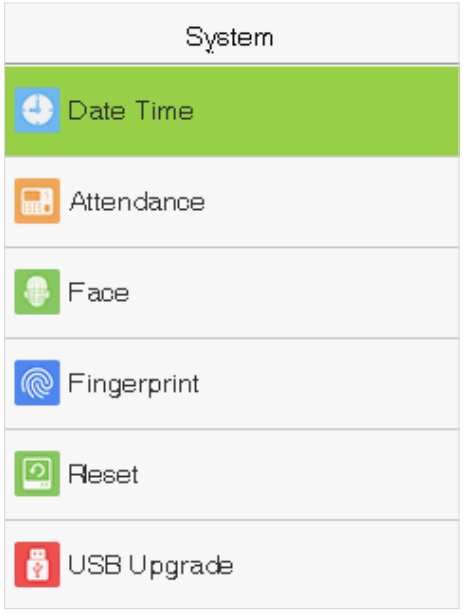


Item	Description
Enable Domain Name	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Server Address	IP address of the ADMS server.
Server Port	Port used by the ADMS server.
Enable Proxy Server	When you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

6 System Settings

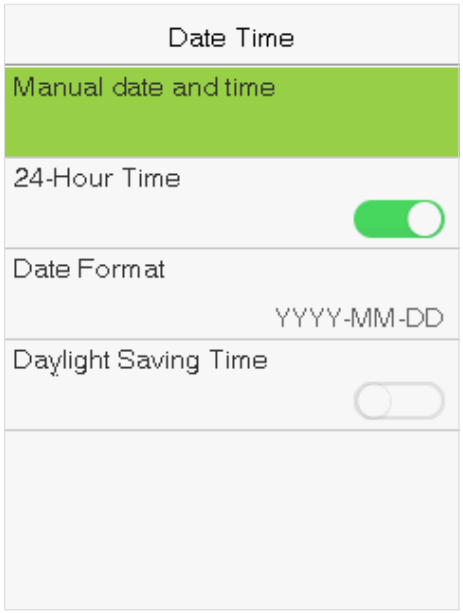
Set related system parameters to optimize the performance of the device.

Select **System** on the main menu interface.



6.1 Date and Time

Select **Date Time** on the System interface.



1. You can manually set date and time and click **M/OK** to save.
2. Select 24-Hour Time to enable or disable this format and select the date format.

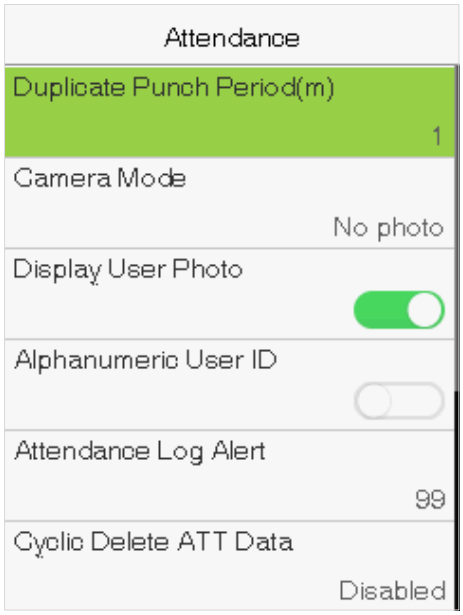
When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the

device date and time cannot be restored.

✍ **Note:** For example, the user sets the time of the device (18:35 on March 15, 2019) to 18:30 on January 1, 2020. After restoring the factory settings, the time of the equipment will remain 18:30 on January 1, 2020.

6.2 Attendance Setting

Select **Attendance Setting** on the System interface.

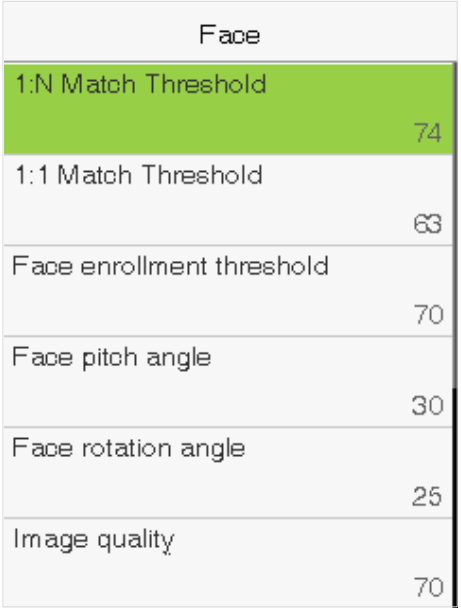


Item	Description
Duplicate Punch Period (m)	Within a set time period (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	Whether to capture and save the current snapshot image during verification. There are 5 modes: **No Photo:** No photo is taken during user verification. **Take photo, no save:** Photo is taken but is not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved during each failed verification.
Display User Photo	Whether to display the user photo when the user passes verification.
Alphanumeric User ID	Whether to support letters in an User ID.
Attendance Log Alert	When the remaining storage is smaller than the set value, the device will automatically alert users to the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.

Cyclic Delete ATT Data	The number of attendance logs allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 999.
Cyclic Delete ATT Photo	When attendance photos have reached full capacity, the device will automatically delete a set value of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Cyclic Delete Blacklist Photo	When blacklisted photos have reached full capacity, the device will automatically delete a set value of old blacklisted photos. Users may disable the function or set a valid value between 1 and 99.
Confirm Screen Delay(s)	The length of time that the message of successful verification displays. Valid value: 1~9 seconds.
Face Detect Interval (s)	To set the facial template matching time interval as needed. Valid value: 0~9 seconds.

6.3 Face Parameters

Select **Face** on the System interface.



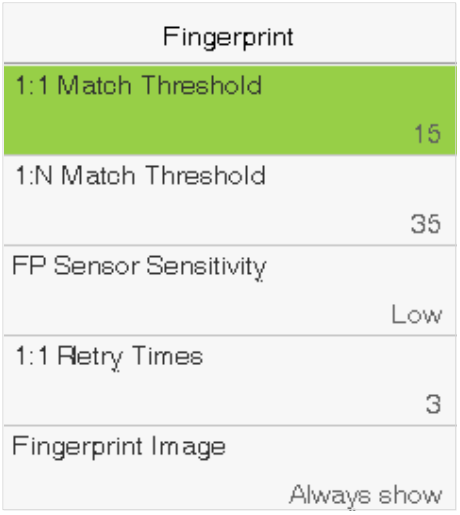
FRR	FAR	Recommended matching thresholds	
		1:N	**1:1**
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Item	Description
1:N Match Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds set, the lower the misjudgment rate, the higher the rejection rate, and vice versa.
1:1 Match Threshold	Under 1:1 verification mode, the verification will only be successful when the

	similarity between the acquired facial image and the facial templates enrolled in the device is greater than the set value. The valid value ranges from 55 to 120. The higher the thresholds set, the lower the misjudgment rate, the higher the rejection rate, and vice versa.
Face registration threshold	During face registration, 1:N verification is used to determine whether the user has been registered. The current face is registered when the similarity between the acquired facial image and all registered facial templates is greater than the set value.
Pitch angle threshold	To limit the pitch angle of face in face recognition, the recommended threshold is 20.
Rotation angle threshold	To limit the rotation angle of face in face recognition, the recommended threshold is 20.
Image Quality	To get the quality threshold of facial images. When the value of image quality is greater than the set value, the device will accept the facial images and start the algorithm processing, otherwise, the device will filter the facial images out.
Threshold of turning on the supplement LED	Detect ambient light intensity. When the ambient brightness is less than the threshold, the fill light is turned on; When ambient brightness is greater than this threshold, the fill light does not turn on. The default value is 80.
Alive body detection switch	If enabled, it will automatically detect whether there is a moving person in front of the device.
Alive body detection threshold	Detect whether there is a moving person in front of the device to determine whether face recognition is enabled. The default value is 100. The valid value ranges from 0 to 100.
Notes	Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

6.4 Fingerprint Parameters

Select **Fingerprint** on the System interface.



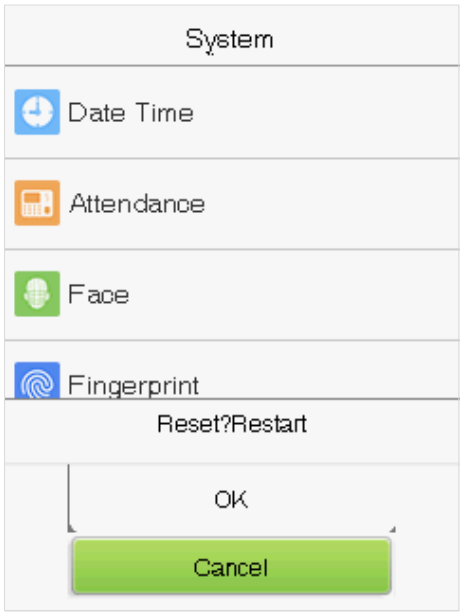
		Match Threshold	
FRR	**FAR**	**1:N**	**1:1**
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Item	Description
1:1 Match Threshold	Under 1:1 Verification Method, only when the similarity between the verifying fingerprint and the user's registered fingerprint is greater than this value can the verification succeed.
1:N Match Threshold	Under 1:N Verification Method, only when the similarity between the verifying fingerprint and all registered fingerprints is greater than this value can the verification succeed.
FP Sensor Sensitivity	To set the sensibility of fingerprint collection. 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 Times	In 1:1 Verification or Password Verification, users might forget the registered fingerprint or password, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed; the number of retry can be within 1~9.
Fingerprint Image	To set whether to display the fingerprint image on the screen in registration or verification. Four choices are available: Show for enroll, Show for match, Always show, None.

6.5 Factory Reset

Restore the device, such as communication settings and system settings, to factory settings (Do not clear registered user data).

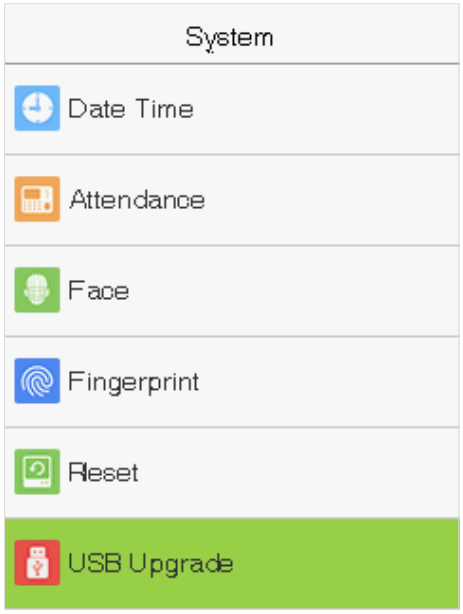
Select **Reset** on the System interface. Select **OK** to reset.



6.6 USB Upgrade

Insert the U disk with upgrade file into the device's USB port, and in the initial interface, press **[M/OK]** > **System** > **USB Upgrade** to complete firmware upgrade operation.

Select **USB Upgrade** on the System interface.

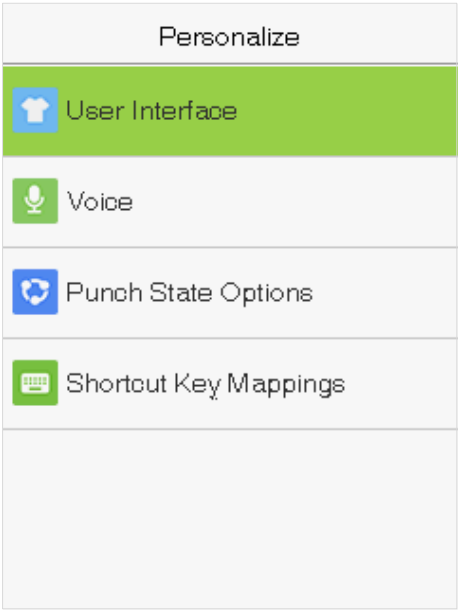


Note: If upgrade file is needed, please contact out technical support. Firmware upgrade is not recommenced under normal circumstances.

7. Personalize Settings

You may customize interface settings.

Select **Personalize** on the main menu interface.



7.1 Interface Settings

You can customize the display style of the main interface.

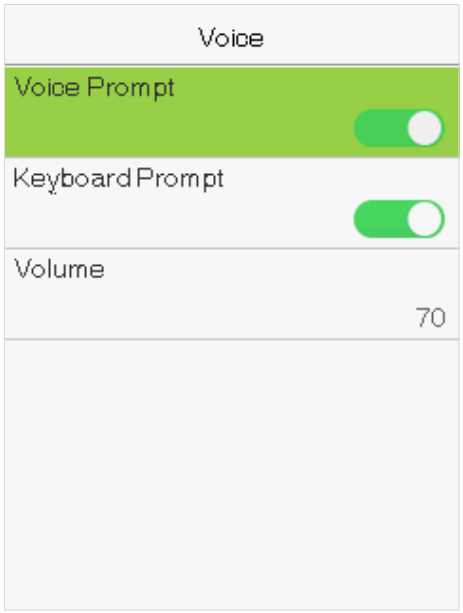
Select **User Interface** on the Personalize interface.

Item	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	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 will automatically go back to the initial interface. You can disable the function or set the 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 will be played. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	This refers to the time interval switching 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 you have activated the sleep mode, when there is no operation, the device will enter standby mode. Press any key or finger to resume normal working mode. You can disable this function or set a value within 1-999 minutes.
Main Screen Style	To select the main screen style according to your personal preference.

7.2 Voice Settings

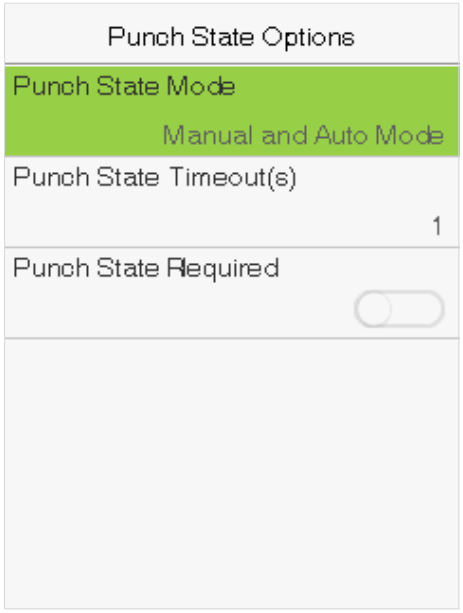
Select **Voice** on the Personalize interface.



Item	Description
Voice Prompt	Select whether to enable voice prompts during operating, press **[M/OK]** to enable it.
Keyboard Prompt	Select whether to enable keyboard voice while pressing keyboard, press **[M/OK]** to enable it.
Volume	et the volume of device. Press ▶ key to increase the volume, press ◀ key to decrease the volume.

7.3 Punch States Settings

Select **Punch State Options** on the Personalize interface.



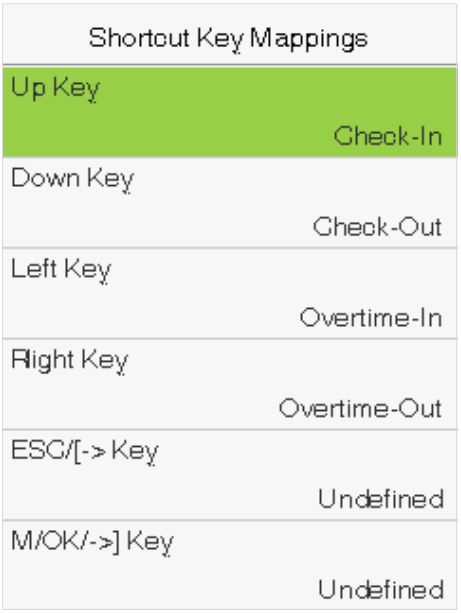
Item	Description
Punch State Mode	To choose the **Punch State Mode**, which includes the following modes: **Off:** To disable the punch state key function. The punch state key set under Shortcut Key Mappings menu will become invalid. **Manual Mode:** To switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. **Auto Mode:** After this mode is chosen, set the switching time of punch state key in Shortcut Key Mappings; when the switching time is reached, the set punch state key will be switched automatically. **Manual and Auto Mode:** Under this mode, the main interface will display the auto-switching punch state key, meanwhile supports manually switching punch state key. After timeout, the manually switching punch state key will become auto-switching punch state key. **Manual Fixed Mode:** After punch state key is manually switched, the punch state key will remain unchanged until being manually switched next time. **Fixed Mode:** Only the fixed punch state key will be shown and it cannot be switched.
Punch State Timeout (s)	The timeout time of the display of punch state. The value ranges from 5~999 seconds.
Punch State Required	Whether it is necessary to choose attendance state in verification. **ON:** Choosing attendance state is needed after verification. **OFF:** Choosing attendance state is not needed after verification.

Remarks: There are four punch states: Check-In, Check-Out, Overtime-In, Overtime-Out.

7.4 Shortcut Keys Settings

Shortcut keys can be defined as punch state keys or menu function key. When the device is on the main interface, pressing the set shortcut key will display the attendance state or enter the menu operation interface.

Select **Shortcut Key Mappings** on the Personalize interface.



To set Auto Switching Time:

Choose any shortcut key, and select **Punch State Options** in **Function**, so that auto switching time can be set.

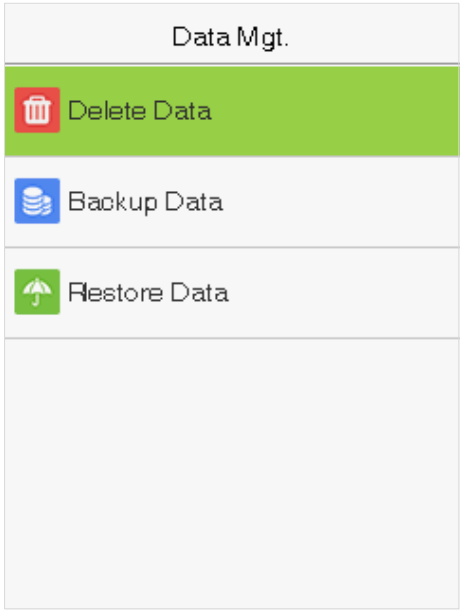
Auto Switch: When the set time is reached, the device will switch the attendance state automatically.

When the shortcut key is set to **Punch State Key**, but **OFF** mode is selected in the **Punch State Mode** (**Personalize** > **Punch State Options** > **Punch State Mode** > Select **OFF**), then the shortcut key will not be enabled.

8. Data Management

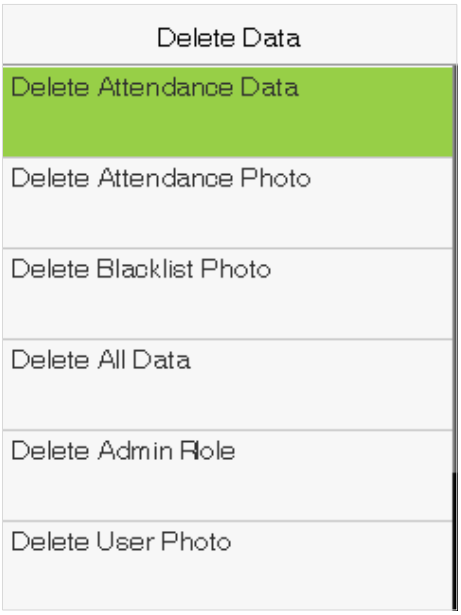
To delete the relevant data in the device.

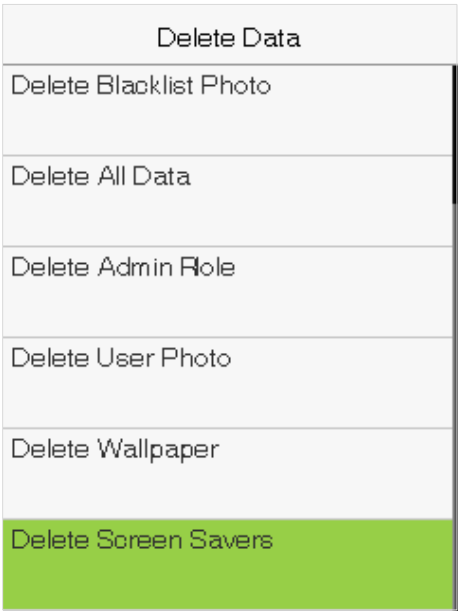
Select **Data Mgt.** on the main menu interface.



8.1 Delete Data

Select **Delete Data** on the Data Mgt. interface.

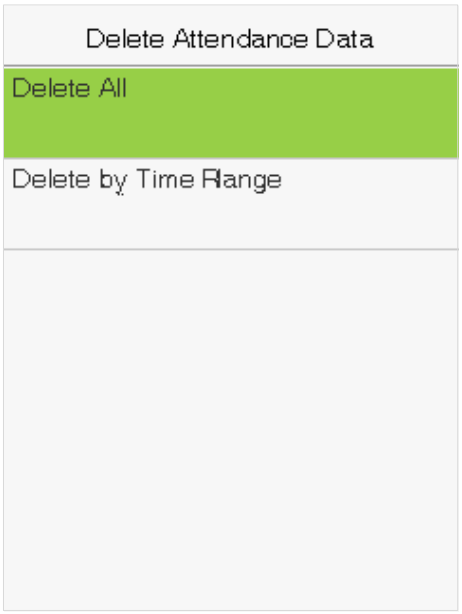




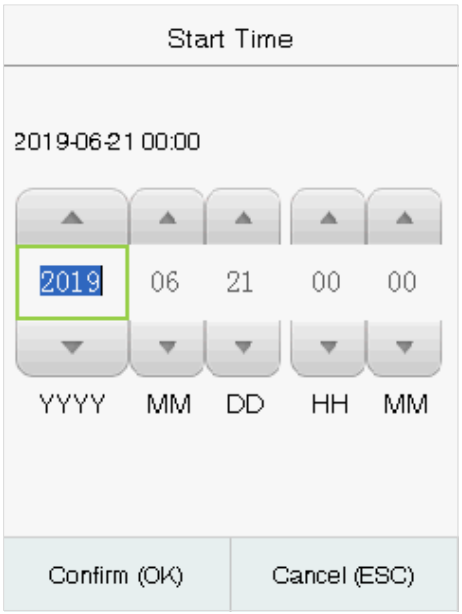
Item	Description
Delete Attendance Data	To delete all attendance data in the device.
Delete Attendance Photo	To delete attendance photos of designated personnel.

Delete Blacklist Photo	To delete the photos taken during verifications which are failed.
Delete All Data	To delete information and access records of all registered users.
Delete Admin Role	To remove administrator privileges.
Delete Access Control	To delete all access data.
Delete User Photo	To delete all user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete screen savers	To delete the screen savers in the device.

Note: When deleting the access records, attendance photos or blacklisted photos, you may select Delete All or Delete by Time Range. Selecting Delete by Time Range, you need to set a specific time range to delete all data with the period.



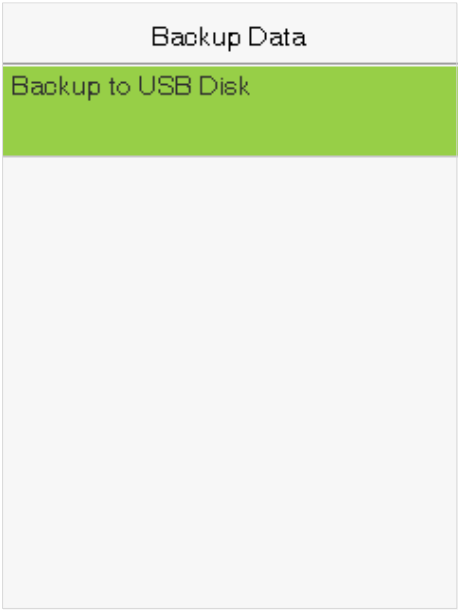
Select Delete by Time Range.



Set the time range and Select Confirm(OK).

8.2 Backup Data

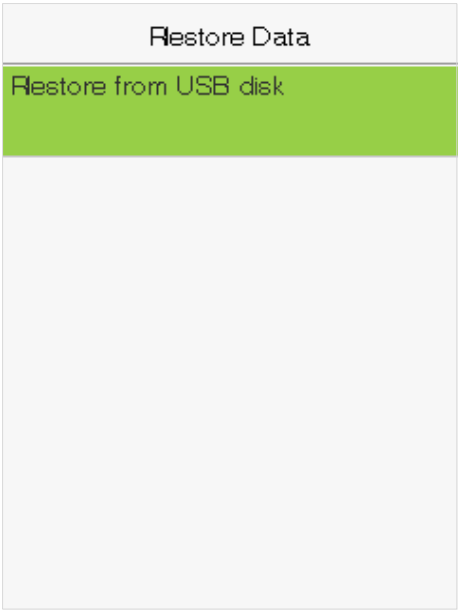
Select **Backup Data** on the Data Mgt. interface.



Insert the USB disk. In the initial interface, press **[M/OK]** > **Data Mgt.** > **Backup Data** > **Backup to USB Disk** > **Backup Content** > choose content to be backed up (**Business Data** / **System Data**) > **Backup Start** to start backup. Restarting the device is not needed after backup is completed.

8.3 Restore Data

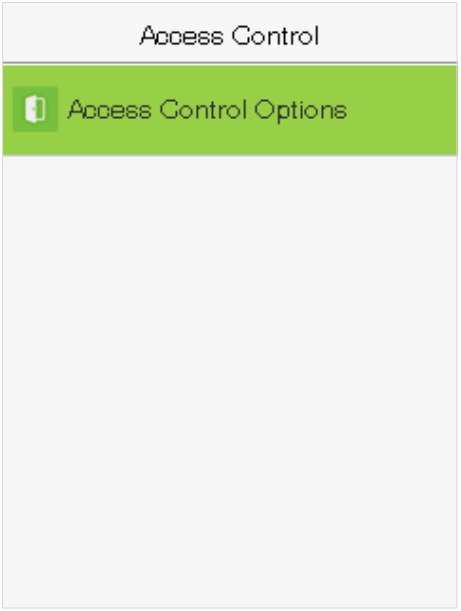
Select **Restore Data** on the Data Mgt. interface.



Insert the USB disk. In the initial interface, click **M/OK** > **Data Mgt.** > **Restore Data** > **Restore from USB Disk** > **Content** > choose content to be restored (**Business Data** / **System Data**) > **Start Restore** > select **Yes** to start restoring. After restoration completes, select **OK** to automatically restart the device.

9. Access Control

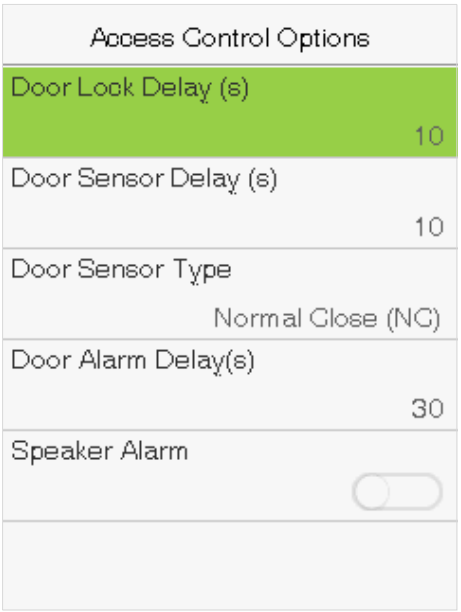
Select **Access Control** on the main menu interface.



9.1 Access Control Options

To set the parameters of the control lock of the terminal and related equipment.

Select **Access Control Options** on the Access Control interface.



Item	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be unlock. Valid value: 1~10 seconds; 0 second represents disabling the function.

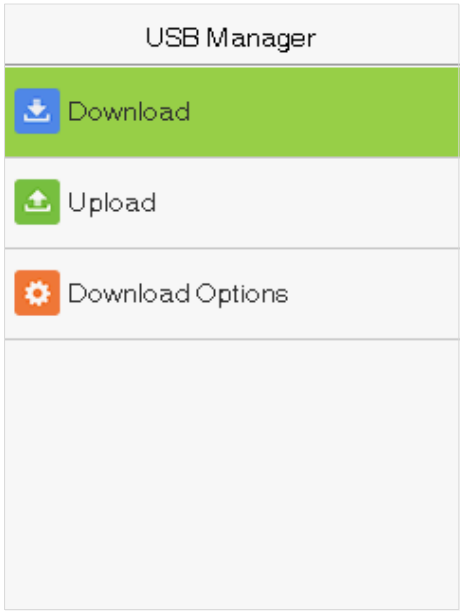
Door Sensor Delay (s)	If the door is not closed and locked after opening for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three types: None, Normal Open, and Normal Closed. None means door sensor is not in use; Normal Open means the door is always opened when electricity is on; Normal Closed means the door is always closed when electricity is on.
Door Alarm Delay (s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the **Door Alarm Delay** (the value ranges from 1 to 999 seconds).
Speaker Alarm	To transmit a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system will cancel the alarm from the local.

10. USB Manager

Upload or download data between device and the corresponding software by USB disk.

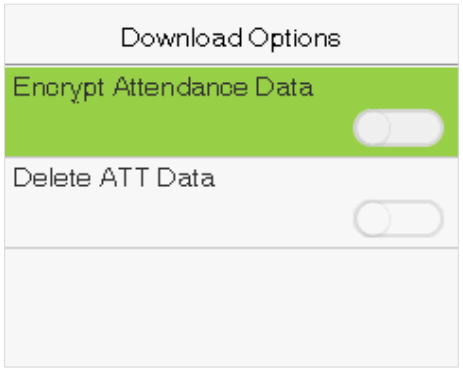
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

Select **USB Manager** on the main menu interface.



10.1 USB Download

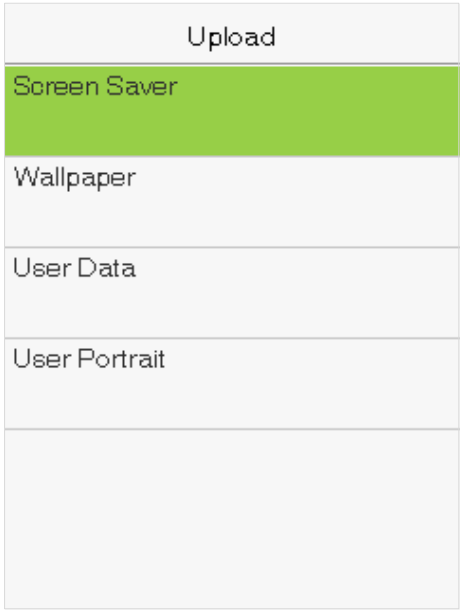
Select **Download** on the USB Manager interface.



Item	Description
Attendance Data	Import all the attendance data from the device to a USB disk.
User Data	Import all the user information, fingerprints and facial images from the device to a USB disk.
User Portrait	Import the employees' photos from the terminal to a USB disk.
Attendance Photo	Download attendance photos saved in device to U disk. The format of photo is JPG.
Blacklist Photo	Download black list photos saved in device to U disk. The format is JPG.

10.2 USB Upload

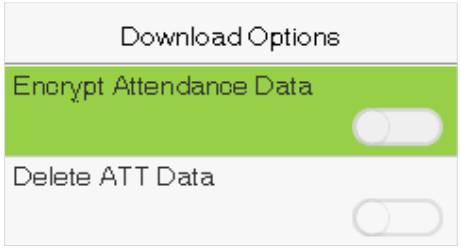
Select **Upload** on the USB Manager interface.



Item	Description
Screen Saver	To upload all screen savers from USB disk into the device. You can choose **[Upload selected picture]** or **[Upload all pictures]**. The images will be displayed on the device's main interface after upload.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose **[Upload selected picture]** or **[Upload all pictures]**. The images will be displayed on the screen after upload.
User Data	Upload the message stored in a USB disk to the terminal.
User Portrait	Upload the JPG documents that are named after the user IDs and stored in a USB disk to the terminal, so that user photos can be displayed after the employees pass the verification.

10.3 Download Options

Select **Download Options** on the USB Manager interface.



Click **[M/OK]** to enable or disable the **[Encrypt Attendance Data]** and **[Delete ATT Data]** options.

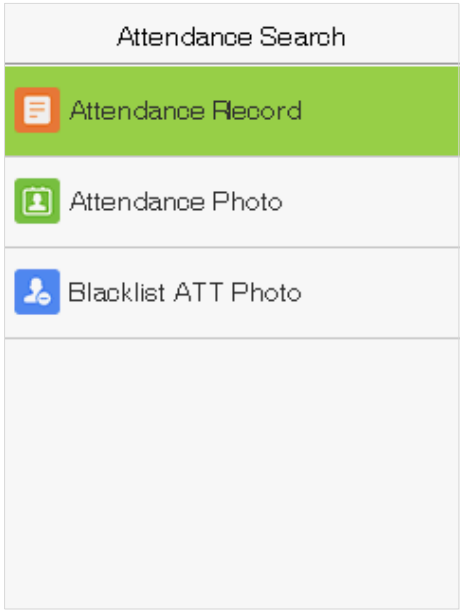
Remarks: The encrypt attendance data can only be imported in the software of Access 3.5.

11. Attendance Search

When the identity of a user is verified, the record will be saved in the device. This function enables users to check their access records.

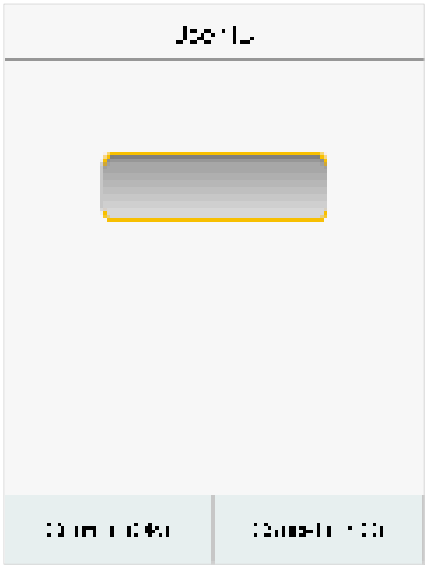
1. Attendance Record

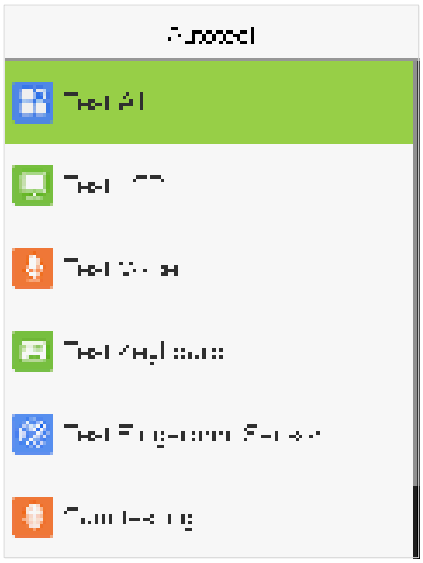
Select **Attendance Search** on the main menu interface.



The process of searching for attendance and blacklist photos is similar to that of searching for access records. The following is an example of searching for access records.

On the Attendance Search interface, Select **Access Records**.

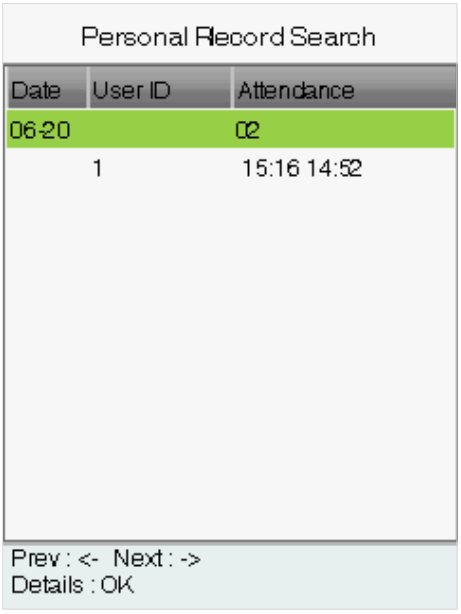




1) Enter the user ID to be searched and Select OK. If you want to search for records of all users, Select OK without entering any user ID.

2) Select the time range in which the records you want to search for.

3) The record search succeeds. Select the record in green to view its details.



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

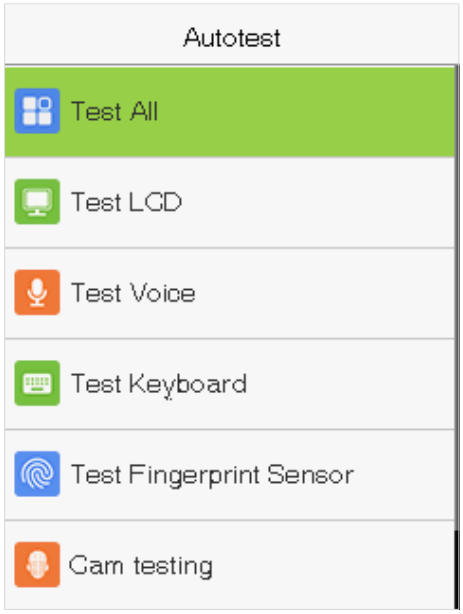
2. Attendance Photo and Blacklist ATT Photo

The operations are similar to those performed to Attendance Record.

12. Autotest

The auto test enables the system to automatically test whether functions of various modules are normal, including the LCD, voice, sensor, keyboard and clock tests.

Select **Autotest** on the main menu interface.

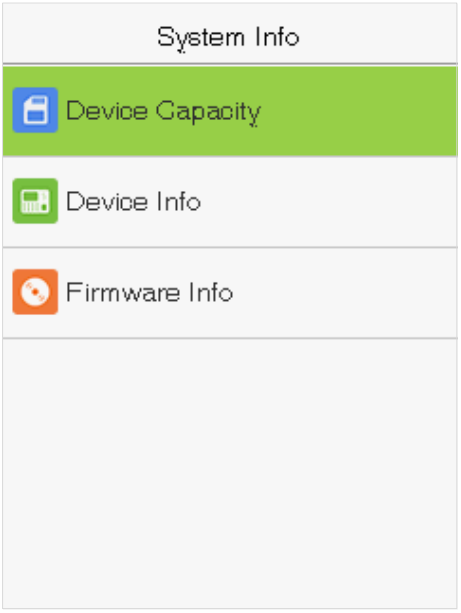


Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Press any key on the **[Keyboard Test]** interface to check whether the pressed key matches the key displayed on screen. The keys are dark-gray before pressed, and turn blue after pressed. Press **[ESC]** to exit the test.
Test Fingerprint Sensor	The terminal automatically tests whether the fingerprint collector works properly by checking whether the fingerprint images are clear and acceptable. When the user places his/her finger in the fingered guide, the collected fingerprint image is displayed on the screen in real-time. Press **[ESC]** to exit the test.
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.

13. System Information

With the system information option, you can view the storage status, the version information of the device, and so on.

Select **System Info** on the main menu interface.



Item	Description
Device Capacity	Displays the current device's user storage, password and face storage, administrators, access records, attendance and blacklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm version information, platform information, and manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.

Statement on the Right to Privacy

Dear Customers:

Thank you for choosing this hybrid biometric recognition product, which was designed and manufactured by ZKTeco. As a world-renowned provider of core biometric recognition technologies, we are constantly developing and researching new products, and strive to follow the privacy laws of each country in which our products are sold.

We Declare That:

1. All of our civilian fingerprint recognition devices capture characteristics, not fingerprint images, and do not involve privacy protection.
2. None of the fingerprint characteristics that we capture can be used to reconstruct an image of the original fingerprint, and do not involve privacy protection.
3. As the provider of this device, we will assume no direct or indirect responsibility for any consequences that may result from your use of this device.
4. If you would like to dispute human rights or privacy issues concerning your use of our product, please directly contact your employer.

Our other police fingerprinting devices or development tools can capture original images of citizens' fingerprints. As to whether or not this constitutes infringement of your rights, please contact your government or the final supplier of the device. As the manufacturers of the device, we will assume no legal liability.

Note:

Chinese law includes the following provisions on the personal freedoms of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons;
2. Personal dignity as related to personal freedom shall not be infringed upon;
3. A citizen's house may not be infringed upon;
4. A citizen's right to communication and the confidentiality of that communication is protected by law.

As a final point we would like to further emphasize that biometric recognition is an advanced technology that will undoubtedly be used in e-commerce, banking, insurance, legal, and other sectors in the future. Every year the world is subjected to major losses due to insecure nature of passwords. Biometric products serve to protect your identity in high-security environments.

Eco-friendly Use

- This product's "eco-friendly use period" refers to the period during which this product will not leak toxic or hazardous substances, when used in accordance with the conditions in this manual.
- The eco-friendly use period indicated 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 use 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 of the homogeneous materials is below the limit requirements specified in SJ/T 11363—2006.

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

Note: 80% of this project's components are made using non-toxic, eco-friendly materials. Those which contain toxins or harmful materials or elements are included due to current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com