timeTec

www.timeteccloud.com

Smart AC1/TD

Face Recognition Access Device with Fever Detection

User Guide

TABLE OF CONTENTS

1   Notice for Use

1.1   Finger Positioning

Recommended fingers: index, middle, or ring fingers; avoid using the thumb or pinky, as they are difficult to accurately pressed onto the fingerprint reader
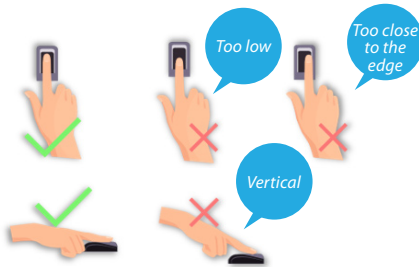
Note: *Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification. Our company assumes no liability for recognition issues that may result from the incorrect usage of the product. We reserve the right of the final interpretation and modification concerning this point.*

1.2   Standing Position, Facial Expression And Standing Posture

The recommended distance between the device and a user whose height is within 1.55m-1.85m is 1.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.
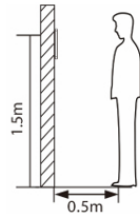
Facial expression and standing posture

Note*:
During enrol-
ment and veri-
fication, please
remain natural
facial expression
and standing
posture.*

1.3   Palm Registration

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device.

Make sure to keep space between your fingers.

Note: *Place your palm within 30-50cm of the device.*

1.4   Face Registration

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

Correct face registration and authentication method

Cautions for registering a face

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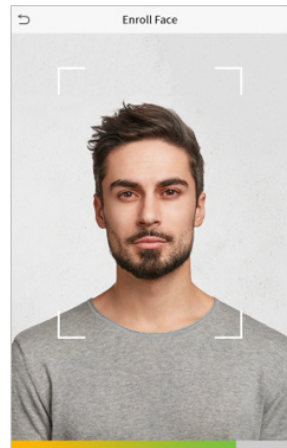
Cautions for authenticating a face

- Ensure that the face appears inside the guideline displayed on the screen of the device.
- If glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses. If only the face with glasses has been registered, authenticate the face with the previously worn glasses again.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

1.5 Standby Interface

After connecting the power supply, enter the following standby interface:
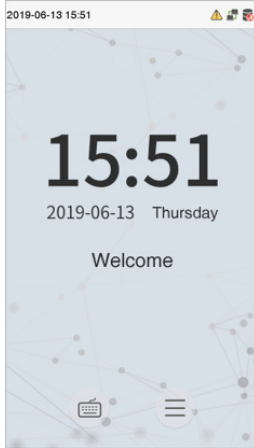
Note:

1 Click 🎹 to enter the User ID input interface.

2 When there is no super administrator set in the device, click ☰ to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register super administrator the first time you use the device.

3 The switch of punch state can be done directly by using the screen shortcut keys. Click anywhere on the screen without icons, and six shortcut keys appear, as shown in the figure below:
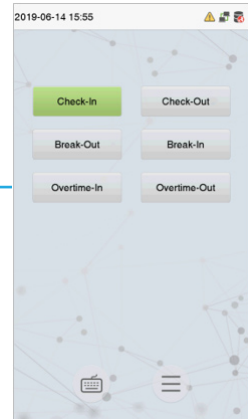
Press the corresponding shortcut key to select the current punch state, which is shown in green. Please refer to "7.5 Shortcut Key Mappings" below for the specific operation method.
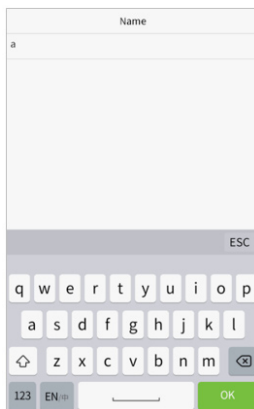
1.6 Virtual Keyboard

Note:

The device supports the input of Chinese, English, numbers and symbols. Click [En] to switch to English keyboard. Press [123] to switch to the numeric and symbolic keyboard, and click [ABC] to return to the alphabetic keyboard. Click the input box, virtual keyboard appears. Click [ESC] to exit the input.

1.7   Verification Mode
Palm Verification

■ **1: N Palm Verification mode**

Compare the palm image collected by the palm collector with all the palm data in the device.

The device will automatically distinguish between the palm and the face verification mode, and place the palm in the area that can be collected by the palm collector, and the device will automatically detect the palm verification mode.

■ **1: 1 Palm Verification mode**

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

Input the user ID and press [OK].
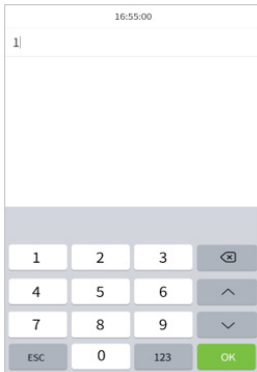
If the user has registered the face and password in addition to his/her palm, and the verification method is set to palm/ face/ password verification, the following screen will appear. Select the palm icon 🖐 to enter palm verification mode.

Fingerprint Verification

■ 1: N fingerprint verification mode

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

The device will enter 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 section 1.1 Finger Positioning.
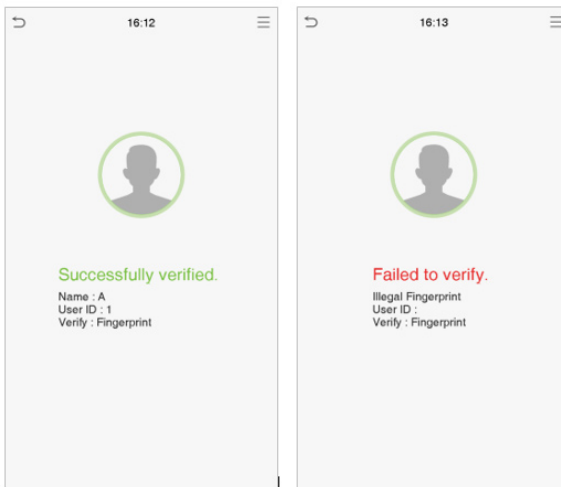
■ 1: 1 fingerprint verification mode

Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

Users may try verifying 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.

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

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

2. Press the fingerprint to verify.

3. Verification is successful.

4. Verification is failed.

Fingerprint Verification

■ 1:N Facial Verification

Conventional 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.
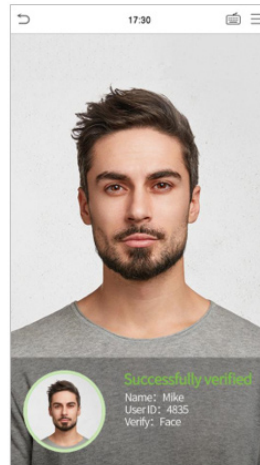
■ 1:1 Facial Verification

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

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

Enter the user ID and click [OK].

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

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

If the verification is failed, it will prompt "Please adjust your position!".

Password Verification

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

Click the [⌨] button on the main screen to enter the 1:1 password verification mode.

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

    If an employee registers palm and face in addition to password, the following screen will appear. Select the [🔑] icon to enter password verification mode.
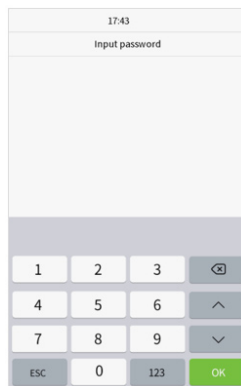
2. Input the password and press [OK].

Combined Verification

To increase security, this device offers the option of using multiple forms of verification methods. A total of 7 different verification combinations can be used, as shown below:

Verification Mode
● Password/Fingerprint/Face/Palm
○ Fingerprint only
○ User ID only
○ Password
○ User ID+Fingerprint
○ Fingerprint+Password
○ User ID+Fingerprint+Password
○ Face Only
○ Face+Fingerprint
○ Face+Password
○ Face+Fingerprint+Password
○ Palm

Note:

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
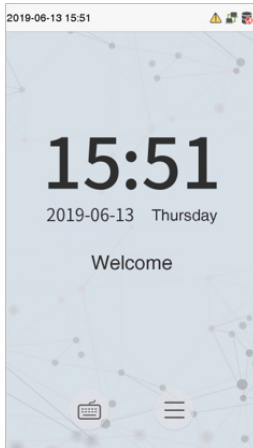
Press ☰ on the initial interface to enter the main menu, as shown below:
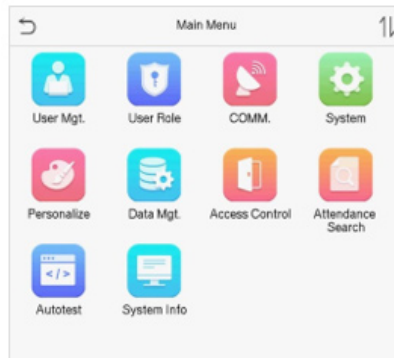
Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of network, PC connection, cloud server and wiegand.
System	To set parameters related to the system, including date & time, attendance/access logs setting, face, palm parameter, resetting to factory settings and detection managementê.
Personalize	This includes user Interface, voice, bell, punch state options and shortcut key mappings settings.
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	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

Click User Mgt. on the main menu.
Click New User.

Register a User ID and Name
Enter the user ID and name.

Note:
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. If a message "Duplicated ID" pops up, you must choose another ID.

Setting the User Role

There are two types of user accounts: the normal user 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 user defined role permissions for the user.

Click User Role to select Normal User or Super Admin.

■ **Register palm**

Click Palm to enter the palm registration page. Select the palmto be enrolled.

■ **Register face**

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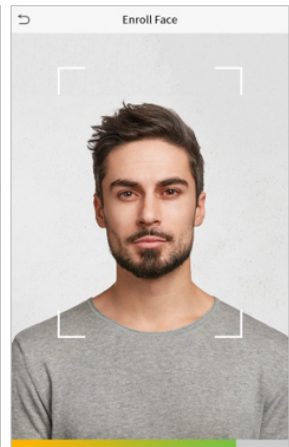
■ **Register password**

Click Password to enter the password registration page. Enter a password and re-enter it. Click OK. If the two entered passwords are different, the prompt "Password not match" will appear.

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.

Click User Photo, click the camera icon to take a photo. The system will return to the New User interface after taking a photo.

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.*

■ Access Control Role

User access control sets the door unlocking rights of each person, including the group and the time period that the user belongs to.

Click Access Control Role > Access Group, assign the registered users to different groups for better management. New users belong to Group 1 by default, and can be reassigned to other groups. The device supports up to 99 access control groups.

Click Time Period, select the time period to use.

3.2   Search For Users

Click the search bar on the user list and enter the retrieval keyword (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 click Edit to enter the edit user interface:

User : 1 A		Edit : 1 A	
Edit		User ID	1
Delete		Name	A
		User Role	Normal User
		Palm	1
		Face	1
		Password	········
		User Photo	0
		Access Control Role	

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. Operation method refers to "3.1 Adding users".*

3.4   Deleting Users

Choose a user from the list and click Delete to enter the delete user interface. Select the user information to be deleted and click 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.

Click User Role on the main menu interface.

⊃	User Role
👤	User Defined Role 1
👤	User Defined Role 2
👤	User Defined Role 3
👤	Enroller
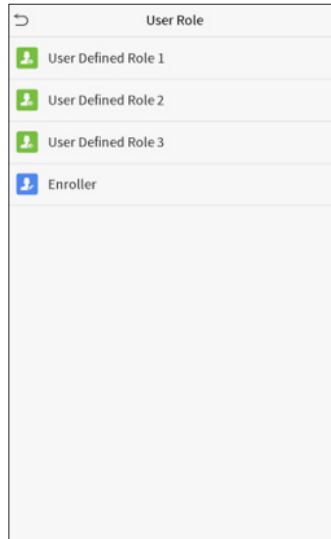
1. Click any item to set a defined role. Click the row of Enable Defined Role to enable this defined role. Click Name and enter the name of the role.
2. Click Define User Role to assign the privileges to the role. The privilege assignment is completed. Click Return.
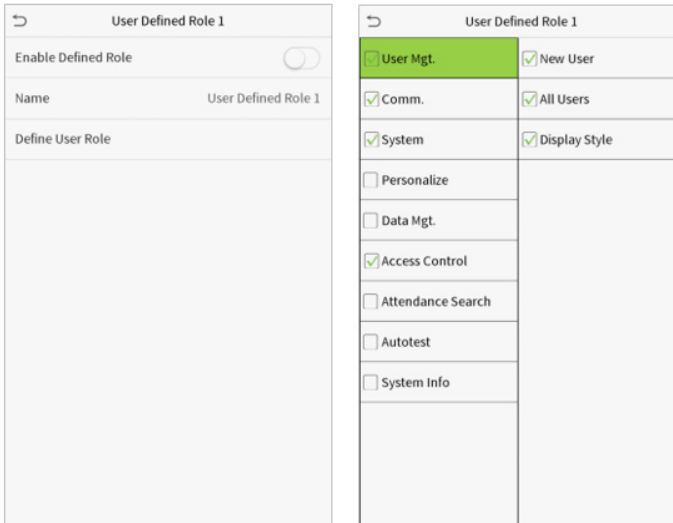
If no super administrator is registered, the device will prompt "Please register super administrator user first!" after clicking the enable bar.

5   Communication Settings

Set parameters of the network, serial communication, PC connection, WIFI, cloud server and Wiegand. Tap 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.

Click Ethernet on the Comm. Settings interface.
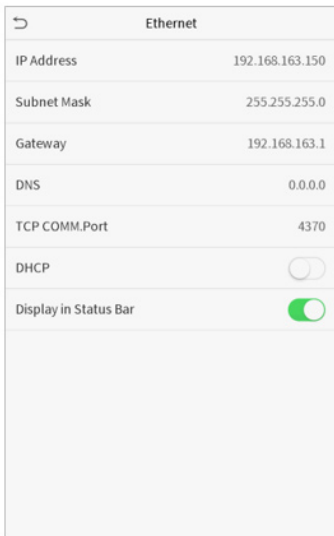
Items	Descriptions
IP Address	The factory default value is 192.168.1.201. Please adjust it according to the actual network situation.
Subnet Mask	The factory default value is 255.255.255.0. Please adjust it according to the actual network situation.
Gateway	The factory default address is 0.0.0.0. Please adjust it according to the actual network situation.
DNS	The factory default address is 0.0.0.0. Please adjust it according to the actual network situation.
TCP COMM. Port	The factory default value is 4370. Please adjust it 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 data security, 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.

Click PC Connection on the Comm. Settings interface.

Items	Descriptions
Comm Key	Comm Key: The default password is 0, which can be 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   Cloud Server Setting

This represents settings used for connecting with the ADMS server.

Click Cloud Server Setting on the Comm. Settings interface.

Items		Descriptions
Enable Domain Name	Server Address	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.
Disable Domain Name	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.

5.4 Wiegand Setup

To set the Wiegand input and output parameters.

Click Wiegand Setup on the Comm.

Settings interface.

	Wiegand Setup
Wiegand Input	
Wiegand Output	

■ **Wiegand input**

	Wiegand Options
Wiegand Format	
Wiegand Bits	26
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	Badge Number

Items	Descriptions
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand Bits	Number of bits of Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 micro-seconds by default, which can be adjusted within the range of 20 to 100 microseconds.
Pulse Interval(us)	The default value is 1000 micro-seconds, which can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between User ID and badge number.

Definitions of various common Wiegand formats:

Wiegand Format	Definitions
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits are the card numbers.
Wiegand26a	ESSSSSSSSSCCCCCCCCCCCCCCCCO Consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits are the card numbers.

Wiegand Format	Definitions
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits are the site codes, while the 10th to 25th bits are the card numbers.
Wiegand36	OFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCMME Consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits are the device codes. The 18th to 33rd bits are the card numbers, and the 34th to 35th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCCO Consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits are the device codes, and the 20th to 35th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCE Consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 16th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFFFSSSSSSSCCCCCCCCCCCCCCCCCO Consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits are the manufacturer codes. The 5th to 14th bits are the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of

"C "denotes the card number; "E" denotes the even parity bit; "O" denotes the odd parity bit; "F" denotes the facility code; "M" denotes the manufacturer code; "P" denotes the parity bit; and "S" denotes the site code.

■ Wiegand output

Items	Descriptions
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.
Wiegand output bits	After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format
Failed ID	If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes of the quantity of electric charge with high-frequency capacitance regularly within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select between User ID and badge number.

6   System Settings

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

Click System on the main menu interface.
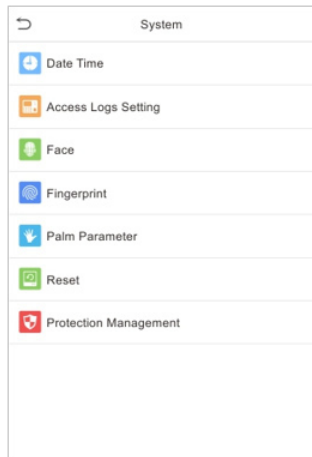
6.1   Date and Time

Click Date Time on the System interface.

1. You can manually set date and time and click Confirm to save.
2. Click 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.*
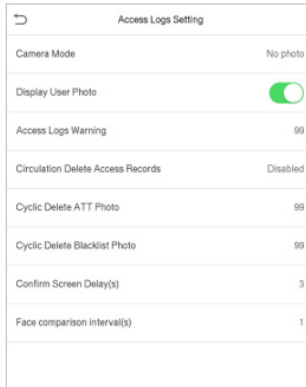
6.2 Access Logs Setting

Click Access Logs Setting on the System interface.

	Access Logs Setting
Camera Mode	No photo
Display User Photo	🟢
Access Logs Warning	99
Circulation Delete Access Records	Disabled
Cyclic Delete ATT Photo	99
Cyclic Delete Blacklist Photo	99
Confirm Screen Delay(s)	3
Face comparison interval(s)	1

Items	Descriptions
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.
Access Logs Warning	When remaining record space reaches a set value, the device will automatically display a remaining record memory warning. Users may disable the function or set a valid value between 1 and 9999.
Circulation Delete Access Records	When access records have reached full capacity, the device will automatically delete a set value of old access records. Users may disable the function or set a valid value between 1 and 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 comparison Interval (s)	To set the facial template matching time interval as needed. Valid value: 0~9 seconds.

6.3   Face Parameters

Click Face on the System interface.

Items	Descriptions
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, the lower the misjudgment rate, the higher the rejection rate, and vice versa. The default value of 75 is recommended.
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, the lower the misjudgment rate, the higher the rejection rate, and vice versa. The default value of 63 is recommended.
Face Enrollment Threshold	During face enrollment, 1:N comparison is used to determine whether the user has already registered before.
	When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered.
Face Pitch Angle	The pitch angle tolerance of a face for facial registration and comparison.
	If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.

Items	Descriptions
Face Rotation Angle	The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Minimum Face Size	Required for facial registration and comparison. If an object's size is smaller than this set value, the object will be filtered and not recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
LED Light Triggered Threshold	This value controls the on and off of the LED light. The larger the value, the more frequently the LED light will be turned on.
Motion Detection Sensitiveity	A measurement of the amount of change in a camera's field of view that qualifies as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and frequently triggered.
Live Detection	Detecting a spoof attempt by determining whether the source of a biometric sample is a live human being or a fake representation using visible light images.
Live Detection Threshold	Helping to judge whether the visible image comes from an alive body. The larger the value, the better the visible light anti-spoofing performance.
Anti-counterfeiting with NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
WDR	Wide Dynamic Range (WDR), which balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environment.
Anti-flicker Mode	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
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

Click Fingerprint on the System interface.

FRR	FAR	Recommended matching thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Items	Descriptions
1:1 Match Threshold	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 Match Threshold	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 Times	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.

6.5 Palm Parameters
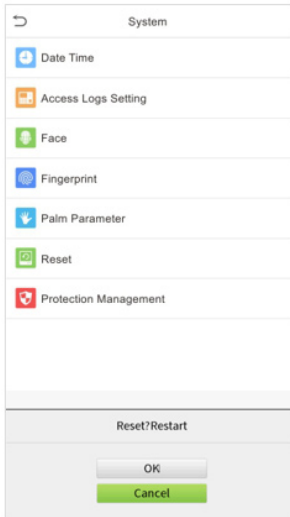
Click Palm on the System interface.
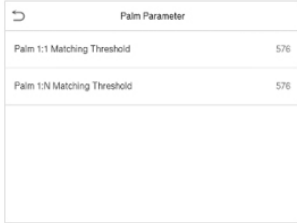
Items	Descriptions
Palm 1:1 Matching Threshold	Under 1:1 Verification Method, only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.
Palm 1:N Matching Threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value can the verification succeed.

Palm Parameter	
Palm 1:1 Matching Threshold	576
Palm 1:N Matching Threshold	576

6.6 Factory Reset

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

Click Reset on the System interface.

System
Date Time
Access Logs Setting
Face
Fingerprint
Palm Parameter
Reset
Protection Management
Reset?Restart
OK
Cancel

Click OK to reset.

7   Personalize Settings

You may customize interface settings, audio and bell.

Click Personalize on the main menu interface.

7.1   Interface Settings

You can customize the display style of the main interface.

Click User Interface on the Personalize interface.

User 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
Main Screen Style	Style 1

Items	Descriptions
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.
dle 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

Click Voice on the Personalize interface.
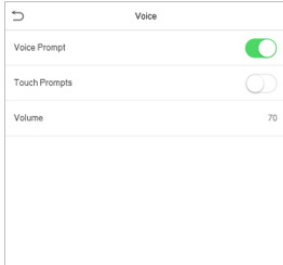
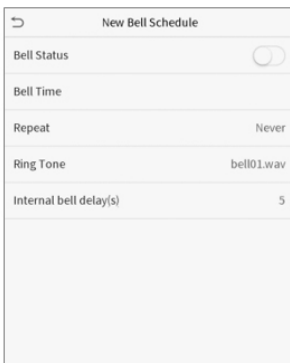| Items	Descriptions
Voice Prompt	Select whether to enable voice prompts during operating.
Touch Prompt	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0-100.

7.3 Bell Schedules

Click Bell Schedules on the Personalize interface.

■ Add a bell

Click New Bell Schedule to enter the adding interface:

Back to the Bell Schedules interface, click All Bell Schedules to view the newly added bell.

Items	Descriptions
Bell Status	Set whether to enable the bell status.
Bell Time	At this time of day, the device automatically rings the bell.
Repeat	Set the repetition cycle of the bell.
Ring Tone	Select a ring tone.
Internal bell delay(s)	Set the duration of the internal bell. Valid values range from 1 to 999 seconds.

■ **Edit a bell**

On the All Bell Schedules interface, tap the bell to be edited.

Click Edit, the editing method is the same as the operations of adding a bell.
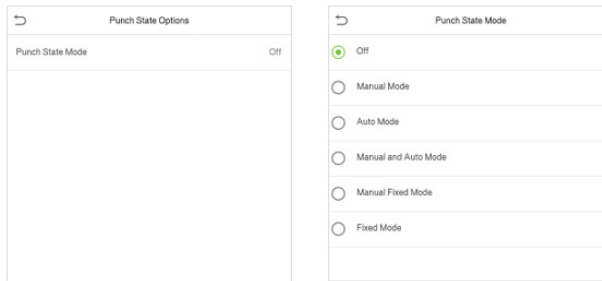
■ **Delete a bell**

On the All Bell Schedules interface, tap the bell to be deleted.

Tap Delete and select [Yes] to delete the bell.

7.4   Punch States Options

Click Punch States Options on the Personalize interface.

Items	Descriptions
Punch State Mode	Select a punch state mode, which can be:
	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.
	Manal 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.

## 7.5 Shortcut Keys Mappings

Users may define shortcuts as attendance status or functional keys. On the main interface, when the shortcut keys are pressed, the corresponding attendance status or function interface will quickly display.

Click Shortcut Key Mappings on the Personalize interface.

| ⊃	Shortcut Key Mappings
F1	Check-In
F2	Check-Out
F3	Break-Out
F4	Break-In
F5	Overtime-In
F6	Overtime-Out

8   Delete Management

Click Delete Data on the Data Mgt. interface.
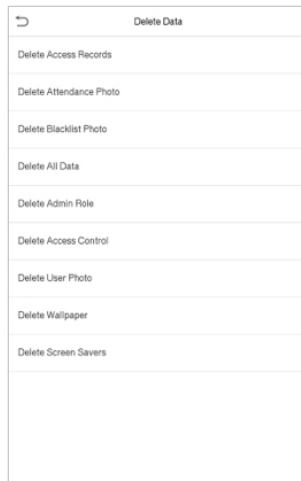
| Items	Descriptions
Delete Access Records	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blacklist Photo	To delete the photos taken during verifications which are failed.
Delete All Data	To delete information and attendance logs/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.
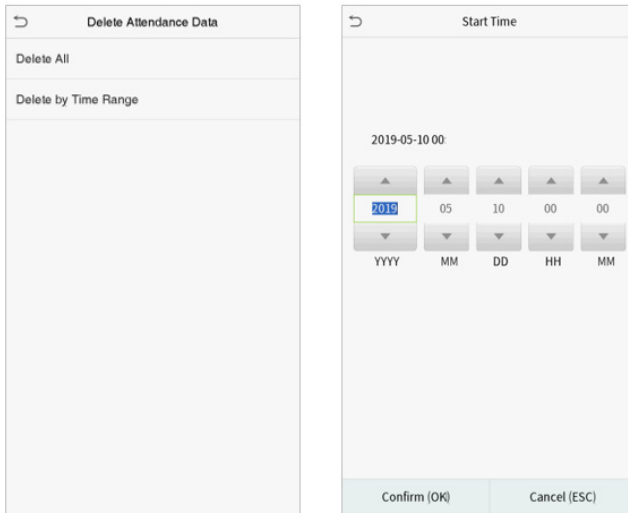
Select Delete by Time Range. Set the time range and click OK.

9   Access Control

Access Control is used to set the schedule of door opening, locks control and other parameters settings related to access control.

Click Access Control on the main menu interface.
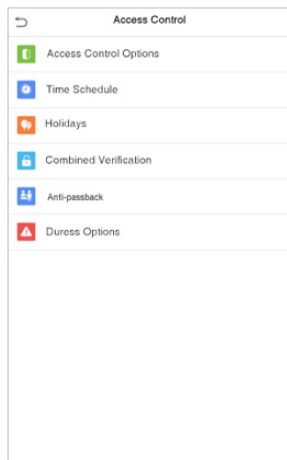
To gain access, the registered user must meet the following conditions:

1. The current door unlock time should be within any valid time zone of the user time period.

2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

   In default settings, new users are allocated into the first group with the default group time zone and access combo as "1" and set in unlocking state.

9.1 Access Control Options

To set the parameters of the control lock of the terminal and related equipment. Click Access Control Options on the Access Control interface.
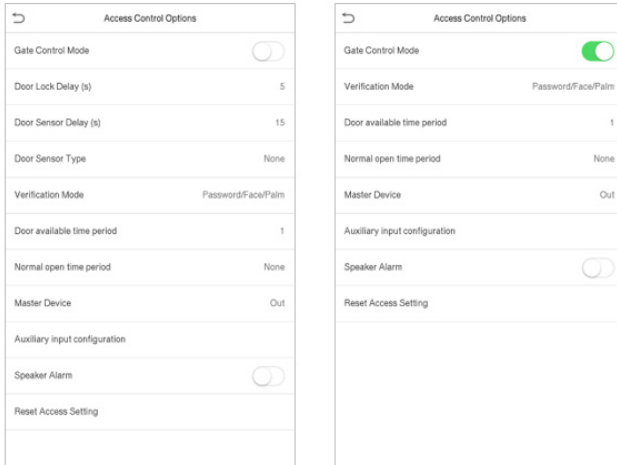
Items	Descriptions
GateControl Mode	Whether to turn on the gate control mode or not, when set to ON, on this interface will remove Door lock relay, Door sensor relay and Door sensor type function.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be unlock. Valid value: 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.
Verification Mode	The supported verification mode includes password/face, User ID only, password, face only, and face + password.
Door available time period	To set time period for door, so that the door is available only during this.

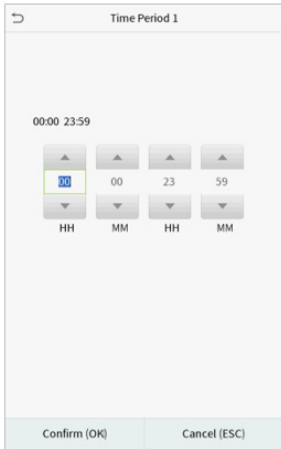| Items	Descriptions
Normal open time Period	Scheduled time period for "Normal Open" mode, so that the door is always unlocked during this period.
Master Device	When setting up the master and slave, the status of the master can be set to exit on enter. Exit: The record verified on the host is the exit record. Enter: The record verified on the host is the entry record.
Auxiliary input configuration	Set the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
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.
Reset Access Setting	The restored access control parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

9.2 Time Schedule

The entire system can define up to 50 time rules. Each time rule represents ten time zones, i.e. one week and 3 holidays, and each time zone is a valid time period within 24 hours per day. You may set a maximum of 3 time periods for every time zone. The relationship among these time periods is "or". When the verification time falls in any one of these time periods, the verification is valid. Each time period format of the time zone: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

Click Time Rule Setting on the Access Control interface.

1. Click the grey box to input a time zone to search. Enter the number of time zone (maximum: 50 zones).

2. Click the date on which time zone settings is required. Enter the starting and ending time, and then press OK.

Note:

1. When the ending time is earlier than the starting time, such as 23:57~23:56, it indicates that access is prohibited all day; when the ending time is later than the starting time, such as 00:00~23:59, it indicates that the interval is valid.

2. The effective time period to unlock the door: open all day (00:00~23:59) or when the ending time is later than the starting time, such as 08:00~23:59.

3. The default time zone 1 indicates that door is open all day long.

9.3   Holiday Settings

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

Click Holidays on the Access Control interface.
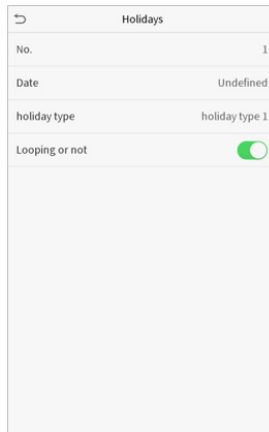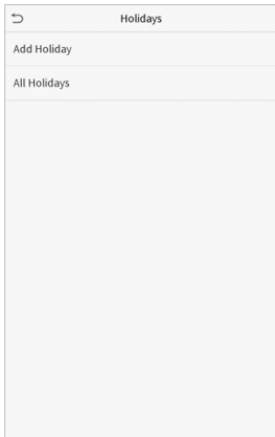
■ **Add a New Holiday**
Click Add Holiday on the Holidays interface and set the holiday parameters.

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

■ **Delete a Holiday**
On the Holidays interface, select a holiday item to be deleted and click Delete. Click OK to confirm deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

9.4 Combined Verification Settings

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

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

Click Combined Verification on the Access Control interface.

	Combined Verification
1	01 02 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00
6	00 00 00 00 00
7	00 00 00 00 00
8	00 00 00 00 00
9	00 00 00 00 00
10	00 00 00 00 00

Click the door-unlocking combination to be set. Click the up and down arrows to input the combination number, then press OK.

Examples:
The door-unlocking combination 1 is set as (01 03 05 06 08), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, access control group 1 (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.

The door-unlocking combination 2 is set as (02 02 04 04 07), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.

The door-unlocking combination 3 is set as (09 09 09 09 09), indicating that there are 5 people in this combination; all of which are from AC group 9.

The door-unlocking combination 4 is set as (03 05 08 00 00), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

Delete a door-unlocking combination
Set all group number as 0 if you want to delete door-unlocking combinations.
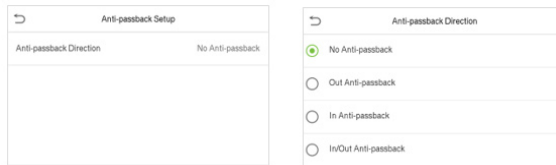
9.5　Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in security problem. So, to avoid this situation, Anti-Passback option is developed. Once it is enabled, the check-in record must match with check- out record so as to open the door.
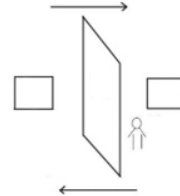
This function requires two devices to work together: one is installed inside the door (master device), the other

one is installed outside the door (slave device). The two

devices communicate via Wiegand signal. The Wiegand format and Output type (User ID / Badge Number) adopted by the master device and slave device must be consistent.

Click Anti-passback Setup on the Access Control interface.

Items	Descriptions
Anti-passback direction	No Anti-passback: Anti-passback function is disabled, which means successful verification through either master device or slave device can unlock the door. Attendance state is not saved.
	Out Anti-passback: After a user checks out, only if the last record is a check-in record, the user can check out again; otherwise, the alarm will be triggered. However, the user can check in freely.
	In Anti-passback: After a user checks in, only if the last record is a check-out record, the user can check in again; otherwise, the alarm will be triggered. However, the user can check out freely.
	In/Out Anti-passsback: After a user checks in/out, only if the last record is a check-out record, the user can check in again; or a check-in record, the user can check out again; otherwise, the alarm will be triggered.

9.6 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is under coercion during authentication with such method, the device will unlock the door as usual, but at the same time a signal will be sent to trigger the alarm.

Click Duress Options on the Access Control interface.
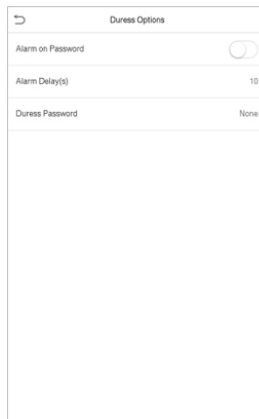
Items	Descriptions
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
Duress Password	Set the 6-digit duress password. When the user enters this duress password for verification, an alarm signal will be generated.

10 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.

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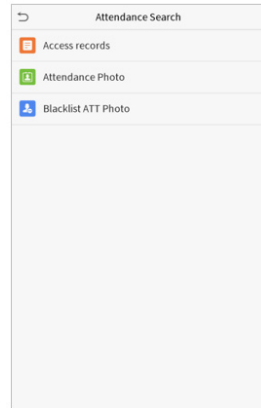
1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.

2. Select the time range in which the records you want to search for.
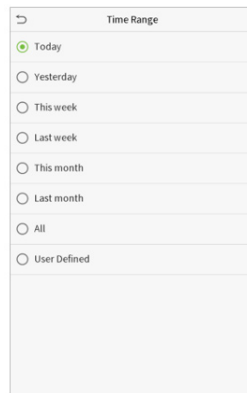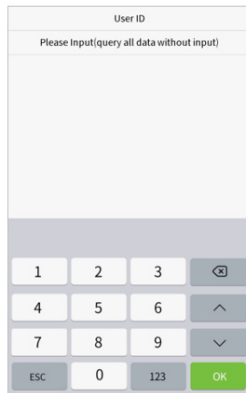
3. The record search succeeds. Click the record in green to view its details.
4. The below figure shows the details of the selected record.

11 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, audio, camera and real-time clock (RTC).

Click Autotest on the main menu interface.
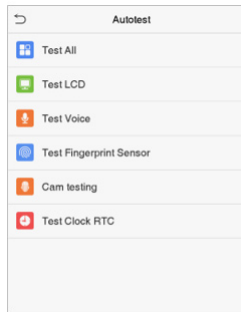
Items	Descriptions
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test 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.
Camera testing	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

12 System Information

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

Click System Info on the main menu interface.
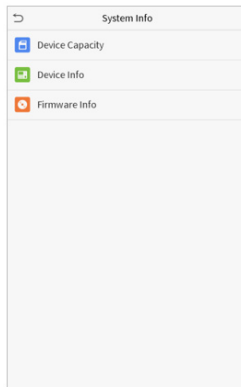
Items	Descriptions
Device Capacity	Displays the current device's user storage, palm, password and face storage, administrators, access records, attendance and blacklist photos, and user photos.
Device Info	Displays the device's name, serial number, MAC address, face algorithm version information, platform information, and manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.

www.timeteccloud.com

13   Connect to Software

13.1   Connect to AWDMS/ Ingress Software

Download this file from this links below:

- **Ingress version 4.0.1.9** (with AWDMS support)

  Ingress Server: *https://s3.amazonaws.com/files.fingertec.com/Software+Releases/In-gress/2020/4.0.1.9/Ingress+Server+(MySQL).zip*

  Ingress Client: *https://s3.amazonaws.com/files.fingertec.com/Software+Releases/In-gress/2020/4.0.1.9/Ingress+(MySQL).zip*

- **ADWMS version 3.1**

  https://s3.amazonaws.com/files.fingertec.com/Software+Releases/AWDMS/AWDMS3.1.zip
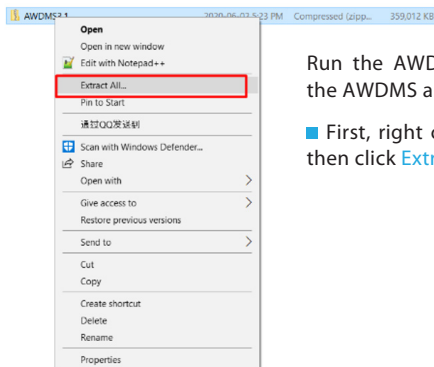
- **ADWMS Setup Tool**

  https://s3.amazonaws.com/files.fingertec.com/Software+Releases/AWDMS/AWDMS+Setup+Tool.zip

13.2   Software Quick Installation

Both Ingress and AWDMS MUST BE INSTALLED on the same PC. First, install the Ingress Server and install the AWDMS after. For Ingress installation, please refer to the Ingress User Manual which can be found at *https://www.fingertec.com/cus-tomer/download/postsales/SUM-Ingress-E.pdf*.

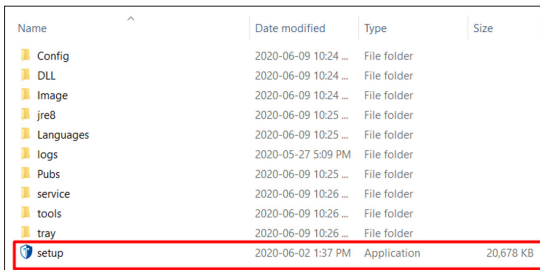Kindly ensure the firewall and Antivirus software on the PC have been switched off before proceeding.

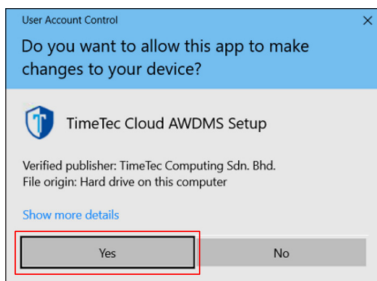Run the AWDMS setup tool after installing the AWDMS and reboot your PC.

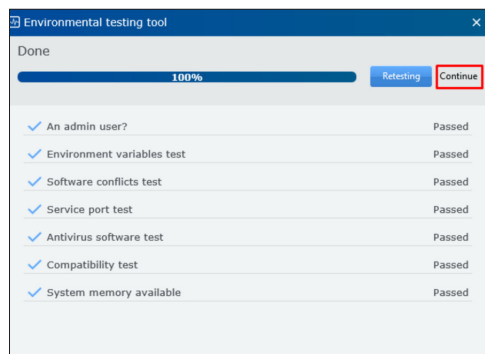■ First, right click on the AWDMS3.1.zip file, then click Extract All
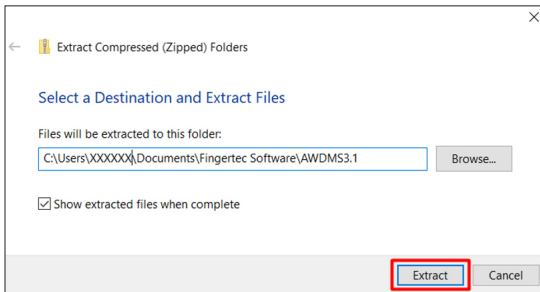
Click Extract

**Go to the AWDMS3.1 folder. Look for setup.exe and click on setup.exe.**

Once the User Account Control permission is prompted, select Yes to continue.

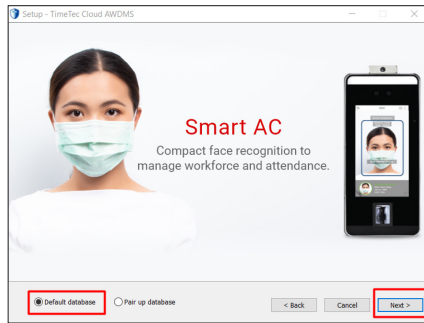**The AWDMS setup will run an environment testing prior to the actual installation, click Continue when the test is completed.**

■ Click Next to continue.

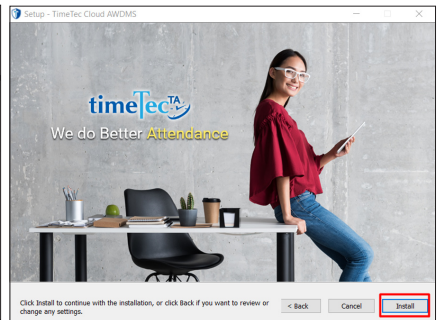■ End-user Software License Agreement. Select "I accept the agreement", then click Next.
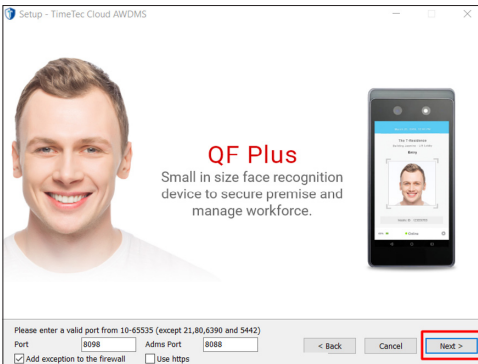
■ Leave the Port and ADMS Port in default mode, click Next.

■ Click Next.

■ Click Next.

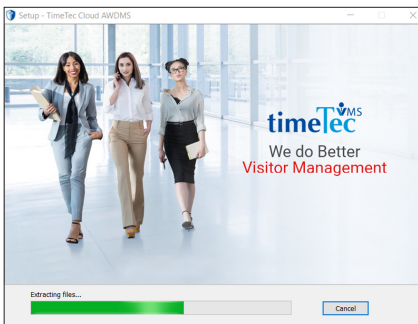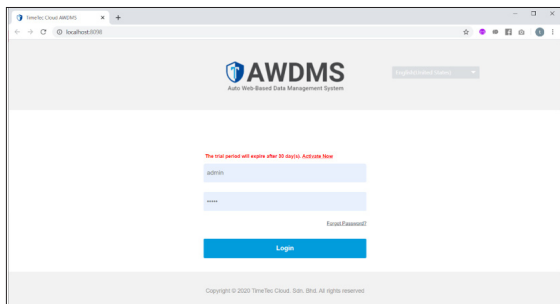■ Set your Backup document path. Then, click Next

■ Click Install button.

■ The installation is now in progress.

■ Click Finish to restart the computer.

■ Once this icon appears on the desktop, double tap on the "TimeTec Cloud AWDMS" icon to run the AWDMS.

■ The ADWMS login screen will be launched in the web browser. The default login username is "admin" and default password is "admin".

13.3 Configure AWDMS Setup Tool

By default, AWDMS will be installed with a Postgresql Server. However, it is recommended to switch to MySQL for better support. In order to switch to MySQL, please run the AWDMS setup tool after the screen below appears.

■ Right click on the AWDMS Setup Tool.zip, click Extract All.
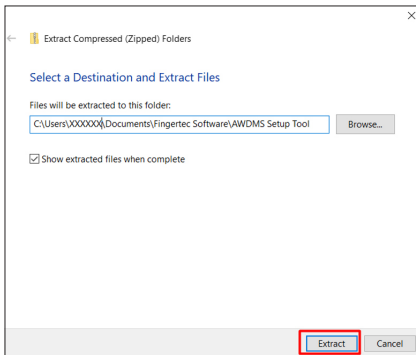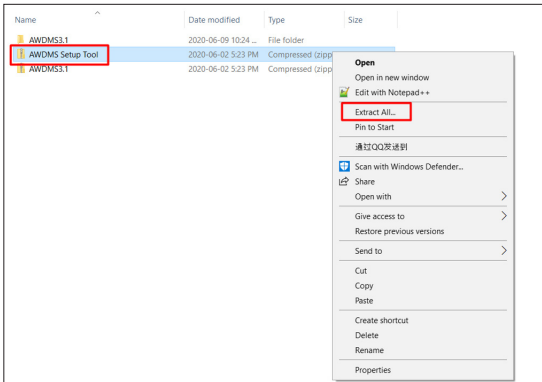
■ Click Extract

■ Go the folder where AWDMS Setup Tool is located. Click AWDMSSetup. exe.
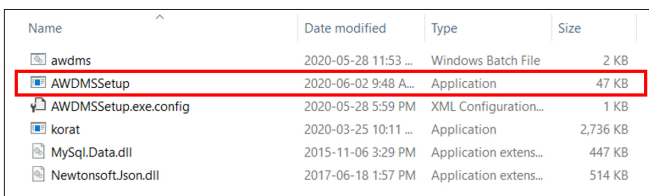
■ Press any key to begin the AWDMS setup. Your computer screen might flash for a few times. Click "Yes" at the popup dialog box to continue. Once completed, press any key to exit this window.

```
Install Path : C:\Program Files\BioSecurity
Please any key to start TimeTec Cloud AWDMS setup

 Step 1 Completed
Step 2 Completed
Step 3 Completed
Step 4 Completed
TimeTec Cloud AWDMS setup completed.


Please any key to exit...
```
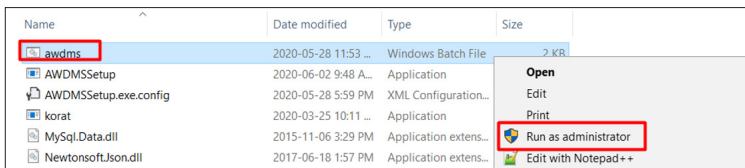
■ Right click on the awdms.bat, click "Run as administrator".

Name	Date modified	Type	Size
awdms	2020-05-28 11:53 ...	Windows Batch File	2 KB
AWDMSSetup	2020-06-02 9:48 A...	Application	
AWDMSSetup.exe.config	2020-05-28 5:59 PM	XML Configuration...	
korat	2020-03-25 10:11 ...	Application	
MySql.Data.dll	2015-11-06 3:29 PM	Application extens...	
Newtonsoft.Json.dll	2017-06-18 1:57 PM	Application extens...	

Open
Edit
Print
Run as administrator
Edit with Notepad++

■ Press any key to start running the batch file. Once completed, press any key to exit this window.

```
**************************************************************
********  This batch file is use to complete TimeTec Cloud AWDMS Setup  ********
**************************************************************

IMPORTANT!!!
Please make sure you run AWDMSSetup.exe before start this bat file
Press any key to start now

Begin Step 1...
Begin Step 2...
Begin Step 3...
Begin Step 4...
Setup completed

Press any key to exit
```

13.4 Configure AWDMS in Ingress Software

By now, you should have your AWDMS setup completed. Now, you may proceed to Ingress to configure the AWDMS.

■ Login to Ingress, go to System Settings > AWDMS Configuration

■ Key in the AWDMS server IP, Port Number, Login Username and Password. Since AWDMS and Ingress are running on the same PC, thus, the server IP is 127.0.0.1, the default port is 8098. The default AWDMS login ID is "admin" and default password is "admin".

■ After keying in the AWDMS information, click on the Test Connection button and check if the Ingress is able to connect to the AWDMS. A popup dialog box will be prompted with "Connected To Server" if successful. Click Apply once it is done.
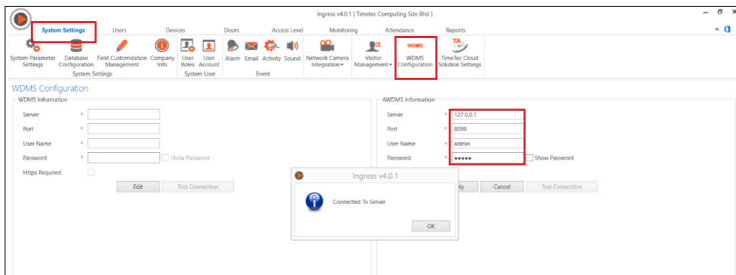
■ You may now add devices to the Ingress software by clicking the Add Device. Name the device and key in the device's serial number. Select online device activation, then click Add.
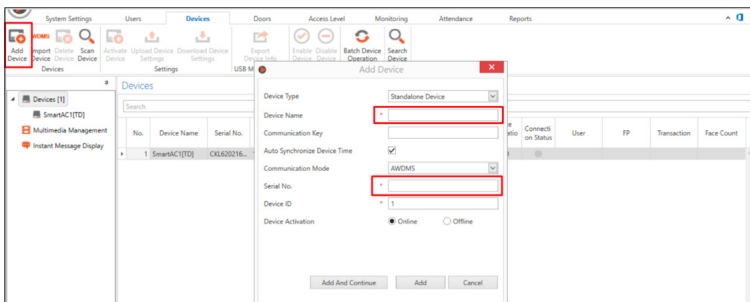
■ After adding the device, it will appear in the Devices list.

The AWDMS installation is now completed. You may now launch the software and start pulling or updating data from the AWDMS devices.

Appendix

Requirements of Live Collection and Registration of Visible Light Face Images

1. It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.

2. Do not shoot towards outdoor light sources like door or window or other strong light sources.

3. Dark-color apparels which are different from the background color are recommended for registration.

4. Please show your face and forehead, and do not cover your face and eyebrows with your hair.

5. It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without.

6. Do not wear accessories like scarf or mask that may cover your mouth or chin.

7. Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.

8. Do not include more than one face in the capturing area.

9. 50cm - 80cm is recommended for capturing distance adjustable subject to body height.
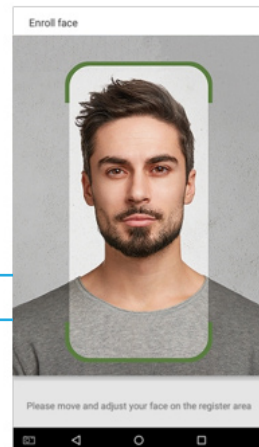
Image1: *Face Capture Area*

Requirements for Visible Light Digital Face Image Data

Digital photo should be straightly edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

■ **Eye Distance**
200 pixels or above are recommended with no less than 115 pixels of distance.

■ **Facial Expression**
Plain face or smile with eyes naturally open are recommended.

■ **Gesture and Angel**
Horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

■ **Accessories**
Masks and colored eyeglasses are not allowed. The frame of the eyeglasses should not shield eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without.

■ **Face**
Complete face with clear contour, real scale, evenly distributed light, and no shadow.

■ **Image Format**
Should be in BMP, JPG or JPEG.

■ **Data Requirement**
Should comply with the following requirements:

1. White background with dark-colored apparel.
2. 24bit true color mode.
3. JPG format compressed image with not more than 20kb size.
4. Definition rate between 358 x 441 to 1080 x 1920.
5. The vertical scale of head and body should be 2:1.
6. The photo should include the captured person's shoulders at the same horizontal level.
7. The captured person should be eyes-open and with clearly seen iris.
8. Plain face or smile is preferred, showing teeth is not preferred.
9. The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appro priate contrast and lightness level.

Right to Privacy

TimeTec thank you for opting this robust biometric recognition product. At TimeTec, we care about privacy. Being one of the renowned providers of core biometric recognition technologies and cloud solutions, we are striving to serve premium qualities of both existing and new products and services, and make compliance to all privacy laws of each country in which our products are sold.

If you have a privacy concern, complaint, or questions, please contact us.