Function Description

Function Name		Description
Enable Domain Name	**Server Address**	Once 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.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

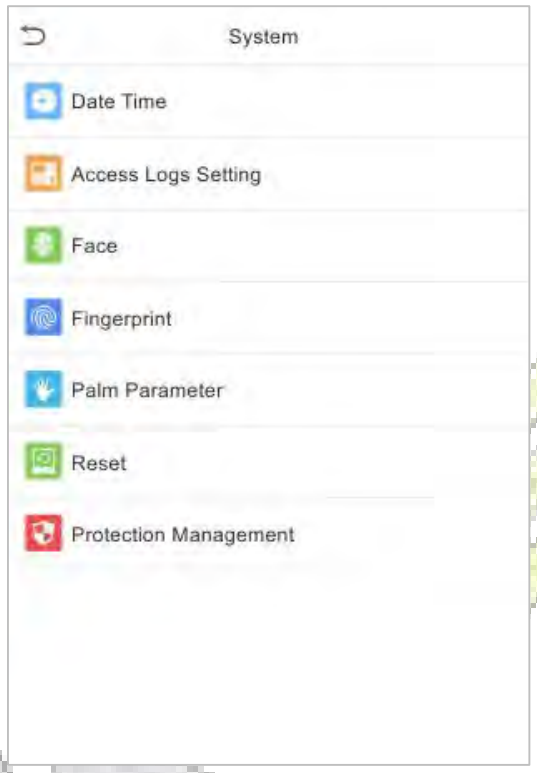
ZKTeco

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

8 System Settings

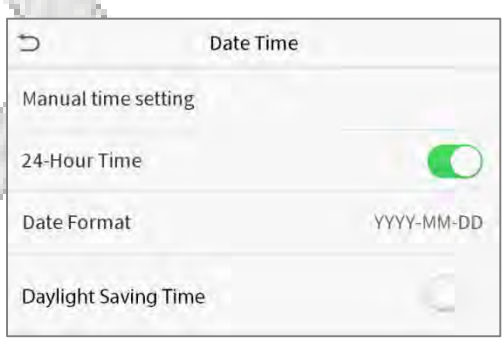
Set related system parameters to optimize the performance of the device.

Tap **System** on the **Main Menu** interface to set the related system parameters so as to optimize the performance of the device.



8.1 Date and Time

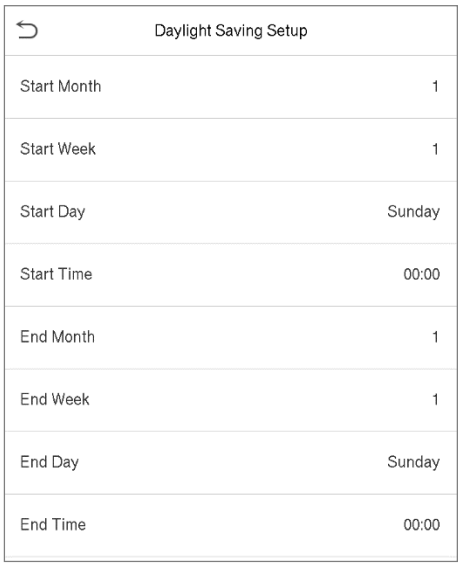
Tap **Date Time** on the **System** interface to set the date and time.



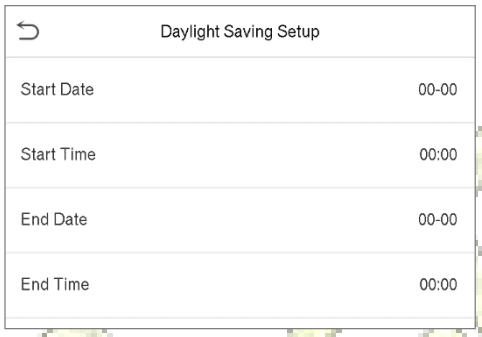
- Tap **Manual time setting** to manually set date and time and tap **Confirm** to save.
- Tap **24-Hour Time** to enable or disable this format. If enabled, then select the **Date Format** to set the date format.
- ★ Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap **Daylight Saving Mode** to select a daylight-saving mode and then tap **Daylight Saving Setup** to set the switch

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

time.



Week mode



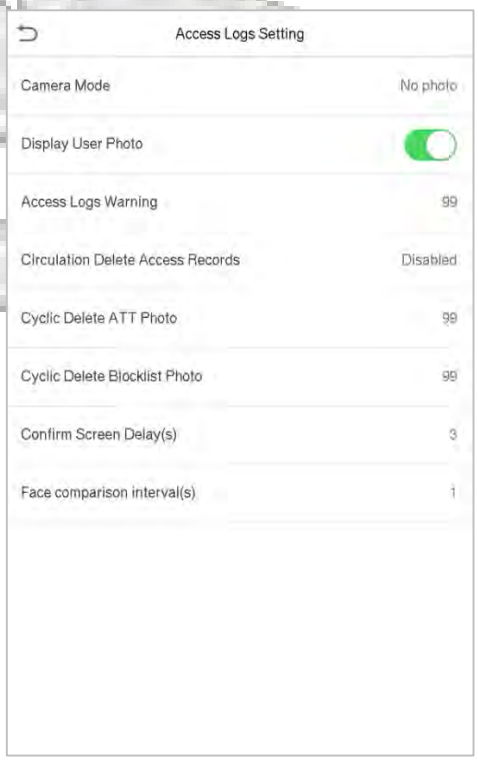
Date mode

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

NOTE: For example, 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.

8.2 Access Logs Setting

Click **Access Logs Setting** on the System interface.



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

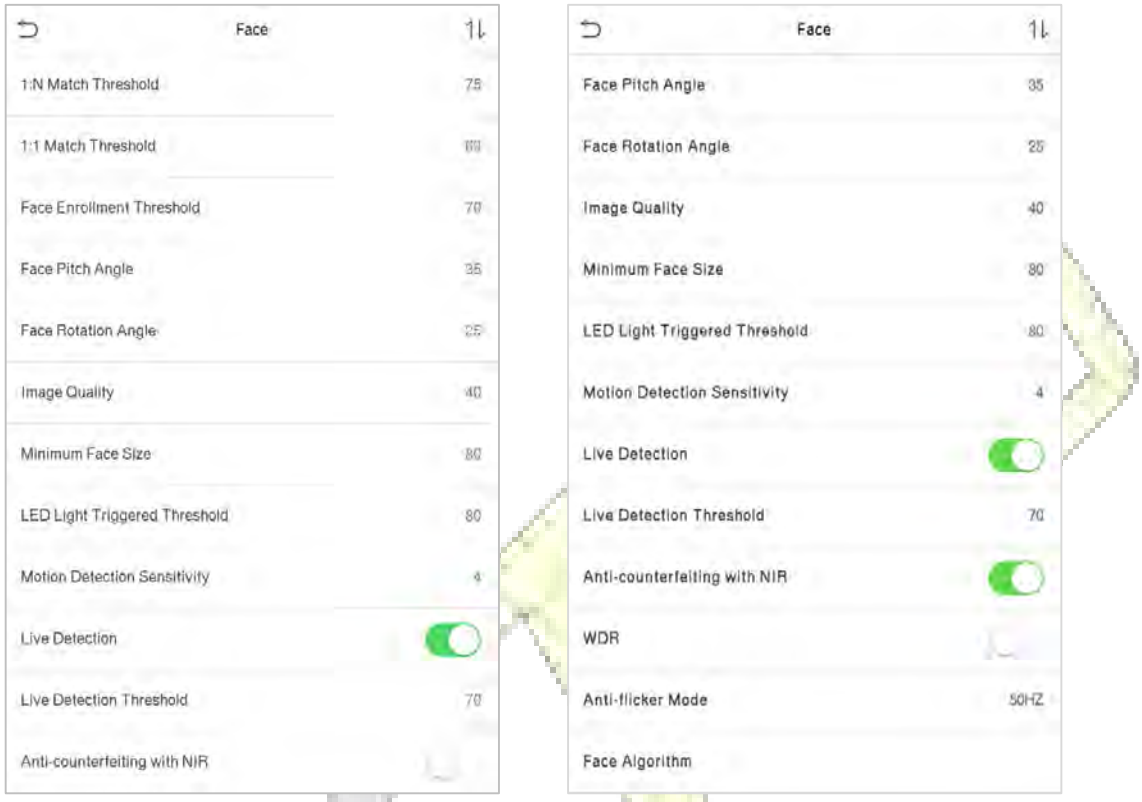
Function Description

Function Name	Description
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 will be taken and saved only for each failed verification.
Display User Photo	Whether to display the user photo when the user passes the verification.
Access Logs Warning	When the record space of the attendance access reaches the maximum threshold value, the device will automatically display the memory space 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 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 of old attendance photos. Users may disable the function or set a valid value between 1 and 99.
Cyclic Delete Blocklist Photo	When block listed photos have reached full capacity, the device will automatically delete a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Confirm Screen Delay(s)	The time length of the message of successful verification displays. Valid value: 1~9 seconds.
Face comparison Interval (s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

8.3 Face Parameters

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



FRR	FAR	Recommended Matching Thresholds	
		1:N	1:1
High	Low	85	80
Medium	Medium	82	75
Low	High	80	70

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Function Description

Function Name	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, the lower the misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 75.
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 user's 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 misjudgement rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.
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.
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 the minimum size of the captured figure is smaller than this set value, then it will be filtered off 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.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

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 Sensitivity	It is to set the value for the amount of change in a camera's field of view, which is known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and the motion detection frequently triggered.
Live Detection	Detecting the spoof attempt using visible light images to determine if the provided biometric source sample is really a person (a live human being) or false representation.
Live Detection Threshold	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
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	It is used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	Facial algorithm related information and pause facial template update.
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.

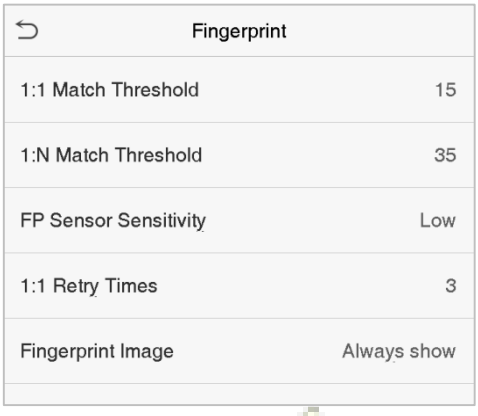
Process to modify the Face Recognition Accuracy

- On the **System** interface, tap on **Face** and then toggle to enable Anti-Spoofing using NIR to set the anti-spoofing.
- Then, on the **Main Menu**, tap **Auto-Test > Test Face** and perform the face test.
- Tap three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.
- Keep one arm distance between the device and the face, and recommended not to move the face in wide range.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

8.4 Fingerprint Parameters

Tap **Fingerprint** on the **System** interface to configure the fingerprint settings.



FRR	FAR	Recommended Matching Thresholds	
		1:N	1:1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

Function Description

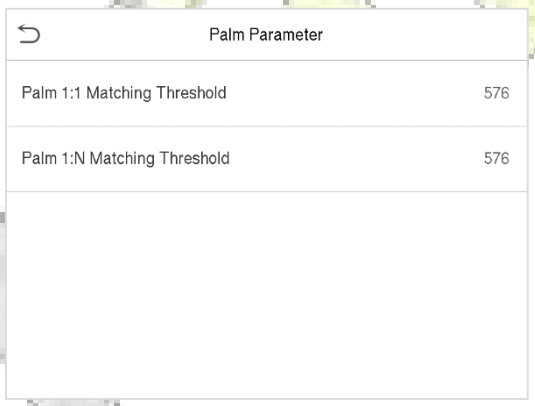
Function Name	Descriptions
1:1 Match Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID that is enrolled in the device is greater than the set value.
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	Users might forget the registered fingerprint or press the finger improperly. 1:1 Verification allows to set the retry authentication attempts for the users

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Function Name	Descriptions
	in order to reduce the process of re-entering user ID and increase the security.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: • **Show for enroll**: to display the fingerprint image on the screen only during enrollment. • **Show for match**: to display the fingerprint image on the screen only during verification. • **Always show**: to display the fingerprint image on screen during enrollment and verification. • **None**: not to display the fingerprint image.

8.5 Palm Parameters

Tap **Palm** on the **System** interface to configure the palm settings.



Function Description

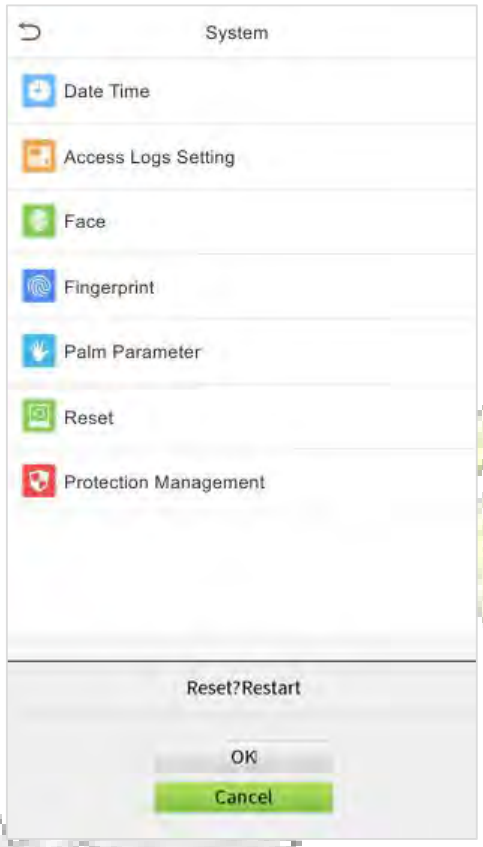
Function Name	Description
Palm 1:1 Matching Threshold	Only when the similarity between the verifying palm and the user's registered palm is greater than this value can the verification succeed.
Palm 1:N Matching Threshold	Under 1:N Verification Method, only when the similarity between the verifying palm and all registered palm is greater than this value can the verification succeed.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

8.6 Factory Reset

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

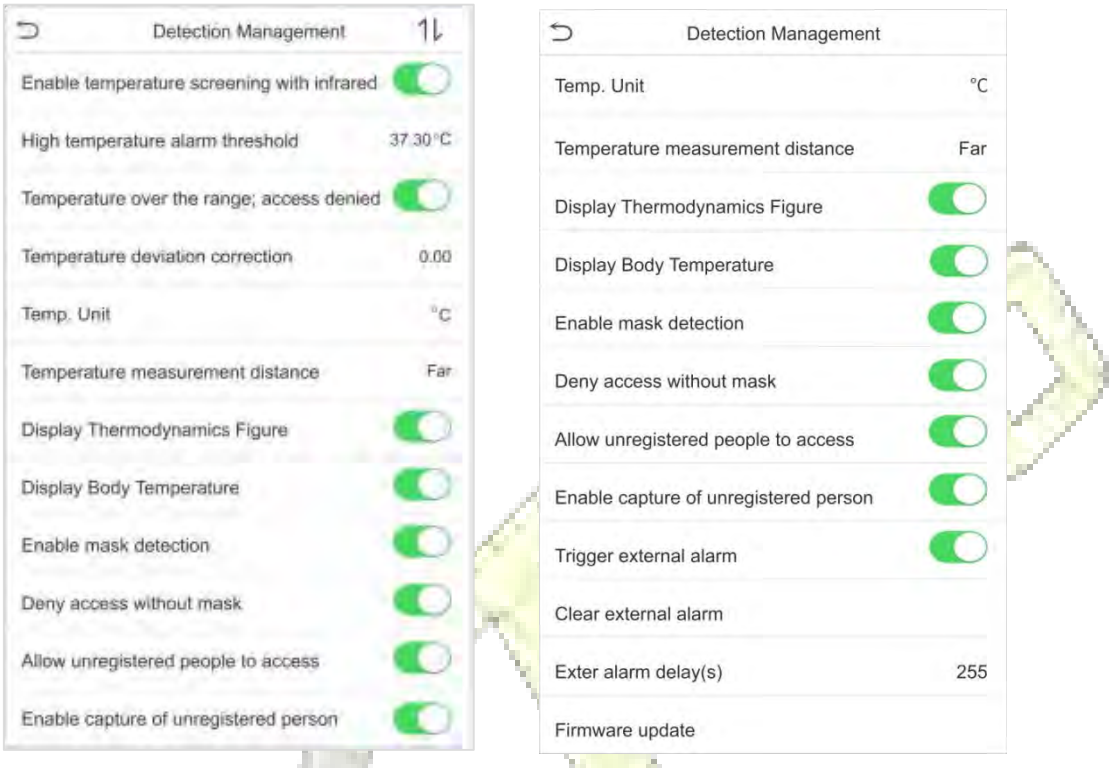
Tap **Reset** on the **System** interface and then tap **OK** to restore the default factory settings.



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

8.7 Detection Management

Click **Detection Management** on the **System** interface to configure the Detection Management settings.



Function Description

Function Name	Description
Enable temperature screening with infrared	To enable or disable the infrared temperature measurement. When this function is enabled, users must pass the temperature screening in addition to identity verification before the access is granted. To measure body temperature, user's faces must be aligned with the temperature measurement area.
High temperature alarm threshold	To set the value of the alarm threshold for high body temperature. When the temperature measured during verification is higher than the set value, the device will give a prompt and audio alarm. The default alarm threshold is 37.30°C.
Temperature over the range; access denied	When enabled, if the user's body temperature measured is above (or below) the alarm threshold, the user will not be granted access even if his/her identity is verified. When disabled, access is granted to the user if his/her identity is verified, regardless of his/her body temperature.

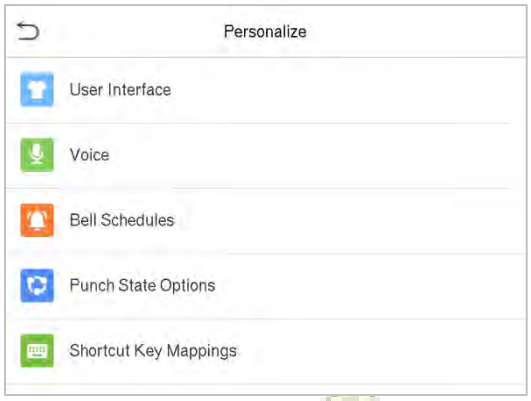
Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Temperature deviation correction	As the temperature measurement module reads a small range of variation of an observed value under unusual environments (humidity, extreme room temperature and such), the users may set the deviation value here to reflect the true temperature of the person.
Temp. Unit	The unit of body temperature can be toggled between Celsius (°C) and Fahrenheit (°F).
Temperature measurement distance	There are three modes while measuring temperature during the verification process, they are: **Near, Close** and **Far**.
Display Thermodynamics Figure	To enable or disable the display of the thermal image of a person. When enabled, the thermal image of the person is be displayed in the upper left corner of the device during the detection process.
Display Body Temperature	To enable or disable the display of body temperature. When enabled, the device will display the user's body temperature value during the verification process.
Enable mask detection	To enable or disable the mask detection function. When enabled, the device will identify whether the user is wearing a mask or not during verification.
Deny access without mask	To enable or disable the access of a person without mask. When enabled, the device will deny access of a person, if not wearing a mask.
Allow unregistered people to access	To enable or disable the access of unregistered person. When enabled, the device allows the person to enter without registration, as long as the person who passes the detection.
Enable capture of unregistered person	To enable or disable the capture photo of unregistered person. When enabled, the device will automatically capture the photo of the unregistered person, enabling this feature requires to enable **Allow unregistered people to access**.
Trigger external alarm	When enabled, if the user's temperature is higher than the set threshold value or the mask detection is enabled, but the mask is not worn by the person, it will trigger an alarm.
Clear external alarm	It clears the triggered alarm records of the device.
External alarm delay(s)	The delay (s) time for triggering an external alarm. It can be set in seconds. Users may disable the function or set a value between 1 to 255.
Firmware update	Choose whether to update the thermal imaging temperature detection module software version.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

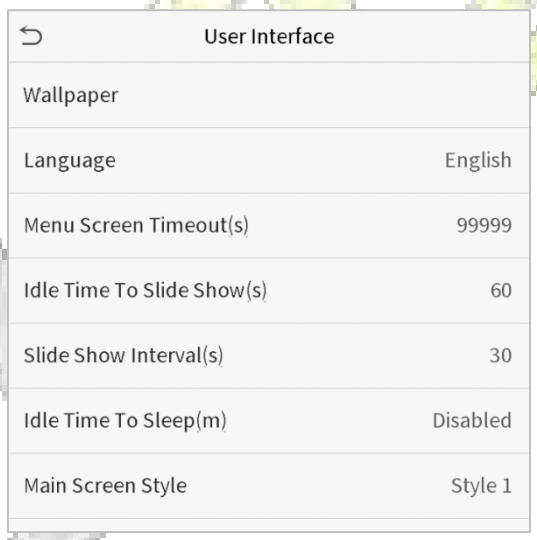
9 Personalize Settings

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



9.1 Interface Settings

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



Function Description

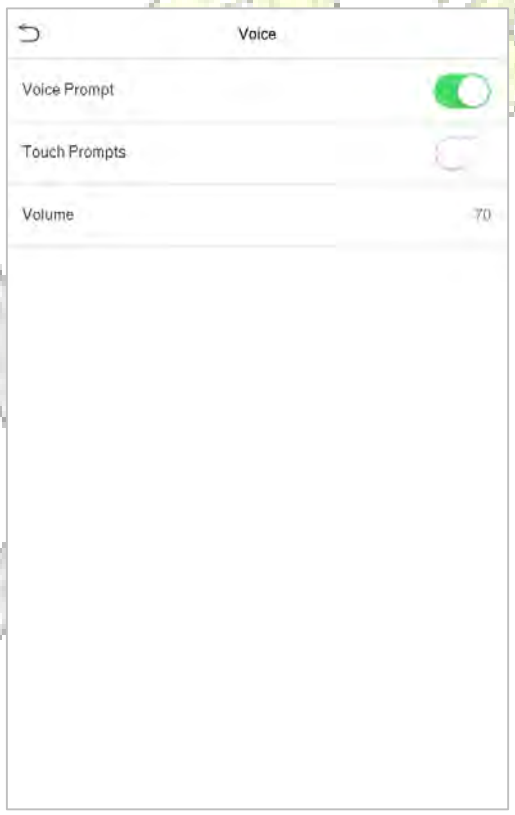
Function Name	Description
Wallpaper	The main screen wallpaper can be selected according to the user preference.
Language	Select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface.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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. Press any key or finger to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	The main screen style can be selected according to the user preference.

9.2 Voice Settings

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



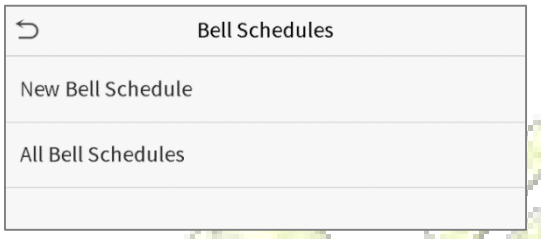
Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Function Description

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

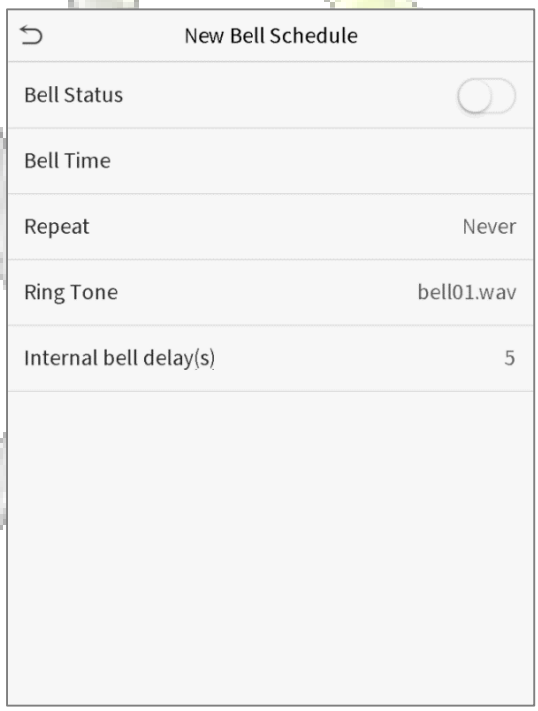
9.3 Bell Schedules

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



New Bell Schedule

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



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Function Description

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

All Bell Schedules

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

Edit the scheduled bell

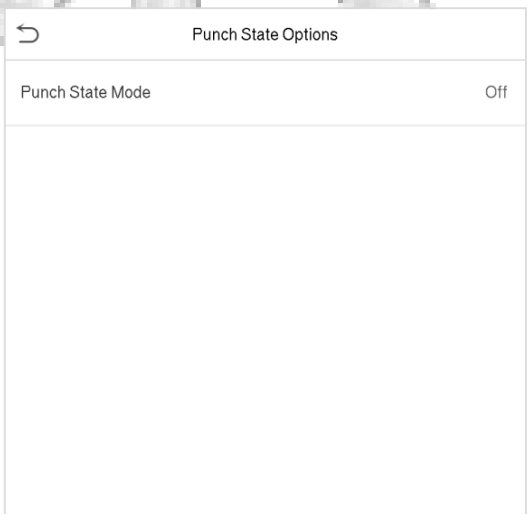
On the **All Bell Schedules** interface, tap on the required bell schedule, and tap **Edit** to edit the selected bell schedule. The editing method is the same as the operations of adding a new bell schedule.

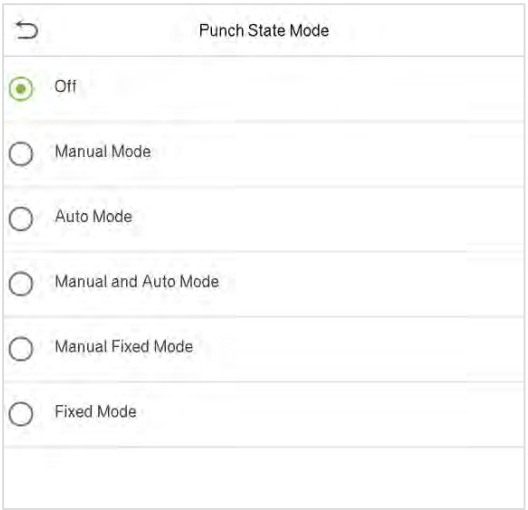
Delete a bell

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

9.4 Punch States Options

Tap **Punch States Options** on the **Personalize** interface to configure the punch state settings.





Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Function Description

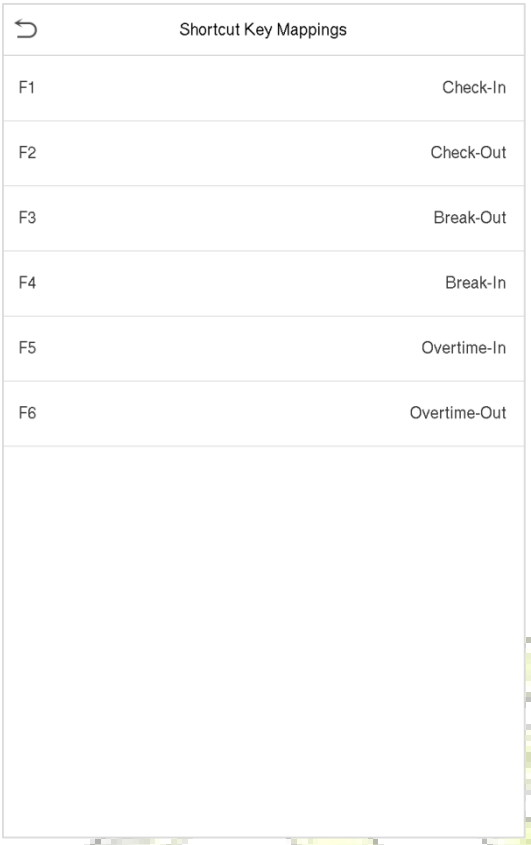
Function Name	Description
Punch State Mode	**Off:** Disable the punch state function. Therefore, the punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after **Punch State Timeout**. **Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. **Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key. **Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until being manually switched again. **Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by pressing any other keys.

9.5 Shortcut Key Mappings

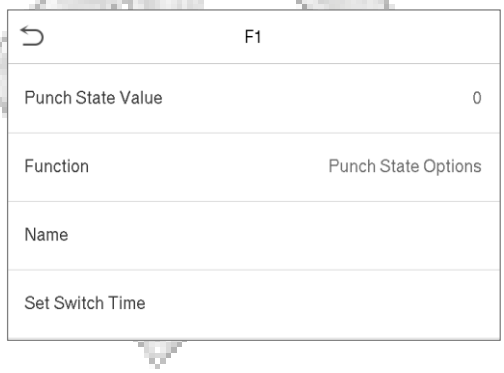
Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are pressed, the corresponding attendance status or the function interface will be displayed directly.

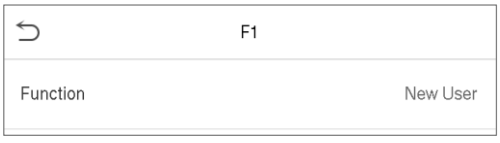
Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.



- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (**that is "F1"**)** interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.



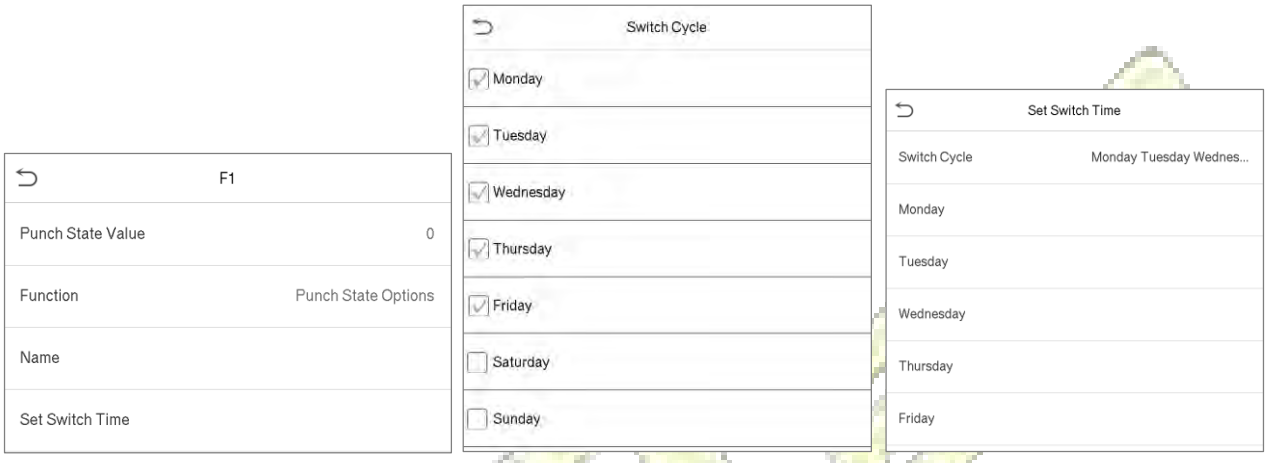


- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name and switch time.

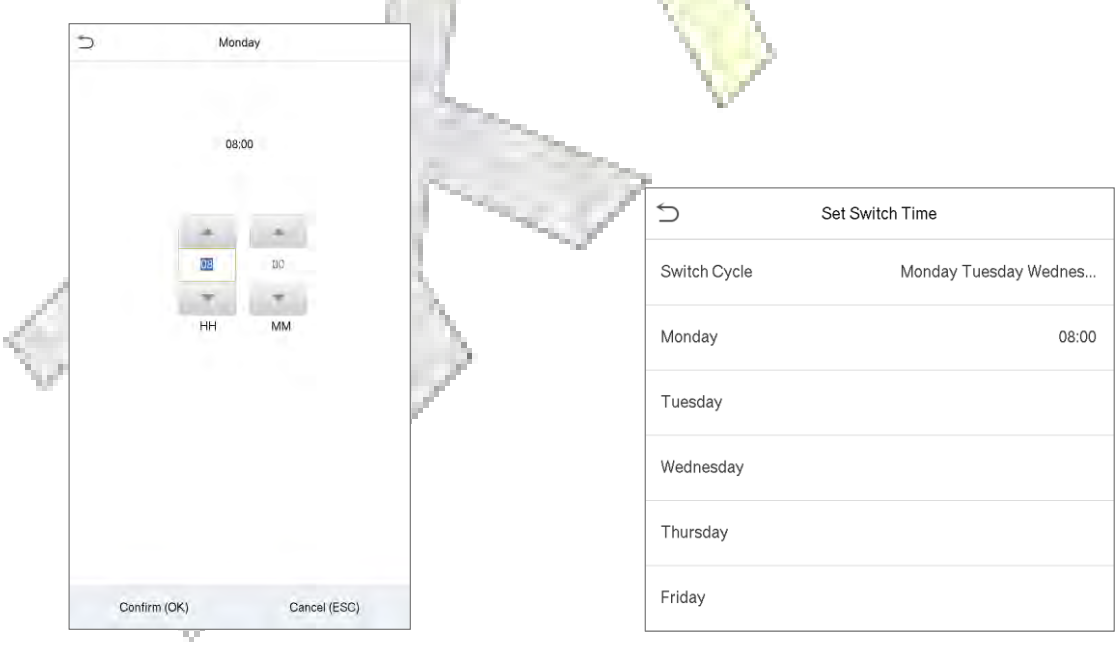
Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Set the switch time

- The switch time is set in accordance with the punch state options.
- When the **punch state mode** is set to **auto mode**, the switch time should be set.
- On the **Shortcut Key** interface, tap **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday etc.) as shown in the image below.



- Once the Switch cycle is selected, set the switch time for each day and tap **OK** to confirm, as shown in the image below.



Note: When the function is set to Undefined, the device will not enable the punch state key.

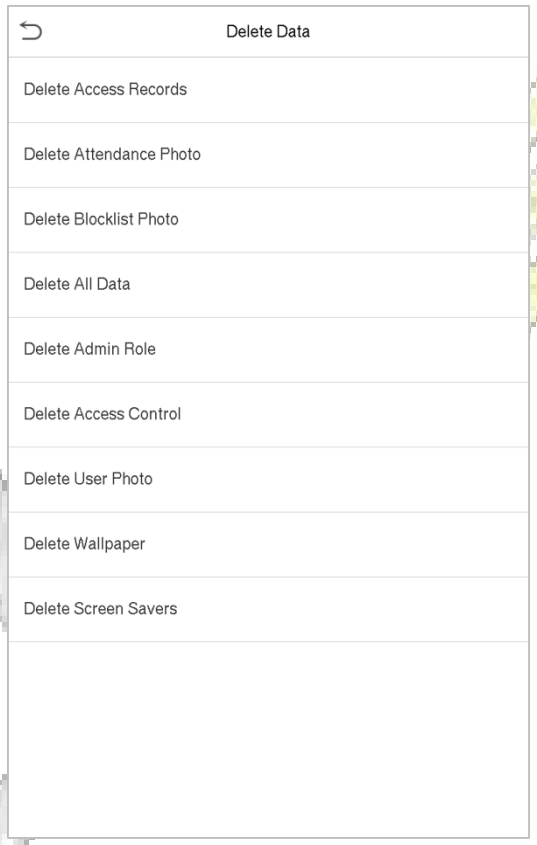
Copyright©2020 ZKTECO CO., LTD. All rights reserved.

10 Data Management

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

10.1 Delete Data

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

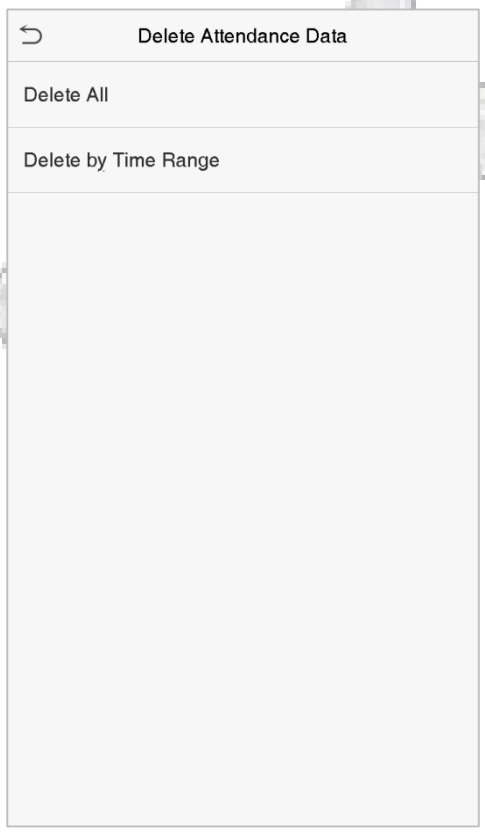


Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Function Description

Function Name	Description
Delete Access Records	To delete attendance data/access records conditionally.
Delete Attendance Photo	To delete attendance photos of designated personnel.
Delete Blocklist Photo	To delete the photos taken during failed verifications.
Delete All Data	To delete information and attendance logs/access records of all registered users.
Delete Admin Role	To remove all 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.

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



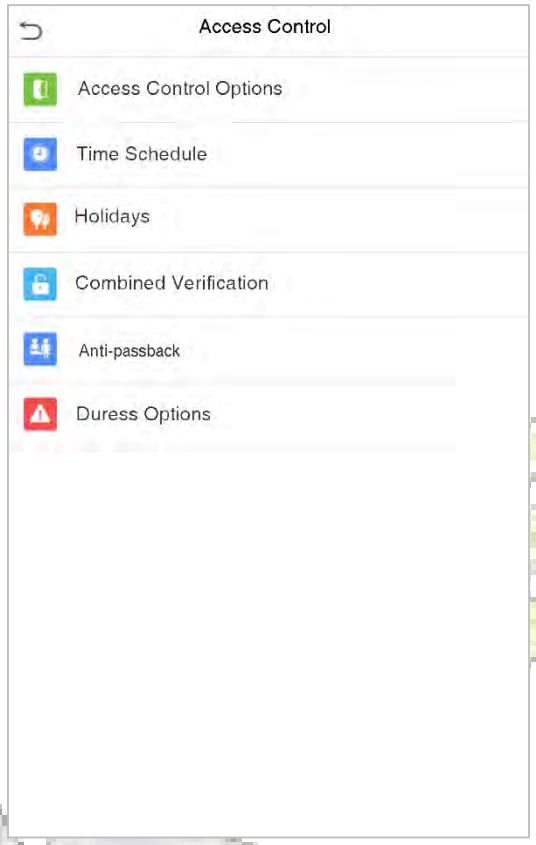
Select Delete by Time Range.

Set the time range and click **OK**.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

11 Access Control

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



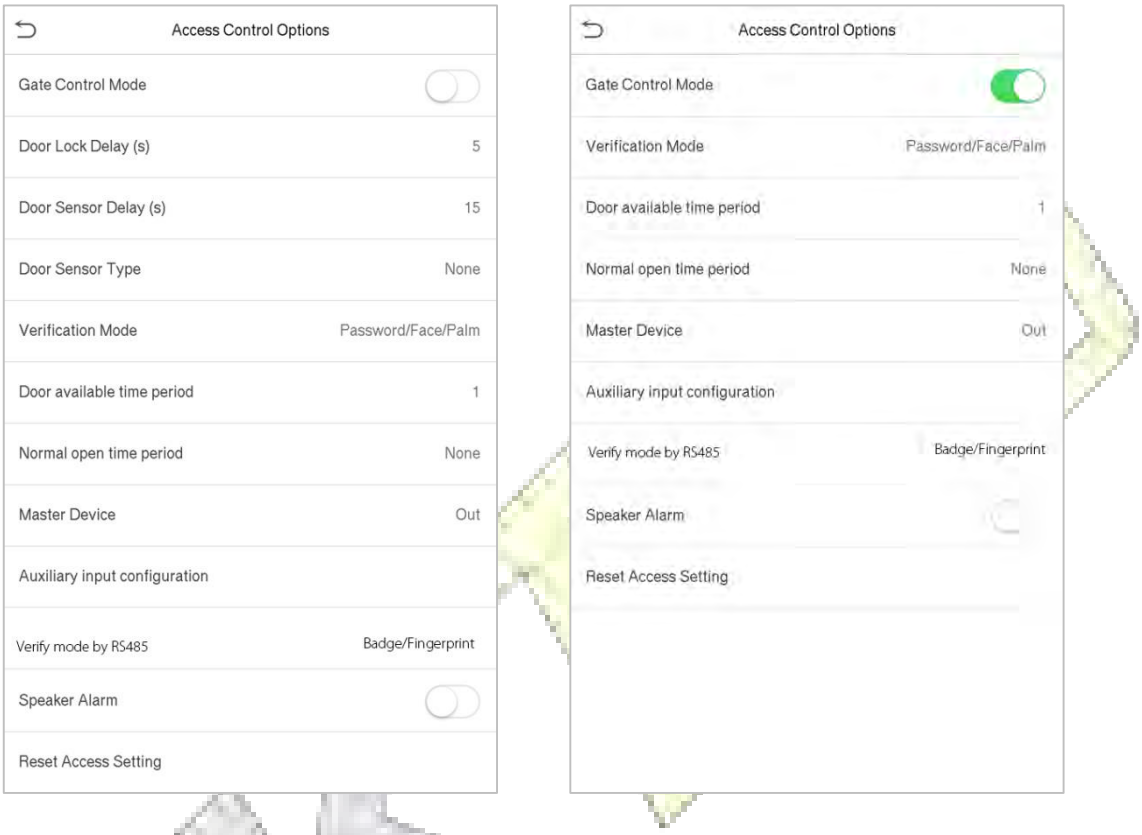
To gain access, the registered user must meet the following conditions:

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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

11.1 Access Control Options

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



Function Description

Function Name	Description
Gate Control Mode	Toggle between ON or OFF switch to get into gate control mode or not. When set to **ON**, on this interface will remove Door lock relay, Door sensor relay and Door sensor type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~10 seconds; 0 second represents disabling the function.
Door Sensor Delay (s)	If the door is not locked and is being left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Door Sensor Type	There are three Sensor types: **None, Normal Open** and **Normal Closed**. **None:** It means door sensor is not in use. **Normal Open:** It means the door is always left opened when electric power is on. **Normal Closed:** It means the door is always left closed when electric power 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 that period.
Normal open time Period	Scheduled time period for "Normal Open" mode, so that the door is always left open 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	Sets 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.
Verify mode by RS485	The verification mode is used when the device is used either as a host or slave. The supported verification mode includes Card/Fingerprint, Fingerprint only, Card only, Fingerprint + Password, Card + Password, Card + Fingerprint, and Card + Fingerprint + Password.
Speaker Alarm	Transmits 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 access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded.

11.2 Time Schedule

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

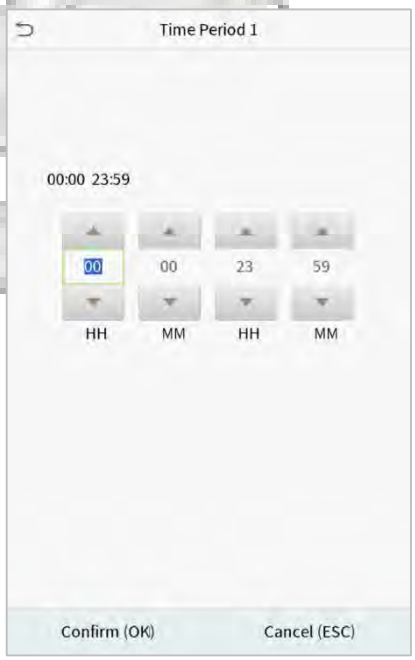
- The entire system can define up to 50 Time Periods.
- Each Time Period represents **10** Time Zones, i.e. **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time period.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

- One can set a maximum of 3 time periods for every time zone. The relationship among these time periods is "**OR**". Thus when the verification time falls in any one of these time periods, the verification is valid.
- The Time Zone format of each Time Period: HH MM-HH MM, which is accurate to minutes according to the 24-hour clock.

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

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



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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

NOTE:

1) When the End Time is earlier than the Start Time, (such as 23:57~23:56), it indicates that access is prohibited all day.

2) When the End Time is later than the Start Time, (such as 00:00~23:59), it indicates that the interval is valid.

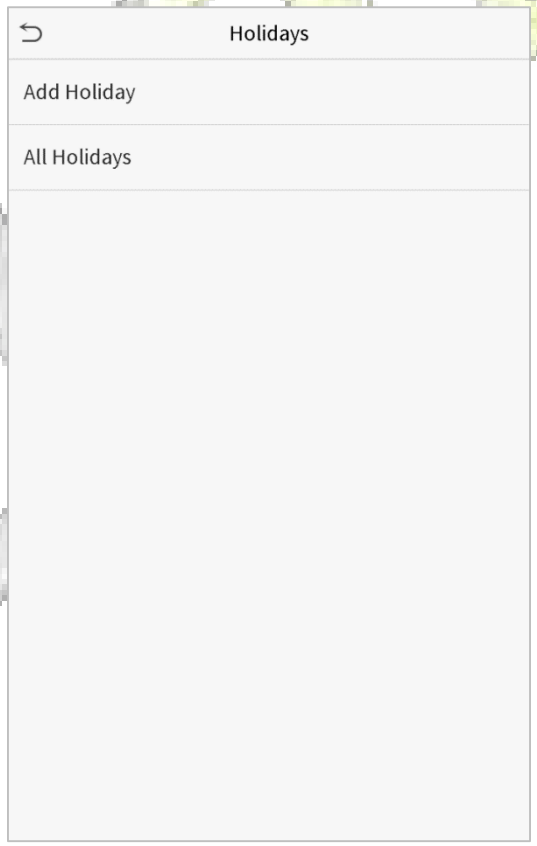
3) The effective Time Period to keep the Door Unlock or open all the day is (00:00~23:59) or also when the Ending Time is later than the Starting Time, (such as 08:00~23:59).

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

11.3 Holidays

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.

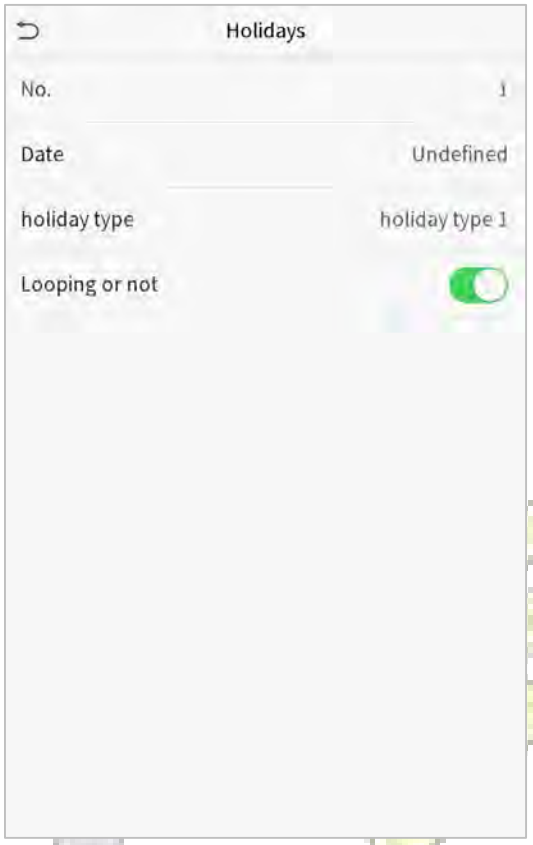
Tap **Holidays** on the **Access Control** interface to set the Holiday access.



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

- **Add a New Holiday**

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



- **Edit a Holiday**

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

- **Delete a Holiday**

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

11.4 Combined Verification

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.

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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

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

For Example:

- The **Door-unlock combination 1** is set as **(01 03 05 06 08)**, indicating that the unlock 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-unlock combination 2** is set as **(02 02 04 04 07)**, indicating that the unlock combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.
- The **Door-unlock 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-unlock combination 4** is set as **(03 05 08 00 00)**, indicating that the unlock combination 4 consists of only three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

Delete a door-unlocking combination

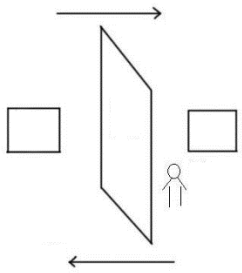
Set all Door-unlock combinations to 0 if you want to delete door-unlock combinations.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

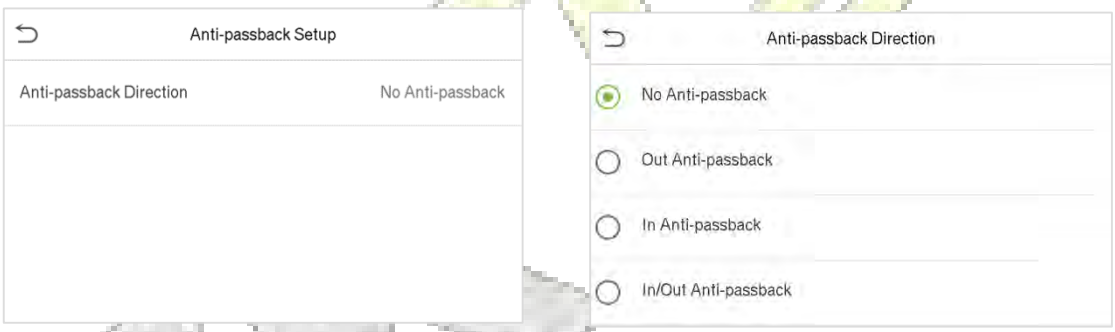
11.5 Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in a security breach. So, to avoid such a situation, the Anti-Passback option was developed. Once it is enabled, the check-in record must match with the 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), and the other one is installed outside the door (slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Tap **Anti-passback Setup** on the **Access Control** interface.



Function Description

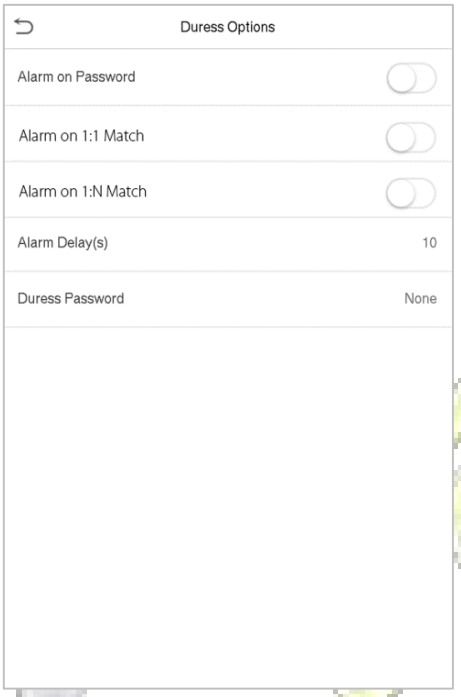
Function Name	Description
Anti-passback direction	**No Anti-passback:** Anti-passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option. **Out Anti-passback:** After a user checks 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-passback:** After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

11.6 Duress Options

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

On **Access Control** interface, tap **Duress Options** to configure the duress settings.



Function Description

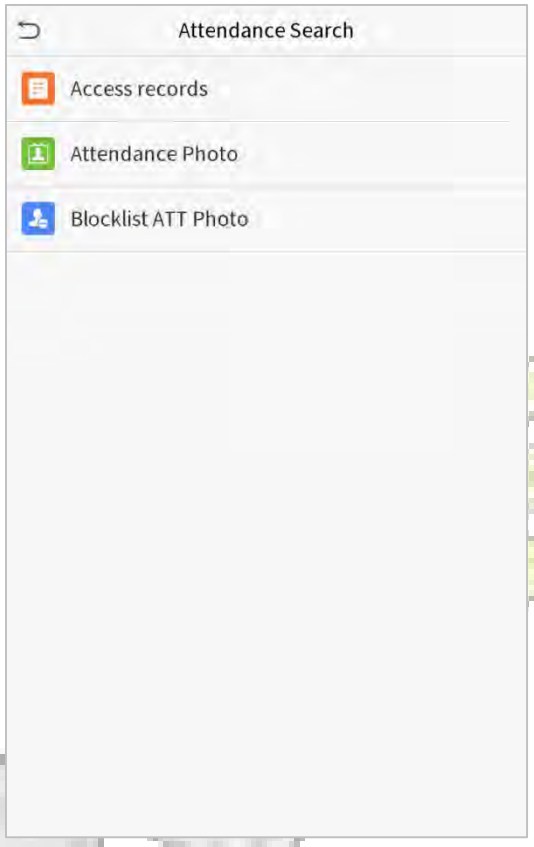
Function Name	Description
Alarm on Password	When a user uses the password verification method, an alarm signal will be generated only when the password verification is successful, otherwise there will be no alarm signal.
Alarm on 1:1 Match	When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated only when the 1:1 verification is successful, otherwise there will be no alarm signal.
Alarm on 1:N Match	When a user uses any fingerprint to perform 1:N verification, an alarm signal will be generated only when the 1:N identification is successful, 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 is be generated.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

12 Attendance Search

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

Click **Attendance Search** on the **Main Menu** interface to search for the required Access/Attendance log.



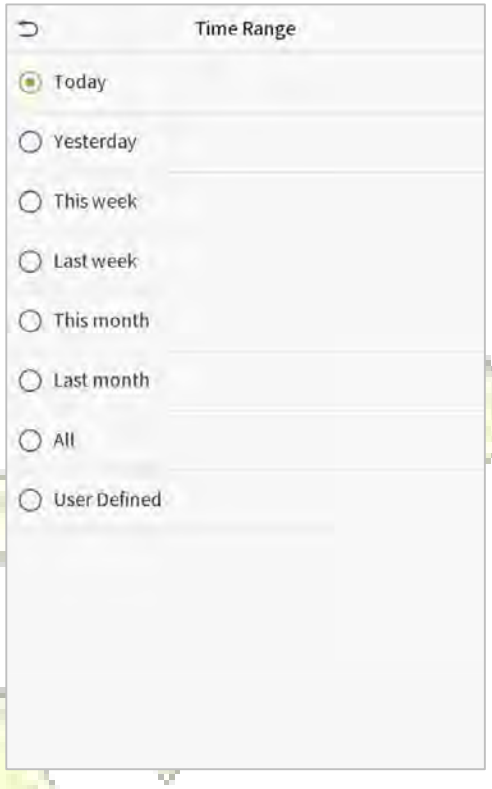
The process of searching for attendance and blocklist photos is similar to that of searching for access records. The following is an example of searching for access records.

On the **Attendance Search** interface, tap **Access Record** to search for the required record.

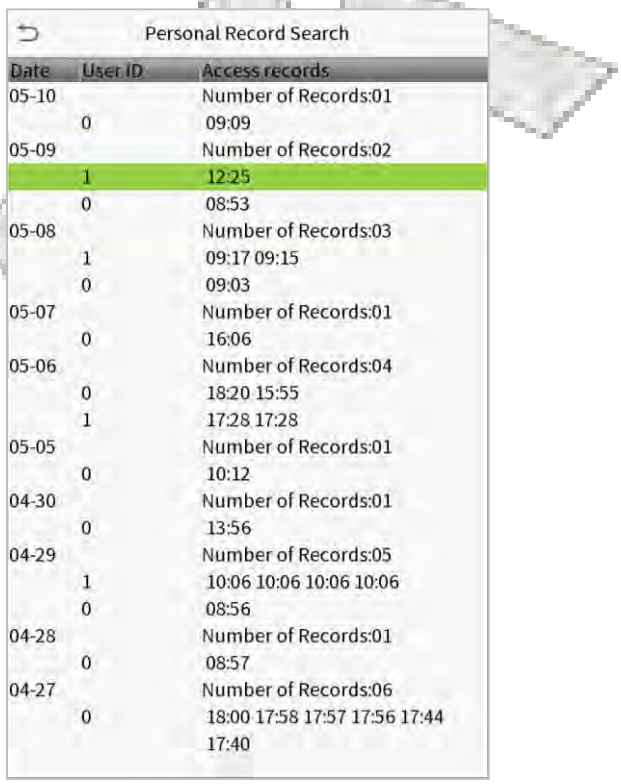
Copyright©2020 ZKTECO CO., LTD. All rights reserved.

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.

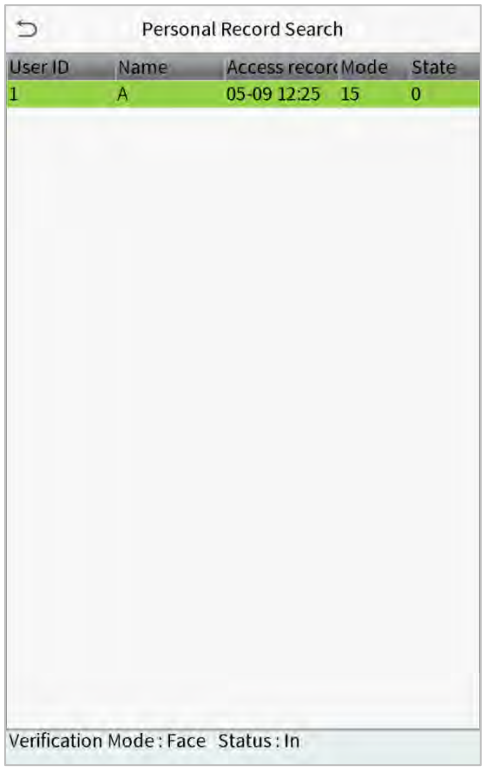
2. Select the time range in which the records need to be searched.



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



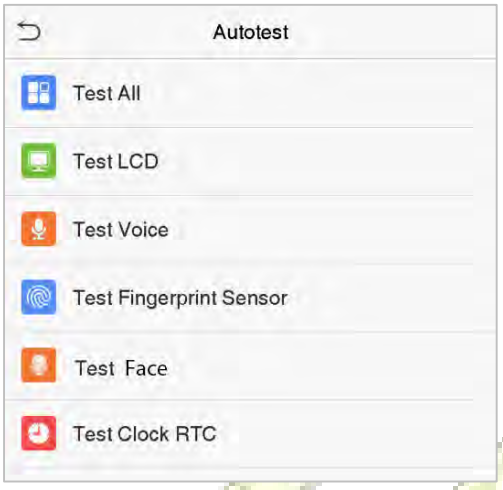
4. The below figure shows the details of the selected record.



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

13 Autotest

On the **Main Menu**, tap **Autotest** to automatically test whether all modules in the device function properly, which include the LCD, Voice, Fingerprint Sensor, Camera and Real-Time Clock (RTC).



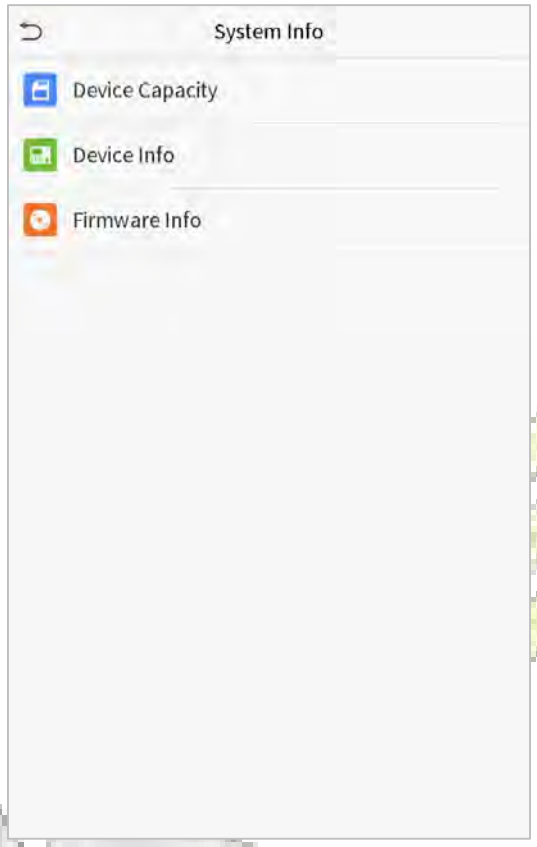
Function Description

Function Name	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 Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Face	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

14 System Information

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



Function Description

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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

15 Connect to ZKBioAccess MTD Software

15.1 Set the Communication Address

- **Device side**

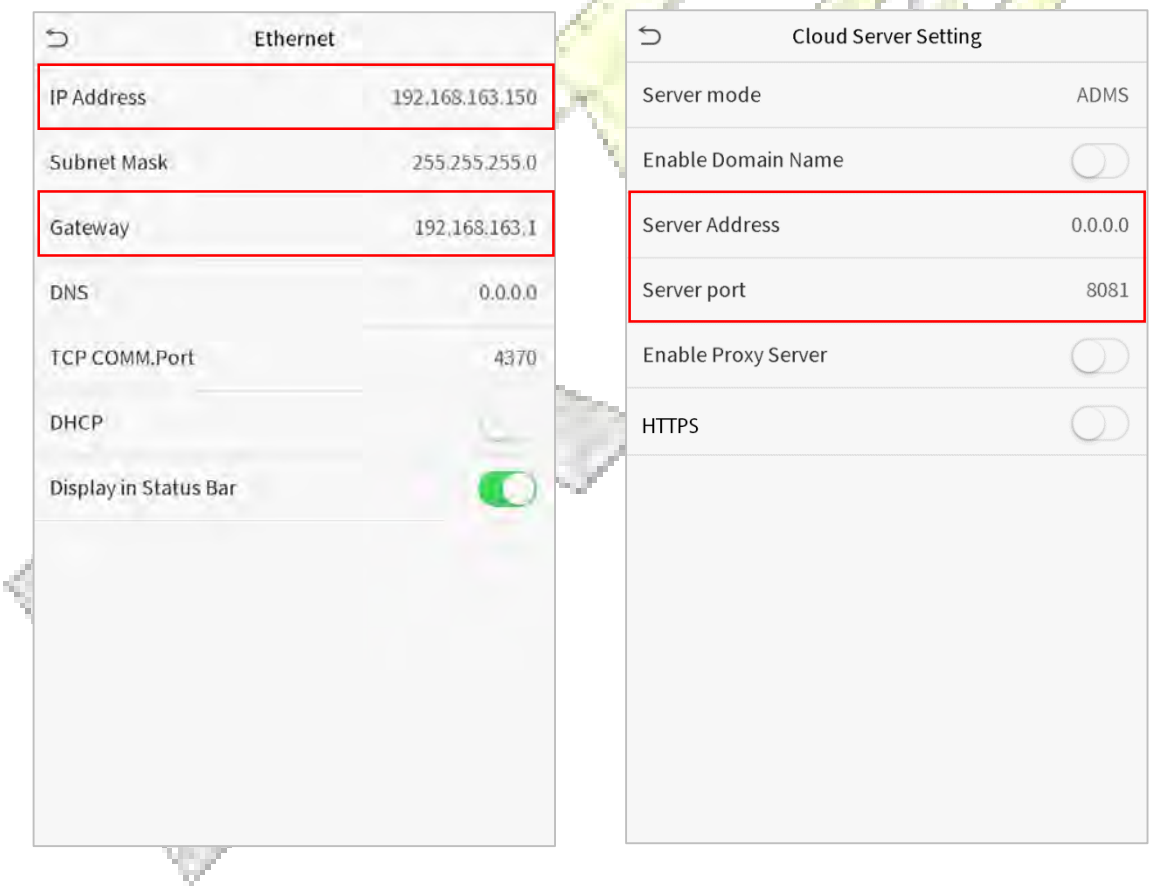
1. Tap **COMM.** > **Ethernet** in the main menu to set the IP address and gateway of the device.

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

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

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

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



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

- **Software side**

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

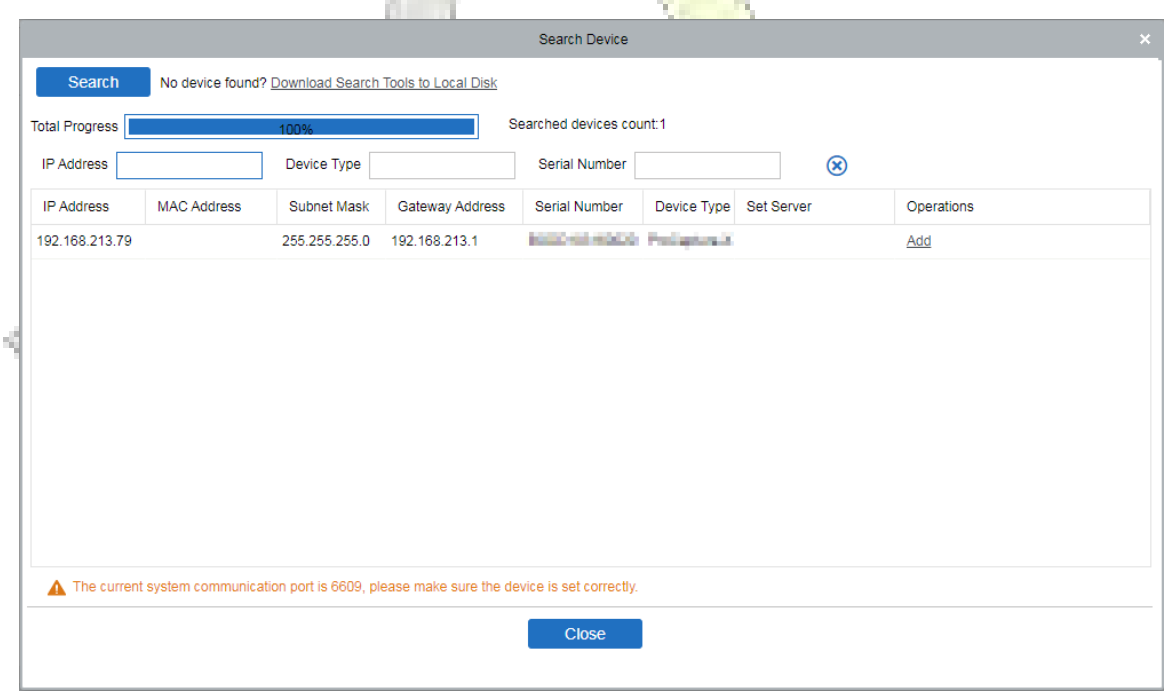
15.2 Add Device on the Software

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

1) Click **Access Control** > **Device** > **Search Device**, to open the Search interface in the software.

2) Click **Search**, and it will prompt [**Searching**……].

3) After searching, the list and total number of access controllers will be displayed.

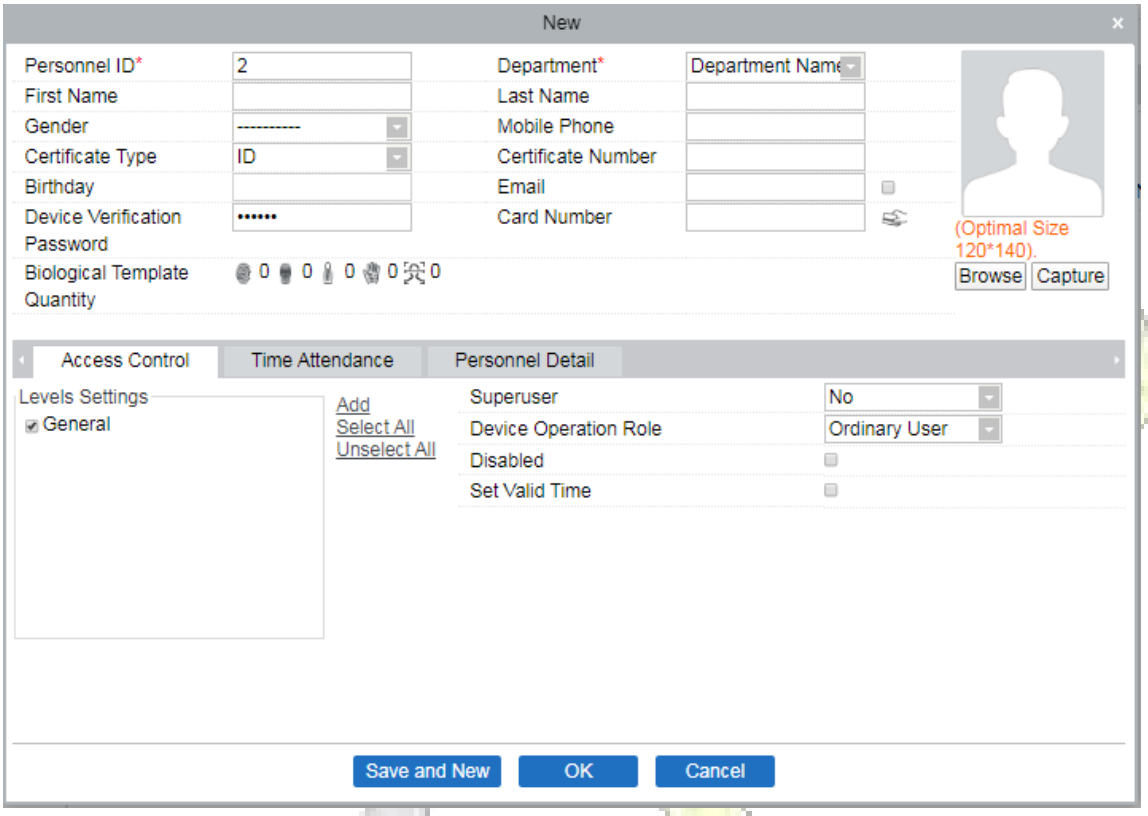


4) Click [**Add**] in operation column, a new window will pop-up. Select Icon type, Area, and Add to Level from each dropdown and click [**OK**] to add the device.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

15.3 Add Personnel on the Software

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

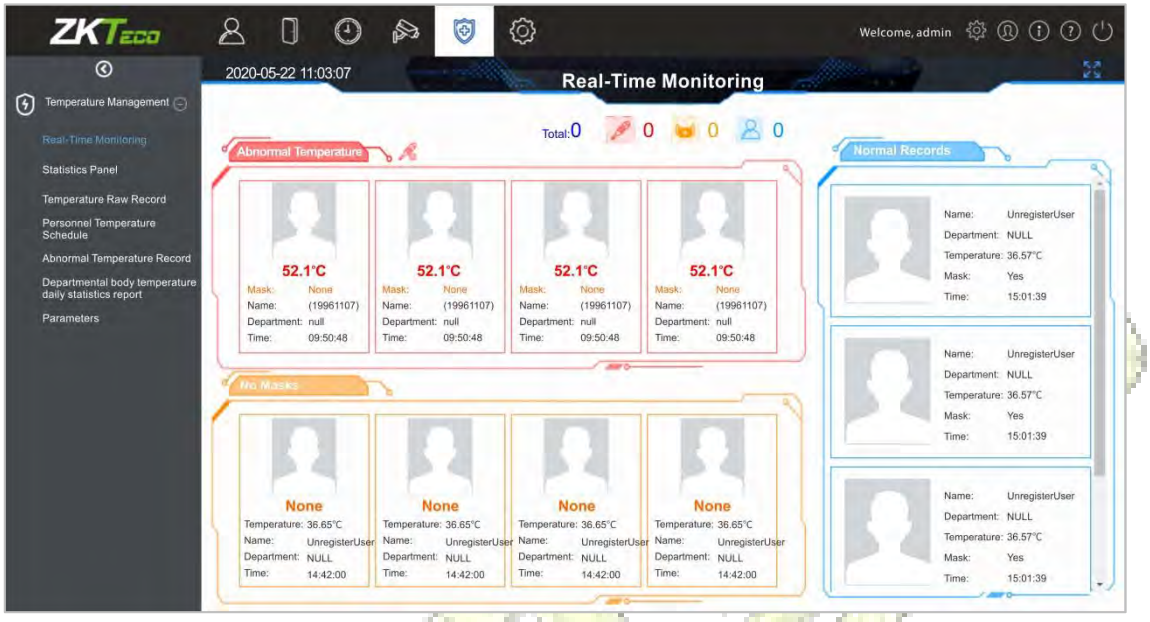


2. Fill in all the required fields and click [**OK**] to register a new user.
3. Click **Access** > **Device** > **Device Control** > **Synchronize All Data to Devices** to synchronize all the data to the device including the new users.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

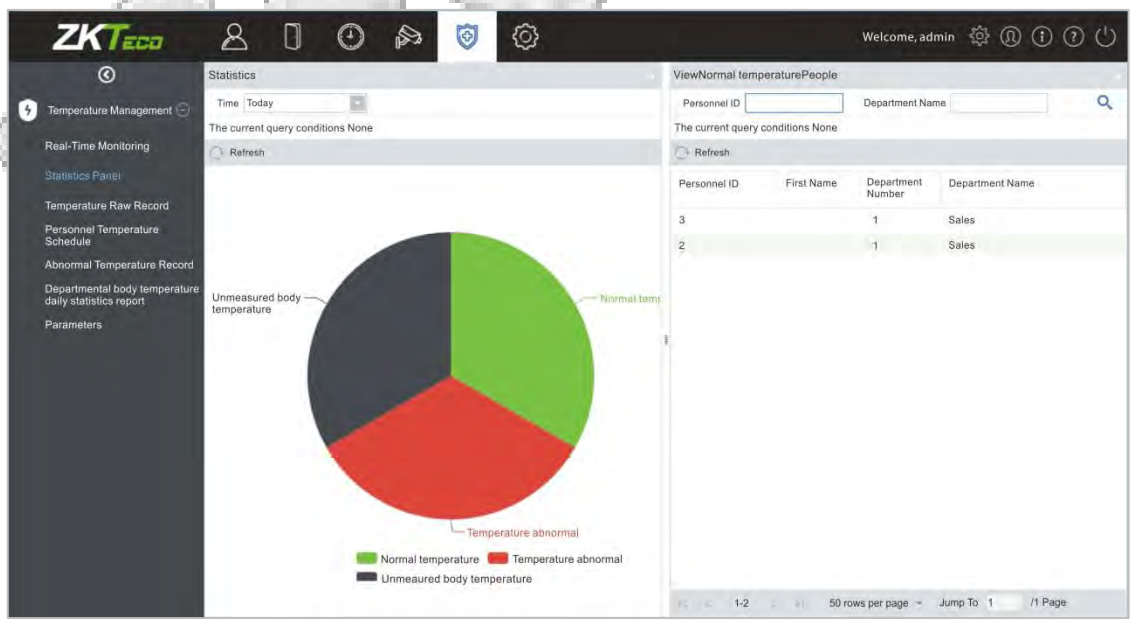
15.4 Real-time monitoring on the ZKBioAccess MTD Software

1. Click **Prevention > Epidemic > Temperature Detection > Real-time monitoring** to view all the personnel's events present under the Abnormal Temperature, No Masks, and Normal Records.



The user data of abnormal body temperature is displayed on the Abnormal Temperature information bar automatically according to the Temperature Threshold Setting is set.

2. Click **Epidemic > Temperature Management > Statistics Panel** to view the analysis of statistical data in the form of a pie-chart and view the personnel with normal temperature, abnormal temperature, and unmeasured body temperature. Also, detailed information of the personnel can be seen on the right by clicking on the particular category on the pie-chart.



NOTE: For other specific operations, please refer to *ZKBioAccess MTD User Manual*.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Appendix 1

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 place the device towards outdoor light sources like door or window or other harsh light sources.

3) Dark-color apparels, different from the background color is recommended for registration.

4) Please expose your face and forehead properly and do not cover your face and eyebrows with your hair.

5) It is recommended to show a plain facial expression. (A smile is acceptable, but do not close your eyes, or incline your head to any orientation).

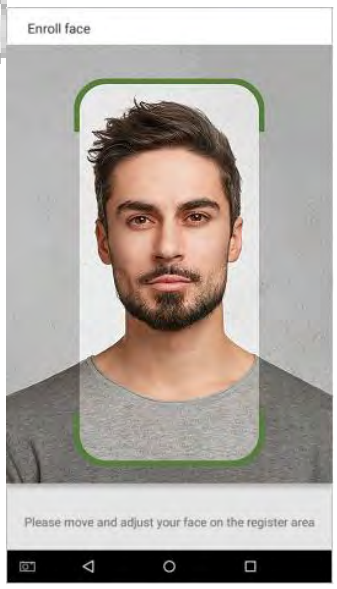
6) Two images are required for a person with eyeglasses, one image with eyeglasses and the other without the eyeglasses.

7) Do not wear accessories like a scarf or mask that may cover your mouth or chin.

8) Please face right towards the capturing device, and locate your face in the image capturing area as shown in the image below.

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

10) A distance of 50cm to 80cm is recommended for capturing the image. (the distance is adjustable, subject to body height).



Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Requirements for Visible Light Digital Face Image Data

The digital photo should be straight-edged, colored, half-portrayed with only one person, and the person should be uncharted and in casuals. Persons who wear eyeglasses should remain to put on eyeglasses for getting photo captured.

- **Eye Distance**

200 pixels or above are recommended with no less than 115 pixels of distance.

- **Facial Expression**

Neutral 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 or colored eyeglasses are not allowed. The frame of the eyeglasses should not cover 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 the eyeglasses.

- **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) Resolution should be between 358 x 441 to 1080 x 1920.
5) The vertical scale of head and body should be in a ratio of 2:1.
6) The photo should include the captured person's shoulders at the same horizontal level.
7) The captured person's eyes should be open and with clearly seen iris.
8) Neutral face or smile is preferred, showing teeth is not preferred.
9) The captured person should be clearly visible, natural in color, no harsh shadow or light spot or reflection in face or background. The contrast and lightness level should be appropriate.

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Appendix 2

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 user fingerprint recognition devices capture only 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 dealer.

Our other law-enforcement fingerprint devices or development tools can capture the original images of user's fingerprints. As to whether or not this constitutes an infringement of your rights, please contact your Government or the final supplier of the device. As the manufacturer of the device, we will assume no legal liability.

Note:

The law includes the following provisions on the personal freedom of its citizens:

1. There shall be no illegal arrest, detention, search, or infringement of persons;
2. Personal dignity is related to personal freedom and 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 the law.

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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Eco-friendly Operation

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

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

Hazardous or Toxic substances and their quantities

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

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

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

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

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

Appendix 3

"Hereby, ZKTECO CO., LTD. declares that this Product is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

"This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body."

Manufacturer: ZKTECO CO., LTD.

Address: No.26, Pingshan 188 Industry zone, Tangxia Town, Dongguan City, Guangdong Province, China

Importers: ZKTECO EUROPE SRL

Address: AVDA CAMINO DE LO CORTAO (DE), NUM.10, PLANTA NAV, PUERTA 1

POLIGONO INDUSTRIAL SUR- S SEBASTIAN DE LOS REYES, 28703, MADRID

Copyright©2020 ZKTECO CO., LTD. All rights reserved.

ZKTeco Industrial Park, No. 26, 188 Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com

Copyright © 2020 ZKTECO CO., LTD. All Rights Reserved.