eSSL®
Security at Fingertips

User Manual
AI-Face-Mercury

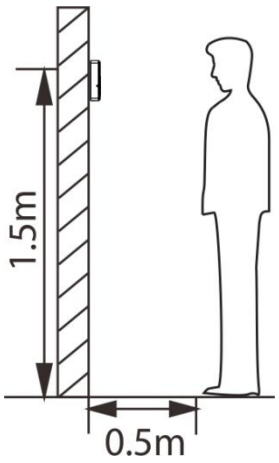
www.esslsecurity.com

Table of Contents

1 Notice for Use

1.1 Standing Position, Facial Expression and Standin Posture

- **The recommended distance**



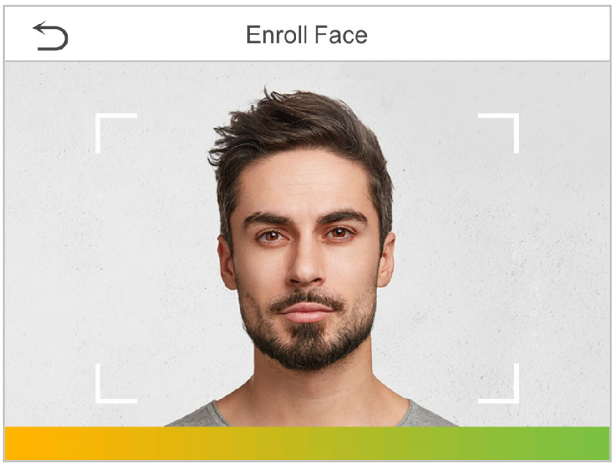
The distance between the device and a user whose height is within 1.55m-1.85m is recommended to be 1.5m. Users may slightly move forwards and backwards to improve the quality of facial images captured.

- **Facial expression and standing posture**

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

1.2 Face Registration

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



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.)

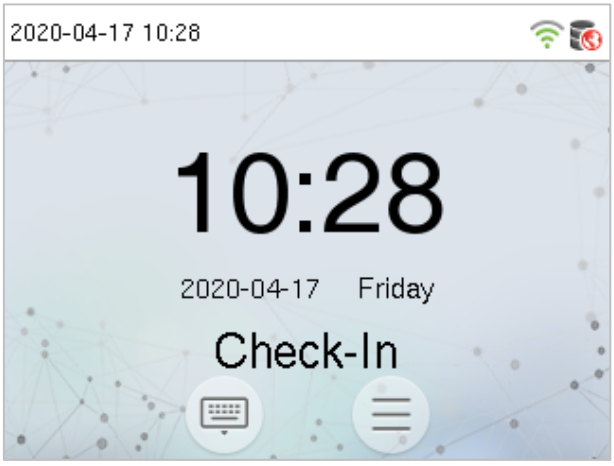
- ❖ If you do not follow the instructions on the screen, the face registration may take longer or may fail.
- ❖ Be careful not to cover the eyes or eyebrows.
- ❖ Do not wear hats, masks, sunglasses or eyeglasses.
- ❖ Be careful not to display two faces on the screen. Register one person at a time.
- ❖ 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.

1.3 Standby Interface

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

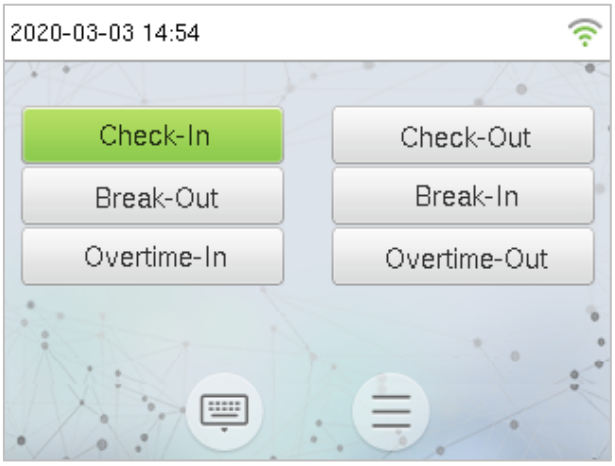


Notes:

1）Click  to enter the User ID input interface.

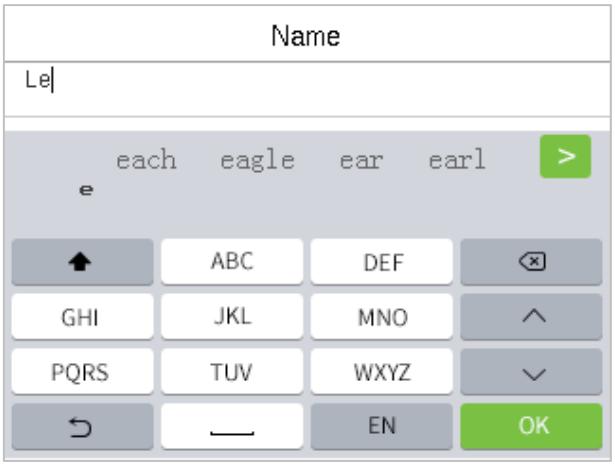
2）When there is no super administrator set in the device, click  to enter the menu. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register super administrator the first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

1.4 Virtual Keyboard



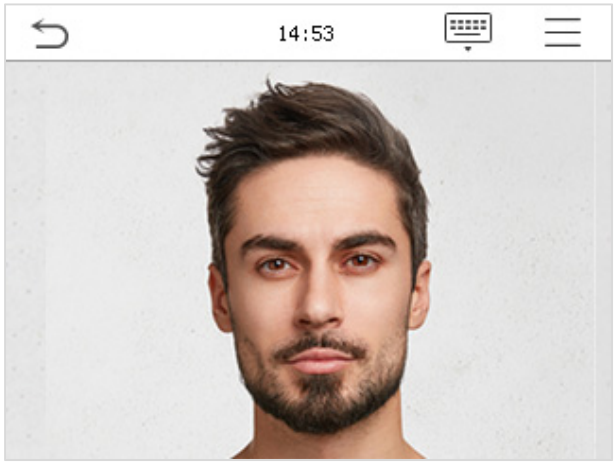
Note: The device supports the input of English, numbers and symbols. Click [**En**] to switch to English keyboard. Press [**123**] to switch to the numeric and symbolic keyboard, and click [**ABC**] to return to the alphabetic keyboard. Click the input box, virtual keyboard appears. Click [**ESC**] to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

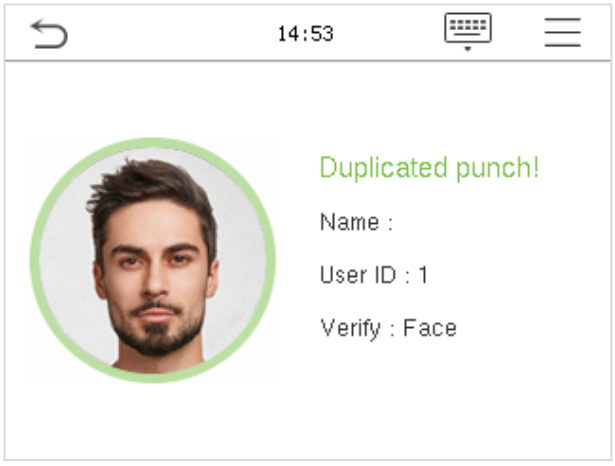
1.5 Verification Mode

1.5.1 Facial Verification

- **1:N Facial 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**

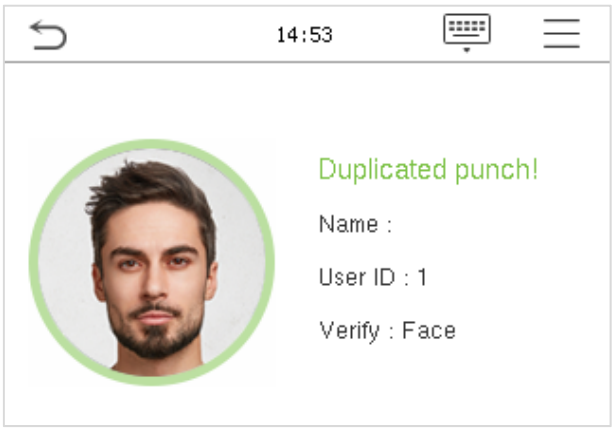
Compare the face captured by the camera with the facial template related to the entered user ID.

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 prompts “Please adjust your position!”.

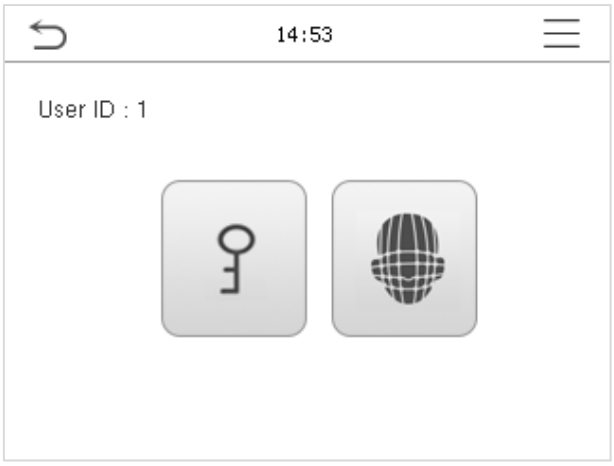
1.5.2 Password Verification

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

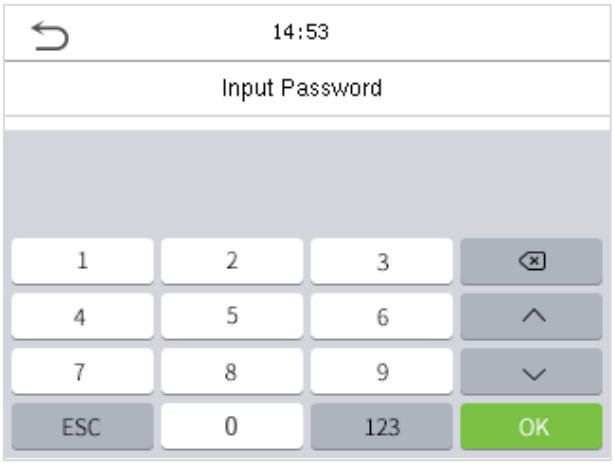
Click the button on the main screen to enter the 1:1 password verification mode.

1. Input the user ID and press **OK**.

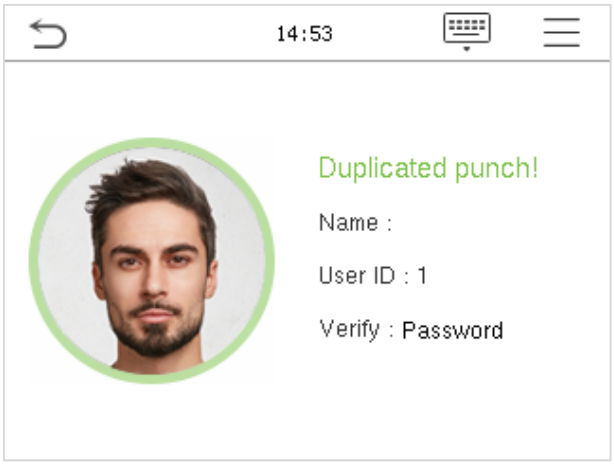
If an employee registers palm and face in addition to password, the following screen will appear. Select the  icon to enter password verification mode.



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

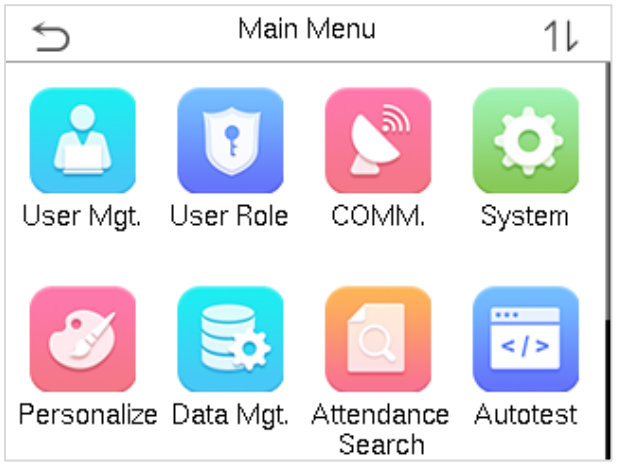


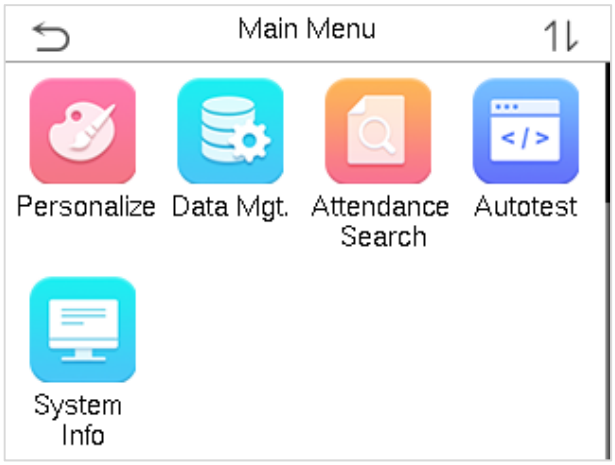
Verification is successful:



2 Main Menu

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



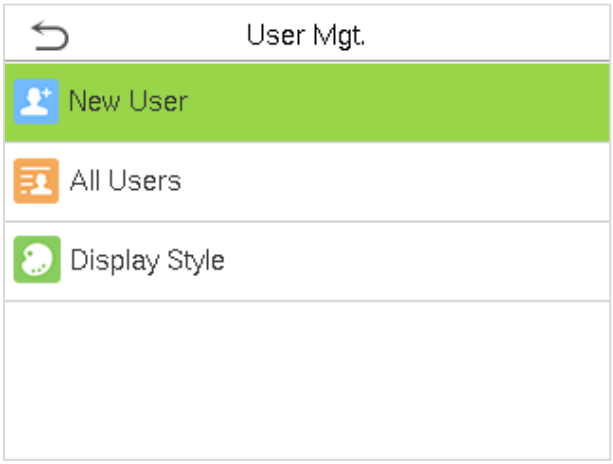


Items	Descriptions
User Mgt.	To add, edit, view, and delete basic information about a user.
User Role	To set the permission scope of the custom role and enroller, that is, the rights to operate the system.
COMM.	To set the relevant parameters of PC connection and wireless network.
System	To set parameters related to the system, including date & time, attendance, face and resetting to factory settings.
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.
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

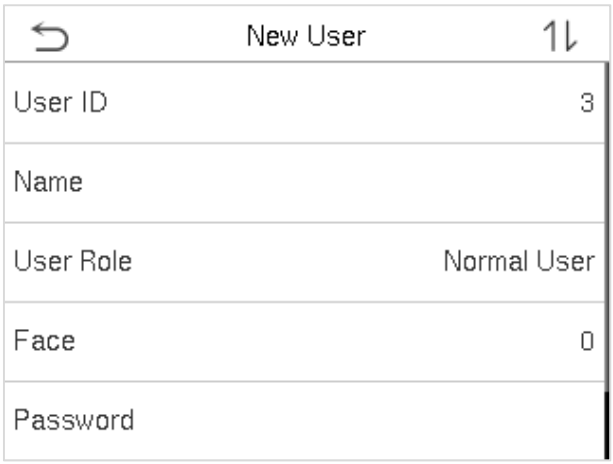
Click **User Mgt.** on the main menu.



Click **New User.**

- **Register a User ID and Name**

Enter the user ID and name.



Notes:

1）A user name may contain 34 characters.

2）The user ID may contain 1-9 digits by default.

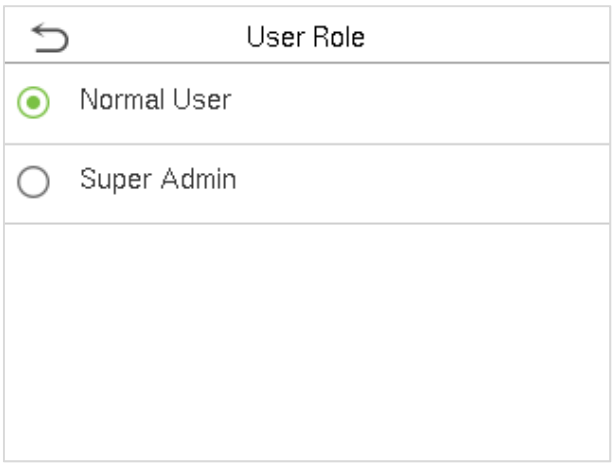
3）During the initial registration, you can modify your ID, which cannot be modified after registration.

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.

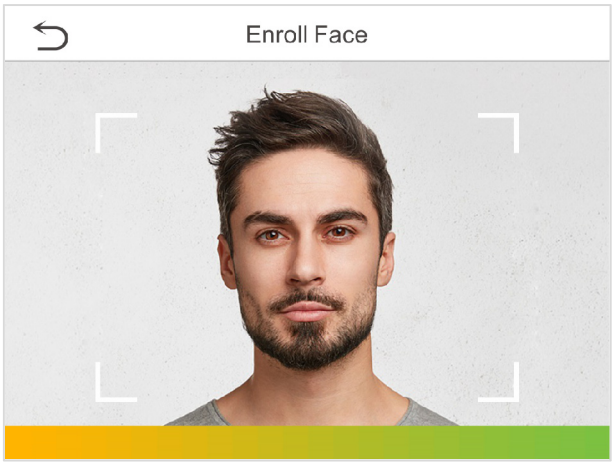
Click **User Role** to select Normal User or Super Admin.



Note: If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. Please refer to 1.5 Verification Mode.

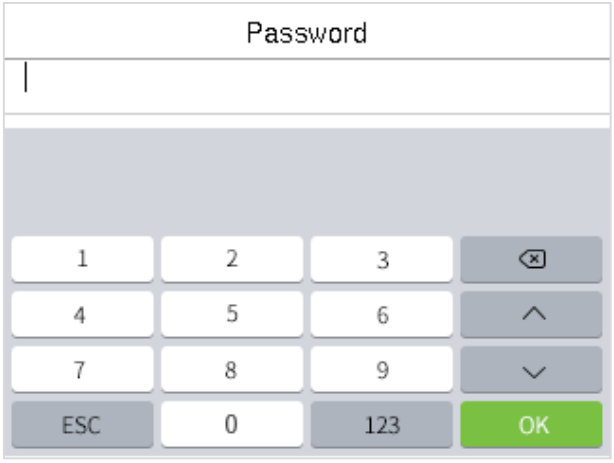
- **Register face**

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.

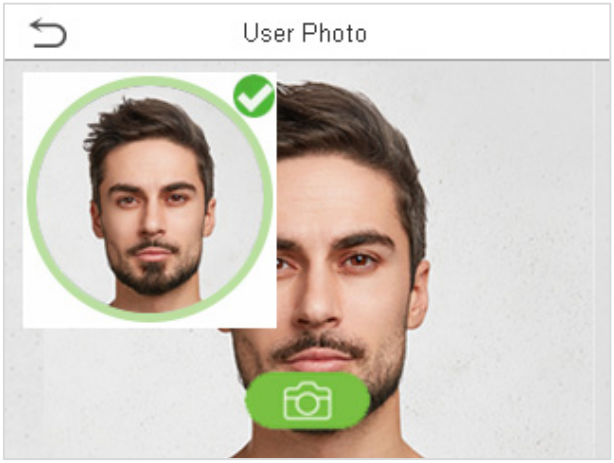


Note: The password may contain one to eight digits by default.

- **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.



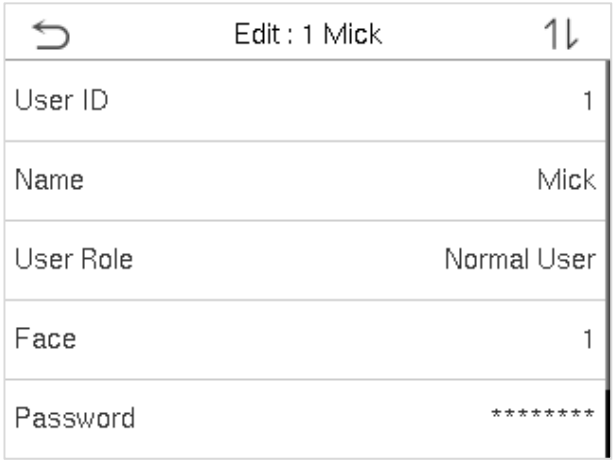
Note: While registering a face, the system will automatically capture a picture as the user photo. If you do not want to register a user photo, the system will automatically set the picture captured as the default photo.

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

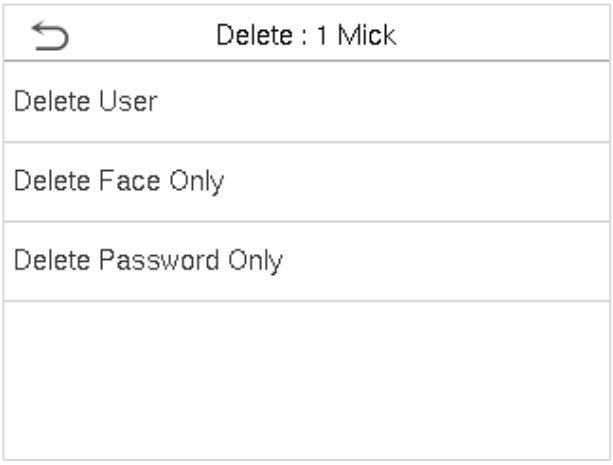
Choose a user from the list and click **Edit** to enter the edit user interface:



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**.



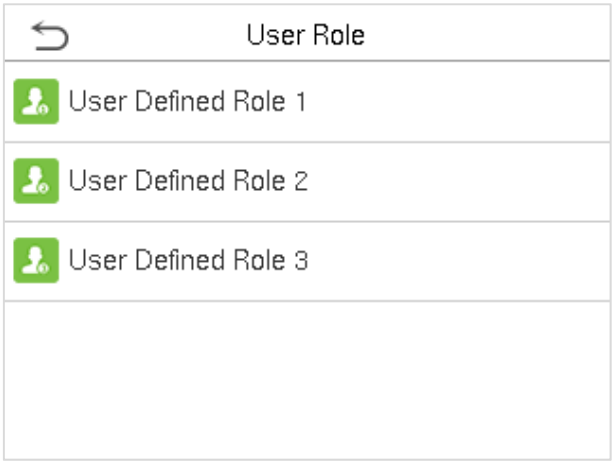
Note: If you select **Delete User**, all information of the user will be deleted.

4 User Role

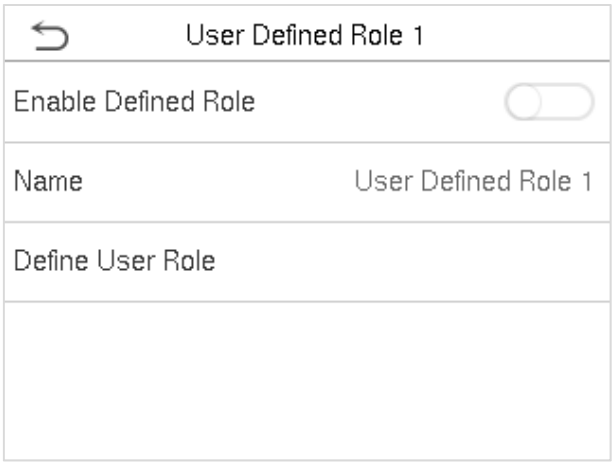
If you need to assign some specific permissions to certain users, you may edit the "User Defined Role" under the **User Role** menu.

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.

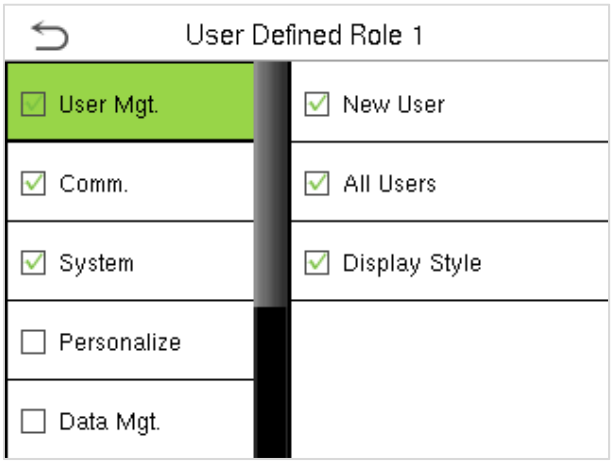
Click **User Role** on the main menu interface.



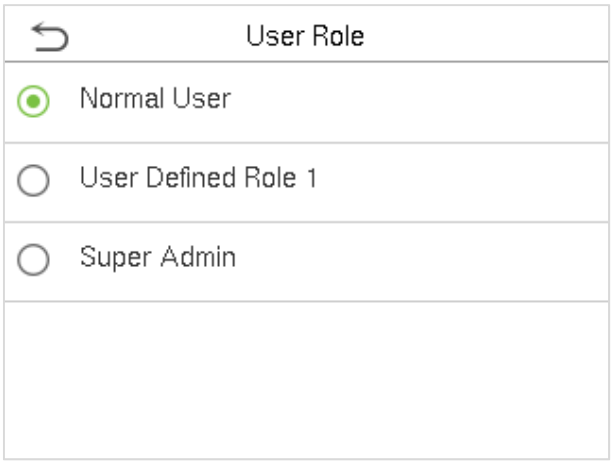
1. Click any item to set a defined role. Click the row of **Enable Defined Role** to enable this defined role. Click **Name** and enter the name of the role.



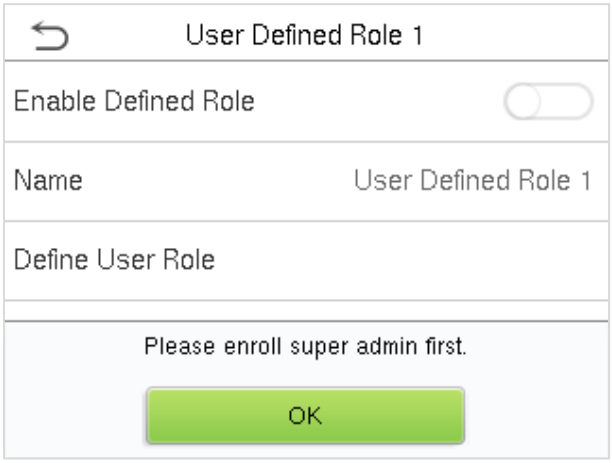
2. Click **Define User Role** to assign the privileges to the role. The privilege assignment is completed. Click Return.



Note: During privilege assignment, the main menu is on the left and its sub-menus are on the right. You only need to select the features in sub-menus. If the device has a role enabled, you may assign the roles you set to users by clicking **User Mgt. > New User > User Role**.



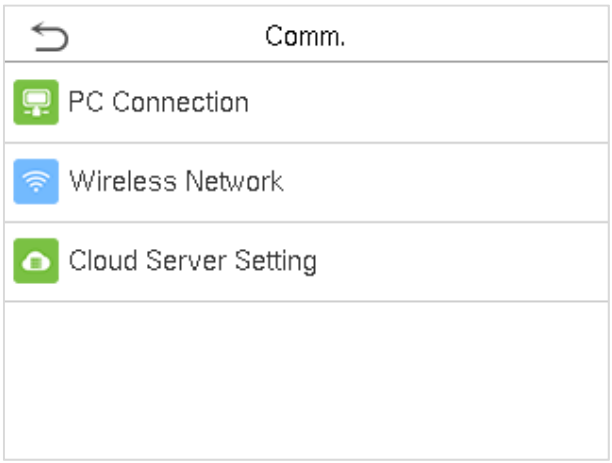
If no super administrator is registered, the device will prompt "Please enroll super admin first." after clicking the enable bar.



5 Communication Settings

Set the relevant parameters of PC connection and wireless network.

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

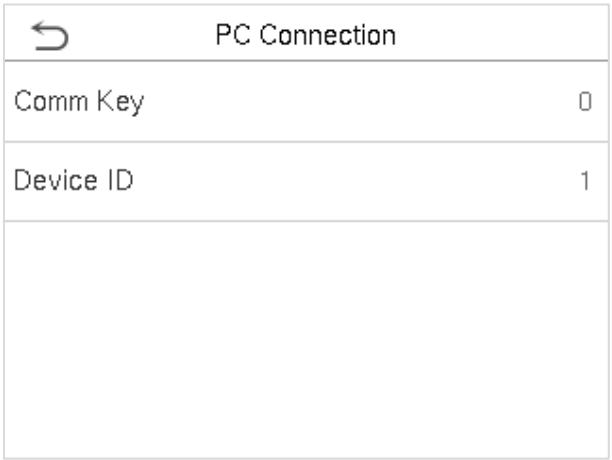


5.1 PC Connection

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

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

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

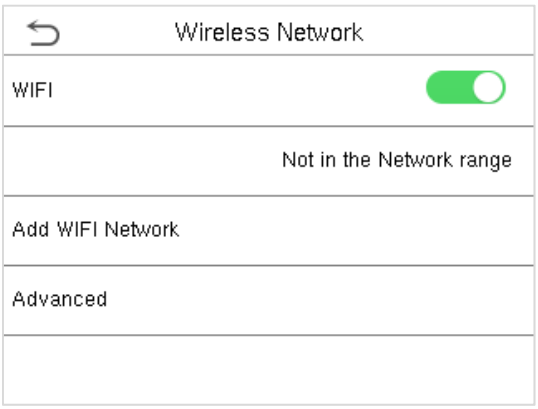


Item	Descriptions
Comm Key	Comm Key: The default password is 0, which can changed. The Comm Key may contain1-6 digits.
Device ID	Identity number of the device, which ranges between 1 and 254. If the communication method is RS232/RS485, you need to input this device ID in the software communication interface.

5.2 Wi-Fi Settings

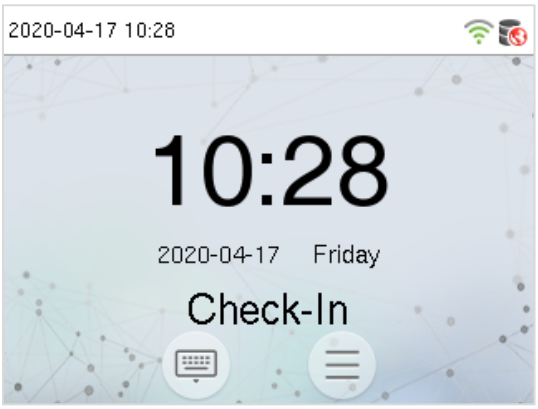
Wi-Fi is short for Wireless Fidelity. The device provides a Wi-Fi module, which can be built in the device mould or externally connected, to enable data transmission via Wi-Fi and establish a wireless network environment.

Wi-Fi is enabled in the system by default. If the Wi-Fi network does not need to be used, you can tap the button to disable Wi-Fi.



When Wi-Fi is enabled, tap the searched network.Tap the password entry text box to enter the password, and tap **Connect to Wi-Fi (OK)**.

The connection succeeds, with status displayed on the icon bar.

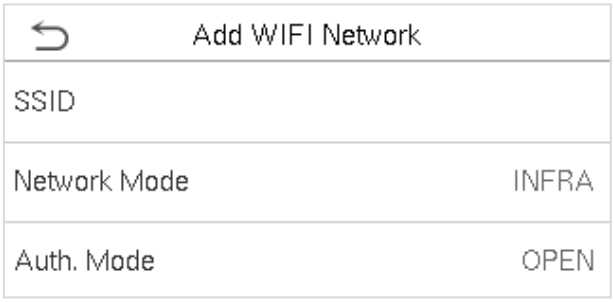


5.2.1 Adding Wi-Fi Network

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

Tap **Page Down** and **Add Wi-Fi Network**.

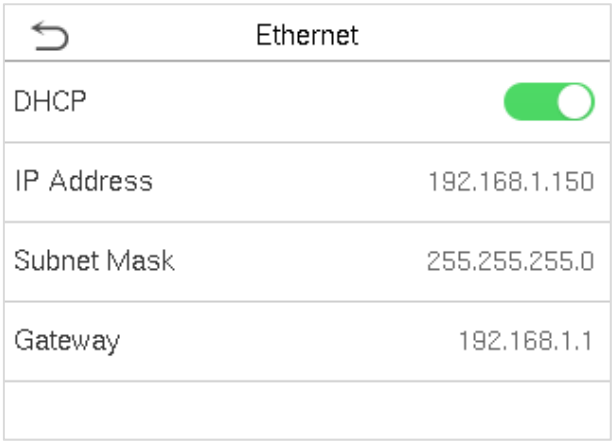
Enter the parameters of Wi-Fi network. (The added network must exist.)



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

5.2.2 Advanced Options

This is used to set Wi-Fi network parameters.

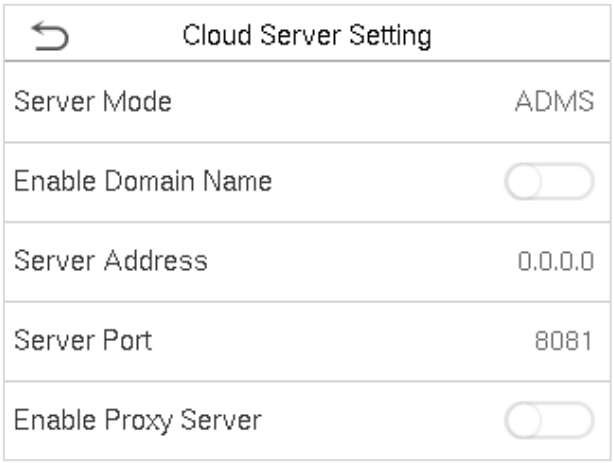


Menu Item	Description
DHCP	Short for Dynamic Host Configuration Protocol, which involves allocating dynamic IP addresses to network clients.
IP Address	IP address of the Wi-Fi network.
Subnet Mask	Subnet mask of the Wi-Fi network.
Gateway	Gateway address of the Wi-Fi network.

5.3 Cloud Server Setting

This represents settings used for connecting with the ADMS server.

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

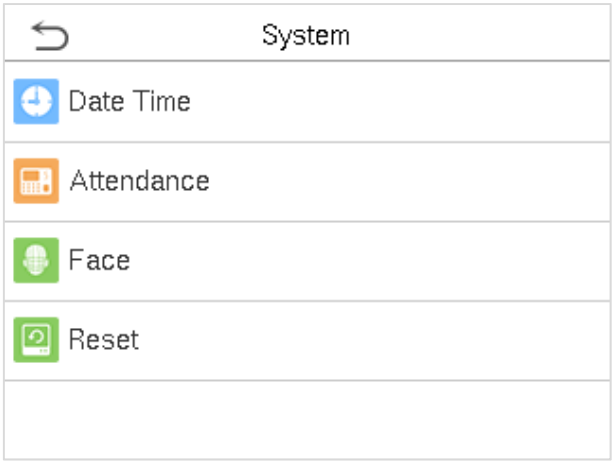


Item		Description
Enable Domain Name	**Server Address**	When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.
Disable Domain Name	**Server Address**	IP address of the ADMS server.
	Server 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.

6 System Settings

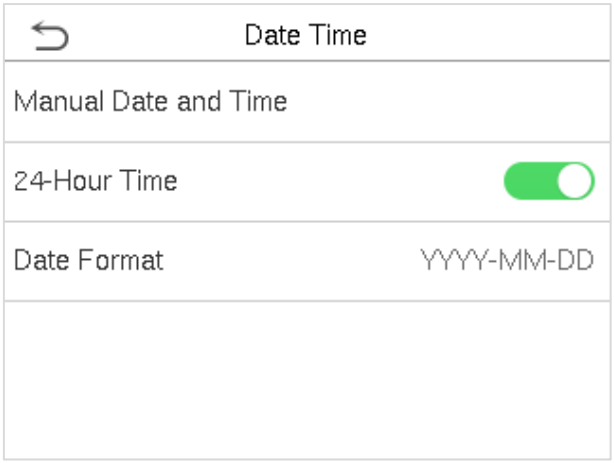
Set related system parameters to optimize the performance of the device.

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



6.1 Date and Time

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



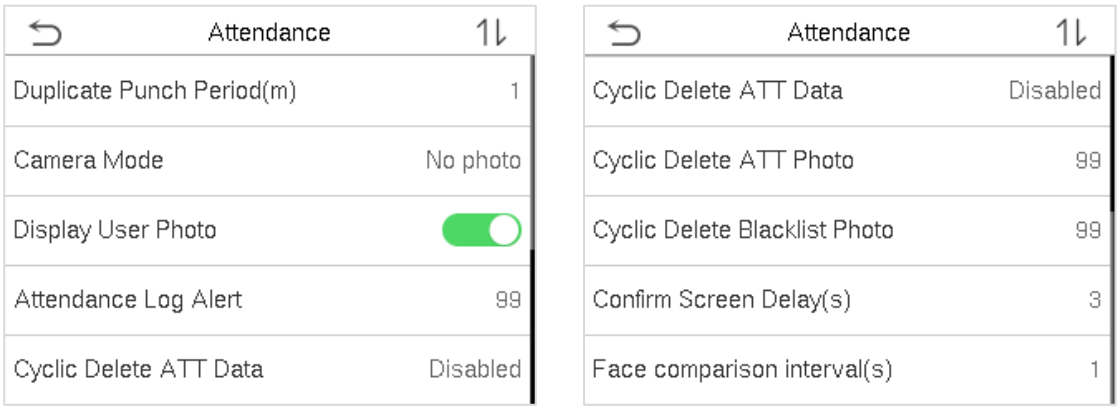
1. You can manually set date and time and click Confirm to save.
2. Click 24-Hour Time to enable or disable this format and select the date format.

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 Attendance Parameters

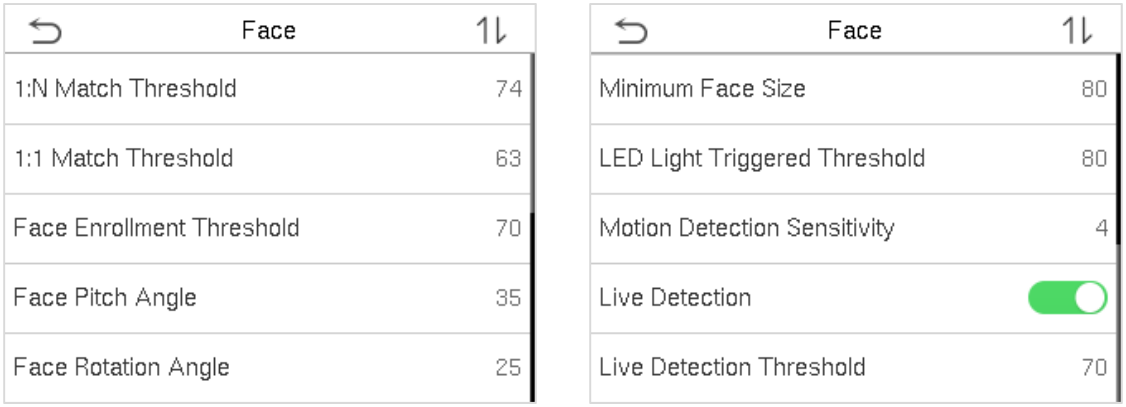
Click **Attendance** on the System interface.



Menu Item	Description
Duplicate Punch Period (m)	Within a set time period (unit: minutes), the duplicated attendance logs will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	To set whether to take and save photos in verification; applicable to all users. The following 5 modes are included: **No Photo:** No photo is taken in user verification. **Take photo, no save:** Photo is taken but not saved in verification. **Take photo and save:** Photo is taken and saved in verification. **Save on successful verification:** Photois taken and saved in successful verification. **Save on failed verification:** Photo is taken and saved in failed verification.
Display User Photo	To set user photo to be displayed when a user passes verification. Turn it **[ON]** to display user photo and **[OFF]** to disable it.
Attendance Log Alert	When the remaining storage is smaller than the set value, the device will automatically alert users to the remaining storage information. It can be disabled or set to a value ranged from 1 to 9999.
Cyclic Delete ATT Data	The number of attendance logs allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 999.
Cyclic Delete ATT Photo	The number of attendance photos allowed to be deleted in one time when the maximum storage is attained. It can be disabled or set to a value ranged from 1 to 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 display of the verification information interface after verification. Value ranges from 1 to 9 seconds.
Face Comparison Interval (s)	To set the face comparison interval as required, within the range of 0-9 s.

6.3 Face Parameters

Click **Face** on the System interface.



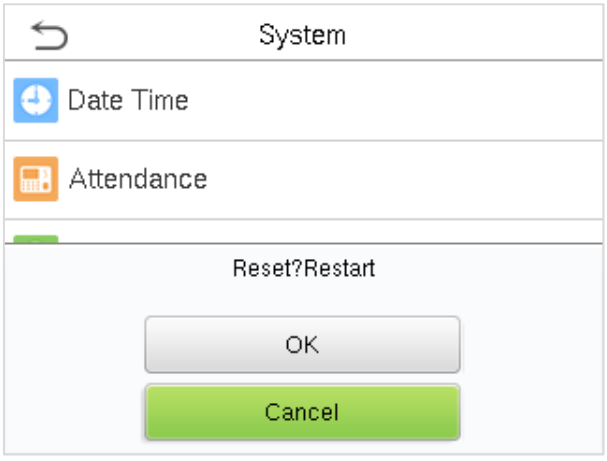
Item	Description
1:N Match Threshold	Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 65 to 120. The higher the thresholds, the lower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

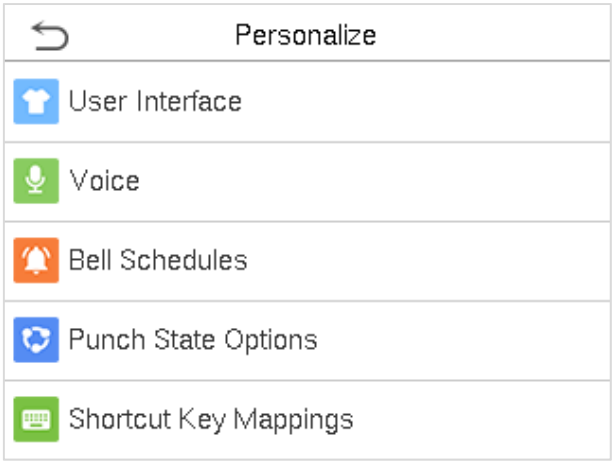


Click **OK** to reset.

7 Personalize Settings

You may customize interface settings, audio and bell.

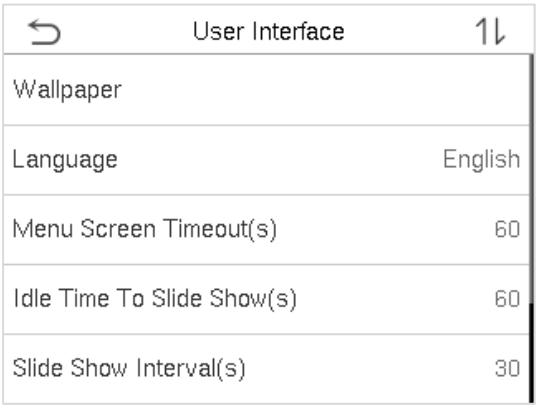
Click **Personalize** on the main menu interface.

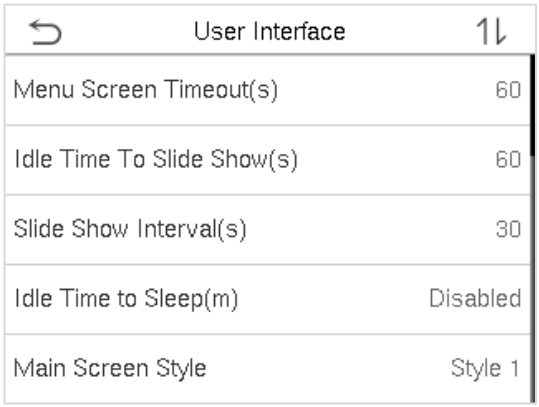


7.1 User Interface Settings

You can customize the display style of the main interface.

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



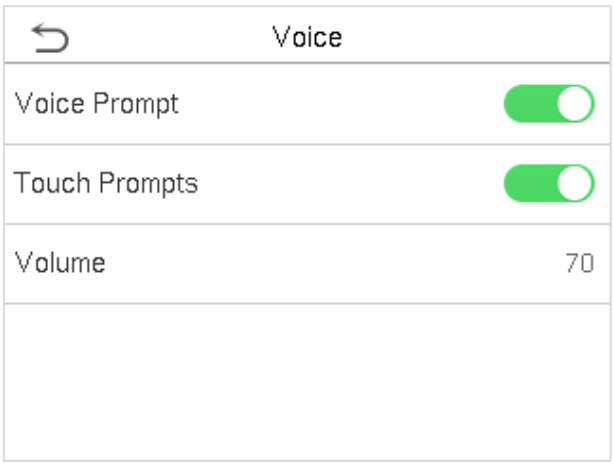


Item	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.

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

7.2 Voice Settings

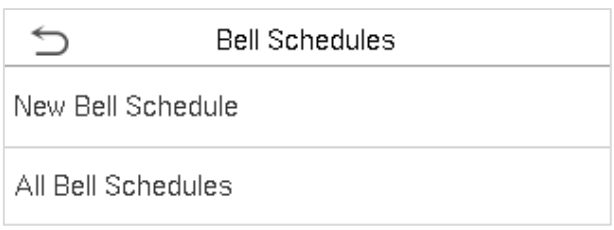
Click **Voice** on the Personalize interface.



Item	Description
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.

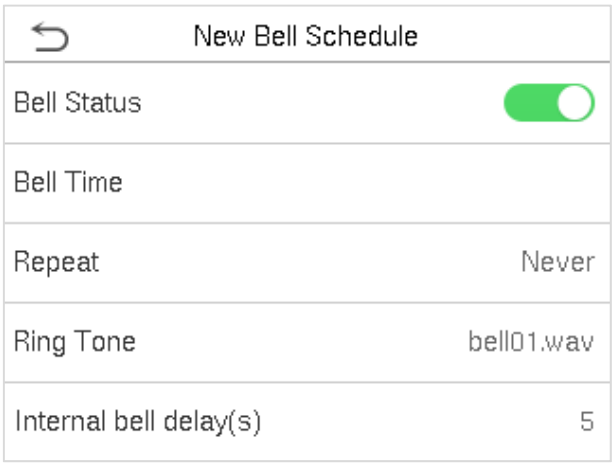
7.3 Bell Schedules

Click **Bell Schedules** on the Personalize interface.



- **Add a bell**

1. Click **New Bell Schedule** to enter the adding interface:



Item	Description
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.

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

- **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.

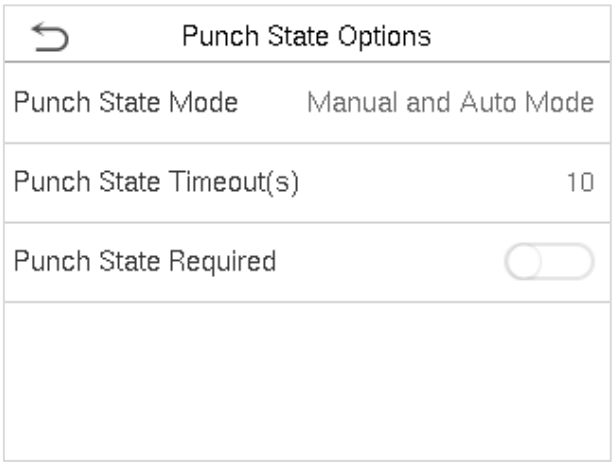
- **Delete a bell**

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

Tap **Delete** and select **Yes** to delete the bell.

7.4 Punch State Options

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

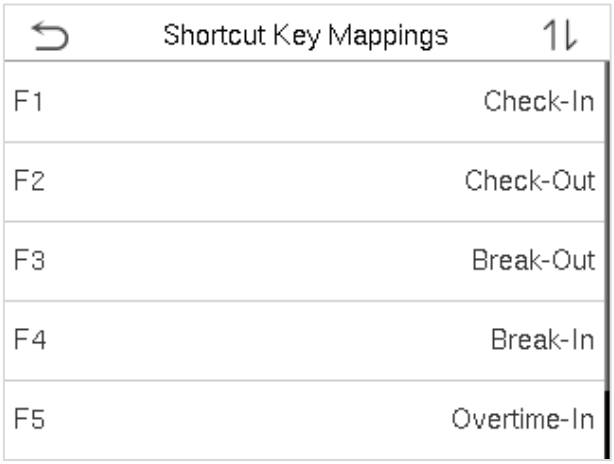


Item	Description
Punch State Mode	Select a punch state mode, which can be: **Off:** To disable the punch state key function. The punch state key set under **Shortcut Key Mappings** menu will become invalid. **Manual Mode:** To switch the punch state key manually, and the punch state key will disappear 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.
Punch State Timeout (s)	The time of one punch state displays. The punch state will disappear or switch to other punch states as the time is out. The value is 5~999 seconds.
Punch State Required	Set whether to select punch state during verification.

7.5 Shortcut Keys Mappings

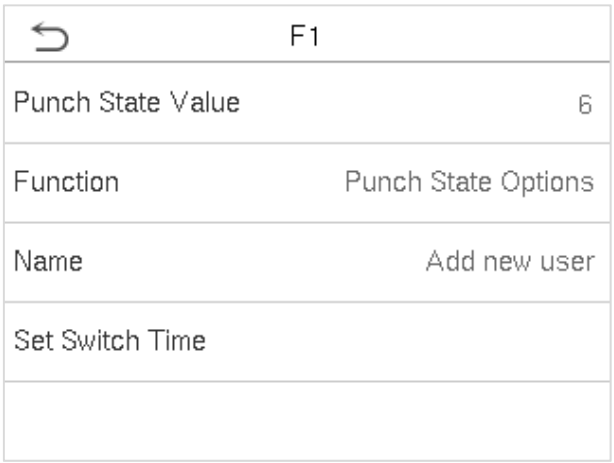
Users may define shortcuts as attendance status or functional keys. On the main interface, when the shortcut keys are pressed, the corresponding attendance status or function interface will quickly display.

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

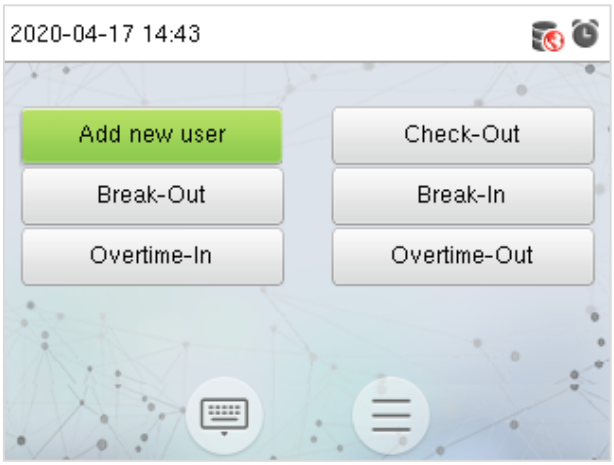


1. Tap the shortcut key to be set.

2. Set the state value , corresponding function and the state key name for this touch key.



3. Tap the main interface to show the shortcut menu.

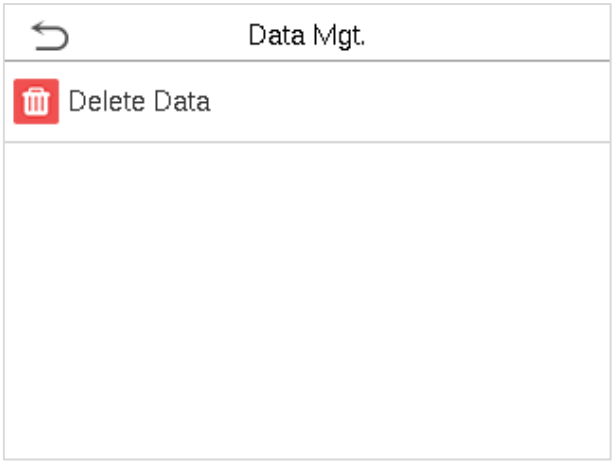


Tap the attendance state to make a switch. Tap the function to rapidly access the function settings. (Tap F1 **New User** to rapidly access this menu.)

8 Data Management

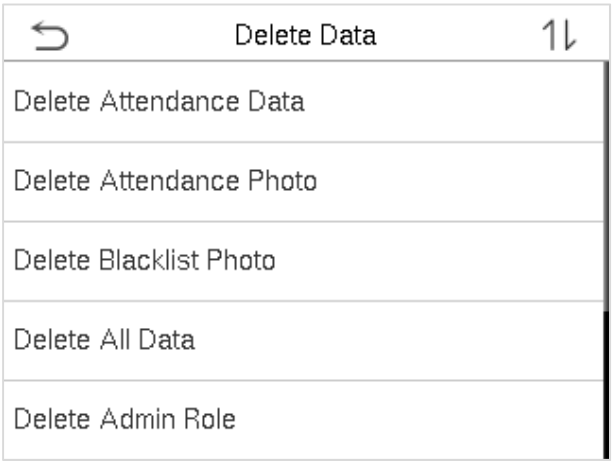
To delete the relevant data in the device.

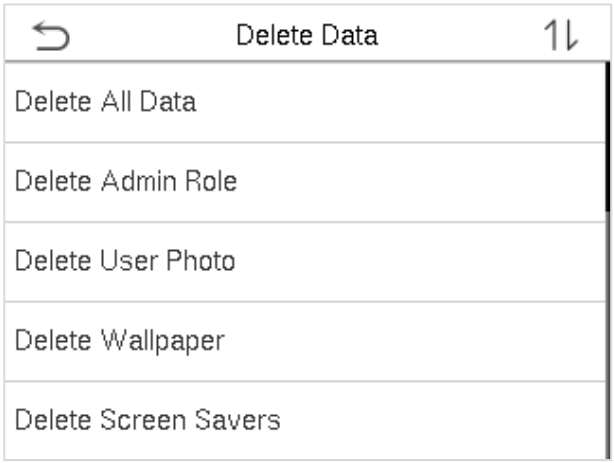
Click **Data Mgt.** on the main menu interface.



8.1 Delete Data

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

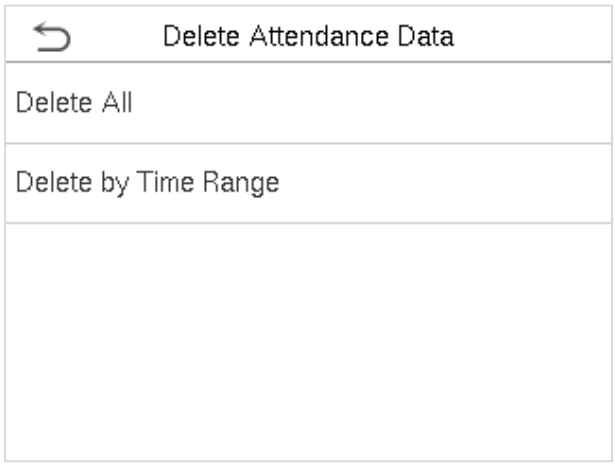




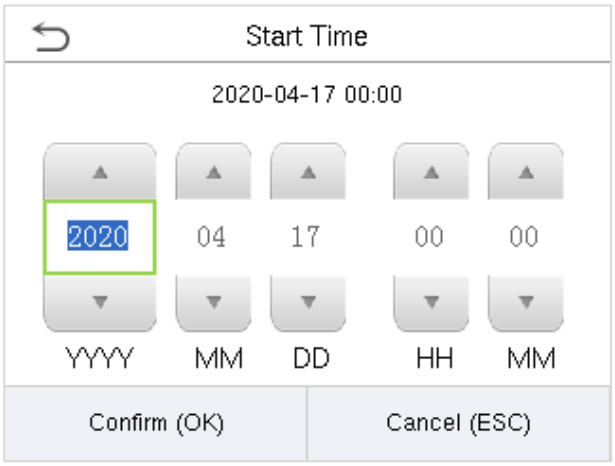
Menu Item	Description
Delete Attendance Data	To delete all attendance data in the device.
Delete Attendance Photo	To delete all users' attendance photos in the device.
Delete Blacklist Photo	To delete all blacklisted photos in the device, which means the photos taken after failed verifications.
Delete All Data	To delete all user information, fingerprints and attendance logs etc.
Delete Admin Role	To make all Administrators become Normal Users.

Delete User Photo	To delete all user photo in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete all screen savers in the device.

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



Select Delete by Time Range.

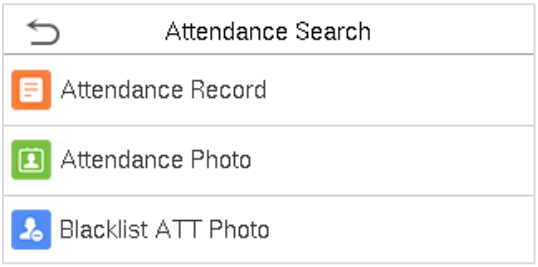


Set the time range and click **OK**.

9 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.

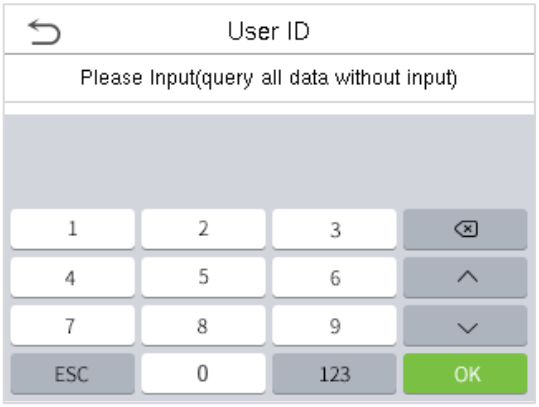
Click **Attendance Search** on the main menu interface.



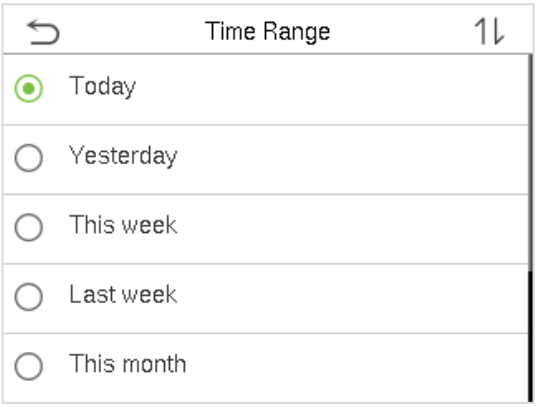
The process of searching for attendance and blacklist photos is similar to that of searching for access records. The following is an example of searching for access records.

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

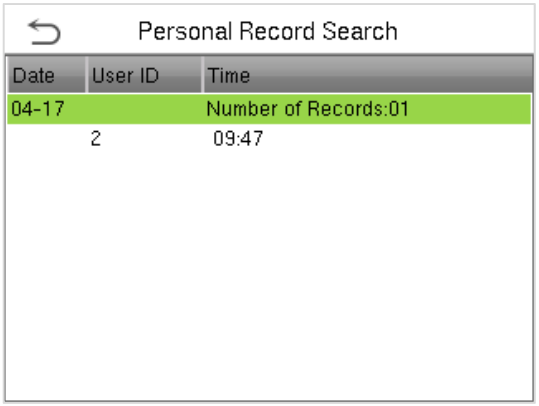
1. Enter the user ID to be searched and click OK. If you want to search for records of all users, click OK without entering any user ID.



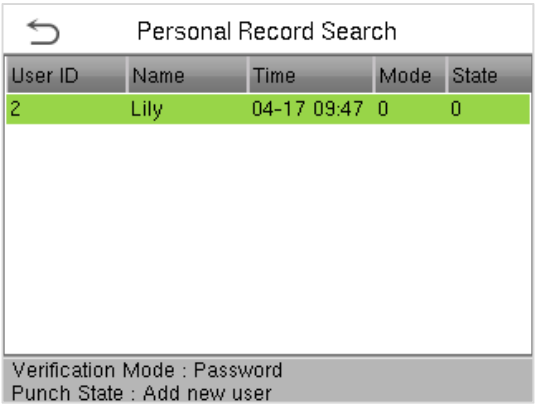
2. Select the time range in which the records you want to search for.



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



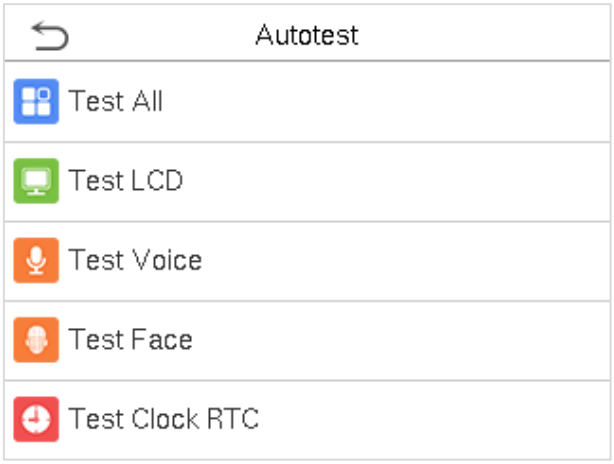
4. The below figure shows the details of the selected record.



10 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.

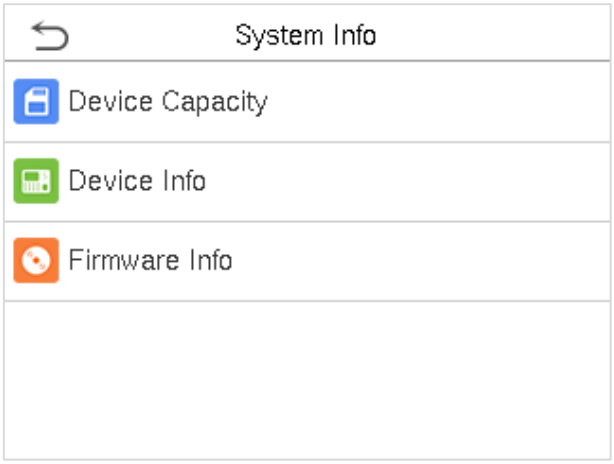


Item	Description
Test All	To automatically test whether the LCD, audio, camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Face	To test if the camera functions properly by checking the photos taken are clear for use.
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.

11 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.



Item	Description
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.

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 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.

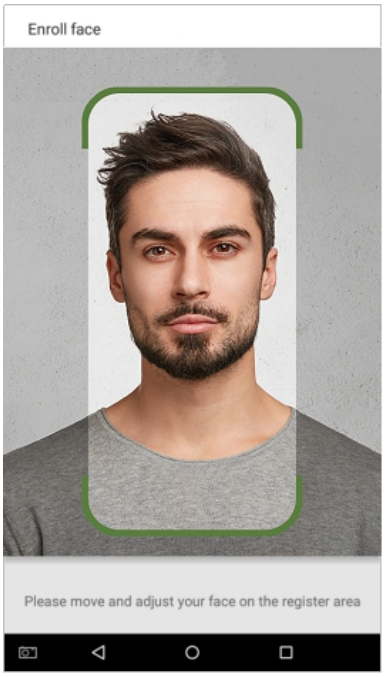


Image1 Face Capture Area

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 appropriate contrast and lightness level.

#24, Shambavi Building, 23rd Main, Marenahalli, JP Nagar 2nd Phase, Bengaluru - 560078
Phone : 91-8026090500 | Email : sales@esslsecurity.com
www.esslsecurity.com