eSSL®
Security at Fingertips

MANUAL

AIFACE NEPTUNE

www.esslsecurity.com | sales@esslsecurity.com

Table of Contents

1 INSTRUCTION FOR USE 4

1.1 STANDING POSITION, FACIAL EXPRESSION AND STANDING POSTURE 4
1.2 FACE REGISTRATION 5
1.3 STANDBY INTERFACE 6
1.4 VIRTUAL KEYBOARD 7
1.5 VERIFICATION MODE 7
1.5.1 FACIAL VERIFICATION 7
1.5.2 CARD VERIFICATION★ 9
1.5.3 PASSWORD VERIFICATION 10
1.5.4 COMBINED VERIFICATION 11

2 MAIN MENU 13

3 USER MANAGEMENT 14

3.1 USER REGISTRATION 14
3.1.1 USER ID AND NAME 14
3.1.2 USER ROLE 14
3.1.3 FACE 15
3.1.4 CARD★ 15
3.1.5 PASSWORD 16
3.1.6 USER PHOTO 17
3.2 SEARCH USER 17
3.3 EDIT USER 18
3.4 DELETE USER 18
3.5 DISPLAY STYLE 19

4 USER ROLE 20

5 COMMUNICATION SETTINGS 21

5.1 ETHERNET SETTINGS 21
5.2 PC CONNECTION 22
5.3 WIRELESS NETWORK★ 22
5.4 CLOUD SERVER SETTING 24
5.5 NETWORK DIAGNOSIS 25

6 SYSTEM SETTINGS 26

6.1 DATE TIME 26
6.2 ATTENDANCE 27
6.3 FACE PARAMETERS 28
6.4 FACTORY RESET 31
6.5 USB UPGRADE 31

7 PERSONALIZE SETTINGS 32

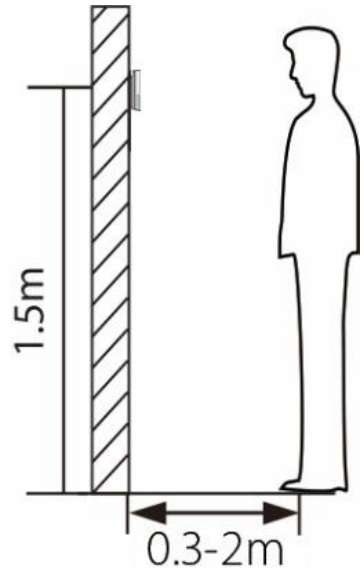
7.1 INTERFACE SETTINGS 32
7.2 VOICE SETTINGS 33
7.3 BELL SCHEDULES 33
7.4 PUNCH STATES OPTIONS 35
7.5 SHORTCUT KEY MAPPINGS 36
8 DATA MANAGEMENT 38
8.1 DELETE DATA 38
9 ACCESS CONTROL 39
9.1 ACCESS CONTROL OPTIONS 39
10 USB MANAGER 40
10.1 DOWNLOAD 40
10.2 UPLOAD 41
10.3 DOWNLOAD OPTIONS 41
11 ATTENDANCE SEARCH 42
12 WORK CODE 43
12.1 ADD A WORK CODE 43
12.2 ALL WORK CODES 44
12.3 WORK CODE OPTIONS 44
13 AUTOTEST 45
14 SYSTEM INFORMATION 46
REQUIREMENTS OF LIVE COLLECTION AND REGISTRATION OF VISIBLE LIGHT FACE IMAGES 47
REQUIREMENTS FOR VISIBLE LIGHT DIGITAL FACE IMAGE DATA 48

1 Instruction for Use

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

1.1 Standing Position, Facial Expression and Standing Posture

- **The recommended distance**



It is recommended to have a 0.5m space between the device and the user whose height is in a range of 1.55m to 1.85m. Users may slightly move forwards or backward to improve the character recognition of facial images captured.

- **Recommended Standing Posture and Facial Expression**

Standing Posture

Facial Expression

NOTE: During enrolment and verification, please maintain natural facial expression and standing posture.

1.2 Face Registration

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

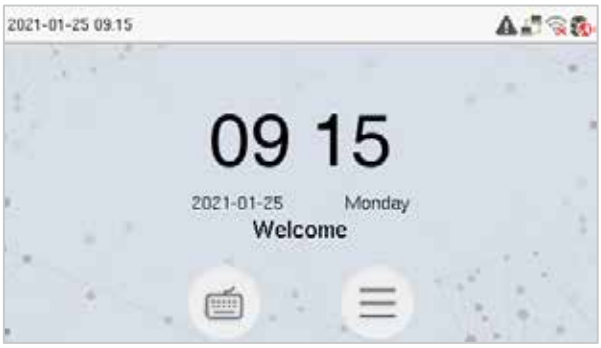
Correct face registration and authentication method

- **Recommendation for registering a face**
  - ❖ When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
  - ❖ Be careful to keep your facial expression natural and not to change. (smiling, 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.

- **Recommendation for authenticating a face**
  - ❖ Ensure that the face appears inside the guideline displayed on the screen of the device.
  - ❖ Sometimes, authentication may fail due to the change in the wearing glasses then the one used while registration. In such a case, you may require authenticating your face with the previously worn glasses. If your face was registered without glasses, you should authenticate your face without glasses further.
  - ❖ 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, the following standby interface is displayed:



- Click to enter the User ID input interface.
- When there is no Super Administrator set in the device, tap to go to the menu.
- After adding a Super Administrator on the device, it requires the Super Administrator's verification before entering the menu functions.

  NOTE: For the security of the device, it is recommended to register super administrator the first time you use the device.

- ★The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:

- Press the corresponding punch state key to select your current punch state, which is displayed in green.

NOTE: The punch state options are off by default and need to be changed to other option. Refer "7.4 Punch States Options" in order to get the punch state options on the standby screen.

1.4 Virtual Keyboard

NOTE:

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

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

1.5 Verification Mode

1.5.1 Facial Verification

- **1:N Facial Verification**

In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.

- **1:1 Facial Verification**

In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Press or main interface and enter the 1:1 facial verification mode and enter the user ID and tap [**OK**].

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

After successful verification, the prompt box displays "**Successfully verified**", as shown below:

If the verification is failed, it prompts "**Please adjust your position!**".

1.5.2 Card Verification★

- **1:N Card Verification**

The 1: N Card Verification mode compares the card number in the card induction area with all the card number data registered in the device; The following is the card verification screen.

- **1:1 Card Verification**

The 1:1 Card Verification mode compares the card number in the card induction area with the number associated with the employee's User ID registered in the device.

Press in the main interface to open the 1:1 card verification mode.

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

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

After successful verification, the prompt box displays "**Successfully verified**", as shown below:

1.5.3 Password Verification

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

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

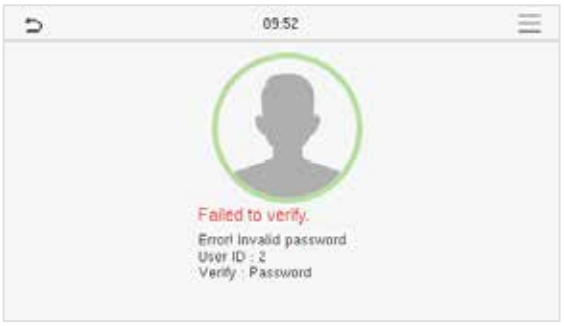
If the user has registered face and card in addition to password, and the verification method is set to password/face/card verification, the following screen will appear. Select the icon to enter password verification mode.

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

Following are the display screen after entering a correct password and a wrong password respectively.

Verification is successful:

Verification is failed:



1.5.4 Combined Verification

For increased security and accessibility, the device offers the option of using multiple forms of verification methods. A total of 9 different verification combinations can be used, as shown below:

Combined Verification Symbol Definition

Symbol	Definition	Explanation
/	or	This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device.
+	and	This method compares the entered verification of a person with all the verification template previously stored to that Personnel ID in the Device.

Procedure to set for Combined Verification Mode

- Combined verification requires personnel to register all the different verification method. Otherwise, employees will not be able to successfully verify through the combined verification process.
- For instance, when an employee has registered only the face data, but the device verification mode is set as "**Face + Password**", the employee will not be able to complete the verification process successfully.
- This is because the device compares the scanned face template of the person with registered verification template (both the Face and the Password) previously stored to that Personnel ID in the Device.
- But as the employee has registered only the Face but not the Password, the verification will not get completed and the Device displays "**Verification Failed**".

2 Main Menu

Press ☰ on the Standby interface to enter the **Main Menu**, the following screen will be displayed:

Function Description

Menu	Descriptions
User Mgt.	To Add, Edit, View, and Delete basic information of a User.
User Role	To set the permission scope of the custom role and enroller for the users, that is, the rights to operate the system.
COMM.	To set the relevant parameters of Ethernet, PC Connection, Wireless Network★, Cloud Server Setting, and Network Diagnosis.
System	To set the parameters related to the system, including Date Time, Attendance, Face Parameter, Reset to factory and USB Upgrade.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options, and Shortcut Key Mappings settings.
Data Mgt.	To delete all relevant data in the device.
Access Control	To set the parameters of the lock.
USB Manager	To upload or download the specific data by a USB drive.
Attendance Search	To query the specified Attendance Record, check Attendance Photo, and Blocklist ATT Photo.
Work Code	Set different type of work.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Camera, and real-time clock.
System Info	To view Data Capacity and Device and Firmware information of the current device.

3 User Management

3.1 User Registration

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

3.1.1 User ID and Name

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

Notes:

1) A name can take up to 36 characters.

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

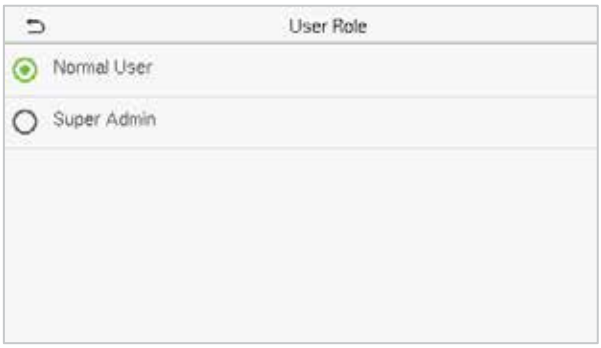
3) During the initial registration, you can modify your ID, which can't be modified after registration.

4） If a message "**Duplicated!**" pops up, you must choose another ID as the enter User ID already exists.

3.1.2 User Role

On the New User interface, tap **User Role** to set the role for the user as either **Normal User** or **Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentication verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with **User Defined Role.** The user can be permitted to access several menu options as required.



NOTE: If the selected user role is the Super Admin, 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 to1.5 Verification Mode.

3.1.3 Face

Tap **Face** in the **New User** interface to enter the face registration page.

- Please face towards the camera and position yourself such that your face image fits inside the white guiding box and stay still during face registration.
- A progress bar shows up while registering the face and a **"Enrolled Successfully"** message is displayed as the progress bar completes.
- If the face is registered already then, the **"Duplicate Face"** message shows up. The registration interface is as follows:

3.1.4 Card★

Tap **Card** in the **New User** interface to enter the card registration page.

- On the Card interface, swipe the card underneath the card reading area. The card registration will be successful.
- If the card is registered already then, the "**Duplicate Card**" message shows up. The registration interface is as follows:

3.1.5 Password

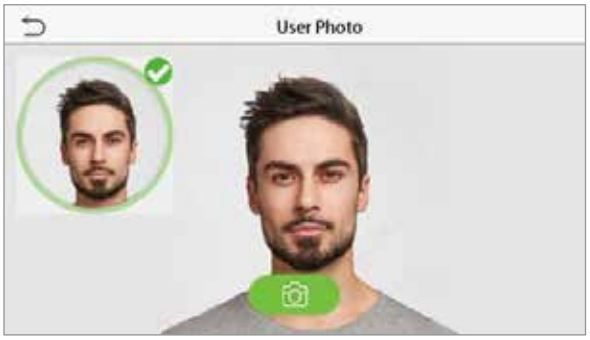
Tap **Password** in the **New User** interface to enter the password registration page.

- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to confirm the password again.

NOTE: The password may contain 1 to 8 digits by default.

3.1.6 User Photo

Tap on **User Photo** in the **New User** interface to go to the User Photo registration page.



- When a user registered with a photo authenticates successfully, the registered photo is displayed.
- Tap **User Photo** to open the device's camera, then tap the camera icon to take a photo. The captured photo is displayed on the top left corner of the screen and the camera opens up again to take a new photo, after taking the initial photo.

NOTE: While registering a face, the system automatically captures a photo as the user photo. If you do not register a user photo, the system automatically sets the photo captured while registration as the default photo.

3.2 Search User

On the **Main Menu**, tap **User Mgt.,** and then tap **All Users** to search for a User.

- On the **All Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.

3.3 Edit User

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

NOTE: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified when editing a user. The process in detail refers to "3 User Management".

3.4 Delete User

On the **All Users** interface, tap on the required user from the list and tap **Delete** to delete the user or a specific user information from the device. On the **Delete** interface, tap on the required operation and then tap **OK** to confirm the deletion.

Delete Operations

Delete User: Deletes all the user information (deletes the selected User as a whole) from the device.

Delete Face Only: Deletes the face information of the selected user.

Delete Password Only: Deletes the password information of the selected user.

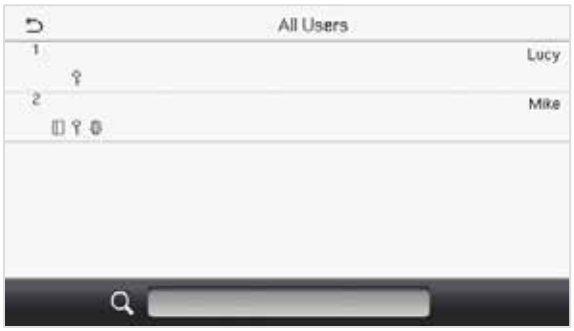
Delete User Photo Only: Deletes the photo of the selected user.

3.5 Display Style

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

All the Display Styles are shown as below:

Single Line Style



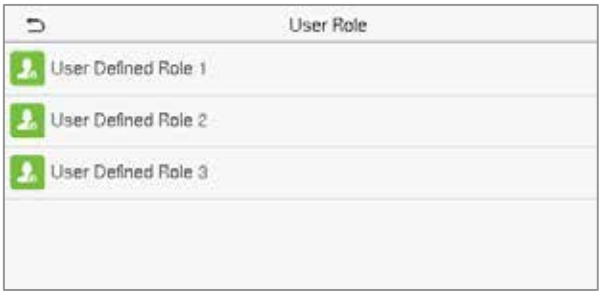
Multiple Line Style

Mixed Line Style

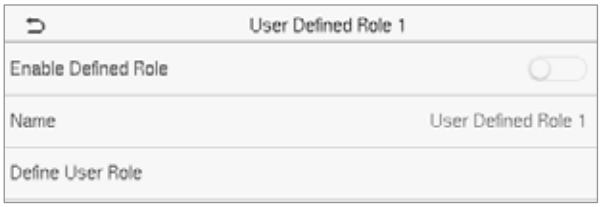
4 User Role

User Role facilitates assigning some specific permissions to certain users based on the requirement.

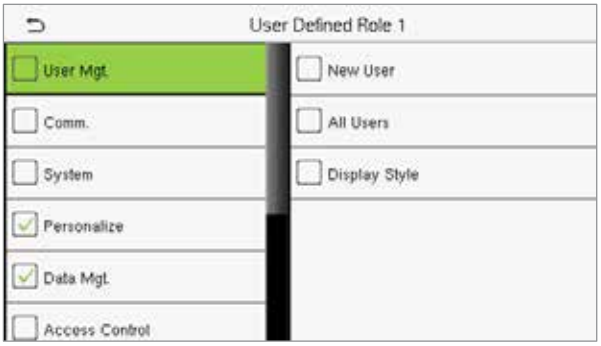
- On the **Main** menu, tap **User Role** > **User Defined Role** to set the user defined permissions.
- A total of 3 different custom roles can be added. It is the custom operating scope of a user.

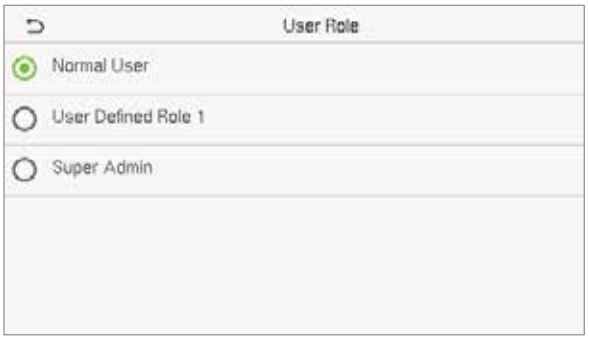


- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.



- Then, tap on **Define User Role** and select the required privileges to assign to the new role, and then tap on the **Return** button.
- During privilege assignment, the **Main Menu** function names are displayed on the left and its sub-menus are listed on its right.
- First, tap on the required **Main Menu** function name, and then select its required sub-menus from the list which the user can access.

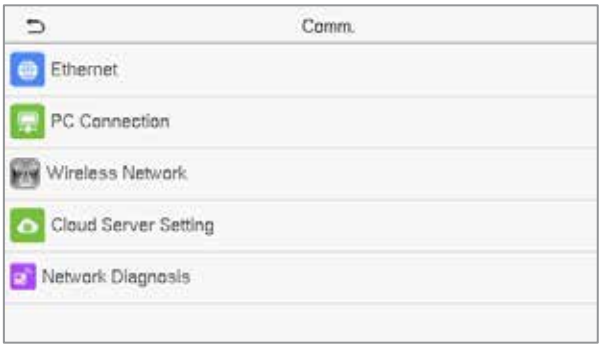




NOTE: If the User Role is enabled for the device, tap on **User Mgt. > New User > User Role** to assign the created roles to the required users. But if there is no super administrator registered in the device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role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

5 Communication Settings

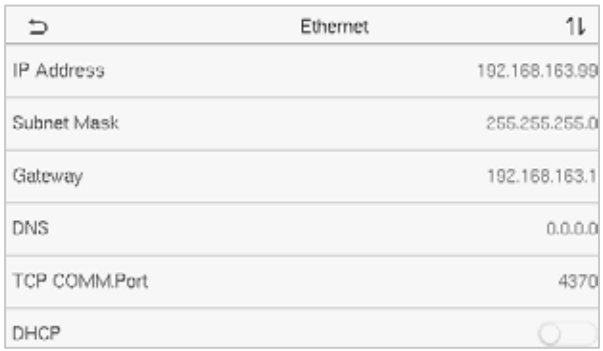
Tap **COMM.** on the **Main Menu** to set the relevant parameters of Ethernet, PC Connection, Wireless Network★, Cloud Server, and Network Diagnosis.



5.1 Ethernet Settings

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

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



Function Description

Function Name	Descriptions
IP Address	The default IP address is 192.168.1.201. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.
DNS	The default DNS address is 0.0.0.0. It can be modified according to the network availability.

TCP COMM. Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
DHCP	It stands for Dynamic Host Configuration Protocol. It dynamically allocates IP addresses for clients via server.
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.

5.2 PC Connection

Comm Key facilitates to improve the security of data by setting the communication between the device and the PC. Once the Comm Key is set, a connection password is required to connect the device to the PC software.

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

Function Description

Function Name	Descriptions
Comm Key	The default password is 0 and can be changed later. The Comm Key can contain1-6 digits.
Device ID	It is the identification number of the device, which ranges between 1 and 254.

5.3 Wireless Network★

The device provides a Wi-Fi module, which can be built-in within the device module or can be externally connected.

The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

Tap **Wireless Network** on the **Comm.** settings interface to configure the Wi-Fi settings.

Search the WIFI Network

- WIFI is enabled in the device by default. Toggle the button to enable or disable WIFI.
- Once the Wi-Fi is turned on, the device searches for the available WIFI within the network range.
- Tap on the required Wi-Fi name from the available list and input the correct password in the password interface, and then tap **Connect to WIFI (OK)**.

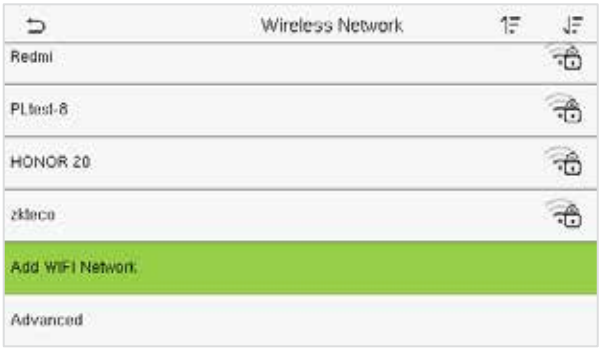
WIFI Enabled: Tap on the required network from the searched network list.

Tap on the password field to enter the password, and then tap on **Connect to WIFI (OK).**

- When the WIFI is connected successfully, the initial interface will display the Wi-Fi logo.

Add WIFI Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.



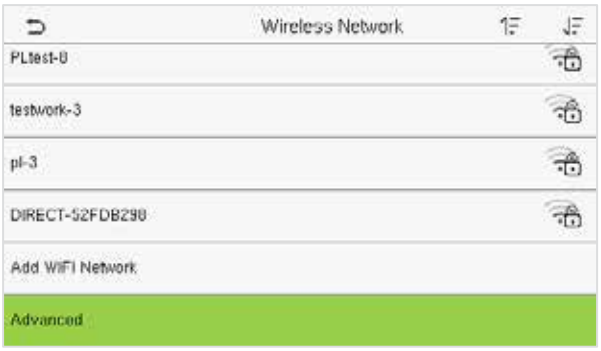
Tap on **Add WIFI Network** to add the WIFI manually.

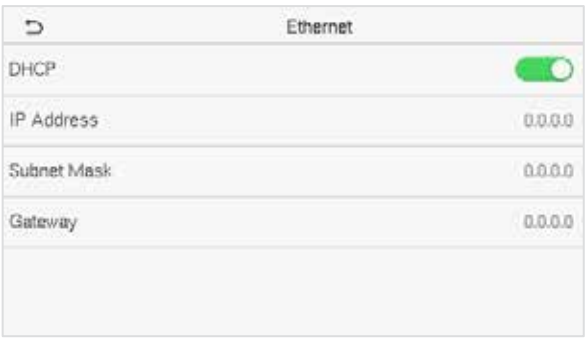
On this interface, enter the WIFI network parameters. (the added network must exist.)

NOTE: After successfully adding the WIFI manually, follow the same process to search for the added WIFI name. Click here to view the process to search the WIFI network.

Advanced Setting

On the **Wireless Network** interface, tap on **Advanced** to set the relevant parameters as required.





Function Description

Function Name	Description
DHCP	Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually.
IP Address	The IP address for the WIFI network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the WIFI network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. It can be modified according to the network availability.

5.4 Cloud Server Setting

Tap **Cloud Server Setting** on the **Comm.** settings interface to connect with the ADMS server.

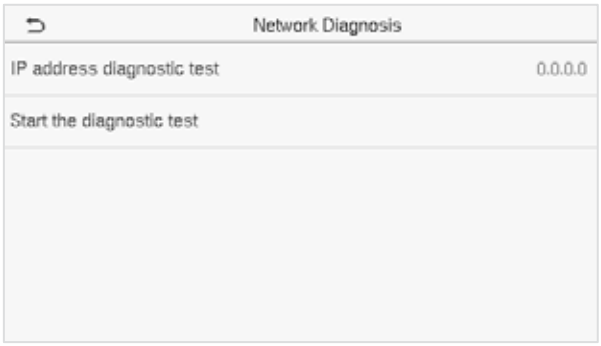
Function Description

Function Name		Description
Enable Domain Name	**Server Address**	Once this function is turned **ON**, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name.
Disable Domain Name	**Server Address**	The IP address of the ADMS server.
	Server Port	Port used by the ADMS server.
Enable Proxy Server		The IP address and the port number of the proxy server is set manually when the proxy is enabled.
HTTPS		Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

5.5 Network Diagnosis

It helps to set the network diagnosis parameters.

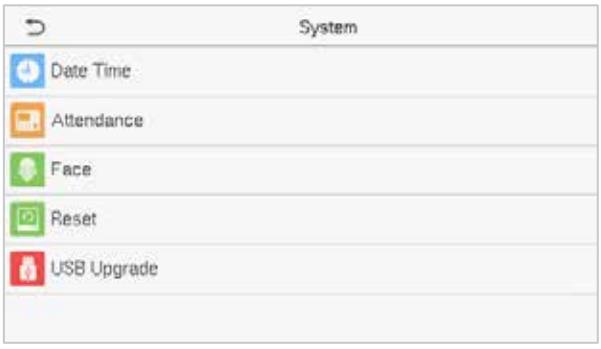
Tap **Network Diagnosis** on the **Comm.** settings interface. Enter the IP address that needs to be diagnosed and tap **Start the diagnostic test** to check whether the network can connect to the device.



6 System Settings

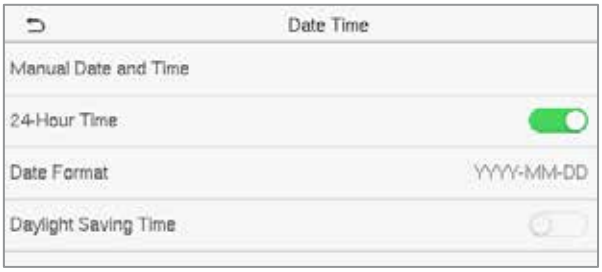
It helps to set related system parameters to optimize the accessibility of the device.

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



6.1 Date Time

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



- Tap **Manual Date and Time** 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 i.e., the way date should be displayed on the device.
- 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 time.

Week Mode

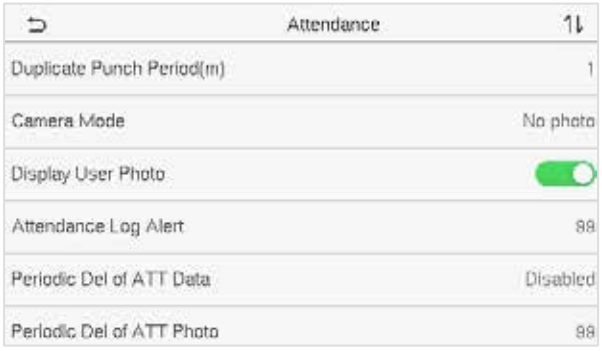
Date Mode

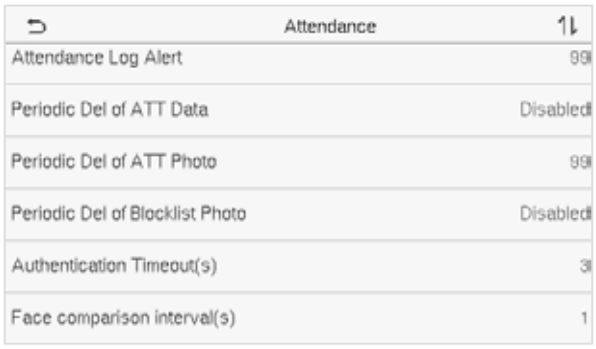
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

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.

6.2 Attendance

Click **Attendance** on the System interface.





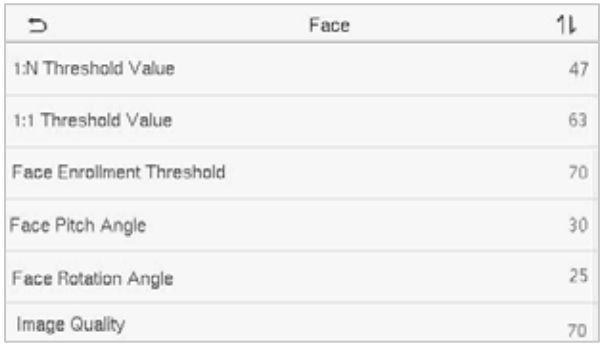
Function Description

Function Name	Description
Duplicate Punch Period(m)	Within a set time period (unit: minutes), the duplicated attendance record will not be reserved (value ranges from 1 to 999999 minutes).
Camera Mode	Choose 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 not saved during verification. **Take photo and save:** Photo is taken and saved during verification. **Save on successful verification:** Photo is taken and saved for each successful verification. **Save on failed verification:** Photo is taken and saved only for each failed verification.
Display User Photo	Choose whether to display the user photo when the user passes the verification.
Attendance Log Alert	When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning. Users may disable the function or set a valid value between 1 and 9999.
Periodic Del of ATT Data	When attendance records reach its maximum storage capacity, the device automatically deletes a set of old attendance records. Users may disable the function or set a valid value between 1 and 999.
Periodic Del of ATT Photo	When attendance photos reach its maximum storage capacity, the device automatically deletes a set of old attendance photos.

	Users may disable the function or set a valid value between 1 and 99.
Periodic Del of Blocklist Photo	When block listed photos reach its maximum storage capacity, the device automatically deletes a set of old block listed photos. Users may disable the function or set a valid value between 1 and 99.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1~9 seconds.
Face comparison interval (s)	The amount of time required to compare facial templates. Valid value: 0~9 seconds.

6.3 Face Parameters

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



Function Description

Function Name	Description
1:N Threshold Value	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 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher the rejection rate, and vice versa. It is recommended to set the default value of 47.
1:1 Threshold Value	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 0 to 100. The higher the thresholds, the lower the misjudgement rate and 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 the set threshold, it indicates that the face has already been registered.
Face Pitch Angle	It is the pitch angle tolerance of a face for facial template registration and comparison. If a face's pitch angle exceeds the 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	It is the rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds the 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	It is the image quality for facial registration and comparison. The higher the value, the clearer image is required.
Minimum Face Size	It sets the minimum face size required for facial registration and comparison. If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face. This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.

LED Light Triggered Value	This value controls the turning on and off of the LED light. The larger the value, the LED light will turn on or off more frequently.
Motion Detection Sensitivity	It sets the value for the amount of change in a camera's field of view 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 activates with much ease, and the motion detection is frequently triggered.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
Anti-spoofing using NIR	It uses near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Face Algorithm	It has facial algorithm related information and pause facial template update.

NOTE: 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

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.

6.5 USB Upgrade

With this option, the device firmware can be upgraded by using the upgrade file on a USB disk. Before conducting this operation, ensure that the USB disk is properly inserted into the device and contains the correct upgrade file.

If no USB disk is plugged in, the system gives the following prompt after you tap **USB Upgrade** on the **System** interface.

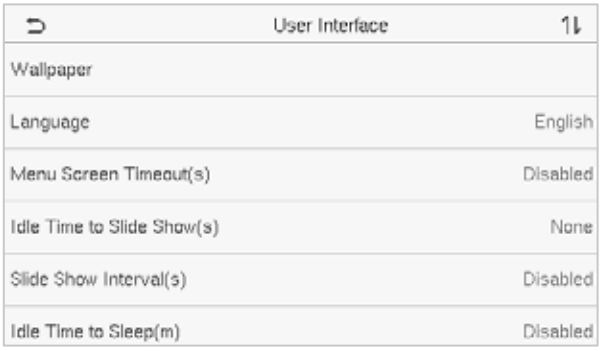
NOTE: If an upgrade file is required, please contact our technical support. A firmware upgrade is not recommenced under normal circumstances.

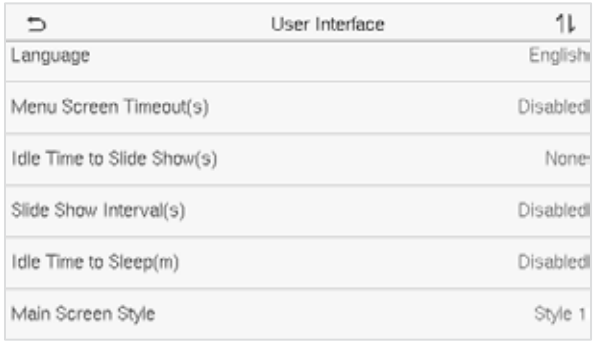
7 Personalize Settings

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

7.1 Interface Settings

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





Function Description

Function Name	Description
Wallpaper	It helps to select the main screen wallpaper according to the user preference.
Language	It helps to select the language of the device.
Menu Screen Timeout (s)	When there is no operation, and the time exceeds the set value, the device automatically goes back to the initial interface. The function can either be disabled or set the required value between 60 and 99999 seconds.
Idle Time To Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show is displayed. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show	It is the time interval in switching between different slide show pictures. The

Interval (s)	function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If the sleep mode is activated, and when there is no operation in the device, then the device will enter standby mode. This function can be disabled or set a value within 1-999 minutes.
Main Screen Style	It helps selecting the main screen style according to the user preference.

7.2 Voice Settings

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

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.

7.3 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.

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 ranges from 1 to 999 seconds.

All Bell Schedules

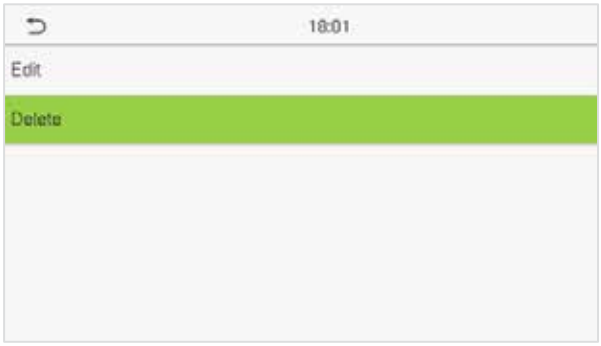
Once the bell is scheduled, on the **Bell Schedules** interface, tap **All Bell Schedules** to view the newly scheduled bell.

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.

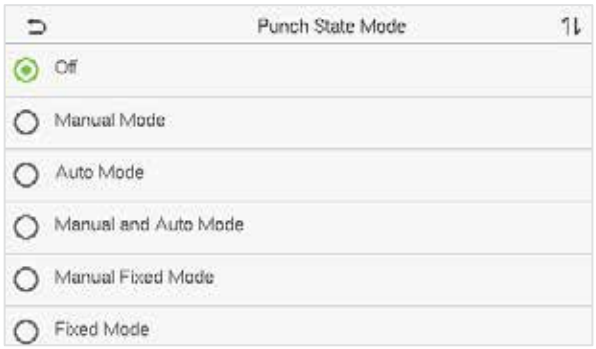
Delete a bell

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



7.4 Punch States Options

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



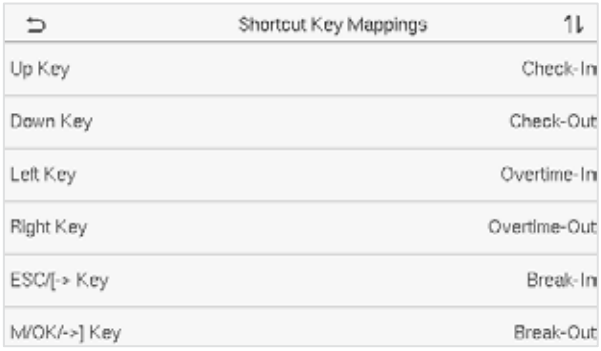
Function Description

Function Name	Description
Punch State Mode	**Off:** It disables the punch state function. And the punch state key set under the **Shortcut Key Mappings** menu becomes 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 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 an 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 is shown. Users cannot change the status by pressing any other keys.

7.5 Shortcut Key Mappings

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

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



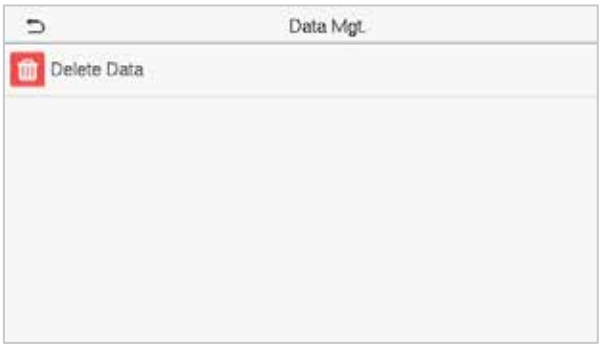
- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key (**that is "Up Key"**)** interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut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

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

8 Data Management

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



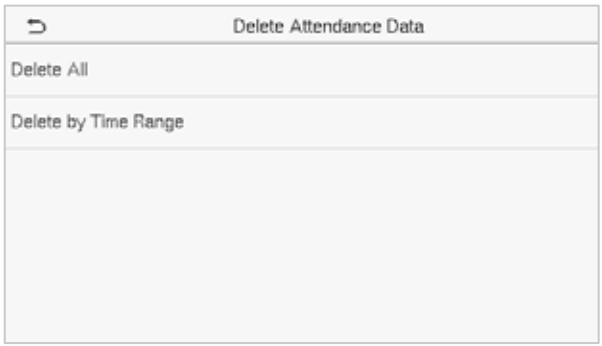
8.1 Delete Data

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

Function Description

Function Name	Description
Delete Attendance Data	To delete attendance 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 records of all registered users.
Delete Admin Role	To remove all administrator privileges.
Delete User Photo	To delete all user photos in the device.
Delete Wallpaper	To delete all wallpapers in the device.
Delete Screen Savers	To delete the screen savers in the device.

NOTE: The user may select Delete All or Delete by Time Range when deleting the attendance records, attendance photos, or block listed photos. When selecting Delete by Time Range, you need to set a time range to delete all data within the specified time.



Select Delete by Time Range

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

9 Access Control

On the **Main Menu**, tap **Access Control** to set the schedule of lock.

9.1 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
Door Lock Delay (s)	The amount of time that the device controls the electric lock to be in unlock

	state. Valid value: 1~10 seconds; 0 seconds represents disabling the function.
Door Sensor Delay (s)	An alarm is triggered if the door is not closed within a defined time (Door Sensor Delay). The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: **None, Normal Open,** and **Normal Closed**. **None:** It means the door sensor is not in use. **Normal Open:** The door is always open when electric power is on. **Normal Closed:** The door is always close when electric power is on.

10 USB Manager

You can import the user information, work code, and attendance data in the device to match the attendance for processing by using a USB disk or import the user information and work code to other fingerprint devices for backup.

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

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

10.1 Download

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

Function Name	Description

Attendance Data	To download attendance data in a specified time into a USB disk.
User Data	To download all user information from the device into a USB disk.
User Portrait	To download all user photos from the device into a USB disk.
Attendance Photo	To download all attendance photos from the device into a USB disk.
Blocklist Photo	To download all block listed photos (photos taken after failed verifications) from the device into a USB disk.
Work Code	To save the work code in the device to a USB disk.

10.2 Upload

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

Function Name	Description
Screen Saver	To upload all screen savers from USB disk into the device. You can choose **Upload selected photo** or **Upload all photos**. The images will be displayed on the device's main interface once uploaded. Create a folder named "**advertise**" in the root directory of the USB disk and put the advertising photos in this directory before uploading.
Wallpaper	To upload all wallpapers from USB disk into the device. You can choose **Upload selected photo** or **Upload all photos**. The images will be displayed on the screen once uploaded. Create a folder named "**wallpaper**" in the root directory of the USB disk and put the wallpaper photos in this directory before uploading.
User Date	To upload all the user information from the USB disk into the device.
User Portrait	To upload all user photos from a USB disk into the device.
Upload Work Code	To upload work code from a USB disk into the device.

10.3 Download Options

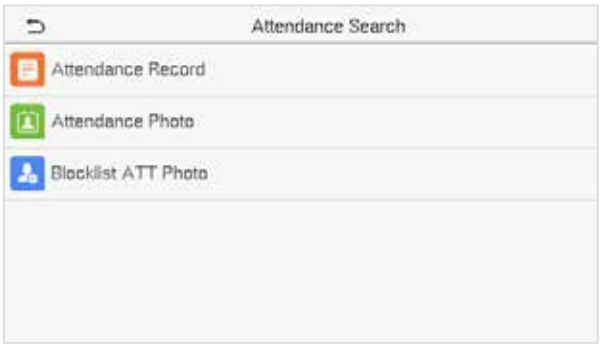
Tap **Download Options** on the **USB Manager interface**.

Function Name	Description
Encrypt Attendance Date	The attendance data is encrypted during the uploading and downloading.
Delete ATT Data	After successful downloading, the attendance data on the device is deleted.

11 Attendance Search

Once the identity of a user is verified, the Attendance Record is saved in the device. This function enables users to check their access records.

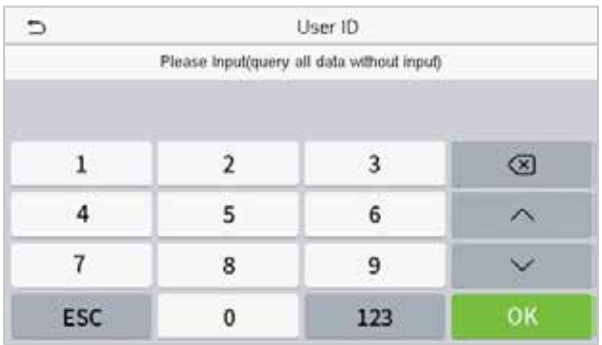
Click **Attendance Search** on the **Main Menu** interface to search for the required Attendance Record.



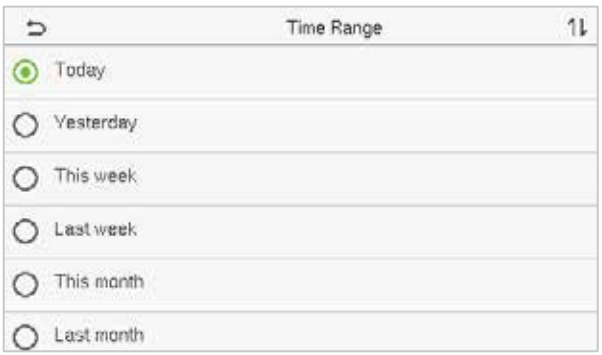
The process of searching for attendance and blocklist photos is similar to that of searching for Attendance Record. The following is an example of searching for Attendance Record.

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

1. Enter the user ID to be searched and click **OK**. For the records of all users, click **OK** without entering any user ID.



2. Select the time range within which the logs need to be searched.



3. Once the log search succeeds, tap the record highlighted in green to view its details.

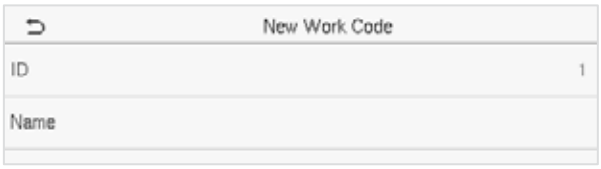
4. The below figure shows the details of the selected record.

12 Work Code

Employees' salaries are subject to their attendance records. An employee can be engaged in more than one type of work which may vary with time. As the pay varies according to the work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

On the **Main Menu**, tap **Work Code** to set the work code.

12.1 Add a Work Code



Function Description

Function Name	Description
ID	It is the digital code of the work code. Users may set a valid value between 1 and 99999999.
Name	It is the naming of the work code.

12.2 All Work Codes

You can view, edit and delete work codes in All Work Codes. The process of editing a work code is the same as adding a work code, except that the ID is not allowed to be modified.

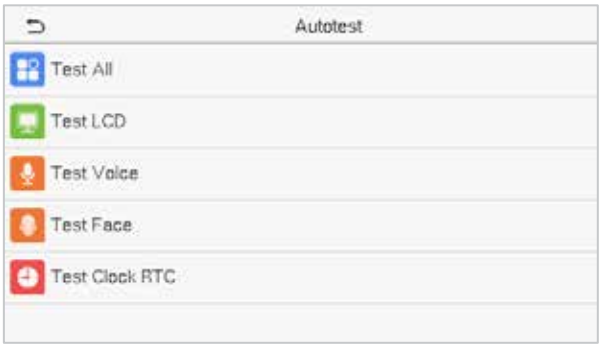
12.3 Work Code Options

To set whether entering the work code is a must and whether the entered work code must exist during authentication.

In **1: N** or **1:1** verification, the system will automatically pop up the following window. Select the corresponding Word Code manually to verify successfully.

13 Autotest

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

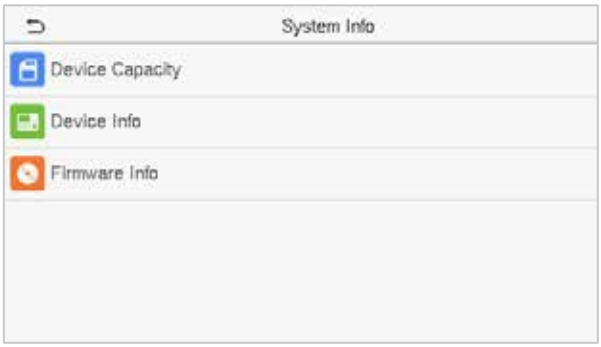


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Audio, Camera and RTC are working normally.
Test LCD	To automatically test the display of the LCD screen by displaying all the color bands including pure white and pure black to check whether the screen displays the colors accurately.
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 it checks the photos taken and determines if they are clear enough.
Test Clock RTC	To test the RTC. The device checks whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and press it again to stop counting.

14 System Information

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



Function Description

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

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 on the face.

2) Do not place the device towards outdoor light sources like door or window or other harsh light sources.

3) Dark-color apparels other than the background color is recommended for registration.

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

5) It is recommended to show a normal 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 them.

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).

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**

A neutral face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

The horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- **Accessories**

Masks or coloured eyeglasses are not allowed. The frame of the eyeglasses should not cover the eyes and should not reflect light. For persons with thick eyeglasses frames, it is recommended to capture two images, one with eyeglasses and the other one without them.

- **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 441 x 358 to 1920 x 1080.

5) The vertical scale of head and body should be in a ratio of 2:1.

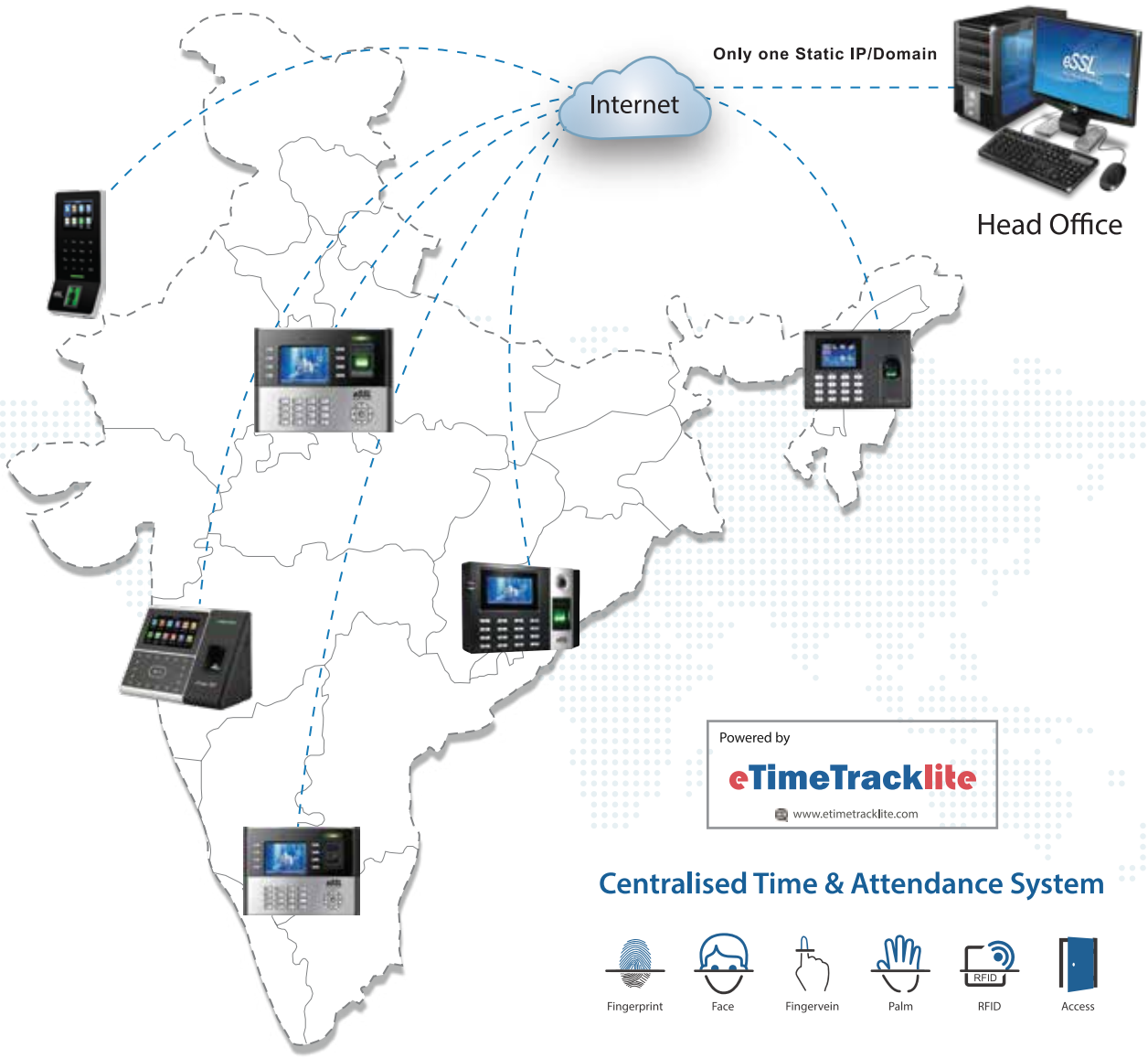
6) The photo should include the captured person's shoulders at the same horizontal level.

7) The captured person's eyes should be open and with a clearly seen iris.

8) A neutral face or smile is preferred, showing teeth is not preferred.

9) The captured person should be easily visible, natural in color, no harsh shadow or light spot or reflection in the face or background. The contrast and lightness level should be appropriate.

Manage Time & Attendance for all your Branches from Head Office



Disclaimer : Specifications can be changed without prior notice.

1. Buying and Selling eSSL products online is prohibited and is termed as illegal
2. Installation / Technical support / Training to end user is the responsibility of the installer or dealer
3. eSSL do not support end user directly, if they want support charges will be applicable

Enterprise Software Solutions Lab Pvt. Ltd. (Corporate-Office)
#24, 23rd main, Shambhavi Building, J P nagar 2nd phase, Bengaluru - 560078
www.esslsecurity.com | sales@esslsecurity.com | Ph : 91-8026090500