

VEGA+W+POE



Table of Contents

1	INSTRUCTION FOR USE	3
1.1	Finger Positioning	4
1.2	Standby Interface.....	4
1.3	Verification Mode	6
1.3.1	Fingerprint Verification.....	6
1.3.2	Card Verification.....	7
1.3.3	Password Verification	8
1.3.4	Combined Verification	9
2	MAIN MENU.....	10
3	USER MANAGEMENT	12
3.1	New User Registration	12
3.1.1	Register a User ID and Name	12
3.1.2	User Role	13
3.1.3	Register Fingerprint.....	13
3.1.4	Card Number	14
3.1.5	Password.....	14
3.1.6	Access Control Role	15
3.2	All Users.....	15
3.2.1	Edit User.....	16
3.2.2	Delete User	16
3.3	Display Style	17
4	USER ROLE.....	18
5	COMMUNICATION	20
5.1	Ethernet	20
5.2	Serial Comm	21
5.3	PC Connection.....	21
5.4	Wi-Fi Settings★.....	22
5.5	Cloud Server Settings	25
5.6	Wiegand Setup	25
5.6.1	Wiegand Input	26
5.6.2	Wiegand Output	28
5.7	Network Diagnosis.....	29
6	SYSTEM SETTINGS	30
6.1	Date and Time	30
6.2	Access Logs Settings / Attendance	31
6.3	Fingerprint.....	32
6.4	Device Type Settings.....	34
6.5	Security Settings	34

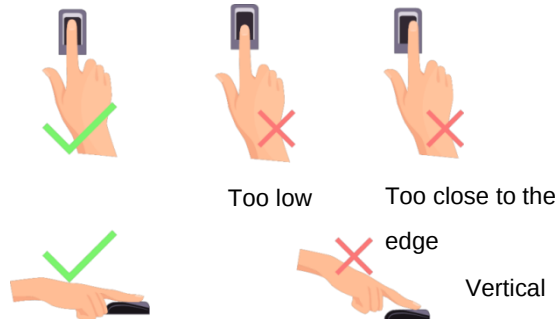
6.6	USB Upgrade	35
6.7	Update Firmware Online	35
6.8	Factory Reset.....	36
7	PERSONALIZE SETTINGS	37
7.1	User Interface	37
7.2	Voice	38
7.3	Bell Schedules	38
7.4	Punch States Options	40
7.5	Shortcut Key Mappings.....	41
8	DATA MANAGEMENT	43
9	ACCESS CONTROL	45
9.1	Access Control Options	46
9.2	Time Rule Settings / Time Schedule	50
9.3	Holidays	51
9.4	Access Groups.....	52
9.5	Combined Verification.....	53
9.6	Anti-passback Setup	54
9.7	Duress Options Settings	56
10	USB MANAGER	58
10.1	USB Download	58
10.2	USB Upload	59
10.3	Download Options.....	60
11	ATTENDANCE SEARCH	61
12	WORK CODE	62
12.1	Add a Work Code.....	62
12.2	All Work Codes	62
12.3	Work Code Options.....	63
13	AUTOTEST.....	64
14	SYSTEM INFORMATION	65

1 Instruction for Use

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

1.1 Finger Positioning

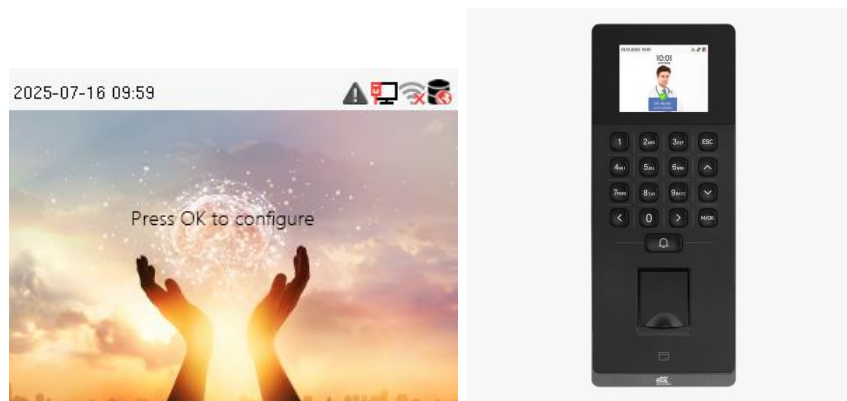
Recommended fingers: The index, middle, or ring finger and avoid using the thumb or pinky fingers, as they are difficult to accurately press onto the fingerprint reader.



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

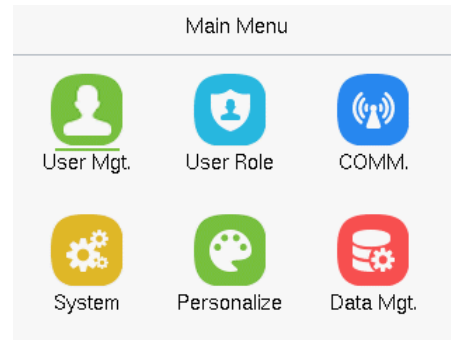
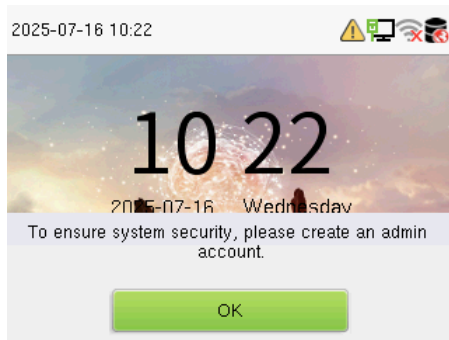
1.2 Standby Interface

The device uses a 2.4-inch color screen, which all operations are performed through the keypad. After connecting the power supply for the first time, the following standby interface is displayed:

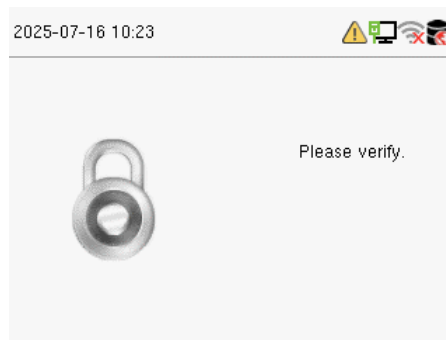


Press **M/OK** to enter the Settings interface:

- When there is no Super Administrator set in the device, press **M/OK** to go to the menu.



- After adding a Super Administrator on the device, it requires the Super Administrator's verification before opening the menu functions.



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

- On the standby interface, the punch state options can also be shown and used directly. The black bold shortcut key mappings will be displayed on the screen if you press the relevant shortcut key on the keypad, as shown in the picture below. For the specific operation method, please see "Shortcut Key Mappings."



Note: The punch state options are only available when the device type is set as T&A PUSH.

1.3 Verification Mode

1.3.1 Fingerprint Verification

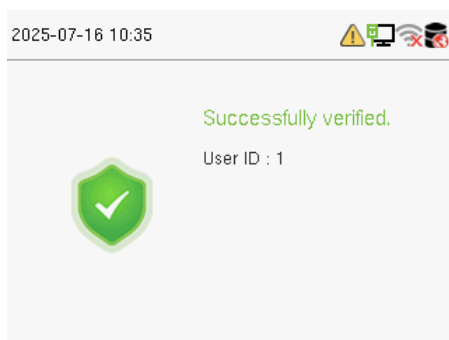
➤ 1: N Fingerprint Verification Mode

The device compares the current fingerprint with the available fingerprint data stored in its database.

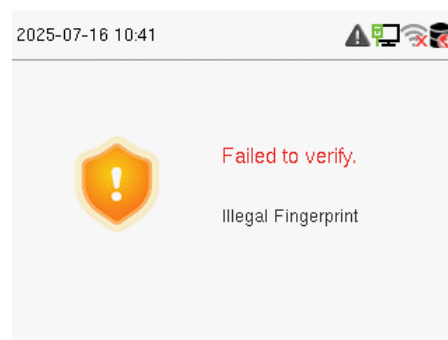
Fingerprint authentication mode is activated when a user places their finger onto the fingerprint scanner.

Please follow the recommended way to place your finger onto the sensor. For details, refer to section Finger Positioning.

Verification is successful:



Verification is failed:

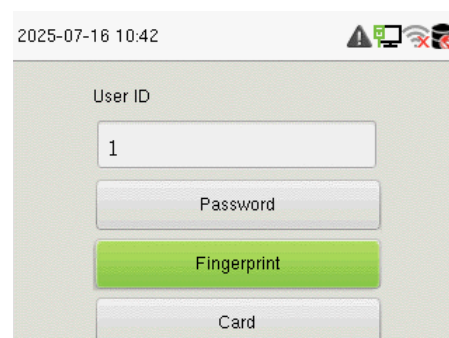
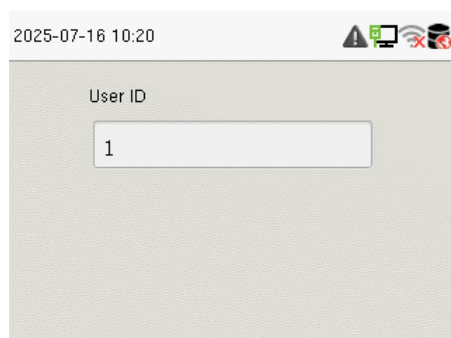


➤ 1:1 Fingerprint Verification Mode

The device compares the current fingerprint with the fingerprints linked to the entered User ID through the virtual keyboard.

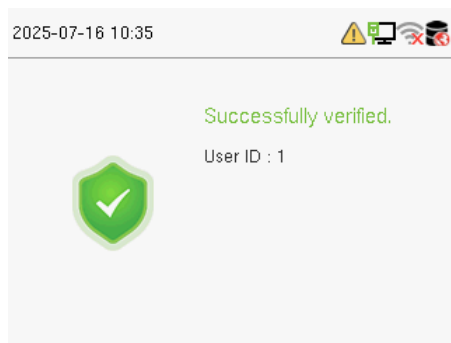
In case users are unable to gain access using the 1:N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

Enter the user ID and press **M/OK**. If an employee registers a password and card in addition to the fingerprint, the following screen will appear. Select **Fingerprint** to enter the 1:1 fingerprint verification mode.

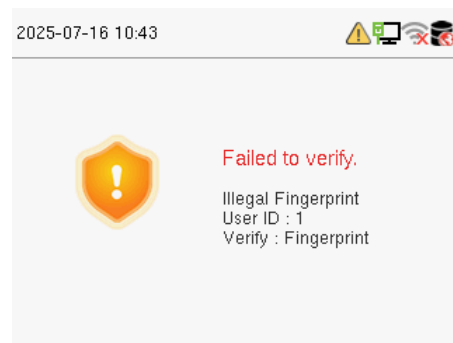


Press the fingerprint to verify.

Verification is successful:



Verification is failed:

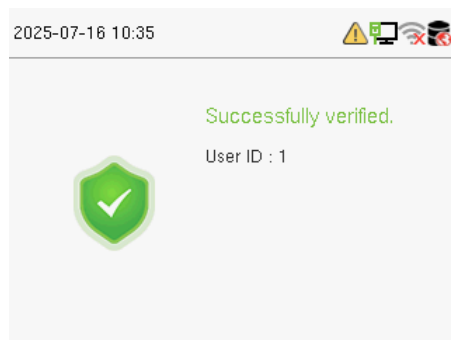


1.3.2 Card Verification

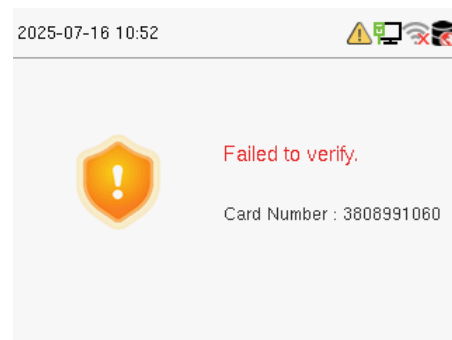
➤ 1: N Card Verification Mode

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 screen displays on the card verification screen.

Verification is successful:



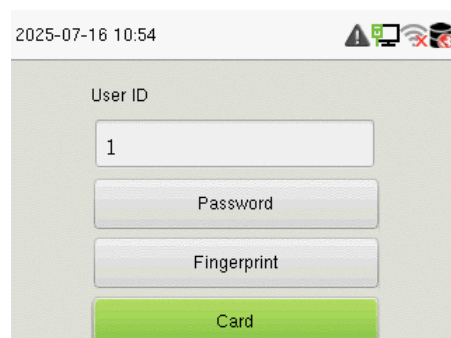
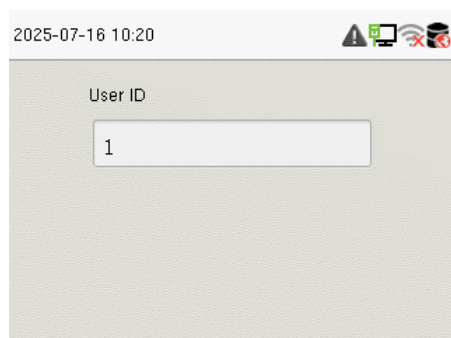
Verification is failed:



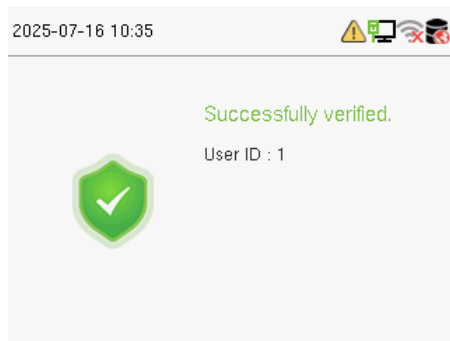
➤ 1:1 Card Verification Mode

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.

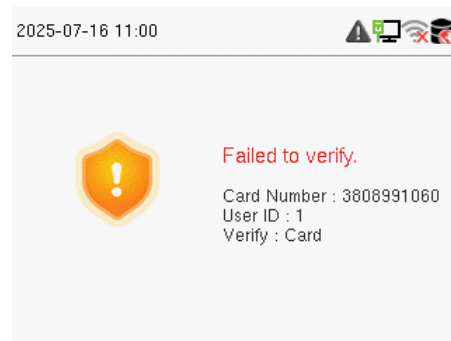
Enter the user ID and press **M/OK**. If an employee registers a fingerprint and password in addition to the card, the following screen will appear. Select **Card** to enter the 1:1 card verification mode.



Verification is successful:



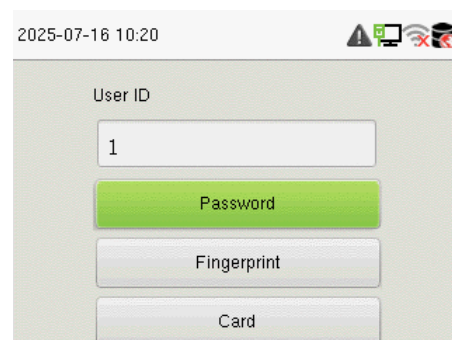
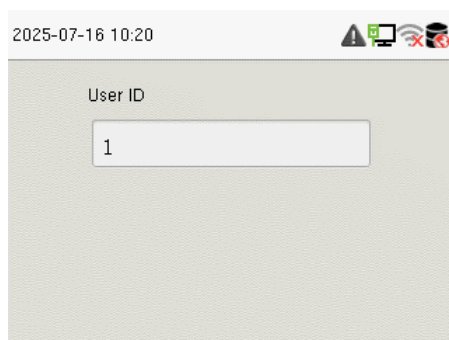
Verification is failed:



1.3.3 Password Verification

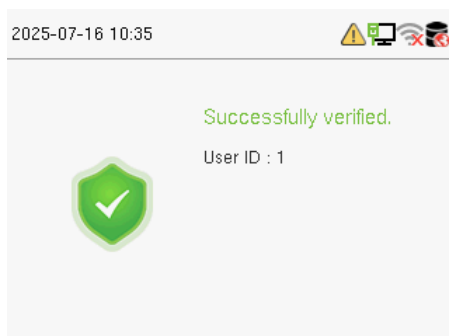
The device compares the entered password with the registered password and User ID.

Enter the user ID and press **M/OK**. If an employee registers a fingerprint and card in addition to the password, the following screen will appear. Select **Password** to enter the 1:1 password verification mode.

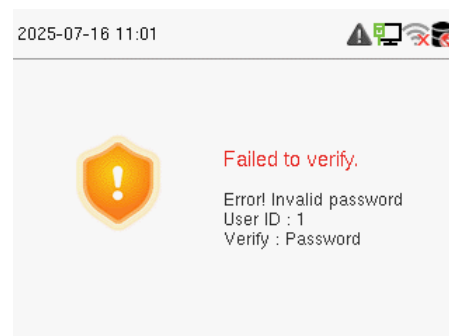


Below are the display screens after entering a correct password and a wrong password, respectively.

Verification is successful:



Verification is failed:

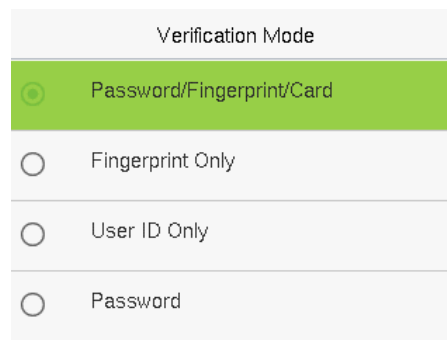


1.3.4 Combined Verification

This device allows you to use different types of verification methods to increase security. There are a total of 15 different verification combinations that can be implemented, as listed 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 templates previously stored to that Personnel ID in the Device.



Verification Mode

☒ Password/Fingerprint/Card

☐ Fingerprint Only

☐ User ID Only

☐ Password

Combined Verification Mode set up procedure:

- Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.
- For example, if an employee has only registered for password data but the Device verification mode is set to "Password + Card", the employee will not be able to successfully complete the verification procedure.

Reason:

- This is because the Device compares the password template of the person with the registered verification template (both the Card and the Password) previously stored to that Personnel ID in the Device.
- But, since the employee has only registered their password and not their card, the verification process will not be successful, and the device will display the "Verification Failed."

2 Main Menu

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

Note: The menu display may vary depending on the device type (BEST Protocol/A&C PUSH/T&A PUSH).



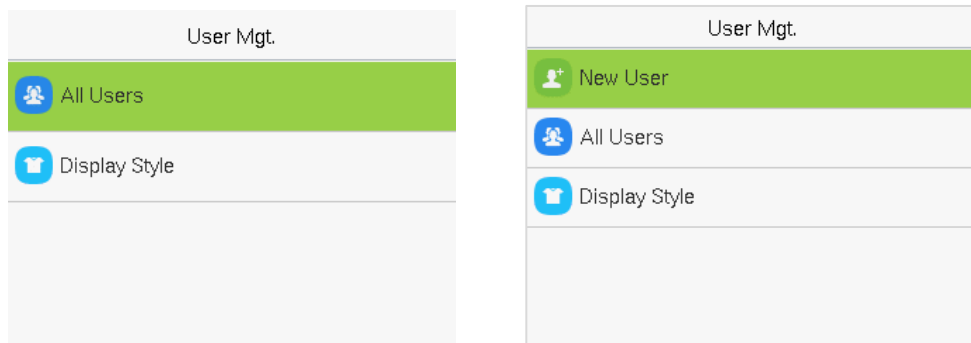
Function Description

Menu	Description
User Mgt.	To Add, Edit, View, and Delete information of a User. (Only support viewing user information when the device type is BEST Protocol.)

User Role	To set the permission scope of the custom role and enroller for the users, for example the system's operating rights.
COMM.	To set the relevant parameters of Network, Serial Comm, PC Connection, Wi-Fi★, Cloud Server, Wiegand and Network Diagnosis.
System	To set parameters related to the system, including Date Time, Attendance/Access Logs Settings, Fingerprint, Device Type Settings, USB Upgrade, Security Settings, Update Firmware Online and resetting to factory settings.
Personalize	To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings.
Data Mgt.	To delete the data.
Access Control	To set the parameters of the lock and the relevant access control device including options like Time schedule/Time rule settings, Holiday Settings, Access groups, Combine verification, Anti-Passback Setup, and Duress Option Settings.
USB Manager	To upload or download the specific data by a USB drive.
Attendance Search	To query the specified event logs.
Work Code	Set different type of work.
Autotest	To automatically test whether each module functions properly, including the LCD Screen, Audio, Keyboard, fingerprint sensor and Real-Time Clock.
System Info	To view Privacy Policy, Data Capacity and Device and Firmware information of the current device.

3 User Management

When the device is on the initial interface, press **[M/OK]** button and enter **User Mgt.**.



3.1 New User Registration

Select **New User** on the **User Mgt.** interface to add a new user.

3.1.1 Register a User ID and Name

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

New User	
User ID	1
Name	
User Role	Normal User
Fingerprint	0

Note:

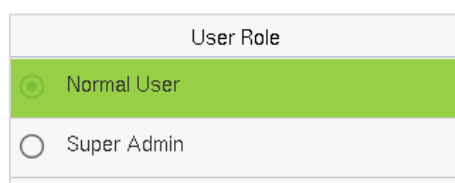
1. A name can be taken up to 36 characters long.
2. The user ID may contain 1 to 14 digits by default, supporting both numbers and alphabetic characters.
3. During the initial registration, you can modify your ID, but not after registration.
4. If the message "**Duplicated!**" appears, you must choose a different User ID because the one

you entered already exists.

3.1.2 User Role

On the **New User** interface, select **User Role** to set the user's role 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 authentic 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.



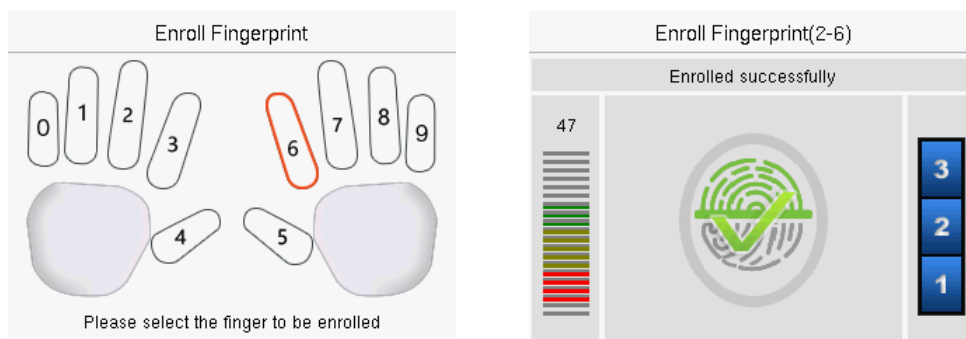
The image shows a 'User Role' selection interface. It features a title bar 'User Role' and two radio button options. The first option, 'Normal User', is selected and highlighted with a green background. The second option, 'Super Admin', is unselected and has a white background.

Note: If the selected user role is the Super Admin, then 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.

3.1.3 Register Fingerprint

Select **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

- Select the finger to be enrolled.
- Press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.



3.1.4 Card Number

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

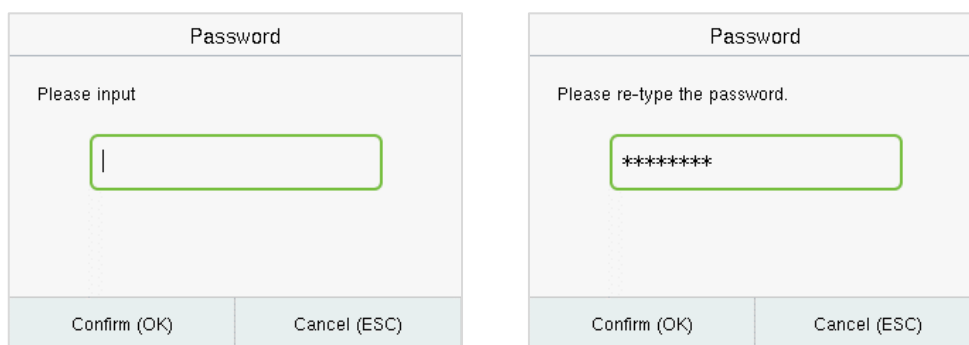
- On the card interface, swipe the card under the card reading area. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface appears as follows:



3.1.5 Password

Select **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 press **M/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 re-confirm the password again.
- The password may contain 6 to 8 digits by default.



3.1.6 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, time period and duress fingerprint.

- Enter **Access Control Role > Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Select **Time Period**, to select the time to use.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate an external alarm.
- Enter **Verification Mode** to select verification mode for the user.
- Select whether to apply the group time period for this user.

Access Control	
Access Group	1
Time Period	
Duress Fingerprint	Undefined

A&C PUSH

Access Control	
Access Group	1
Verification Mode	Apply Group Mode
Duress Fingerprint	Undefined
Apply Group Time Period	☒

T&A PUSH

3.2 All Users

When the device is on the initial interface, press **[M/OK]** button and enter **User Mgt. > All Users**.

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

All Users	
1	
2	Bella
33	A

3.2.1 Edit User

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

User : 1
Edit
Delete

Edit : 1	
User ID	1
Name	
User Role	Normal User
Fingerprint	1

Note: The process of editing the user information is the same as adding a new user, except that the User ID cannot be modified while editing a user. The process in detail refers to "[User Registration](#)".

3.2.2 Delete User

On the **All Users** interface, select the required user from the list and select **Delete** to delete the user or specific user information from the device. On the **Delete** interface, select the required operation, and then press **M/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 User Role Only:** Deletes the user's administrator privileges and make the user a normal user.
- **Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Number Only:** Deletes the card information of the selected user.

User : 1
Edit
Delete

Delete : 1
Delete User
Delete User Role Only
Delete Fingerprint Only
Delete Password Only

3.3 Display Style

When the device is on the initial interface, press **[M/OK]** button and enter **User Mgt. > Display Style**.

Display Style	
☐	Multiple Line
☒	Mixed Line

All the Display Styles are shown as below:

Multiple Line:

All Users	
1	
[Icons]	
2	Bella
[Icons]	
33	A
[Icons]	
[Search Bar]	

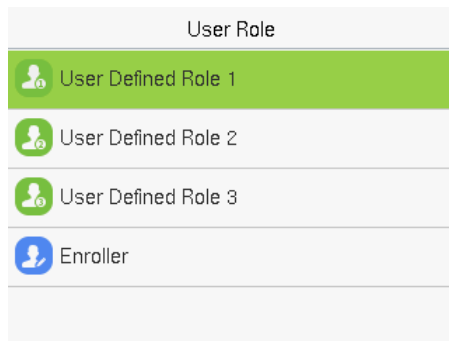
Mixed Line:

All Users	
1	[Icons]
2	[Icons]
Bella	
33	[Icons]
A	
[Search Bar]	

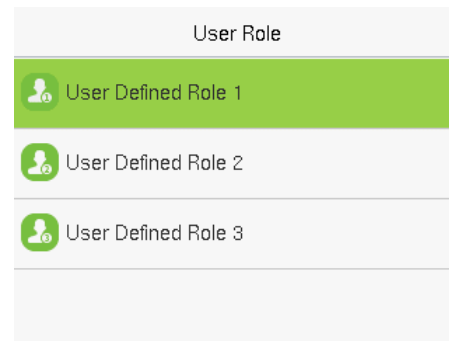
4 User Role

User Role allows you to assign specific permissions to certain users based on their requirements.

- When the device is on the initial interface, press **[M/OK]** button and enter **User Role > User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.

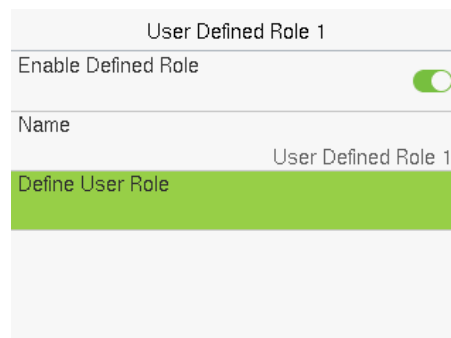


A&C PUSH



T&A PUSH

- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.



- Then, by selecting on Define User Role, select the required privileges for the new role, and then press the **M/OK** key.
- When assigning privileges, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First select the required **Main Menu** function name, then press **M/OK** and select its required sub-menus from the list.

User Defined Role 1
☐ User Mgt.
☒ COMM.
☒ System
☐ Personalize

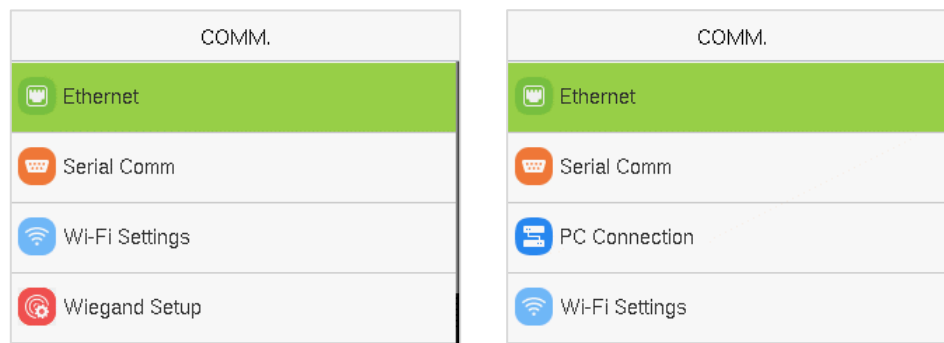
User Mgt.
☐ New User
☒ All Users
☒ Display Style

Note: If the User Role is enabled for the Device, enter **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

Communication Settings are used to set the parameters of the Network, Serial Comm, PC Connection, Wi-Fi★, Cloud Server, Wiegand, and Network Diagnosis.

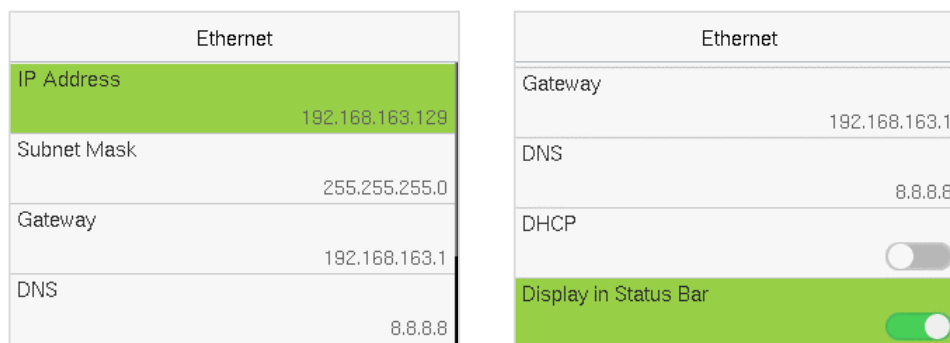
When the device is on the initial interface, press **[M/OK]** button and enter **COMM.**



5.1 Ethernet

When the device needs to communicate with a PC via the Ethernet, you need to configure network settings and make sure that the device and the PC connecting to the same network segment.

Select **Ethernet** on the **COMM.** Settings interface to configure the settings.



Function Description:

Function Name	Description
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.
DHCP	Dynamic Host Configuration Protocol 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 Serial Comm

Serial Comm function establishes communication with the device through a serial port (Primary Unit function).

Select **Serial Comm** on the **COMM.** Settings interface.

Serial Comm

Serial Port

No Using

Baudrate

115200

Serial Port

☒ No Using

☐ Primary Unit

Function Description

Function Name	Description
Serial Port	No Using: No communication with the device through the serial port. Primary Unit: When RS485 is used as the function of " Primary Unit ", it can be connected to a reader.
Baudrate	When the serial port is set as Primary Unit , the baudrate is 115200 by default and cannot be modified.

5.3 PC Connection

Select **PC Connection** on the **COMM.** Settings interface to configure the communication settings.

PC Connection	
Comm Key	*****
Device ID	1
TCP COMM.Port	4370
HTTPS	☒

Function Description

Function Name	Description
Comm Key	This menu only appears after enabling Standalone Communication function in System> Security Settings . To improve the security of data, the Comm Key needs to be entered before the device can be connected to the C/S software. It can be changed as needed.
Device ID	It is the identification number of the device, which ranges between 1 and 254.
TCP COMM.Port	The default TCP COMM Port value is 4370. It can be modified according to the network availability.
HTTPS	Based on HTTP, transmission encryption and identity authentication ensure the security of the transmission process.

5.4 Wi-Fi Settings★

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

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.

Select **Wi-Fi Settings** on the **COMM.** Settings interface to configure the Wi-Fi settings.

Wi-Fi Settings	
WIFI mode	WIFI-STA
WIFI	☒
ATP-LINK_XYP-2.4G	
2	

➤ WiFi mode

It is **WIFI-STA** by default. The **WIFI-AP** mode is suitable for use in scenarios where there is no network coverage or when quick configuration of the access control system is required. For example, it can be used for simple testing after installation.

In **WIFI-AP** mode, the device can emit an AP hotspot, allowing users to connect to the WiFi hotspot via mobile devices (smartphones, tablets, etc.) and then access the device's built-in webserver directly through a browser for remote management.

When connecting to the AP hotspot for the first time, the default SSID and password are:

[Device Serial Number] / [Device Serial Number].

Wi-Fi Settings	
WIFI mode	WIFI-AP
WIFI-AP	☒
SSID	JPY3252600081
Password	JPY3252600081

Note: For security considerations, the device's AP hotspot will automatically turn off **every 30 minutes** to prevent unauthorized access.

➤ Searching the Wi-Fi Network

- Wi-Fi is enabled in the device by default. Toggle the  button to enable or disable Wi-Fi.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Select the required Wi-Fi name from the available list and input the correct password in the password interface, and then press **M/OK**.

Wi-Fi Settings	
WIFI mode	WIFI-STA
WIFI	☒
ATP-LINK_XYP-2.4G	
2	

WIFI Enabled: Select the required network from the searched network

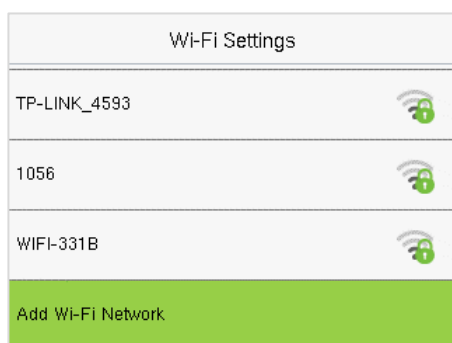
CS	
Security: WPAPSK/WPA2PSK	
Signal Strength: Very Strong	
Password	
Connect to Wi-Fi (OK)	Cancel (ESC)

Select the password field to enter the password and press **M/OK**.

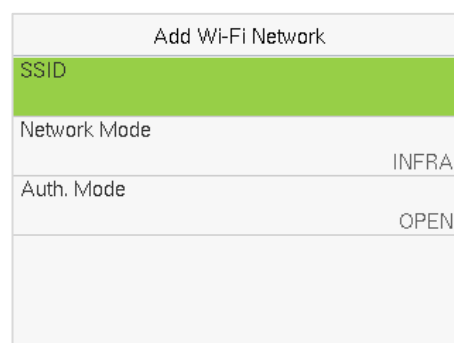
- When the Wi-Fi is connected successfully, the initial interface will display the Wi-Fi  logo.

➤ Adding Wi-Fi Network Manually

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



Select **Add Wi-Fi Network** to add the Wi-Fi manually.

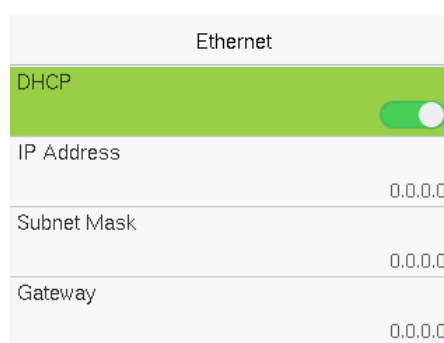
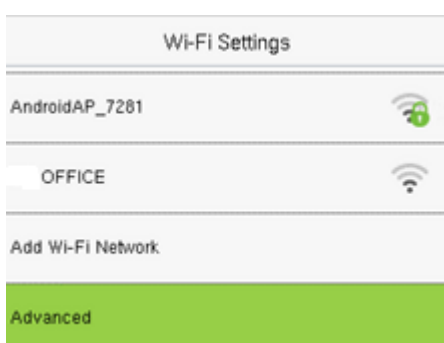


On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

Note: After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name.

➤ Advanced Setting

On the **Wi-Fi Settings** interface, select **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 Wi-Fi 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 Wi-Fi 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.

DNS	The default DNS is 0.0.0.0. It can be modified according to the network availability.
------------	---

5.5 Cloud Server Settings

Select **Cloud Server Settings** on the **COMM.** Settings interface to connect with the ADMS server.

Function Description

Function Name		Description
Enable Domain Name	Server Address	Once this mode 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.

5.6 Wiegand Setup

It is used to set the Wiegand input and output parameters.

Select **Wiegand Setup** on the **COMM.** Settings interface to set up the Wiegand input and output parameters.

Note: The Wiegand interface is shared, and the user can choose to use either the Wiegand input or Wiegand output function to interface with different Wiegand devices.

Wiegand Setup	
ID Type	Wiegand Input
Wiegand Options	

5.6.1 Wiegand Input

Wiegand Options	
Wiegand Format	
Wiegand Bits	26
Pulse Width(us)	100
Pulse Interval(us)	1000

Function Description

Function Name	Description
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 64 bits.
Wiegand Bits	The number of bits of the Wiegand data.
Pulse Width(us)	The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds.
Pulse Interval(us)	The default value is 1000 microseconds and can be adjusted within the range of 200 to 20000 microseconds.
ID Type	Select between the User ID and card number.

Various Common Wiegand Format Description:

Wiegand Format	Description
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers.

Wiegand26a	ESSSSSSSSSCCCCCCCCCCCCCCCCCCCCO It consists of 26 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 13 th bits, while the 26 th bit is the odd parity bit of the 14 th to 25 th bits. The 2 nd to 9 th bits is the site codes, while the 10 th to 25 th bits are the card numbers.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 25 th bits is the card numbers.
Wiegand34a	ESSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO It consists of 34 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 17 th bits, while the 34 th bit is the odd parity bit of the 18 th to 33 rd bits. The 2 nd to 9 th bits is the site codes, while the 10 th to 25 th bits are the card numbers.
Wiegand36	OFFFFFFFFFCCCCCCCCCCCCCCCCMME It consists of 36 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 36 th bit is the even parity bit of the 19 th to 35 th bits. The 2 nd to 17 th bits is the device codes. The 18 th to 33 rd bits is the card numbers, and the 34 th to 35 th bits are the manufacturer codes.
Wiegand36a	EFFFFFFFFFCCCCCCCCCCCCCCCCCCO It consists of 36 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 36 th bit is the odd parity bit of the 19 th to 35 th bits. The 2 nd to 19 th bits is the device codes, and the 20 th to 35 th bits are the card numbers.
Wiegand37	OMMMMSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCE It consists of 37 bits of binary code. The 1 st bit is the odd parity bit of the 2 nd to 18 th bits, while the 37 th bit is the even parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits is the manufacturer codes. The 5 th to 16 th bits is the site codes, and the 21 st to 36 th bits are the card numbers.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCCO It consists of 37 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 18 th bits, while the 37 th bit is the odd parity bit of the 19 th to 36 th bits. The 2 nd to 4 th bits is the manufacturer codes. The 5 th to 14 th bits is the device codes, and 15 th to 20 th bits are the site codes, and the 21 st to 36 th bits are the card numbers.
Wiegand50	ESSSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCC CCCCCO It consists of 50 bits of binary code. The 1 st bit is the even parity bit of the 2 nd to 25 th bits, while the 50 th bit is the odd parity bit of the 26 th to 49 th bits. The 2 nd to 17 th bits is the site codes, and the 18 th to 49 th bits are the card numbers.

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

5.6.2 Wiegand Output

Wiegand Options	
SRB	☐
Wiegand Format	
Wiegand Output Bits	26
Failed ID	Disabled

Wiegand Options	
Site Code	Disabled
Pulse Width(us)	100
Pulse Interval(us)	1000
ID Type	User ID

Function Description

Function Name	Description
SRB	When SRB is enabled, the lock is controlled by the SRB to prevent the lock from being opened due to device removal.
Wiegand Format	Its value can be 26 bits, 34 bits, 36 bits, 37 bits, 50 bits and 64 bits.
Wiegand Output Bits	After selecting the required Wiegand format, select the corresponding output bit digits from the Wiegand format.
Failed ID	If the verification fails, the system will send the failed ID to the device and replace the card number or personnel ID with the new one.
Site Code	It is similar to the device ID. The difference is that a site code can be set manually and is repeatable on a different device. The valid value ranges from 0 to 256 by default.
Pulse Width(us)	The time width represents the changes in the quantity of electric charge with regular high-frequency capacitance within a specified time.
Pulse Interval(us)	The time interval between pulses.
ID Type	Select the ID types as either User ID or card number.

5.7 Network Diagnosis

It helps to set the network diagnosis parameters.

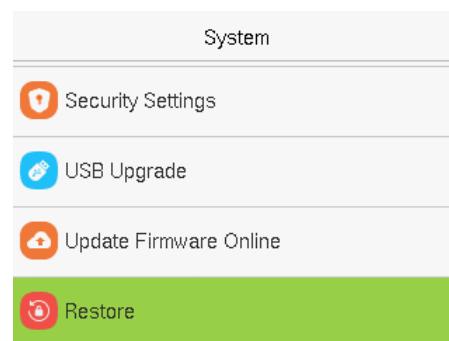
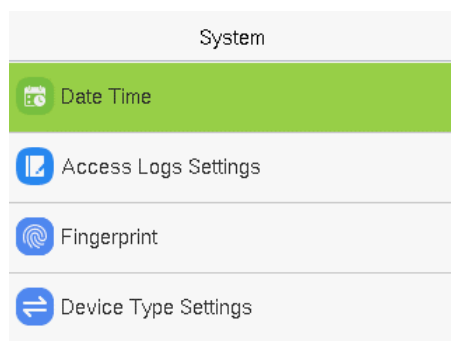
Select **Network Diagnosis** on the **COMM.** Settings interface. Enter the IP address that needs to be diagnosed and select **Start the Diagnostic Test** to check whether the network can connect to the device.

Network Diagnosis	
IP Address Diagnostic Test	110.80.38.74
Start the Diagnostic Test	

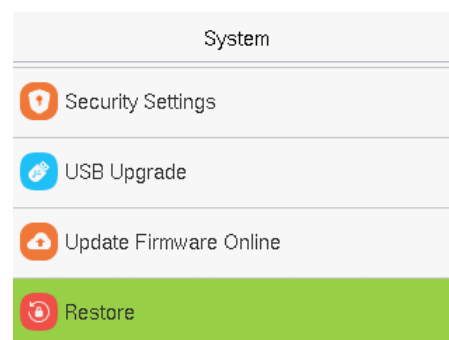
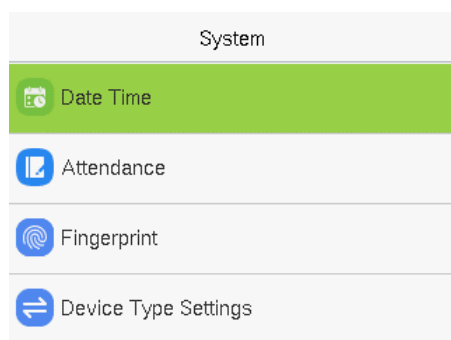
6 System Settings

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

When the device is on the initial interface, press **[M/OK]** button and enter **System**.



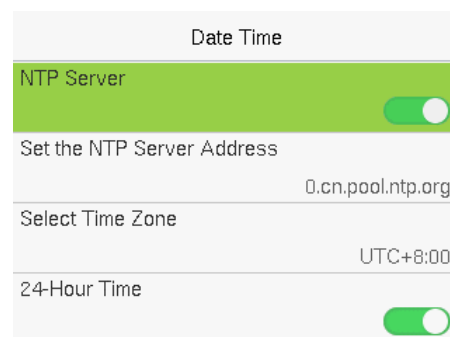
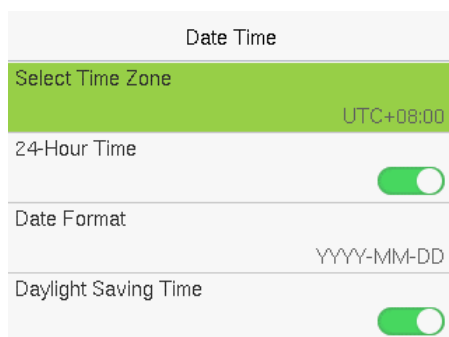
BEST Protocol/A&C PUSH



T&A PUSH

6.1 Date and Time

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



- Select **NTP Server** to enable automatic time synchronization based on the service address you enter.
- Select **Manual Date and Time** to manually set the date and time and then press **M/OK** and save.

- Select **Time Zone** to manually select the time zone where the device is located.
- Enable or disable the **24-Hour Time**. Select the **Date Format** to set the date format.
- Select **Daylight Saving Time** to enable or disable the function. If enabled, enter **Daylight Saving Mode** to select a daylight-saving mode and then enter **Daylight Saving Setup** to set the switch time.

Daylight Saving Setup	
Start Month	1
Start Week	1
Start Day	Sunday
Start Time	00:00

Week Mode

Daylight Saving Setup	
Start Date	00-00
Start Time	00:00
End Date	00-00
End Time	00:00

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, if a user sets the time of the device from 18:35 on March 15, 2020 to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will remain at 18:30 on January 1, 2021.

6.2 Access Logs Settings / Attendance

Select **Access Logs Settings / Attendance** on the **System** interface.

Access Logs Settings	
Alphanumeric User ID	☐
Access Log Alert	99
Periodic Del of Access Logs	Disabled
Authentication Timeout(s)	3

A&C PUSH

Attendance	
Duplicate Punch Period(m)	1
Alphanumeric User ID	☐
Attendance Log Alert	99
Periodic Del of T&A Data	Disabled

T&A PUSH

A&C Terminal:

Function Name	Description
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
Access Log Alert	When the record space of the access 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 Access Logs	When access logs reach its maximum capacity, the device automatically deletes a set of old access logs. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

T&A Terminal:

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).
Alphanumeric User ID	Enable/Disable the alphanumeric as User ID.
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 T&A Data	When attendance logs reach its maximum capacity, the device automatically deletes a set of old attendance logs. Users may disable the function or set a valid value between 1 and 999.
Authentication Timeout(s)	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.

6.3 Fingerprint

Select **Fingerprint** on the **System** interface to go to the Fingerprint parameter settings.

Fingerprint	
1:1 Threshold	15
1:N Threshold	35
FP Sensor Sensitivity	Low
1:1 Retry Attempts	3

Function Description

Function Name	Description
1:1 Threshold Value	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold Value	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level " Medium ". When the environment is dry, resulting in slow fingerprint detection, you can set the level to " High " to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to " Low ".
1:1 Retry Times	In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed.
Fingerprint Image	To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available: Show for Enroll: to display the fingerprint image on the screen only during enrollment. Show for Match: to display the fingerprint image on the screen only during verification. Always Show: to display the fingerprint image on screen during enrollment and verification. None: not to display the fingerprint image.

6.4 Device Type Settings

Select **Device Type Settings** on the **System** interface to configure the Device Type Settings.

Device Type Settings	
Communication Protocol	PUSH Protocol
Device Type	A&C PUSH

Note: After changing the device type, the device will delete all the data and restart, and some functions will be adjusted accordingly.

6.5 Security Settings

Select **Security Settings** on the **System** interface to go to the Security settings.

Security Settings	
Standalone Communication	☐
SSH	☒
User ID Masking	☒
Display Verification Name	☐

Function Description

Function Name	Description
Standalone Communication	By default, this function is disabled. When it is switched on, a security prompt appears, and you need to set the Comm Key, the device will restart after you confirm.
SSH	SSH is used to enter the background of the device for maintenance.
User ID Masking	When enabled, and then the user is successfully compared and verified, the User ID in the displayed verification result will be replaced with an * to achieve secure protection of sensitive private data.
Display Verification Name	Set whether to display the username in the verification result interface.
Display Verification Mode	Set whether to display the verification mode in the verification

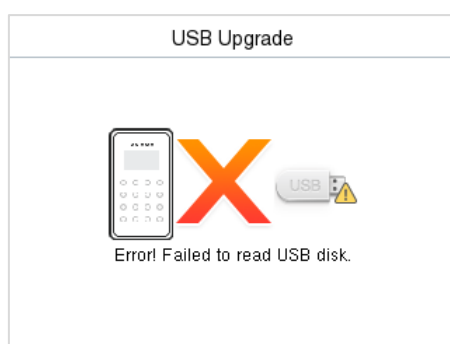
result interface.

6.6 USB Upgrade

The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device.

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

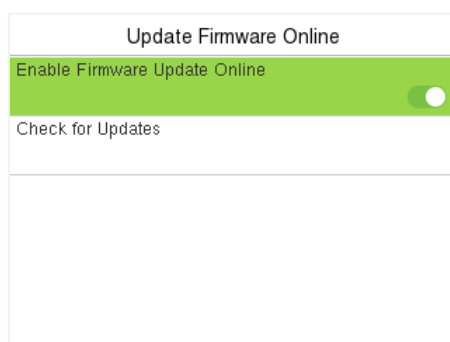
Select **USB Upgrade** on the **System** interface.



 **Note:** If upgrade file is needed, please contact our technical support. Firmware upgrade is not advised under normal circumstances.

6.7 Update Firmware Online

Select **Update Firmware Online** on the System interface.



The Firmware Update Online function is enabled by default. Select **Check for Updates** it may have the following 3 scenarios:

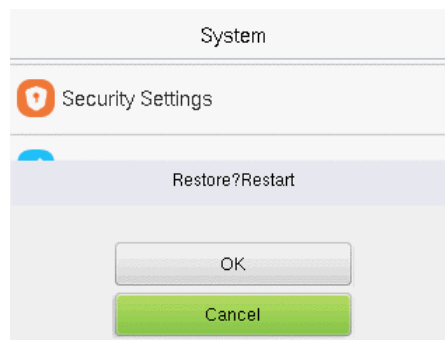
- If the query fails, the interface will prompt "Query failed".

- If the firmware version of the device is latest, it will prompt that the current firmware version is already the latest.
- If the firmware version of the device is not the latest, the version number and change log of the latest version will be displayed. Users can choose whether to update to the latest firmware version.

6.8 Factory Reset

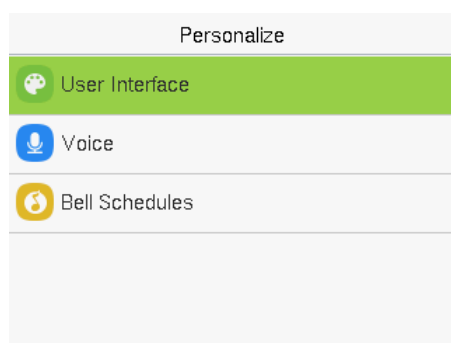
The Factory Reset function restores the device settings such as communication settings and system settings, to the default factory settings (this function does not clear registered user data).

Select **Restore** on the **System** interface and then press **M/OK** to restore the default factory settings.

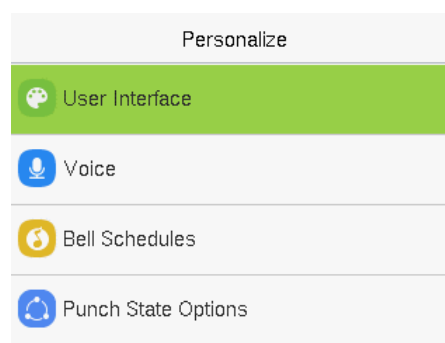


7 Personalize Settings

When the device is on the initial interface, press **[M/OK]** button and enter **Personalize** to customize the interface settings, voice, bell, punch state options, and shortcut key mappings.



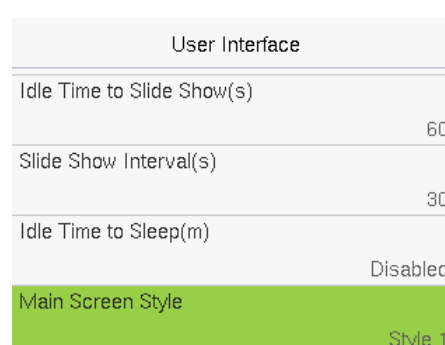
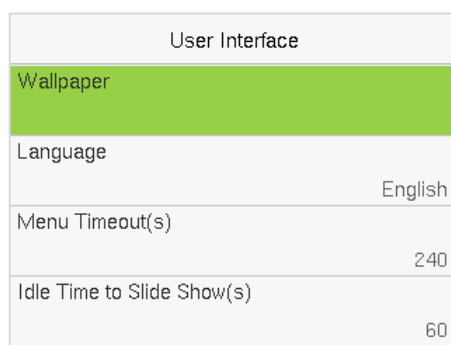
BEST Protocol/A&C PUSH



T&A PUSH

7.1 User Interface

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



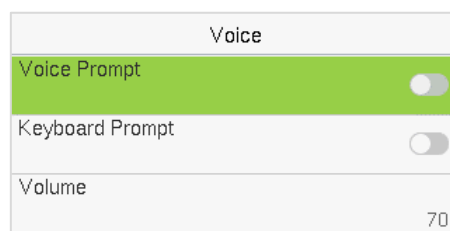
Function Description

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

7.2 Voice

Select **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.
Keyboard Prompt	Toggle to enable or disable the keypad sounds.
Volume	Adjust the volume of the device which can be set between 0 to 100.

7.3 Bell Schedules

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

Bell Schedules
New Bell Schedule
All Bell Schedules

➤ **New Bell Schedule:**

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

Bell Schedules	New Bell Schedule
New Bell Schedule	Bell Status ☐
All Bell Schedules	Bell Time
	Repeat Never
	Ring Tone bell01.wav

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 automatically triggers to ring the bell during that time.
Repeat	Set the required number of counts to repeat the scheduled bell.
Ring Tone	Select a ringtone.
Internal Bell Delay(s)	Set the replay time of the internal bell. Valid values range from 1 to 999 seconds.

➤ **All Bell Schedules:**

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

➤ **Edit the Scheduled Bell:**

On the **All Bell Schedules** interface, select the required bell schedule, and select **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 Schedules:**

On the **All Bell Schedules** interface, select the required bell schedule, select **Delete**, and then press **M/OK** to delete the selected bell.

7.4 Punch States Options (T&A PUSH)

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

Punch State Options	
Punch State Mode	Manual and Auto Mode
Punch State Timeout(s)	5
Punch State Required	☐

Punch State Mode	
☐	Off
☐	Manual Mode
☐	Auto Mode
☒	Manual and Auto Mode

Function Description

Function Name	Description
Punch State Mode	Off: Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid. Manual Mode: Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout. Auto Mode: The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings. Manual and Auto Mode: The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching to 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 it is being manually switched again. Fixed Mode: Only the manually fixed punch state key will be shown. Users cannot change the status by tapping any other keys.
Punch State Timeout(s)	It is the time for which the punch state displays. The value ranges from 5 to 999 seconds.

Punch State Required	Select whether an attendance state needs to be selected after verification. ON: Attendance state needs to be selected after verification. OFF: Attendance state need not requires to be selected after verification.
-----------------------------	---

7.5 Shortcut Key Mappings (T&A PUSH)

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

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

Shortcut Key Mappings	
Up Key	Check-In
Down Key	Check-Out
Left Key	Overtime-In
Right Key	Overtime-Out

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

Up Key	
Punch State Value	0
Function	Punch State Options
Name	Check-In
Set Switch Time	

Up Key	
Function	New User

- 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 to 250), name.
- **Set the Switch Time**
- The switch time is set in accordance with the punch state options.

- When the **Punch State Mode** is set to **Auto Mode**, the switch time should be set.
- On the **Shortcut Key** interface, select **Set Switch Time** to set the switch time.
- On the **Switch Cycle** interface, select the switch cycle (Monday, Tuesday, etc.) as shown in the image below.

Switch Cycle

☐ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday

Set Switch Time

Switch Cycle	Monday Tuesday ...
Monday	
Tuesday	
Wednesday	

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

Monday

13:57

+

13

—

HH

+

57

—

MM

Confirm (OK)
Cancel (ESC)

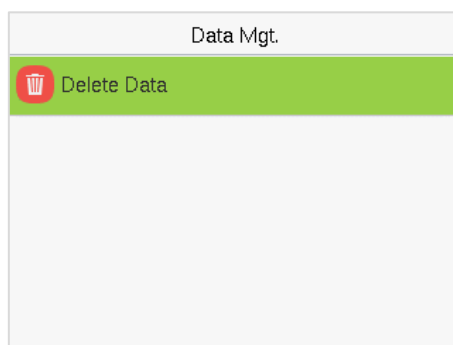
Set Switch Time

Switch Cycle	Monday Tuesday ...
Monday	13:57
Tuesday	
Wednesday	

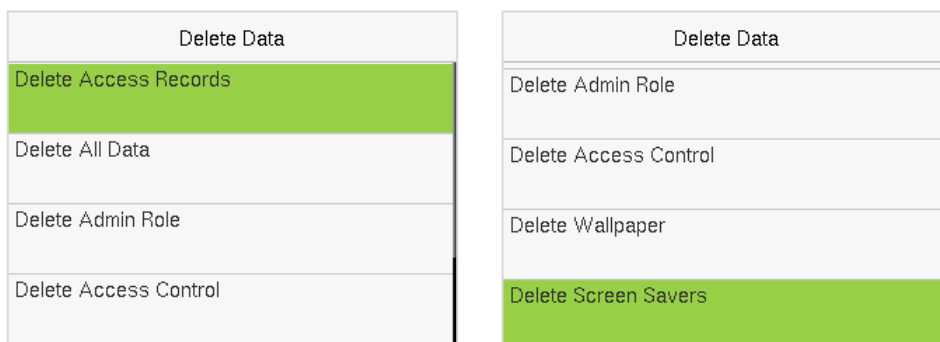
Note: When the function is set to Undefined, the device will not enable the punch state key.

8 Data Management

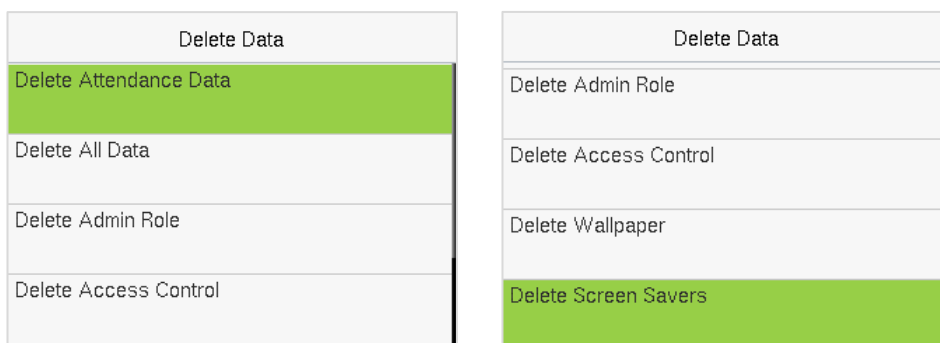
When the device is on the initial interface, press **[M/OK]** button and enter **Data Mgt.** to manage the relevant data in the device.



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



A&C PUSH



T&A PUSH

Function Description

Function Name	Description
Delete Access Records / Attendance Data	To delete the access records / attendance data conditionally.
Delete All Data	To delete the information and access records / attendance data

	of all registered users.
Delete Admin Role	To remove all the administrator privileges.
Delete Access Control	To delete all the access data.
Delete Wallpaper	To delete all the wallpapers in the device.
Delete Screen Savers	To delete all the screen savers in the device.

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

Delete Access Records

Delete All
Delete by Time Range

Start Time

2023-08-10 00:00

+

+

+

+

+

2023

08

10

00

00

–

–

–

–

–

YYYY

MM

DD

HH

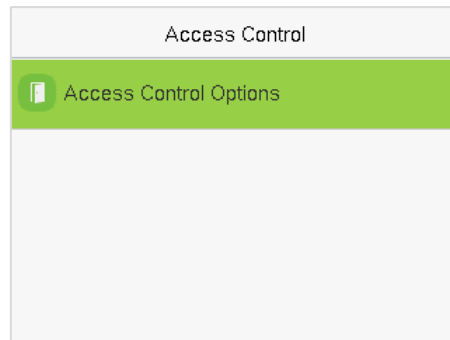
MM

Confirm (OK)

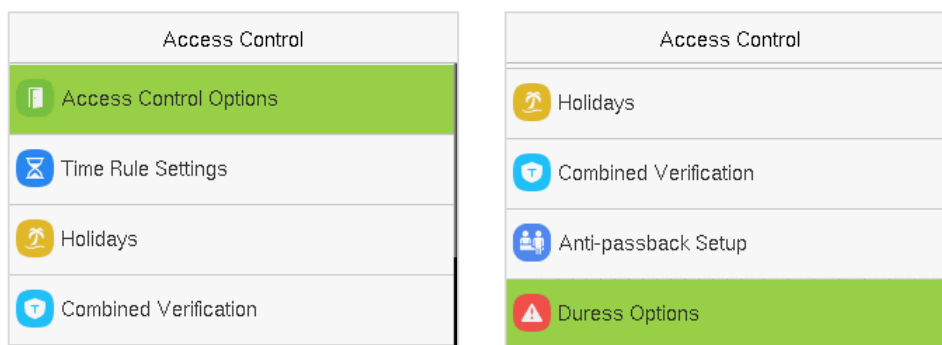
Cancel (ESC)

9 Access Control

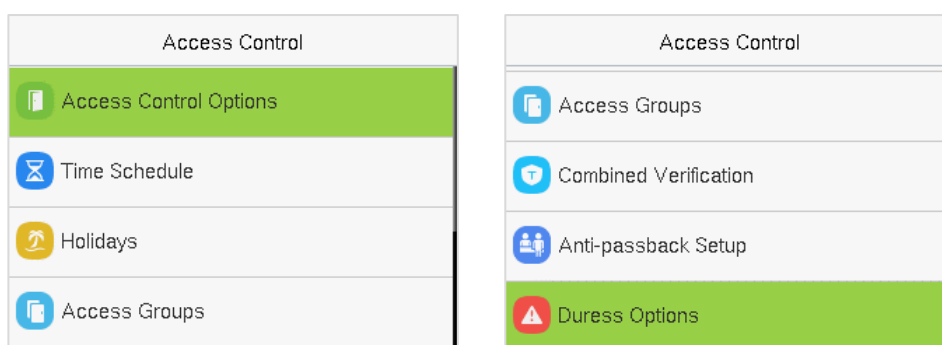
When the device is on the initial interface, press **[M/OK]** button and enter **Access Control** to set the schedule of the door opening, locks control and to configure other parameters settings related to access control.



BEST Protocol



A&C PUSH



T&A PUSH

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

1. The relevant door's current unlock time should be within any valid time zone of the user's time period.
2. The corresponding user's group must be already set in the door unlock combination (and if there are other groups, being set in the same access combo, then the verification of those

group's members is also required to unlock the door).

3. In default settings, new users are allocated into the first group with the default group time zone, where the access combo is "1" and is set in unlock state by default.

9.1 Access Control Options

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

BEST Protocol:

Access Control Options	
Gate Control Mode	☐
Door Lock Delay(s)	5
Door Sensor Delay(s)	10
Door Sensor Type	Normal Close(NC)

Access Control Options	
Door Lock Delay(s)	5
Door Sensor Delay(s)	15
Door Sensor Type	None
Speaker Alarm	☐

Function Name	Description
Gate Control Mode	It toggles between ON or OFF switch to get into gate control mode or not. When set to ON , the interface removes the Door Lock Delay, Door Sensor Delay, and Door Sensor Type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: None , Normal Open , and Normal Close . None: It means the door sensor is not in use. Normal Open: It means the door is always left open when electric power is on. Normal Close: It means the door is always left closed when electric power is on.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local.

When the door is closed or the verification is successful, the system cancels the alarm from the local.

A&C PUSH:

Access Control Options

Gate Control Mode

Door Lock Delay(s)

Door Sensor Delay(s)

Door Sensor Type

Normal Close(NC)

Access Control Options

Auxiliary Input Configuration

Verify Mode by RS485

Card Only

Speaker Alarm

Reset Access Settings

Function Name	Description
Gate Control Mode	It toggles between ON or OFF switch to get into gate control mode or not. When set to ON, the interface removes the Door Lock Delay, Door Sensor Delay, and Door Sensor Type options.
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 1~99 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: None, Normal Open, and Normal Close. None: It means the door sensor is not in use. Normal Open: It means the door is always left open when electric power is on. Normal Close: It means the door is always left closed when electric power is on.
Verification Mode	The supported verification mode includes Password/Fingerprint/Card, Fingerprint Only, User ID Only, Password, Card Only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID).

Door Available Time Period	It sets the timing for the door so that the door is accessible only during that period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Primary Device	While configuring the primary and secondary devices, you may set the state of the primary as Out or In. Out: A record of verification on the primary device is a check-out record. In: A record of verification on the primary device is a check-in record.
Secondary Device	While configuring the primary and secondary devices, you may set the state of the secondary as Out or In. Out: A record of verification on the secondary device is a check-out record. In: A record of verification on the secondary device is a check-in record.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	When the RS485 reader function is turned on, the verification method is used when the device is used as a primary or a secondary.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Settings	The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, and alarm. However, erased access control data in Data Mgt. is excluded.

T&A PUSH:

Access Control Options	
Door Lock Delay(s)	10
Door Sensor Delay(s)	10
Door Sensor Type	Normal Close(NC)
Door Alarm Delay(s)	30

Access Control Options	
Verify Mode by RS485	Card Only
Valid Holidays	☐
Speaker Alarm	☐
Reset Access Settings	

Function Name	Description
Door Lock Delay (s)	The length of time that the device controls the electric lock to be in unlock state. Valid value: 0 to 10 seconds.
Door Sensor Delay (s)	If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered. The valid value of Door Sensor Delay ranges from 1 to 255 seconds.
Door Sensor Type	There are three Sensor types: None , Normal Open , and Normal Close . None: It means the door sensor is not in use. Normal Open (NO): It means the door is always left open when electric power is on. Normal Close (NC): It means the door is always left closed when electric power is on.
Door Alarm Delay(s)	When the state of the door sensor is inconsistent with that of the door sensor type, alarm will be triggered after a time period; this time period is the Door Alarm Delay (the value ranges from 1 to 999 seconds).
Retry Times to Alarm	When the number of failed verifications reach the set value (value ranges from 1 to 9 times), the alarm will be triggered. If the set value is None, the alarm will not be triggered after failed verification.
Normal Close Time Period	It is the scheduled time-period for "Normal Close" mode so that the door is always closed during this period.
Normal Open Time Period	It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period.
Auxiliary Input Configuration	Sets the door unlock time period and auxiliary output type of

	the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Verify Mode by RS485	When the RS485 reader function is turned on, the verification method is used when the device is used as a primary or a secondary.
Valid Holidays	To set if Normal Close Time Period or Normal Open Time Period settings are valid in set holiday time period. Choose [ON] to enable the set NC or NO time period in holiday.
Speaker Alarm	It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local.
Reset Access Setting	The access control reset parameters include door lock delay, door sensor delay, door sensor type, door alarm delay, normal close time period, normal open time period, and alarm. However, erased access control data in Data Mgt. is excluded.

9.2 Time Rule Settings / Time Schedule

Select **Time Rule Settings / Time Schedule** on the **Access Control** interface to configure the time settings.

- The entire system can define up to 50 Time Rules.
- Each time-period represents **10** Time Zones, i.e., **1** week and **3** holidays, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- One can set a maximum of 3 time periods for every time zone. The relationship among these time-periods is "**OR**". Thus, when the verification time falls in any one of these time-periods, the verification is valid.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Search the required Time Rule in the grey box and specify the required Time Rule number (maximum up to 50 rules).

Time Rule[2/50]		
Sunday	[00:00 23:59]	[00:00 23:59]
Monday	[00:00 23:59]	[00:00 23:59]
Tuesday	[00:00 23:59]	[00:00 23:59]

A&C PUSH

Time Schedule:01/50	
Sunday	00:00 23:59
Monday	00:00 23:59
Tuesday	00:00 23:59

T&A PUSH

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

Time Period 1			
00:00 23:59			
+	+	+	+
00	00	23	59
-	-	-	-
HH	MM	HH	MM
Confirm (OK)		Cancel (ESC)	

Specify the start and the end time, and then press **M/OK**.

Note:

1. The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as **23:57 to 23:56**).
2. It is the time interval for valid access when the End Time occurs after the Start Time (such as **08:00 to 23:59**).
3. The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is **00:00** and End Time is **23:59**).
4. The default Time Rule 1 indicates that the door is open all day long.

9.3 Holidays

When there is a holiday, you may need a different access time; however, altering everyone's access time one by one is extremely time-consuming. Thus, a holiday access time that applies to all workers can be set, and the user will be able to open the door during the holidays.

Select **Holidays** on the **Access Control** interface to set the holiday access.

Holidays
Add Holiday
All Holidays

➤ **Add a New Holiday:**

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

Holidays	
No.	1
Date	Undefined
Holiday Type	Holiday Type 1
Repeats Every Year	☒

A&C PUSH

Holidays	
No.	1
Start Date	Undefined
End Date	Undefined
Time Period	1

T&A PUSH

➤ **Edit a Holiday:**

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

➤ **Delete a Holiday:**

On the **Holidays** interface, select a holiday item to be deleted and select **Delete**. Press **M/OK** to confirm the deletion. After deletion, this holiday does not display on the **All Holidays** interface.

9.4 Access Groups (T&A PUSH)

Grouping is to manage users in groups, only for time attendance terminal.

The default time zone for group members is the group time zone, while users can set their personal time zone. When the group verification mode and the user verification mode overlap, the user verification mode takes priority. Each group can set a maximum of 3 time zones; as long as one of them is valid, the group can be successfully verified. The newly enrolled user is assigned to Access Group 1 by default, but can be assigned to another access group.

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

Access Groups
New Group
All Groups

➤ **Add a New Holiday:**

Select **New Group** on the **Access Group** interface.

Access Groups	
No.	2
Verification Mode	Password/Fingerprint/Card
Time Period 1	1
Time Period 2	0

Access Groups	
Time Period 1	1
Time Period 2	0
Time Period 3	0
Include Holidays	☐

Note:

1. The system has a default access group numbered 1, which cannot be deleted but can be modified.
2. A number cannot be modified again after being set.
3. When the holiday is set to be valid, the personnel in a group can open the door only when group time period overlaps with the holiday time period.
4. When the holiday is set to be invalid, the access control time of the personnel in this group is not affected by holidays.

➤ **Edit Group:**

On the **All Group** interface, tap to select the access group item to be modified. Select **Edit** to modify group parameters.

➤ **Delete a Group:**

On the **All Group** interface, select an access group item to be deleted and select **Delete**. Press **M/OK** to confirm the deletion. After deletion, this group does not display on the **All Group** interface.

9.5 Combined Verification

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

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

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

Combined Verification	
1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00

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

For Example:

- If the **Door-unlock combination 1** is set as **(01 03 05 06 08)**. It indicates that the unlock combination 1 consists of 5 people and all the 5 individuals are from 5 groups, namely, AC Group 1, AC Group 3, AC Group 5, AC Group 6, and AC Group 8, respectively.
- If the **Door-unlock combination 2** is set as **(02 02 04 04 07)**. It indicates that the unlock combination 2 consists of 5 people; the first two are from AC Group 2, the next two are from AC Group 4, and the last person is from AC Group 7.
- If the **Door-unlock combination 3** is set as **(09 09 09 09 09)**. It indicates that there are 5 people in this combination; all of which are from AC Group 9.
- If the **Door-unlock combination 4** is set as **(03 05 08 00 00)**. It indicates that the unlock combination 4 consists of only three people. The first person is from AC Group 3, the second person is from AC Group 5, and the third person is from AC Group 8.

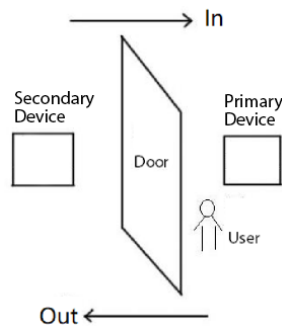
Note: To delete the door-unlock combination, set all Door-unlock combinations to 0.

9.6 Anti-passback Setup

A user may be followed by some person(s) to enter the door without verification, resulting in a security breach. So, to avoid such situations, the Anti-Passback option was developed. Once it is enabled, the check-in and check-out record must occur alternatively to open the door to represent a consistent pattern.

This function requires two devices to work together:

One device is installed on the indoor side of the door (primary device), and the other one is installed on the outdoor side of the door (the secondary device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID/Card Number) adopted by the primary device and secondary device must be consistent.



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

Anti-passback Setup
Anti-passback Direction
No Anti-pass...

A&C PUSH

Anti-passback Setup
Anti-passback Direction
No Anti-passback
Device Status
In
Secondary Device
Out

T&A PUSH

Function Description:

Function Name	Description
Anti-passback Direction	No Anti-passback: The Anti-Passback function is disabled, which means successful verification through either the primary device or secondary device can unlock the door. The attendance state is not saved in this option. Out Anti-passback: The user can check-out only if the last record is a check-in record otherwise an alarm is raised. However, the user can check-in freely. In Anti-Passback: The user can check-in again only if the last record is a check-out record otherwise an alarm is raised. However, the user can check-out freely. In/Out Anti-passback: In this case, a user can check-in only if the last record is a check-out or the user can check-out only if the last record is a check-in otherwise the alarm is triggered.
Device Status	Set the state of the device as Out or In. Out: A record of verification on the device is a check-out record. In: A record of verification on the device is a check-in record.
Secondary Device	Set the state of the secondary as Out or In. Out: A record of verification on the secondary device is a

check-out record.

In: A record of verification on the secondary device is a check-in record.

9.7 Duress Options Settings

Once a user activates the duress verification function with a specific authentication method(s), and when he/she is under coercion and authenticates using duress verification, the device unlocks the door as usual. At the same time, a signal is sent to activate the alarm as well.

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

A&C PUSH

T&A PUSH

A&C PUSH:

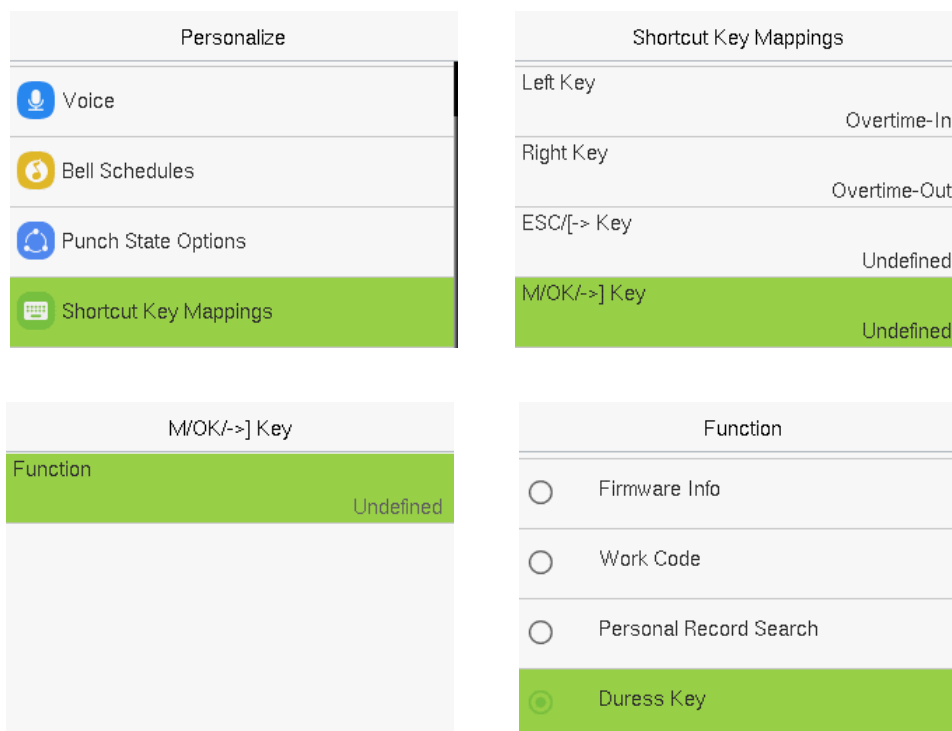
Function Name	Description
Alarm on Password	After enabled, when a user uses the password verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	After enabled, when a user uses the 1:1 verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	After enabled, when a user uses the 1:N verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.
Duress Password	Set the 6-digit duress password. When the user enters this duress password for verification, an external alarm signal will be generated.

T&A PUSH:

Function Name	Description
Duress Function	After enabled, Duress Key can be set in the Shortcut Key Mappings. After pressing the "Duress Key", then (within 10 seconds) press any registered fingerprint to generate an external alarm upon successful verification.
Alarm on Password	After enabled, when a user uses the password verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:1 Match	After enabled, when a user uses the 1:1 verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm on 1:N Match	After enabled, when a user uses the 1:N verification method, an external alarm signal will be generated, otherwise there will be no alarm signal.
Alarm Delay (s)	Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds.

- **Duress Key Settings (Such as set [M/OK] as Duress Key)**

After enabled the Duress Function, enter **Personalize > Short Shortcut Key Mappings**. Select the **[M/OK]** key > **Function** > select the “**Duress Key**” option.

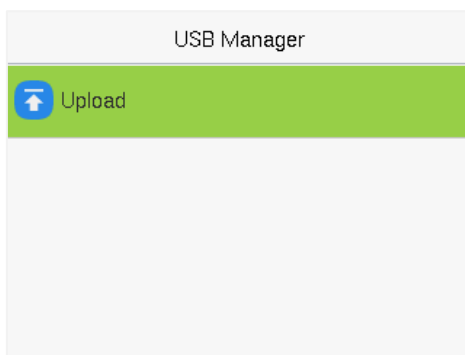


10 USB Manager

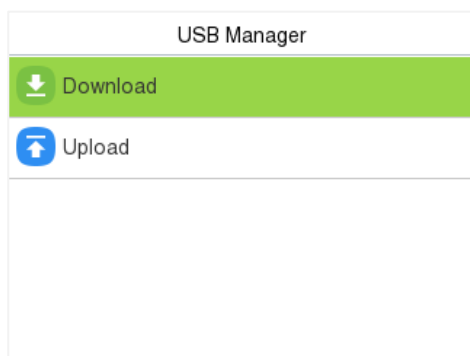
You can import user information, access data and other data from a USB drive to computer or other devices.

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

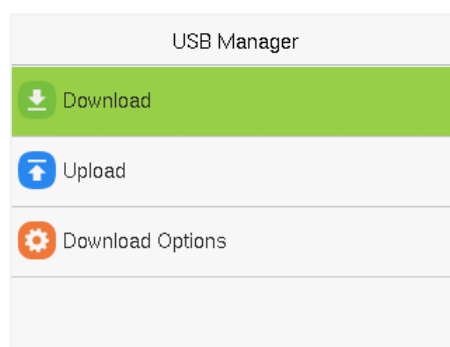
Select **USB Manager** on the main menu interface.



BEST Protocol



A&C PUSH



T&A PUSH



Note: Only FAT32 format is supported when downloading data using USB disk.

10.1 USB Download

On the **USB Manager** interface, select **Download**.

Download
Download Access Records
User Data

A&C Terminal

Download
Attendance Data
User Data
Work Code

T&A Terminal

Menu	Description
Download Access Records/Attendance Data	To download access record/attendance data in specified time period into USB disk.
User Data	To download all user information from the device into USB disk.
Work Code	To download all work code from the device into USB disk.

10.2 USB Upload

On the **USB Manager** interface, select **Upload**.

Upload
Screen Saver
Wallpaper

BEST Protocol

Upload
Screen Saver
Wallpaper
User Data

A&C PUSH

Upload
Screen Saver
Wallpaper
User Data
Upload Work Code

T&A PUSH

Menu	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 after upload.
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 after upload.
User Data	To upload all the user information from USB disk into the device.
Upload Work Code	To upload all work code from USB disk into the device.

10.3 Download Options (T&A PUSH)

On the **USB Manager** interface, select **Download Options**.

Download Options
Encrypt Attendance Data ☐
Delete T&A Data ☐

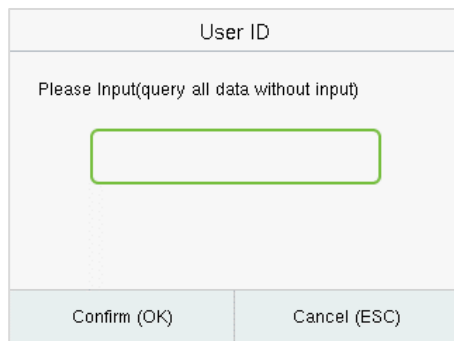
Function Name	Description
Encrypt Attendance Date	The attendance data is encrypted during the uploading and downloading.
Delete T&A Data	After successful downloading, the attendance data on the device is deleted.

11 Attendance Search

Once the identity of a user is verified, the access record/attendance data is saved in the device. This function enables users to check their event logs.

When the device is on the initial interface, press **[M/OK]** button and enter **Attendance Search** to search for the required event Logs.

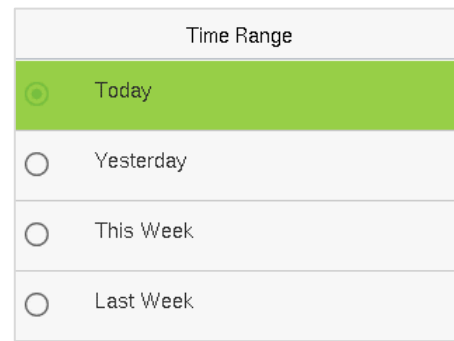
Note: The event logs include not only successful verification records, but also the failed verification records.



User ID

Please Input(query all data without input)

Confirm (OK) Cancel (ESC)



Time Range

☒ Today

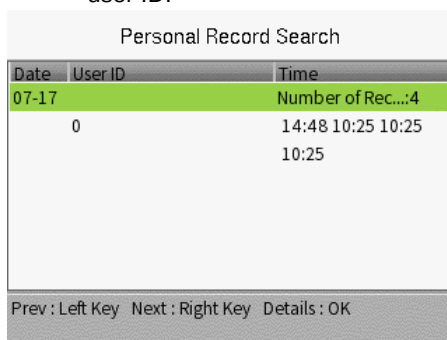
☐ Yesterday

☐ This Week

☐ Last Week

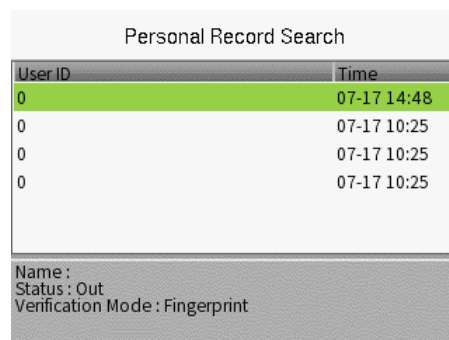
1. Enter the user ID to be searched and press **M/OK**. If you want to search for records of all users, press **M/OK** without entering any user ID.

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



Date	User ID	Time
07-17		Number of Rec...:4
	0	14:48 10:25 10:25

Prev : Left Key Next : Right Key Details : OK



User ID	Time
0	07-17 14:48
0	07-17 10:25
0	07-17 10:25
0	07-17 10:25

Name :
Status : Out
Verification Mode : Fingerprint

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

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

12 Work Code (T&A PUSH)

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 rates vary according to the work types, the 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.

Select **Work Code** on the main menu interface. It is only for time attendance terminal.

Work Code	
	New Work Code
	All Work Codes
	Work Code Options

12.1 Add a Work Code

New Work Code	
ID	1
Name	

Menu	Description
ID	The unique digital identifier for the work code. Valid range: 1-99999999.
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.

All Work Codes	
1	Test

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.

Work Code Options	
Work Code Required	☒
Input Screen Timeout(s)	5
Work Code Must Defined	☐

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.

Work Code	
1	Test

Enter Work Code :

2025-07-16 10:35

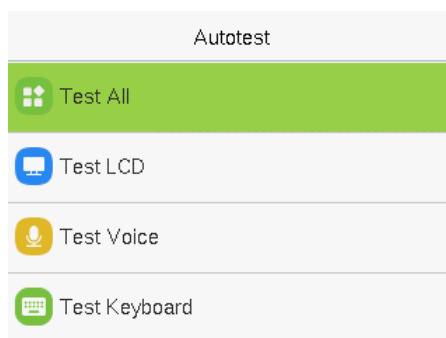

Successfully verified.

User ID : 1



13 Autotest

When the device is on the initial interface, press **[M/OK]** button and enter **Autotest**, it enables the system to automatically test whether the functions of various modules are working normally, including the LCD, Voice, Keyboard, Fingerprint and Real-Time Clock (RTC).

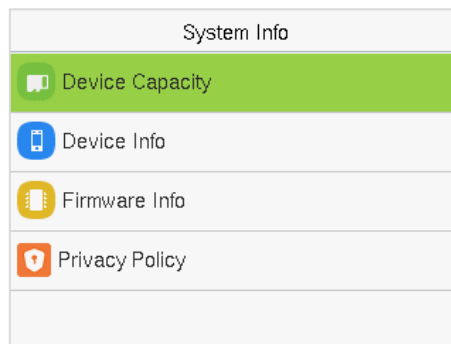


Function Description

Function Name	Description
Test All	To automatically test whether the LCD, Voice, Fingerprint and Real-Time Clock (RTC) are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Keyboard	The terminal tests whether every key on the keyboard works normally. Press any key on the Test Keyboard interface to check whether the pressed key matches the key displayed on the screen. The keys are displayed as dark grey before and turn green after pressed. Press ESC to exit the test.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Press M/OK to start counting and press it again to stop counting.

14 System Information

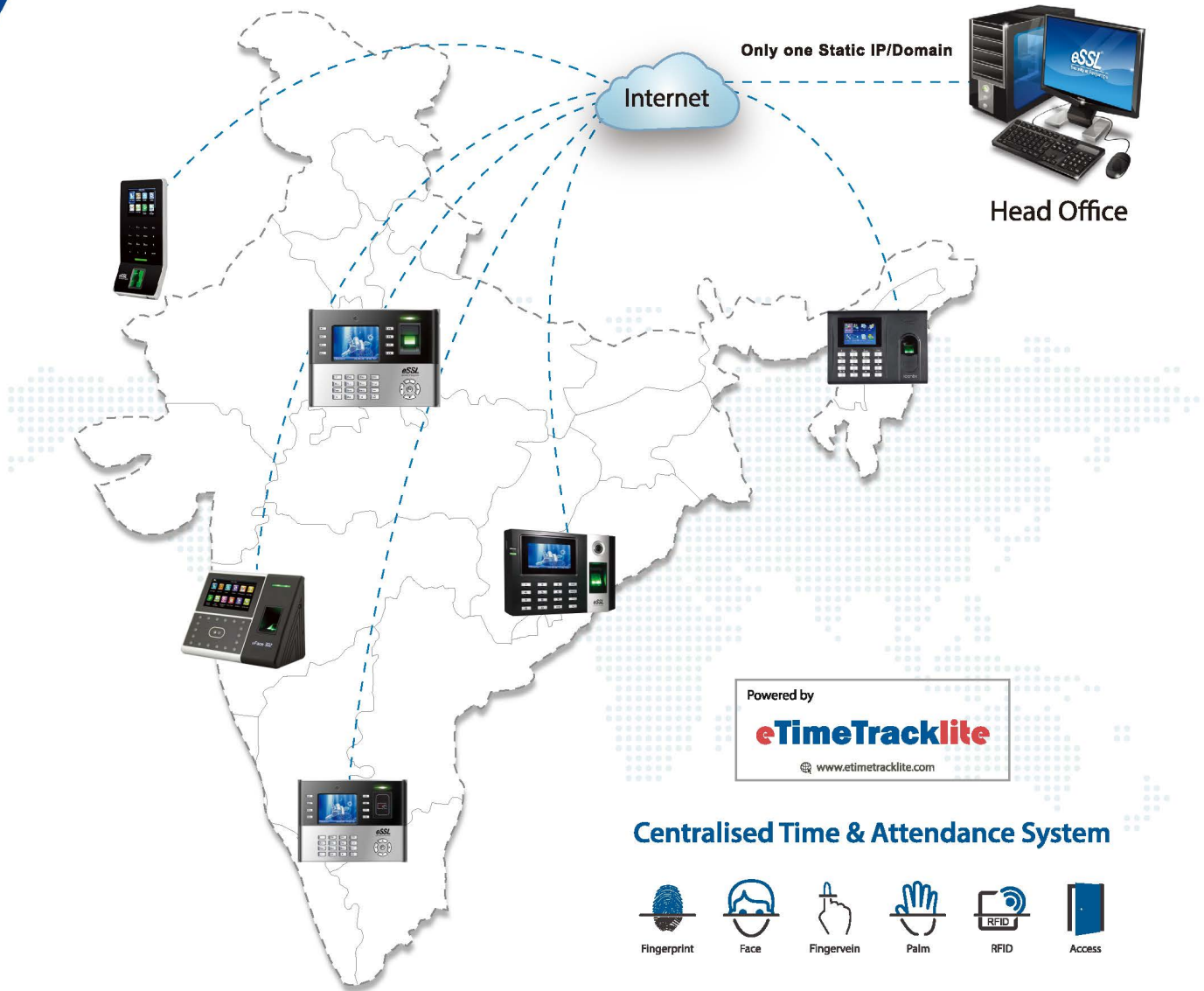
When the device is on the initial interface, press **[M/OK]** button and enter **System Info** to view the storage status, version information of the device, firmware information and privacy policy.



Function Description

Function Name	Description
Device Capacity	Displays the current device's user storage, fingerprint, card and password storage, administrators and records.
Device Info	Displays the device's name, serial number, MAC address, Fingerprint algorithm, Platform information, MCU Version and Manufacturer.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	Display the device's privacy policy.

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