

# User Manual

NG-TC1

Date: December 2023

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.



For further details, please visit our Company's website [www.ngteco.com](http://www.ngteco.com).

## About the Manual

This manual introduces the operations and usage of the **NG-TC1**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.






## Document Conventions

Conventions used in this manual are listed below:

### GUI Conventions

For Software	
Convention	Description
<b>Bold font</b>	Used to identify software interface names e.g. <b>OK</b> , <b>Confirm</b> , <b>Cancel</b> .
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	Description
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

### Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

# Table of Contents

<b>1</b>	<b>OVERVIEW</b> .....	<b>7</b>
<b>2</b>	<b>OPERATIONAL PROCEDURE</b> .....	<b>8</b>
2.1	STANDING POSITION, POSTURE AND FACIAL EXPRESSION .....	8
2.2	STANDBY INTERFACE .....	9
2.3	FACE TEMPLATE REGISTRATION .....	10
2.4	FINGER ENROLLMENT .....	11
2.4.1	FINGER SELECTION FOR ENROLLMENT .....	11
2.4.2	ENROLLMENT OPERATION .....	11
2.4.3	QUALITY IMPROVEMENT OF FINGERPRINT READS.....	12
2.5	VERIFICATION MODES.....	12
2.5.1	FACE VERIFICATION .....	12
2.5.2	FINGERPRINT VERIFICATION.....	14
2.5.3	CARD NUMBER VERIFICATION .....	16
2.5.4	PASSWORD VERIFICATION .....	17
2.6	T9 MODE.....	19
<b>3</b>	<b>PRIVILEGES</b> .....	<b>21</b>
3.1	ADMINISTRATOR.....	22
3.2	NORMAL USER.....	22
<b>4</b>	<b>MAIN MENU</b> .....	<b>23</b>
<b>5</b>	<b>USER</b> .....	<b>24</b>
5.1	SEARCH FOR USERS .....	24
5.2	REGISTER FINGERPRINT .....	25

---

5.3	REGISTER FACE .....	26
5.4	REGISTER CARD .....	27
5.5	REGISTER PASSWORD .....	28
5.6	DISPLAY STYLE .....	28
<b>6</b>	<b>COMMUNICATION PARAMETERS .....</b>	<b>29</b>
6.1	MANUAL ETHERNET CONFIGURATION.....	29
6.2	MANUAL WI-FI CONFIGURATION .....	30
6.2.1	CONNECTION TO AN EXISTING WI-FI .....	30
6.2.2	NEW WI-FI CONNECTION .....	32
6.2.3	ENABLE/DISABLE DHCP .....	32
6.3	NETWORK DIAGNOSIS.....	33
<b>7</b>	<b>SYSTEM .....</b>	<b>34</b>
7.1	DATE AND TIME.....	34
7.2	ATTENDANCE.....	35
7.3	FACE PARAMETERS.....	36
7.4	FINGERPRINT .....	39
7.5	SECURITY SETTINGS .....	41
7.6	FACTORY RESET .....	42
<b>8</b>	<b>PERSONALIZE SETTINGS .....</b>	<b>43</b>
8.1	INTERFACE SETTINGS.....	43
8.2	VOICE SETTINGS.....	44
8.3	BELL SCHEDULES .....	45
8.3.1	ADD A BELL.....	45

---

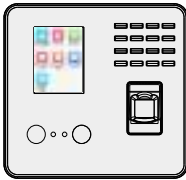
- 8.3.2 EDIT A BELL ..... 46
- 8.3.3 DELETE A BELL ..... 47
- 9 ATTENDANCE SEARCH ..... 48**
- 10 AUTOTEST ..... 49**
- 11 SYSTEM INFORMATION ..... 51**
- 12 CONNECT TO NGTECO OFFICE ..... 52**
  - 12.1 CREATE YOUR ACCOUNT ..... 52
  - 12.2 CREATE THE ORGANIZATION ..... 53
  - 12.3 PERSON MANAGEMENT ..... 55
    - 12.3.1 ADD PERSON ..... 55
    - 12.3.2 EDIT PERSON ..... 56
    - 12.3.3 DELETE PERSON ..... 57
  - 12.4 DEPARTMENT MANAGEMENT ..... 57
    - 12.4.1 ADD DEPARTMENT ..... 58
    - 12.4.2 EDIT DEPARTMENT ..... 58
    - 12.4.3 DELETE DEPARTMENT ..... 59
  - 12.5 SITE MANAGEMENT ..... 60
    - 12.5.1 ADD SITE ..... 60
    - 12.5.2 EDIT SITE ..... 61
    - 12.5.3 DELETE SITE ..... 61
  - 12.6 ZONE MANAGEMENT ..... 62
    - 12.6.1 ADD ZONE ..... 62
    - 12.6.2 EDIT ZONE ..... 63
    - 12.6.3 DELETE ZONE ..... 64
  - 12.7 DEVICE MANAGEMENT ..... 64

---

- 12.7.1 ADD DEVICE..... 65
- 12.7.2 VIEW DEVICE ..... 67
- 12.7.3 EDIT DEVICE..... 67
- 12.7.4 DELETE DEVICE ..... 68
- 12.7.5 OPERATION DEVICE..... 69
  
- 12.8 SYNCHRONIZE PERSONS TO DEVICE ..... 72**
- 12.8.1 ADD TIMESHEET..... 72
- 12.8.2 ADD SHIFT SCHEDULE..... 73
  
- 12.9 REPORT ATTENDANCE ..... 77**
- 12.9.1 VIEW ATTENDANCE REPORTS ..... 77
- 12.9.2 EXPORTING REPORTS..... 79

# 1 Overview

This document outlines the menu operation of **NG-TC1** and creates an ecologically interconnected, hardware and software interoperability platform in conjunction with NGTeco Office software. It is convenient to unified management of device, set up organization, attendance rules, managing user information, managing user privileges, set up verification modes, generate timecard reports and attendance logs, etc.



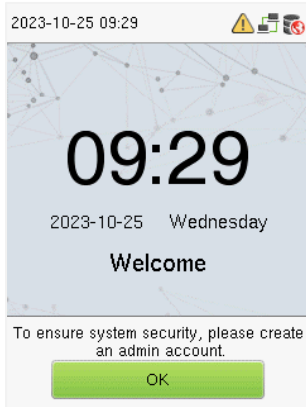
## Key Features

- Easy to monitor and straight-forward services.
- Reduces management cost for attendance related procedures.
- Unified management of device.
- Setting up timesheet and staff schedule anytime, anywhere
- Advanced attendance analytics.
- Granular visibility into attendance patterns.
- Greatly reduces month-end hassles and compliance challenges.
- Data encrypted in the cloud, safe and secure.



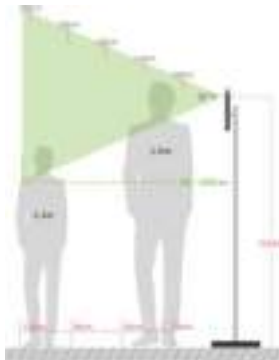
## 2 Operational Procedure

**Note:** When there is no super administrator registered in the device, press the <M/OK> key to open the menu. After setting the super administrator, it requires the super administrator’s verification before entering the menu operation. For the security of the device, it is recommended to register a super administrator the first time you use the device.



### 2.1 Standing Position, Posture and Facial Expression

- The recommended distance



The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward or backward to improve the quality of facial images captured.

- Recommended Standing Posture and Facial Expression



Standing Posture

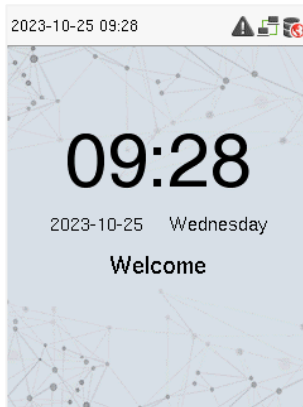


Facial Expression

**Note:** Please maintain a natural facial expression and standing posture during enrolment or verification.

## 2.2 Standby Interface

The device's home screen displays the current attendance status:



## 2.3 Face Template Registration

Keep your face centered on the screen during registration. Face towards the camera and remain still during face template registration. The screen should look like this:



### Correct face registration and authentication method:

➤ **Recommendation for registering a face:**

- When registering a face template, maintain a distance of 40cm to 80cm between the device and your face.
- Be careful not to change your facial expression, such as smiling, drawn, winking, etc.)
- Not following on-screen instructions may result in longer or failed face template registration.
- 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 template:**

- Ensure that the face appears inside the guideline displayed on the screen of the device.
- If glasses are changed, authentication may fail. If a face without glasses is registered, authenticate without glasses; if a face with glasses is registered, authenticate with the previously worn glasses.
- 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.

## **2.4 Finger Enrollment**

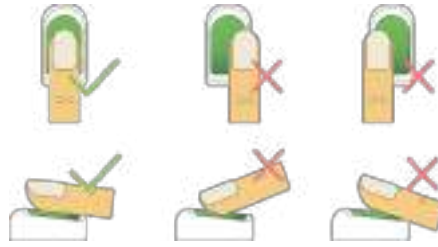
Finger Enrollment procedure involves capturing a user's fingerprint and saving it as a template to the corresponding User ID. To enhance the fingerprint authentication rate, make sure you enroll the finger in a proper manner.

### **2.4.1 Finger Selection for Enrollment**

- It is recommended to use the index finger or middle finger to enroll your fingerprint.
- If the fingerprints on your selected hand are worn or damaged, try using the other hand.
- If the fingers are small, try enrolling the thumb finger.

### **2.4.2 Enrollment Operation**

- Place the finger flat and centered on the sensor surface.
- The score for each enrollment will be displayed. Make sure the score is high enough to ensure proper enrollment and authentication.
- Place the finger consecutively until the success message appears. An illustration is given below:



### 2.4.3 Quality Improvement of Fingerprint Reads

- Place the finger firmly on the sensor surface.
- Always use clean fingers for enrollment.
- Do not slide the finger while enrolling it.
- Avoid angled or tilted finger positions for enrollment.

For further details, refer [Fingerprint Enrollment](#).

## 2.5 Verification Modes

In the device, there are four verification modes, namely:

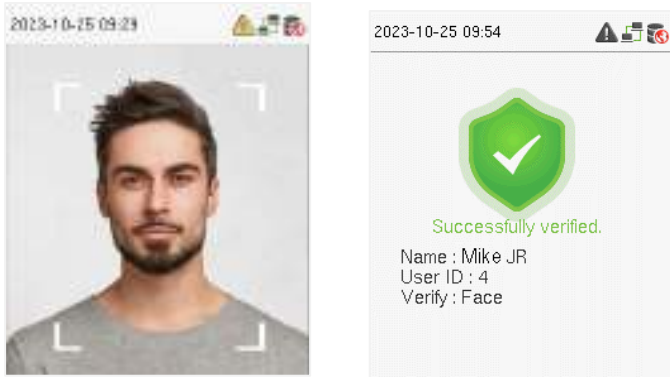
- Fingerprint verification
- Face verification
- Card Number verification
- Password verification

These verification modes can be used for check-in and check-out punches and access to the admin menu.

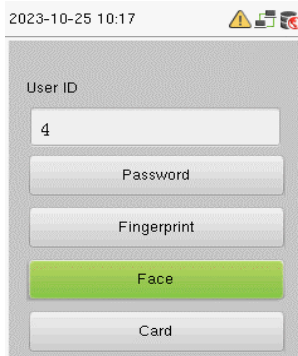
### 2.5.1 Face Verification

The face verification can be done in two ways:

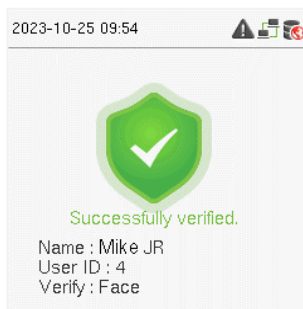
**1: N Verification:** In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.



**1:1 Verification:** In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Enter your User ID through the keypad and select the face to enter face verification mode.



If the verification is successful, the success message will be displayed as shown below:

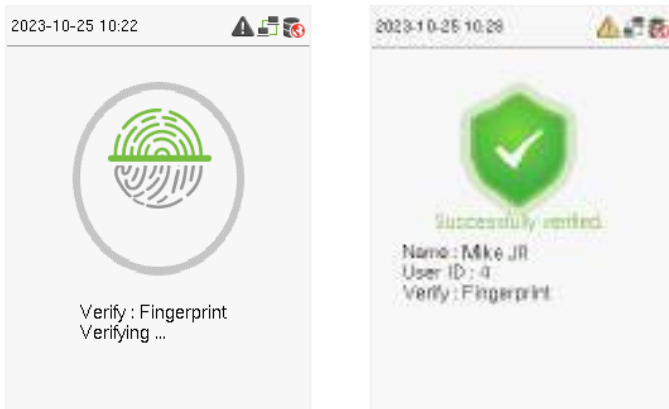


## 2.5.2 Fingerprint Verification

The fingerprint verification can be done in two ways:

**1: N Verification:** The device compares the current fingerprint collected by the fingerprint sensor with all the fingerprints on the device. Press your finger properly on the fingerprint sensor. If the fingerprint matches with the saved template, the verification is successful.

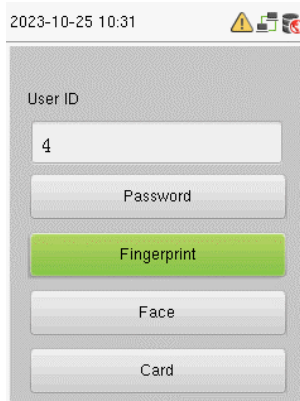
If the verification is successful, the success message will be displayed as shown below:



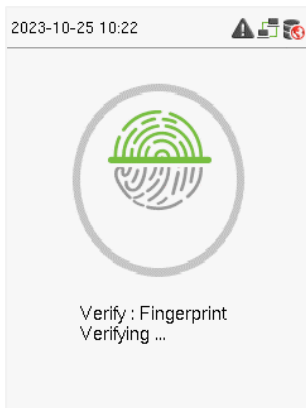
If the verification failed, the message will be displayed as shown below:



**1:1 Verification:** The device compares the current fingerprint collected by the fingerprint sensor with the fingerprint template saved for the corresponding User ID. Enter your User ID through the keypad and press your finger.

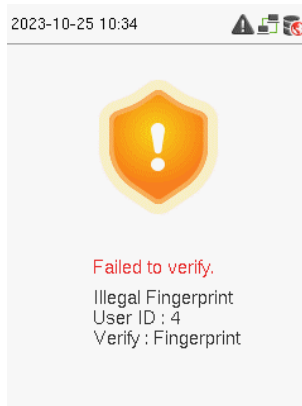


If the fingerprint matches the saved template, the verification is successful, and the success message will be displayed as shown below:





If the verification failed, the message will be displayed as shown below:

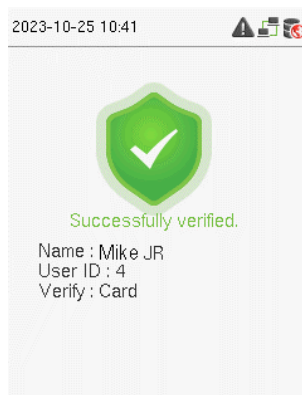


If the device instructs "**Failed to verify.**", then press your finger again. You can try 2 more times. If the verification fails after trying for 2 more times, then the device returns to the home screen.

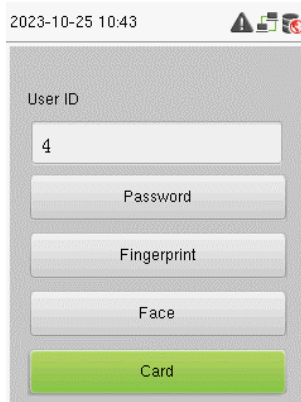
### 2.5.3 Card Number Verification

The card number verification can be done in two ways:

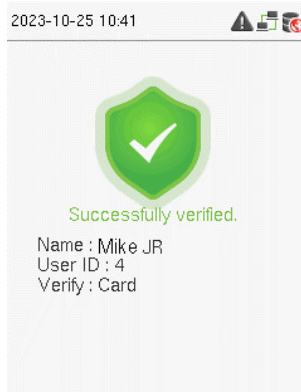
**1: N Verification:** The device compares the card number in the card induction area with all the card number data registered in the device; The following is the card verification screen.



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

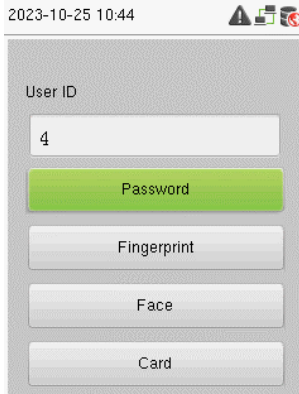


If the verification is successful, the success message will be displayed as shown below:



## 2.5.4 Password Verification

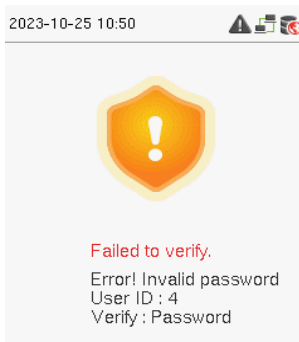
In the Password verification mode, the device compares the entered password with the registered password corresponding to the User ID. If both the passwords match, then the verification is successful.



If the verification is successful, the success message will be displayed as shown below:



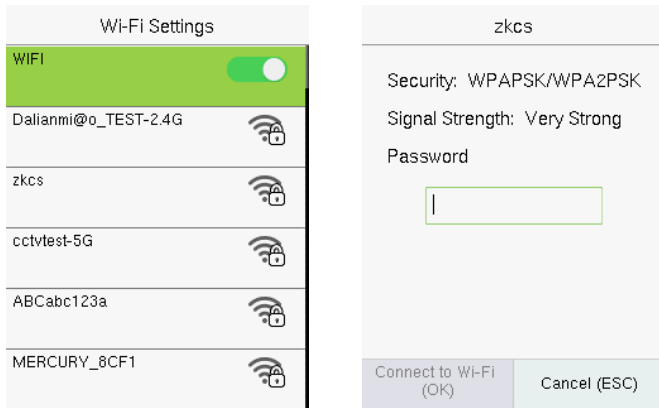
If the verification failed, the message will be displayed as shown below:



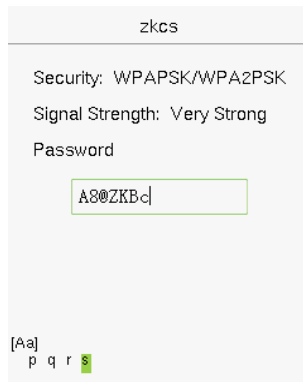
## 2.6 T9 Mode

T9 mode allows you to enter the Uppercase, Lowercase, and Special characters in the text input fields. You can enter the alphabets and special characters by pressing one keystroke per letter. Press the <▶> key in the text box to activate T9 mode.

1. Navigate to the required text field and press <M/OK>.



2. Each key on the keypad has a few letters printed above them. For example, pressing 3 can enter D, E, and F. To enter "F", press 3 thrice. This is accomplished by comparing the number of keystrokes with the internal syntactical dictionary to determine the letter.
3. Press <▶> to switch between Uppercase, Lowercase, and Special characters.



4. To add the special character, press the corresponding key once. For example, to enter "@" press 2 once.
5. After the input is complete, press the **<M/OK>** key twice to save.

### 3 Privileges

The user privileges are classified as:

- Administrator
- Normal user

Normal user and super admin settings can be set in **[Device Management] > [Person in Devices]** in NGTeco Office. As shown in the figure below:



## 3.1 Administrator

The Administrator privilege safeguards the device's important configurations. Administrators can operate all menus, manage attendance through fingerprint/password, make configuration changes, add/modify user details, and query attendance records. Click here for detailed menu operations. Click [here](#) to view the detailed menu operations.

After registering as an administrator, you must use the administrator authentication method to enter the menu. The administrator presses the **<M/OK>** key and is then authenticated to the menu screen.



The admin must verify the face/fingerprint/card number or enter user ID to verify the password. Please refer to [2.5 Verification Modes](#).

## 3.2 Normal User

Normal users can make attendance punch through face/fingerprint/card number/password verification methods. For further details, please refer to [2.5 Verification Modes](#).

# 4 Main Menu

Press the <M/OK> key to open the menu.



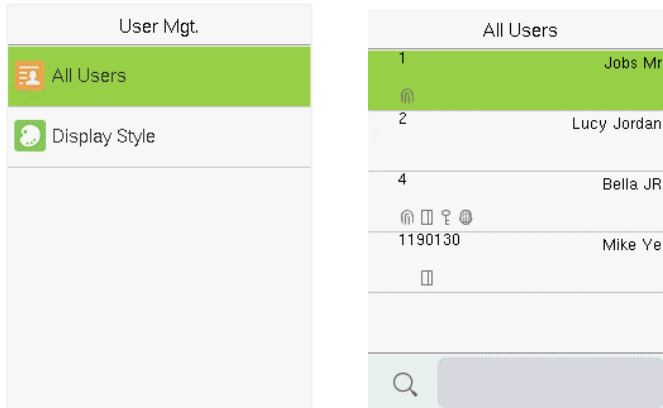
Menu	Description
<b>Users</b>	View user information and register verification modes.
<b>Comm. (Communication Settings)</b>	To set the relevant parameters of the network, Wi-Fi and Network Diagnosis.
<b>System</b>	To set the parameters related to the system, including Date Time, Attendance, Face and Fingerprint templates, Resetting to factory settings, Security Settings.
<b>Personalize</b>	To customize settings of User Interface, Voice, and Bell Schedules.
<b>Attendance Search</b>	To query the specified attendance record.
<b>Autotest</b>	To automatically test whether each module functions properly, including the screen, audio, keyboard, camera, fingerprint and real-time clock.
<b>System Info</b>	To view the data capacity, device and firmware information and privacy policy of the device.



## 5 User

The **[User]** of the device only supports browsing user information and registration verification mode. Adding, editing and deleting user information must be done on NGTeco Office, please refer to [12.3.1 Add Person](#).

Select **[User]** on the main menu interface and press **<M/OK>**.



### 5.1 Search for Users

Select **[All Users]** to search a user.

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



## 5.2 Register Fingerprint

Select **[Fingerprint]** in the **[All Users]** interface to enter the fingerprint registration page.

Edit : 1 Jobs Mr	
User ID	1
Name	Jobs Mr
User Role	Normal User
Fingerprint	1
Face	0
Card Number	

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



## 5.3 Register Face

Select **[Face]** in the **[All Users]** interface to enter the face registration page.

Edit : 1 Jobs Mr	
User ID	1
Name	Jobs Mr
User Role	Normal User
Fingerprint	2
Face	0
Card Number	

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

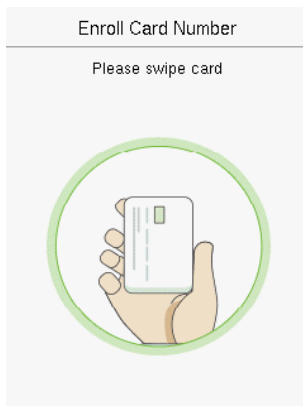


## 5.4 Register Card

Select **[Card Number]** in the **[All Users]** interface to enter the face registration page.

Edit : 1 Jobs Mr	
User ID	1
Name	Jobs Mr
User Role	Normal User
Fingerprint	2
Face	0
Card Number	

- Swipe the card underneath the card reading area on the Card interface. 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 looks like this:

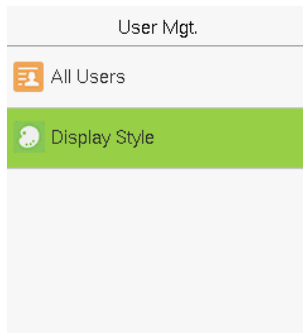


## 5.5 Register Password

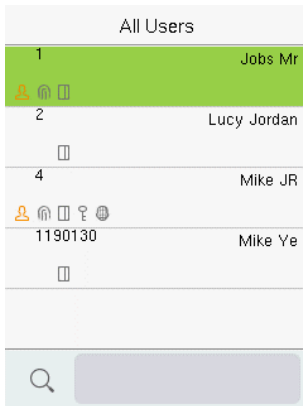
For security reasons, passwords can only be set through NGTeco Office, please refer to [12.7.5 Operation Device](#) for details.

## 5.6 Display Style

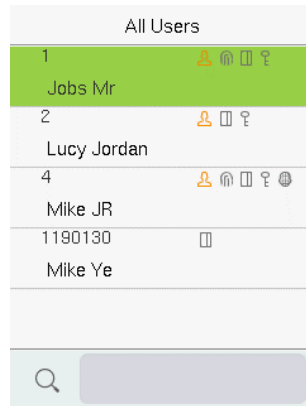
On the main menu, select **[User]**, and then select **[Display Style]** to enter Display Style setting interface.



Multiple Line:



Mixed Line:

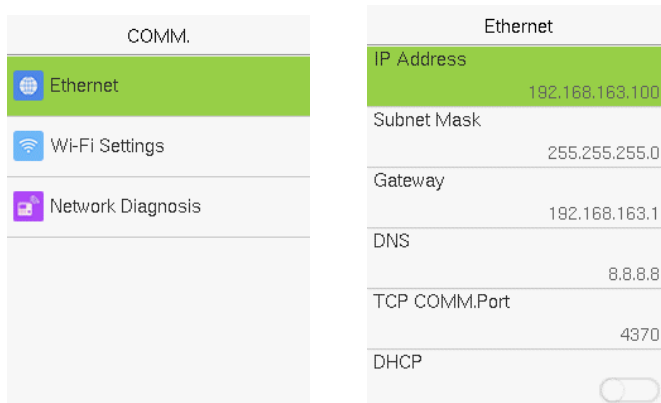


## 6 Communication Parameters

Select **[COMM.]** on the main menu interface and press **<M/OK>**.

### 6.1 Manual Ethernet Configuration

On the **[Comm.]** interface, select **[Ethernet]** and press **<M/OK>**.



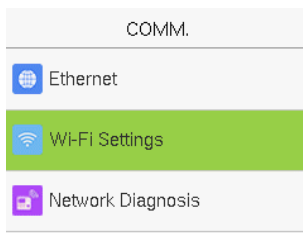
Menu	Description
<b>IP Address</b>	The factory default value is 192.168.1.201. Please set the IP Address as per the requirements.
<b>Subnet Mask</b>	The factory default value is 255.255.255.0. Please set the value as per the requirements.
<b>Gateway</b>	The factory default address is 0.0.0.0. Please set the value as per the requirements.
<b>DNS</b>	The factory default address is 0.0.0.0. Please set the value as per the requirements.
<b>TCP COMM. Port</b>	The factory default value is 4370. Please set the value as per the requirements.

<b>DHCP</b>	Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.
<b>Display in Status Bar</b>	To set whether to display the network icon on the status bar.

## 6.2 Manual Wi-Fi Configuration

### 6.2.1 Connection to an Existing Wi-Fi

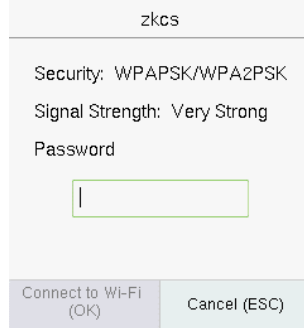
On the **[Comm.]** interface, select **[Wi-Fi Settings]** and press **<M/OK>**.



The list of available Wi-Fi connections will be displayed as shown below:



1. Navigate to the required Wi-Fi connection and press **<M/OK>**.
2. The interface to connect Wi-Fi will be displayed as shown below. If the signal strength is weak, the device may fail to connect.



3. Navigate to **[Password]** and press the <▶> key to enter the password to connect. Please refer to [T9 Mode](#).
4. Then navigate to **[Connect to Wi-Fi (OK)]** and press <M/OK>.
5. Once connected, the connectivity status will be displayed as shown below:



**Note:**

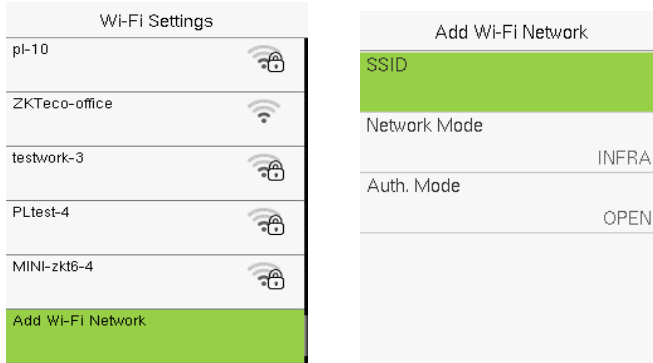
1. Device Wi-Fi only supports 2.4GHz communication.
2. It is recommended that you connect your device within approximately 15 metres of the Wi-Fi.
3. If the Wi-Fi connection status of your device shows not connected for a long time, please enter the password again.



## 6.2.2 New Wi-Fi Connection

On the **[Comm.]** interface, select **[Wi-Fi Settings]** and press **<M/OK>**.

1. Press **[Add Wi-Fi Network]** to add a new connection. The interface to add a new connection will be displayed as shown below:



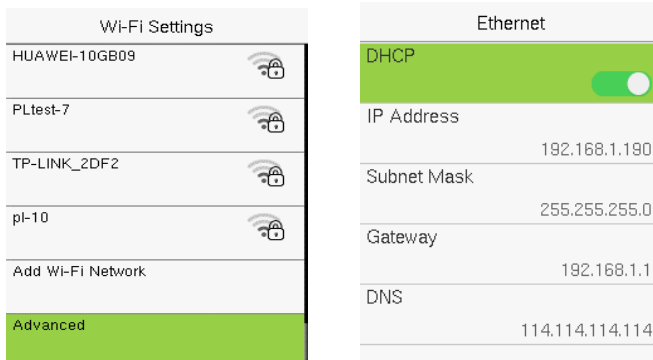
2. On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name. Click [here](#) to view the process to search the Wi-Fi network.

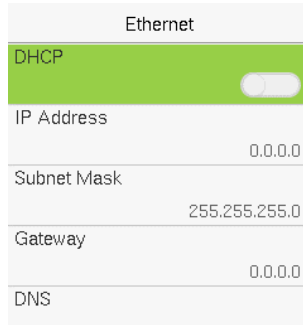
## 6.2.3 Enable/Disable DHCP

On the **[Comm.]** interface, select **[Wi-Fi Settings]** and press **<M/OK>**.

1. Press **[Advanced]** to view the DHCP settings.
2. Turn on DHCP if unable to connect to Wi-Fi.

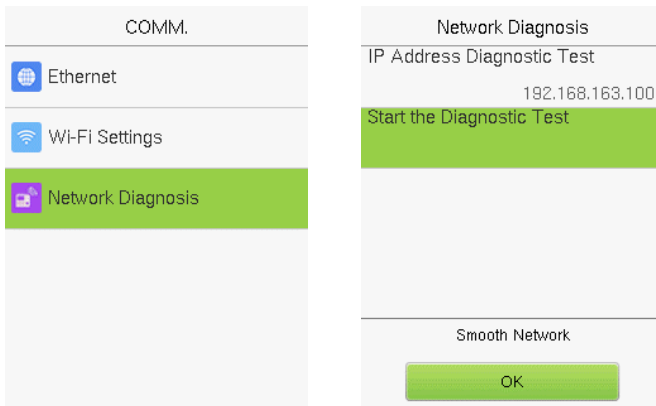


- If you disable DHCP, you must manually set the IP Address, Subnet mask, and Gateway by pressing <▼>. The interface is shown below:



### 6.3 Network Diagnosis

On the [Comm.] interface, select [Network Diagnosis] and press <M/OK>.

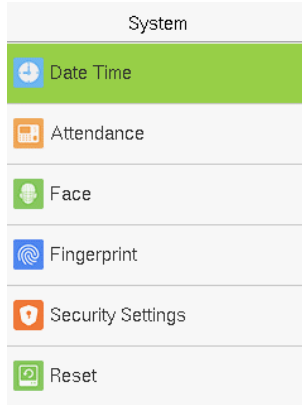


Menu	Description
<b>IP Address Diagnostic Test</b>	The factory default address is 0.0.0.0. Please set the value as per the requirements.
<b>Start the Diagnostic Test</b>	Press start to automatically diagnose the network.

## 7 System

Here, the user can set the related system parameters to maximize the performance of the device.

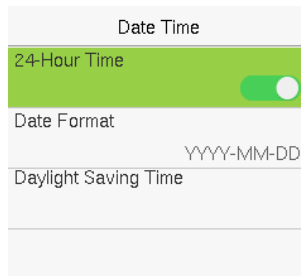
Select **[System]** on the main menu interface and press **<M/OK>**.



### 7.1 Date and Time

It is necessary to calibrate the date and time of the device before usage to ensure accurate attendance time. The procedure to set the date and time is given below:

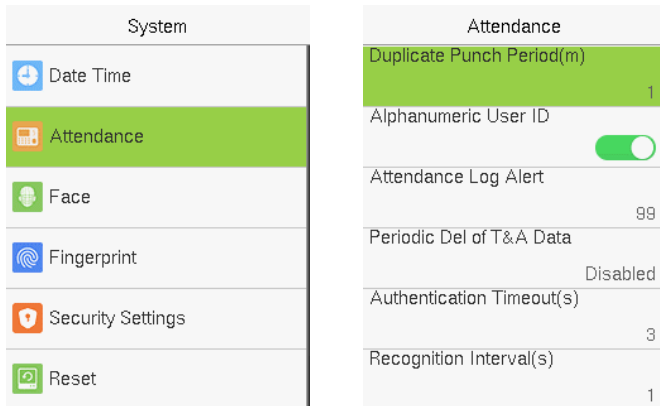
On the **[System]** interface, select **[Date Time]** and press **<M/OK>**.



Menu	Description
<b>24-Hour Time</b>	Select whether to use the 24-hour display mode. If not, the 12-hour display mode is adopted.
<b>Date Format</b>	Set the Date Format from the available options using <▲> or <▼> key.
<b>Daylight Saving Time</b>	Enable or Disable the Daylight Saving using <M/OK> key.

## 7.2 Attendance

On the [System] interface, select [Attendance] and press <M/OK>.

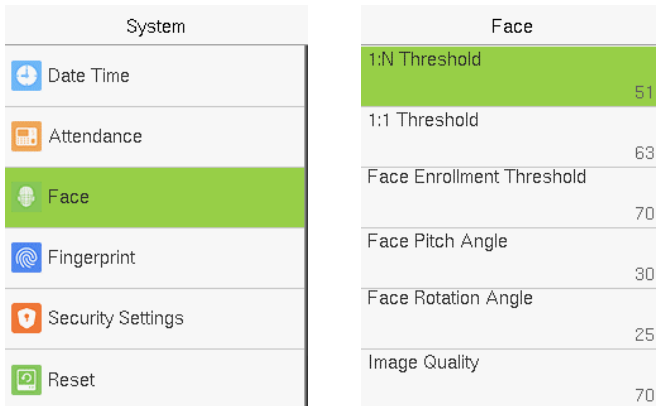


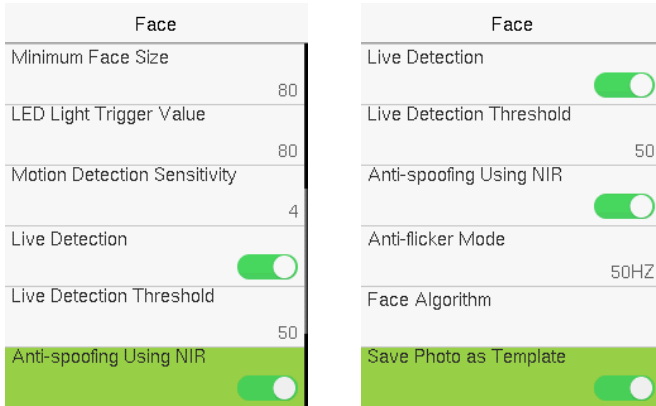
Menu	Description
<b>Duplicate Punch Period (m)</b>	Within the set time range, the attendance record of the same person will not be saved; the valid value ranges from 1 to 999999 minutes.

<b>Alphanumeric User ID</b>	Enable/Disable the alphanumeric as User ID.
<b>Attendance Log Alert</b>	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.
<b>Periodic Del of T&amp;A Data</b>	When attendance 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.
<b>Authentication Timeout(s)</b>	The amount of time taken to display a successful verification message. Valid value: 1 to 9 seconds.
<b>Recognition Interval(s)</b>	To set the verification time interval as required. Valid value: 0~9 seconds.

### 7.3 Face Parameters

On the **[System]** interface, select **[Face]** and press **<M/OK>**.





Menu	Description
<b>1:N Threshold</b>	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, the higher the rejection rate, and vice versa. It is recommended to set the default value of 51.
<b>1:1 Threshold</b>	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 is the rejection rate, and vice versa. It is recommended to set the default value of 63.
<b>Face Enrollment Threshold</b>	During face enrolment, 1:N comparison is used to determine whether the user has already registered before. When the similarity between the acquired facial image and all registered facial templates is greater than this threshold, it indicates that the face has already been registered.
<b>Face Pitch Angle</b>	The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.

<b>Face Rotation Angle</b>	The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.
<b>Image Quality</b>	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
<b>Minimum Face Size</b>	Required for facial registration and comparison. If the minimum size of the captured figure is smaller than this set value, then it will be filtered off and not recognized as a face. This value can be understood as the face comparison distance. The farther the person is, the smaller the face is, and the smaller the face pixel will be obtained by the algorithm. Therefore, adjusting this parameter can adjust the furthest comparison distance of faces. When the value is 0, the face comparison distance is not limited.
<b>LED Light Triggered Value</b>	This value controls the on and off the LED light. The larger the value, the more frequently the LED light will be turned on.
<b>Motion Detection Sensitivity</b>	It is to set the value for the amount of change in a camera's field of view, which is known as potential motion detection that wakes up the terminal from standby to the comparison interface. The larger the value, the more sensitive the system would be, i.e. if a larger value is set, the comparison interface is much easier and the motion detection frequently triggered.
<b>Live Detection</b>	Detecting the spoof attempt using visible light images to determine if the provided biometric source sample is really a person ( a live human being) or false representation.
<b>Live Detection Threshold</b>	Facilitates to judge whether the captured visible image is really a person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.
<b>Anti-spoofing Using NIR</b>	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
<b>Anti-flick Mode</b>	Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.

<p><b>Face Algorithm</b></p>	<p>It has facial algorithm related information and pause facial template update.</p>
<p><b>Save Photo as Template</b></p>	<p>This function is enabled by default, and the menu interface supports enabling or disabling this function, and there is a security prompt when switching. When this function is disabled, it will indicate that there is a risk reminder: <b>"Face re-registration is required after an algorithm upgrade."</b></p>

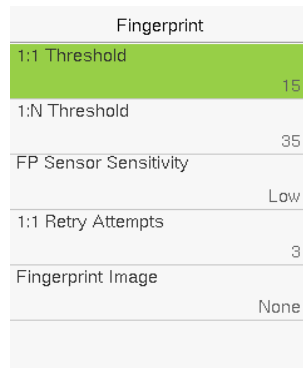
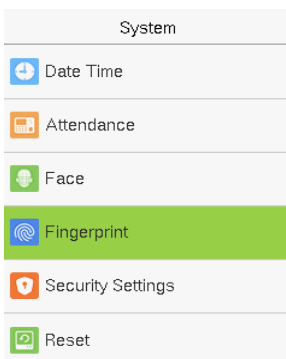
**Note:** Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.

**Process to modify the Face Recognition Accuracy**

- On the System interface, select Face and then toggle to enable Anti-Spoofing using NIR to set the anti-spoofing.
- Then, on the Main Menu, select Autotest > Test Face and perform the face test.
- Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

## 7.4 Fingerprint

On the [System] interface, select [Fingerprint] and press <M/OK>.

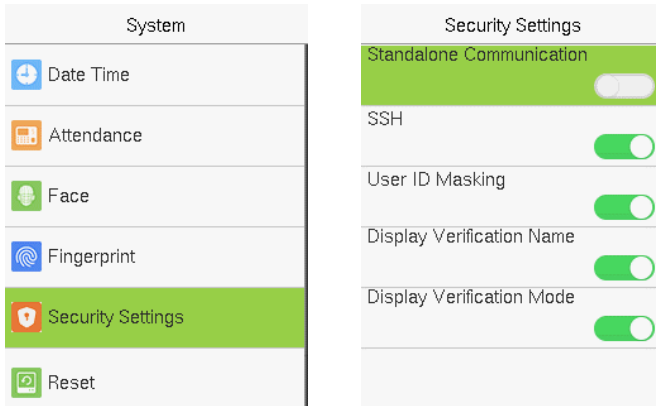




Menu	Description
<b>1:1 Threshold</b>	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
<b>1:N Threshold</b>	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.
<b>FP Sensor Sensitivity</b>	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".
<b>1:1 Retry Times</b>	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.
<b>Fingerprint Image</b>	<p>This function is disabled by default. After disabling it, the fingerprint image will not be displayed when registering and verifying fingerprints. The menu interface allows to enable or disable this function, and there are security prompts when switching. Four choices are available:</p> <p><b>Show for Enroll:</b> To display the fingerprint image on the screen only during enrollment.</p> <p><b>Show for Match:</b> To display the fingerprint image on the screen only during verification.</p> <p><b>Always Show:</b> To display the fingerprint image on screen during enrollment and verification.</p> <p><b>None:</b> Not to display the fingerprint image.</p>

## 7.5 Security Settings

On the **[System]** interface, select **[Security Settings]** and press **<M/OK>**.



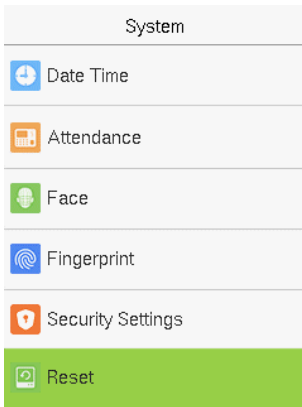
Menu	Description
<b>Standalone Communication</b>	By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm.
<b>SSH</b>	The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation.
<b>User ID Masking</b>	After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default.
<b>Display Verification Name</b>	After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it.

<b>Display Verification Mode</b>	After enabled, the personnel verification result will show the user's verification mode. The verification result will not show the verification mode after you disable it.
----------------------------------	--

## 7.6 Factory Reset

This option restores the device, such as communication settings and system settings, to factory settings (does not clear registered user data).

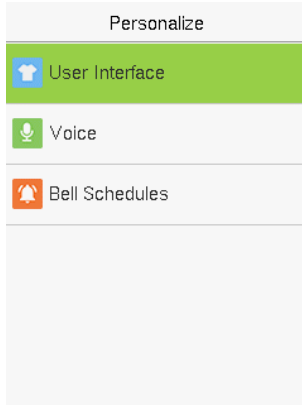
On the **[System]** interface, select **[Reset]** and press **<M/OK>**.



# 8 Personalize Settings

You may customize the interface settings, audio, and bell.

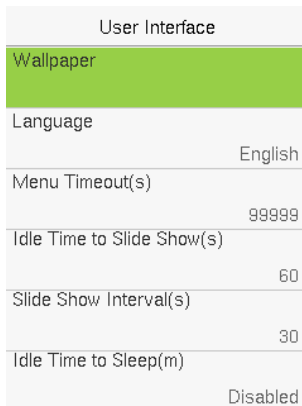
Select [**Personalize**] on the main menu interface and press <M/OK>.



## 8.1 Interface Settings

You can customize the display style of the main interface.

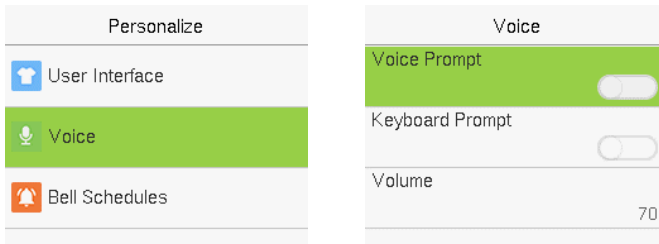
On the [**Personalize**] interface, select [**User Interface**] and press <M/OK>.



Menu	Description
Wallpaper	To select the main screen wallpaper according to your personal preference.
Language	To select the language of the device.
Menu Timeout (s)	When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds.
Idle Time to Slide Show (s)	When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	This refers to the time interval switching different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds.
Idle Time to Sleep (m)	If you have activated the sleep mode, when there is no operation, the device will enter the standby mode. You can disable this function or set a value within 1-999 minutes.

## 8.2 Voice Settings

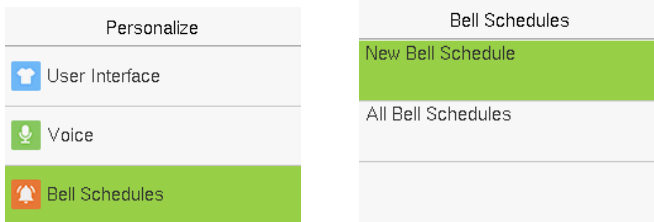
On the **[Personalize]** interface, select **[Voice]** and press **<M/OK>**.



Menu	Description
Voice Prompt	Select whether to enable voice prompts during operation.
Keyboard Prompts	Select whether to enable keypad sounds.
Volume	Adjust the volume of the device; valid value: 0 to 100.

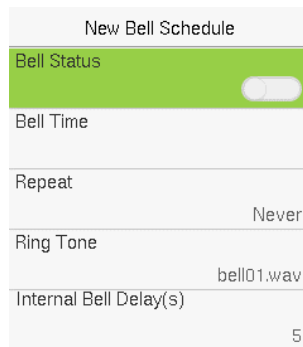
### 8.3 Bell Schedules

On the **[Personalize]** interface, select **[Bell Schedules]** and press **<M/OK>**.



#### 8.3.1 Add a Bell

On the **[Bell Schedule]** interface, select **[New Bell Schedules]** and press **<M/OK>**.



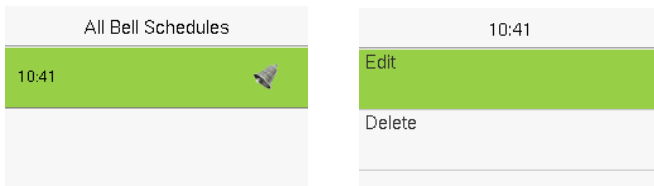
Menu	Description
<b>Bell Status</b>	Set whether to enable the bell status.
<b>Bell Time</b>	At this time of day, the device automatically rings the bell.
<b>Repeat</b>	Set the repetition cycle of the bell.
<b>Ring Tone</b>	Select a ring tone.
<b>Internal Bell Delay (s)</b>	Set the duration of the internal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

Back to the **[Bell Schedules]** interface; select **[All Bell Schedules]** to view the newly added bell.

### 8.3.2 Edit a Bell

On the **[All Bell Schedule]** interface, select the bell to be edited and press **<M/OK>**.

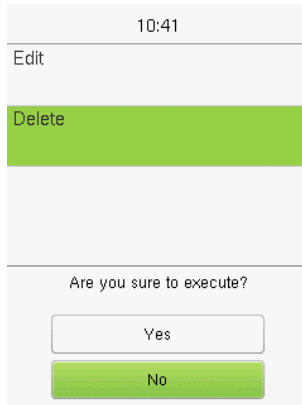
Select **[Edit]**, the editing method is the same as the operations of adding a bell.



### 8.3.3 Delete a Bell

On the **[All Bell Schedule]** interface, select the bell to be deleted and press **<M/OK>**.

Select **[Delete]** and select **[Yes]** to delete the bell.





# 9 Attendance Search

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

Select **[Attendance Search]** on the main menu interface and press **<M/OK>**.

On the **[Attendance Search]** interface, 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.

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

User ID

---

Please Input(query all data without input)

Right key to switch input method, Left key to back space

Confirm (OK)
Cancel (ESC)

Time Range

Today

Yesterday

This Week

Last Week

This Month

Last Month

Personal Record Se...

Date	User ID	Time
10-26		01
	4	09:37
10-25		20
	4	15:55 15:50 15:47
		15:46 11:10 11:05
		10:47 10:41 10:38
		10:28 10:24 10:23
		10:21 10:18 09:54
		09:50 09:49
	1	15:54 15:51 15:49
10-24		01

Prev : <- Next : ->  
 Details : OK

Personal Record Se...

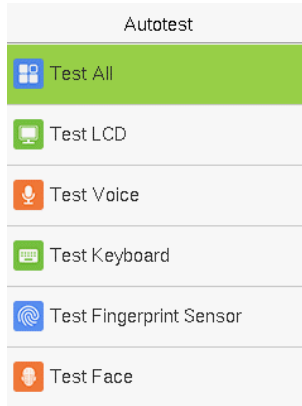
User ID	Name	Time
4	Mike ...	10-26 09:37

Verification Mode : Face  
 Punch State : 255

# 10 Autotest

The auto test enables the system to automatically test whether the functions of various modules are normal, including the LCD, Voice, Face, Fingerprint, Keyboard and Clock tests.

Select **[Autotesst]** on the main menu interface and press **<M/OK>**.



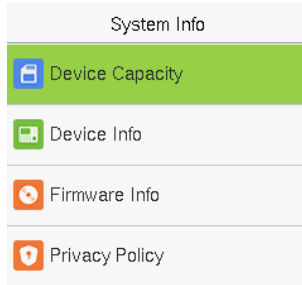
Menu	Description
<b>Test All</b>	The device automatically tests the LCD, Voice, Keyboard, Face, Fingerprint and Clock RTC, press <b>&lt;M/OK&gt;</b> to continue and press <b>&lt;ESC&gt;</b> to exit.
<b>Test LCD</b>	The device tests the display effect of LCD screen by displaying full color, pure white, and pure black to check whether the screen displays colors properly.
<b>Test Voice</b>	The device automatically tests whether the voice files stored in the device are complete and the voice quality is good.
<b>Test Keyboard</b>	Checks if the keyboard is available.

<b>Test Fingerprint Sensor</b>	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.
<b>Test Face</b>	To test if the camera functions properly by checking the pictures taken to see if they are clear enough.
<b>Test Clock RTC</b>	Checks if the RTC (Real-Time Clock) is accurate.

# 11 System Information

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

Select **[System Information]** on the main menu interface and press **<M/OK>**.



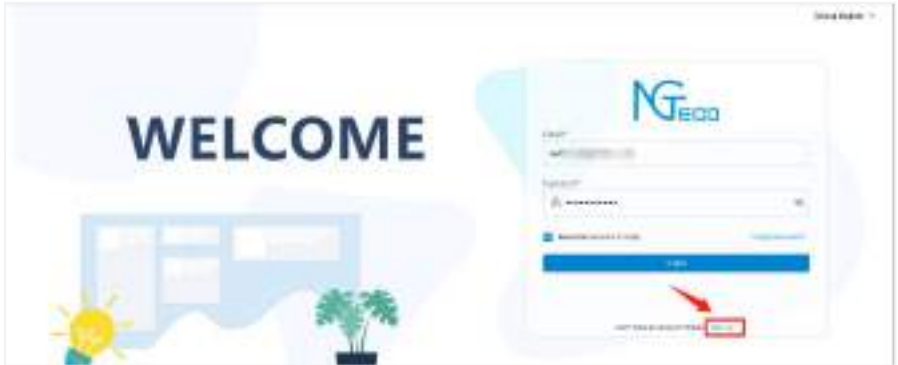
Menu	Description
<b>Device Capacity</b>	Displays the current device's user storage, password, fingerprint, face and card storage, administrators and attendance records.
<b>Device Info</b>	Displays the Device's name, Serial number, MAC Address, Face and fingerprint algorithm version information, platform information, MCU Version, manufacturer and manufacture Date.
<b>Firmware Info</b>	Displays the Firmware version and other version information of the device.
<b>Privacy Policy</b>	<p>The privacy policy control will appear when the gadget turns on for the first time. After selecting "I have read it," the customer can use the product regularly. Select System Info -&gt; Privacy Policy to view the content of the privacy policy. The privacy policy's content does not allow for U disc export.</p> <p>Note: The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations.</p>

## 12 Connect to NGTeco Office

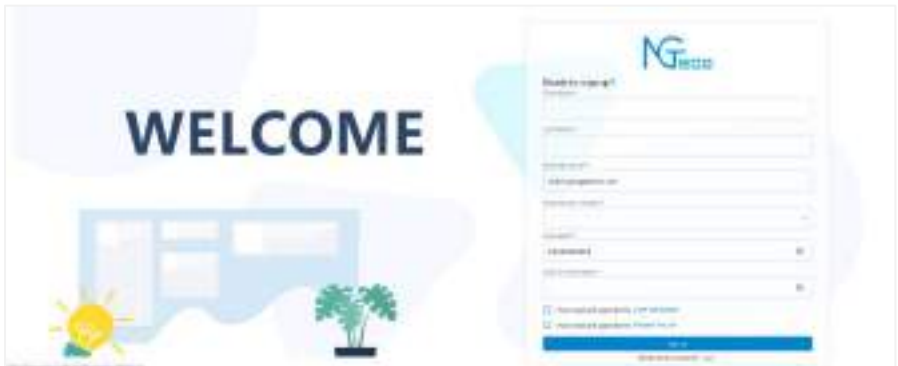
### 12.1 Create Your Account

Access the NGTeco Office <https://office.ngteco.com/>.

1. Click **[Sign up]** to create an account with your Email ID.

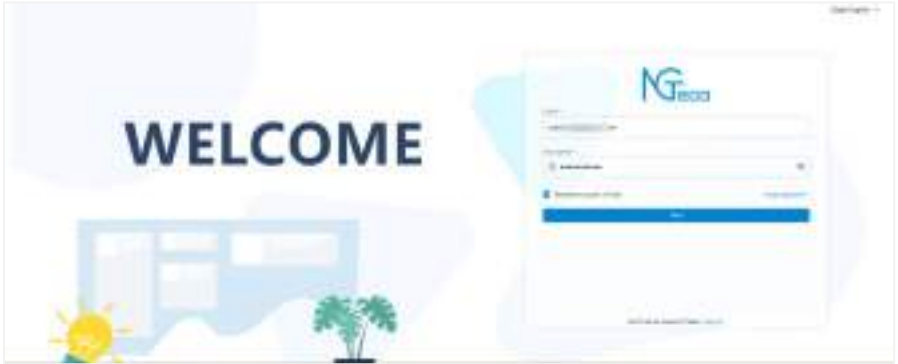


2. Enter user information to complete account registration.

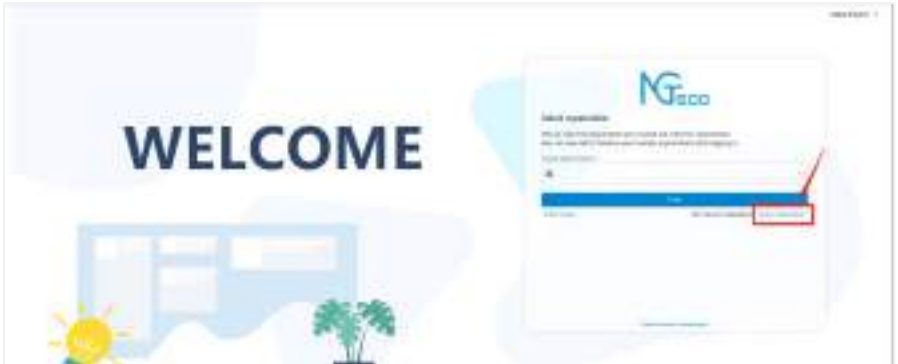


## 12.2 Create the Organization

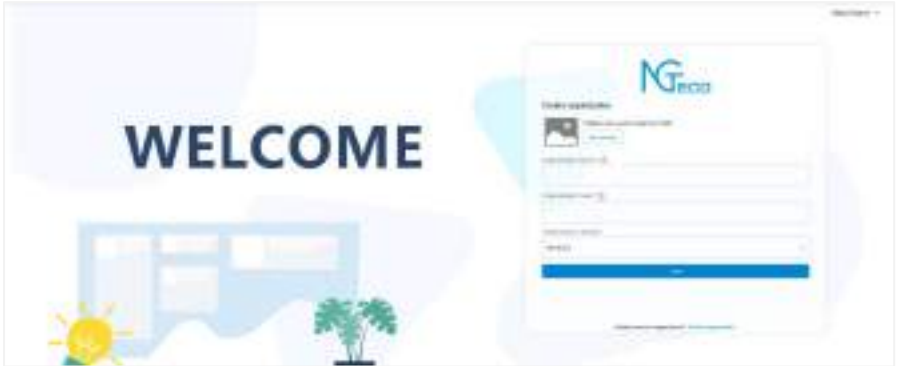
1. Log in with your registered account and follow the prompts to create an organization.



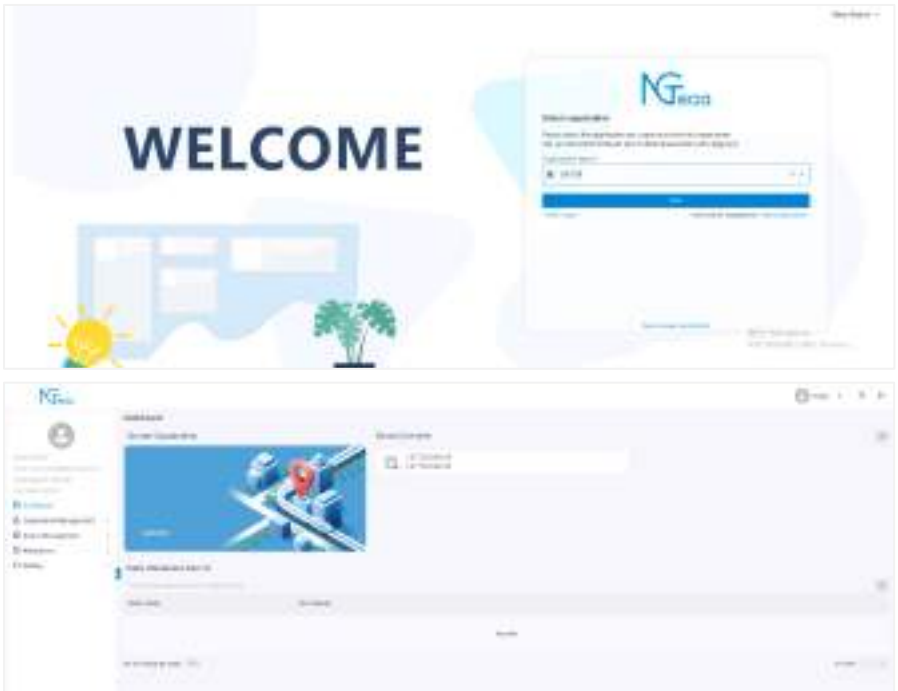
2. Click on **[Create organization]** on the pop-up page.



3. Enter information about the organization.



4. Select the successfully created organization to log in to NGTeco Office.



## 12.3 Person Management

Click **[Organization Management] > [Person]** on the NGTeco Office main menu to support adding person, editing person, and deleting person.



### 12.3.1 Add Person

1. Click the add icon  to add a new person.






- 2. Enter the person's information, and click **[Save]**.



**Note:** During the initial registration, you can modify your ID; you cannot be modifying the registered ID once after the successful registration.


### 12.3.2 Edit Person

On the **[Person]** interface, click the  icon after the person you want to edit, and you can edit the information about the person on the pop-up screen.



**Note:** Person ID does not support modification.

### 12.3.3 Delete Person

On the **[Person]** interface, click the  icon after the person you want to delete.




### 12.4 Department Management

Click **[Organization Management]** > **[Department]** on the NGTeco Office main menu to support adding department, editing department, and deleting department.



## 12.4.1 Add Department


1. Click the add icon  to add a new department.



2. Enter the department's information, and click **[Save]**.




## 12.4.2 Edit Department

On the **[Department]** interface, click the icon  of the department you want to edit to edit the department information on the pop-up screen. Editing a department is the same as adding a department.



### 12.4.3 Delete Department


On the [Department] interface, click the  icon of the department to be deleted.

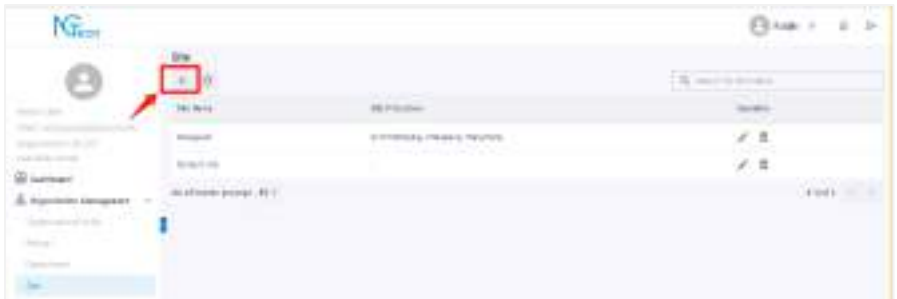




## 12.5 Site Management

### 12.5.1 Add Site


1. Click on **[Organization Management] > [Site]**, click the add icon  to add a new site.



2. Enter the site's information, and click **[Save]**.



### 12.5.2 Edit Site

On the [Site] interface, click the  icon of the site you want to edit, and then you can operate it like adding a site in the pop-up interface.




### 12.5.3 Delete Site

On the [Site] interface, click the  icon after the site you want to delete.



## 12.6 Zone Management

### 12.6.1 Add Zone


1. Click on **[Organization Management] > [Zone]**, click the add icon  to add a new zone.



- 2. Enter the zone's information, and click **[Save]**.




### 12.6.2 Edit Zone

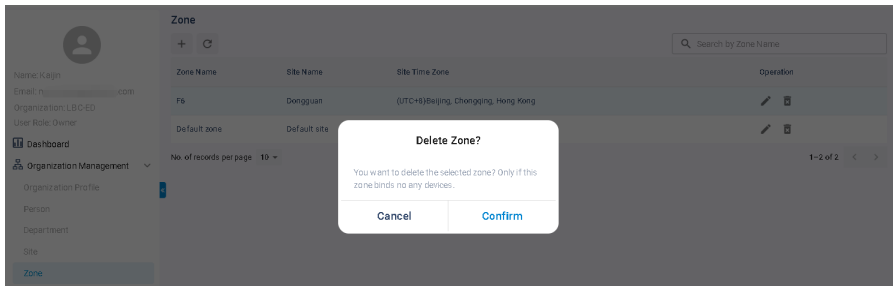
On the **[Zone]** interface, click the  icon after the zone you want to edit, and you can edit the information about the zone on the pop-up screen.





### 12.6.3 Delete Zone

On the **[Zone]** interface, click the  icon after the zone you want to delete.



## 12.7 Device Management

Click **[Device Management] > [Device Management]** on the NGTeco Office main menu to support adding device, editing device, deleting device, viewing device details, and operating devices remotely.



## 12.7.1 Add Device

1. Click the add icon  to add a new device.



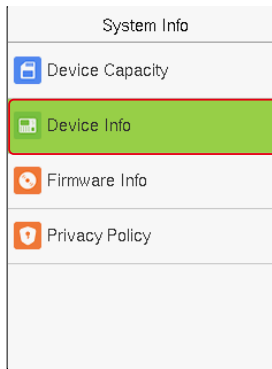
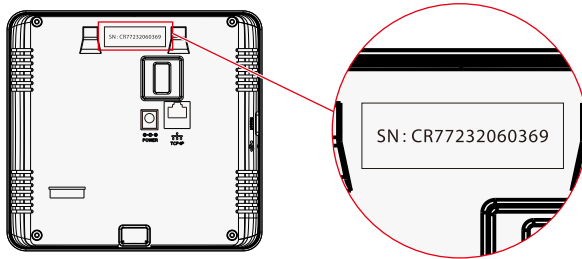
2. Follow the prompts to complete the operation.



3. Enter the device's SN code, and click **[Confirm]**.



The SN code is in the barcode on the back of the device or in the device information menu.




Device Info	
Device Name	NG-TC1
Serial Number	CR77232060369
MAC Address	00:17:61:11:dd:16
Fingerprint Algorithm	NGFinger VX10.0
Face Algorithm	NGFace VX3.5
Platform Info	ZMM510_TFT

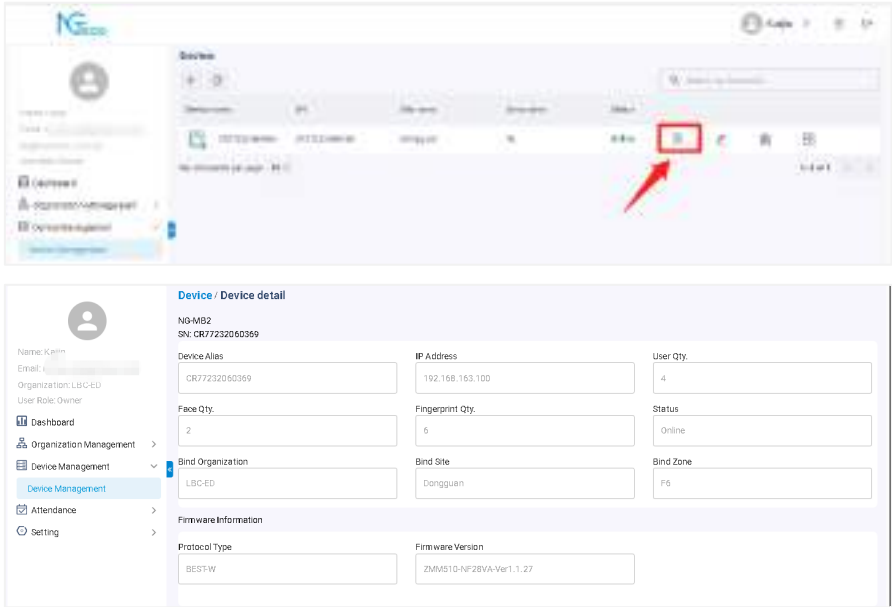
4. Site and zone assigned to the device.




## 12.7.2 View Device

On the [Device Management] interface, all successfully connected devices can be viewed,

both online and offline. Click  to view detailed information about each device.




## 12.7.3 Edit Device

On the [Device Management] interface, click the  icon, and you can edit the information about the device.






### 12.7.4 Delete Device

On the **[Device Management]** interface, click the  icon after the device you want to delete.



## 12.7.5 Operation Device

On the **[Device Management]** interface, click the  icon to remotely operate the successfully connected device. Support reboot device, sync date and time according to site and registering the person verification modes.



Click on **[Person in this device]**, you can delete the person on the current interface, set the person as normal user or super admin and register the verification modes of password/card number/fingerprint/face for the user. All the operation on the current interface is instantly synchronized to the device.




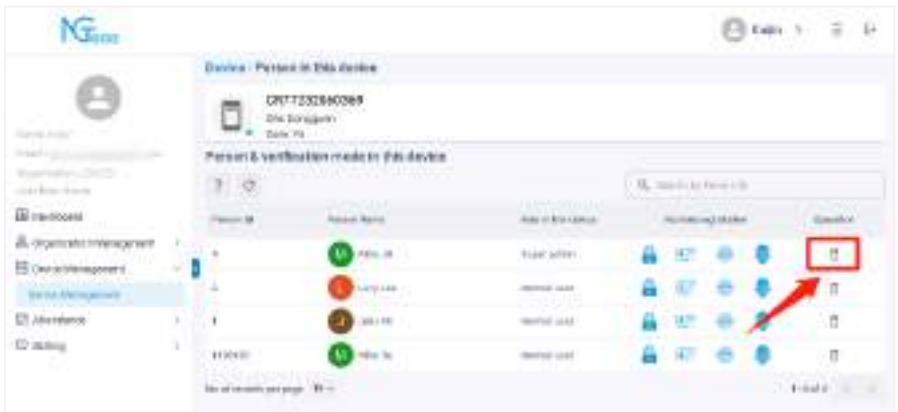
### Privileges

On the current interface, double-click the **[Role in this device]** column corresponding to person to change the user privileges.



### Delete Person


On the current interface, click the  icon to remove person from NGTeco Office and devices.

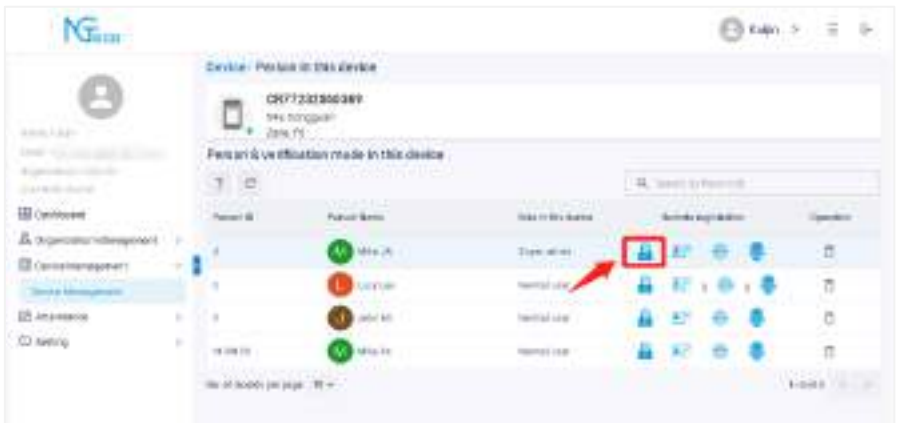




### Register Verification Modes

On the current interface, click the relevant biometric function icon (password/card/fingerprint/face) to remotely register the personnel biometric identification method. Take the registration password as an example:

1. Click on the  icon of the person who needs to register the password verification modes.





- On the pop-up page, follow the prompts to complete the password registration.



## 12.8 Synchronize Persons to Device

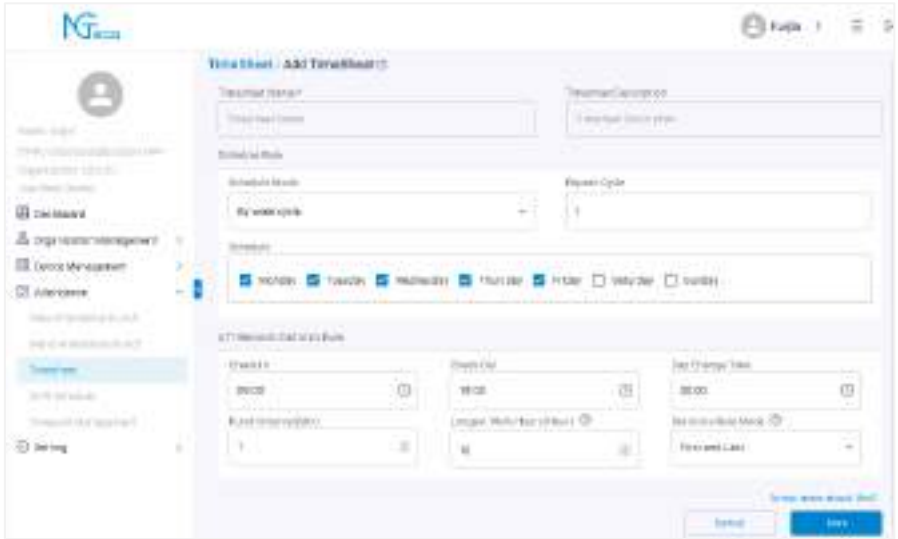
### 12.8.1 Add Timesheet

Click **[Attendance]** > **[Timesheet]** on the NGTeco Office main menu to add a timesheet.

- Click the add icon  to add a new timesheet.



2. Enter the timesheet-related information.



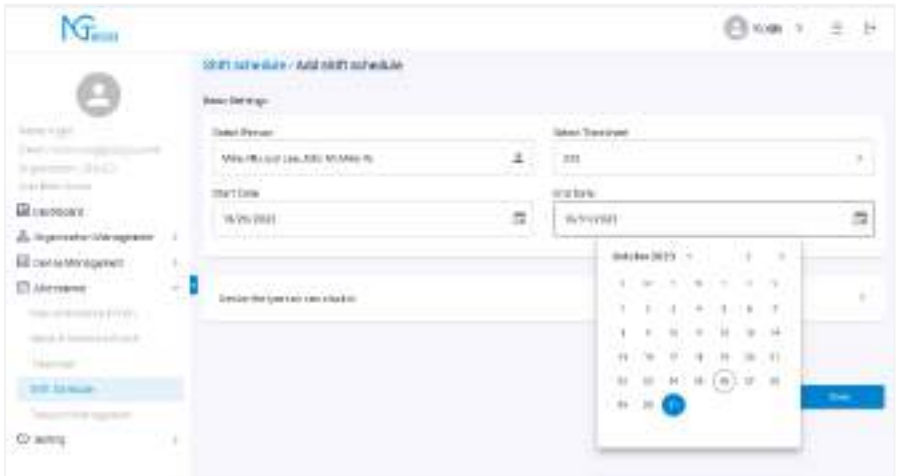
### 12.8.2 Add Shift Schedule


Click **[Attendance]** > **[Shift Schedule]** on the NGTeco Office main menu to add a shift schedule.

1. Click the add icon  to add a new shift schedule.

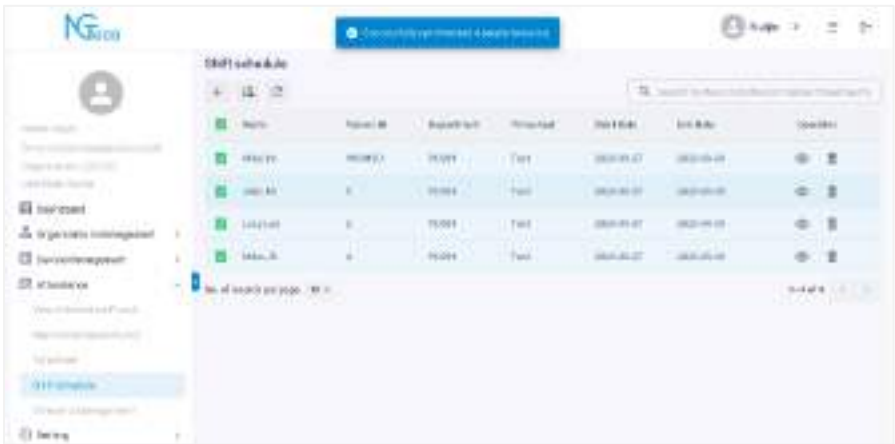
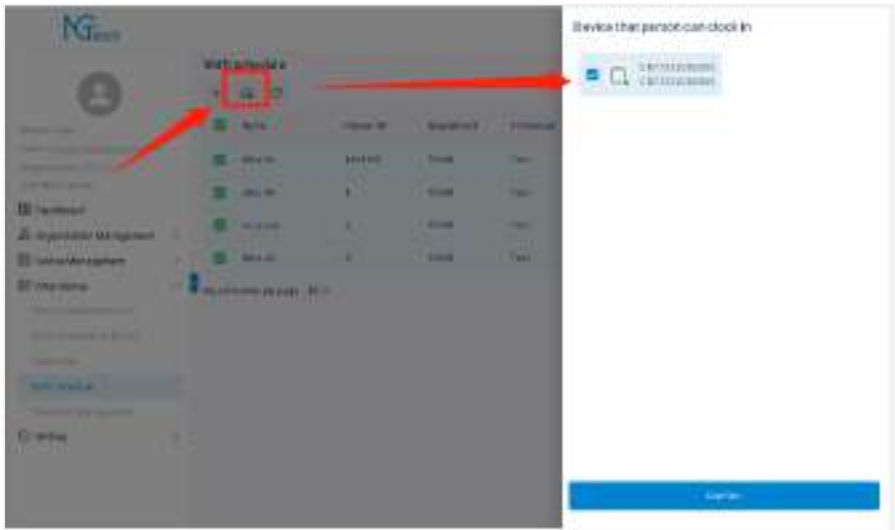






3. Select the person to be scheduled and click  to synchronize the personnel to the device.





The selected personnel will then be synchronized to the selected device, and those who are successfully synchronized will be able to check-in and check-out on the device by password/card/fingerprint/face, and so on.

## 12.9 Report Attendance

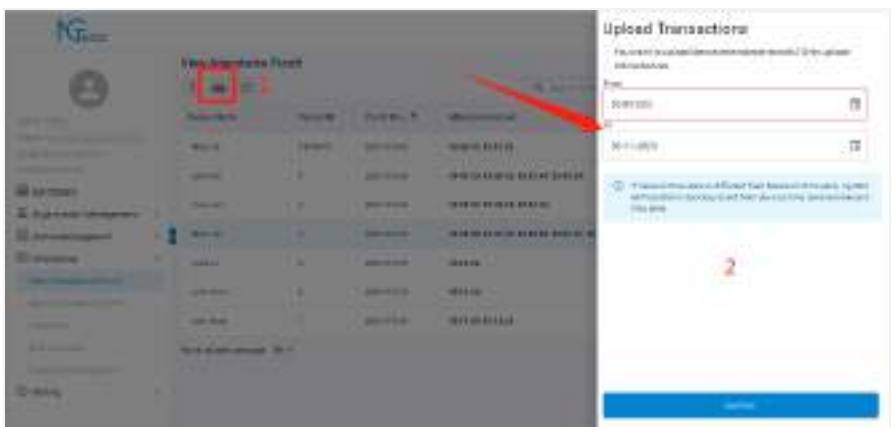
Attendance records of all employees will be displayed on this interface, including the attendance record of uploaded attendance transactions. The record of the normal punch on the device will be uploaded to the software as the original record.

### 12.9.1 View Attendance Reports

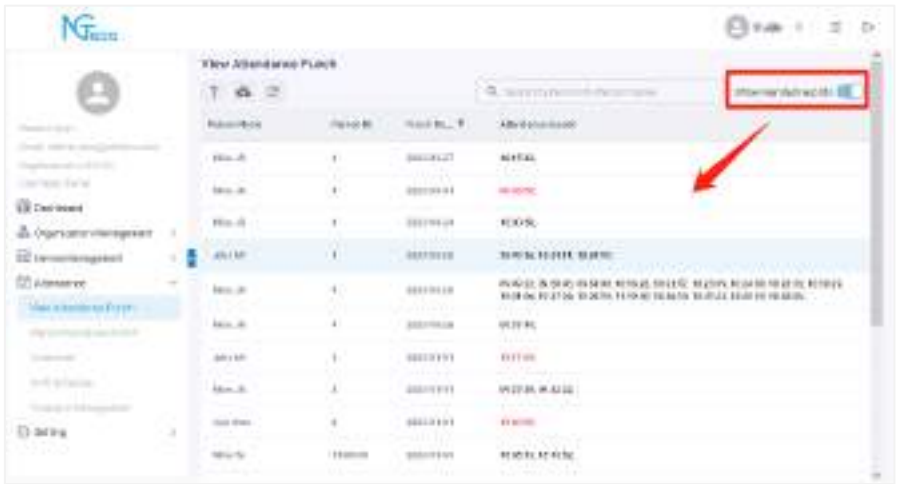
1. Click **[Attendance]** > **[View Attendance Punch]** on the NGTeco Office.



2. Click the  and set the time range to upload device attendance records.

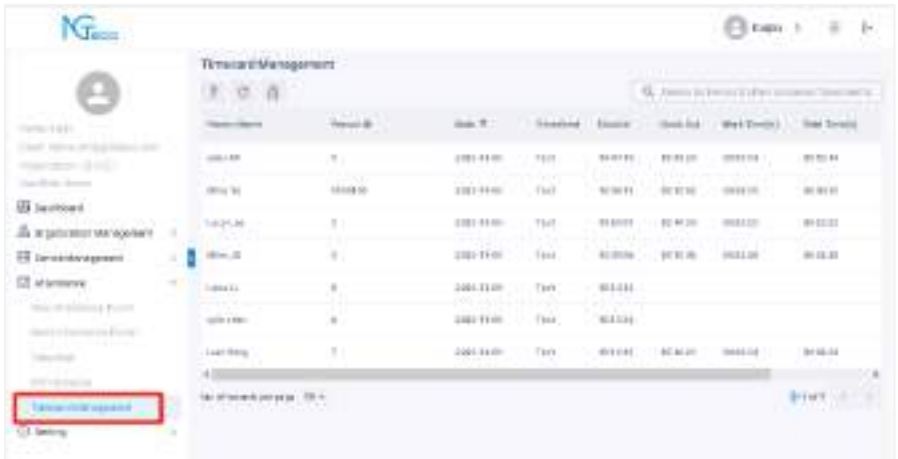






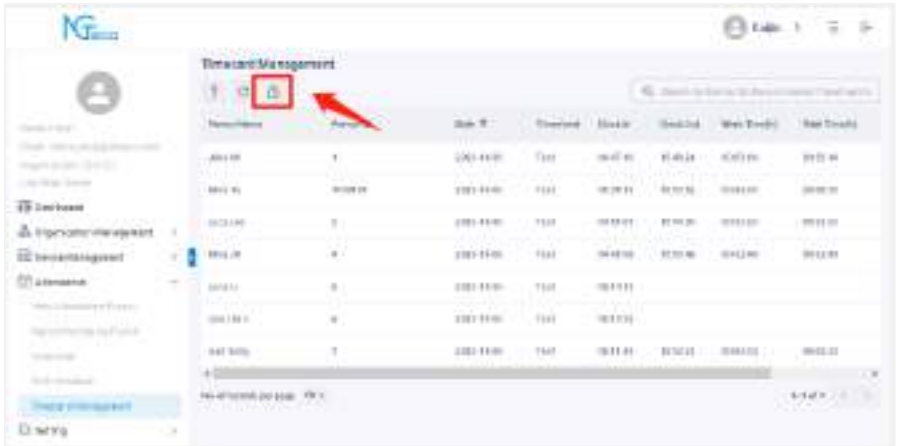
### 12.9.2 Exporting Reports

1. Click [Attendance] > [Timecard Management] on the NGTeco Office.





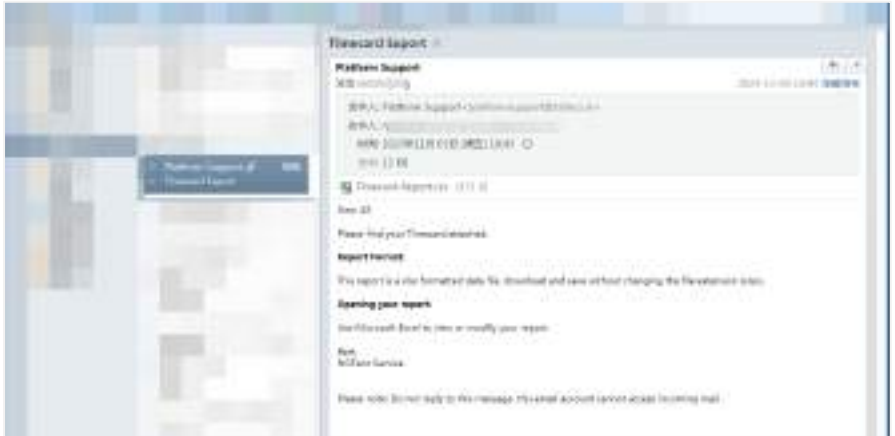
- Click the  to export the attendance report according to the person ID, person name or Timesheet name, unchecked to export all.



- Set the time and enter the email address to receive the report on the pop-up page.



- 4. Check your email and download the attachment to view the report of attendance.



The screenshot shows an Excel spreadsheet with the following columns: Person ID, First Name, Last Name, Date, Timezone, Clock In, Clock Out, Puch, Case No, Total Time(O), Start Date, and End Date. The data is organized into rows for different dates and individuals.

Person ID	First Name	Last Name	Date	Timezone	Clock In	Clock Out	Puch	Case No	Total Time(O)	Start Date	End Date
1190109	John	Ng	2020-11-2	Taipei	14:14:00	17:10:00	00:00:00		3:56	Start	Last
2	Liam	Ng	2020-11-2	Taipei	15:05:15	17:00:00	00:14:10		2:20	Start	Last
3	Liam	Ng	2020-11-3	Taipei	14:25:00	17:00:00	00:20:00		2:47	Start	Last
4	John	Ng	2020-11-7	Taipei	14:41:00	17:10:00	00:20:12		3:40	Start	Last
5	Liam	Ng	2020-11-8	Taipei	13:19:15	17:10:00	00:00:00		3:38	Start	Last
6	Liam	Ng	2020-11-9	Taipei	15:42:00	17:10:00	00:00:00		2:08	Start	Last
7	John	Ng	2020-11-9	Taipei	16:41:40	17:10:00	00:00:00		3:15	Start	Last
8	John	Ng	2020-11-20	Taipei						Start	Last
1190109	John	Ng	2020-11-20	Taipei						Start	Last
2	Liam	Ng	2020-11-20	Taipei						Start	Last
4	John	Ng	2020-11-20	Taipei						Start	Last
5	Liam	Ng	2020-11-20	Taipei						Start	Last

NGTeco

Website: [www.ngteco.com](http://www.ngteco.com)

Email: [ngtime@ngteco.com](mailto:ngtime@ngteco.com)

Phone: (770) 800-2321

Support: <https://www.ngteco.com/contact/>

