User Manual

NG-TC3

Date: May 2025

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.

About the Manual

This manual introduces the operations and usage of the **NG-TC3**.

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

Features and parameters with ★ are not available in all devices.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**.
>	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

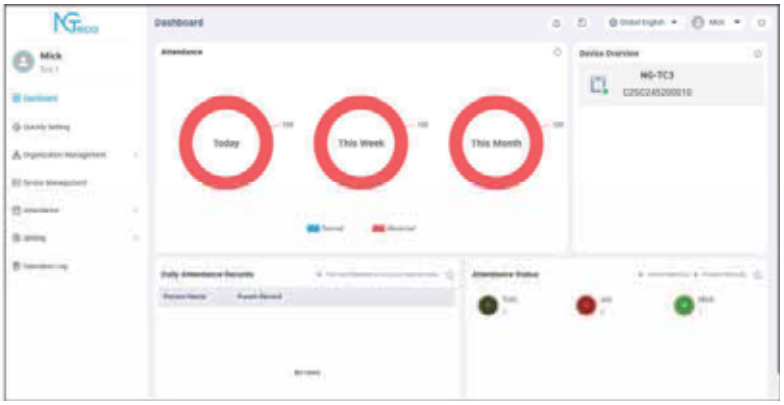
Convention	Description
	This represents a note that needs to pay more attention to.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves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

Table of Contents

1 Overview

1.1 Introduction

This document outlines the menu operation of **NG-TC3** 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.



1.2 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.

1.3 Dimension

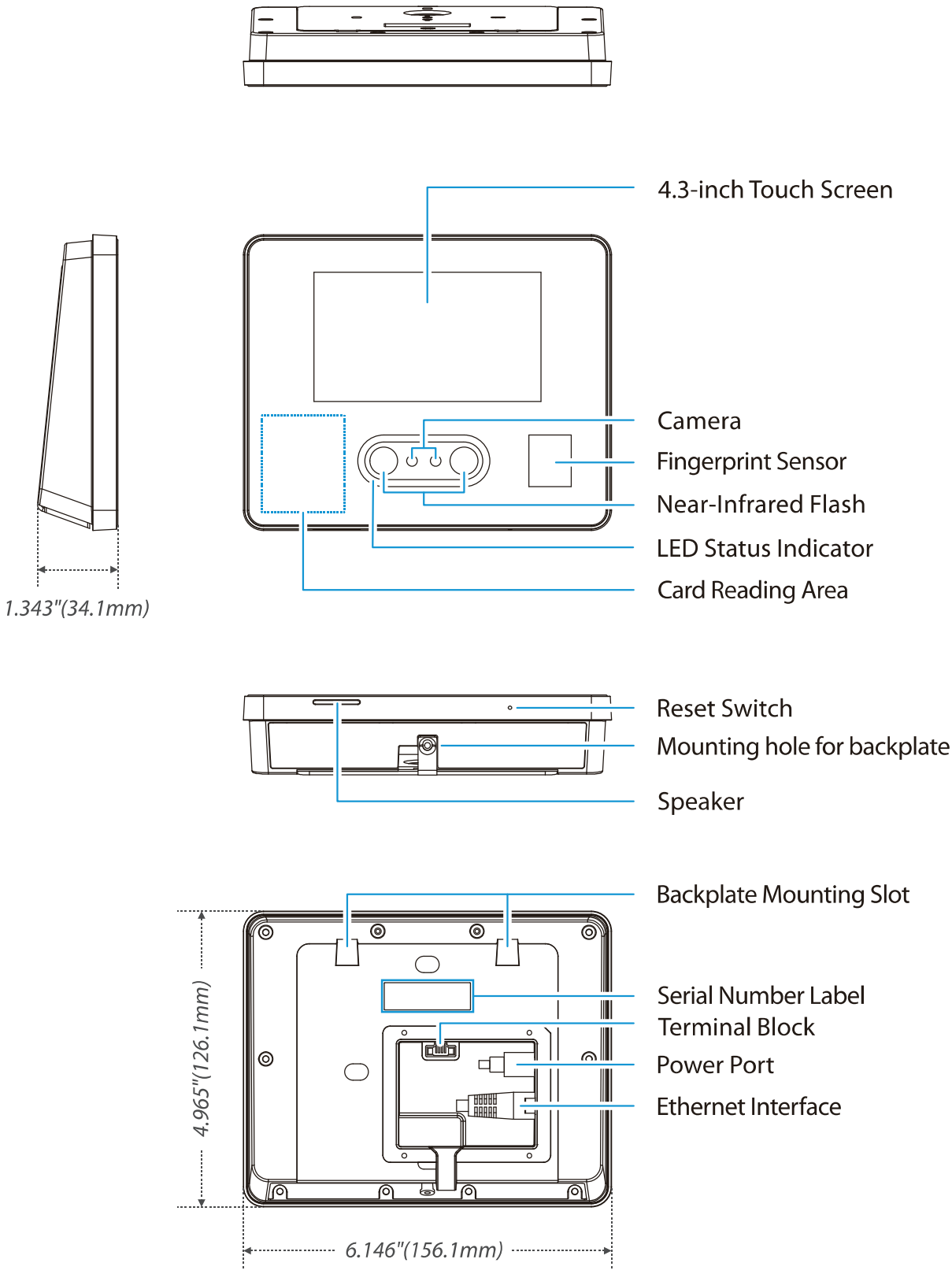


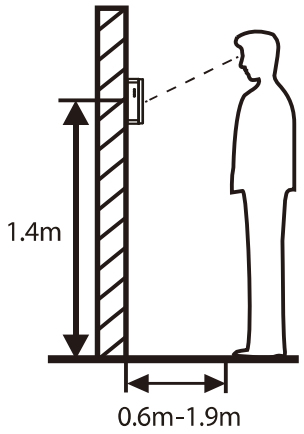
Figure 1-1 Product Appearance

2 Instruction for Use

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

2.1 Standing Position, Posture and Facial Expression

The recommended distance



The recommended distance between the device and a user whose height ranges from 1.55 m to 1.85 m, is between 0.6 m and 1.9 m. Users may slightly move forward or backward to improve the quality of facial images captured.

Recommended standing posture and facial expression:

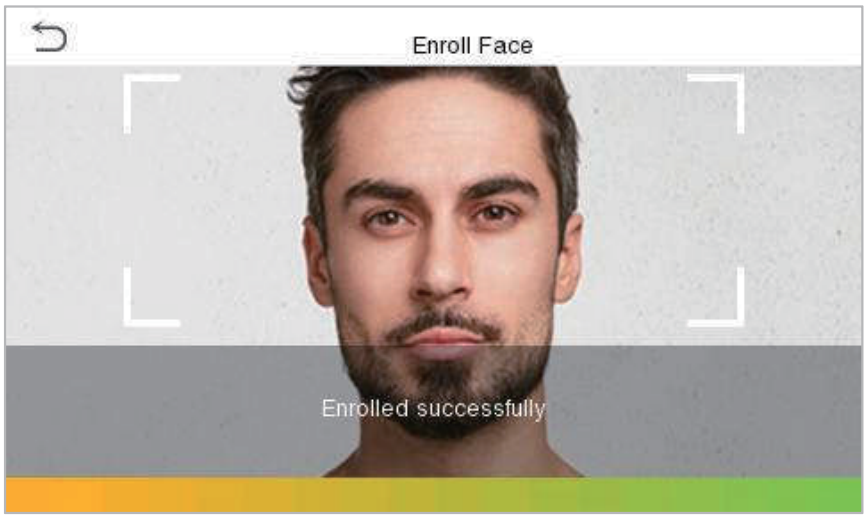
Standing Posture

Facial Expression

Note: *During enrollment and verification, please maintain natural facial expression and standing posture.*

2.2 Face Template Registration

Please ensure that the face template is centered on the screen during registration. Please face towards the camera and stay still during face template registration. The screen should look like the image below:



Correct face template registration and authentication method

➢ **Recommendation for Registering a Face Template**

- When registering a face template, maintain a distance of 40 cm to 80 cm between the device and the face template.
- Be careful not to change your facial expression. (e.g., Smiling face template, drawn face template, wink, etc.)
- If the user do not follow the instructions on the screen, the face template registration may take longer or may fail.
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses, or eyeglasses.
- Be careful not to display two face templates on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both face templates with and without glasses.

➢ Recommendation for Authenticating a Face Template

- Ensure that the face template appears inside the guideline displayed on the screen of the device.
- If the glasses have been changed, authentication may fail. If the registered face template does not include glasses, authenticate using the template without glasses.. If the face template with glasses has been registered, authenticate the face template with the previously worn glasses.
- If a part of the face template is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face template, allow the device to recognize both the eyebrows and the face template.

2.3 Standby Interface

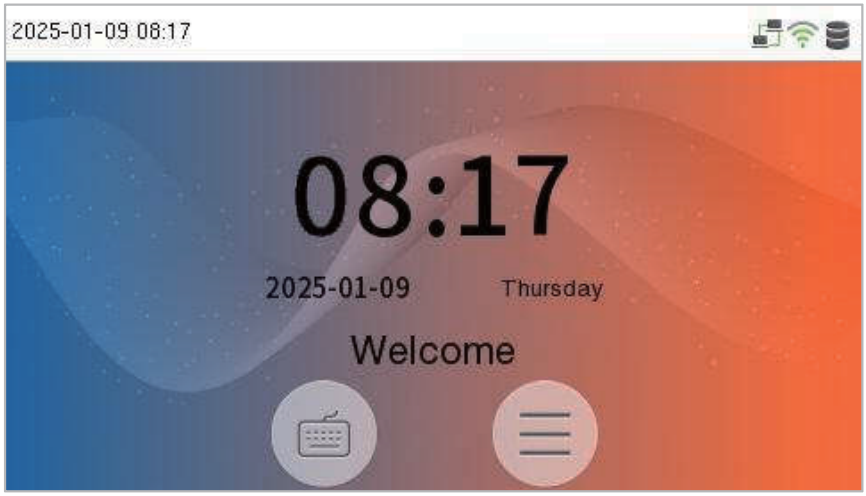
1. Power on the device. If it is used for the first time and no network has been configured for the device, it will enter the device QR code interface as shown in the figure below. Users can bind the device by scanning the QR code with the NGTeco APP or by entering the SN code on the Web.

Note:

1) *This device needs to be used in combination with NGTeco Office software and NGTeco App. After binding the device, you can unify the management of the device, set up organization, attendance rules, managing user information, managing user privileges, set up verification modes, generate timecard reports and attendance logs, etc.*

2) *For details on how to bind the device, see* ***14 Binding the Device****.*

2. After successfully binding the device, the standby screen will be displayed as shown below.



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

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

Status of Icons

Icon Status	Name	Description
	**Ethernet**	Indicates that the Ethernet connection has been established.
		Indicates that the Ethernet connection is disconnected.
	**ADMS Server**	The connection between device and the ADMS server is successful.
		Indicates that the server is weak or has failure.
		The communication data of ADMS are transmitting.
	**Wi-Fi signal**	Indicates that the Wi-Fi connection is normal.
		Indicates that the Wi-Fi connection failure.

2.4 Verification Modes

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

- Password verification
- Fingerprint verification
- Facial verification
- Card verification

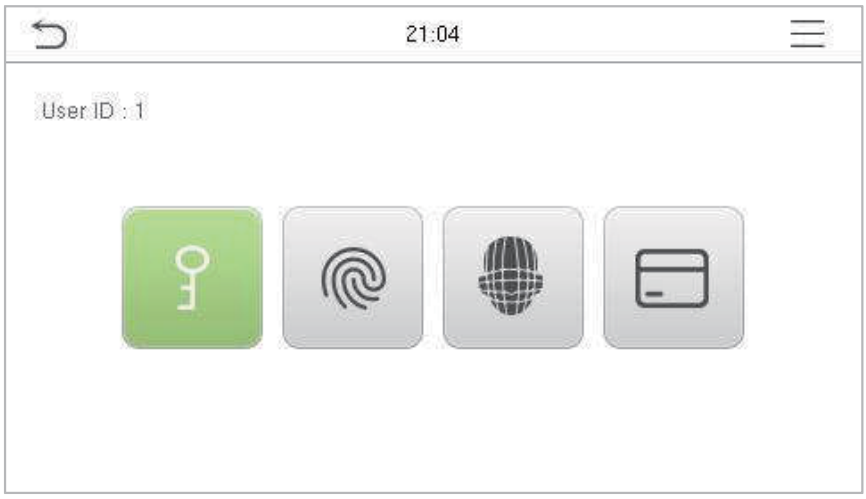
These verification modes can be used for check-in and check-out punches and access to the admin menu.

2.4.1 Password Verification

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

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

If the user has registered a face template, fingerprint, and card in addition to password, and the verification method is set to Password/Fingerprint/Card/Face verification, the following screen will appear. Select the icon to enter password verification mode.



Input the password and press **OK**.

The following screen displays, after inputting a correct password and a wrong password, respectively.

Successfully verified:

Failed to verify:

2.4.2 Fingerprint Verification

Finger Enrolment

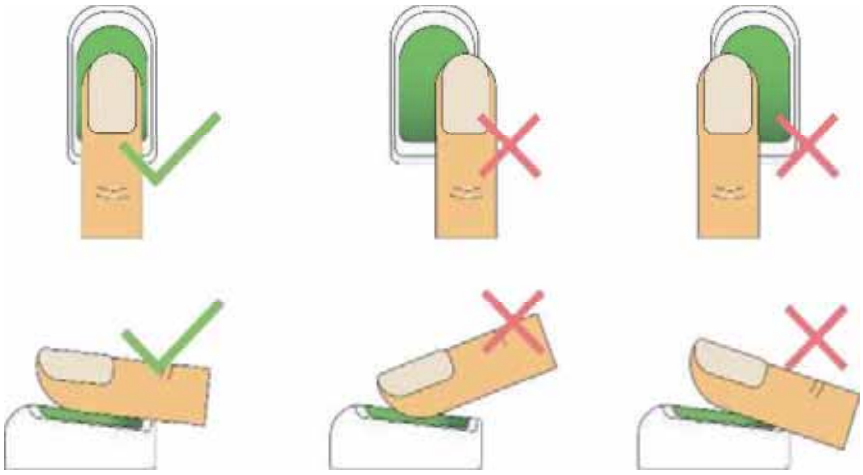
Finger Enrolment procedure involves capturing a user's fingerprint and saving it as a template to the corresponding User ID. To enhance the fingerprint authentication rate, make sure that you enrol the finger correctly.

Finger Selection for Enrolment

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

Enrolment Operation

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



This method compares the fingerprint of the user that is being pressed onto the fingerprint reader with all the fingerprint data that is pre-stored in the device.

To enter fingerprint identification mode, simply tap your finger on the fingerprint reader.

- **1: N Fingerprint Verification**

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 on the sensor.

The following is the pop-up prompt box displaying the result of the comparison.

Successfully verified:

Failed to verify:

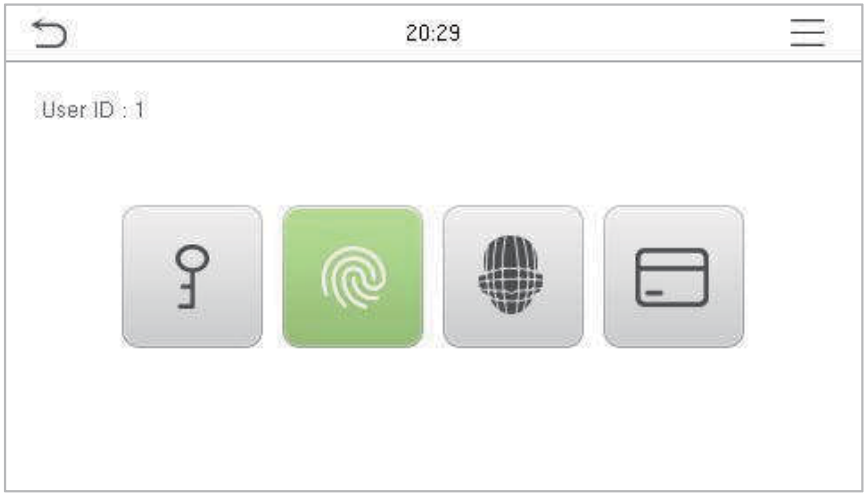
If the device instructs "**Failed to verify.**" then press your finger again. You can attempt verification **two** more times. If the verification fails after these attempts, then the device will return to the standby interface.

- **1:1 Fingerprint Verification**

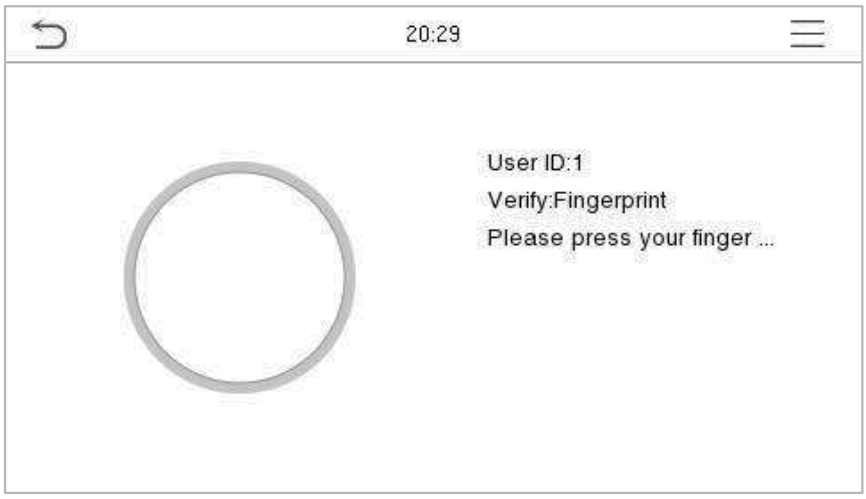
The device compares the current fingerprint with the fingerprints linked to the entered User ID through the virtual keyboard.
In case users are unable to gain access using the 1: N authentication method, they can attempt to verify their identity using the 1:1 verification mode.

Click the button on the main screen to enter 1:1 fingerprint verification mode. Input the user ID and press **OK**.

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



Press the fingerprint to verify.



Successfully verified:

Failed to verify:

2.4.3 Facial Verification

- **1:N Facial Verification**

The device compares the currently acquired facial images with all the registered face template data stored in its database. The following is the pop-up prompt box displaying the result of the comparison.

Successfully verified:

- **1:1 Facial Verification**

In this verification mode, the device compares the face template captured by the camera with the facial template related to the entered user ID. Click the button on the main screen and enter the 1:1 facial verification mode and enter the user ID and click **OK**.

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

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

2.4.4 Card Verification

- **1:N Card Verification**

The 1: N card verification mode compares the card number in the card induction area with all the card number data registered in the device; The following screen displays on the card verification:

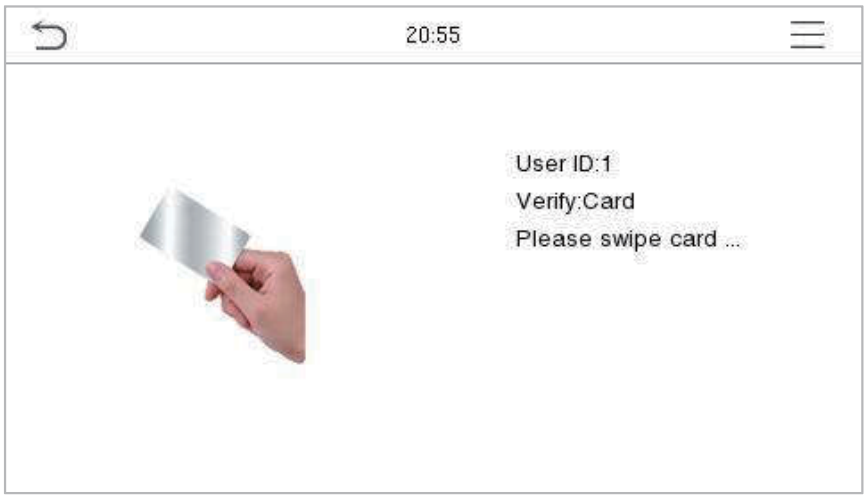
- **1:1 Card Verification**

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

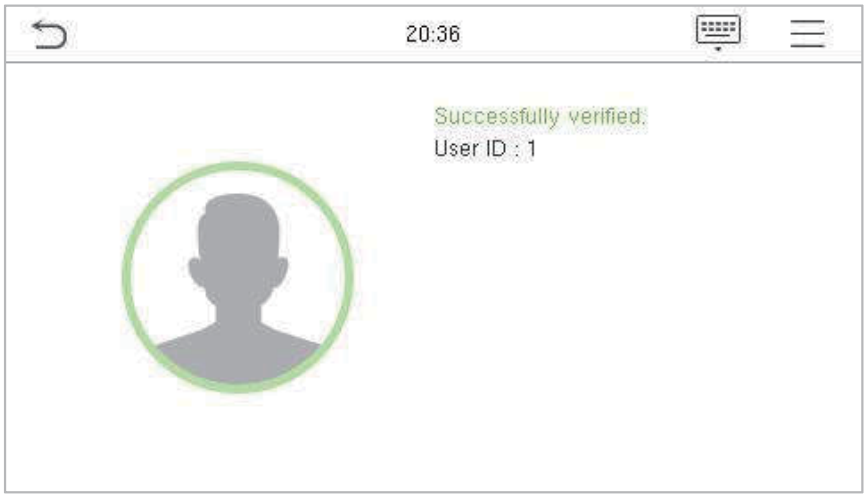
Click the button on the main screen to open the 1:1 card verification mode. Enter the user ID and click **OK**.

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

Place the card in the collection area for verification.



Successfully verified:

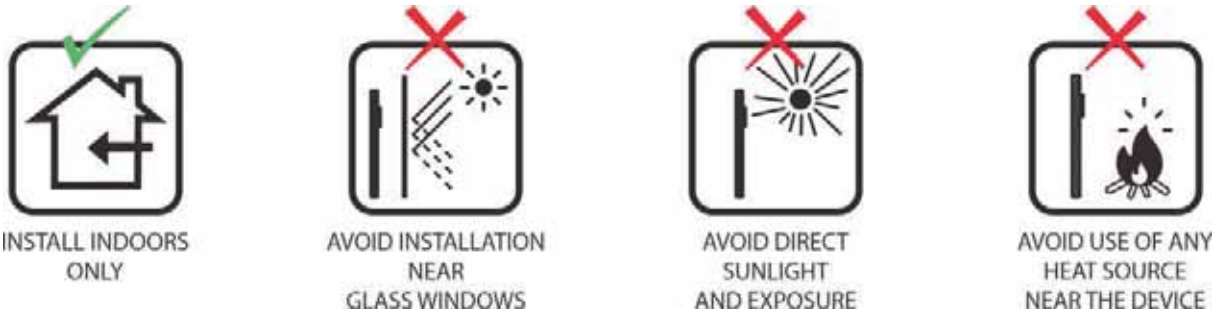


Failed to verify:

3 Installation

3.1 Installation Environment

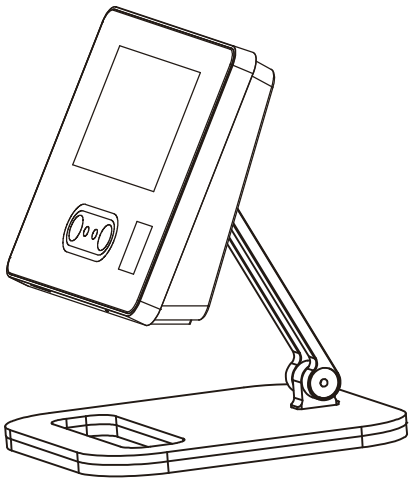
Please refer to the following recommendations for installation.



3.2 Installation Methods

The NG-TC3 is available in both desktop and wall mounting.

Desktop Mounting (Factory Default):



Wall Mount:

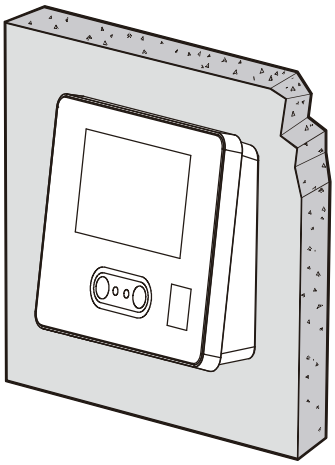


Figure 3-1 Installation view of the NG-TC3

3.3 How to Install the Device on the Desktop?

1. Secure the backplate to the desktop bracket with two screws and place horizontally.
2. Hook and fasten the device to the backplate from top to bottom.
3. Secure the device with screws from the bottom.
4. Remove the tool from the bottom of the desktop stand and adjust the stand to a suitable angle.

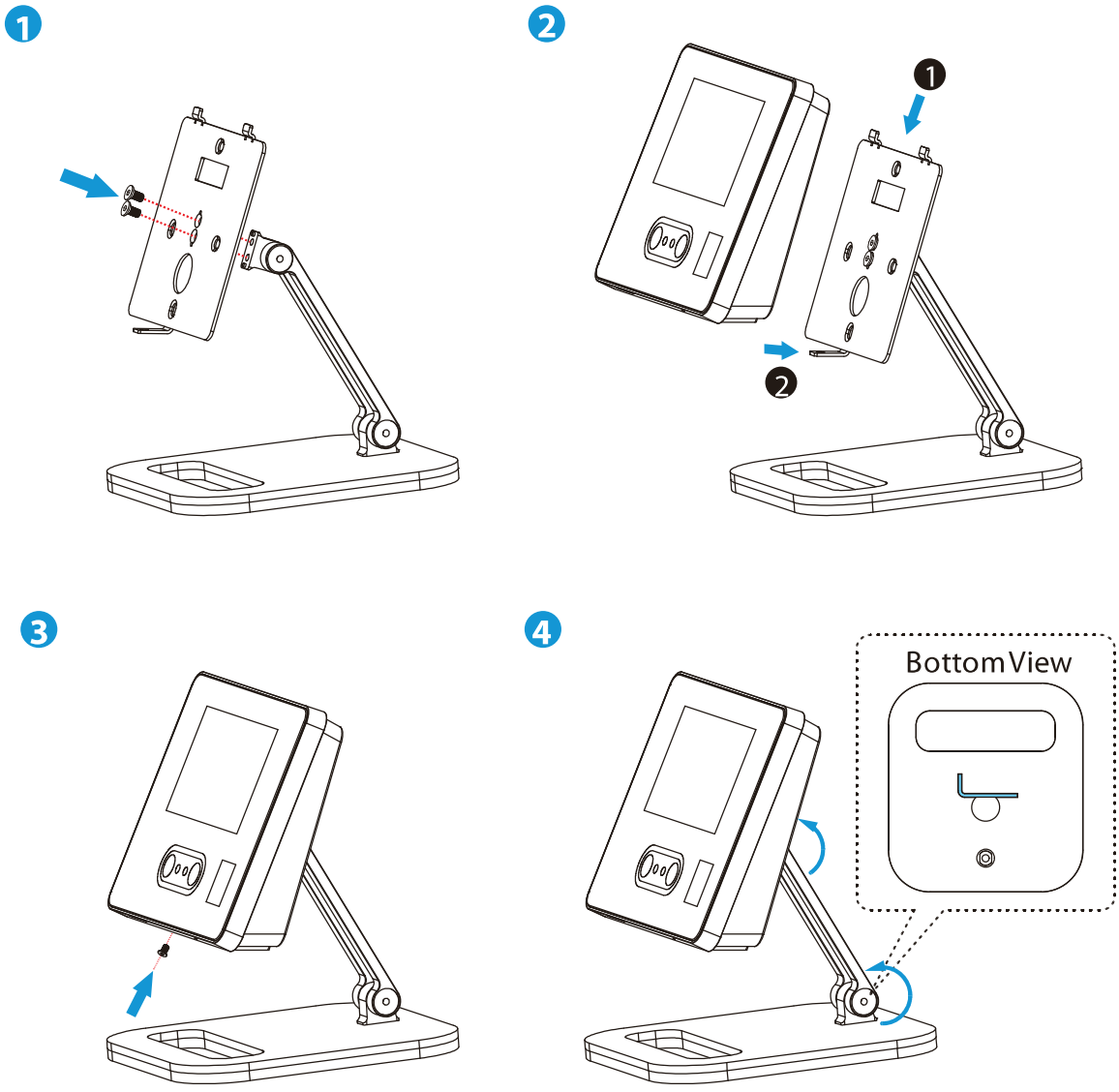


Figure 3-2 Mounting the NG-TC3 on the desktop.

Note: *The desktop stand is not included as a standard accessory; users need to purchase it separately.*

3.4 How to Install the Device on the Wall?

1. Attach the mounting template sticker to the wall, and drill holes according to the mounting paper.

   Note: It is recommended that the fingerprint sensor be **55** inches (**1.4m**) from the floor.
2. Attach the backplate to the wall using the wall mounting screws.
3. Connect the cable to the device, secure the back cover, and then hang the device onto the backplate from top to bottom.
4. Fasten the device to the backplate with security screws from the bottom.

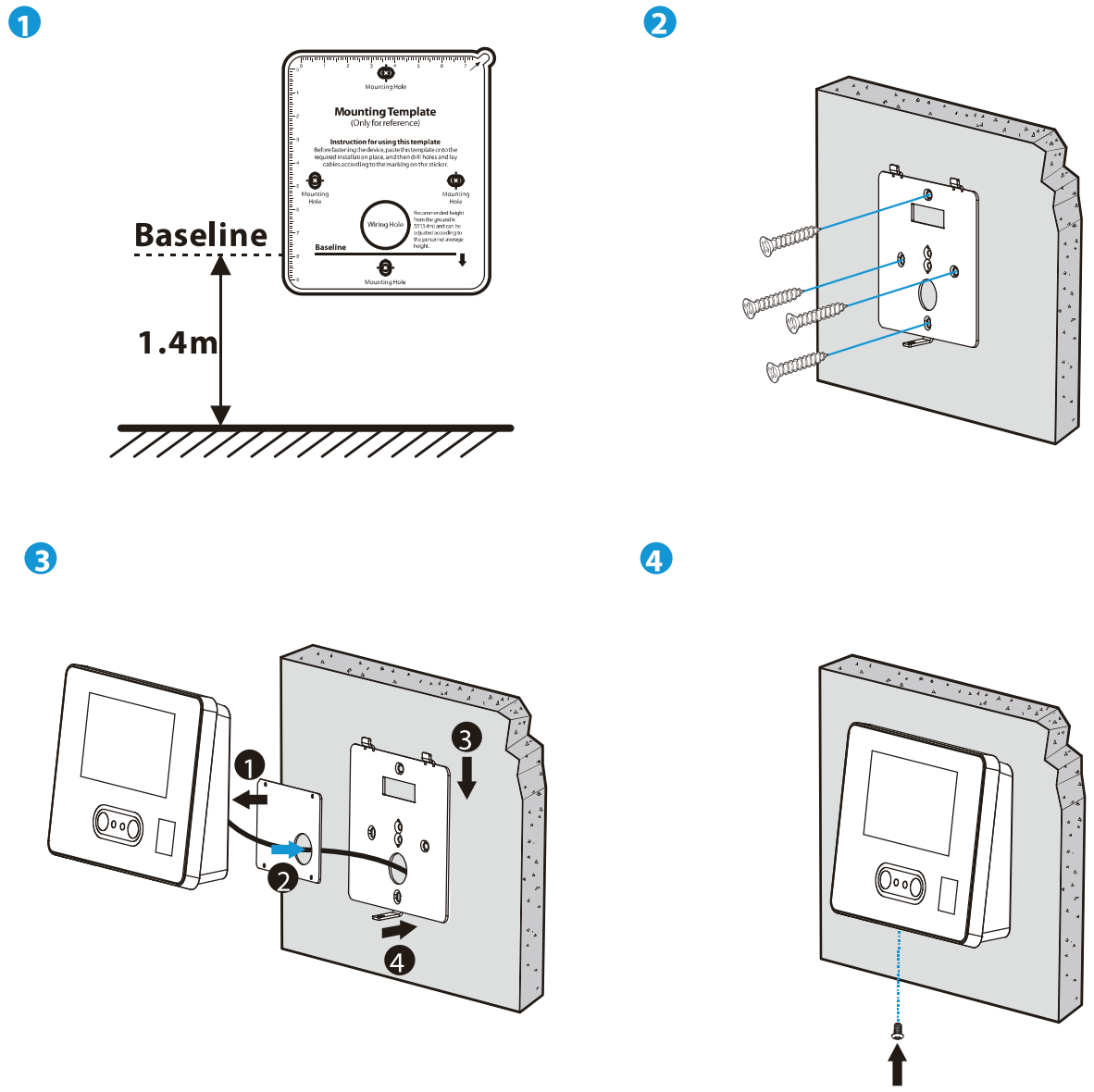
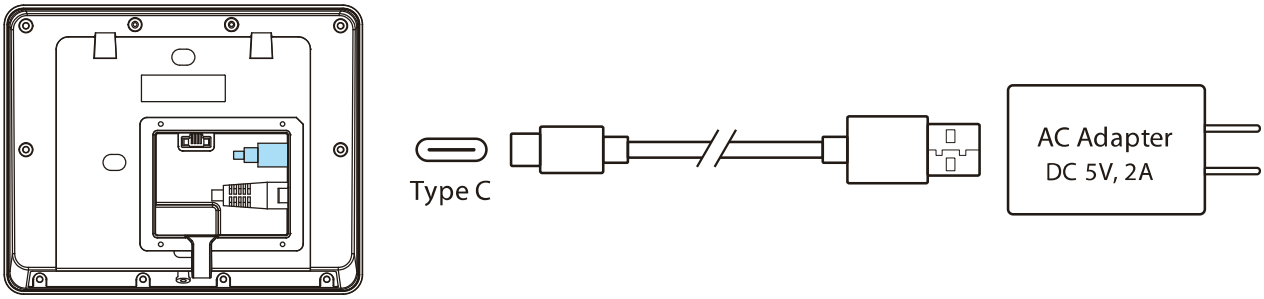


Figure 3-3 Mounting the device on the wall.

4 Wiring Description

4.1 Power Connection

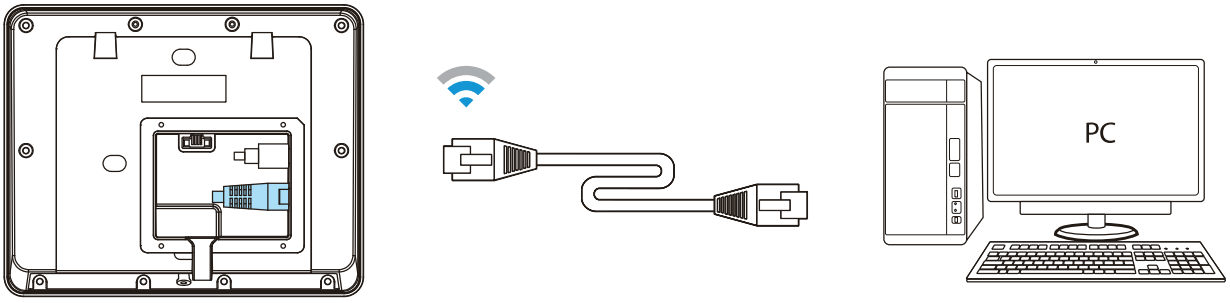


Recommended power supply:

- Recommended AC adapter: **5V**, **at least 2A**.
- To share the power with other devices, use an AC Adapter with higher current ratings.

4.2 Ethernet Connection

There are two ways to connect the NG-TC3 to the network: Wi-Fi and Ethernet.



Default IP address: 192.168.**1**.201
Subnet mask: 255.255.255.0

IP address: 192.168.**1**.130
Subnet mask: 255.255.255.0

Note: *In LAN, IP addresses of the server (PC) and the device must be in the same network segment when connecting to the software.*

5 Main Menu

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

Function Description

Menu	Descriptions
User Mgt.	To view basic information about users that have been added to the device.
COMM.	To set the relevant parameters of the network, wireless network, and network diagnosis.
System	To set the parameters related to the system, including date time, attendance, face template & fingerprint parameters, security setting, update firmware online, and reset to factory.
Personalize	This includes the user interface, voice, and bell schedule settings.
Attendance Search	To query the specified event logs and check attendance records.
Autotest	To automatically test whether each module functions properly, including the LCD screen, audio, microphone, camera, fingerprint sensor, and real-time clock.
System Info	To view data capacity, device and firmware information, and the privacy policy of the device.

Note: *When users use the product for the first time, they should operate it after setting administrator privileges. On the NGTeco Office app or web, the user can add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.*

6 User Management

6.1 Search for Users

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

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

6.2 Edit User

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

Note:

1) To modify user information, you need to operate on NGTeco Office App or Web.

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

6.3 Display Style

On the **Main Menu**, tap **User Mgt.**, and then tap **Display Style** to choose the style of the All-Users interface's list.

Different display styles are shown as below:

Multiple Line:

Mixed Line:

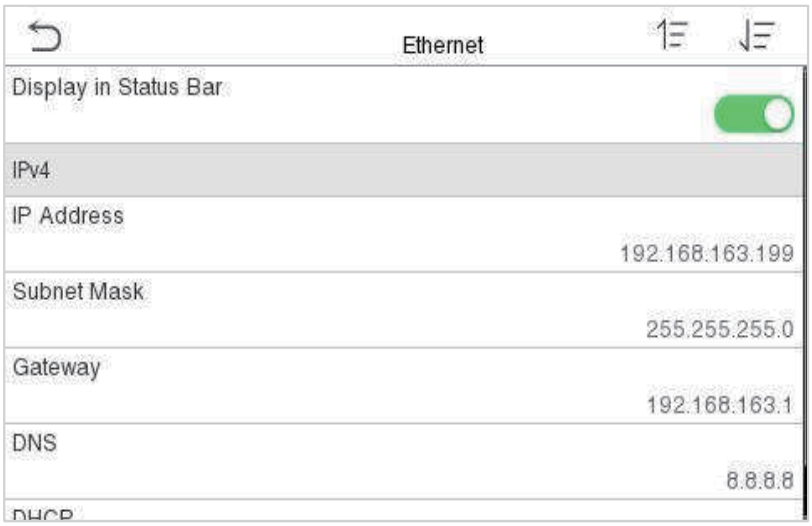
7 Communication Settings

Tap **COMM.** on the **Main Menu** to set the relevant parameters of the Network, Wireless Network, and Network Diagnosis.

7.1 Network Settings

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

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



Function Description

Function Name	Descriptions
Display in Status Bar	Toggle to set whether to display the network icon on the status bar.
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 is to dynamically allocate IP addresses for clients via server.

7.2 Wireless Network

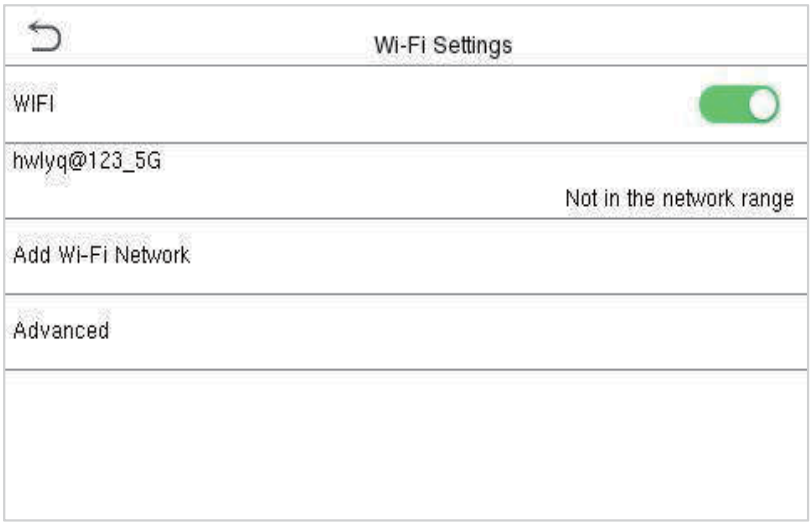
The device has a built-in Wi-Fi module.

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

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

- **Search the Wi-Fi Network**

1) Wi-Fi is enabled in the Device by default. Toggle on button to enable or disable Wi-Fi.
2) Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
3) Choose the appropriate Wi-Fi name from the available list, and input the correct password in the password interface, and then tap **Connect to Wi-Fi (OK)**.
4) When the Wi-Fi is connected successfully, the initial interface will display the Wi-Fi logo.



- **Add Wi-Fi Network Manually**

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

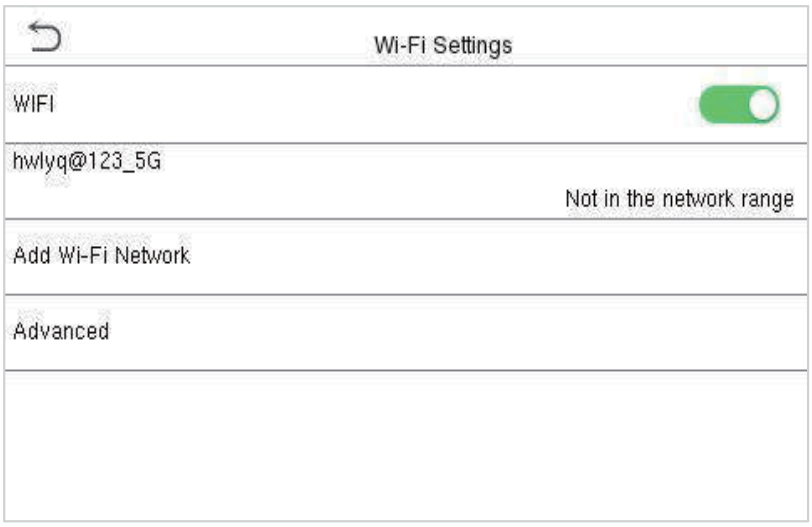
1) Tap on **Add Wi-Fi Network** to add the Wi-Fi manually.

2) On this interface template, 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. Click here to view the process to search the Wi-Fi network.*

- **Advanced Setting**

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



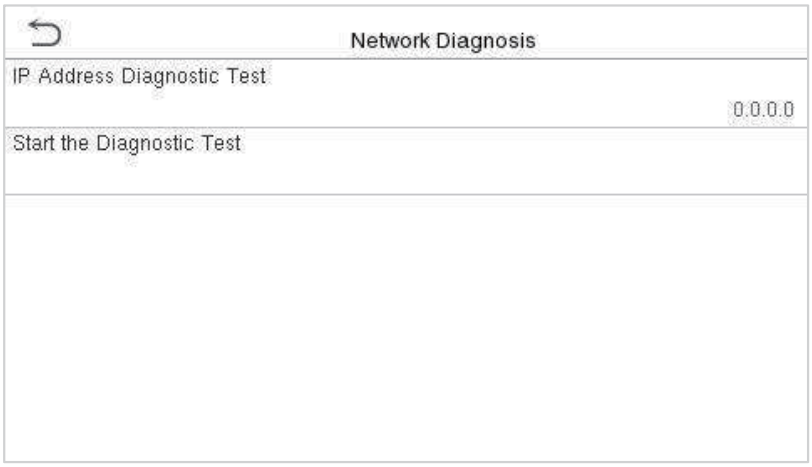
Function Description

Function Name	Descriptions
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	IP address for the WIFI network, the default is 0.0.0.0. It can be modified according to the network availability.
Subnet Mask	The default Subnet Mask of the WIFI network is 255.255.255.0. It can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. 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.

7.3 Network Diagnosis

To set the network diagnosis parameters.

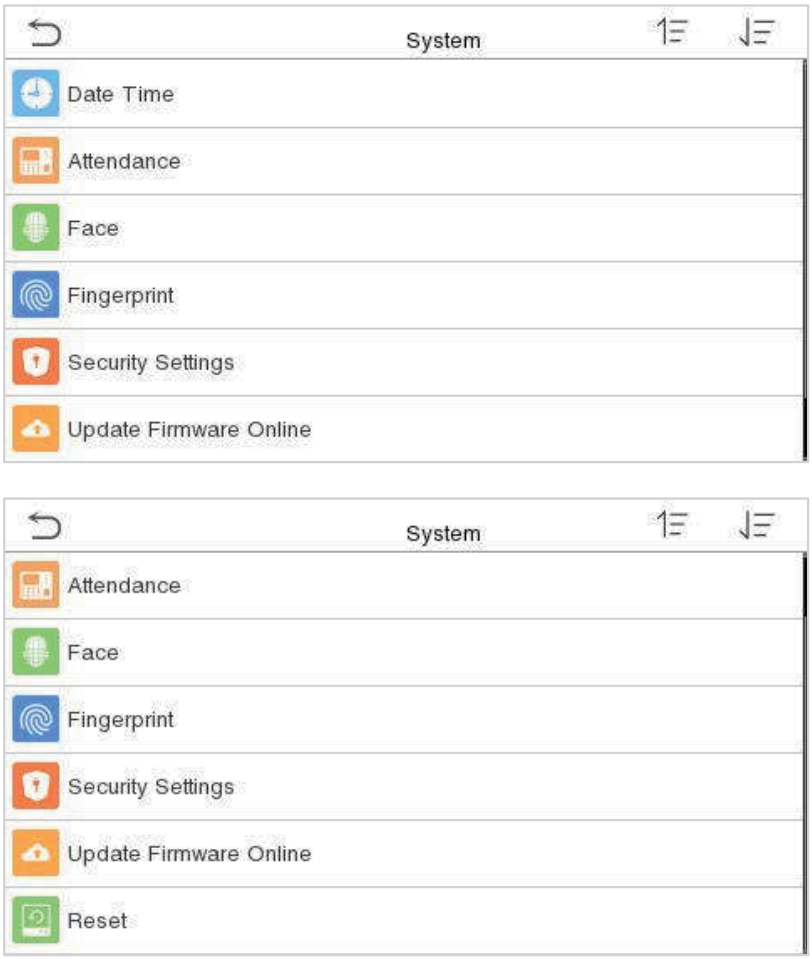
Tap **Network Diagnosis** on the **Comm.** settings interface to set the IP address diagnostic and start the diagnostic parameters.



8 System Settings

System Settings sets the related system parameters to optimize the performance of the device.

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



8.1 Date and Time

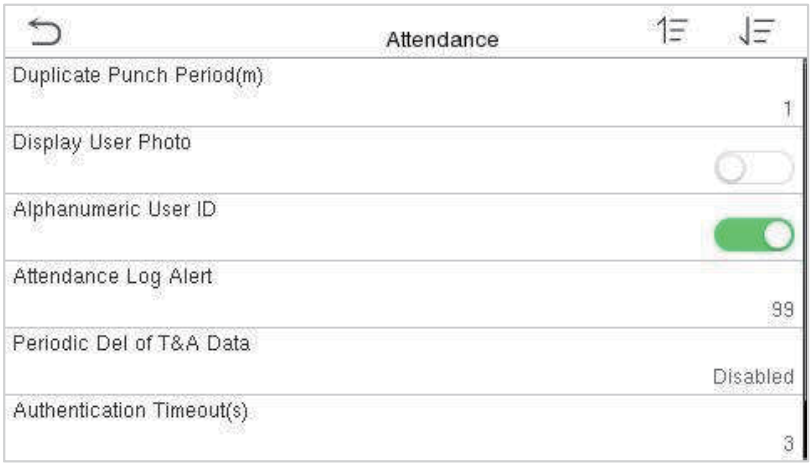
Tap **Date Time** on the **System** interface to set the date and time.

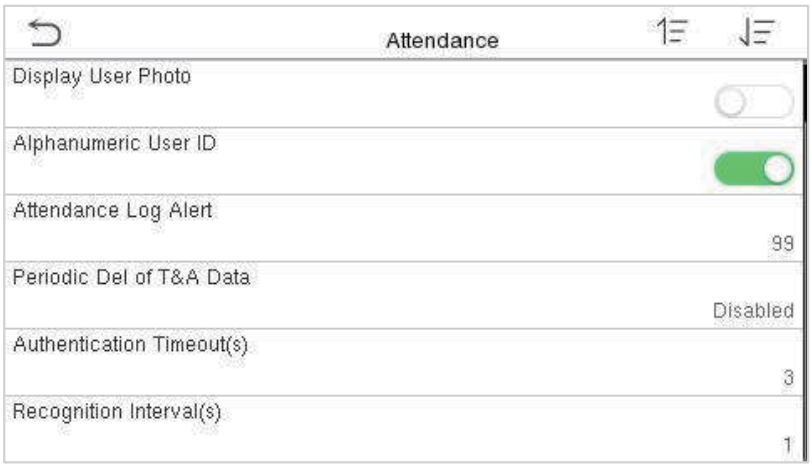
- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping **24-Hour Time**. If enabled, then select the **Date Format** to set the date.
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.
- Tap **Daylight Saving Time** to enable or disable the function. If enabled, tap Daylight Saving Mode to select a daylight-saving mode and then tap Daylight Saving Setup to set up the switch time.

- 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.

8.2 Attendance

Tap **Attendance** on the **System** interface.





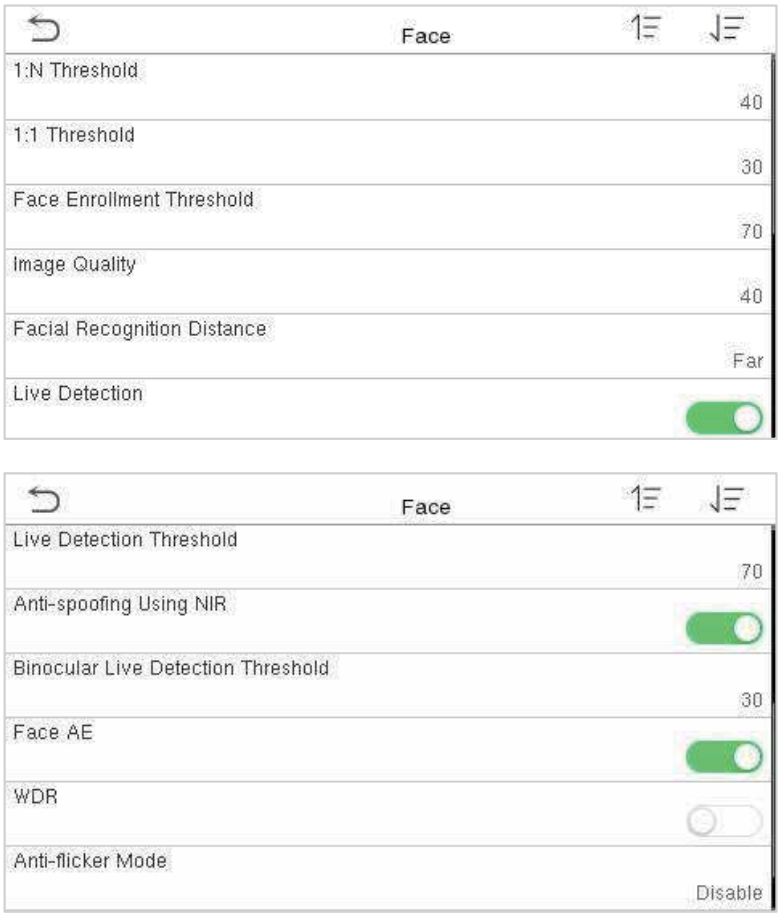
Function Description

Function Name	Descriptions
Duplicate Punch Period (m)	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.
Display User Photo	Whether to display the user photo when the user passes the verification.
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 older 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.
Recognition Interval (s)	To set the facial template matching time interval as required. Valid value: 0~9 seconds.

8.3 Face Template Parameters

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



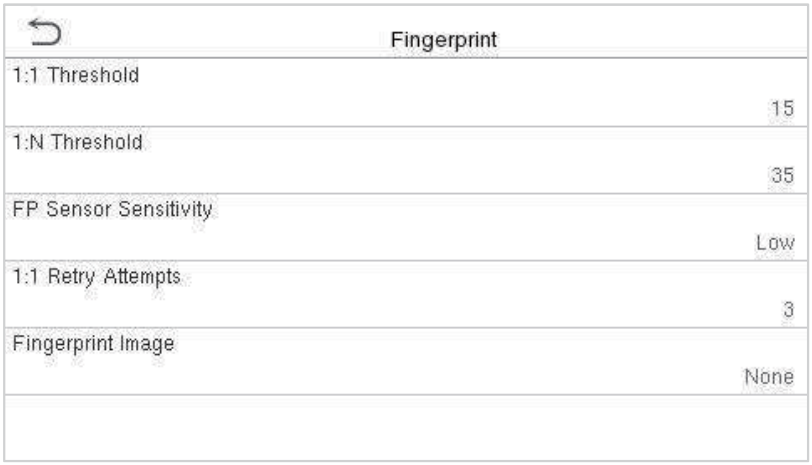
Function Description

Function Name	Descriptions
1: N Threshold	Under 1: N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 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 75.
1:1 Threshold	Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value. The valid value ranges from 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 63.
Face Enrollment Threshold	During face template 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 template has already been registered.
Image Quality	Image quality for facial registration and comparison. The higher the value, the clearer the image requires.
Facial Recognition Distance	Face template recognition of the maximum distance, greater than this value will be filtered. The parameter value can be understood as the face template size required for registration and comparison. The farther the distance from people, the smaller the face template pixels obtained by the algorithm. When the value is 0, it means that the face template comparison distance is not limited.
Live Detection	It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.
Live Detection Threshold	It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.

Anti-counterfeiting with NIR	Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.
Binocular Live Detection Threshold	It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.
Face AE	When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while the other areas become darker.
WDR	Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and improves object identification under bright and dark environments.
Anti-flicker Mode	It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light.
Face Algorithm	It has facial algorithm related information and pause facial template update.

8.4 Fingerprint Parameters

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



Function Description

Function Name	Descriptions
1:1 Threshold	Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value.
1:N Threshold	Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value.
FP Sensor Sensitivity	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
1:1 Retry Attempts	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	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: **Show for Enroll:** To displays the fingerprint image on the screen only during enrollment. **Show for Match:** To displays the fingerprint image on the screen only during verification. **Always Show:** To displays the fingerprint image on screen during enrollment and verification. **None:** Not to display the fingerprint image.

8.5 Security Settings

Tap **Security Settings** on the **System** interface.

Function Description

Function Name	Descriptions
Standalone Communication	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.
SSH	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.
User ID Masking	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.
Display Verification Name	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.
Display Verification Mode	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.

Save Photo as Template	After disabling this function, face template re-registration is required after an algorithm upgrade.

8.6 Update Firmware Online

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

Click **Enable firmware update online** function, the device will prompt that the update may bring some data security risks, which requires manual confirmation by the user (If the security setting function is turned off, the risk warning will not be displayed when the online update is turned on).

Click **Check for Updates** it may have the following 3 scenarios:

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

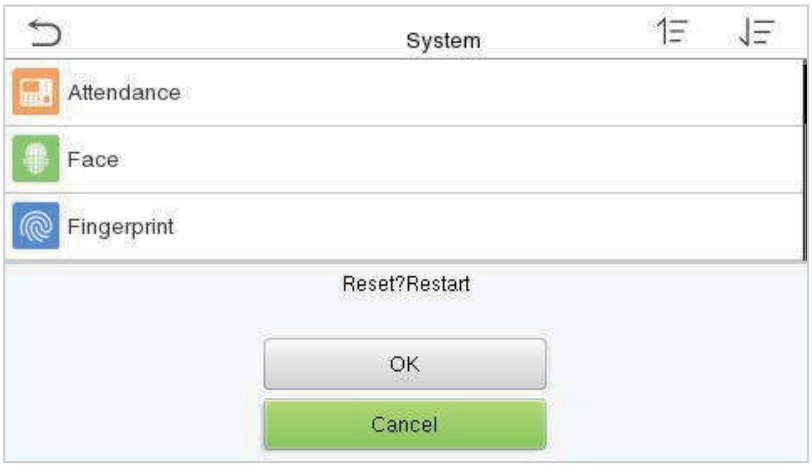
2) If the firmware version of the device is the latest, it will prompt that the current firmware version is already the latest.

3) 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.

8.7 Factory Reset

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

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

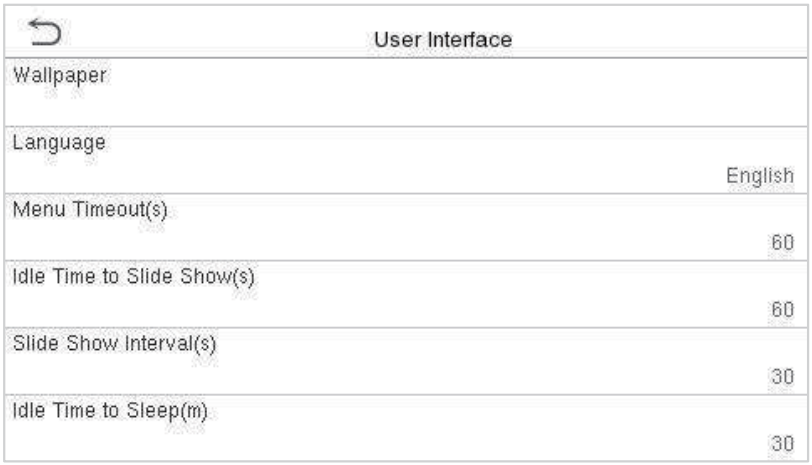


9 Personalize Settings

Tap **Personalize** on the **Main Menu** interface to customize user interface, voice and bell schedules.

9.1 User Interface Settings

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



Function Description

Function Name	Descriptions
Wallpaper	The main screen wallpaper can be selected according to the user preference.
Language	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. The function either can 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 will be played. The function can be disabled, or you may set the value between 3 and 999 seconds.
Slide Show Interval (s)	It is the time interval in switching between different slide show photos. 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. Tap the screen anywhere to resume normal working mode. This function can be disabled or set a value within 1-999 minutes.

9.2 Voice Settings

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

Function Description

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

9.3 Bell Schedules

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

- **New bell schedule**

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

Function Description

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

- **All bell schedules:**

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

- **Edit the scheduled bell:**

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

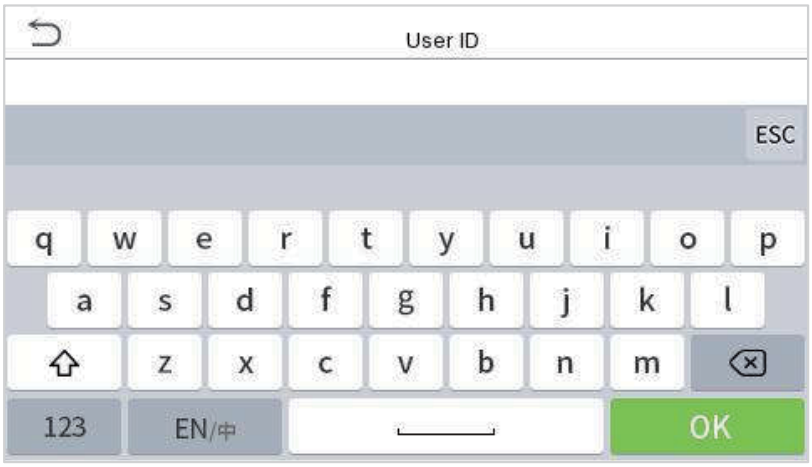
- **Delete a bell:**

On the **All-Bell Schedules** interface, tap the desired bell schedule, and tap **Delete**, and then confirm by tapping **Yes** to delete the selected bell.

10 Attendance Search

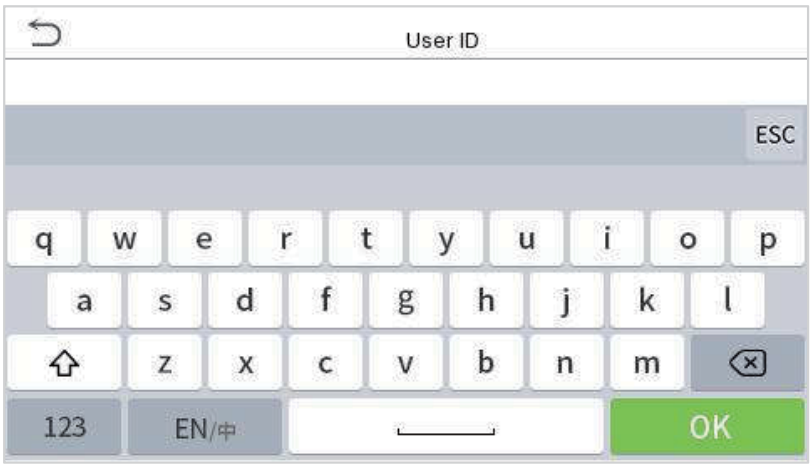
Once the identity of a user is verified, the Event Logs will be saved in the device. This function enables users to check their attendance records.

Tap **Attendance Search** on the **Main Menu** interface to search for the required Attendance log.



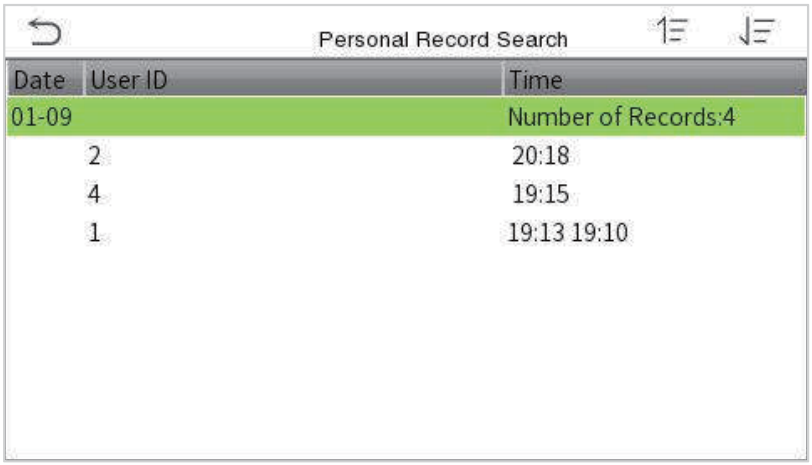
The following is an example of searching for attendance logs.

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

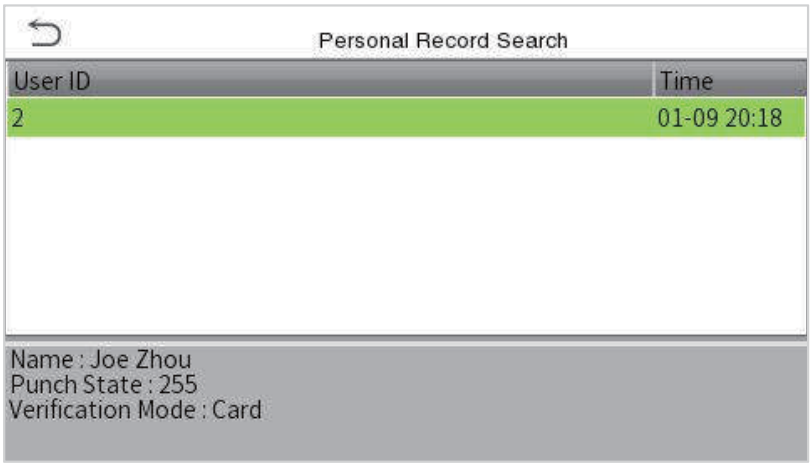


2. Select the time range in which the records need to be searched.

3. Once the record search is complete, the relevant records searched for will be displayed in a list, click on the record to view its details.

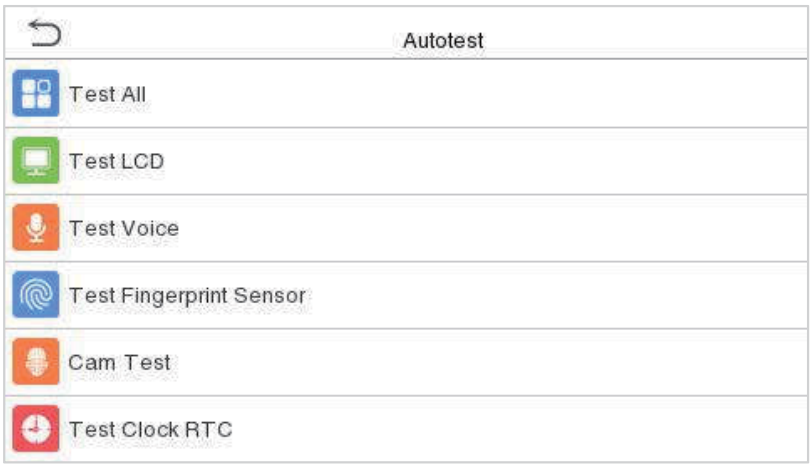


4. The below figure shows the details of the selected record.



11 Autotest

On the **Main Menu**, tap **Autotest** to automatically assess whether each module functions properly, including the LCD screen, audio, microphone, camera, fingerprint sensor and real-time clock (RTC).

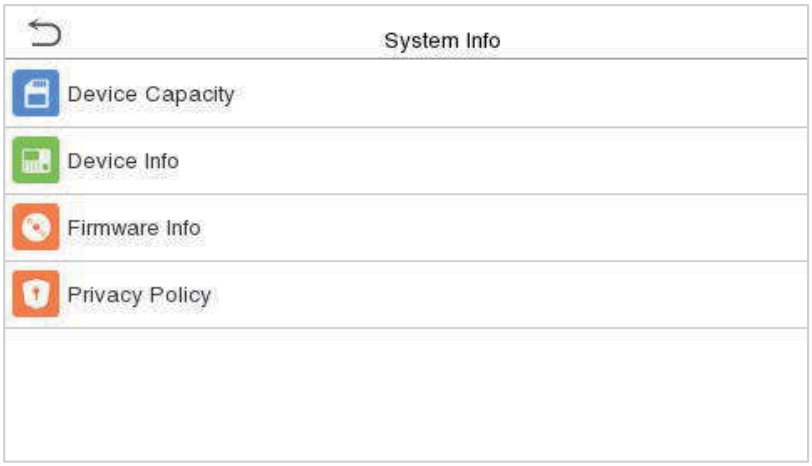


Function Description

Function Name	Descriptions
Test All	To automatically test whether the LCD, Audio, Camera and RTC are normal.
Test LCD	To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays colors normally.
Test Voice	To automatically test whether the audio files stored in the device are complete and the voice quality is good.
Test Fingerprint Sensor	To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.
Cam Test	To test if the camera functions properly by checking the photos taken to see if they are clear enough. Same as "**Test Face**".
Test Clock RTC	To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Tap the screen to start counting and press it again to stop counting.

12 System Information

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



Function Description

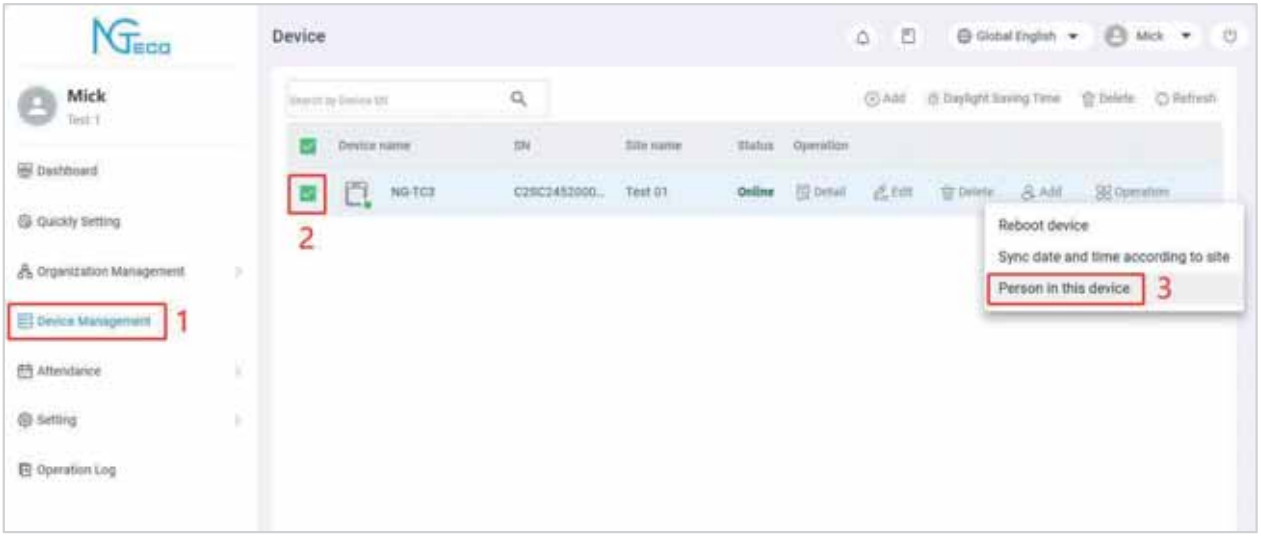
Function Name	Descriptions
Device Capacity	Displays the current device's user storage, admin user, password, fingerprint, face template and card storage, T&A records and profile photos.
Device Info	Displays the device's name, serial number, MAC address, fingerprint algorithm, face template algorithm, platform information and manufacture date.
Firmware Info	Displays the firmware version and other version information of the device.
Privacy Policy	The privacy policy control will appear when the gadget turns on for the first time. After clicking "**I have read it**," the customer can use the product regularly. Click **System Info** > **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export. **Note:** The current privacy policy's text is only available in English. However, translation of other multi-language content is underway, with more iterations.

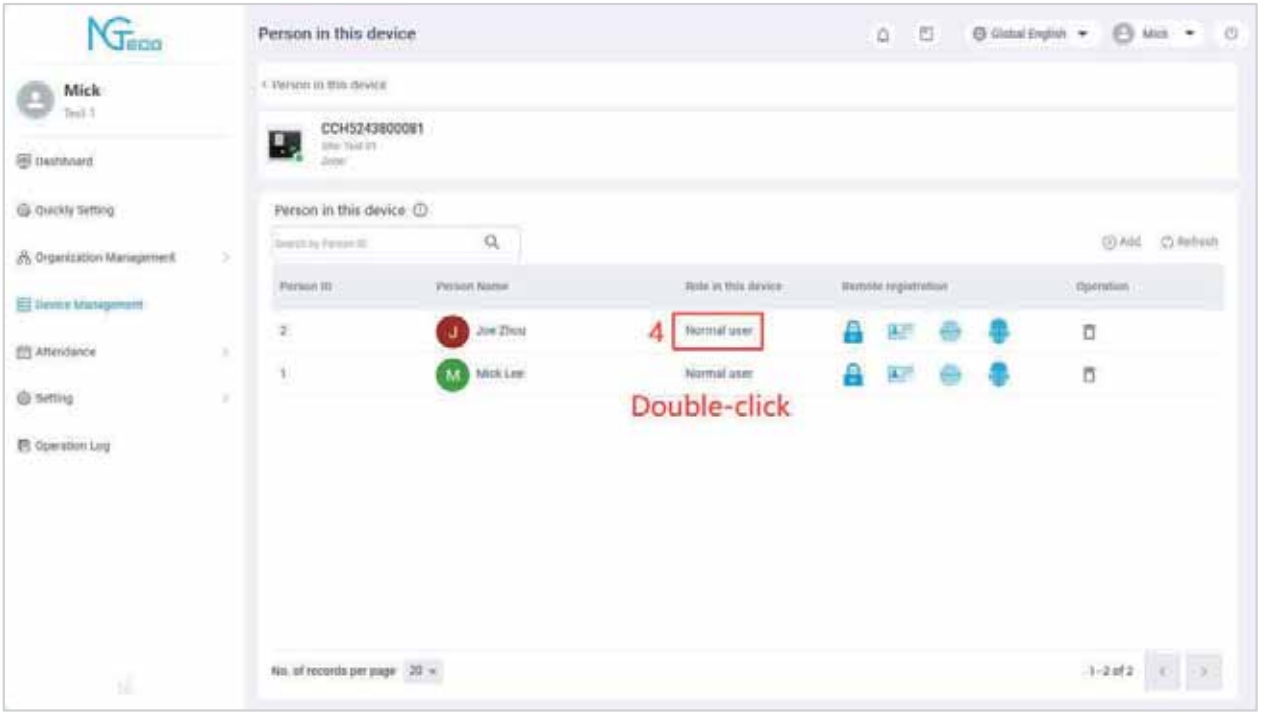
13 Privileges

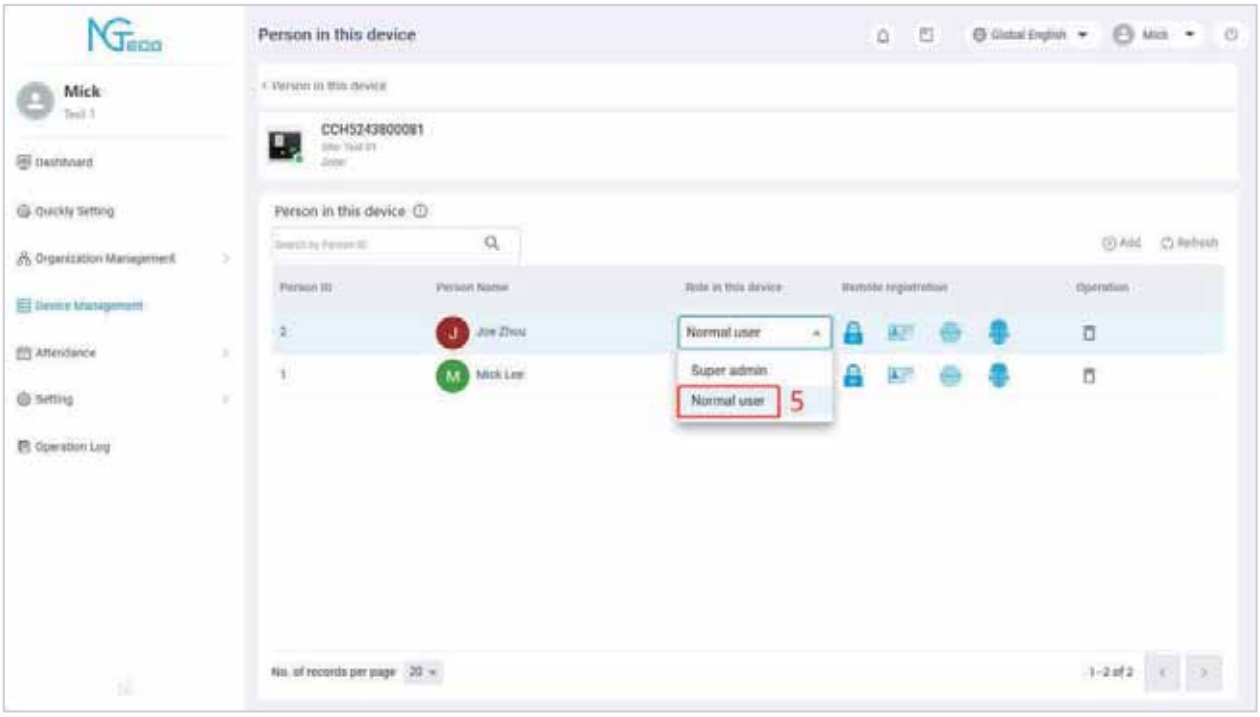
The user privileges are classified as:

- 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:







13.1 Administrator

The Administrator privilege safeguards the device's important configurations. Administrators can operate all menus, manage attendance through facial, make configuration changes, add or modify user details, and query attendance records.

13.2 Normal User

Normal users can make attendance punch through facial verification methods. For further details, please refer to 2.4 Verification Modes.

14 Binding the Device

14.1 Binding Devices via the NGTeco Office Mobile App

Download the NGTeco Office App

Search for the "NGTeco Office" app in the iOS App Store or Google Play Store (Android), or scan the QR code below to install the app.

NGTeco Office

Google play

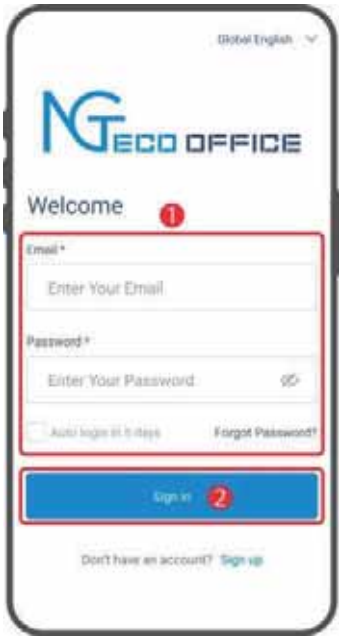
NGTeco Office

Download on the App Store

14.1.1 Login to the App

1. If the user has an account, please follow the steps below:
   1) Access the NGTeco Office Mobile Application at the App Store.
   2) Log in using your user credentials: Email ID and password. Then, click **[Sign in]**.

Note: *By checking the box, you can enable automatic login to the app for the next 5 days.*



2. If you do not have an account, follow these steps to create a new account:

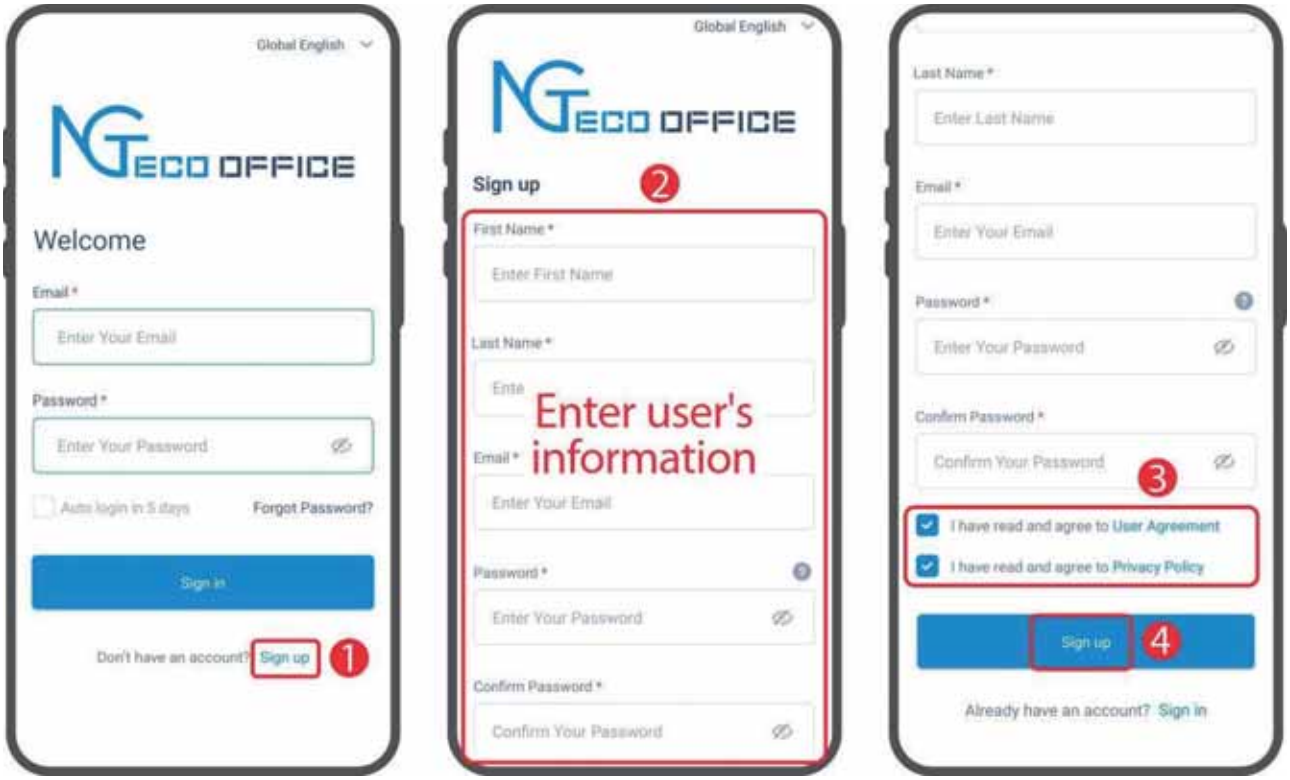
1) Access the NGTeco Mobile App and click on **[Sign Up]** to add a new account.

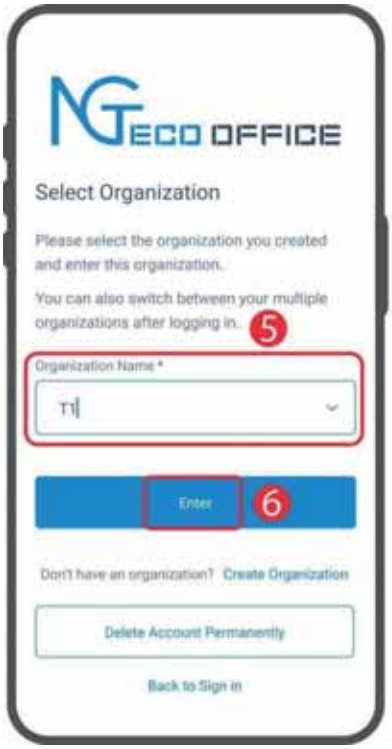
2) To create a new account, enter the user's information and set the password. Please, read and agree to the User Agreement and Privacy Policy then click [**Sign Up**].

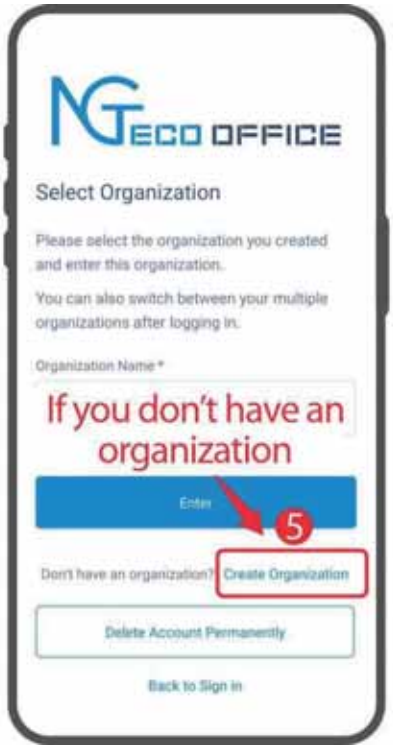
3) Log in with your account and select the organization if already you have one. If you don't have an organization, click on [**Create Organization**].

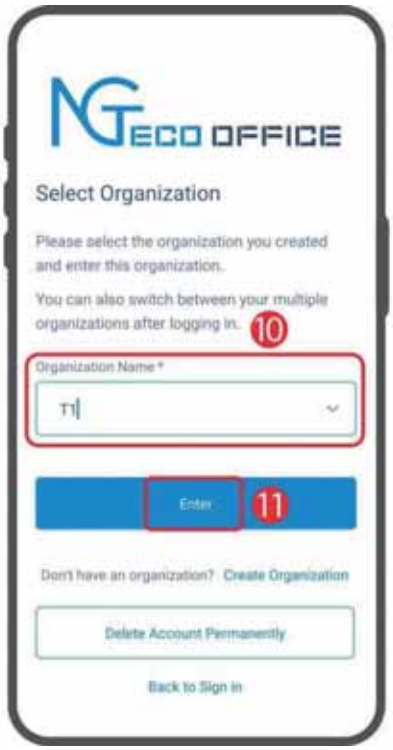
4) Set the organization's name and code, click [**Create**], and then complete the registration.

Note: *To permanently delete your account, click [**Delete Account Permanently**] and then click [**Confirm**].*







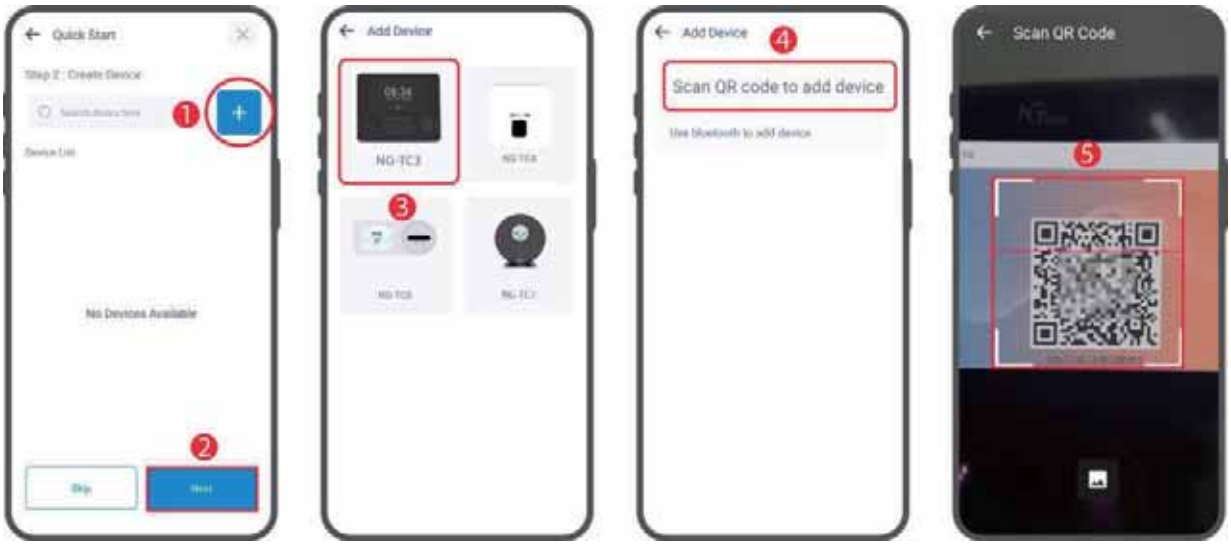


14.1.2 Add device.

Two Ways to Create Device and Set Up the Network:

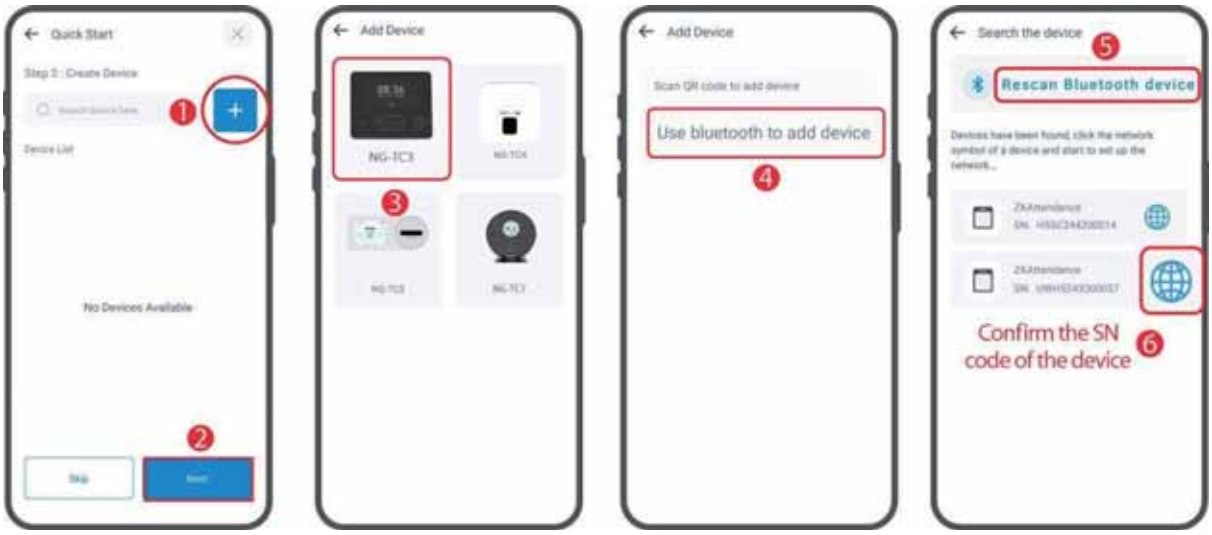
Scan QR code to add device

1. Click [**Device**] > [**Device**] to enter the Device screen.
2. Click + icon to add a new device.
3. Select the device model you need to add in the Add Device screen.
4. Click [**Scan QR code to add device**] to enter the scan QR code screen.
5. Then aim your phone's camera at the QR code on the device and scan it.



Use bluetooth to add device

1. Click [**Device**] > [**Device**] to enter the Device screen.
2. Click + icon to add a new device.
3. Select the device model you need to add in the Add Device screen.
4. Then click [**Use bluetooth to add device**] to enter the search the device screen.
5. Click [**Rescan Bluetooth device**] to search for the device via Bluetooth. And the searched Bluetooth devices will be displayed in the list. Then just select the device you want to add based on the serial number.



a. Wi-Fi connection

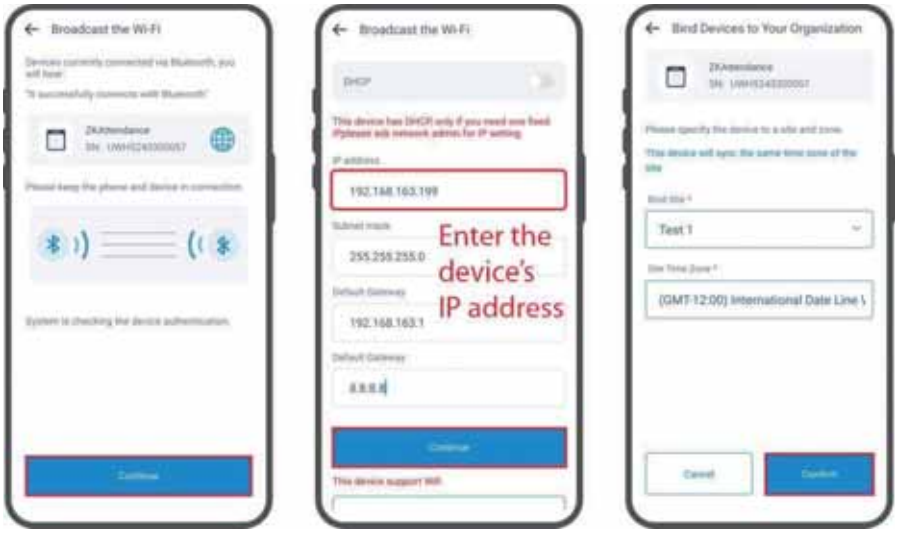
1. After successful code scanning, the App navigates to the **Broadcast the Wi-Fi** interface.
2. Click [**Continue to set Wi-Fi**] at the bottom to select the Wi-Fi then Enter the password and click [**Continue**] to connect.
3. When the device voice prompts" Network **Connection Successful**", it means the Wi-Fi connection is successful.
4. Then specify the device to a site and zone. Enter the parameters and click [**Confirm**], when prompted successfully, the configuration is complete.

   Note: *The device supports connection to 2.4G and 5G dual-band Wi-Fi wireless networks.*

b. Ethernet connection

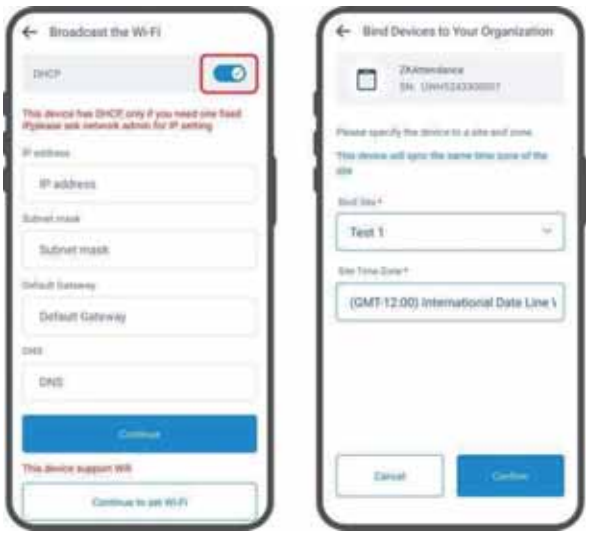
If the network is in an encrypted state:

1. After selecting the device, follow the interface prompts and click [**Continue**].
2. Then enter the device IP address and click [**Continue**] to connect.
3. Then specify the device to a site and zone. Enter the parameters and click [**Confirm**], when prompted successfully, the configuration is complete.



If the network is not in an encrypted state:

1. Click the icon to enable DHCP.
2. Then assign the device to a site and zone by entering the required parameters, and click [**Confirm**].

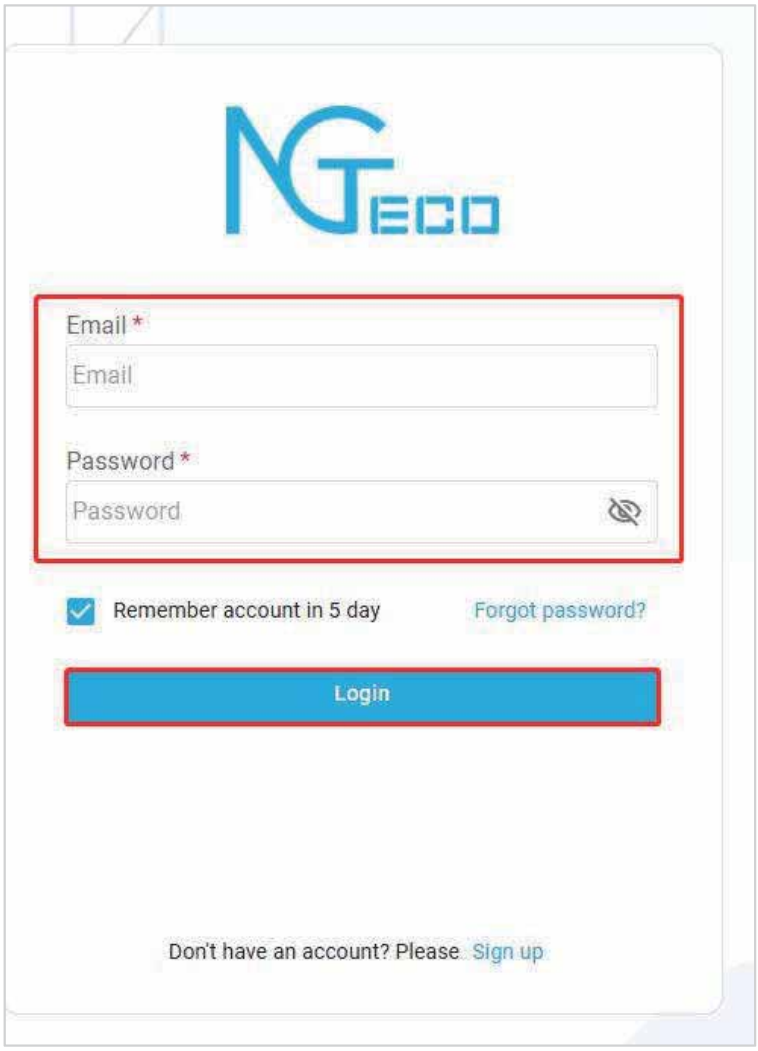


Note: *After the device is added, it will take a few moments for the device to change from "Offline" to "Online" status.*

14.2 Binding Devices via the NGTeco Office Web

14.2.1 Login to the NGTeco Office Web

1. If the user has an account, please follow the steps below:
   1) Please open the recommended browser and enter the IP address to access the NGTeco Office Web: https://office.ngteco.com/
   2) Enter your Email ID and password on the login screen and click **[Login]** to login.

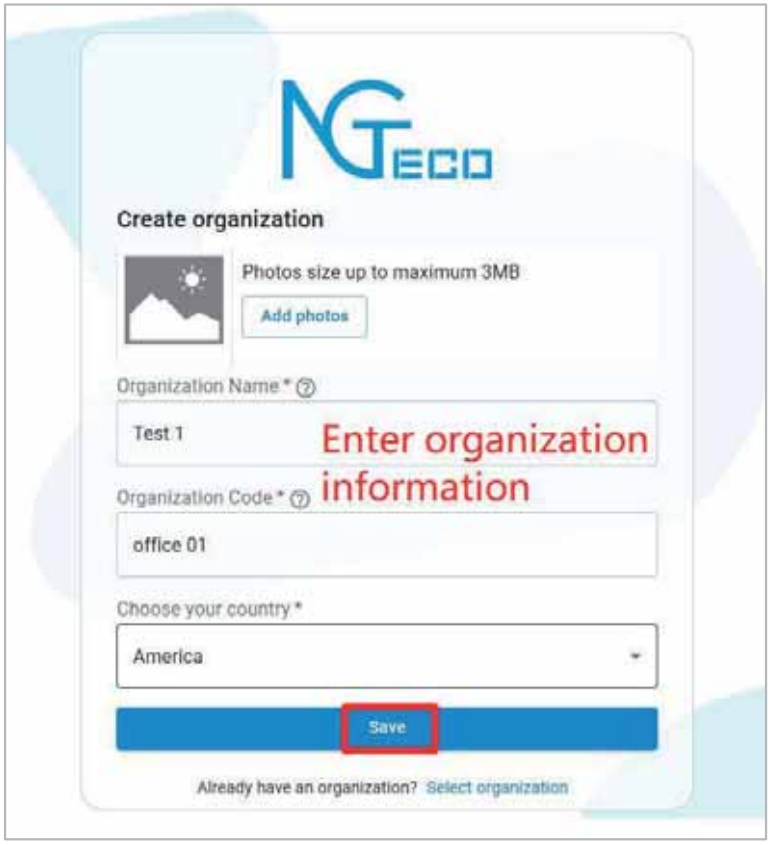


2. If you do not have an account, follow these steps to create a new account:
   1) Click [**Sign up**] on the login screen to add a new account as shown below.

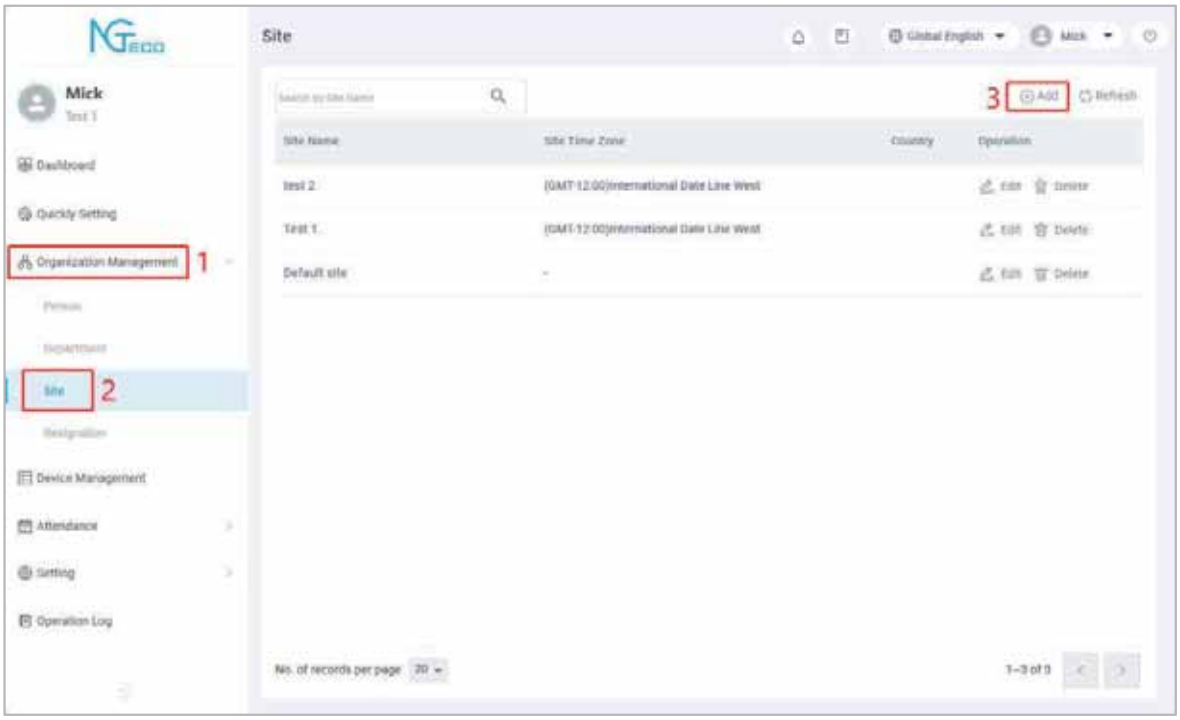
2) Then enter the user's information and set the password. Please, read and agree to the User Agreement and Privacy Policy then click [**Sign up**].

3) Log in with your account and select the organization, if you already have one. If you don't have an organization, click on [**Create organization**].

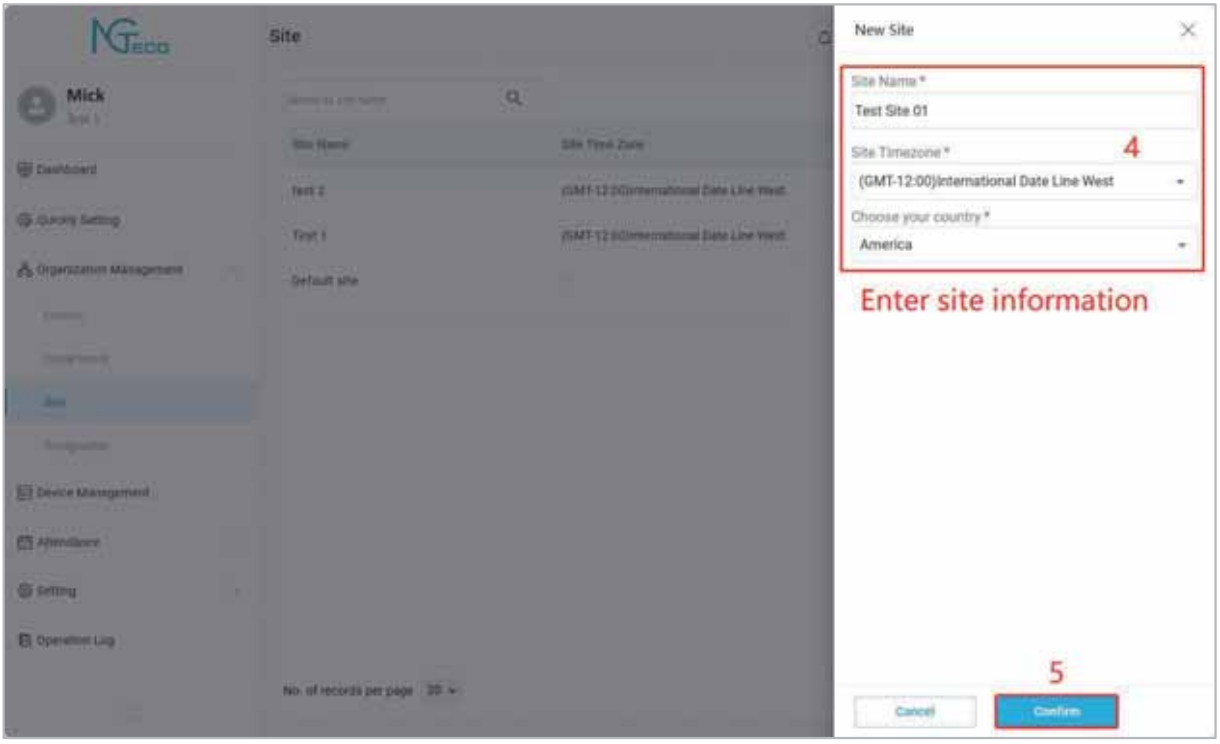
4) Set the organization's name and code, click **[Save]**, and then complete the registration.



5) Then log in back into the Web with the created account, click [**Organization Management**] > [**Site**] to enter the setup interface, and click ⊕ to add a new site.

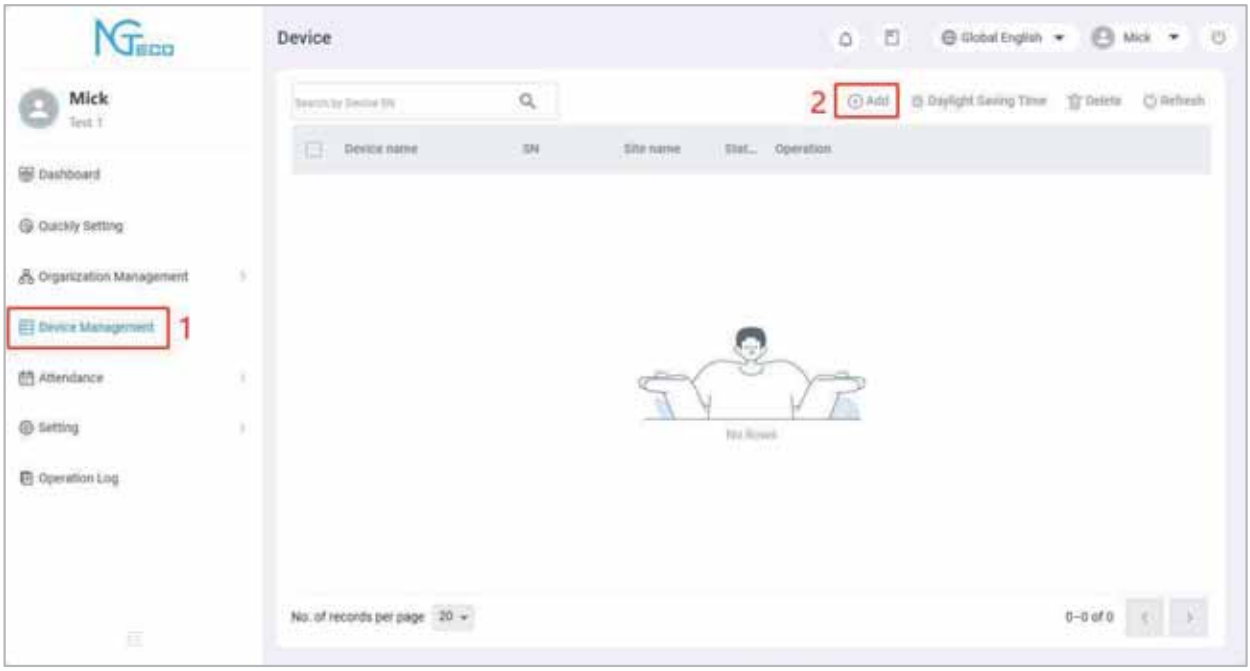


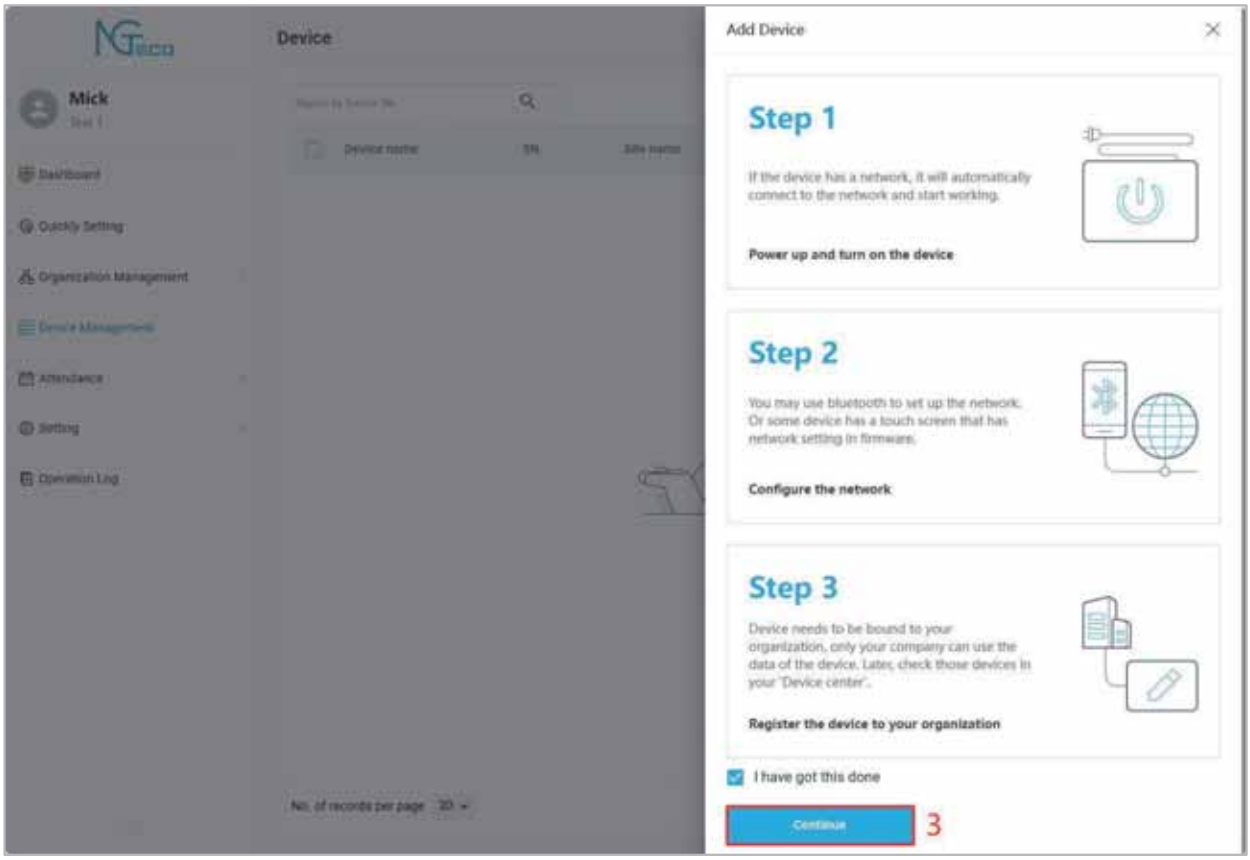
6) Then enter the site information in the New Site screen and click [**Confirm**].



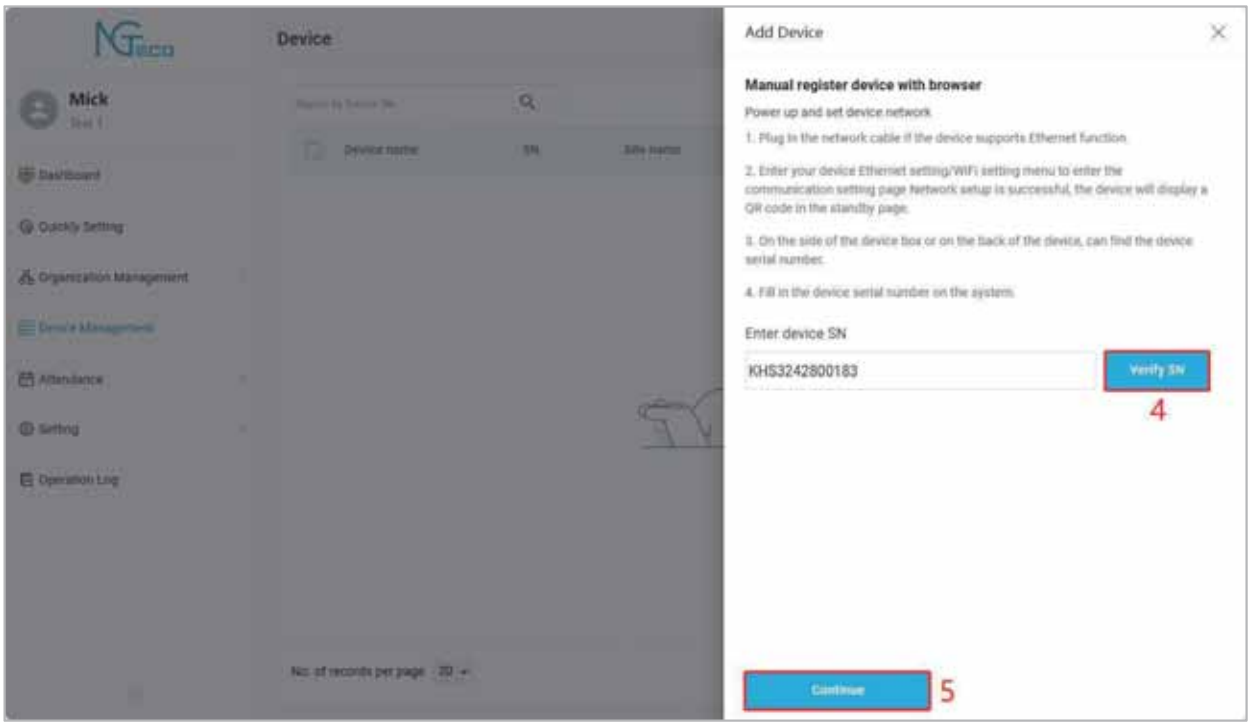
14.2.2 Add Device

1. Click [**Device Management**] > ⊕ icon to enter the add Device screen. Then review the instructions and click [**Continue**].



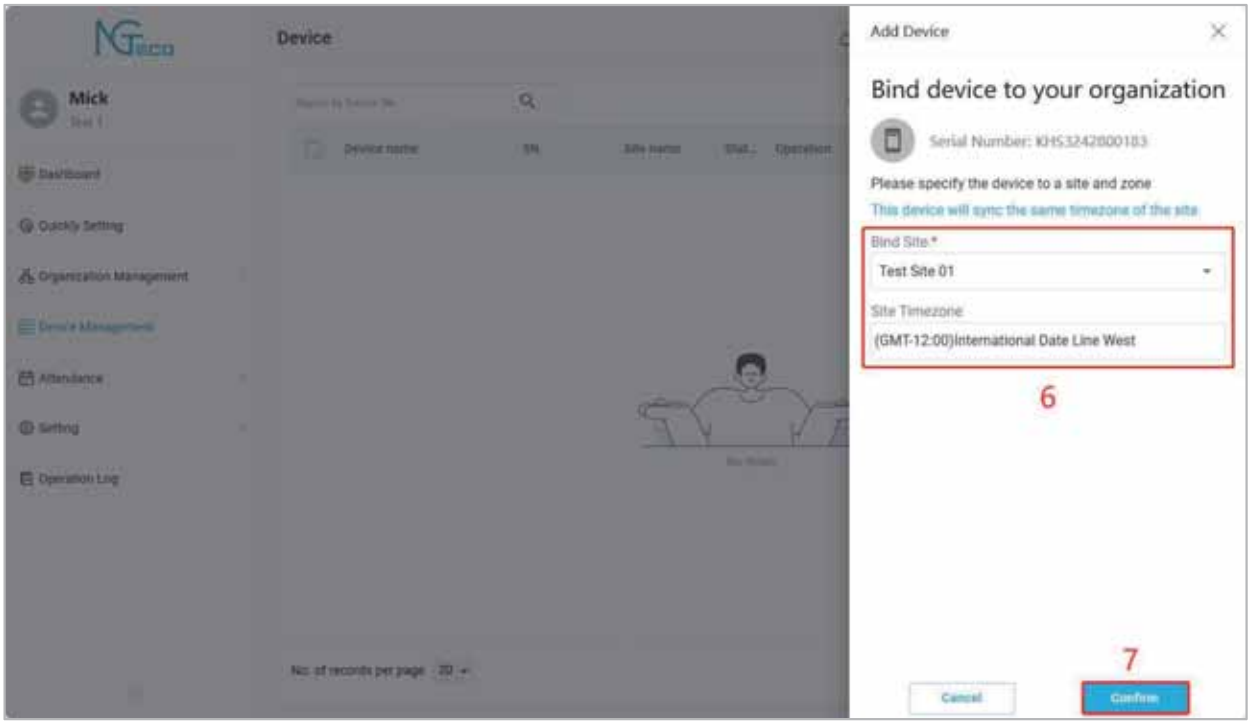


2. Fill in the device serial number on the Add Device interface and click [**Continue**].



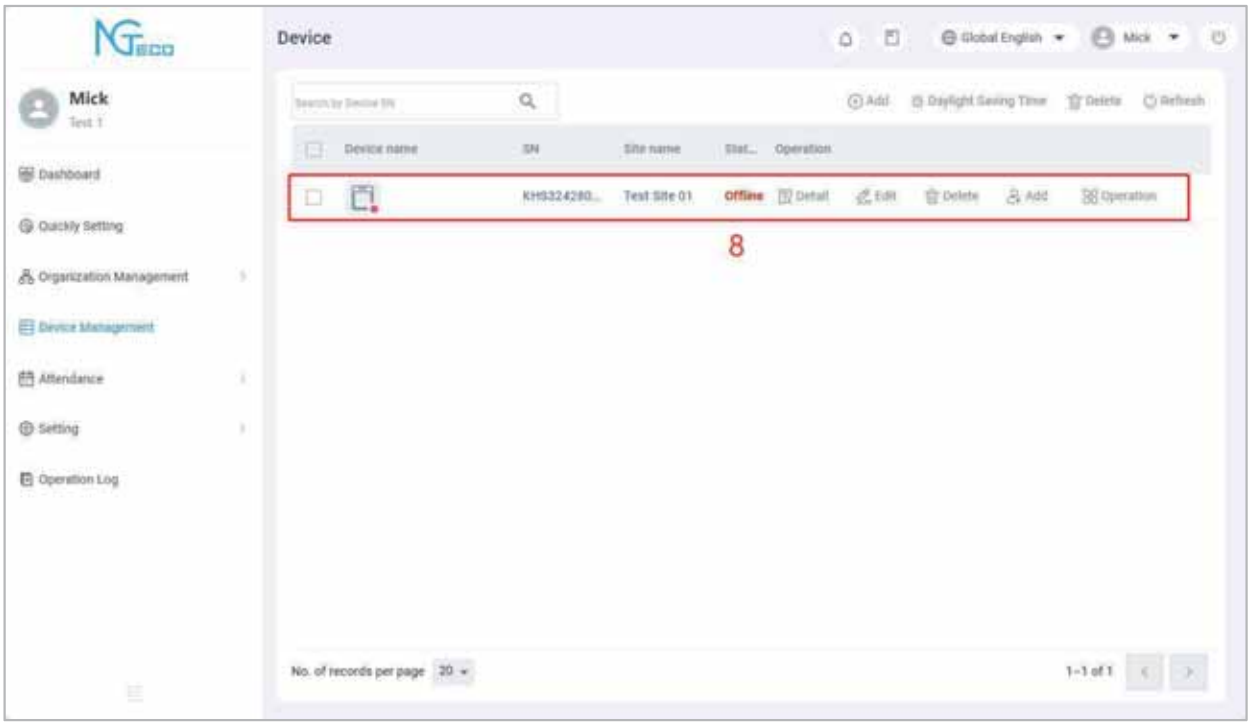
Note: *The serial number can be viewed on the rear case label of the unit.*

3. Select Site and Timezone in the right pop-up screen to bind the device to the organization and then click [**Confirm**].



Note: *This device will synchronize with the site's timezone.*

4. Once added, the device is displayed in the device list.



Note: *There may be a delay, please wait a moment, after receiving the device voice prompts, refresh in the [**Device Management**] interface to see the device display online status.*

15 Operation on NGTeco Office Mobile App

15.1 Login

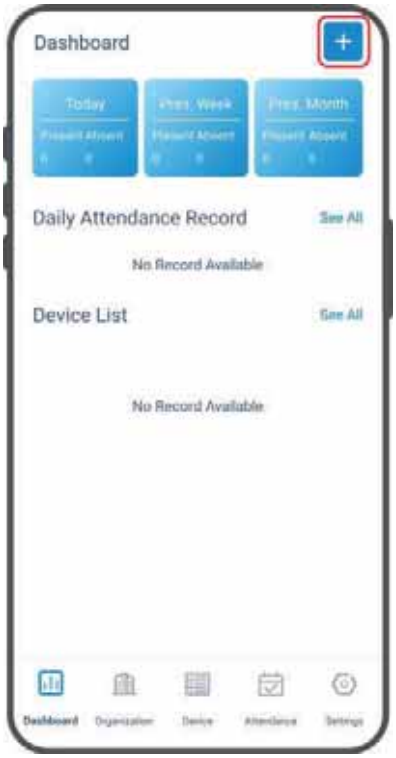
Access the NGTeco Office Mobile Application at the App store.

Log in using your user credentials: Email ID and password. Then, click **[Login]**.

Note: *By checking the box, you can enable automatic login to the app for the next 5 days.*

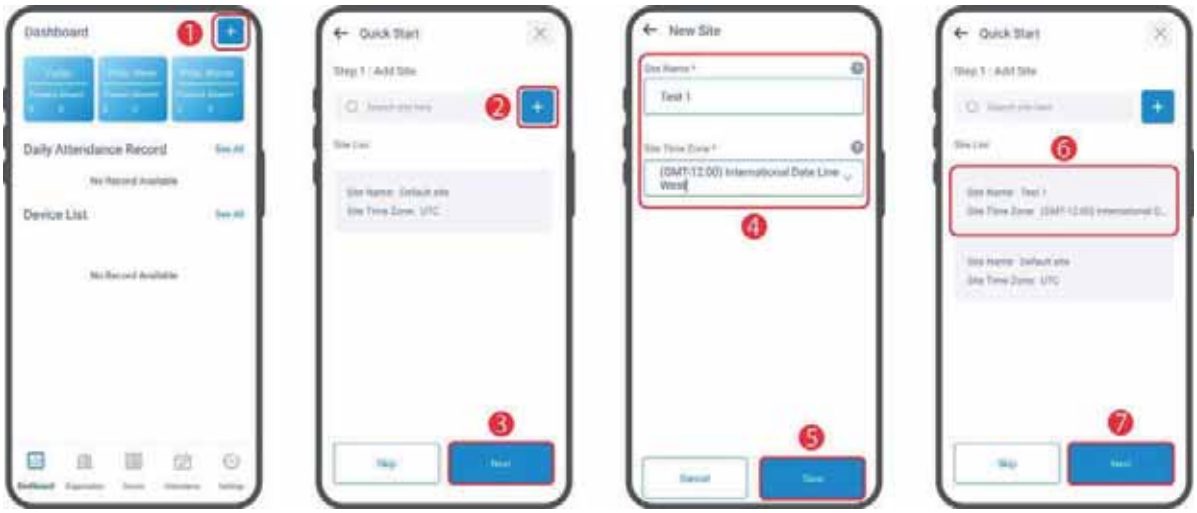
15.2 Quick Start

Users can tap [**Quick Start**] in the upper right corner of the APP to quickly start the relevant parameter settings, then follow the prompts to complete the setting.



Tip: *Click [**Skip**] to skip the current step and go directly to the next step. Please enable the Bluetooth function of your phone before connecting the device.*

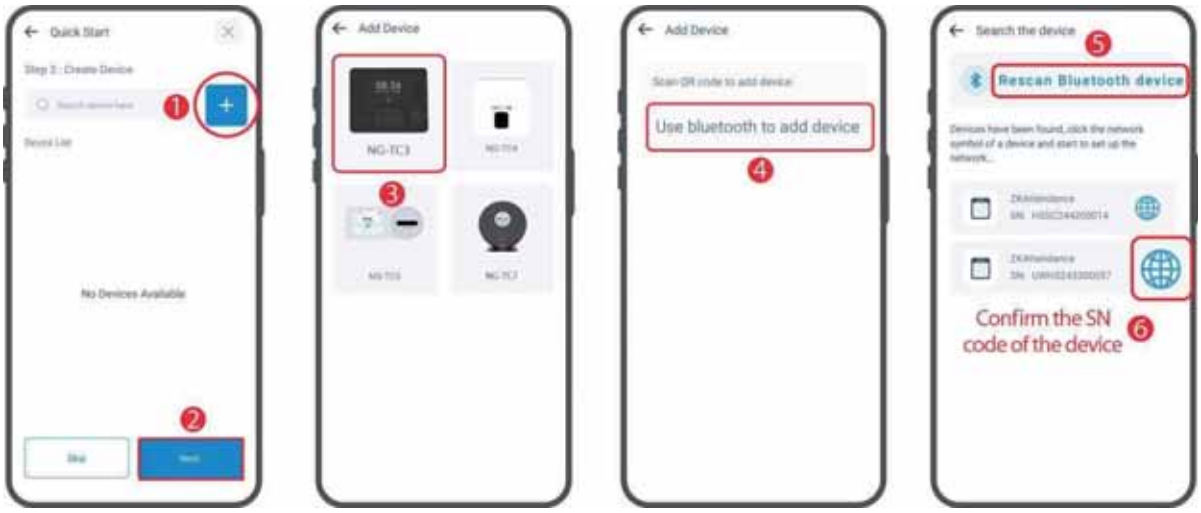
Step 1: Add Site



Step 2: Two Ways to Create Device and Set Up the Network

1. Scan QR code to add device

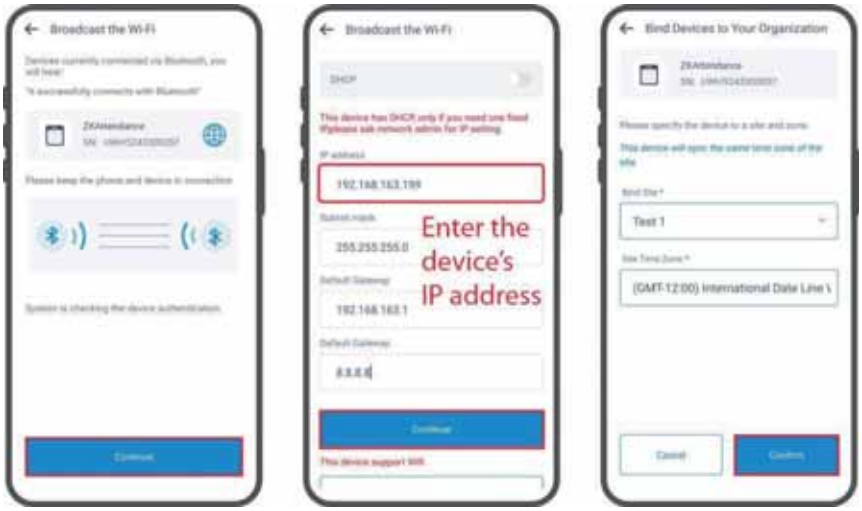
2. Use bluetooth to add device



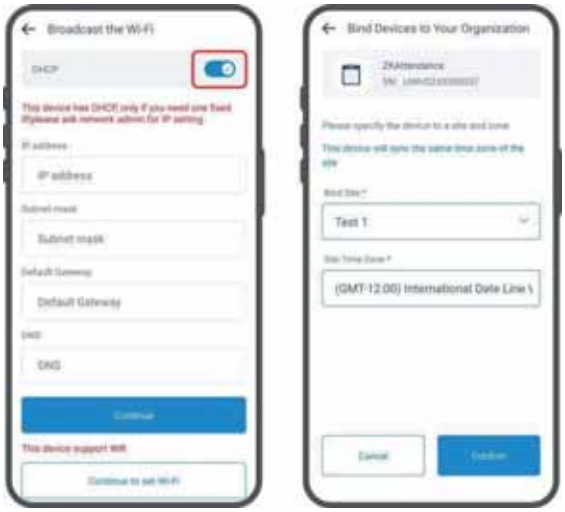
a. Wi-Fi connection

b. Ethernet connection

If the network is in an encrypted state:

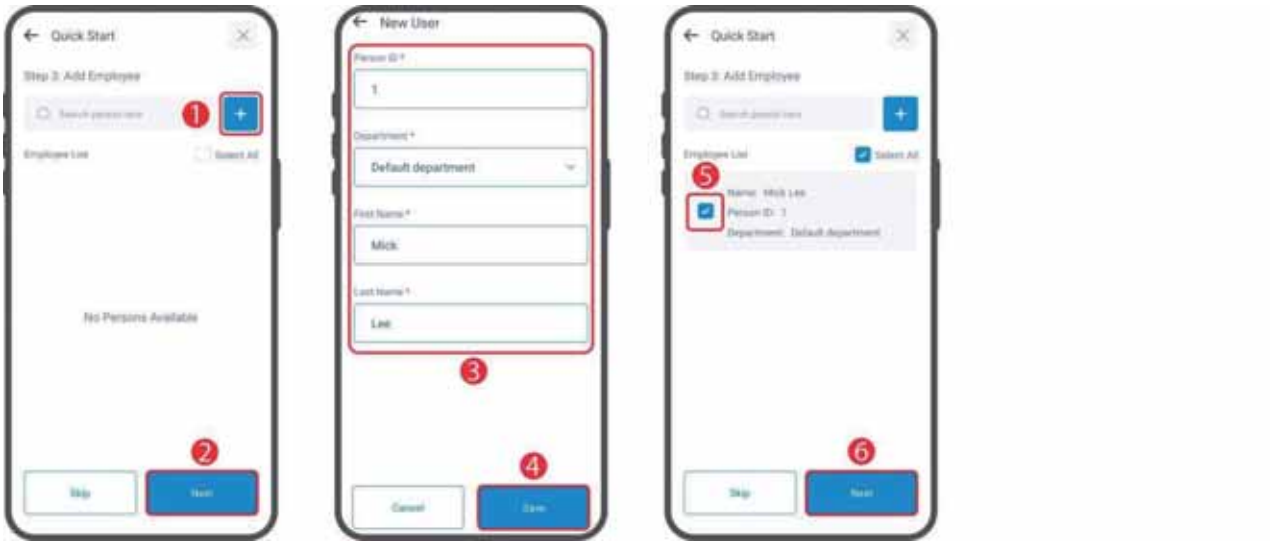


If the network is not in an encrypted state:

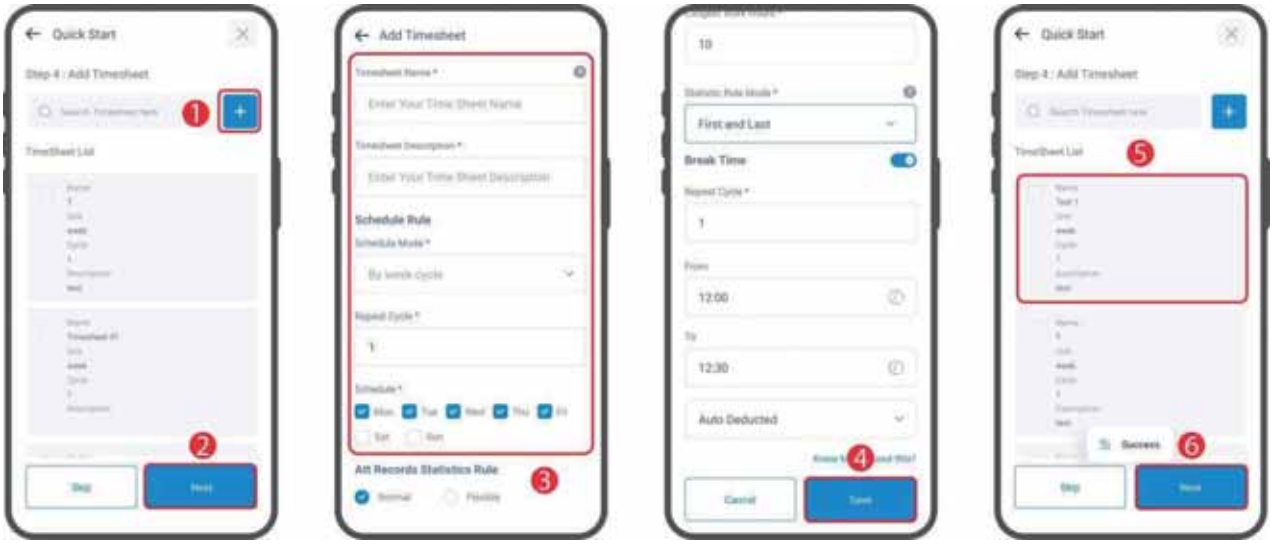


Note: *The device supports connection to 2.4G and 5G dual-band Wi-Fi wireless networks.*

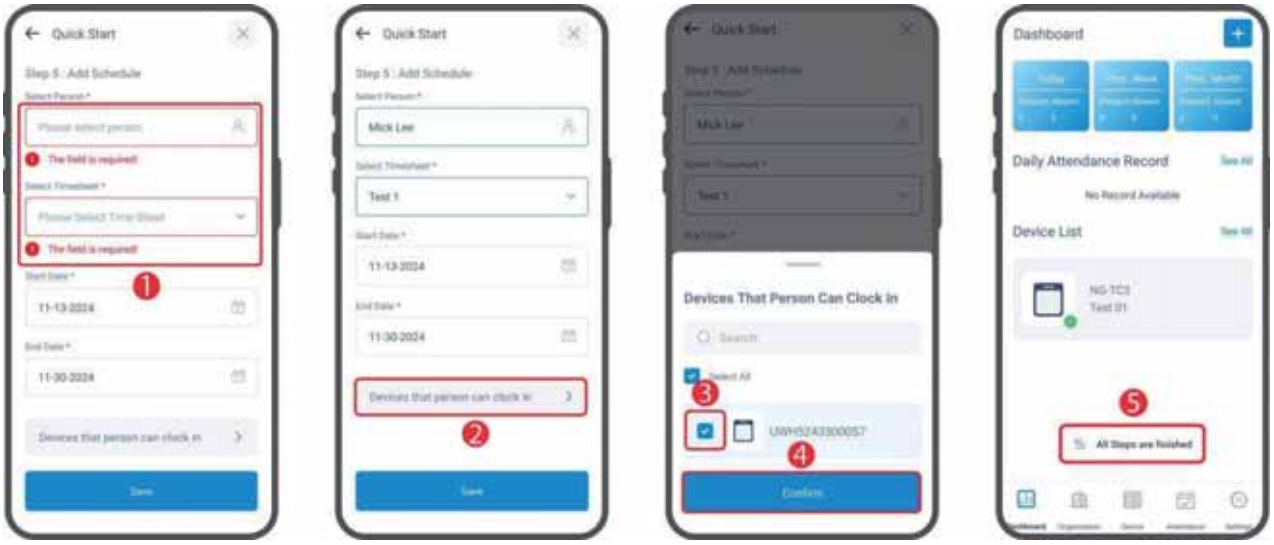
Step 3: Add Employee



Step 4: Add Timesheet



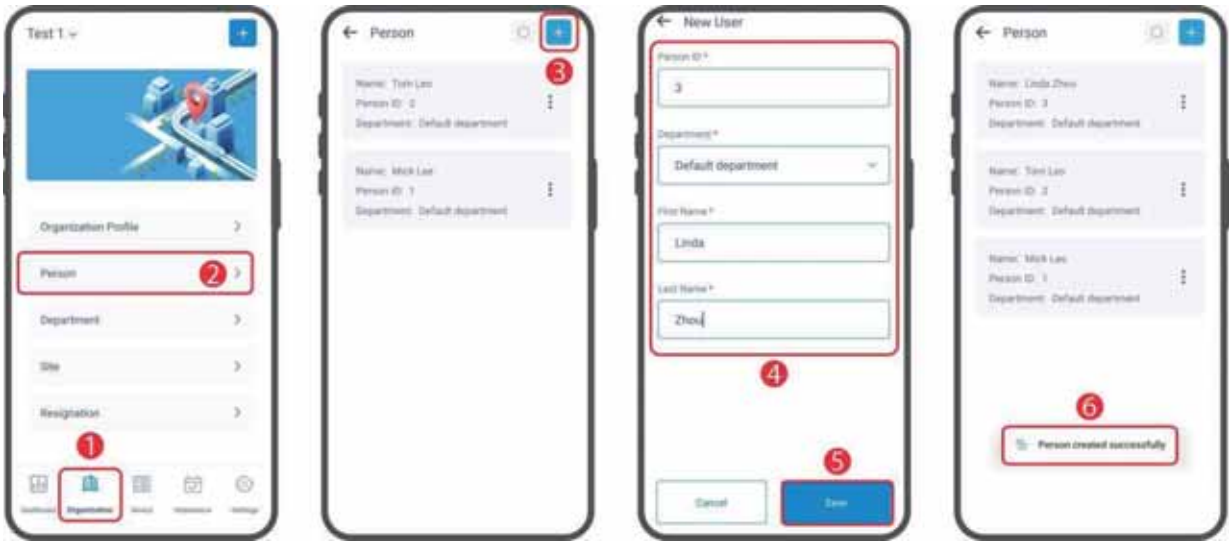
Step 5: Add Schedule



15.3 Organization Management

15.3.1 Add Person

Click [**Organization**] > [**Person**] at the NGTeco Office App and refer to the following procedure to add a new person.



15.3.2 Add Department

Click [**Organization**] > [**Department**] at the NGTeco Office App and follow the steps below to add a department.