NGTECO

User Manual

NG-MB1/NG-MB2

Date: February 2022

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-MB1/NG-MB2**.

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

This document outlines the menu operations of the **NG-MB1/NG-MB2**. The device provides convenience for users and minimizes the requirement of the computer skills of users. The device allows the setting of attendance rules, managing user information, managing user privileges, setting pay periods, generating timecard reports and attendance logs, etc.

Key Features

- Easy to monitor and straight-forward services.
- Reduces management cost for attendance related procedures.
- Advanced attendance analytics.
- Granular visibility into attendance patterns.
- Greatly reduces month-end hassles and compliance challenges.

2   Operational Procedure

Note: Press and Hold **<M/OK>** key for 3 seconds to open the menu.

2.1   Standing Position, Posture and Facial Expression

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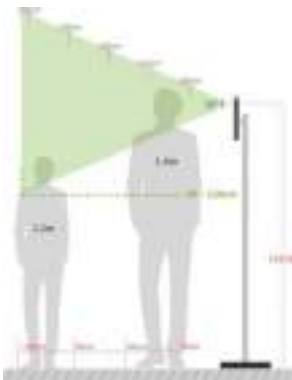
The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2.5m. Users may slightly move forward or backward to improve the quality of facial images captured.

- **Recommended Standing Posture and Facial Expression**

Standing Posture   **Facial Expression**

Note: Please keep your facial expression and standing posture natural while enrolment or verification.

2.2   Standby Interface

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

2.3   Face Enrollment

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

Correct face registration and authentication method

➢ **Recommendation for registering a face**

✓ When registering a face, maintain a distance of 40cm to 80cm between the device and the face.

✓ Be careful not to change your facial expression. (smiling face, drawn face, wink, etc.)

✓ If you do not follow the instructions on the screen, the face registration may take longer or may fail.

✓ Be careful not to cover the eyes or eyebrows.

✓ Do not wear hats, masks, sunglasses, or eyeglasses.

✓ Be careful not to display two faces on the screen. Register one person at a time.

✓ It is recommended for a user wearing glasses to register both faces with and without glasses.

➢ **Recommendation for authenticating a face**

✓ Ensure that the face appears inside the guideline displayed on the screen of the device.

✓ If the glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face without glasses further. If the face with glasses has been registered, authenticate the face 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 includes 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

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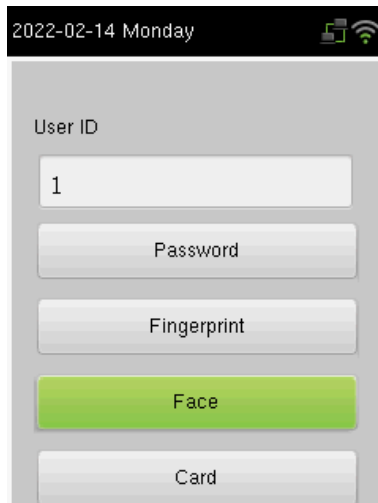
If the verification is successful, the success message will be displayed as shown below:
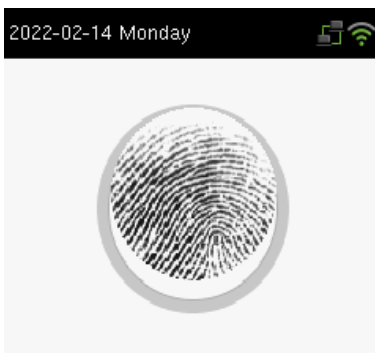

2.5.2   **Fingerprint**

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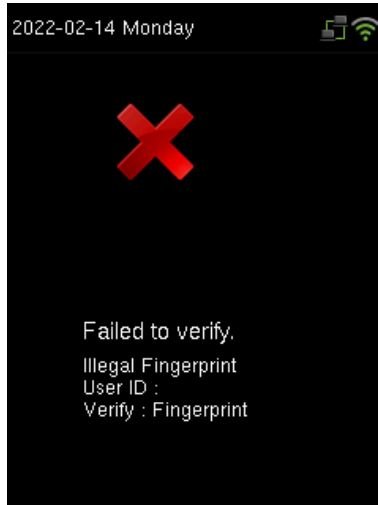
1: N Verification: The device compares the current fingerprint collected by the fingerprint sensor with all the fingerprints on the device. Press your finger properly on the fingerprint sensor. If the fingerprint matches with the saved template, the verification is successful.

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.

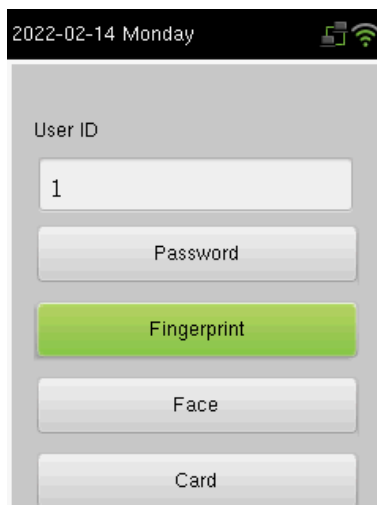If the fingerprint matches the saved template, the verification is successful, and the success message will be displayed as shown below:
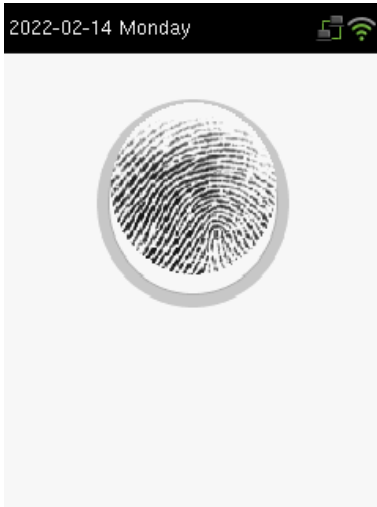
If the verification failed, the message will be displayed as shown below:
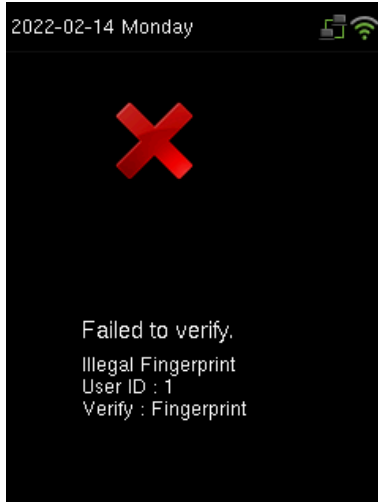
⭐ If the device displays **"Error! Invalid user ID"**, then the User ID is not yet created.
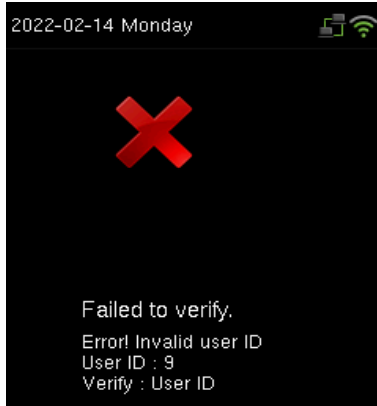
If the device instructs **"Please try again"**, then press your finger again. You can try 2 more times. If the verification fails after trying for 2 more times, then the device returns to the home screen.

2.5.3   Card Number★

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.

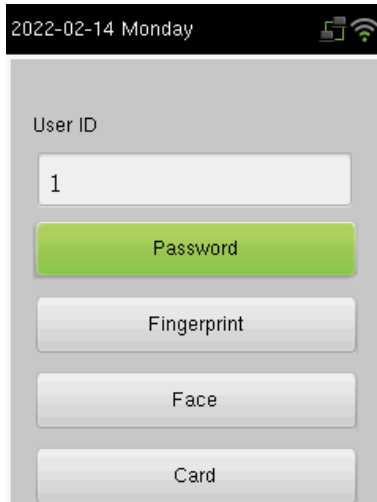If the verification is successful, the success message will be displayed as shown below:

2.5.4   Password

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:
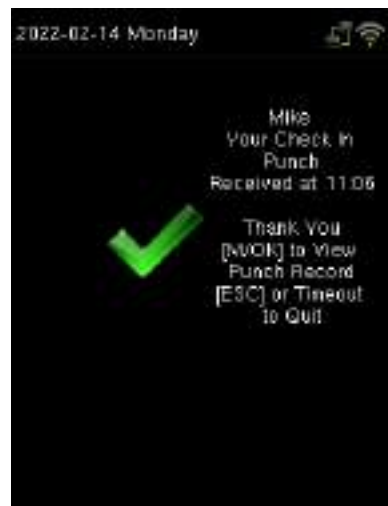
If the verification failed, the message will be displayed as shown below:
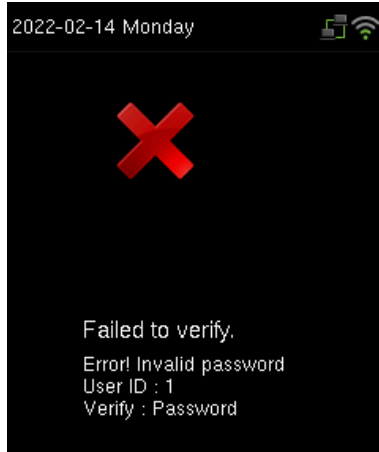
2.6 **T9 Mode**

The 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.

1. Navigate to the required text field and press **<M/OK>**.
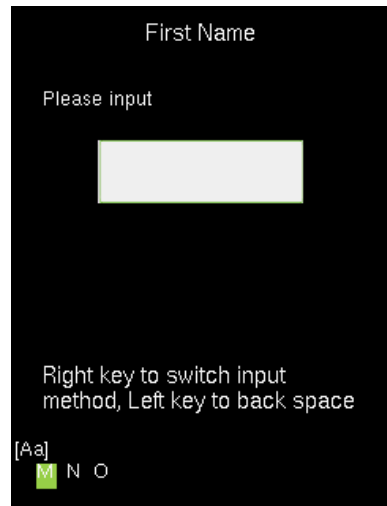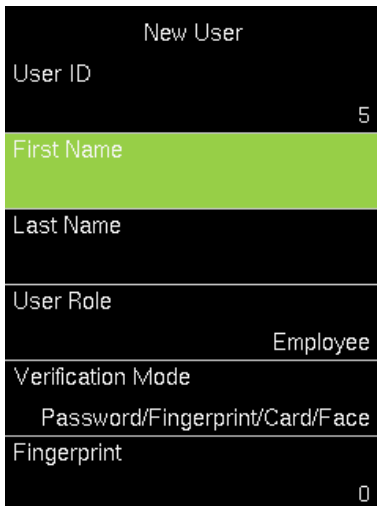
2.   Each key on the keypad has a few letters printed above them. For example, pressing 3 can enter D, E, and F. To enter "**F**", press 3 thrice. This is accomplished by comparing the number of keystrokes with the internal syntactical dictionary to determine the letter.

3.   Press < ▶ > or <▲> to switch between Uppercase, Lowercase, and Special characters.
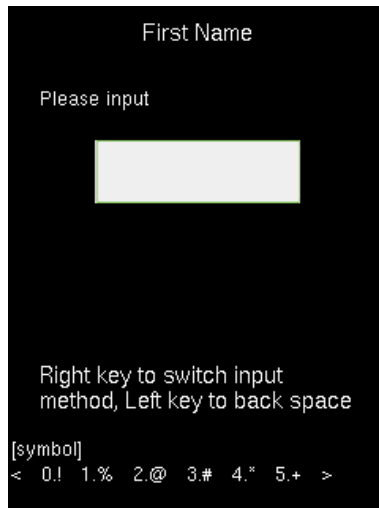
4.   To add the special character, press the corresponding key once. For example, to enter "@" press 2 once.

5.   After the input is complete, press the **<M/OK>** key twice to save.

3   Privileges

The user privileges are classified as:

- Administrator
- Employee

3.1   Administrator

The Administrator privilege protects the device against unwanted damage to important configurations and unwanted changes. The Administrator has the privilege to operate all the menus in addition to fingerprint/password-based attendance maintenance. The Admin can make changes to the configuration, add and modify user details, and query on attendance records. Click here to view the detailed menu operations.

Initially, the Admin must press and hold the **<M/OK>** key for 3 seconds. Then the Admin verification screen appears as shown below:
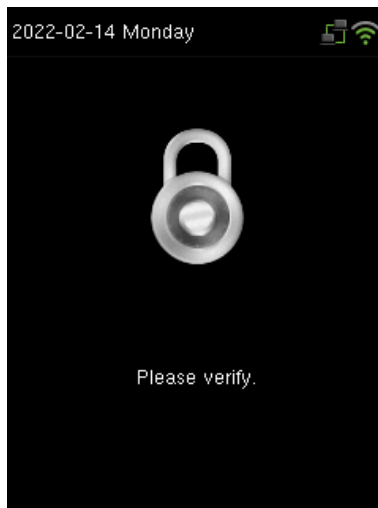
The Admin must verify the face/fingerprint/card number★ or enter user ID to verify the password. Please refer to 2.5 Verification Modes.

If a person other than Admin tries to open the menu with his own credentials, an error will be displayed as shown below:
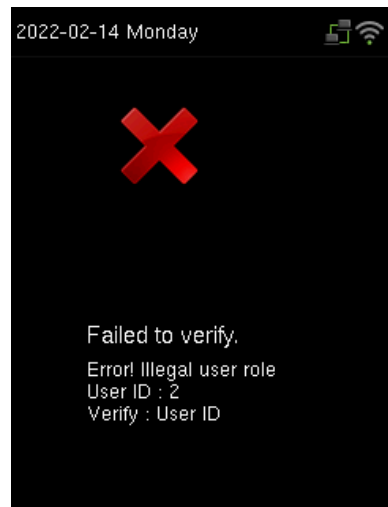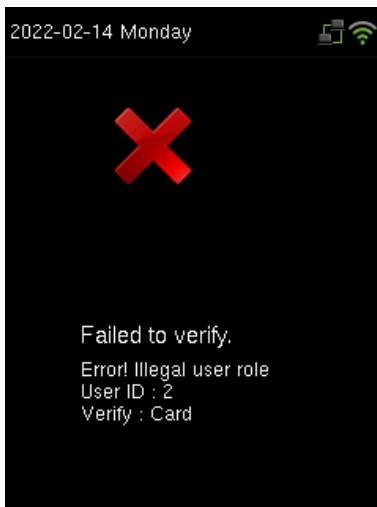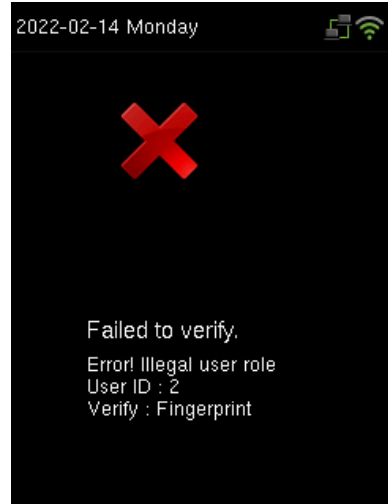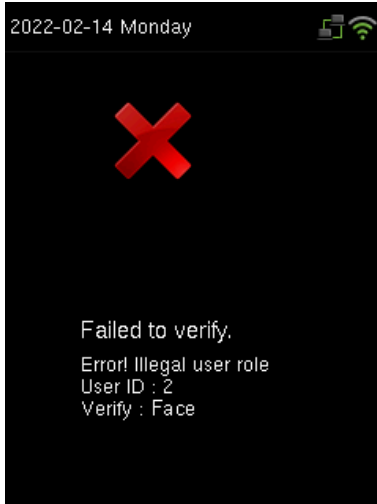
Note: After registering as an administrator, you must use the administrator authentication method to enter the menu.

3.2   Employee

Users can make attendance punch through face/fingerprint/card number★/password verification methods. For further details, please refer to 2.5 Verification Modes.

4   <u>Main Menu</u>

The device comprises the following menu. Long press 3s **<M/OK>** to enter the menu.
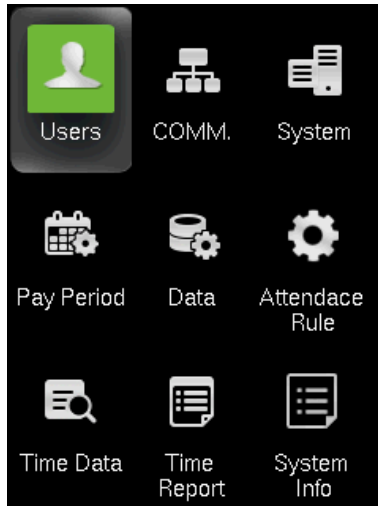
Function Definition:

Users (User Management): Add, Edit, and Delete user's information, including User ID, Frist Name, Last name, User role, Verification mode. Use the USB disk to Upload or Download the user's function.

Comm. (Communication Settings): Set the communication parameters between device and PC, such as DHCP, IP Address, Subnet mask, Gateway, Wi-Fi, WIFI setup by USB, set the App connection.

System: Set the system parameters, such as Date Time, Face parameters, Autotest, Reset, Firmware Upgrade and Help Menu.

Pay Period: Set the Pay period type and Start day of the week.

Data (Data Management): Download Attendance Log, Delete Attendance/All Data, Delete User Photo and Clean Permission.

Attendance Rule: Set the Attendance rule, such Maximum work hours, Day cutoff time, Duplicate punch interval, Enable auto punch mode and View punch record.

Time Data: View the user's Today's record, History record, and Add missing punch.

Time Report: Select the Pay period, set the report hours format to download the time report.

System Info: Check the Device usage, Basic information, and Firmware information etc.

5   <u>User Management</u>

The **Users** menu frames a role-based access control and the tasks they can perform in the device. The Administrator(s) can grant and revoke roles and permissions at the device level. To change the permission of a user, the administrator(s) updates the role. It allows the Administrator(s) to add new users, edit the details of an existing user, uploading/downloading the user details from/to a USB drive.
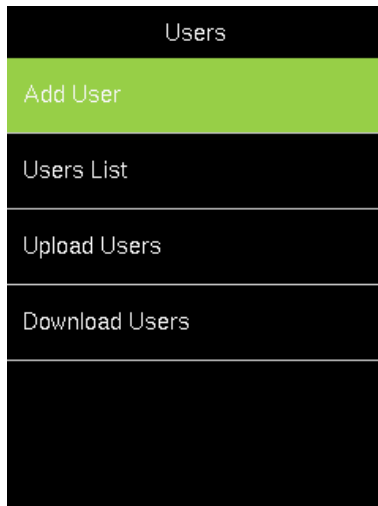
5.1   New User Registration

New users in an organization can be added to the device by an Administrator. It includes simple steps that can be performed without much effort. The steps to add a new user are given below:

1.   Go to **[Users]** and navigate to **[Add User]** by pressing the respective navigation key. The Interface to add a new user will be displayed as shown below:

2.   Enter the following details:

- **ID:** The User ID will be auto-generated beginning from 1. If you want to change the User ID generated by the device, delete the displayed ID by pressing **<M/OK>** and enter the new User ID.

- **First Name:** Enter the First Name of the user.

- **Last Name:** Enter the Last Name of the user. Refer **T9 Mode** for further details.

- **User Role:** Set the User Role of the user as Employee/Admin. Press the <▲> or <▼> key to select the User Role, and then press **<M/OK>**.

- **Verification Mode:** The available verification modes are: Password/Fingerprint/Card/Face, Fingerprint only, User ID only, Password, Card only, Fingerprint/Password, Fingerprint/Card, User ID + Fingerprint, Fingerprint + Password, Fingerprint + Card, Fingerprint + Password + Card, Password + Card, Password/Card, User ID + Fingerprint + Password, Fingerprint + (Card/User ID), Face only, Face + Fingerprint, Face + Password, Face + Card, Face + Fingerprint + Card, Face + Fingerprint + Password. (**Note:** "/" means "or", and "+" means "and".)

- **Fingerprint:** To enroll the fingerprint, press **<M/OK>**. The interface to enroll the fingerprint will be displayed as shown below:
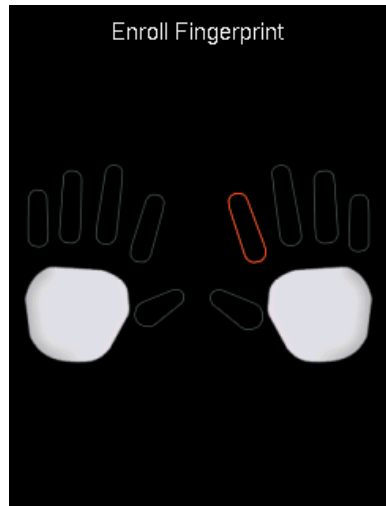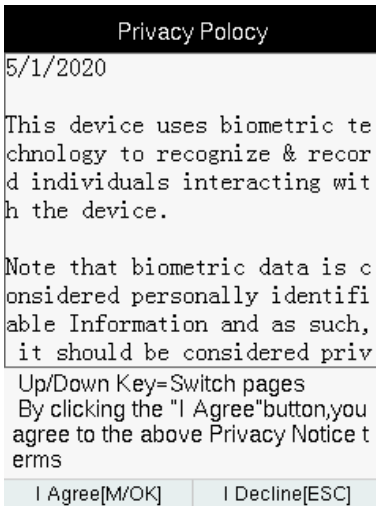
After successful enrollment, the success message will be displayed as shown below, for further details, please refer to 2.4 Finger Enrollment.

- **Face:** To enroll the face, press **<M/OK>**. The interface to enroll the face will be displayed as shown below:
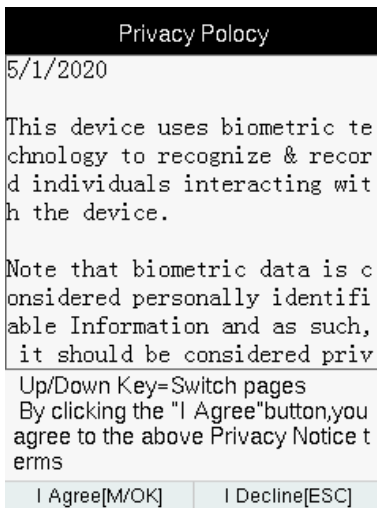
- **Card Number★:** To enroll the card, press **<M/OK>**. The interface to enroll the card number will be displayed as shown below:
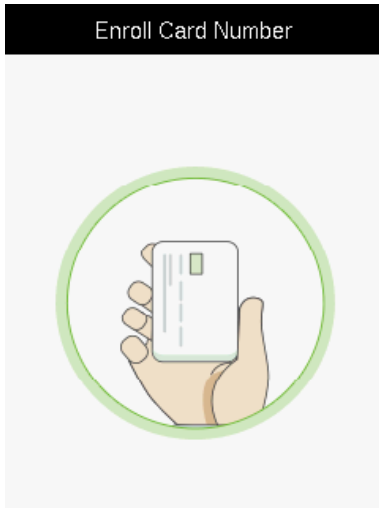
- **Password:** To register a password, press the **<M/OK>** key. The interface to register the password will be displayed as shown below:
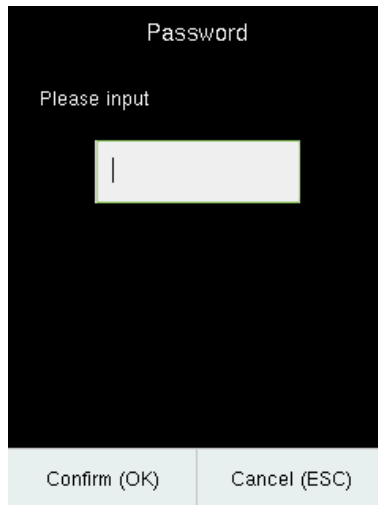
The valid value of the entered password is 6 to 8 digits.

5.2   User Data Management

The Administrator can also modify the existing user data. The steps to edit the user data are
given below:

1.   Go to **[Users]** and navigate to **[Users List]**.
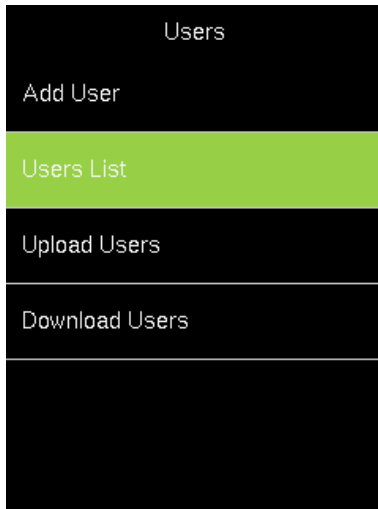
2.   The user's list will be displayed as shown below:
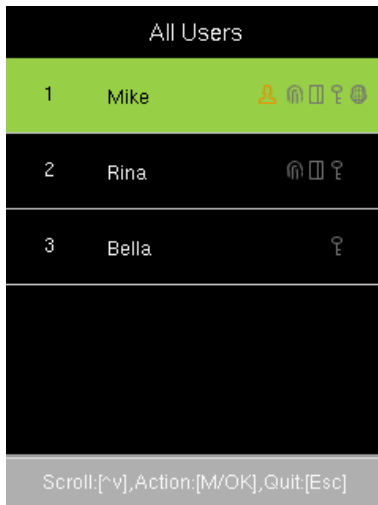
5.2.1   Edit User Details

1. Navigate to the corresponding field and make necessary changes. To add another fingerprint, navigate to Fingerprint and press **<M/OK>**. Enroll the fingerprint. Similarly, navigate to Password and press **<M/OK>**. Enter the New Password and confirm the same.

2. Finally, press **<M/OK>** to save.

You cannot edit the ID of the user.

5.2.2   Delete User

1. If you require to delete a user permanently, navigate to the corresponding user and select **[Delete User].**

User : 1 Mike	Delete : 1 Mike
Edit	**Delete User**
Delete	Delete User Role Only
	Delete Fingerprint Only
	Delete Face Only
	Delete Password Only
	Delete Card Number Only

2.   An alert will be displayed as shown below:

Delete : 1 Mike

Delete User

Delete User Role Only

Delete Fingerprint Only

Delete Face Only

Delete User

OK

Cancel
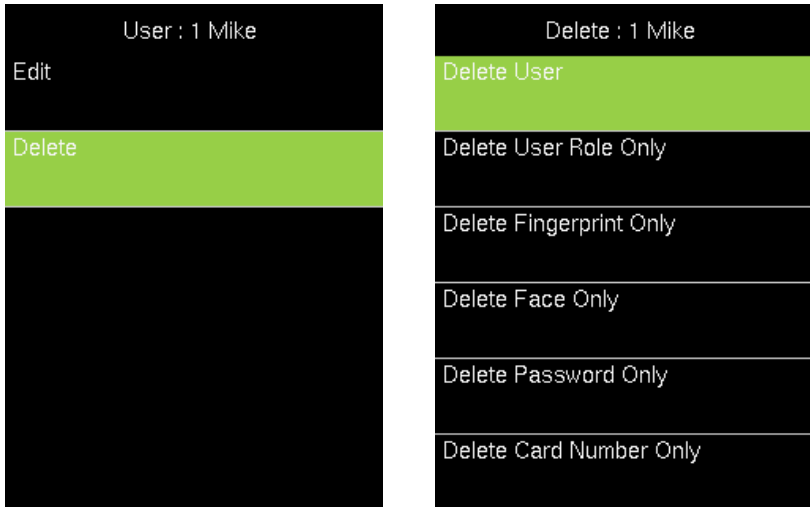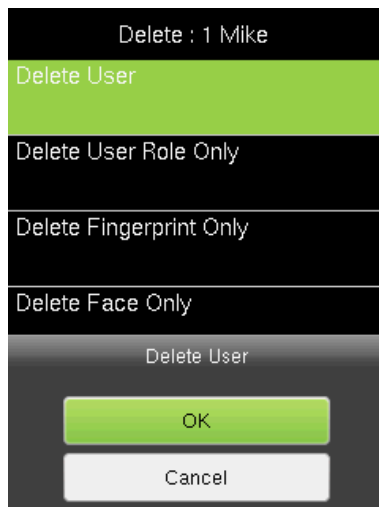
3.   Press **<M/OK>** to delete the User.

5.3   How to Transfer User Data

The user data can be transferred in two ways:

● From Device to the USB drive
● From USB drive to Device

5.3.1   Upload User Data from USB Drive toDevice

To add a large number of user data, you can directly upload it from a USB drive. The device facilitates you to add bulk user data without any complexity in a short duration of time. The procedure to upload the user data is given below.

1.   Go to **[Users]** and navigate to **[Upload Users]**.
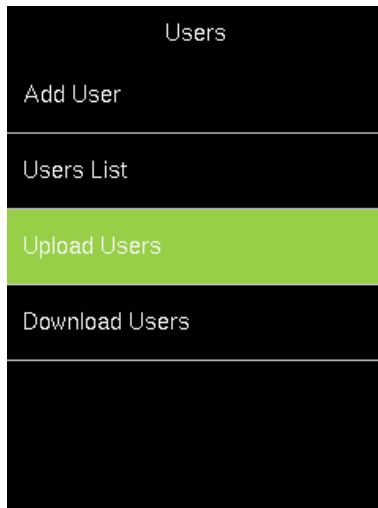
2.   Insert the USB drive into the USB slot.
3.   Navigate to **[Download users template file]** and press **<M/OK>**.

4. The template will be downloaded to the USB drive with the file name **ecuser.txt** and the success message will be displayed as shown below:

5. Insert the USB drive to your PC to edit the template file.

6. The template file will be displayed as shown below:

7. Double-click to open the template file. The template file details will be displayed as shown below:

8. Edit the ID, First Name, Last Name, Password, and permission. An example is shown below:
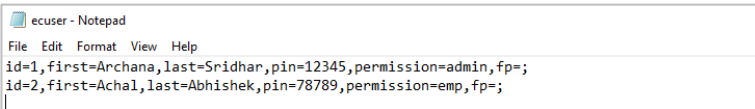
9. Save the template and insert the USB drive into the device again.

10. Go to **[Users]** and navigate to **[Upload Users]**.

11. Navigate to **[Upload user file]** and press **<M/OK>**.

12. After uploading, the success message will be displayed as shown below:

If any existing User ID is the same as the uploaded User ID, then the existing user details will be replaced by the newly uploaded user details.

5.3.2   Download User Data from Device to USB Drive

If you need to download all the user details, perform the following steps:

1. Go to **[Users]** and navigate to **[Download Users]**.
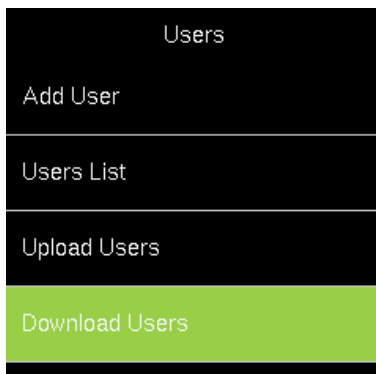
2.   Insert a USB Drive into the device.
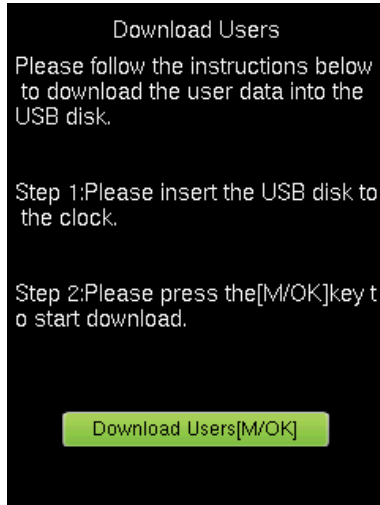
3.   Navigate to **[Download Users]** and press **<M/OK>**.

4.   The success message after downloading the user data will be displayed as shown
      below:

5.   Insert the USB drive to your PC and the file will be downloaded in the name of
      "ecuser.txt".

6. The downloaded file will be displayed as shown below:

6   Communication Parameters

Open the "Comm." Menu to set the communication parameters.

6.1   Manual Ethernet Configuration

The steps to connect to Ethernet is given below:

1. Go to **[Comm.]** then **[Ethernet]**.
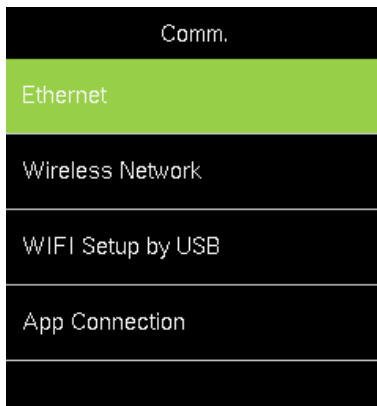
2. Set Ethernet parameters.

- **Enable DHCP:** Dynamic Host Configuration Protocol, which is used to allocate dynamic IP addresses to clients by a server.
- **IP Address:** Modify if necessary. It cannot be the same with PC.
- **Subnet Mask:** Modify it if necessary.
- **Gateway:** It is necessary to set an address if the device and PC are in different network segment. Modify if necessary.

6.2   Manual Wi-Fi Configuration

6.2.1   Connection to an Existing Wi-Fi

The steps to connect to Wi-Fi is given below:

1. Go to **[Comm.]** then **[Wireless Network]**.

2. The list of available Wi-Fi connections will be displayed as shown below:
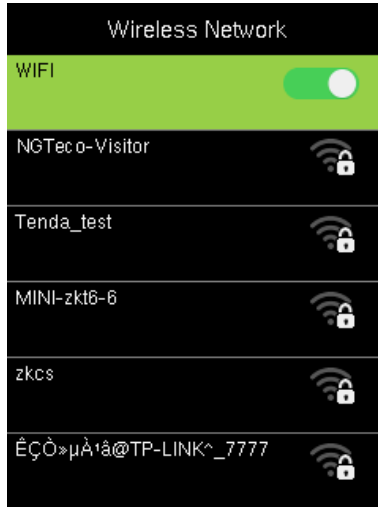
3. Navigate to the required Wi-Fi connection and press **<M/OK>**.

4. The interface to connect Wi-Fi will be displayed as shown below. If the signal strength is weak, the device may fail to connect.
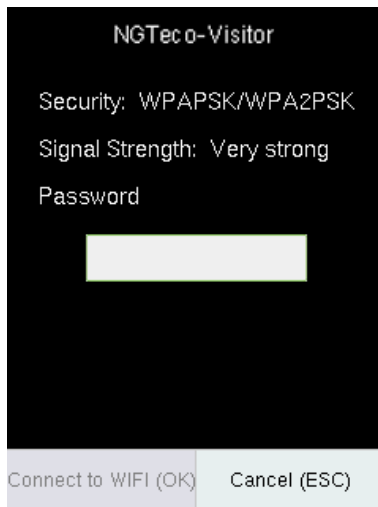
5. Navigate to **[Password]** and enter the password to connect.

6. Then navigate to **[Connect to WIFI (OK)]** and press **<M/OK>**.

7. Once connected, the connectivity status will be displayed as shown below:
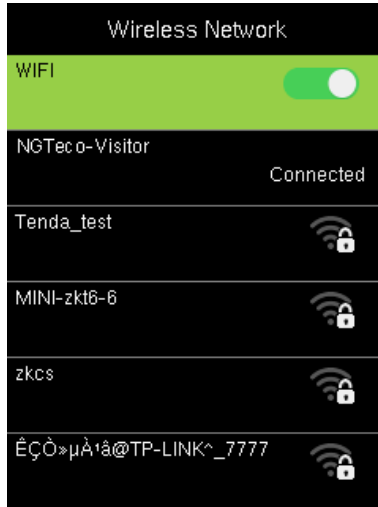
If the special symbol is set as the Wi-Fi password, only these are supported:

0. ,	9. #	18. {	27. &
1. .	10. *	19. }	28. _
2. ;	11. +	20. <	29. |
3. :	12. -	21. >	30. $
4. /	13. =	22. ~	31. (Space symbol)
5. ?	14. (	23. "	32. ^
6. !	15.)	24. `	
7. %	16. [	25. \	
8. @	17.]	26. '	

Note:

1. Device Wi-Fi only supports 2.4GHz communication.

2. It is recommended that you connect your device within approximately 15 metres of 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

To add a new Wi-Fi connection, perform the following steps:

1.   Go to **[Comm.]** then **[Wireless Network]**.

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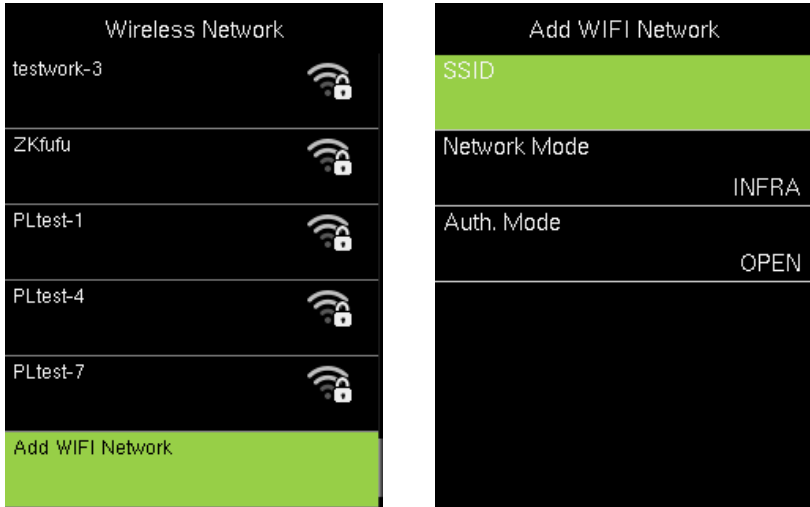
3.   Press Add Wi-Fi Network to add the Wi-Fi manually.

4.   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 <u>here</u> to view the process to search the Wi-Fi network.

6.2.3   Enable/Disable DHCP

To enable/disable DHCP, perform the following steps:

1.   Go to **[Comm.]** then **[Wireless Network]**.

2.   Press **[Advanced]** to view the DHCP settings.

3.   Turn on DHCP if unable to connect to WI-FI.
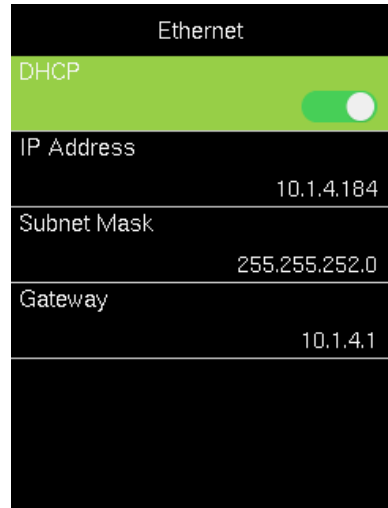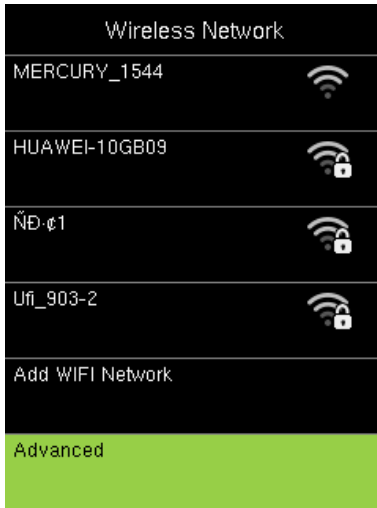
4. If you disable DHCP, you must manually set the IP Address, Subnet mask, and Gateway by pressing < ▼ >. The interface is shown below:
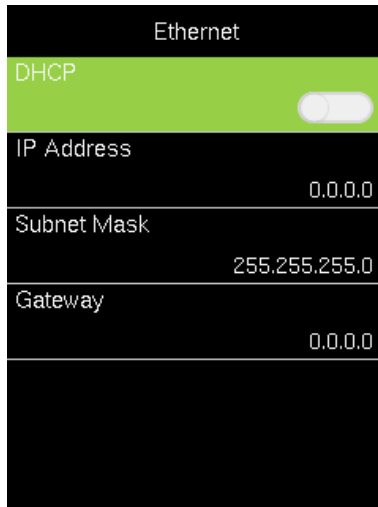
6.3   Wi-Fi Configuration through USB

You can also configure Wi-Fi through the Wi-Fi configuration template uploaded from a USB disk.

To configure Wi-Fi through a USB disk, perform the following steps:

1.   Go to **[Comm.]** then **[Wi-Fi Setup by USB]**.
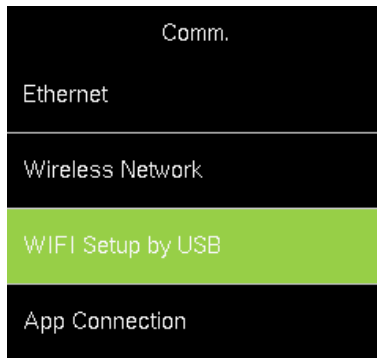
2.   The interface to download the template will be displayed as shown below:
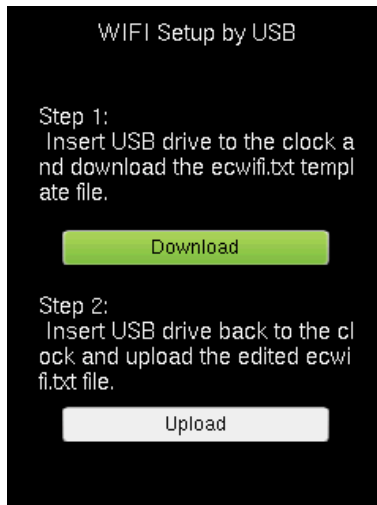
3.   Insert a USB drive into the device.

4.   Navigate to **[Download]** and press **<M/OK>**.

5.   After downloading the template, a success message will be displayed as shown below:

6.   Now, insert the USB drive into your PC. The Wi-Fi configuration file will be downloaded as shown below:

7.   Modify the template file by entering the SSID and Password.
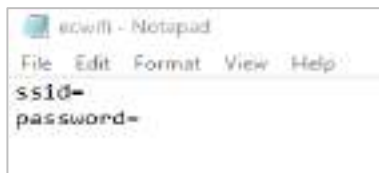
8.   Save the file and again insert the USB drive to the device.

9.   Go to **[Comm.]** then **[Wi-Fi Setup by USB]**.

10.   Then select **[Upload]**.

11.   The device will be connected to the configured Wi-Fi with the uploaded SSID and Password.

6.4   App Connection

Go to **[Comm.]** and then **[App Connection]** to view the QR code.
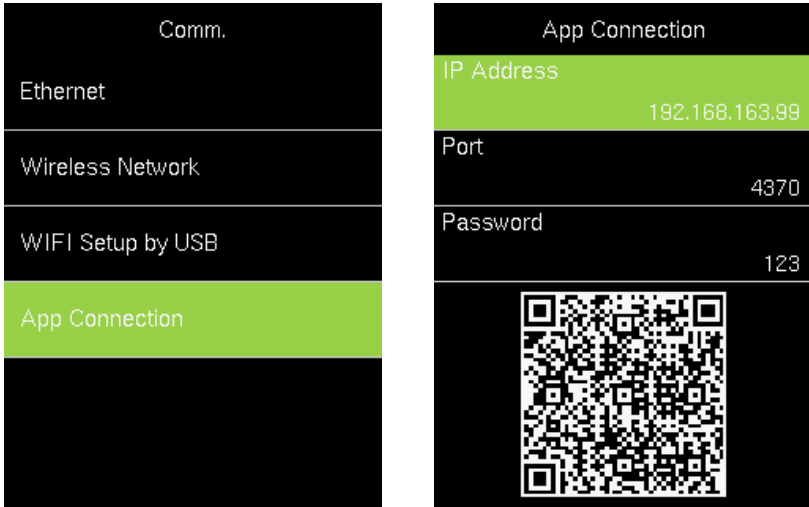
- **IP Address:** IP Address of the device.
- **Port:** The Port number of the device.
- **Password:** Password to connect to the NGTeco Time app.

Note: The device must be connected to Wi-Fi or the Ethernet successfully, otherwise the QR code will not be displayed.

The process in detail refers to **14 Connect to NGTeco Time App**.

7   <u>System</u>

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

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:

1. Go to **[System]** and press **<M/OK>**.
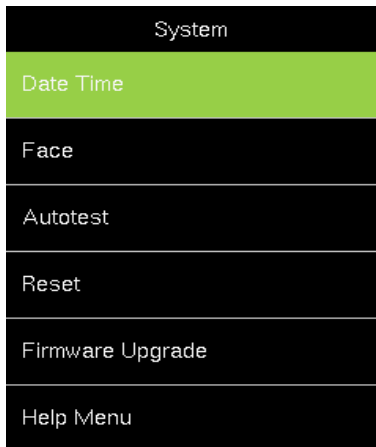
2. Then go to **[Date Time]** and press **<M/OK>**. The interface appears as shown below:

P a g e | 45
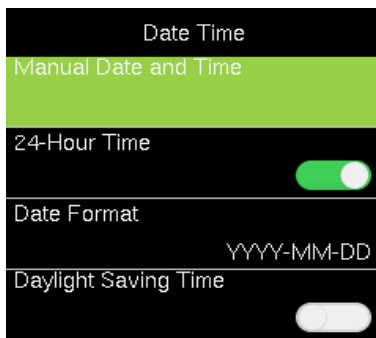
The following are the required parameters to set the date and time.

- **Manual Data and Time:** Set date and time of the device.
- **24-Hour Time:** Select whether to use the 24-hour display mode. If not, the 12-hour display mode is adopted.
- **Date Format:** Set the Date Format from the available options using <▲> or <▼> key.
- **Daylight Saving:** Enable or Disable the Daylight Saving using **<M/OK>** key.

After setting the parameters press **<M/OK>** to save the date and time.

7.2   Face Parameters

1. Go to **[System]** and press **<M/OK>**.
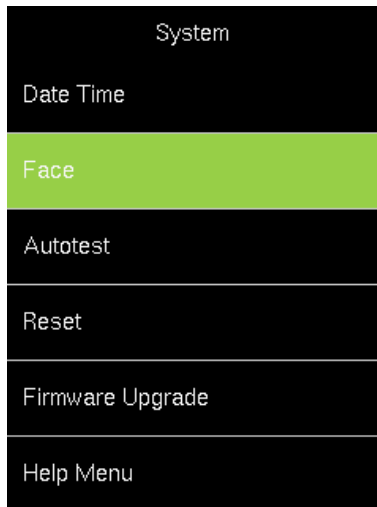
2. Then go to **[Face]** and press **<M/OK>**. The interface appears as shown below:

Face		Face	
1:N Threshold Value	47	Minimum Face Size	80
1:1 Threshold Value	63	LED Light Trigger Value	80
Face Enrollment Threshold	70	Motion Detection Sensitivity	4
Face Pitch Angle	30	Live Detection	
Face Rotation Angle	25	Live Detection Threshold	70
Image Quality	70	Anti-spoofing using NIR	

Face	
Motion Detection Sensitivity	4
Live Detection	
Live Detection Threshold	70
Anti-spoofing using NIR	
Anti-flicker Mode	50HZ
Face Algorithm	

The following are the required parameters to set the Fingerprint.

- **1:N Threshold Value:** Under 1:N verification mode, the verification will only be successful when the similarity between the acquired facial image and all registered facial templates is greater than the set value. The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgment rate, the

higher the rejection rate, and vice versa. It is recommended to set the default value of 47.

- **1:1 Threshold Value:** The recognition rate of mask wearing under the setting of 1:N verification mode. The higher the thresholds, the lower the misjudgment rate, the higher the rejection rate, and vice versa. It is recommended to set the default value of 63.

- **Face Enrollment Threshold:** 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.

- **Face Pitch Angle:** The pitch angle tolerance of a face for facial registration and comparison. If a face's pitch angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.

- **Face Rotation Angle:** The rotation angle tolerance of a face for facial template registration and comparison. If a face's rotation angle exceeds this set value, it will be filtered by the algorithm, i.e. ignored by the terminal thus no registration and comparison interface will be triggered.

- **Image Quality:** Image quality for facial registration and comparison. The higher the value, the clearer the image requires.

- **Minimum Face Size:** Required for facial registration and comparison. If 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.

- **LED Light Triggered Value:** This value controls the on and off of the LED light. The larger the value, the more frequently the LED light will be turned on.

- **Motion Detection Sensitivity:** 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.

- **Live Detection:** 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.

- **Live Detection Threshold:** 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.

- **Anti-spoofing using NIR:** Using near-infrared spectra imaging to identify and prevent fake photos and videos attack.

- **Anti-flick Mode:** Used when WDR is turned off. This helps reduce flicker when the device's screen flashes at the same frequency as the light.

7.3   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.

1. Go to **[System]** and press **<M/OK>**.
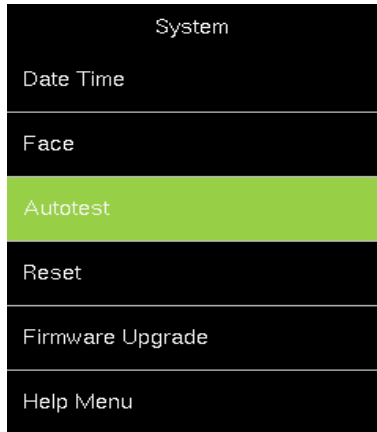
2. Then go to **[Auotest]** and press **<M/OK>**. The interface appears as shown below:
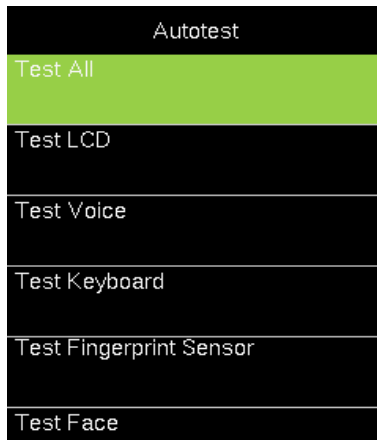
- **Test All:** The device automatically tests the LCD, Voice, Keyboard, Face, Fingerprint and Clock RTC, press **<M/OK>** to continue and press **<ESC>** to exit.

- **Test LCD:** 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.

- **Test Voice:** The device automatically tests whether the voice files stored in the device are complete and the voice quality is good.

- **Test Keyboard:** Checks if the keyboard is available.

- **Test Fingerprint Sensor:** To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen.

- **Test Face:** To test if the camera functions properly by checking the pictures taken to see if they are clear enough.

- **Test Clock RTC:** Checks if the RTC (Real-Time Clock) is accurate.

7.4   Reset

The menu is used to reset the Communication settings, System settings, etc.

1. If you need to reset the device, please enter **[System]**, select **[Reset]**, and press **<M/OK>**.
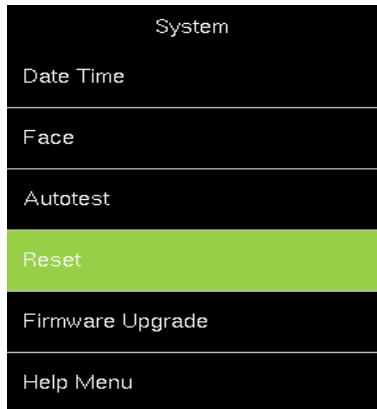
2.   An alert will be displayed as shown below:
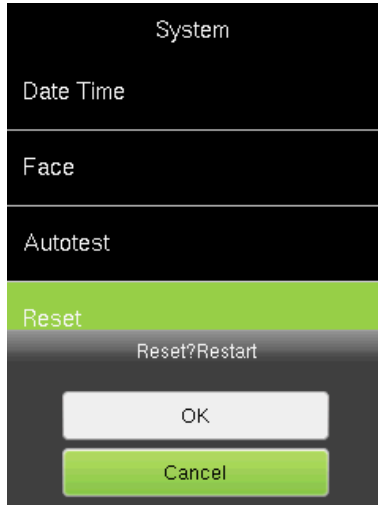
7.5   Firmware Upgrade

The firmware program of device can be updated with upgrade package in USB disk. You are not suggested to upgrade the firmware by yourself. If you need the upgrade file, please contact our technical support personnel.
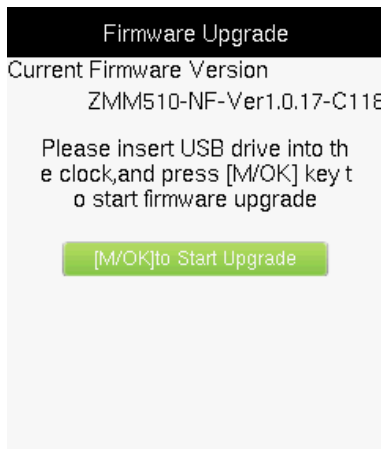
7.6   Help

You can contact us for any queries related to the working of the device. Go to **[System]** and then **[Help]**.

8   Pay Period

A pay period is a length of time over which the user's attendance time is recorded and paid. It is a recurring time schedule that determines how often the users will be paid. The pay period ensures that the users will be paid regularly for their work. It also simplifies the reporting requirements for employer liabilities.

The types of pay periods adopted in this deive are:

- Weekly Pay Period
- Bi-Weekly Pay Period
- Semi-Monthly Pay Period
- Monthly Pay Period

8.1 Weekly Pay Period

A weekly pay period consists of 52 pay periods in a year, one week of each. The payroll is scheduled to run on the same day every week.

Perform the following steps to set the Weekly Pay Period:

1. Go to **[Pay Period]**.
2. Press <**M/OK>** to view the available pay period options.
3. Select **[Weekly Pay Period]**.
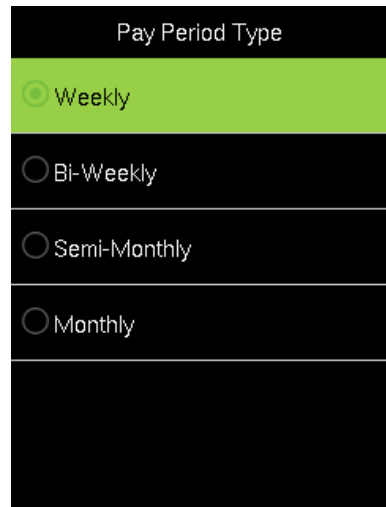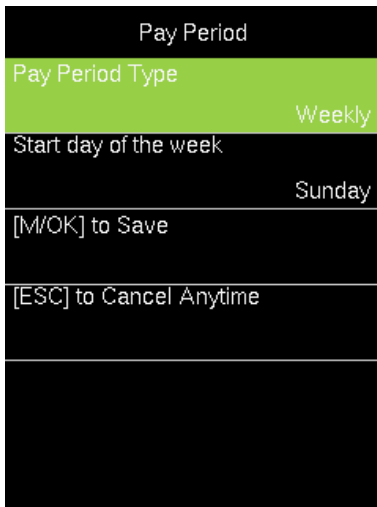
- **Start day of the Week:** It means that the start of the week is counted from this day.
4. Then press **<▾>** to navigate and set the starting day of the week.
5. Then navigate to **[M/OK to Save]** and press **<M/OK>**.

8.2 Bi-Weekly Pay Period

A bi-weekly pay period consists of 26 pay periods in a year (2 weeks or 14 days). Like the weekly pay period, a bi-weekly pay period also starts on the known day of a week.

Perform the following steps to set the Bi-Weekly Pay Period:

1. Go to **[Pay Period]**.

2. Press <**M/OK>** to view the available pay period options.

3. Select **[Bi-Weekly Pay Period]**.

- **Start day of the Week:** It means that the start of the week is counted from this day.

- **Pay period effective start date:** This date is bi-weekly pay start day.

4. Then press **<▼>** to navigate and set the effective starting date of the pay period.

5. Press **<▼>** to select the start day of the week.

6. Then navigate to **[M/OK to Save]** and press **<M/OK>**.

8.3   Semi-Monthly Pay Period

A semi-monthly pay period consists of 24 pay periods in a year. Each month will have exactly 2 pay periods. By default, the first pay period runs from the 1st-15th date of the month and the second pay period runs from 16th to the last date of the month. (Note: The start day of Semi-month may vary for each company)

Perform the following steps to set the Semi-Monthly Pay Period:

1.   Go to **[Pay Period]**.

2.   Press <**M/OK>** to view the available pay period options.

3.   Select **[Semi-Monthly Pay Period]**.

- **Start date of first half month:** The first half of the month is calculated from this day.

- **Start date of second half month:** The second half of the month starts from this day.

- **Start day of the week:** It means that the start of the week is counted from this day.

4.   Then, press **<▼>** to navigate and set the start day of the first and second half of the month.

5.   Then, press **<▼>** to navigate and set the start day of the week.

6.   Navigate to **[M/OK to Save]** and press **<M/OK>**.

8.4   Monthly Pay Period

The payroll runs on the same date of every month.

Perform the following steps to set the Monthly Pay Period:

1. Go to **[Pay Period]**.
2. Press <**M/OK>** to view the available pay period options.
3. Select **[Monthly Pay Period]**.

- **Start date of the month:** The beginning of each month is calculated from this day.
- **Start day of the week:** It means that the start of the week is counted from this day.
4. Then, press <▾> to navigate and set the start day of the month.
5. Then, press <▾> to navigate and set the start day of the week.
6. Navigate to **[M/OK to Save]** and press **<M/OK>**.

9   Data Management

Data Management is an administrative process that includes acquiring, validating, and processing the required data to ensure the smooth functioning of the device.
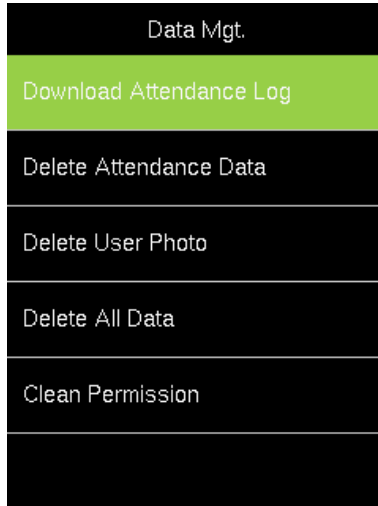
9.1   Attendance Log Management

Attendance logs are usually updated in the attendance software for further processing.

9.1.1   Download Attendance Logs

Perform the following steps to download the attendance logs:

1.   Insert the USB drive into the device
2.   Go to **[Data]** and then **[Download Attendance Log]**.
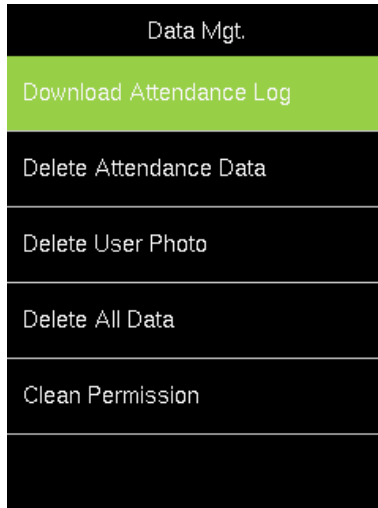
3. After downloading the attendance logs, a success message will be displayed as shown below:

4. Now, insert the USB drive to your PC and upload the logs to the attendance software.

5. The downloaded file on the USB drive will be named **AttendanceLogxxxx.dat** as below. You can open it with a text editor to view the attendance data.

9.1.2   Delete Attendance Data

Perform the following steps to delete the attendance data:

1.   Go to **[Data]** then **[Delete Attendance Data]**.
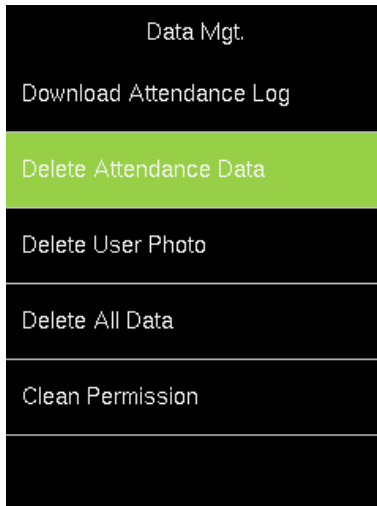
2. An alert will be displayed as shown below:

3. Press **<M/OK>** to delete all the attendance data.

9.2 Delete User Photo

Perform the following steps to delete user photo:

1. Go to **[Data]** then **[Delete User Photo]**.
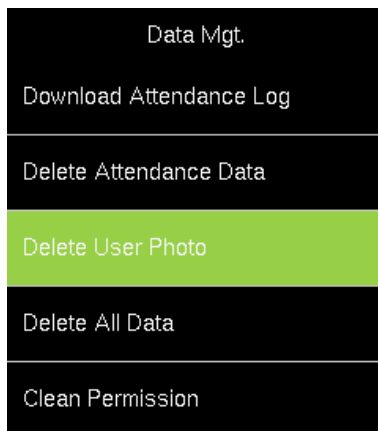
2.   An alert will be displayed as shown below:
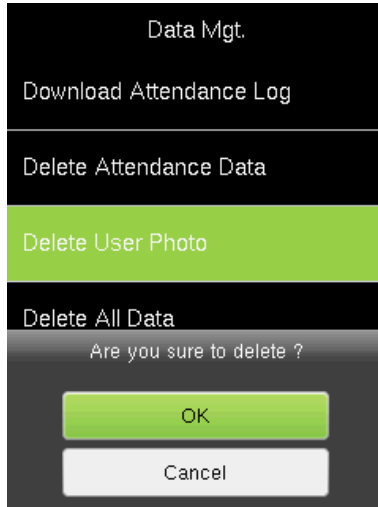
3.   Press **<M/OK**> to delete user photo.

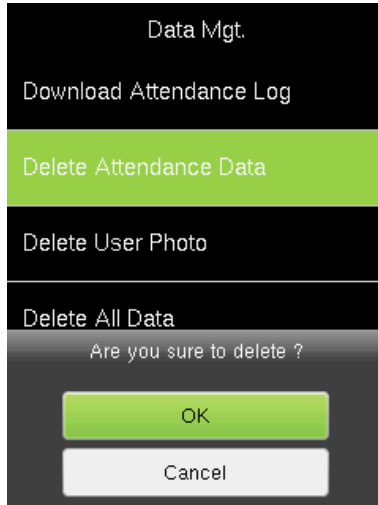# 9.3   Delete All Data

Perform the following steps to delete all the data:

1.   Go to **[Data]** then **[Delete All Data]**.
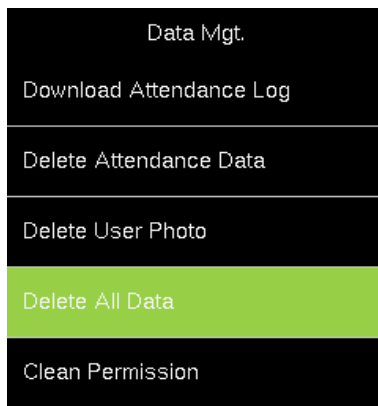
2. An alert will be displayed as shown below:
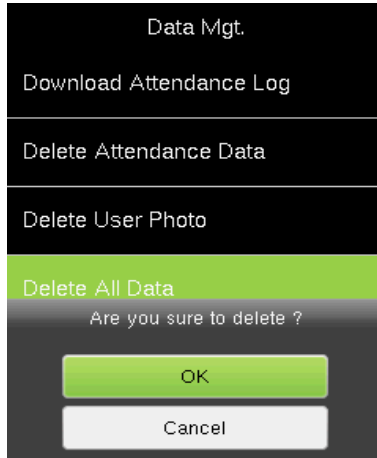
3. Press **<M/OK>** to delete all the data.

If you are sure to Delete All Data, all the information in the device will be deleted.

9.4 Clear Admin Privileges

You can reset the Admin privileges, and this can be done at a single instance instead of doing one by one. The procedure is given below:

1. Go to **[Data]** then **[Clear Permission].**
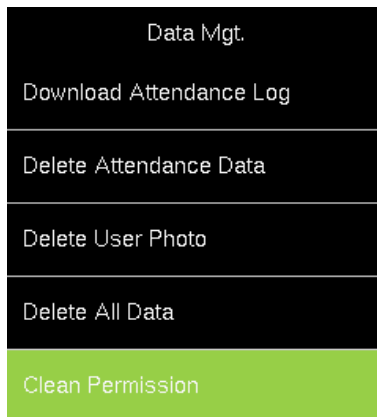
2.   An alert will be displayed as shown below:
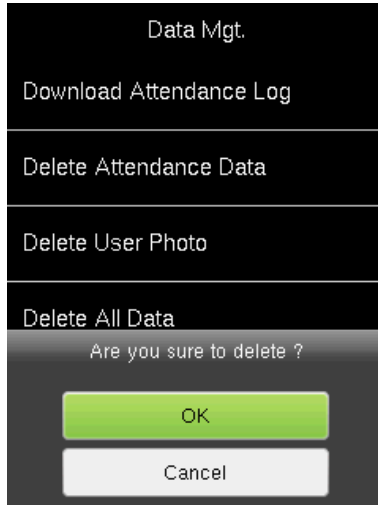
3.   Press **<M/OK>** if you want to reset the Admin Privileges.

10   Attendance Management
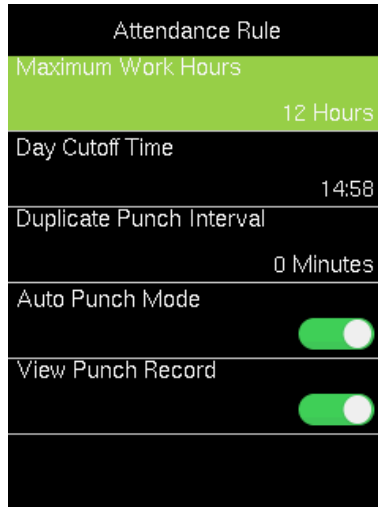
The device automates and provides a simple way to record the attendance of users with Face/Fingerprint/Card Number★/Password verification. It also assists the employer to track the user's attendance analytics such as work hours, absenteeism, missing attendance punches, etc. This automated device greatly reduces the computational errors and transcriptional errors thus facilitating hassle-free attendance calculation.

10.1   Attendance Rules

Attendance Rules are a predefined set of specifications framed to maintain clear and consistent attendance management of the users.

The procedure to set the attendance rules is given below:

1.   Go to **[Rule]**.

2.   The interface to set the attendance rules will be displayed as shown below:

3. Enter the following details:

- **Maximum Work Hours:** Set the maximum number of working hours in a day. When the time difference between two attendance punches (check-in and check-out) exceeds this maximum work hour, then the attendance will be calculated separately for that day. Then you can identify that there are missing attendance punches between the actual punches made by the users. The default value is 12 hours.

- **Day Cutoff Time:** Set the time on which the day is changed to the next day on the device.

    Example: Consider the day change time is set to 2:00 AM. If the users start to work before 2:00 AM, then the total worked hours until check-out will be added to the previous day. If the users start to work after 2:00 AM, then the total worked hours until check-out will be added to the next day.

- **Duplicate Punch Interval:** The Duplicate Punch interval defines the time duration in which the device considers only the first attendance punch, even if you make many attendance punches within the defined period. The unit is minutes.

Example: Assume that the duplicate punch period is 5 minutes. If you make several check-in attendance punches within 5 minutes, the device considers only the first punch time and ignores the rest of the attendance punches.

- **Auto Punch Mode:** When this feature is enabled, the punch state will not be displayed on the home screen and the punch state will be updated automatically based on the previous punch state of the user. For example, if the user's first punch state is Check-in, then the next punch state is Check-out. This feature is enabled by default.

  Note: When the time exceeds the Day Cutoff Time, the punch state will be reset to Check-in.

  If the Auto Punch Mode is turned off, the user needs to select the punch state manually and the punch state will be displayed on the home screen. Press the ⊙ /< button to change the punch state to IN, and the <M/OK> button to change the punch state to OUT. The punch state is Check-in by default and if the user presses the <M/OK> button the state will change to Check-out for five seconds. Then, the state will be auto-changed to Check-in.

- **View Punch Record:** When this option is turned on, the users can view their attendance records by themselves.

  If the View Punch Record is turned off, the users cannot view the attendance records.

11   Attendance Tracking

You can track and monitor the user's attendance to ensure productivity and workflow during working hours.

11.1   Every Day's Attendance

The device is equipped with a provision to view the daily attendance of users. The steps to view the daily attendance is given below:

1. Go to **[Time Data]** and then **[Today's Record]**.
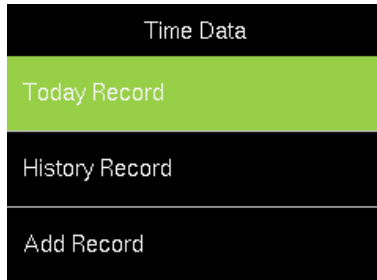
2. The attendance details of the day will be displayed as shown below:

3. The columns are described as follows:

- **Name:** Displays the Name of the users.
- **Time:** Displays the time when the attendance punch is made.
- **State:** Displays the state of the attendance punch (check-in/check-out).
- **Verify:** Displays the Users verification mode.

11.2   Attendance of Individual Users

The device has a provision to track the attendance of individual users to ensure all users are fulfilling their obligations. It also helps the Management to identify the potential attendance issues. The steps to track the attendance of individual users are given below:

1.   Go to **[Time Data]** and then **[History Record]**.
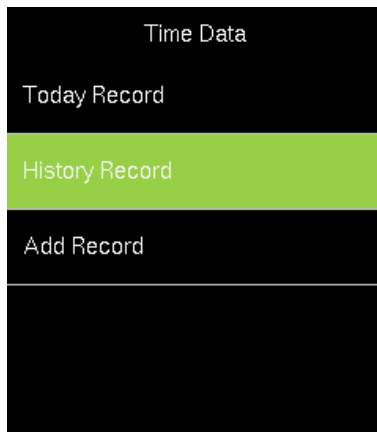
2.   The list of users will be displayed as shown below:

3.   To select a user, and press **<M/OK>**.

4.   The attendance of the selected users will be displayed as shown below:

11.3   Add Missing Attendance Punch

When a user forgets to punch for check-in/check-out, the attendance details can be logged in manually. The steps to add manual logs is given below:

1.   Go to **[Time Data]** and then **[Add Record]**.
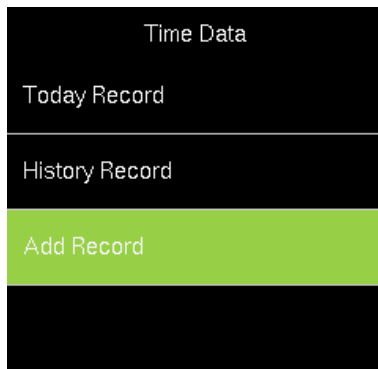
2. The interface to select users will be displayed.
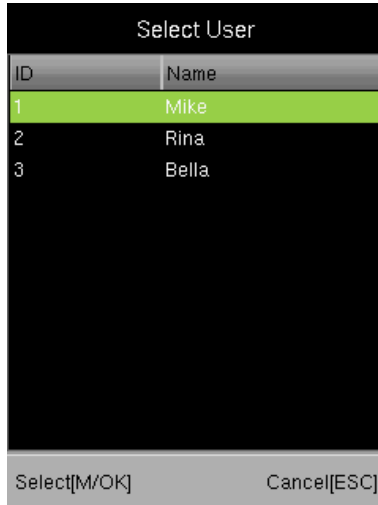
3. The interface to add the missing punches will be displayed as shown below:
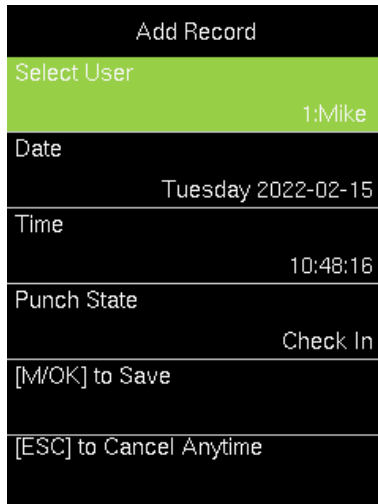
4. **Date:** Enter the date on which you must add the missing attendance punch by navigating to Month, Date, and Year text boxes by pressing <▲> or <▼> key.

5. **Time:** Enter the Time by navigating to Hour and Minute text boxes by pressing <▲> or <▼> key. If the time format is 12-hours, then select **[AM/PM]** by pressing <▲> or <▼> key.

6. Select the attendance state as Check-in/Check-out by pressing <▲> or <▼> key.

7. Navigate to **[M/OK to Save]** and press **<M/OK>**.

Note: Check-in and check-out information cannot be deleted from the device, but administrators can use the edit check-in/check-out function in the NGTeco Time app. For details, see **Edit Punch**.

12 Time-Attendance Reports

You can generate statistical reports that display the attendance details of the users in the specified pay period. The difficulty of maintaining the user's time and attendance is lessened with this simple reporting system. The data generated from these attendance reports assist with efficient management of user's resources and report accuracy.

12.1 Report Parameters

The procedure to set the report parameters is given below:

Go to **[Time Report]**. The interface to generate reports will be displayed as shown below:
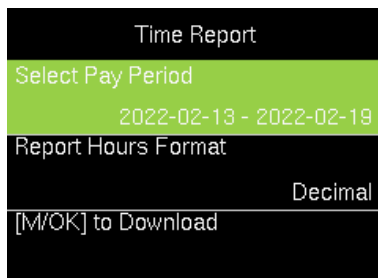
- **Select Pay Period:** The available pay period options are the **Current Pay Period** and **Custom Pay Period**. You can also select the date range of the pay period

which is currently being used. In the Custom Pay period, you can define the date

range within 31 days.

- **Report Hours Format:** Select the report hours format.

The Start and End dates are predefined based on the selected pay periods except for the

Custom Pay period.

12.2   Download Reports

1. Insert a USB drive to download the report.

2. Navigate to **M/OK to Download]** and press **<M/OK>**.

3. After downloading the report, the success message will be displayed as shown below:

4. Now insert the USB drive into your PC to view the reports.

5. The report will be downloaded by the name of date and time as shown below:

6. The report will be displayed as shown below:

	A	B	C	D	E	F	G
43	**Pay Period**			01/01/2020-01/30/2020			
44	**Employee**			Jjmtj Tmjtm (3)			
45	**Date**		**IN**	**OUT**	**Work Time**	**Daily Total**	**Note**
46	WED	01/01/2020	01:53 PM	03:55 PM	02:01	02:01	
47	THU	01/02/2020					
48	FRI	01/03/2020					
49	SAT	01/04/2020					
50	SUN	01/05/2020					
51	MON	01/06/2020	10:45 AM	11:45 AM	01:00	01:00	
52	TUE	01/07/2020	10:26 AM	11:31 AM	01:05	01:05	
53	WED	01/08/2020	11:01 AM	11:15 AM	00:14	00:14	
54	THU	01/09/2020	03:36 PM	05:36 PM	02:00	02:00	
55	FRI	01/10/2020					
56	SAT	01/11/2020	05:54 PM	09:57 PM	04:03	04:03	
57	SUN	01/12/2020	07:59 AM	10:02 AM	02:03	02:03	
58	MON	01/13/2020	02:03 AM	09:07 AM	07:03	07:03	
59	TUE	01/14/2020	09:07 AM	11:11 AM	02:04	02:04	
60	WED	01/15/2020	02:12 AM	10:16 AM	08:03	08:03	
61	THU	01/16/2020					
62	FRI	01/17/2020					
63	SAT	01/18/2020	01:27 AM	10:27 AM	09:00	09:00	
64	SUN	01/19/2020					
65	MON	01/20/2020					
66	TUE	01/21/2020					
67	WED	01/22/2020					
68	THU	01/23/2020					
69	FRI	01/24/2020					
70	SAT	01/25/2020					
71	SUN	01/26/2020					
72	MON	01/27/2020					
73	TUE	01/28/2020					
74	WED	01/29/2020					
75	THU	01/30/2020					
76	**Total Hours**					38:40	

7. The report consists of the specific Pay period, Name of the employee, Date-wise check-in and check-out time, actual work time, and total worked time.

8. The report uses the nearest rule calculation. For example, if the punch states are IN, IN, and OUT for the same user, the device will match the second IN and OUT and the report displays Missing OUT for the first IN.

ID	Name	Date	IN	OUT	Work Time	Note
999	wang1 wu	01-20-2021	06:01 AM			Missing OUT
999	wang1 wu	01-21-2021	05:51 AM	06:22 AM	0.51	

9. If the time interval between the IN and OUT states is more than the maximum work hours, then the report will show Missing IN and Missing OUT.

13 System Info

You can check the storage status as well as the firmware information of the device through the **[System Info]** option.

Go to **[System Info]** and press **<M/OK>**.
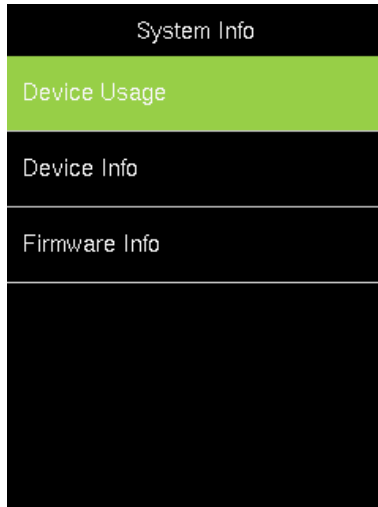
Select the specific option to check the parameters:

- **Device Usage:** Displays the Number of users, Admin users, Password, Fingerprint, Face, Card ★ and Attendance record.
- **Device Info (Information):** Displays the Device name, Serial number, MAC address, Fingerprint algorithm, Face algorithm, Platform information, MCU version, Manufacturer and Manufacturer date.
- **Firmware Info:** Displays the Firmware version and other version information of the device.

14   Connect to NGTeco Time App

The App Connection interface allows you to connect the NGTeco Time Mobile app with the device. Once connected, you can perform User management, Report management, etc. on the Mobile app. The process is as follows:
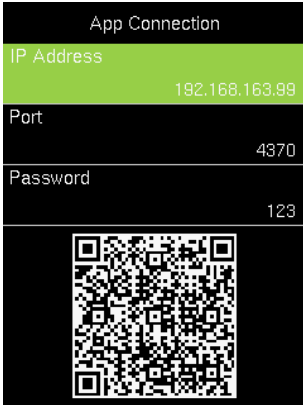
1. Download and install the NGTeco Time App on your phone.
2. Connect the mobile and device to the same Wi-Fi network.
3. Select **[Comm.]** and then **[App Connection]** to view the QR code.
4. Enter the Password and Confirm.

1. Open the NGTeco Time App and press [icon] to scan the QR code from the device.
2. After a successful connection, you can set the device parameters from your mobile.

14.1 Register Users from App

1. Go to **Users** menu.
2. Click the **Add User** icon to add a **New user**.
3. The User ID can be auto generated or manually assigned.
4. Enter the First Name, Last Name and Password.
5. Set the permission.
6. Click **Save & Sync** to sync the user details to thedevice.
7. Open the User List on the device to enroll user's verification modes.

14.2 Attendance

View Attendance Record

1. Go to **Attendance** menu.
2. Select **View User's Attendance Record**. You can also select the date.

Add Missing Punch from App

1. Go to **Attendance** menu.
2. Click the **Add Punch** icon.
3. Select the user to add the missing check-in/out.
4. Select the Punch Date and Time.
5. Select the Punch State.
6. Click **Save & Sync** to sync the attendance details to the device.

Edit Punch

1. Go to **Attendance** menu.
2. Select the user record you want to edit, and click the **Edit Punch** icon.
3. Select the Punch Date and Time.
4. Select the Punch State.
5. Click **Save & Sync** to sync the attendance details to the device.

14.3   Download Time Report from App
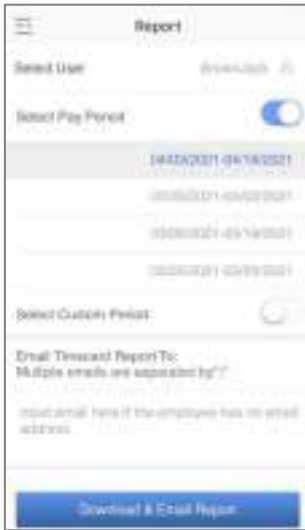
1. Go to **Report** menu.
2. Select a user or all the users.
3. Select the specific **Pay Period**.
4. Or, select **Custom Period** and set a date range within 31 days.
5. Enter the email addresses.
6. Click **Download & Email Report** to generate the time report.

Note: Connection to a computer and remote download of reports is not supported.

14.4   Setup Pay Period and Attendance Rule from App

1. Go to **Setup** menu.
2. Set the **Pay Period**.
3. Set the **Start Day of the Week**.
4. Set the **Day Cutoff Time**.
5. Set the **Duplicate Punch Interval**.
6. Set the **Maximum Work Hours**.
7. Set the Time format for report generation. Click **Save & Sync** to sync the settings to the device.

15 Troubleshooting

Category	Issue	Quick fix
Power	The device does not operate after the power is supplied	• Check the Power Cable for any damages.
PIN	I lost my PIN	• Contact the Administrator to change the PIN. • If you have lost the Admin PIN, contact the supplier.
Fingerprint	The enrolled fingerprint could not be authenticated	• Place the finger in a proper position. • Make sure your finger is free from cuts and stains. If the registered finger has such flaws, enroll another finger.
Admin	I lost my Admin credentials	• Contact another Admin to reset your credentials. • Contact the supplier for further proceedings.

NGTeco

Website: www.ngteco.com

Email: ngtime@ngteco.com

Phone: (770) 800-2321

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