



TQ600F

Face Recognition Terminal
User Manual

Important Claim

Thank you for purchasing the TQ600F Face Recognition Terminal. Before installing your terminal please read this manual carefully to avoid damage to the unit! This manual provides information on the proper use of your terminal.

You may not distribute or change any content of this manual in part or in full without written consent from Acroprint Time Recorder Co.

Table of Contents

1. Instructions for Use	1
1.1 Standing Position, Posture and Face Expressions	1
1.2 Enrolling Face Expressions	1
1.3 Use of the Touch Screen	2
1.4 Touch Operations.....	2
1.5 Appearance of Device.....	4
1.6 Main Interface.....	5
1.7 Verification Modes	6
1.7.1 Face Verification.....	6
1.7.2 Password Verification.....	7
1.7.3 Proximity Badge Verification	7
1.7.4 Combination Verification	8
2. Main Menu.....	11
2.1 Accessing the Main Menu on a Terminal with an Administrator	12
2.1.1 Administrators with Face Enrollment.....	12
2.1.2 Administrators with Password Enrollment	12
2.1.3 Administrators with Proximity Badge Enrollment.....	12
3. Add User	13
3.1 Entering a User ID	13
3.2 Entering a Name.....	14
3.3 Enrolling a Password	14
3.4 Enrolling Proximity Badges.....	15
3.5 Enrolling a Face.....	15
3.6 Modifying User Rights.....	16
3.7 Enroll Photo	17
4. User Management	18
4.1 Edit a User.....	18
4.2 Delete a User.....	19
4.3 Query a User	19
5. Communication Settings	20

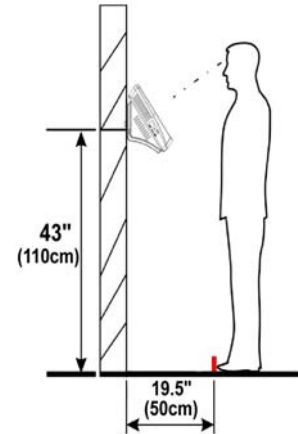
6. System Settings	21
6.1 General Parameters	21
6.2 Interface Parameters	21
6.3 Face Parameters	22
6.4 Log Settings.....	23
6.5 Shortcut Definitions.....	23
6.5.1 Set Shortcut Keys	23
6.5.2 How to Use the Workcode Shortcut Key	24
6.6 Update	25
7. Data Management	26
7.1 Query Record	26
7.2 SMS.....	27
7.2.1 Set a Short Message.....	27
7.2.2 View a Short Message	30
7.3 Work Code.....	31
7.3.1 Add a Work Code	31
7.3.2 Edit a Work Code Label	31
7.3.3 Delete a Work Code.....	31
8. Date/Time Setting	32
8.1 Set Date/Time.....	32
8.2 Bell Setting	32
8.3 Daylight Savings Time (DLST).....	33
9. Auto Test	35
10. USB Disk Management	36
11. System Information	37
12. Appendix	38
12.1 Entering Text Using the Keyboard	38
12.2 Photo ID Function.....	39
12.3 Multi-combination Authentication Mode	40

1. Instructions for Use

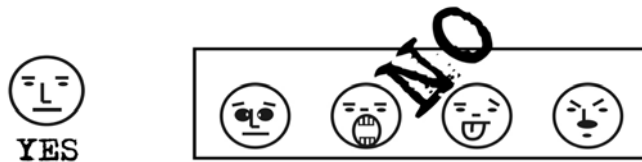
1.1 Standing Position, Posture and Face Expressions

1. Recommended standing-distance from device:

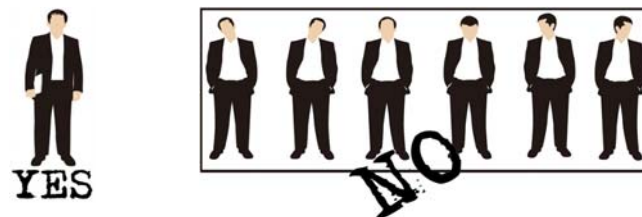
It is recommended that users 5-6 feet tall (1.55m-1.85m) stand about 2 feet (0.5m) from the wall. When viewing your image on the device display window, step away if your image appears too bright. Step closer if your image appears too dark.



2. Recommended face Expressions vs. Poor Expressions:



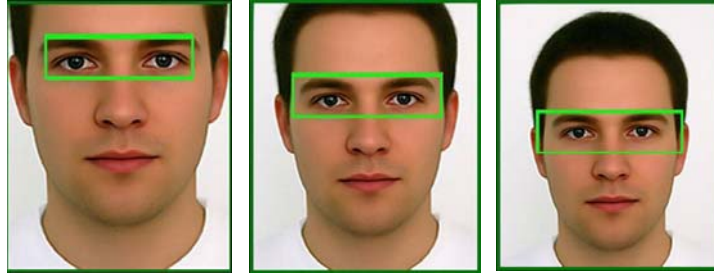
3. Recommended Posture (pose) vs. poor Posture (pose):



Note: During enrollment and verification, try to have a relaxed unstrained facial expression and stand upright.

1.2 Enrolling Face Expressions

During the enrollment, user should following the voice prompts "Focus eyes inside the green box" and position head so that his face appears in the center of the device display window. The user needs to move forward and backward to adjust the eyes position during the face registration. Use a "neutral" face expression when enrolling, i.e., do not frown or smile. Users that wear glasses should wear them during the enrollment. They will be able to "punch" with or without their glasses.



1.3 Use of the Touch Screen

Touch the screen with one of your fingertips or the edge of a fingernail, as shown in the following figure. A broad point of contact may lead to inaccurate pointing.

Note: A stylus has also been included to facilitate keyboard entry. The stylus telescopes to 3-1/2" by simultaneously pulling on both ends.



When the touch screen accuracy is off, you can perform a screen calibration through the following menu operations: Press **[Menu]** → **[Auto Test]** → **[Calibration]** on the screen and a cross icon will be displayed. After you touch the center of the cross at five locations on the screen correctly, the system will automatically return to the **Auto Test** menu. Press **[Exit]** to return to the **Menu** screen. For details, see [9. Auto Test](#). Smudges or dust on the touch screen may affect performance. Clean the screen as necessary.

1.4 Touch Operations

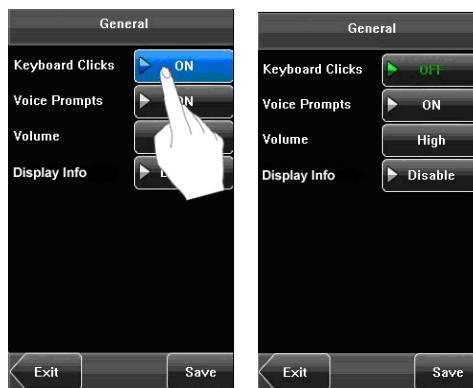
- **Enter numbers:** Press the **[User ID]** key. The system will automatically display the keypad screen. After entering the user ID, press **[OK]** to save or press **[X]** to cancel and return to the previous screen.



-
- **Enter Text:** Press the **[Name]** key. The system will automatically display the keyboard. After entering the user name, press **[X]** to save and return to the previous screen.

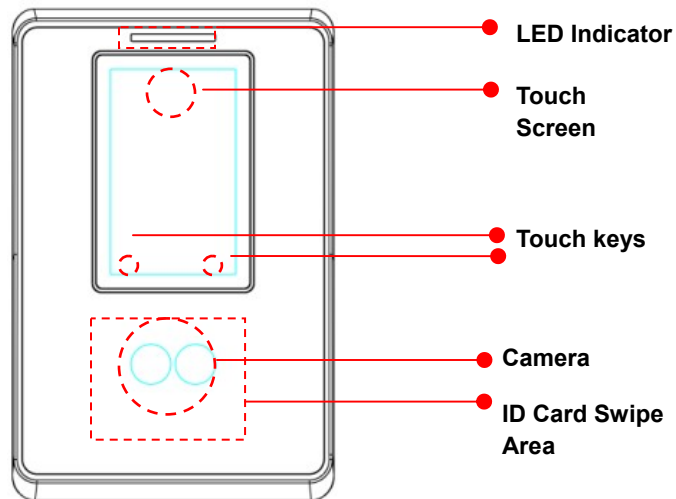


- **Modify parameters:** Press the default value of a parameter and the system will automatically switch to another value of this parameter.

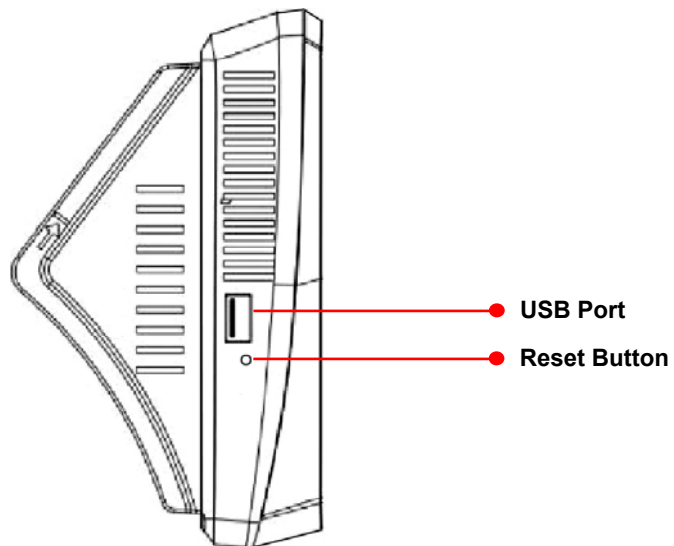


1.5 Appearance of Device

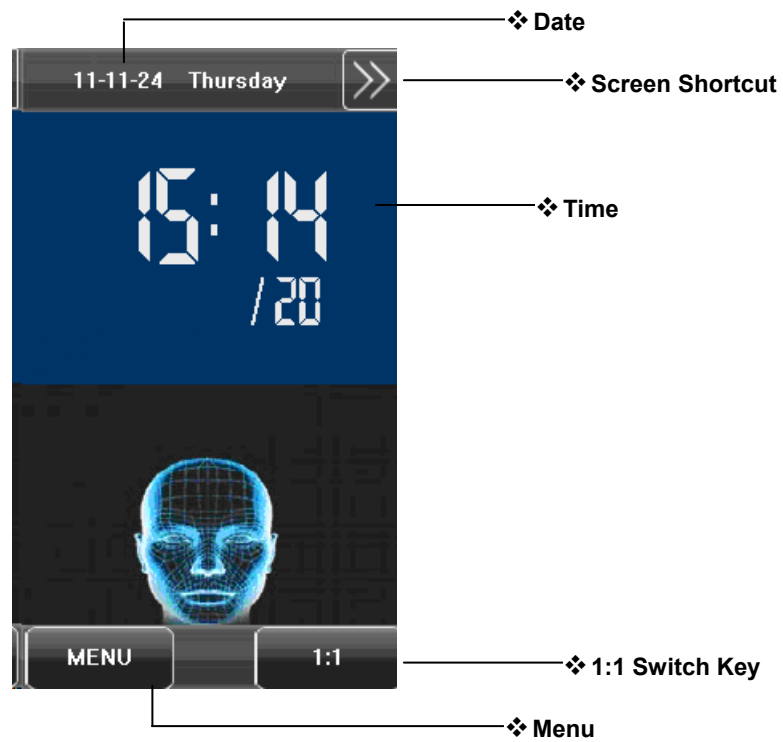
(1) Front View



(2) Side View



1.6 Main Interface



- **Date:** The current date is displayed.
- **Screen Shortcut Key:** Press the shortcut key to display the **WorkCode** button. For details, see [6.5 Shortcut Definitions](#).
- **Time:** The current time is displayed. Both 12-hour and 24-hour display formats are available.
- **1:1 Switch Key:** Switch to the 1:1 verification and display the keypad for user ID input.
- **Menu:** Display the Main Menu.

Note: **WorkCode** is currently the only supported shortcut function.

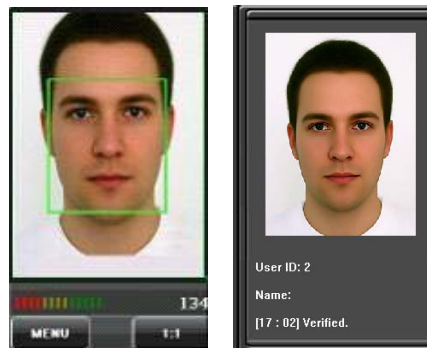
1.7 Verification Modes

1.7.1 Face Verification

1: N Face Verification

The terminal compares the current face template (image) with all face templates on the terminal.

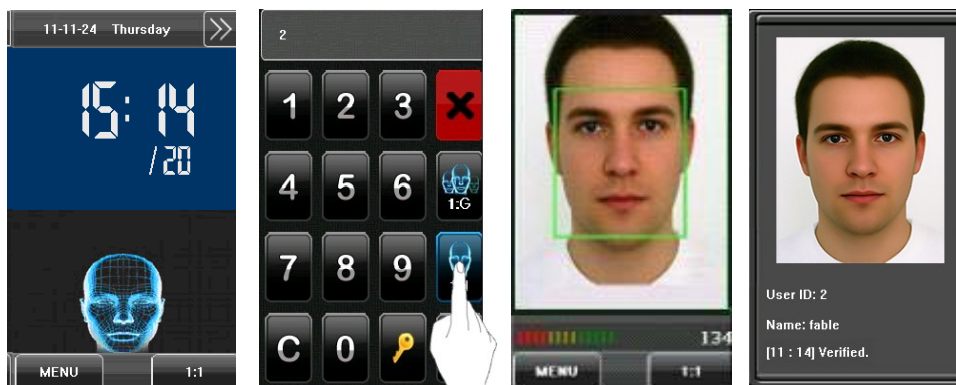
- Scan your face using the proper technique. For details, see [1.1 Standing Position, Posture and Face Expressions](#). Your image will appear on the display as shown by the figure on the left below.
- If your face template is matched to a template in the terminal, your face template will be displayed as shown by the figure on the right below.



1:1 Face Verification

In the 1:1 face verification mode, the device compares your face with the template stored for the user ID you entered. Use this mode when you are having difficulty verifying your identity. The terminal will only have to compare your face with one face template.

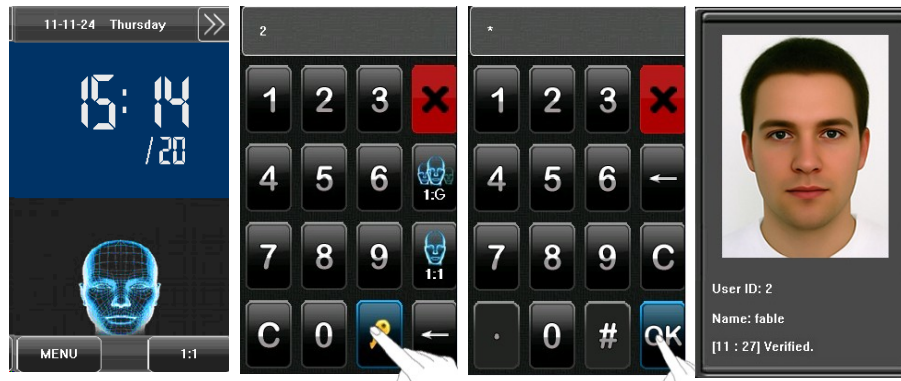
- Press **[1:1]** on the Main Interface screen to enter the 1:1 recognition mode.
- Enter your User ID, then press the **[1:1 Face]** icon to enter 1:1 face recognition mode. If the prompt "Not Registered!" is displayed, the user ID does not exist.
- Scan your face using the proper technique. For details, see [1.1 Standing Position, Posture and Face Expressions](#).
- If the verification is successful, the device will display "Verified". The system will return to the Main Interface if the verification is not made within 20 seconds.



1.7.2 Password Verification

In the password verification mode, the device compares the password entered with the password assigned to the user ID.

- Press [1:1] on the Main Interface to enter the 1:1 recognition mode.
- Enter the user ID and then press the "Key" icon to enter the password verification mode. If the prompt "Not Registered!" is displayed, the user ID does not exist.
- Enter the password and press the "OK" icon to start the password comparison.
- If the verification is successful, the device will display "Verified", otherwise the device will prompt "Verify fail" and return to password input screen.

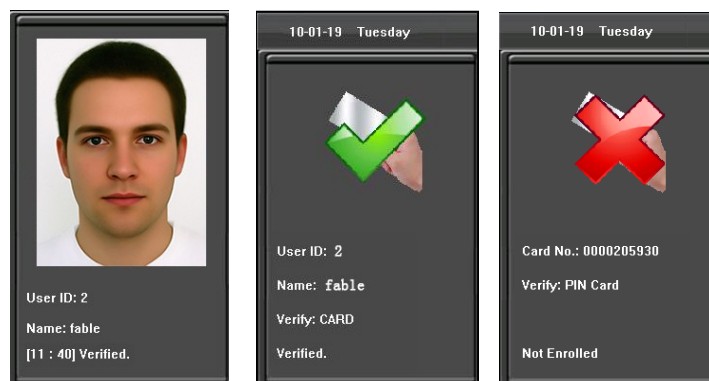


1.7.3 Proximity Badge Verification

The TQ600F supports the following proximity badge verification modes: **Badge Only**, **Badge + Facial Verification**, and **Badge + Password**.

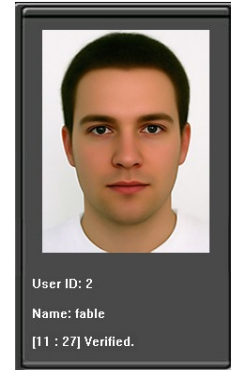
Badge Only

- Swipe your badge over the swipe area. For details on locating the swipe area, see [1.5 Appearance of Device](#).
- If the verification is successful, the device will display "Verified".
- If the verification is not successful, the device will display "Not Enrolled".



Badge + Facial Verification

- Swipe your badge over the swipe area to enter the 1:1 facial verification mode.
- Scan your face using the proper technique. For details, see [1.1 Standing Position, Posture and Face Expressions](#).
- If the verification is successful, an interface as shown in Figure 3 on the right will be displayed. The system will return to the Main Interface if the verification is not passed within 20 seconds.



Badge + Password Verification

- Swipe your badge over the swipe area.
- Enter password on key pad.

1.7.4 Combination Verification

The device supports up to 8 verification modes: FACE/RF/PW, FACE&PW, FACE&RF, PW, RF, FACE, PW/RF, PW&RF. For the detail, please refer to [12.3 Multi-combination Authentication Mode](#).

Note: RF means proximity badge verification.



FACE/RF/PW verification:

Users can punch in/out by scanning their face or by scanning their badge or by entering their pin# & password.

Face Verification: Scan your face using the proper technique. For details, see [1.1 Standing Position, Posture and Face Expressions](#). If the verification is successful, the display will show a punch in or out.

Badge Verification: Scan your badge. If the verification is successful, the display will show a punch in or out.

Password Verification: Press “1:1” on the Main Interface. Input your User ID (Pin#) & press the password button (the Key icon). Enter your password and press “OK”. If the verification is successful, the display will show a punch in or out.

FACE & PW verification:

Users can punch in/out by scanning their face. Once their face has been verified they are prompted to enter their password. Enter password and press “OK”. If the verification is successful, the display will show a punch in or out.

FACE & RF verification:

Users can punch in/out by scanning their face. Once their face has been verified they are prompted to scan their proximity badge. Scan badge. If the verification is successful, the display will show a punch in or out. Note that if a user attempts to punch using a different verification method such as PW they will receive a Verify Mode error even if they have a password saved in the terminal. Users can only use Face & proximity badge in this verification mode.

PW verification:

Users can punch in/out using their Pin# & Password. Press “1:1” on the Main Interface. Enter User ID (Pin#) and press the password button (Key icon). Enter password and press “OK”. If the verification is successful, the display will show a punch in or out. Note that if a user attempts to punch using a different verification method such as Face or RF they will receive a Verify Mode error even if they have a face template or proximity badge saved in the terminal. Users can only use password in this verification mode.

RF verification:

Users can punch in/out by scanning their proximity badge. Scan badge. If the verification is successful, the display will show a punch in or out. Note that if a user attempts to punch using a different verification method such as Face or PW they will receive a Verify Mode error even if they have a face template or password saved in the terminal. Users can only use a proximity badge in this verification mode.

FACE verification:

Users can punch in/out by scanning their face. Once their face has been verified, the display will show a punch in or out. Note that if a user attempts to punch using a different verification method such as PW or RF they will receive a Verify Mode error even if they have a password or badge saved in the terminal. Users can only use Face in this verification mode.

PW/RF verification:

Users can punch in/out using their Pin#/Password or proximity badge. Press “1:1” on the Main Interface. Enter User ID (Pin#) and press the password button (Key icon). Enter password and press “OK”. If the verification is successful, the display will show a punch in or out.

A user can also scan their proximity badge to punch. Note that if a user attempts to punch using a different verification method such as Face they will receive a Verify Mode error even if they have a face template saved in the terminal. Users can only use Pin#/Password or proximity badge in this verification mode.

PW & RF verification:

Users can punch in/out using their Pin#/Password and proximity badge. Press “1:1” on the Main Interface.

Users can punch using two different sequences:


Sequence #1: Scan proximity badge. Enter your password when prompted and press “OK”. If the verification is successful, the display will show a punch in or out.

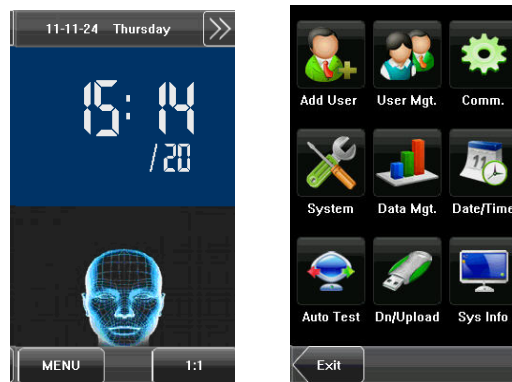
Sequence #2: Press “1:1” on the Main Interface. Enter User ID (Pin#) and press the password button (Key icon). Enter password and press “OK”. You are now prompted to scan your proximity badge. Scan your badge. If the verification is successful, the display will show a punch in or out. Note that if a user attempts to punch using a different verification method such as Face they will receive a Verify Mode error even if they have a face template saved in the terminal. Users can only use password & proximity badge in this verification mode.

2. Main Menu

There are two types of users: **Ordinary users** and **Administrators**. Ordinary users are only granted the rights of face, password or card verification, while administrators are granted access to the main menu in addition to the privileges granted to ordinary users.

Press **[Menu]** on the main screen to access the main menu, as shown in the figures below.

Note: If a lock icon  appears after pressing **[Menu]**, then one or more administrators exist on the device. An administrator will need to be successfully verified before the Menu options are displayed. For details on how a user is verified, see [1.7 Verification Modes](#).



The main menu includes nine sub menus:

Add User: Add a new user and input the information on the device, including the User ID, Name, Face, Badge, Password, Role, and Verification Type.

User Mgt.: Browse the user information stored on the device, including the User ID, Name, Face, Badge, Password, Role, and Verification Type. You can also add, modify or delete a user's information.

Comm.: Set related parameters for communication between the device and PC, including the IP address, subnet mask, gateway, device number and communication password.

System: Set system-related parameters, including the basic parameters, screen parameters, face and attendance parameters, keyboard definitions, firmware update, etc. to configure the device as required.

Data Mgt.: Perform management of data stored on the device, for example, deleting the attendance records, all data, clear administrator, restore to factory settings and query records.

Date/Time: Set the Date/Time, Date Format, Time Display Format, Internal Bell Schedule on the terminal including Bell Duration & DLST (Daylight Saving Time).

Auto Test: Test operational status of various hardware components including the display, voice prompts, camera, keyboard screen, clock (time) tests and touch screen calibration.

Dn/Upload: Download user information and attendance data stored in the device through a USB flash drive to the timeQplus software.

Sys Info: Browse records and device information.

Note: Any user can access the main menu by pressing the [Menu] key if the system does not have an administrator. After an administrator is enrolled on the device only an administrator will be able to access the main menu. For security purposes it is recommended that you enroll an administrator before installing the terminal. For detailed operations, see [3.6 Modifying User Rights](#).

2.1 Accessing the Main Menu on a Terminal with an Administrator

Only employees with Administrator rights can access the Main Menu of a secured terminal (a terminal that has an Administrator enrolled). When [Menu] is pressed a Padlock is displayed on the screen indicating that an Administrator is enrolled on the terminal and the menu has been secured. The following steps show how to access the Main Menu depending on how an Administrator is set up for User verification:

2.1.1 Administrators with Face Enrollment

Press Menu. A Padlock is displayed on the screen. Scan your face. Once the user with Administrator rights is verified the menu will be displayed.

2.1.2 Administrators with Password Enrollment

Press Menu. A Padlock is displayed on the screen. Press [1:1]. Enter User ID (Pin#) and press the button with the Key Icon at the bottom of the screen. Enter your Password when prompted and press [OK]. Once the user with Administrator rights is verified the menu will be displayed.

2.1.3 Administrators with Proximity Badge Enrollment

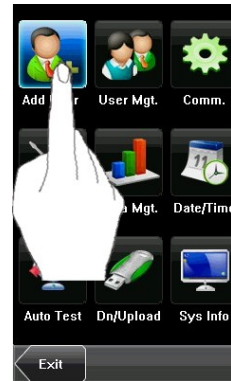
Press Menu. A Padlock is displayed on the screen. Scan your proximity badge. Once the user with Administrator rights is verified the menu will be displayed.

Note: If an Administrator wants to access the terminal Menu and they press [1:1] and then verify their identity they will hear “Thank You” because they did not press [Menu] before pressing [1:1]. The employee recorded a punch instead of accessing the Menu.

3. Add User

Press **[Add]** on the **User Mgt.** screen to display the **Add User** screen as shown to the right.

- **User ID:** Enter a user ID. 1 to 9 digit user IDs are supported by default.
- **Name:** Enter a user name. 12 characters user names are supported by default.
- **Password:** Enroll a user's password. The device supports 1 to 8 digit passwords by default.
- **Card:** Enroll a Badge.
- **Face:** Enroll a user's face.
- **Role:** Set the rights of a user. A user is set to **ordinary user** by default and can also be set to **administrator**. Ordinary users are only granted the rights of face or password verification, while administrators are granted access to the main menu.
- **Photo:** Enroll a user's photo. The user's photo is displayed on screen after a successful verification.
- **VerType:** Select the method of User verification.



3.1 Entering a User ID

The device automatically allocates user IDs starting from 1. If you use the user ID allocated by the device, you may skip this section.

- Press **[User ID]** on the **Add User** screen to display the user ID management screen.

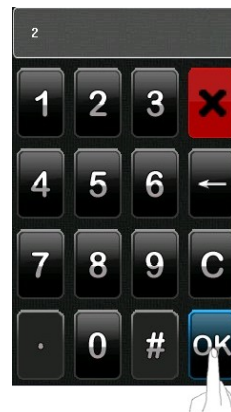


Note: The user ID can be modified during initial enrollment, but once enrolled, it cannot be modified.

- Using the keypad screen, enter a user ID and press **[OK]**. If the message “User ID exists!” is displayed, enter another ID.

Note: The device supports 1 to 9 digit user IDs by default.

- After the user ID is entered, press **[Save]** to save the current information and return to the previous screen. Press **[Exit]** to return to the previous screen without saving the current information.



3.2 Entering a Name

- Press **[Name]** on the **Add User** screen to display the name input screen with keyboard.
- On the displayed keyboard, enter a user name and press **[X]**. For details on using the keyboard screen, see [12.1 Entering Text Using the Keyboard](#).
- After the user name is entered, press **[Save]** to save the current information and return to the previous screen. Press **[Exit]** to return to the previous screen without saving the current information.



Note: The device supports 1 to 12 character names by default.

3.3 Enrolling a Password

- Press **[Password]** on the **Add User** screen to display the password management screen.
- Using the keyboard, enter a password and press **[OK]**. When prompted to input password again, re-enter the password and press **[OK]**.

Note: The device supports 1-8 digit passwords by default.



- After the password is entered, a screen is displayed as shown to the right. Press **[Save]** to save the current information and return to the previous screen. Press **[Exit]** to return to the previous screen without saving the current information.



3.4 Enrolling Proximity Badges

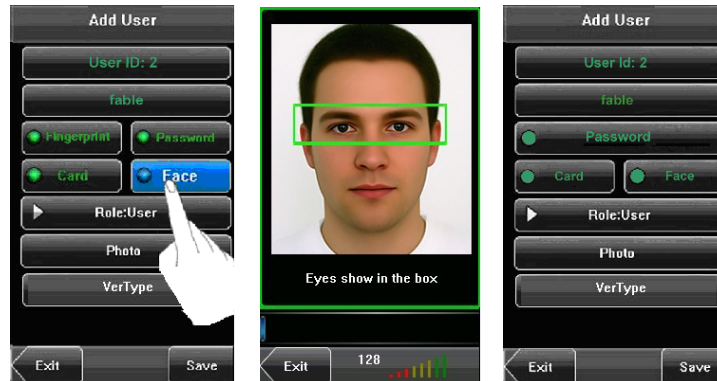
- Press **[Card]** on the **Add User** screen to display the **Enroll Card** screen.
- The **Punch Card!** screen displays as shown below. Swipe your badge over the swipe area. For details on locating the swipe area, see [1.5 Appearance of Device](#).
- If the badge passes the verification, the device will display a prompt message “Read Successfully! Card No.: *****”, and return to the **Add User** screen.
- Press **[Save]** to save the current information and return to the previous screen. Press **[Exit]** to return to the previous screen without saving the current information.



3.5 Enrolling a Face

- Press **[Face]** on the **Add User** screen to display the face enrollment screen.
- On the displayed face enrollment screen, turn your head to the left and right slightly, raise and lower your head according to the voice prompts, so as to enroll different parts of your face into the system. See [1.2 Enrollment Face Expressions](#).

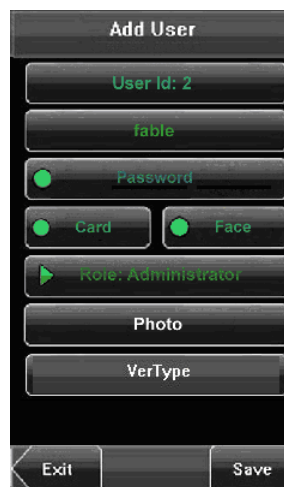
- If your face image is enrolled successfully, the system will display a prompt message and automatically return to the **Add User** screen.
- Press **[Save]** to save the current information and return to the previous screen. Press **[Exit]** to return to the previous screen without saving the current information.



3.6 Modifying User Rights

There are two types of rights respectively granted to two types of users: the **ordinary users** and **administrators**. Ordinary users are only permitted to punch, while administrators are granted access to the Main Menu.

- On the **Add User** screen, press **[Role: User]** to toggle from "User" to "Administrator" (see figure below).
- Press **[Save]** to save the current information and return to the previous screen; press **[Exit]** to return to the previous screen without saving the current information.




3.7 Enroll Photo

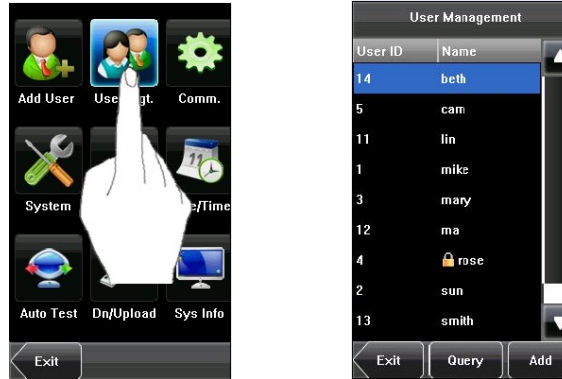
If you enrolled your photo in the system, the system will display your enrolled photo in addition to your ID and name after you pass the verification.

1. Press **[Photo]** on the **Add User** screen to display the photo enrollment screen.
2. On the photo enrollment screen, stand naturally in front of the screen. For details, see [1.1 Standing Position, Posture and Face Expressions](#). Press **[Capture]** to capture the photo.
3. After taking the photo, press **[Done]** to return to the previous screen.
4. Press **[Save]** to save the current information and return to the previous screen; press **[Exit]** to return to the previous screen without saving the current information.



4. User Management

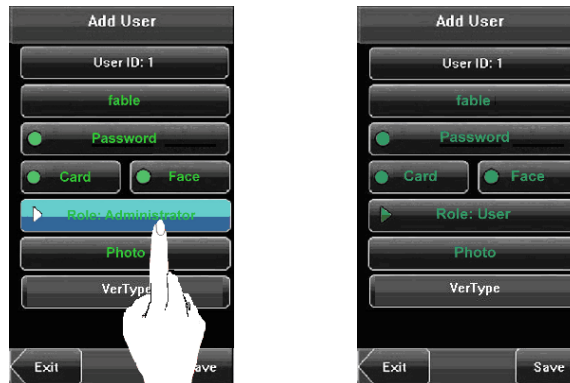
Press [User Mgt] on the main menu screen to display the user management screen. Users are listed in alphabetical order by last name. The lock icon  next to a user's name indicates that this user is an administrator.



4.1 Edit a User

Press a user name from the list to enter the **User Info** screen. The User ID cannot be modified, and the other operations are similar to those performed in **Add User**. You can re-enroll your face, change your password, and modify the management rights.

For example: Change the user rights from Administrator to ordinary User as shown below:



4.2 Delete a User

On the **User Info** screen, you can delete all or partial user information.

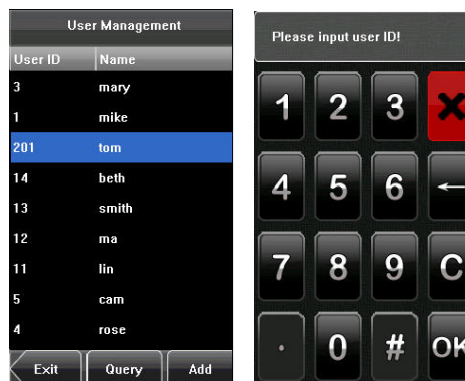
- Press **[Delete]** to delete a user.
- On the displayed screen, press **[YES]** to delete the current user or **[NO]** to return to the previous screen.
- On the **User Info** screen, press **[Name]**, **[Password]**, **[Card]** or **[Face]** to delete the related user information and to re-enroll new information by following the device prompt.



4.3 Query a User

To enable administrators to locate a user quickly from a large number of enrolled users, the device allows a query by "User ID".

- Press **[Query]** on the **User Mgt.** screen to display the User ID input screen.
- Enter the user ID and press **[OK]**. If the user id is valid, the user will be highlighted in the list.



5. Communication Settings

You can set related parameters for the communication between the device and PC, including the **IP address**, **Subnet Mask**, **Gateway**, **DNS Server**, **Device ID**, and **Comm Key**.



- **IP Address:** The IP address is 192.168.1.201 by default and can be changed as required.
- **Subnet Mask:** The subnet mask is 255.255.255.0 by default and can be changed as required.
- **Gateway:** The gateway is 0.0.0.0 by default and can be changed as required.
- **DNS Server:** The DNS server is 0.0.0.0 by default and can be changed as required.
- **Device ID:** This parameter is used to set the ID of device from 1 to 254. If the RS232/RS485 communication is adopted, you need to enter the device ID on the software communication screen.
- **Comm. Key:** To enhance the security of attendance data, you can set a password for the connection between the device and PC. Once the password is set, you can connect the PC with the device to access the attendance data only after entering the correct password. The default password is 0 (that is, no password). Once a password is set, you need to enter this password before connecting the PC software with the device; otherwise, the connection is unsuccessful. 1 to 6 digit passwords are supported.

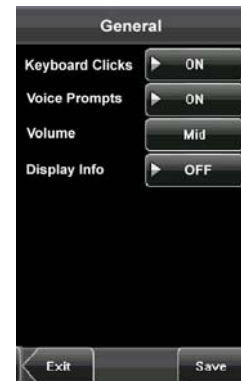
6. System Settings

Through the **System** menu, you can set system-related parameters, including General Settings, Display Settings, Face, Log settings, Shortcut Def. and Firmware Update.



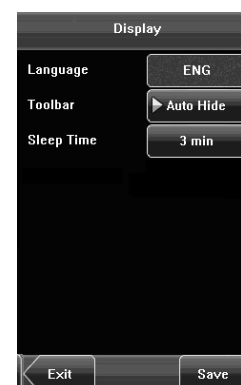
6.1 General Parameters

- **Keyboard Clicks:** Used to set whether to generate a beep sound in response to every keyboard touch. Select “ON” to enable the beep sound, and select “OFF” to mute.
- **Voice Prompts:** Used to set whether to play voice prompts during the operation of the device. Select “ON” to enable the voice prompt, and select “OFF” to mute.
- **Volume:** Used to adjust the volume of voice prompts. Options are Low, Mid and High.
- **Display Info:** Used by the timeQplus software to display employee status (punching IN/OUT) and number of hours worked for the pay period. Select “ON” to display information.



6.2 Interface Parameters

- **Language:** Allows user to switch to a different language (both on the display and voice prompts). The terminal must be restarted (press reset button) in order for the new language to take effect.
- **Toolbar:** Used to display the style of the shortcut keys on the initial screen. It can be set to “Auto Hide” and “Unhide”. By selecting “Auto Hide”, you can manually display or hide the toolbar.
- **Sleep Time:** Used to specify the number of minutes of inactivity before the device is put into sleep mode. You can wake up the device by touching the screen or scanning your face. The numerical range is 1 ~ 30 minutes; the factory default is 3 minutes.



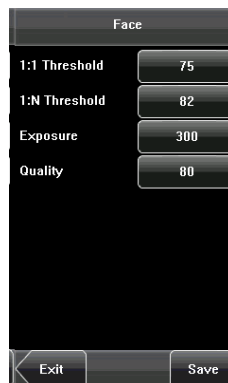
6.3 Face Parameters

- **1: 1 Threshold:** Used to set the threshold of matching between the current face and the face template enrolled in the device in the 1:1 verification mode. If the similarity between the current face and the face template enrolled in the device is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 70-120. The higher the threshold, the lower the False Acceptance Rate (FAR) and the higher the False Rejection Rate (FRR) are, and vice versa.
- **1: N Threshold:** Used to set the threshold of matching between the current face and the face template enrolled in the device in the 1: N verification mode. If the similarity between the current face and the face template enrolled in the device is larger than this threshold, the matching is successful; otherwise, the matching is not successful. The valid value scope is 80-120. The higher the threshold, the lower the FAR and the higher the FRR are, and vice versa.

Recommended Thresholds Values

(FRR)	(FAR)	Threshold	
		1: N	1: 1
High	Low	45	25
Medium	Medium	35	15
Low	High	25	10

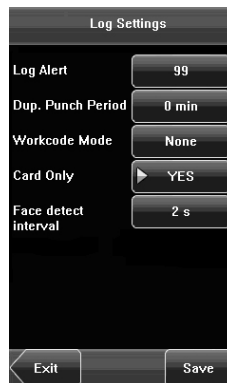
- **Exposure:** This parameter is used to set the exposure value of the camera.
- **Quality:** This parameter is used to set a min. quality (accuracy) threshold for a successful comparison. The device captures face images and compares them to face templates stored in the terminal using a face algorithm. When the accuracy of the comparison is higher than the threshold a successful punch is recorded.



Note: Improper adjustment of the Exposure and Quality parameters may severely affect the performance of the device.

6.4 Log Settings

- **Log Alert:** When the available space is insufficient to store the specified number of attendance records, the device will automatically generate an alarm (Valid values: 1-99).
- **Dup. Punch Period (m):** If a user's attendance record already exists and the user punches in again within the specified period (unit: minute), the second attendance record will not be stored (Valid values: 1-60 minutes).
- **Card Only:** If this parameter is set to "YES", users can punch by only using a badge. If this parameter is set to "NO", you will need to verify your face after badge verification.
- **Workcode Mode:** The default value is "None"; only mode 3 and mode 4 are supported by the timeQplus software.
- **Face detect interval:** The default value is 0, i.e., there is no interval.



6.5 Shortcut Definitions

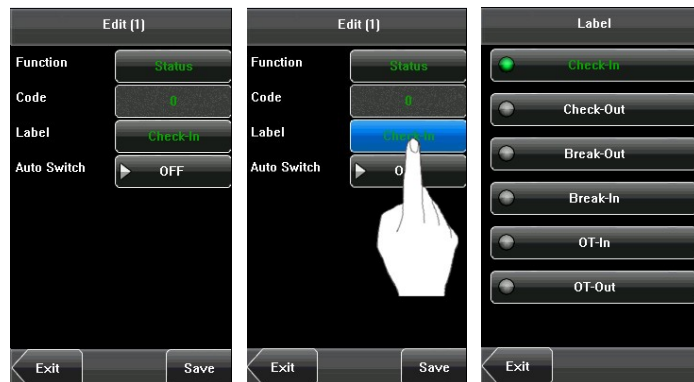
You can define the following touch screen functional shortcut keys: **Status**, **WorkCode**, and **SMS**.

6.5.1 Set Shortcut Keys

- Press **Shortcut Def.** to display the list of the existing shortcut keys; press the shortcut key to be modified. On the edit screen, press **Function**. On the **Function** screen, select the desired shortcut function.



- To configure the **Status** function, press **Status** on the Function screen. The **Edit** screen will appear, allowing the user to configure individual settings for the Status shortcut. Press the **Label** box to enter the **Label** screen. Press the row of the label (six options for Status) to select it.




- The **Code** cannot be modified; it is changed accordingly with the selected label for the status key. Select **Auto Switch**, and select **On**, as shown in the figures below.
- Press **Define** to enter the time setting screen. Press the key on the touch screen to set the time; press **[OK]** to save and return to the edit screen.

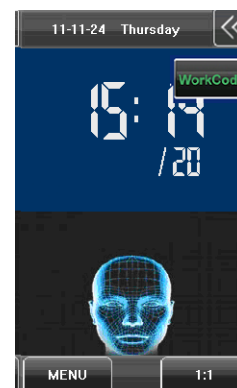


- After the setting is completed, press **[Save]** to save the setting and return to the **Shortcut Def.** screen.

Note: The shortcut function “Status” is currently NOT supported by the timeQplus software.

6.5.2 How to Use the Workcode Shortcut Key

- Press  on the initial screen to display the assigned function keys.
- Press **[Workcode]**. “Verify” will be displayed on the screen.
- Proceed with face/card/password verification. After successful verification, a list of assigned work codes will be presented to the user.
- Press a work code to select it. User will then be punched in.



6.6 Update

You can upgrade the device firmware by using an upgrade file stored on a USB Flash Drive.



Note: If you need a firmware upgrade file, please contact Acroprint Technical Support. Firmware upgrades are not normally needed.

7. Data Management

Through the **[Data Mgt.]** menu, you can perform management of data stored on the device, for example, delete attendance records, delete all data, clear administrators, restore the device to factory settings, and query user records.



- **Delete Transactions:** Delete all attendance records.
- **Delete All Data:** Delete all enrolled personnel and any stored data such as face templates, badge numbers and attendance records.
- **Clear Administrator:** Change all Administrators to Ordinary Users.
- **Restore to Factory Settings:** Restore all parameters on the device to the original factory settings. Employee information and attendance records are **NOT** deleted during restoration to factory settings.
- **Record:** Query attendance records. For more details, see [7.1 Query Record](#).
- **SMS:** Write public or personal short messages and display them for designated persons at designated times. In addition, short messages can also be prepared in advance.
- **WorkCode:** Set one or multiple WorkCodes for an employee according to the job in process. WorkCodes are used for Job Costing. For detailed operations, see [6.5.2 How to Use the Workcode Shortcut Key](#).

7.1 Query Record

Since employee “punches” are saved in the terminal, you can easily query them by pressing **[Record]** on the **Data Mgt.** screen.

- **User ID:** Enter the user ID of the employee to query. If this field is left blank, you can query the attendance records of all employees.
- **Query Time Period:** You can query a specific time period such as Yesterday, This Week, Last Week, This Month, Last Month or All.
- **Start and End:** You can use the default start time (00:00) and end time (23:59) or you can input a custom start and end time. Each time you select other options for the time period, the start and end time will be automatically changed to the default for that time period.
- After setting the query conditions, press **[Query]** to display the records that meet the specified query conditions.



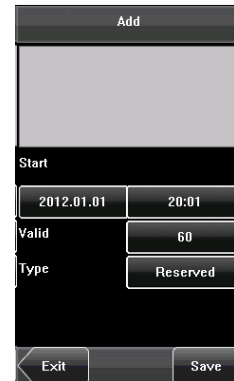
7.2 SMS

Administrators can write a short message to be displayed on the terminal screen during a designated period. Short messages are classified into Public and Personal short messages. If a short message is configured as public, it will be automatically displayed every minute, on the minute, for 4 seconds. The message will remain active for the duration of the designated period; alternatively, users can use the shortcut keys to view the message. If a short message is configured as Personal, the message will be displayed after the designated employee punches.

7.2.1 Set a Short Message

Add a short message

- Press [SMS] on the **Data Mgt.** Screen. Press **[Add]** to begin configuring the following SMS settings:
 - **Start:** the time when the short message takes effect.
 - **Valid:** the short message is only displayed within a validity period.
 - **Type:**
 1. **Reserved:** the short message is prepared in advance but not configured as personal or public.
 2. **Personal:** the short message can only be viewed by a specific user.
 3. **Public:** the short message can be viewed by all users.

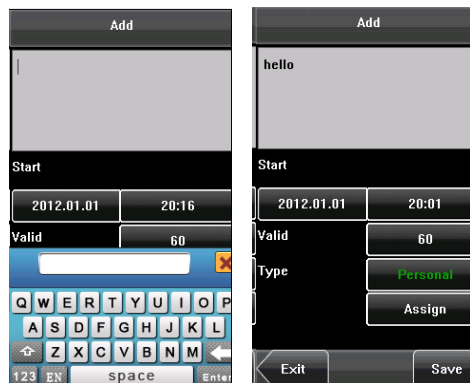


The screenshot shows the 'Add' screen with the following fields and values:

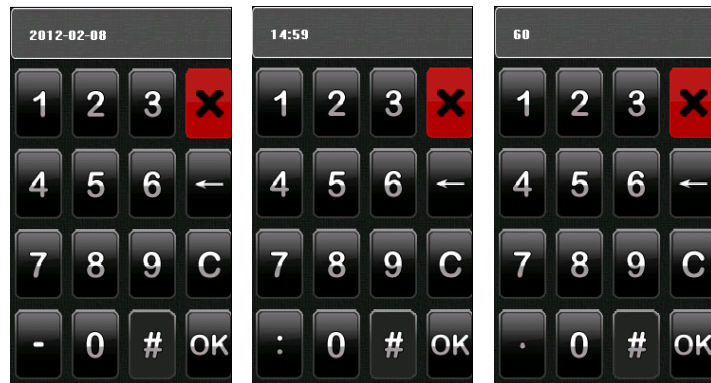
Field	Value
Start	2012.01.01 20:01
Valid	60
Type	Reserved

Buttons: Exit, Save

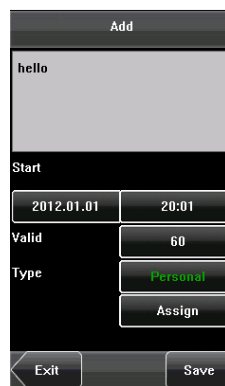
- As shown in the following figures, press the short message input area to bring up the keyboard to input SMS contents. See [Appendix 12.1 "Entering Text Using the Keyboard"](#).



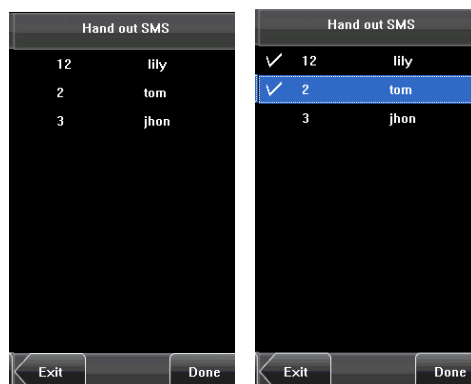
- Press **Start** or **Valid** to start the configuration screen shown in the following figures:



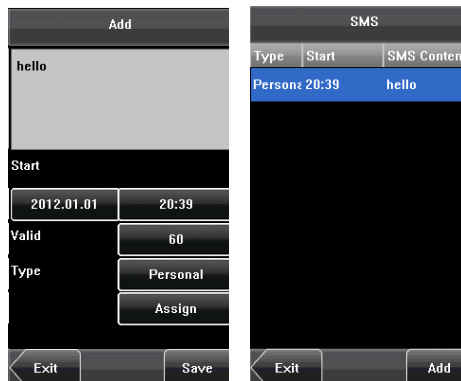
- Press the number key to input values to be set, and press **OK** to save the settings and return to the previous screen.
- Press **Type** to select the type for the short message, which include personal, public, and reserved. The following figure shows the personal type:



- Press **Assign** to start the **Hand out SMS** screen. As shown in the following figures, by pressing the name of an employee, the employee is **Checked** and the short message will be displayed to him:

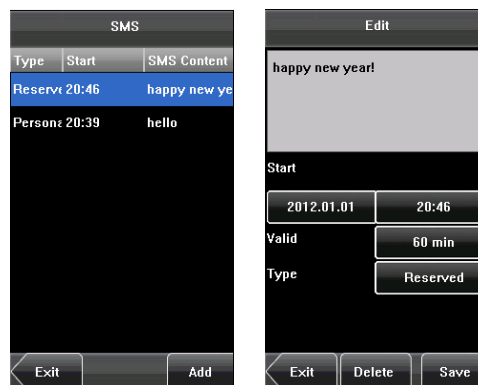


- Press **Done** to save the settings and return to the previous screen. Press **Save** to store the short message and go back to the previous screen. The new short message is displayed on the screen.



Edit a short message

- Press the message to be edited in the **SMS** screen. The procedure of editing a short message is the same as that of adding a short message.



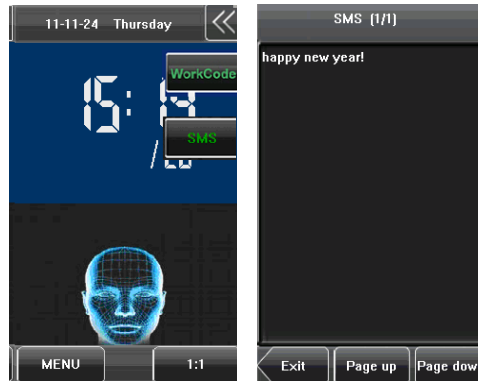
Delete a short message

By pressing **Delete** on the **Edit** screen, the short message is removed. In addition, any information related to the message is deleted simultaneously.

7.2.2 View a Short Message

View a public short message

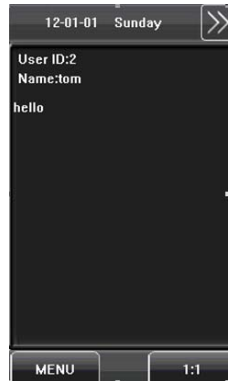
On the initial screen, public short messages are automatically displayed on the minutes. Alternatively, the public short messages can be viewed by pressing the shortcut keys on the screen, as shown in the following figures. For details on creating shortcut keys, see [6.6 Shortcut Definitions](#).



After viewing, press **[Exit]** to return to the main screen.

View a personal short message

After a user is authorized, his short message will be displayed, as shown in the following figure:



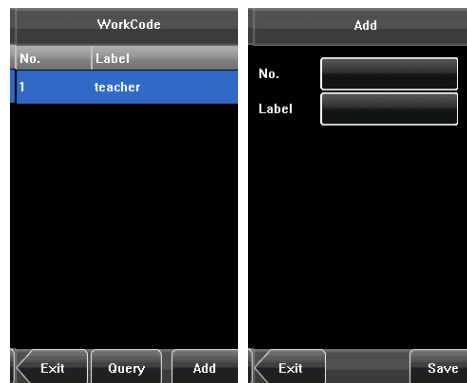
7.3 Work Code

Note: If using timeQplus software, work codes with labels are defined in the software and are then uploaded to the terminal. DO NOT enter work codes directly into the terminal.

The Work Code function is designed to capture and assign labor hours worked by employees. Work Codes can be departments, projects, activities, or any other segmentation associated with labor hours.

7.3.1 Add a Work Code

- Press **[WorkCode]** on the **Data Mgt.** screen and then press **[Add]** to display the **Add** screen as shown in the figures below.
- Press **[No.]** to enter the digital code of for the work code.
- Press **[Label]** to display the text entry screen. On this screen, enter a label for the work code. (See [12.1 Entering Text Using the Keyboard](#))



7.3.2 Edit a Work Code Label

- Press **[WorkCode]** on the **Data Mgt.** screen.
- Press the row of a work code to display the **Edit** screen.
- To edit this work code, enter a new label with the same operation steps as described in "Add a work code".
- Press **[Save]** when done.

7.3.3 Delete a Work Code

- Press **[WorkCode]** on the **Data Mgt.** screen
- Press the row of a work code to display the **Edit** screen.
- Press **[Delete]** and then press **[Yes]** on the "Are You Sure?" screen.

8. Date/Time Setting

8.1 Set Date/Time

The date and time of the device must be set accurately to ensure the accuracy of attendance time.

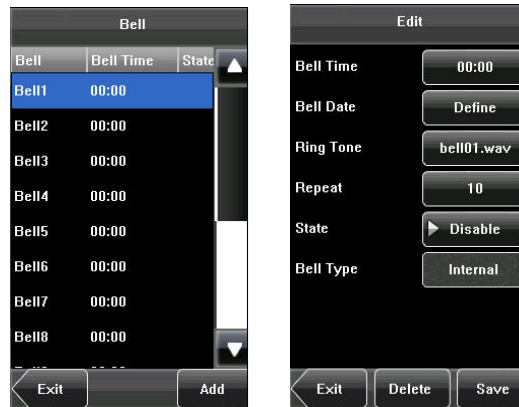
- Press **[Menu]** on the initial screen to display the main menu screen.
- Press **[Date/Time]** to display the Date/Time setting screen.
- Select the desired date and time by pressing the parameter. For the time format, there are 10 formats available. Both 12-hour and 24-hour time systems are supported.
- Press **[Save]** to save the current information and return to the previous screen. Press **[Exit]** to return to the previous screen without saving the current information.



8.2 Bell Setting

Many companies ring bells to signal the start and end of work shifts. They usually manually ring them or use electric bells. To lower costs and facilitate management, the time bell function has been integrated into the TQ600F. You can set the alarm time and duration for ringing the bell based on your requirements. The device will then automatically play the selected ring tone and trigger the relay simultaneously, as well as stop playing the ring tone after the set duration. Each device is predefined with 15 alarm bells.

- Press **[Bell]** on the **Date/Time** screen. The displayed bell setting screen lists all the predefined bells.
- Press a bell in the list on the bell setting screen to display the **[Edit]** screen.



- The following parameters can be configured:
 - **Bell Time:** Used to set time when the device automatically plays a bell ring tone every day.
 - **Bell Date:** Used to set which day the device automatically plays a bell ring tone.
 - **Ring Tone:** Used to set the bell ring tone.
 - **Repeat:** Used to set the alarm times.
 - **State:** Used to disable/enable the bell.
 - **Bell Type:** You can select between internal ringing and external ringing. For internal ringing, the ring tone is played by the loudspeaker of the device. For external ringing, the ring tone is played by an external electric bell that is connected with the device.
- To add a bell, press **[Add]** on the **Bell** listing screen.
- To delete a bell, press the bell on the **Bell** listing screen to display the **Edit** screen and then press **[Delete]**.

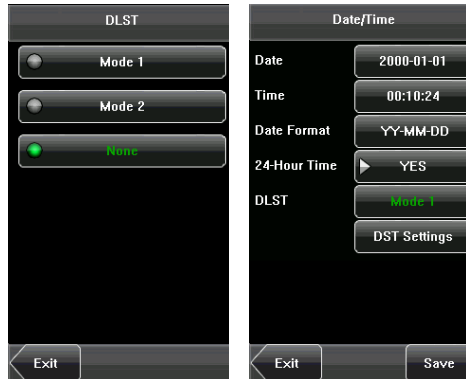
8.3 Daylight Savings Time (DLST)

DLST, also called Daylight Savings Time, is a system to prescribe local time in order to save energy. The unified time adopted during the system date is called “DLST”. Usually, the time will be moved one hour forward in spring. It can make people sleep early and get up early. It can also reduce lighting to save power. In autumn, the time will be moved back 1 hour. The regulations are different in different countries. At present, nearly 110 countries adopt DLST.

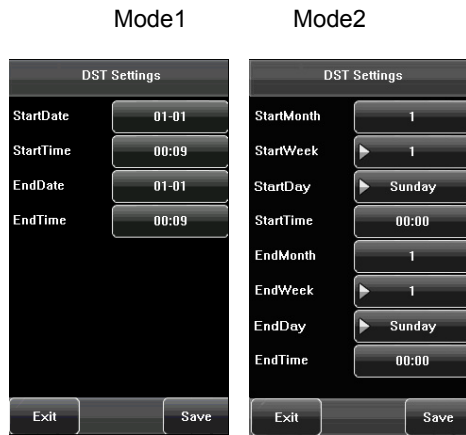
To meet the demand of DLST, a special option can be customized on the TQ600F. Automatically set the time one hour forward at XX (minute) XX (hour) XX (day) XX (month), and/or one hour backward at XX (minute) XX (hour) XX (day) XX (month) if necessary.



- Press **[None]** to display the DLST mode selection screen. The available options are Mode 1, Mode 2 and None.
- Select the DLST mode; you will automatically return to the Date/Time screen:

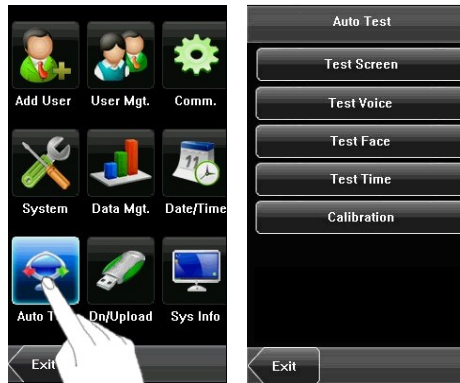


- Press **[DLST Settings]** to enter the DLST settings edit screen. After setting, press **[Save]** to complete and return.



9. Auto Test

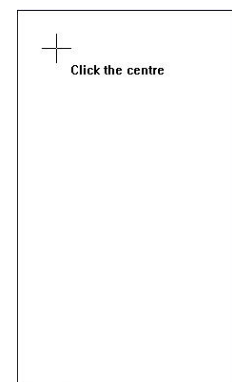
The auto test enables the system to automatically test whether functions of various modules are normal, including the screen, sensor, voice, face, keyboard and clock tests.



1. **Test Screen:** The device automatically tests the display effect of the color TFT display by displaying full color, pure white and pure black and checks whether the screen displays properly. You can continue the test by touching the screen or quit by pressing **[Exit]**.
2. **Test Voice:** The device automatically tests whether the voice files are complete and the voice quality is good by playing the voice files stored in the device. You can continue the test by touching the screen or quit by pressing **[Exit]**.
3. **Test Face:** The device automatically tests whether the camera works properly by checking whether the collected face images are clear and acceptable. Press **[Exit]** to quit the test.
4. **Test Time:** The device tests whether its clock works properly by checking the stopwatch of the clock. Touch the screen to start counting, and touch it again to stop. Check whether the counting is accurate. Press **[Exit]** to exit the test.
5. **Calibration:** You can perform all the menu operations by touching the screen with one of your fingers or a stylus. When the touch screen is less sensitive to the touch, you can perform a screen calibration.

Calibration

1. Press **[Menu]** on the Main Interface and then press **[Auto Test]**.
2. Press **[Calibration]** to display the calibration screen.
3. Touch the center of the cross “+”.
4. Repeat Step 3 following the move of the “+” icon to different locations on the screen.
5. Touch the center of the cross at five locations on the screen correctly. The calibration succeeds when the message “Calibrating screen, please wait” is displayed on screen and the system automatically returns to the main menu. If the calibration fails, the system recalibration will start from Step 3.



10. USB Disk Management

Through the [Dn/Upload] menu, you can download user information and attendance data stored to a USB disk to be uploaded to related software.

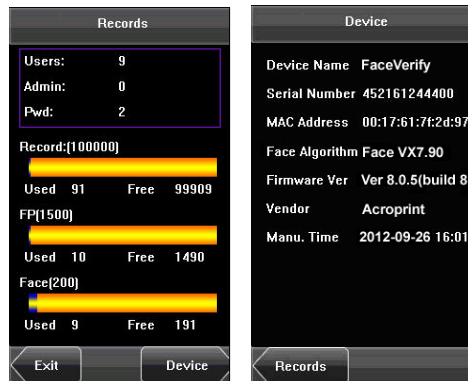


- **Download Transactions:** Download all the attendance data from the device to a USB disk.
- **Download User:** Download all the user information, fingerprints and face images from the device to a USB disk.
- **Download user photos:** Download the employees' photos from the device to a USB disk.
- **Upload User:** Upload the user information, fingerprints and face images stored in a USB disk to the device.
- **Upload User Photo:** Upload the JPG documents that are named after the user IDs and stored in a USB disk to the device, so that user photos can be displayed after the employee passes the verification. See [12.5 Photo ID Function](#).

11. System Information

You can check the storage status as well as version information of the device through the [Sys Info] option.

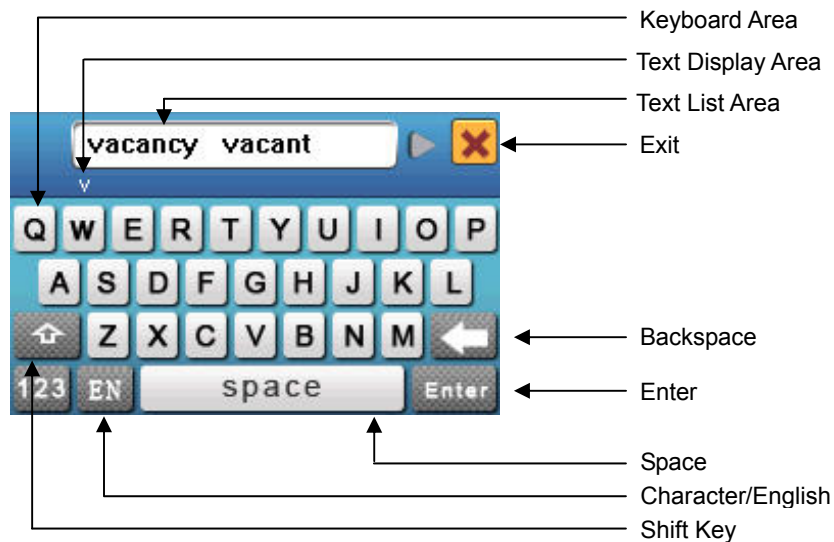
- **Records:** The number of enrolled users, administrators and passwords are displayed on the **Records** screen; the total face storage capacity and used capacity as well as the total attendance storage capacity and used capacity are graphically displayed respectively.
- **Device:** The device name, serial number, version information, vendor and date of manufacture are displayed on the **Device** screen.



12. Appendix

12.1 Entering Text Using the Keyboard

The device has a full QWERTY keyboard that supports upper and lower case Alpha characters, numbers and symbols. Press a button that requires text input to display the keyboard. For example, press **[Name]** and the keyboard will appear:



To enter a name, proceed as follows:

- Press **[Name]** on the **Add** screen, as shown in figure below.
- Enter the letter characters, and a list of characters in relation to the letter is presented in the text display area.
- If the desired text is displayed in the text display area, press this text. This text is then displayed on the **[Name]** button. Enter next character by repeating Step 2.

- After finishing the entry of name, press **[X]** to exit the Keyboard Interface and return to the previous screen.

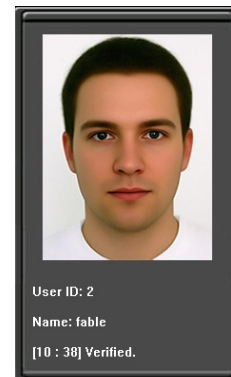


12.2 Photo ID Function

The Photo ID function is used to display on screen the photo enrolled by a user or stored on a USB disk in addition to such information as the user ID and name. When the photo taken by the device is used, the photo can be displayed upon successful verification.

To use a photo stored on a USB disk:

- Create a folder with the name of “photo” on the USB disk, and store users' photos under this folder.
- The user photos must be in JPG format and named after their IDs. For example, for the user with the user ID of 154, the photo name must be 154.jpg.
- Insert the USB disk into USB slot on the device, and select **[Menu]** → **[Dn/Upload]** → **[Upload User Photo]**. User photos can now be displayed upon successful verification.



Note:

- The length of a user name cannot exceed 24 digits.
- The recommended size of a user photo is less than 64k bit.
- The uploaded new user photo will overwrite the existing photo assigned to the user ID.
- To download user photos, select **[Menu]** → **[Dn/Upload]** → **Download User Photos**. A folder with the name of “photo” will be automatically created on the USB disk, and all downloaded user photos are stored under this folder.

12.3 Multi-combination Authentication Mode

Four elements can be combined to authenticate a user: User Number (PIN#), Face (FACE), Password (PW) and Proximity Badge (RF).

Meaning of symbols used in table below:

- "/" is or
- "&" is and
- PWD (Password)
- PIN (user ID)
- "+" follow next operation
- FACE (Face)
- RF (RF card)

If Face, Password and Proximity Badge have been enrolled for the user, the verification procedure is as described in the table below.

Type	Verification Steps
FACE/RF/PW	FACE or RF or PW are verified
	1) FACE(1:N)
	2) Proximity Badge (RF) 3) Pin# + Password
FACE&PW	FACE + PW are verified
	1) FACE(1:N)+PW+"OK"
	2) PIN+FACE(1:1)+PW 3) PIN+PW+FACE
FACE&RF	FACE + RF are verified
	1) FACE(1:N)+RF
	2) PIN+FACE(1:1)+RF 3) RF(1:N)+FACE
PW	Only PW is verified
	PIN+PW+"OK"
RF	Only RF is verified
	RF(1:N)
FACE	FACE verified
	PIN+FACE(1:1)
PW/RF	PW or RF is verified
	1) PIN+PW+"OK"
	2) RF(1:N)
PW&RF	1) Proximity Badge & PW are verified
	2) Pin#/PW & Proximity Badge are verified