

AC6000™ Configuration Manual

Version eng-1.22



UNION
COMMUNITY

Copyright 2009 By UNION COMMUNITY Co., Ltd.

Disclaimers

Information in this document is provided in connection with UNION COMMUNITY products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in UNION COMMUNITY's Terms and Conditions of Sale for such products, UNION COMMUNITY assumes no liability whatsoever, and UNION COMMUNITY disclaims any express or implied warranty, relating to sale and/or use of UNION COMMUNITY products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

UNION COMMUNITY products are not intended for use in medical, life saving, life sustaining applications, or other applications in which the failure of the UNION COMMUNITY product could create a situation where personal injury or death may occur. Should Buyer purchase or use UNION COMMUNITY products for any such unintended or unauthorized application, Buyer shall indemnify and hold UNION COMMUNITY and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that UNION COMMUNITY was negligent regarding the design or manufacture of the part.

UNION COMMUNITY reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." UNION COMMUNITY reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Please contact UNION COMMUNITY, local UNION COMMUNITY sales representatives or local distributors to obtain the latest specifications and before placing your product order.

About UNION COMMUNITY

With regard to any fingerprint-related issues, UNION COMMUNITY is always in readiness to find out well fitted solutions, depending on customers' requirements and needs.

As a leading provider of fingerprint core technology, UNION COMMUNITY has set up wide variety of fingerprint product lines from fingerprint OEM modules to several choices of fingerprint finished products including access control, time & attendance, door lock, PC peripherals, safety box, etc, that incorporate UNION COMMUNITY's groundbreaking biometrics technology. Based on its proprietary algorithm, its own

sensor and in-house one-stop processing capability regarding hardware, software, product design, etc., our services to government sector and various commercial sectors like security, construction and enterprise are in full swing through fast problem-solving approach to meet market trends or demands. As a result, UNION COMMUNITY exports its market-proven fingerprint products to over 40 countries including Japan, USA, Europe and China.

As the biggest and the most promising company in the commercial sector of biometrics industry in Korea, UNION COMMUNITY was awarded “Korean World-class Product Award” for its excellent performance by Minister of Commerce, Industry and Energy in December 2005.

To be the world-class company in biometrics field, UNION COMMUNITY and all the members continue to do all-out efforts for the world-best quality product, creation of new paradigm and customers’ satisfaction through accumulated expertise and working experience from various reference sites and versatile hardware & software development.

About This Manual

This is an introduction to operation of AC6000 series supplied by UNION COMMUNITY. This manual describes how to do user registration in local terminal, terminal settings, network settings, etc. The purpose of this manual is to provide instructions on using AC6000 series and troubleshooting minor problems.

< Glossary >

- Admin, Administrator
 - As a user who can enter into the terminal menu mode, he can register/modify/delete terminal users and change the operating environment by changing settings.
 - If there is no administrator for a terminal, anyone can change the settings. In this regard, it is recommended to register at least one administrator.
 - Caution is required with registration and operation because an administrator has the right to change critical environmental settings of the terminal.

- 1 to 1 Verification
 - A user's verification fingerprint (template) is compared to the user's enrollment fingerprint (template) previously registered. The terminal performs 1:1 matches against the user's enrolled template until a match is found.
 - It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.

- 1 to N Identification
 - The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
 - Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered.

- I-Capture (Intelligent Capture)
 - Reinforces detection capability for residual fingerprints (fingerprints left on a sensor window due to sweat or contaminants on a finger) and automatically adjusts sensor settings to detect good-quality fingerprints regardless of the conditions (dry or wet) of the fingerprints.

- Authentication level
 - Depending on the fingerprint match rate, it is displayed from 1 to 9. Authentication is successful only if the match rate is higher than the set level.
 - The higher the Authentication level, the higher the security. However, it requires a relatively high match rate, so Authentication is vulnerable to failure.
 - 1:1 Level: Authentication level used for 1:1 verification
 - 1:N Level: Authentication level used for 1:N identification

- Authentication Method
 - Various kinds of authentication including FP (fingerprint) authentication, PW (password) authentication, RF (card) authentication, or a combination of these methods
 - Ex) FP|PW: fingerprint or password authentication; password is used for authentication if fingerprint authentication fails

- Function keys

[F1], [F2], [F3], [F4] are used, and they are used for direct authentication and each key represents each authentication mode.

Table of Contents

< Glossary>..... 4

Table of Contents..... 5

1. Before use..... 11

 1.1. Safety precautions 11

 1.2. Terminal description 12

 1.3. List of Icons 13

 1.4. Voice Operation 16

 1.5. Sound Operation 16

 1.6. LED operation..... 16

 1.7. Touchscreen Usage..... 16

 1.8. Correct fingerprint registration and input methods 18

 1.9. Ultraviolet (UV) Option 19

2. Introduction 20

 2.1. Features 20

 2.2. Configuration..... 23

 2.2.1. Network configuration 23

 2.2.2. Standalone configuration 23

 2.3. Specifications 24


3. Device configuration settings 25


 3.1. Terminal Setup..... 25

 3.1.1. Entering Administrator Programming 25


 3.1.2. Administrator Main Screen 26


 3.1.3. Programming Reference Chart 27


 3.2. User Management  31


 3.2.1. Registering a User  31


 3.2.1.1. User Registration Window..... 33


















 3.2.1.2. Registering a Fingerprint  34










 3.2.1.3. Registering a Card  35















 3.2.1.4. Registering a Password  36

 3.2.1.5. Authentication Type  37

 3.2.1.6. User Fingerprint Options  39

		
3.2.1.7. User Picture Registration		40
3.2.1.8. User Type (Normal/Administrator)		40
		
3.2.2. Deleting a User		41
		
3.2.3. Modifying a User		42
		
3.2.4. Viewing Users		43
		
3.2.5. Deleting All Users		44
		
3.3. Network Settings		45
3.3.1. Terminal ID Number		45
3.3.2. Wireless (WiFi) Settings		46
3.3.2.1 WiFi Advanced Settings		48
		
3.4. Application Settings		50
		
3.4.1. Access Control Mode		50
		
3.4.2. Time & Attendance		50
		
3.4.2.1 Time & Attendance Schedules		51
		
3.4.3. Meal Application		52
		
3.4.3.1 Meal Mode Schedules		52
		
3.4.4 Shift Management		53
		
3.4.4.1 Shift Management Options		53
		
3.4.5 People Count		54
		
3.4.6. Function Key Programming		55
3.4.6.1. Extended Function Keys		55
		
3.5. System Settings		57

	 System	
3.5.1. System Settings		58
3.5.1.1. User ID Length		58
3.5.1.2. Authentication Mode		58
3.5.1.3. Fingerprint Template Format		59
	 Fingerprint Sensor	
3.5.2. Fingerprint Sensor Settings		60
3.5.2.1. 1:N Level		60
3.5.2.2. 1:1 Level		60
3.5.2.3. Fake Finger Detection		60
3.5.2.4. Enhanced Registration		61
3.5.2.5. Multiple Fingerprints		61
	 Date/Time	
3.5.3. Date/Time Settings		61
3.5.3.1. Display Format		61
3.5.3.2. Set Current Date		62
3.5.3.3. Set Current Time		63
	 Database	
3.5.4. Database Options		63
3.5.4.1. Compress User Data		63
3.5.4.2. Delete All Users		64
3.5.4.3. Clear Settings		64
3.5.4.4. Clear Log Data		64
3.5.4.5. Clear Picture Logs		64
3.5.4.6. Delete All		64
	 Authentication	
3.5.5. Authentication Settings		65
3.5.5.1. User Group ID		65
3.5.5.2. User Display Option		65
3.5.5.3. 1:N Matching		66
3.5.5.4. Card Only		66
		
3.6 Terminal Settings		67
	 Sound	
3.6.1. Sound Settings		68
3.6.1.1. Voice Volume		68
3.6.1.2. Sound Volume		68
	 Wiegand	
3.6.2. Wiegand Settings		69
3.6.2.1. Site Code		69
3.6.2.2. Format		69
	 Lock Terminal	
3.6.3. Terminal Options		70
3.6.3.1. Terminal Locking/Unlocking		70
3.6.3.2. Case Tamper Audible		70
3.6.3.3. Card Reader		71





	 Door Options	
3.6.4. Door Option Settings	71
3.6.4.1. Door Monitor	71
3.6.4.2. Lock Type	71
3.6.4.3. Warn Time	71
3.6.4.4. Open Time	71
		
3.7. Display Settings	72
	 Theme	
3.7.1. Theme Settings	72
3.7.1.1. Daily Background Update	73
3.7.1.2. Arrange Icons	73
3.7.1.3. Main Background	74
	 Camera	
3.7.2. Camera Settings	75
3.7.2.1. Save Authorized Users	75
3.7.2.2. Save Unauthorized Users	75
3.7.2.3. Camera Display Options	75
	 Language	
3.7.3. Language	76
	 LCD Option	
3.7.4. LCD Options	77
3.7.4.1 Screen Saver	77
3.7.4.2 Touchscreen Calibrate	77
		
3.8. Terminal Information	78
	 System	
3.8.1. System Information	78
	 Terminal	
3.8.2. Terminal Information	79
	 Ethernet	
3.8.3. Ethernet Information	79
	 User	
3.8.4. User Information	80
	 Log Data	
3.8.5. Log Data Information	80
	 View Log	
3.8.6. View Log Information	81
		
3.9. USB Options	82
3.9.1. Database Export	83
3.9.2. Database Import	84
3.9.3. Firmware Upgrading	84

4. User Interface Customization	85
4.1. Standard Customization/Languages	85
4.1.1 Main Window Backgrounds.....	85
4.1.2 Language Translations/Customizing Text Items	85
4.1.3 Font Importing	86
4.1.4 Updating MP3 Files in AC6000	86
4.1.5 Customizing Sounds.....	87
5 How to use the terminal.....	88
5.1. Main Screen	88
5.2. ID Entry Screen.....	90
5.3. Authentication Result Display	91
5.4. Application Modes.....	93
5.4.1. Access Control Application.....	93
5.4.2. Time & Attendance Application.....	94
5.4.3. Cafeteria Application.....	95
5.4.4. Shift Management Application	96
5.4.5. People Counter Application.....	97
6. Firmware Upgrading.....	98
6.1 Upgrading from USB.....	99
6.2 Upgrading from UNIS.....	99
6.3 Upgrading to Factory Settings.....	99
7. Troubleshooting Guide.....	100

1. Before use






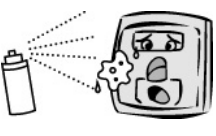

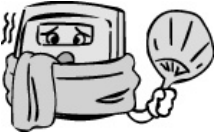
1.1. Safety precautions

● Warning

<p>Handling with wet hands or allowing liquid to flow into it is prohibited. -> It may cause an electric shock or damage.</p>		<p>Do not place a fire source near the terminal. -> It may cause a fire.</p>	
<p>Do not disassemble, repair, or modify the terminal at discretion. -> It may cause an electric shock, fire or damage.</p>		<p>Keep out of reach of children. -> It may cause an accident or damage.</p>	

- If the above warning is ignored, it may result in death or serious injury.

● Cautions

<p>Keep away from direct sunlight -> It may cause deformation or color change.</p>		<p>Avoid high humidity or dust -> The terminal may be damaged.</p>	
<p>Avoid using water, benzene, thinner, or alcohol for cleaning -> It may cause an electric shock or fire.</p>		<p>Do not place a magnet close to the terminal. -> The terminal may break down or malfunction.</p>	
<p>Do not contaminate the fingerprint input area. -> Fingerprints may not be well recognized.</p>		<p>Avoid using insecticide or flammable spray near the terminal. -> It may result in deformation or color change.</p>	
<p>Avoid impacts or using sharp objects on the terminal. -> The terminal may be damaged and broken.</p>		<p>Avoid severe temperature changes -> The terminal may be broken.</p>	

- If the above cautions are ignored, it may result in property loss or human injury.

※ Under no circumstances will UNION COMMUNITY be responsible for accidents or damages caused by inappropriate use of the product without referring to the user manual.














1.2. Terminal description





















No.	item	description
1	Camera Sensor	Picture image taken during authentication
2	Touchscreen LCD	Color LCD with Touchscreen
3	LED indicator	LED Power(RED), Card(Blue), Door(Green)
4	Approach Sensor	User approach turns on the LCD
	IRED sensor	Person's approach makes it automatically turn on button LED and LCD window with ID input screen.
5	Function Keys	Function Keys (see function key section)
6	USB	USB for memory stick, or computer (mini)
7	Call Button	Used for applications with a door phone.
8	Speaker	Speaker for voice or sound output.
9	Card Sensor	Card Sensor area, scan card in this area.
10	Finger Sliding Door	Door for finger sensor for environmental protection
11	Finger Sensor Window	Finger input area, place finger here during fingerprint entry.
12	UV Sensor	UV Sensor used for cleaning bacteria from sensor window

1.3. List of Icons

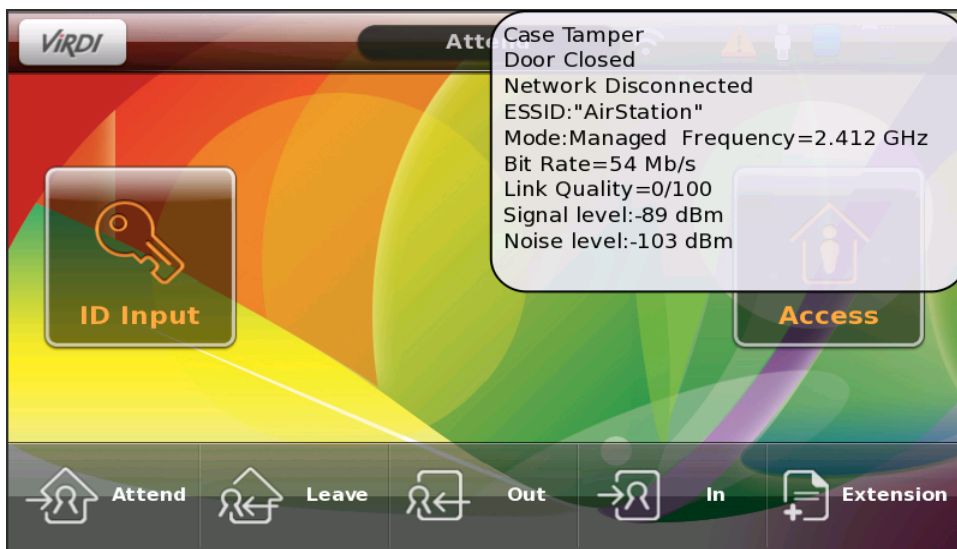
During normal operation or when a new event occurs an icon will appear on the current display. Each icon is a symbol representing the event that has just occurred. Below is a list of possible icons that can appear on the display.

Icon	Description
	ID Icon – displayed when an id number is used to access the terminal.
	Password Icon – displayed when a password is used to access the terminal.
	Card Icon – displayed when a card is used to access the terminal.
	Fingerprint – when a fingerprint is used to access the terminal the user's fingerprint will be displayed on the lcd. This can assist the user when entering their fingerprint.
	Picture – depending on the configuration options when any user accesses the terminal a picture will be taken and displayed on the lcd.
	Fail Icon – displayed when authentication is invalid from an unregistered user
	Success Icon – displayed when a registered user is successfully authenticated.
	UV Status Icon ON – when the UV protection is ON an animation picture will appear.
	UV Status Icon OFF – when the UV protection is OFF a grayed out picture will appear.
	Network Status Icon SERVER ON – when the server is actively communicating with the terminal an animation picture will appear.
	Network Status Icon NO LINK – when the server program is not communicating with the terminal and an Ethernet link is not present a grayed out network picture will appear.
	Network Status Icon LINK PRESENT – when the Ethernet link is active and the server program is not communicating with the terminal a white network picture will appear.
	Trouble Status Icon ON – when there is a terminal trouble, case tamper, this picture will appear. If no trouble is present i.e. case tamper, this icon will disappear.

	Fire Status Icon ON – when the terminal is notified of an external fire event this picture will appear. If there is no fire trouble no icon will appear.
	Door Status Icon OPEN – when the door connected to the terminal is opened this picture will appear.
	Door Status Icon CLOSE – when the door connected to the terminal is closed and normal status this picture will appear.
	Proximity Status Icon ON – when a person is near the terminal this picture will appear
	Proximity Status Icon OFF – when there is no activity in the area of the terminal a grayed out picture will appear.
	Wireless Status Icon ON – when using WiFi and the wireless device is actively connected this icon will appear.
	Wireless Status Icon OFF – If WiFi USB device is connected to the terminal but not active (WiFi Disabled) this icon is shown. If WiFi is enabled but the link is inactive this icon will show as white.
	Access Buttons – these buttons are used to reset the current mode of operation. This button is used with Function keys, Time/Attendance or Cafeteria Mode. If the current mode is attend, leave, in, or out touching this button will return to normal access mode. Both of these icons perform the same function.
	ID Button – this button is used when the user needs to input their ID number for authentication. When this button is touched a number pad window will appear.
	Function Key Attend – this button is used for time & attendance mode. It will change the current mode to Attend Mode. If the user is arriving at the office that day they will touch this button.
	Function Key Leave – this button is used for Time & attendance mode. It will change the current mode to Leaving mode. If the user is leaving the office for the day they will touch this button.
	Function Key In – this button is used for Time & Attendance mode. It will change the current mode to IN mode. If the user is arriving to the office from lunch or a break they will touch this button.
	Function Key Out – this button is used for Time & Attendance mode. It will change the current mode to OUT mode. If the user is leaving the office for lunch or a break they will touch this button.
	Function Key Extension – this button is mainly used in Time & Attendance mode. If the four function keys (Attend, Leave, In, Out) are not enough for the application this button can be used to extend the amount of function keys. A new window will appear with a selection of function keys.

	<p>Function Key Meal – this button is used in Cafeteria meal mode. When the meal is breakfast, lunch, snack or dinner the user will touch this button.</p>
	<p>Close/Cancel Button – this button will close the current window without saving any changes</p>
	<p>Configuration Button – when terminal setup and configuration is needed touching this button will enter terminal configuration mode. See configuration manual for setup details.</p>
	<p>Status Bar – all status items will appear in this bar. The text item in the center will show the current status of the terminal. Access; Attend, Leave, In, Out, Meal etc.</p>

Anytime the main window is displayed and the top right corner of the Touchscreen is touched where the status icons are, a popup message will appear with the current status. After 5 seconds the window will automatically hide.



1.4. Voice Operation

Voices are played during certain events. Below is a list of possible voices that will be played. Voice volume can be controlled separately from the sound volume. The voice feedback can be turned off if needed.

“Please enter your fingerprint”	Enter fingerprint using the fingerprint input window
“You are authorized”	Successful authentication
“Please try again”	Authentication failed
“Input your ID”	When a user ID is required
“Please enter your card”	Scan your card when you hear this message

1.5. Sound Operation

Sounds are played during events or interaction with the Touchscreen. Button presses, message popup, correct and incorrect entries, failed or success authentication will produce a single sound tone. Sound volume can be controlled separately from the voice volume. Sounds can be turned off if needed.

1.6. LED operation

On the front of the terminal on the bottom left corner there is a Virdi logo. When power is applied to the unit and during normal operation this will light up as red when a card is used to access the terminal the color will turn green for half a second then back to red.

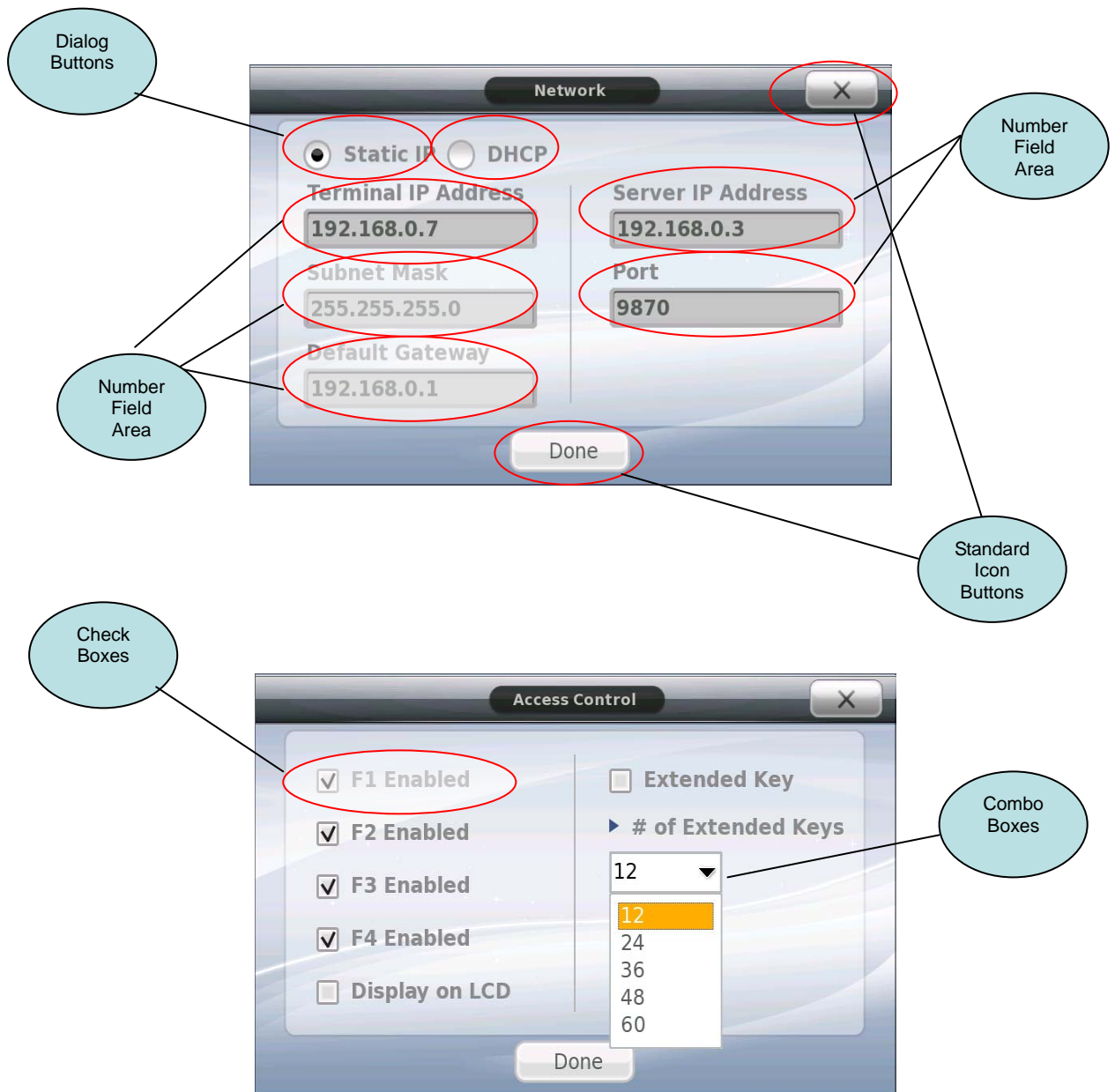
When the door is opened the color will turn green for the duration of the door open period, then turn back to red when the door is closed.

1.7. Touchscreen Usage

To use the Touchscreen correctly it is recommended to use your finger only. For cleaning use a dry cloth to wipe the surface. You can use a stylus pen if you wish. **Do not use sharp objects.** Almost anywhere on the screen is touch interactive. For example, if a popup window is displayed, touching the window will make the window disappear. Firmly touch the icon that you wish to use. The icon color will change and a sound should be heard.

In the administrator programming area, if a number entry is needed just touch the number field or text you wish to change, a number pad will appear for you to enter the data.

The example windows show the red areas that are interactive. When touching the number field entry area a number pad will appear for you to enter data. When touching a button the image will change. When touching a combo box, a list of items will appear, while your finger is down slide your finger to the selection and release. For Dialog Buttons and Check Boxes just touch the area and the option will change to a new icon.



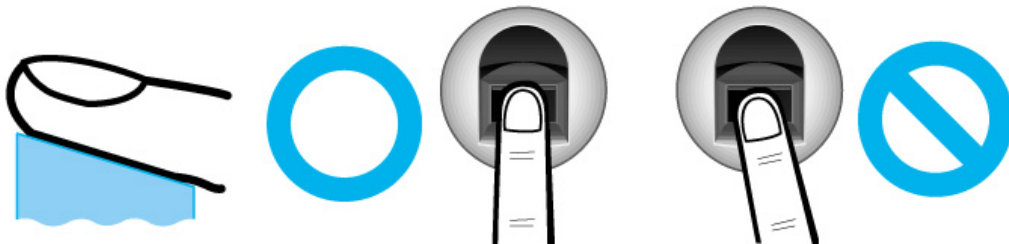
1.8. Correct fingerprint registration and input methods

The AC6000 makes it easy for scanning fingerprints. The color LCD will show a picture of the fingerprint on the display, this picture is not saved, only displayed. This can be used as a guide when scanning your finger. When registering or scanning a fingerprint, the user should see their fingerprint on the LCD; they should check the alignment and placement of their finger on the sensor window. Below are examples of fingerprints during various conditions. After your fingerprint is properly scanned you will hear a 'beep' sound from the terminal.



- Correct fingerprint registration methods

Place your index finger on the window just as you do with a finger stamp.
Do not use the tip of the finger.
Make sure the center of your finger touches the window.



- Use your index finger if possible, it is the easiest for orientation and guarantees a stable input method. Using the thumb or baby finger can be awkward and may result in a bad image.
- Check if your fingerprint is unclear or damaged. It is tricky to recognize fingerprints on dry, wet, unclear, or injured fingers. Use another finger in this case.



- Be aware of certain fingerprint conditions

Depending on the user's fingerprint condition, some fingerprints may not be used or may cause an inconvenience.

- If the fingerprint is damaged or very unclear, then it cannot be recognized. Please use a password instead in this case.
- When a finger is dry, breathe on the finger for smooth operation.
- For kids, it may be tricky or impossible to use the terminal because their fingerprints are too small or very unclear. It is recommended to register their fingerprints every six months.
- For the elderly, it may not be possible to register their fingerprints if there are too many fine lines on the fingerprints.
- If fingerprints are very unclear, it may be convenient if you register 2~3 fingerprints.
- It is recommended that you register more than 2 fingerprints.

1.9. Ultraviolet (UV) Option

The UV function is for sterilizing the window surface of the fingerprint sensor. This is available as an option only. The UV will turn on if the approach sensor is inactive and the fingerprint window cover is closed. You should see the UV icon turning blue and white when it is active, and the blue LED inside the fingerprint sensor window will be on. When the approach sensor is activated (person is near the terminal) or the fingerprint sensor door is opened the UV will turn off. Also in order to conserve the life of the UV LED the LED will turn off automatically after 20 minutes.

2. Introduction

2.1. Features

New Features in V1.20 Firmware

- Application Mode – Shift Management
 - Application Mode – People Counter
 - Application Mode – Cafeteria
 - Programmable Fingerprint Template Format
-
- Access control system using LAN
 - Communication between the unit and the authentication server is done through a UTP cable and TCP/IP protocol, so an existing LAN can be used. This guarantees network-based administration and monitoring as well as easy expansion, high reliability, and higher speed. The AC6000 can work on 10 or 100mb LAN.

 - Convenient Auto Sensing function
 - Simple authentication process without any key input; simple fingerprint touching is sufficient.

 - Camera Sensor
 - Camera options are available to take a picture of authorized or unauthorized users. Capable of 12,500 pictures used for user pictures and/or log data pictures.

 - USB Operation
 - USB 2.0 Host (memory stick) or USB Client (to computer). The USB operation allows import of firmware upgrading, user background images, languages, pictures or information from another terminal. The USB can export log data, picture data or terminal information to be transferred from terminal to terminal or terminal to computer.

 - Simple authentication using fingerprints
 - Fingerprint authentication technology prevents users from forgetting passwords, cards or stolen keys or cards, etc. This is a good way to improve security level.

 - High processing capacity of terminal and server
 - When a server is used there is no limitation on user information. Even in standalone operation by using local terminal, it is possible to manage fingerprint authentication of more than 50,000 users (in optional case).

- Color LCD Touchscreen

- A colorful 16bit LCD ensures easy operation for the user. The display will show various windows during the authentication process and registration to ensure the user of correct operation. In order to conserve the life of the LCD, the LCD will turn off during no operation conditions. When any message or popup window is displayed touching anywhere will close or cancel the window.

- Touch Buttons

- The function keys and call button are specially designed for easy operation.

- Customized Look

- The main screen can be customized by adding any background (customer logo), and also can be programmed to automatically change everyday at midnight. The background wallpaper should be 800x480 in jpg or bmp format. Icons can be moved anywhere on the main window.

- Door phone

- Easy visitor identification and convenient response.

- Various and flexible access controls

- No risk of rent, forgery, or loss of keys or cards
- Perfect control by assigning different security clearances to each user or group
- Flexibility provided by allowing limited time for entry/exit
- Low maintenance
- No need to issue visitor card for visitor

- Various applications

- Time & Attendance
- Meal/Cafeteria
- Access Control
- Various operation modes depending on the terminal menu settings

- Enhanced security with detection of fake finger

- Adopted detection technology of fake finger enhances security level.

- Translatable and Customizable Text

- All text can be translated or customized to the user's native language using an external application. The text can be imported via USB without having to upgrade the firmware. This can also be used for customizing labels on items.

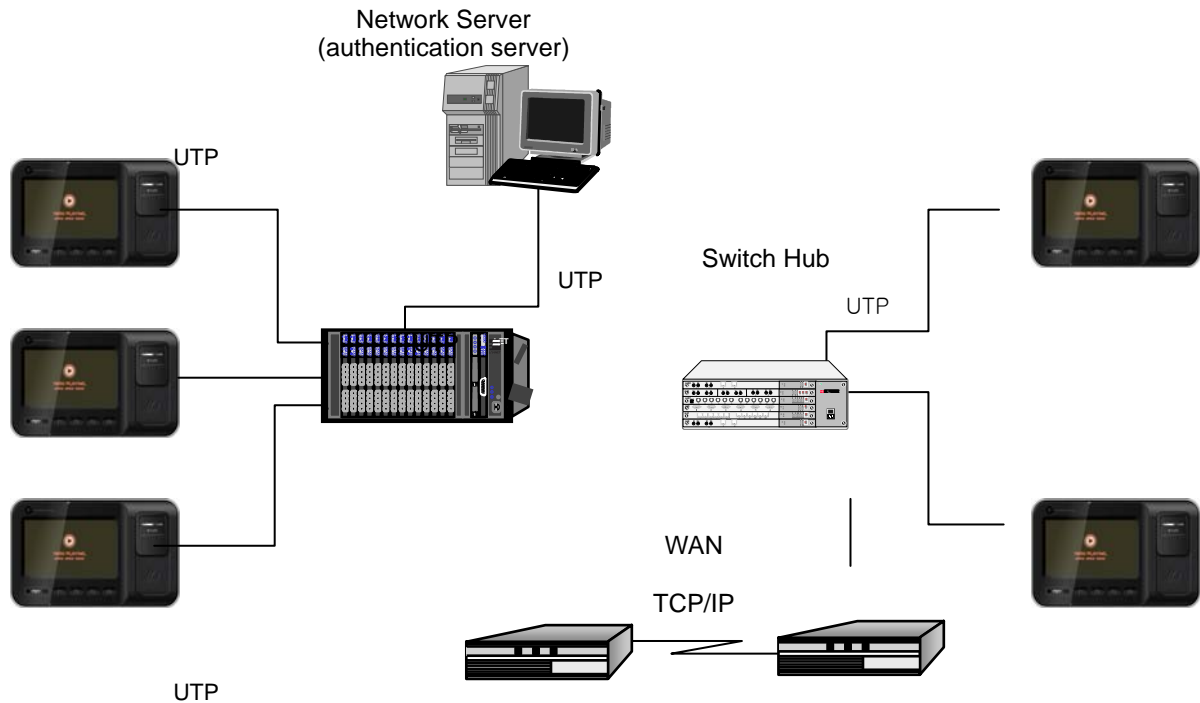
- Various registration and authentication methods

- There are a total of 12 registration and authentication methods (4 methods if the card reader is not installed), so you are required to select one method before registering users and an administrator.

Registration	Registration and authentication method
FP	Fingerprint registration Fingerprint authentication
ID&PW	Password registration Password authentication after ID input
FP PW	Fingerprint and password registration Fingerprint or password authentication
FP&PW	Fingerprint and password registration Password authentication after fingerprint authentication
RF	Card registration Card authentication
RF FP	Card or fingerprint authentication
RF&FP	Card and fingerprint registration Fingerprint authentication after card authentication
RF PW	Card and password registration Card or password authentication
RF&PW	Card and password registration Password authentication after card authentication
ID&FP RF&FP	Card and fingerprint registration Fingerprint authentication after ID input or fingerprint authentication after card authentication
ID&PW RF&PW	Card and password registration Password authentication after ID input or password authentication after card authentication
RF & PW & FP	Card and Password and Fingerprint. A Card is required, then password, then fingerprint.

2.2. Configuration

2.2.1. Network configuration



2.2.2. Standalone configuration



2.3. Specifications

ITEM	SPEC	REMARK
CPU	32Bit RISC CPU	
MEMORY	128M/256 DDRAM	
	256M FLASH (Default)	
Fingerprint sensor	Optical	
Authentication speed	<1 sec.	
Scan Area / Resolution	12.9 * 15.2mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Communication Port	TCP/IP, RS-232, Wiegand	
	RS-485 (Option)	
Temperature / Humidity	-10 ~ 50 / Lower than 90% RH	
LCD	800x480 TFT LCD	
Display Area	103.8 x 62.28 mm	
AC / DC Adapter	INPUT : Universal AC 100 ~ 250V	
	OUTPUT : DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Option	RF Card Reader	EM Card, 125kHz
	Smart Card Reader	13.56MHz
	Door phone	
	UV	
Users	100,000	
Fingerprints	100,000 1:1 12,000 1:N (128MB DDRAM) 30,000 1:N (256MB DDRAM)	


3. Device configuration settings

3.1. Terminal Setup

The terminal should be setup by the administrator prior to using. The terminal configurations allow different setup options for the fingerprint sensor, card reader, add/delete modify users, view log information, set time/date, change languages etc. It is important the administrator setup the terminal to the desired settings before using. This section will describe each setting and show a picture of the required window when setting the option(s).

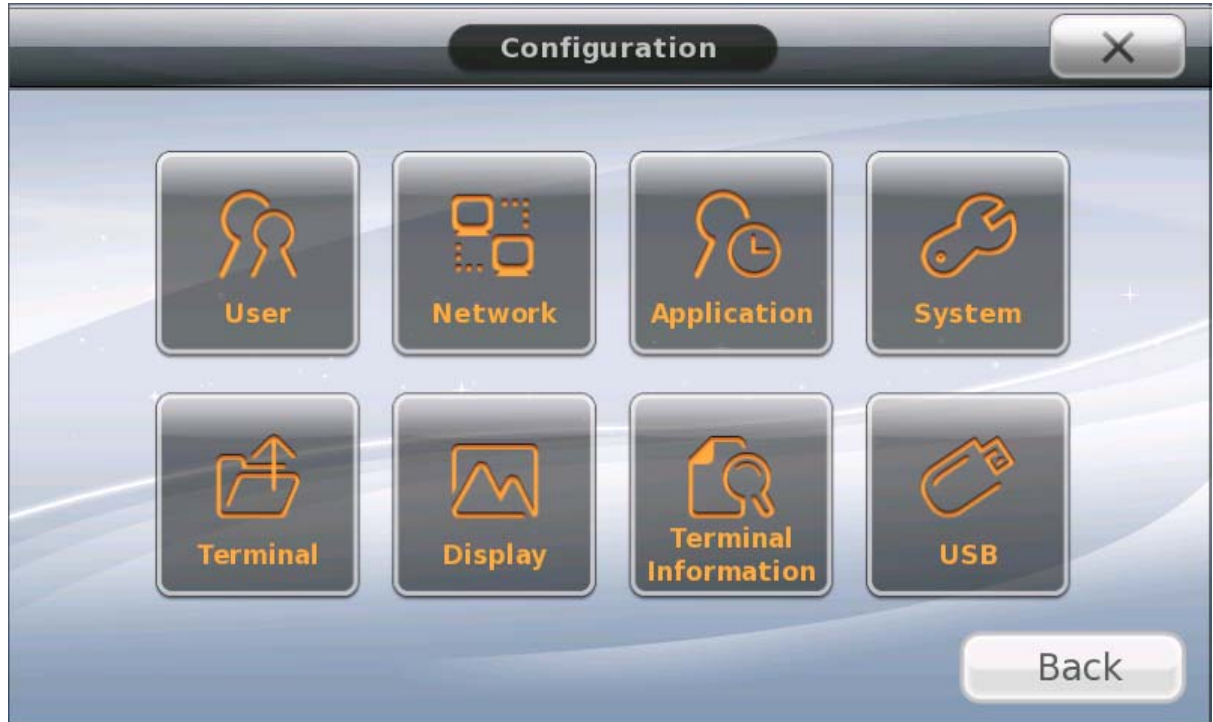
Note: It is highly recommended that all the terminal settings, users and log data are backed up regularly, either to the server program or USB device. See section [3.9.1. Database Export](#) for backing up to USB.

3.1.1. Entering Administrator Programming

From the Main Screen touch the  icon to enter administrator mode. If there is an administrator programmed they will be required to authenticate with a fingerprint, card or password. While in administrator mode if no Touchscreen activity occurs within one minute the terminal will return to the main screen. Before starting the administration programming it is recommend you read section [1.7. Touchscreen Usage](#)






3.1.2. Administrator Main Screen



3.1.3. Programming Reference Chart

This chart is a summary of each programming option available; it will help you quickly locate the option you need to program. Use this chart as a reference.

Operation Icon	Description
	<p><u>User Management</u></p> <ul style="list-style-type: none"> Add Delete Modify View Delete All
	<p><u>Network Settings</u></p> <ul style="list-style-type: none"> Server IP address Terminal IP address Server Port Gateway Subnet Mask DHCP or Static Terminal ID Number
	<p><u>Application</u></p> <ul style="list-style-type: none"> Time & Attendance mode Access control mode Cafeteria mode Shift Management mode People Count mode Function key settings Time schedules



System Settings

User ID Length

Authentication Method

- terminal/server
- server/terminal
- server only

Fingerprint Template Format

- Union
- ISO Standard
- ISO Extended

Fingerprint Sensor

- 1:N level
- 1:1 level
- Fake finger level
- Enhanced Registration
- Multiple Fingerprints



Authentication

- user ID/Group ID
- user display option
- 1:N matching
- Card only

Date/Time Settings

Database control

- compress user data
- delete All Users
- clear settings
- clear log data
- clear picture data
- delete all

	<p><u>Terminal Settings</u></p> <p>Sound Settings</p> <ul style="list-style-type: none"> - voice volume - sound volume <p>Wiegand</p> <ul style="list-style-type: none"> - Site Code - Format <p>Terminal Options</p> <ul style="list-style-type: none"> - lock/unlock terminal - Case Tamper Audible - Card Reader <p>Door Options</p> <ul style="list-style-type: none"> - Door monitor (enable/disable) - Normal open/close - Lock type (motor/strike) - Open warning time - Open Time
	<p><u>Display Settings</u></p> <p>Theme</p> <ul style="list-style-type: none"> - main background - daily update - arrange icons <p>Camera</p> <ul style="list-style-type: none"> - display options - save options <p>Language</p> <p>LCD Options</p> <ul style="list-style-type: none"> - screen saver timeout - Touchscreen calibrate
	<p><u>Terminal Information</u></p> <p>System Information Terminal Information Ethernet Information User Capacity Summary Log Data Summary View Log Data</p>



USB Operation

Import to AC6000 from USB


- system options
- user data
- background images/languages
- firmware upgrade

Export from AC6000 to USB

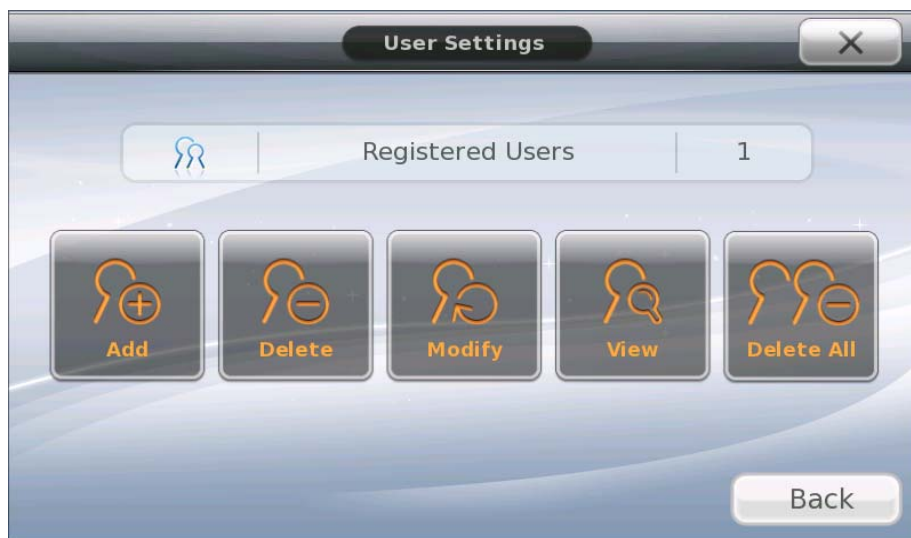
- User data
- Event Log
- System Options
- Picture Data
- All

3.2. User Management



Touch the  icon to enter the user management area.

In the user management section you can add, delete, modify, view all, or delete all users in the terminal. This window will show you how many registered users are in the terminal.



3.2.1. Registering a User



When registering a user the following steps are necessary.

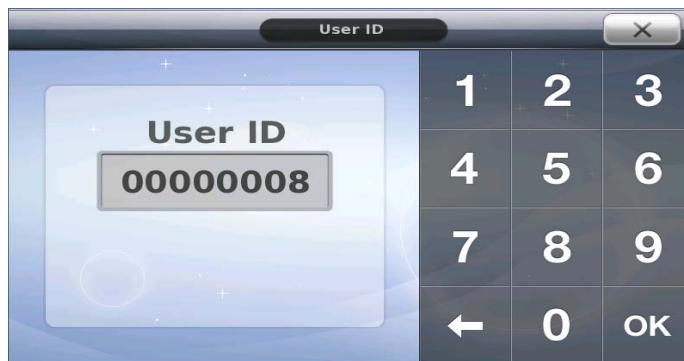
- 1) Assign a user ID number for the user. The terminal will automatically choose the next available number, if you do not want this number; enter your own pre-assigned value.
- 2) Determine how the user will be authenticated. Fingerprint, card, ID, password or combination.
- 3) Register the user's fingerprint, card or password first.
- 4) Choose the authentication type for this user. i.e. fingerprint only, fingerprint with card, id and password, etc. (See section [3.2.1.5. Authentication Type](#))
- 5) If a user picture is required for the database, take the user picture.
- 6) Select the user as an administrator or regular user.


The following is a step by step guide on registering a user.




Touch the  icon to register a new user.

A window will appear to enter a user ID. This is an identification number that uniquely identifies the user in the system. This window will always show the next available user ID number.



Touch  to use the current displayed number. OR

To enter a new ID number touch the  until the id is blank, then enter the user ID number you wish to use

When finished entering the user ID number touch 

If the user ID is already used in the terminal you will hear an error sound and a message will show.

3.2.1.1. User Registration Window

After the OK button is touched a window will be displayed with all the user information. If some options are not programmed for the user they will not show until they are programmed.

The screenshot shows the 'Add User' window with the following callout boxes:

- User database picture if picture is taken. Use Picture Button**: Points to the user's photo.
- Status area displays - number of fingerprints number of cards password authentication type 1:1 or 1:N User**: Points to the 'Status' section showing 'FingerPrint Only', '1', '1', and '1:N'.
- Select the user as Administrator or Regular User**: Points to the radio buttons for 'Administrator' and 'User'.
- Save the user information when finished.**: Points to the 'Save' button.
- Touch these buttons to cancel without saving any changes**: Points to the 'Cancel' button and the 'X' close button.

Once your user settings are finished touch the SAVE icon to save the user information. If you touch the Cancel or X icon your user settings will not be saved.



3.2.1.2. Registering a Fingerprint

Touch the finger registration button. You will have 30 seconds to complete this process before the window automatically closes. When registering a fingerprint you are required to enter the finger two times for verification. If more than 5 fingerprints are already registered for a user this icon will not appear, to cancel the process at anytime just touch the fingerprint registration window.

- 1) Place Finger on fingerprint sensor window



- 2) Remove finger from fingerprint sensor window



- 3) Place same finger on fingerprint sensor window



- 4) Finished, Successful



If successful the window will close automatically or you can touch the window to close it, to register another fingerprint touch the finger register icon again. In the status area of the user

window the fingerprint icon will appear with the number of fingerprints for that user.

If unsuccessful you can enter your finger again and repeat steps 1-5, or touch the window to finish.

Note: If the option 'Enhanced Registration is enabled and the user fingerprint is already registered under another ID number, the registration will fail. See [3.5.2.4. Enhanced Registration](#)



3.2.1.3. Registering a Card

Touch the card registration icon. You will have 30 seconds to scan your card to register it before the window automatically closes. Follow the messages that are displayed on the window. If more than 5 cards are registered for the user this icon will not appear.

- 1) Scan your card



- 2) Successful card registration.




If successful the window will close automatically or you can touch the window to close it, to register another card repeat steps touch the card register icon again. A success sound will be heard and a card icon with the number of cards will appear in the status area of the user window.

3.2.1.4. Registering a Password



Touch the password registration icon. When registering a password you must enter a unique 1-8 digit number. You must re-enter the number to confirm the password. After 10 seconds the window will close automatically.

- 1) Password screen will appear, touch  anytime to cancel.



- 2) Enter your password.



- 3) Touch OK when finished.



- 4) Re-enter the same password to confirm, touch OK to finish



If a mistake is entered when confirming, a popup window will appear and you will hear an error tone sound. Repeat the process again. If successful you will hear a success sound and the password icon will appear in the status area of the user window.



3.2.1.5. Authentication Type

There are up to 12 different ways a user can be authenticated at the terminal, this provides flexibility for users who do not have a card, or have an unreadable fingerprint, or where extra verification is needed for authentication. This depends on the setup by the administrator.

The four basic authentication methods are:


- Fingerprint
- Card
- ID
- Password

Combinations of the four basic methods are available.

- 1) **Fingerprint Only** – the user can enter their fingerprint on the fingerprint sensor and the terminal will authenticate the result.
- 2) **Card Only** – the user can swipe their card at the terminal and the terminal will authenticate the result
- 3) **ID & Password** – the user enters their ID, the terminal will request the user to then enter their password.
- 4) **Card & Fingerprint** – the user swipes their card at the terminal then the terminal will request the user to enter their fingerprint.
- 5) **Fingerprint & Password** – the user enters their fingerprint on the fingerprint sensor and then the terminal will request the user to enter their password.
- 6) **Fingerprint OR Password** – the user can either enter their fingerprint only, OR the user can enter their ID followed by their password.
- 7) **Fingerprint OR Card** – the user can either enter their fingerprint only OR swipe their card only.
- 8) **Card OR Password** – the user can either swipe their card OR enter their ID followed by their password.
- 9) **Card & Password** – after the user swipes their card the terminal will request the user to enter their password.
- 10) **ID & Fingerprint OR Card & Fingerprint** – after the user enters their ID the terminal will request the user to enter their fingerprint OR the user can swipe their card, then the terminal will request their fingerprint.
- 11) **ID & Password OR Card & Password** – this is a combination of #3 or #9. The user can enter their ID followed by their password OR swipe their card first then enter their password.
- 12) **Card & Password & Fingerprint** – The user must enter their card first, followed by their password, then their fingerprint. If the card is not entered first the authentication will fail.

Note: For password authentication the user must always first enter their ID.

Touch the auth type icon to select the authentication type for the user. A window with different options will appear. Just touch the appropriate authentication type icon for the user.

Touch  to cancel and close the window at anytime.



After you have touched the appropriate authentication button type the window will close and the authentication type you selected will be displayed in the status area of the user window.

Note: The authentication type should only be programmed after a fingerprint; card or password has been registered. If they have not been registered you cannot select any options for authentication.



3.2.1.6. User Fingerprint Options

User fingerprint options only apply if a fingerprint has been registered. These options are advanced features, and should only be set if needed. If no fingerprint is registered for the user this icon will not be visible.

There are two options available


- 1) 1:1 Verification Level – this is the ‘security level’ of the registered fingerprint. The higher the number, the higher the security level. There is a higher chance of authentication failing if the security level is too high. If you need a specific user to have a higher or lower fingerprint authentication level you can set this value. Some user fingerprints may be difficult to read or some users require higher security.

If this value is programmed as 0 then the fingerprint authentication 1:1 level will follow the value that is programmed in [3.5.2.2. 1:1 Level](#).

1= low security level, 5 = higher security level.

- 2) 1:N Enabled/Disabled – 1:N means One to many. This means the user’s fingerprint is matched only by comparing fingerprint information. If this option is disabled the user is then 1:1, the user will be required to enter their ID number first then enter their fingerprint for authentication. If this option is disabled and an attempt is made to enter a fingerprint only, the terminal will not allow access.

Touch the finger options icon and a window will appear with the current 1:1 level. Enter a value from 0-5.

Touch  to cancel and close the window at anytime.

Enter the value, the touch OK.



The next window will appear. Touch OK to enable 1:N or Cancel to disable 1:N.



3.2.1.7. User Picture Registration

A user database picture is not required for authentication. It is used for displaying on the LCD when the user is authenticated at the terminal or displaying on the server. It is a quick and easy way to identify the users in the terminal without having to know their ID number.

Registering a picture is easy; just touch the camera icon. The picture should show in the center of the user information window. You can touch the camera icon as many times as you wish until you are satisfied with the picture. The picture will not be saved until you touch the save icon when exiting the user area.

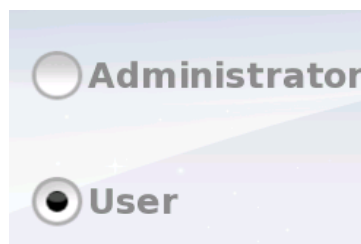
Note: You must enable the display picture option see section [3.7.2.3. Camera Display Options](#) in order to take the user picture in the user registration area. If you do not enable this function the user picture will not be taken when you touch the camera icon button. This is to ensure unnecessary pictures are not added to the database.

3.2.1.8. User Type (Normal/Administrator)

A normal 'User' has standard privileges in the terminal. An administrator can change terminal options, add/delete/modify users, view log reports, etc.

Note: When setting a user as Administrator you will be required to authenticate before entering program mode. You should make note of the user. If you cannot remember the user credentials you cannot enter programming mode. If you forget the user, from UNIS server program you must upload the users from the terminal and then delete the administrator user from the terminal.

- 1) Touch the appropriate dialog button for the user type. Touching the button or the text will select the option.



3.2.2. Deleting a User



The deleting user option will allow you delete a single user. If you delete a single user you must know the user ID of the user you would like to delete.



Touch the icon

- 1) At this time you can enter the user ID number of the user you wish to delete. Touch OK when finished. At anytime touch the X icon to cancel.



- 2) If OK is touched a message will ask you to confirm your selection, touch OK to continue to delete the user.



3.2.3. Modifying a User

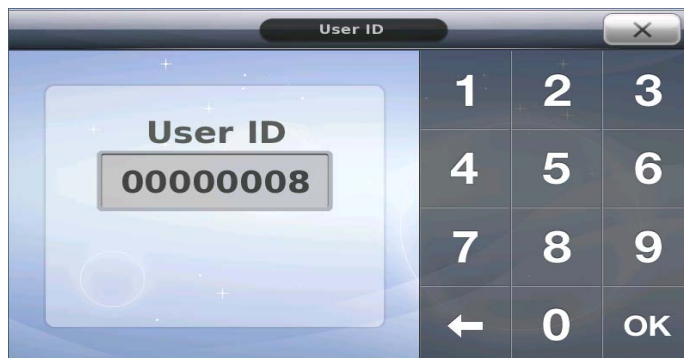


Modifying an existing user requires that you know the user ID of the user you wish to change. You must enter the user ID to change the user settings.



Touch the icon to modify an existing user.

A window will appear to enter a user ID. Enter the user ID you wish to change.



Touch  icon if you have made a mistake when entering a number



When finished entering the user ID number touch

If the user does not exist you will hear an error sound and a message window will show.

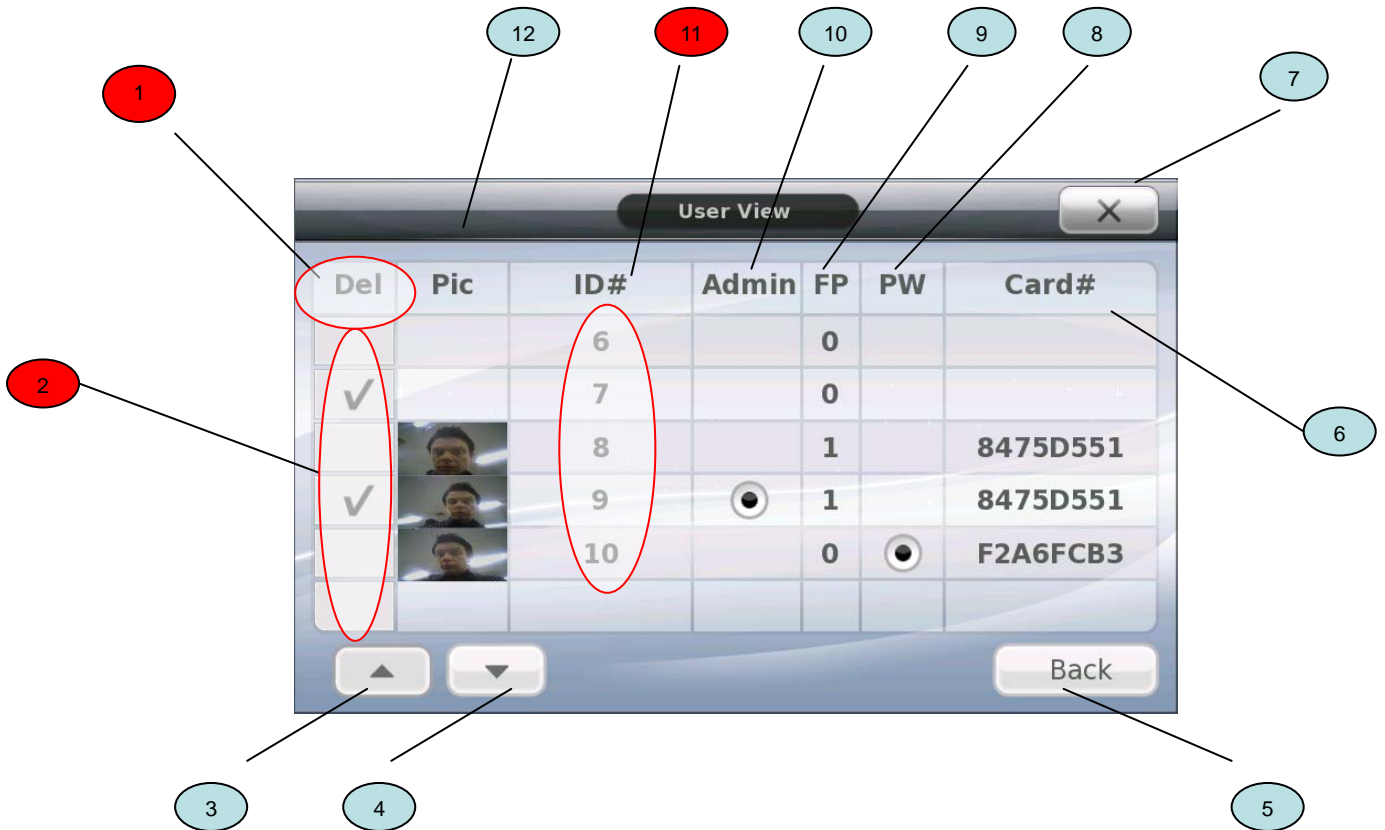
If successful you will see a user information window, See [3.2.1.1. User Registration Window](#). Repeat any steps in section 3.2.1.X to add a new fingerprint, card, and password or change other options. Touch the save icon when finished.







3.2.4. Viewing Users

The viewing users screen is an interactive screen. There are areas in which you can touch to select to delete users, or select an individual user for modifying. A maximum of six users can be displayed on one window at a time. The areas marked in red are interactive and can be touched for selection.



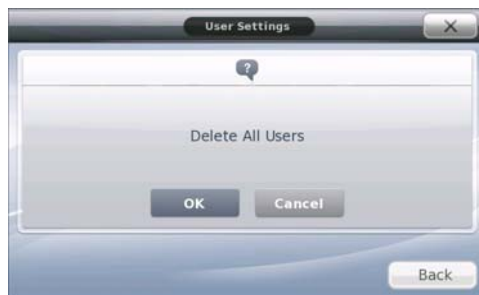
Number	Description
1	Delete Column Title. This area is interactive. If this title is touched you will be asked to delete the selected users you have checked. (using #2)
2	Delete Row Selection Box. Select the users you wish to delete. If a user exists on this row touch the box in the column beside the user picture, a check mark will appear. Touch again and the check mark will disappear.
3	Up Icon. Similar to scrolling backward. Touching this will go to the previous page of six users.

4	Down Icon. Similar to scrolling forward. Touching this will go forward through the list of users. If you have reached the maximum users this button will not do anything
5	Back Icon. Touch this to exit
6	Card Number Column. If the registered user has a card, the card number will be displayed.
7	Close Icon. Same as #5. Touch this to exit.
8	Password Column. If the registered user has a password, an  icon will show.
9	Fingerprint Column. This area will show the number of registered fingerprints for the user.
10	Administrator Column. If the registered user is an administrator, an  icon will show.
11	ID Column. This column is interactive. It will show the user id of the registered user. If you touch the user ID number (for example, 6, 7, 8 ,9 or 10) you can automatically go to the user modify area for the user ID you have touched.
12	Picture Column. If the user has a registered picture it will appear in this column.



3.2.5. Deleting All Users

This option allows you to delete all registered users in the terminal. After selecting the option a popup window will confirm if you would like to delete all users. Press OK to delete all or cancel if you do not wish to delete all users.



3.3. Network Settings



The networks settings area allows you to setup IP addresses, gateways, subnet mask, DHCP or static settings, Terminal ID Number or wireless settings. See section [1.7. Touchscreen Usage](#). When selecting DHCP ensure that your network has a properly enabled DHCP server available. Also you should give time for the terminal to acquire the DHCP address; usually this can take from 1-60 seconds. While in this menu if you press the DONE button the server will be disconnected and the link will be reconnected to the server. You can re-initiate the network connection by entering this menu and pressing done.

Ethernet Setup Procedure:

- 1) Setup Static OR DHCP
- 2) If Static then set the terminal IP/Subnet Mask and Default Gateway.
- 3) Set the Server IP Address, PORT and Terminal ID
- 4) If using Wireless go to Wireless Options and Press “Available Networks” until your router appears in the available network window.
- 5) Press/Select the station you wish to connect to, it should be highlighted.
- 6) Go to wireless advance settings to set the Security Level/Rate or Channel.
- 7) Press Done.

Pressing DONE will disconnect the current connection and then try to re-establish a new link from the setup parameters that were just entered. At anytime press the X button to cancel and not save any changes.

3.3.1. Terminal ID Number

The terminal ID number uniquely identifies the terminal on the server program network. For every terminal on the server network you should program a different terminal number. This value should be 1-8 digits in length.

For static IP usage you must program the Terminal IP, Subnet Mask and Default Gateway. If DHCP is selected, these values cannot be programmed and will be grayed out. The port number must match the port number that is programmed in the Authentication Server.

- 1) Touch the field you wish to change




2) A number pad will appear, and the field will be highlighted of the data you wish to change.



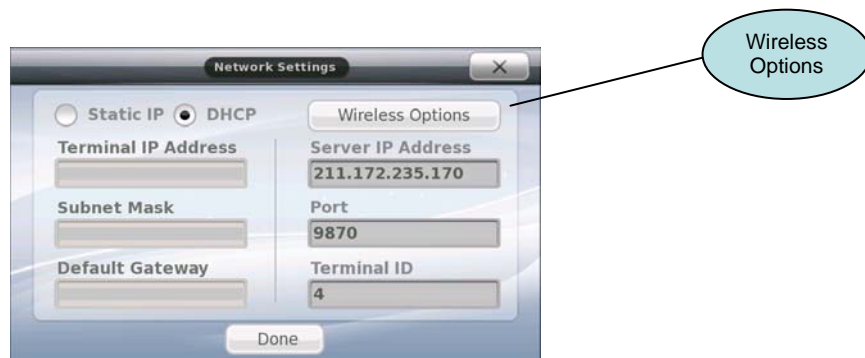
3) Touching the number will erase the current data. Just enter the number you wish to use. Touch OK when finished, or arrow key to re-enter the data.



Touch  to cancel and close the window at anytime, any data that was entered will not be saved. To save the data touch 'Done'.

3.3.2. Wireless (WiFi) Settings

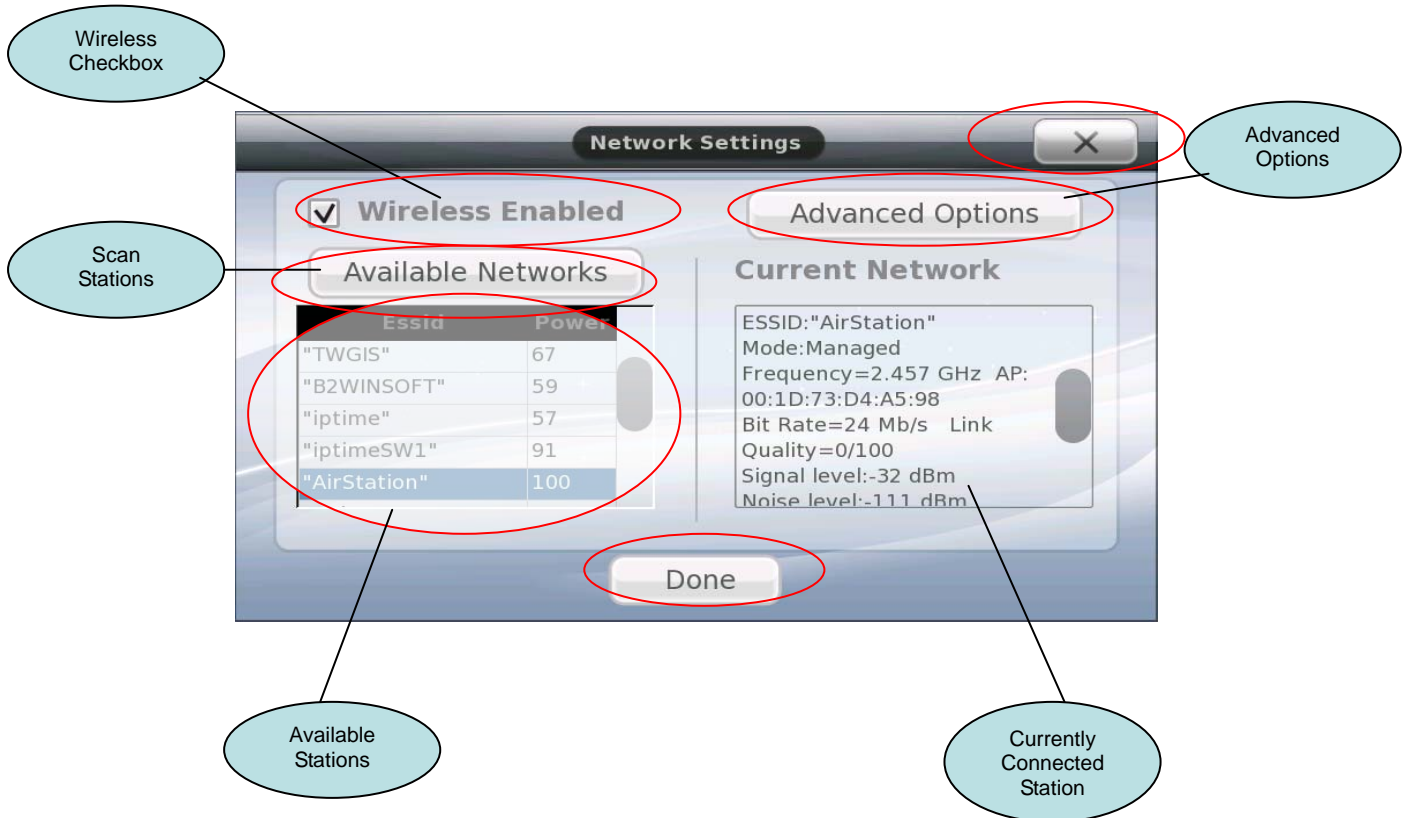
The AC6000 wireless only supports one type of USB WiFi dongle. This may be plugged into the AC6000 by opening the back casing. When a USB dongle is plugged into the AC6000 you will see a new button in the wireless settings called Wireless Options. All network settings should be complete before entering the Wireless Options area. Set Static/DHCP, IPs and terminal id before entering this menu.



After pressing the Wireless Options button a popup window will show as below, the wireless device will search for stations in the area.



Only one communication link is possible at one time, if you select (checked) Wireless Enabled then all network communication will be done with wireless. The hardware LAN connection will not be used, even as a backup. You must disable (uncheck) the Wireless Enabled checkbox to use the hardware LAN connection. The areas marked in RED are touch interactive.



Wireless Checkbox – If checked, wireless will be used to communicate on the network connection

Available Networks – if the button is pressed a scan of available networks in the area will be

done and a message like the above window “Searching for Wireless Stations..” will appear.

Available Stations – After the scan is complete a list of available stations will appear, the station should have ‘broadcast essid’ on. Once you find the station you want just press the row that has the name of the station you want to connect to. The station that is currently connected will be highlighted in dark blue.

Current Network – this area will provide information about the currently connected station.

Advanced Options – Press this button to set advanced settings (Rate/Channel/Encryption Type)

3.3.2.1 WiFi Advanced Settings

The advanced WiFi settings are used for setting the security level (encryption/authentication), tx rate and channel. Normally the Tx Rate and Channel can remain at “Auto” unless your wireless station is configured for a specific channel or Tx Rate. Usually you will change the channel when there are other stations in the area, on the same channel, that interfere with the wireless communication. Each area in this window is a pull-down combo box; select the appropriate setting you wish to use. You should set these settings to match the configuration of your wireless router. You should know these setting before setting the AC6000 wireless.

Wireless Router – channel, tx rate, authentication type, encryption type.

WEP Encryption Key, WPAPSK password.



Security Level – this is the authentication type (how the wireless connection is established) and encryption type (how the data is secured when communicating). There are five levels of security.

Level 0 = none, the terminal will connect to any available station that has an open authentication without encryption enabled or authentication type.

Level 1 = Open authentication, WEP (Wired Equivalent Privacy) – basic encryption 64 to 128bit encryption

Level 2 = Shared authentication, WEP – shared key – 64 to 128bit encryption

Level 3 = WPAPSK authentication, TKIP encryption

Level 4 = WPAPSK authentication, AES encryption

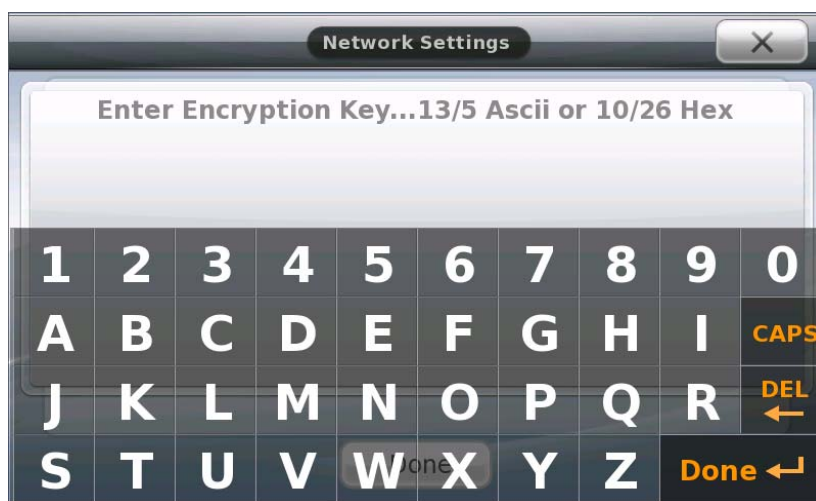
When selecting Level 1 or 2 this window will immediately show. This is the WEP encryption key. You will be required to enter a 13 or 5 digits Ascii Encryption key or a 10 or 26 digit Hex value. This value should match the encryption key that is set in the wireless router. Hex values are from 0 – F. Ascii values can be any key value. If a value is already entered it will show '*'. You can press Done to finish, Del to delete (backspace) or CAPS to change the case from A to a, B to b, etc.

Ascii 13 digit example = 'ac6000test123'

Ascii 5 digit example = 'test1'

10 digit hex value example = 'abcdef123456' = 64 bit

26 digit hex or 13 digit Ascii = 128 bit



When selecting Level 3 or 4 an encryption key is not required, for this type of encryption (TKIP/AES), the router will auto generate an encryption key and change it dynamically. However you must enter an authentication password to logon the router. See the window below. Here you must enter the WPA/PSK password which was setup in the router. Enter 8 to 63 digits.




3.4. Application Settings

In Application programming area you can setup the terminal in 1 of 5 Application Modes. The terminal can only operate in one mode. The top status bar will show the current mode of operation and the icon will be highlighted.

3.4.1. Access Control Mode


Time schedules are not programmable in this mode. An Access Control application is normally used for providing access to a secure area, function keys are not needed unless extra tracking of the user is needed. If the system is setup for Access Control and Function keys are used for authentication the user is required to touch the mode function key before entering their ID, Card or Fingerprint. See Section [5.4.1. Access Control Application](#)

Touch the  icon to change to this mode.



3.4.2. Time & Attendance

Time schedules should be programmed when using this mode. Time and Attendance Application is for systems that require tracking of employee's work time. If the system is setup for Time and Attendance, for authentication the user is required to touch the function key before entering their ID, Card or Fingerprint. See Section [5.4.2. Time & Attendance Application](#)

Touch the  icon to change to this mode. A time schedule icon will appear.

3.4.2.1 Time & Attendance Schedules



Touch the icon to change the start time, normal time and finish time. For programming the times see section [1.7. Touchscreen Usage](#). Touch the area you wish to change and a number pad will appear for you to enter your data. Touch 'Done' to save and finish. For each area enter a time range that best represents that time.

Each field requires two time entries; this is a range for example start time is from 08:00 to 10:00



Start Time: This is the time that represents the start of the day, a normal time range of when the employees arrive at the office for that day.

Normal Time: This is the time between the start time and finish time, the time of normal working hours.

Finish Time: This is the time that represents the end of the work day, normally when employees begin to leave the office for the day.

3.4.3. Meal Application



Meal Application is for systems that require tracking of user's meal time. If the system is setup for Meal mode; for authentication the user is required to touch the mode function key before entering their ID, Card or Fingerprint. See Section [5.4.3. Cafeteria Application](#)



Touch the icon to change to this mode. A time schedule icon will appear.



3.4.3.1 Meal Mode Schedules



Touch the icon to change the start time, normal time and finish time. See section [1.7. Touchscreen Usage](#). Touch the area you wish to change and a number pad will appear for you to enter your data. Touch 'Done' to save and finish. Each programmable time area is self explanatory. For each area enter a time range that best represents that time. Each field requires two time entries, this is a range for example Breakfast Time is from 08:00 to 10:00.

Ticket Print Check Box: Touch this area to enable/disable the ticket print. This option will enable the option to print a record at each transaction. A serial printer is required to be connected to the AC6000 terminal – See Installation guide for connection instructions.

Allow Duplicate Check Box: When this box is checked the user will be allowed multiple meals in one meal period. If this box is unchecked the user will only be allowed one meal per meal period.



3.4.4 Shift Management



Shift management application mode is used for applications that require control of employee's shift's (start/end/break/meals). This mode is similar to time/attendance. When selecting this mode, function keys are not used (F1-F4 are automatically disabled). You will see an 'Options' icon appear when selecting this mode. See Section [5.4.4. Shift Management Application](#).

There are six transaction modes in shift mode

Start Shift, End Shift, Start Break, End Break, Start Meal, End Meal.



3.4.4.1 Shift Management Options



Smart Checking Check Box: When checked the terminal will check the previous transaction to make sure the transaction occurred in correct order. For example, Meal, Break cannot start unless the shift has started, or you cannot end a transaction unless it has been started. If this option is not checked then transactions can occur in any order.

Transaction Interval (secs): Program a value from 000-999 to set the minimum amount of time between transactions. For example, if a user 'Starts Shift', they cannot 'Start Break' for unless this period has elapsed. The default value is 1minute. A user must wait 1 minute between transactions.

3.4.5 People Count



People count application is used in applications which connect an external sensor to the AC6000. The external sensor provides a relay output which activates when a person comes IN or OUT of an area which is setup by the sensor. The AC6000 will count the number of IN/OUT instances from the external sensor. The sensor is not provided by Union Community. When set in People Count Mode, function keys are not used and there are no options to program them. See section [5.4.5. People Counter Application](#)

Two sensors can connect to the AC6000.

M0 input = Zone 1 Out Relay

M1 input = Zone 1 in Relay

IO = Zone 2 In Relay

M2 = Zone 2 Out Relay



3.4.6. Function Key Programming



Function Keys can be used for a variety of different applications. They are used to identify the current mode of operation by the user. When using function keys the user is required to touch the function key, then authenticate their fingerprint, card, ID number or password. Function Keys are grouped together as a set of four keys. On the main terminal case there are four function keys. These keys are 'touch less', meaning that your finger does not need to touch down on the key, they will sense your finger when it is close to the key. These four buttons are the same function keys that are displayed on the main screen; the operation is the same. The function keys on the main screen will have different names depending on the system setup.

Application Mode Function Keys – F1, F2, F3, F4

Time and Attendance Function Keys – Attend, Leave, Out, In

Cafeteria/Meal Mode Function Keys – Breakfast, Lunch, Snack, Dinner

See the ICON list for a description of each function key.

3.4.6.1. Extended Function Keys

In some cases additional function keys are needed in addition to the four main function keys. The administrator will setup the terminal for this operation. Up to 60 additional function keys are available. Five pages of 12 function keys can be used.



On the main screen touching this button will show the extension window. The window will close after 10 seconds of no activity. Next, touch the number key assigned to you by your administrator, this can be any number from 1 – 60.

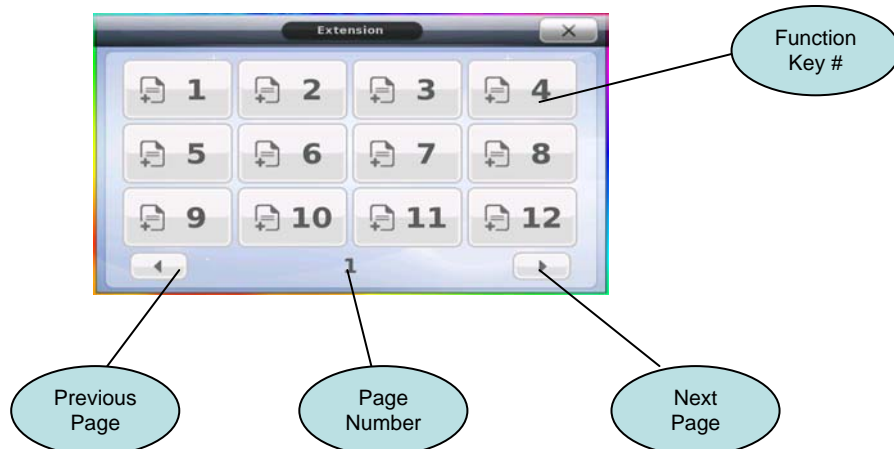
If your number is not displayed then touch the



or




until your number is displayed in the window.



After the number is pressed the top status text (see [5.1. Main Screen](#)) will change the 'Access Mode 1-60. Depending on which number was pressed. Then the user must authenticate

with with their authentication method (fingerprint,card,password or id).

Touch the  icon to change the function key settings.



The four function keys on the terminal case are the same four function keys that can be displayed on the LCD. To change options just touch the area.

'F1, F2, F3, F4 Enabled/Disabled' – if a check mark appears in the box next to the option the function key is enabled. This also controls the function keys on the terminal case. A function key that is disabled will not produce any action, sound or display on the LCD.

'Display on LCD' – if checked then the four function keys will appear on the main LCD. See Section [5.1. Main Screen](#) for the main screen window.

Note: If the function key is not enabled, it will not show on the main screen.

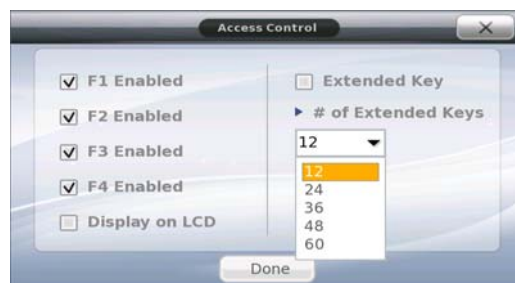
'Extended Key' – if checked then the extended function key can be used. In some cases additional function keys are needed in addition to the four main function keys.



This icon will appear on the main screen now

Note: If 'Display on LCD' is disabled the Extended Key will not show on the main screen.






'# of Extended Keys' – this is a selection box, you can select up to 60 additional function keys. Touch the number box and slide your finger down until the number is selected. The box will close with your number displayed.



3.5. System Settings



System settings allow operational characteristics of the terminal to change. In this screen all you need to do is to touch the icon button on the left (system/display/sound/Date/time/Database/Authentication) and a window with the options will appear on the right. Touching the Done button will close and save the changes. The following options are available in this section.

-  System
 - User ID Length
 - Fingerprint Template Format
 - Authentication Method
 - terminal/server
 - server/terminal
 - server only
-  Fingerprint Sensor
 - 1:N Level
 - 1:1 Level
 - Fake Detection Level
 - Enhanced Registration
 - Multiple Fingerprints
-  Authentication
 - Authentication
 - user ID/Group ID
 - user display option
 - 1:N matching
 - Card only
-  Date/Time
 - Display Format
 - Set Current Date
 - Set Current Time
-  Database
 - Database control
 - compress user data
 - delete All Users
 - clear settings
 - clear log data
 - clear picture data
 - delete all

 System

3.5.1. System Settings

Touch the system icon. Then touch the area which you would like to change.



3.5.1.1. User ID Length

The user ID length can be 2 to 8 digits in length. The user ID length will be the length of the user ID required to authenticate. The user ID length should be the same value that is programmed in the UNIS software. Any place that requires the entry of a user ID will be restricted to the length that is programmed in this area. This value should reflect the amount of users in your terminal. For example, if you have fewer than 100 users than enter 3. If your have more than 10000 users, then program a 6 digit length.

Note: When changing the ID length shorter than the previous programmed value; be aware that an administrator may not be authenticated properly to enter administrator programming if their ID length was longer than the current length. It is recommended this value be changed at the time of setting up the terminal, and not during regular usage.

3.5.1.2. Authentication Mode

One of three options is available for the authentication mode. This setting determines where the user authentication is done, in the server or locally at the terminal, or both. Change this setting when there is high network traffic, many users, or authentication is too slow. The default setting is Server/Terminal.

- Terminal/Server – If the local terminal is properly connected to the network server, the authentication is done at the local terminal and the result is sent to the server in real time. However, if the user ID entered does not exist in the local terminal the authentication is requested at the server.
- Server/Terminal - If the local terminal is properly connected to the network server, authentication is done in the server. If there is a disconnection or communication trouble between the server and terminal the authentication is done at the terminal.
- Server Only – The authentication is done only at the network server.

3.5.1.3. Fingerprint Template Format

This selection combo box allows you to select the fingerprint template type. Some applications using external software (Software development kit) require a different fingerprint template format. This feature should only be changed when customizing your server software.

Note: *When changing the fingerprint template format, all users that are registered with a fingerprint will be deleted and the terminal will reboot. This will re-initialize the terminal for the new fingerprint format change.*

Union Format: This is the default factory format, template sizes are 400 bytes. All features associated with fingerprints (1:1 level, 1:N level, Fake finger, etc) can be used. All of these features are optimized for this format. Selecting any other template formats will not guarantee accurate and fast authentication.

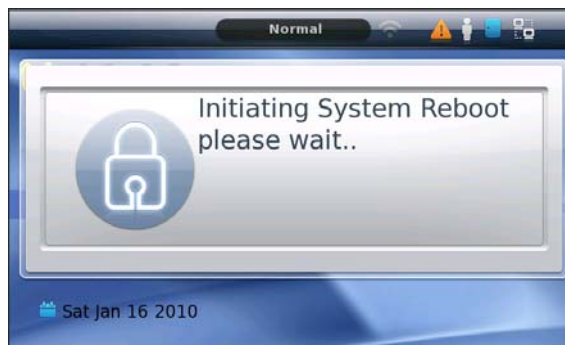
ISO Standard Format: The fingerprint data will be saved as an ISO template with a size of 500 bytes/ template.

ISO Extended Format: The fingerprint data will be saved as an ISO extended template with a size of 600 bytes/template.

After you change the combo box format the message below will be shown. Press OK, will change the combo box to the new format. Pressing Cancel will keep the old value in the combo box.



After pressing 'done' the terminal will exit admin mode and after 3 seconds display the following message. Wait for the system to reboot. If 'X' is pressed your changes will not be saved and the system will not reboot.



3.5.2. Fingerprint Sensor Settings



3.5.2.1. 1:N Level

This option represents the security level between the captured fingerprint (from the sensor window), and the fingerprints stored in the terminal that are marked for 1:N authentication. This level represents the terminal level, not individual users. Possible values are from 3-9. The default value is 5. The higher the value, the higher the security level, which means more comparisons are done on the fingerprint data. If your user's fingerprints have a difficult time during authentication you should lower this value. If you are protecting a high security area then you may want to increase this value. This setting is an advanced setting and normally doesn't need to be changed.

3.5.2.2. 1:1 Level

This option represents the matching security level in the terminal between the captured fingerprint (from the sensor window) and the stored fingerprint in the database for that user. Possible values are from 1-9. The default value is 4. The higher the value level, the higher the security level; however authentication matching may fail since more matching is done on the fingerprint data. For example if a user registered as user ID 1234 and they have also registered a fingerprint, when the fingerprint is captured from the sensor, the terminal will compare the fingerprint data stored in the database for user ID 1234. If you are protecting a high security area then you may want to increase this value. This setting is an advanced setting and normally doesn't need to be changed.

3.5.2.3. Fake Finger Detection

This option represents the detection level of fake fingerprints. This is a combo box, you can select one of four options. The default value is 'disabled'. You should only need to adjust this value in higher security situations.

- Disabled (the terminal will not have any protection against fake fingerprints)
- Low
- Medium
- High

3.5.2.4. Enhanced Registration

If this option is enabled (checked) the terminal will check if the fingerprint is already registered under another user in the system. The fingerprint cannot be registered and an error tone will be heard when registering the fingerprint. This will prevent the user from being registered twice under two different ID numbers. The default is checked.

3.5.2.5. Multiple Fingerprints

If this option is enabled (checked) and the user is registered with more than one fingerprint, the user will be required to enter all registered fingerprints before authentication can take place. This feature can be used in a high security protected area where multiple fingerprints of the same user need authentication.

3.5.3. Date/Time Settings



Touch the Date/Time icon. Then touch the area which you would like to change.



3.5.3.1. Display Format

The Date/Time Display Format will change the way the date and time is displayed on the main screen. Only English Language allows the selection of different formats. All other languages will only have Enable/disable, and the date will appear in their locale format. There are six choices:

- Short form day (three letters), Short form month (three letters), DD, YYYY, HH:MM AM/PM (Thu, Mar 24 2009 08:19AM)
- Short form day(three letters), Short form month (three letters), DD, YYYY, HH:MM (24 hour time) (Thu, Mar 24 2009 23:44)
- MM-DD-YY HH:MM AM/PM (03-24-09 08:19AM)
- MM-DD-YY HH:MM (24 hour time) (03-24-09 23:44)
- YYYY-MM-DD HH:MM AM/PM (2009-04-24 08:19AM)
- YYYY-MM-DD HH:MM (24 hour time) (2009-04-24 23:44)

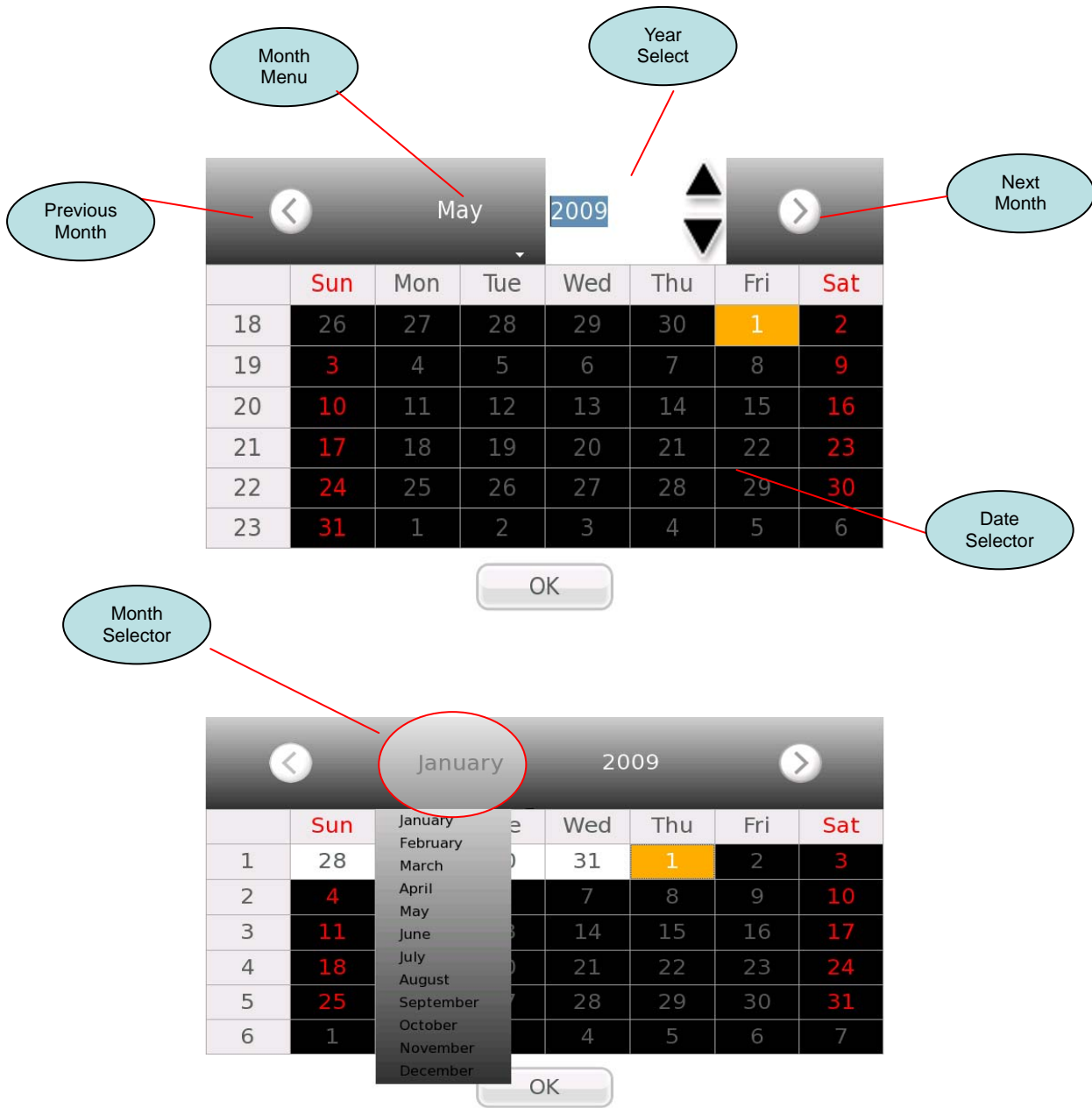
3.5.3.2. Set Current Date

Touch the current date that is displayed in the edit box, a calendar will appear.

Month: You can either; touch the 'Next Month' or 'Previous Month' arrow icons and scroll to the month you want or you can touch the Month Name and directly select the month you want.

Year: Touch the year number and then an arrow up/down icon will appear. Touch the up or down button until the number you want appears.

Date: Touch the calendar number of the date you want. The date will appear in yellow. Press OK when finished. **Note: The date should always be the last item you program.**



3.5.3.3. Set Current Time

Touch the area where the time is displayed. A number pad will appear. Enter the time in the format HH:MM:SS. For example current time is 11:14:00pm, enter 2,3,1,4,0,0, and then press OK when finished. If a number is invalid or there is no entry, pressing OK will do nothing.



3.5.4. Database Options



When any of the options are selected a popup window will show and ask you to confirm what you are about to do.



3.5.4.1. Compress User Data

When users are deleted from the system they are marked for deletion in the database, from the server and the terminal. When a new user is added to the system it will not overwrite the users marked for deletion. When you use this option it will delete the marked users in the system and reorder the database. Use this option if you frequently add and delete users from the system. In larger systems this can help speed up the authentication times and provide more space for adding new users.

3.5.4.2. Delete All Users

This option will allow you to delete all users in the system. **Note: User data can be exported to USB device before deleting.** [3.9.1. Database Export](#)

3.5.4.3. Clear Settings

This option will clear/delete all the terminal settings. The factory settings will be used. User, log data and pictures will not be deleted.

3.5.4.4. Clear Log Data

This option will clear/delete all the log data in the terminal. This will not delete picture log data or terminal settings. **Note: Log Data can be exported to a USB device, before clearing the log data see section [3.9.1. Database Export](#)**

3.5.4.5. Clear Picture Logs

This option will clear/delete all the picture log data. The terminal can hold up to 12,500 pictures (user pictures + log pictures). If you need more user database pictures you can delete the picture logs. **Note: Picture log data can be exported to a USB device, see section [3.9.1. Database Export](#).**

3.5.4.6. Delete All

This option will reset the terminal settings, delete all the picture logs, delete all users and all log information.

3.5.5. Authentication Settings



3.5.5.1. User Group ID

If User ID is selected for this option then normal authentication is performed when the user enters their ID number.

If Group ID is selected authentication is performed among users with the same first digit and/or less than the user ID number. For example, if the user ID is '1234', the user would enter '12' only for their authentication. When Group ID is selected, 1:N Matching is automatically performed, the option for 1:N will also be enabled. The matching is performed with user IDs from 1200 – 1299. If the ID is '0012', enter '0012' or '00' for authentication. This option is particularly useful in situations where there are many users in the system and the matching time for 1:N is too long. In the example the matching comparison is only done for 100 users (1299-1200) compared to all 1200 users. After the user enters their user ID, they will be required to enter their card, fingerprint or password, depending on the authentication type for that user.

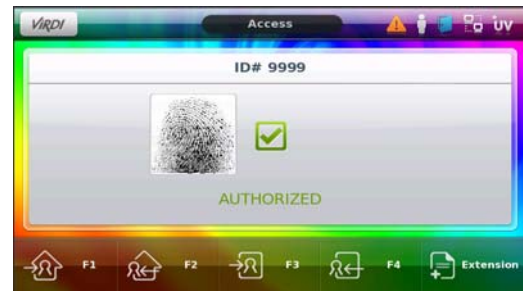
3.5.5.2. User Display Option

This option controls what is displayed on the main screen when a registered user is authenticated. On the response window you will see the top area change. The Key ID and the User Name can be programmed in the server program. If the display option is set for 'none' when authenticating with a fingerprint in 1:N, the matching time will be displayed. The matching time is the time in seconds of how long the fingerprint algorithm has taken to properly match the finger with a fingerprint template in the database.

User Display Option = None



User Display Option = User ID



User Display Option = Key ID**User Display Option = User Name****3.5.5.3. 1:N Matching**

When this option is checked, it is possible for the user to authenticate with a fingerprint only. A user ID or card is NOT required. If this option is not checked then 1:1 authentication is performed. The default setting is 1: N Matching. See Glossary of Terms for 1:1 and 1:N. When using 1:1 (option off) anytime the user presents their fingerprint at the terminal, the terminal will first request the id number of the user.

Note: If the user is registered for 1:N authentication, only 1:1 is allowed if this option is disabled (1:1 authentication) See section [3.2.1.6. User Fingerprint Options](#)

3.5.5.4. Card Only

When this option is checked and the user is registered with a card & fingerprint, or a card & password, only a card is required for access to an area. When this option is not checked the user's registered authentication method is used. This option is useful in situations where the terminal is located near a frequently used entrance or exit and no need for a high security level.

3.6 Terminal Settings



Terminal Settings control the operation of sound/wiegand/terminal options and door options. In this screen all you need to do is to touch the icon button on the left and a window with the options will appear on the right. Touching the Done button will close and save the changes. The following options are available in this section.

Sound

- Voice Volume
- Sound Volume

Wiegand

- Site Code
- Format

Lock Terminal

- Lock/Unlock Terminal
- Case Tamper Audible
- Card Reader

Door Options

- Door Monitor
- Lock Type
- Warning Time
- Open Time

3.6.1. Sound Settings



Touch the Sound icon. Then touch the area which you would like to change.



3.6.1.1. Voice Volume

The voice volume controls the volume of the voice prompts in the terminal. This volume is separate from the sound volume. If you do not want any voice prompts put the slider all the way to the left, off. For maximum volume put the slider all the way to the right. A simple sound file will play when sliding the button from the left to the right to give you indication of the volume you have selected.

3.6.1.2. Sound Volume

The sound volume controls the volume of the sounds in the terminal. These sounds are short tone sounds (button presses, window popup, error, success tones, etc). This volume is separate from the voice volume. If you do not want any system sounds put the slider all the way to the left, off. For maximum sound volume put the slider all the way to the right. A simple sound file will play when sliding the button from left to right to give you indication of the volume you have selected.

Note: A sound tone and a voice cannot play at the same time. For example when the voice says 'You are authorized', you will not hear any sound tones.

3.6.2. Wiegand Settings



Wiegand support is available in the terminal. In the back of the AC6000 there are terminals for Wiegand IN0 and Wiegand IN1, Wiegand OUT0 and Wiegand OUT1.

Wiegand Connection Option 1

When using an external reader that supports wiegand you can connect the reader to Wiegand IN0 and Wiegand IN1. This will allow the reader data to be sent to the AC6000 terminal.

IN0 = Data0

IN1 = Data1

Wiegand Connection Option 2

When using an external controller that supports wiegand, you can use the AC6000 as a dummy reader. The AC6000 will send the site code and user id to the external controller.

OUT0 = Data0

OUT1 = Data1



3.6.2.1. Site Code

The site code is a unique three digit value that should be different for every terminal. Values are from 0-255. To program this value just touch the number field and a number pad will appear, enter the value and press OK.

3.6.2.2. Format

There are many different formats for wiegand. Select the appropriate format that your external controller or reader supports.

3.6.3. Terminal Options



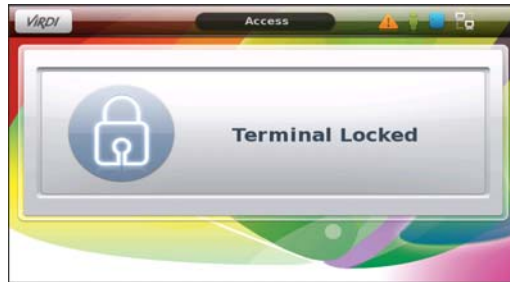
3.6.3.1. Terminal Locking/Unlocking

The purpose of terminal locking is to prevent access to the terminal.. This feature can be used when you do not want any users to access the terminal. No functions on the main window are available, only entering configuration mode is possible. You should have an administrator programmed to allow unlocking and locking. The server program can also lock out the terminal.

Terminal Locked: When checked the terminal will be locked out. When unchecked the terminal will operate as normal and allow any transactions

For this setting make sure the server program configuration 'Allow admin to Access' is set.

Main Window Display When Locked.



3.6.3.2. Case Tamper Audible

If this option is enabled and the case tamper on the back of the terminal is 'opened' (terminal removed from the wall), an error sound will be heard every 5 seconds when the main window is displayed. During administrator programming this sound does not occur. Also, if a case tamper occurs the status icon for 'trouble' will be on. See Icon list for details.



If this option is disabled the error sound will not occur, however the trouble icon will still appear on the main screen.

3.6.3.3 Card Reader

This section is for display only. When you scan your card the card number of the card will be displayed in this area. This is useful for determining your card number in cases where you do not have a reader for your software when enrolling a user. The number is displayed in hexadecimal or decimal depending on the card number.

3.6.4. Door Option Settings



Door option settings control the period of time the locks are unlocked for and the warning time when the locks are open too long. You can set the details of the lock type for normally closed, normally open or disabled. See lock installation instructions on setting up the door locks for different lock types.

When using Lock type as strike/auto, door lock 1 will activate when a successful authentication is performed, if the authentication is unsuccessful lock 2 will activate.



3.6.4.1. Door Monitor

This option is a combo selection box; you have three choices, disabled, normal open or normal closed. Select the appropriate value depending on your lock type.

3.6.4.2. Lock Type

This option is a combo selection box; the choices are Motor type or strike/auto door type. Select the appropriate value depending on your lock type application.

3.6.4.3. Warn Time

The Door Warning Time is programmable from 00-99 seconds. The default value is 20 seconds. If your system is properly connected to the door monitoring inputs on the terminal; and if the door lock is opened longer than this time a warning alarm will sound. If 00 is programmed the warning alarm will not sound.

3.6.4.4. Open Time

The Door Open Time is programmable from 00-99 seconds. The default value is 5 seconds. This time represents how long the door lock will be opened for after a successful authentication.

3.7. Display Settings



Theme

- Main Background
- Daily Update
- Arrange Icons

Camera

- Authorized Users
- Unauthorized Users
- Display Picture

Language

- Language Change

LCD Option

- Screen Saver Timeout
- Touchscreen Calibrate

3.7.1. Theme Settings

Theme

The Theme Settings area allows you to customize the look of the main window. You can change the background, move icons or automatically change the background everyday.

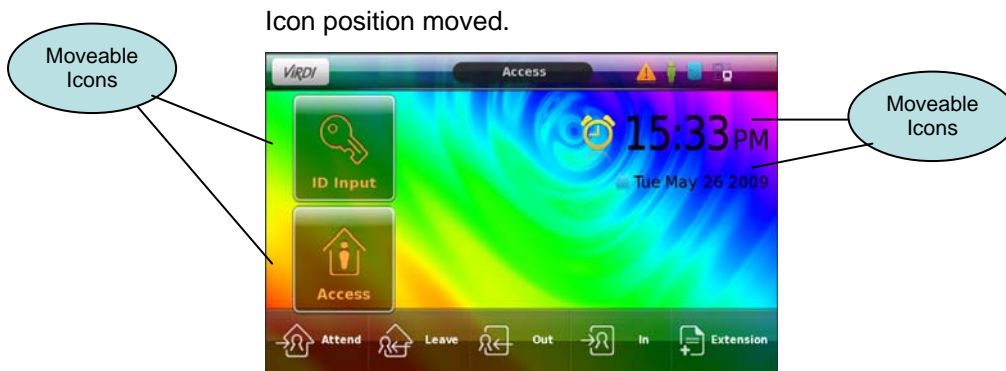


3.7.1.1. Daily Background Update

If this option is checked (enabled) the terminal will automatically change the background image every day at midnight. The terminal will use the list of images that are shown in the main background selection preview.

3.7.1.2. Arrange Icons

If this option is checked (enabled) you will be able to move the time and date icons, ID and Access Icons on the main screen to any location you want. When you are finished arranging your icons on the main screen turn the option off (unchecked). Turning the option off will 'lock' the positions and not allow any movement. When this option is enabled the ID and Access buttons will not function. If you attempt to move the icons off the screen the icon will go back to the original position. The positions of the icons are saved in the system options and can be imported/exported via USB.

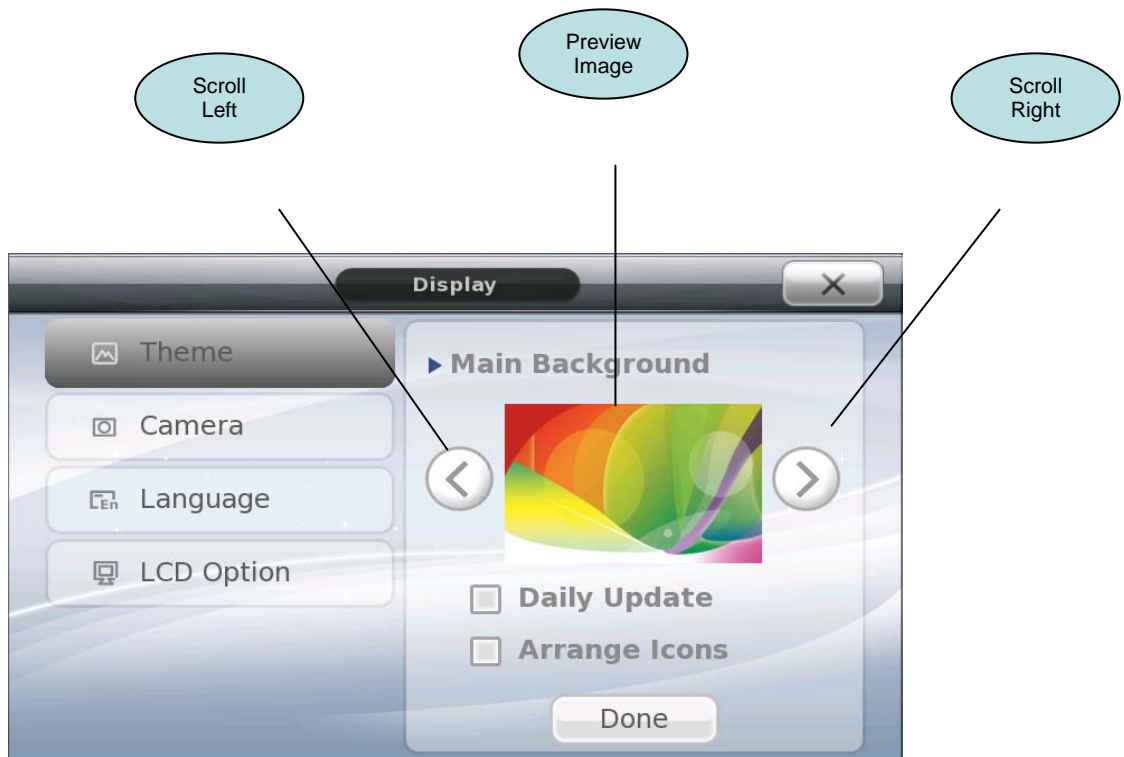


Factory set Icon positions.



3.7.1.3. Main Background

The terminal has 15 preset images to choose from. The image names are background1-background15.jpg. The terminal is also capable of importing new images with the USB device. See [3.9.2. Database Import](#). A maximum of 24 background images can be used, 15 system and 9 user. To select the background just touch the scroll right or scroll left arrow keys. You can hold down the button to cycle through the images. The preview image in the middle will show the current selected background image.



3.7.2. Camera Settings



The terminal has the ability to store a total of 12,500 pictures. These pictures can be either user registered pictures or log data pictures. The user registered picture is the picture taken when the user is registered [3.2.1.7. User Picture Registration](#). Log pictures are stored when a user (either registered or unregistered) attempts to access the terminal. All picture data can be exported to a USB device.



3.7.2.1. Save Authorized Users

When this option is checked (enabled) a picture of the registered user is taken when the user successfully authenticates/accesses the terminal. The picture is stored as a log picture and can be viewed later. If this option is unchecked (disabled), no new picture will be taken of registered users.

3.7.2.2. Save Unauthorized Users

When this option is checked (enabled) a picture of the user is taken when they unsuccessfully authenticate/access the terminal. The picture is stored as a log picture and can be viewed later.

3.7.2.3. Camera Display Options

'No Display' = The response window will not display any picture.

'Current Picture' = When this option is selected the current picture that was taken will be shown on the response window.

'Registered Picture' = When this option is selected the registered user picture will be displayed on the response window. See [3.2.1.7. User Picture Registration](#). If there is no registered picture then the current picture will be displayed. For Unauthorized users the current picture will always be displayed if this option is selected.

With the default settings of the camera if anyone attempts access to the terminal a picture is taken and displayed on the authentication window, but no pictures are stored in the log database.

If 'Authorized Users' or 'Unauthorized Users' is enabled, and 'Display Picture' is disabled no picture is displayed on the authentication window, but the picture is still taken and stored in the log database. Pictures are capable of showing real-time on the server application.

Note: From time to time you should export your log pictures to a USB device and delete the log pictures in the database. See Section [3.5.4.5. Clear Picture Logs](#)

Display Picture Option	Save Authorized Users	Save UnAuthorized Users	Take Picture	Display	Store Database
No Display	OFF	OFF	No	No	No
No Display	OFF	ON	Yes	No	Yes
No Display	ON	OFF	Yes	No	Yes
No Display	ON	ON	Yes	No	Yes
Current Picture or Registered Picture	OFF	OFF	Yes	Yes*	No
Current Picture or Registered Picture	OFF	ON	Yes	Yes	Yes
Current Picture or Registered Picture	ON	OFF	Yes	Yes*	Yes
Current Picture or Registered Picture	ON	ON	Yes	Yes*	Yes

* Note: If registered user has a registered picture, the registered picture will show if 'Registered Picture' is selected, if not the current picture will show. Current picture always shows for Unauthorized users.

3.7.3. Language

 Language

The language can be dynamically changed. This means when the new language is selected, the text and font will change immediately without the need to repower the system. The default languages available are English and Korean. If you require another language you should contact your local sales representative for this request. Languages can be easily imported via the USB device.



3.7.4. LCD Options

LCD Option



3.7.4.1 Screen Saver

The screen saver option will allow you to select the timeout value of the LCD after no activity; the LCD will appear black during this time. This will conserve the lifetime of the LCD. The default is 1 minute. Selectable values are 1, 5, 10, 15, 20, 25, and 30 minutes. If the approach sensor, function key, fingerprint cover, card scan or fingerprint scan is activated the LCD will automatically turn back on.

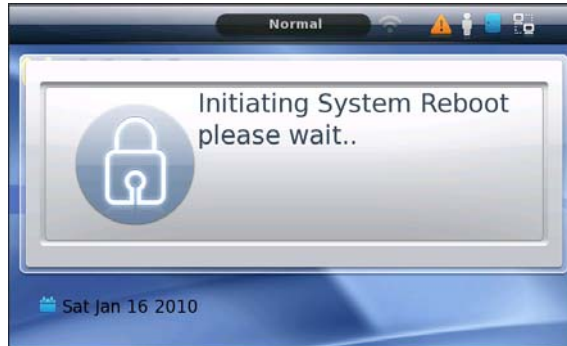


3.7.4.2 Touchscreen Calibrate

If your Touchscreen responsiveness does not seem normal or your touching is not accurate you may need to recalibrate the Touchscreen. Normally this is done from the factory, rare occasions you may need to recalibrate. Press the button to recalibrate and a confirmation window will appear. After you select OK the terminal will reboot and a Touchscreen calibration program will run before the program starts again. Please touch each X on the calibration screen. When Touchscreen calibration is performed you should use a stylus type pen device for selecting the points on the LCD. Please remember to touch each point carefully, if you make a mistake you will not be able to navigate with the Touchscreen. You will need to perform a hardware reset calibration.



After touching 'ok' the terminal will automatically exit admin mode and within 3 seconds a message will appear as below. Wait for the system to reboot, and then follow the calibration instructions.



Note: If during extreme cases you have no response on your touch screen at all it may be impossible to navigate to this screen. You can force a hardware reset calibration. Power down the terminal and place a short (wire) between Wiegand IN1 (WI1) and Wiegand OUT1 (WO1), power up the terminal and wait for a reboot. The calibration program will appear.



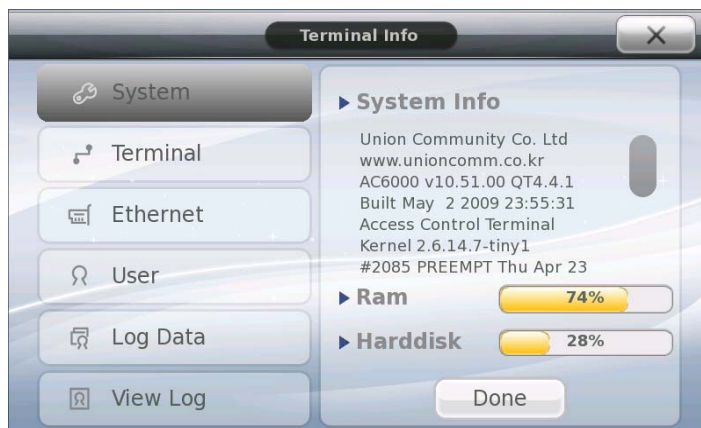
3.8. Terminal Information

In the terminal information section system, event, picture, network information can be viewed here. Nothing is programmable in this section; this section provides the status of the system and a summary of some key settings. Touch the Done icon when finished.



3.8.1. System Information

This area provides important information about the terminal. The firmware version, ram usage and harddisk usage is in this area. These can be important for troubleshooting and determining the terminal's limit. The harddisk is the amount of memory being used for user data, log events, pictures and system settings.



3.8.2. Terminal Information



This area provides an overview of the key terminal settings.



3.8.3. Ethernet Information



This area provides an overview of the Ethernet settings.



3.8.4. User Information

User

This area provides an overview about the registered users in the terminal. This will show you the limits for the users, fingerprints and cards and what the current limit is at. This can be helpful in determining how much storage space is remaining for your terminal setup.



3.8.5. Log Data Information

Log Data

This area provides an overview of the log events in the terminal. This will show you how many log events are in the system, picture for users and log pictures.



3.8.6. View Log Information



This area allows you to view the key log information in the terminal, such as authorized, unauthorized access. If more details are required it is recommended to use the server program.

Log Type: This is a combo box, you can select; All, Authorized Access, Unauthorized Access.

Event Information: This is a text area that will show the following information:

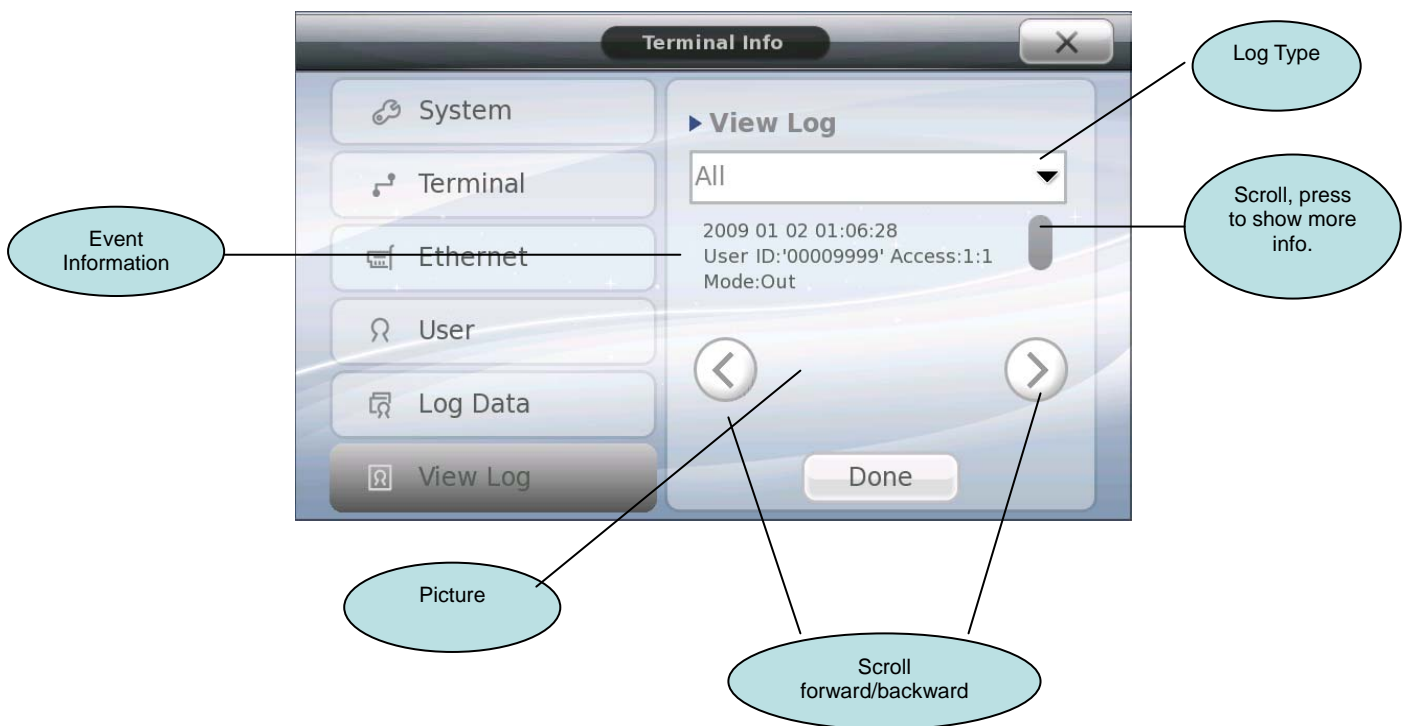
User ID – id of the user who accessed the terminal, 'unknown' if unregistered

Access - Type of access which could be 1:1 or 1:N

Mode – The mode that was used for access. (F1,F2,F3,F4, Access Mode 1-60, In, Out, Leave, Exit)

Picture: If there was a picture taken during the event it will be displayed in this area.

Scroll Keys: Use these keys to scroll forward or backward through the events. You can hold down the button for faster access.





3.9. USB Options

The USB options area will allow you to import and export files to and from the terminal. User data, log data, pictures, images and firmware upgrading can be performed. It is recommended that your USB has at least 250mbytes available for storage. You cannot select any options in this area until a USB device is connected. The USB device can be connected at anytime before or after entering this area. Once you connect your device you must wait up to 10 seconds before the terminal will recognize it and a 'detected' message will appear.

NOTE: AT ANYTIME DURING FIRMWARE UPGRADE OR IMPORTING/EXPORT DO NOT REMOVE THE USB DEVICE. THE SYSTEM MAY BECOME UNUSABLE IF YOU REMOVE THE USB DEVICE DURING A FIRMWARE UPGRADE.

If the USB device is not connected this message will appear. Touching Cancel will close the window, or you can insert the USB device.



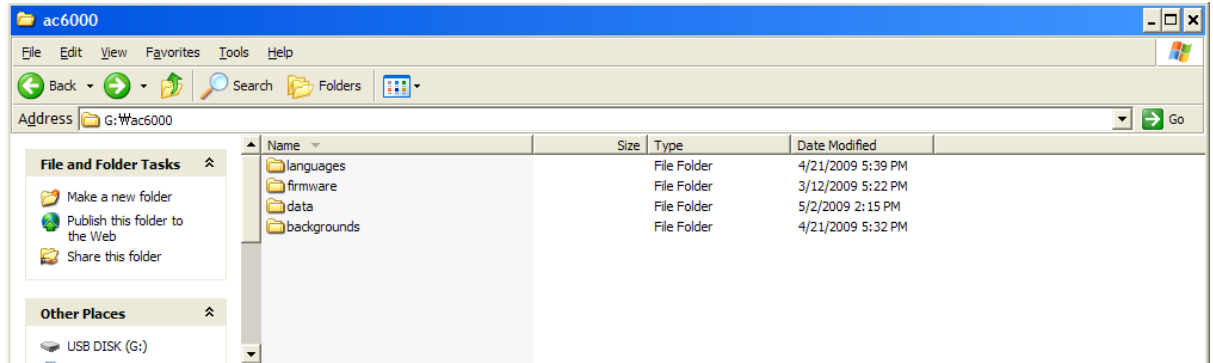
Once the USB device is connected a message will appear indicating the USB type.



If the USB is connected properly you will see this window and you can now select the options you want.



In order to import files (System Options, User Data, Theme/Images and firmware upgrading) your USB device should be formatted as follows. Create a directory called ac6000/, then create subdirectories called firmware, languages, and backgrounds.



Languages directory – put language files in this folder. If you have a language file AC6000_en_US.qm. (For example English), put it in this directory for importing. A separate program is required to produce the .qm language files. See your local sales representative for details. If successful you will be able to select the new language see section [3.7.3. Language](#).

Firmware directory – put all firmware files needed for upgrade in this folder. From time to time the factory will release new firmware versions for bug fixing or feature enhancements. These binary images can be upgraded from this folder. There can be up to 5 files for upgrading. Only put the files that should be upgraded in this folder. Do not keep old firmware versions here.

Data directory – this directory will be created by the terminal when inserting the usb device. This directory will contain data that will be exported to the usb device. (User data, log data, system options, picture data)

Background directory – this should contain all .jpg, .bmp images you would like to copy to the terminal. The name of the file must be called user1 – user9.jpg or .bmp. For example if copying four image files to the terminal you should call the image files user1.jpg, user2.jpg, user3.jpg and user4.jpg. In order to ensure a quality background image you should use the same size as the lcd device, 800 x 480. After successfully copying you will be able to select a new background, see section [3.7.1.3. Main Background](#).

/data/Logpicture directory – this directory will be created by the terminal when exporting picture data to the usb device. Log pictures will be put by the terminal in this directory.

3.9.1. Database Export

Exporting means files will be copied from the terminal to the USB device. User data, event log data, system options or picture log data can be exported. Choose the appropriate option. When first touching the icon a message will popup indicating the status and a sound will be heard. Some files may be larger than others, so copying time may take longer in some cases, usually during (User data, picture logs or event log data). When the copying process is finished another popup message and sound will be heard indicating success and/or the amount of files copied. Please do not remove the usb device during this operation.

When exporting, listed below are the files that will be created. The user data and system options can be used to import to another AC6000. The files are compressed.

Export User Data - /ac6000/data/userdata.tar.gz
Export Event Log - /ac6000/data/logdata.tar.gz
Export Picture Logs - /ac6000/data/logpictures/piclogdata.tar.gz
Export System Options - /ac6000/data/sysoptdata.tar.gz
Export All - /ac6000/data/database.tar.gz

3.9.2. Database Import

Importing means files will be copied from the USB device to the terminal. User background images, user data, system options and languages can be imported. The following is a list of directories and file names which must be on the USB device for importing.

Import User Data - /ac6000/data/userdata.tar.gz
Import System Options - /ac6000/data/sysoptdata.tar.gz
Import Theme/Images - /ac6000/languages/AC6000_xx_xx.qm (language file)

- /ac6000/languages/xx_xx.ttf (font file)
- /ac6000/backgrounds/userX.jpg/bmp

Where xx_xx = language and country, for example korean, korea is ko_KR

3.9.3. Firmware Upgrading

If a new firmware version is released from the factory you can update your firmware from the USB device. Make sure you put the binary image in the firmware directory. Do not keep old firmware files in this directory. The firmware upgrade process may take up to 1 minute or longer. You will see a popup message and hear a sound when the process is finished. **DO NOT REMOVE THE USB DURING THIS PROCESS.** The system will automatically reboot when the upgrade has finished. OR if you press and hold down the F1, F2 and F4 button at the same time the system will automatically reboot. See Section [6.1 Upgrading from USB](#)

4. User Interface Customization

The sounds, images, backgrounds, voices and text can be changed to provide a customized look and feel to your AC6000 terminal. These files can be imported using the USB memory stick. See Section [3.9. USB Options](#).

The factory can provide a file with all the resources from the AC6000. Resources include sounds, images, icons, language files, fonts, etc. This file is called resources.tar.gz. This file is a compressed directory structure with files. If you do not have this file you can import sounds, mp3 files, text (language) files and backgrounds individually following the procedure below.

4.1. Standard Customization/Languages

You can change the look of the main screen by changing the background, arranging icons or customizing the text. Once you have followed the procedure below you should insert your USB device into the AC6000 and navigate to the USB options menu. Next select the 'Themes/Images' button, there should be a popup showing you the number of files that were copied if it was successful. For text changes you will have to go to the language selection menu in Display Options and reselect your language. For backgrounds just go to the Display options menu and you should see your new background in the preview area.

4.1.1 Main Window Backgrounds

There are 15 factory background images. You can import an additional 9 more backgrounds. The background images should be 800x480 and in .jpg or .bmp format. Copy your customized backgrounds to your USB device in a directory /ac6000/backgrounds/. The files should be called user1.jpg or user1.bmp, up to user9.jpg/bmp.

4.1.2 Language Translations/Customizing Text Items

All text can be changed. The factory can provide a file with the phrases for your language. It is important that your file be named after your locale name of your country and language, for example en_US = English, US, ko_KR = Korean, Korean. You can easily find your locale by searching the internet.

AC6000_en_US.ts = English

AC6000_ko_KR.ts = Korean

TS File = from the factory, given to the customer for translations

QM File = created by the application program. Used by the AC6000.

1) Download the translation tool from the following link

<http://www.qt-apps.org/content/show.php/Qt+Linguist+Download?content=89360>. The user should download the appropriate one for their pc. Select the v4.4.3 version.

2) Install the application. User should read the instructions on how to translate. It is fairly simple. They just click on the the text and type in the new text.

3) Once the application is opened, you should go to FILE->OPEN-> and open the ac6000_.ts file. The ts file is supplied by the factory. For English the TS file is called AC6000_us_EN.ts, for

Korean it is called AC6000_ko_KR.ts.

Once the user completes the translation they need to click on the FILE->RELEASE AS, this will save the file as AC6000_us_EN.qm. The QM file is used by the AC6000.

If we require a special language the user should send the factory the TS file.

User should then copy the QM file to a USB device in /ac6000/languages/ folder.

In the AC6000 go to USB options, touch the 'Themes/images' button, after the file is copied they should be able to see their new language in the terminal programming ->display area to select.

4.1.3 Font Importing

Some Languages require special fonts to display their characters. In most cases the default English (Latin) font will work for most translations. You may only need to do this in special cases. Find a suitable True Type Font file (ttf) file if your language is selectable in the display menu, select your language first.

- 1) Copy the TTF file to the usb /ac6000/languages/NAME.ttf.
- 2) NAME=locale name of your language. i.e if polish then use pl_PL.ttf.
You must also have the language translation file in the same folder AC6000_pl_PL.qm.
- 3) Insert USB into AC6000
- 4) Go to USB options->Select Theme/images
- 5) After copying the message should display 2 files copied.
- 6) If you already have your language selected you should go to Themes->Language and reselect your language (Change from Korean to English, then back to Korean again)

4.1.4 Updating MP3 Files in AC6000

There are four voices available in the AC6000. You should have your language selected in the language menu when importing mp3s.

Voice	File Name
Please Enter Your Fingerprint	E01_PleaseEnterYouFingerprint2.mp3
Please Try Again	E02_PleaseTryAgain.mp3
You Are Authorized	E03_YouAreAuthorized.mp3
Input Your ID	E04_InputYourID.mp3
Please Enter Your Card	E05_PleaseEnterYourCard.mp3

- 1) On the USB device make a directory /ac6000/firmware/mp3/LOCALE
LOCALE = your language locale name, if Polish, then pl_PL. For example,
/ac6000/firmware/mp3/pl_PL/
- 2) Create your mp3 file and then copy the file to the usb directory you just created (Make sure to name your file the same name as above or else the voice will not play)
- 3) Go to USB options, press the Theme/Images, after it is finished a popup will appear.
- 4) The files are updated depending on the language that is currently selected. So if you have the language set for English and you copy new files, the new files will replace the English files. This is ok for testing.
- 5) If you are making a new language you should perform the translation first with the translation program. Then you will have your 'own' language in the selection menu and your voice files will be updated for YOUR language.

4.1.5 Customizing Sounds

All sounds can be changed (popup, error, keypress beeps). The file must be in a .wav format and should be the appropriate length depending on the operation. For example, if you change your keypress sound the new sound should be as short as possible. If you create a sound that sounds too long you may have undesirable results.

Function Key Sound = file name = fx0135.wav
Camera Sound = file name = cam3.wav
Success Sound = file name = sound110.wav
Error Sound = file name = error3.wav
Number pad sound = file name = fx0195.wav
Case Tamper Sound = file name = error.wav
Popup sound = file name = popup.wav
Authentication Success = file name = ding_dong.wav
All other keypress sound = file name = fx0072.wav
Card scan sound = file name = Beep1c.wav
Door Open Warning Sound = file name = door3.wav

On your USB stick copy the new file name to "ac6000/firmware/sounds". For example if you are changing the Function Key Button sound create your wav file and name the wav file 'fx0135.wav' and then copy that file to the USB stick.

5 How to use the terminal

5.1. Main Screen

The appearance of the main screen is highly configurable and can change appearance depending on the setup by the administrator. When no activity has occurred for a programmed number of minutes set by the administrator the LCD will turn off and the display will be blank. When a user approaches the terminal, touches the screen, scans a card, or enters a fingerprint the screen will show again.



Number	Item	Description
1	Configuration Button	For entering terminal configuration mode
2	ID Input Button	For entering a user id number for authentication
3	Time/Date	Time/Date display. Different display options available in configuration mode.
4	Function Keys	These keys are used for changing authentication modes. Same function as the F1-F4 Buttons on the terminal.
5	Status	Status text indicating the current mode of authentication. (access/leave/attend/in/out)
6	Status Icons	Status icons (fire, trouble, proximity, door, network and UV)

7	Access Button	To change the current authentication mode to 'normal mode'
8	Extension Button	If more than four functions keys are needed this button is used for extending the number of function keys

Below are some different pictures of the main screen when configured with Access Control, Function keys, or Time and Attendance.

Window#1
Time and Attendance with Function Keys



Window#2
No Function Keys





Window#3
Time and Attendance with Function Keys and Extension Key



Window#4
Access Control with Function Keys No extension key





Note: The Access Icon  and  perform the same function. When the extension button is used the larger icon will appear, if not the smaller icon will appear on the bottom.


5.2. ID Entry Screen



When the ID Button is touched a window will appear for the user to enter their ID number. The user must input their ID number then touch the OK button. If a mistake is made when entering the number touching arrow will erase the number one digit at a time. The window will close after 10 seconds of no activity.

- Touch  button to cancel and close the window.

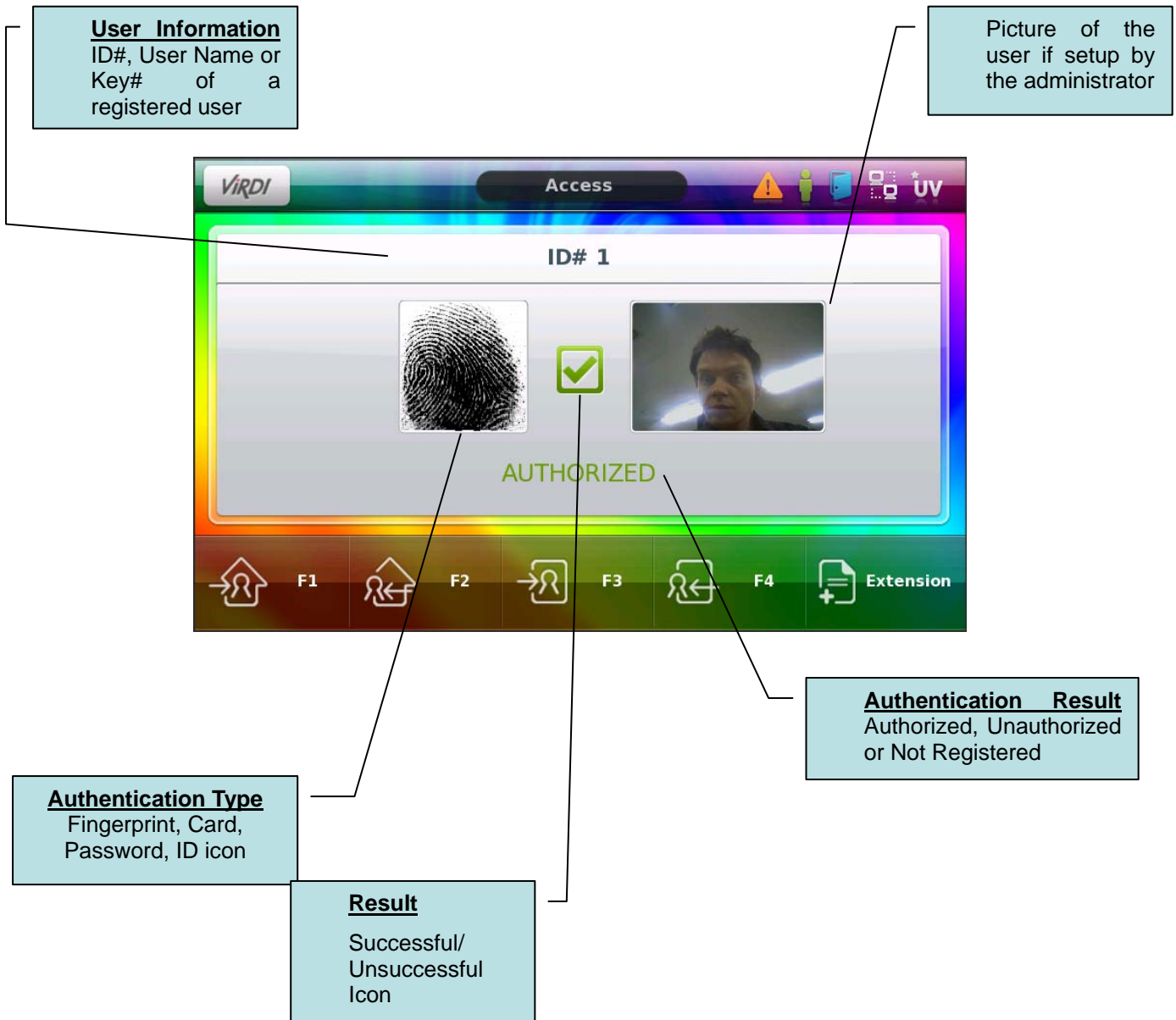
- Touch  button to backspace to the previous digit entered (erase).

- Touch  button when you finished entering the id number.



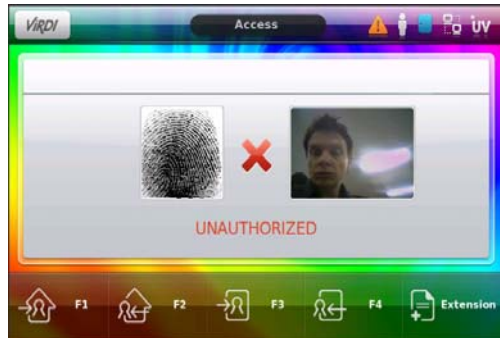
5.3. Authentication Result Display

After a user is authenticated as authorized, unauthorized or not registered a result window will appear with the result and a voice or sound can be heard. The result window may have different icons, pictures or words depending on how the terminal is setup by the administrator. This window will close automatically after a few seconds or can be closed immediately by touching the window area. See below for examples. See [1.3. List of Icons](#) for a description of each icon.

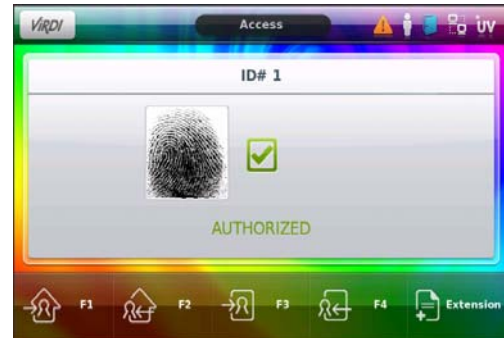


Here are some examples of different authentication result windows. See the Icon list [1.3. List of Icons](#)

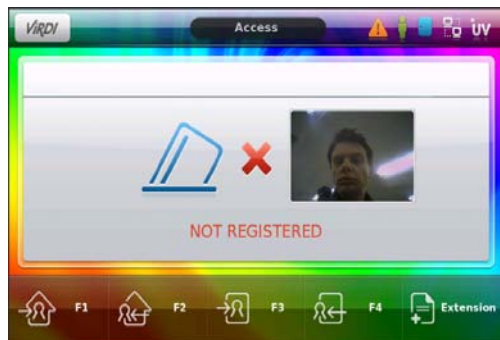
Unauthorized fingerprint with picture



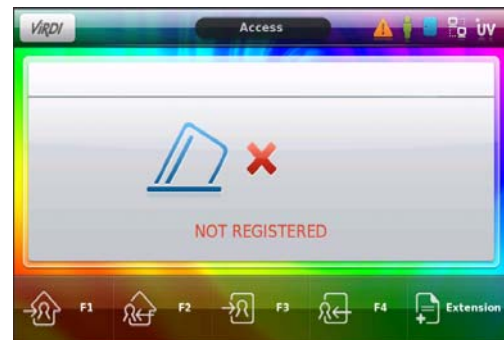
Authorized fingerprint UserID#1 No picture



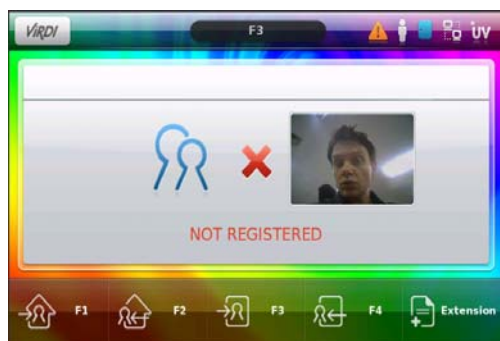
Unregistered card with picture



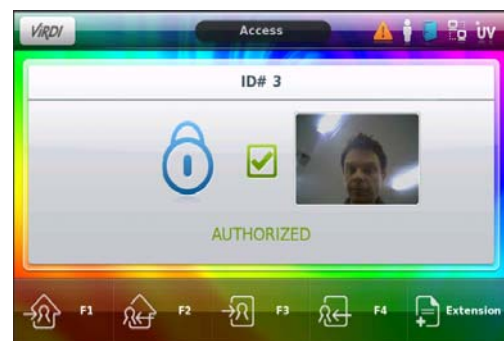
Unregistered card with no picture



Unregistered ID with picture



Authorized password, userID #3 with picture





5.4. Application Modes

5.4.1. Access Control Application

An Access Control application is normally used for providing access to a secure area, function keys are not needed unless extra tracking of the user is needed. If the system is setup for Access Control and Function keys are used for authentication the user is required to press the mode function button before entering their ID, Card or Fingerprint. Anytime the mode is changed the top status bar will show the current mode. (F1, F2, F3, F4 or Normal). Once the user is authenticated as successful the door will open.

Normal Mode – Touch the  or the  button then authenticate with card, ID, password or fingerprint.

F1 Mode – Touch the  then authenticate with card, ID, password or fingerprint.

F2 Mode – Touch the  then authenticate with card, ID, password or fingerprint

F3 Mode – Press the  then authenticate with card, ID, password or fingerprint

F4 Mode – Touch the  then authenticate with card, ID, password or fingerprint

5.4.2. Time & Attendance Application

Time and Attendance Application is for systems that require tracking of employee's work time. If the system is setup for Time and Attendance, for authentication the user is required to press the mode function key before entering their ID, Card or Fingerprint. Anytime the mode is changed the top status bar will show the current mode. (Attend, Leave, In, Out, Access).


Attend – when the user is attending the office the first time that day.


Leave – when the user is leaving the office for the day and will not return until the next day.

In – when the user is returning to the office from a break or lunch.

Out – when the user is leaving the office during normal work hours for a break or such.

Access Mode – Touch the  or the  button then authenticate with card, ID, password or fingerprint. This is normal Access Mode.

Attend Mode – Touch the  then authenticate with card, ID, password or fingerprint.

Leave Mode – Touch the  then authenticate with card, ID, password or fingerprint

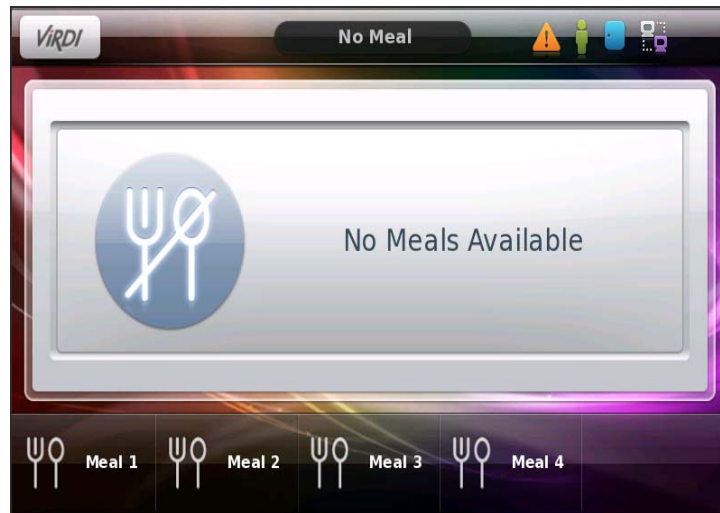
In Mode – Touch the  then authenticate with card, ID, password or fingerprint

Out Mode – Touch the  then authenticate with card, ID, password or fingerprint

- Note: Start Time, Normal Time and Leaving time can be fixed by the administrator in the terminal programming. The system will automatically change to Start, Normal or Leaving mode when these times are setup.

5.4.3. Cafeteria Application

Cafeteria or Meal Application is for systems that require tracking of user's meal time. If the system is setup for Cafeteria Mode, for authentication the user is required to press the mode function key before entering their ID, Card or Fingerprint. There are five programmable time periods (Breakfast, Lunch, Dinner, Snack, Supper). The user can select four types of meals. If no meal time is valid a screen will show like below. Authentication or meal acceptance will be denied during this period.





If the terminal Cafeteria schedule times are setup and the current time is within the period the main window will appear as below. The text in the upper status field will change depending on the current mode: Supper/Lunch/Dinner/Breakfast/Snack.


When the time is valid for the current mode a meal count will display on the window. This is a count of how many meals during the mode. For example, if a user transacts during supper mode the meal count will increase by 1. If another different user transacts, the meal count will increase. When the terminal switches to a new time mode (Breakfast, Lunch..etc) the counter will change.


Each time mode (Breakfast, Lunch, Dinner, Snack, Supper) has a separate meal count for each. The function keys are used to select the meal type during the time mode. For example, Meal 1 can be a salad, meal 2 = Hamburger, etc)



Meal 1 Mode – Touch the  then authenticate with card, ID, password or fingerprint.

Meal 2 Mode – Touch the  then authenticate with card, ID, password or fingerprint

Meal 3 Mode – Touch the  then authenticate with card, ID, password or fingerprint

Meal 4 Mode – Touch the  then authenticate with card, ID, password or fingerprint

Note: Meal times can be fixed depending on the programming of the administrator for Breakfast, Lunch, Dinner, Snack or supper.

5.4.4. Shift Management Application

This application mode is used for applications where the terminal is managing employee's shift cycles. There are no time schedules associated with this mode. The shift cycle is a 12 hour period. This means that after 12 hours if the user has not ended a shift, the terminal will automatically close off the shift. After touching an icon, the main window will appear and all other shift icons will disappear, the user must transact (with fingerprint/card/ID) at this time. If no transaction occurs in five seconds the terminal will go back to Shift Control Window (with icons) will. You cannot use a fingerprint/card/password or ID unless a shift icon is touched first. Note: There is a minimum time in which you can select the next transaction. You cannot Start Shift, then immediately Start Break, you must wait until the minimum transaction interval has expired (default 60 seconds). This is programmable by the administrator.



Start Shift – Touch this icon when starting your shift for the current day.

Start Break – Touch this icon when starting your break during the current shift. You cannot start a break if you are already on meal OR you are not on shift.

Start Meal – Touch this icon when starting your meal during the current shift. You cannot start a meal if you are already on break OR you are not on shift.

End Shift – Touch this icon when your shift is done for the day. You cannot end shift unless you have started a shift.

End Break – Touch this icon when ending your break during the current shift. You cannot end a break unless you have started a break

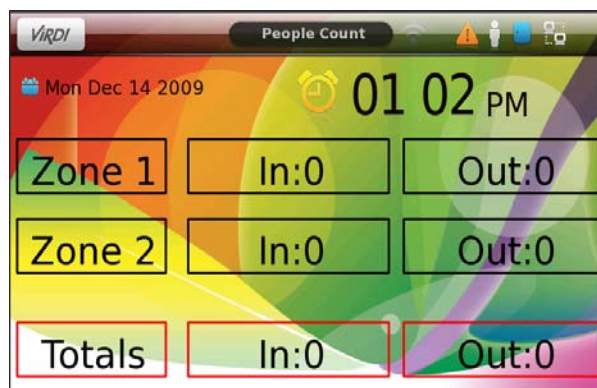
End Meal – Touch this icon when you are ending your current meal break. You cannot end a meal unless you started a meal.

Shift Info – Touch this icon when you want to see your last transaction. A user can check their last transaction time, this may be important in cases where the user would like to see how much time is left before their break has started. See below window. The user ID, Last transaction, date/time will appear.



5.4.5. People Counter Application

In People Counter Mode the AC6000 will show the main window as below. When the external sensor is activated, the zone counter will increase and show the totals on the main window. Function keys are not used in this mode. When the application mode is changed the counters will be reset.



6. Firmware Upgrading

Firmware upgrading is needed from time to time to fix problems or add additional features to the AC6000. The factory will issue the binary files for upgrading. They will be posted on the unioncomm.co.kr website. You must register to login and download the new files. Firmware upgrading can be done from USB or the UNIS server program. In order to make the upgrading easy and flexible there are many files available, however only 1 or 2 is needed. When the factory issues a file there will be a built date and version number in which you should verify before and after to make sure the upgrade was successful OR if you need to upgrade at all.

Ac6000gui.bin, resources.bin, nor.bin, zImage.bin, boot.bin, ramdisk.bin, filesystem.tar.gz

Ac6000gui.bin – this file is the main program. If there are no resources that need upgrading this file can be used. This is smaller and the upgrading will be faster. Approximate size = 2.5 to 3mb.

Resources.bin – this file includes the main program plus fonts, images, background pictures, sounds, mp3s. When any of these need to be changed or added this file will be used for upgrading. Approximate size is 16-20mb. . All custom backgrounds/sounds/languages/fonts will be lost during this update. Please re-import when upgrade has finished.

Nor.bin – this file includes zImage.bin, boot.bin and ramdisk.bin. The individual files are also available for upgrading which are smaller. If a change is made to a specific area then only the individual file can be used for faster upgrading. If changes are made to two or three files then it is convenient to use the nor.bin file.

Filesystem.tar.gz – this file includes ac6000gui.bin and resources.bin, plus additional program libraries to make the main program run. This is the largest file, approximately 50mb or more. This file is only upgradeable from USB when the system is powered up. It cannot be upgraded from the usb options menu. When this file is upgraded all the memory is erased (users, pictures, settings, etc). This will reset the system to factory settings.

Unless specifically stated in the upgrade instructions you should most always use the nor.bin and resources.bin for upgrading, this will ensure you have all of the files needed. Before and after upgrading you should check the current version information of your terminal. See section [3.8.1. System Information](#) , you should note the version and build dates on this system page. The factory will provide the current version and built date that you should have, if you do not have that then you should upgrade to the newest files. If you want to check the version information of your terminal from the UNIS program you should go to the server computer and look in folder C:\Program Files\UNIS\Log, there will be a file called UNIS_Troubleshooting_XXXX-XX-XX.txt, the XX will be the date, check the most recent dated file. It will list all the terminals that are connected to the server and provide detailed information about each terminal (same information that is in the Terminal Information area of the AC6000 Terminal).

AC6000 v1X.XX.XX.XXX/QT4.4.1/2.6.14.7#XXXX/1

AC6000 V1X.XX.XX QT4.41 Built XX, XX, XX = if this version and date is out of date you should upgrade the resources.bin or ac6000gui.bin file.

Kernel 2.6.14.7 #XXXX Built XX, XX, XX, XX = if this version and date is out of date you should upgrade the nor.bin file

Ramdisk Built XX,XX,XX,XX = if this date is out of date you should upgrade the nor.bin file.

6.1 Upgrading from USB

When upgrading from USB you must copy the binary file to the USB /ac6000/firmware folder. Next insert the USB in the AC6000 terminal, go to the USB options menu and select firmware upgrade. Ensure that only the needed file is on the USB and no other firmware files are in the directory.

6.2 Upgrading from UNIS

When upgrading from UNIS, go to terminal management->firmware upgrade, then browse to the file to select the correct file, select the terminal then press SEND.

After the file has been successfully copied to the AC6000 terminal from USB or UNIS the server will be disconnected and admin mode will be exited. The terminal will be locked and no access will be allowed, after the file has been installed in the terminal the terminal will automatically reboot. The main window will display a message. **Note: DO NOT POWER DOWN DURING THIS MESSAGE your system may become unusable.**



6.3 Upgrading to Factory Settings

The filesystem.tar.gz file is used when you want to erase all the memory in the AC6000. Normally upgrading the resources.bin file is enough; however in very rare cases this procedure is necessary.

- 1) Copy the filesystem.tar.gz to the USB device /ac6000/firmware/ folder.
- 2) Power down the AC6000 terminal.
- 3) Insert the USB in the terminal.
- 4) Put a wire connection (short) between terminal connectors (14 and 11). W0I and WIO
- 5) Power up the AC6000 terminal, the Virdi logo will be displayed and approximately after 2 minutes the system will reboot.
- 6) When the system reboots remove the USB memory stick and short.

7. Troubleshooting Guide

This is a general guide on troubleshooting. Follow these guidelines if you are having troubles with using the terminal.

Problem	Solution
LCD is blank or black.	<ul style="list-style-type: none"> • Ensure the RED power LED is on • Check LCD timeout, LCD will turn off after a programmed period of time.
Cannot hear voices	<ul style="list-style-type: none"> • Ensure the voice volume is turned on. See 3.6.1.1. Voice Volume
Cannot hear sounds when keys are touched	<ul style="list-style-type: none"> • Ensure the sound volume is turned on. See 3.6.1.2. Sound Volume
Picture not showing.	<ul style="list-style-type: none"> • Ensure the picture options are enabled. See 3.7.2. Camera Settings • Check terminal information (system). Ensure the 'Camera Sensor OK' is shown.
Card not working.	<ul style="list-style-type: none"> • When scanning the card make sure the BLUE LED lights up for half a second. A sound should be heard also. • Ensure the card is registered. • Ensure the authentication type for the user is correct. See 3.2.1.5. Authentication Type • Check terminal information (system). Ensure the 'Card OK' is shown.
Fingerprint not registering	<ul style="list-style-type: none"> • See section 1.8. Correct fingerprint registration and input methods • Ensure the auto sense LED (red led on sensor window) appears when the finger is on the sensor window. • Check if the user is already registered under another id using the same fingerprint. See Section 3.5.2.4. Enhanced Registration

User not authenticating after registration.	<ul style="list-style-type: none"> • See section 1.8. Correct fingerprint registration and input methods • Ensure the auto sense LED (red led on sensor window) appears when the finger is on the sensor window. • If using the server, make sure the authentication method is correct. See 3.5.1.2. Authentication Mode • Check user authentication type.
Door Not Opening	<ul style="list-style-type: none"> • Ensure lock is properly connected to terminal. See installation instructions. • Ensure the Door Option section is correctly programmed. 3.6.4. Door Option Settings • Ensure the GREED LED is on when the authentication is successful.
Cannot connect to Server	<ul style="list-style-type: none"> • Ensure the LEDs near the Ethernet plug are ON. • Ensure the network ICON is shown on the main screen. See ICON list. If Ethernet LINK is good the ICON will be white, if connected to the server the icon will be animated. • Ensure the terminal ID is correct in the server program and the terminal. 3.3.1 Terminal ID Number • Ensure the network settings are correct. 3.3. Network Settings
I hear a loud buzzer sound every 5 seconds	<ul style="list-style-type: none"> • Please check if your case tamper is secured. The button on the back of the terminal must be pressed in • 3.6.3.2. Case Tamper Audible