

# *VIRDI* AC-1000

Terminal de Identificação Biométrica



Guia de Usuário



## Índice

Glossary .....	01
Before Use .....	02
Safety Precautions .....	02
Terminal Description .....	03
Button Description .....	04
Screen Description (During Operation) .....	04
LCD Icon During Operation .....	06
Voice Information During Operation .....	06
Buzzer Sound During Operation .....	06
Introduction .....	07
Features .....	07
Configuration .....	08
Network Configuration .....	08
Standalone Configuration .....	08
Specifications .....	09
Environment Settings .....	09
Check Items Before Setting the Environment .....	09
Entering Menu .....	09
Change Settings .....	10
Save Environment Settings .....	10
User Registration .....	13
"1. RF" Registration .....	13
"2. ID&PW" Registration .....	14
"3. RFIPW" Registration .....	14
"4. RF&PW" Registration .....	15
"5. ID&PWIRF&PW" Registration .....	15
Delete User .....	15
Modify User .....	16
"1. RF" User .....	17
"2. ID&PW" User .....	17
"3. RFIPW", "4. RF&PW", "5. ID&PWIRF&PW" User .....	17
Administrator Registration .....	18
Delete All Users .....	18
Network Settings .....	19

## Índice

Terminal ID Settings .....	19
Connection [NS / SN / NO] Mode Settings .....	19
Connection Method Settings .....	20
IP address Settings .....	21
Subnet Mask Settings .....	21
Gateway Settings .....	21
Server IP Settings .....	27
Server Port Settings .....	22
Option Settings .....	22
Application Mode Settings .....	22
[0]: Access Control .....	23
[1] Time Attendance Control .....	23
[2] Meal (Cafeteria) Service Control .....	24
Authentication Method Settings .....	25
Settings for ID Display When Authentication is Successful .....	26
Auto Enter Key Setting .....	26
Settings for Card Only Authentication .....	27
Door Settings .....	27
Door Opening Time Settings .....	27
Door Status Monitor .....	28
Door Open Alarm Settings .....	28
Volume Settings .....	29
Voice Settings .....	29
Buzzer Volume Settings .....	30
Current Time Settings .....	30
Other Setting .....	30
LCD Backlight On/Off Settings .....	31
LCD Brightness Settings .....	31
Display Time Settings .....	32
Terminal Information View .....	32
Extended Functions .....	33
Terminal Lock Settings .....	34
Read Card Number .....	34
Device Settings .....	35

## Índice

System Configuration Settings .....	35
User ID Length Settings .....	35
Language Settings .....	36
Function Key Settings .....	36
Card Reader Settings .....	37
Wiegand Output Settings .....	38
Terminal Initialization .....	39
Settings Initialization .....	39
Authentication Record Initialization .....	40
Factory Initialization .....	40
How to Use the Terminal .....	40
Access Control .....	40
Authentication Mode .....	41
Card Authentication .....	41
Password Authentication .....	42
Time Attendance Control .....	43
Authentication Mode .....	44
Working Mode Expansion Using Multi-key Authentication .....	45
Meal Control .....	46
Meal Classification .....	46
Card Authentication .....	47
Password Authentication .....	47
Notes .....	47

## Tabela de Revisões

Revisão	Data	Descrição
A.0	22/10/10	Criação deste documento

## Glossary

### Admin, Administrator

- As a user who can enter into the terminal menu mode, he / she 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, so 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 fingerprint recognition unit.

### Authentication Method

- Various kinds of authentication including RF(card) authentication, PW (password) authentication or a combination of these methods  
Ex) RFIPW: card or password authentication; ID&password is used for authentication if card is not used.

### Function Keys

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

### [NS] / [SN] / [NO] Mode

- [NS] Mode: When there is a live connection to the server, authentication is done through the server. If not, it is done through the terminal.
- [SN] Mode: Even though there is a live connection to the server, authentication is done through the terminal and the result is forwarded to the server in real time. However, in the case of 1:1 authentication, if the entered user ID is not registered in the server, authentication is done through the server.
- [NO] Mode: Even though a user is registered in the terminal, authentication is done through the server in any event.

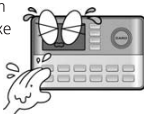
## Cuidados Especiais Durante o Uso

### Cuidados e Avisos de Segurança

#### Atenção:

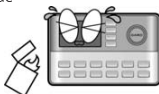
Não opere o dispositivo com mãos molhadas ou não deixe cair líquidos no dispositivo.

- Pode quebrar ou causar choque elétrico.



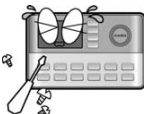
Não aproxime objetos que causam fogo perto do terminal.

- Pode causar incêndio.



Não desmonte, abra ou modifique o dispositivo.

- Podem quebrar, causar choque elétrico ou incêndio.



Mantenha o terminal fora do alcance de crianças.

- Pode quebrar o terminal ou causar acidentes com crianças.

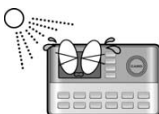


- Se os itens não forem seguidos devidamente, pode causar sérios prejuízos a saúde ou até mesmo morte.

### Precauções

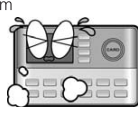
Não exponha diretamente à luz do sol.

- Pode ocorrer deformação ou descoloração.



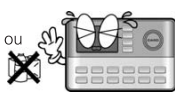
Não coloque em lugares com muita umidade ou poeira.

- Pode quebrar o terminal.



Não borrife água para fazer a limpeza do terminal. Não use benzeno, tiner ou álcool para limpeza.

- Pode ocorrer choque elétrico ou incêndio.



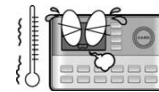
Não aproxime materiais magnéticos.

- Podem quebrar ou causar mau funcionamento do terminal.



Não coloque em lugares com grandes variações de temperatura.

- Pode quebrar o terminal.



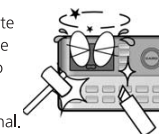
Não borrife pesticidas ou líquidos inflamáveis no terminal.

- Podem ocorrer deformação ou descoloração.



Dispositivo não resistente a impactos. Não encoste objetos pontiagudos no dispositivo.

- Pode quebrar o terminal.



- Se os itens não forem seguidos devidamente, podem ocorrer danos e prejuízos.

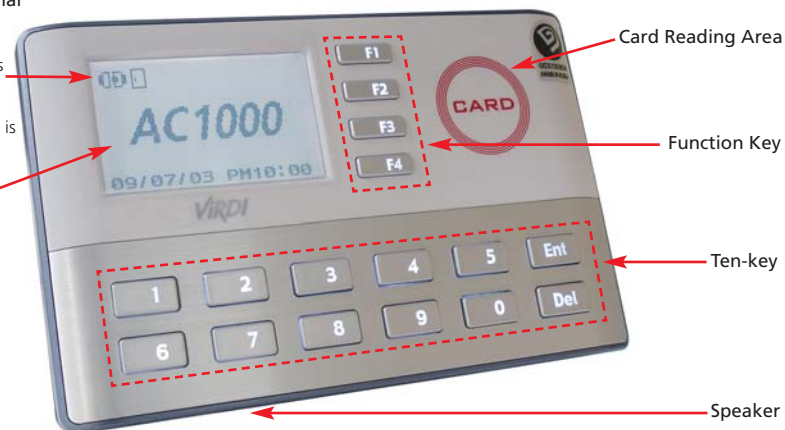
- Não nos responsabilizamos por acidentes ou estragos causados se as recomendações não forem seguidas.

### Terminal Description

LCD icon: Terminal operation state

- LAN: Server connection status
- DOOR: Door open/close status
- CARD: Card data is read

LCD display window: Display character message for all the operations



Button Description

Function key	Access mode	T&A mode	Cafeteria mode
F1	F1	Start	Menu 1
F2	F2	Leave	Menu 2
F3	F3	Outside	Menu 3
F4	F4	Return	Menu 4

12345\*67890#

Enter menu after pressing over 2 sec

Change setting. Move to upper menu. Return to normal mode

Input number '0' value or Menu scroll button

Screen Description (During Operation)

START

Sucesso

2009/08/25 16:58

Network status with server

Door open / close status

Card data is read

Access mode is displaying (F1, F2, F3, F4)

T&A mode is displaying (START / LEAVE / OUT / BACK / NORMAL)

Menu type is displaying during cafeteria mode

Information message

Current time

AC1000

2009/08/25 16:58

Initial screen

Input ID

2009/08/25 16:58

Waiting for a user's ID to be input

Password

2009/08/25 16:58

Password input

Success

2009/08/25 16:58

Authentication is successful

Matching Fail

2009/08/25 16:58

Authentication is failed

No Record

2009/08/25 16:58

Entered a non-registered user ID  
Connection method is [SN] and 1:N identification is accessed even though there is no user allowed for 1:N identification

Duplicate

2009/08/25 16:58

A registered user tried authentication twice time during same menu time when terminal is cafeteria mode.

Net Error

2009/08/25 16:58

There is no response from the server during the authentication process.  
Network to server is disconnected during the authentication process.

Connecting

2009/08/25 16:58

There is no user registered on the terminal or no connection to the server, so it is trying to connect.

Place your card

2009/08/25 16:58

Ready status for card data input

Time Expired

2009/08/25 16:58

A registered user tried authentication when entry/exit is not allowed.

Verifying

2009/08/25 16:58

Waiting for server authentication.

Locked

2009/08/25 16:58


Terminal is locked.  
A registered user tried authentication when Cafeteria time is not allowed

Upgrading

2009/08/25 16:58

Terminal program upgrade (Power switch should not be turned off when this message is displayed.)

## LCD Icon During Operation


 : LAN cable is not connected.

Network status  : LAN cable is connected, but server is not connected.

 : Server is connected.

Door status  : Door Close

 : Door Open

Card input  : Displayed 1sec after card data is read

## Voice Information During Operation

"You are authorized"	Authentication is successful
"Please try again"	Authentication is failed

## Buzzer Sound During Operation

Confirmation Tone (One beep)	When a button is pressed or a card is being read
Error Tone (Two short beeps)	Authentication failed or wrong user input
Beeping	Waiting for fingerprint input
Confirmation Tone (Three short beeps)	Authentication successful or settings for the current user are completed

## Introduction

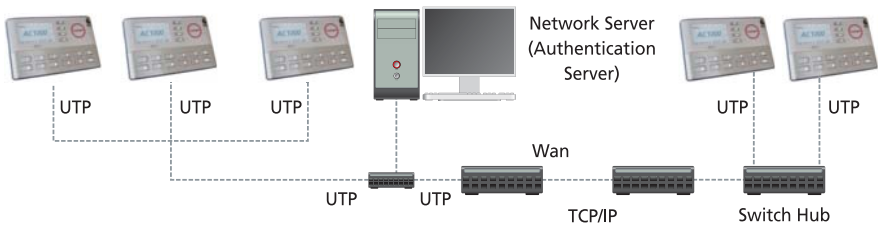
### Features

- Access control system using LAN
  - Communication between the terminal and authentication server is done through d TCP/IP protocol, so an existing LAN can be used as it is. It guarantees network-based administration and monitoring as well as easy expansion, high reliability, and higher speed.
- Simple and fast authentication process.
- High capacity of terminal and server
  - There is no limit on user registration for the server, and the terminal itself can store up to 20,000 card user.
- Various information messages
  - It ensures easy fingerprint recognition because voice and LCD window information are provided during the authentication process. In addition, the backlight installed in the LCD window helps with easy key operation in the dark
- Various and flexible Access controls
  - Perfect control by assigning different security clearances to each user or group
  - Provides flexibility by allowing limited time for entry/exit
- Various applications including Access, T&A, Cafeteria management.
  - Various operation modes depending on the terminal menu settings
- Various registration and authentication methods
  - There are a total of 5 registration and authentication methods, so you are required to select one method before registering users and an administrator.

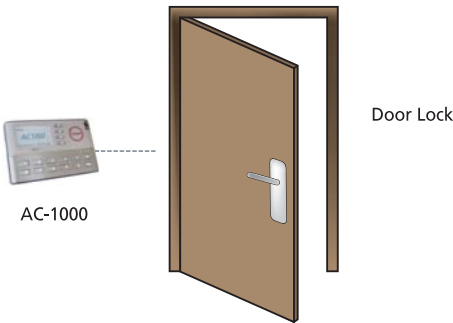
RF	Card registration, Card authentication
ID&PW	Password registration, Password authentication
RF / PW	Card and password registration, Card or password authentication.
RF&PW	Card and password registration, Password authentication after card authentication.
ID&PW / RF&PW	Card and password registration, Password authentication after ID input or password authentication after card authentication.

Configuration

Network Configuration



Standalone Configuration



Specifications

Item	Spec	Remark
CPU	32 Bit RISC CPU	
Memory	8 M SDRAM	
	2 M FLASH (Default)	User: 10,000 / Log: 20,000
	4 M FLASH (Option)	User: 20,000 / Log: 98,000
Authentication speed	<0.2 sec.	
Communication Port	TCP/IP, Wiegand In&Out	
	RS-232, RS-485, 2 Relay	
Temperature / Humidity	-10 ~ 50 / Lower than 90% RH	
LCD	128 X 64 Graphic LCD	
SIZE	140 X 89 X 28 mm	
Power consumption	INPUT: Universal AC 100 ~ 220V	
	OUTPUT: DC 12V (Option: DC 24V)	
	UL, CSA, CE Approved	
Card Reader	RF Card Reader (AC-1000RF Model)	EM Card, 125 kHz
	Smart Card Reader (AC-1000SA Model)	ISO 14443 A-type, 13.56 MHz

Environment Settings

Check items before setting the environment

Entering Menu

The following screen appears when the [ENT] button is pressed for over 2 sec.

1. User
  2. Network
  3. Option
  4. Terminal Info
  5. Ext Function
  6. Device

Press [0] to view menus not shown in the LCD window.

If a number corresponding to the menu required is pressed (ex. [1] for user account), the following screen for administrator authentication appears:



Press [ENT] after entering the administrator’s ID and the administrator authentication is processed according to the previous setting such as fingerprint authentication or password authentication. If authentication is successful, sub-menus of the menu chosen appear.

- Administrator authentication is required only once, so all menus are accessible until he exits from the menus altogether.

Change Settings

To change settings, press the [DEL] button to delete old values and input new values.

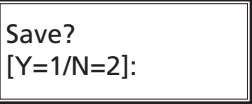
Press [0] to see menus not shown in the LCD window, and press the corresponding number to select a menu.

Press [ENT] for settings verification or to move to the next setting, and press the [DEL] button to move to upper menus.

Hold the [DEL] button for over 2 sec. to cancel the current setting and move to the upper menu.

Save Environment Settings

Press the [DEL] button in the main menu to save environment settings and the following screen appears:



Press [0] to view menus not shown in the LCD window.

- If there are no changes made to the settings, “Save?” does not appear, and the initial screen appears.
- If there is no input for a certain period of time while setting the environment, the settings process will finish. If there are changes made to the settings, “Save?” appears. If not, it does not appear and the initial screen appears.

Menu Configuration

1. User	1) Add 2) Delete 3) Modify 4) Add Admin 5) Delete All	
2. Network	1) Terminal ID 2) Mode [NS/SN/NO] 3) Network Type [Static IP/DHCP] 4) IP Address 5) Subnet Mask 6) Gateway 7) Server IP 8) Server port	
3. Option	1. Application - 0 = Access - 1 = Time Attendance - 2 = Cafeteria	1. T&A mode <Application> <Start Time> <Leave Time> <Normal Time> <Multi Fn-Key>
	2. Verify Option	2. Meal mode <Breakfast> <Lunch> <Dinner> <Supper> <Snack> <Without Limit> <Ticket Printer>  <Show User ID> <Auto Enterkey> <Only Card>



3. Option	3. Set Door lock	<Open Duration> <Door Monitor> <Door Open Alarm>
	4. Sound Control	<Use Voice> <Beeper Volume>
	5. Time Setting	
	6. Other Setting	<LCD Backlight > <LCD Brightness> <Display Time>
4. Terminal Info	Terminal ID =0001 Version =10.01.00 Application=Access Language=ENG Mode=NS Network Type=Static(1) Mac-Address=000265101111 I IP Address =192.168.0.3 Gateway =192.168.0.1 Subnet Mask =255.255.255.0 Server IP =192.168.0.2 SVR Port =2201 Card Reader =RF Max User =10416 All User =0 All Admin =0 All Log =0 Max Log=20479 Dip Switch=000000	
5. Ext function	1. Lock Terminal 2. Read Card No.	
6. Device setting	1. System Config	<ID Length> <Language>
	2. Set Fn-Key	
	3. Card Reader	<Card Reader> <Card Format>
	4. Wiegand	
	5. Initialize	1. Init Config 2. Delete Log 3. Init Terminal

## User Account

### User Registration

Press the [1] button in the main menu to select "1.User," and the following screen appears:

1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All

Press [1] to register a new user.

User ID [NEW]  
ID : \_ \_ \_ \_

Enter a new user ID, and press [ENT].

If the entered ID is already used, you will hear an error tone and the screen will go to the previous menu. If not, the following authentication method selection screen appears:

- 1.RF
- 2.ID&PW
- 3.RFIPW
- 4.RF&PW
- 5.ID&PW/RF&PW

Select one from 1~5 registration methods

#### "1. RF" registration

Card registration and card authentication.

[ENT] -> [1] -> [1] -> User ID + [ENT] -> [5] -> Place the card

< Add Card >  
Place Your Card

To cancel registration, press the [DEL] button.

If a user places the card close to the unit, three short beeps(registration is successful) will be heard and the "1. Add" menu appears. If the entered ID is already used, you will hear an error tone and the screen will go to the previous menu.

## "2. ID&PW" registration

Password registration and password authentication for a user

[ENT] -> [1] -> [1] -> User ID + [ENT] -> [2] -> Input password + [ENT] -> Input same password + [ENT]

< Input PW >  
PW : \_\_\_\_\_

Input password. Password should be 1~8 characters in length.

Press [ENT] to input the password.

< Confirm PW >  
PW : \_\_\_\_\_

Input the same password once more for verification.

If you hear three short beeps, registration is successful. If the passwords are different you will hear an error tone indicating failure and the "1.Add" menu screen appears.

## "3. RFIPW" registration

Card and password registration, card or password authentication

[ENT] -> [1] -> [1] -> User ID + [ENT] -> [8] -> Place the card -> Input password + [ENT] -> Input same password

After card registration (refer to "1. RF" registration), password registration (refer to "2. ID&PW" registration) follows.

## "4. RF&PW" registration

Card and password registration, card and password authentication

[ENT] -> [1] -> [1] -> User ID + [ENT] -> [9] [1] -> Place the card -> Input password + [ENT] -> Input same password + [ENT]

After card registration (refer to "1. RF" registration), password registration (refer to "2. ID&PW" registration) follows.

## "5. ID&PWIRF&PW" registration

RF-Card and password registration, ID input and password authentication or card and password authentication

[ENT] -> [1] -> [1] -> User ID + [ENT] -> [9] [3] -> Place the card -> Input password + [ENT] -> Input same password + [ENT]

In this case, a card is used instead of ID for authentication. This is helpful to users who have difficulty inputting their ID.

After Card registration (refer to "1. RF" registration), password registration (refer to "2. ID&PW" registration) follows.

## Delete User

[ENT] -> [1] -> [2] -> User ID + [ENT]

In the main menu, press [1] to select "1.User" and the following screen appears:

1. Add
2. Delete
3. Modify
4. Add Admin
5. Delete All

To select delete user, press [2].

After entering the user ID to delete, press [ENT] you will hear three short beeps and all the information about the user is deleted. However, the information is still stored in the server. To completely delete this information, the data in the server shall also have to be deleted.

If a non-registered user ID is entered, "2.Delete" appears together with an error tone.

Caution is required when deleting a user or an administrator. The user just registered in the unit (not in the server) is not recoverable, so special care is required.

## Modify User

[ENT] -> [1] -> [3] -> User ID + [ENT] -> Select changing menu -> Change value

In the main menu, press [1] to select "1. User" to see the following screen:

1. Add  
2. Delete  
3. Modify  
4. Add Admin  
5. Delete All

To Modify a user, press [3].

Input ID [MOD]  
ID: \_ \_ \_ \_

Enter the user's ID to Modify, and press [ENT].

When changing an ID, there is no difference between a user and an administrator. If a non-registered user (or administrator) is entered, you will hear an error tone and the "1. Add" menu appears.

## "1. RF" user

### 1. Change Card

To change the card, press [1].  
To cancel, press the [DEL] button

Press [1] button to change the card.

<Change Card>  
Place Your Card

To cancel, press the [DEL] button.

If a user places the card close to the unit, three short beeps (Modification is successful) will be heard and the "1. Add" menu appears.

## "2. ID&PW" user

### 1. Modify PW

To change passwords, press [1]. To cancel it, press [DEL].

Press the [1] button to change the passwords

<Input PW>  
PW: \_ \_ \_ \_ \_

Input new password. Password should be 1~8 characters in length.

Press [ENT] to input the password.

<Confirm PW>  
PW: \_ \_ \_ \_ \_

Input the same password once more for verification.

Press [ENT] to confirm the password.

If the password change is successful, you will hear three short beeps if not, you will hear an error tone and the "1. Add" menu appears.

## "3. RFIPW", "4.RF&PW", "5.ID&PWIRF&PW" user

1. Modify PW  
2. Change Card

To cancel, press the [CLR] button.

Press the [1] button to change passwords (refer to "3.3.3.2").  
Press the [2] button to change the card (refer to "3.3.3.1")

## Administrator Registration

[ENT] -> [1] -> [4] -> Admin ID + [ENT]

In the main menu, press [1] to select "1.User" and press [0] to view menus not shown in the LCD window. And the following screen appears:

1. Add  
2. Delete  
3. Modify  
4. Add Admin  
5. Delete All

For administrator registration, press [4].

<Admin ID [NEW]>  
ID : \_ \_ \_ \_

Enter the administrator ID to register and press [ENT].

- The procedures for administrator registration are the same as for user registration.

Only an administrator can change the terminal operation environment and register/change/delete user information stored in the unit, so special care is required when registering an administrator.

## Delete All Users

[ENT] -> [1] -> [5]

In the main menu, press [1] to select "1. User" and select [0] to see the following screen:

1. Add  
2. Delete  
3. Modify  
4. Add Admin  
5. Delete All

To delete all users, press [5].

Delete All?  
[Y=1/N=2] : \_

To delete all users, press [1]. If not, press [2].

Special care is required because all user accounts including the administrator are deleted with this operation.

When this operation is successful, you will hear three short beeps and the "1. Add" menu appears.

## Network Settings

In the main menu, press [2] to select "2.Network" to see the following screen. When the setting is chosen, press [ENT] to move to the next setting.

## Terminal ID Settings

[ENT] -> [2]

< Terminal ID >  
ID : 00000001

This ID is unique for each terminal and used by an authentication server to distinguish each terminal. The default is '00000001'.

It should be identical to the door ID set in the server program, and its length should be 1~8 characters.

If the terminal ID is '1000', enter [1][0][0][0] in sequence. If it is '0001', enter only [1]. Press [ENT] to move to the next setting.

## Connection [NS / SN / NO] Mode Settings

[ENT] -> [2] -> [ENT]

Mode [ NS / SN / NO ]  
( 0-2 ) : 1

NS mode: '0', SN mode: '1',  
NO mode: '2'

This defines the authentication method between the terminal and network server, and the default is '1' (SN). Each authentication method is described below:

- **NS mode:** select [0]. When there is a live connection to the server, authentication is done through the server. If not, it is done through the terminal.
- **SN mode:** select [1]. Even though there is a live connection to the server authentication is done through the terminal and the result is forwarded to the server in real time.  
However, in the case of 1:1 authentication, if the entered user ID is not registered in the server, authentication is done through the server.
- **NO mode:** select [2]. Even though a user is registered in the terminal, authentication is done through the server in any event.

Depending on the number of terminals, the number of users, or network conditions, each different mode can be used flexibly, but if there are more than 10 terminals connected to the server for simultaneous authentication or there are frequent network problems, it is recommended to use SN authentication (setting '1').

Press [ENT] to move to the next setting.

## Connection Method Settings

[ENT] -> [2] -> [ENT] -> [ENT]

**Network Type:0**  
**0:Static 1:DHCP**

Press [0] for Static IP.  
Press [1] for DHCP.

The default is '0' (Static IP). If a fixed IP is assigned to the unit in a network, press [0]. If there is a DHCP server in the network to which the unit is connected, press [1].

Press [ENT] to move to the next setting.

- For Static IP (0), refer to 3.4.4. IP address, 3.4.5. Subnet mask and 3.4.6. Gateway. For DHCP, skip those sections.

## IP Address Settings

**< IP Address >**  
**192.168.000.003**

Press [DEL] to delete an old IP and enter the new IP.

If the IP address is '210.98.100.50', enter as below:

[2] [1] [0] [0] [9] [8] [1] [0] [0] [5] [0]

Press [ENT] to move to the next setting.

## Subnet Mask Settings

**< Subnet Mask >**  
**255.255.255.000**

Press [DEL] to delete an old value and enter the new value.

If the subnet mask is '255.255.255.0', enter as below:

[2] [5] [5] [2] [5] [5] [2] [5] [5] [0]

Press [ENT] to move to the next setting.

## Gateway Settings

**< Gateway >**  
**192.168.000.001**

Press [DEL] to delete an old value and enter the new value.

If the gateway IP address is '210.98.100.1', enter as below:

[2] [1] [0] [0] [9] [8] [1] [0] [0] [1]

Press [ENT] to move to the next setting.

## Server IP Settings

< Server IP >  
192.168.000.002

Press [DEL] to delete an old value and enter the new value.

If the sever address is "210.98.100.121", enter as below:

[2] [1] [0] [9] [8] [ENT] [1] [0] [0] [1] [2] [1]

Press [ENT] to move to the next setting.

## Server Port Settings

< Server port >  
Num : 2201

Press [DEL] to delete an old value and enter the new value.

As the port number of the authentication server, the default is '2201'. Special care is required when changing this number because the corresponding number in the server should also be changed.

If the server port is '2201', enter as below:

[2] [2] [0] [1]

Once the network setting is complete, press [ENT] to return to the main menu.

## Option Settings

### Application Mode Settings

In the main menu, press [3] to select "3. Option" and following screen appears:

1. Application  
2. Verify Option  
3. Set Door lock  
4. Sound Control  
5. Time Setting  
6. Other Setting

To set the basic operation mode of a terminal, press [1].

[ENT] -> [3] -> [1]

<Application>:0  
0=Access Ctrl  
1=T&A Ctrl  
2=Meal Ctrl

The default is '0' (Access Ctrl).

For simple Access control mode, select '0'.

For Time Attendance control mode, select '1'.

For Meal (Cafeteria) control mode, select '2'.

Press [ENT] to move to detailed settings for each operation mode.

### [0]: Access Control

No more detailed settings. It moves to the upper menu.

### [1] Time Attendance Control

Default time can be set to Start/Leave/Out/Back. After authentication, the terminal display mode can be automatically changed to programmed operation mode. If <multi-key authentication> is set as the operation mode, over 40 sub modes can be defined.

< Start Time >  
00:00-00:00

If time setting is not necessary,  
Set as '00:00-00:00'.

To change the start time from '00:00~00:00' to '06:00~09:59', press [DEL] to delete the existing setting time, and enter [0][6][0][0][0][9][5][9] in sequence.

As long as no other function button is pressed during the setting time, it operates in start time mode. Even if it is set to outside work, the terminal display mode automatically changes to start mode, so authentication is convenient.

After setting <start time>, set <leave time> and <normal time> in the same manner. Each time shall not be overlapped.

Ex) Start time: 06:00~09:59, Leave time: 17:00~22:00, Normal time: 10:00~16:59

< Start Time > 06:00~09:59	< Leave Time > 17:00~22:00	< Normal Time > 10:00~16:59
-------------------------------	-------------------------------	--------------------------------

After setting normal time, press [ENT] to see the "Multi Fn-key" setting menu, which allows more than 5 working modes.

< Multi Fn-key > 1=F1:X 2=F2:X 3=F3:X 4=F4:X
--

Default setting: all 'X'

This menu is useful when more than 5 working modes are necessary.

- X setting: each function key represents a working mode such as F1=Start, F2=Leave, F3=Outside work and F4=Back. When a function key is pressed, authentication mode changes to the corresponding working mode.
- O setting: a mode is defined by the combination of a function key and a number key such as "F3+1".  
(Ex.) If the setting is 1=F1: X 2=F2: X 3=F3: X 4=F4: O,  
14 different working modes can be defined according to user input such as [ENT]: normal, [F1]: start, [F2]: leave, [F3]: outside work and [F4]+'0'~[F4]+'9'.

The O/X setting can be changed by pressing the corresponding number key. After setting is completed, press [ENT] to move to the upper menu.

## [2] Meal (Cafeteria) Service Control

<Breakfast> 00:00-00:00
----------------------------

If time setting is not necessary,  
Set as '00:00-00:00'.

If <Breakfast> time is set from 07:00 to 09:00, all authentication data is recorded as <breakfast>.

After setting <Breakfast> time, continue to set <Lunch>, <Dinner>, <Supper> and <Snack> with same manner. If some menu is not necessary, set as '00:00-00:00'.

Each menu time shall not be overlapped. User can authenticate only one time during same menu time.

If user has to authenticate more than one time, he/she has to authenticate fingerprint after <ENTER> button is pressed.

'Terminal Locked' message will be displayed during an interval time between each <Menu> setting time. Nobody can authenticate until the terminal is locked except entering a menu mode.

Press [ENT] to see <Without Limit> menu setting after setting all the menu time

<Without Limit> (N=0/Y=1):0
--------------------------------

Default setting: '0'

- Select [0]: Only one authentication for each user at the same menu. If a user wants double authentication, a user has to scan a fingerprint pressing F4 button.
- Select [1]: There is no limitation of authentication times.

## Authentication Method Settings

In the main menu, press [3] to select "3. Option" and the following screen appear:

1. Application
2. Verify Option
3. Set Door lock
4. Sound Control
5. Time Setting
6. Other Setting

To set the default authentication method, press [2].

### Settings for ID Display When Authentication is Successful

[ENT] -> [3] -> [2]

**< Show User ID >  
(0-2):0**

Default setting: '0'

If it is set to the default setting [0], only the "Success" message is displayed.

If it is set to [1], user ID is displayed in the LCD window when authentication is successful as shown below:

(Ex.) OK! <0001>

If it is set to [2], user name is displayed in the LCD window when authentication is successful as shown below:

(Ex.) OK! <William>

Press [ENT] to move to the next setting.

### Auto Enter Key Setting

[ENT] -> [3] -> [2] -> [ENT]

**<Auto Enter Key>  
(N=0/Y=1):0**

Default setting: '0'

If it is set to the default setting '0', a user should input ID and push [F1]~[F4], [ENTER] or go through fingerprint verification.

If it is set to [1], for a example, a user who uses password inputs ID, which goes for authentication process without pushing any function key.

The authentication mode is the currently setting mode.

Press [ENTER] to move to the next setting.

### Settings for Card Only Authentication

[ENT] -> [3] -> [2] -> [ENT]

**< Only Card >  
(N=0/Y=1):0**

Default setting: '0'

Even for a user who is registered to be authenticated with a card & PW / card & fingerprint, he/she only needs to use a card if this option is set to '1'.

This option is usually used when there are many terminals installed at the building entrance door where user entry/exit is frequent and the security level is relatively low.

Once the setting is complete, press [ENT] to move to the upper menu.

### Door Settings

In the main menu, press [3] to select "3. Option" and the following screen appear:

1. Application
2. Verify Option
3. Set Door lock
4. Sound Control
5. Time Setting
6. Other Setting

Press [3] for door settings.

### Door Opening Time Settings

[ENT] -> [3] -> [3]

**< Open Duration >  
(00-30):03**

Default setting: '03' (unit: sec.)



This is used to set the door opening time after authentication is successful. For the strike type, this means the door opening time. For the dead bolt type or auto door, this time is not effective.

If this is set to '00', the door is out of control, so it may be set to '00' only for the start/leave time period.

Once the setting is complete, press [ENT] to move to the next setting.

### Door Status Monitor

[ENT] -> [3] -> [3] -> [ENT]

< Door Monitor >  
[0/1=NO/2=NC]:0

Default setting: '0'

- '0': NW - no check
- '1': NO - dead bolt type or auto door  
(Lock monitoring is on when the door is locked)
- '2': NC - strike type  
(Lock monitoring is off when the door is locked)  
'0' is for no check, '1' is for dead bolt type or auto door; '2' is for strike type. When this is set to '1' or '2', the door condition connected to the terminal is sent to the server periodically.

Once the setting is complete, Press [ENT] to move to the next setting.

### Door Open Alarm Settings

[ENT] -> [3] -> [3] -> [ENT] -> [ENT]

< Door Open Alarm >  
(00-30):00

Default setting: '00'

The terminal checks if the door has been open for more than setting time (5sec~30sec) if so, it makes an alarm sound. If this is set to '00', there is no alarm sound.

This alarm helps the relevant person check what has caused the problem in a timely manner and eliminate the problem.

For this function, the lock shall be able to monitor whether the door is open or closed and its monitoring pin shall be connected to the terminal. The door open check shall be set to '1' or '2' for this operation.

Once the setting is complete, press [ENT] to move to the upper setting.

### Volume Settings

In the main menu, press [3] to select "3. Option" and the following screen appear:

1. Application
2. Verify Option
3. Set Door lock
4. Sound Control
5. Time Setting
6. Other Setting

Press [4] for volume settings.

### Voice Settings

[ENT] -> [3] -> [4]

< Use Voice >  
(N=0/Y=1):1

Default setting : '1'

To make voice information available, set it to '1'. If not, set it to '0'. Press [ENT] to move to the next setting.

## Buzzer Volume Settings

[ENT] -> [3] -> [4] -> [ENT]

< Beeper volume >  
(0-2):1

Default setting : '1'

This controls the terminal buzzer volume. If this is set to '0', there is no buzzer sound. '1' means low volume, and '2' means high volume.

Press [ENT] to move to the next setting.

## Current Time Settings

[ENT] -> [3] -> [5]

In the main menu, press [3] to select "3. Option". Press [5] to see the following screen:

< Time Setting >  
20060401211806

This is for the terminal current time. The above example represents the year 2006, month 04, date 01, hour 21, min. 18, and sec. 06. To change it, delete the old numbers with the [DEL] button before adding the new numbers.

Press [ENT] to check that the current time is updated and move to the upper menu.

## Other Setting

In the main menu, press [3] to select "3.Option". Press [6] to see the following screen:

1. Application
2. Verify Option
3. Set Door lock
4. Sound Control
5. Time Setting
6. Other Setting

Press [6] for other settings.

## LCD Backlight On/Off Settings

[ENT] -> [3] -> [6]

<LCD Backlight >  
(0=Off/1=On):

Default : '0'

This is for LCD backlight on/off settings.

If it is set to the default setting '0', LCD backlight is normally off. Only in cases that a user operates with keypad or card, LCD backlight goes on and after the working operation is done, it goes off in about 10 seconds. If it is set to '1', it always stays on.

Press [ENT] to move to the next setting

## LCD Brightness Settings

[ENT] -> [3] -> [6] -> [ENT]

<LCD Brightness>  
(0-2):1

Default : '1'

This is for LCD brightness level setting menu. The higher setting value is for high brightness.

Press [ENT] to move to the next setting.

Display Time Settings

[ENT] -> [3] -> [6] -> [ENT] -> [ENT]

<Display Time> : 1  
0=20:30  
1=PM 8:30

Default : '1'

This is for current time display mode setting menu.

If it is set to the default setting '0', time is displayed as below.  
[ 07/08/25 21:30 ]

If it is set to the default setting '1', time is displayed as below.  
[ 07/08/25 PM 9:30 ]

Once the setting is complete, press [ENT] to move to the upper menu.

Terminal Information View

[ENT] -> [4]

In the main menu, press [4] to select "4.Terminal info" and the following screen appears where all the environmental settings are displayed:

Terminal ID=0001  
Ver=10.00.01  
Application  
=Access  
Language=ENG  
Mode=SN ▼

Press [0] to scroll up and down the screen.

Terminal ID	terminal ID
Version	Terminal firmware version
Application	terminal Application mode (Access/T&A)
Language	Language for text and voice of the LCD screen
Mode	connection mode between terminal and network server
Network type	network connection type (fixed IP/variable IP)
Mac Address	terminal Ethernet hardware address
IP address	terminal IP address
Gateway	terminal Gateway address
Subnet mask	terminal Subnet Mask address
Server IP	IP address of network server connected to the terminal
SVR port	Port number of network server program
Card Reader	connected card reader type
Max User	Max. number of users registered to a terminal
All User	Number of current users registered to a terminal including administrators
All Admin	Number of administrators registered to a terminal
All Log	Authentication records stored in a terminal
Max Log	Max. number of authentication records stored in a terminal
Dip Switch	Dip Switch setting status SW2_1, SW2_2, SW2_3, SW2_4, SW2_5 SW2_6

Extended Functions

[ENT] -> [5]

In the main menu, press [5] to select "5.Ext functions" and the following screen appears:

1. Lock Terminal  
2. Read Card No.

## Terminal Lock Settings

[ENT] -> [5] -> [1]

< Lock?>  
(N=0/Y=1):0

Default setting '0': terminal lock clear  
'1': terminal lock set

Instead of a server program, an administrator can directly set up a terminal lock for a terminal. If it is set to '1', the terminal is locked and nobody can pass the door until an administrator unlocks the terminal.

- For this function, 'administrator entering OK' shall be checked in the terminal option of the server program.

Once the setting is complete, press [ENT] to move to the upper menu.

## Read Card Number

[ENT] -> [5] -> [2]

Place Your Card

As an auxiliary function regardless of the terminal environmental settings, a terminal with a card reader can read the card number to register the card to a server.

When the card is read by the terminal, the card number is displayed on the LCD window.

To exit from the card reader, press [CLR] to move to the upper menu

## Device Settings

In the main menu, press [6] to select "6. Device" and the following screen asking for the setting password appear:

A device setting is an option that is not necessary to change after installation, so it is recommended not to change it except when it is really required.

< Input PW >  
PW: \_ \_ \_ \_ \_

This setting password is just for user information, so it cannot be changed.

Enter "084265" as the setting password and press [ENT] to view the detailed setting items.

## System Configuration Settings

1. System Config  
2. Set Fn-Key  
3. Card Reader  
4. Wiegand  
5. Initialize

Press [1] for system settings.

## User ID Length Settings

[ENT] -> [6] -> '084265' + [ENT] -> [5]

< ID Length >  
(2-8):4

Default setting: '4'

This can be 2~8 digits and shall be the same as the ID registered in the server program. If the ID registered in the server program is '000075', enter 6.

Special care is required when reducing the number of digits during normal operation because an administrator may not be able to be authenticated when he wants to enter menus due to the reduced number of digits.

Press [ENT] to move to the next setting.

### Language Settings

[ENT] -> [6] -> '084265' + [ENT] -> [5] -> [ENT]

< Language >:1	
0=KOR	1=ENG
2=JPN	3=CHN
4=SPN	5=UAE
6=ITLY	7=VIET
8=OTH	

Default setting: '4'

Voice information languages follow these settings: '0': Korean, '1': English, '2': Japanese, '3': Spanish, '4': Chinese, '5': Arabic, '6': Italian, '7': Vietnam '8': Other language.  
'0', '1', '2', '4': LCD characters also correspond to the language.  
'3', '5', '6', '7', '8': LCD characters are in English.

Once the setting is complete, press [ENT] to move to the upper menu

### Function Key Settings

[ENT] -> [6] -> '084265' + [ENT] -> [2]

<Key On/Off>	
1=F1:O	2=F2:O
3=F3:O	4=F4:O
5=Ent:O	

Default setting: all 'O'

This is for enabling/disabling the function keys. 'O' is 'enable' and 'X' is 'disable'. Whenever a function key is pressed, it toggles between O/X.

1 is for [F1], 2 is for [F2], 3 is for [F3], 4 is for [F4], and 5 is for [Ent]. If F1 becomes X by pressing [1], you can not change to start mode even if you press [F1].

Additionally, if only [F1] or [F2] is set to 'O', the terminal can be used in either always start or always leave mode.

Once the setting is complete, press [ENT] to move to the upper menu.

### Card Reader Settings

[ENT] -> [6] -> '084265' + [ENT] -> [3]

<Card Reade>:0
0=RF/SC
1=Wiegand

Default setting: '0'

This is the setting for the card reader connected to a terminal. This shall be set to 0 except in the following cases:

- '0': 125 kHz card or 13.56 MHz card
- '1': Additional card reader is connected through wiegand interface. (EX: HID reader)

If it is set to the default setting '0', it is possible to set <Card Format> to change card number display format.

<Card Format >:0
0=Hexa 8byte
1=Hexa 16byte
2=Decimal

Default setting: '0'

- '0': Displayed 8 digit number of 16 antilogarithm -> A5CBEF12
- '1': Displayed 8 digit added behind of 8 digit number of 16 antilogarithm -> A5CBEF1200000000
- '2': Displayed 10 digit number of 10 antilogarithm -> 0317705125

Once the setting is complete, press [ENT] to move to the upper menu.

## Wiegand Output Settings

[ENT] -> [6] -> '084265' + [ENT] -> [4]

Wiegand Out:0  
0=None 1=26bit  
2=34bit

Default setting: '0'

When this is set to [1], "Site code + user ID" is sent to the Wiegand port of the terminal when authentication is done. It can be used only for systems where there is a lock controller and the controller is operated by a Wiegand input. This is usually set to [0].

- If it is set to '1', user ID shall be shorter than 4 digits because "Site code [1 byte] + user ID [2 bytes]" is transferred.
- If it is set to '2', user ID shall be shorter than 7 digits because "Site code [1 byte] + user ID [3 bytes]" is transferred.
- this is not effective when a Wiegand-type card reader is used, and set the following site code when the setting is higher than '1'

<Site code>  
(0-255):000

Default setting: '0'

This is only available when Wiegand Out is set to '1' or '2'. Enter the site code (0-255) to be sent to the Wiegand port together with the user ID.

Once the setting is complete, press [ENT] to move to the upper menu.

## Terminal Initialization

In the main menu, press [6] to select "6. Device" and then press [6] to select "6. Initialize" and the following screen will be appeared:

1. Init Config
2. Delete Log
3. Init Terminal

Press [1] for settings initialization, press [2] for authentication record initialization, press [3] for factory initialization.

## Settings Initialization

[ENT] -> [6] -> '084265' + [ENT] -> [6] -> [1]

< Init Config >  
[ Y=1 / N=2 ]:

To initialize settings, press [1]. If not, press [2].

All the settings except Mac (physical) address are initialized, but the user and authentication records are not deleted.

- If the settings are initialized, the language of the voice and menus becomes English. If you need to set other language ("6. Set Device" -> "5. System Config" -> <Language>: set to 0~4)

If initialization is successful three short beeps will be heard and the screen will go to the upper menu.

## Authentication Record Initialization

[ENT] -> [6] -> '084265' + [ENT] -> [6] -> [2]

< Delete All Log >  
[ Y=1 / N=2 ] :

To initialize the record, press [1]. If not, press [2].

Deletes all logs related to authentication, but settings and users are not deleted.

Once initialization is done successfully, it moves to the upper menu together with a beeping sound

## Factory Initialization

[ENT] -> [6] -> '084265' + [ENT] -> [6] -> [3]

< Init Terminal >  
[ Y=1 / N=2 ] :

To Factory Default settings, press [1]. If not, press [2].

Except for the Mac (physical) address stored in the terminal, all settings, users and log information are deleted for the factory default.

- If the settings are initialized, the language of the voice and menus becomes English. If you need to set other language ("6. Set Device" -> "5. System Config" -> <Language>: set to 0~4)

Once initialization is done successfully, the terminal is rebooted after three short beeps.

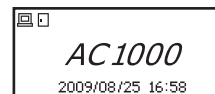
## How to Use the Terminal

### Access Control

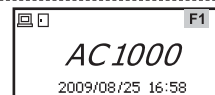
- Menu "3.Option" -> "1.Application" -> [0] Access control settings

## Authentication Mode

- Authentication mode display screen



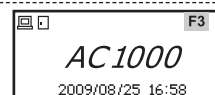
Normal mode; authentication with [ENT]



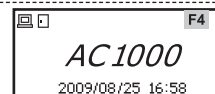
F1 mode; authentication with [F1]



F2 mode; authentication with [F2]



F3 mode; authentication with [F3]



F4 mode; authentication with [F4]

- Card authentication

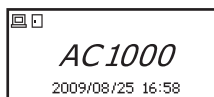
Before place the card, change the authentication mode by pressing the corresponding function key. or place the card for authentication.

- Password authentication

After entering the user ID and changing the authentication mode by pressing the corresponding function key, enter the password for authentication.

## Card Authentication

For a user who is registered as [RF], [RFIFP], or [RFIPW], when placing the card close to the default screen, a beep sound will be heard and the authentication result appears on the LCD.



If you place your card close to the unit, you will hear a beep.

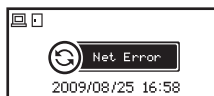


If authentication is successful, you will see a success message on the LCD together with the voice message "You are authorized". The door open icon and the card icon turn on LCD. The default screen appears after 1~2 sec., and the door is closed when the door open setting time has elapsed.

- Error message: An error message appears together with the voice message "Please try again".

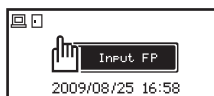


Non-registered card used.



During the authentication request to the authentication server, network trouble occurred or the line is disconnected.

For a user who is registered as [RF&FP] or [ID&FP I RF&FP], when placing the card close to the default screen, a beep will be heard and the following fingerprint authentication screen appears.



When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", enter your fingerprint and hold it there until you hear a beep.

## Password Authentication

If the user ID is "0001", enter "0001" and press the function key. You will hear a beeping sound and the terminal waits for the user password to be input. Enter the password and press [ENT], and the authentication result appears on the LCD.



If the user ID is '0001', enter '0001' and press the function key.



You will hear a beeping sound and the terminal waits for the user password to be input. Enter the password and press [ENT]. (The password is displayed as '\*' on the LCD screen, rather than the actual numbers.)



If authentication is successful, you will see a success message on the LCD together with the voice message "You are authorized". The door open icon and the card icon turn on LCD. The default screen appears after 1~2 sec., and the door is closed when the door open setting time has elapsed.

- Error message: An error message appears together with the voice message "Please try again".



Password authentication failed.



Non-registered user ID entered.



During the authentication request to the authentication server, network trouble occurred or the line is disconnected.

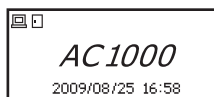
## Time Attendance Control

- Menu "3.Option" -> "1.Application" -> [1] T&A (Time Attendance) settings
- If the start/leave time is fixed, set <start time>, <leave time>, and <normal time> to reduce user input errors.

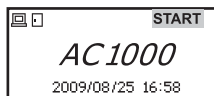


## Authentication Mode

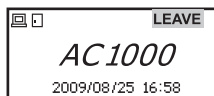
- Authentication mode display screen



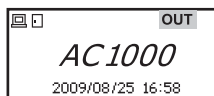
Normal mode; authentication with [Ent]



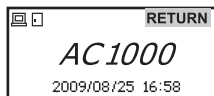
Start mode; authentication with [F1]



Leave mode; authentication with [F2]



Outside work mode; authentication with [F3]



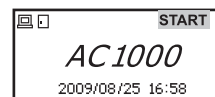
Return mode; authentication with [F4]

- Card authentication  
Before place the card, change the authentication mode by pressing the corresponding function key. or place the card for authentication.
- Password authentication  
After entering the user ID and changing the authentication mode by pressing the corresponding function key, enter the password for authentication.

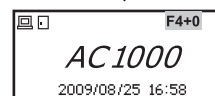
Working mode after authentication depends on <start time>, <leave time>, and <normal time> settings. The previous authentication mode is maintained if no mode is set for a specific time period.

## Working Mode Expansion Using Multi-key Authentication

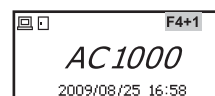
- If more than 5 working modes such as start, leave, outside work, return, and general are required, it can be expanded up to 41 modes.
- After setting Menu -> 3.Option -> 1.Application -> [1] T&A, in <Multi Fn-key>, set more than one key to 'O'. However, the keys set to 'X' are not the case.
- Because a mode is defined with a number key, enter a number key after entering the function key for authentication. In the server program, authentication mode is "F3+1".
- For example, when [F4] is set to [O] and <start time> is set to '07:00~09:30', if a fingerprint user tries authentication "F4+1" mode



In the default screen, press [F4].



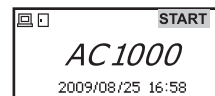
The mode is changed to "F4+0". Press [1].



When the mode is changed to "F4+1", enter the fingerprint.



When authentication is successful, a success message appears.



The current time is 7:58, so it returns to the start mode.

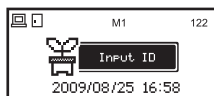
## Meal Control

- Menu -> "3. Option" -> "1.Application" -> [2] Meal settings
- If the terminal is set for meal control, as the terminal is in "lock setting!" status during other time frames except for the meal times previously set, at least more than one time frame as meal time should be set for meal control usage.
- Basically, a single authentication is allowed for each meal per user but double authentication is also possible

"3. Option" -> "1.Application" -> [2] Meal setting -> <Without Limit>

## Meal Classification

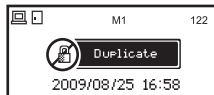
- In meal control, the function key is just an operation key for authentication. There is just meal classification with a meal time frame - there is no mode classification. The number shown in the LCD screen means the number of authentication for a specific meal time period.
- Screen description



Total number of successful authentication is displayed.



Not in meal time period.



In case that a user tries double authentication during the same meal time period.

## Card Authentication

- Same as 4.1.2., but [Ent] cannot be used as a function key.

## Password Authentication

- Same as 4.1.3., but [Ent] cannot be used as a function key.

## Notes

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins or other markings on the paper.