Biometric Access Control System I9

User's Guide

CAUTION: Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment

WARNING
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

INFORMATION TO USER:
This equipment has been tested and found to comply with the limit of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation; if this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
1. Reorient / Relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit difference from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help

Innovative Fingerprint Terminal for Access Control and Time Attendance

- **Fingerprint recognition, now look and feel!**
  - Features 2.5" 16M color LCD to display multimedia contents including animation and photos.
- **Invincible speed and capacity**
  - Delivers fingerprint identification speed to perform 3,000 matches in 1 second and internal memory storing up to 40,000 fingerprints and 200,000 event logs.
- **No more wiring!**
  - Provides various external interfaces including Wi-Fi wireless LAN for easy access to the internal user info and event log from a remote PC.
- **Data into your USB drive**
  - Using USB memory, copies and backs up user info and event log data very easily.
- **World's best fingerprint recognition algorithm**
  - World's most reliable fingerprint solution that ranked No. 1 in an international fingerprint algorithm contest (FVC2004) with the lowest error rate.
- **Various fingerprint sensors**
  - Supports various fingerprint sensors, including optical, capacitive, and thermal swipe, so users can choose the most suitable fingerprint sensor for their application.
- **Mifare Card Support!**
  - Mifare module is built in a Terminal itself. Fingerprint, card, and password can be selected as the authentication method for each user.
  - Template on card supported
- **Real Time Network operation through Server!**
  - Connected to the BioAdmin Server, terminals can be managed in real time.

Contents

Contents

Safety precautions

■ **The list below is to keep user's safety and prevent any loss. Please read carefully before use.**

Do not install the device in a place subject to direct sun light, humidity, dust or soot.

Do not place a magnet near the product. Magnetic objects such as magnet, CRT, TV, monitor or speaker may damage the device.
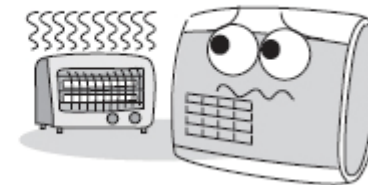
Do not place the device next to heating equipments.

Be careful not to let liquid like water, drinks or chemicals leak inside the device.
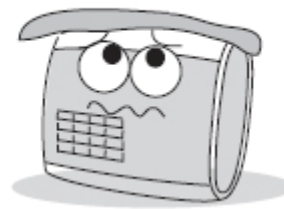
Clean the device often to remove dust on it.

In cleaning, do not splash water on the device but wipe it out with smooth cloth or towel.

Safety precautions

- **The list below is to keep user's safety and prevent any loss. Please read carefully before use.**

Do not drop or damage the device.

Do not press two buttons at the same time.

Do not disassemble, repair or alter the device.

Do not let children touch the device without supervision.

Do not use the device for any other purpose than specified.

Contact your nearest dealer in case of a trouble or problem.

Glossary

- **Administrator**
  - A special user who are authorized to manage the settings and user information of a device. Administrators can enroll or delete users and change settings of the device.
- **1:1 Mode**
  - In 1:1 mode, a user should enter his/her user ID first. After then, the user is requested to place a finger or enter a PIN. In this mode, user's scanned fingerprint is matched against only one fingerprint specified by the user ID.
- **1:N Mode**
  - In 1:N mode, a user places his/her finger without entering any ID. Then the device compares the user's scanned fingerprint with the whole enrolled fingerprints in its internal database.
- **Template on card**
  - The user information can be stored to a smartcard, including fingerprint templates. This eliminates the need to store user's information to the device, enhancing security and ease of management.
- **Fingerprint Enrollment**
  - A process of extracting features of a fingerprint image obtained from a fingerprint sensor and saving them into the internal memory of a device. The fingerprint data is called a fingerprint template.

Basics of fingerprint recognition

- **What is fingerprint recognition?**
  - Fingerprint is an individual's own biometric information and does not change throughout his/her life. Fingerprint recognition is a technology that verifies or identifies an individual using such fingerprint information.
  - Free from the risk of theft or loss, fingerprint recognition technology is being widely used in security systems replacing PIN or cards.

- **Process of fingerprint recognition**
  - Fingerprint consists of ridges and valleys. Ridge is a flow of protruding skin in a fingerprint while valley is a hollow between two ridges. Each individual has different pattern of ridges and valleys and finger recognition makes use of such originality and uniqueness of these patterns.
  - Fingerprint sensor generates 2-dimentional fingerprint image using different technology. According to the sensing technology, fingerprint sensors are classified into optical, capacitive, or thermal.
  - Fingerprint template is a collection of numeric data representing the features of a fingerprint. Fingerprint templates are saved inside the memory of i9 and used for identification.

- **Secure way to protect personal information**
  - To avoid privacy concern, Suprema's fingerprint products do not save fingerprint images itself. It is impossible to reconstruct a fingerprint image from a fingerprint template which is just numeric data of the features of a fingerprint.

How to place a finger

Suprema's fingerprint products show an outstanding recognition performance regardless of the user's fingerprint skin condition or the way of fingerprint positioning. However, following tips are recommended to get more optimal fingerprint recognition performance.

- **Select a finger to enroll**
  - It is recommended to use an index finger or a middle finger.
  - Thumb, ring or little finger is relatively more difficult to place in a correct position.
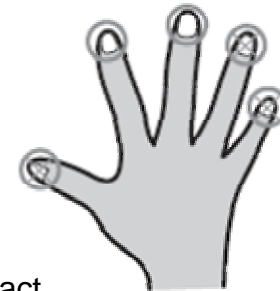
- **How to place a finger on a sensor**
  - Place a finger such that it completely covers the sensor area with maximum contact.
  - Place core part of a fingerprint to the center of a sensor.
    - People tend to place upper part of a finger.
    - The core of a fingerprint is a center where the spiral of ridges is dense.
    - Usually core of fingerprint is the opposite side of the lower part of a nail.
    - Place a finger such that the bottom end of a nail is located at the center of a sensor.
  - If a finger is placed as in the right picture, only a small area of a finger is captured. So it is recommended to place a finger as shown in the left picture.
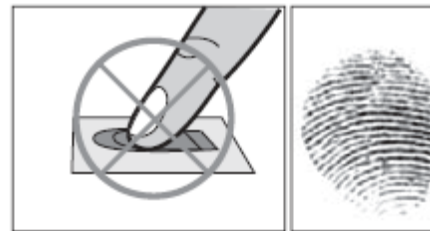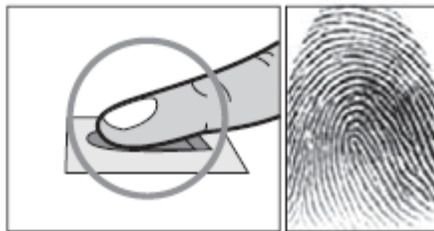
How to place a finger

- **Tips for different fingerprint conditions**
  - Suprema's fingerprint products are designed to scan fingerprint smoothly regardless of the conditions of a finger skin. However, in case a fingerprint is not read well on the sensor, please refer to the followings tips.
    - If a finger is stained with sweat or water, scan after wiping moisture off.
    - If a finger is covered with dust or impurities, scan after wiping them off.
    - If a finger is way too dry, place after blowing warm breath on the finger tip.

- **Tips for fingerprint enrollment**
  - In fingerprint recognition, enrollment process is very important. When enrolling a fingerprint, please try to place a finger correctly with care.
  - In case of low acceptance ratio, the following actions are recommended.
    - Delete the enrolled fingerprint and re-enroll the finger.
    - Enroll the same fingerprint additionally.
    - Try another finger if a finger is not easy to enroll due to scar or worn-out.
  - For the case when an enrolled fingerprint cannot be used due to injury or holding a baggage, it is recommended to enroll more than two fingers per user.

Product Contents

Basic Contents

i9 fingerprint terminal
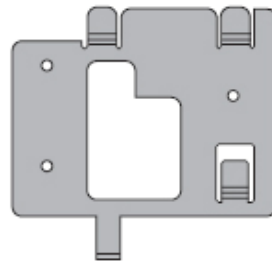
Wall mounting metal bracket

Wall mounting screws and holders - 3 ea

Star-shape screw for fixing main body

USB cable

Star-shape small wrench

Ext cables
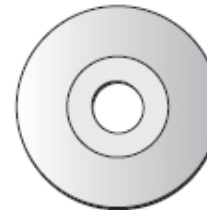
Software CD

Product Contents

■ **Optional accessories**
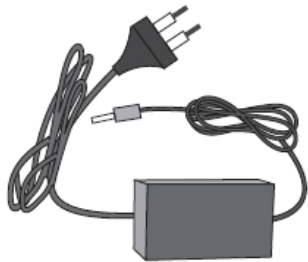
12V power adaptor

● **Recommended power supply**
12V ±10%, at least 1500mA for i9 alone installation.
Comply with standard IEC/EN 60950-1
To share the power with other devices, use a power supply with higher current ratings.
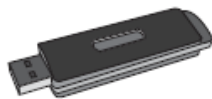
USB memory   Wireless LAN Access Point   Interphone
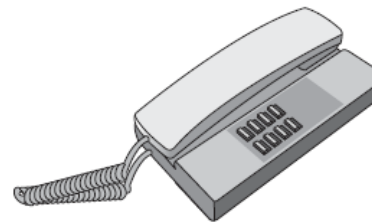
Name of each part

■ **Front**

Microphone
Used when connected to interphone.

Color LCD
Displays terminal status (T&A mode, notice, etc.) and current time.

Navigation key
▼ : Move down in Admin menu or view detailed T&A function key
▲ : Move up in Admin menu or hide detailed T&A function key
► : Show the next setting value in Admin menu or input a dot (.) when entering IP address
◄ : Show the previous setting value in Admin menu or delete a numeric when entering user ID or PIN
OK : Confirm the selected setting or initiate a fingerprint scanning manually.

LED
Blue LED is turned on with power supplied and flickers when waiting for fingerprint scanning.

Speaker
Outputs various sound effects, music, and voices.

Fingerprint sensor
Place a finger here to scan fingerprint.

Numeric key 0~9
Used to enter user ID or PIN.

Function key
Used to input a T&A event and initiate fingerprint scanning.

ESC key
Used to enter Admin menu from initial display or return to the previous menu from Admin menu.

CALL key
When connected to interphone, press this button to ring the interphone.

RF card reading part (RF model only)
Place RF card here to read

13

Installation example

PC

Network hub   Ethernet

6pin cable

3pin cable   Door Lock

RS232   7pin cable

Exit Button

USB   USB

14

Cable spec.

INTERCOM CABLE

PIN DESCRIPTION	PIN NUMBER	WIRE SPECIFICATION
POWER +	1	RED/24AWG/300mm
POWER −	2	BLACK/24AWG/300mm
INTERCOM AUDIO	3	ORANGE/24AWG/300mm
INTERCOM DATA	4	BLUE/24AWG/300mm
SHIELD GND	5	GRAY/24AWG/300mm

RELAY CABLE

PIN DESCRIPTION	PIN NUMBER	WIRE SPECIFICATION
RELAY NORMAL OPEN	1	WHITE/26AWG/300mm
RELAY COMMON	2	BLUE/26AWG/300mm
RELAY NORMAL CLOSE	3	ORANGE/26AWG/300mm

RS-485 CABLE

PIN DESCRIPTION	PIN NUMBER	WIRE SPECIFICATION
RS−485 TRX−	1	YELLOW/26AWG/300mm
RS−485 TRX+	2	BLUE/26AWG/300mm
RS−485 GND	3	BLACK/26AWG/300mm
SHIELD GND	4	GRAY/26AWG/300mm

RS-232 CABLE

PIN DESCRIPTION	PIN NUMBER	WIRE SPECIFICATION
RS−232 TX	1	WHITE/26AWG/300mm
RS−232 RX	2	ORANGE/26AWG/300mm
RS−232 GND	3	BLACK/26AWG/300mm
SHIELD GND	4	GRAY/26AWG/300mm

TTL IN/OUT CABLE

PIN DESCRIPTION	PIN NUMBER	WIRE SPECIFICATION
TTL IN0/WIEGAND IN0	1	BLUE/26AWG/300mm
GND	2	BLACK/26AWG/300mm
TTL IN1/WIEGAND IN1	3	YELLOW/26AWG/300mm
GND	4	BLACK/26AWG/300mm
TTL OUT0/WIEGAND OUT0	5	GREEN/26AWG/300mm
TTL OUT1/WIEGAND OUT1	6	WHITE/26AWG/300mm
GND	7	BLACK/26AWG/300mm
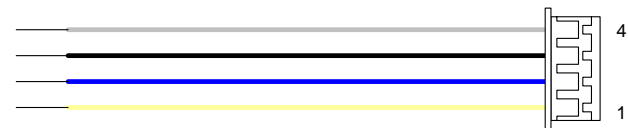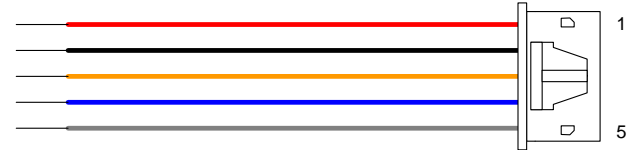
For Administrators - Basic Functions

Basic information for the device administrators. It includes key items such as basic menu usage, operation mode setting, network connection, and user management.

Enter Admin Menu

- **Press ESC key to enter Admin menu from the initial display.**

```
                                    ▼ T&A

        Admin fingerprint or
         master password

          OK        ESC
```

- **Enter master password and press OK key.**
    - [Note] As there's no master password enrolled in a device by factory default, you can enter Admin menu just by pressing OK key. For security reason, set a master password right after the product installation. Please refer to <Change master PW> to see how to set a master password.
- **Instead of entering master password, administrator can place his/her finger to enter Admin menu.**
    - [Note] "Master password" is a unique password of the device, different from the PIN (user password) of an administrator. It is necessary to enter master PW or place a finger. It is not possible to enter Admin menu by entering his/her PIN.
    - [Note] If an administrator is enrolled, entering the master password is inhibited, allowing only administrator fingers to access the admin menu.
- **If the master password is entered successfully, initial Admin menu appears on display.**

User	Log
Mode	Device
Display	Network
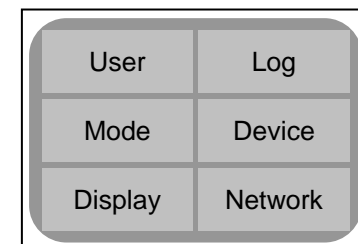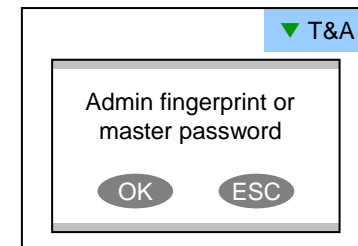
Using Admin Menu

- **Main functions of initial Admin menu are as follows. For the entire Admin menu list, refer to <List of Admin menu>.**
    - User : user management such as user enroll/delete/edit.
    - Mode : set device's operating mode.
    - Display : set device's language, background, sound volume, etc.
    - Log : check the access and attendance event records.
    - Device: set various settings for finger scan, I/O ports, door relay, etc.
    - Network : set interface such as TCP/IP, serial communications, USB.
- **To enter a desired submenu from initial Admin menu, move to the desired menu using a navigation key and press OK key.**
- **In a submenu, you can move to desired item using up/down navigation key. To change settings of each item, use left/right navigation key.**
    - If you press OK key, changed setting is applied and move to the previous menu. If you press ESC key, changed setting is not applied and move to the previous menu.
- **Press F4 key anytime in Admin menu to exit from Admin menu and move to initial display.**
    - [Note] For security reasons, the display will automatically return to the initial display after a certain time period without any key input in Admin menu. If you do not want this function or want to change the time period, refer to <Display and sound setting>.

Operation mode setting

After installation, it is necessary to select an operation mode suitable for its usage.

- **If you select Mode on initial Admin menu, following menus appear on the display.**

Mode	
1:1 Mode	◁Finger or PIN▷
1:N Mode	◄　　Auto　　►
T&A	◄　Enabled　►
T&A key	◄　　F1　　►
	◄　　In　　►
	◄　Use Relay　►
Card Mode	◄　CSN Only　►

1:1 Mode

- Setting : Finger or PIN / Finger Only / Pin Only / Card Only / Card+Finger+PIN
- After entering ID on 1:1 mode, set whether you will use fingerprint, PIN, or either for authentication. In case of card, using card only enables users to access just by placing the card.

1:N Mode

- Setting: Auto / OK/T&A Key / Disabled
- Auto : Fingerprint sensor is always on standby. So, if a finger is placed, identification starts automatically.
- OK/T&A key : After pressing OK key or T&A function key, fingerprint sensor is turned on to scan a fingerprint.
- Disabled : 1:N identification is not used. In order to enhance the security level of your system, you can use 1:1 mode in which users should enter their ID first.

T&A

- Setting : enabled/disabled
- Decide whether or not to use T&A function. In case of using T&A, user can input T&A events using basic function keys F1~F4. Also, after pressing ▼ key on initial display, user can enter extended T&A events.
- In case of using the device for access control only, you don't need to use T&A functions.

T&A key

- Shows T&A event set on each function key.
- In order to set extended T&A events for a specific application, use BioAdmin program on PC.

Operation mode setting

■ **If you select Mode on initial Admin menu, following menus appear on the display.**

Card Mode

- Setting : CSN Only / Template on card
- CSN Only : The CSN(Card Serial Number) of the Mifare card is used as unique identifier for a user. The user information is stored to the device.
- Template on card : The user information, including the fingerprint template, is stored on the smartcard, rather than the i9 device

Mode	
1:1 Mode	◁Finger or PIN▷
1:N Mode	◄ Auto ►
T&A	◄ Enabled ►
T&A key	◄ F1 ►
	◄ In ►
	◄ Use Relay ►
Card Mode	◄ CSN Only ►

20

TCP/IP

To use the device connected to PC, you need to set up the network according to your connection type.

- **If you select Network on initial Admin menu, Network Setup menus appear on the display.**

- **If you select TCP/IP on network menu, following menus appear on the display.**

Network Setup
USB Memory TCP/IP Serial USB

LAN Type
- Setting : Disable/Ethernet/Wireless LAN
- Used when connected to PC via Ethernet using RJ45 connector on the rear of the device.

Max conn
- Setting : 1/4/8/16
- Shows figures of BioAdmin that are accessible to terminal.

SSL
- Setting : Use/not use.
- It sets Use or Not Use of SSL between the BioAdmin and i9.

DHCP
- Setting : Use/not use
- Using DHCP, you can receive IP address and other necessary setting from server automatically.
- Check whether an appropriate DHCP server is available in your network environment before use.

IP Address, gateway, subnet
- Without using DHCP, IP address, gateway, and subnet need to be entered manually. Inquire necessary settings to network administrator.

TCP/IP	(F1) More
LAN Type	◁ Ethernet ▷
Port	1470
Max Conn.	◀ 1 ▶
SSL	◀ Not Use ▶
DHCP	◀ Use ▶
IP Address	
Gateway	
Subnet	

21
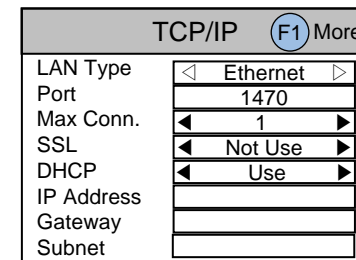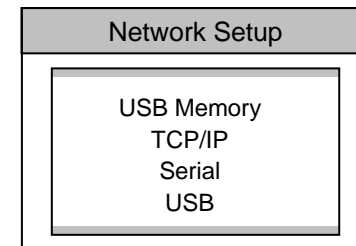
Wireless LAN

To set up the wireless LAN, select the wireless LAN AP.

■ **If you press F2 key on TCP/IP menu, following menus appear on the display.**

Wireless LAN	
Preset	◁　WPA　▷
Mode	Infrastructure
ESSID	i9_wep
Authentication	Open
Encryption	WEP64/128/256
Link Quality	0%

Preset
- Select a wireless LAN AP among the preset AP devices.
- If there is no preset wireless LAN AP, add the wireless LAN AP using BioAdmin program on PC. You can add up to 4 wireless LAN AP.

Mode
- Shows the operation mode of the wireless LAN AP.

ESSID
- Shows the ESSID of the wireless LAN AP.

Authentication
- Shows the authentication mode of wireless LAN AP.

Encryption
- Shows the encryption method of the wireless LAN AP.

Link Quality
- Shows the network condition of the currently used wireless LAN AP.

22

Server

To set up the network to the Server.

■ **If you press F3 key on Server menu, following menus appear on the display.**

Server	
Server	◁ Not Use ▷
Server IP	
Port	

Server
● Set Use or Not use of server.

Server IP
● Set Server IP

Port
● Set Server port

● Set SSL Mode as "Not Use" and Server mode to "Use"(Put server IP and Port information) if sever access is executed for the first time and another server DB rather than previously is accessed.

● After the previous process, i9 with unauthorized certificate in BioAdmin client program will be shown and issuing certificate is needed.

● After issuing certificate, system will be rebooted and accessed to server automatically.

● After rebooting, SSL mode will be automatically change to "USE",

● After issuing certificate, SSL Mode and server mode will be set to "USE" and there is no need to set up configurations of server and i9.

● To use previous version of BioAdmin or access to i9 directly using BioAdmin 4.1 without accessing to server (3.* version), SSL and server mode are set on "Not Use"

● For more information on server setup, please refer to BioAdmin manual.

Serial

To connect i9 to the serial port of PC, you need to select the buadrate of the serial communication.

■ **To connect the i9 to the serial port of host PC, designate the baudrate of the serial communication.**

Serial	
RS485	◁　115200　▷
RS232	◀　115200　▶
Controller	◀　Disable　▶
Controller ID	◀　12345678　▶

RS485
- Setting :Disable/9600/19200/38400/57600/115200
- Used when connecting to the serial port of PC using 4pin connector on the rear of the device.
- In the serial communication, the speed represents the frequency of carrier wave's changing status per sec, called baudrate.
- Default is 115200 bps.
- If you have communication error in serial communication, setting a lower baudrate may solve the problem.

RS232
- Setting : Disable/9600/19200/38400/57600/115200
- Used when connecting to the serial port of PC using 4pin connector on the rear of the device, or with i4 controller via RJ45 connector.

Controller
- Setting: Disable / Enable
- Used to connect to i4 controller. You should set 38400 bps for RS232 option above to connect to a i4 controller.

Controller ID
- Setting: i4 controller's serial number
- Enter i4 controller's serial number to get connected.

24

USB

To connect the i9 to the USB port of host PC, enable the USB communication.

■ **If you select USB on network submenu, USB setting menu appears on the display.**

USB	
USB Port	◁ Disable ▷

USB

- Setting : Enable/Disable
- Used to connect the mini USB port on the bottom of the device to the USB port of PC.
- [Note] For security reasons, USB is set as Disable by the factory default. When you connect device to PC using USB, the setting should be changed to Enable in advance.
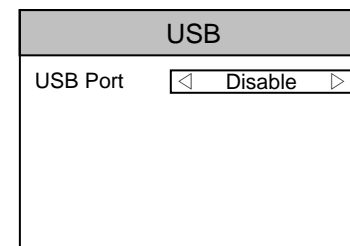
Enroll New User

How to enroll the user information and fingerprint.

■ **If you select User on initial Admin menu, User Management menus appear on the display.**

■ **If you select Enroll User on user menu, following menus appear on the display.**

User ID

- Setting: Device/Card
- Specifies the target the user is enrolled to.
- Select "Device" to store the user data to the i9's memory.
- Select "Card" to issue a smartcard with templates and user data. No data will be stored to the device.

Admin Level

- By default, the lowest available ID is displayed on the ID part of the menu. Enter your desired ID.
- User ID can be set between 1 and 4,294,967,295.

Password

- Setting : Normal/Admin
- Decide user level as normal user or administrator.
- Administrator is authorized to manage user info, ie. enroll user, delete user, and change various settings of the device.
- It is recommended to enroll at least 1 or 2 users as administrator.

Group 1 ~ Group 4

Format Card

- Enter password used in 1:1 mode. If you want to use fingerprint only, leave password as blank.

- Select access group in which the user belongs to. To edit access group, use BioAdmin program on PC.

User Management
Enroll User
Edit User
Delete All Users
Check User DB
Format Card

Enroll User	
User ID	123456
Admin Level	◄ Normal ►
Password	
Group 1	◄ None ►
Group 2	◄ None ►
Group 3	◄ None ►
Group 4	◄ None ►

Enroll New User

■ **If you enter all the necessary items for enrollment and press OK key, the following fingerprint menus appear on the display.**

Enroll Finger	
Finger No	◁　None　▶
Duress	◄　None　▶
Daily Limit	0
Time Limit	0
Card	◄　Wiegand　▶
Bypass Card	◄　Use　▶
Input Type	◄ Read Card ID ▶
Card ID	

Finger No

- Setting : 1/…/5/None
- 1-5 fingers can be enrolled for each ID.
- Enrolling more than two fingers per user can be useful in a case of injury of a finger.
- For a user whose fingerprint is weak or worn-out, enrolling the same finger twice or more can reduce failure rate.
- If you want to use PIN only instead of fingerprint, select None.

Duress

- Setting : None/Last Finger
- Duress is of vital importance in a situation when user is threatened to open a door by an intruder. If a duress finger is entered, a door opens normally but the device can send a duress signal to ring an emergency call or alarm.
- If you select Last Finger on the duress menu, the last fingerprint enrolled is assigned as a duress finger. For example, if you enroll three fingers and select Last Finger for duress, the first and second fingers are enrolled as normal fingers and the third finger as a duress finger.
- To use duress finger, more than two fingerprints should be enrolled, ie., Finger No. should be more than 2.
- Duress finger should be different from normal finger enrolled in advance.

Enroll New User

■ **If you enter all the necessary items for enrollment and press OK key, the following fingerprint menus appear on the display.**

Enroll Finger	
Finger No	◁ None ▶
Duress	◀ None ▶
Daily Limit	0
Time Limit	0
Card	◀ Wiegand ▶
Bypass Card	◀ Use ▶
Input Type	◀ Read Card ID ▶
Card ID	

Daily Limit
- It sets the limit to the number of access for a user in a day. If this is set as 0, user can access many times without limit.

Time Limit
- It sets the minimum interval between the accesses of a user. If it is set as 0, there will be no minimum interval between the accesses for that user.

Card
- Setting : Not Use/RF Card/Wiegand
- It sets Use or Not use of card and the type of card.

Bypass Card
- Setting : Use/Not Use
- It sets authentication with card only, not with any additional procedure.

Input Type
- Setting : Direct Input/Use ID/Read Card ID.
- It sets Card ID Input type.

Card ID
- In case of Manual Input, users enter card ID directly. In case of User ID, users set card ID as user ID. In case of Read Card ID, it will be read from card.

Enroll New User

- **After selecting Finger No. and Duress and pressing OK, now you should place a finger on a sensor for enrollment.**
  - For enrollment, the same finger should be placed twice according to the messages shown in the display.
  - If Finger No. is set more than 2, the device asks for the scan of the next fingerprint continously.
  - After placing a finger on a sensor, user can see the captured fingerprint image on the display. If you do not want to display fingerprint images on display, you can change settings at "Device – Fingerprint – View Image" menu.
  - If the two fingerprints are different from each other, enrollment process stops with a message "Two fingerprints do not match".
  - If duress finger is same as normal finger enrolled beforehand, enrollment process also stops with a message "Duress not allowed for the same finger".

- **Please place a finger correctly referring to <How to place a finger>.**

- **If all the fingerprints are entered correctly, Enroll Success message appears on the display together with a user ID and the fingerprint enrollment process is completed.**

- **After enrolling fingerprints of one user, the display shows the next user ID to enroll the next user. If you do not want to enroll more users, press F4 to exit to initial display.**

Enroll Finger
Finger 1
Place the First Finger

Enroll Finger
Enroll Success
123456

29
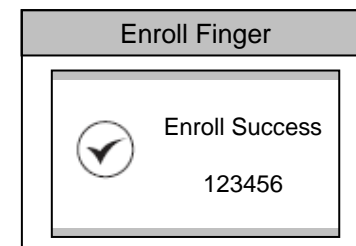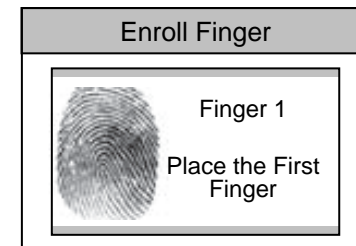
Check User Info

Check user info of currently enrolled users.

- **If you select Edit User on User Management menu, user info of each users are displayed.**

- **You can change user ID using a left/right navigation key.**

- **If you enter user ID with the numeric key, you can directly move to the user info the entered user ID.**
  - If there is no user with the selected ID, "None" message is indicated on the Name field of the display. In that case, if you press left/right navigation key, you can go to the closest valid user ID.

- **Additional info such as user name, department and company name can be entered using BioAdmin software on PC.**

- **If you press F1 key, active function keys at this menu are displayed, OK, F2 and F3.**

Edit User	(F1) More
User ID	◄ 123456 ►
Name	
Dept.	
Admin Level	Admin
Password	Registered
No of Finger	2
Group 1	None

Edit User	(F1) More
User ID	
Name	(OK) Edit User
Dept.	
Admin Level	(F2) Finger
Password	(F3) Delete
No of Finger	
Group 1	None

Edit User Info

User info can be changed and fingerprints can be re-enrolled.

- **If you press OK key at Edit User menu, the selected user info is displayed and can be edited in the same way as in the Enroll User process. You can change admin level, password and groups.**

Edit User : 123456		
Admin Level	◁ Normal	▷
Password	*******	
Group 1	◀ None	▶
Group 2	◀ None	▶
Group 3	◀ None	▶
Group 4	◀ None	▶

- **If you want to re-enroll fingerprints of the user, press F2 key at Edit User menu.**
- **You can select the number of fingerprints and duress and then re-enroll fingerprints.**

Enroll Finger	
Finger No	2
Duress	◀ Last Finger ▶

31

Delete User

Delete user from device while checking currently enrolled user info.

■ **If you want to delete the user, press F3 key at Edit User menu.**

■ **Press OK key to confirm the deletion of the user.**
- [Note] Deleted user info can't be retrieved unless the info remains in BioAdmin software on PC.

Edit User (F1) More

Do you want to delete this user?

OK   ESC

32
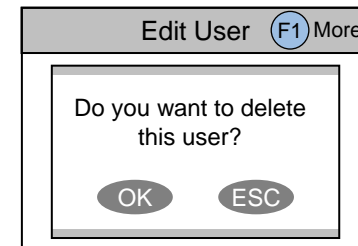
Delete All Users

Delete all user currently enrolled in device.

■ **Back to User Management menu, select Delete All User to delete all users in the device.**

User Management
Do you want to delete all users?
OK   ESC

■ **Press OK key to confirm the deletion of all users.**
- [Note] Once all users are deleted, deleted user info cannot be retrieved unless the info remains in BioAdmin software on PC.
- [Note] The data of administrators who is operating the menu is also deleted by this operation. Therefore, in order to enter Admin menu again, you should remember the master password before deleting all users.
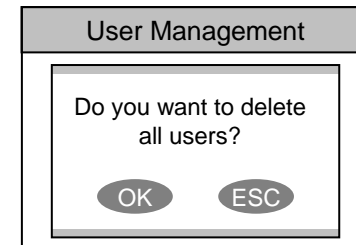
Check User DB

Check and correct errors in the user information stored on device.

■ **If you press Check User DB on User menu, following menus appear on the display.**

User Management
Do you want to check user DB errors?
OK   ESC

■ **Press OK key to check the user DB.**
- If there is an error on the user DB, it will be automatically corrected by this procedure. If it fails to correct, an error message appear on display.
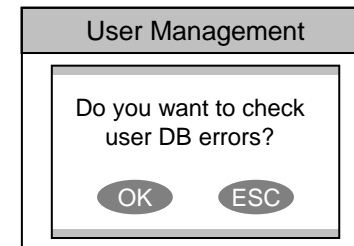
Format Card

How to enroll the user information and fingerprint.

- **Select Format Card on user menu, to delete user information on a smartcard.**

- **Place a template card to delete user information**
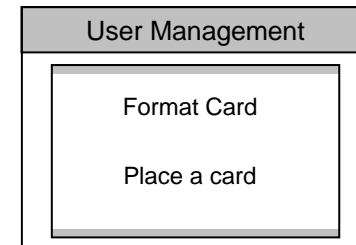
User Management
Format Card
Place a card

35

Enroll to Card

How to enroll the user information and fingerprint.

■ **If you select User on initial Admin menu, User Management menus appear on the display.**

■ **If you select Enroll to Card on user menu, following menus appear on the display.**

User ID
- Enter your desired ID.
- User ID can be set between 1 and 4,294,967,295.

Finger No
- Setting : 1/2/None
- 1-2 fingers can be enrolled for a card.
- For a user whose fingerprint is weak or worn-out, enrolling the same finger twice can reduce failure rate.
- If you want to use PIN only instead of fingerprint, select None

Duress
- Setting : None/Last Finger
- Duress is of vital importance in a situation when user is threatened to open a door by an intruder. If a duress finger is entered, a door opens normally but the device can send a duress signal to ring an emergency call or alarm.
- If you select Last Finger on the duress menu, the last fingerprint enrolled is assigned as a duress finger. For example, if you enroll three fingers and select Last Finger for duress, the first and second fingers are enrolled as normal fingers and the third finger as a duress finger.
- To use duress finger, more than two fingerprints should be enrolled, ie., Finger No. should be more than 2.
- Duress finger should be different from normal finger enrolled in advance.

User Management
Enroll User
Edit User
Delete All Users
Check User DB
Format Card
Enroll To Card

Enroll to Card	
User ID	123456
Finger No	◄ None ►
Duress	◄ None ►
Bypass Card	◄ Not use ►
Password	
Group 1	◄ None ►
Group 2	◄ None ►
Group 3	◄ None ►
Group 4	◄ None ►

36

Enroll to Card

How to enroll the user information and fingerprint.

■ **If you select User on initial Admin menu, User Management menus appear on the display.**

Bypass Card
- Setting : Use/Not Use
- It sets authentication with card only, not with any additional procedure.

Password
- Enter password used in 1:1 mode. If you want to use fingerprint only, leave password as blank.

Group 1 ~ Group 4
- Select access group in which the user belongs to. To edit access group, use BioAdmin program on PC.

User Management
Enroll User
Edit User
Delete All Users
Check User DB
Format Card
Enroll To Card

Enroll to Card	
User ID	123456
Finger No	◄ None ►
Duress	◄ None ►
Bypass Card	◄ Not use ►
Password	
Group 1	◄ None ►
Group 2	◄ None ►
Group 3	◄ None ►
Group 4	◄ None ►

For Administrators - Advanced Functions

Detailed information for device administrators. It includes specific items such as display and sound setting, fingerprint authentication setting, and log check.

Display & Sound Setting

Change device's display and sound settings.

■ **If you select Display on initial Amin menu, following menus will appear on the display.**

		Display (F1) Time
		Language ◁ English ▷
		Background ◀ Logo ▶
		Sub Info ◀ Time ▶
		Timeout ◀ Infinite ▶
		Msg Time ◀ 2 sec ▶
		Volume ▬ 20%

Language
- Setting :Korean/English/Custom
- Select a language to be used
- To use custom language, appropriate language config. file needs to be downloaded to the device using BioAdmin program on PC. Please contact Suprema for details.

Background
- Setting : Logo/Slide Show/Notice
- Decide background of initial display. In case of Logo, one photo assigned as logo is displayed all the time. In case of Slide Show, multiple photos are displayed at the interval of 5 seconds in turn. In case of Notice, one photo is displayed as a background and a notice is scrolled down over the background.
- In order to change background images, use BioAdmin program on PC.

Sub Info
- Setting : Time/None
- Sub Info is a display area in the bottom side of the display. Current date and time will be shown with a selection of Time. Or the area can be left blank with the selection of None.

Timeout
- Setting : Infinite/10 sec/20 sec/30 sec
- If there's no key input during this time out period on Admin menu, the device automatically returns to initial display for security reason.

Msg Time
- Setting : 0.5sec/1sec/2sec/3sec/4sec/5sec
- It sets message time in display upon the fingerprint matching.

Volume
- Setting : 0%/10%/20%/…/100%
- Set output volume of the device sounds. 100% is the maximum. At setting 0%, sound is turned off.

Display & Sound Setting

Change device's display and sound settings.

■ **If you select Display on initial Amin menu, following menus will appear on the display.**

Time

- ● Date : YYYYMMDD
- ● Tim : hhmmss
- ● Time synchronization : Terminal time will be synchronized with server time.
- ● Date format : MM/DD or DD/MM

Display	(F1) Time
Language	◁ English ▷
Background	◀ Logo ▶
Sub Info	◀ Time ▶
Timeout	◀ Infinite ▶
Msg Time	◀ 2 sec ▶
Volume	20%

40

Fingerprint Setting

Change various settings for fingerprint authentication.

- ■ **If you select Device on initial Admin menu, Device Setup menus appear on the display.**

Device Setup
Fingerprint
I/O
Door Relay
Master Password
Device Info
Device Reset
Factory Default

- ■ **If you select Fingerprint, following menus appear on the display.**
- ■ **In this manual, the default setting is in bold font.**

Fingerprint		
Security	◄	Normal	►
Fast Mode	◄	Normal	►
Quality	◄	Normal	►
View Image	◄	Visible	►
Sensitivity	◄	7 (Max)	►
Timeout(Sec)	◄	10	►
Encryption		Not Use	

Security

- ● Setting : **Normal**/Secure/Most Secure
- ● Security level is determined by FAR (False Acceptance Ratio). FAR refers to the percentage of acceptance by unregistered fingerprints. Therefore, the lower the percentage is, the higher the security level is. However, as the FAR and FRR (False Reject Rate) are in reverse proportion to each other, the higher security level will indue bigger FRR, ie., more failure for registered fingers.
- ● For general T&A applications, normal level is recommended. However, in case of an access control application requiring a higher security level, it is recommended to apply the security level as secure or most secure.

41

Fingerprint Setting

Fast Mode
- Setting : **Normal**/Fast/Fastest
- Using 1:N mode with more than hundreds of users, identification may take somewhat longer. In this case, you can change the fast mode to Fast or Fastest. By doing so, identification speed becomes faster in sacrifice of a little higher FRR.

Quality
- Setting: Weak/**Normal**/Strict
- Quality level decides the strictness of quality check of the input images. With a strict quality level, the device may reject a low quality input fingerprint more.

View Image
- Setting : **Visible**/Invisible
- Proper enrollment can be induced by showing the image of the entered fingerprint on LCD screen upon enrollment.

Sensitivity
- Setting : 0(min)/1/2/3/4/5/6/**7(max)**
- Set sensitivity of fingerprint sensor in a capture of a fingerprint. At a high sensitivity level, it is easier and faster to capture a fingerprint. On the other hand, at a low sensitivity level, the image quality of the captured fingerprint can be more stable.
- In normal applications, maximum level is recommended. If the recognition is not satisfactory for wet fingerprints, reducing sensitivity may solve the problem.

Timeout(Sec)
- Setting : 1/2/…/**10**/…/19/20
- Set standby time for fingerprint enrollment. If a user does not place a finger within the time, a timeout message appears on the display.

1:N Delay
- Setting : 0/1/**2**/…./10
- It means the time of delay from 1:N authentication to next stand-by authentication

Encryption
- Setting : Not Use / Use
- Shows whether the i9 is currently using the template encryption or not. Encryption can not be set on the device itself, but should be set using BioAdmin program on PC.

I/O Setting

Change various settings for I/O.

■ **If you select I/O on device menu, following menus appear on display.**

I/O	
Input 0	◁ Disabled ▷
Input 1	◀ Disabled ▶
Output 0	◀ Disabled ▶
Output 1	◀ Disabled ▶
Duration(ms)	1000
Tamper SW	◀ None ▶

Input 0 & Input 1

- Setting : Disabled/Exit/Wiegand
- In case of using the input port for RTE(exit button), select Exit.
- In case of using input as Wiegand, input 0 and input 1 are set as Wiegand.

Output 0 & Output 1

- Setting: Disabled/Duress/Tamper SW/Auth Success/Auth Fail/Wiegand
- Can send outputs for various events.
- In case of using output as Wiegand, output 0 and output 1 are set as Wiegand.

Duration(ms)

- Set the cycle of output signal. Default is 1sec (1000ms).

Tamper S/W

- Setting : None/Lock System
- Tamper switch is turned on when a housing(case) of i9 is opened.
- If the setting is in "Lock System", the device is automatically locked when a tamper switch is on.
- This can be useful in security when an intruder opens the housing of i9 to enter a building.
- [Note] Once i9 is locked, lock can be released only when the master password is entered. It cannot be released by administrator's fingerprint.

Door Relay Setting

Change various settings for door relay.

■ **If you select Door Relay on device menu, following menus appear on the display.**

Door Relay	
Driven by	◁ All Event ▷
Duration(sec)	3
Lock Time	◄ None ►
Unlock Time	◄ None ►
Interphone	◄ Disable ►

Driven by
- Setting: All events / Authentication +T&A event/T&A event/Verification/Disabled
- In case of All events, door opens for all authentication success(1:1 PIN auth.,1:1 fingerprint auth.,1:1 fingerprint verification)
- In case of authentication with T&A event, door opens only by the specific events for which door use is allowed and also door opens only by authentication.
- In case of selected T&A, door opens only by the specific events for which door use is allowed.
- In case of authentication, door opens only by authentication without T&A event
- In case of disabled, i9 will not drive an internal relay to open a door by any of events or authentication.

Duration (sec)
- Once a door is open, the door can be locked again after this duration.

Lock time
- Decide time to lock(close) the door by force.
- During lock time, general users cannot open door while only administrators are allowed.
- The lock time can be set by BioAdmin program on PC.

Unlock time
- Decide time to open the door by force
- The unlock time can be set by BioAdmin program on PC.

Interphone
- Setting : Disable / Enable
- To connect and use an optional interphone with i9, enable interphone on this menu. CALL button and interphone communication of i9 will operate only when this menu is set as Enable.

44

Change Master Password

Change master PW.

■ **If you select Master Password on device menu, Master Password menus appear on the display.**

Master Password
Current
New
New(Again)

■ **Enter current master password to "Current" and a new master password to "New" & "New (again)". Then press OK key to confirm.**

- Default password is blank (no need to type).
- [Note] With this master password, one can enroll or delete users and change settings of i9. Please be careful not to disclose master password except Administrators.

■ **When you forget master password**

- If there is a user enrolled as administrator : you can enter Admin menu using administrator's fingerprint and return the password as blank by selecting the Factory Default on Device menu. However, in this case, other settings of the device also return to defaults.
- If there's no user enrolled as administrator : contact the dealer you purchased the device.

View Device Info

View device's basic info such as model name and version.

■ **If you select Device Info on device menu, following menus appear on the display.**

Device Info	
Model	Standard
Device ID	1301
MAC	00:17:fc:10:05:15
HW Version	Rev. E
FW Version	V1.0
Kernel Ver.	
Memory	7/19 MB

Model
- Model name is displayed according to types of fingerprint sensor.
- Optical sensor : BST-OC
- Capacitive sensor : BST-TC
- Thermal swipe sensor : BST-FC

Device ID
- Device ID number is displayed.

MAC
- Device's Ethernet MAC address is displayed.

HW Version
- Device's hardware version is displayed.

FW Version
- Device's firmware version is displayed.
- Firmware and kernel can be upgraded using BioAdmin program when new firmware is released.

Kernel Ver.
- Device's Kernel ver. Info is displayed.

Memory
- Overall available storage and currently used storage are displayed.
- In the internal memory of i9, various information like user info, log, background and sounds are stored, so used memory changes by the size of these information.

Device Reset

Reset system.

- **If you select Device Reset on device menu, a message to restart i9 appears on the display.**

- **Press OK key to reset device. Device reset takes normally 20-30 seconds and it may take a bit longer for network connection.**

- **If you change language of i9, you should reset i9 to apply the new language.**

- **If device becomes unstable for any reason, in most of cases, device reset can solve the problem.**

Device Setup
Do you want to restart i9?
OK   ESC

47
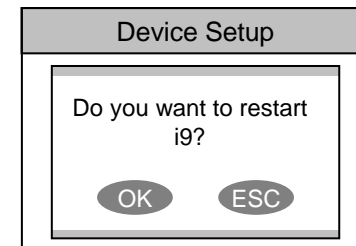
Factory Default

Restore device's all settings to factory defaults.

■ **If you select Factory Default on device menu, a message to reset to default appears on the display.**

```
Device Setup

Do you want to reset
    to default?

  OK      ESC
```

■ **Press OK key to change system's various settings as factory defaults.**

● [Note] Be sure that various settings, background, sounds and notice will be deleted.

■ **User info and log data are not deleted. To delete user info, refer to <Delete All Users>. To delete log data, refer to <Delete Entire Log>.**

48
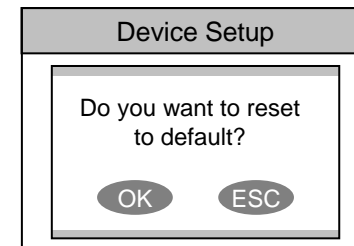
Check Log

Check logs for various events accumulated in device.

■ **If you select Log on initial Admin menu, log events appear on the display. You can check logs from the latest one.**

Log List (F1) More
9/14 13:39 Duress (Menu) 123456
9/14 13:30 Identify OK (Menu) 1111
9/14 13:25 Duress (Menu) 123456
9/14 12:51 Identify OK (Menu) 1111
9/14 12:45 Duress (Menu) 123456
9/14 12:43 Identify OK (Menu) 1111
9/14 12:39 Duress (Menu) 123456
9/14 12:26 Identify OK (Menu) 1111

■ **Press up/down navigation key to scroll a log one by one.**

■ **Press left/right navigation key to scroll a log by page (8 logs).**

■ **Press F1 key to display available additional function key.**
- OK : Latest
- F2 : Filter
- F3 : Delete

■ **Press OK key to display the latest log.**

Filter Log

Check specific log events by filtering the log events stored on device.

■ **If you press F2 key on Log menu, following menus appear on the display.**

	Filter
Filter ID	◁ 1 ▷
Time	◀ All ▶
Event	◀ All ▶
T&A Event	◀ All ▶
User	0

Filter ID
- Select the filter ID.
- Device can store up to 4 filters.

Time
- Setting : All/Today/Yesterday/Last 3 days/Last 1 week/Last 1 month
- Designate the time to filter.

Event
- Setting : All/Success/Fail/IO/Duress/Tamper/System
- Select the events to be shown on the log list.

T&A Event
- Select the T&A events to be shown on the log list.

User
- To check the log events of a specific user, enter the user's ID. If you press 0, log events of all users are displayed.

Delete Entire Log

Delete entire event logs accumulated in device.

■ **If you press F3 on log list screen, a message to delete all logs appears on the display.**

Log List (F1) More

Do you want to delete
all logs?

OK   ESC

■ **Press OK key to delete all logs.**
- [Note] Be sure that a deleted log can not be retrieved unless it remains in BioAdmin program on PC.
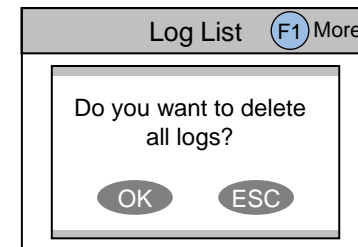
USB Memory

How to use USB memory to transfer user information, log data, and various settings of device.

- ■ **If you select USB Memory on Network menu, following menus appear on the display.**

- ■ **When you are using wireless LAN, the wireless LAN is automatically disconnected in this menu. When you go out of this menu, wireless LAN is reconnected.**

USB Memory
Synchronize
Export Virtual Terminal
Import Virtual Terminal
Firmware Upgrade
Initialize
Refresh

Synchronize

- Transfer the user information and various settings from the virtual terminal of USB memory to the connected i9. At the same time, transfer the log data from the connected i9 to the virtual terminal of USB memory.
- [Note] Synchronize menu erases the current user information and various settings of the device and overwrite with the information and settings on USB memory.
- Useful in transferring the data from BioAdmin program to device.
- Enabled only when the USB memory has a virtual terminal with the same device ID as that of the connected i9.

Export Virtual Terminal

- Create a virtual terminal on USB memory with the same device ID. Export the user information, log data, and various settings of the connected device to the virtual terminal on USB memory.
- It may take a few minutes depending on the size of the user information and log data to export.
- To synchronize or import virtual terminal, you need to create a virtual terminal first on the USB memory by using Export Virtual Terminal menu.
- This menu is enabled only when a USB memory is connected to i9.

52

USB Memory

How to use USB memory to transfer user information, log data, and various settings of device.

Import Virtual Terminal

- Apply the user information and various settings in USB memory to the connected device.
- Import starts by selecting the an ID of the virtual terminals on USB memory.
- [Note] This menu erases the current user information and various settings of the device and overwrite with the information and settings on USB memory.
- Used to transfer the user information and various settings from one device to another.
- Useful in periodical back up and restoration of device information.
- This menu is enabled only when the connected USB memory has a virtual terminal.

Firmware Upgrade

- Upgrade the firmware of the connected device with the firmware file stored on USB memory.
- Firmware upgrade starts by selecting one of the firmware files stored on the root directory of USB memory.
- Upon finishing the firmware upgrade, device automatically restarts.
- This menu is enabled only when a firmware file exists in the root directory of USB memory.

Initialize

- Delete all virtual terminals on USB memory.
- This menu is enabled only when a USB memory is connected to i9.

Refresh

- Refresh the connection of the USB memory and the stored information on the connected USB memory.

| USB Memory |
| --- |
| Synchronize |
| Export Virtual Terminal |
| Import Virtual Terminal |
| Firmware Upgrade |
| Initialize |
| Refresh |

53

For General Users

Describes directions for general users. It explains how to open a door in each operation mode and to enter T&A events.

Access using 1:N mode

How to open a door using fingerprint when 1:N mode is set as Auto or OK/T&A key.
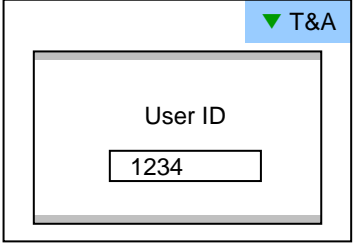
- **When 1:N mode is set as Auto**
  - If you enter a fingerprint without pressing any key, a message showing the identification result appears and door is opened.

- **When 1:N mode is set as OK/T&A key**
  - If you press OK or T/A key, blue LED flickers and a message requesting user's fingerprint appears on the display.
  - Place a finger to open the door.

- **Use of personal info**
  - When personal info image and message are set, the set image and message by successful authentication will be shown.
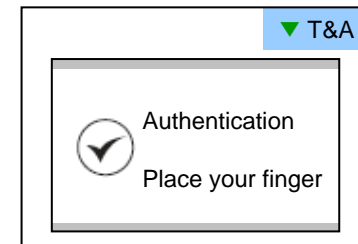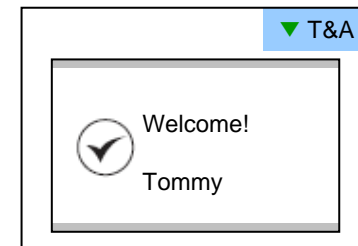
▼ T&A

Welcome!

Tommy

▼ T&A

Authentication

Place your finger

Access using 1:1 mode

How to open a door by entering ID first and then entering fingerprint or password.

- **If you press a numeric key, ID input window appears.**

- **Enter your ID and press OK key.**

- **In case 1:1 mode is set as Fingerprint Only**
  - Enter a fingerprint to open the door.

- **In case 1:1 mode is PIN Only**
  - Enter your password and press OK key to open the door.

- **In case 1:1 mode is set as Fingerprint or PIN**
  - You can either enter a fingerprint or enter password and press OK key.

- **In case 1:1 mode is set as RF Card**
  - If the 1:1 mode is set as Card Only, user can access just by placing the card to i9 without any additional procedure.
  - If the 1:1 mode is not set as Card Only, card is used to suggest the user's ID. After putting the card, user should verify himself with fingerprint or password.

▼ T&A

User ID

1234

56

Access using 1:1 mode

How to open a door by entering ID first and then entering fingerprint or password.

1:1 verification	How to suggest user ID	How to authorize
Fingerprint or password	Enter user ID or put the card	Put finger or enter password
Fingerprint Only	Enter user ID or put the card	Put finger
Password Only	Enter user ID or put the card	Enter password
Card Only	Put the Card	

▼ T&A

User ID

1234

57

T&A event using 1:N mode

How to enter T&A events with fingerprint when 1:N mode is set as Auto or OK/T&A key, and T&A is set as Enabled.

- **If you press F1~F4 key, blue LED flickers and a message requesting user's fingerprint appears on the display.**

▼ T&A

T&A: In

Place your finger

- **If you place a finger, designated T/A event appears on the display and applies to the user.**

▼ T&A

In: Tommy

8/1(Tue) AM 8:00

- **In case that 'Driven by' on the door relay menu is set as 'Selected T&A' and that 'Activate Relay by this Event' is checked on the BioAdmin program, a door opens upon the occurrence of the T&A events.**

- **You can check on 'Activate Relay by this Event' in T&A event with BioAdmin program on your PC.**
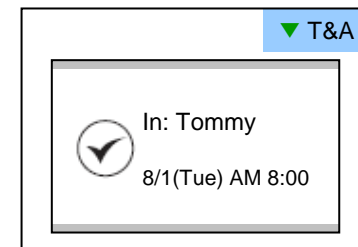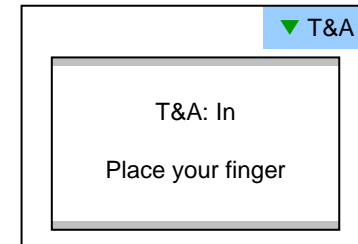
T&A event using 1:1 mode

How to enter T&A event by first entering ID and then entering fingerprint or password when T&A is set as enabled.

■ **If you press a numeric key, ID input window appears on the display.**

```
                                    ▼ T&A

                            User ID

                            1234
```

■ **Enter your ID and press F1~F4.**

■ **In case 1:1 mode is set as Fingerprint Only**
- Enter fingerprint to apply applicable T&A event.

■ **In case 1:1 mode is set as PIN Only**
- Enter your PW and press OK key to apply applicable T&A event.

■ **In case 1:1 mode is set as Fingerprint or PIN**
- You can either enter fingerprint or enter password and press OK key.

59
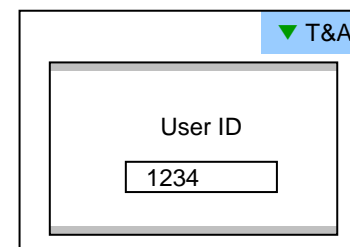
Using extended T&A events

*In case of using 4 or more T&A events, you can use extended T&A events.*

- **If you press down navigation key, extended T&A events info appears on the display.**

1	2	3	F1 In
4	5	6	F2 Out
7	8	9	F3 In duty
CALL	0	ESC	F4 Out duty

- **If you press one of 16keys corresponding to the desired T&A event, next operation starts for the extended T&A event.**
- **Factory default T&A events are defined as below.**
  - F1 (In), F2 (Out), F3 (In duty), F4 (Out duty)
- **You can edit the default T&A events and extended T&A events with BioAdmin program on your PC.**
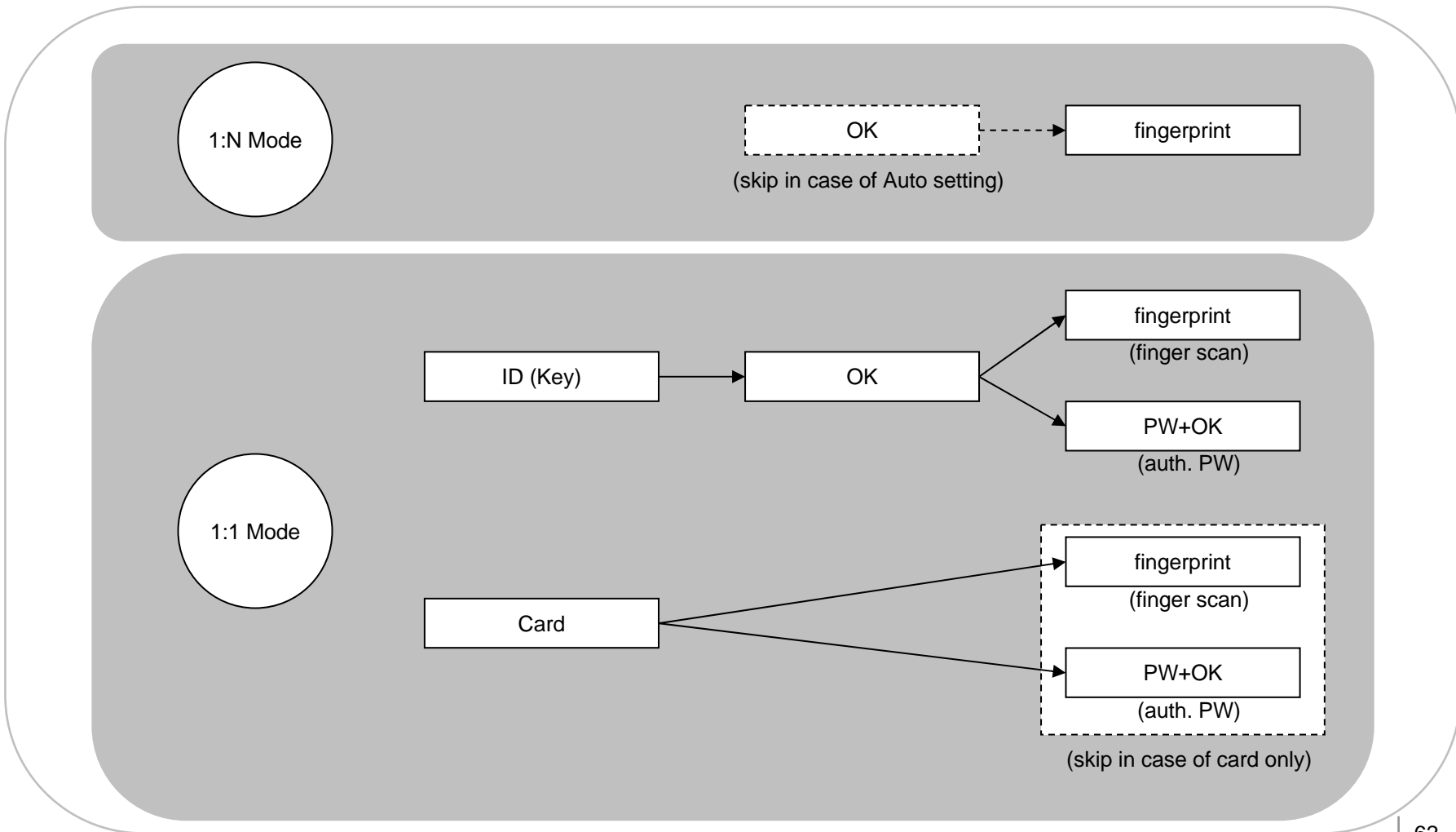
60

View user's Access/T&A event records

General users can check their own access and T&A event records.

- **If you press ESC key on initial screen, a message requesting user fingerprint or password appears on the display.**

- **If user enter his/her fingerprint or password, access and T&A event records displays as below.**

- **Press up/down navigation key to scroll a log one by one.**
- **Press left/right navigation key to scroll a log page by page (8 logs).**
- **Press OK key to display the latest log.**

▼ T&A

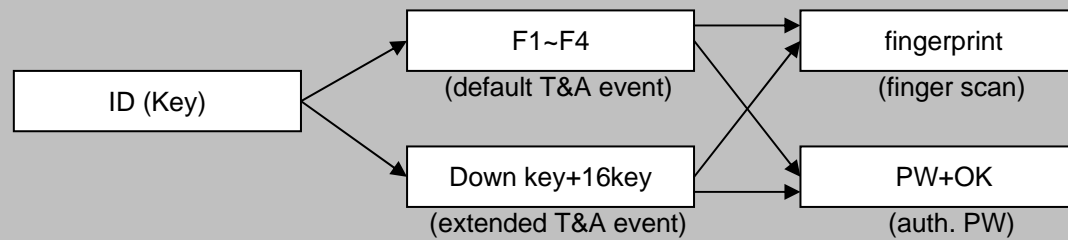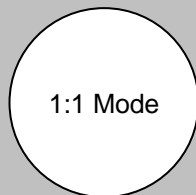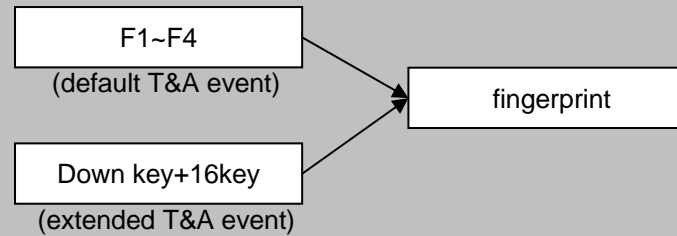Admin fingerprint or
master password

OK   ESC
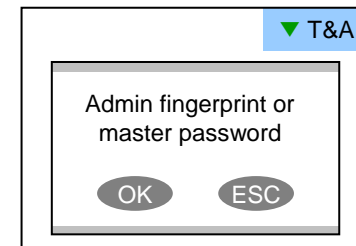
User Log: 123456

9/14 13:39 Duress (Menu) 123456
9/14 13:30 Identify OK (Menu) 1111
9/14 13:25 Duress (Menu) 123456
9/14 12:51 Identify OK (Menu) 1111
9/14 12:45 Duress (Menu) 123456
9/14 12:43 Identify OK (Menu) 1111
9/14 12:39 Duress (Menu) 123456
9/14 12:26 Identify OK (Menu) 1111

61

Authentication procedure as per operation mode

1:N Mode

OK → fingerprint

(skip in case of Auto setting)

1:1 Mode

ID (Key) → OK →
- fingerprint (finger scan)
- PW+OK (auth. PW)

Card →
- fingerprint (finger scan)
- PW+OK (auth. PW)

(skip in case of card only)

1:N Mode

F1~F4
(default T&A event)

Down key+16key
(extended T&A event)

fingerprint

1:1 Mode

ID (Key)

F1~F4
(default T&A event)

Down key+16key
(extended T&A event)

fingerprint
(finger scan)

PW+OK
(auth. PW)

63
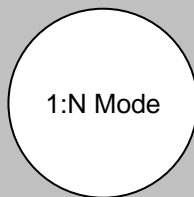
List of Admin Menu

User
- Enroll User
  - User ID
  - Admin Level
  - Password
  - Group 1
  - Group 2
  - Group 3
  - Group 4

  - Finger No
  - duress

- Edit User
  - OK: Edit User
  - F2: Finger
  - F3: Delete

- Delete All users
- Check User DB

Mode
- 1:1 Mode
- 1:N Mode
- T&A
- T&A key

Display
- Language
- Background
- Sub Info
- Timeout
- Date
- Time
- Volume

Log
- OK: Latest
- F2: Filter Log
  - Filter ID
  - Time
  - Event
  - T&A Event
  - User
- F3: Delete

Device
- Fingerprint
  - Security
  - Fast Mode
  - Quality
  - View Image
  - Sensitivity
  - Timeout
  - Encryption
- I/O
  - Input 0, Input 1
  - Output 0, Output 1
  - Duration(ms)
  - Tamper SW
- Door Relay
  - Driven by
  - Duration(sec)
  - Lock Time
  - Unlock Time
  - Interphone
- Master
- Password
- Device info
- Device Reset
- Factory default

Network
- USB Memory
  - Synchronize
  - Export Virtual Terminal
  - Import Virtual Terminal
  - Firmware Upgrade
  - Initialize
  - Refresh
- TCP/IP
  - LAN Type
  - Port
  - Server IP
  - DHCP
  - IP Address
  - gateway
  - Subnet
- Serial
  - RS485
  - RS232
- USB
  - USB

64

Specifications

- **CPU : Dual CPU (32 bit RISC + 400MHz DSP)**
- **Memory : 72MB flash + 34MB RAM**
- **Display : 2.5 inch QVGA 16 million color LCD**
- **Identification speed : 3,000 fingerprints in 1 second**
- **Fingerprint capacity : 40,000 fingerprint templates**
- **Log capacity : 200,000 events**
- **Host interface : Wireless LAN, TCP/IP, RS485**
- **PC interface : USB, RS232**
- **USB memory slot : USB host**
- **1 relay for deadbolt, EM lock, door strike, or automatic door**
- **Wiegand input/output, 4 TTL input/output**
- **Built-in microphone and speaker supporting door phone**
- **Convenient menu navigation key**
- **4 function keys for user defined functions**
- **Operation mode : Fingerprint, PIN, PIN+Fingerprint,**
- **Card only*, Card+Fingerprint*, Card+PIN* (*RF model only)**
- **RF Card : 13.56MHz Mifare**
- **RTC with backup battery (CR2032)****
- **Product size : 135 x 128 x 50 mm (width x length x depth)**

** **CAUTION** : RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERY ACCORDING TO THE INSTRUCTIONS

Troubleshooting

- **Fingerprint can not be read well or it takes too long.**
  - Check whether a finger or fingerprint sensor is stained with sweat, water, or dust
  - Retry after wiping off finger and fingerprint sensor with dry towel.
  - If a fingerprint is way too dry, blow on the finger and retry.
- **Fingerprint is entered but authorization keeps failing.**
  - Check whether the user is restricted by door zone or time zone.
  - Inquire of administrator whether the enrolled fingerprint has been deleted frin the device for some reason.
  - If message 'not enrolled ID' appears after ID is entered and OK is pressed, it means that the fingerprint has not been enrolled.
- **Authorized but door is not opened.**
  - Check whether the time is set as lock time.
  - Check 'driven by' on Admin menu.
  - In case it is set as disabled or selected T/A events, door may not open.
- **Partial key can't be entered or device is unstable.**
  - In case device is unstable for any reason, enter Admin menu and reset device.
- **All keys are not entered**
  - If LCD display and blue LED are off, it is possible that power is off. Check power condition such as blackout.
  - If LCD display and blue LED are on, something is wrong with machine. In such a case, contact A/S center.

Device cleaning

- **Wipe out machine surface with dry towel or cloth.**
- **In case there is dust or impurities on the sensor of the i9, wipe off the surface with dry towel.**
- **Note that if the sensor is cleaned by detergent, benzene or thinner, surface is damaged and fingerprint can't be entered.**
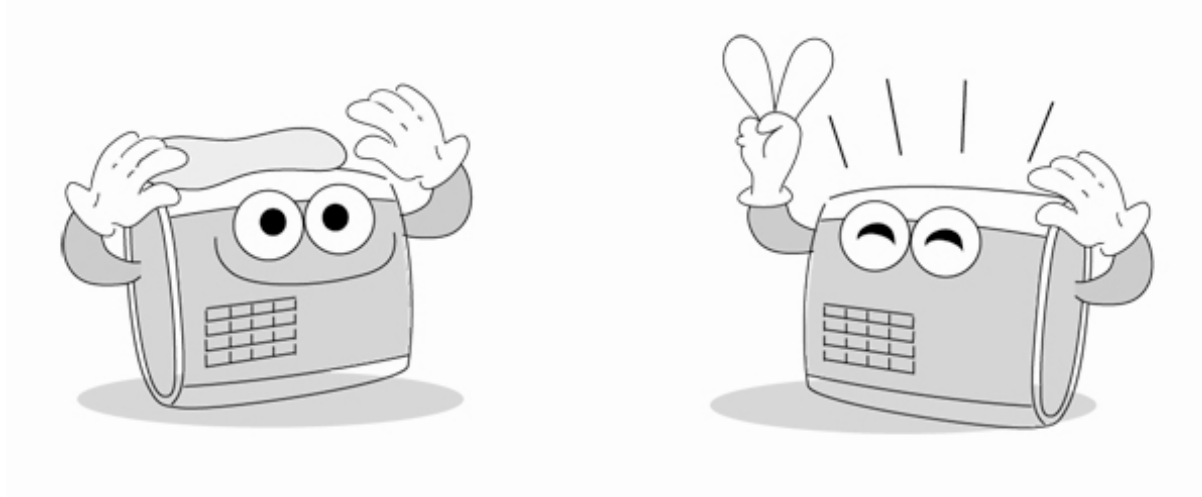
RCG

RCG Corporation Limited

Website ： www.rcg.tv

E-mail ： support@rcg.tv

Fax : 852-3669 6888

Functions and specifications of the product are subject to changes without notice due to quality enhancement or function update.