www.supremainc.com



biostation

Innovative Fingerprint Terminal

User Guide
EN 102.00.BST V1.96

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 400,000 fingerprints and 1,000,000 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. (Optional)
- **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 & FVC2006) 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.
- **RF Card Support!**
  - RF module is built in a Terminal itself. Fingerprint, card, and password can be selected as the authentication method for each user.
- **Real Time Network operation through Server!**
  - Connected to the BioAdmin Server, terminals can be managed in real time.

©Copyright 2008 Suprema Inc.

Contents

Before start

- Safety precautions 5
- Glossary 7
- Basics of fingerprint recognition 8
- How to place a finger 9
- Product Contents 11
- Name of each part 13
- Installation 15
- Cable spec. 16

For administrators (Basic functions)

- Enter Admin menu 18
- Using Admin menu 19
- Operation mode setting 20
- Network setup
  - TCP/IP 24
  - Wireless LAN 25
  - Server 26
  - Serial 27
  - USB 28
- User management
  - Enroll New User 29
  - Check User Info 35
  - Edit User Info 36
  - Delete User 37
  - Delete All Users 38
  - Check User DB 39
  - Format Card 40

©Copyright 2008 Suprema Inc.

Contents

For Administrators (Advanced functions)

- Display & sound setting 42
- Device setup
  - Fingerprint Setting 44
  - I/O Setting 47
  - Door Relay Setting 49
  - Zone 52
  - Sub Zone 53
  - APB Zone 54
  - Change Master Password 55
  - View Device Info 56
  - Device Reset 57
  - Factory Default 58
- Log
  - Check log 59
  - Filter log 60
  - Delete entire log 61
- USB memory 62

For General Users

- Open door
  - Access using 1:N mode 65
  - Access using 1:1 mode 66
- Using T&A event
  - T&A event using 1:N mode 68
  - T&A event using 1:1 mode 69
  - Using extended T&A events 70
- View user's Access/T&A event records 71
- Authentication procedure as per operation mode 72
- Authentication procedure for T&A event 73

Appendix

- Specifications 74
- Troubleshooting 75
- Device cleaning 76

©Copyright 2008 Suprema Inc.

Safety precautions

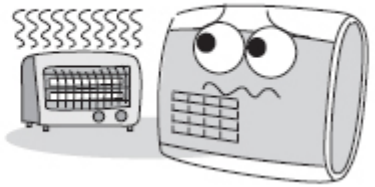
- **The list below is to keep user's safety and prevent any loss. Please read carefully before use.**



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



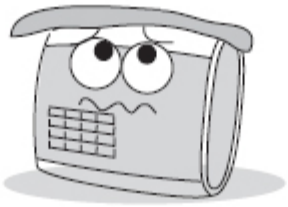
Do not place a magnet near the product. Magnetic objects such a s magnet, CRT, TV, monitor or speaker may damage the device .



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.

©Copyright 2008 Suprema Inc.

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.



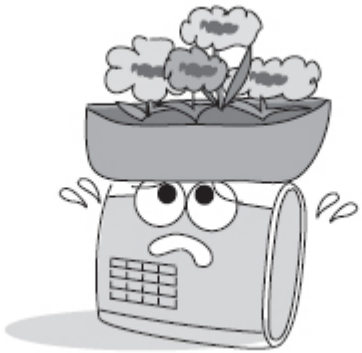
Do not press two buttons at the same time.



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.

©Copyright 2008 Suprema Inc.

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.
- **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.

©Copyright 2008 Suprema Inc.

Basics of fingerprint recognition

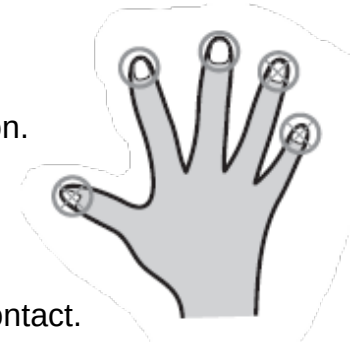
- **What is fingerprint recognition?**
  - Fingerprint is an individual's own biometric information and does not change throughout his/her life. Fingerprint recognition is a technology that verifies or identifies an individual using such fingerprint information.
  - Free from the risk of theft or loss,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

©Copyright 2008 Suprema Inc.

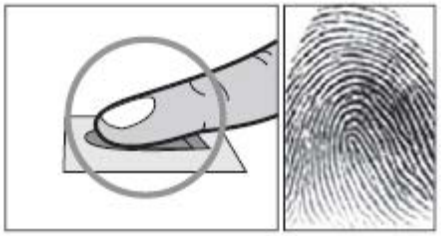
How to place a finger

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.





©Copyright 2008 Suprema Inc.

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.

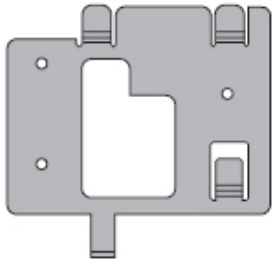
©Copyright 2008 Suprema Inc.

Product Contents

Basic Contents



BioStation fingerprint terminal



Wall mounting metal bracket



Wall mounting
screws and holders - 3 ea



Star-shape screw for fixing
main body



USB cable



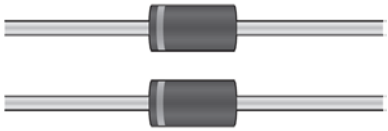
Star-shape small wrench



5pin, 3pin, 6pin, 4pin, 7pin cable – 1 ea



Software CD

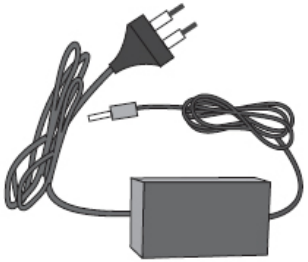


Diodes

©Copyright 2008 Suprema Inc.

Product Contents

- **Optional accessories**



12V power adaptor



Plastic stand type A



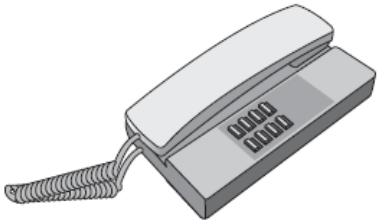
USB fingerprint scanner for enrollment on PC



Wireless LAN Access Point



Secure I/O



Interphone

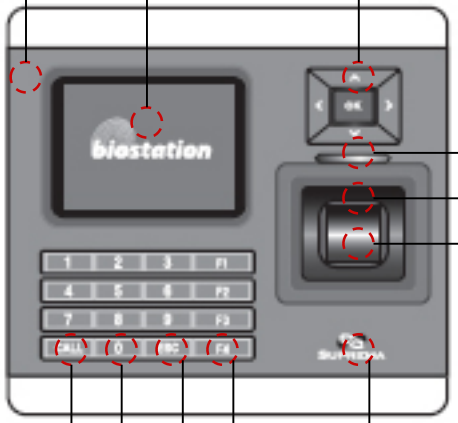


USB Mifare reader/writer

©Copyright 2008 Suprema Inc.

Name of each part

Front

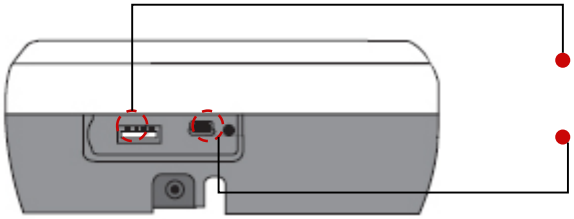


- Microphone
  - Used when connected to interphone.
- Color LCD
  - Displays terminal status (T&A mode, notice, etc.) and current time.
- Navigation key
  - ▼ : Move down in Admin menu or view detailed T&A function key
  - ▲ : Move up in Admin menu or hide detailed T&A function key
  - ► : Show the next 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

©Copyright 2008 Suprema Inc.

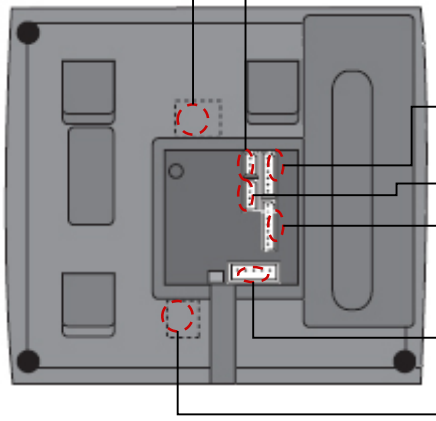
Name of each part

Bottom



- Slot for USB memory device : USB type A
- Slot for PC USB connection : Mini USB

Rear

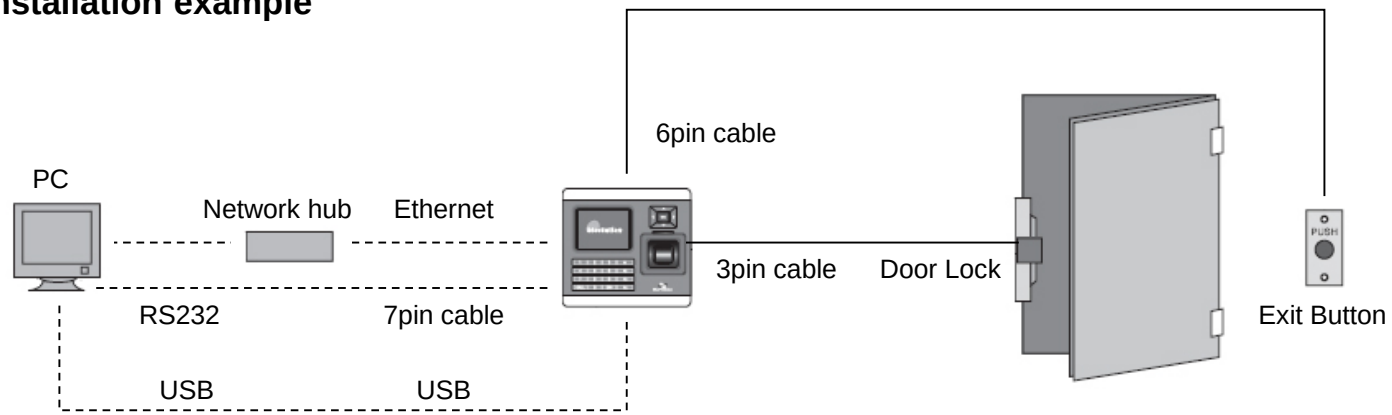


- Ethernet cable connector : RJ45
- 3pin cable connector - Door
- 6pin cable connector – Input/Output or Wiegand
- 4pin cable connector - RS485
- 7pin cable connector - RS232 or BEACon
- 5pin cable connector – Power and door phone
- 12V power adaptor

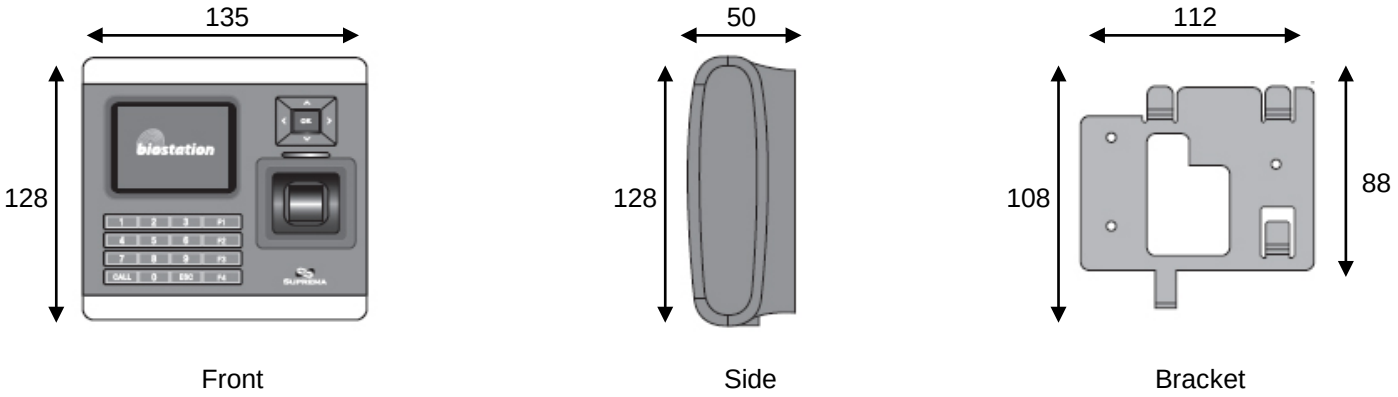
©Copyright 2008 Suprema Inc.

Installation

Installation example



Product dimension (mm)



Front Side Bracket

©Copyright 2008 Suprema Inc.

Cable spec.

Power & Doorphone



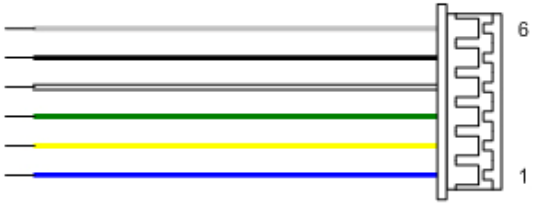
PIN	PIN DESCRIPTION	WIRE
1	PWR +VDC	RED
2	PWR GND	BLACK
3	INPH AUD	ORANGE
4	INPH DTA	BLUE
5	SH GND	GRAY

Relay



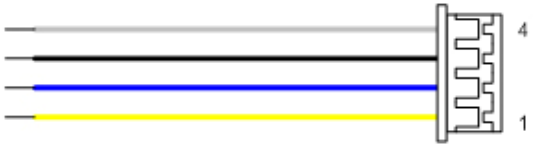
PIN	PIN DESCRIPTION	WIRE
1	RLY NO	WHITE
2	RLY COM	BLUE
3	RLY NC	ORANGE

TTL I/O or Wiegand



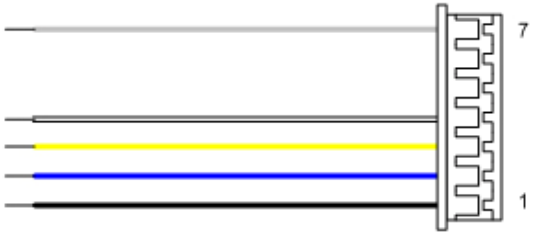
PIN	PIN DESCRIPTION	WIRE
1	TTL / WG IN0	BLUE
2	TTL / WG IN1	YELLOW
3	TTL / WG OUT0	GREEN
4	TTL / WG OUT1	WHITE
5	TTL / WG GND	BLACK
6	SH GND	GRAY

RS485



PIN	PIN DESCRIPTION	WIRE
1	485 TRXN	YELLOW
2	485 TRXP	BLUE
3	485 GND	BLACK
4	SH GND	GRAY

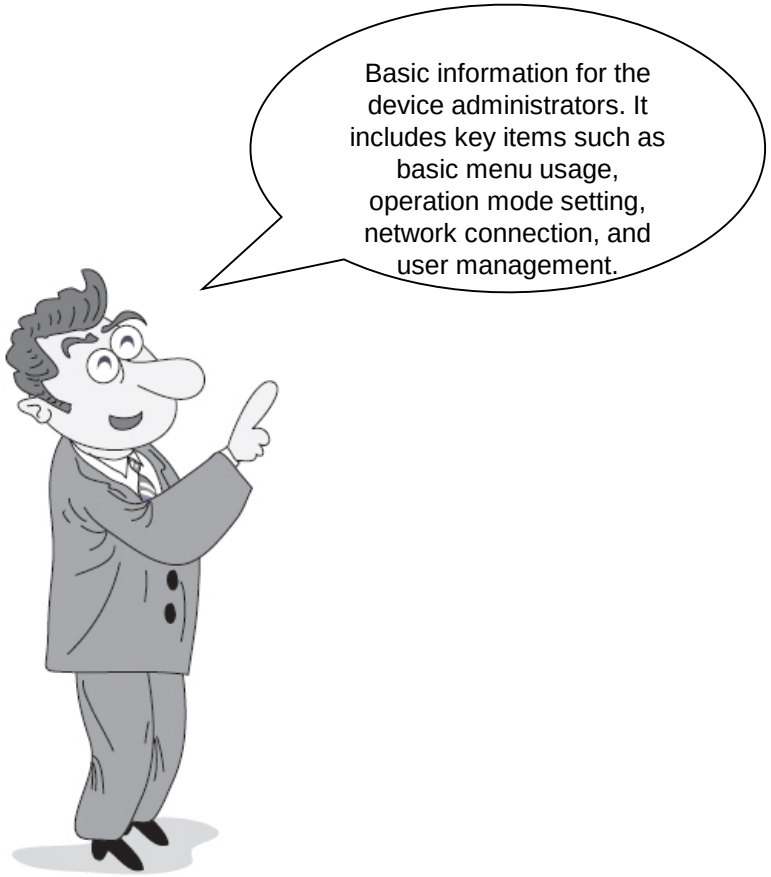
RS232



PIN	PIN DESCRIPTION	WIRE
1	232 GND	BLACK
2	232 TX	BLUE
3	232 RX	YELLOW
4	TTL OUT1	WHITE
7	SH GND	GRAY

©Copyright 2008 Suprema Inc.

For Administrators - Basic Functions

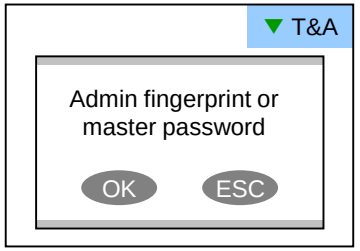


©Copyright 2008 Suprema Inc.



Enter Admin Menu

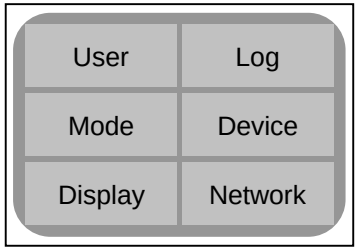
- **Press ESC key to enter Admin menu from the initial display.**



- **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.

- **If the master password is entered successfully, initial Admin menu appears on display.**



©Copyright 2008 Suprema Inc.



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 and different settings
  - 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, RS232, RS485, USB, Secure I/O, etc.
- **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>.

©Copyright 2008 Suprema Inc.



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.**

1:1 Mode

- Setting : ID/Card+Finger, ID/Card+PIN, ID/Card+Finger/PIN, Card Only, ID/Card+Finger+PIN

1:1 Time

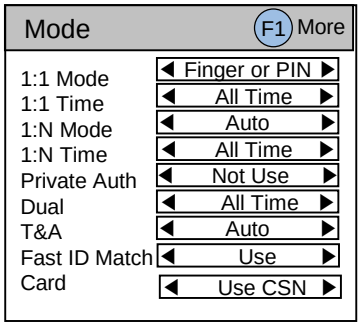
- After entering ID on 1:1 mode, set whether you will use fingerprint, PIN, or either for authentication. In case of card, using card only enables users to access just by placing the card.
- Set schedules to apply the above 1:1 mode.
- Select “All Time”, “No Time” or a specific schedule set by BioAdmin program

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.

1:N Time

- Set schedules to apply the above 1:N mode
- Select “All Time”, “No Time” or a specific schedule set by BioAdmin



©Copyright 2008 Suprema Inc.



Operation mode setting

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

Fast ID Matching

- In fast ID matching mode, a user is required to input the first part of his/her ID and to place a finger. Then, matching will be done within the specific user IDs which contains the first part of ID inputted. For example, after inputting '11', the first two digits of user ID and placing a fingerprint, it matches users whose ID start '11', so matching speed is faster. (available in BioStation firmware V1.7 above)
- It will be disable when Server Matching option is on.
- When use function keys for TA mode, only F1~F4 are available to use

Private Auth

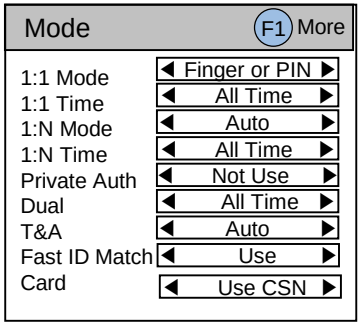
- Use or Not Use for private authentication

Dual

- Dual Authentication needs consecutive authentications from two different users within 15 seconds for high security
- If only the first user is authenticated, the device signals authentication success but does not activate a relay.

Dual Time

- Set schedules to apply the above "Dual Authentication" mode.



©Copyright 2008 Suprema Inc.

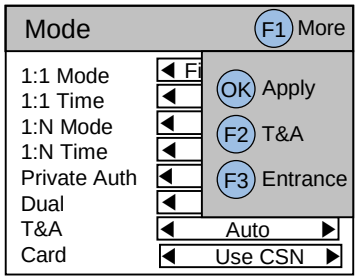


Operation mode setting

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

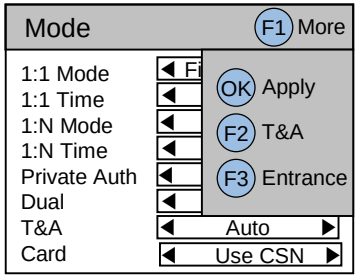
T & A

- Setting : Function key / Auto / Manual / Fixed
- Function key :Press function key F1~F4 first to enter an T&A event before authentication. Pressing ▼ key on initial display, user can enter extended T&A events.
- Auto : Apply T&A events set by time schedules
- Press F1 and F2 to change settings
- Choose a specific event by changing “T&A Key” and select a time schedule to apply the event. (Time schedules should be downloaded to the device using BioAdmin in advance.)
- Manual : Keep the T&A event of the last pressed function key. If one press F1(IN) and authenticate, the next ones do not need to press F1 again but still the events are recorded as F1(IN) event.
- Fixed : Keep the selected T&A event (function key).
- Press F1 and F2 to change settings
- Choose a function key to fix in “Fixed” menu



Mifare support (4K) (BioStation Mifare model)

- CSN mode : Select when use a Mifare card as a normal card (Same as RF card).
- Use Template : Select when use a Mifare card as a template on card.
  - Only the card formatted in User Menu available.
  - Setting of PIN, Group and period can be adjusted in BioAdmin.



©Copyright 2008 Suprema Inc.

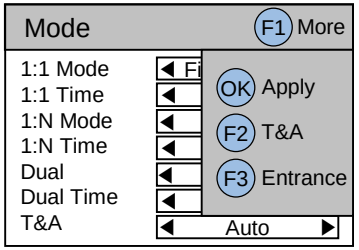


Operation mode setting

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

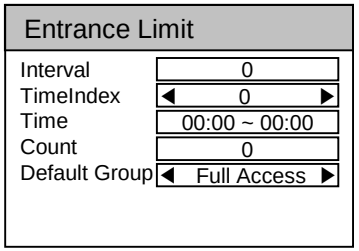
Auto Change

- In case of T&A manual /Auto/Fixed, it shows on T&A screen.



Entrance Limit

- Press F1 and F3 to enter “Entrance Limit” window
- Interval : Time period for re-authentication (min)
- Time Index : Select 4 different time periods per day
  - Time : Set time period
  - Count : Set max number of entrance during the period
- Default : Set default entrance mode for users who are not assigned a specific access group.



©Copyright 2008 Suprema Inc.



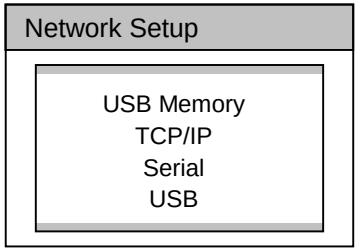
Network Setup - TCP/IP

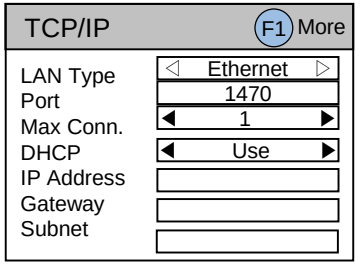
To use the device connected to PC, you need to set up the network according to your connection type.

- **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.**

LAN Type	• Setting : Disable/Ethernet/Wireless LAN (Optional) • Used when connected to PC via Ethernet using RJ45 connector on the rear of the device.
Port	• Set port number of TCP/IP (Default:1470)
Max Conn.	• Setting : 1/4/8/16 • Max number of BioAdmin clients that can access the device at the same time.
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. (Press right key (►) to input a dot (.) when entering IP address)





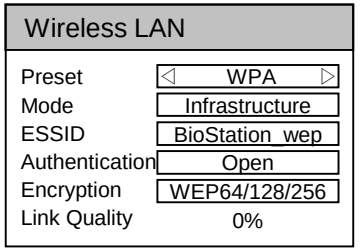
©Copyright 2008 Suprema Inc.



Network Setup - 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.**



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.

©Copyright 2008 Suprema Inc.



Network Setup - Server

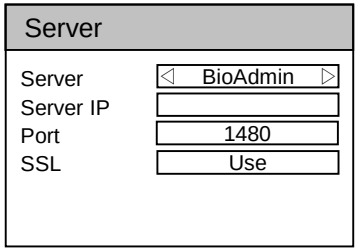
To set up the network to the Server.

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

Server	• Setting : BioAdmin / BioStar / Not Use
Server IP	• Set Server IP address
Port	• Set Server port (default : 1480)

- 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, BioStation 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 BioStation.
- To access BioStation from BioAdmin Client directly without accessing to server, SSL and server mode are set on “Not Use”
- For more information on server setup, please refer to BioAdmin manual.

SSL	• Setting : Use / Not Use



©Copyright 2008 Suprema Inc.



Network Setup - Serial

To connect BioStation to the serial port of PC, you need to select the baudrate of the serial communication.

RS485

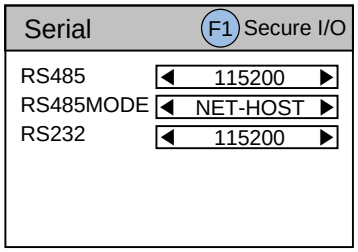
- Setting :Disable/9600/19200/38400/57600/115200
- Used when connecting to the serial port of PC using 7pin connector on the rear of the device.
- In the serial communication, the speed represents the frequency of carrier wave's changing status per sec, called baudrate.
- Default is 115200 bps.
- If you have communication error in serial communication, setting a lower baudrate may solve the problem.

RS485Mode

- Set RS485 communication (PC Connect/NET-HOST/NET-SLAVE)
- PC Connect : Select when communicating with PC host
- NET-HOST : Select whether device is a host in the RS485 loop
- NET-SLAVE : Select whether device is a slave in the RS485 loop
- This will be applied only using a BioStar to apply RS485 setting

RS232

- Setting : Disabled/9600/19200/38400/57600/115200
- Used when connecting to the serial port of PC using 4pin connector on the rear of the device.



©Copyright 2008 Suprema Inc.



Network Setup - USB

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

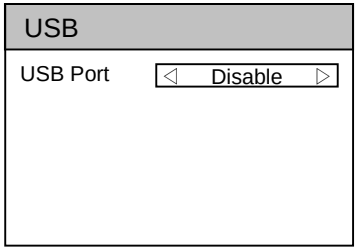
- **If you select USB on network submenu, USB setting menu appears on the display.**

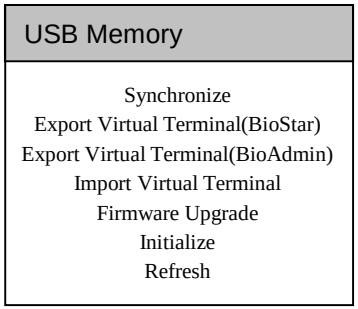
USB

- 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.

USB Memory

- The data from BioStation to BioStar or BioAdmin using compatible USB memory stick
- Virtual terminal should be generated by initializing USB memory
- Synchronize : Synchronize with USB memory
- Export Virtual Terminal : Transfer user information & log history from device to USB memory
- Import Virtual Terminal : Recognize as a virtual terminal
- Firmware Upgrade :Upgrade firmware via a virtual terminal
- Initialize : Initialize USB memory to recognize as a virtual terminal





©Copyright 2008 Suprema Inc.



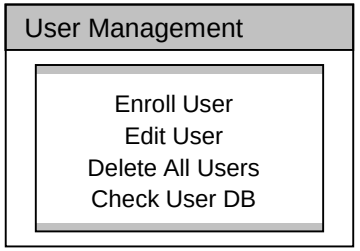
User Management - Enroll New User (Enroll to Device)

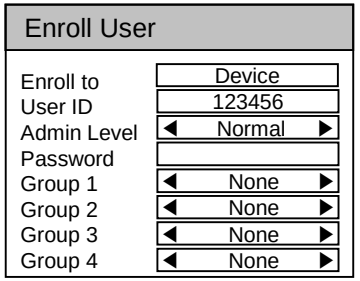
How to enroll the user information and fingerprint.

- **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.**

Enroll to	• Select where to enroll a user fingerprint • Setting : Device / Card (13.56MHz Mifare Card)
User ID	• 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.
Admin Level	• 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.
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. Default access group can be set as “Full Access” or “No Access” for whom without a specific access group assigned.





©Copyright 2008 Suprema Inc.



User Management - Enroll New User (Enroll to Device)

- **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
Count Limit	0
Timed APB	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.

©Copyright 2008 Suprema Inc.



User Management - Enroll New User (Enroll to Device)

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

Count 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.

Timed APB
- 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.

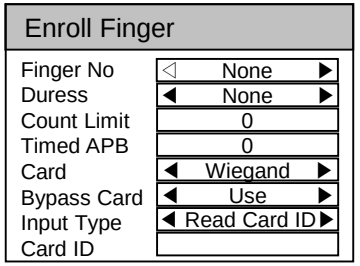
Card
- Setting : Not Use/RF Card/Wiegand
- It sets Use or Not use of card and the type of card.

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.

– In case of issuing template card via BSM model, administrator card can be issued.
– When enrolling a card, it can be divided as administrator and user authority.



Card ID display change (from V1.3)
Since firmware V1.3, card ID display type has been changed. So, cards registered before V1.3 may show a different ID display. But it doesn't affect card authentication.

©Copyright 2008 Suprema Inc.



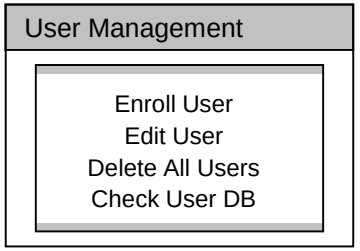
User Management - Enroll New User (Enroll to Card)

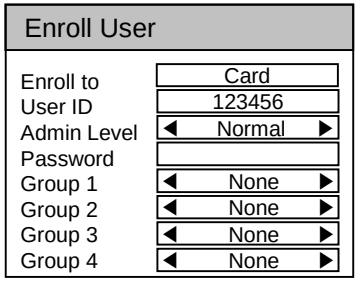
How to enroll the user information and fingerprint.

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

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

Enroll to	• Select where to enroll a user fingerprint • Setting : Device / Card (13.56MHz Mifare Card)
User ID	• 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.
Admin Level	• 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.
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. Default access group can be set as “Full Access” or “No Access” for whom without a specific access group assigned.





©Copyright 2008 Suprema Inc.



User Management - Enroll New User (Enroll to Card)

- **If you choose Enroll to Card and enter all the necessary items for enrollment and press OK key, the following fingerprint menus appear on the display.**

Finger No

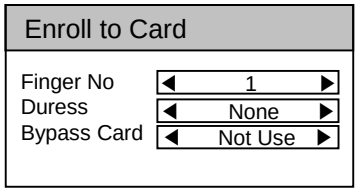
- Setting : 1 / 2 / None
- One or two fingers can be enrolled for each ID.
- Formatted Mifare card should be placed to enroll a fingerprint. (Refer to Format Card in page 40)
- When use a 4k Mifare card to enroll 4 fingerprints to the card, Mifare card layout should be changed in BioAdmin.

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, two fingerprints should be enrolled, ie., Finger No. should be 2.
- Duress finger should be different from normal finger enrolled in advance.

Bypass Card

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



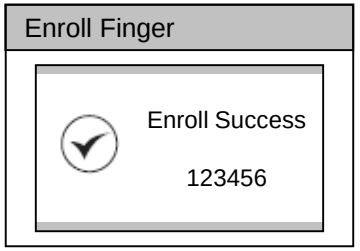
©Copyright 2008 Suprema Inc.



User Management - Enroll New User

- **After selecting Finger No. and Duress and pressing OK, now you should place a finger on a sensor for enrollment.**
- **Please place a finger correctly referring to <How to place a finger>.**
  - 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 continuously.
  - 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”.
- **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.**





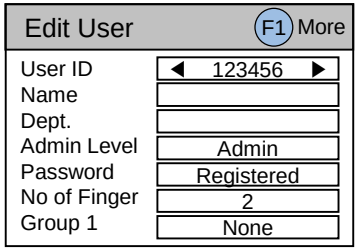
©Copyright 2008 Suprema Inc.

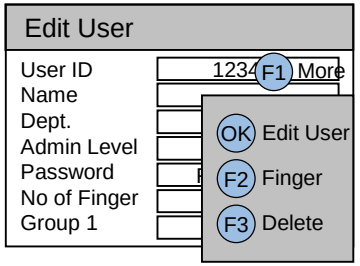


User Management - Check User Info

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.**





©Copyright 2008 Suprema Inc.



User Management - Edit User Info

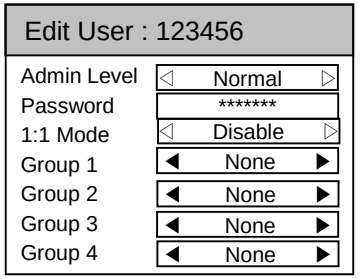
User info can be changed and fingerprints can be re-enrolled.

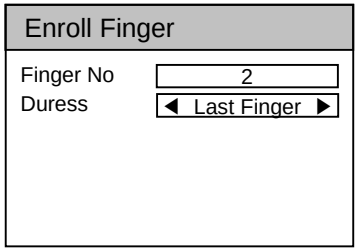
- **If you press OK key at Edit User menu, the selected user info is displayed and can be edited in the same way as in the Enroll User process. You can change admin level, password and groups.**

- **1:1 Mode : You can set different 1:1 mode per user**
  - Setting : ID/Card+Finger
    ID/Card+PIN
    ID/Card+Finger/PIN
    ID/Card+Finger+PIN
    Card Only

- **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.**





©Copyright 2008 Suprema Inc.



User Management - 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.



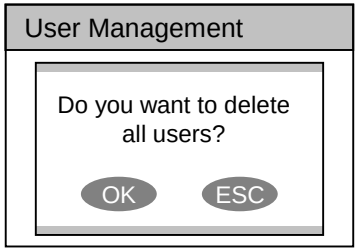
©Copyright 2008 Suprema Inc.



User Management - 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.**



- **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.

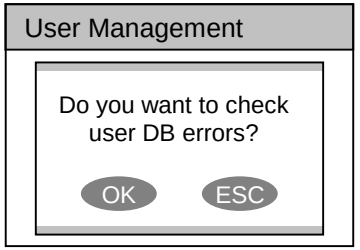
©Copyright 2008 Suprema Inc.



User Management - 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.**



- **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.

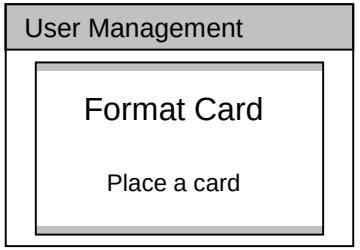
©Copyright 2008 Suprema Inc.



User Management - Format Card (only for Mifare card)

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

- **If you press Format Card on User menu, following menus appear on the display. (This is for Mifare Card only)**



- **Place card to the device for format.**
  - In order to enroll a user template to a card, this should be done.
  - "Format failed" message will be displayed, if you don't place card to the device within 3 second after card format setting.

©Copyright 2008 Suprema Inc.

For Administrators - Advanced Functions



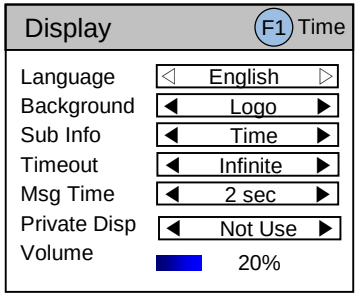
©Copyright 2008 Suprema Inc.



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.**



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.

©Copyright 2008 Suprema Inc.



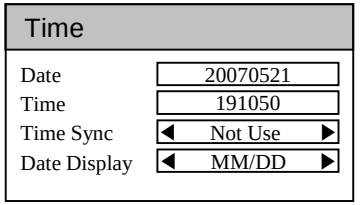
Display & Sound Setting

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
- Time : hhmmss
- Time sync : Terminal time will be synchronized with server time.
- Date Display : MM/DD or DD/MM



©Copyright 2008 Suprema Inc.



Device Setup - Fingerprint Setting

Change various settings for fingerprint authentication.

- **If you select Device on initial Admin menu, Device Setup menus appear on the display. Then select Fingerprint for setting related to fingerprint authentication.**

Security

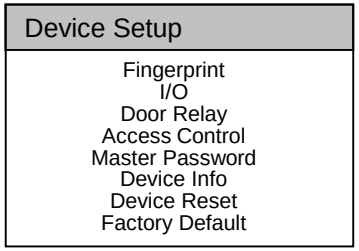
- Setting : **Normal**/Secure/Most Secure
- Security level is determined by FAR (False Acceptance Rate). FAR refers to the percentage of acceptance by unregistered fingerprints. Therefore, the lower the percentage is, the higher the security level is. However, as the FAR and FRR (False Rejection Rate) are in reverse proportion to each other, the higher security level will induce 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.

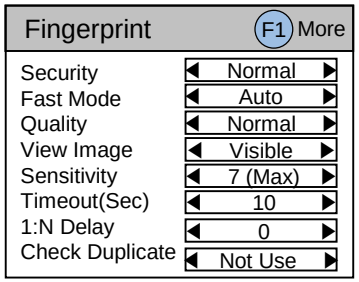
Fast Mode

- 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.





©Copyright 2008 Suprema Inc.



Device Setup - Fingerprint Setting

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)

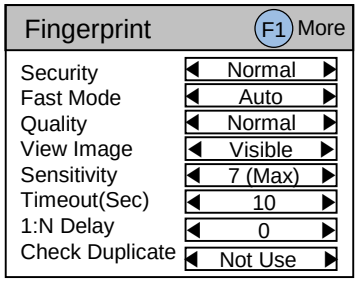
- Setting : 1/2/…/**10**/…/19/20
- Set standby time for fingerprint enrollment. If a user does not place a finger within the time, a timeout message appears on the display.

1:N Delay

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

Duplicate

- Setting : Not Check / Check
- In enrollment, checks whether the fingerprint is duplicated or not.



©Copyright 2008 Suprema Inc.



Device Setup - Fingerprint Setting

Change detailed settings for fingerprint authentication.

- **Press F1 on Fingerprint menu to set detailed fingerprint options.**

Match Timeout

- Setting : 1/2/**3**/…/19/20
- Timeout in 1:N identification. If the device cannot find a matched fingerprint in this period, it results in identification fail. This is to avoid too long waiting time in case of large enrollments.

Calibration

- For TC sensor, this menu calibrates the sensor's internal parameters according to outer environment. Since sensor calibration is done in factory, it doesn't need to do this usually except the case where sensors are replaced or sensitivity of the sensor is abnormal.
- To calibrate the sensor, select "Enable" and click OK button.
- This menu disappears for OC or FC model.

SIF Support

- BioStarion supports the standard template format, as defined in ISO19794-2
- SIF Support can be configurable, when no user is enrolled in the device.

Fake Finger

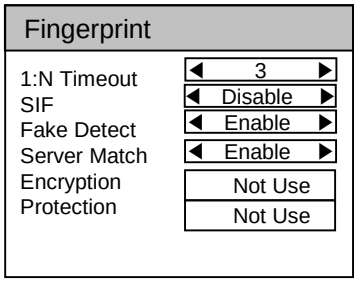
- Setting : Disable / Enable
- Detect a fake finger input to enhance security.

Server Match

- Setting : Disable / Enable
- Perform fingerprint or card ID matching at the BioStar server, instead of the device (Available only for BioStar SE(Standard Edition))

Encryption

- Shows current device setting whether to encrypt fingerprint templates or not for security purpose.
- This menu only shows current setting and the settings can be changed only by BioAdmin program on PC.



©Copyright 2008 Suprema Inc.



Device Setup - I/O Setting

Change various settings for I/O.

- **If you select I/O on device menu and click Input, following menus appear on display.**

Input 0/1

- Setting : Disabled/Exit/Wiegand User ID/Wiegand Card ID/Generic Input/Emergency Open/Alarm Off/Reset/Lock System
- In case of using the input port for RTE(exit button), select Exit.
- In case of using input as Wiegand User/Card ID, input 0 and input 1 are set as Wiegand User/Card ID.
- Generic Input : general input. Can be configured with output.
- Emergency Open : All relays for doors are turned on for door open
- Alarm Off : All relays are turned off to release alarm
- Reset : System reset
- Lock System : the device gets locked. Can be released with master password only.

Duration 0/1(ms)

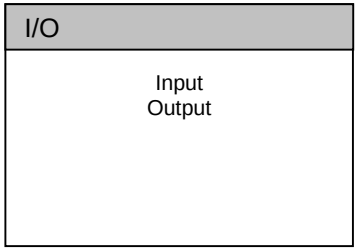
- Minimum duration of input signal to decide validity

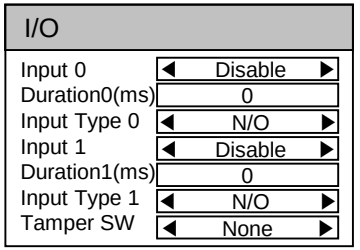
Input Type 0/1

- Set N/O (Normal Open) or N/C (Normal Close)

Tamper S/W

- Setting : None/Lock System/Generic Input/Emergency Open/Alarm Off/Reset
- Tamper switch is turned on when a housing (case) of BioStation is opened. If the setting is in “Lock System”, the device is automatically locked when a tamper switch is on for security.
- [Note] Once BioStation is locked, lock can be released only when the master password is entered. It cannot be released by administrator’s fingerprint.





©Copyright 2008 Suprema Inc.



Device Setup - I/O Setting

Change various settings for I/O.

- **If you select I/O on device menu and click Output, following menus appear on display.**

Output 0/1

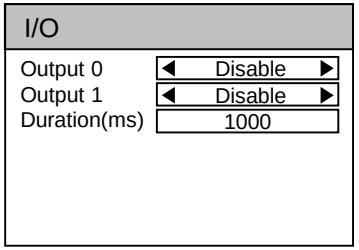
- Setting: Disabled/Duress/Tamper SW/Auth Success/Auth Fail/Wiegand User ID/Wiegand Card ID
- Can send outputs for various events.
- In case of using output as Wiegand User/Card ID, output 0 and output 1 are set as Wiegand User/Card ID.

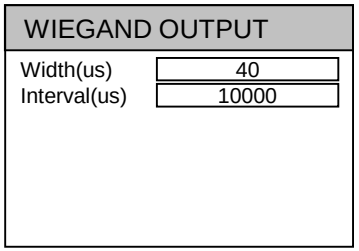
Duration(ms)

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

Wiegand Output

- Width (us) : Set Pulse Width.
- Interval (us) :Set Pulse Interval.





©Copyright 2008 Suprema Inc.



Device Setup - Door Relay Setting

Change various settings for door relay.

- **In a simple standalone door control, internal relay of BioStation can be used to drive a door lock. For increased security, external device like Secure I/O or another BioStation can be installed inside of a room. Two devices are connected by RS485 and support a local anti-pass back functions. Up to 2 BioStations and 4 Secure I/Os can be connected in a single RS485 loop.**
- **If you select Door Relay on device menu and select Door#, following menus appear on the display.**

Relay

- Select which relay shall be used
- Setting: Internal Relay/Slave Relay/SIO# Relay#/Not Use

Out/In Device

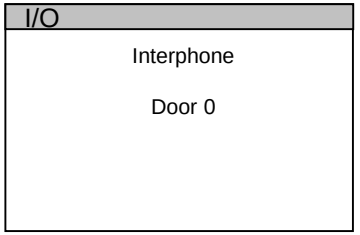
- Select a device to be installed inside and outside.
- Setting: Not Use/Device ID (It is not available from firmware v1.5)

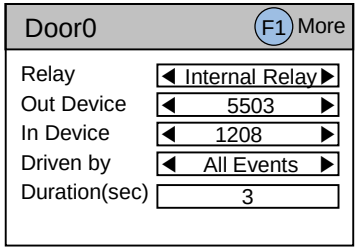
Driven by

- Setting: All events / Authentication +T&A event/Authentication/T&A event/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 authentication, door opens only by authentication without T&A event
- In case of selected T&A, door opens only by the specific events for which door use is allowed.
- In case of disabled, BioStation will not drive an internal relay to open a door by any of events or authentication.

Duration (sec)

- Duration of the relay activation (door open)





©Copyright 2008 Suprema Inc.



Device Setup - Door Relay Setting

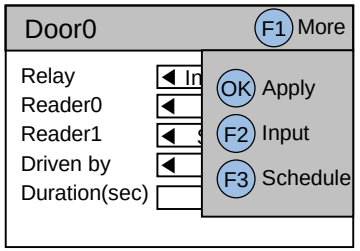
Change various settings for door relay.

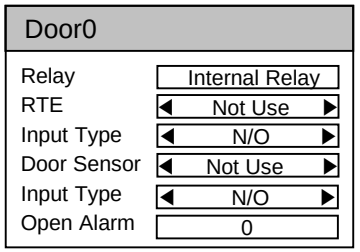
- **If you select F1 – F2(Input) on Door# setting menu, following menus appear on the display.**

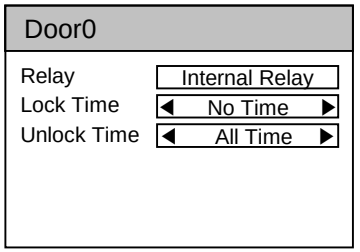
RTE	• Select Request To Exit (Exit button) setting related to the relay • Setting: Not Use/Input# (input port of the selected device)
Input Type	• Set N/O (Normal Open) or N/C (Normal Close)
Door Sensor	• Select Door Sensor setting related to the relay (door) • Setting: Not Use/Input# (input port of the selected device)
Input Type	• Set N/O (Normal Open) or N/C (Normal Close)
Open Alarm	• When the door is open longer than this period (sec), door open alarm is activated. Specific output can be set by BioAdmin program on PC. Default is 0 meaning no alarm.

- **If you select F1 – F3(Schedule) on Door# setting menu, following menus appear on the display.**

Lock time	• Decide time to lock (close) the door by force. • During lock time, general users cannot open door while only administrators are allowed. • Specific schedule for lock time can be set by BioAdmin program on PC.
Unlock time	• Decide time to open the door by force • Specific schedule for unlock time can be set by BioAdmin program on PC.







©Copyright 2008 Suprema Inc.



Device Setup - Door Relay Setting

Change various settings for door relay.

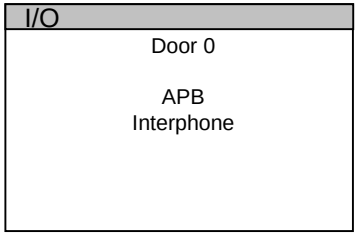
- **If you select APB on Door Relay menu, following menus appear on the display.**

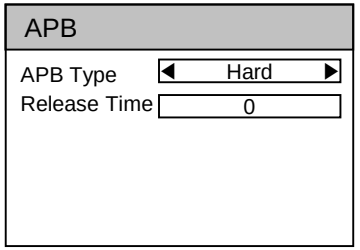
APB Type

- Select anti-pass back setting
- Setting: Disable/Hard/Soft
- In “Hard” mode, relay does not work and log is recorded in case of anti-pass back events. In “Soft” mode, log is recorded but relay works as usual.

Reset Time

- Duration(min) of automatic reset of APB for each user. If it is set as 30(min), for example, APB record is erased for 30 minutes after each authentication of users. If 0, there is no automatic reset.

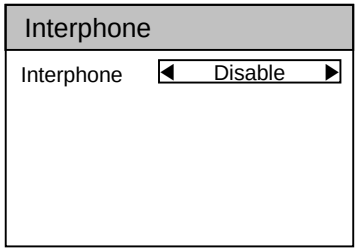




- **If you select Interphone on Door Relay menu, following menus appear on the display.**

Interphone

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



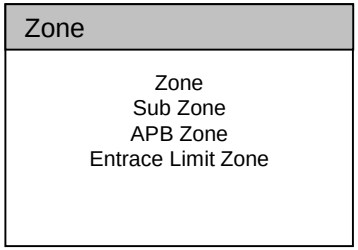
©Copyright 2008 Suprema Inc.



Device Setup - Zone

Change advanced access control settings- Zone

- **Zone is a group of devices connected by TCP/IP and integrated together supporting data synchronizations, global anti-pass back and entrance limits. One of the devices should be assigned as a master in the zone. Master device collects and synchronize user and log information and makes a decision for anti-pass back and entrance limit control.**
- **If you select Access Control on device menu and select Zone, following menus appear on display.**



Node Type

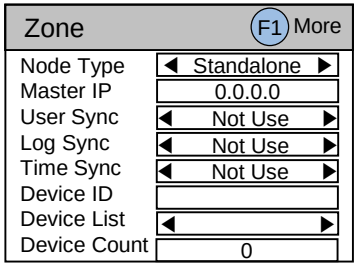
- Setting : Standalone/Master/Device
  - Standalone – works independently without zone concept
  - Master – a master device in the zone
  - Device – the rest of the device in the zone

Master IP

- Enter IP of master device (only works when Node Type is Device)

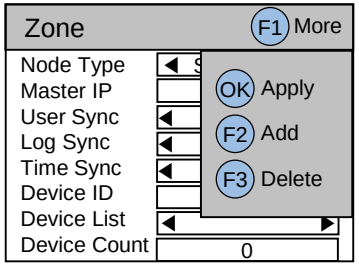
User/Log/Time Sync

- Options to enable synchronize user, log and time data among devices



Device ID/List/Count

- When Node Type is Master, enter IDs of the rest devices
- Enter ID of a device to add in “Device ID”. Then press F1 and press F2 (Add).
- Then you can see the added device in “Device List” and the increased number of the total devices in “Device Count”
- For deleting, select the device in “Device List” and then press F1 and F3 (Delete).



- **In case of using BioStar, “Zone” menu won’t be displayed.**

©Copyright 2008 Suprema Inc.



Device Setup - Sub Zone

Change advanced access control settings – Sub Zone

- **To add anti-pass back or entrance limit functions, Sub Zone should be created in a Zone.**
- **If you select Access Control on device menu and select Sub Zone, following menus appear on display.**

- To make a Sub Zone, the device should be a master (Node Type of Zone menu). If the device is a member but not a master, only “Device Auth” can be set in this menu.

SubZone ID

- Select an ID of a sub zone (from 0 to 15)

Zone Type

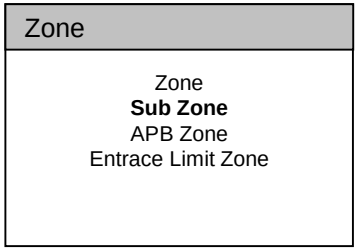
- Select a sub zone type either “APB” or “Entrance Limit”.

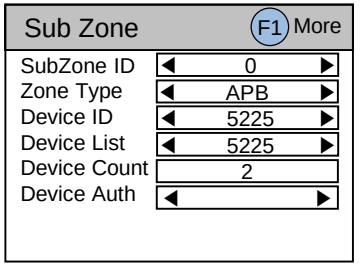
Device ID/List/Count

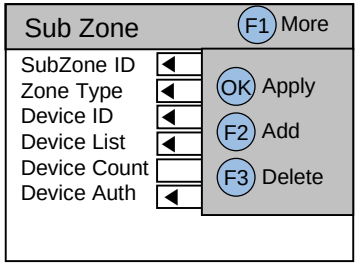
- Select a “Device ID” of a device to add in a sub zone. Then press F1 and press F2 (Add).
- Then you can see the added device in “Device List” and the increased number of the total devices in “Device Count”
- For deleting, select the device in “Device List” and then press F1 and F3 (Delete).

Device Auth

- When the device is a member of a zone (Node Type of Zone is set as “Device”), Device Auth menu can be set to determine whether authentication decision is done by master or standalone
- Setting: Standalone/Notify/Deferred
  - Standalone, Notify : decision made by device itself.
  - Deferred : Zone master decides the authentication result. For APB and Entrance Limit, select this option.







©Copyright 2008 Suprema Inc.



Device Setup - APB Zone

Change advanced access control settings – APB Zone

Select APB Zone on Zone menu

SubZone ID
- Select Sub Zone ID to make APB setting

APB Type
- Setting: Disable/Hard/Soft
- In “Hard” mode, relay does not work and log is recorded in case of anti-pass back events. In “Soft” mode, log is recorded but relay works as usual.

Reset Time
- Duration(min) of automatic reset of APB for each user. If it is set as 30(min), for example, APB record is erased for 30 minutes after each authentication of users. If 0, there is no automatic reset.

Device List
- Select a device for In and Out setting

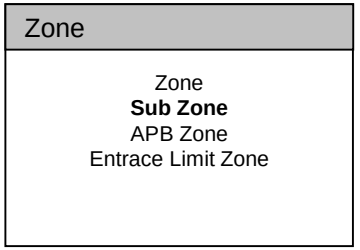
IN/OUT
- Select IN or OUT for anti-pass back function of the selected device.
- One who entered a room with authentication by IN devices must go out by OUT devices.

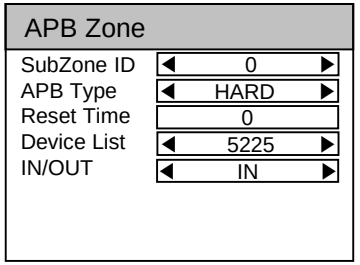
Select Entrance Limit Zone on Zone menu

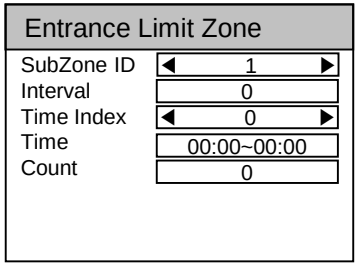
SubZone ID
- Select Sub Zone ID to make APB setting

Interval
- Interval : Time period for re-authentication (min)

Time Index/Time/Count
- Time Index : Select 4 different time periods per day
  - Time : Set time period
  - Count : Set max number of entrance during the period







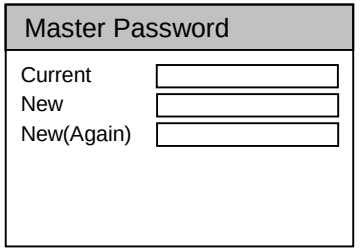
©Copyright 2008 Suprema Inc.



Device Setup - Change Master Password

Change master PW.

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



- **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 BioStation. 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.

©Copyright 2008 Suprema Inc.



Device Setup - 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.**

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 BioStation, various information like user info, log, background and sounds are stored, so used memory changes by the size of these information.

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

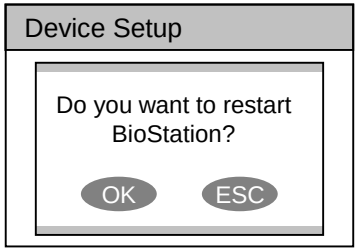
©Copyright 2008 Suprema Inc.



Device Setup - Device Reset

Reset system.

- **If you select Device Reset on device menu, a message to restart BioStation 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 BioStation, you should reset BioStation to apply the new language.**
- **If device becomes unstable for any reason, in most of cases, device reset can solve the problem.**



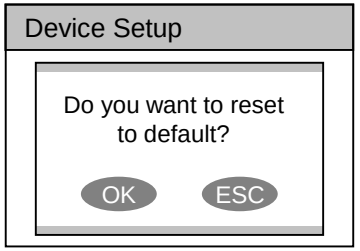
©Copyright 2008 Suprema Inc.



Device Setup - 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.**



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>.**

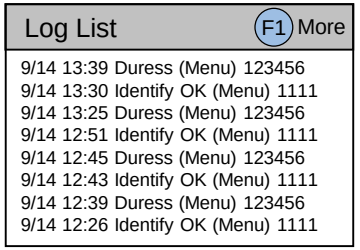
©Copyright 2008 Suprema Inc.



Log - 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.**



- **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.**

©Copyright 2008 Suprema Inc.

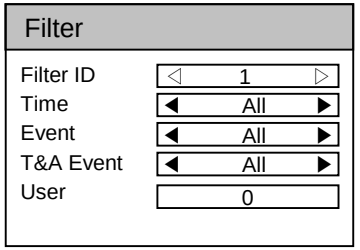


Log - Filter Log

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 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.



©Copyright 2008 Suprema Inc.



Log - 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.**



- **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.

©Copyright 2008 Suprema Inc.



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 BioStation. At the same time, transfer the log data from the connected BioStation 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 BioStation.

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 BioStation.

©Copyright 2008 Suprema Inc.



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 BioStation.

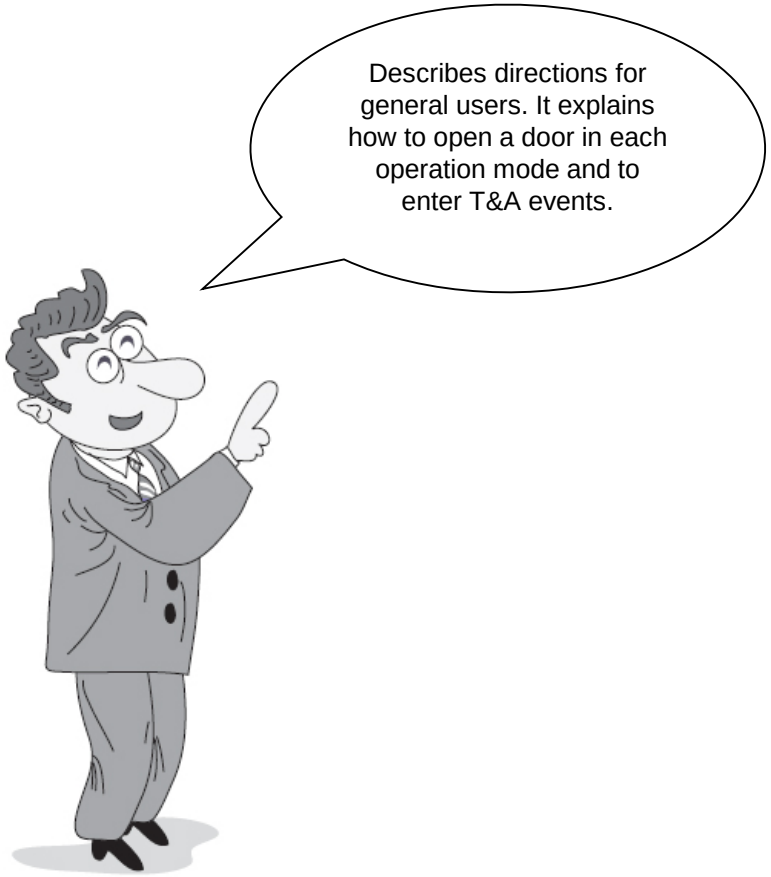
Refresh

- 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

©Copyright 2008 Suprema Inc.

For General Users



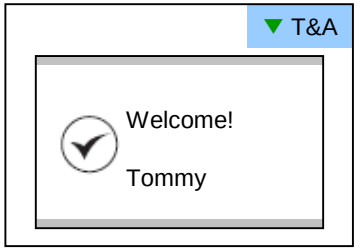
©Copyright 2008 Suprema Inc.



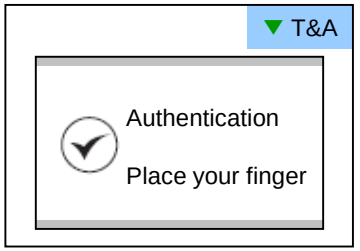
Access using 1:N mode

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.

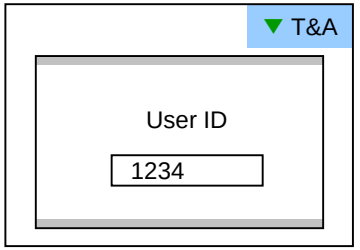
©Copyright 2008 Suprema Inc.



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 BioStation 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.

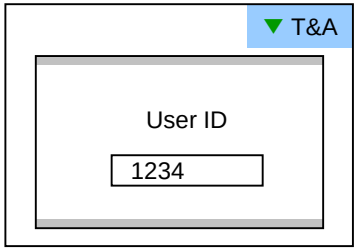
©Copyright 2008 Suprema Inc.



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	



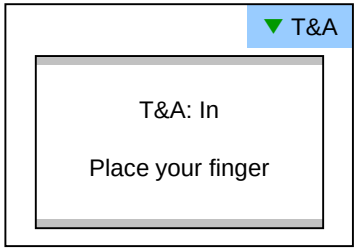
©Copyright 2008 Suprema Inc.



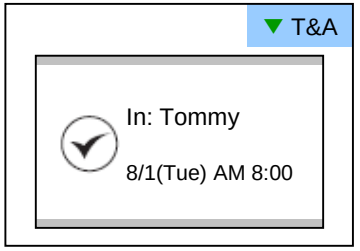
T&A event using 1:N mode

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.**



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



- **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.**

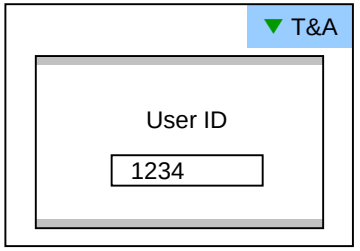
©Copyright 2008 Suprema Inc.



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.**



- **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.

©Copyright 2008 Suprema Inc.



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.**

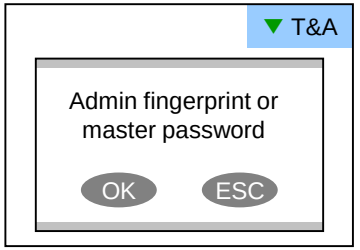
©Copyright 2008 Suprema Inc.



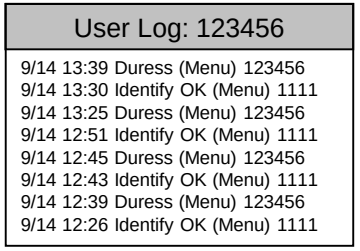
View user's Access/T&A event records

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.**

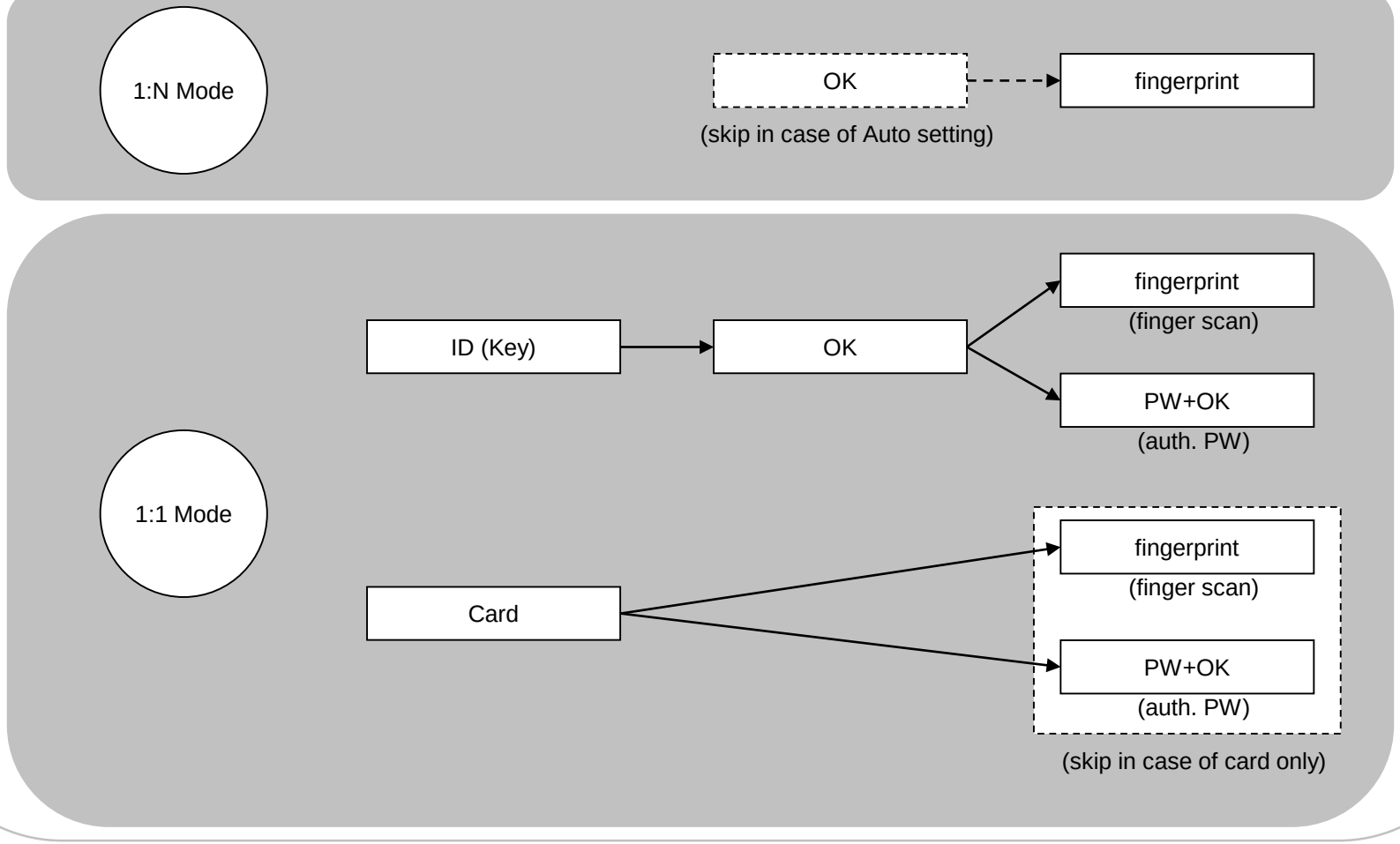


- **Press up/down navigation key to scroll a log one by one.**
- **Press left/right navigation key to scroll a log page by page (8 logs).**
- **Press OK key to display the latest log.**

©Copyright 2008 Suprema Inc.



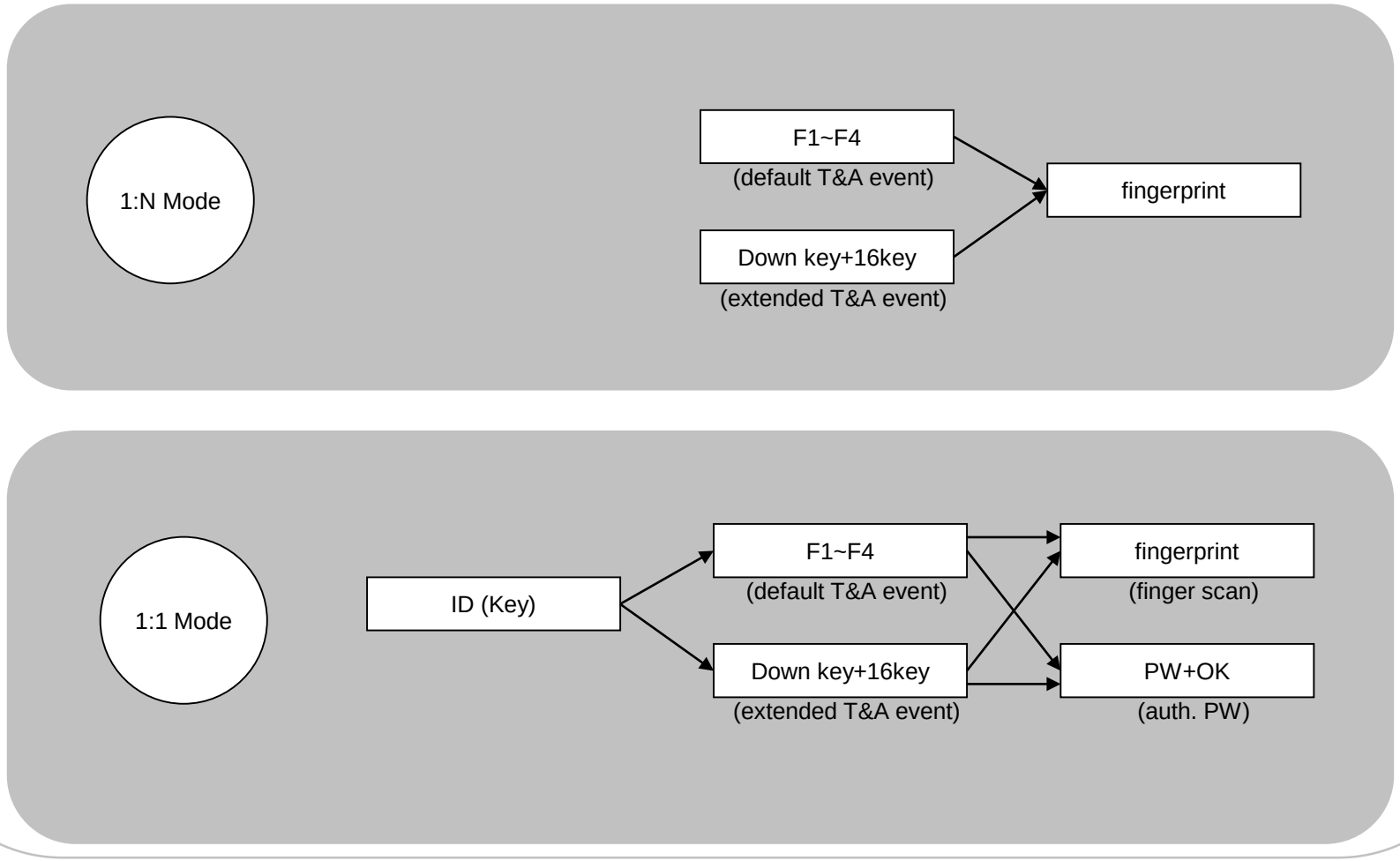
Authentication procedure as per operation mode



©Copyright 2008 Suprema Inc.



Authentication procedure for T&A event



©Copyright 2008 Suprema Inc.

System Specifications

- CPU : Dual CPU (32 bit RISC + 533MHz DSP)
- Memory : 1GB flash + 34MB RAM
- Display : 2.5 inch QVGA 16 million color LCD
- Identification speed : 3,000 fingerprints in 1 second
- Fingerprint capacity : 400,000 fingerprint templates
- Log capacity : 1,000,000 events
- Host interface : Wireless LAN (optional), 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 : 125KHz EM, 125KHz HID Prox, 13.56MHz Mifare/DESFire
- 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

©Copyright 2008 Suprema Inc.

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 from 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.

©Copyright 2008 Suprema Inc.

Device cleaning

- **Wipe out machine surface with dry towel or cloth.**
- **In case there is dust or impurities on the sensor of the BioStation, 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.**





©Copyright 2008 Suprema Inc.

Suprema Inc.
16F Parkview Office Tower, Jeongja-dong, Bundang-gu,
Seongnam, Gyeonggi, 463-863 Korea
E-mail : support@supremainc.com
Website : www.supremainc.com

Technical Support & Inquiry

Functions and specifications of the product are subject to changes without notice due to quality enhancement or function update. For any inquiry on the product, please contact **Suprema Inc**.