suprema

BioStation 2

USER GUIDE

Version 1.38
English

EN 102.00.BS2 V1.38A

Contents

Safety Instructions

Please read the following instructions carefully before using the product. This information is important for ensuring the safety of the user and for preventing damage to the user's property.

⚠Warning

Failure to follow the instructions may cause serious injury or death.

Installation Instructions

Do not install the product in direct sunlight or in a location that is damp or dusty.

- This can cause a fire or electric shock.

Do not install the product near any heat source such as electric heaters.

- This can cause a fire from overheating or electric shock.

Install the product in a dry place.

- Moisture can cause product damage or electric shock.

Install the product in a place where there is no electromagnetic interference.

- This can cause product damage or electric shock.

Have qualified service professionals install or repair the product.

- Otherwise, it can cause a fire, electric shock, or injury.
- If the product is damaged due to a user's unauthorized installation or dismantling of the product, a service fee will be charged for repair.

Operating Instructions

Be careful not to spill any liquid such as water, drinks, or chemicals inside the product.

- This can cause fire, electric shock, or product damage.

⚠Caution

Ignoring these instructions may result in minor injuries or damage to the product.

Installation Instructions

Protect the power cord from being walked on or pinched.

- This can cause product damage or injury.

Keep the product away from strong magnetic objects such as magnets, TVs, monitors (especially CRT monitors), or speakers.

- This can cause a failure.

Only use a DC 12V power adapter that provides a current of at least 500mA.

- This device does not work if the proper power source is not used.

After all the cables are properly installed, apply the liquid silicone underneath and above the cables within the groove ap proximately 10mm wide. The cable cover must be installed to ensure the IP65 rating.

- Non-proper installation of the cable cover may cause device malfunction or damage from water and dust.

If installing the product outside where the product is completely exposed, it is recommended to install the product together with the enclosure.

Use a separate power supply for Secure I/O 2, electric lock and BioStation 2 respectively.

- If connecting and using the power supply to these devices together, the devices may malfunction.

Operating Instructions

Do not drop the product or subject it to shock or impact during use.

- This can cause a failure.

Keep the password secret from others and change it periodically.

- Failure to do so may lead to an illegal intrusion.

Do not press the buttons on the product with excessive force or with a sharp tool.

- This can cause a failure.

Be careful not to contaminate or damage the fingerprint reader with dirty hands or materials.

- This can decrease performance or cause failures to read fingerprints.

Clean the product with a soft, dry cloth. Do not use alcohol, benzene, or water.

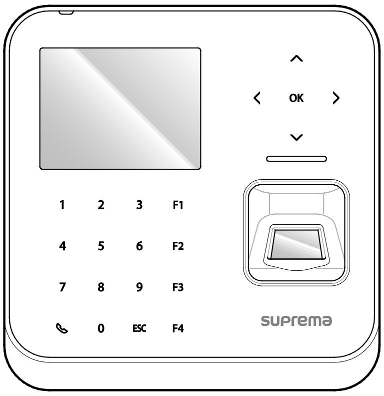
- This can cause a product failure.

BioStation 2 uses the capacitive button. If there is much moisture (humidity) like a rainy weather or on the product, wipe with a soft and dry cloth.

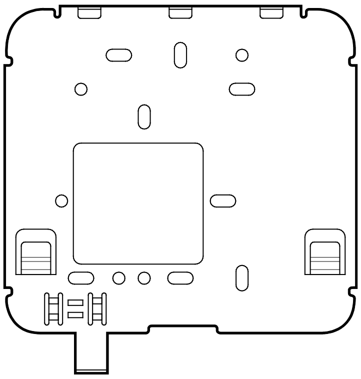
There is a risk of fire if batteries are replaced by an incorrect type.
Dispose of batteries in accordance with local and national disposal regulations.

Getting Started

Components

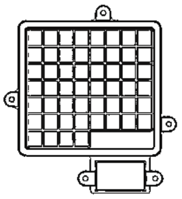


BioStation 2



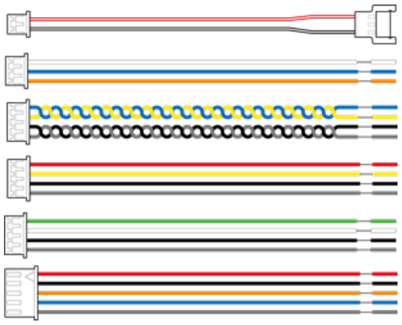
Wall Bracket

Product installation height is about 1,400 mm above the floor.

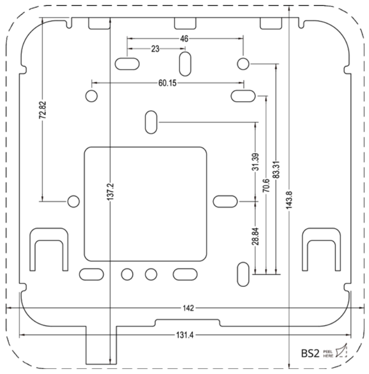


Cable Cover

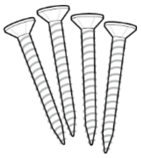
Bracket Fixing Screw (Star Shaped)



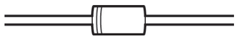
Connector Cables (1x2-pin, 1x3-pin, 3x4-pin, 1x5-pin)



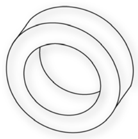
Drilling Template



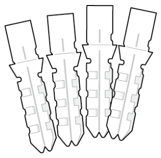
Fixing Screws x4



Diode

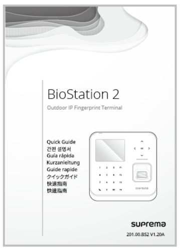


Ferrite Core



PVC Anchors x4

Open Source Software Guide

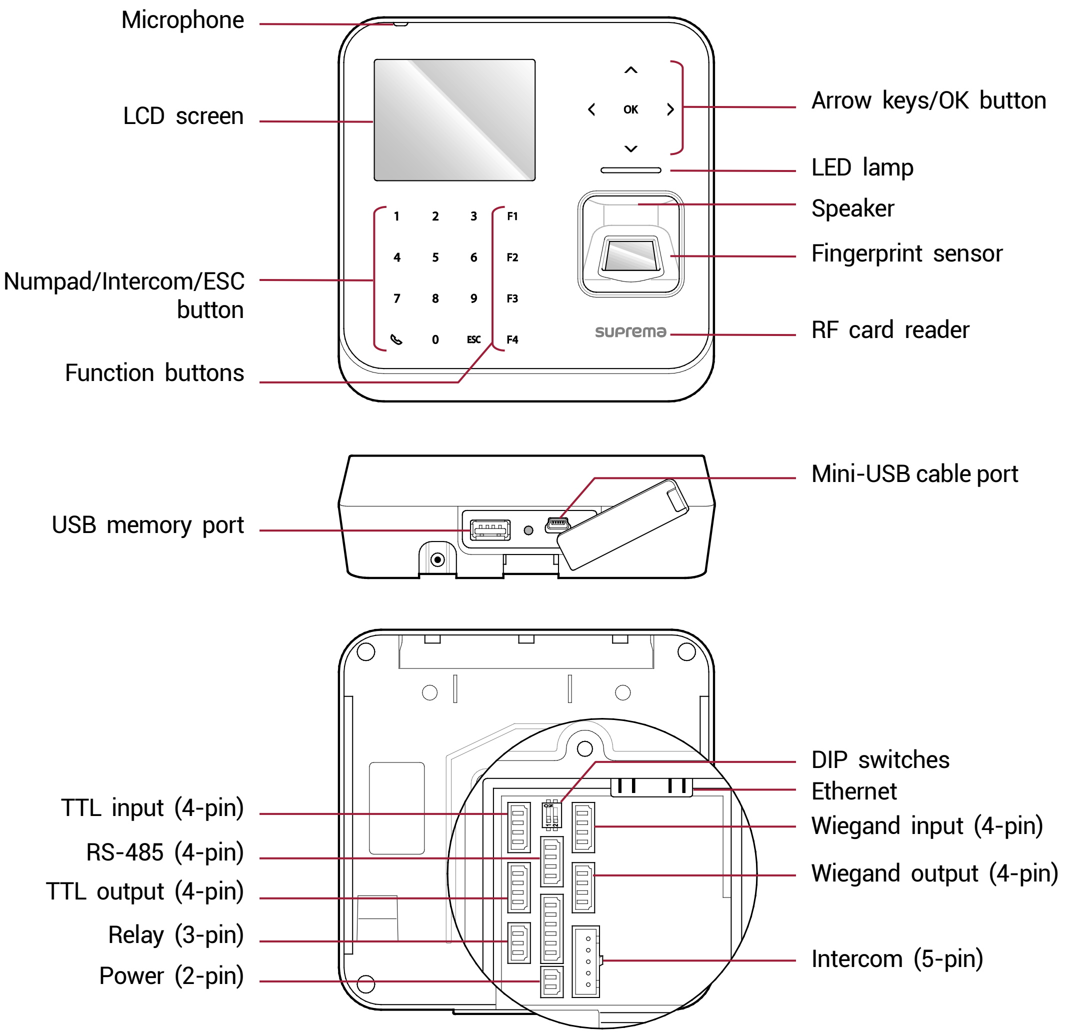


Quick Guide

NOTE

- The components may differ depending on where the product is installed.
- When assembling the product with the bracket, you can use the included bracket fixing screw(Star Shaped) instead of the product fixing screw for enhanced security.
- For more information on installation, visit the Suprema website (www.supremainc.com) to see the installation guide.

Parts

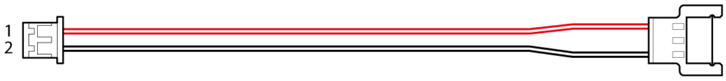


Name	Description
Microphone	Transmits the user's voice to the intercom.
LCD screen	Displays various information or settings.
Numpad/Intercom/ESC button	• **1** to **9**: Enters numbers/characters or selects a menu item. • ☎: Connects to the intercom. • **ESC**: Opens the menu, moves back to the previous screen, or cancels input
Function buttons	Serves as T&A function key or selects a sub-menu item.
Arrow keys/OK button	• ∧: Changes the character type. • ∨: Changes the character type or selects a T&A event. • <: Deletes numbers/characters. • >: Inserts symbols or configures an item. • **OK**: Selects an item or saves the settings.
Speaker	Makes a sound.
LED lamp	Shows the status of the product with different colors.
Fingerprint sensor	Reads fingerprints.

RF card reader	Reads RF cards.
USB memory port	Connects a USB memory stick.
Mini-USB cable port	To be supported later.
TTL input (4-pin)	Connects a TTL input/output cable.
RS-485 (4-pin)	Connects an RS-485 cable.
TTL output (4-pin)	Connects a TTL input/output cable.
Relay (3-pin)	Connects a relay cable.
Power (2-pin)	Connects the power cable.
DIP switch	Turns on the termination resistor for the RS-485 interface ● To use the termination resistor, set DIP switch 1 to ON.
Ethernet	Connects an Ethernet cable.
Wiegand input (4-pin)	Connects a Wiegand input/output cable.
Wiegand output (4-pin)	Connects a Wiegand input/output cable.
Intercom (5-pin)	Connects the intercom cable.

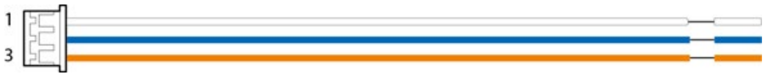
Cables and connectors

Power



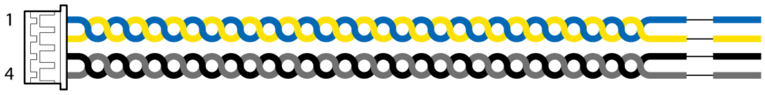
Pin	Name	Color
1	PWR +VDC	Red (White stripe)
2	PWR GND	Black (White stripe)

Relay



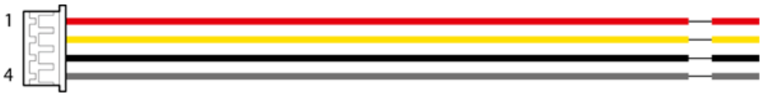
Pin	Name	Color
1	RLY NO	White
2	RLY COM	Blue
3	RLY NC	Orange

RS-485



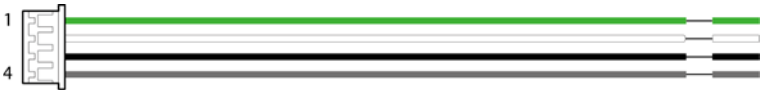
Pin	Name	Color
1	485 TRXP	Blue
2	485 TRXN	Yellow
3	485 GND	Black
4	SH GND	Gray

TTL input/output



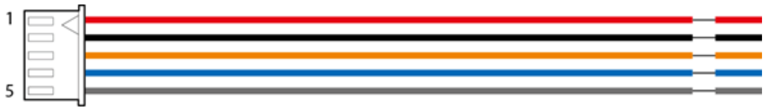
Pin	Name	Color
1	TTL IN0 / OUT0	Red
2	TTL IN1 / OUT1	Yellow
3	TTL GND	Black
4	SH GND	Gray

Wiegand input/output



Pin	Name	Color
1	WG IN0 / OUT0	Green
2	WG IN1 / OUT1	White
3	WG GND	Black
4	SH GND	Gray

Intercom



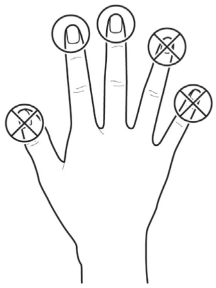
Pin	Name	Color
1	INPH +VDC	Red
2	INPH GND	Black
3	INPH AUD	Orange
4	INPH DTA	Blue
5	SH GND	Gray

How to Enroll a Fingerprint

Correct fingerprint enrollment is critical in improving fingerprint recognition. BioStation 2 is loaded with powerful fingerprint algorithm which is capable of recognizing a fingerprint even when the angle or position of the finger on the reader is not optimal. Nevertheless, enrolling a fingerprint with the following instructions can improve the recognition performance.

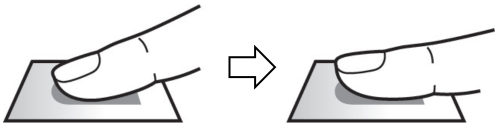
Choose Ideal Fingers to Enroll

- Each person can enroll up to ten fingerprints. If a finger is injured or scratched, it is recommended to use another finger.
- If the fingerprint recognition fails, you can enroll the same finger multiple times, which will improves the recognition performance.
- If a finger is injured or the fingerprint is not clear, please enroll a different finger.
- The index finger and middle finger are preferred for enrolling fingerprints. Other fingers may have a lower recognition rate because those fingers tend to have difficulty being placed at the center of the fingerprint sensor.



How to Enroll Fingerprints

1 When enrolling a fingerprint, the “Scan 1st finger” message will appear on the LCD screen. Place a finger on the fingerprint sensor, and then press softly in order to improve the recognition.



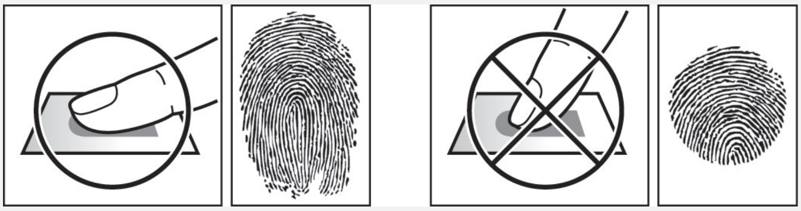
2 After a beep sounds, you will be notified to scan again then remove your finger and place it again to scan. (You are required to scan the same finger twice for enrollment.)

NOTE

Precautions for enrolling fingerprints

Enrolling fingerprints is the most important procedure because this device uses enrolled fingerprints to compare them with a scanned fingerprint. Please ensure the following when enrolling fingerprints:

- Place the finger firmly on the fingerprint sensor for it to be read completely.
- The center of the fingerprint should be placed at the center of the fingerprint sensor.
- If a finger is injured or the fingerprint is not clear, please enroll another finger.
- Follow the instructions on the screen and place the finger correctly without movement when the finger is read.
- Place your finger to completely cover the sensor with maximum surface.



When the fingerprint recognition fails

BioStation 2 can read fingerprints regardless of the change in seasons or condition of the fingers. However, the external environment or the finger's position can affect the recognition performance.

If the fingerprint recognition fails, the following actions are recommended.

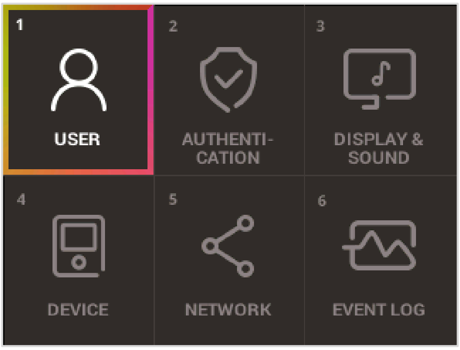
- If there is water or sweat on the finger, please wipe it off before scanning the finger.
- If the finger is too dry, please blow softly on the fingertip before scanning the finger.
- If the finger is injured, please enroll another finger.
- If the fingerprint recognition failure persists, please follow ‘**Precautions for enrolling fingerprints**’ to re-enroll the fingerprint.

Administrator Menus

Full Menu

1 Press the **ESC** button then authenticate as an administrator.

2 Select the desired menu item.



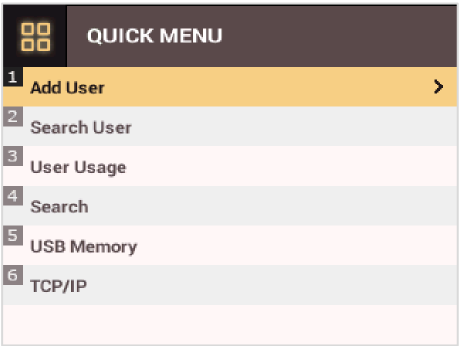
NOTE

- If there is no administrator on the device, anyone can access the menu just by pressing the **ESC** button.

Quick Menu

1 Press and hold the **ESC** button for more than one second and then release the button. Next, authenticate yourself as an administrator.

2 Select the desired menu item.



NOTE

- If there is no administrator on the device, anyone can access the quick menu just by pressing and holding the **ESC** button and then releasing the button.

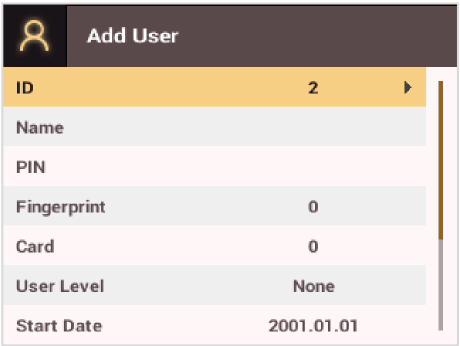
User Management

Add User Information

You can register the user information and fingerprints.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **USER** > **Add User** and press **OK**.



Add User

ID	2	▸
Name		
PIN		
Fingerprint	0	
Card	0	
User Level	None	
Start Date	2001.01.01	

3 Select an item then press the 〉 button. Press **OK** after configuring the item to register the user information.

- **ID**: Enter a number between 1 and 429467295 to register as the user ID. If **User ID Type** set to **Alphanumeric**, a combination of alphanumeric characters and symbols (_, -) can be used for the ID. Up to 32 characters can be input.
- **Name**: Enters the user name with the number buttons. Press the ⌃⌄ buttons to switch between letters and numbers. Press **F1**/**F2** to show more letters.
- **PIN**: Enters a PIN. Enter the PIN and press **OK**. Enter the PIN again to confirm it, then press the **OK** button. PIN numbers must be 4 to 16 digits to prevent leaking of the PIN.
- **Fingerprint**: Enrolls fingerprints for user authentication. After scanning the fingerprint of the registered finger, the same finger should be scanned one more time. Press the **ESC** button if you do not want to enroll a fingerprint.
- **Card**: Registers cards for user authentication. Scan the cards that you want to assign to users. Press the **ESC** button if you do not want to register another card.
- **User Level**: Selects the privileges to assign to the user. Use the 〈/〉 buttons to select the user level.
- **Start Date**: Sets the start date for the user account. Press the number buttons to enter the date. Use the 〈 button to delete the date. Use the 〉 button to enter a separator.
- **Expiration Date**: Sets the end date for the user account. Press the number buttons to enter the date. Use the 〈 button to delete the date. Use the 〉 button to enter a separator.
- **Security Level**: Sets the security level for 1:1 Authentication.
- **Duress**: Selects the index of the fingerprints to be used as duress fingerprints. This is available only when there are two or more registered fingerprints.
- **Private Auth Mode**: Changes the authentication mode for each user. Select a desired item and press the 〈/〉 buttons to change the settings.

NOTE

The available menus vary depending on the selected user level.

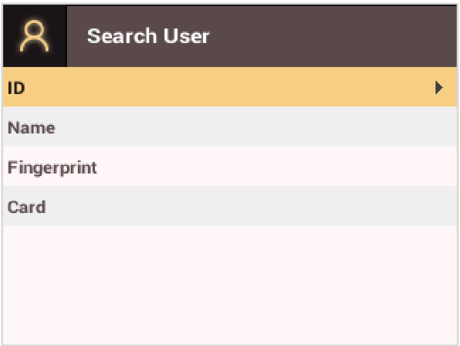
- **None**: Indicates the level for normal users who cannot use the menu.
- **Administrator**: The user can use all menus.
- **Configuration**: The user can use **AUTHENTICATION**, **DISPLAY & SOUND**, **DEVICE**, **NETWORK**, and **EVENT LOG** menus.
- **User Mgmt**: The user can use **USER** and **EVENT LOG** menus.

Edit User Information

Users with the user level of Administrator and User Mgmt can change user information. They can add fingerprints or a card for a user, and also change PIN numbers and access levels.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **USER** > **Search User** and press **OK**.



3 Select a search method and press the > button. You can search for users by **ID**, **Name**, **Fingerprint**, or **Card.**

- If you press **OK** without selecting a search method, a list of all users will be displayed.

4 Select the user you want to edit and press **F2**. Edit the information by referring to **Adding User Information**.

- Press **F3** and then the **OK** button to delete a user.

NOTE

- **Access Group** can be registered in BioStar 2. For more information on registering access groups, see the BioStar 2 Administrator Guide.

Delete All Users

You can delete all registered users.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **USER** > **Delete User**, then press **OK**.

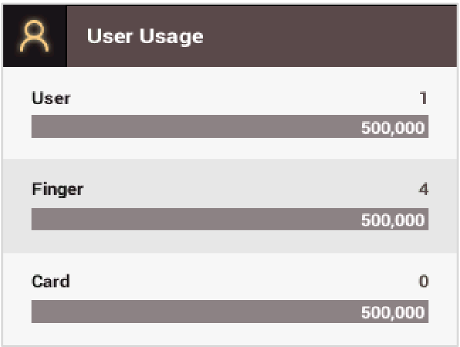
3 If you press **OK**, all registered users will be deleted.

Check User Usage

Shows the numbers of registered users, fingerprints, and cards.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **USER** > **User Usage**, then press **OK**.



User 1
500,000

Finger 4
500,000

Card 0
500,000

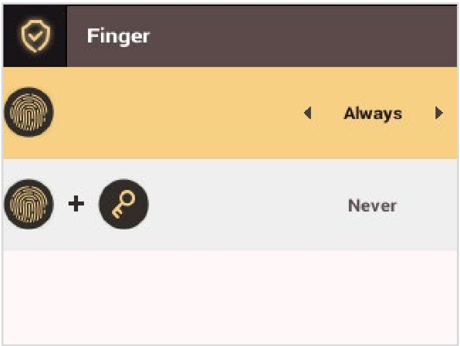
Authentication Configuration

Finger

A schedule can be configured for each authentication method using fingerprints.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **AUTHENTICATION** > **Finger**, then press **OK**.



Finger

◉ ◂ Always ▸

◉ + 🔑 Never

3 Select an item and press the ‹/› buttons to set a schedule.

- ◉: This mode only uses fingerprints.
- ◉ + 🔑: In this mode, a PIN must be entered after fingerprint authentication.

4 Press **OK** to save the settings.

NOTE

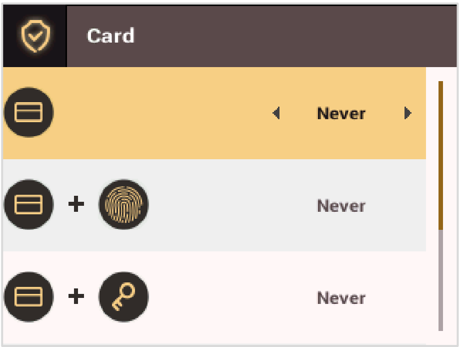
- You can configure a schedule in BioStar 2. You can select **Never** or **Always** if there is no configured schedule.
- For more information on configuring schedules, see the BioStar 2 Administrator Guide.

Card

A schedule can be configured for each authentication method using cards.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **AUTHENTICATION** > **Card,** then press **OK**.



Card

💳 ◂ Never ▸

💳 + ◉ Never

💳 + 🔑 Never

3 Select an item and press the ‹/› buttons to set a schedule.

- 💳: This mode only uses a card.
- 💳 + ◉: In this mode, fingerprint authentication is required after card authentication.
- 💳 + 🔑: In this mode, a PIN must be entered after card authentication.
- 💳 + ◉ / 🔑: In this mode, fingerprint authentication or entering a PIN is required after card authentication.
- 💳 + ◉ + 🔑: In this mode, both fingerprint authentication and entering a PIN are required after card authentication.

4 Press **OK** to save the settings.

NOTE

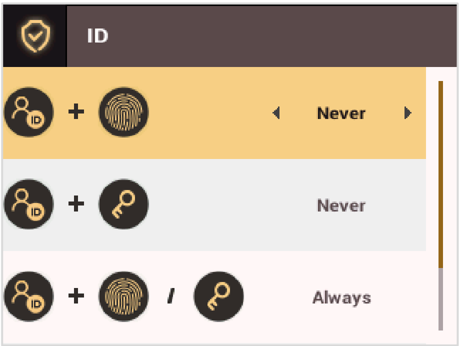
- You can configure a schedule with BioStar 2. You can select **Never** or **Always** if there is no configured schedule.
- For more information on configuring schedules, see the BioStar 2 Administrator Guide.

ID

A schedule can be configured for each authentication method using IDs.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **AUTHENTICATION** > **ID,** then press **OK**.



ID

ID + 👆 ◀ Never ▶

ID + 🔑 Never

ID + 👆 / 🔑 Always

3 Select an item and press the </> buttons to set a schedule.

- ID + 👆: In this mode, fingerprint authentication is required after entering an ID.
- ID + 🔑: In this mode, a PIN must be entered after entering an ID.
- ID + 👆 / 🔑: In this mode, fingerprint authentication or entering a PIN is required after entering an ID.
- ID + 👆 + 🔑: In this mode, both fingerprint authentication and entering a PIN are required after entering an ID.

4 Press **OK** to save the settings.

NOTE

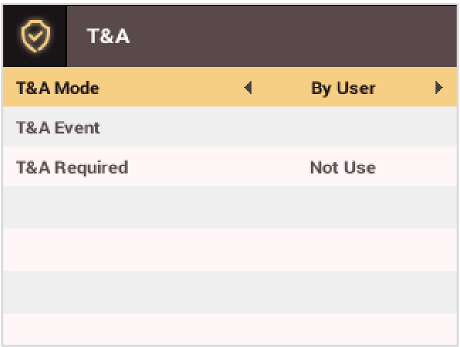
- You can configure a schedule with BioStar 2. You can select **Never** or **Always** if there is no configured schedule.
- For more information on configuring schedules, see the BioStar 2 Administrator Guide.

T&A Mode

You can select registration options for the T&A Mode.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **AUTHENTICATION** > **T&A Mode,** then press **OK.**



T&A

T&A Mode ◀ By User ▶

T&A Event

T&A Required Not Use

3 Select an item and configure the settings.

- **T&A Mode**: Selects how to use the T&A Mode.
- **T&A Event**: Checks T&A Events.
- **T&A Required**: Selects the registration option for the T&A Mode. If **Use** is selected, you can set the T&A Event as a required option to select during authentication.

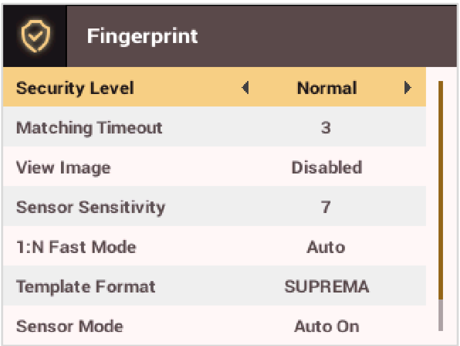
4 Press **OK** to save the settings.

Fingerprint

You can configure the fingerprint authentication settings.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **AUTHENTICATION** > **Fingerprint,** then press **OK**.



Fingerprint

Security Level	◀ Normal ▶
Matching Timeout	3
View Image	Disabled
Sensor Sensitivity	7
1:N Fast Mode	Auto
Template Format	SUPREMA
Sensor Mode	Auto On

3 Select an item and press the </> buttons to change the settings.

- **Security Level**: Configures the security level for 1:N Authentication.
- **Timeout**: Sets a timeout period. If the authentication is not completed within the set time, the authentication fails.
- **View Image**: You can view the original image when a fingerprint is scanned.
- **Sensor Sensitivity**: Sets the sensitivity level of the fingerprint reader sensor. Set the sensor sensitivity high if you wish to use a higher sensor sensitivity level and obtain more detailed fingerprint information.
- **1:N Fast Mode**: Sets the fingerprint authentication speed. Select **Auto On** to have the authentication speed configured according to the total fingerprint templates enrolled on the device.
- **Template Format**: Sets the fingerprint template format. The default format is SUPREMA. Be careful when changing the template format as it can render all previously stored fingerprints unusable.
- **Sensor Mode**: If **Auto On** is selected, the fingerprint sensor detects if a finger is present. And the sensor is on while the finger is present on the sensor. If **Always On** is selected, the fingerprint sensor is always on.
- **Advanced Enrollment**: You can check the quality of a scanned fingerprint to save high quality fingerprint data. If **Enabled** is selected, the user will be notified when the fingerprint quality is low. This helps users to scan the fingerprints correctly.
- **Duplicate Check**: When registering fingerprints, you can check duplicates.

4 Press **OK** to save the settings.

NOTE

- Change the template type after deleting all user fingerprint information. If there is any user fingerprint information stored on the device, the template type cannot be changed.

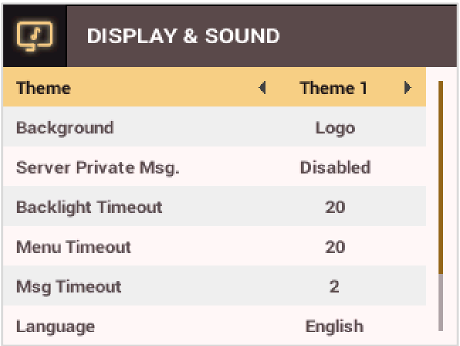
System Setup

Display & Sound

You can configure the display and sound settings on the device.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **DISPLAY & SOUND,** then press **OK**.



DISPLAY & SOUND

Theme	◀ Theme 1 ▶
Background	Logo
Server Private Msg.	Disabled
Backlight Timeout	20
Menu Timeout	20
Msg Timeout	2
Language	English

3 Select an item and press the </> buttons to change the settings.

- **Theme**: Changes the style of the home screen.
- **Background**: Selects items to display on the home screen background.
- **Server Private Msg.**: Set whether or not to use a Private Message, which will be displayed on the screen when the user authenticates.
- **Backlight Timeout**: Configures how long (in seconds) the LCD screen light stays on.
- **Menu Timeout**: Configures the time (in seconds) for the menu screen to automatically disappear. If there is no button input for the specified period, the display goes back to the home screen.
- **Msg Timeout**: Configures the time (in seconds) for the configuration completion message or notification message to automatically disappear.
- **Language**: Selects the language to use.
- **Voice Instruction**: You can use voice instructions instead of beep.
- **Volume**: Adjusts the volume.

NOTE

- You can set the **Server Private Msg.** on the server. If you have not set it on the server, the device does not display a message when authentication is successful even if **Server Private Msg.** is **enabled** on the device.

4 Press **OK** to save the settings.

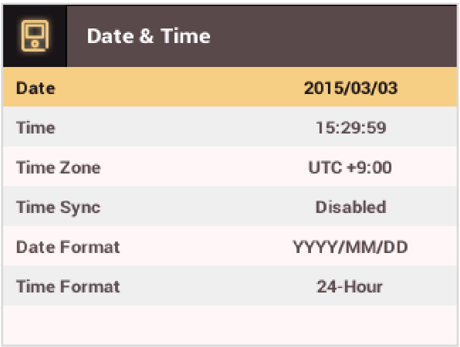
Device

Date & Time

You can configure the date and time settings. Be sure to correctly configure the settings to collect accurate log data.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **DEVICE** > **Date & Time,** then press **OK**.



Date & Time	
Date	2015/03/03
Time	15:29:59
Time Zone	UTC +9:00
Time Sync	Disabled
Date Format	YYYY/MM/DD
Time Format	24-Hour

3 Select an item and press the </> buttons to change the settings.

- **Date**: Sets the current date. Press the number buttons to enter the date.
- **Time**: Sets the current time. Press the number buttons to enter the time.
- **Time Zone**: Sets the time zone for your area.
- **Time Sync**: Synchronizes the time with the server. To synchronize the time with the server, select **Use**.
- **Date Format**: Selects the date format. You can select from among the **YYYY/MM/DD**, **MM/DD/YYYY**, or **DD/MM/YYYY** formats.
- **Time Format**: Selects the time format. You can select from among the **24 hour** or **12 hour (AM/PM)** formats.

NOTE

- Press the number buttons to enter the **date** and **time**. Use the < button to delete the values entered. Use the > button to enter a separator.

Daylight Saving Time

You can use the device by applying daylight saving time. Set the start and end time correctly.

1 Press **ESC** and authenticate with the Admin level credential.

2 Select **DEVICE** > **Daylight Saving Time**, then press **OK**.

3 Select an item and press the </> buttons to change the settings.

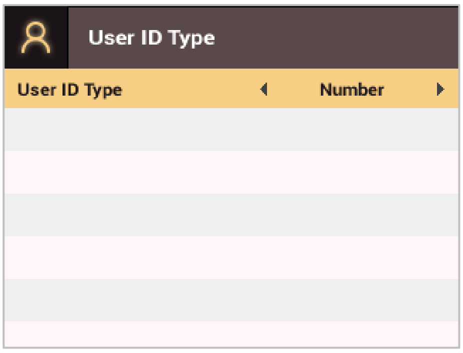
4 To save settings, press **OK**.

User ID Type

You can set the type of user ID to be registered on the device to Number or Alphanumeric characters.

1 Press **ESC** and authenticate with the Admin level credential.

2 Select **DEVICE** > **User ID Type**, then press **OK**.



User ID Type

User ID Type ◀ Number ▶

3 Press the </> buttons to change the settings.

4 To save settings, press **OK**.

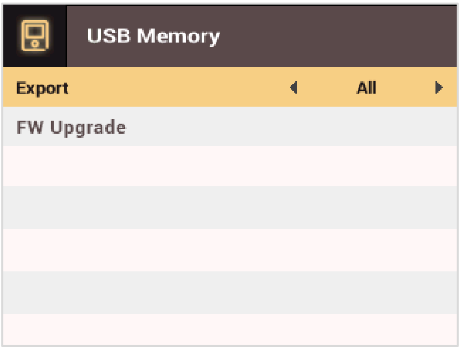
5 Press **OK** to save the settings.

USB Memory

By connecting a USB memory stick, you can import or export the log, data and configurations data to or from the USB memory stick and upgrade the firmware.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **DEVICE** > **USB Memory,** then press **OK**.



USB Memory

Export ◀ All ▶

FW Upgrade

3 Select an item and change the settings.

- **Export**: Selects data to export to the connected USB memory stick. Press the </> buttons to select an item and press **OK**.
- **FW Upgrade**: If there are firmware files stored on the USB memory stick, select the firmware file to use and press **OK** to upgrade the firmware.

NOTE

Supported USB memory sticks are as follows. If you use other memory sticks, they may not work properly.

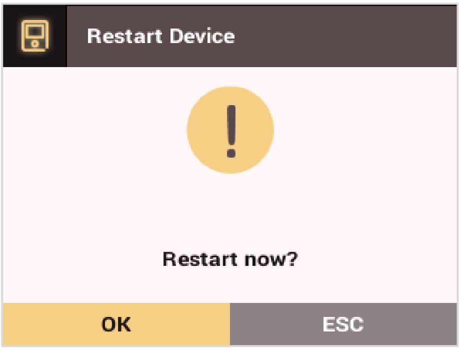
- Samsung Electronics: SUM-LSB 8 GB, SUM-PSB 8 GB, SUM-PSB 16 GB, and SUM-BSG 32 GB
- LG Electronics: XTICK J3 WINDY 8 GB, SMART USB MU1 White 8 GB, MU 1 USB 32 GB, MU28GBC 32 GB, XTICK MOBY J1 16 GB
- SanDisk: Cruzer 16 GB, Cruzer Blade CZ50 4 GB, Cruzer Blade CZ50 32 GB, CZ48 Ultra USB 3.0 64 GB, CZ80 USB3.0 64 GB, CZ52 64 GB, Cruzer Glide Z60 128 GB, Cruzer Force CZ71 32 GB
- Sony: Micro Vault Click 8 GB, MicroVault CLICK 16 GB, USM-SA1 32 GB
- Transcend: JetFlash 760 8 GB, JetFlash 760 32 GB, JetFlash 500 8 GB
- Memorette: MINI500 8 GB
- A-DATA: S102 PRO 8 GB
- TriGem: Pastel 8 GB

Restart Device

The user can restart the device.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **DEVICE** > **Restart Device,** then press **OK**.



3 Press **OK** to restart the device. Press **ESC** to cancel.

Restore Default

Device settings, network settings, and operator levels will be reset.

1 Press the **ESC** button then authenticate as an administrator.

2 Go to **DEVICE** > **Restore Default**, then press OK.

- **Reset All Settings**: You can reset all settings stored on the device. Press **OK** to reset all device settings. To cancel, press **ESC**.
- **Reset without Network Settings**: You can reset all settings except network settings. Press **OK** to reset all settings except netwo rk settings. To cancel, press **ESC**.
- **Factory Default**: You can delete all the information saved in the device and the root certificate and restore default settings.
- **Delete the Root Certificate**: You can delete the root certificate saved in the device.

3 If you proceed to restore the defaults, the device will restart.

NOTE

- When you reset, the operator level will be reset as well. After resetting, make sure to set the operator level again.
- Language setting will not change after resetting.
- **Factory Default** menu can be used when the root certificate is saved in the device.
- **Delete the Root Certificate** menu can be used only when the root certificate is saved in the device and Administrator has been designated.

More Settings

Relay

You can set the open time and the input port of the exit button in the device. This option is useful when the device is used as a standalone.

1 Press **ESC** and authenticate with the Admin level credential.

2 Select **DEVICE** > **Relay**, then press **OK**.

- **Relay**: You can set whether relay is enabled or not. To set the open time and the input port of the exit button, set to **Enabled**.
- **Open Time**: Set the duration for the door to remain open when standard user authentication has been carried out.
- **Exit Button**: Select the input port where the exit button is connected.

3 To save settings, press **OK**.