www.supremainc.com

USER GUIDE

BioStation 2

English

Version 1.3

EN 102.00.BS2 V1.30A

Contents

ААМ СИСТЕМЗ системы технической безопасности

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 approximately 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.

ААМ СИСТЕМЗ системы технической безопасности

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.

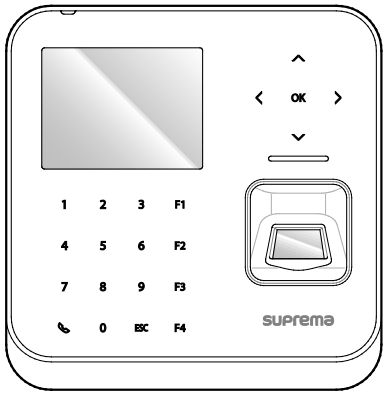
- This can cause a product failure.

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.

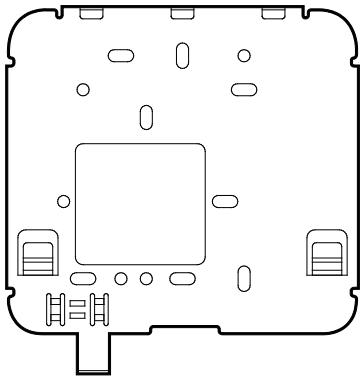
There is a risk of fire if batteries are replaced by an incorrect type.
Dispose of batteries in accordance with local and national disposal regulations.

Getting Started

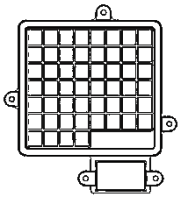
Components



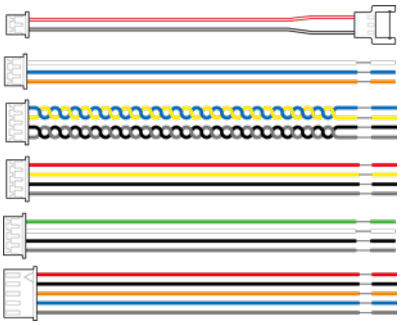
BioStation 2



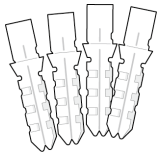
Wall bracket



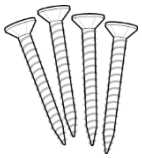
Cable cover



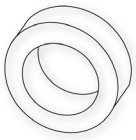
Connector cables
(1x2-pin, 1x -pin3, 3x4-ping, 1x5-pin)



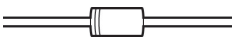
PVC anchors
(4)



Fixing screws
(4)

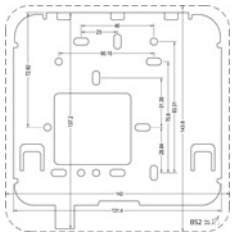


Ferrite core
(1)

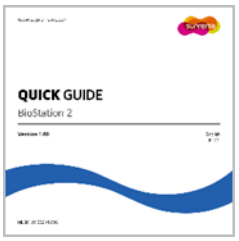


Diode
(1)

Allen Key
(For bracket)



Drilling Template



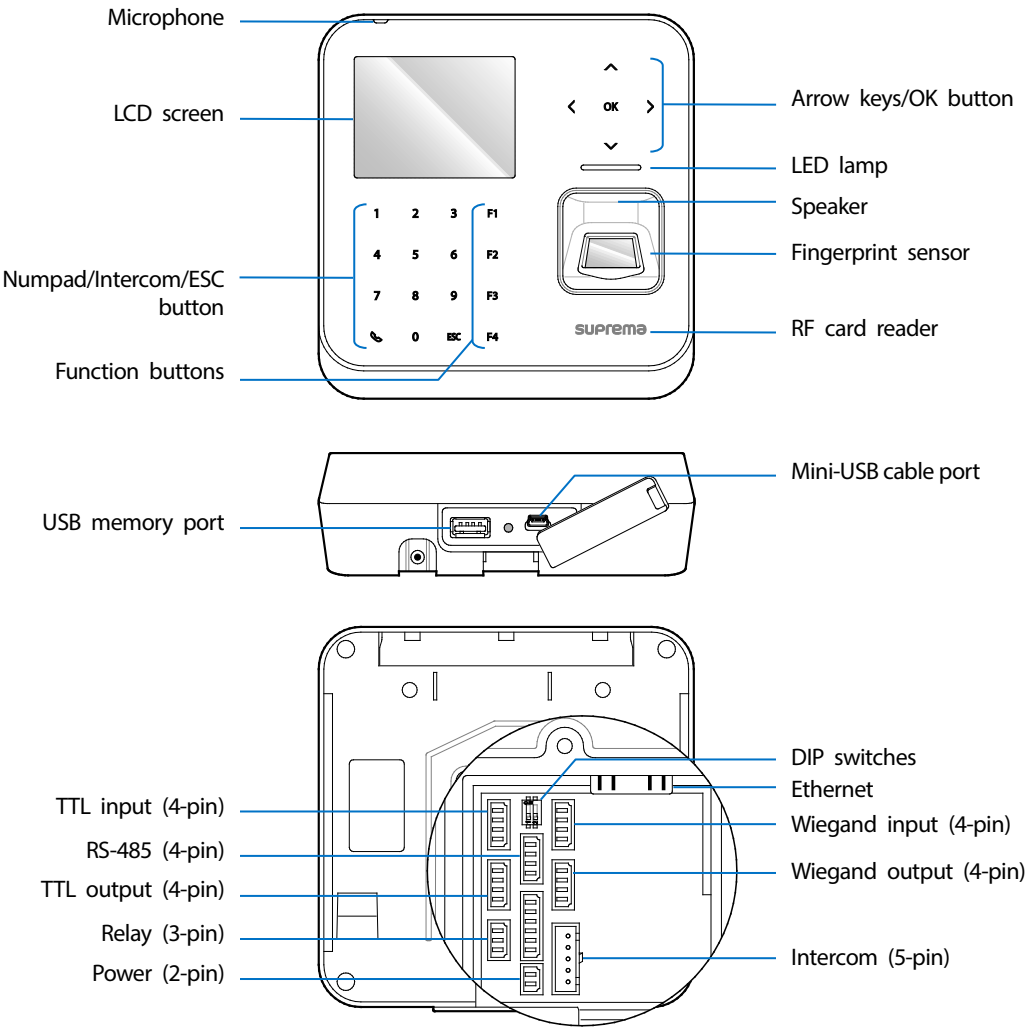
Quick Guide

Notes

- The components may differ depending on where the product is installed.
- For more information on installation, visit the Suprema website (www.supremainc.com) to see the installation guide.

ААМ СИСТЕМЗ

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. • v: 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

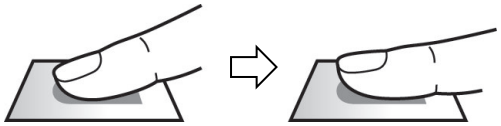
Correct fingerprint enrollment is critical in improving fingerprint recognition. BioStation 2 is loaded with powerful fingerprint algorithm which is capable of recognizing a fingerprint even when the angle or position of the finger on the reader is not optimal. Nevertheless, enrolling a fingerprint with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

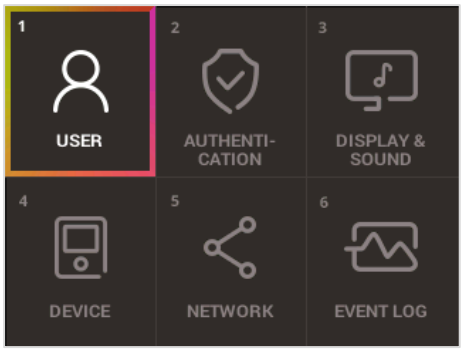
- If there is water or sweat on the finger, please wipe it off before scanning the finger.
- If the finger is too dry, please blow softly on the fingertip before scanning the finger.
- If the finger is injured, please enroll another finger.
- If the fingerprint recognition failure persists, please follow '**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.



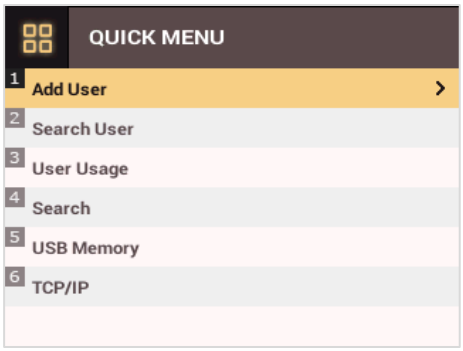
Note

- 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.

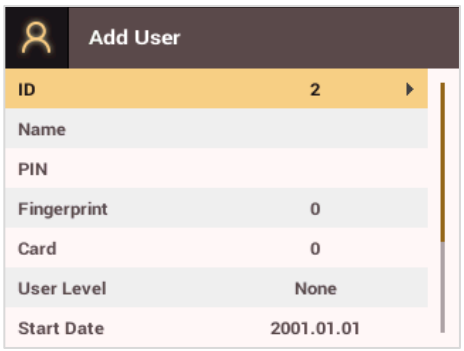
User Management

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**.



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

- **ID**: Enters the User ID to be registered. Press OK after entering the ID with the number buttons. An ID must be a number in the range of 1 to 4294967295.
- **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

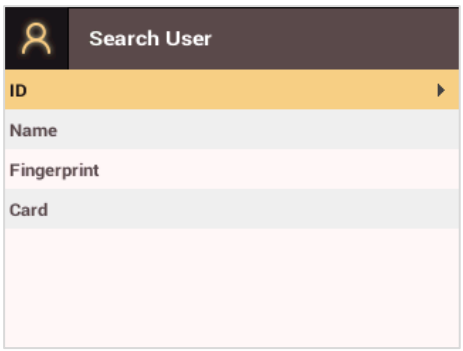
The available menus vary depending on the selected user level.

- **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

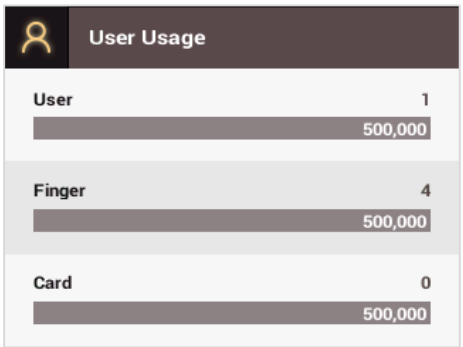
You can delete all registered users.

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**.

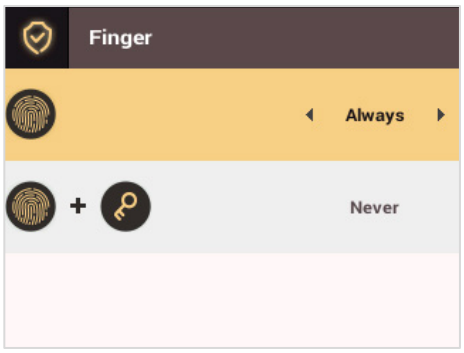


Authentication Configuration

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**.



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.

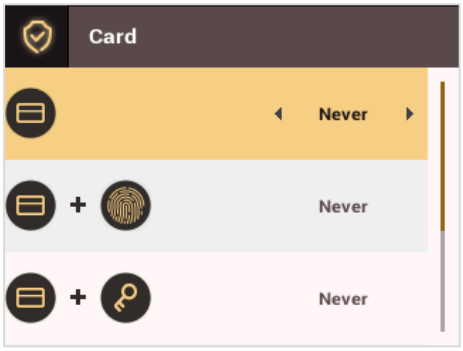
Note

- 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**.



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.

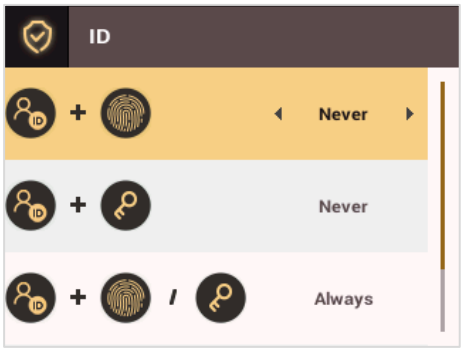
Note

- 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**.



3. Select an item and press the </> buttons to set a schedule.
   - + : In this mode, fingerprint authentication is required after entering an ID.
   - + : In this mode, a PIN must be entered after entering an ID.
   - + / : In this mode, fingerprint authentication or entering a PIN is required after entering an ID.
   - + + : In this mode, both fingerprint authentication and entering a PIN are required after entering an ID.
4. Press **OK** to save the settings.

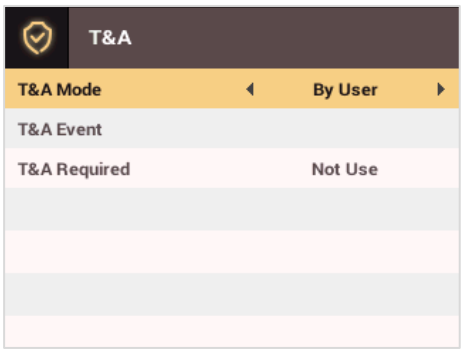
Note

- 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**.



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.

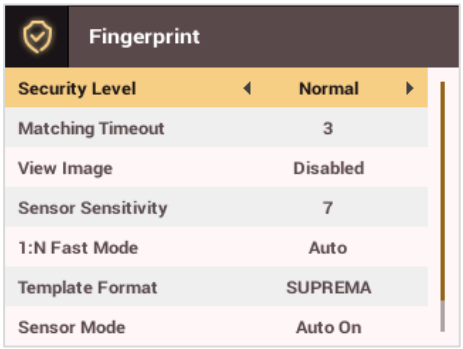
4 Press **OK** to save the settings.

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**.



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.

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.

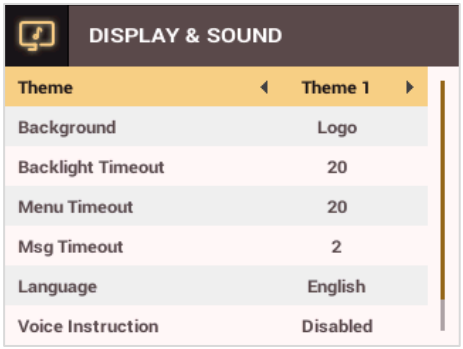
System Setup

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**.



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.
- **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.

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

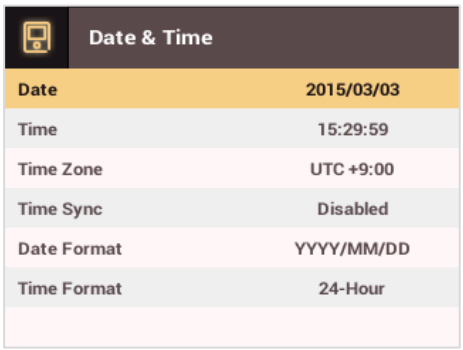
Device

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**.



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.

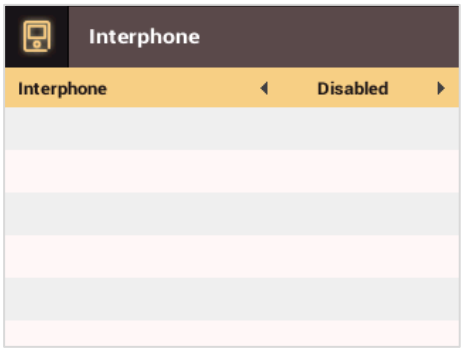
Note

- 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.

Intercom

You can select whether or not to use the intercom.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **DEVICE** > **Interphone,** then press **OK**.



3. When the intercom is connected, press the </> buttons to select **Enabled**.
4. Press **OK** to save the settings.

Device Info

Shows the model name, device ID, FW version, and MAC address.

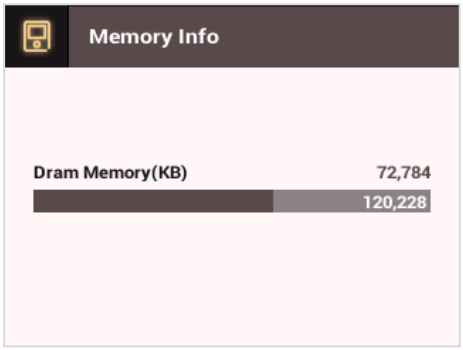
1. Press the **ESC** button then authenticate as an administrator.
2. Go to **DEVICE** > **Device Info,** then press **OK**.
   - Shows the model name, device ID, HW / FW / Kernel versions and Ethernet/WiFi MAC addresses.
3. Check the device information and press **OK**.

Memory Info

Shows the memory usage status.

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

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



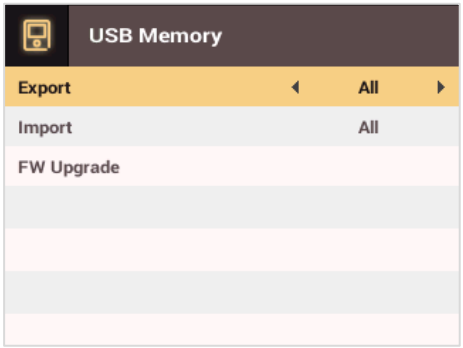
3 Check the memory information and press OK.

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**.



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**.
- **Import**: Selects data to import from 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

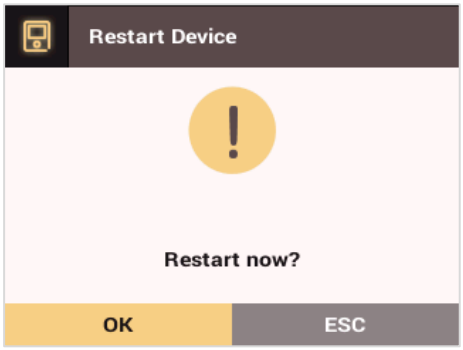
Supported USB memory sticks are as follows. If you use other memory sticks, they may not work properly.

- 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**.

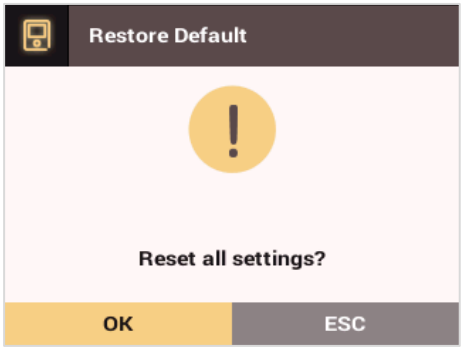


3. Press **OK** to restart the device. Press **ESC** to cancel.

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**.



3. Press **OK** to reset all the device settings. Press **ESC** to cancel.

Note

- If you reset the device, the user levels will be reset as well. Be sure to configure the user level settings after resetting the device.
- The language settings do not change even if you reset the device.

Factory Default

This will delete all data and root certificate on the device and reset the settings.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **DEVICE** > **Factory Default**, then press **OK**.
3. Press **OK** to restore the factory defaults. Press **ESC** to cancel.

Note

- You can only use **Factory Default** when the root certificate is stored on the device..

Delete the Root Certificate

This will delete the root certificate on the device.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **DEVICE** > **Delete the Root Certificate**, then press **OK**.
3. Press **OK** to delete the root certificate. Press **ESC** to cancel.

Note

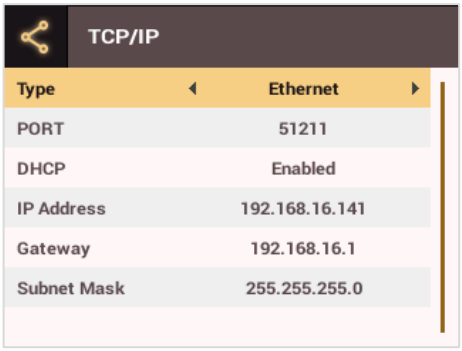
- You can only use **Delete the Root Certificate** when the root certificate is stored on the device and device administrator is set.

Network

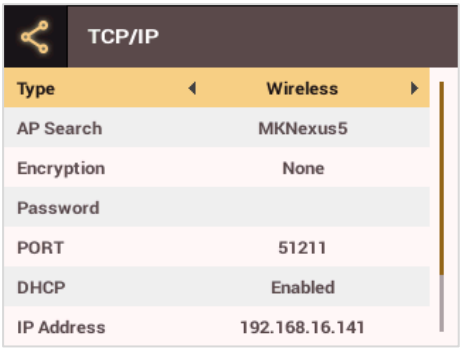
TCP/IP Settings

You can configure the network settings for the device.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **NETWORK** > **TCP/IP** then press **OK**.
3. Press the </> buttons to select a **Type** then select an item. You can select **Ethernet** or **Wireless**.



- **Port**: Enter the port number of the device.
- **DHCP**: Select whether or not to use DHCP. If **Disabled** is selected, the user can modify **IP Address**, **Gateway**, and **Subnet Mask**.
- **IP Address**: Enter the IP address of the device.
- **Gateway**: Enter the gateway address of the device.
- **Subnet Mask**: Enter the subnet mask address of the device.



- **AP Search**: Select the AP to connect to.
- **Encryption**: Shows the encryption method of the AP.
- **Password**: Enter the AP login password.
- **Port**: Enter the port number of the device.
- **DHCP**: Select whether or not to use DHCP. If **Disabled** is selected, the user can modify the **IP Address**.
- **IP Address**: Enter the IP address of the device.

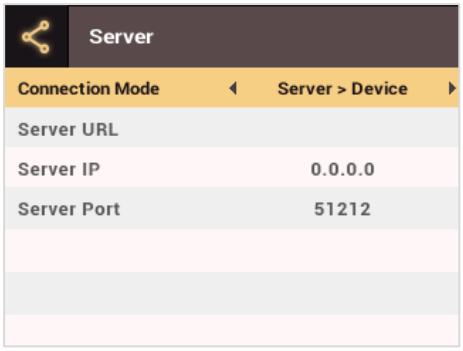
4. Press **OK** to save the settings.

Notes

- Press the number buttons to enter the IP address, gateway address, and subnet mask address. Use the < button to delete the values entered. Use the > button to enter a separator.
- To use **Wireless**, you need a wireless router. For more information on installing and configuring the wireless router, see the manual of the wireless router.

Server Settings

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **NETWORK** > **Server** then press **OK**.



3 Select an item and change the settings.

- **Connection Mode**: Select **Device > Server** to send the connect signal from the device directly to the server. If **Server > Device** is selected, **Server IP** and **Server Port** address cannot be entered.
- **Server URL**: Enter the BioStar 2 server's URL instead of **Server IP**. You can enter the values when **Device > Server** is selected for **Connection Mode**.
- **Server IP**: Enter the IP address of the PC where BioStar 2 is installed. You can enter the values when **Device > Server** is selected for **Connection Mode**.
- **Server Port**: Enter the port address of the PC with BioStar 2 installed. You can enter the values when **Device > Server** is selected for **Connection Mode**.

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

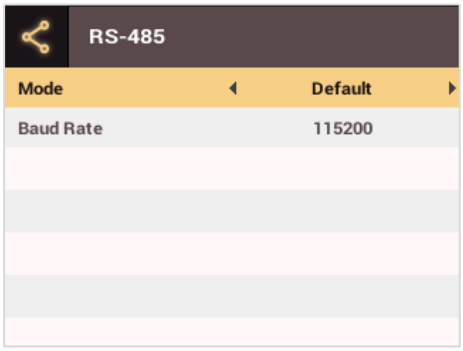
Notes

- Press the number buttons to enter the values for **Server IP** and **Server Port**. Use the < button to delete the values entered. Use the > button to enter a separator.

RS-485 Settings

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

2 Go to **NETWORK** > **RS-485** then press **OK**.



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

- **Mode**: Select RS-485 mode.
- **Baud Rate**: Select a baud rate.

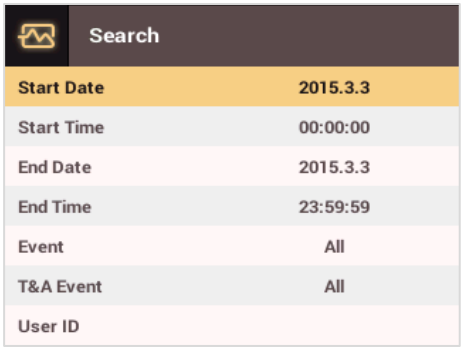
4 Press **OK** to save the settings.

Check Event Log

Search Logs

You can search logs after setting the condition.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **EVENT LOG** > **Search** then press **OK**.

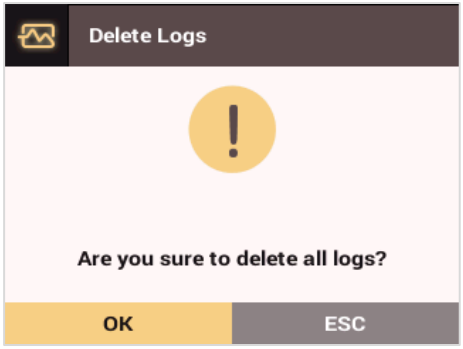


3. Select an item and press the </> buttons to change the condition. If you press **OK**, matching logs will be displayed on the screen.
4. Press **ESC** to return to the previous screen.

Delete All Logs

You can delete all logs stored on the device.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **EVENT LOG** > **Delete All** then press **OK**.

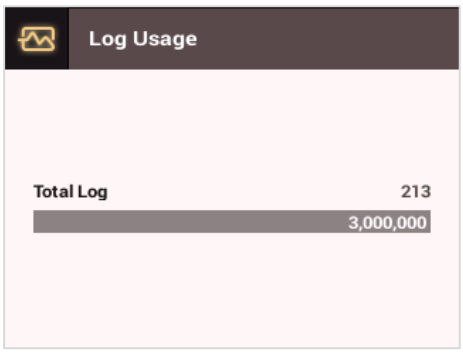


3. Press **OK** to delete all logs. Press **ESC** to cancel.

Check Log Usage

Shows the status of the log usage.

1. Press the **ESC** button then authenticate as an administrator.
2. Go to **EVENT LOG** > **Log Usage** then press **OK**.



3. Press **OK** after checking the log usage.

Troubleshooting

Checklist Before Requesting Service

Category	Problem	Possible Causes & Remedy
Power	Power is supplied to the device, but the device does not work.	• If the terminal is apart from the bracket, it may not work due to the tamper switch. • Check the adapter or power connection cable.
PIN	I've lost my PIN.	• For a normal user's PIN, contact your administrator and then enter the PIN again. • If an administration's PIN is lost, contact your installer.
	I cannot open a locked door when I enter a PIN and then press the **OK** button.	• Check whether the registered PIN is entered correctly. • Check whether the PIN has recently been changed. • If you cannot find the PIN, contact your administrator to change the PIN.
Fingerprint	A fingerprint is enrolled successfully, but the fingerprint recognition fails too often.	• Refer to '**How to Register Fingerprints**', and then enroll the fingerprint again. • Since there are variations in recognition rates due to the different characteristics of each fingerprint, please try to enroll another fingerprint. • If there are many number of enrolled fingerprints, change the **Matching Timeout** setting and then try again. • If a finger is injured, the finger may be recognized as another person's finger.
	The fingerprint recognition does not work.	• Check whether the finger or the fingerprint sensor has sweat, water, or dust on it, and then wipe it clear. • Try again after clearing the finger and the fingerprint sensor with a dry cloth. • If the finger is too dry, try again after blowing gently on the finger.
	The fingerprint sensor does not turn on.	• When **Sensor Mode** set to **Auto On**, the fingerprint sensor detects if a finger is present. And the sensor is on while the finger is present on the sensor. If you want to keep the fingerprint sensor on, go to **AUTHENTICATION** > **Fingerprint** > **Sensor Mode** and then select **Always On**.
Door lock	The lock does not work when the door is closed.	• The electric lock may have a problem. Ask your installer to examine it.
Time	The time displayed on the device is not correct.	• Even though BioStation 2 includes an internal battery, the time could become incorrect due to the discharge of the internal battery if power has not been applied to the system for a long time. Refer to **Date & Time** to adjust the time.
Administrator Connection	The administrator mode cannot be accessed due to losing the administrator PIN.	• Since BioStation 2 administrators are in charge of permitting the right of entrance, only the administrators can access the menu. • If the administrator menu cannot be accessed, it is possible to get a PIN issued in accordance with a predefined procedure. Ask your installer about the procedure to issue a password.

Product Specifications

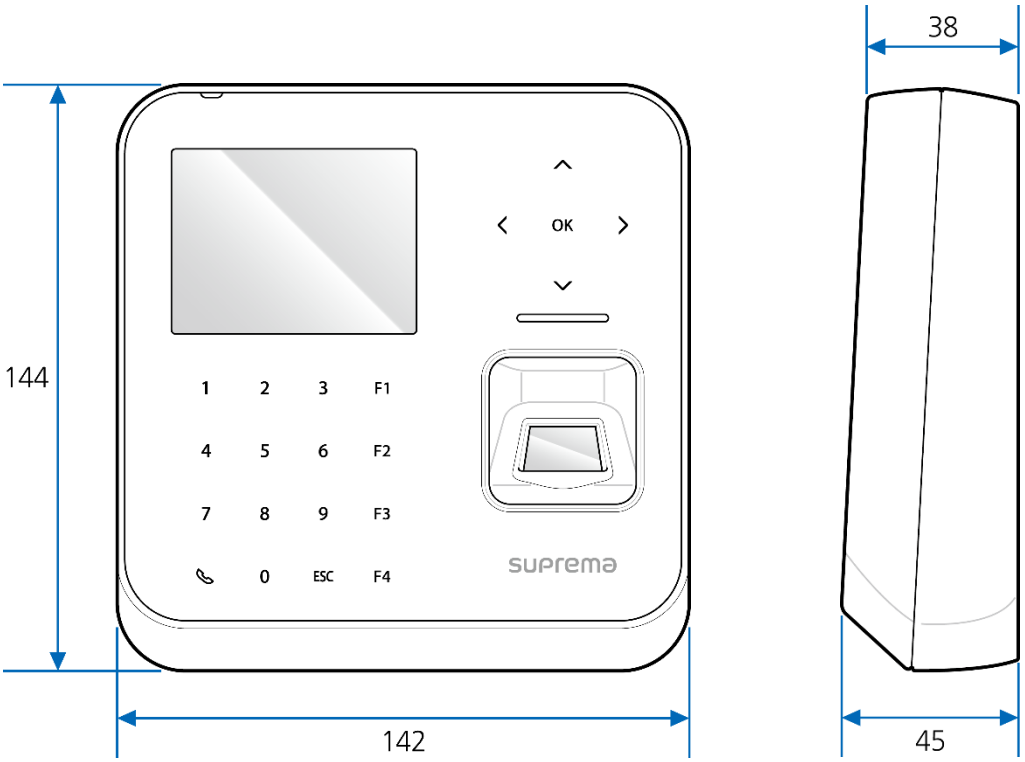
Category	Feature	Specification
Main	Biometric	Fingerprint
	IP Rating	IP 65
	RF Option*	• BS2-OMPW: 13.56Mhz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, NFC, ISO14443A, ISO15693 • BS2-OIPW: 13.56MHz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, iCLASS SE/SR, NFC, ISO14443A/B, ISO15693 • BS2-OHPW: 125kHz HID Prox • BS2-OEPW: 125kHz EM
Capacity	Max. User (1:1)	500,000
	Max. User (1:N)	20,000
	Max. Template (1:1)	1,000,000
	Max. Template (1:N)	40,000
	Max. Text Log	3,000,000
Interface	Wi-Fi	Yes
	TCP/IP	Yes
	RS-485	1ch Host or Slave (Selectable)
	RS-232	Yes
	Wiegand	1ch Input, 1ch Output
	TTL Input	2ch Inputs, 2ch Outputs
	Relay	1 Relay
	USB	USB 2.0 (Host)
Relay	Voltage	Max. 24VDC
	Current	0.5A, Max. 1.A
Hardware	CPU	1.0 GHz
	Memory	8GB Flash + 128 MB RAM
	LCD	2.8" QVGA Color LCD
	LED	Multi-Color
	Sound	16-bit Hi-Fi
	Operating Temp.	-20°C ~ 50°C
	Tamper	Yes
	Power	9V ~ 18V
	PoE	Optional
	Dimensions (W x H x D mm)	142 x 144 x 45(38)
	Certificates	CE, FCC, KC, RoHS, REACH, WEEE

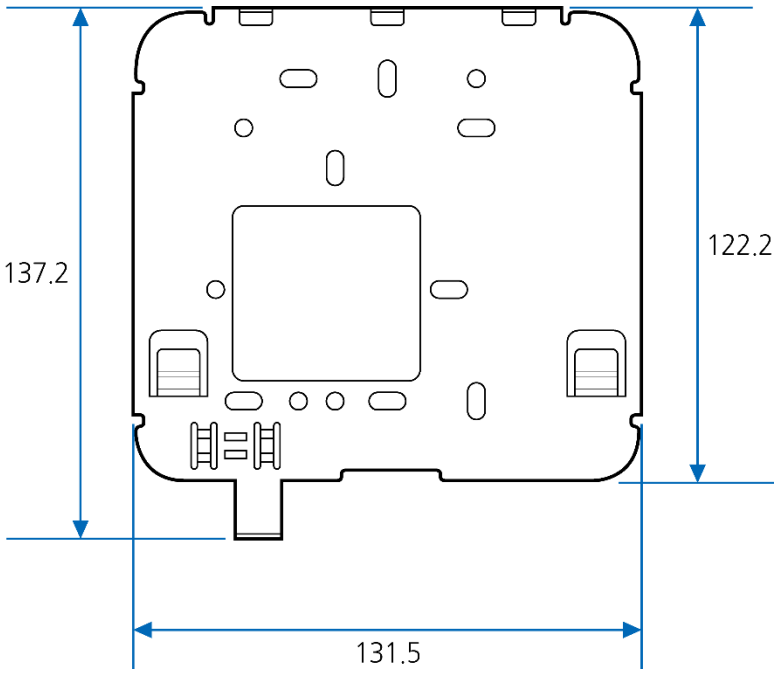
* For detailed information on our supported card list, contact Suprema technical support team at support@supremainc.com.

ААМ СИСТЕМЗ системы технической безопасности

Dimensions

(Unit: mm)





FCC Compliance Information

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

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications of the product not expressly approved by the manufacturer could void the user's authority to operate the equipment according to the FCC Rules.

This appliance and its antenna must not be co-located or operation in conjunction with any other antenna or transmitter.
A minimum separation distance of 20 cm must be maintained between the antenna and the person for this appliance to satisfy the RF exposure requirements.

Appendix

Disclaimers

- The information contained in this Guide is provided in regard to the Suprema product.
- Your right of usage is recognized only for products included in sales agreements and conditions guaranteed by Suprema. No license rights over other intellectual properties mentioned in this Guide are recognized.
- Suprema makes no representations or warranties concerning infringement of patents, copyrights or other intellectual property rights as well as merchantability and fitness of the product for a particular purpose in regard to the sale or use of the Suprema product.
- Do not use the Suprema product in medical, life-saving and life-sustaining situations or in situations where malfunction of the product could lead to personal injury or loss of life. However, if an accident occurs while the purchaser is using the product in any of the situations stated above, even if shortcomings are discovered in the design or production process of the product and are claimed as a point of major negligence, employees, subsidiaries, branches, affiliates, or distributors of Suprema shall not be liable and shall not make reimbursements for any direct or indirect costs or expenses associated, including lawyer fees.
- Suprema may change the product standards and specifications at any time without any adequate notice for improvements in stability, performance or design of the product. Designers should keep in mind that features or descriptions marked as "to be implemented" or "to be defined" are always subject to change. Suprema will implement or define such features or descriptions in the near future and shall not be liable for any consequential problems, including problems of compatibility.
- If you wish to obtain the latest specification documentation before you place an order for the product, please contact Suprema, a sales agent of Suprema, or a regional distributor.

Copyright Notice

Suprema owns the copyright for this document. The rights of other product names, brands, and trademarks belong to the individuals or organizations who own them.

ААМ СИСТЕМЗ системы технической безопасности

www.supremainc.com

Suprema Inc. 16F Parkview Office Tower, Jeongja-dong, Bundang-gu Seongnam, Gyeonggi, 463-863 Korea
Tel) +82-31-783-4502 Fax) +82-31-783-4503
Sales information sales@supremainc.com **Technical support** support@supremainc.com