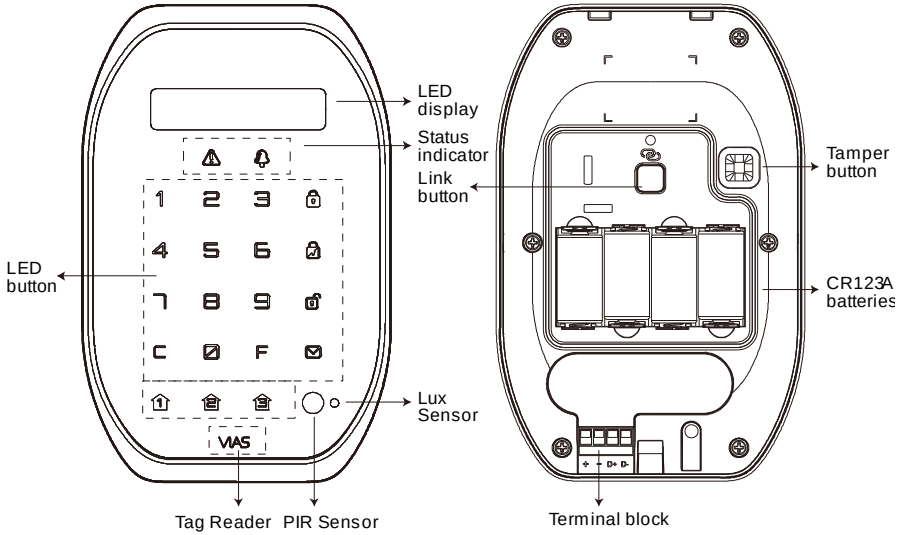
SK202 NFC LCD Keypad

SK202 is a wireless touch keypad for managing the Everspring alarm eco-system with encrypted contactless tag/card. The keypad manages security mode using PIN code and NFC tags/cards. It displays the current security mode with LCD panel and LED indicator.

Main Features

- LCD screen and LED indicator
- MIFARE DESFire NFC tag/card supported
- Touchpad input
- Built-in buzzer for alarm
- Dual power supply mode
- Wakes up by motion sensor
- Display room and zone names
- Customized scene hotkey
- IP54 for sheltered outdoor installation

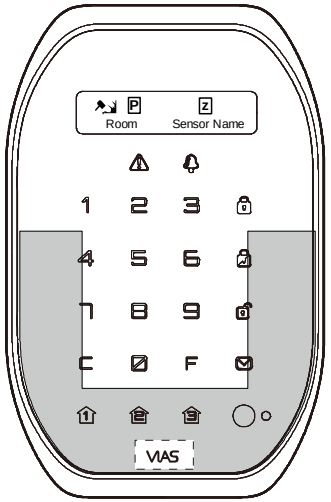
Product Layout



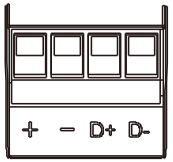
Front view Rear view

- LCD display: The visible interface used to display the alarm system status and interaction with user.
- LED Status indicator: Displays tamper, fault, or alarm conditions.
- LED button: Touch buttons that provide visibility in the dark environment.
- Tag reader: Supports encrypted VIAS tags for arming and disarming the alarm system.
- Motion sensor: Detects motion and wakes up keypad for power-saving purpose.
- Light sensor: Automatically adjusts the LED brightness for optimal visibility and touch input readability.
- Link button: Used for binding with the controller.
- Tamper button: Triggers an alarm when the keypad is tampered with under threat.
- Battery holder: Installs four CR123A batteries to power the keypad.
- Terminal block: Allows connection to an external power supply

Note1: The NFC detection area is as shown below. It is strongly recommended to place the tag at the logo position, which is the optimal detection area.



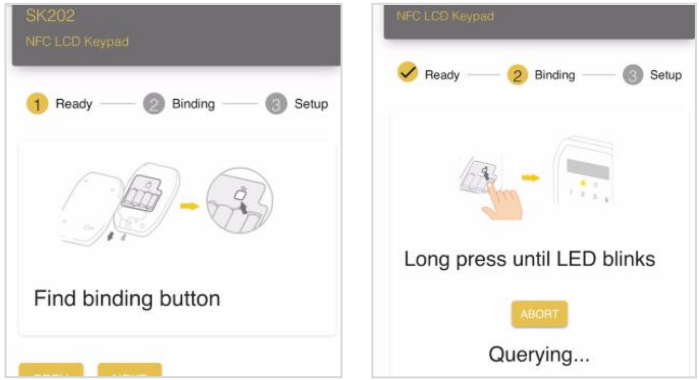
Note2: The NFC tag is not supplied with this product.
Note3: The wire connection for power and data transmission



+: Power anode
- : Power cathode
D+:Data signal(+)
D-:Data signal(-)

Binding the Keypad to the Controller

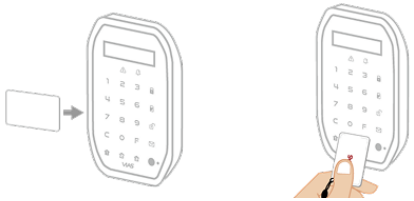
1. Set a controller that is compatible with the Keypad e.g. SC109.
2. Insert four CR123A batteries or connect a 12V DC to power the keypad.
3. Press and hold the Link button for at least 3 seconds, then release. The ⚠ indicator will blink within 30 seconds of countdown.
4. Follow the binding procedure in the app to complete the learning process.



Adding an NFC Tag/Card for the Keypad

Follow the activation procedure in the app to bind an NFC tag for keypad use.

1. Launch the app and initiate the NFC tag binding process.
2. Ensure the keypad is detected and swipe the NFC tag over the tag reader area.



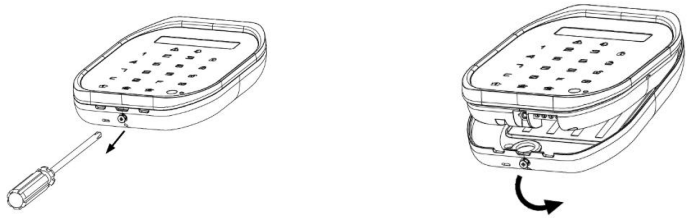
3. Once the tag is recognized, the app will confirm successful binding.

Mounting the Keypad

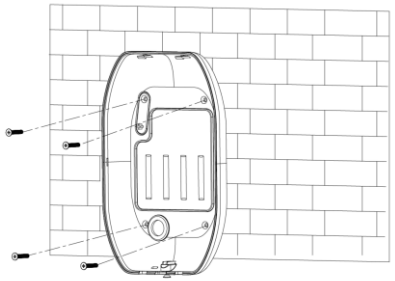
It is recommended to install the Keypad near the main entrance to ensure convenient access for code input. Ensure that the selected position for the Keypad is within the effective range of the controller.

Note: Do NOT fix the Keypad to metalwork or locate the unit within 1 meter of metalwork (i.e. radiators, water pipes, etc) as this could affect its radio range.

1. Loosen the screw from the bottom edge of the keypad and remove the wall mounting plate.



2. Using the mounting plate as a template, mark the positions of the four fixing holes on the wall. Fix the mounting plate to the wall using the screws and wall plugs provided. Do not over-tighten the fixing screws as this may distort or damage the mounting plate.



3. With batteries installed inside, slide the keypad into its wall mounting plate and screw the fixing screw to secure it in place.

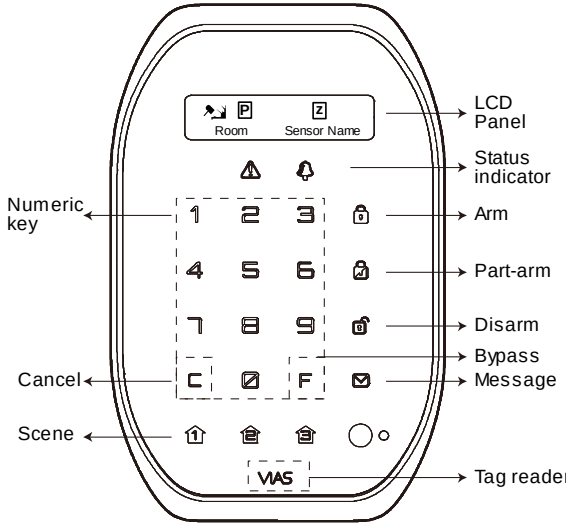
Operation& Function

Creating a personal PIN is required before using the keypad for arming or disarming operations. This can be done using the App. The PIN is 4 digitals long and can be changed via app (Users →Select user name→PIN code)

The LCD panel serves as a visual interface to display the status of the alarm system. It not only shows the current security mode, but also displays fault and tamper information, including partition and zone details. The built-in buzzer will sound to indicate the alarm condition.

When powered by battery, the LCD and LED will turn off while the keypad is in idle mode to conserve power. The keypad will automatically wake up when motion is detected or when the user touches the keypad. If keypad powers by mains electricity, LCD will show the logo.

Note1: The system supports a maximum of 50 users and administrator has permission to edit the list.



Arm
Activates the entire alarm system, enabling monitoring of all secured zones. Ensure all zones are closed before arming the system. Once the system arms successfully, the keypad will emit a long-beep to confirm completion.

- Enter your PIN code or swipe NFC tag/card then press

C(Cancel)
To correct an input error, press the button to clear and re-enter.

Part-arm
Activates selected zones only, allowing movement in excluded areas (e.g., inside the home).
Ensure all active zones are closed before part-arming the system.

- Enter your PIN code and Partition ID then

Note: The Partition ID can be found in the app, in the second rows of each Alarm modes (Main page→Alarm mode).

F(Bypass)
To bypass the fault and tamper, press the F button to clear the LCD display.

Disarm
Deactivates the alarm system and stops all monitoring and alerts. Once the system arms successfully, the keypad will emit a long-beep to confirm completion.

- Enter your PIN code or swipe NFC tag/card then press

Note: If the system was triggered prior to disarming, the alarm log and LCD indicators may display an alert or require further acknowledgement.

Message
If the system has previously entered an alarm state, you must first disarm it by entering the PIN code or using an NFC tag/card. At this point, the message icon will show in the LCD panel and display the stored alarm message from the controller's memory.
To restore the system, press the button to acknowledge and clear the alarm notification.

Note: All alarms must be restored before the system can be armed again.

Exit delay
After arming the system, you have a short period of time to leave the premises before the alarm becomes active, the duration time can be adjusted through the app(gateway config→Settings→Alarm→Exit delay).

Entry delay
When entering while the system is armed, you have a few seconds to disarm the system before the alarm is triggered. the duration time can be adjusted through the app(gateway config→Settings→Alarm→Entry delay).

Panic
Press and hold "1" key for 3 seconds to activate the Panic.

Duress Code
The code is used after the PIN code on keypad to send out the emergency to monitoring center when you disarm the system. The default of duress code is 9-1-1 and it can be adjusted through the app (gateway config→Settings→Duress).

- Enter your PIN code with duress code then press the

Force Arm Code
This code is used for skipping arm checking when any sensor is not ready.

The force arm code can be changed through the app and default is 9-9-9(gateway config→PIN codes→Force Arm code).

- Enter your PIN code and arm button with force arm code.

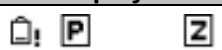
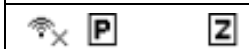
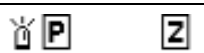
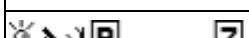
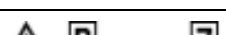
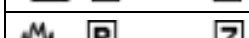
Tamper & Fault
A tamper condition is triggered by any sabotage attempt. It indicates that a device (such as a keypad, sensor, or controller) has been opened, removed, or physically interfered with.

A fault condition indicates a malfunction or abnormal status in the system, such as low battery, communication failure, or sensor error. It requires attention before the system can operate normally.

Fault: At Controller

LCD display	Description
	AC power loss, running on backup battery
	Battery error
	ATS(Alarm Transmission System)
	Network interruption
	No RF signal 20 minutes before arming
	Controller physical tamper
	RF jamming
	RF supervision

Fault: At Sensors

LCD display	Description
	Sensor low battery
	Interconnections loss (Device RF)
	Siren fault
	Sensor physical tamper (Keypad, detector, etc…)
	Siren Tamper
	Intruder/Flood/Mask
	Fire alarm

Fault: At Keypad

LCD display	Description
	Keypad low battery
	Keypad keylock
	Panic

Keylock
Once you enter the wrong PIN code, keypad touch input will be locked for a while, when this situation happens, a tamper event will be generated and logged.

Note: The times of keypad retry is 3 times and it can be adjusted through the app (gateway config→Settings→Alarm→keypad Retry Max)

Scene (1/2/3)
Users can easily activate home automation scenes directly from the Keypad. Customized scenes can be designated to buttons Scene 1/2/3 located in Sensor Information page (press and hold the keypad icon →Settings.
The keypad offers many ways to active the Scenes 1/2/3, user can also configure whether authorization is required for executing Scenes using PIN code or NFC tag/card, especially if placed outdoors.

- Simply long press the Scene button.
- Enter your PIN code then short press the Scene button
- Swipe your NFC tag then short press the Scene button

NFC Mode
The Keypad supports 4 NFC modes, depending on level of authentication required. This can be adjusted in the sensor information page. (press and hold the keypad icon →Settings)

NFC Mode	Description
Simple	Operation via tag/card without pressing any function keys. Swiping the tag/card each time toggles between arming and disarming the system.
Standard	NFC tag/card swipe must be followed by a function button press
2 factor authentication	Both PIN code and tag must be used to operate the keypad and none of them can be omitted. ● PIN+ button first, then tag swipe
Off	When this mode is selected, the NFC function is disabled

Combination of PIN code or tag/card swipe for arming/disarming the system can be summarized as below:

NFC Mode	PIN code	Tag/Card
Simple	O	O
Standard	O	O
2 factor authentication	Both	
Off	O	X

DC power operation
The Keypad can be powered by an external DC source of 12V. When powered by DC, besides waking up motion sensor, the Keypad will also wakeup on demand by controller to sound the Exit/Entry delay beeps and alarm siren.

Maintenance

Keypad offer a Cleaning mode, allowing the keypad surface to be safely cleaned without triggering any operation. By press and holding the “0”key for 3 seconds, the keypad enters this mode and any input is disabled for 30 seconds.

Specifications

Frequency range	868.30MHz /923.00 MHz
RF range (open space)	>1000m
RF protocol	U-net 5.0
Input method	Touch contact, NFC card/tag
NFC Read distance	Maximum 5cm (with unencrypted card)
Battery type	CR123A x 4
External DC input	12V
Operation temperature	-15 ~ - 60°c
Operating humidity	85% RH max
Dimension (mm)	178 (W) x 33.7 (D) x 115(H)
Weight	355g, including batteries
Environment	Indoor /Outdoor shaded environment

***Specifications are subject to change without notice.

WARNING:
Do not dispose of electrical appliances as unsorted municipal waste, use separate collection facilities. Contact your local government for information regarding the collection systems available.

If electrical appliances are disposed of in landfills or dumps, hazardous substances can leak into the groundwater and get into the food chain, damaging your health and well-being.

When replacing old appliances with new ones, the retailer is legally obligated to take back your old appliance for disposal free of charge.

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

Federal Communication Commission Interference Statement
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 of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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.
FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EVERSPRING
www.everspring.com
50 Sect. 1 Zhonghua Rd Tucheng
NewTaipeiCity 236 Taiwan