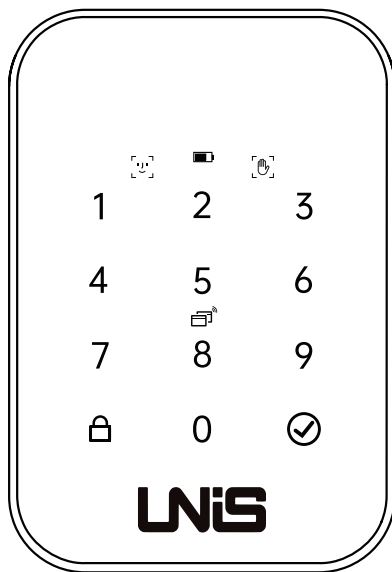


P290 Smart Keypad

User Manual



Please read this user manual carefully
before using your device.

Content

Components	01
List of Components	02
Specifications	02
Installation	03
Installation Precautions	03
Install the mounting plate	04
Install Batteries	05
Install KeyPad	05
Initial Setup	06
Usage Precaution	07
Storage Capacity	08
Radar	08
Face	09
Palm Vein	09
Passcode	10
NFC Card	12
Quick Lock	12
BLE Connection	12
Reset/Restoring Factory Settings	13
Bind Lock	14
Unbind Lock	15
Lost Device	16
Updating Firmware.....	16
LED Indicator	16
Battery Usage Guide	17
Usage Precautions	18
Safety Information	18
COMPLIANCE	19
Disclaimers	21
Warranty	21
Contact & Support	21

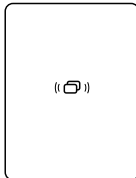
Important Precautions

- KeyPad must be bound with Lock in the app before any access credentials can be added.
- Face and palm vein recognition can still operate normally in low-light environments.
- Avoid installing KeyPad in locations exposed to prolonged direct sunlight or rain:
 - High temperatures may accelerate device aging and increase the risk of malfunction.
- Although KeyPad is rated IP65, rain exposure may trigger the radar sensor and touch KeyPad, leading to increased power consumption.

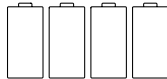
Components



KeyPad Assembly



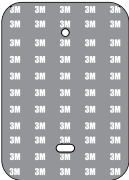
Key Card*3



CR123A Batteries*4



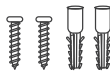
L-Shaped
Screwdriver



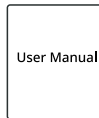
Mounting Plate
with 3M Adhesive Pad



Mounting Screws*2



Wall Anchor Kit



User Manual

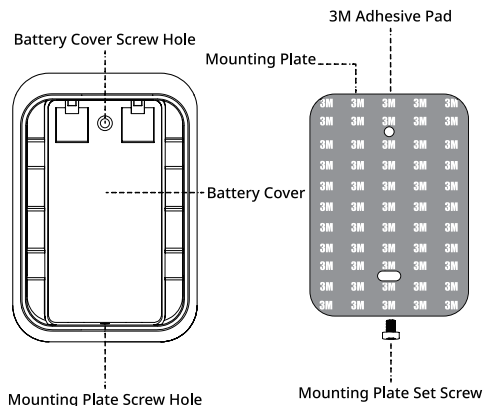
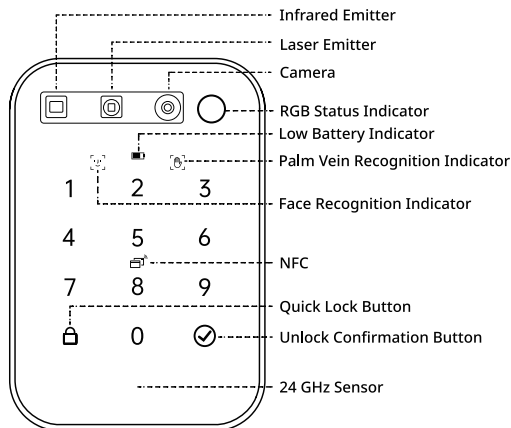


Handle Clip



Wet & Dry
Cleaning Wipes

List of Components

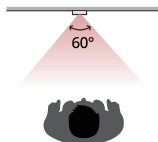
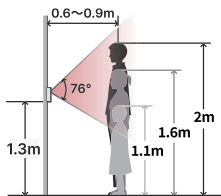


Specifications

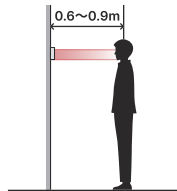
Model	P290
Material	PC (with UV-resistant coating)
Size	102 × 70 × 38 mm
Weight	108.2 g
Power Supply	CR123A batteries × 4 (2S2P)
Connectivity	BLE 5.2 (Bluetooth 5.2)
Ingress Protection	IP65
Operating Temperature	-20° C to 50° C
Operating Humidity	10% ~90% RH (non-condensing)
Operating Voltage	6 V
Operating Frequency	2402 MHz to 2480 MHz
Maximum Transmit Power	4 dBm

Installation Precautions

- Face Recognition Range: Vertical angle: 76°, horizontal angle: 60°.



- For single-user use, install the device in a position where the user can face the camera directly for optimal performance.

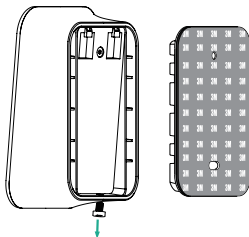


- Suggest the position according to the user's height:

Mounting Height	User Height
120 cm(47 inches)	110 cm (43 inches) to 180 cm (71 inches)
130 cm (51 inches)	120 cm (47 inches) to 190 cm (75 inches)
140 cm (55 inches)	130 cm (51 inches) to 200 cm (79 inches)

**Note: To ensure better signal strength, avoid installing the device on metal surfaces.*

Install the mounting plate



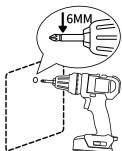
**Note: Remove the screws shown in the diagram and detach the mounting plate, then select an installation method:*

Method1: Screw Mounting

***Tools needed: Electric drill, Phillips screwdriver, Rubber hammer.**
Select the installation location and mark the drilling positions.

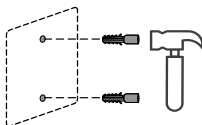


1. For hard surfaces such as plaster, brick, or concrete.



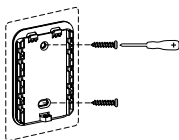
1

- Drill holes using a 6 mm drill bit.



2

- Insert the wall anchors into the drilled holes.



3

- Secure the mounting plate with the provided screws.

2. For wooden surfaces: Drill holes using a 6 mm drill bit.

- Secure the mounting plate directly with self-tapping screws.

***Note:** Consult with a professional drill if needed.

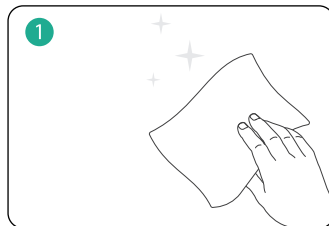
Method2: 3M Tape Mounting

***Precautions:**

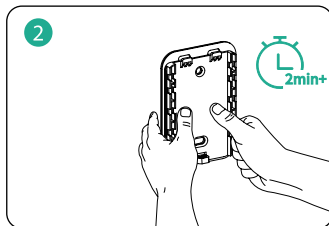
This method is suitable for smooth surfaces such as glass, tiles, and stainless steel. Make sure the surface is clean to ensure optimal adhesion.

Clean the surface before installation. This method is not recommended for rough walls, porous wood, wallpaper, or cracked surfaces.

1. Select the installation location, then clean the surface with the provided wet & dry cleaning wipes.

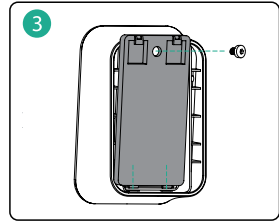
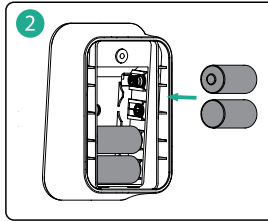
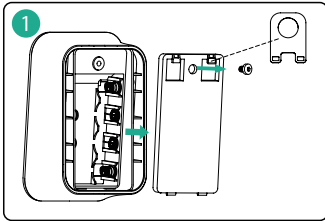


2. Peel off the adhesive backing, attach the mounting plate to the installation surface, and press firmly for 2 minutes to ensure optimal adhesion.



Install Batteries

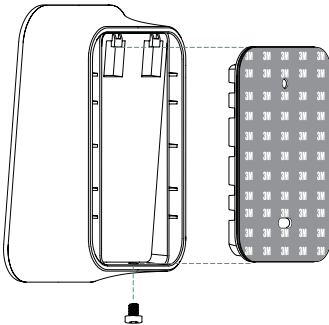
1. Remove the screws shown in the diagram and use the handle clip to remove the battery cover.
2. Insert the batteries according to the indicated polarity.
3. Reinstall the battery cover as shown and tighten the screws.



Note: After installing the batteries, the KeyPad status indicator will flash white during initialization and flash green when the device is ready.

Install KeyPad

1. Hook the KeyPad onto the two clips at the top of the mounting plate, then press it into the bottom clips.
2. Secure the KeyPad to the mounting plate with screws.



Getting Started

1. This product must be used with the SmartLife App. Follow the instructions to bind the device first.
2. The App requires a smartphone with Bluetooth 4.2 and iOS / iPadOS 13.0 or above, or Android 7.0 or above.

Download the App:

- Search for and download "SmartLife" from the following platforms:



Apple and the Apple logo are trademarks of Apple Inc.

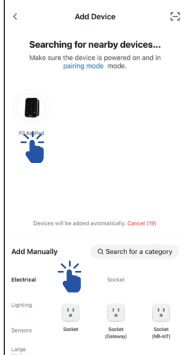
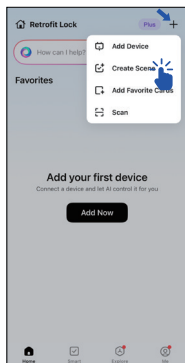


Google Play and the Google Play logo are trademarks of Google Inc.

- Alternatively, scan the QR codes below to download the SmartLife App.



Initial Setup



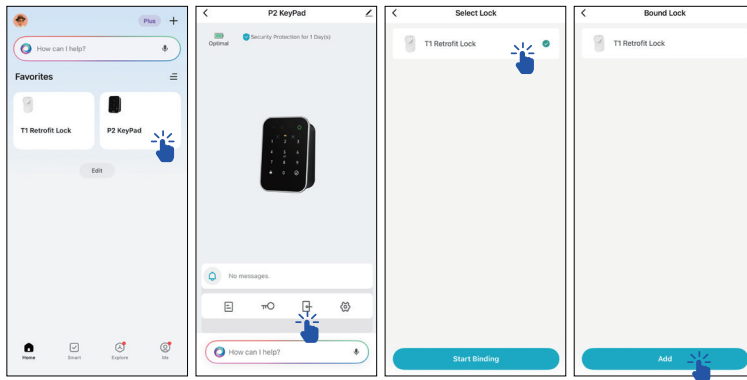
Add KeyPad to the SmartLife app

- Make sure you have created a SmartLife App account.
- Make sure Bluetooth is enabled on your smartphone.
- On the Smart Life App home screen, tap "+" in the upper-right corner, select "Add Device", and follow the on-screen instructions.
 - If the app does not detect your KeyPad, touch and activate the touchpad to enter pairing mode. The KeyPad will then be detected by the app.

*Note:

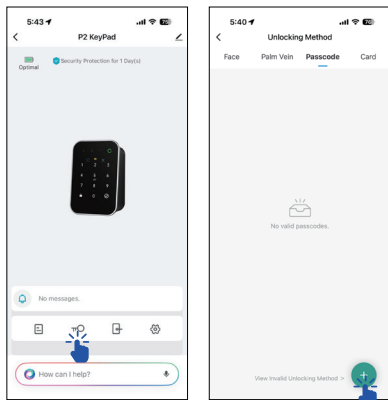
- After adding the device, go to the device page and tap the "🔒" icon to bind KeyPad to Lock.
- Multiple KeyPads can be bound to the same Lock, but each KeyPad can only be bound to one Lock.

Usage Guide



Usage Precaution

- KeyPad must be used with a smart lock. Go to the KeyPad device page in the app, tap the "🔑" icon, and follow the on-screen instructions to bind it to the lock.



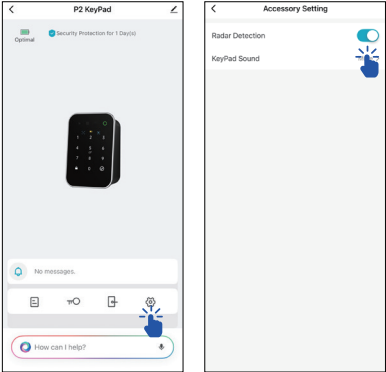
- To register or manage access permissions such as face recognition, palm vein recognition, passcodes, or key cards, tap the "🔑" icon at the bottom of the KeyPad device home page. Then, on the next page, select the corresponding access type from the top menu bar to add or manage it.
- To remove access, ensure the app and KeyPad are connected via Bluetooth or Hub.
- KeyPad prioritizes face recognition by default. When a hand enters the detection range, it automatically switches to palm vein recognition. The face indicator "👤" and palm indicator "🖐️" will flash to indicate the current mode.

***Note:**Keep the glass surface clean and free of water or dirt, as this may affect recognition performance.

Storage Capacity

Type	Capacity	Note
Face	50	Each "Home" in the app supports up to 20 members, and each member can register multiple face profiles.
Palm Vein	50	Each "Home" in the app supports up to 20 members, and each member can register multiple palm vein profiles.
Passcode	50	Up to 50 (online passcodes only).
Card	50	Up to 50.

Radar



- KeyPad is equipped with a millimeter-wave radar to detect nearby presence and activate face or palm vein recognition.
- Passersby may trigger the radar unintentionally, which may increase power consumption.
- Radar detection can be disabled in the app to save power and reduce frequent false triggers.
- Face or palm vein recognition can also be activated by touching the KeyPad. However, recognition will stop once a passcode is entered.

***Note:** Do not place any objects over the radar area, as this may affect detection performance.

Face

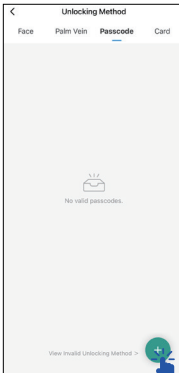
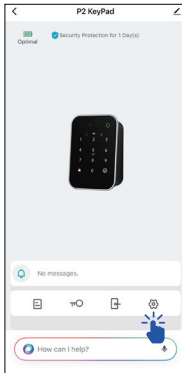
- **Recognition Priority** : KeyPad prioritizes recognizing the closest face in front.
- **Enrollment Distance** : Keep a distance of 40 cm to 70 cm (15.7–27.6 inches) when registering a face.
- **Recognition Distance** : The effective recognition distance is 40 cm to 90 cm (15.7–35.4 inches).
- **Face Requirements** : Keep the face tilt within $\pm 25^\circ$, and ensure the face is fully visible (avoid wearing hats, sunglasses, or masks).
- **Status Indication** : When the face indicator " " flashes, face recognition is in progress.
- **Failure Lockout** : If face recognition fails 10 times within 2 minutes, KeyPad will disable recognition and only allow it again after 5 minutes.

Palm Vein

- **Recognition Priority** : KeyPad prioritizes recognizing the closest palm vein in front.
- **Enrollment Distance** : Keep a distance of 10 cm to 20 cm (3.9–7.9 inches) when registering palm veins.
- **Recognition Distance** : Keep a distance of 10 cm to 25 cm (3.9–9.8 inches) during palm vein recognition.
- **Palm Requirements** : The optimal recognition area is the center of the palm. Keep the tilt angle within 20° and the rotation angle within 90° . Do not cover the palm (e.g., gloves).
- **Status Indication** : When the palm indicator " " flashes, palm vein recognition is in progress.
- **Failure Lockout** : If palm vein recognition fails 10 times within 2 minutes, KeyPad will disable recognition and only allow it again after 5 minutes.

Passcode

- Add the required passcode types in the app and assign them to the appropriate members.
- Passcodes must be 6 to 10 digits long. After entering the passcode, tap "✓" to confirm. The KeyPad will then verify the passcode.
- Anti-Peeping Feature: To help protect your passcode from being observed, you can enter random digits before and/or after the correct passcode when unlocking the door.
- Failure Lockout: If passcode verification fails 10 times within 2 minutes, the KeyPad will disable passcode entry and will only accept input again after 5 minutes.



Passcode Types

Passcode Type	User-Friendly Description	Connection Requirement	Validity / Usage Rules	Deletion or Expiration
Online Passcode Can be added when the device is connected.				
Permanent Passcode	A long-term passcode for family members, employees, or regular users.	The device must be connected to the app, Bluetooth, or a gateway when adding, editing, or deleting the passcode.	Remains valid after creation unless manually deleted.	Must be deleted in the app while the device is connected; otherwise, the passcode may remain stored on the lock.
Palm Vein	An online one-time passcode for temporary visitors or single-entry access.	The device must be connected when the passcode is created.	Can be used only once and becomes invalid after use.	Automatically expires after one use, or can be deleted in the app while the device is connected.
Passcode	An online time-limited passcode for access during a specific date, time range, or schedule.	The device must be connected when adding, editing, or deleting the passcode.	Can be used within the configured validity period or schedule, and may be used multiple times depending on the settings.	Must be deleted or modified in the app while the device is connected.
Offline Passcode Can be added when the device is connected or disconnected.				
One-Time Passcode	An offline one-time passcode for temporary access when the device is not connected.	Can be generated whether the device is connected or disconnected.	Valid for a short period after creation, typically up to 6 hours, and can be used only once.	Automatically expires after one use, or when the validity period ends.
Time-Limited Passcode	An offline time-limited passcode for granting temporary access when the device is not connected.	Can be generated whether the device is connected or disconnected.	Can be used within the configured validity period. It typically must be used once within 24 hours after becoming valid to activate; after activation, it can be used multiple times until it expires.	To delete it early, generate a Clearing Code and enter it on the lock.
Clearing Code	A code used to remove an active offline time-limited passcode.	Can be generated whether the device is connected or disconnected.	Not used for unlocking. It is only used to cancel offline passcodes.	Enter the Clearing Code on the lock to remove a specific offline passcode or all offline passcodes, depending on device support.
Dynamic Passcode Can be added when the device is connected or disconnected.				
Dynamic Passcode	A short-term passcode for quick, temporary access.	Can be generated and used whether the device is connected or disconnected.	Valid for a very short time, typically around 5 minutes. A new code must be generated after it expires.	Expires automatically and does not need to be deleted.

NFC Card

- Please follow the instructions in the app to add NFC cards and assign them to the appropriate family members.
- When the NFC card storage limit is reached, you need to delete existing NFC cards before adding new ones.
- If your NFC card is lost, please promptly delete the corresponding card access permission through the app.
- **Failure Lockout** : If NFC card recognition fails 10 times within 2 minutes, the KeyPad will stop recognizing NFC cards and will only allow recognition again after 5 minutes.

Quick Lock

- After waking up the KeyPad, tap the " " button to lock the door.
- When locking is complete, the status indicator " " will turn green.
- If the lock is already locked, the indicator will still turn green as a confirmation.

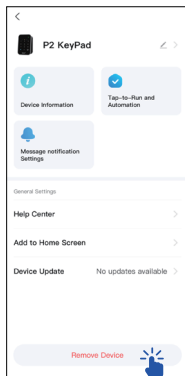
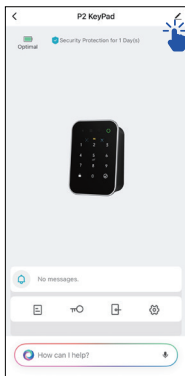
Connection

- KeyPad must establish a Bluetooth connection before controlling the lock. Connection time may vary depending on the environment, typically taking 1 to 2 seconds.
- When the status indicator " " flashes blue, it indicates that the KeyPad is connecting to the Lock via Bluetooth. If the indicator flashes blue twice and the buzzer beeps twice, the Bluetooth connection has failed. Please try again.
- When the app is connected to the KeyPad or Lock, it may interfere with the Bluetooth communication between the KeyPad and Lock. Please disconnect the app (turn off Bluetooth on your phone) before trying to use the KeyPad to control the Lock again.
- When using Bluetooth to manage and control the door lock, you generally need to be within 5 meters of the lock, and make sure Bluetooth is enabled on your phone and connected to the lock.
- The effective Bluetooth range may be affected by obstructions such as walls, especially metal walls. In addition, the surrounding wireless environment may also affect Bluetooth communication. Moving closer to the door lock can help reduce these effects.

Restoring Factory Settings

1. App Reset

- To reset the device, select it in the App, tap the " " icon in the upper-right corner of the device page, then tap "Remove Device" at the bottom of the page.



*Note:

- The KeyPad can only be reset through the app and does not support local reset.
- If the device is not connected via Bluetooth when you reset it through the app, the device itself will remain unchanged (the reset will not actually be completed). The reset will only take effect once an app scans and connects to the device via Bluetooth.
- A long beep and a solid blue indicator light mean the device has been successfully reset, all user data has been erased, and the device has been restored to factory settings.

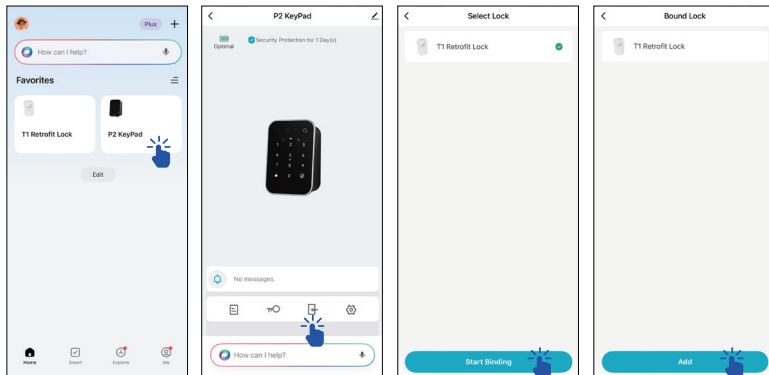
After restoring the device to factory settings:

- All data will be erased.
- Any app account can bind the device again.

Please perform device reset operations with caution, and keep the App connected to the device via Bluetooth whenever possible during the reset process.

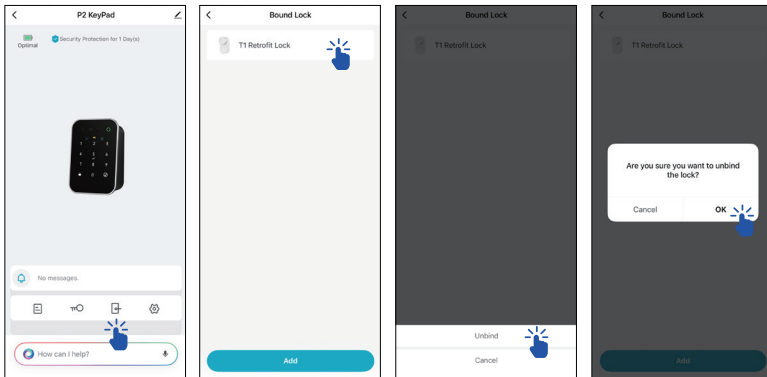
Bind Lock

- After the Lock and KeyPad are bound, the KeyPad can wirelessly lock and unlock the Lock via Bluetooth.
- Please ensure that both the Lock and the KeyPad are first bound to the same "Home" in the app.
- In the app, select the corresponding KeyPad to enter its device home page
- Tap the "+" icon in the bottom menu, then tap "Add" at the bottom of the page.
 - Select the corresponding Lock, then tap "Start Binding".



Unbind Lock

- If you want to unbind the Lock from the KeyPad, follow the steps below:
- In the app, select the corresponding KeyPad to enter its device home page.
- Tap the "🔗" icon in the bottom menu.
- Press and hold the corresponding Lock, then tap "Unbind".



***Note:**

- After unbinding the Lock and KeyPad, both devices will remain in your app account.
- Once the KeyPad is unbound from the Lock, it will no longer be able to control the Lock, and all Face ID / palm vein / passcode / NFC card permissions stored in the KeyPad will also be erased.
- Resetting either the KeyPad or the Lock will also remove the binding relationship between them, and all Face ID / palm vein / passcode / key card permissions stored on the KeyPad will be erased at the same time.

Lost Device

- If your device is lost, please remove it from your account in the app.
- If you recover the lost device, you can pair the KeyPad with the Lock again.

Updating Firmware

- In order to improve your experience, we will regularly release firmware updates to introduce new functions and solve any software defects that may occur during usage.
- When a new firmware version is available, we will send an upgrade notification to your account via our app
- When upgrading, please make sure your product has sufficient battery or stays powered on and make sure your smartphone is within range to prevent interference.

LED Indicator

Icon	Green	Red	White	Blue	Yellow
	Lock/Unlock Successful	Lock/Unlock Fail	In Progress	Bluetooth Connecting	/
	Face Recognition Successful	Face Recognition Failed	Face Recognition in Progress	/	/
	Palm Vein Recognition Successful	Palm Vein Recognition Successful	Palm Vein Recognition in Progress	/	/
	/	Low Battery – Device Locked Replace the batteries to restore operation.	/	/	Low Battery – Replace Batteries Immediately

Battery Guide

1. Battery Type and Configuration

- This product uses 2S2P CR123A primary lithium batteries (3.0V), with a total voltage of approximately 6.0 V.
- The device can operate with one set (2 cells), but battery life will be reduced by approximately half, and the low battery indicator will activate earlier.
- For optimal performance, install two sets of batteries (4 cells).
- Do not use other battery types (such as 3.6–3.7 V rechargeable Li-ion or LiFePO₄ batteries), as higher voltage may damage the device or pose safety risks.

2. Installation and Replacement

- Make sure the battery polarity is correct. Incorrect installation may prevent the device from powering on or cause damage.
- Ensure proper contact: keep the battery contacts clean and free of dust, and make sure the springs are not damaged.
- Do not mix old and new batteries, as this may cause unstable voltage or trigger low battery warnings.
- Do not mix batteries of different brands or types to ensure stable operation.

3. Operating Environment

- Operating temperature: -20°C to 50°C. Battery capacity may decrease at low temperatures, and device response may slow down.
- Storage: avoid prolonged exposure to high temperatures or humid environments.
- Do not expose batteries to moisture or water to prevent short circuits or leakage.

4. Handling Precautions

- Do not short-circuit, disassemble, puncture, or burn batteries, as this may cause explosion or leakage.

5. Low Battery Warning and Lockout

- Low battery warning: When the main battery level is below 10%, the yellow indicator will flash after each operation.
- Low battery lockout: When the main battery level is below 5%, all operations will be disabled and the red indicator will flash.
- Recommendation: Replace the batteries as soon as a low battery warning appears to avoid unexpected shutdown.

6. Replacement and Disposal

- Use primary (non-rechargeable) batteries only. Do not recharge.
- Replace all batteries at the same time with new batteries of the same brand and specifications.
- Dispose of used batteries in accordance with local regulations. Do not discard them improperly.
- Do not use recycled or low-capacity batteries, as this may affect performance or damage the device.

7. Additional Note

- If only one set of batteries is installed, the device will operate, but battery life will be reduced by half
- Ignoring low battery warnings may cause the device to stop working at critical moments.
- High temperatures (>60°C) may accelerate battery aging or cause leakage.
- At temperatures below 0°C, battery capacity decreases and may reduce operating time.

Usage Precautions

1. Operational Risk:

- If the batteries are depleted, the lock cannot be locked or unlocked. Keep a physical key available as a backup.

2. Firmware Updates:

- Check for firmware updates regularly and install them promptly to ensure optimal performance and security.

3. Operating Environment:

- This product is intended for indoor use or sheltered outdoor use only. It is not waterproof. Avoid exposure to rain, moisture, or direct sunlight.

Safety Information

- Keep this product away from heat and humidity, and make sure it does not come into contact with fire or water.
- Do not touch or operate this product with wet hands.
- This product is a precision-based electronic product. Please avoid physical damage.
- Do not attempt to disassemble, repair, or modify this product.
- Do not use this product where wireless devices are not allowed.

Compliance

FCC REGULATORY COMPLIANCE

- 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.
- Any changes or modifications not expressly Approved by the party responsible for compliance could void the user's authority to operate this equipment. 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.

RF Exposure Statement

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IC NOTICE TO CANADIAN USERS

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:
 - (1) This device may not cause interference.
 - (2) This device must accept any interference, including interference that may cause undesired operation of the device.This Class B digital Apparatus complies with Canadian ICES - 003.
This device complies with RSS - 247 of Industry Canada. Operation is subject to the condition that this device does not cause harmful interference. This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

WEEE Information



All products bearing this symbol are waste electrical and electronic equipment (WEEE as in directive 2012/19/EU) which should not be mixed with unsorted household waste. Instead, you should protect human health and the environment by handing over your waste equipment to a designated collection point for the recycling of waste electrical and electronic equipment, Appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. Please contact the installer or local authorities for more information about the location as well as terms and conditions of such collection points.

EU Declaration of Conformity



UNIS d.o.o. hereby declares that the radio equipment type Smart Keypad (model: P290) is in compliance with directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.unis.hr.

RF Exposure Information:

The Maximum Permissible Exposure (MPE) level has been calculated based on a distance of $d=20$ cm between the device and the human body. To maintain compliance with RF exposure requirement, use product that maintain a 20cm distance between the device and human body.

Frequency bands and power :

- Bluetooth Operation Frequency: 2402-2480 MHz
- Bluetooth Max Power: EIRP 0.39 dBm

RoHS Declaration of Conformity

We, UNIS d.o.o. hereby declare under our sole responsibility that the above-referenced product(s) comply with the following directives:

- Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS Directive)
- Commission Delegated Directive (EU) 2015/863 of 31 March 2015 amending Annex II to Directive 2011/65/EU

Warning and safety information

- Risk of explosion if the battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.
- Do not ingest battery, Chemical Burn Hazard.
- This product contains battery. If the battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Keep new and used batteries away from children.
- If the battery compartment does not close securely, stop using the product and keep it away from children.
- If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

Packaging Environmental Information



The packaging materials of this product are made from recyclable materials in accordance with national environmental regulations. Do not dispose of packaging materials together with household or other waste. Please take them to the collection points designated by local authorities for packaging materials.

Disclaimer

Liability:

- The company shall not be liable for any damage caused by improper operation, unauthorized repair, or natural disasters. The company is not responsible for any damage to the door surface or paint peeling caused during product installation or removal.

Intended Use:

- This product is designed for lock control only and is not a security or anti-theft device

Warranty:

- The product is warranted by the original purchaser to be free from defects in materials and workmanship. The warranty does not cover batteries, normal wear and tear, misuse, or products purchased from unauthorized sellers.

Warranty

We warrant the original owner of the product that the product will be free from defects in materials and workmanship. Please note that this limited warranty does not cover:

- Products submitted beyond the original limited warranty period.
- Products on which repairs or modifications have been attempted.
- Products subjected to falls, extreme temperatures, water, or other operating conditions outside the product specifications
- Damage due to natural disasters (including but not limited to lightning, flood, tornado, earthquake, or hurricane, etc.).
- Damage due to misuse, abuse, negligence or casualty (e.g. fire).
- Other damage that is not attributable to defects in the manufacture of product materials.
- Products purchased from unauthorized resellers.
- Consumable parts (including but not limited to batteries).
- Natural wear of the product.

Contact & Support

If you have any questions about this product, please visit the following website

- for more information: www.unis.hr
- Online Customer Service: www.unis.hr/support
- Manufacturer: UNIS d.o.o.
- Address: Malešnica 31, HR-10000 Zagreb, Croatia
- Email: info@unis.hr

