PARADOX ⩗

PGMZ1M
1-Output Expander

INSTALLATION MANUAL

FW Version: V1.01.000

Introduction

The PGMZ1M is a two-way wireless containing one programmable output relay and one zone input. It communicates with the Paradox M systems using 2-way wireless communication, featuring the latest Gaussian Frequency Shift Keying (GFSK) technology with frequency and encryption hopping. This ensures superior wireless range, enhanced encryption, supervision, and reliability. The PGMZ1M includes dual tamper protection (wall and cover).

Quick Installation - Experienced Installers
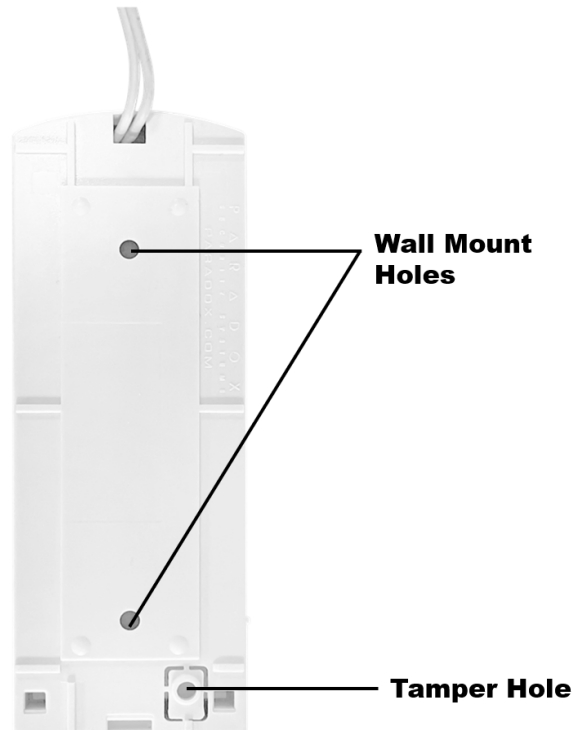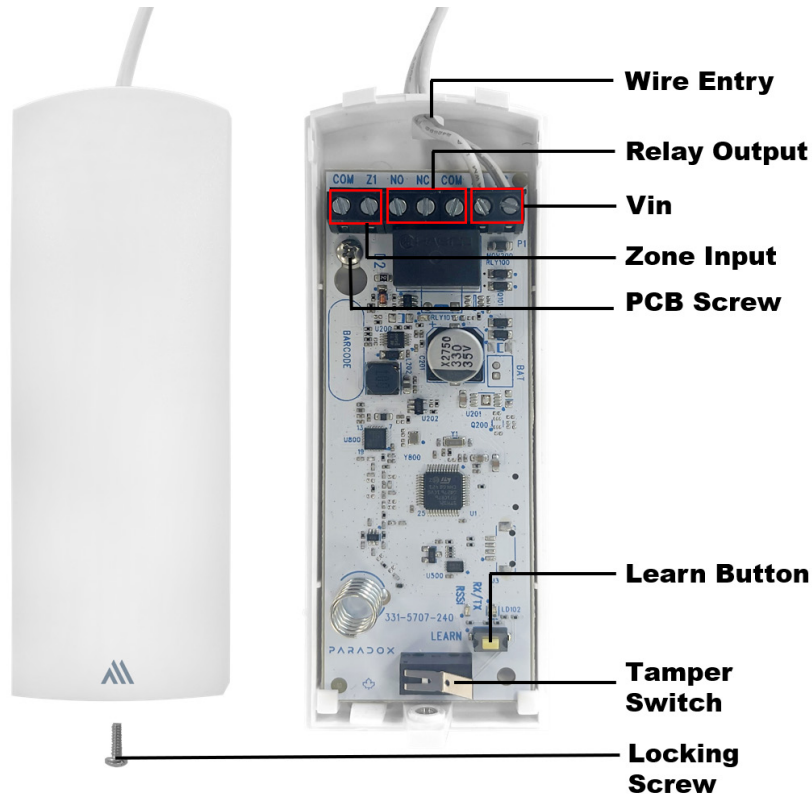
To install PGMZ1M:
1. Unscrew and open the front cover of the device.
2. Remove the PCB and mount the backplate.
3. Connect to a zone input and an output. Provide a **Vin** of **5-16V AC or DC** with a minimum current of 300mA. Secure the device.
4. Pair PGMZ1M with the console (Using the BlueEye application):
   - Go to: **Hardware** > Tap **Add Devices** > **Wireless Devices Auto learn**.
     NOTE: *You can instantly pair PGMZ1M by pressing the Learn button momentarily or activating the tamper.*
5. Configure PGMZ1M (Using the BlueEye application):
   - Go to: **Hardware** > Tap **PGMZ1M** from the device list > Enter the necessary details > **Save**.
   Built-in status indications of PGMZ1M:
   - Red blinking 5 times – Not connected to the console (new or unpaired)
   - Green blinking 5 times – Connected to the console
   - 8 x Red/Green – Tamper detected
   - 8 x Green blinking - Tamper closed

Components of PGMZ1M

The following figure displays the components of PGMZ1M.

Wire Entry

Relay Output

Vin

Zone Input

PCB Screw

Learn Button

Tamper Switch

Locking Screw

Wall Mount Holes

Tamper Hole

Components of PGMZ1M

Physical Mounting

To mount PGMZ1M:

1. Release the screw from the bottom of the PGMZ1M and remove the front cover.
2. To attach the backplate to a surface, loosen the PCB screw by about one turn. Then, slide and remove the PCB.

3. Mount the backplate on the wall using mounting and tamper holes.
NOTE: A*s per the EN security standards, one screw must be secured in the tamper hole. The use of double-sided tape does not trigger a wall tamper alarm.*
4. Secure the PCB on the backplate.
5. Connect to a zone and output by routing cables through the wire entry hole of the device.
6. Provide a **Vin** of **5-16V AC or DC** with a minimum current of 300mA.
7. After completing the wire connection, reattach the front cover and tighten the screw at the bottom.

Pairing PGMZ1M with the Wireless M Console

The pairing and configuration settings of PGMZ1M are managed through the BlueEye application.

Prerequisites

Ensure that:
1. The PGMZ1M is within the range of the console.
2. The BlueEye application is installed on your mobile and connected to the site.
3. The M console is powered on (Paradox logo color - white, red, or green).

Pairing PGMZ1M

To pair the PGMZ1M with the wireless console by an installer:
1. In BlueEye, when in the M site (the **Hardware** tab), tap **Add Devices**, and then tap **Wireless Devices Auto learn**.
   The wireless console searches for new devices and a rotating radar icon is displayed. This may take up to 6 minutes. To pair instantly, press momentarily on the Learn button, or activate the tamper. The device pairs with the console and it appears at the top of the device list with a ***new*** tag and voice announcements.
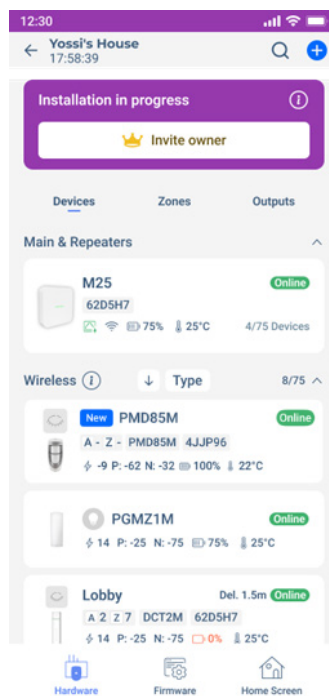
After pairing, to identify the new device, you can trigger the PGMZ1M tamper. A **T** symbol appears on the device tab in the BlueEye application.
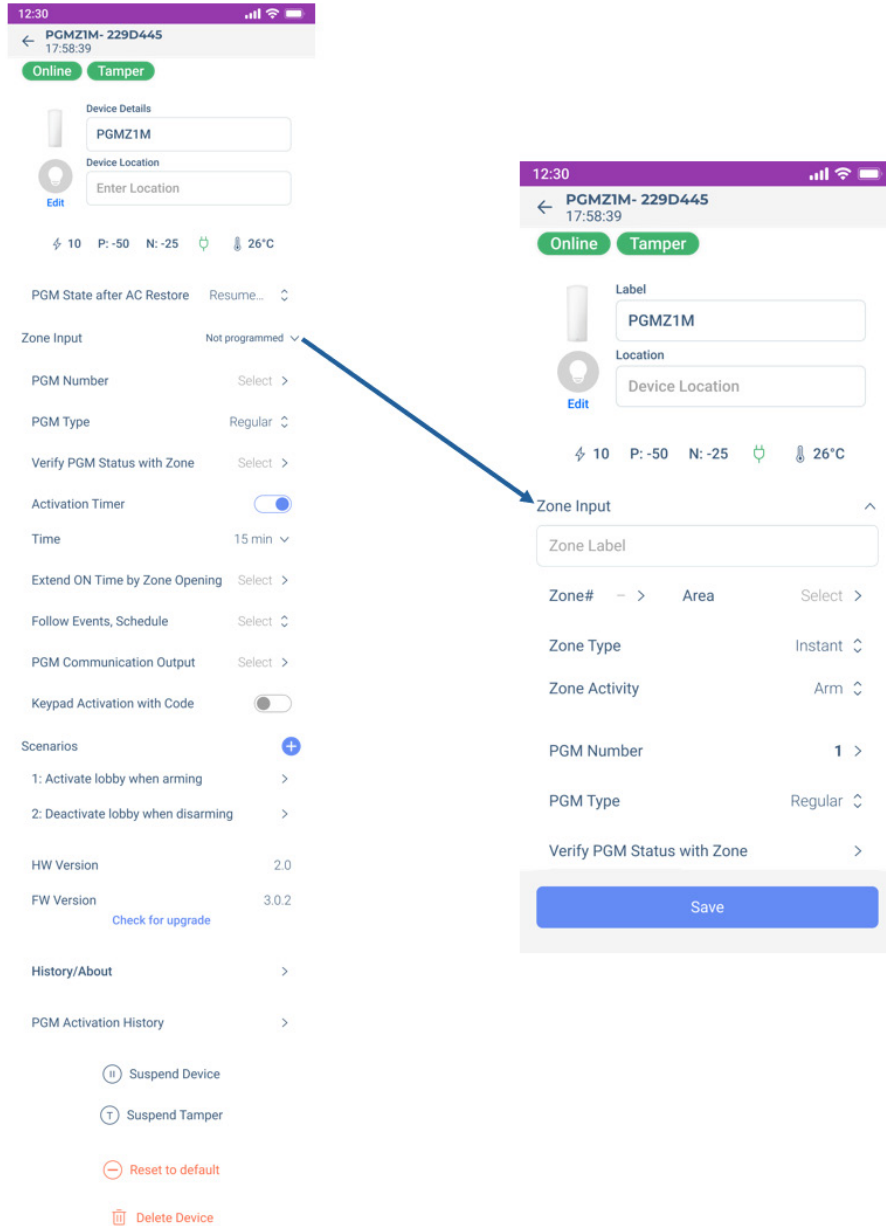
Configuring

To configure the PGMZ1M settings:
1. When in the **Hardware** tab, tap the **PGMZ1M** device.
2. On the screen that opens, enter the necessary details.

3. Tap **Save**.
   For details about each parameter displayed on the page, see Table 1.

The following table lists the parameters displayed for configuring the PGMZ1M, along with their descriptions.

Table 1

Parameter	Description
Edit	Select a new icon from the list or choose a new one from the gallery.
PGM State after AC Restore	Select the desired PGM status after power restoration: • **Resume Last State (Default)** • **On** • **Off**
Zone Input	Configure the settings for a zone input.
Zone # and **Area**	Assign a zone and area number.

Type/Activity	Select the type of zone.
	The following are the different zone types:
	• Arm
	• Arm/Sleep
	• Arm/Stay
	• Arm/Sleep/Stay
	• **24 hours** – Always armed. The system remains in alarm as long as this zone is open. The system can be armed even if the 24-hour zone is in alarm.
	• 24 Water
	• 24 Fire
	• 24h Fire, 2 Wired Smoke
	• 24h Fire, 4 Wired Smoke
Follow Delay Zone	This zone is instant and becomes a delay zone if a delay zone is opened first.
Entry Delay	When this option is enabled, opening a zone triggers an entry delay in any arming mode.
	• **Instant** – When in any armed status, an immediate alarm occurs. However, a delay period can be added to the **Instant** zone when arming in the Stay and Sleep modes.
	• 5 sec
	• 10 sec
	• 15 sec
	• 30 sec
	• 45 sec
	• 1 minute
	• 1.5 minute
	You can select the delay duration from the available options.
Intellizone	When the **Intellizone** option is enabled for a device, the system will trigger an alarm under one of the following conditions, within the configured Intellizone Timer window (default: 30 seconds):
	• **Two separate openings** are detected within the timer period.
	• A **trigger from an Intellizone**, followed by a **trigger from any other zone** within the timer period.
	• The **same zone remains open** throughout the timer period.
	Intellizone is not available for any 24H zones.
PGM Number	Select the PGM number.
PGM Type	Define the PGM type:
	• **Regular**
	• **Restricted**
	• **Installer**
Verify PGM Status with Zone	Assigns zone to verify the status of the PGM.
Activation Timer	Sets the duration for PGM activation.
Extend on Time by Zone Opening	Extends the PGM activation duration when the assigned zone is triggered.
Keypad Activation with Code	PGM can be activated only after entering the user code on the keypad.
Follow Events, Schedule	Defines the PGM activation behavior:
	• **None**: Inactive
	• **Zone**: Activates the PGM when a specific zone is triggered.
	• **Area Status**: Activates the PGM based on the status of a particular area.
	• **Trouble**: Activates the PGM in response to system trouble conditions.
	• **Schedule**: Activates the PGM according to a predefined schedule.
PGM Communication Output	*(Coming Soon)* Specify the notification type, method, and receivers for PGM communication.
Scenarios	*(Coming Soon)* Example automation scenarios:
	• Activate lobby when arming
	• Deactivate the lobby when disarming

PGM Activation History	(*Coming Soon*) Displays the history of PGM activations.
Reset to Default	This will reset the device to the factory default settings. **NOTE**: *Only an installer can reset the device.*
About	This tab displays details such as the installation date, production date, last programming date, battery replacements, battery history, and upgrade history.
Suspend Device	Disables the monitoring of the device in the system.
Suspend Tamper	Disables tamper monitoring for the device.
Reset to Default	This will reset the device to the factory default settings. **NOTE**: *Only an installer can reset the device.*
Delete Device	This option deletes the device from the system completely. After deletion, the system generates a push notification only if the owner registration is complete, not during installation. **NOTE**: *Only an installer can delete the device.*

LED Indications

After configuring PGMZ1M, the detector displays various LED indications based on specific events.
The following table lists the LED indications and their corresponding event.

Table 2

LED Indication	Event
Red Blinking 5 times	Not connected to the console (new or unpaired).
Green Blinking 5 times	Connected to the console.
8 x Red/Green	Tamper detected
8 x Green blinking	Tamper closed

Resetting

Press and hold the **Learn** button for 8 seconds to reset the device to its default settings. Reset is indicated by LED flashing red three times followed by device restart.

Upgrading Firmware

To upgrade the firmware:

1. In the **Hardware** tab, tap on the device > **Check for Upgrade**.
2. If an upgrade is available, tap **Upgrade** when prompted.
   The process may take a few minutes. Monitor the progress in the BlueEye application to ensure that the upgrade is completed successfully. Both the Installers and owners can perform the upgrade.

IMPORTANT: The firmware upgrade can be done only when the system is disarmed.

Signal Strength and Transmit Power Monitoring

The BlueEye application provides insights into each device's received signal strength and transmission power to optimize performance.

To view the RSSI and transmit power range:

1. When in the **Hardware** tab, tap the ⓘ icon next to the **Wireless** tab.
   A pop-up window with the RSSI and transmit power range is displayed.
2. Maximum power transmitted by PGMZ1M:
   - 868 MHz: +14 dBm
   - 914 MHz: +22 dBm
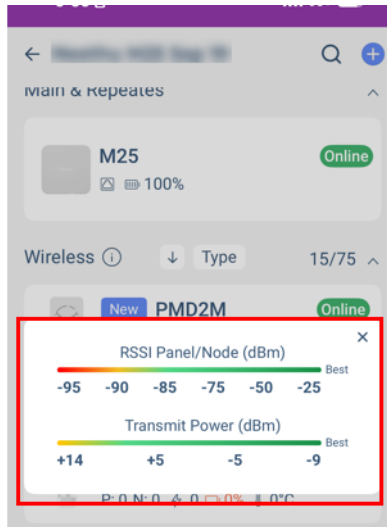
Tap on any listed device to view signal strength and additional device metrics. The following parameters are displayed for each device:

- **P** - Received signal strength at the panel
- **N** - Received signal strength at the device
- ⚡ - Transmit power of the device.
- 🌡 - Current temperature reading of the device.
- 🔋 - Battery level of the device

A higher P and N value indicates stronger and clearer communication between the console and the device.
- If **P** is low, the console struggles to receive signals from the device.
- If **N** is low, the device struggles to receive signals from the console.

NOTE: *Values below -93 with maximum Tx power are not recommended values, and RPT5M can be used to extend the range.*

Power transmission impacts only **P**:
- When **power transmission** increases, the **P** value at the console generally improves, as a stronger signal is sent.
- If the **P** value is good, the device can reduce its transmission power to save battery life.

IMPORTANT: All nodes adjust their transmission power. The adjustment depends on the surrounding noise level and is updated at intervals set by the supervision timer or during a node status update.

Dual Tamper Protection

The PGMZ1M programmable output module is equipped with dual tamper protection (wall and cover). If the system is armed, any tamper activation immediately triggers a system alarm. When the system is disarmed, a tamper activation generates a report to the CMS, sends a push notification, and displays a tamper trouble alert in the BlueEye application.

Technical Specifications

The following table lists the technical specifications of PGMZ1M along with their descriptions.
NOTE: *The specifications are subject to change without prior notice.*

Table 3

Specification	Description
Power Input	AC/DC 5-16V, 300mA minimum
Wireless Type	GFSK two-way with frequency and encryption hopping
RF Frequency	868 (865.05 - 867.95) MHz or 914 (902.25 - 927.55) MHz May vary by region.
RF Power	868 MHz: +14 dBm radiated, 914 MHz: up to +22 dBm in permitted countries.
Number of Outputs, inputs	One relay output 24V/1A, One zone input
Status Indicators in Application	Output status indications, tamper status, power supply, temperature, TX/RX values
Transmission Time	Less than 20 ms
Supervision Time	20 minutes, 10 minutes (Default), and 3 minutes
Installation Environment	Indoor/Outdoor
Firmware Upgrade	Remotely over the air, via BlueEye, about 2 minutes after start delay.
Operating Temperature	-30°C to +50°C (-22°F to 122°F)
Auto Learn	Yes
Colors	White
Dimensions	4.6W x 12.45H x 3.3D cm (1.8" W x 4.9" H x 1.3" D)
Weight	77 g
Certification	CE, FCC 15.247 Certification Body: Applica Test & Certification

FCC Statements

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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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:
1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

WARNING – RF EXPOSURE COMPLIANCE: This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC ID: KDYPGMZ1M
   IC: 2438A-PGMZ1M

- This Class B digital apparatus complies with Canadian ICES-003.
- -Cet appareil numerique de la classe B est conforme a la norme NMB-003 du Canada.

IC Statements

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.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

AVERTISSEMENT – CONFORMITÉ AUX NORMES D'EXPOSITION AUX RF: Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Warranty

For complete warranty information on this product, see the Limited Warranty Statement document, or contact your local Paradox distributor.

Patents

US, Canadian, and international patents may apply. Paradox is a trademark or registered trademark of Paradox Security Systems (Bahamas) Ltd.