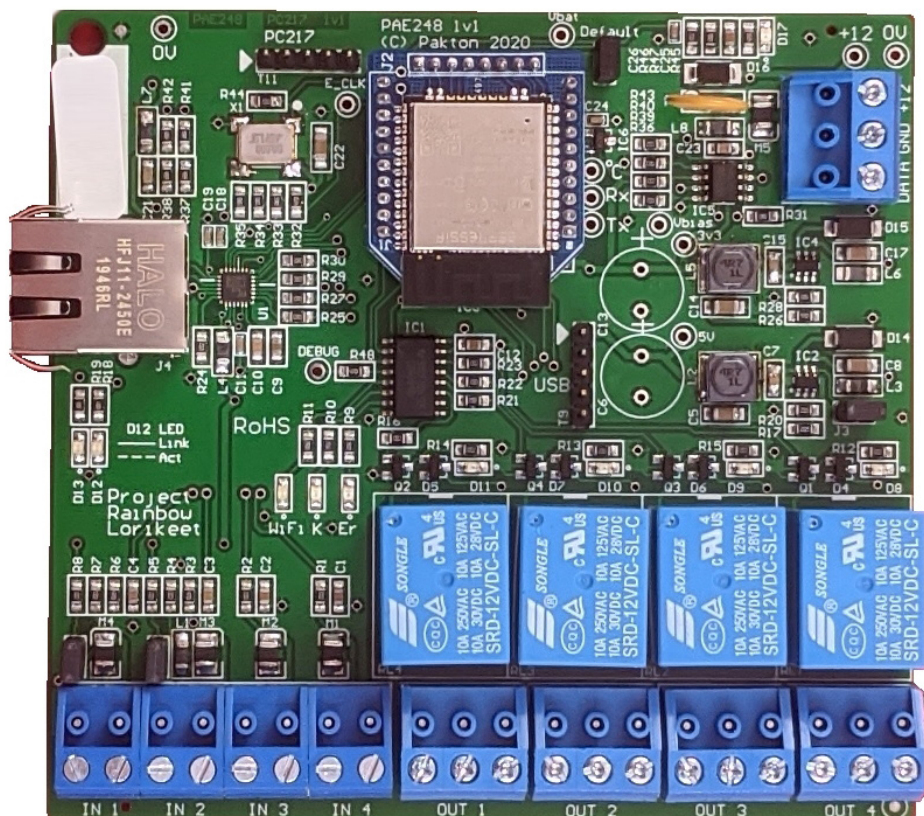


Wi-Fi GPIO MANUAL



CONTENTS

1	INTRODUCTION.....	4
1.1	Variants	4
1.2	Glossary	5
2	SPECIFICATIONS	6
3	VIRTUAL KEYPAD.....	7
3.1	Device Settings	9
3.1.1	Detected Devices	9
3.1.2	Keypad Address	9
3.1.3	User PIN	9
3.1.4	Installer PIN	9
3.1.5	Input Configuration	10
3.1.6	Input Timers	11
3.1.7	Output configuration	12
3.1.8	Output Options - Input Alarm	13
3.1.9	Output Options - Zone Alarm.	13
3.1.10	Output Options - Sector Alarm.	14
3.2	Wi-Fi Settings	15
3.3	IP Settings	16
3.4	TCP Connections	17
3.5	Check for Update	18
3.6	Virtual Keypad Settings.	19
4	PERIMETER PATROL CONFIGURATION	20
4.1	Automatic Detection	20
4.2	Adding Zones	21
4.3	Manually Adding Active Zones	23
5	DESCRIPTION.....	24
5.1	Circuit Board Layout	24
5.2	Default Jumper	24

5.3 Input 1 and 2 Wiring25

5.4 Input 3 and 4 wiring25

5.5 Output States26

5.6 LED Indications27

1 INTRODUCTION

The Z-Series Electric Fence Energizers and Peripheral Devices are designed and manufactured by Pakton Group of Brisbane, Australia.

This document is a User Manual for the JVA Wi-Fi GPIO. It provides stand alone Input and Output functionality to the JVA system.

The inputs can be used monitor devices such as motion detectors, IR beams and door contacts, while the outputs can be used to turn on security lighting, sirens and even water pumps.

This product can be used with the Perimeter Patrol software system or as an Output Expansion for one or more Energizers/Monitors by monitoring their status. Each output is individually configurable to provide a combination of Perimeter Patrol Outputs and Energizer Expansion Outputs on the one device for greater flexibility.

This manual relates to:

PCB version:	1v1 and higher
Firmware version:	2.00 or higher
Current Firmware:	2.00

1.1 VARIANTS

There are 3 separate versions of the Wi-Fi GPIO.

- Perimeter Patrol Interface
- Cloud Router Interface
- IPEC (IP Energizer App)

The default version installed is the Perimeter Patrol Interface. The other two options can be selected through the Check for Updates section in the Virtual Keypad.

As these are separate software version, the Wi-Fi GPIO cannot be both a Perimeter Patrol Interface and a Cloud Router Interface, etc.

1.2 GLOSSARY

GPIO	– General Purpose IO
IO	– Inputs/Outputs
Zone	– A high voltage fence output and return to provide perimeter security.
Sector	– A number of smaller sections of fence which is part of a Zone
On/Armed	– The Energizer is transmitting high (or low) voltage pulses onto the fence. The fence is secure.
Off/Disarmed	– The fence zone is unsecure, but is safe to perform maintenance on.
PCB	– Printed Circuit Board
VPK	– Virtual Keypad. The Web Browser User Interface
PP	– Perimeter Patrol. PC Software for Security Electric Fencing
CR	– Cloud Router. Internet of Things solution for Security Electric Fencing
POE	– Power Over Ethernet

2 SPECIFICATIONS

Specification Name	Specification
Energizer Connection	Keypad Bus (+12, 0V, DAT)
Max Power Consumption (+12Vdc)	300mA
Inputs	4
Switched Outputs	4 x Form C (10 Amp) relay
Recommended Operating Temperature	-15°C to +60°C
Enclosure	IP4x ABS Plastic
Size – PCB only	100mm high, 100mm wide, 30mm deep
Size – Enclosure	120mm high, 72mm wide, 35mm deep
Weight – packed (PCB only)	80 grams
Weight – packed (with Enclosure)	120 grams
POE (Power Over Ethernet)	Not Compatible

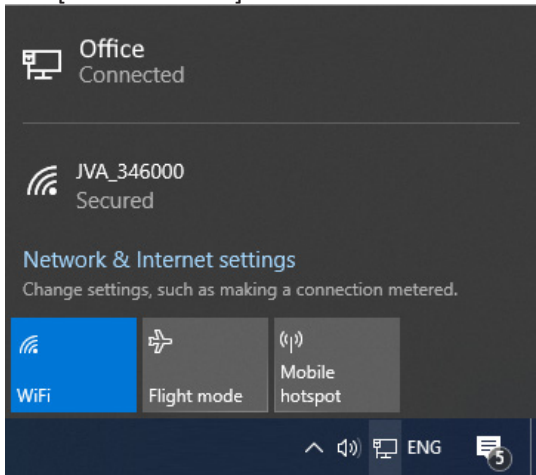
3 VIRTUAL KEYPAD

The Wi-Fi GPIO is configured using a Virtual Keypad accessed via a PC, Smart Phone or Tablet. The PC is connected to the Wi-Fi GPIO via a 2.4GHz link, or through the LAN if the GPIO is already connected to it.

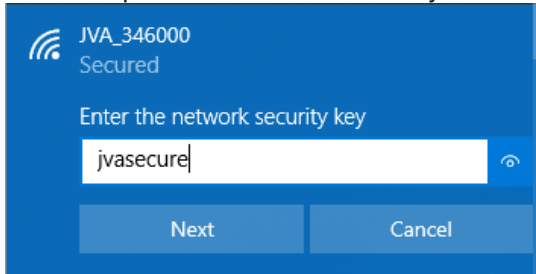
NOTE: The Virtual Keypad Access Point will shutdown 5 minutes after a TCP connection is established to either Perimeter Patrol or a Keydpd. To enable the Virtual Keypad again, either power cycle the Wi-Fi GPIO or use Perimeter Patrol’s Scan function.

If the GPIO is connected to the LAN, skip to step 5.

1. Open the Wi-Fi settings menu and select the Access Point JVA-[Serial Number].

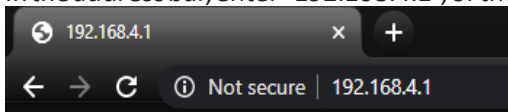


2. Enter the password. The default is “jvasecure”

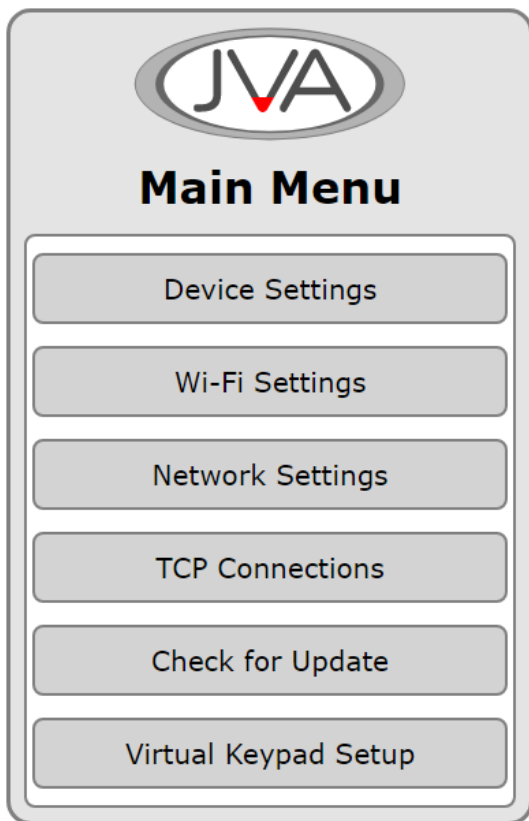


3. The connection does not have Internet Access and if a warning message appears asking to “Remain Connected”, select Yes.
4. Smart phones may require the Mobile Data to be turned off.

5. Open an Internet Browser (Chrome / Firefox recommended).
6. In the address bar, enter "192.168.4.1", or the LAN IP address of the board.

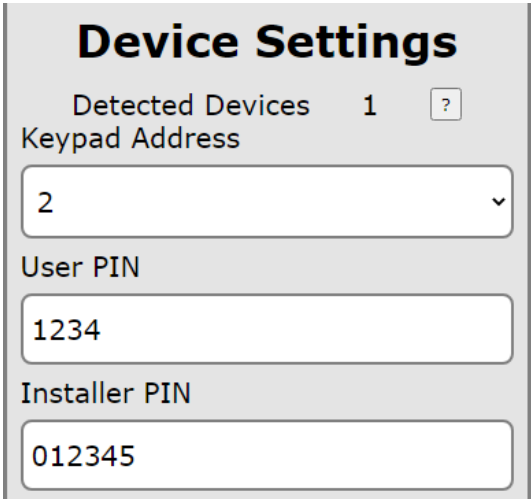


7. The Virtual Keypad page will be displayed. On some devices this page may need to be refreshed once to download all components to the device.



3.1 DEVICE SETTINGS

The device settings page contains the Input and Output configuration options. The Keypad ID option is also updated here.



The screenshot shows a web interface titled "Device Settings". It contains four sections: "Detected Devices" with a count of 1 and a question mark icon; "Keypad Address" with a dropdown menu showing the value 2; "User PIN" with a text input field containing 1234; and "Installer PIN" with a text input field containing 012345.

3.1.1 Detected Devices

This is the number of devices the Wi-Fi GPIO has detected on the Keypad Bus. Press the ? to see a list and description of these. If the list does not match the site, press the Clear Detected Devices button at the bottom of this menu.

3.1.2 Keypad Address

This device acts as a Keypad to control the devices connected on the Keypad Bus. If no other Keypad devices are connected to the Bus, leaving this at ID 2 is a decent option. All Keypad devices must have a unique Keypad Address.

3.1.3 User PIN

This needs to be changed to the User PIN on the site to Arm/Disarm the Wi-Fi GPIO using a Keypad.

3.1.4 Installer PIN

This needs to be changed to the Installer PIN on the site so that Installer PIN commands are recognised correctly. This is necessary for Menu Driven Programming using the 4-line Keypad or Touch Keypad.

3.1.5 Input Configuration

Input 1

Pass Thru ▼

Arm My Group

Alarm Instant

Alarm 3sec

Alarm Gate

Entry/Exit Route

Entry Route

Exit Route

Pass Thru

Tamper

N/O ▼

N/C

N/O

Tag

Analog

All Alarms are Latched (unless otherwise stated). The Alarms require the Wi-Fi GPIO to be Armed (through PP, CR, Keypad) before they will activate. Latched alarm are cleared when Disarmed or Cleared through PP, CR or a Keypad.

Function	Description
Arm My Group	The Input will send an Arm All/Disarm All command to the devices connected to the Keypad Bus.
Alarm Instant	An Input Alarm will trigger on Input Activation.
Alarm 3sec	An Input Alarm will trigger after 3 seconds of continuous Input Activation.
Alarm Gate	The Input will trigger on continuous Input Activation for the Gate Time value.
Entry/Exit Route	Combined Entry and Exit route system.
Entry Route	When activated, the Entry Time starts to count down. The Alarm will trigger if the timer reaches zero and the GPIO is not disarmed. This allows someone to enter the site through a dedicated path and access a keypad to disarm without triggering the alarm.
Exit Route	Inputs configured as Exit are “bypassed” for the Exit Delay after the GPIO is armed. This allows someone to arm and then exit the site through a dedicated path.

Function	Description
Pass Thru	The value of the Input is passed to Perimeter Patrol.
Tamper	A Tamper Alarm will trigger on Input Activation.
Panic Alarm	(24hr alarm). This triggers the Panic Alarm in the GPIO. PP, CR, Keypad will indicate "Panic" (when fully implemented).
Silent Alarm	(24hr alarm). This triggers the Silent Alarm in the GPIO. PP and CR will indicate "Silent Alarm" (when fully implemented).
Alarm Instant 24hr	(24hr alarm). This alarm is not latched. It will follow the Input state allowing an alarm that does not require clearing through PP, CR, or a Keypad.

Function	Description
N/C	The Input is Normally Closed. Activation when Open.
N/O	The Input is Normally Open. Activation when Closed.
Tag	Activation toggles ON/OFF when the Input changes momentarily.
Analog	Inputs 1 and 2 can be configured to measure a 0-10Vdc voltage and pass this through to Perimeter Patrol.

3.1.6 Input Timers

The Input timers are configurable to the second. This provides simple flexibility through an easy to use drop-down interface.

The timeout selected is used across all Inputs configured for the same function. Therefore if two Inputs are configured for Gate Alarm, they will both operate independently, but the timeout will be the same.

Gate Time

1 min ▾

0 sec ▾

Entry Time

0 min ▾

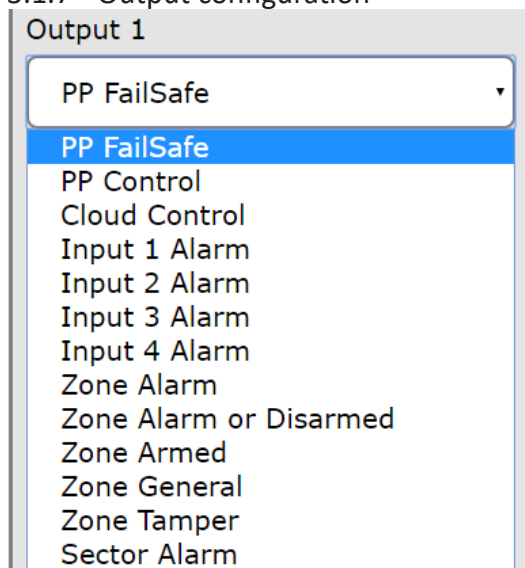
30 sec ▾

Exit Time

1 min ▾

30 sec ▾

3.1.7 Output configuration



Function	Description
PP FailSafe	Controlled by Perimeter Patrol. If the connection to Perimeter Patrol is broken for 30 seconds, the Output will trigger.
PP Control	Controlled by Perimeter Patrol. If the connection is broken, the current output state will remain.
Cloud Control	Controlled by Cloud Router
Input 1 Alarm	The output will trigger if Input 1 Alarms
Input 2 Alarm	The output will trigger if Input 2 Alarms
Input 3 Alarm	The output will trigger if Input 3 Alarms
Input 4 Alarm	The output will trigger if Input 4 Alarms
Zone Alarm	The output will trigger based on the Alarm Information from a device connected to the Keypad Bus
Zone Alarm or Disarmed	The output will trigger based on the Alarm Information from a device connected to the Keypad Bus. If the device is Disarmed, it will also trigger
Zone Armed	The output will trigger depending on Arm state of the device connected on the Keypad Bus

Function	Description
Zone General	The output will trigger if the device connected on the Keypad Bus indicates a General Alarm
Zone Tamper	The output will trigger if the device connected on the Keypad Bus indicates a Tamper Alarm
Sector Alarm	The output will trigger if the connected ZM20/ZM50 device indicates the Sector is in Alarm.

3.1.8 Output Options - Input Alarm

Output 1

Input 1 Alarm ▼

Pulse Time. 0=Mimic Alarm

0 min ▼
0 sec ▼

A pulse time can be selected for an Input Alarm. This allows the output to automatically reset either after the alarm clears or the pulse time elapses, whichever happens first.

As the “Instant Alarm 24hr” function is not a latched alarm, setting a pulse time will ensure this is effectively latched for this pulse time.

3.1.9 Output Options - Zone Alarm

Output 1

Zone Alarm ▼
Any Zone ▼

Pulse Time. 0=Mimic Alarm

0 min ▼
0 sec ▼

When an output is configured as a Zone Alarm, the choice of the specific zone is made available. If the Any Zone option is chosen then the output will trigger if any connected zones indicate the specific alarm type.

A pulse time can be selected for an Input Alarm. This allows the output to automatically reset either after the alarm clears or the pulse time elapses, whichever happens first.

3.1.10 Output Options - Sector Alarm

Output 1

Sector Alarm ▾

Any Z ▾

Any S ▾

Pulse Time. 0=Mimic Alarm

0 min ▾

0 sec ▾

When an output is configured as a Sector Alarm, the choice of the specific zone and sector is made available.

A pulse time can be selected for an Input Alarm. This allows the output to automatically reset either after the alarm clears or the pulse time elapses, whichever happens first.


3.2 WI-FI SETTINGS

Wi-Fi Settings

Device Serial346000

Access Point SSID

Access Point Password



Scan

Connecting to an Access Point will disable the Ethernet Hardware. This board will reset to complete this change.

Connect

Main Menu

The Wi-Fi settings pages allows the JVA Wi-Fi GPIO to connect to a 2.4GHz Access Point (AP) to transfer data to Perimeter Patrol. Be aware that this will disable the Ethernet Port.

The Scan button will start a search for nearby Access Points and these will be displayed in the list. The signal strength of each AP will be listed next to the SSID. When comparing APs, the smaller dB value indicates a stronger signal. For example -56dB is stronger than -89dB.

Select the SSID from the list and then enter the AP password into the box. If you need privacy when entering the password, click on the eye next to the box. Press the Connect button to complete the process. The GPIO will restart.

3.3 IP SETTINGS

Network Settings

☒ DHCP

Current IP Address

192.168.1.115

Static IP Address

192.168.0.38

Subnet Mask

255.255.255.0

Gateway

192.168.1.1

DNS

192.168.1.1

Save Config

The Network Settings page is used to alter the network interface values. These options are normally configured directly in Perimeter Patrol, however this option provides an alternative.

If the Wi-Fi GPIO is connected to a LAN and DHCP is checked, the values listed will have been provided by the LAN DHCP Server.

Un-checking the DHCP value and changing the IP address requires advanced knowledge of the LAN configuration to ensure there is not an IP address conflict.

3.4 TCP CONNECTIONS

TCP Connections

Device Serial346000

The maximum number of TCP connections is 4

Secure Connection Count

0

TCP port 17290

Encryption Key

5afd840629a2bdb7f1c1

Un-secure Connection Count

1

TCP port 17289

NOTES:
Increasing a value from Zero will require a reset
Decreasing a value to Zero will require a reset

Save Config

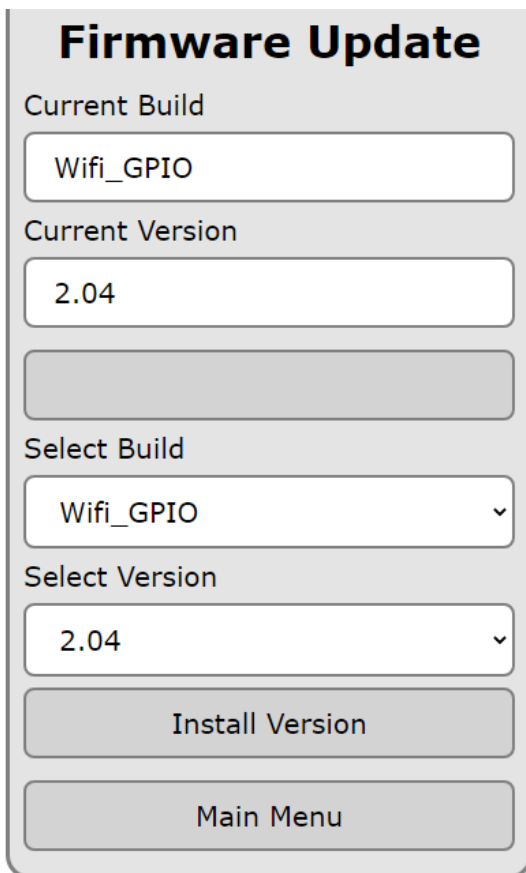
The TCP Connections page is used to limit the number of secured (Encrypted) and unsecured connections. If the Wi-Fi GPIO is to be connected to Perimeter Patrol and a Touch Screen keypad, then two TCP connections will be required. These will normally be unsecured connections.

If more secure communications are required on the site, then the Secure Count will need to be altered. The Encryption Key will need to be entered into Perimeter Patrol or the keypad for this to work. The Key is unique to each Wi-Fi GPIO.

A screen capture of this page can be very useful as it provides both the Serial Number of the Wi-Fi GPIO and the Encryption Key.

A reset may be required after saving the updated configuration.

3.5 CHECK FOR UPDATE



Firmware Update

Current Build

Wifi_GPIO

Current Version

2.04

Select Build

Wifi_GPIO

Select Version

2.04

Install Version

Main Menu

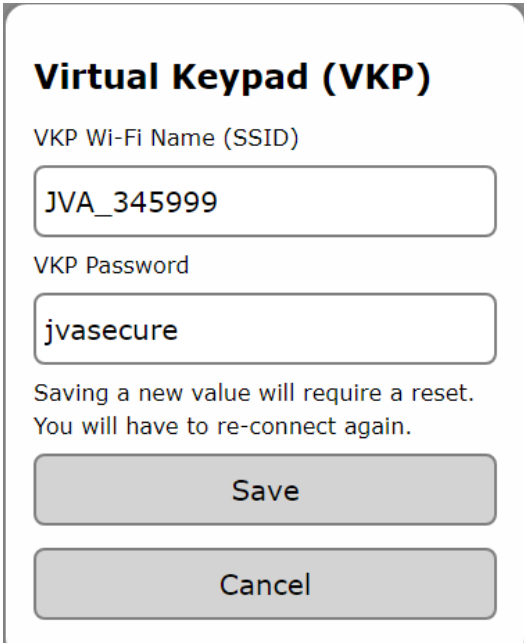
The Update system requires that the Wi-Fi GPIO is connected to the Internet. The wired Ethernet Connection is the preferred method, however a connection over Wi-Fi will work, just slower.

When this page is opened the system will automatically check if a newer version is available. The “Select Version” box will be updated with the latest version that can be Installed by pressing the “Install Version” button.

Changing the Build allows the Wi-Fi GPIO to be configured to connect to the Cloud Router system, or the IPEC App. This will ‘uninstall’ the PP Interface software. This requires a manual factory default after the new software has been installed to ensure correct operation.

The VKP User Interface will change depending on the Build.

3.6 VIRTUAL KEYPAD SETTINGS



Virtual Keypad (VKP)

VKP Wi-Fi Name (SSID)

JVA_345999

VKP Password

jvasecure

Saving a new value will require a reset.
You will have to re-connect again.

Save

Cancel

The VKP Wi-Fi Name (SSID) and VKP Password can be changed. This affects the Virtual Keypad when using the Wi-Fi Access Point. It is good practice to change the Password from the default value of “jvasecure” to stop unauthorised configuration of these devices.

Changing the SSID Name can be useful to “Name the Location” instead of relying on the default “JVA_[Serial Number]” SSID.

Any change to these settings will trigger a reset of the device and as the AP details have changed, a new Wi-Fi connection will need to be established to access the Virtual Keypad again.

4 PERIMETER PATROL CONFIGURATION

In Perimeter Patrol open the System Configuration window (Setup -> System Configuration...)

1. In the Zones Tab, Select the Ethernet option
2. Press the **Add/Remove Zones** button

4.1 AUTOMATIC DETECTION

JVA Add/Remove Zones

Interface to scan: 192.168.0.230 - Ethernet 4 Scan

Detected Ethernet Devices:

- ☒ ETH-345999 - 192.168.0.42 - ID0
- ☐ ETH-346000 - 192.168.0.43 - ID0
- ☐ ETH-362006 - 192.168.0.152 - ID3

Detected Zones:

- ☐ ETH-345999:1:1 (Ethernet Digital IO Expander)
- ☐ ETH-346000:1:1 - 6000 (Ethernet Digital IO Ex)
- ☐ ETH-362006:2:1 (Z28)
- ☐ ETH-362006:2:2 (Z28)

Check None Check All

Selected Ethernet Device

Net. Name: ETH-345999 *Firmware 2v00*

IP Address: 192.168.0.42

Ethernet ID: 0

DHCP: ☒ New Settings: ☒

Static IP: 192.168.0.42 192.168.0.42

Subnet Mask: 255.255.255.0 255.255.255.0

Gateway: 192.168.0.222 192.168.0.222

DNS: 192.168.0.222 192.168.0.222

MAC: C8:90:3E:05:47:8F

Count: 1 Clear Known Energisers List

Assign Unique Ethernet IDs to Checked Devices

Commit Changes to Ethernet Devices

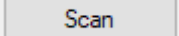
zones used 2/50 NOTE: If zone not detected, try disarming

Energiser Type: Z14

Contact Using:

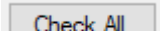
- Z11
- Z13
- Z14
- Z14 Bipolar
- Z14R
- Z14R Bipolar
- Z18
- Z18 Bipolar
- Z114
- Z114 Bipolar
- Z25
- Z28
- ZM1
- ZM20
- ZM50
- ZLM1
- ZLM4
- JMB ZM1
- JMB ZM2
- JMB ZM50
- JMB Sec
- JMB Agric
- In/Out Expander
- Ethernet IO Expander
- Ethernet Digital IO Expander

1. Select the Interface to Scan. This is the connection to the LAN.

- Press the  button. This will detect all of the Ethernet devices connected to the same network as Perimeter Patrol. These will be displayed in the Detected Ethernet Devices box

Contact Using	Network Name
Network Name	Network Name
Keypad Bus ID	IP Address
	DNS Lookup

Contact Using	IP Address
IP and Port	192.168.0.42 0

- Press the  button.

- Now press both

Assign Unique Ethernet IDs to Checked Devices
Commit Changes to Ethernet Devices

This will ensure that all energizers will be synchronised and able to respond to Perimeter Patrol commands.

- Tick each detected ethernet device in turn and assign new settings:
 - Disable DHCP (recommended)
 - Enter a Static IP Address (one that is un-used)
 - Update the Subnet Mask/Gateway/DNS if required

- Click to save

Commit Changes to Ethernet Devices

- The Count box at the bottom of the list indicates the number of Keypad Bus devices the GPIO has remembered. If this number does not match the number of Energizers/Monitors connected, press the

Clear Known Energisers List

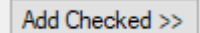
button. This forces the device to re-evaluate the Keypad bus similar to the *68# function of a Keypad. Press the

Scan

button again to update the Detected Zones box.

4.2 ADDING ZONES

- In the Detected Zones box, check the Zones to be added to Perimeter Patrol.

- Click on the  button

The Detected Zones follow this numbering:

ETH-[SerialNumber]:Y:Z

- Where **ETH** represents **Ethernet Interface**
- [Serial number]** is the Serial Number of the device
- Y** is the **Group ID** number of the Energizer (26xx#) with values from **2** to **15**

- **Z** is the **Zone number** of that Energizer. **1** for a Single Zone Energizer, **1** or **2** for a Dual Zone Energizer

Detected Zones:		Active Zones:	
<input checked="" type="checkbox"/>	ETH-345999:1:1 (Ethernet Digital IO Expander,	<input type="checkbox"/>	ETH-345999:1:1
<input checked="" type="checkbox"/>	ETH-345999:2:1 (Z14)	<input checked="" type="checkbox"/>	ETH-345999:2:1
<input checked="" type="checkbox"/>	ETH-346000:1:1 (Ethernet Digital IO Expander,	<input type="checkbox"/>	ETH-346000:1:1
<input type="checkbox"/>	ETH-362006:2:1 (Z28)		
<input type="checkbox"/>	ETH-362006:2:2 (Z28)		

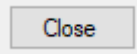
Check None	Check All	Delete Checked
Move Up	Move Down	Delete

Selected Active Zone	
Name	<input type="text"/>
Energiser Type	Z14 <input type="button" value="v"/>
Contact Using	Network Name <input type="button" value="v"/>
Network Name	ETH-345999
Keypad Bus ID	2
Zone (Channel)	1

Check None	Check All	Add Checked >>	Add New	Close
------------	-----------	----------------	---------	-------

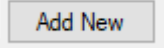
All Zones that are Added to the system will be displayed in the Active Zones box. Select each Active Zone in turn and update the following:

- Name
- Energizer Type. If the detected device chosen is incorrect, the value can be changed. For example a ZM50 device is automatically detected as a ZM20. The ZM20 option limits the sector count to 20.

- Connect Using. If the device was configured for a Static IP, the recommendation is to change this to IP Address. The IP address will be displayed. Leave the Port at 0 to use the default connection port.
3. Press the  button when you have finished editing the devices.
 4. The Map window of Perimeter Patrol will now have all of the Active Zone boxes in the top Left Corner of the Map

4.3 MANUALLY ADDING ACTIVE ZONES

An Active Zone can be added to Perimeter Patrol before the Wi-Fi GPIO is connected to the LAN, or before the Energizer is connected to the keypad bus. This requires knowledge of the Energizer Group ID and the expected Wi-Fi GPIO IP Address.

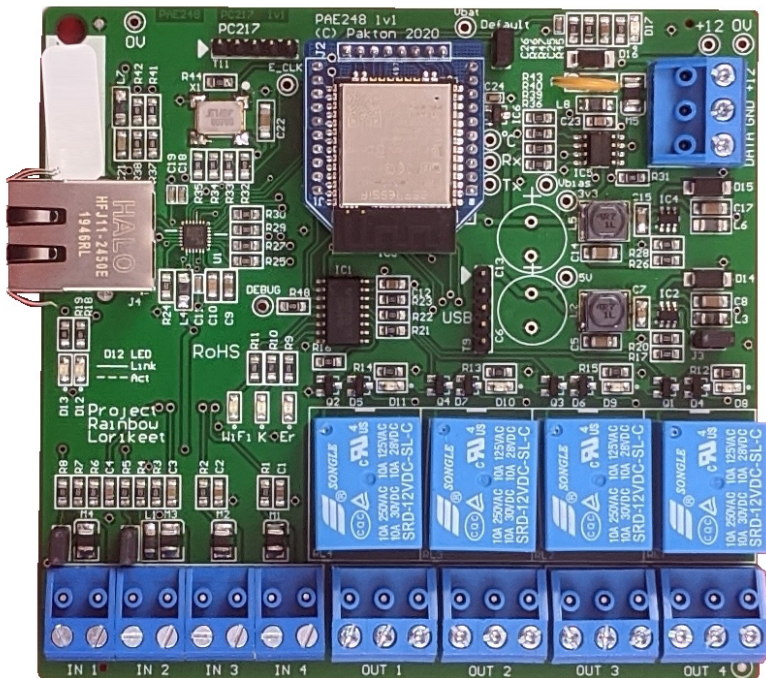
1. Pressing the  button in the Active Zones section will create a new Active Zone entry
2. Select the newly created Zone and then update all of the Zone information
 - Enter a suitable Name for the Zone
 - Select the Energizer Type from the list.
 - Connect Using. Choose IP Address
 - IP and Port. Enter the intended IP address of the GPIO.
 - Enter the Group ID of the Energizer into the Keypad Bus ID box
 - Enter the Zone (Channel) number. This will always be 1 except for a Z-28

Both Zones of a Z-28 need to be Added to the Active Zones box separately. The difference between the settings for these is the Zone (Channel) value. 1 for Zone 1, 2 for Zone 2.

When the Energizer and Wi-Fi GPIO are connected to the LAN, the Zone will become active on the Map page. Until this occurs, the Zone will display Coms Fail.

5 DESCRIPTION

5.1 CIRCUIT BOARD LAYOUT

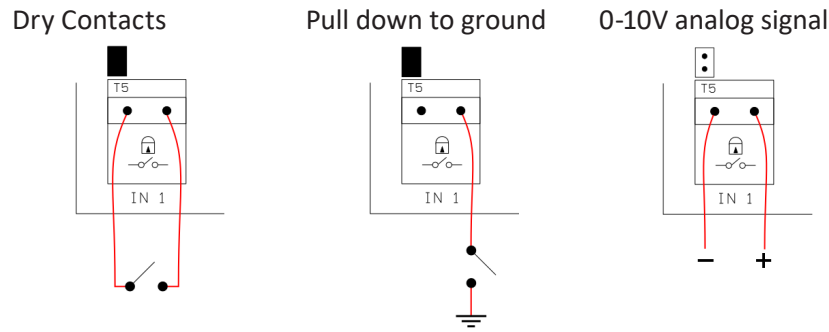


5.2 DEFAULT JUMPER

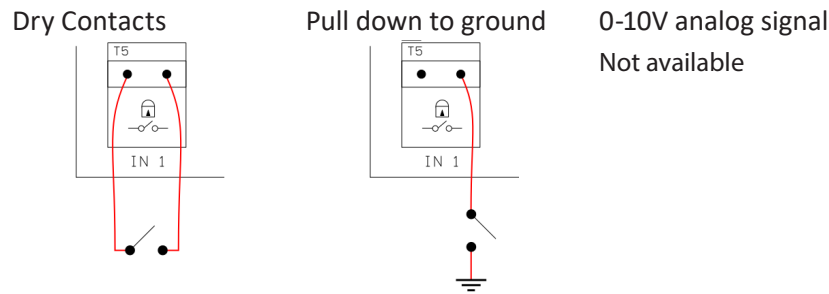
This black jumper/shunt is located on the top edge of the board. To return the Wi-Fi GPIO to factory defaults, remove the shunt and power-cycle the board. This will reset all settings to default and all detected devices will be cleared.

Fit the J4 jumper/shunt back onto both pins after 5 seconds to ensure that new settings are remembered.

5.3 INPUT 1 AND 2 WIRING



5.4 INPUT 3 AND 4 WIRING

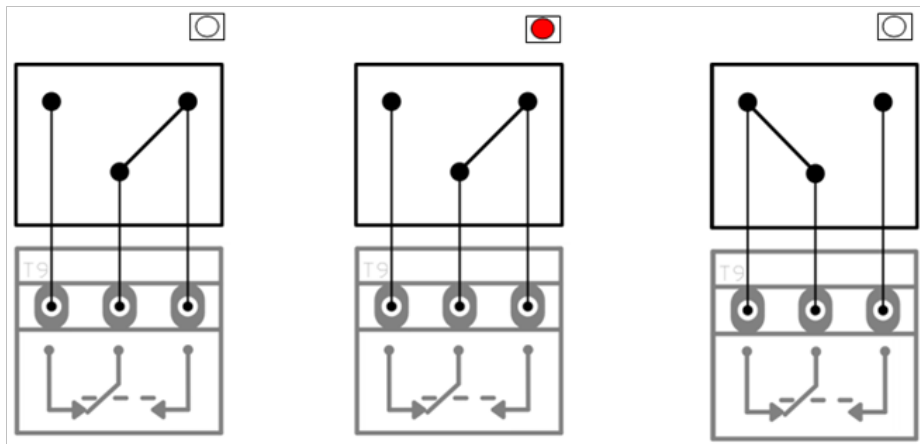


5.5 OUTPUT STATES

Without Power

Relay Function in Alarm/
Coms Fail to Energizer/
Perimeter Patrol
Disconnected

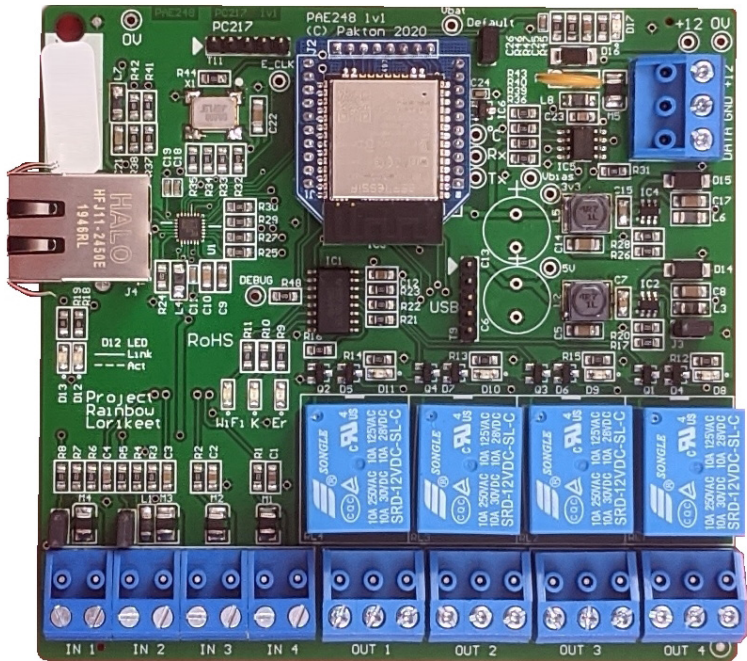
Relay Function
not in Alarm



When an Output is configured as PP FailSafe (default setting for all outputs) or PP Controlled, the Output State will vary depending on how Perimeter Patrol is configured for this output.

If the Output is configured as PP FailSafe the relay will go into the Alarm state 30 seconds after a disconnection to Perimeter Patrol. Or at 30 seconds from power-up if Perimeter Patrol does not connect to it.

5.6 LED INDICATIONS



LED	Information
Wi-Fi	1 Flash - Access Point is read for connection 2 Flash - Device connected to Access Point 3 Flash - Connected to LAN via Wi-Fi
K	Data is seen on the Keypad Bus
Er	This is the Error LED
D13 and D12 Ethernet LEDs	Both OFF - Ethernet system is disabled D13 ON - Ethernet system is enabled, not connected D14 Flashing - Ethernet connected to LAN



DEALER

Manufactured for JVA by Pakton Group
The JVA logo is trademark of JVA Technologies Pty Ltd
PTE0248 User Manual Version 24



WWW.JVA-FENCE.COM