

## User Manual - PPS-04-S

### GUI & SNMP for Z series IP PDU



Designed and manufactured by Austin Hughes



## Legal Information

First English printing, April 2025

Information in this document has been carefully checked for accuracy; however, no guarantee is given to the correctness of the contents. The information in this document is subject to change without notice. We are not liable for any injury or loss that results from the use of this equipment.

## Safety Instructions

**Please read all of these instructions carefully before you use the device. Save this manual for future reference.**

- Unplug equipment before cleaning. Don't use liquid or spray detergent; use a moist cloth.
- Keep equipment away from excessive humidity and heat. Preferably, keep it in an air-conditioned environment with temperatures not exceeding 40° Celsius (104° Fahrenheit).
- When installing, place the equipment on a sturdy, level surface to prevent it from accidentally falling and causing damage to other equipment or injury to persons nearby.
- When the equipment is in an open position, do not cover, block or in any way obstruct the gap between it and the power supply. Proper air convection is necessary to keep it from overheating.
- Arrange the equipment's power cord in such a way that others won't trip or fall over it.
- If you are using a power cord that didn't ship with the equipment, ensure that it is rated for the voltage and current labelled on the equipment's electrical ratings label. The voltage rating on the cord should be higher than the one listed on the equipment's ratings label.
- Observe all precautions and warnings attached to the equipment.
- If you don't intend on using the equipment for a long time, disconnect it from the power outlet to prevent being damaged by transient over-voltage.
- Keep all liquids away from the equipment to minimize the risk of accidental spillage. Liquid spilled on to the power supply or on other hardware may cause damage, fire or electrical shock.
- Only qualified service personnel should open the chassis. Opening it yourself could damage the equipment and invalidate its warranty.
- If any part of the equipment becomes damaged or stops functioning, have it checked by qualified service personnel.

## What the warranty does not cover

- Any product, on which the serial number has been defaced, modified or removed.
- Damage, deterioration or malfunction resulting from:
  - ☐ Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
  - ☐ Repair or attempted repair by anyone not authorized by us.
  - ☐ Any damage of the product due to shipment.
  - ☐ Removal or installation of the product.
  - ☐ Causes external to the product, such as electric power fluctuation or failure.
  - ☐ Use of supplies or parts not meeting our specifications.
  - ☐ Normal wear and tear.
  - ☐ Any other causes which does not relate to a product defect.
- Removal, installation, and set-up service charges.

## Regulatory Notices Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in business, industrial and commercial environments.

Any changes or modifications made to this equipment may void the user's authority to operate this equipment. 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:

- Re-position 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.

# Contents

## < Section 1 > General

< 1.1 >	Key Features of PPS-04-S WEBUI	P.1
< 1.2 >	Z series IP PDU Meter Specification	P.2
< 1.3 >	M series serial PDU Meter Specification	P.3
< 1.4 >	Initial network configuration of Z series IP PDU	P.4
< 1.5 >	PDU Cascade	P.5
< 1.6 >	PDU Level Setting	P.6
< 1.7 >	Login PPS-04-S WEBUI	P.6
< 1.8 >	Remote PDU Level Setting	P.7

## < Section 2 > Usage of WEBUI ( PPS-04-S )

< 2.1 >	PPS-04-S ( WEBUI for Z series IP PDU )	P.8
< 2.2 >	Outlet Grouping	P.11
< 2.3 >	Outlet Sequencing	P.12
< 2.4 >	System	P.14
< 2.5 >	Network	P.15
< 2.6 >	Wifi Network Configuration	P.16
< 2.7 >	Login	P.23
< 2.8 >	SNMP Setup	P.30
< 2.9 >	Notification	P.35
< 2.10 >	Syslog	P.36
< 2.11 >	Firmware upgrade of Z series IP PDU	P.37
< 2.12 >	Bulk Firmware Upgrade of Z series IP PDU	P.39
< 2.13 >	802.1X authentication	P.51

## < Section 3 > Command Line Interface Access

< 3.1 >	Command Line Interface Access	P.57
---------	-------------------------------	------

## < Section 1 > General

### < 1.1 > Key Features of PPS-04-S WEBUI

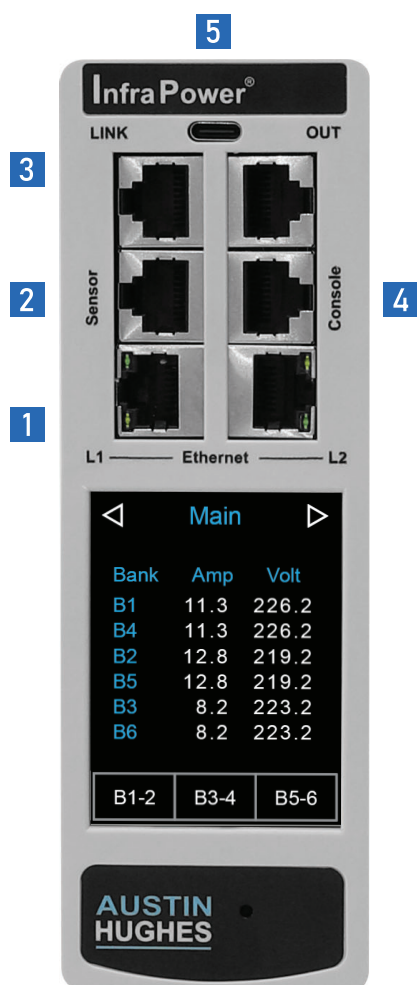
#### InfraPower PPS-04-S

Features		
Capacity	Max PDU number per Z series IP PDU	32
	Concurrent Users	1
Enhanced Features	Power-on Sequencing with Customized Delays	✓
	Customized Outlet Power-on Sequencing **	✓
	Outlet Grouping Across Linked PDUs **	✓
	Outlet ON / OFF / Power Cycle in Group **	✓
	Outlet Level kWh & Amp Measurement	✓
	Energy Consumption ( kWh ) Monitoring	✓
	Apparent Power ( kVA ) Monitoring	✓
	Power Factor Measurement	✓
	Circuit Breaker ( MCB ) Monitoring	✓
	Remote level & ID Setting for Cascaded iPDU	✓
Basic Features	Aggregate Current ( Amp ) Monitoring	✓
	Individual Outlet Switch ON / OFF	✓
	Temp-Humid Monitoring	✓
	Alarm Threshold Setting	✓
	Rising Alert Setting	✓
	Remote Access via Web	✓
	Graphic User Interface	✓
PDU Series Support	All Single & Three Phase iPDU	✓
	All Single & Three Phase Dual Feed iPDU	✓
	All Single & Three Phase inline meter	✓
	All Single & Three Phase Dual Feed inline meter	✓

\*\* : For Z & M series PDU only

## < 1.2 > Z series IP PDU Meter Specification

	IP PDU Series			
	Z-2100 ( Z )	Z-2200 ( Zi )	Z-2300 ( ZS )	Z-2400 ( ZSi )
Embedded Dual IP	•	•	•	•
Strip Power Monitoring	•	•	•	•
Circuit Power Monitoring	•	•	•	•
Circuit Breaker Monitoring	•	•	•	•
Outlet Level Monitoring		•		•
Outlet Level Switching			•	•



### Z IP Meter

- 1 Embedded dual LAN IP
  - 2 Sensor port x 1
    - support single or daisy chain sensors ( up to 4 )
  - 3 LINK & OUT cascading ports
    - up to 32 levels of M / Z meter iPDU
  - 4 Console port x 1
    - PDU configuration
  - 5 USB-C function port x 1
    - WIFI
    - firmware update
    - backup power for meter against PDU power failure
- \* The latest Z PDU controller, powered by ARM9 CPU ( Microchip AT91SAM9G25 )

#### 2.8" Touchscreen Color Display

The sharp & highly visible display of 2.8" touchscreen LCD provides local data of:

- Energy Consumption (kWh)
- Power (KW)
- Power Factor
- Current (Amp)
- Voltage (V)
- Temperature & Humidity

#### Billing Grade Meter Accuracy

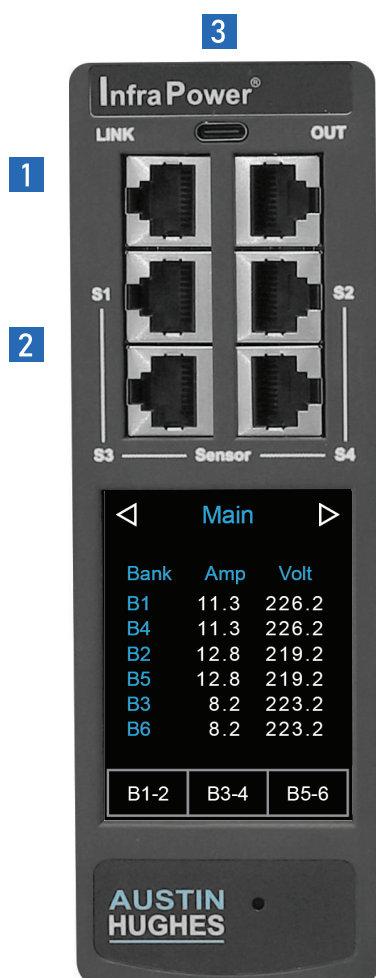
The +/- 0.5% accuracy of the InfraPower PDU meter is vital for billing accuracy, energy efficiency, capacity planning and performance monitoring.

#### Hot-swappable Meter Design

Easily replace meter & power module without interrupting critical operations, ensuring maximum uptime and flexibility. Simplify maintenance and minimize downtime with this innovative and user-friendly solution.

## < 1.3 > M series serial PDU Meter Specification

	Serial PDU Series			
	M-2100 ( M )	M-2200 ( Mi )	M-2300 ( MS )	M-2400 ( MSi )
Embedded Dual IP	×	×	×	×
Strip Power Monitoring	•	•	•	•
Circuit Power Monitoring	•	•	•	•
Circuit Breaker Monitoring	•	•	•	•
Outlet Level Monitoring		•		•
Outlet Level Switching			•	•



### M Serial Meter

\* IP connection via Z meter PDU or IP dongle

- 1 LINK & OUT cascading ports
  - up to 32 levels of M / Z meter iPDU
- 2 Sensor port x 4
  - support single or daisy chain sensors
- 3 USB-C function port x 1
  - backup power for meter against PDU power failure

#### 2.8" Touchscreen Color Display

The sharp & highly visible display of 2.8" touchscreen LCD provides local data of:

- Energy Consumption (kWh)
- Power (KW)
- Power Factor
- Current (Amp)
- Voltage (V)
- Temperature & Humidity

#### Billing Grade Meter Accuracy

The +/- 0.5% accuracy of the InfraPower PDU meter is vital for billing accuracy, energy efficiency, capacity planning and performance monitoring.

#### Hot-swappable Meter Design

Easily replace meter & power module without interrupting critical operations, ensuring maximum uptime and flexibility. Simplify maintenance and minimize downtime with this innovative and user-friendly solution.

## < 1.4 > Initial Network Configuration of Z series IP PDU

You can configure the Z series IP PDU by connecting it to a computer or to a TCP/IP network that supports DHCP. If the computer or the TCP/IP network does not support DHCP, the Z series IP PDU will configure an IP address automatically. An IPv4 address 192.168.0.1 will be assigned to LAN 1 and an IPv4 address 192.168.11.1 will be assigned to LAN2.

Configuration over a DHCP-enabled network :

1. Connect a Cat 5e / 6 cable to one of the LAN port of Z series IP PDU.
2. Connect the other end of the Cat 5e / 6 cable to your TCP/IP network.
3. Get the DHCP assigned IPv4 address which can be found on the “ **Network** ” page of the touchscreen LCD display.
4. Open a web browser to enter the DHCP assigned IPv4 address into the address bar to access the login page.

Configuration using a connected computer :

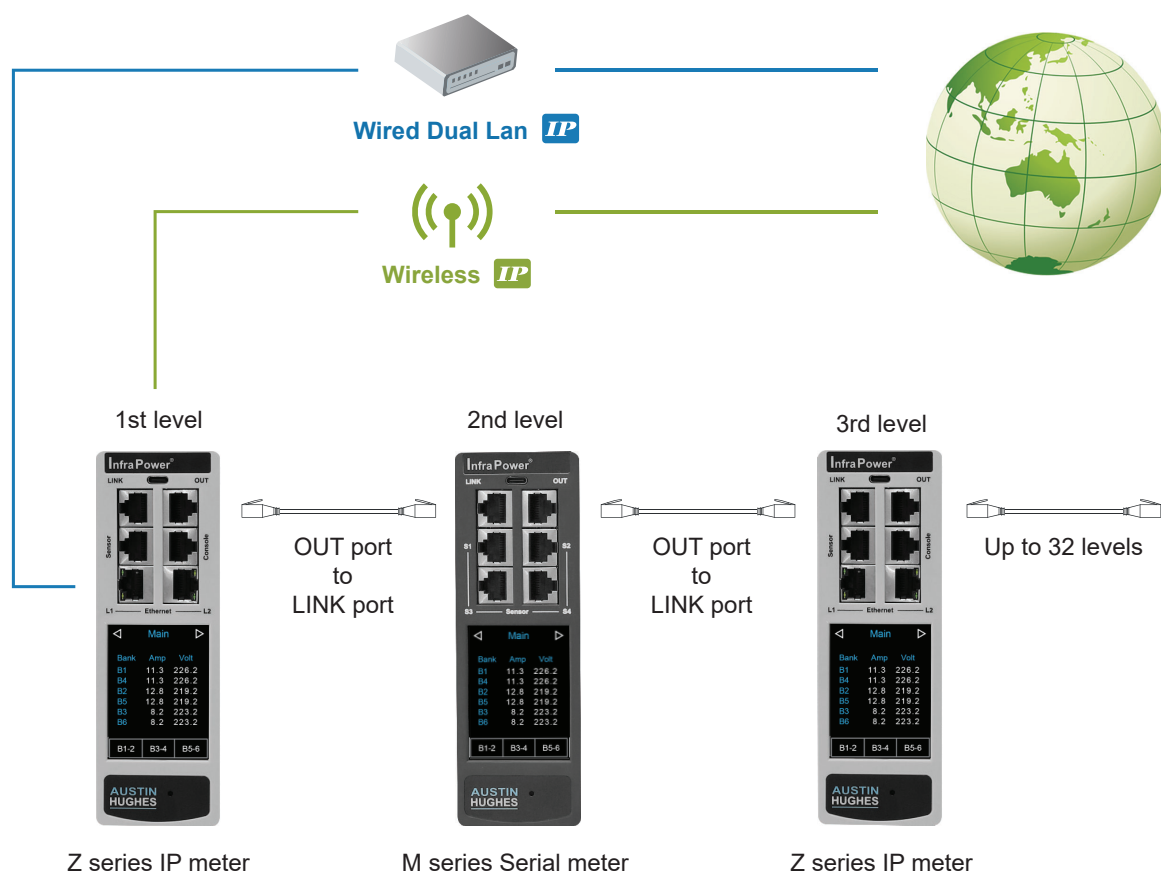
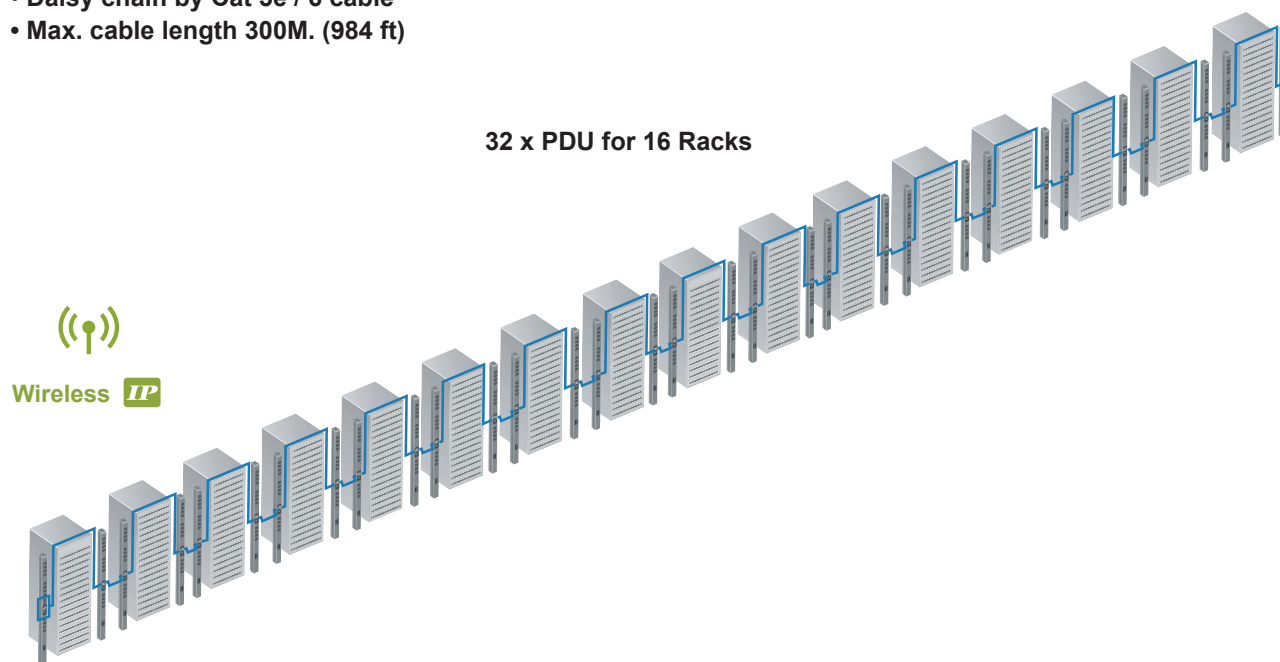
1. Connect a Cat 5e / 6 cable to one of the LAN port of Z series IP PDU and the computer.
2. Configure the IP setting of the computer as the same network of the connected LAN port of the Z series IP PDU.
3. Default IP setting of the Z series IP PDU will be assigned automatically.

LAN 1 IP address :	192.168.0.1	LAN 2 IP address :	192.168.11.1
Subnet Mask :	255.255.0.0	Subnet Mask :	255.255.0.0
Gateway :	N/A	Gateway :	N/A
4. Open a web browser to enter the assigned IPv4 address into the address bar to access the login page.



## < 1.5 > PDU Cascade

- One Z series IP PDU can connect max. 31 x PDUs ( M / Z series, One / Three Phase PDU )
- Daisy chain by Cat 5e / 6 cable
- Max. cable length 300M. (984 ft)

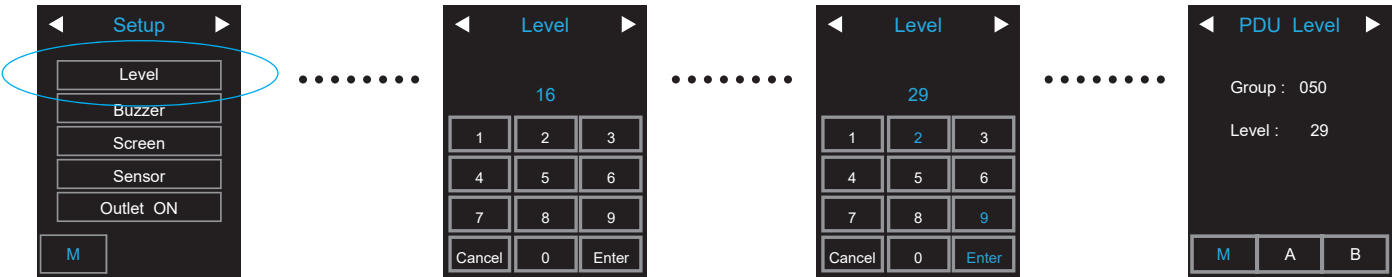


- Only 1st level Z series IP PDU can provide the function of PPS-04-S ( Please refer to Section II for details )
- For those Z series IP PDUs act as expansion unit, please DO NOT connect any LAN cable to LAN1 and LAN2 port of the Z series IP Meter.



< 1.6 > PDU Level Setting

1. PDU Level Setting on local meter display



2. PDU Level Setting by Remote ( see < 1.8 > Remote PDU Level Setting )

< 1.7 > Login PPS-04-S WEBUI

- 1. Open a browser and type the IP address of the Z series IP PDU.
- 2. The login page displays. Input the login name and password. Default login name is “00000000” and default login password is “00000000”. You are required to change the login password if this is the first time you login the WEBUI

Device Z IP PDU

You are required to change the default password.

Login name

Default Password

New Password

Confirm Password

Apply

Cancel

3. After change the login password, the login page changes as the image shown below. Input the login name and the new password.

Device Z IP PDU

Login name 00000000

Password

Login

Cancel

4. Click “Login” and the WEBUI similar to the following image opens.

Status

Z IP PDU name : default\_z4m\_name

LAN 1 IPv4 address : not available

LAN 2 IPv4 address : 192.168.0.1

LAN 1 IPv6 address : not available

LAN 2 IPv6 address : ::ffff:c0a8:1f120

Level	Name	Location	Amp					kWh		kVA		Total			Sensor 1	
			Max.	Load	Alarm	R. alert	L. alert			Amp	kWh	kVA	Load			
01	default_pdu_name	default_pdu_loc.	Circuit A	16.000	0.000	12.800	0.000	0.000	0.00	0.00			0.000	0.00	0.00	-

☐ Auto data refresh :  Untick during data input

Search


Search new installed devices

Time Sync

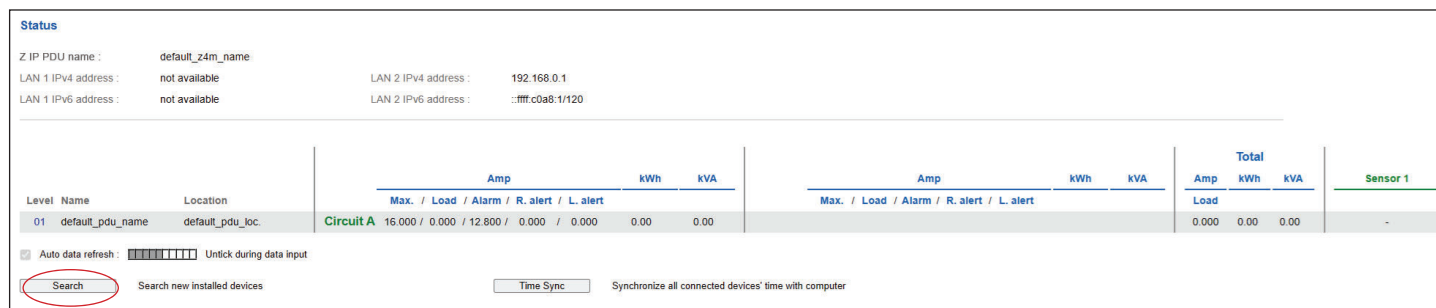
Synchronize all connected devices' time with computer

## < 1.8 > Remote PDU Level Setting

Remote level setting facilitates you to set the PDU level connected to the Z series IP PDU in the same cascade chain remotely. Please follow the steps below to complete the remote level setting.

 To ensure the correct PDU level setting, please have the serial number of the PDUs and order of the PDUs in the daisy chain.

1. In < **Status** >, Click “ **Search** ” to start the PDU searching



**Status**

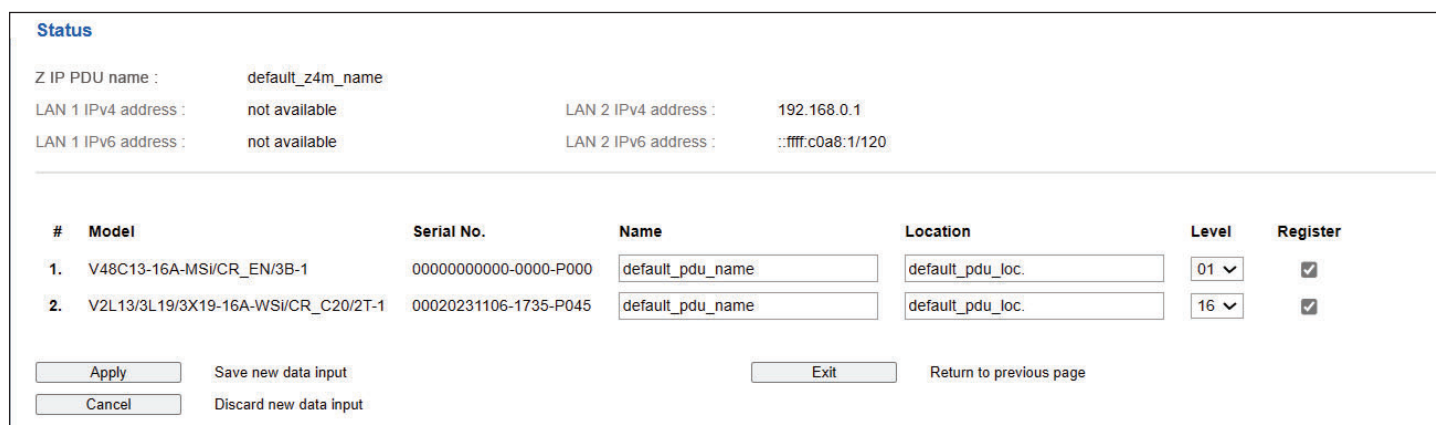
Z IP PDU name : default\_z4m\_name  
LAN 1 IPv4 address : not available LAN 2 IPv4 address : 192.168.0.1  
LAN 1 IPv6 address : not available LAN 2 IPv6 address : ::ffff:c0a8:1/120

Level	Name	Location	Amp					kWh	kVA	Amp					kWh	kVA	Total			Sensor 1
			Max.	Load	Alarm	R. alert	L. alert			Max.	Load	Alarm	R. alert	L. alert			Amp	kWh	kVA	
01	default_pdu_name	default_pdu_loc.	Circuit A	16.000	0.000	12.800	0.000	0.000	0.00	0.00							0.000	0.00	0.00	-

☒ Auto data refresh : ☐ Unlock during data input

**Search** Search new installed devices  Synchronize all connected devices' time with computer

2. After searching completes, the following screen will display



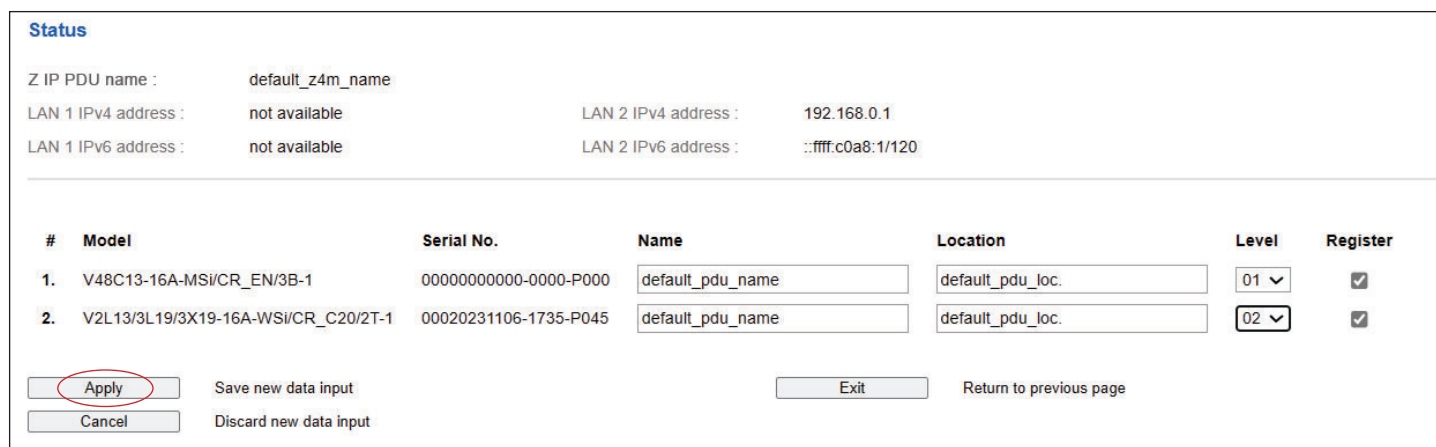
**Status**

Z IP PDU name : default\_z4m\_name  
LAN 1 IPv4 address : not available LAN 2 IPv4 address : 192.168.0.1  
LAN 1 IPv6 address : not available LAN 2 IPv6 address : ::ffff:c0a8:1/120

#	Model	Serial No.	Name	Location	Level	Register
1.	V48C13-16A-MSI/CR_EN/3B-1	00000000000-0000-P000	default_pdu_name	default_pdu_loc.	01	<input checked="" type="checkbox"/>
2.	V2L13/3L19/3X19-16A-WSI/CR_C20/2T-1	00020231106-1735-P045	default_pdu_name	default_pdu_loc.	16	<input checked="" type="checkbox"/>

Save new data input  Return to previous page  
 Discard new data input

3. Assign a unique “ **Level** ”, “ **Name** ” & “ **Location** ” to each connected PDU and ensure to tick the register box. Click “ **Apply** ” to complete the settings.



**Status**

Z IP PDU name : default\_z4m\_name  
LAN 1 IPv4 address : not available LAN 2 IPv4 address : 192.168.0.1  
LAN 1 IPv6 address : not available LAN 2 IPv6 address : ::ffff:c0a8:1/120

#	Model	Serial No.	Name	Location	Level	Register
1.	V48C13-16A-MSI/CR_EN/3B-1	00000000000-0000-P000	default_pdu_name	default_pdu_loc.	01	<input checked="" type="checkbox"/>
2.	V2L13/3L19/3X19-16A-WSI/CR_C20/2T-1	00020231106-1735-P045	default_pdu_name	default_pdu_loc.	02	<input checked="" type="checkbox"/>

**Apply** Save new data input  Return to previous page  
 Discard new data input

## < Section 2 > General

### < 2.1 > PPS-04-S ( WEBUI for Z series IP PDU )

PPS-04-S allows you to monitor and control up to 32 levels of Z / M series PDU in a single cascade chain remotely over a TCP/IP network.

In < **Status** > ,

- Click “ **Search** ” to search all new installed PDUs
- View all installed PDUs’ status
- View latest loading on each PDU’s circuits
- View aggregate current & energy consumption on each PDU
- View status & latest reading of Temp. & Humid sensors connected to each PDU
- Click “ **Time Sync** ” to update all connected PDUs’ real time clock from the computer login to PPS-04-S

Level	Name	Location	Amp	kWh	kVA	Total	Sensor 1
			Max. / Load / Alarm / R. alert / L. alert			Load kWh kVA	
01	default_pdu_name	default_pdu_loc.	Circuit A 16.000 / 0.000 / 12.800 / 0.000 / 0.000	0.00	0.00	0.000 0.00 0.00	-
02	default_pdu_name	default_pdu_loc.	Circuit A 16.000 / 0.000 / 12.800 / 0.000 / 0.000	0.00	0.00	0.000 0.00 0.00	-

In < **Details** > ,

- Change “ **Name** ” and “ **Location** ” of PDU & Click “ **Apply** ”
- Change “ **Alarm amp.** ”, “ **Rising alert amp.** ” & “ **Low alert amp.** ” of PDU’s circuits & Click “ **Apply** ”
- Click “ **Reset** ” to reset peak amp. or kWh of PDU’s circuits
- Click “ **ON / OFF** ” to switch ON / OFF outlet ( Switched PDU only )
- View On / Off status of each PDU’s outlet
- View aggregated current on the PDU
- View latest loading & energy consumption of each PDU’s outlet ( Outlet Measurement PDU only )
- Click “ **Time Sync** ” update PDU’s real time clock from the computer login to PPS-04-S

Outlet	Name	Amp	kWh	kVA	Status	Switch
01	outlet_name_01	0.000	0.00	0.00	ON	OFF
02	outlet_name_02	0.000	0.00	0.00	ON	OFF
03	outlet_name_03	0.000	0.00	0.00	ON	OFF
04	outlet_name_04	0.000	0.00	0.00	ON	OFF
05	outlet_name_05	0.000	0.00	0.00	ON	OFF
06	outlet_name_06	0.000	0.00	0.00	ON	OFF
07	outlet_name_07	0.000	0.00	0.00	ON	OFF
08	outlet_name_08	0.000	0.00	0.00	ON	OFF

## < 2.1 > PPS-04-S ( WEBUI for Z series IP PDU )

In < **Outlet setting** > ,

- Change PDU's outlet name
- Change “ **Power up sequence delay** ” of PDU's outlet ( Switched PDU only )  
Default : 1 second. Min. 1 seconds, max. 3600 seconds
- Change “ **Alarm amp.** ”, “ **Rising Alert amp.** ” & “ **Low alert amp.** ” of PDU's outlet ( Outlet Measurement PDU only )  
Click “ **Apply** ” to complete the settings
- Click “ **Reset** ” to reset peak amp. or kWh of PDU's outlet ( Outlet Measurement PDU only )

**Outlet details**

Level :  V2L13/3L19/3X19-16A-ZSI

Status : Connected

Name :

Location :

**Circuit A**

Outlet :  

Name :

Status : ON

Power up sequence delay :  ( Min. 1s, Max: 3600s )

Load amp :

Alarm amp :

R. alert amp :

L. alert amp :

Peak amp :  2015/01/01 00:00:00

kWh :  2015/01/01 00:00:00

In < **Sensor Status** > ,

- View status, location, latest reading & alarm setting of Temp. & Humid sensors



 The WEBUI will NOT show the status / reading if sensors are NOT installed & activated.

**Sensor Status**

Z IP PDU name :

LAN 1 IPv4 address :  LAN 2 IPv4 address :

LAN 1 IPv6 address :  LAN 2 IPv6 address :

Level	Name	Setting	Sensor 1			Sensor 2		
			Location	Type	Status Alarm R.alert	Location	Type	Status Alarm R.alert
01	default_pdu_name		sensor_loc_S1.01	Temp. °C	27.8 40.0 0.0	-	-	- - -
				Humid. %	45.6 90.0 0.0			
02	default_pdu_name		sensor_loc_S1.01	Temp. (°C)	32.0 40.0 0.0	-	-	- - -

☒ Auto data refresh :   
☐ Untick during data input

## < 2.1 > PPS-04-S ( WEBUI for Z series IP PDU )

In < **Sensor Setting** > ,

- Default Sensor setting : Deactivate
- “ **Activate** ” sensors ONLY when they are connected
- Change “ **Location** ” , “ **Rising alert Setting** ” & “ **Alarm Setting** ” of Temp. & Humid sensors



If no any sensor connected, NEVER activate.

**Sensor Setting**

Level :  V2L13/3L19/3X19-16A-ZSI

Status : Connected

Name : default\_pdu\_name

Location : default\_pdu\_loc.

**Sensor 1**

☒ Activate ☐ Deactivate

Type :

Status : Installed

Location :

Alarm

Rising alert

Setting

Reading

Temp.(°C) :   36.5

**Sensor 2**

☐ Activate ☒ Deactivate

Type :

Status : -

Location :

Save new data input

Return to previous page

Discard new data input

## < 2.2 > Outlet Grouping

Outlet Grouping allows you to group multiple outlets from same PDU or across PDUs in the same cascade chain. You can ON / OFF / Power Cycle all the outlets in the Group.

Please follow the steps below to complete the Outlet Grouping.

1. Select “Outlet Group” from the left navigation pane. The display below will show. Then Click “**Create**” to add a new outlet group

**Outlet Group**

Create

Group ID	Group Name	Outlets	Action
----------	------------	---------	--------

2. Input the outlet group name and tick the outlets you want to add to the group. I select all outlets of PDU level 01 for this illustration. Click “**Apply**” to complete the settings

**Outlet Group 01**

Name:

PDU Level: 01

Circuit A

<input checked="" type="checkbox"/>	01		outlet_name_01
<input checked="" type="checkbox"/>	02		outlet_name_02
<input checked="" type="checkbox"/>	03		outlet_name_03

PDU Level: 02

Circuit A

<input type="checkbox"/>	01		outlet_name_01
<input type="checkbox"/>	02		outlet_name_02
<input type="checkbox"/>	03		outlet_name_03
<input type="checkbox"/>	04		outlet_name_04
<input type="checkbox"/>	05		outlet_name_05
<input type="checkbox"/>	06		outlet_name_06
<input type="checkbox"/>	07		outlet_name_07
<input type="checkbox"/>	08		outlet_name_08

PDU Level: 03

Circuit A

<input type="checkbox"/>		outlet_name_01
<input type="checkbox"/>		outlet_name_02
<input type="checkbox"/>		outlet_name_03
<input type="checkbox"/>		outlet_name_04
<input type="checkbox"/>		outlet_name_05
<input type="checkbox"/>		outlet_name_06
<input type="checkbox"/>		outlet_name_07
<input type="checkbox"/>		outlet_name_08

Save new data input  Return to previous page

Discard new data input

3. Click “**Outlet Group**” of the left navigation pane, you can see all the outlet group you create. You can switch ON / OFF / Power Cycle all outlets in a specific group.






**Outlet Group**

Create

Group ID	Group Name	Outlets	Action
01	Group-01	Circuit A 01  outlet_name_01 02  outlet_name_02 03  outlet_name_03	<input type="button" value="ON"/> <input type="button" value="OFF"/> <input type="button" value="Power Cycle"/> <input type="button" value="Remove"/>

## < 2.3 > Outlet Sequencing

By default, outlets are powered on ONE by ONE in the ascending order when power ON or power cycle all the outlets on Z / M series PDU. You can change the power ON sequence of the outlets. It is useful for you to set the outlet power ON sequence where some IT equipment should be powered up first.

Button	Function
	Top
	Up
	Down
	Bottom
	Reset the default sequence

Please follow the steps below to complete the outlet sequencing setup.

1. Select “ **Outlet Sequence** ” from the left navigation pane. Select the PDU level you want to change the outlet sequence. Level 2 is selected in this illustration.

Device

Status

Details

Outlet Group

Outlet Sequence

Sensor

Setting

System

Network

Login

Local User

Domain/LDAP

SNMP














Notification

Syslog

Firmware

Outlet Power Up Sequence

Level : 02

	Sequence Order	Delay
	01  outlet_name_01	1 s
	02  outlet_name_02	1 s
	03  outlet_name_03	1 s
	04  outlet_name_04	1 s
	05  outlet_name_05	1 s
	06  outlet_name_06	1 s
	07  outlet_name_07	1 s
	08  outlet_name_08	1 s

Apply

Cancel



## < 2.3 > Outlet Sequencing

2. Select the outlet by clicking on the number next to the outlet icon you want to change the power ON sequence. Move outlet 4 up in this illustration.

**Outlet Power Up Sequence**

Level : 02 ▼

	Sequence Order		Delay
	01	outlet_name_01	1 s
↕	02	outlet_name_02	1 s
↑	03	outlet_name_03	1 s
↓	04	outlet_name_04	1 s
↓	05	outlet_name_05	1 s
↻	06	outlet_name_06	1 s
	07	outlet_name_07	1 s
	08	outlet_name_08	1 s

Apply Cancel

3. Click “” button once and outlet 4 moved prior to outlet 3. Click “**Apply**” to complete the settings. The new outlet sequence will apply when power cycle the Z / M series PDU or perform the power on or power cycle operation on partial outlets.

**Outlet Power Up Sequence**

Level : 02 ▼

	Sequence Order		Delay
	01	outlet_name_01	1 s
↕	02	outlet_name_02	1 s
↑	04	outlet_name_04	1 s
↓	03	outlet_name_03	1 s
↓	05	outlet_name_05	1 s
↻	06	outlet_name_06	1 s
	07	outlet_name_07	1 s
	08	outlet_name_08	1 s

Apply Cancel

## < 2.4 > System

In < **System** > ,

- Change Z series IP PDU name & location
- Change temperature unit displayed in WEBUI
- Set the “ **Date & Time** ” of the Z series IP PDU ( by “ **Manually** ” or “ **NTP server** ” ). Default is “ **Manually** ”
- Select “ **Web Access** ” Protocol ( “HTTPS” or “HTTP” ). Default Web Access Protocol is “HTTPS”.
- Click “ **Apply** ” to finish the above settings

The screenshot shows the 'Z IP PDU' configuration page. On the left is a sidebar with 'Device' and 'Setting' sections. Under 'Setting', 'System' is selected. The main area contains fields for Name, Location, Temperature unit (°C selected), Date & Time (set manually to 2007-01-01 02:08:49), and Web Access (HTTPS, port 443, use default certificate). At the bottom are buttons for Apply, Cancel, Reset to Factory Default, and Reboot Z IP PDU.

Z IP PDU	
Name :	default_z4m_name
Location :	default_z4m_loc.
Temperature unit :	<input checked="" type="checkbox"/> °C <input type="checkbox"/> °F
Date & Time	2007-01-01 02:08:49
Time zone :	GMT+00:00
Time setting :	Manually
Date (YYYY-MM-DD) :	2007-01-01
Time :	02 : 08 : 49
Web Access	
Protocol :	HTTPS
Port :	443 ( Default: 443 )
SSL Certificate :	<input checked="" type="radio"/> Use default certificate <input type="radio"/> Use custom certificate
Apply Cancel Reset to Factory Default Reboot Z IP PDU	

This screenshot is similar to the previous one but shows the 'Time setting' as 'Synchronize with NTP server'. The NTP server field is set to 'time.google.com' with a 'Sync Now' button next to it. The 'Apply' button at the bottom is circled in red.

Z IP PDU	
Name :	default_z4m_name
Location :	default_z4m_loc.
Temperature unit :	<input checked="" type="checkbox"/> °C <input type="checkbox"/> °F
Date & Time	2007-01-01 02:08:49
Time zone :	GMT+08:00
Time setting :	Synchronize with NTP server
NTP server :	time.google.com Sync Now
Web Access	
Protocol :	HTTPS
Port :	443 ( Default: 443 )
SSL Certificate :	<input checked="" type="radio"/> Use default certificate <input type="radio"/> Use custom certificate
Apply Cancel Reset to Factory Default Reboot Z IP PDU	

## < 2.5 > Network

In < **Network** >, Z series IP PDU can be configured to operate as Dual Lan or failover mode.

Default is “ **Dual Lan mode** ”

Dual Lan mode :

- Enter LAN 1 “ **IPv4 address** ”, “ **IPv6 address** ”, “ **Subnet mask** ”, “ **Gateway** ”.  
( For static IP setting only)
- Enter LAN 2 “ **IPv4 address** ”, “ **IPv6 address** ”, “ **Subnet mask** ”, “ **Gateway** ”.  
( For static IP setting only)
- Enter the IP address of “ **Primary DNS** ”. Default is “ **8.8.8.8** ”
- Enter the IP address of “ **Secondary DNS** ”. Default is “ **0.0.0.0** ”
- Click “ **Apply** ” to finish the above settings

The screenshot shows the 'Network' configuration window. It has two columns: 'LAN 1 settings' and 'LAN 2 settings'. Both columns have fields for DHCP (set to OFF), IPv4 address, IPv6 address, Subnet mask, and Gateway. Below these columns is a checkbox for 'Enable automatic failover' which is unchecked. At the bottom, there is a 'DNS' section with a checked checkbox for 'Manually configure DNS server', and fields for 'Primary DNS' (8.8.8.8) and 'Secondary DNS' (0.0.0.0). At the very bottom, there are 'Apply' and 'Cancel' buttons. The 'Apply' button is circled in red.

LAN 1 settings	LAN 2 settings
DHCP : OFF	DHCP : OFF
IPv4 address : 192.168.1.62	IPv4 address : 192.168.0.2
IPv6 address : 2001:0:1:a2::ec11/64	IPv6 address : 2001:0:1:a2::ec01/64
Subnet mask : 255.255.255.0	Subnet mask : 255.255.255.0
Gateway : 192.168.1.1	Gateway : 192.168.0.254

Enable automatic failover : ☐

**DNS**

Manually configure DNS server : ☒

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Apply Cancel

Failover mode :

- Tick “ **Enable automatic failover** ” to operate the failover mode
- Enter “ **IPv4 address** ”, “ **IPv6 address** ”, “ **Subnet mask** ”, “ **Gateway** ”. ( For static IP setting only)
- Enter the IP address of “ **Primary DNS** ”. Default is “ **8.8.8.8** ”
- Enter the IP address of “ **Secondary DNS** ”. Default is “ **0.0.0.0** ”
- Click “ **Apply** ” to finish the above settings

The screenshot shows the 'Network' configuration window for failover mode. It has a single 'LAN settings' column with fields for DHCP (set to OFF), IPv4 address, IPv6 address, Subnet mask, and Gateway. Below this column is a checked checkbox for 'Enable automatic failover'. At the bottom, there is a 'DNS' section with a checked checkbox for 'Manually configure DNS server', and fields for 'Primary DNS' (8.8.8.8) and 'Secondary DNS' (0.0.0.0). At the very bottom, there are 'Apply' and 'Cancel' buttons. The 'Apply' button is circled in red.

LAN settings
DHCP : OFF
IPv4 address : 192.168.0.1
IPv6 address : 2001:0:1:a2::ec31/64
Subnet mask : 255.255.255.0
Gateway : 192.168.0.254

Enable automatic failover : ☒

**DNS**

Manually configure DNS server : ☒

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Apply Cancel

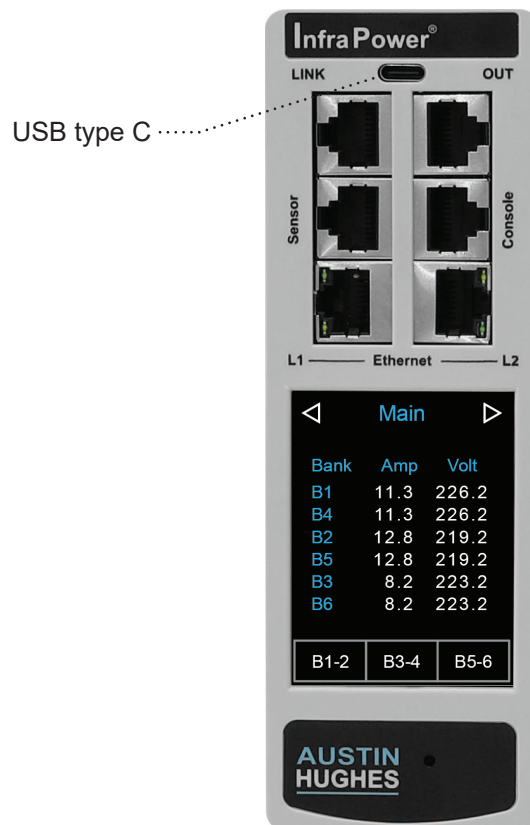
## < 2.6 > Wifi Network Configuration

### < Preparation >

- Make sure the network meets the security WPA2 - Personal or WPA2 - Enterprise.
- Z series IP PDU is powered ON.
- Login PPS-04-S WEBUI via L1 / L2 of Z series IP PDU to configure the Wifi network.



3rd party WIFI kit is not compatible to InfraPower.  
Make sure IPD-WIFI has been used for the WIFI network connection.



### ( I ) Wifi Static IP setting

Step 1. Prepare a USB type A (Female) to USB type C ( Male) adapter

Step 2. Connect the USB Wifi kit to the USB type A side

Step 3. Connect the USB type C side of the adapter to the USB type C port of Z series IP PDU

## < 2.6 > Wifi Network Configuration

Step 4. Click “ **Scan Wifi** ” to search the available Wifi network.

**Network**

**LAN 1 settings**

DHCP :  ▾

IPv4 address : not available

IPv6 address : fe80::220a:dff:feff:ab09/64

Subnet mask : not available

Gateway : not available

Authentication :  ▾

**LAN 2 settings**

DHCP :  ▾

IPv4 address : 192.168.0.100

IPv6 address : fe80::220a:dff:feff:fb87/64

Subnet mask : 255.255.255.0

Gateway : 192.168.0.10

Authentication :  ▾

Enable automatic failover : ☐

**WiFi settings**

ESSID :  ▾

Authentication :  ▾

DHCP :  ▾

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

**DNS**

Manually configure DNS server : ☒

Primary DNS :

Secondary DNS :

Step 5. Select the appropriate network from the pull down menu of “ **ESSID** ”.

**Network**

**LAN 1 settings**

DHCP :  ▾

IPv4 address : not available

IPv6 address : fe80::220a:dff:feff:ab09/64

Subnet mask : not available

Gateway : not available

Authentication :  ▾

**LAN 2 settings**

DHCP :  ▾

IPv4 address : 192.168.0.100

IPv6 address : fe80::220a:dff:feff:fb87/64

Subnet mask : 255.255.255.0

Gateway : 192.168.0.10

Authentication :  ▾

Enable automatic failover : ☐

**WiFi settings**

ESSID :  ▾

Authentication :  ▾

Password :

DHCP :  ▾

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

**DNS**

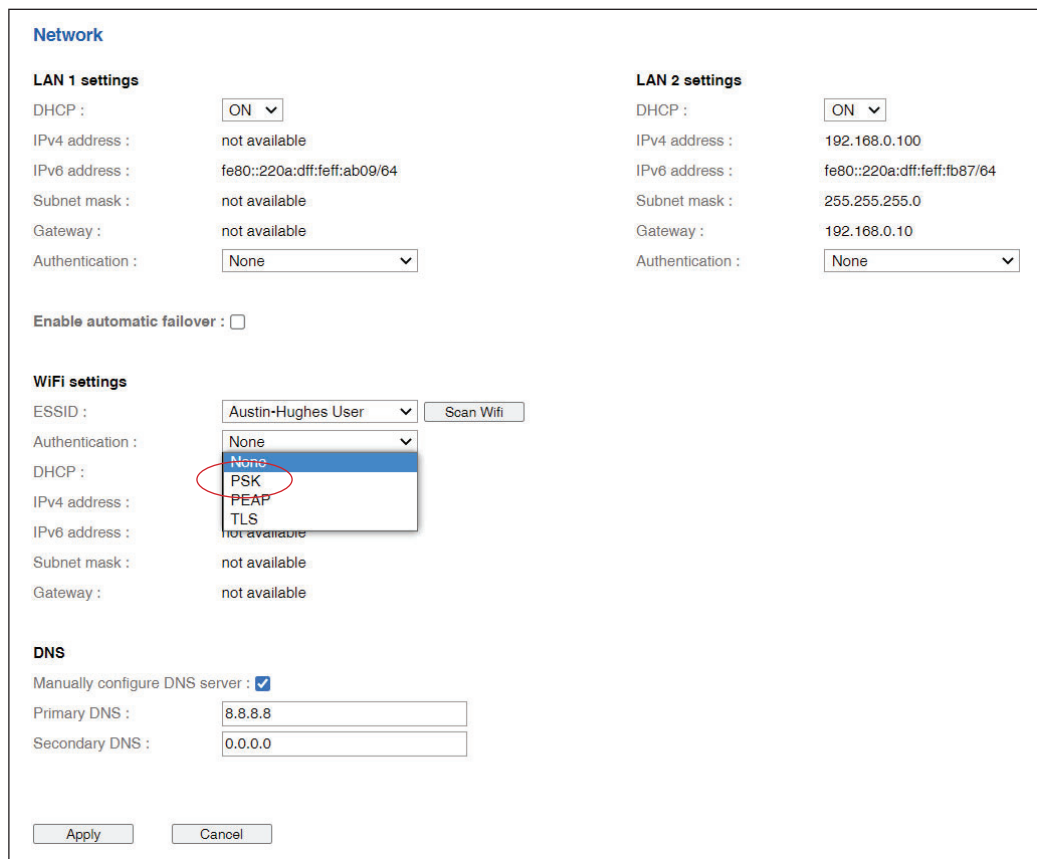
Manually configure DNS server : ☒

Primary DNS :

Secondary DNS :

## < 2.6 > Wifi Network Configuration

Step 6. Select “**PSK**” from Authentication. For PEAP or TLS , please refer to < 2.13 > 802.1X authentication.



**Network**

**LAN 1 settings**

DHCP :  ▾

IPv4 address : not available

IPv6 address : fe80::220a:dff:feff:ab09/64

Subnet mask : not available

Gateway : not available

Authentication :  ▾

**LAN 2 settings**

DHCP :  ▾

IPv4 address : 192.168.0.100

IPv6 address : fe80::220a:dff:feff:fb87/64

Subnet mask : 255.255.255.0

Gateway : 192.168.0.10

Authentication :  ▾

Enable automatic failover : ☐

**WiFi settings**

ESSID :  ▾

Authentication :  ▾

DHCP :  ▾

IPv4 address :  ▾

IPv6 address : not available

Subnet mask : not available

Gateway : not available

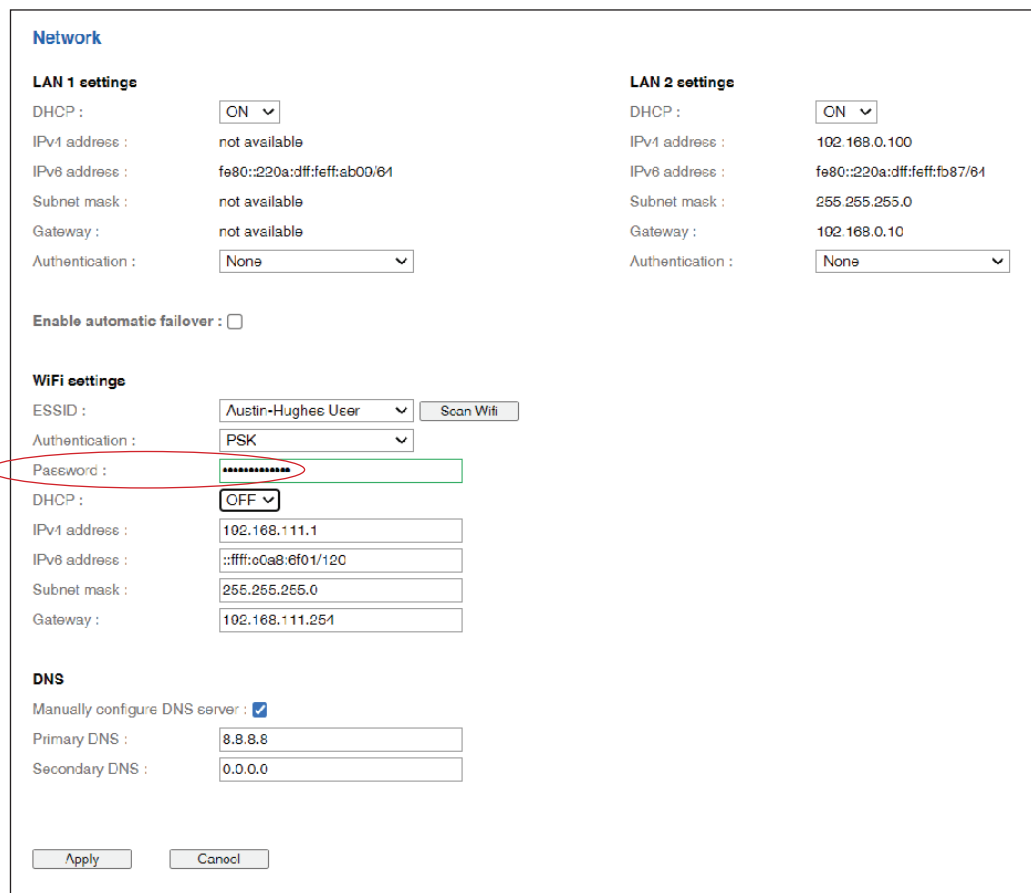
**DNS**

Manually configure DNS server : ☒

Primary DNS :

Secondary DNS :

Step 7. Input “**Password**” for authentication.



**Network**

**LAN 1 settings**

DHCP :  ▾

IPv4 address : not available

IPv6 address : fe80::220a:dff:feff:ab00/64

Subnet mask : not available

Gateway : not available

Authentication :  ▾

**LAN 2 settings**

DHCP :  ▾

IPv4 address : 102.168.0.100

IPv6 address : fe80::220a:dff:feff:fb87/64

Subnet mask : 255.255.255.0

Gateway : 102.168.0.10

Authentication :  ▾

Enable automatic failover : ☐

**WiFi settings**

ESSID :  ▾

Authentication :  ▾

Password :

DHCP :  ▾

IPv4 address :

IPv6 address :

Subnet mask :

Gateway :

**DNS**

Manually configure DNS server : ☒

Primary DNS :

Secondary DNS :

## < 2.6 > Wifi Network Configuration

Step 8. Select “ **DHCP** ” to “ **OFF** ”. Default is “ **ON** ”

Step 9. Enter “ **IPv4 address** ”, “ **IPv6 address** ”, “ **Subnet Mask** ”, “ **Gateway** ” & Click “ **Apply** ” to finish the above settings.

### ( II ) Wifi DHCP setting

Step 1. Prepare a USB type A (Female) to USB type C ( Male) adapter

Step 2. Connect the USB Wifi kit to the USB type A side

Step 3. Connect the USB type C side of the adapter to the USB type C port of Z series IP PDU

Step 4. Click “ **Scan Wifi** ” to search the available Wifi network.

The screenshot displays a 'Network' configuration window with the following sections:

- LAN 1 settings**: DHCP is set to 'ON'. IPv4 address is 'not available', IPv6 address is 'fe80::220a:dff:feff:ab09/64', Subnet mask is 'not available', Gateway is 'not available', and Authentication is 'None'.
- LAN 2 settings**: DHCP is set to 'ON'. IPv4 address is '192.168.0.100', IPv6 address is 'fe80::220a:dff:feff:fb87/64', Subnet mask is '255.255.255.0', Gateway is '192.168.0.10', and Authentication is 'None'.
- Enable automatic failover**: A checkbox that is currently unchecked.
- WiFi settings**: ESSID is set to 'NONE', Authentication is 'None', DHCP is 'ON', and IPv4, IPv6, Subnet mask, and Gateway are all 'not available'. A red circle highlights the 'Scan Wifi' button next to the ESSID dropdown.
- DNS**: 'Manually configure DNS server' is checked. Primary DNS is '8.8.8.8' and Secondary DNS is '0.0.0.0'.

At the bottom, there are 'Apply' and 'Cancel' buttons.



## < 2.6 > Wifi Network Configuration

Step 5. Select the appropriate network from the pull down menu of “ **ESSID** ”.

**Network**

**LAN 1 settings**

DHCP :  ▾

IPv4 address : not available

IPv6 address : fe80::220a:dff:feff:ab09/64

Subnet mask : not available

Gateway : not available

Authentication :  ▾

**LAN 2 settings**

DHCP :  ▾

IPv4 address : 192.168.0.100

IPv6 address : fe80::220a:dff:feff:fb87/64

Subnet mask : 255.255.255.0

Gateway : 192.168.0.10

Authentication :  ▾

Enable automatic failover : ☐

**WiFi settings**

ESSID :  ▾

Authentication :

Password :

DHCP :

IPv4 address :

IPv6 address :

Subnet mask :

Gateway :

**DNS**

Manually configure DNS server : ☐

Primary DNS :

Secondary DNS :

Step 6. Select “ **PSK** ” from Authentication. For PEAP or TLS , please refer to < 2.13 > 802.1X authentication.

**Network**

**LAN 1 settings**

DHCP :  ▾

IPv4 address : not available

IPv6 address : fe80::220a:dff:feff:ab09/64

Subnet mask : not available

Gateway : not available

Authentication :  ▾

**LAN 2 settings**

DHCP :  ▾

IPv4 address : 192.168.0.100

IPv6 address : fe80::220a:dff:feff:fb87/64

Subnet mask : 255.255.255.0

Gateway : 192.168.0.10

Authentication :  ▾

Enable automatic failover : ☐

**WiFi settings**

ESSID :  ▾

Authentication :

DHCP :

IPv4 address :

IPv6 address :

Subnet mask : not available

Gateway : not available

**DNS**

Manually configure DNS server : ☒

Primary DNS :

Secondary DNS :

## < 2.6 > Wifi Network Configuration

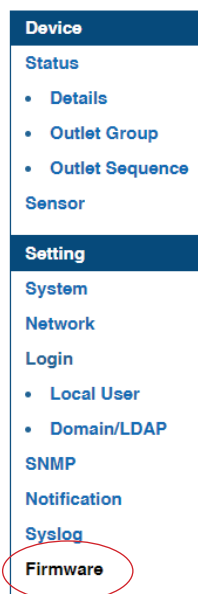
Step 7. Input “ **Password** ” for authentication.

The screenshot shows the 'Network' configuration page. It is divided into three main sections: LAN 1 settings, LAN 2 settings, and WiFi settings. LAN 1 settings include DHCP (ON), IPv4 address (not available), IPv6 address (fe80::220a:dff:feff:ab09/64), Subnet mask (not available), Gateway (not available), and Authentication (None). LAN 2 settings include DHCP (ON), IPv4 address (192.168.0.100), IPv6 address (fe80::220a:dff:feff:fb87/64), Subnet mask (255.255.255.0), Gateway (192.168.0.10), and Authentication (None). There is an 'Enable automatic failover' checkbox which is unchecked. The WiFi settings section includes ESSID (Austin-Hughes User), Authentication (PSK), Password (masked with asterisks), and DHCP (ON). The Password field is highlighted with a red circle. Below the WiFi settings are DNS settings: 'Manually configure DNS server' is checked, Primary DNS is 8.8.8.8, and Secondary DNS is 0.0.0.0. At the bottom are 'Apply' and 'Cancel' buttons.

Step 8. Select “ **DHCP** ” to “ **OFF** ”. Default is “ **ON** ”

Step 9. Click “ **Apply** ” to finish the above settings.

Step 10. Select “ **Firmware** ” from the left navigation pane.



## < 2.6 > Wifi Network Configuration

Step 11. Record the “ **MAC address** ” of the Wifi kit.

**Firmware**

**Device information**

Device :

Z IP PDU

Firmware version:

Z4M-Z100-240328

Hardware revision:

2.0

**LAN 1 information**

IPv4 address

: not available

IPv6 address

: not available

MAC address

: 20:0A:0D:FF:AB:09

**LAN 2 information**

IPv4 address

: 192.168.0.100

IPv6 address

: fe80::220a:dff:feff:fb87/64

MAC address

: 20:0A:0D:FF:FB:87

**Wifi information**

IPv4 address

: 192.168.1.234

IPv6 address

: fe80::1ebf:ceff:fe93:6bdc/64

MAC address

: 1C:BF:CE:93:6B:DC

**Upgrade firmware**

File path :

Browse

**Warning :** Upgrading firmware may take a few minutes,  
please don't turn off the power or press the reset button.

Upgrade

Cancel

Step 12. Assign an IP address of the Wifi kit from your DHCP server.

## < 2.7 > Login

For security purpose, users log in to PPS-04-S MUST be authenticated. PPS-04-S provides the following authentication methods:

- Local User on PPS-04-S
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (Radius) protocol

You can perform the authentication configuration in < **Login** >.

Local User authentication :

- Select Login > Local User
- Change “ **Login name** ” OR “ **Password** ”
- Re-enter password in “ **Confirm password** ”
- Click “ **Apply** ” and “ **OK** ” on the pop up window to make changes effective

The screenshot shows the 'Web UI' configuration page for 'Local User' authentication. On the left is a navigation menu with categories: 'Device' (containing 'Status' with sub-items 'Details', 'Outlet Group', and 'Outlet Sequence'), 'Sensor', and 'Setting' (containing 'System', 'Network', 'Login' with sub-items 'Local User', 'LDAP', and 'Radius', 'SNMP' with sub-item 'SNMP Traps', 'Notification', 'Syslog', and 'Firmware'). The 'Local User' option under 'Login' is selected. The main content area is titled 'Web UI' and contains a 'Password' section with three input fields: 'Login name :', 'Password :', and 'Confirm password :'. The 'Login name' field contains '00000000', the 'Password' field contains eight dots, and the 'Confirm password' field is empty. Below the input fields are two buttons: 'Apply' (circled in red) and 'Cancel'.

## < 2.7 > Login

LDAP ( OpenLDAP ) authentication :

- Select **Login > LDAP**
- Enable “ **LDAP authentication** ”
- Select “ **OpenLDAP** ” from “ **LDAP Type** ”
- Input the IP address or host name of the LDAP server in “ **Server** ”
- Input the port no. in “ **Port** “. Default is 389
- Select encryption type from “ **Encryption** ” ( None / SSL / StartTLS )
- Select the checkbox “ **Enable CA certificate** “. This field is optional.
- Input the “ **Bind DN** ”
- Input the “ **Bind Password** ”
- Input the “ **User Search DN** ”
- Input the “ **User Login Attribute** ”
- Input the “ **User Entry Object Class** ”
- Input the “ **User Search Subfilter** “. This field is optional.
- Select the checkbox “ **Group searching with memberOf attribute** ” if the user group in the LDAP server has an attribute name “ **memberOf** “. Otherwise, deselect it. This field is optional.
- Input “ **Group Member Attribute** ” & “ **Group Entry Object Class** ” if you deselect “ **Group searching with memberOf attribute** ”
- Input “ **Group Search Subfilter** “. This field is optional.
- Click “ **Apply** ” to save the settings.

**Domain / LDAP**

**LDAP Authentication :** ☒ Enable ☐ Disable

LDAP Type :

Server :

Port :

Encryption :

CA certificate :

☐ Enable CA certificate

Bind DN :

Bind Password :

User Search DN :

User Login Attribute :

User Entry Object Class :

User Search Subfilter :

☐ Group searching with memberOf attribute

Group Member Attribute :

Group Entry Object Class :

Group Search Subfilter :

## < 2.7 > Login

LDAP ( MS Active Directory ) authentication :

- Select **Login > LDAP**
- Enable “ **LDAP authentication** ”
- Select MS Active Directory from “ **LDAP Type** ”
- Input the IP address or host name of the AD server in “ **Server** ”
- Input the port no. in “ **Port** “. Default is 389
- Select encryption type from “ **Encryption** ” ( None / SSL / StartTLS )
- Select the checkbox “ **Enable CA certificate** “. This field is optional.
- Input the “ **Bind DN** ”
- Input the “ **Bind Password** ”
- Input the “ **User Search DN** ”
- Input the “ **User Search Subfilter** “. This field is optional.
- Select the checkbox “ **Group searching with memberOf attribute** ” if the user group in the AD server has an attribute name “ **memberOf** “. Otherwise, deselect it. This field is optional.
- Input “ **Group Member Attribute** ” & “ **Group Entry Object Class** ” if you deselect “ **Group searching with memberOf attribute** ”
- Input “ **Group Search Subfilter** “. This field is optional.
- Input the “ **Domain** ” of the AD server.
- Click “ **Apply** ” to save the settings.

**Domain / LDAP**

**LDAP Authentication :** ☒ Enable ☐ Disable

LDAP Type : MS Active Directory ▼

Server : 192.168.1.60

Port : 389

Encryption : StartTLS ▼

CA certificate :  Browse

☐ Enable CA certificate

Bind DN : CN=adminiator,CN=Users,DC=au

Bind Password :

User Search DN : CN=Users,DC=austin-hughes,DC=c

User Login Attribute : sAMAccountName

User Entry Object Class : person

User Search Subfilter :

☐ Group searching with memberOf attribute

Group Member Attribute : uniqueMember

Group Entry Object Class : groupOfUniqueNames

Group Search Subfilter :

Domain : example.dc

Connection Test

**Apply** Cancel

## < 2.7> Login

LDAP Role :

Once you finish the LDAP ( OpenLDAP ) or LDAP ( MS Active Directory ) configuration, you need to determine which users and roles ( groups ) are allowed to log in PPS-04-S.

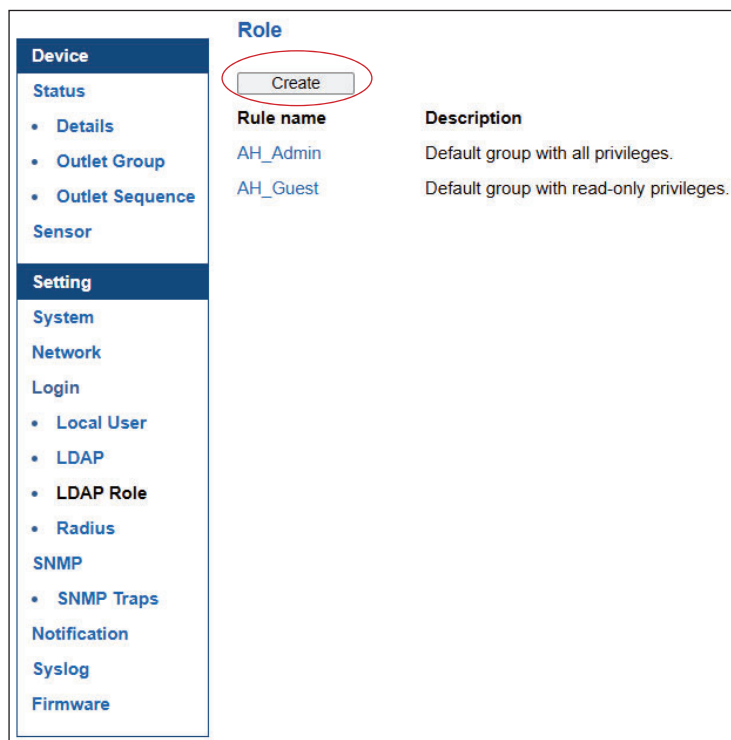
By default, PPS-04-S has two built-in roles – AH\_Admin and AH\_Guest. Users with AH\_Admin role having all privileges in PPS-04-S and users with AH\_Guest role only having Read only privileges in PPS-04-S.

These two built-in roles NOT allowed to modify or delete.

You can create other roles in PPS-04-S for your specific requirement.

To create roles in PPS-04-S, please follow the steps below :

1. Select **Login > LDAP Role**



2. Click “ **Create** ”



## < 2.7> Login

### 3. Input the Role name

The screenshot shows a web interface for configuring a new role. On the left is a sidebar menu with categories: Device, Status, Sensor, Setting, and System. Under 'Setting', 'Login' is selected, and 'LDAP Role' is highlighted. The main area is titled 'New Role' and contains three input fields: 'Name' (filled with 'LdapUser'), 'Description' (filled with 'Ldap user with read only right'), and 'Privilege' (a dropdown menu set to 'Read Only'). At the bottom, there are two buttons: 'Apply' and 'Cancel'. To the right of these buttons are two links: 'Save new data input' and 'Discard new data input'. Further right are two buttons: 'Exit' and 'Return to previous page'.

New Role	
Name :	<input type="text" value="LdapUser"/>
Description :	<input type="text" value="Ldap user with read only right"/>
Privilege :	<input type="button" value="Read Only"/>
<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
<input type="button" value="Save new data input"/>	<input type="button" value="Discard new data input"/>
<input type="button" value="Exit"/>	<input type="button" value="Return to previous page"/>

4. Input the description of the role. This field is optional.
5. Select the privilege of this role. ( Read Only / Read and Write )
6. Click “ **Apply** ” to finish the role creation.

## < 2.7> Login

After Role creation in PPS-04S, user can ONLY log in the PPS-04-S after users are added to the groups ( roles ) on the AD server / LDAP server.

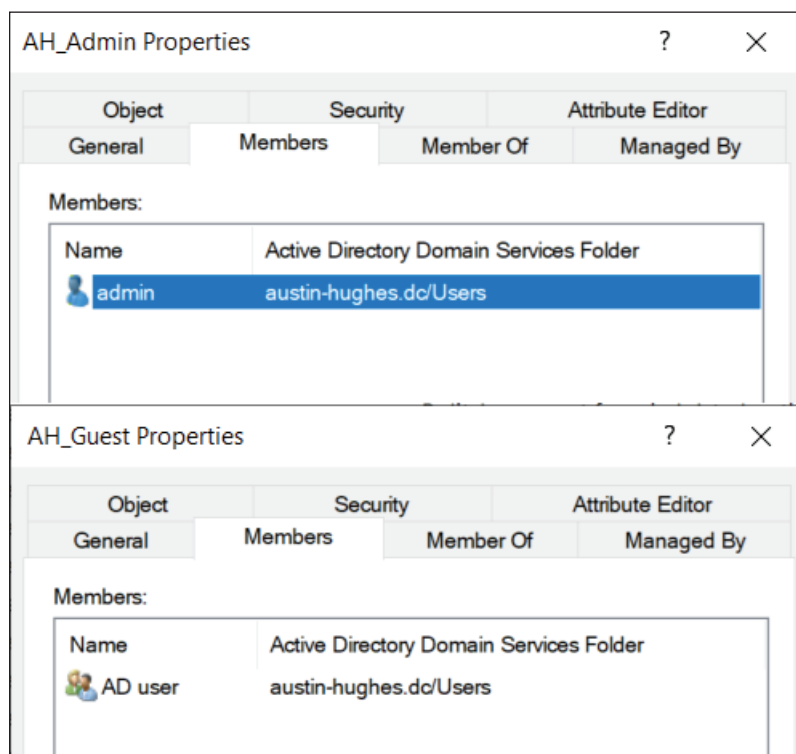
### AD Server

In this illustration, we assume :

- The groups ( roles ) for PPS-04-S are AH\_Admin and AH\_Guest
- User accounts admin and AD user already exist on the AD server.

To configure user groups on the AD server, follow the steps below :

1. On the AD server, create new groups – AH\_Admin and AH\_Guest.
2. Add user account admin to the AH\_Admin group.
3. Add user account AD user to the AH\_Guest group.



4. Now, user account admin can log in PPS-04-S with full privilege and user account AD user can log in PPS-04-S with Read-only privilege.

## < 2.7> Login

### LDAP Server

In this illustration, we assume :

- The groups ( roles ) for PPS-04-S are LdapUserAdmin and LdapUser
- User accounts LDAP\_Admin and LDAP\_User already exist on the LDAP server.

To configure user groups on the LDAP server, follow the steps below :

1. On the LDAP server, create new groups – LdapUserAdmin and LdapUser.
2. Add user account LDAP\_Admin to the LdapUserAdmin group.
3. Add user account LDAP\_User to the LdapUser group.
4. Now, user account LDAP\_Admin and LDAP\_User can log in PPS-04-S with the privilege you assign to LdapUserAdmin and LdapUser role in PPS-04-S.

Radius authentication :

- Select Login > Radius
- Enable “ **Radius authentication** ”
- Input the IP address or host name of the Radius server in “ **Server** ”
- Select “ **Type of authentication** “. ( MS-CHAPv2 / CHAP / PAP )
- Input the “ **Authentication port** “. Default is 1812
- Select the checkbox “ **Enable Accounting** “. This field is optional.
- Input the “ **Accounting port** “ if you “ **Enable Accounting** “. Default is 1813.
- Input “ **Timeout** “. Default is 2 in second.
- Input “ **Retries** “. Default is 0.
- Input “ **Shared secret** ”
- Input “ **Confirm shared secret** ”.
- Click “ **Apply** ” to save the settings.

The screenshot displays the 'Radius' configuration page within the 'InfraPower PPS-04-S' web interface. The left sidebar shows a navigation menu with 'Radius' selected under the 'Login' section. The main content area is titled 'Radius' and contains the following settings:

- Radius authentication:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Server:** Text input field containing '192.168.1.60'.
- Type of authentication:** Dropdown menu set to 'MS-CHAPv2'.
- Authentication port:** Text input field containing '1812'.
- Enable Accounting:** Checked checkbox.
- Accounting port:** Text input field containing '1813'.
- Timeout:** Text input field containing '2'.
- Retry:** Text input field containing '0'.
- Shared secret:** Text input field containing 'secret'.
- Confirm shared secret:** Text input field containing 'confirm secret'.
- Test Username:** Text input field containing 'username'.
- Test Password:** Text input field containing 'password'.
- Test Connection:** Button.

At the bottom of the configuration area, there are two buttons: 'Apply' (circled in red) and 'Cancel'.

## < 2.8 > SNMP Setup

PPS-04-S can manage the connected single & three phase intelligent PDUs in a single daisy-chain up to 32 levels via SNMP v1/v2 or v3 ( Simple Network Management Protocol )

### ( I ). Accessing MIB Files

**Step 1.** Click the following link to go to the mangement software download page :

<http://www.austin-hughes.com/resources/infrapower/software>

**Step 2.** Select the appropriate MIB file of the PDU series

### ( II ). Enabling SNMP Support

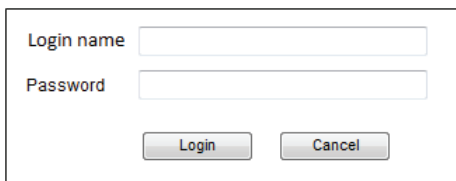
i. The following steps summarize how to enable SNMP v1 / v2 support for PPS-04-S.

**Step 1.** Connect one of the LAN port of Z series IP PDU to a computer

**Step 2.** Open the MS Edge

**Step 3.** Enter the configured IP address into the address bar

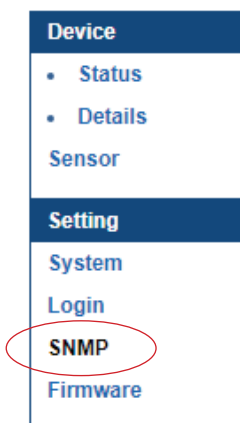
**Step 4.** Enter “ **Login name** ” & “ **Password** ”.



A login dialog box with a white background and a thin black border. It contains two text input fields: the first is labeled "Login name" and the second is labeled "Password". Below the fields are two buttons: "Login" on the left and "Cancel" on the right.

## < 2.8 > SNMP Setup

**Step 5.** Select the **SNMP** from the left navigation pane



**Step 6.** The **SNMP** Settings window appears as below:

A screenshot of the 'SNMP' configuration window. At the top left is the title 'SNMP'. Below it, the 'SNMP agent' section has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. Below this are input fields for 'SNMP version' (a dropdown menu showing 'v1/v2'), 'SNMP port' (a text box with '161'), 'sysContact' (a text box with 'human.being<nobody@but.you>'), 'sysLocation' (a text box with 'Earth'), and 'sysName' (a text box with 'PPS-03-S'). The 'SNMP configuration' section follows, with 'Read community' (a text box with 'public') and 'Write community' (a text box with 'private'). Below this are three identical sections for 'Station 1', 'Station 2', and 'Station 3'. Each station section has radio buttons for 'Deactivate' (selected) and 'Activate'. Below the radio buttons are input fields for 'Trap Station IP' (all with '192.168.0.254'), 'Trap port' (all with '162'), and 'Trap community' (all with 'private'). At the bottom left are 'Apply' and 'Cancel' buttons.

**Step 7.** Click “ **Enable** ” in “ **SNMP agent** ” to start the SNMP agent service

**Step 8.** Select “ **v1/v2** ” in “ **SNMP version** ”

**Step 9.** Input “ **SNMP port** “. Default is 161

**Step 10.** Input “ **sysContact** “. Default is human.being<nobody@but.you>

**Step 11.** Input “ **sysLocation** “. Default is Earth

**Step 12.** Input “ **sysName** “. Default is Z4M

**Step 13.** Input “ **Read Community** “. Default is public

**Step 14.** Input “ **Write Community** “. Default is private

**Step 15.** Click “ **Activate** ” in Station 1 to enable the trap service

**Step 16.** Input “ **Trap Station IP** ”, “ **Trap Port** ” & “ **Trap Community** ” of Station 1

**Step 17.** Repeat Step 14 & 15 for Station 2 & 3

**Step 18.** Click “ **Apply** ” to finish the SNMP v1 / v2 settings

## < 2.8 > SNMP Setup

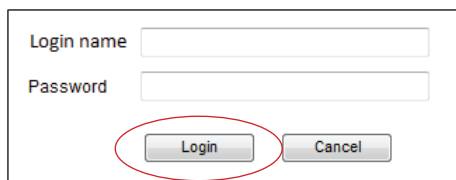
ii. The following steps summarize how to enable SNMP v3 support for PPS-04-S.

**Step 1.** Connect one of the LAN port of Z series IP PDU to a computer

**Step 2.** Open MS Edge

**Step 3.** Enter the configured IP address into the address bar

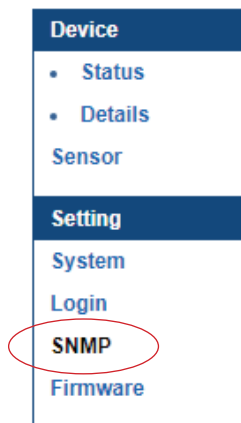
**Step 4.** Enter “ **Login name** ” & “ **Password** ”.



Login name

Password

**Step 5.** Select SNMP from the left navigation pane



**Device**

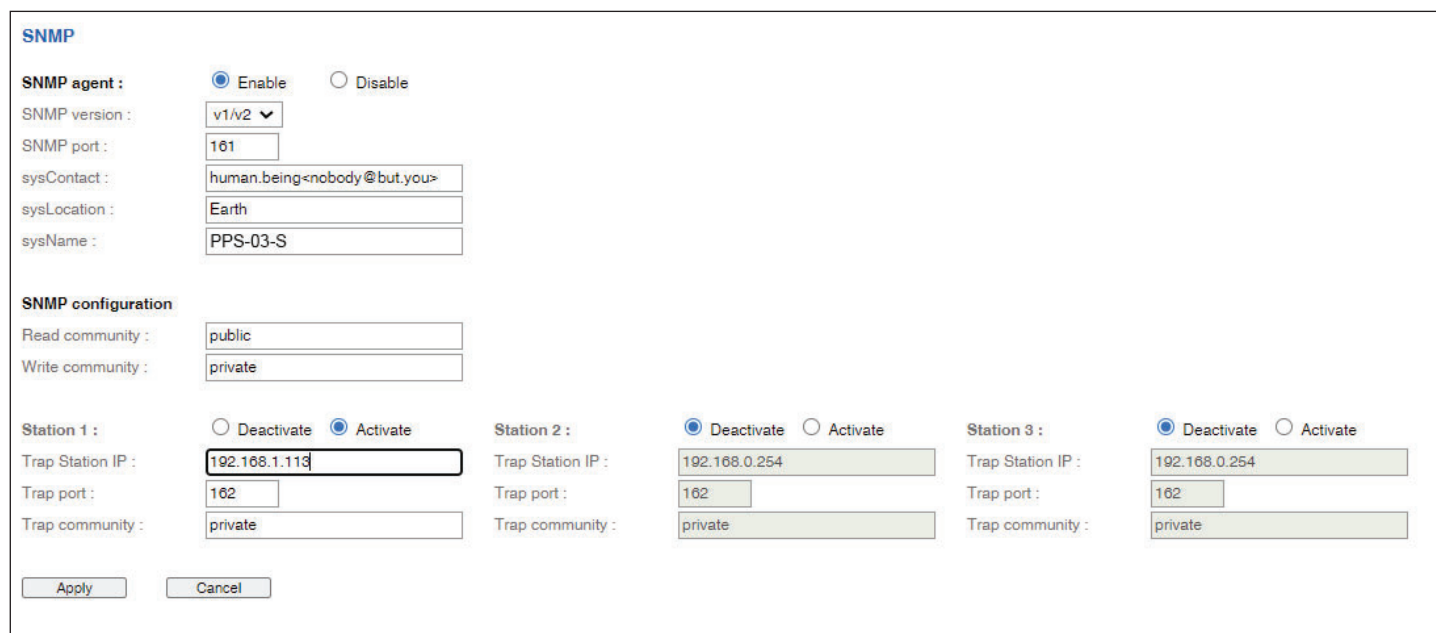
- Status
- Details

**Sensor**

**Setting**

- System
- Login
- SNMP**
- Firmware

**Step 6.** The **SNMP** Settings window appears as below:



**SNMP**

**SNMP agent :** ☒ Enable ☐ Disable

SNMP version :

SNMP port :

sysContact :

sysLocation :

sysName :

**SNMP configuration**

Read community :

Write community :

**Station 1 :** ☐ Deactivate ☒ Activate

Trap Station IP :

Trap port :

Trap community :

**Station 2 :** ☒ Deactivate ☐ Activate

Trap Station IP :

Trap port :

Trap community :

**Station 3 :** ☒ Deactivate ☐ Activate

Trap Station IP :

Trap port :

Trap community :

## < 2.8 > SNMP Setup

**Step 7.** Click “ **Enable** ” in “ **SNMP agent** ” to start the SNMP agent service

**Step 8.** Select “ **v3** ” in “ **SNMP version** ” & the SNMP v3 settings window appears as below :

**SNMP**

**SNMP agent :** ☒ Enable ☐ Disable

SNMP version : **v3**

SNMP port : 161

sysContact : human.being<nobody@but.you>

sysLocation : Earth

sysName : PPS-03-S

**SNMP configuration**

**User 1 :** ☐ Deactivate ☒ Activate

User role : read only

USM user : usm\_user1

Auth algorithm : None

Auth password :

Privacy algorithm : None

Privacy password :

SNMP trap : Disabled

Trap Station IP : 192.168.1.113

Trap port : 162

**User 2 :** ☒ Deactivate ☐ Activate

User role : read only

USM user : usm\_user2

Auth algorithm : None

Auth password :

Privacy algorithm : None

Privacy password :

SNMP trap : Disabled

Trap Station IP : 192.168.0.254

Trap port : 162

**User 3 :** ☒ Deactivate ☐ Activate

User role : read only

USM user : usm\_user3

Auth algorithm : None

Auth password :

Privacy algorithm : None

Privacy password :

SNMP trap : Disabled

Trap Station IP : 192.168.0.254

Trap port : 162

Apply Cancel

**Step 9.** Input “ **SNMP port** “. Default is 161

**Step 10.** Input “ **sysContact** “. Default is human.being<nobody@but.you>

**Step 11.** Input “ **sysLocation** “. Default is Earth

**Step 12.** Input “ **sysName** “. Default is Z4M

**Step 13.** Click “ **Activate** ” in User 1

**Step 14.** Select “ **Read Only** ” or “ **Read & Write** ” in User role :

**Step 15.** Input the name of “ **USM user** ” . Default is usm\_user1

**Step 16.** Select “ **None / MD5 / SHA** ” in “ **Auth algorithm** ”.  
If you select “ **Read & Write** ” in “ **User role:** ” ,  
you MUST select “ **MD5 / SHA** ” in “ **Auth algorithm** ”

**Step 17.** Input the “ **Auth password:** ” Default is “ 00000000 ”

**Step 18.** Select “ **None / DES / AES / AES192 / AES256** ” in “ **Privacy algorithm** ”.  
If the Auth algorithm is “ **NONE** ” , NO privacy algorithm can be selected.

**Step 19.** Input the “ **Privacy password** ”

**Step 20.** If you want to receive trap message, select “ **Enable** ” in **SNMP trap**

**Step 21.** Input the “ **Trap Station IP** ” & “ **Trap port** ”

**Step 22.** Repeat step 12 to 20 for User 2 & 3

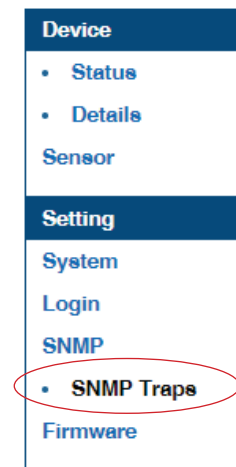
**Step 23.** Click “ **Apply** ” to finish the SNMP v3 settings.



## < 2.8 > SNMP Setup

### ( III ). SNMP Traps Setting

After enable SNMP, you can click “ SNMP Traps ” to go to the “ SNMP Traps Setting ” page



Below is the default setting for each PDU SNMP trap.

You can set the SNMP trap option and Click “ Apply ” to finish the settings.

**SNMP Traps Setting**

pduConnectionLost :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
pduConnectionRecovered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
circuitLoadEventTriggered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
circuitLoadEventCleared :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
circuitBreakerTripped :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
circuitBreakerRecovered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
sensorConnectionLost :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
sensorConnectionRecovered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
tempSensorEventTriggered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
tempSensorEventCleared :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
humiSensorEventTriggered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
humiSensorEventCleared :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
rcmSensorConnectionLost :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
rcmSensorConnectionRecovered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
rcmSensorEventTriggered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
rcmSensorEventCleared :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
smokeSensorEventTriggered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
smokeSensorEventCleared :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	
doorSensorEventTriggered :	<input type="radio"/> Disable	<input checked="" type="radio"/> Once	<input type="radio"/> Cyclic
doorSensorEventCleared :	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable	

☒ Apply ☐ Cancel

## < 2.9 > Notification

In < **Notification** > , you can configure the alarm email server & max. 5 email recipients to receive alarm notifications from PPS-04-S.

Default is “ **Disable** ”.

**Step 1.** “ **Enable** ” alarm email

**Step 2.** Enter “ **SMTP server** ” and “ **SMTP port** ”. Default is “ **Port 25** ”

**Step 3.** “ **Enable** ” or “ **Disable** ” the “ **SMTP authentication** “. Default is “ **Disable** ”

**Step 4.** Enter “ **User name** “ and “ **Password** “ when SMTP authentication is enabled

**Step 5.** Select the “ **secure connection** “ ( None, SSL / TLS & STARTTLS ). Default is “ **None** ”

**Step 6.** Enter the “ **Sender Name** ” and “ **Sender Email** ”

**Step 7.** Enter the “ **Alarm Interval** “. ( Min. 10, Max. 60 mins )

**Step 8.** Enter the alarm recipient email account in “ **Recipient 01** ”

**Step 9.** Repeat step 8 for other recipients

**Step 10.** Click “ **Apply** “ to finish the alarm email server setting

**Email Notification**

Alarm email : ☒ Enable ☐ Disable

SMTP server : smtp.austin-hughes.com

SMTP port : 25 ( Default: 25 )

Authentication : Enable ▾

User name : sender@mail.com

Password : \*\*\*\*\*

Secure connection : None ▾

Sender name : Email alarm

Sender email : sender@mail.com

Interval (minutes) : 10 (Min. 10, Max. 60)

Recipient 01 : recipient-01@mail.com

Recipient 02 :

Recipient 03 :

Recipient 04 :

Recipient 05 :

Apply Cancel

## < 2.10 > Syslog

In < **Syslog** > , you can view the latest 2000 device and system log

Syslog			
#	Type	Date & Time	Event
1	Device	2020-09-07 11:55:39	Door alarm (open) - PDU level 24 - Door sensor 1(sensor_location )
2	Device	2020-09-07 11:55:38	Sensor reconnection - PDU level 24 - door sensor 1(sensor_location )
3	Device	2020-09-07 11:55:28	Sensor reconnection - PDU level 23 - T sensor 1(TH_Sensor_01 )
4	WebUI	2020-09-07 11:52:11	[Email Notification] has been Updated
5	Device	2020-09-07 11:50:11	Activate(1) T sensor - PDU level 25 - sensor 2 (sensor_location )
6	Device	2020-09-07 11:49:50	Deactivate(0) T sensor - PDU level 25 - sensor 1 (sensor_location )
7	Device	2020-09-07 11:48:37	Sensor disconnection - PDU level 25 - T sensor 2(sensor_location )
8	Device	2020-09-07 11:48:27	Activate(1) T sensor - PDU level 25 - sensor 2 (sensor_location )
9	Device	2020-09-07 11:48:08	Deactivate(0) T sensor - PDU level 25 - sensor 1 (sensor_location )
10	WebUI	2020-09-07 11:47:31	[Email Notification] has been Updated
11	WebUI	2020-09-07 11:47:16	[Email Notification] has been Updated
12	Device	2020-09-07 11:34:06	Sensor disconnection - PDU level 25 - T sensor 1(sensor_location )
13	Device	2020-09-07 11:33:55	Activate(1) T sensor - PDU level 25 - sensor 1 (sensor_location )
14	WebUI	2020-09-07 11:33:37	[Email Notification] has been Updated
15	Device	2020-09-07 10:43:29	Activate(1) T sensor - PDU level 24 - sensor 2 (sensor_location )
16	Device	2020-09-07 10:43:20	Sensor disconnection - PDU level 24 - door sensor 1(sensor_location )

## < 2.11 > Firmware upgrade of Z series IP PDU

### < Firmware Upgrade >

For function enhancement of PPS-04-S, please take the following steps to remotely upgrade the firmware of Z series IP PDU :

**Step 1.** Click the following link to go to the mangement software download page :

<http://www.austin-hughes.com/resources/infrapower/software>

**Step 2.** Select appropriate firmware for Z series IP PDU

**Step 3.** Connect one of the LAN port of Z series IP PDU to a computer

**Step 4.** Open the MS Edge

**Step 5.** Enter the configured IP address into the address bar

**Step 6.** Enter “ **Login name** “ & “ **Password** “.



A login form with two input fields: "Login name" and "Password". Below the fields are two buttons: "Login" and "Cancel".

**Step 7.** Select the Firmware from the left navigation pane



## < 2.11 > Firmware upgrade of Z series IP PDU

**Step 8.** The firmware upgrade window appears as below :

**Firmware**

**Device information**

Device : Z IP PDU

Firmware version: Z4M-Z100-240326

Hardware revision: 2.0

---

**LAN 1 information**

IPv4 address : 192.168.1.227

IPv6 address : fe80::220a:dff:fe68:3c/64

MAC address : 20:0A:0D:68:00:3C

---

**LAN 2 information**

IPv4 address : 192.168.1.225

IPv6 address : fe80::220a:dff:fe68:3d/64

MAC address : 20:0A:0D:68:00:3D

---

**Upgrade firmware**

File path :

**Warning :** Upgrading firmware may take a few minutes,  
please don't turn off the power or press the reset button.

**Step 9.** Click “ **Browse** ” and select the firmware file (.enc ) from the specific path in the pop up window and Click “ **Open** ”

**Step 10.** Click “ **Upgrade** ” to start the upgrade process. It takes a few minutes to complete.

**Step 11.** Once complete, UI will return to the login page.

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

### < Bulk Firmware Upgrade via DHCP/TFTP >

If a TFTP server is available, you can use it to perform firmware upgrade for a huge number of Z series IP PDU the same network.



- The feature of bulk firmware upgrade via DHCP/TFTP only works on Z series IP PDU directly connected to the network.
- The bulk fi rmware upgrade can ONLY be performed via IPv4 network.
- Do NOT perform the fi rmware upgrade via a wireless network connection.

### < Procedure for Bulk Firmware Upgrade >

#### Steps of using DHCP/TFTP for bulk firmware upgrade

**Step 1.** Prepare some or all of the following files:

- Fwupdate.cfg ( always required )
- Devices.csv
- Firmware file for Z series IP PDU in .enc format

**Step 2.** Configure your TFTP server properly. See ***TFTP Requirements***

**Step 3.** Put ALL required files into a folder and COPY the folder to the TFTP root directory

**Step 4.** Properly configure your DHCP server so that it refers to the file “ **fwupdate.cfg** ” on the TFTP server for your Z series IP PDU. See ***DHCP IPv4 Confi guration in Windows***

**Step 5.** Make sure all of the Z series IP PDUs use DHCP as the IP confi guration method and have been directly connected to the network.




The default IP configuration of Z series IP PDU is “ **DHCP** ”

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

**Step 6.** Reboot the Z series IP PDU. The DHCP server will execute the commands in the “**fwupdate.cfg**” file on the TFTP server to upgrade those Z series IP PDUs supporting DHCP in the same network. You can Click “**Reboot Z series IP PDU**” in “**System**” of PPS-04-S.

The screenshot shows the configuration interface for a Z IP PDU. On the left is a sidebar menu with categories: Device, Status, Setting, and System. Under 'Setting', 'System' is selected. The main area is titled 'Z IP PDU' and contains several sections: 'Name' and 'Location' (text inputs), 'Temperature unit' (checkboxes for °C and °F), 'Date & Time' (date and time pickers), and 'Web Access' (protocol, port, and SSL certificate options). At the bottom, there are four buttons: 'Apply', 'Cancel', 'Reset to Factory Default', and 'Reboot Z IP PDU'. The 'Reboot Z IP PDU' button is circled in red.

 You must enable firmware upgrade via DHCP in SSH ( default is ENABLED ) and input the username and password for bulk firmware upgrade in the “**fwupdate.cfg**” file. You can change the username and password for bulk firmware upgrade via SSH. **See *Configuration of username / password for bulk firmware upgrade.***

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

### Configuration of username / password for bulk firmware upgrade

**Step 1.** Access the SSH using putty

**Step 2.** Input the login name and password to login the CLI.

```
Z4M login: 00000000
Password:

*****
*                               *
*          System Status        *
*                               *
*****
* Firmware                      *
*   -FirmwareID      : Z4M-Z100-240311 *
*   -Build_info     : 20240311         *
*                               *
* Device                  *
*   -Model          : Z4M              *
*   -Name           : default_z4m_name *
*   -Location       : default_z4m_loc. *
*   -Temp. unit     : C                *
*                               *
* Network settings          *
*   -Auto failover: Disable            *
*   [ LAN 1 (1000) ]                *
*   -LAN 1 link      : down            *
*   -Authen.         : None            *
*   -DHCP            : Enable          *
*   -MAC address     : 20:0A:0D:68:00:34 *
*                               *
```

**Step 3.** Select “ (U) Firmware upgrade ” and “ Enter ”

```
*   -IPM-04 support  : Yes             *
*   -SNMP agent      : Disable          *
*   -WebUI HTTPS     : Enable TLSv1/1.2/1.3 *
*   -FTP server       : Disable          *
*   -UDP discovery   : Enable           *
*   -Telnet          : Enable           *
*   -SSH console     : Enable           *
*   -Service account : Disable          *
*   -Firmware upgrade: Enable DHCP onBoot *
*****
*****
*                               *
*          Menu (Ver. 20.06.19)  *
*                               *
*****
* (0) Show system status          *
* (1) Change System settings      *
* (2) Change Login settings       *
* (5) Reboot                      *
* (U) Firmware upgrade            *
* (F) Reset to factory default and reboot *
* (?) This menu                   *
* (Q) Exit                       *
*****
Input menu item number(? for help):
```



## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

**Step 4.** Select “ (5) Change firmware upgrade authentication ” and “ Enter ”

```
*          Menu (Ver. 20.06.19)          *
*****
* (0) Show system status                *
* (1) Change System settings            *
* (2) Change Login settings             *
* (5) Reboot                           *
* (U) Firmware upgrade                  *
* (F) Reset to factory default and reboot *
* (?) This menu                         *
* (Q) Exit                             *
*****
Input menu item number(? for help):U

*****
*          Menu (Ver. 20.06.19)          *
*****
* (0) Show system status                *
* (1) Enable/Disable firmware upgrade via DHCP *
* (5) Change firmware upgrade authentication *
* (R) Reboot                           *
* (?) This menu                         *
* (Q) Exit                             *
*****
Input menu item number(? for help):
```

**Step 5.** Select “ (1) Change authentication name ” or “ (2) Change authentication password ” to change the username or password for bulk firmware upgrade purpose.

```
Input menu item number(? for help):U

*****
*          Menu (Ver. 20.06.19)          *
*****
* (0) Show system status                *
* (1) Enable/Disable firmware upgrade via DHCP *
* (5) Change firmware upgrade authentication *
* (R) Reboot                           *
* (?) This menu                         *
* (Q) Exit                             *
*****
Input menu item number(? for help):5

*****
* Firmware upgrade authentication        *
*****
* (0) Show system status                *
* (1) Change authentication name        *
* (2) Change authentication password    *
* (?) This menu                         *
* (Q) Exit                             *
*****
Input menu item number(? for help):
```

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

### < TFTP Requirements >

To perform bulk firmware upgrade successfully, your TFTP server must meet the following requirements :

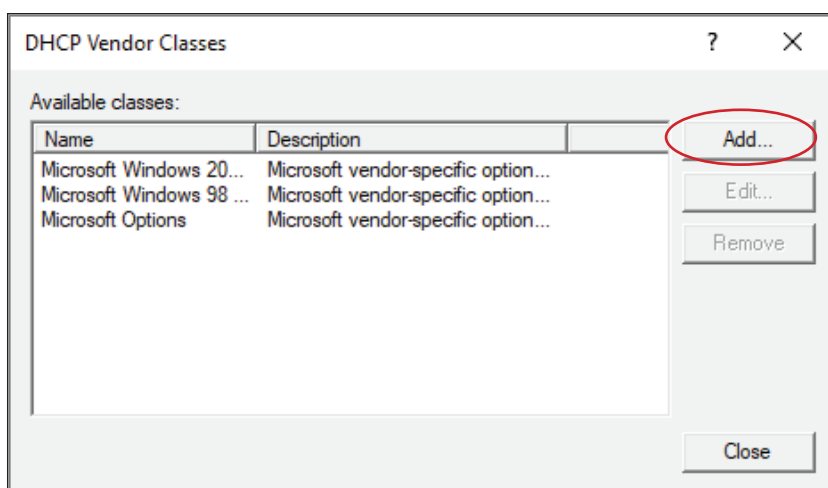
- Able to work with IPv4
- A folder containing all required files is available in the TFTP root directory. The folder name MUST be the same as the String value of the Magic code. Details please refer to DHCP IPv4 Configuration in Windows
- The TFTP server supports the write operation including file creation and upload.

### < DHCP IPv4 Configuration in Windows >

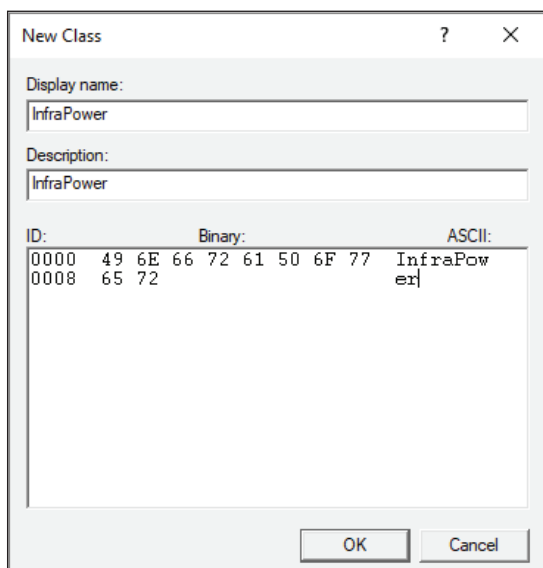
Please follow the procedures below to configure your DHCP server. The illustration below is based on Microsoft Windows Server 2019

**Step 1.** Add a new vendor class for Austin Hughes Z series IP PDU.

- Right Click the IPv4 node in DHCP to select Define Vendor Classes ( under server manager, select tools > DHCP
- Click “ **Add** ” to add a new vendor class.



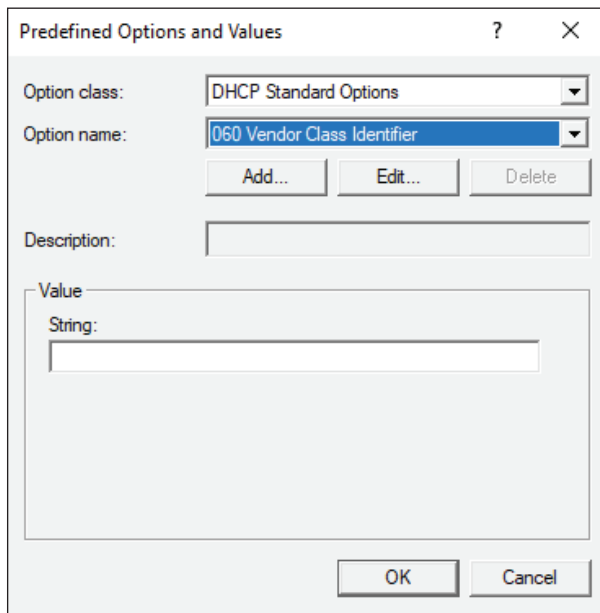
- Specify a unique name for this vendor class and type the binary codes of “ **InfraPower** ” in the New Class dialog. The vendor class is named “ **InfraPower** ” in this illustration.



## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

### Step 2. Define one DHCP standard option – Vendor Class Identifier

- Right Click the IPv4 node in DHCP to select Set Predefined Options.
- Select “ **DHCP Standard Options** ” in the “ **Option class** ” field, and  
“ **Vendor Class Identifier** ” in the “ **Option name** ” field. Leave the String field blank.



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 060 Vendor Class Identifier

Add... Edit... Delete

Description:

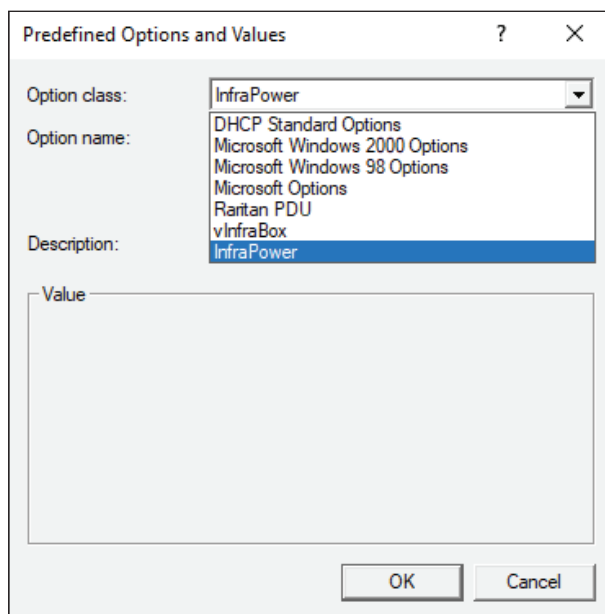
Value

String:

OK Cancel

### Step 3. Add four options to the new vendor class “ **InfraPower** ” in the same dialog. The fourth option is an optional item if the UDP port you set for the TFTP server is NOT 69.

- Select “ **InfraPower** ” in the “ **Option class** ” field.



Predefined Options and Values

Option class: InfraPower

Option name: DHCP Standard Options  
Microsoft Windows 2000 Options  
Microsoft Windows 98 Options  
Microsoft Options  
Raritan PDU  
vInfraBox  
InfraPower

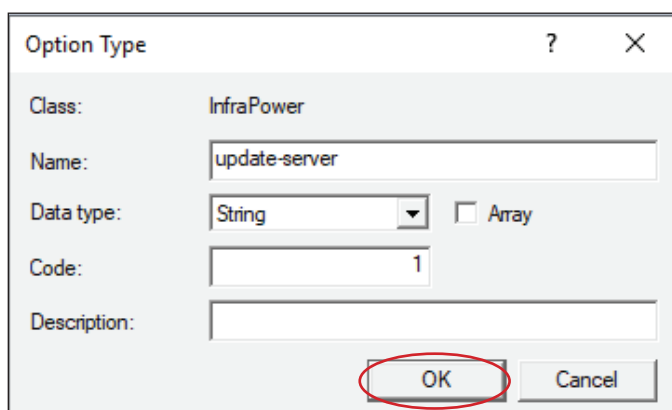
Description:

Value

OK Cancel

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

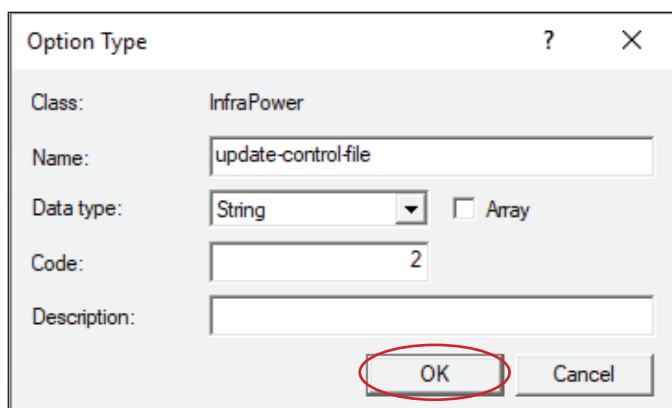
- Click “ **Add** ” to add the first option. Type “ **update-server** ” in the Name field, select String as the data type, and type 1 in the Code field and Click “ **OK** ”.



The dialog box titled "Option Type" has a close button (X) and a help button (?). It contains the following fields:

- Class: InfraPower
- Name: update-server
- Data type: String (selected from a dropdown menu), with an unchecked checkbox for Array.
- Code: 1
- Description: (empty text box)
- Buttons: OK (circled in red) and Cancel.

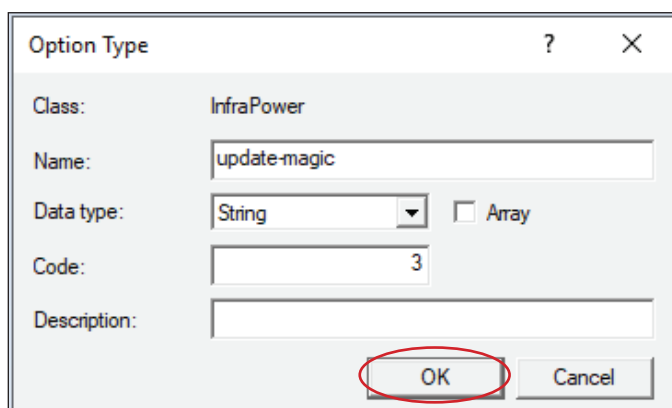
- Click “ **Add** ” to add the second option. Type “ **update-control-file** ” in the Name field, select String as the data type, and type 2 in the Code field and Click “ **OK** ”.



The dialog box titled "Option Type" has a close button (X) and a help button (?). It contains the following fields:

- Class: InfraPower
- Name: update-control-file
- Data type: String (selected from a dropdown menu), with an unchecked checkbox for Array.
- Code: 2
- Description: (empty text box)
- Buttons: OK (circled in red) and Cancel.

- Click “ **Add** ” to add the third option. Type “ **update-magic** ” in the Name field, select String as the data type, and type 3 in the Code field and Click “ **OK** ”.

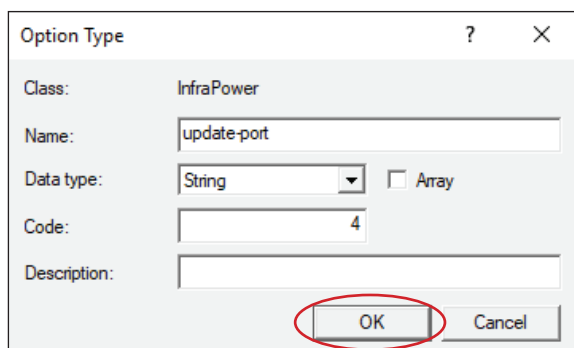


The dialog box titled "Option Type" has a close button (X) and a help button (?). It contains the following fields:

- Class: InfraPower
- Name: update-magic
- Data type: String (selected from a dropdown menu), with an unchecked checkbox for Array.
- Code: 3
- Description: (empty text box)
- Buttons: OK (circled in red) and Cancel.

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

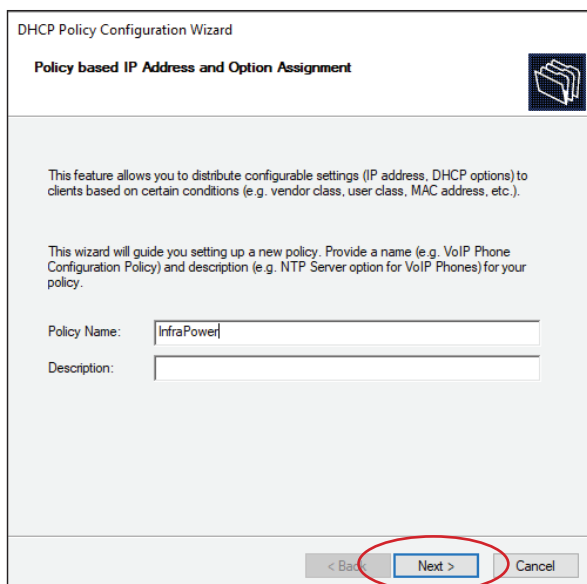
- Click “ **Add** ” to add the fourth option. Type “ **update-port** ” in the Name field, select String as the data type, and type 4 in the Code field and Click “ **OK** ”.



The 'Option Type' dialog box is shown. It has a title bar with a question mark and a close button. The 'Class' field is set to 'InfraPower'. The 'Name' field contains 'update-port'. The 'Data type' dropdown is set to 'String', and the 'Array' checkbox is unchecked. The 'Code' field contains the number '4'. The 'Description' field is empty. At the bottom, the 'OK' button is circled in red, and the 'Cancel' button is to its right.

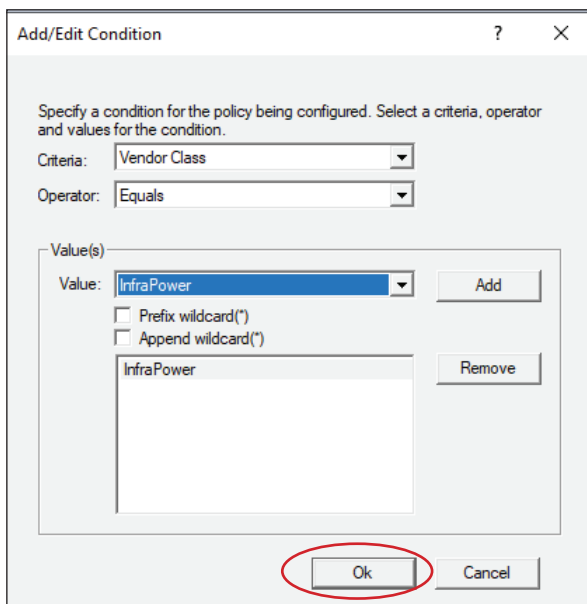
**Step 4.** Create a new policy associated with the “ **InfraPower** ” vendor class.

- Right Click the Policies node under IPv4 to select New Policy.
- Specify a policy name and click “ **Next** ”. The policy is named “ **InfraPower** ” in this illustration.



The 'DHCP Policy Configuration Wizard' is shown. The title bar says 'DHCP Policy Configuration Wizard'. The main title is 'Policy based IP Address and Option Assignment'. Below this, there is explanatory text: 'This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).' and 'This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.' Below the text are two input fields: 'Policy Name' with 'InfraPower' entered, and 'Description' which is empty. At the bottom, the 'Next >' button is circled in red, with '< Back' and 'Cancel' buttons to its left and right respectively.

- Click “ **Add** ” to add a new condition
- Select the vendor class “ **InfraPower** ” in the Value field, click “ **Add** ” and then “ **OK** ”.



The 'Add/Edit Condition' dialog box is shown. It has a title bar with a question mark and a close button. The text says 'Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.' Below this are two dropdown menus: 'Criteria' set to 'Vendor Class' and 'Operator' set to 'Equals'. Below these is a 'Value(s)' section. It has a 'Value:' dropdown set to 'InfraPower' and an 'Add' button. Below the dropdown are two checkboxes: 'Prefix wildcard(\*)' and 'Append wildcard(\*)', both unchecked. Below these is a list box containing 'InfraPower' and a 'Remove' button. At the bottom, the 'Ok' button is circled in red, and the 'Cancel' button is to its right.

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

- Click “ **Next** ”.
- Select “ **DHCP Standard Options** ” in the “ **Vendor class** ” field, select “ **060 Vendor Class Identifier** ” from the Available Options list, and type “ **InfraPower** ” in the “ **String value** ” field.

DHCP Policy Configuration Wizard

**Configure settings for the policy**  
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: DHCP Standard Options

Available Options	Description
<input checked="" type="checkbox"/> 060 Vendor Class Identifier	
<input type="checkbox"/> 064 NIS+ Domain Name	The name of the client's NIS+
<input type="checkbox"/> 065 NIS+ Servers	A list of IP addresses indicatinc

Data entry

String value:  
InfraPower

< Back   Next >   Cancel

- Select the “ **InfraPower** ” in the “ **Vendor class** ” field, select “ **001 update-server** ” from the Available Options list, and type your TFTP server’s IPv4 address in the “ **String value** ” field.

DHCP Policy Configuration Wizard

**Configure settings for the policy**  
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: InfraPower

Available Options	Description
<input checked="" type="checkbox"/> 001 update-server	
<input type="checkbox"/> 002 update-control-file	
<input type="checkbox"/> 003 update-magic	
<input type="checkbox"/> 004 vendorclass	vendorclass

Data entry

String value:  
192.168.0.1

< Back   Next >   Cancel

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

- Select “ **002 update-control-file** ” from the Available Options list, and type the filename “ **fwupdate.cfg** ” in the “ **String value** ” field.

The screenshot shows the 'DHCP Policy Configuration Wizard' window. At the top, it says 'Configure settings for the policy' and 'If the conditions specified in the policy match a client request, the settings will be applied.' Below this, the 'Vendor class' is set to 'InfraPower'. In the 'Available Options' list, '001 update-server' and '002 update-control-file' are checked. '003 update-magic' and '004 vendorclass' are unchecked. The 'Data entry' section shows the 'String value' field containing 'fwupdate.cfg'. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

- Select “ **003 update-magic** ” from the Available Options list, and type folder name of the files you stored in the root directory of the TFTP server in the “ **String value** ” field. This String value is the magic code to prevent the fwupdate.cfg commands from being executed repeatedly.

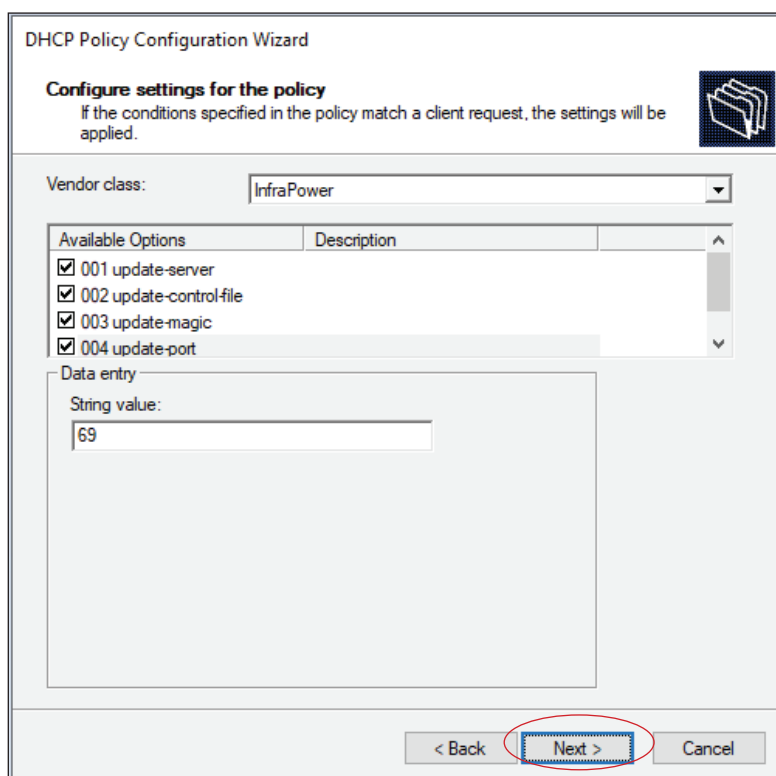
The screenshot shows the 'DHCP Policy Configuration Wizard' window. At the top, it says 'Configure settings for the policy' and 'If the conditions specified in the policy match a client request, the settings will be applied.' Below this, the 'Vendor class' is set to 'InfraPower'. In the 'Available Options' list, '001 update-server', '002 update-control-file', and '003 update-magic' are checked. '004 vendorclass' is unchecked. The 'Data entry' section shows the 'String value' field containing 'IPD-03-FW-3.0-2020207'. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.



The magic code is transmitted to and stored in Z series IP PDU at the time of executing the “ **fwupdate.cfg** ” commands. The DHCP/TFTP operation is triggered **ONLY** when there is a mismatch between the magic code in DHCP and the one stored in Z series IP PDU. Therefore, you must modify the magic code’s value in DHCP when intending to execute the “ **fwupdate.cfg** ” commands next time.

## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

- Select “ **004 update-port** ” from the Available Options list, and type UDP port number you set for the TFTP server in the “ **String value** ” field. Port number 69 is used in this illustration.



The screenshot shows the 'DHCP Policy Configuration Wizard' window. At the top, it says 'Configure settings for the policy' with a sub-note: 'If the conditions specified in the policy match a client request, the settings will be applied.' Below this, the 'Vendor class' is set to 'InfraPower'. A table titled 'Available Options' lists four options, all of which are checked: '001 update-server', '002 update-control-file', '003 update-magic', and '004 update-port'. Below the table is a 'Data entry' section with a 'String value:' label and a text box containing the number '69'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red oval.

Available Options	Description
<input checked="" type="checkbox"/> 001 update-server	
<input checked="" type="checkbox"/> 002 update-control-file	
<input checked="" type="checkbox"/> 003 update-magic	
<input checked="" type="checkbox"/> 004 update-port	

Data entry

String value:

69

< Back   **Next >**   Cancel

- Click “ **Next** ” and “ **Finish** ” to complete the setup.



## < 2.12 > Bulk Firmware Upgrade of Z series IP PDU

### Description of Devices.csv

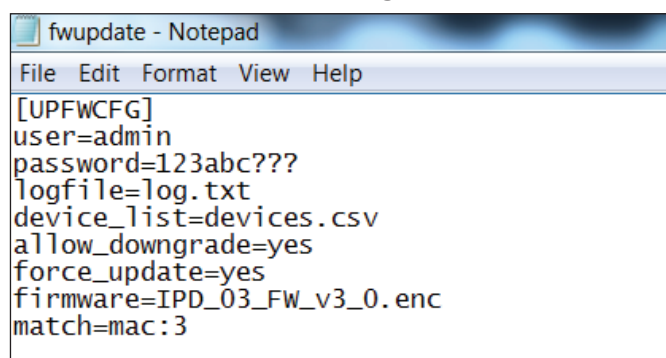
	A	B	C	D	E
1	1	1	20:0A:0D:FF:CA:BF	192.168.0.123	192.168.0.1
2	1	1	20:0A:0D:FF:3C:E6	192.168.0.122	192.168.0.1
3	#--keep this be the last line of this file--				
4					
5					

Column A & B is reserved for future use

Column C is the MAC address of the network interface of the Z series IP PDU. As the Z series IP PDU comes with two network interface, we highly recommend to do the bulk firmware upgrade via either one of the network interface.

Column D & E is the IP address of the network interface of the Z series IP PDU and the TFTP server respectively.

### Description of fwupdate.cfg



```
[UPFWCFG]
user=admin
password=123abc???
logfile=log.txt
device_list=devices.csv
allow_downgrade=yes
force_update=yes
firmware=IPD_03_FW_v3_0.enc
match=mac:3
```

First and second row is the user and password for authentication of bulk firmware upgrade which can be configured via SSH. Details refer to Section “**Configuration of username / password for bulk firmware upgrade**”.

Fourth row tells the TFTP server to generate a log file after bulk firmware upgrade is performed. It is stored at the same location of the fwupdate.cfg and the filename is the same as the MAC address of the Z series IP PDU.

Fifth row lets Z series IP PDU to check if its’ MAC address exists in the column 3 of devices.csv to execute the firmware upgrade.

Eighth row is the firmware version you want to upgrade, it MUST be the same as the filename of the firmware stored in the folder under the root directory of the TFTP server.

## < 2.13 > 802.1X authentication

### User Guide of 802.1X Authentication

802.1X is an authentication protocol which provides protected authentication for secure network access with the use of a Radius server. It opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.

Before configure the 802.1X authentication, ensure the system clock of the Z series IP PDU is set up properly. Otherwise, the authentication will fail while the RADIUS server verifies the validity of the certificate. You can go the System of PPS-04-S to set up the date and time of the Z series IP PDU.

InfraPower PPS-04-S

Version : Q125V1

Device

Status

• Details

• Outlet Group

• Outlet Sequence

Sensor

Setting

System

Network

Login

• Local User

• LDAP

• Radius

SNMP

Notification

Syslog

Firmware

Z IP PDU

Name :  
default\_z4m\_name

Location :  
default\_z4m\_loc

Temperature unit :  
☒ °C ☐ °F

Date & Time  
2025-04-22 15:59:53

Time zone :  
GMT+08:00 ▾

Time setting :  
Synchronize with NTP server ▾

NTP server :  
time.google.com Sync Now

Web Access

Protocol :  
HTTPS ▾

Port :  
443 ( Default: 443 )

SSL Certificate :  
☒ Use default certificate  
☐ Use custom certificate

Apply Cancel Reset to Factory Default Reboot Z IP PDU

## < 2.13 > 802.1X authentication

Please follow the procedures below to setup the 802.1X authentication in PPS-04-S.

### < 802.1X authentication for Wired network >

**Step 1.** Login the PPS-04-S and go the Network.

**Device**

- Status
- Details
- Outlet Group
- Outlet Sequence
- Sensor
- Setting**
- System
- Network**
- Login
- Local User
- LDAP
- LDAP Role
- Radius
- SNMP
- Notification
- Syslog
- Firmware

**Network**

**LAN 1 settings**

DHCP :

IPv4 address : 192.168.2.105

IPv6 address : fe80::220a:dff:fe62:5/64

Subnet mask : 255.255.252.0

Gateway : 192.168.1.1

Authentication :

Preferred Hostname :

Enable automatic failover : ☐

**DNS**

Manually configure DNS server : ☐

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

**LAN 2 settings**

DHCP :

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

Authentication :

Preferred Hostname :

**Step 2.** Click the Authentication pull down menu and you will see the authentication method.

**Device**

- Status
- Details
- Outlet Group
- Outlet Sequence
- Sensor
- Setting**
- System
- Network**
- Login
- Local User
- LDAP
- LDAP Role
- Radius
- SNMP
- Notification
- Syslog
- Firmware

**Network**

**LAN 1 settings**

DHCP :

IPv4 address : 192.168.2.105

IPv6 address : fe80::220a:dff:fe62:5/64

Subnet mask : 255.255.252.0

Gateway : 192.168.1.1

Authentication :

Preferred Hostname :

Enable automatic failover : ☐

**DNS**

Manually configure DNS server : ☐

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

**LAN 2 settings**

DHCP :

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

Authentication :

Preferred Hostname :

None

PEAP

TLS

## < 2.13 > 802.1X authentication

**Step 3.** To use PEAP as authentication method, select PEAP. Then input the “**Identity**”, “**Password**” and “**CA certificate**” in PEM format. You can uncheck “**Enable CA certificate**” to bypass the authentication using CA certificate. Click “**Apply**” to save the configuration.

The screenshot shows the 'Network' configuration page. On the left is a sidebar with a tree view containing 'Device', 'Status', 'Details', 'Outlet Group', 'Outlet Sequence', 'Sensor', 'Setting', 'System', 'Network', 'Login', 'Local User', 'LDAP', 'LDAP Role', 'Radius', 'SNMP', 'Notification', 'Syslog', and 'Firmware'. The 'Setting' section is expanded, and 'Network' is selected. The main area is divided into 'LAN 1 settings' and 'LAN 2 settings'. 'LAN 1 settings' includes DHCP (ON), IPv4 address (192.168.2.105), IPv6 address (fe80::220a:dff:fe62:5/64), Subnet mask (255.255.252.0), Gateway (192.168.1.1), Authentication (None), Preferred Hostname, and an 'Enable automatic failover' checkbox. 'LAN 2 settings' includes DHCP (ON), IPv4 address (not available), IPv6 address (not available), Subnet mask (not available), Gateway (not available), Authentication (PEAP), Identity (redacted), Password (redacted), CA certificate (redacted with a 'Browse' button), 'Enable CA certificate' (checked), and Preferred Hostname. Red text indicates 'Identity is required.' and 'CA cert is required.'. At the bottom, the 'Apply' button is circled in red, next to a 'Cancel' button. A 'DNS' section at the bottom allows manually configuring DNS servers with Primary DNS (8.8.8.8) and Secondary DNS (0.0.0.0).

**Step 4.** To use TLS as authentication method, select TLS. Then input the “**Identity**”, “**Certificate**”, “**Private key**”, “**Private key password**” and “**CA certificate**”. (Certificate, private key and CA certificate are in PEM format ) Click “**Apply**” to save the configuration.

This screenshot shows the same 'Network' configuration page as Step 3, but with 'Authentication' set to 'TLS' in the 'LAN 2 settings'. The 'Identity' field is redacted. The 'Certificate' field is redacted with a 'Browse' button, and red text indicates 'Certificate is required.'. The 'Private key' field is redacted with a 'Browse' button, and red text indicates 'Private key is required.'. The 'Private key password' field is empty. The 'CA certificate' field is redacted with a 'Browse' button, and red text indicates 'CA cert is required.'. The 'Enable CA certificate' checkbox remains checked. The 'Apply' button at the bottom is circled in red. The 'DNS' section at the bottom is identical to the previous screenshot.

## < 2.13 > 802.1X authentication

### < 802.1X authentication for Wireless network >

**Step 1.** Login the PPS-04-S and go to Network. Click the Authentication pull down menu and you will see the authentication method

The screenshot displays the 'Network' configuration page for a PPS-04-S device. On the left is a navigation menu with sections: Device (Status, Details, Outlet Group, Outlet Sequence, Sensor), Setting (System, Network, Login, Local User, LDAP, LDAP Role, Radius, SNMP, SNMP Traps, Notification, Syslog, Firmware), and the 'Network' section is currently selected. The main content area is titled 'Network' and contains several configuration sections:

- LAN 1 settings:** DHCP is set to 'ON'. IPv4, IPv6, Subnet mask, and Gateway are all 'not available'. Authentication is set to 'None' (a dropdown menu is open showing 'None', 'PSK', 'PEAP', and 'TLS'). Preferred Hostname is 'nVent'.
- LAN 2 settings:** DHCP is set to 'ON'. IPv4 is '192.168.2.121', IPv6 is 'fe80::220a:dff:fe68:31/64', Subnet mask is '255.255.252.0', and Gateway is '192.168.1.1'. Authentication is set to 'None'. Preferred Hostname is empty.
- WiFi settings:** ESSID is 'dlink-7614' (with a 'Scan Wifi' button), Authentication is 'None' (dropdown open), DHCP is 'None', IPv4, IPv6, Subnet mask, and Gateway are 'not available'. Preferred Hostname is empty.
- Enable automatic failover:** An unchecked checkbox.
- DNS:** 'Manually configure DNS server' is unchecked. Primary DNS is '192.168.1.60' and Secondary DNS is '202.130.97.65'.

At the bottom are 'Apply' and 'Cancel' buttons.

## < 2.13 > 802.1X authentication

**Step 2.** To use PEAP as authentication method, select PEAP. Select the Wireless network from “ **ESSID** ”, input the “ **Identity** ”, “ **Password** ” and “ **CA certificate** ” in PEM format. You can uncheck “ **Enable CA certificate** ” to bypass the authentication using CA certificate. If you have the DHCP server to assign the IP address to the Wireless network, select “ **ON** ” from DHCP.

If you select “ **OFF** ” from DHCP, please input the “ **IPv4 address** ”, “ **Subnet mask** ” and “ **Gateway** ”. Click “ **Apply** ” to save the configuration.

The screenshot displays the Network configuration interface. On the left, a sidebar menu includes 'Device' (Status, Details, Outlet Group, Outlet Sequence, Sensor) and 'Setting' (System, Network, Login, Local User, LDAP, LDAP Role, Radius, SNMP, SNMP Traps, Notification, Syslog, Firmware). The 'Network' section is active, showing 'LAN 1 settings' and 'LAN 2 settings'. The 'WiFi settings' section is highlighted, showing 'ESSID' (dlink-7614), 'Authentication' (PEAP), 'Identity' (redacted), 'Password' (redacted), and 'CA certificate' (redacted). The 'Identity is required.' message is displayed. The 'DHCP' setting is 'ON'. The 'DNS' section shows 'Manually configure DNS server' (unchecked), 'Primary DNS' (192.168.1.60), and 'Secondary DNS' (202.130.97.65). The 'Apply' button is circled in red.

Device	Setting
Status	
Details	
Outlet Group	
Outlet Sequence	
Sensor	
Setting	
System	
Network	
Login	
Local User	
LDAP	
LDAP Role	
Radius	
SNMP	
SNMP Traps	
Notification	
Syslog	
Firmware	

### Network

#### LAN 1 settings

DHCP :

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

Authentication :

Preferred Hostname : nVent

Enable automatic failover : ☐

#### LAN 2 settings

DHCP :

IPv4 address : 192.168.2.121

IPv6 address : fe80::220a:dff:fe68:31/64

Subnet mask : 255.255.252.0

Gateway : 192.168.1.1

Authentication :

Preferred Hostname :

#### WiFi settings

ESSID :

Authentication :

Identity :

Identity is required.

Password :

CA certificate :

☐ Enable CA certificate

DHCP :

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

Preferred Hostname :

#### DNS

Manually configure DNS server : ☐

Primary DNS :

Secondary DNS :

## < 2.13 > 802.1X authentication

**Step 3.** To use TLS as authentication method, select TLS. Select the Wireless network from “ **ESSID** ”, input the “ **Identity** ”, “ **Certificate** ”, “ **Private key** ”, “ **Private key password** ” and “ **CA certificate** ”.  
( Certificate, private key and CA certificate are in PEM format )

If you have the DHCP server to assign the IP address to the Wireless network, select “**ON**” from DHCP.

If you select “ **OFF** ” from DHCP, please input the “ **IPv4 address** ”, “ **Subnet mask** ” and “ **Gateway** ”.  
Click “ **Apply** ” to save the configuration.

The screenshot displays the 'Network' configuration page. On the left is a sidebar with a 'Setting' menu where 'Network' is selected. The main area is divided into several sections:

- LAN 1 settings:** DHCP is set to 'ON'. IPv4, IPv6, Subnet mask, and Gateway are all 'not available'. Authentication is set to 'None'. Preferred Hostname is 'nVent'.
- LAN 2 settings:** DHCP is set to 'ON'. IPv4 address is '192.168.2.121', IPv6 address is 'fe80::220a:dff:fe68:31/64', Subnet mask is '255.255.252.0', and Gateway is '192.168.1.1'. Authentication is set to 'None'.
- WiFi settings:** ESSID is 'dlink-7614'. Authentication is set to 'TLS'. The Identity field is empty with a red error message 'Identity is required.'. Certificate and Private key fields are also empty with red error messages 'Certificate is required.' and 'Private key is required.' respectively. There are 'Browse' buttons for these fields. Private key password and CA certificate fields are empty. There is an 'Enable CA certificate' checkbox which is unchecked.
- DNS:** Manually configure DNS server is unchecked. Primary DNS is '192.168.1.60' and Secondary DNS is '202.130.97.65'.

At the bottom, there are 'Apply' and 'Cancel' buttons. The 'Apply' button is circled in red.



## < Section 3 > Command Line Interface ( CLI ) Access

### < 3.1 > Command Line Interface ( CLI ) Access

Command Line Interface ( CLI ) allows you access the Z series IP PDU via Telnet or Secure Shell ( SSH ) to configure the system settings and login settings. If the Z series IP PDU is in factory default setting or password is “ 00000000 “, you MUST change the password during the login. After you change the password, you can configure the system and login settings of the Z series IP PDU.

By default, CLI access via SSH is enabled and Telnet is disabled whereas the Telnet can be enabled.

CLI and PPS-04-S shares the same login name & password. The CLI session will be terminated automatically if three unsuccessful login attempts.

You can change the following settings via CLI access :

- i. System settings
  - Change temperature display unit : change the temp unit to be displayed in the PPS-04-S
  - Change system RTC date time : set the system time of the Z series IP PDU
  - Change network settings : change the IP settings of the Z series IP PDU
  - Change features & services
    - a. Enable / disable management software support
    - b. Enable / disable SNMP agent
    - c. Enable / disable FTP server
    - d. Enable / disable WEBUI
    - e. Enable / disable UDP
    - f. Enable / disable Telnet
    - g. Enable / disable maintenance ( service ) account
- ii. Login settings
  - Change login name
  - Change login password
  - Reset to default login name & password

The company reserves the right to modify product specifications without prior notice and assumes no responsibility for any error which may appear in this publication.

All brand names, logo and registered trademarks are properties of their respective owners.

Copyright 2025 Austin Hughes Electronics Ltd. All rights reserved.