InfraPower®

Inspired by Your Data Center

User Manual - PPS-04-S

GUI & SNMP for Z series IP PDU

Designed and manufactured by Austin Hughes

Legal Information

First English printing, April 2024
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 40º Celsius (104º Fahrenheit).
- ■ When installing, place the equipment on a sturdy, level surface to prevent it from accidentally falling and causing dam age 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 dam aged 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 invali date 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 a residential installation.
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

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

< Section 3 > Command Line Interface Access

< Section 1 > General

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

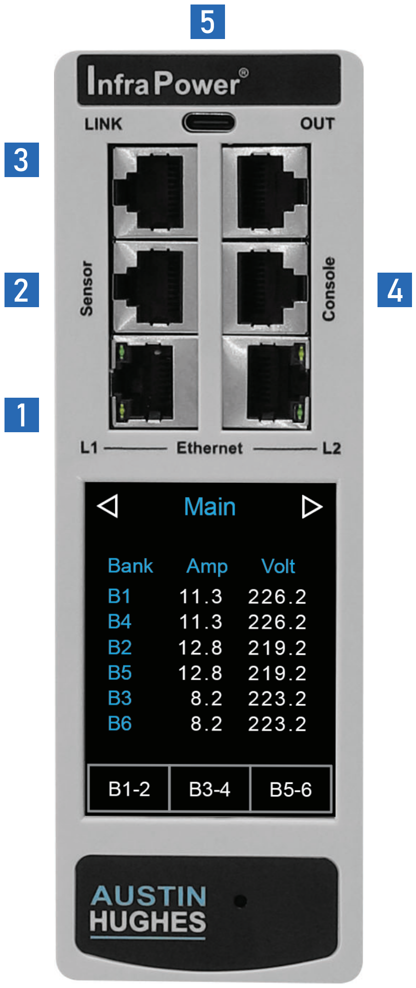
InfraPower PPS-04-S

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

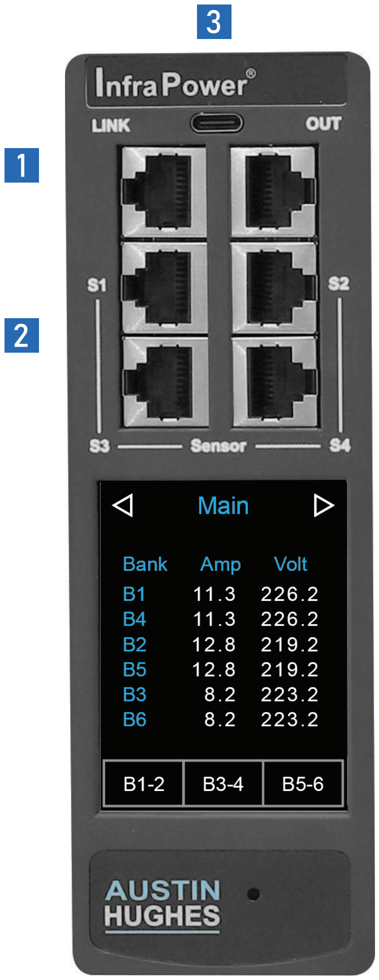
The +/- 0.5% accuracy of the InfraPower PDU meter is vital for billing accuracy, energy efficiency, capacity planning and performance monitoring.

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

The Z series IP PDU supports Automatic Private Internet Protocol Addressing (APIPA). 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. The IP address range for APIPA is 169.254.0.1 to 169.254.255.254.

Configuration over a DHCP-enabled network :

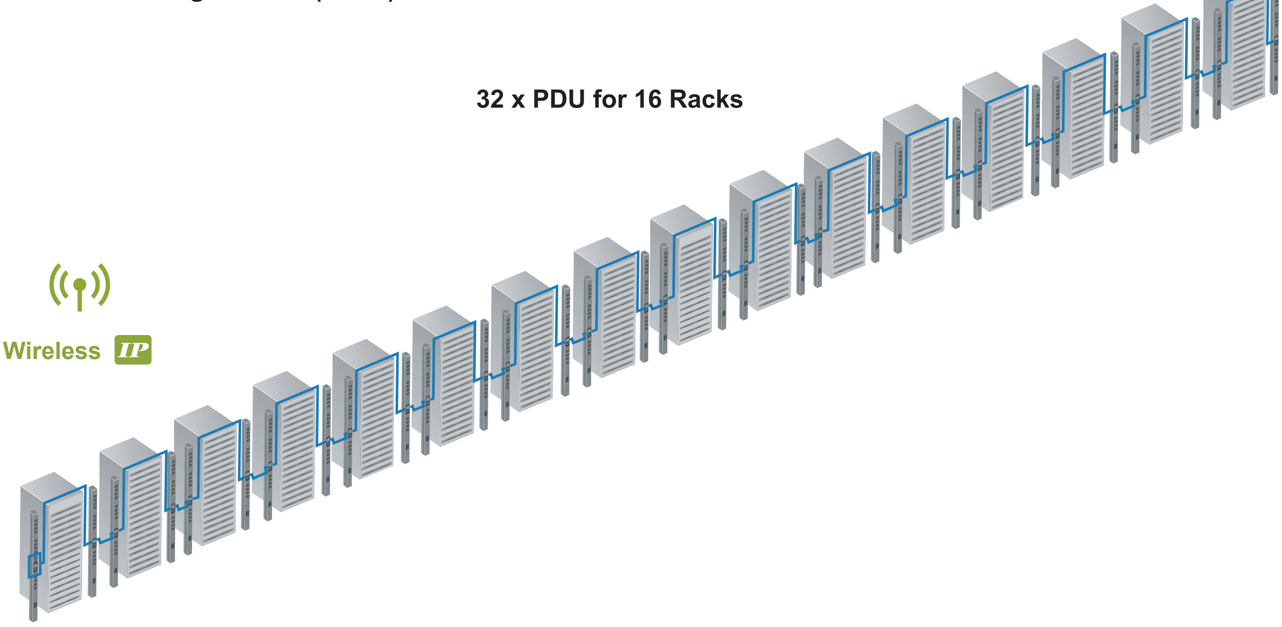
1. Connect a Cat 5e / 6 cable to one of the LAN port of Z series IP PDU.
2. Connect the other end of the Cat 5e / 6 cable to your TCP/IP network.
3. Get the DHCP assigned IPv4 address which can be found on the “ Network ” page of the touchscreen LCD display.
4. Open a web browser to enter the DHCP assigned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

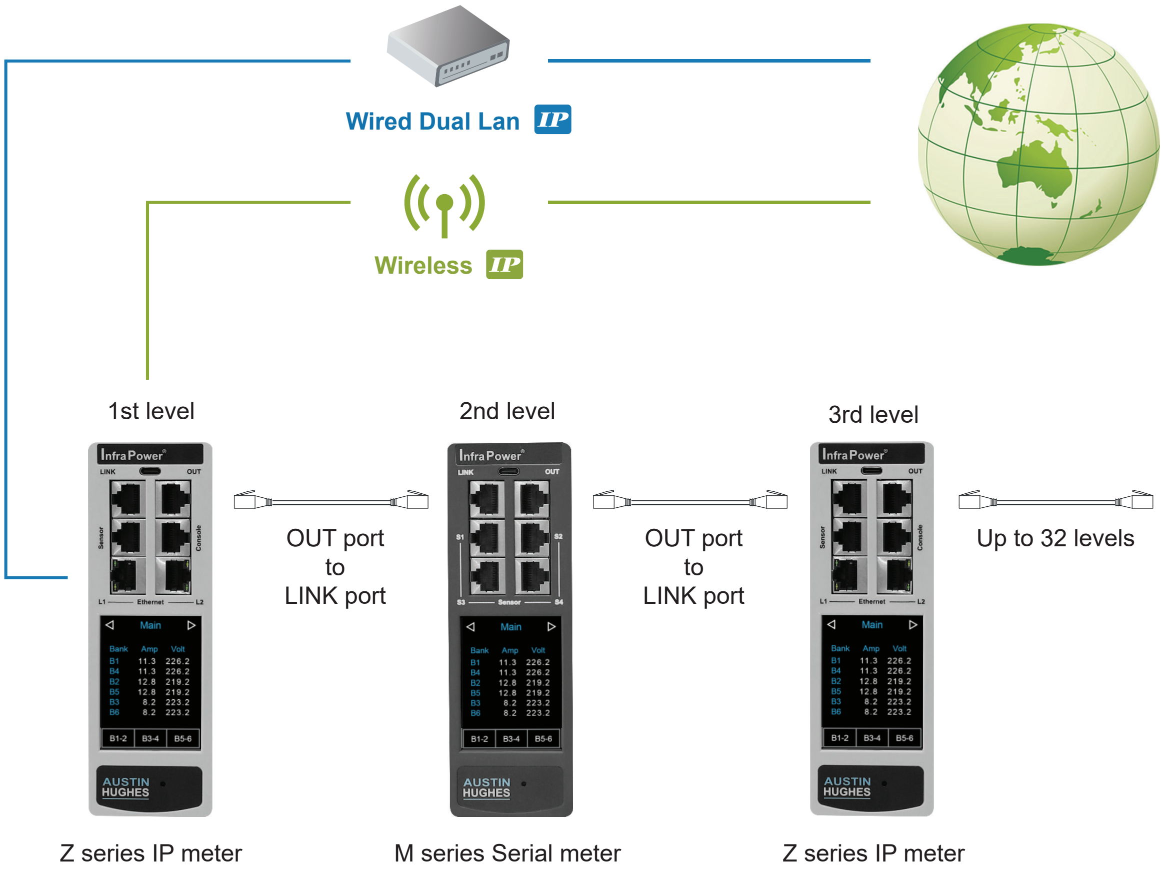
Configuration using a connected computer :

1. Connect a Cat 5e / 6 cable to one of the LAN port of Z series IP PDU.
2. Connect the other end of the Cat 5e / 6 cable to the computer. Ensure the network configuration of the computer is DHCP.
3. Get the DHCP assigned IPv4 address which can be found on the “ Network ” page of the touchscreen LCD display. Both the IP addresses of the Z series IP PDU and the computer will be automatically configured with the IP address range for APIPA if the computer connected to Z series IP PDU is NOT a DHCP server.
4. Open a web browser to enter the DHCP / APIPA 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)

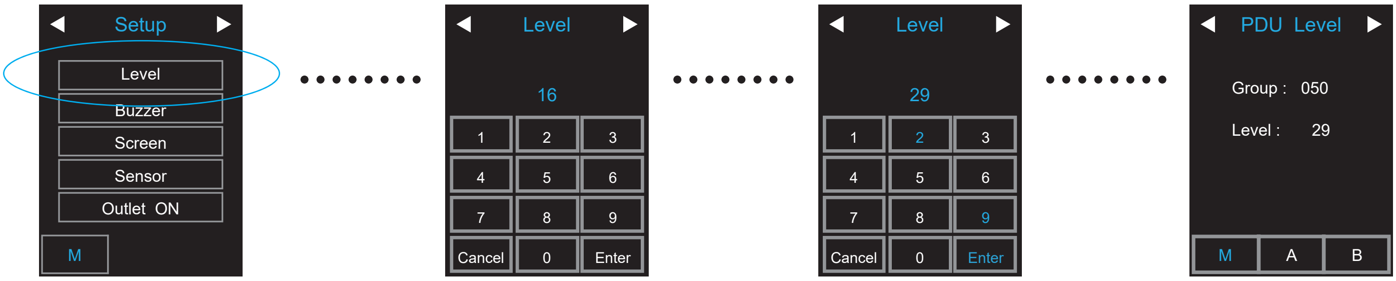




- Only 1st level Z series IP PDU can provide the function of PPS-04-S (Please refer to Section II for details)
- All Z series IP PDUs NOT in 1st level MUST be set to expansion mode.

< 1.6 > PDU Level Setting

1. PDU Level Setting on local meter display

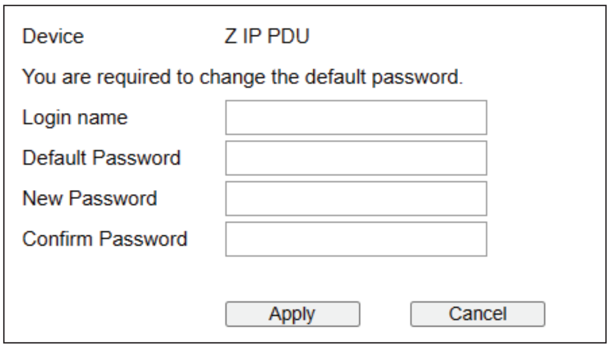


2. PDU Level Setting by Remote (see < 1.8 > Remote PDU Level Setting)

< 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

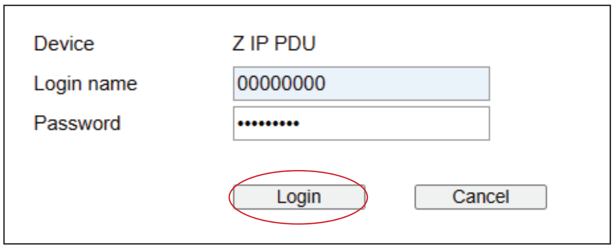


Device	Z IP PDU

You are required to change the default password.

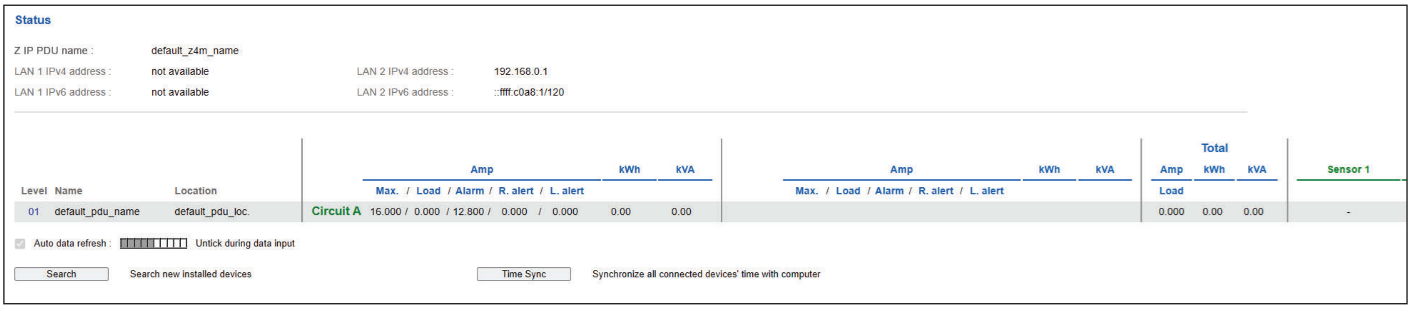
Login name	
Default Password	
New Password	
Confirm Password	

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	•••••••••

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:c0a8:1/120

				Amp	kWh	kVA	Amp	kWh	kVA	Total Amp	Total kWh	Total kVA	Sensor 1
Level	Name	Location		Max. / Load / Alarm / R. alert / L. alert			Max. / Load / Alarm / R. alert / L. alert			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 new installed devices

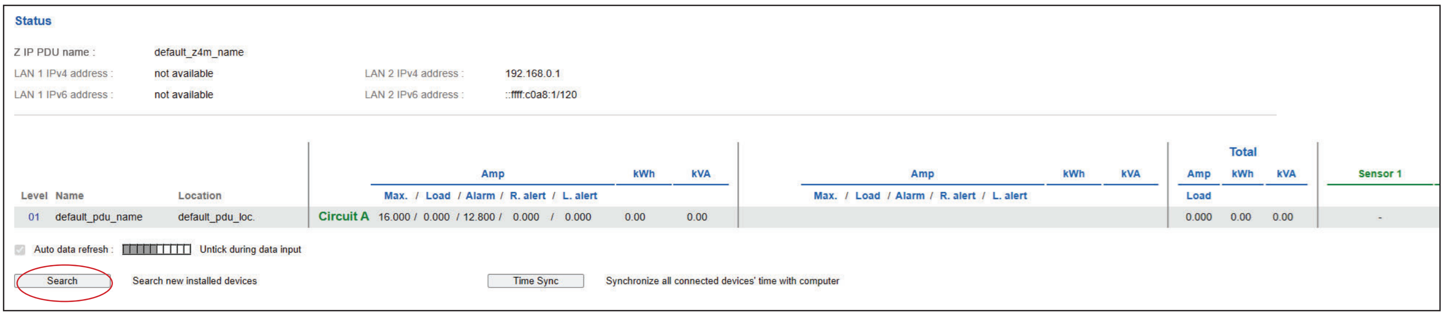
Synchronize all connected devices' time with computer

< 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

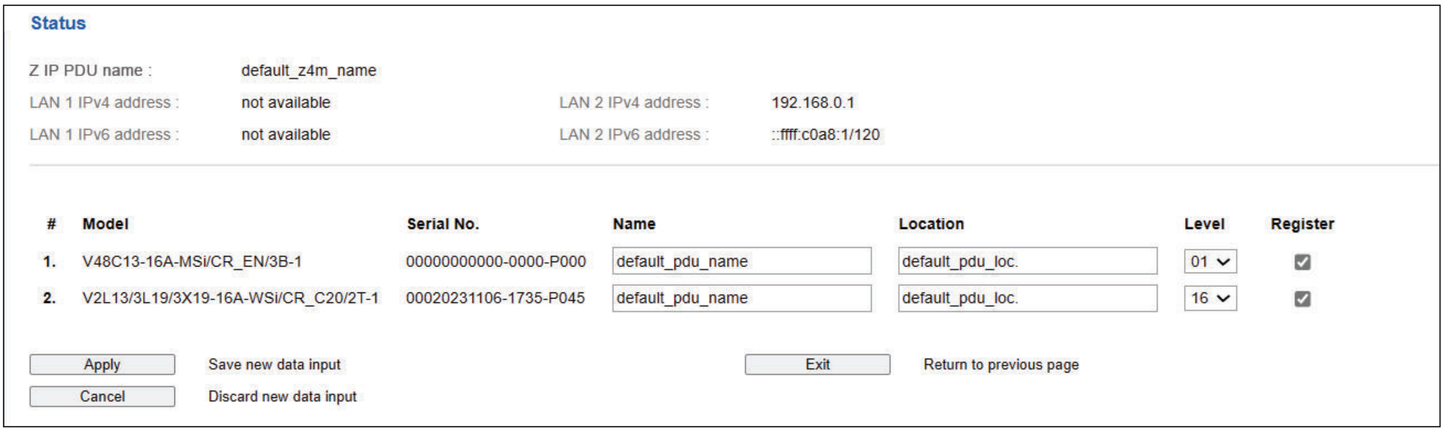
										Total			
				Amp	kWh	kVA		Amp	kWh	kVA	Amp	kWh	kVA	Sensor 1
Level	Name	Location		Max. / Load / Alarm / R. alert / L. alert				Max. / Load / Alarm / R. alert / L. alert			Load			
01	default_pdu_name	default_pdu_loc.	Circuit A	16.000 / 0.000 / 12.800 / 0.000 / 0.000	0.00	0.00					0.000	0.00	0.00	-

☑ Auto data refresh : Untick during data input

Search — Search new installed devices

Time Sync — Synchronize all connected devices' time with computer

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

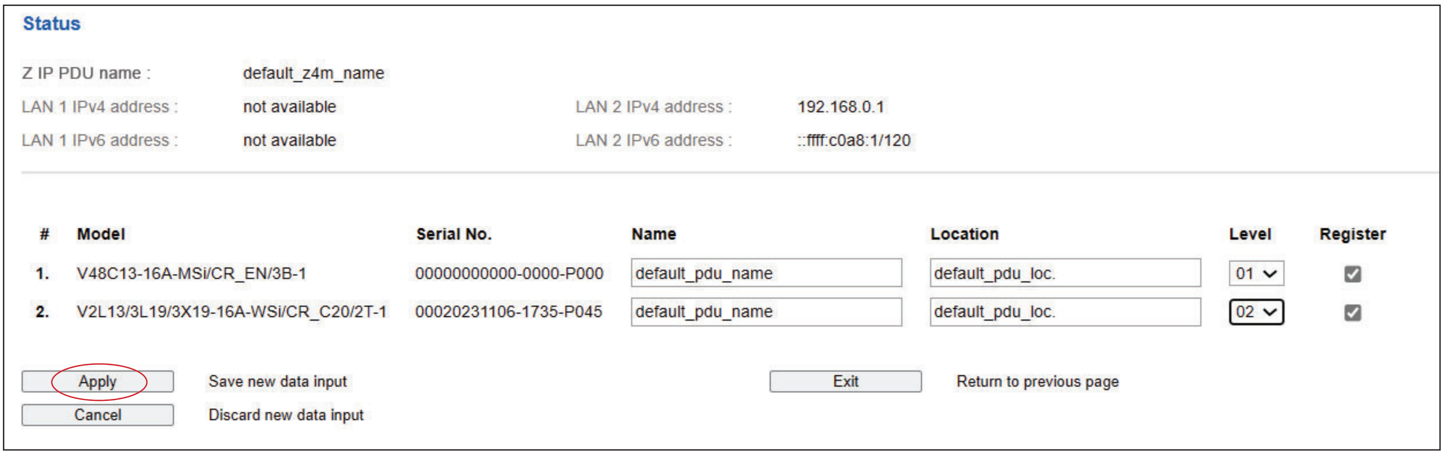
#	Model	Serial No.	Name	Location	Level	Register
1.	V48C13-16A-MSi/CR_EN/3B-1	00000000000-0000-P000	default_pdu_name	default_pdu_loc.	01	☑
2.	V2L13/3L19/3X19-16A-WSi/CR_C20/2T-1	00020231106-1735-P045	default_pdu_name	default_pdu_loc.	16	☑

Apply — Save new data input

Cancel — Discard new data input

Exit — Return to previous page

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	☑
2.	V2L13/3L19/3X19-16A-WSi/CR_C20/2T-1	00020231106-1735-P045	default_pdu_name	default_pdu_loc.	02	☑

Apply — Save new data input

Cancel — Discard new data input

Exit — Return to previous page

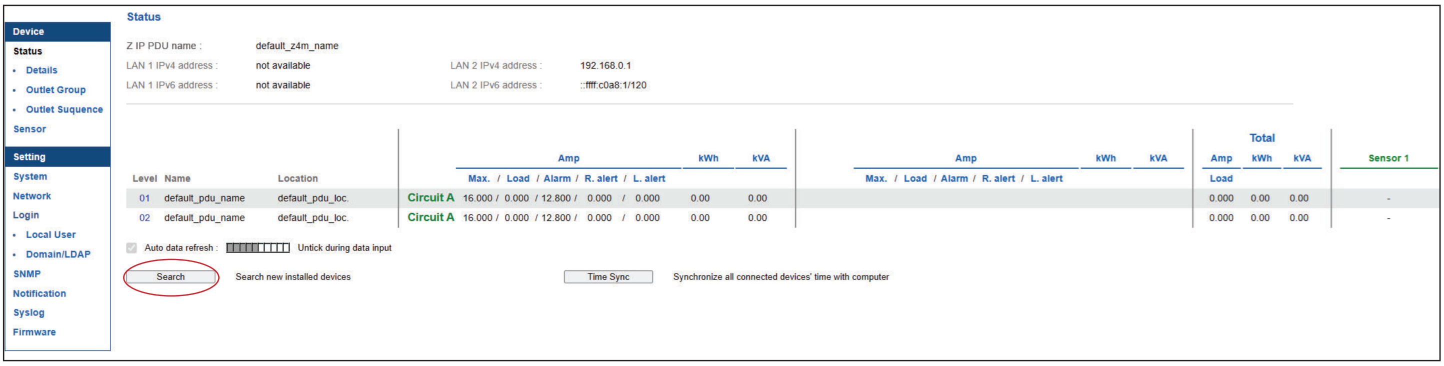
< Section 2 > General

< 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



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

				Amp	kWh	kVA	Amp	kWh	kVA	Total Amp	Total kWh	Total kVA	Sensor 1
Level	Name	Location		Max. / Load / Alarm / R. alert / L. alert			Max. / Load / Alarm / R. alert / L. alert			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	-
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	-

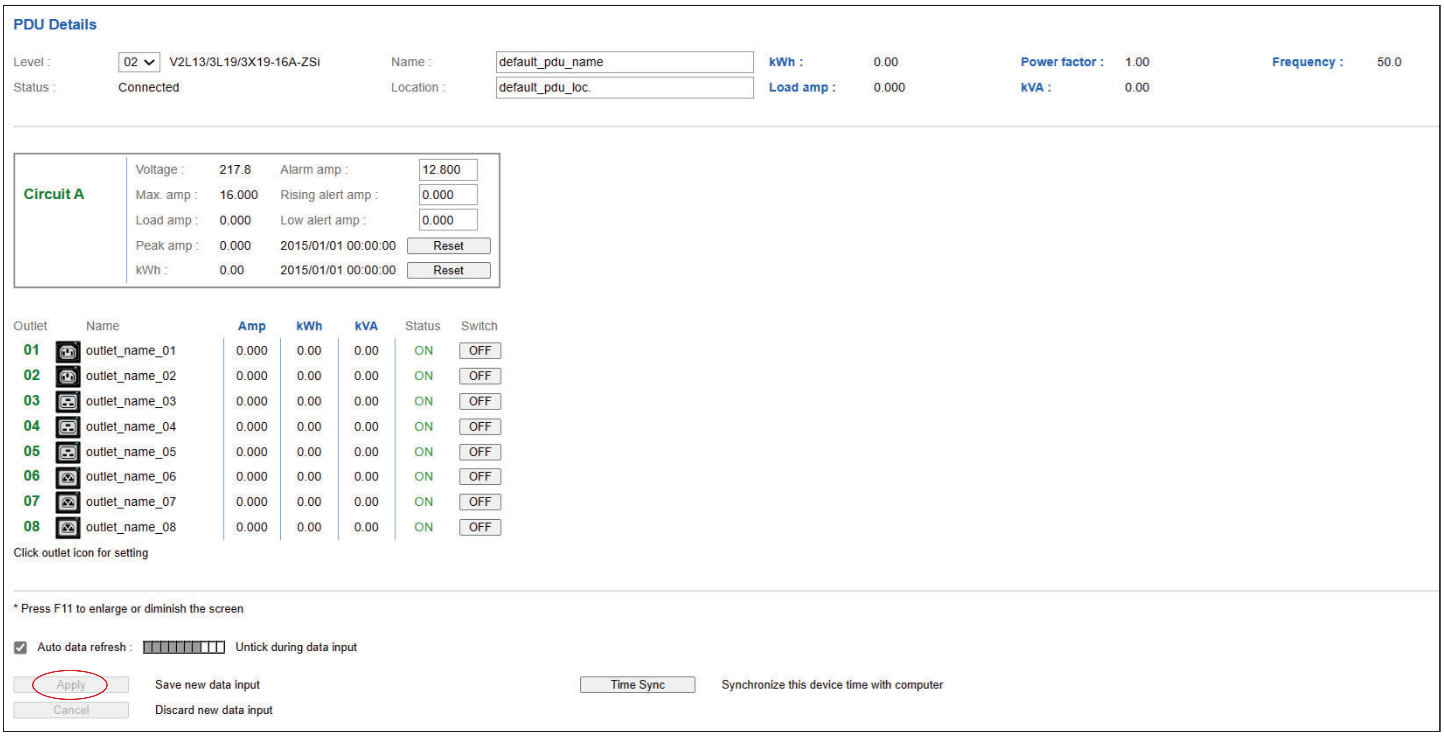
☑ Auto data refresh : Untick during data input

Search — Search new installed devices

Time Sync — Synchronize all connected devices' time with computer

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 swich 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



PDU Details

Level : 02 V2L13/3L19/3X19-16A-ZSi — Name : default_pdu_name — kWh : 0.00 — Power factor : 1.00 — Frequency : 50.0

Status : Connected — Location : default_pdu_loc. — Load amp : 0.000 — kVA : 0.00

Circuit A				
	Voltage :	217.8	Alarm amp :	12.800
	Max. amp :	16.000	Rising alert amp :	0.000
	Load amp :	0.000	Low alert amp :	0.000
	Peak amp :	0.000	2015/01/01 00:00:00	Reset
	kWh :	0.00	2015/01/01 00:00:00	Reset

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

Click outlet icon for setting

* Press F11 to enlarge or diminish the screen

☑ Auto data refresh : Untick during data input

Apply — Save new data input

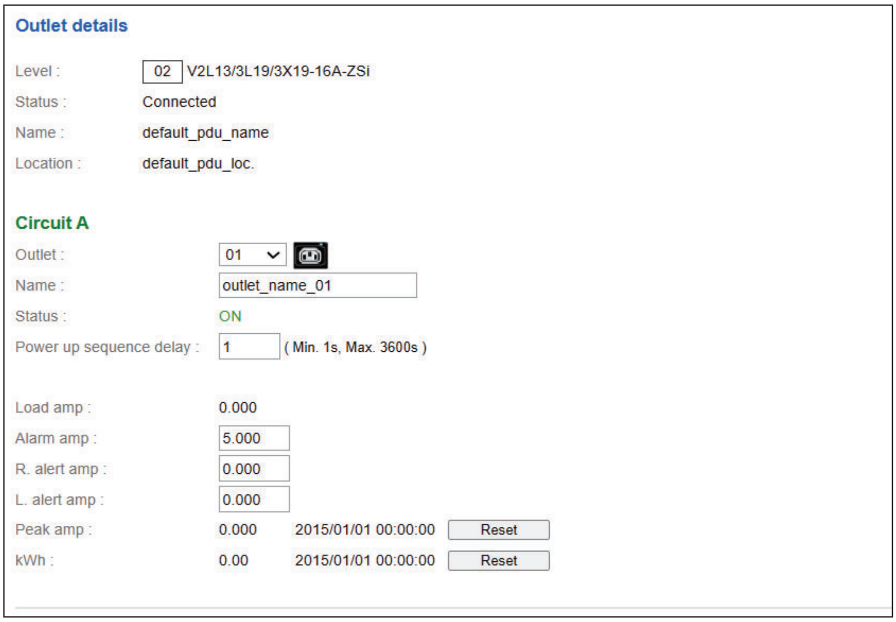
Cancel — Discard new data input

Time Sync — Synchronize this device time with computer

< 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 :	02 V2L13/3L19/3X19-16A-ZSi		
Status :	Connected		
Name :	default_pdu_name		
Location :	default_pdu_loc.		

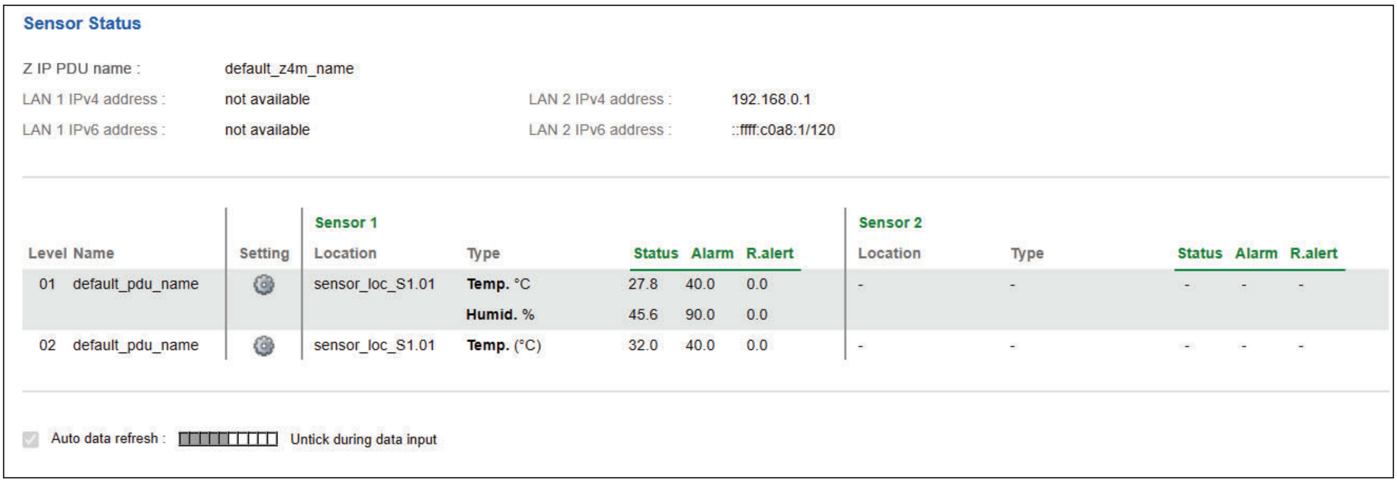
Circuit A

Outlet :	01		
Name :	outlet_name_01		
Status :	ON		
Power up sequence delay :	1 (Min. 1s, Max. 3600s)		
Load amp :	0.000		
Alarm amp :	5.000		
R. alert amp :	0.000		
L. alert amp :	0.000		
Peak amp :	0.000	2015/01/01 00:00:00	Reset
kWh :	0.00	2015/01/01 00:00:00	Reset

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 :	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

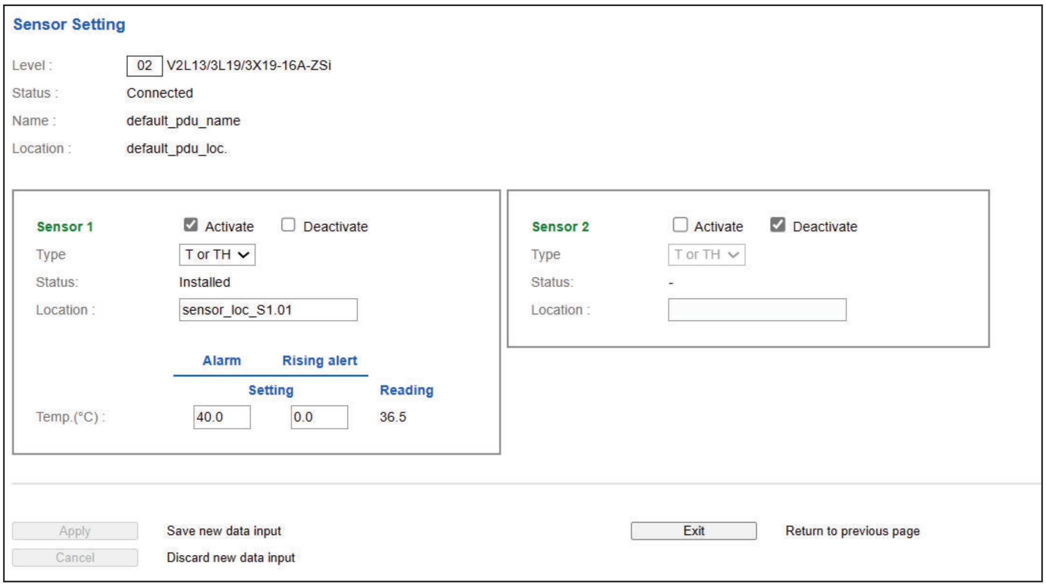
			Sensor 1					Sensor 2				
Level	Name	Setting	Location	Type	Status	Alarm	R.alert	Location	Type	Status	Alarm	R.alert
01	default_pdu_name	⚙	sensor_loc_S1.01	**Temp.** °C	27.8	40.0	0.0	-	-	-	-	-
				Humid. %	45.6	90.0	0.0					
02	default_pdu_name	⚙	sensor_loc_S1.01	**Temp.** (°C)	32.0	40.0	0.0	-	-	-	-	-

☑ 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 :	02 V2L13/3L19/3X19-16A-ZSi
Status :	Connected
Name :	default_pdu_name
Location :	default_pdu_loc.

Sensor 1 ☑ Activate ☐ Deactivate

Type	T or TH
Status:	Installed
Location :	sensor_loc_S1.01

	Alarm Setting	Rising alert Setting	Reading
Temp.(°C) :	40.0	0.0	36.5

Sensor 2 ☐ Activate ☑ Deactivate

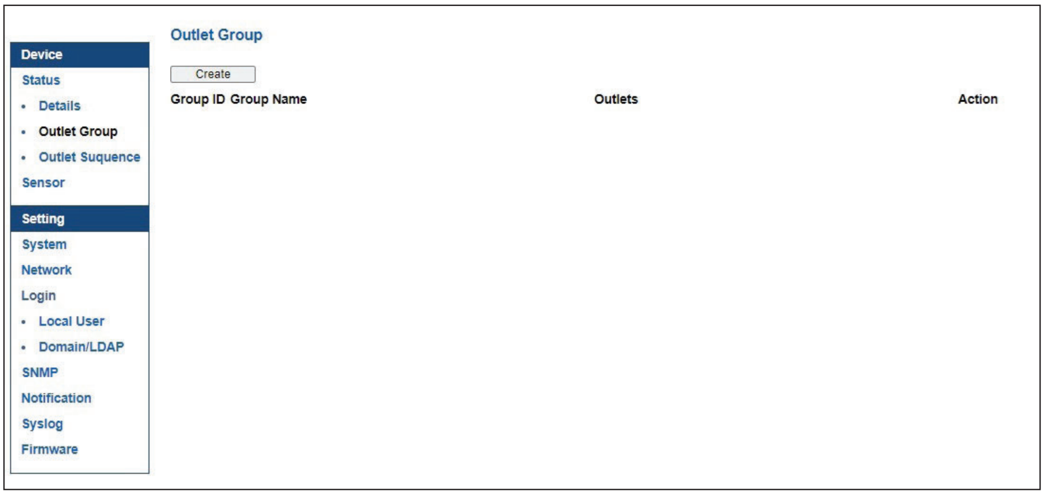
Type	T or TH
Status:	-
Location :	

< 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.

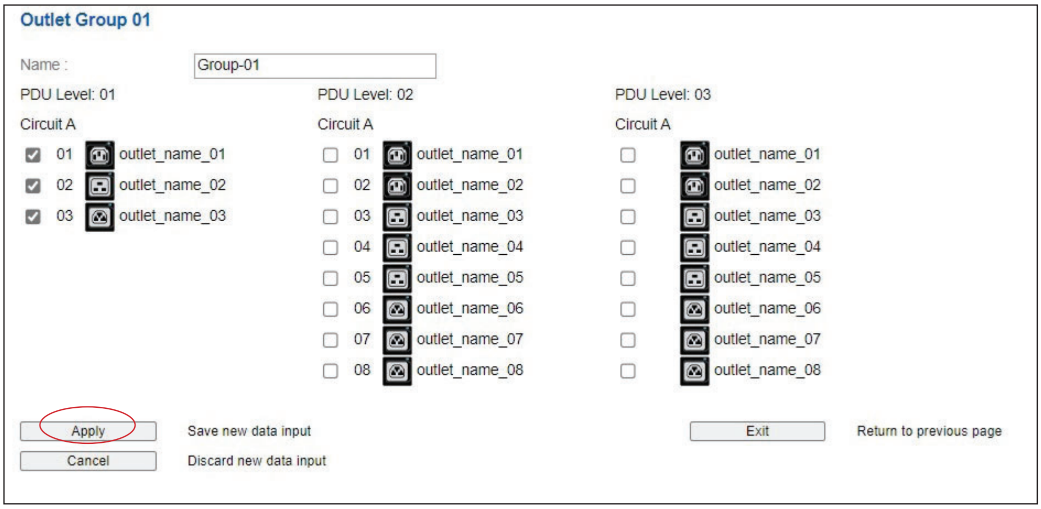
1. Select " Outlet Group " from the left navigation pane. The display below will show. Then Click " **Create** " to add a new outlet group



Outlet Group

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 : Group-01

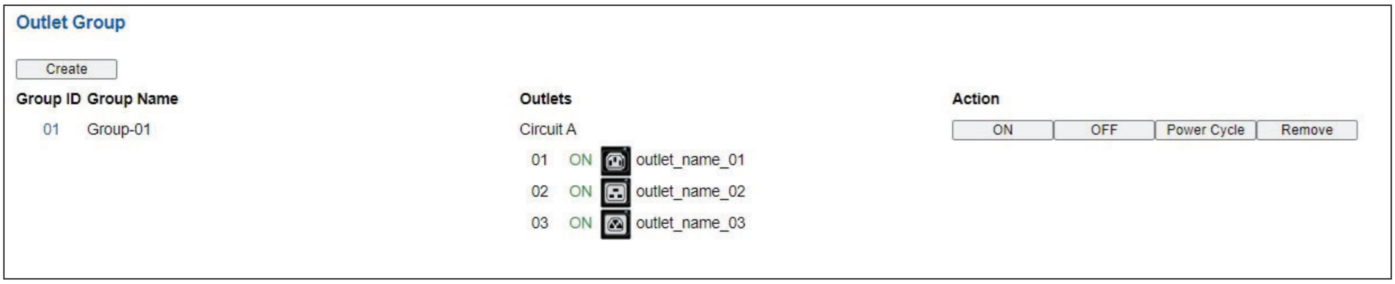
PDU Level: 01	PDU Level: 02	PDU Level: 03
Circuit A	Circuit A	Circuit A
☑ 01 outlet_name_01	□ 01 outlet_name_01	□ outlet_name_01
☑ 02 outlet_name_02	□ 02 outlet_name_02	□ outlet_name_02
☑ 03 outlet_name_03	□ 03 outlet_name_03	□ outlet_name_03
	□ 04 outlet_name_04	□ outlet_name_04
	□ 05 outlet_name_05	□ outlet_name_05
	□ 06 outlet_name_06	□ outlet_name_06
	□ 07 outlet_name_07	□ outlet_name_07
	□ 08 outlet_name_08	□ outlet_name_08

Apply Save new data input

Cancel Discard new data input

Exit Return to previous page

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

Group ID	Group Name	Outlets	Action
01	Group-01	Circuit A 01 ON outlet_name_01 02 ON outlet_name_02 03 ON outlet_name_03	ON OFF Power Cycle Remove

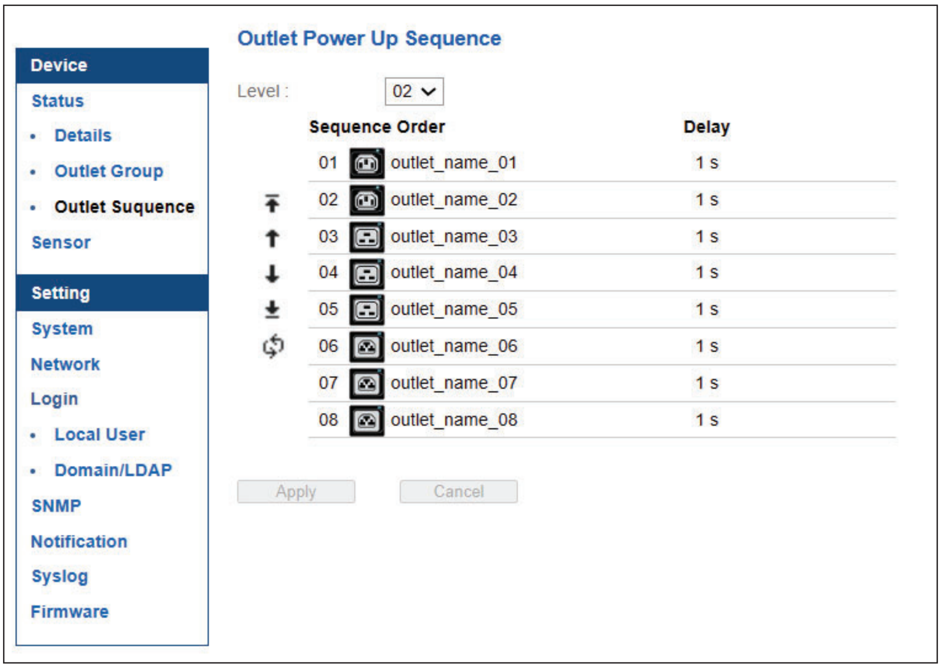
< 2.3 > Outlet Sequencing

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.

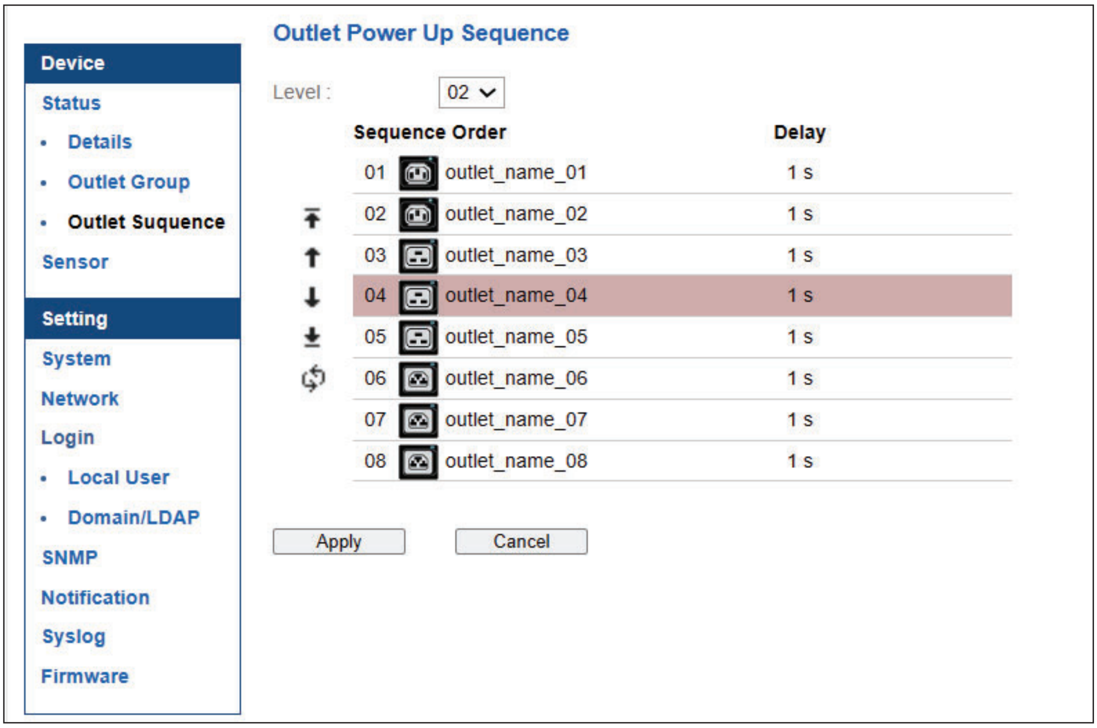


Outlet Power Up Sequence

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

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.

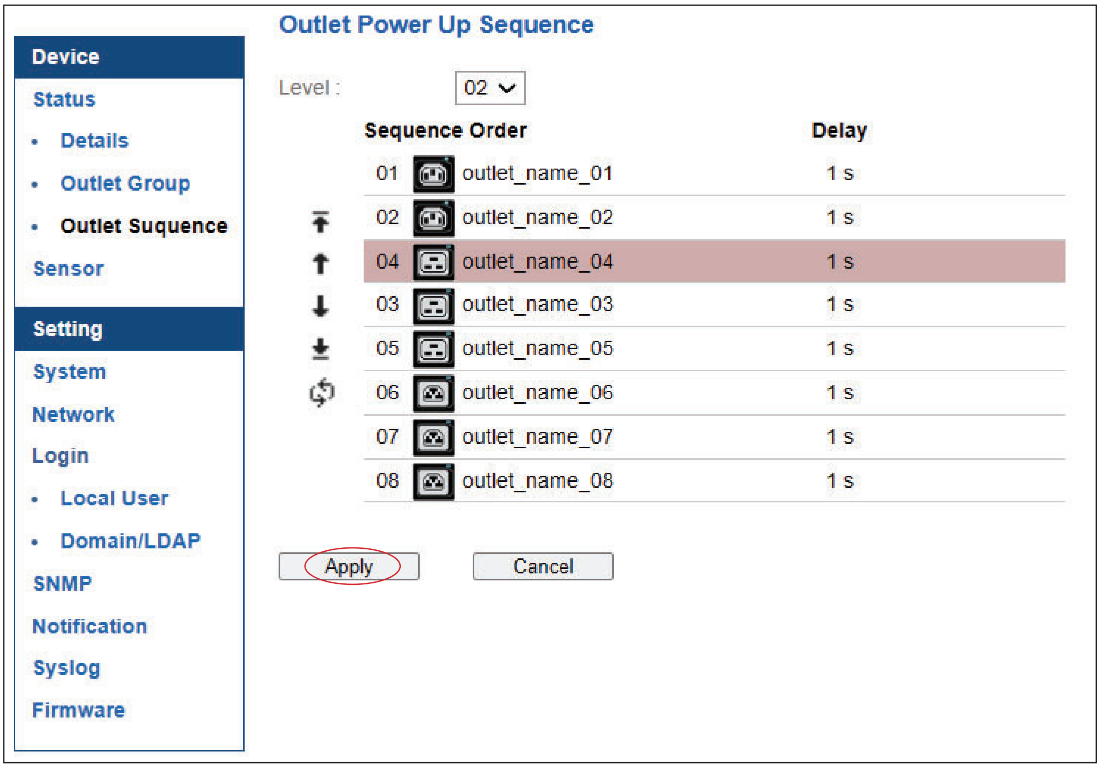


Outlet Power Up Sequence

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

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

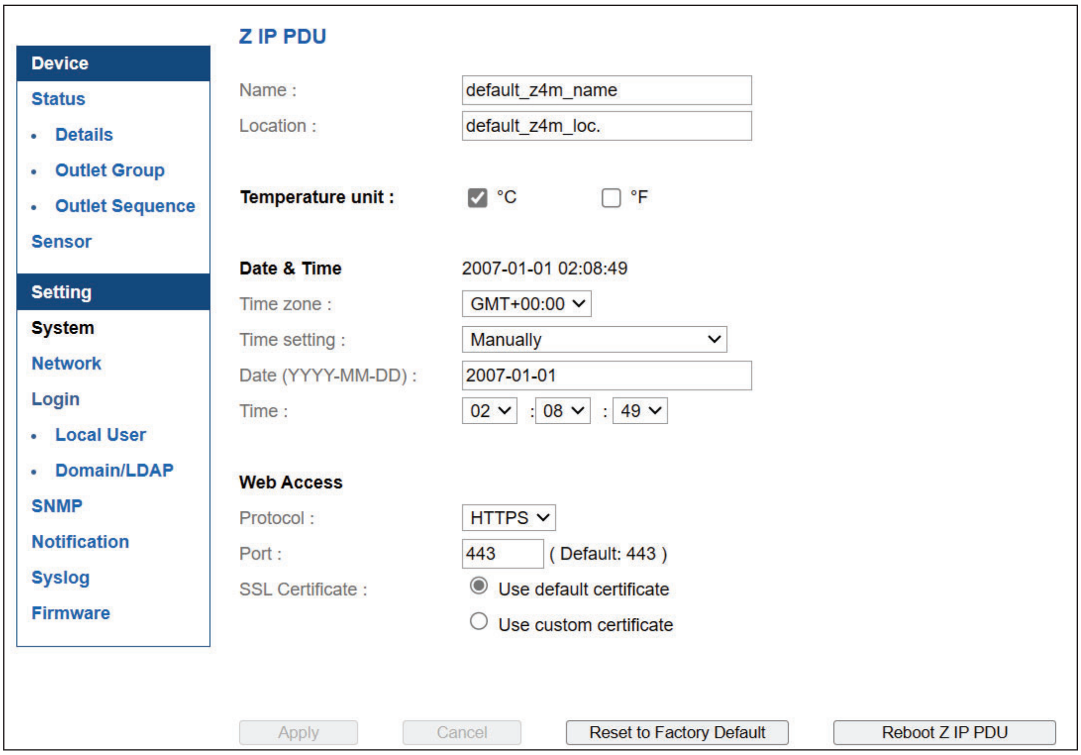
Level : 02

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

< 2.4 > System

In < **System** >,

- Change Z IP PDU name & location
- Change temperature unit displayed in WEBUI
- Set the " **Date & Time** " of the IP dongle (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



Z IP PDU

Name : default_z4m_name

Location : default_z4m_loc.

Temperature unit : ☑ °C ☐ °F

Date & Time 2007-01-01 02:08:49

Time zone : GMT+00:00

Time setting : Manually

Date (YYYY-MM-DD) : 2007-01-01

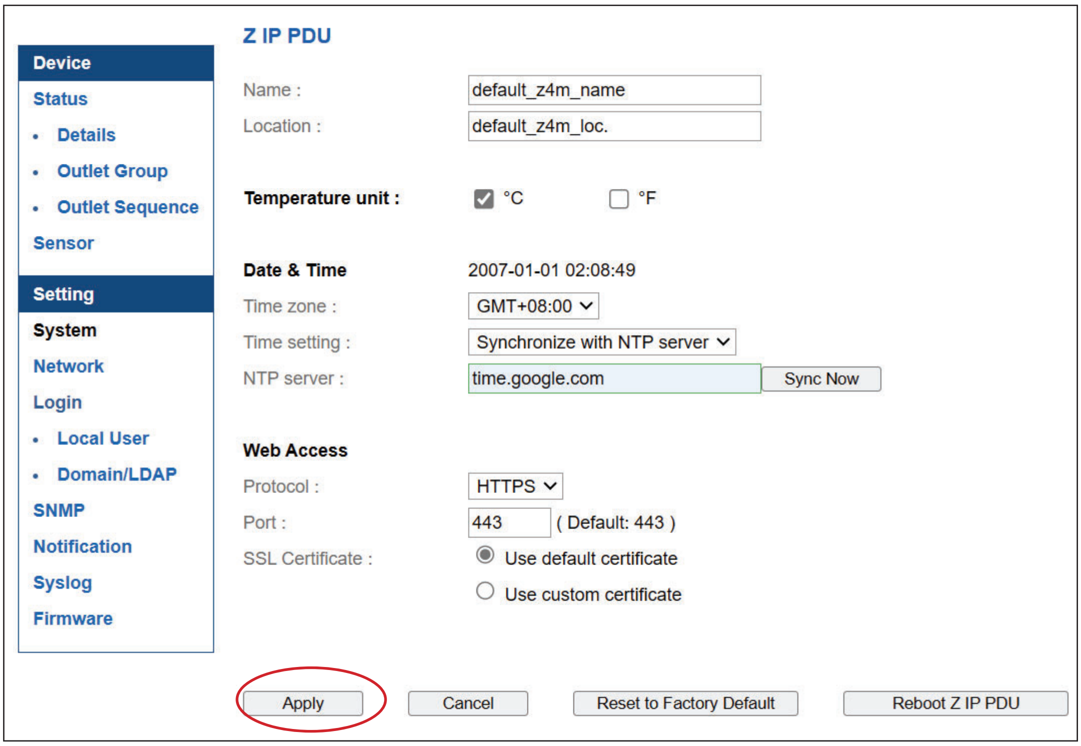
Time : 02 : 08 : 49

Web Access

Protocol : HTTPS

Port : 443 (Default: 443)

SSL Certificate : ● Use default certificate ○ Use custom certificate



Z IP PDU

Name : default_z4m_name

Location : default_z4m_loc.

Temperature unit : ☑ °C ☐ °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

Web Access

Protocol : HTTPS

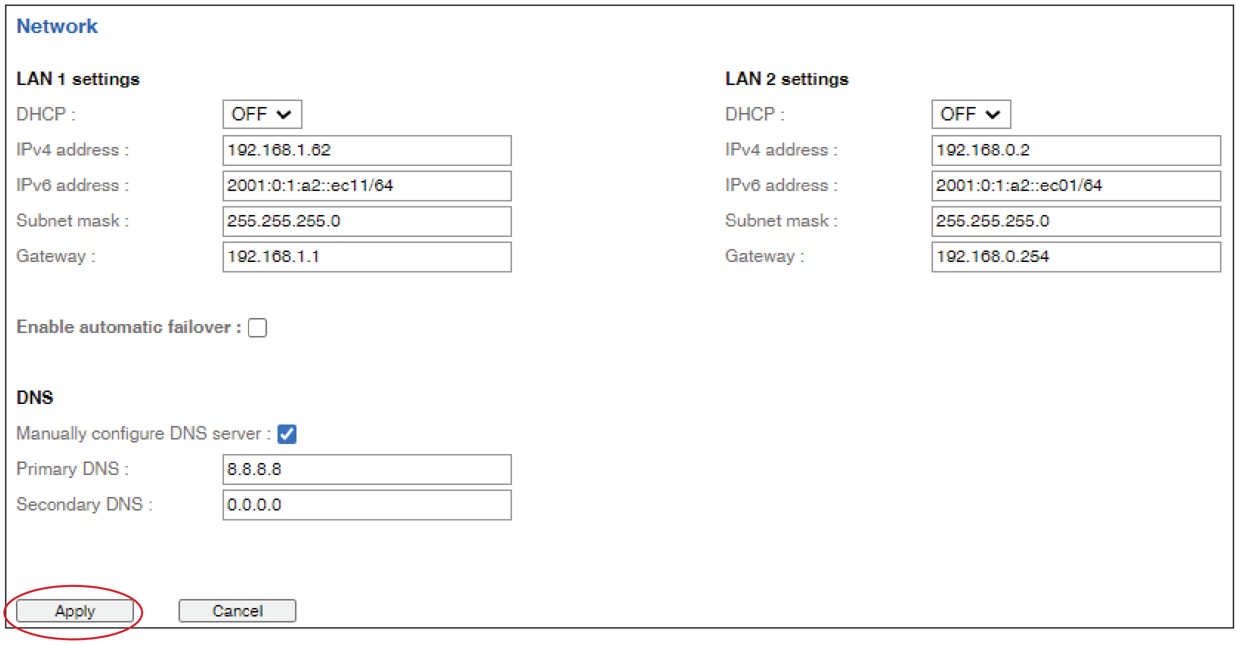
Port : 443 (Default: 443)

SSL Certificate : ● Use default certificate ○ Use custom certificate

< 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



Network

LAN 1 settings

DHCP : OFF
IPv4 address : 192.168.1.62
IPv6 address : 2001:0:1:a2::ec11/64
Subnet mask : 255.255.255.0
Gateway : 192.168.1.1

LAN 2 settings

DHCP : OFF
IPv4 address : 192.168.0.2
IPv6 address : 2001:0:1:a2::ec01/64
Subnet mask : 255.255.255.0
Gateway : 192.168.0.254

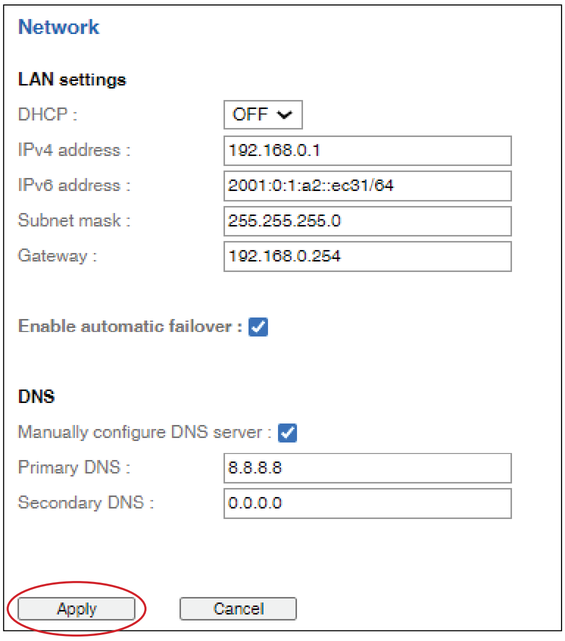
Enable automatic failover : □

DNS

Manually configure DNS server : ☑
Primary DNS : 8.8.8.8
Secondary DNS : 0.0.0.0

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



Network

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

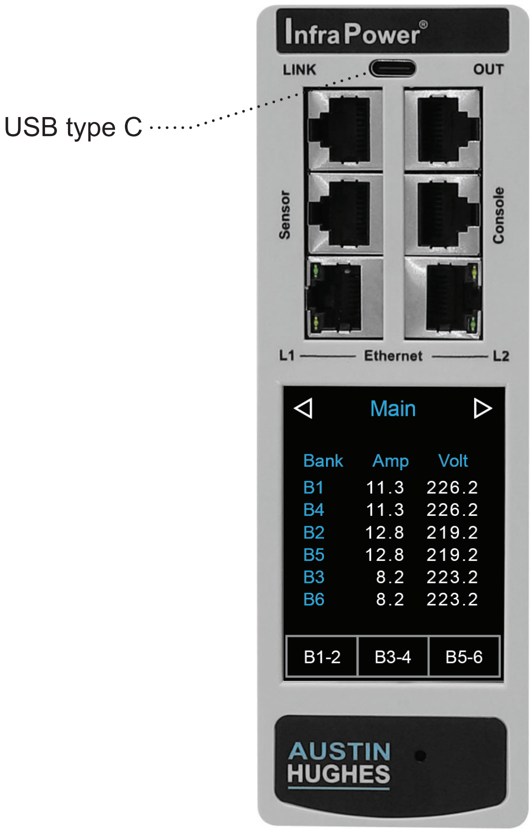
Manually configure DNS server : ☑
Primary DNS : 8.8.8.8
Secondary DNS : 0.0.0.0

< 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

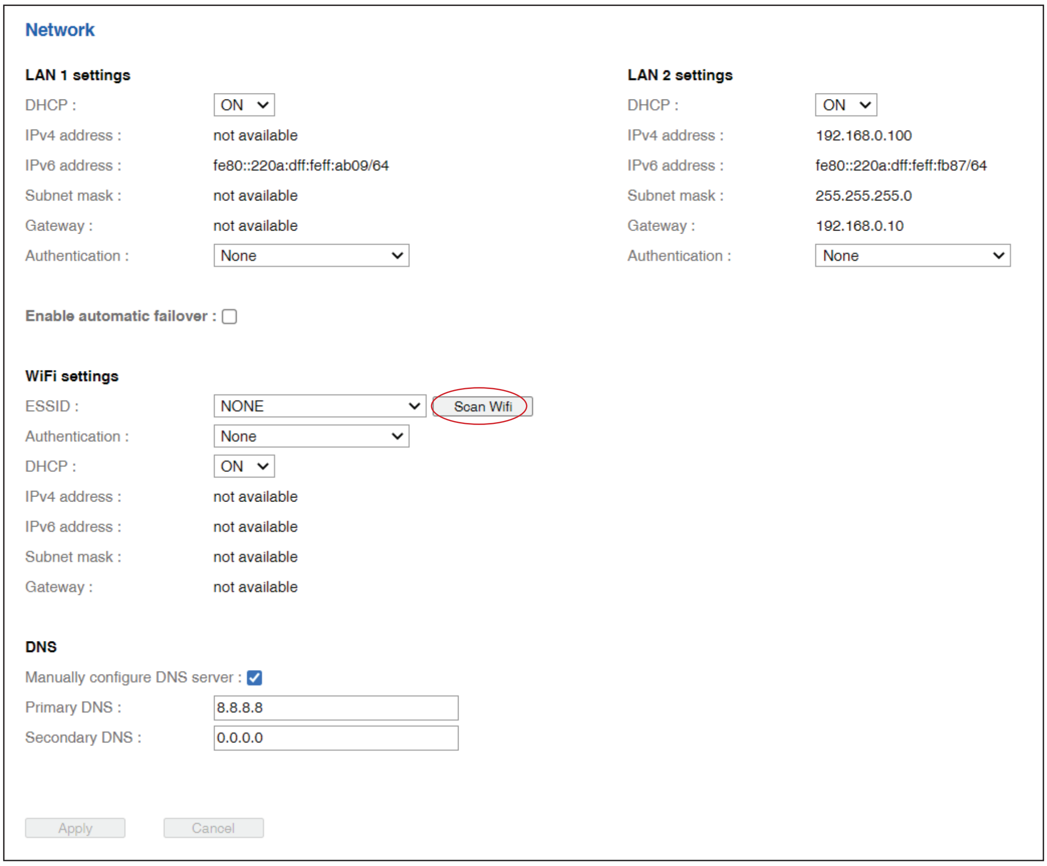
Step 1. Prepare a USB type A (Female) to USB type C (Male) adapter

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		LAN 2 settings	
DHCP :	ON	DHCP :	ON
IPv4 address :	not available	IPv4 address :	192.168.0.100
IPv6 address :	fe80::220a:dff:feff:ab09/64	IPv6 address :	fe80::220a:dff:feff:fb87/64
Subnet mask :	not available	Subnet mask :	255.255.255.0
Gateway :	not available	Gateway :	192.168.0.10
Authentication :	None	Authentication :	None

Enable automatic failover : □

WiFi settings

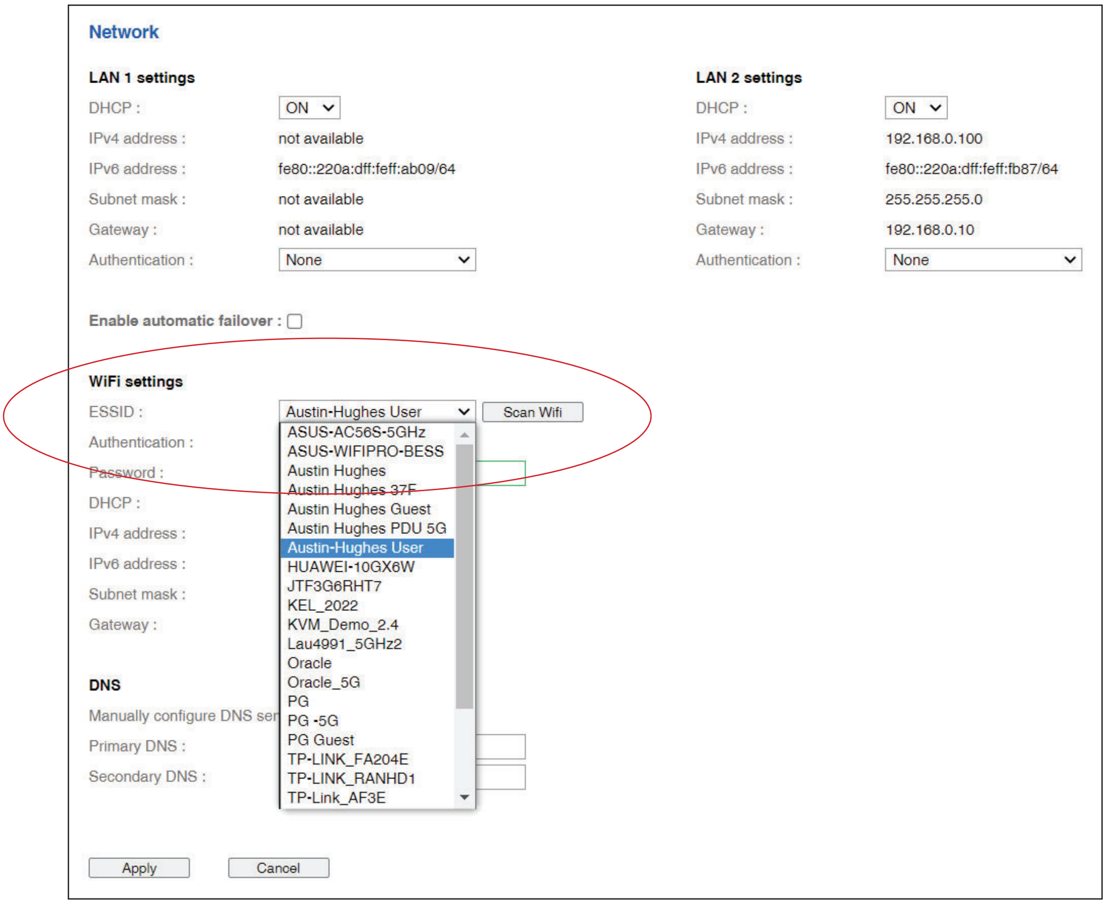
ESSID :	NONE
Authentication :	None
DHCP :	ON
IPv4 address :	not available
IPv6 address :	not available
Subnet mask :	not available
Gateway :	not available

DNS

Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

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



Network

LAN 1 settings		LAN 2 settings	
DHCP :	ON	DHCP :	ON
IPv4 address :	not available	IPv4 address :	192.168.0.100
IPv6 address :	fe80::220a:dff:feff:ab09/64	IPv6 address :	fe80::220a:dff:feff:fb87/64
Subnet mask :	not available	Subnet mask :	255.255.255.0
Gateway :	not available	Gateway :	192.168.0.10
Authentication :	None	Authentication :	None

Enable automatic failover : □

WiFi settings

ESSID : Austin-Hughes User

Authentication :

Password :

DHCP :

IPv4 address :

IPv6 address :

Subnet mask :

Gateway :

DNS

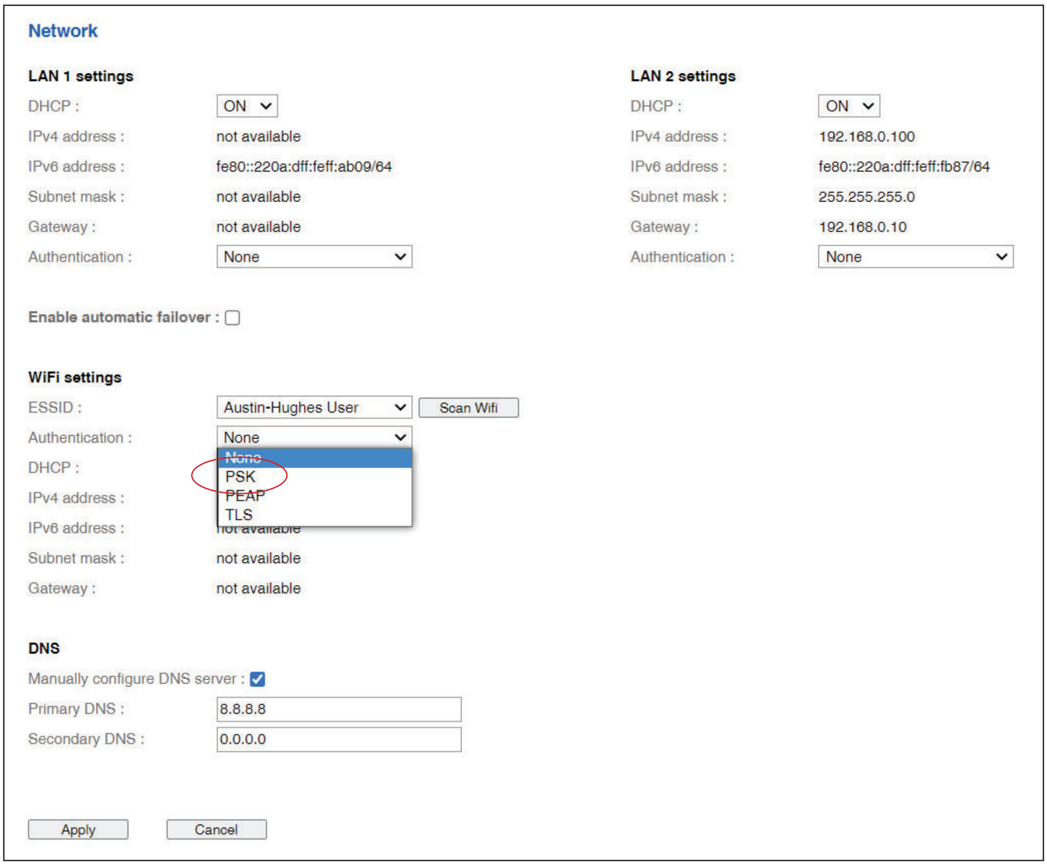
Manually configure DNS ser

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 :	ON
IPv4 address :	not available
IPv6 address :	fe80::220a:dff:feff:ab09/64
Subnet mask :	not available
Gateway :	not available
Authentication :	None

LAN 2 settings

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
Authentication :	None

Enable automatic failover : □

WiFi settings

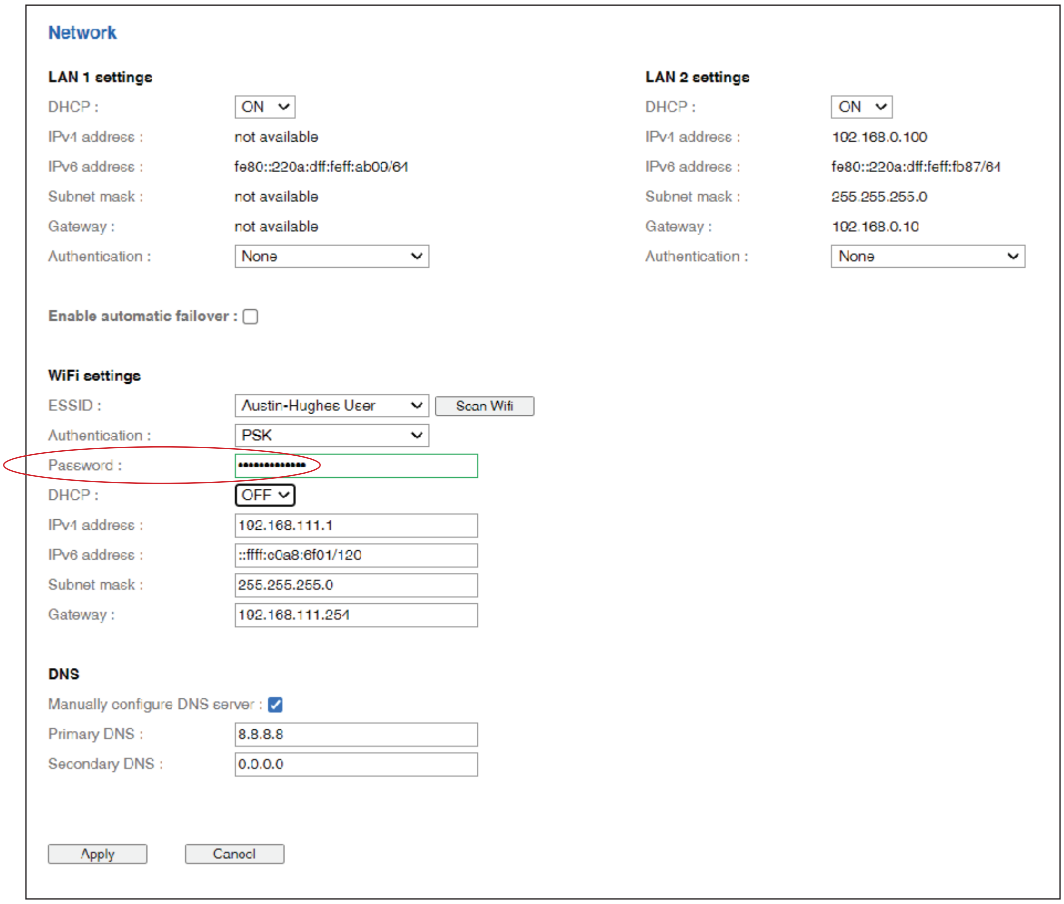
ESSID :	Austin-Hughes User
Authentication :	None
DHCP :	
IPv4 address :	
IPv6 address :	not available
Subnet mask :	not available
Gateway :	not available

DNS

Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

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



Network

LAN 1 settings

DHCP :	ON
IPv4 address :	not available
IPv6 address :	fe80::220a:dff:feff:ab09/64
Subnet mask :	not available
Gateway :	not available
Authentication :	None

LAN 2 settings

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
Authentication :	None

Enable automatic failover : □

WiFi settings

ESSID :	Austin-Hughes User
Authentication :	PSK
Password :	••••••••••••••
DHCP :	OFF
IPv4 address :	192.168.111.1
IPv6 address :	::ffff:c0a8:6f01/120
Subnet mask :	255.255.255.0
Gateway :	192.168.111.254

DNS

Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

< 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.

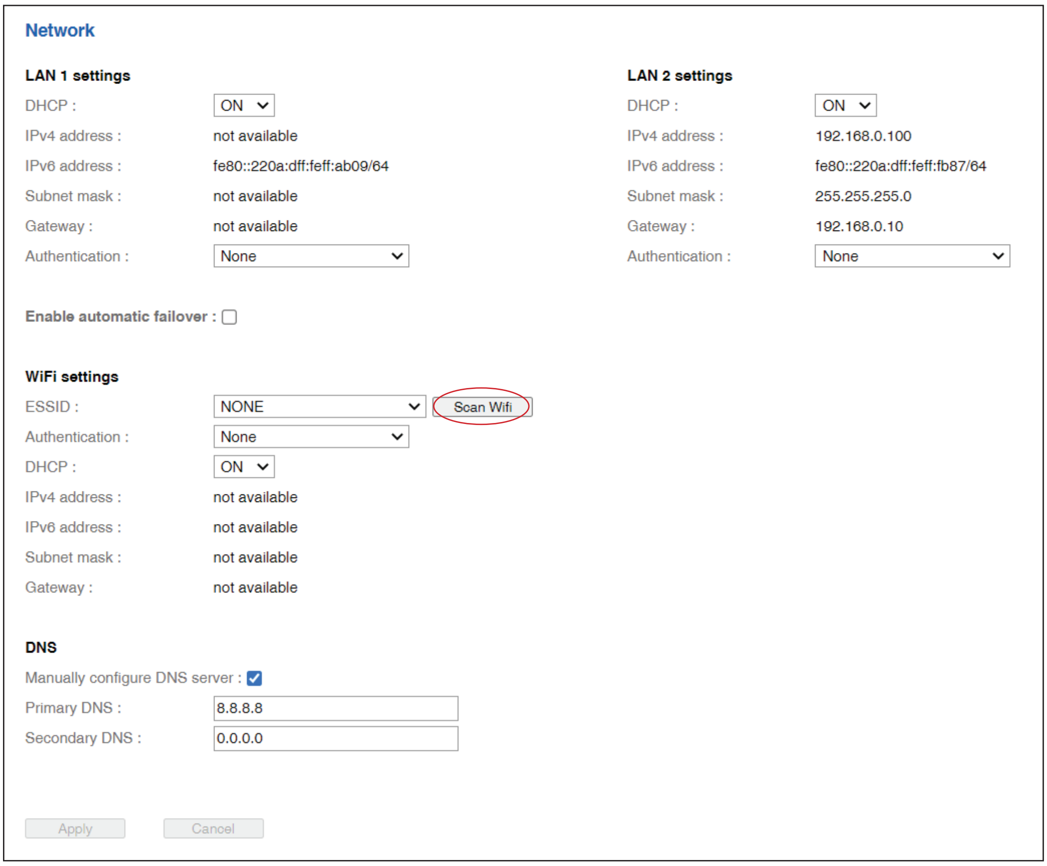
(II) Wifi DHCP setting

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.



Network

LAN 1 settings

DHCP : ON
IPv4 address : not available
IPv6 address : fe80::220a:dff:feff:ab09/64
Subnet mask : not available
Gateway : not available
Authentication : None

LAN 2 settings

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
Authentication : None

Enable automatic failover : □

WiFi settings

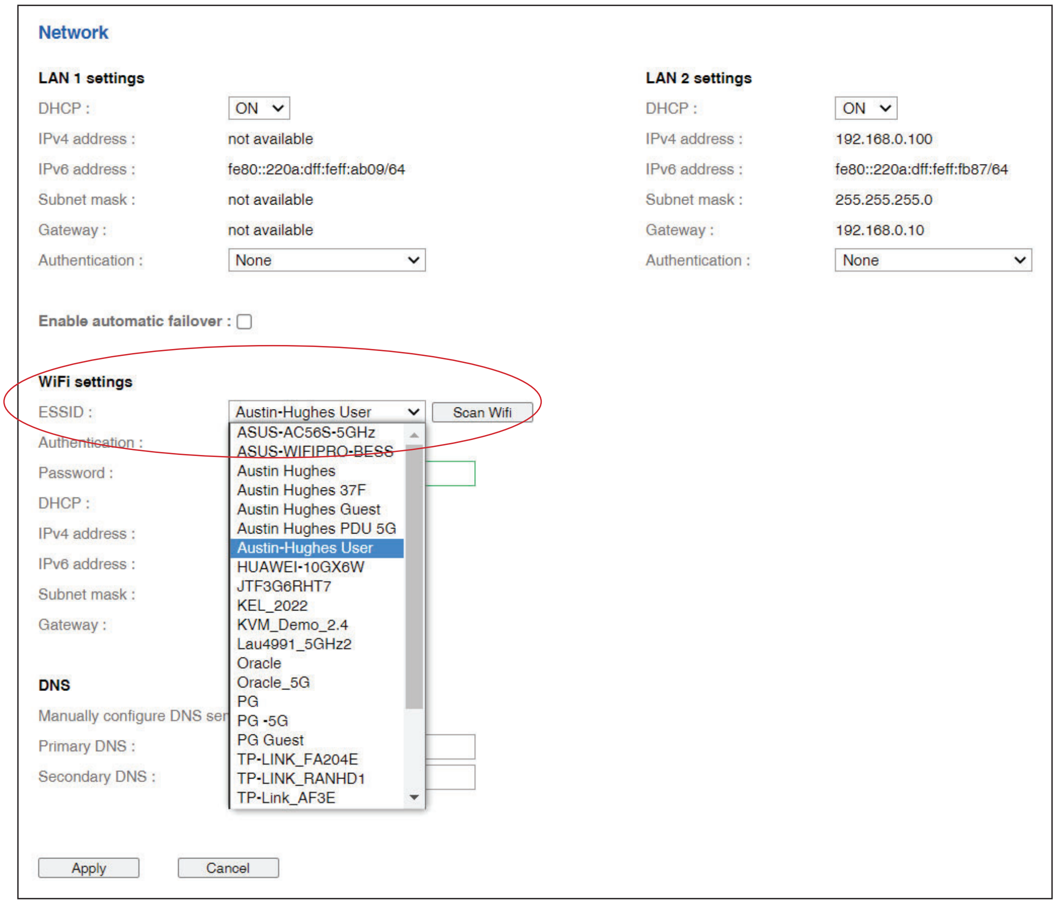
ESSID : NONE
Authentication : None
DHCP : ON
IPv4 address : not available
IPv6 address : not available
Subnet mask : not available
Gateway : not available

DNS

Manually configure DNS server : ☑
Primary DNS : 8.8.8.8
Secondary DNS : 0.0.0.0

< 2.6 > Wifi Network Configuration

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



Network

LAN 1 settings

DHCP : ON

IPv4 address : not available

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

Subnet mask : not available

Gateway : not available

Authentication : None

LAN 2 settings

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

Authentication : None

Enable automatic failover : □

WiFi settings

ESSID : Austin-Hughes User

Authentication :

Password :

DHCP :

IPv4 address :

IPv6 address :

Subnet mask :

Gateway :

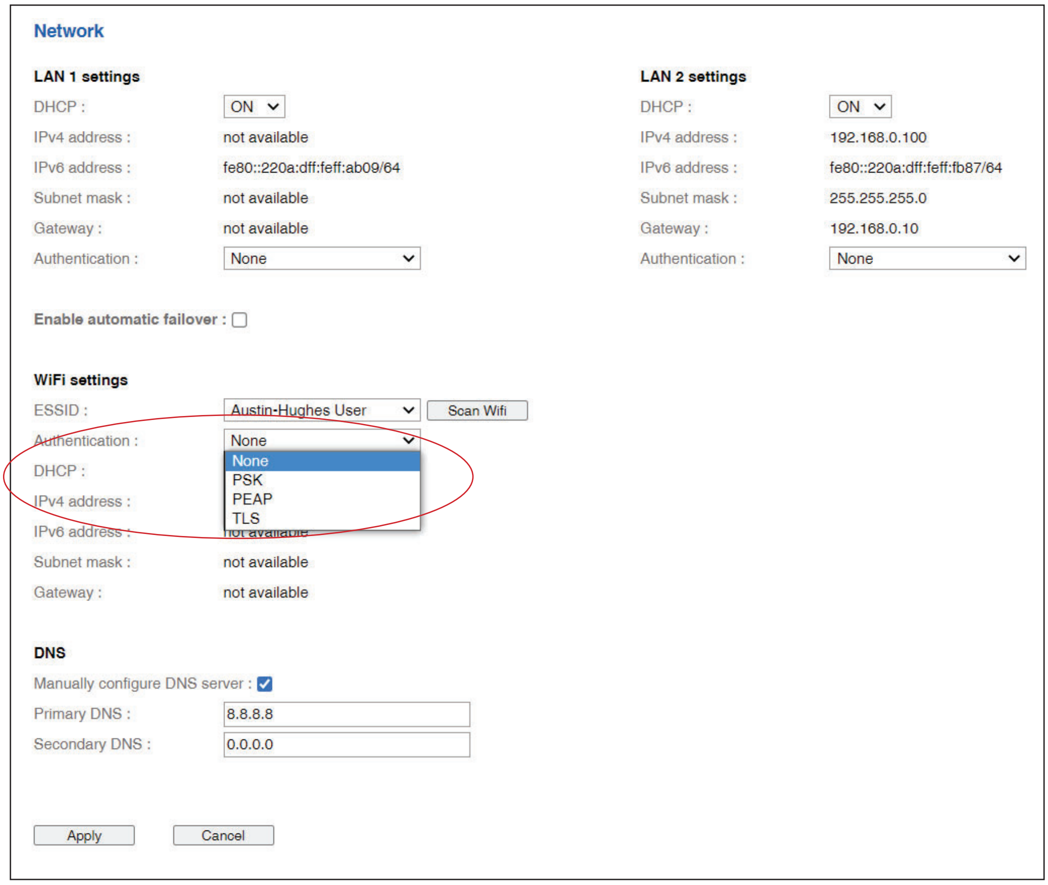
DNS

Manually configure DNS ser

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 : ON

IPv4 address : not available

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

Subnet mask : not available

Gateway : not available

Authentication : None

LAN 2 settings

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

Authentication : None

Enable automatic failover : □

WiFi settings

ESSID : Austin-Hughes User

Authentication : None

DHCP :

IPv4 address :

IPv6 address : not available

Subnet mask : not available

Gateway : not available

DNS

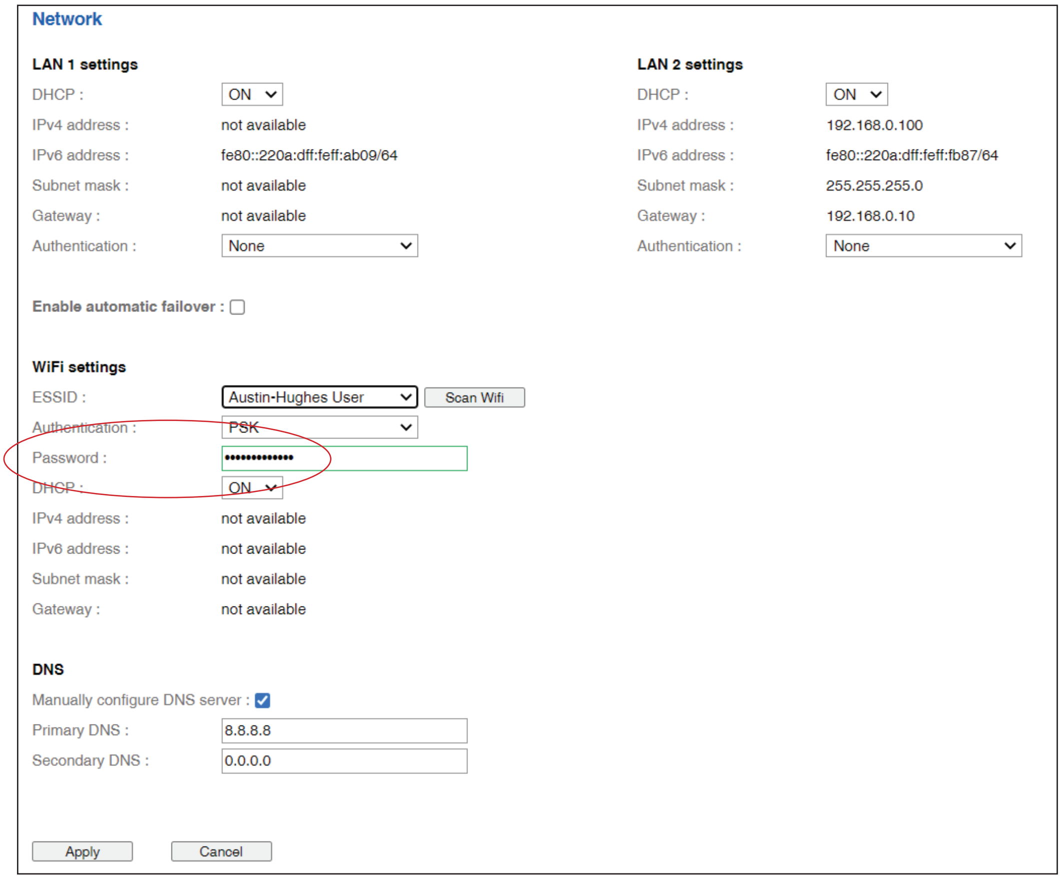
Manually configure DNS server : ☑

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

< 2.6 > Wifi Network Configuration

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



Network

LAN 1 settings		LAN 2 settings	
DHCP :	ON	DHCP :	ON
IPv4 address :	not available	IPv4 address :	192.168.0.100
IPv6 address :	fe80::220a:dff:feff:ab09/64	IPv6 address :	fe80::220a:dff:feff:fb87/64
Subnet mask :	not available	Subnet mask :	255.255.255.0
Gateway :	not available	Gateway :	192.168.0.10
Authentication :	None	Authentication :	None

Enable automatic failover : □

WiFi settings

ESSID :	Austin-Hughes User
Authentication :	PSK
Password :	•••••••••••••
DHCP :	ON
IPv4 address :	not available
IPv6 address :	not available
Subnet mask :	not available
Gateway :	not available

DNS

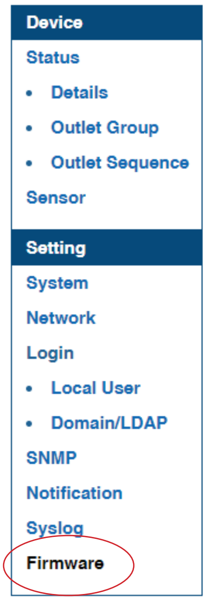
Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

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

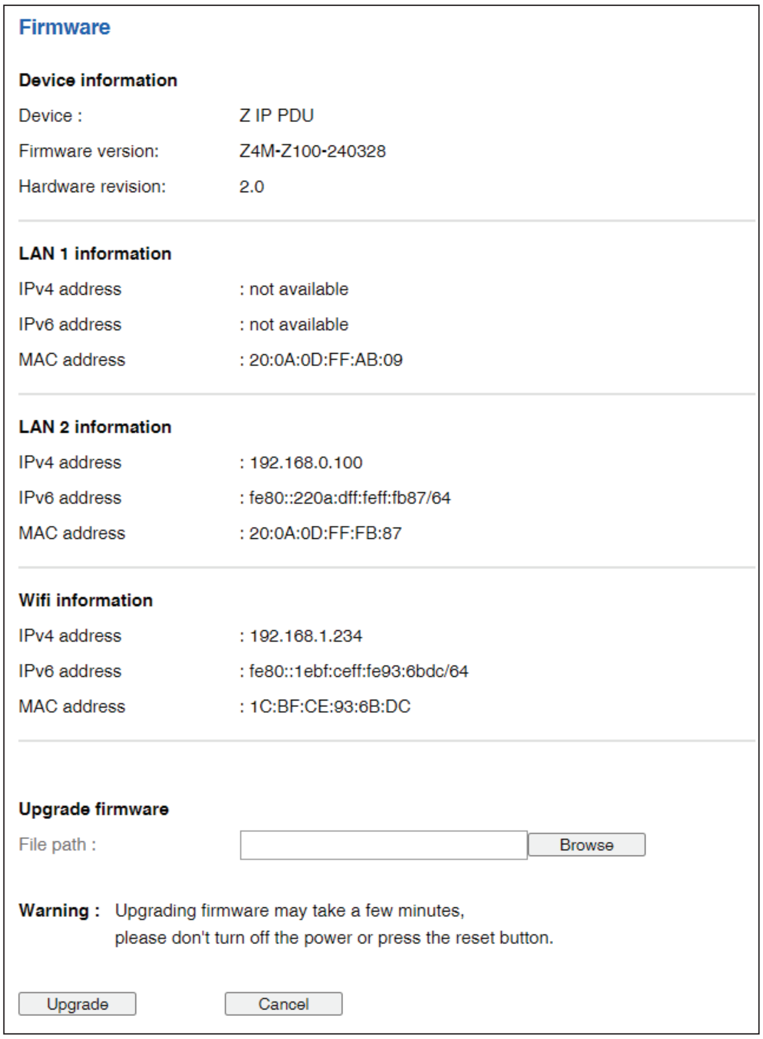
Step 9. Click “ **Apply** ” to finish the above settings.

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 :

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

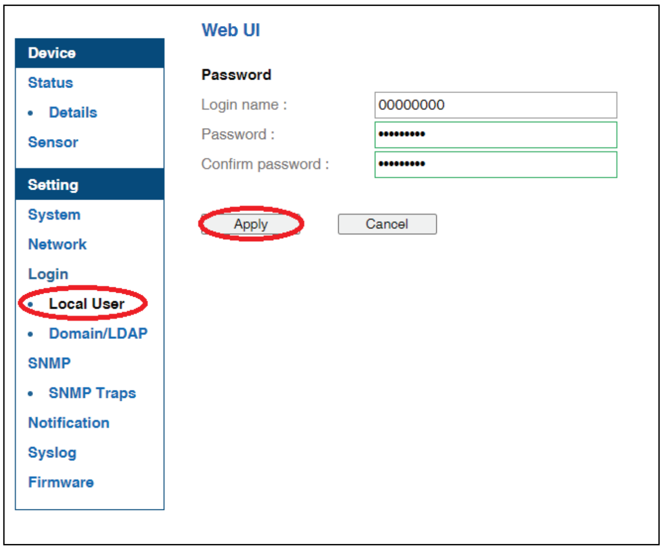
Step 12. Assign an IP address of the Wifi kit from your DHCP server.

< 2.7 > Login

In < **Login** >, you can login the PPS-04-S by “ **Local User** ” or “ **Domain/LDAP** ” login.
(Default login : “ **Local User** ”)

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



Password

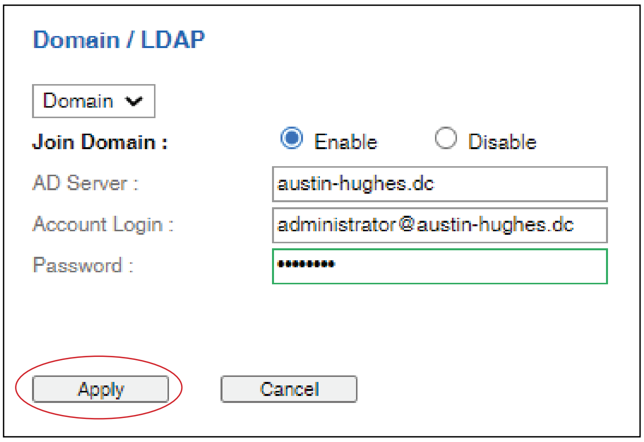
Login name : 00000000

Password : •••••••••

Confirm password : •••••••••

Domain/LDAP :

- Default Join Domain is **“ Disable “**
- Enable “ **Join Domain** ” only when you want to login the PPS-04-S by AD server
- Enter “ **AD Server** ”,“ **Account Login** ” & “ **Password** ”
- Click “ **Apply** ” and “ **OK** “ on the pop up window to make changes effective
- You can now go to “ **Domain Users** ” to assign access right to the **“ Domain Users ”** or the **“ Domain Group ”**



Domain

Join Domain : ● Enable ○ Disable

AD Server : austin-hughes.dc

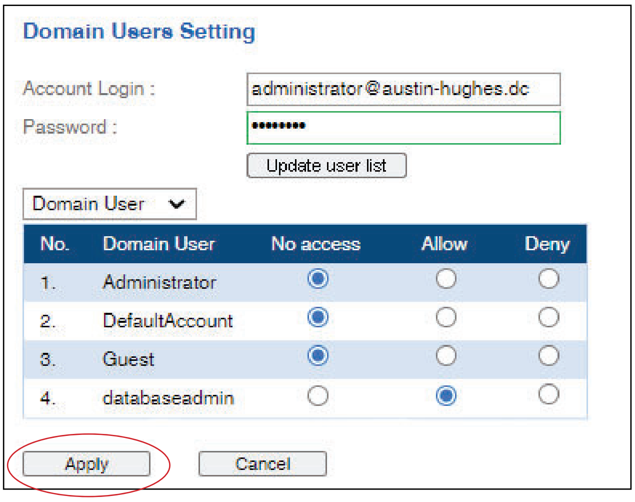
Account Login : administrator@austin-hughes.dc

Password : ••••••••

< 2.7 > Login

In “ **Domain Users Setting** ”,

- Click **“ Update domain data ”** to update domain user list.
- Assign access right (No access / Allow / Deny) to **“ Domain Users ”** and click **“ Apply ” .**
- The Domain User assigned **“ Allow “** access right can login the PPS-04-S.



Domain Users Setting

Account Login : administrator@austin-hughes.dc

Password : ••••••••

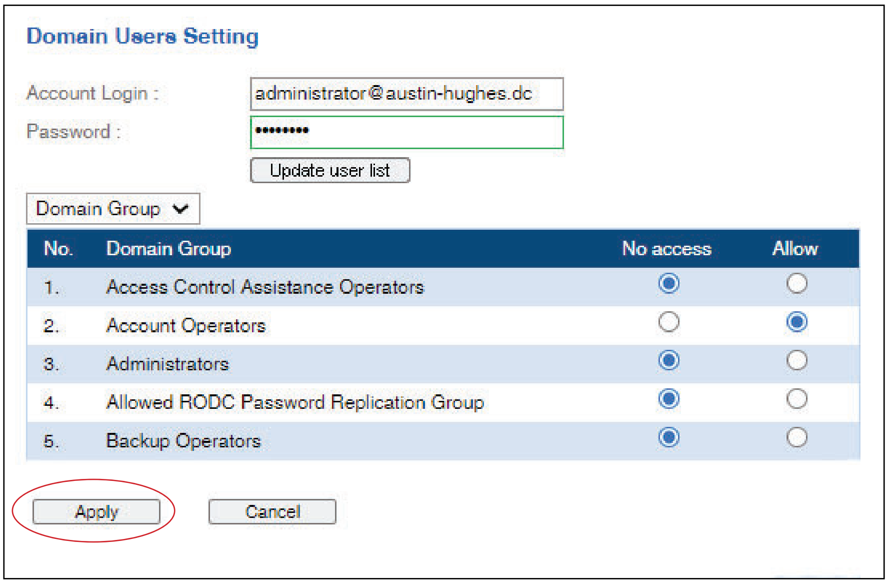
Update user list

Domain User

No.	Domain User	No access	Allow	Deny
1.	Administrator	●	○	○
2.	DefaultAccount	●	○	○
3.	Guest	●	○	○
4.	databaseadmin	○	●	○

In “ **Domain Users Setting** ”,

- Click **“ Update domain data ”** to update domain group list.
- Assign access right (No access / Allow) to **“ Domain Group ”** and click **“ Apply ” .**
- The Users of the Domain Group assigned **“ Allow “** access right can login the PPS-04-S.



Domain Users Setting

Account Login : administrator@austin-hughes.dc

Password : ••••••••

Update user list

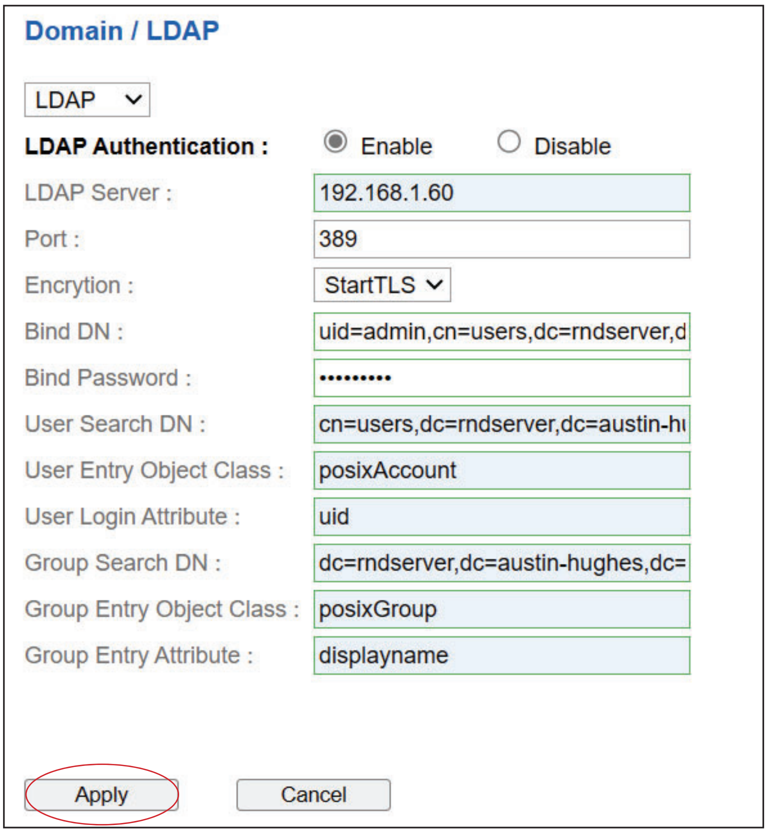
Domain Group

No.	Domain Group	No access	Allow
1.	Access Control Assistance Operators	●	○
2.	Account Operators	○	●
3.	Administrators	●	○
4.	Allowed RODC Password Replication Group	●	○
5.	Backup Operators	●	○

< 2.7 > Login

Domain/LDAP:

- Default LDAP Authentication is “ Disable “
- Enable “ **LDAP Authentication** ” only when you want to login PPS-04-S by LDAP
- Enter “ **LDAP Server** ”
- Enter “ **Port** “. Default is “ **389** ”
- Select “ **Encryption** ” (None / SSL / StartTLS). Default : None
- Enter “ **Bind DN** ”
- Enter “ **Bind Password** ”
- Enter “ **User Search DN** ”
- Enter “ **User Entry Object Class** ”
- Enter “ **User Login Attribute** ”
- Enter ” **Group Search DN** ”
- Enter “ **Group Entry Object Class** ”
- Enter “ **Group Entry Attribute** ”
- Click “ **Apply** ” and “ **OK** “ on the pop up window to make the changes effective
- You can now go to “ **Remote User** “ to assign right to the LDAP user or LDAP Group



Domain / LDAP

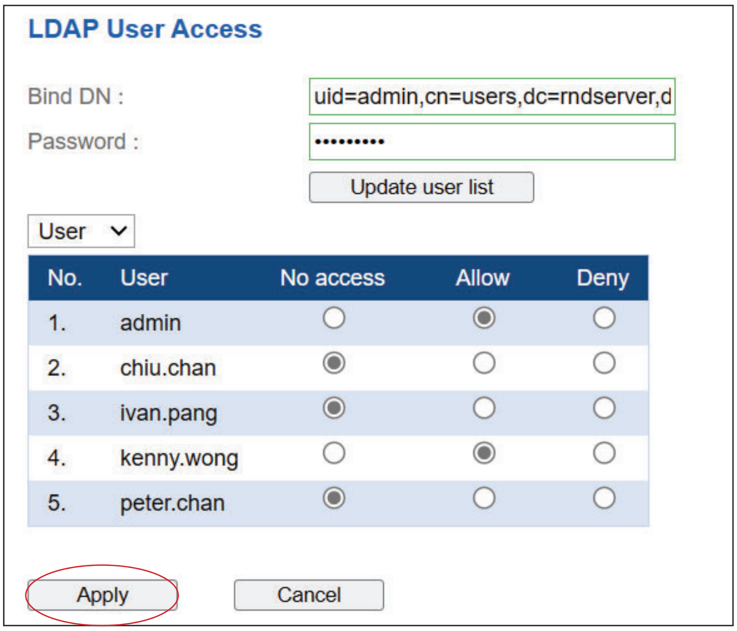
LDAP

LDAP Authentication :	● Enable ○ Disable
LDAP Server :	192.168.1.60
Port :	389
Encrytion :	StartTLS
Bind DN :	uid=admin,cn=users,dc=rndserver,d
Bind Password :	•••••••••
User Search DN :	cn=users,dc=rndserver,dc=austin-hı
User Entry Object Class :	posixAccount
User Login Attribute :	uid
Group Search DN :	dc=rndserver,dc=austin-hughes,dc=
Group Entry Object Class :	posixGroup
Group Entry Attribute :	displayname

< 2.7> Login

In “ **LDAP User Access** ”,

- Enter the Password of “ **admin** ” to update the user list.
- Assign access right (No access / Allow / Deny) to “ **User** ” and Click “ **Apply** ”
- The user assigned “ **Allow** ” access right can login the PPS-04-S



LDAP User Access

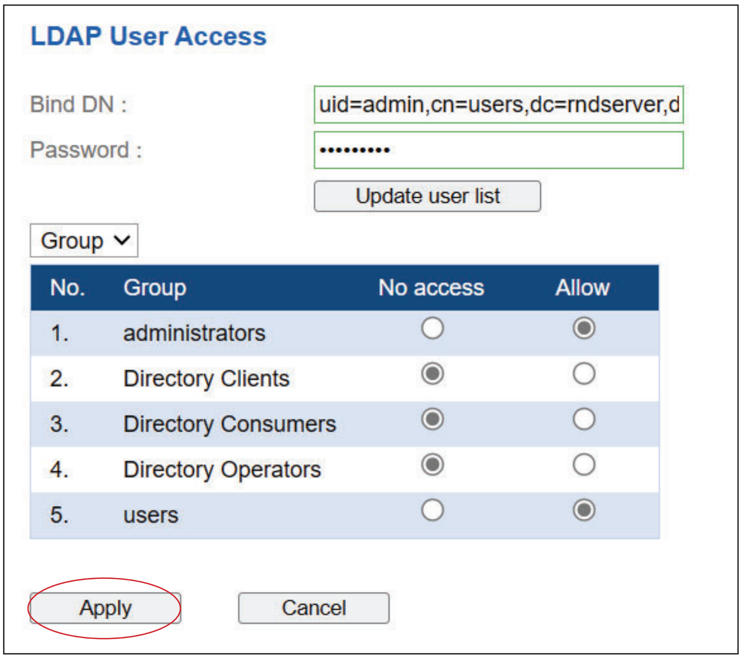
Bind DN : uid=admin,cn=users,dc=rndserver,d

Password : •••••••••

No.	User	No access	Allow	Deny
1.	admin	○	●	○
2.	chiu.chan	●	○	○
3.	ivan.pang	●	○	○
4.	kenny.wong	○	●	○
5.	peter.chan	●	○	○

In “ **LDAP User Access** ”,

- Select “ **Group** “
- Assign access right (No access / Allow) to “ **Group** ” and Click “ **Apply** ”
- The group assigned “ **Allow** ” access right can login the PPS-04-S



LDAP User Access

Bind DN : uid=admin,cn=users,dc=rndserver,d

Password : •••••••••

No.	Group	No access	Allow
1.	administrators	○	●
2.	Directory Clients	●	○
3.	Directory Consumers	●	○
4.	Directory Operators	●	○
5.	users	○	●

< 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

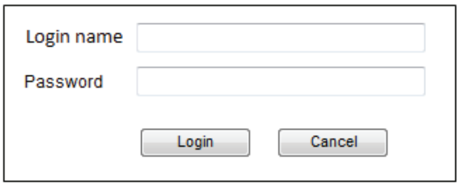
i. The following steps summarize how to enable SNMP v1 / v2 support for PPS-04-S.

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

Step 2. Open the MS Edge

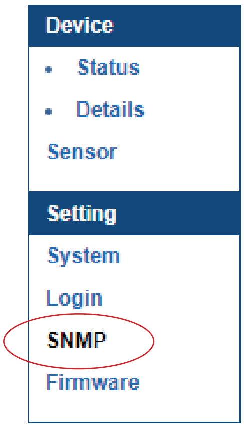
Step 3. Enter the configured IP address into the address bar

Step 4. Enter " **Login name** " & " **Password** ".

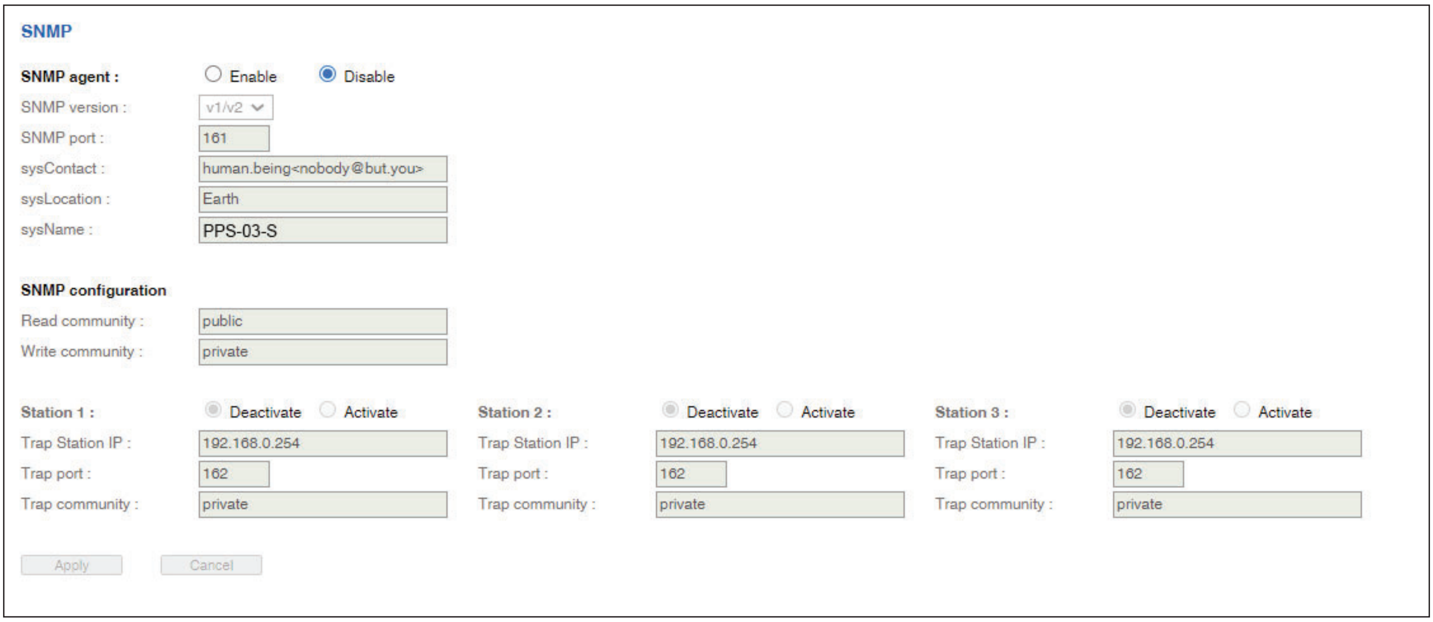


< 2.8 > SNMP Setup

Step 5. Select the SNMP from the left navigation pane



Step 6. The SNMP Settings window appears as below:



SNMP

SNMP agent : ○ Enable ● Disable

SNMP version : v1/v2

SNMP port : 161

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

sysLocation : Earth

sysName : PPS-03-S

SNMP configuration

Read community : public

Write community : private

Station 1 :	● Deactivate ○ Activate	Station 2 :	● Deactivate ○ Activate	Station 3 :	● Deactivate ○ Activate
Trap Station IP :	192.168.0.254	Trap Station IP :	192.168.0.254	Trap Station IP :	192.168.0.254
Trap port :	162	Trap port :	162	Trap port :	162
Trap community :	private	Trap community :	private	Trap community :	private

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

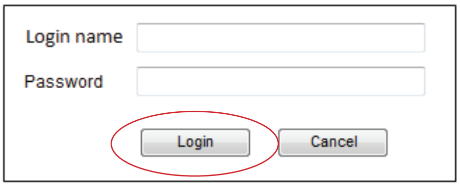
ii. The following steps summarize how to enable SNMP v3 support for PPS-04-S.

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

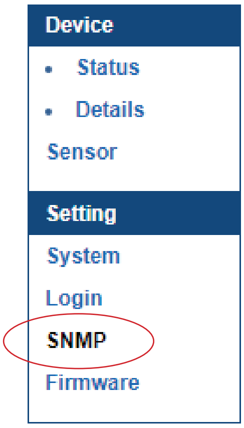
Step 2. Open MS Edge

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

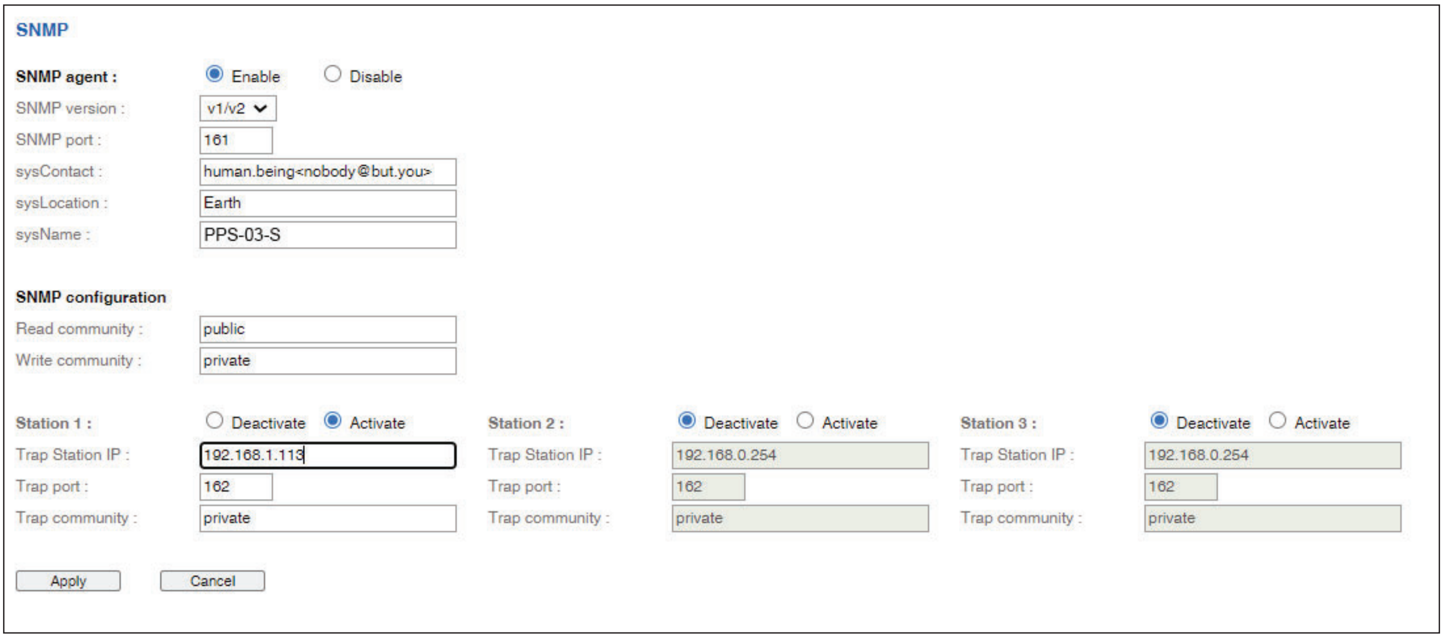
Step 4. Enter “ **Login name** “ & “ **Password** “.



Step 5. Select SNMP from the left navigation pane



Step 6. The SNMP Settings window appears as below:



SNMP

SNMP agent : ● Enable ○ Disable
SNMP version : v1/v2
SNMP port : 161
sysContact : human.being<nobody@but.you>
sysLocation : Earth
sysName : PPS-03-S

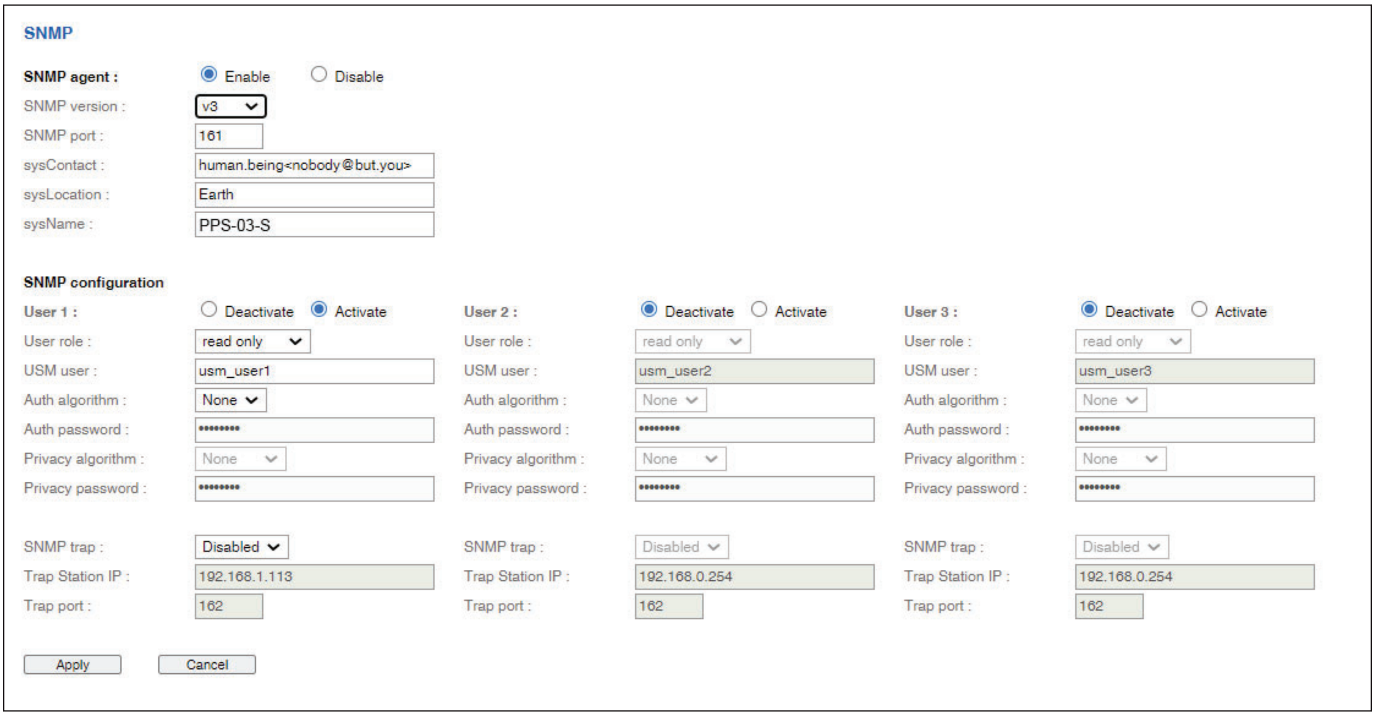
SNMP configuration
Read community : public
Write community : private

Station 1 :	○ Deactivate ● Activate	Station 2 :	● Deactivate ○ Activate	Station 3 :	● Deactivate ○ Activate
Trap Station IP :	192.168.1.113	Trap Station IP :	192.168.0.254	Trap Station IP :	192.168.0.254
Trap port :	162	Trap port :	162	Trap port :	162
Trap community :	private	Trap community :	private	Trap community :	private

< 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 2 :	● Deactivate ○ Activate	User 3 :	● Deactivate ○ Activate
User role :	read only	User role :	read only	User role :	read only
USM user :	usm_user1	USM user :	usm_user2	USM user :	usm_user3
Auth algorithm :	None	Auth algorithm :	None	Auth algorithm :	None
Auth password :	••••••••	Auth password :	••••••••	Auth password :	••••••••
Privacy algorithm :	None	Privacy algorithm :	None	Privacy algorithm :	None
Privacy password :	••••••••	Privacy password :	••••••••	Privacy password :	••••••••
SNMP trap :	Disabled	SNMP trap :	Disabled	SNMP trap :	Disabled
Trap Station IP :	192.168.1.113	Trap Station IP :	192.168.0.254	Trap Station IP :	192.168.0.254
Trap port :	162	Trap port :	162	Trap port :	162

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** “

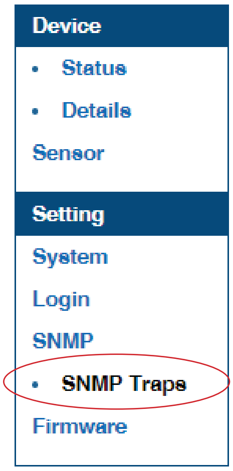
Step 22. Repeat step 12 to 20 for User 2 & 3

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

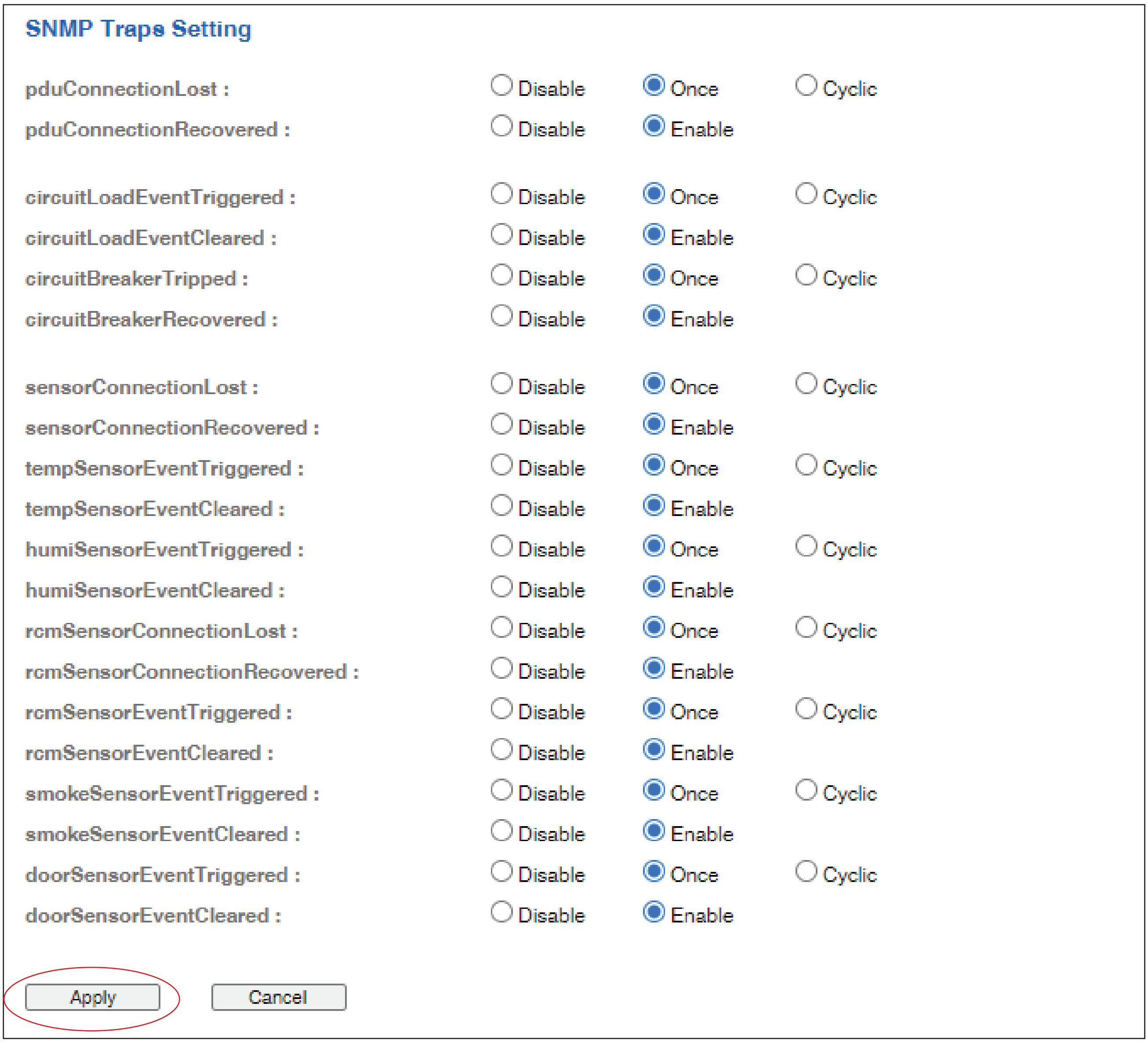
< 2.8 > SNMP Setup

(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 :	○ Disable	● Once	○ Cyclic
pduConnectionRecovered :	○ Disable	● Enable	
circuitLoadEventTriggered :	○ Disable	● Once	○ Cyclic
circuitLoadEventCleared :	○ Disable	● Enable	
circuitBreakerTripped :	○ Disable	● Once	○ Cyclic
circuitBreakerRecovered :	○ Disable	● Enable	
sensorConnectionLost :	○ Disable	● Once	○ Cyclic
sensorConnectionRecovered :	○ Disable	● Enable	
tempSensorEventTriggered :	○ Disable	● Once	○ Cyclic
tempSensorEventCleared :	○ Disable	● Enable	
humiSensorEventTriggered :	○ Disable	● Once	○ Cyclic
humiSensorEventCleared :	○ Disable	● Enable	
rcmSensorConnectionLost :	○ Disable	● Once	○ Cyclic
rcmSensorConnectionRecovered :	○ Disable	● Enable	
rcmSensorEventTriggered :	○ Disable	● Once	○ Cyclic
rcmSensorEventCleared :	○ Disable	● Enable	
smokeSensorEventTriggered :	○ Disable	● Once	○ Cyclic
smokeSensorEventCleared :	○ Disable	● Enable	
doorSensorEventTriggered :	○ Disable	● Once	○ Cyclic
doorSensorEventCleared :	○ Disable	● Enable	

< 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 SNMP authentication is enabled

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

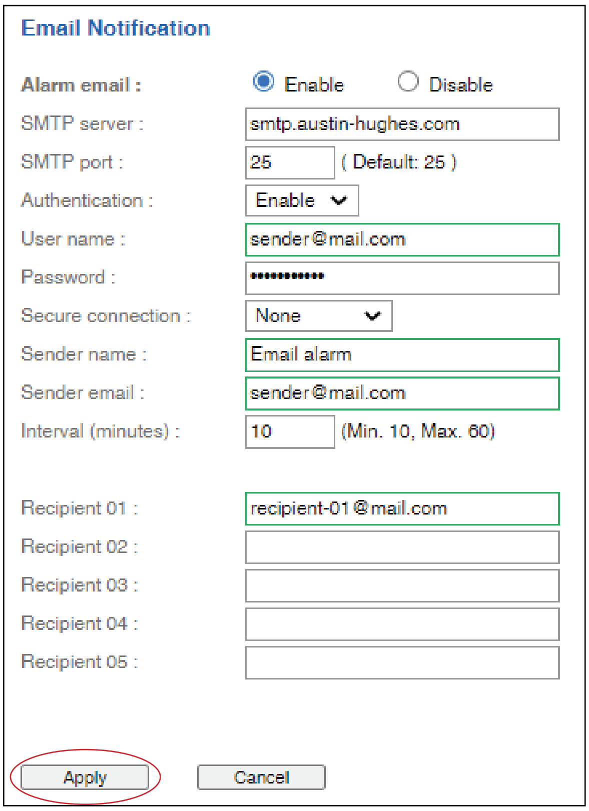
Step 6. Enter the “ **Sender Name** ” and “ **Sender Email** ”

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

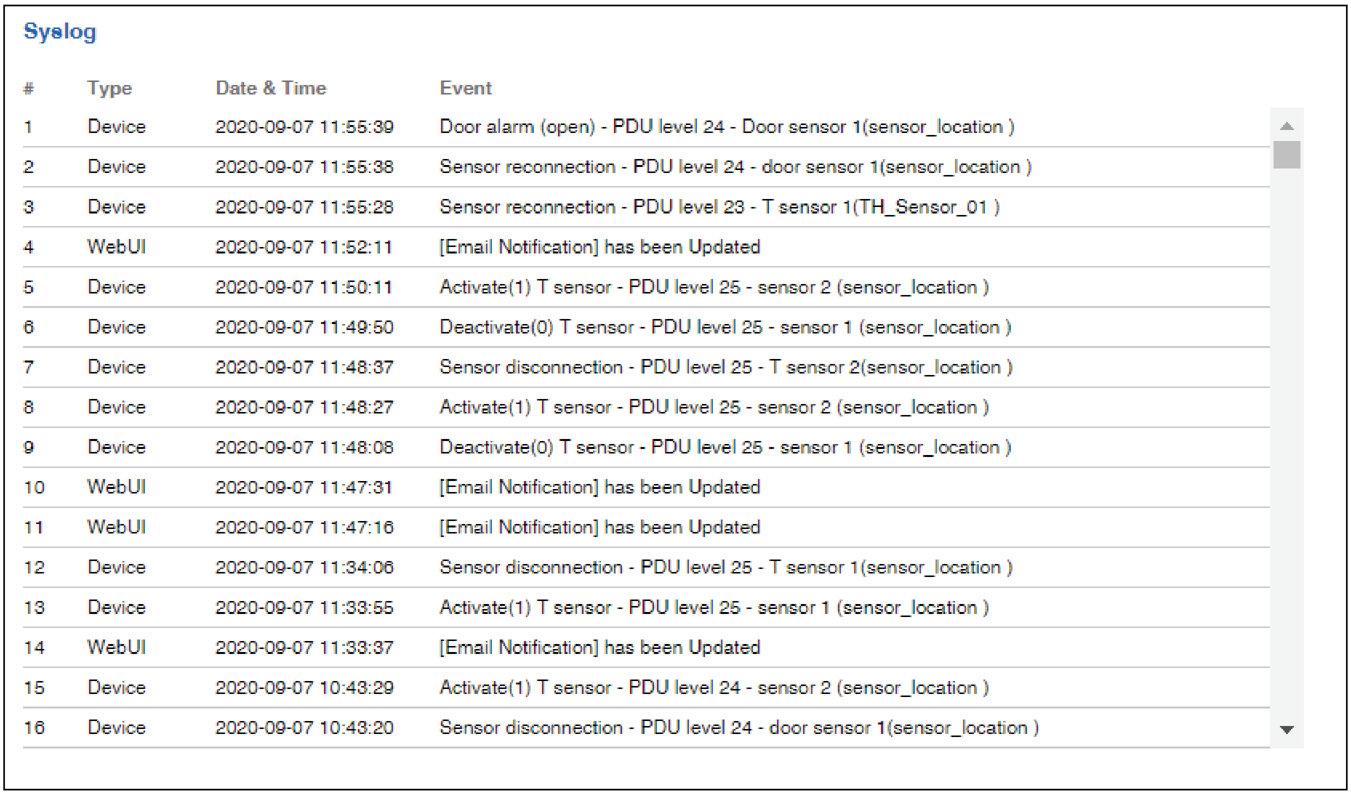


Email Notification

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 :	

< 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

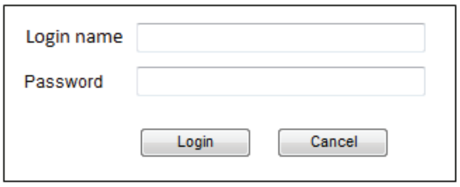
Step 2. Select appropriate firmware for Z series IP PDU

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

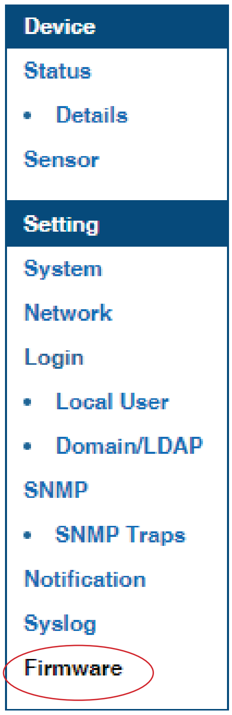
Step 4. Open the MS Edge

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

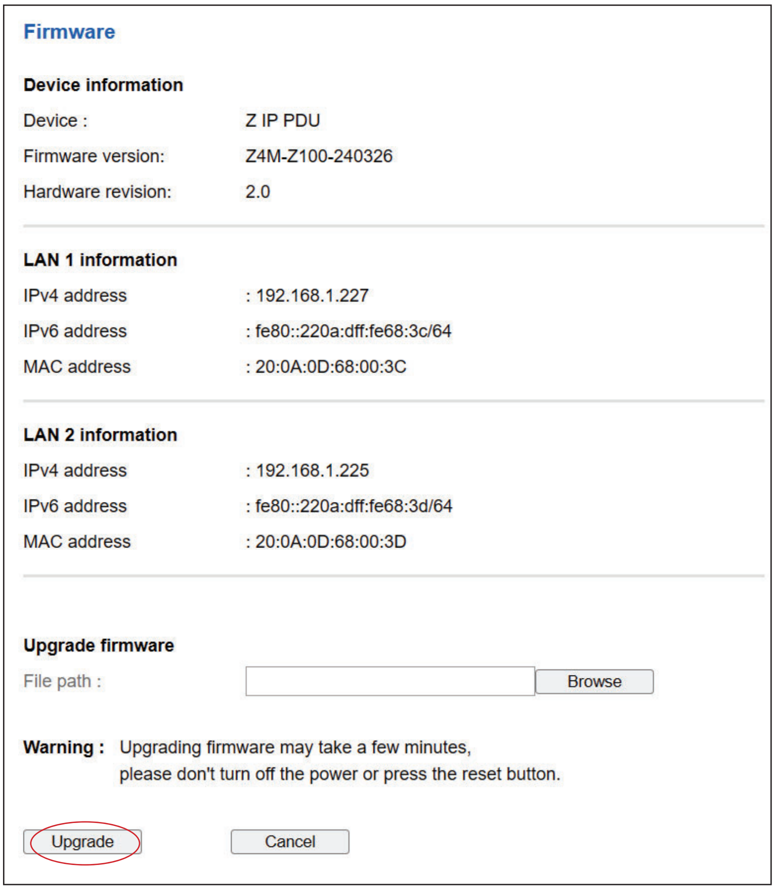
Step 6. Enter “ **Login name** “ & “ **Password** “.



Step 7. Select the Firmware from the left navigation pane



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 firmware upgrade can ONLY be performed via IPv4 network.
- Do NOT perform the firmware 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

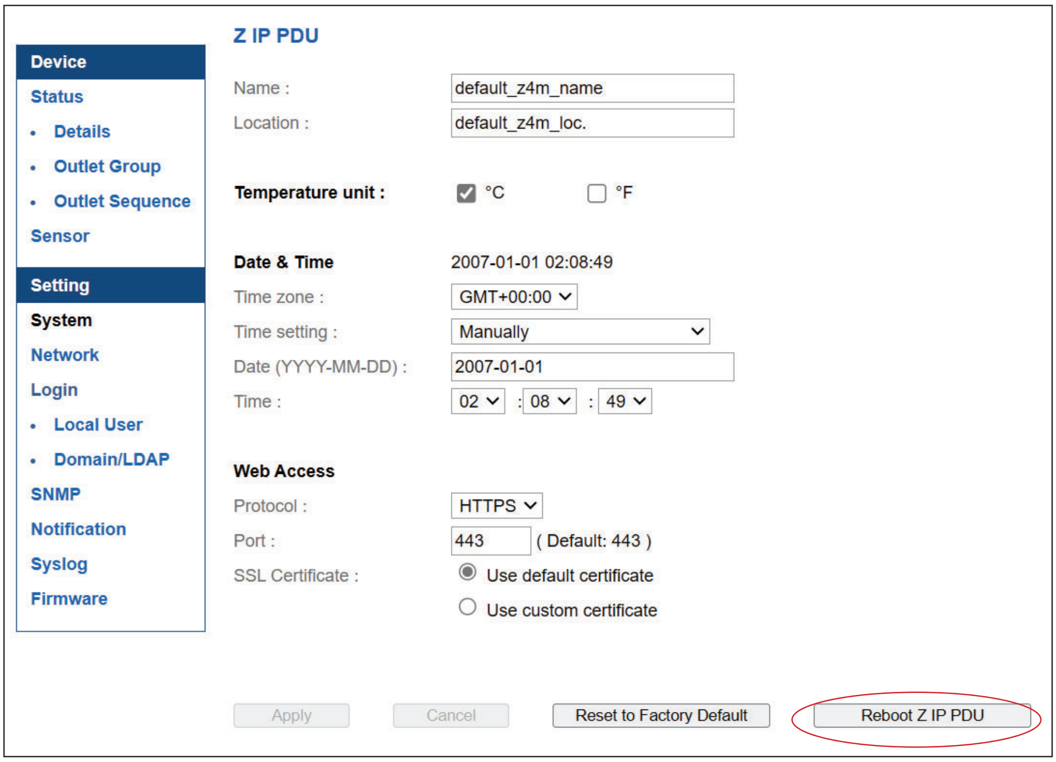
Step 4. Properly configure your DHCP server so that it refers to the file " **fwupdate.cfg** " on the TFTP server for your Z series IP PDU. See ***DHCP IPv4 Configuration in Windows***

Step 5. Make sure all of the Z series IP PDUs use DHCP as the IP configuration 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 IP PDU** ” in “ **System** ” of PPS-04-S.



Z IP PDU

Name : default_z4m_name

Location : default_z4m_loc.

Temperature unit : ☑ °C □ °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 : ● Use default certificate ○ Use custom certificate

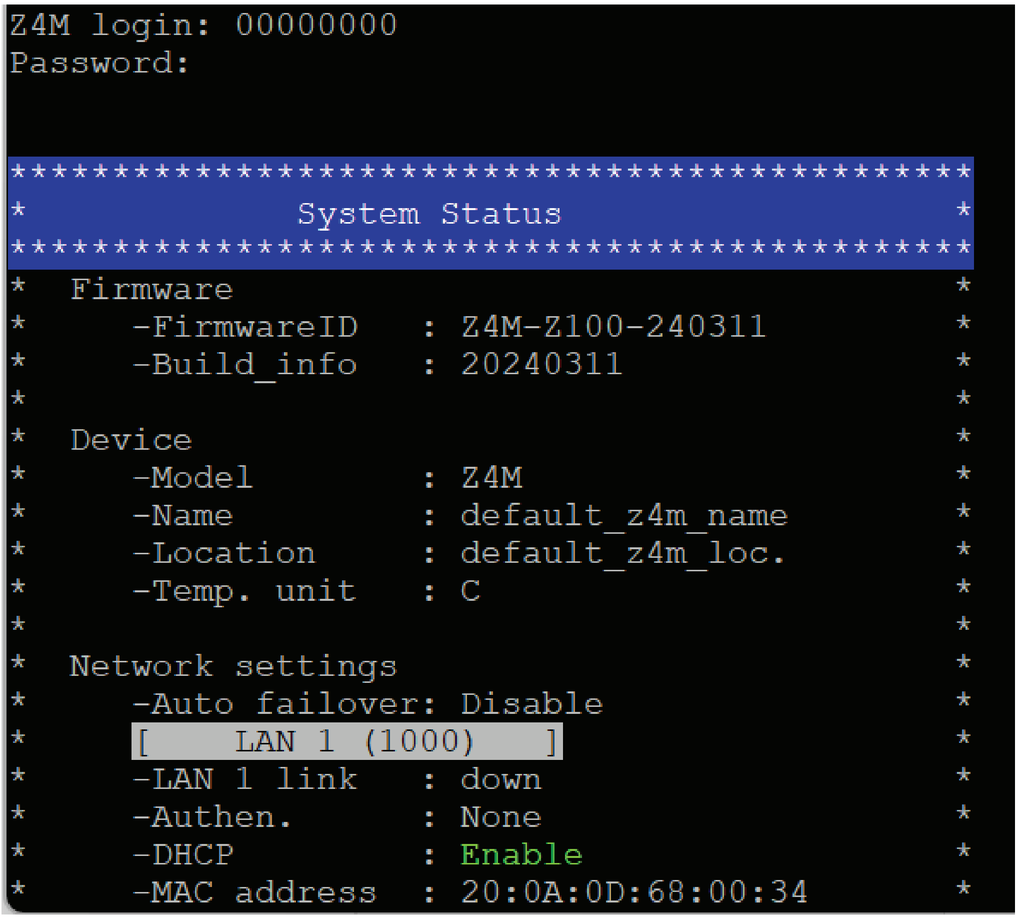
⚠ You must enable firmware upgrade via DHCP in SSH (default is ENABLED) and input the username and password for bulk firmware upgrade in the “ **fwupdate.cfg** ” file. You can change the username and password for bulk firmware upgrade via SSH. **See *Configuration of username / password for bulk firmware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

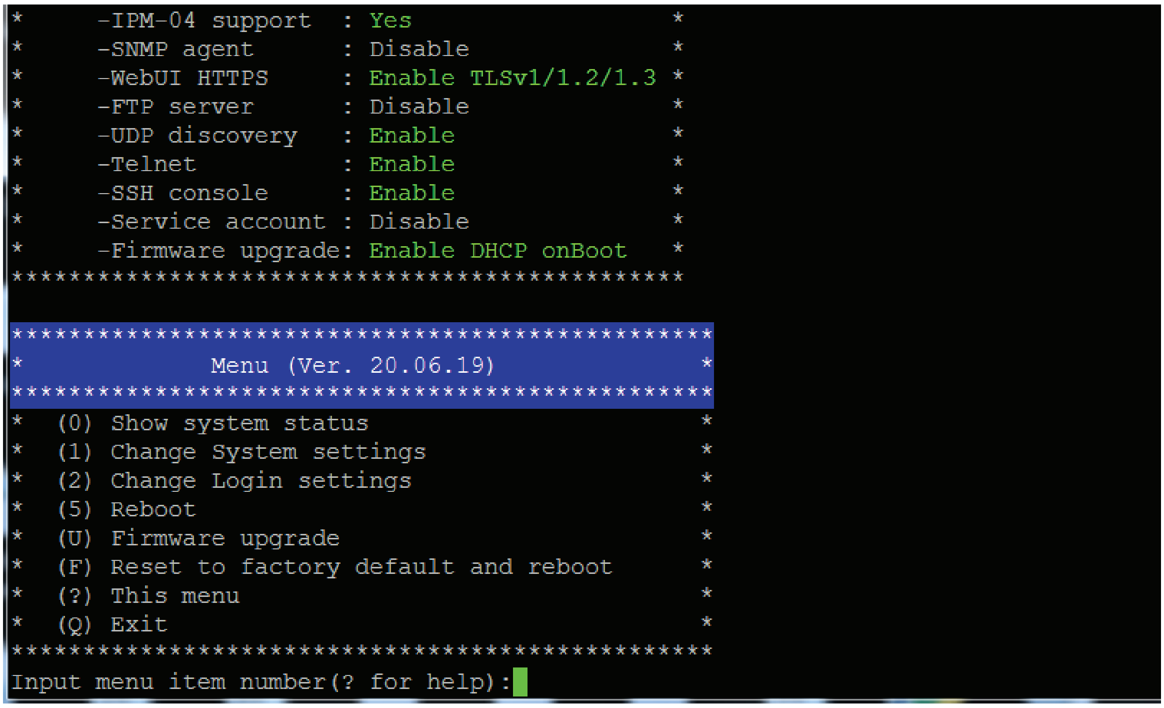
Step 2. Input the login name and password to login the CLI.



```
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** "

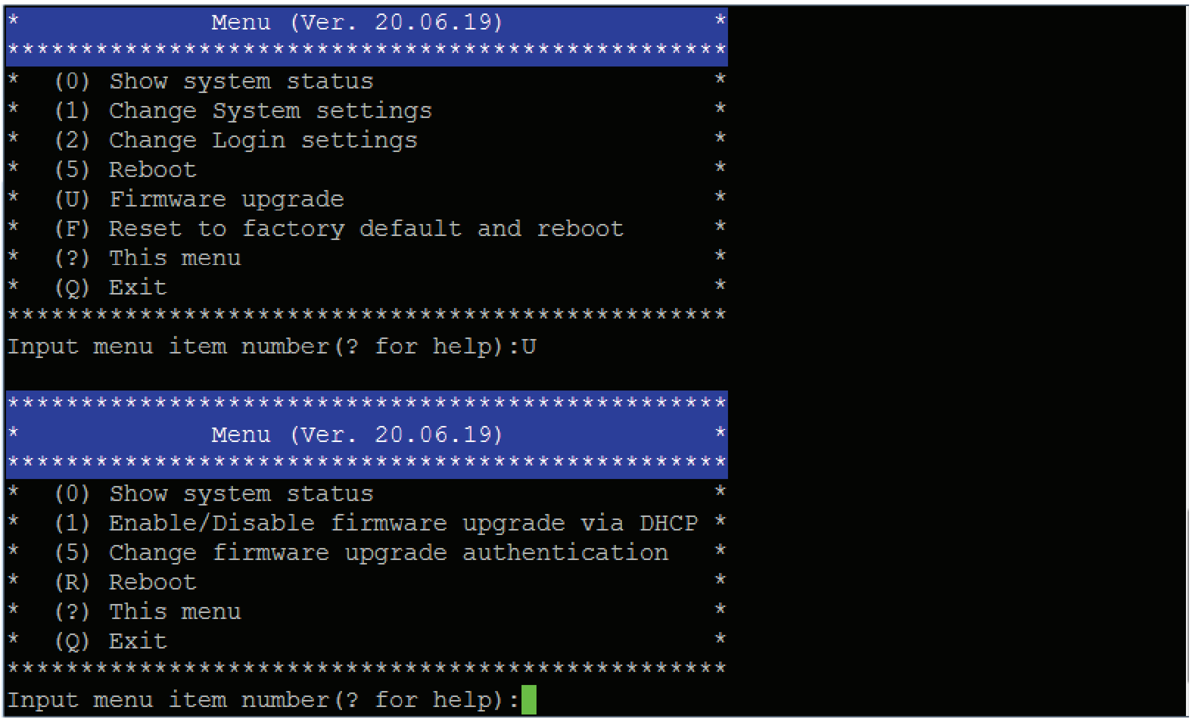


```
*      -IPM-04 support  : Yes                 *
*      -SNMP agent      : Disable             *
*      -WebUI HTTPS     : Enable TLSv1/1.2/1.3 *
*      -FTP server      : Disable             *
*      -UDP discovery   : Enable              *
*      -Telnet          : Enable              *
*      -SSH 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

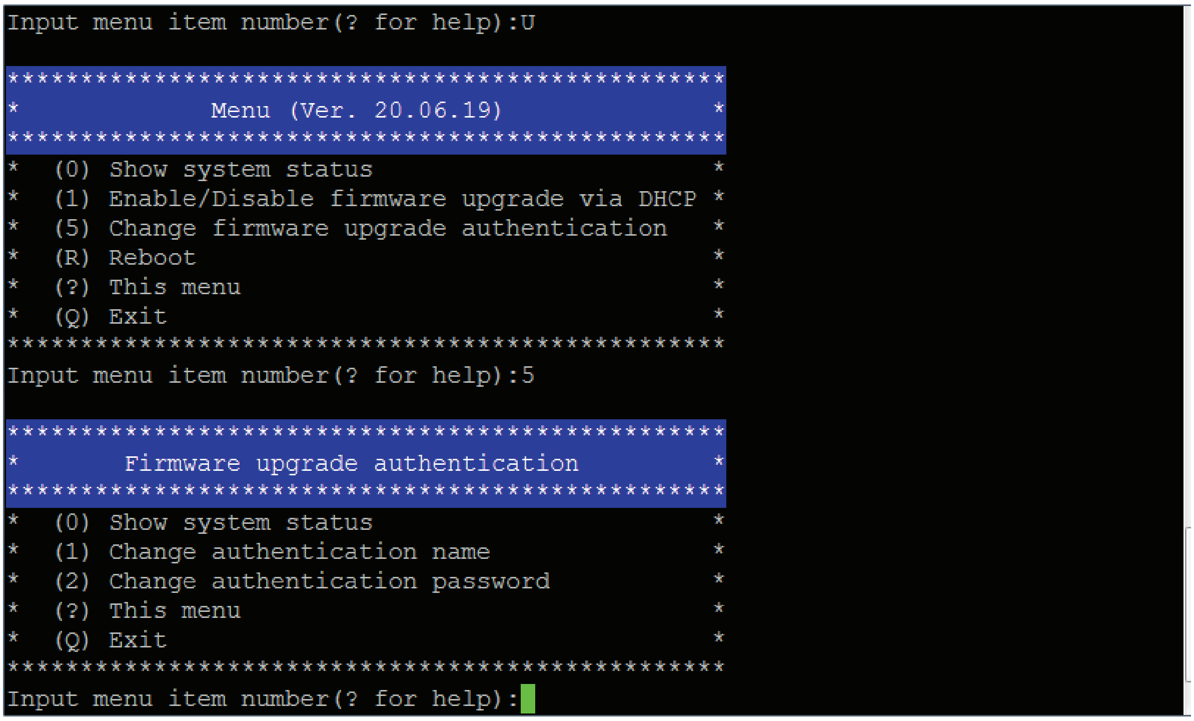
Step 4. Select " **(5) Change firmware upgrade authentication** " and " **Enter** "



```
*              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 :

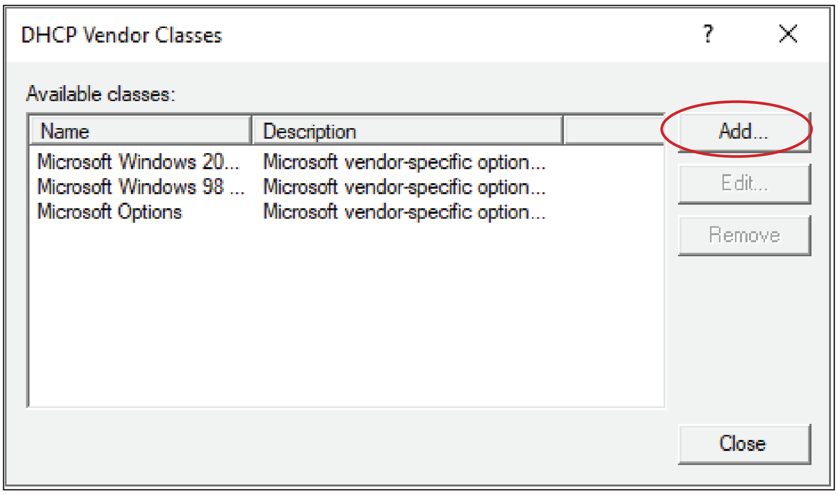
- Able to work with IPv4
- A folder containing all required files is available in the TFTP root directory. The folder name MUST be the same as the String value of the Magic code. Details please refer to DHCP IPv4 Configuration in Windows
- The TFTP server supports the write operation including file creation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

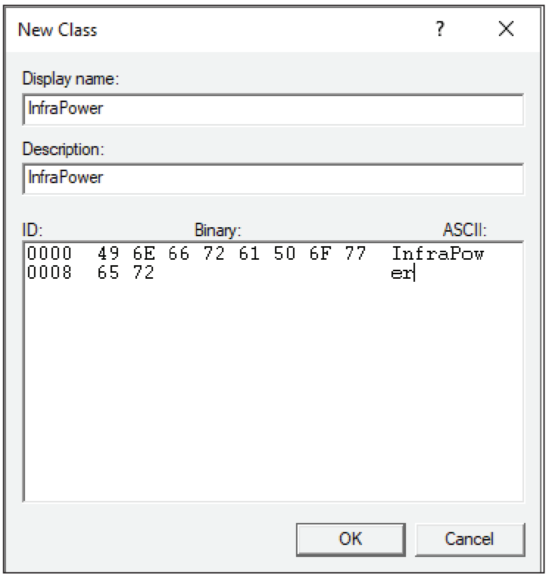


DHCP Vendor Classes

Available classes:

Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

- 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.



New Class

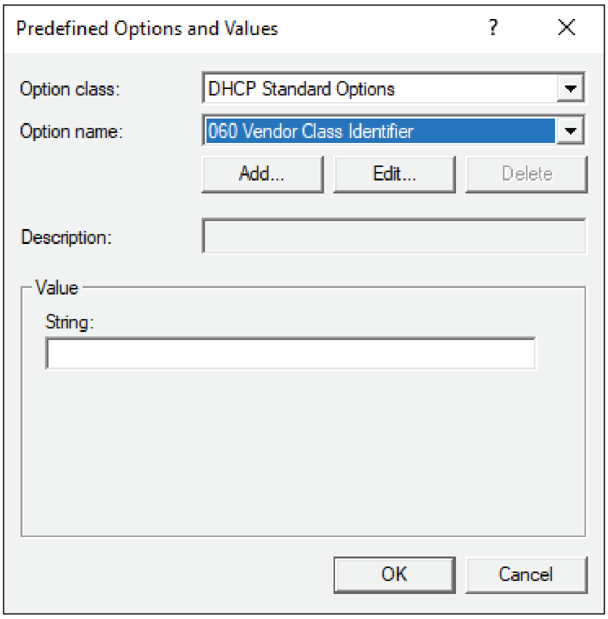
Display name: InfraPower

Description: InfraPower

```
ID:        Binary:                    ASCII:
0000   49 6E 66 72 61 50 6F 77   InfraPow
0008   65 72                     er
```

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

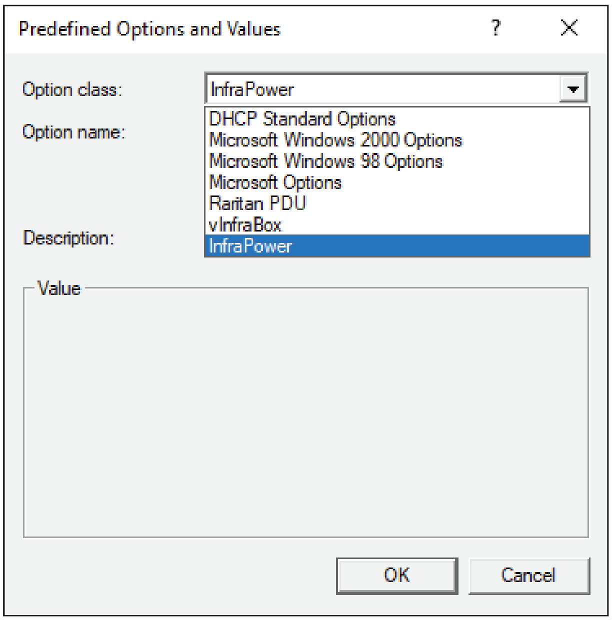
Description:

Value

String:

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

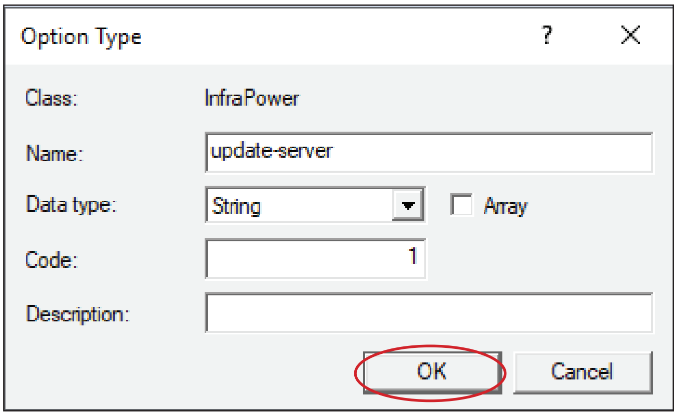
Option name:

Description:

Value

< 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** “.



Class: InfraPower

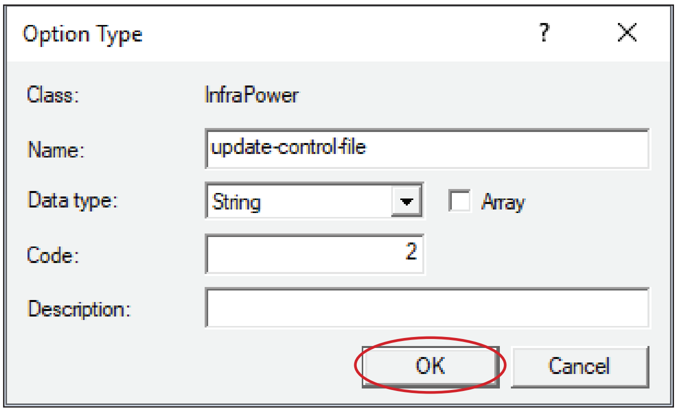
Name: update-server

Data type: String ☐ Array

Code: 1

Description:

- 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** “.



Class: InfraPower

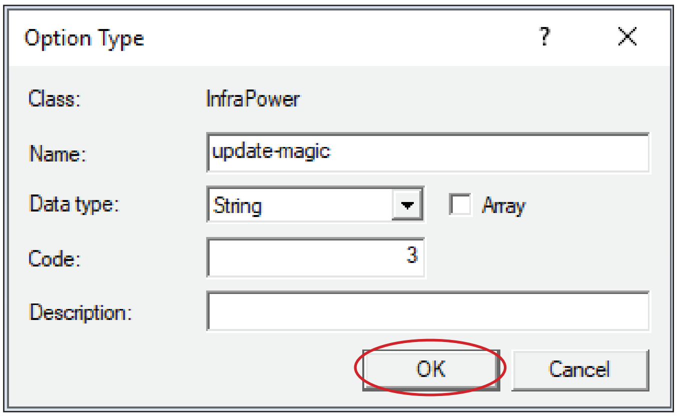
Name: update-control-file

Data type: String ☐ Array

Code: 2

Description:

- 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** “.



Class: InfraPower

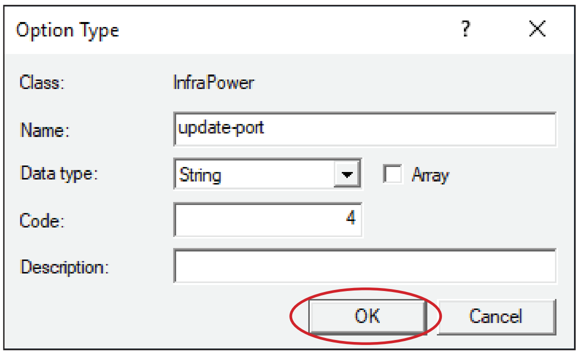
Name: update-magic

Data type: String ☐ Array

Code: 3

Description:

- 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** “.



Option Type

Class: InfraPower

Name: update-port

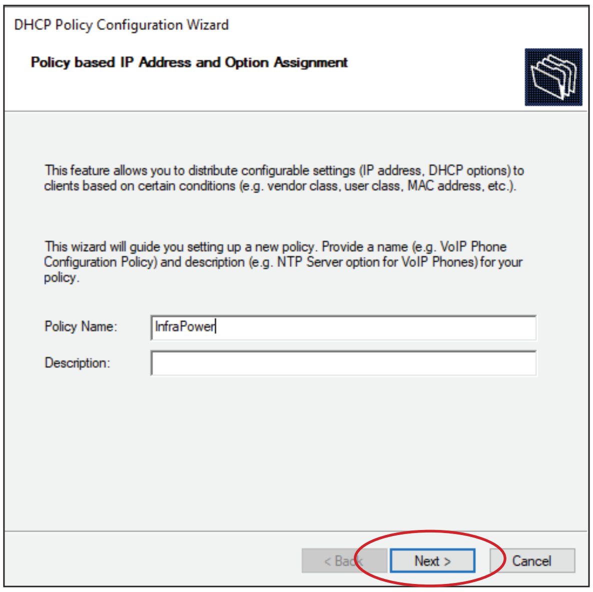
Data type: String □ Array

Code: 4

Description:

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.



DHCP Policy Configuration Wizard

Policy based IP Address and Option Assignment

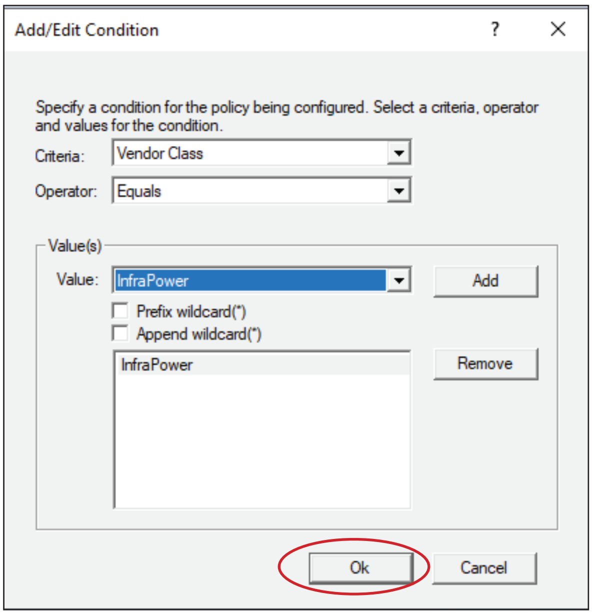
This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

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.

Policy Name: InfraPower

Description:

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



Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Vendor Class

Operator: Equals

Value(s)

Value: InfraPower

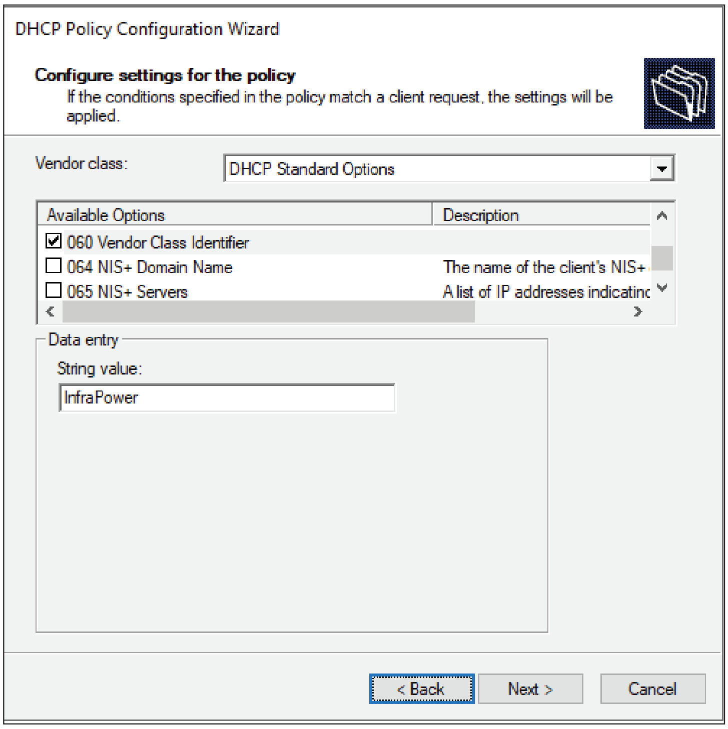
□ Prefix wildcard(*)

□ Append wildcard(*)

InfraPower

< 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.

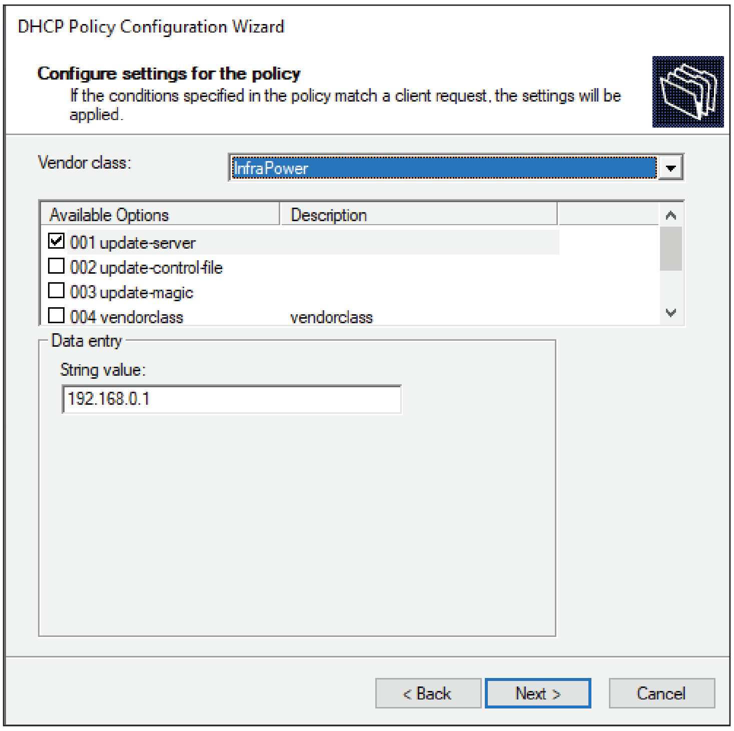
Vendor class: DHCP Standard Options

Available Options	Description
☑ 060 Vendor Class Identifier	
□ 064 NIS+ Domain Name	The name of the client's NIS+
□ 065 NIS+ Servers	A list of IP addresses indicatinc

Data entry

String value: InfraPower

- 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.

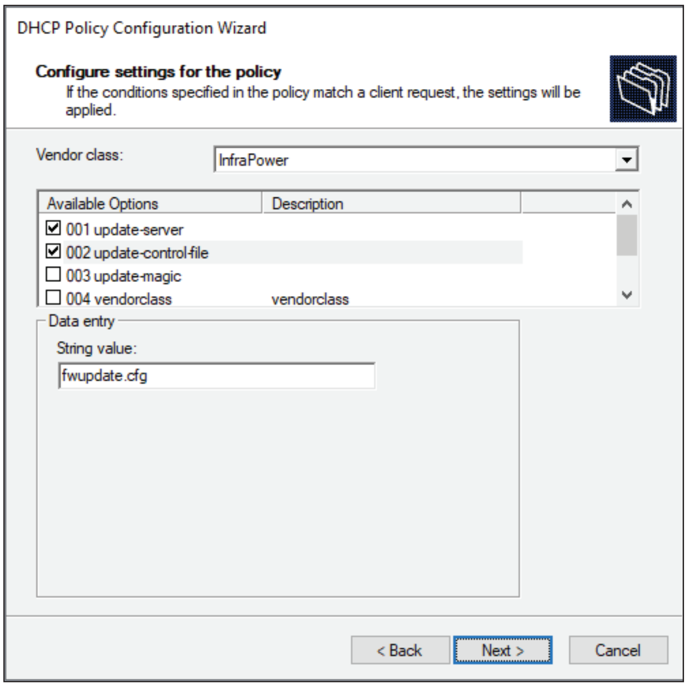
Vendor class: InfraPower

Available Options	Description
☑ 001 update-server	
□ 002 update-control-file	
□ 003 update-magic	
□ 004 vendorclass	vendorclass

Data entry

String value: 192.168.0.1

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

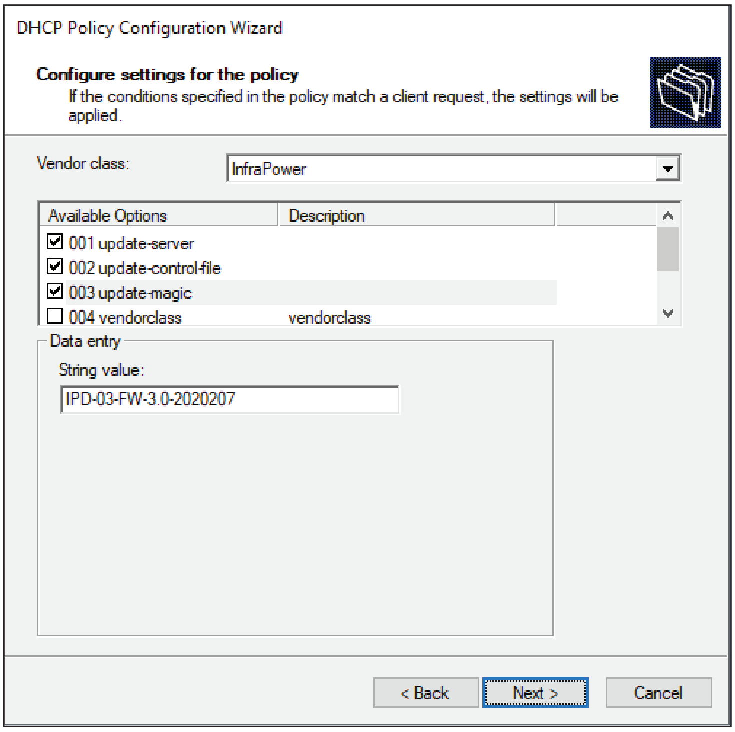
Vendor class: InfraPower

Available Options	Description
☑ 001 update-server	
☑ 002 update-control-file	
□ 003 update-magic	
□ 004 vendorclass	vendorclass

Data entry

String value: fwupdate.cfg

- 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.



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

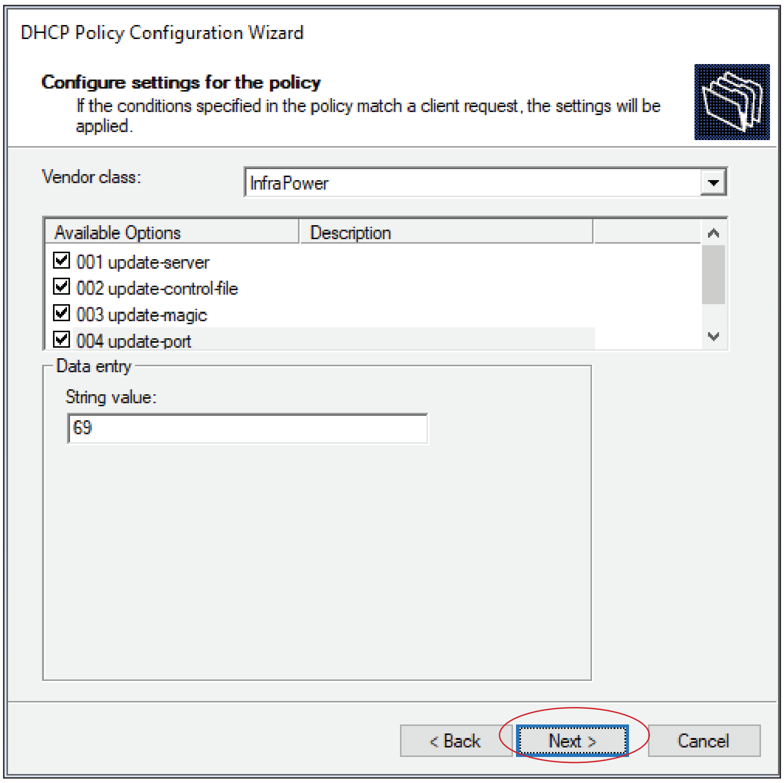
Available Options	Description
☑ 001 update-server	
☑ 002 update-control-file	
☑ 003 update-magic	
□ 004 vendorclass	vendorclass

Data entry

String value: IPD-03-FW-3.0-2020207

⚠ 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.

- 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.



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
☑ 001 update-server	
☑ 002 update-control-file	
☑ 003 update-magic	
☑ 004 update-port	

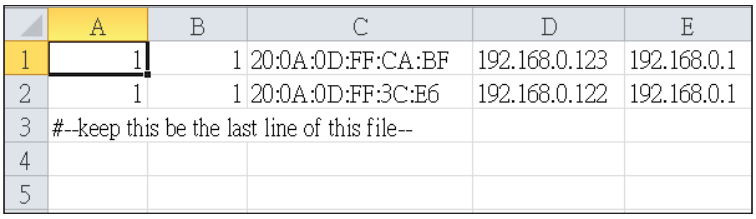
Data entry

String value: 69

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

< 2.12 > Bulk Firmware Upgrade of Z series IP PDU

Description of Devices.csv



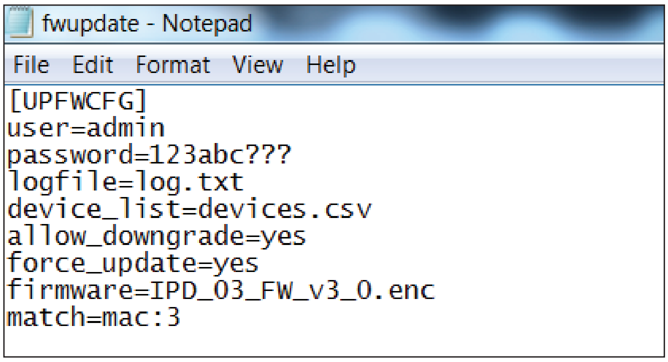
	A	B	C	D	E
1	1	1	20:0A:0D:FF:CA:BF	192.168.0.123	192.168.0.1
2	1	1	20:0A:0D:FF:3C:E6	192.168.0.122	192.168.0.1
3	#--keep this be the last line of this file--				
4					
5					

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.

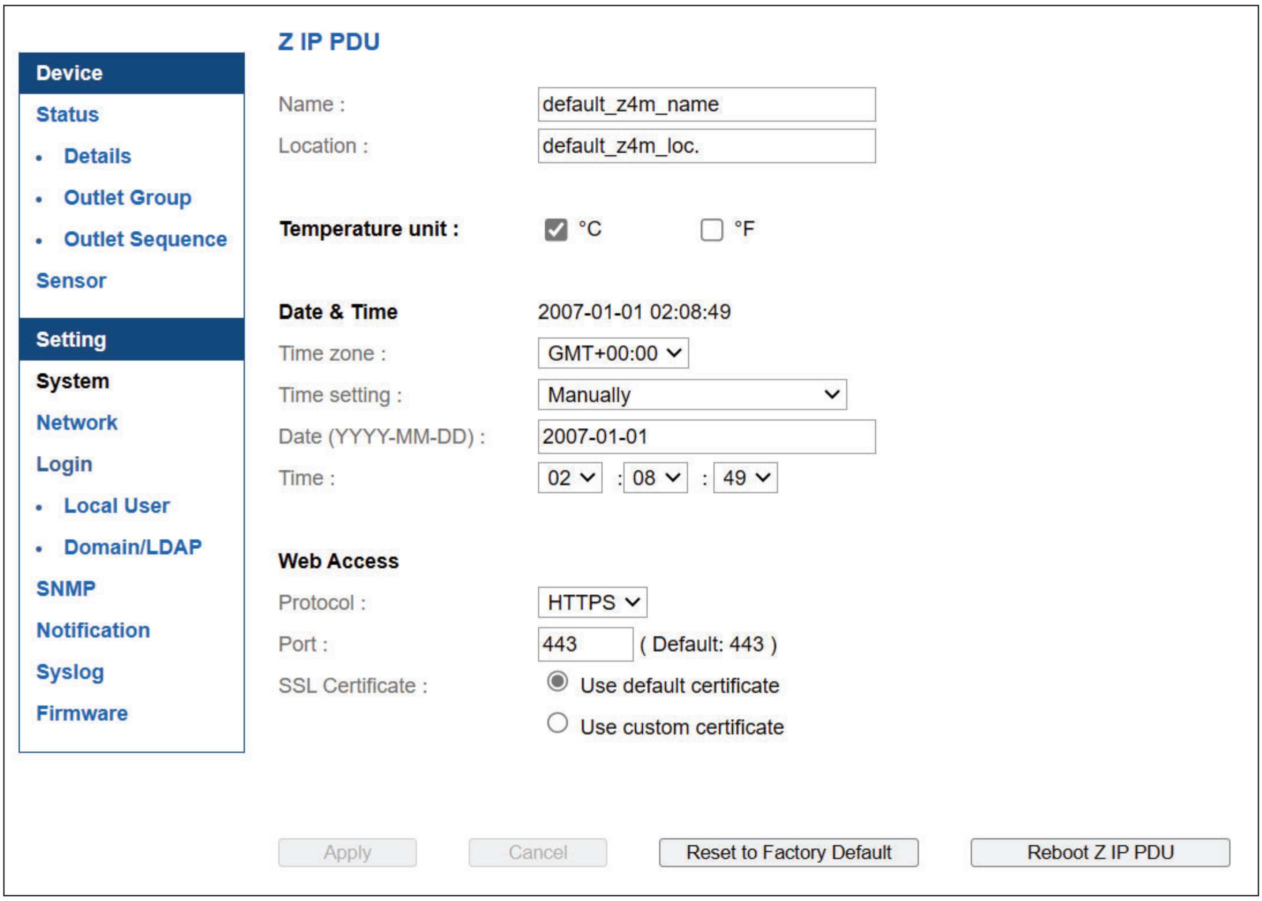
Eighth row is the firmware version you want to upgrade, it MUST be the same as the filename of the firmware stored in the folder under the root directory of the TFTP server.

< 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.



Z IP PDU

Name : default_z4m_name

Location : default_z4m_loc.

Temperature unit : ☑ °C ☐ °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)

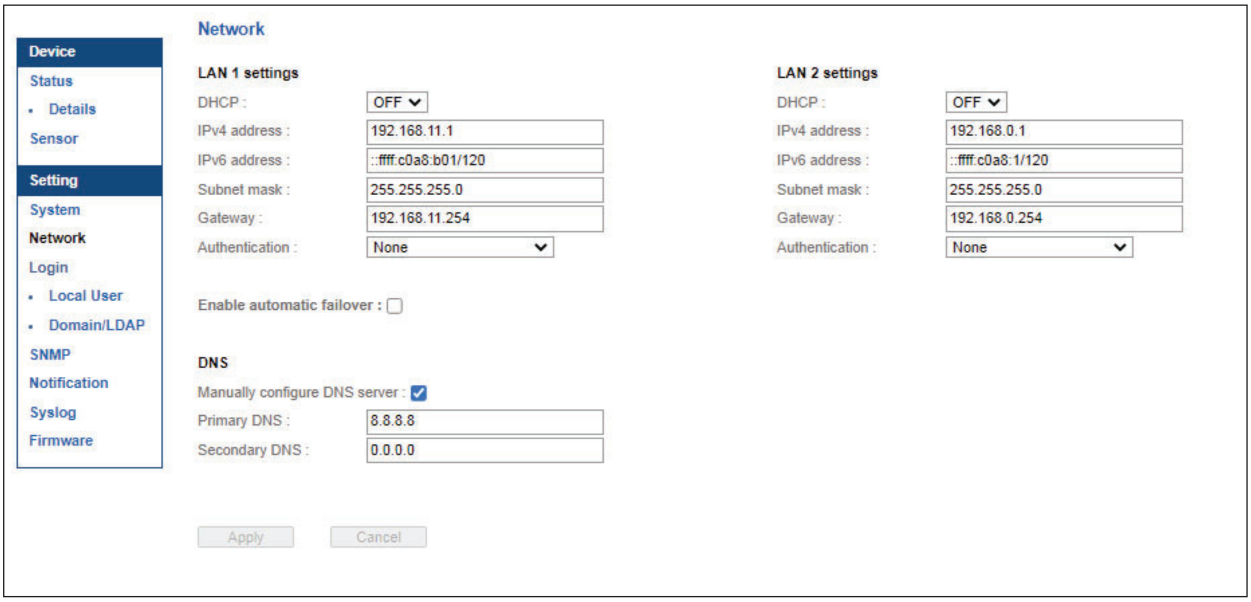
SSL Certificate : ● Use default certificate ○ Use custom certificate

< 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.



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.1
IPv6 address :	::ffff:c0a8:b01/120	IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0	Subnet mask :	255.255.255.0
Gateway :	192.168.11.254	Gateway :	192.168.0.254
Authentication :	None	Authentication :	None

Enable automatic failover : □

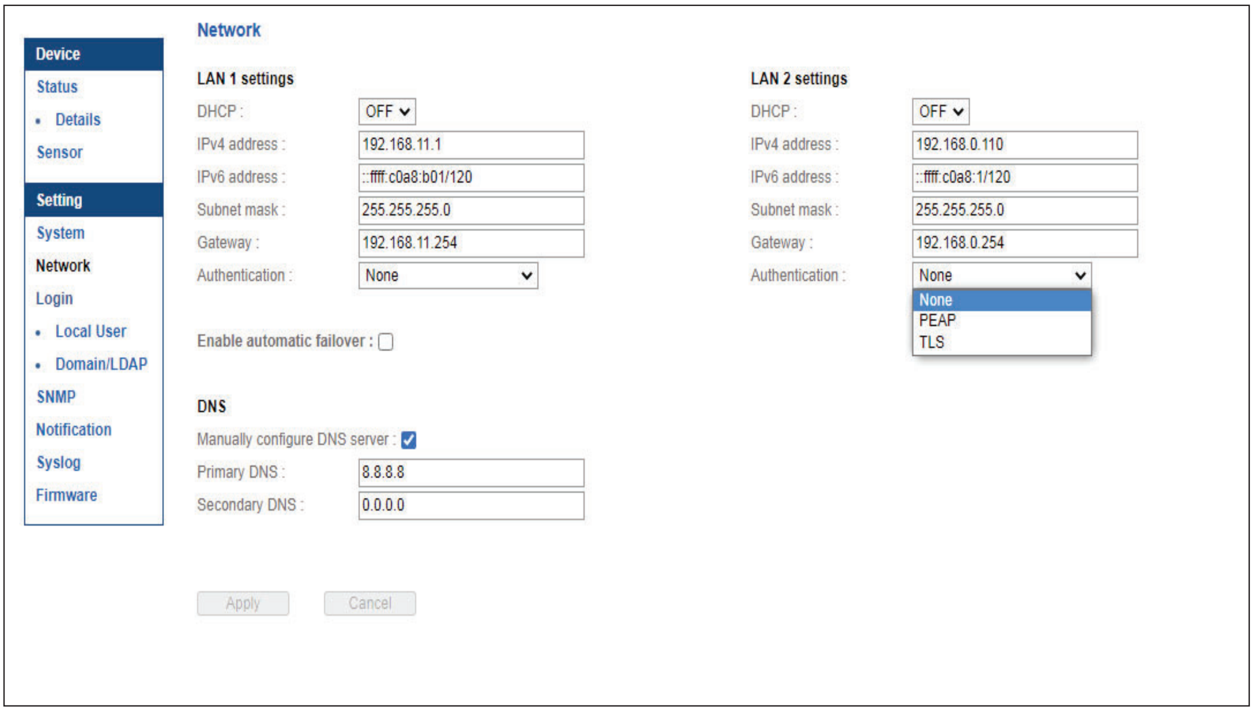
DNS

Manually configure DNS server : ☑

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

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



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.110
IPv6 address :	::ffff:c0a8:b01/120	IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0	Subnet mask :	255.255.255.0
Gateway :	192.168.11.254	Gateway :	192.168.0.254
Authentication :	None	Authentication :	None

Enable automatic failover : □

DNS

Manually configure DNS server : ☑

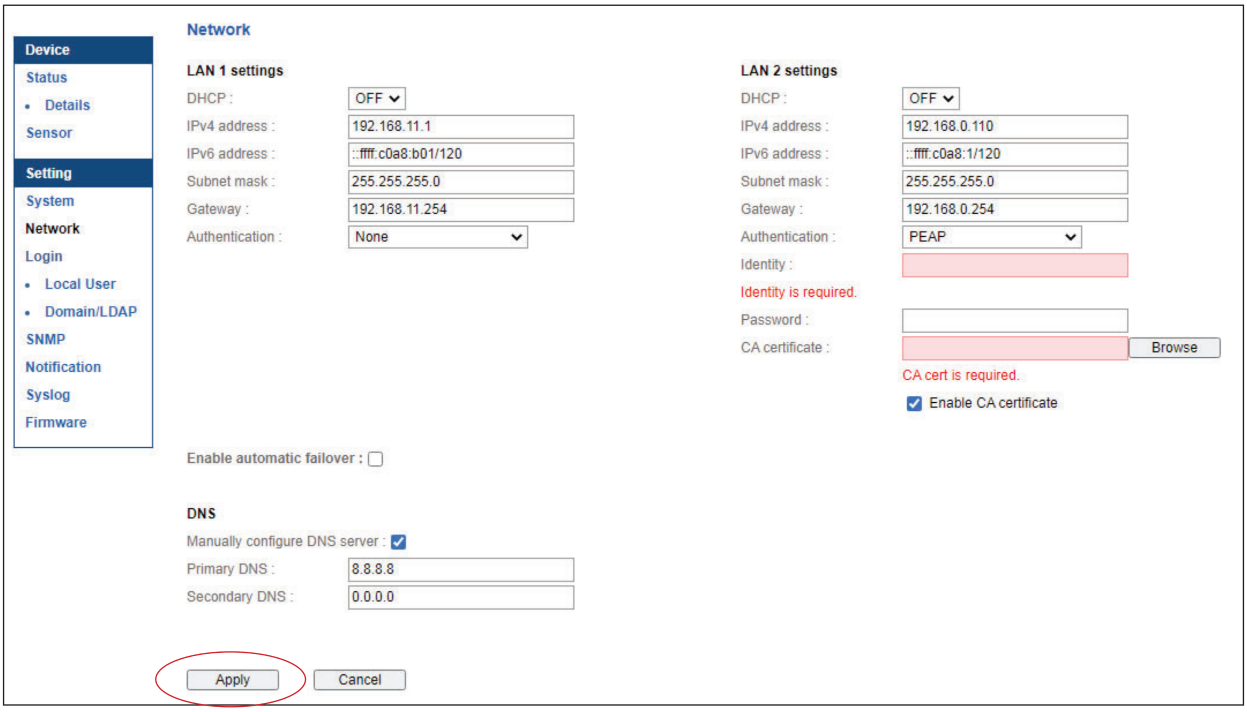
Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

< 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.



Network

LAN 1 settings

DHCP : OFF
IPv4 address : 192.168.11.1
IPv6 address : ::ffff:c0a8:b01/120
Subnet mask : 255.255.255.0
Gateway : 192.168.11.254
Authentication : None

LAN 2 settings

DHCP : OFF
IPv4 address : 192.168.0.110
IPv6 address : ::ffff:c0a8:1/120
Subnet mask : 255.255.255.0
Gateway : 192.168.0.254
Authentication : PEAP
Identity :
Identity is required.
Password :
CA certificate :
CA cert is required.
☑ Enable CA certificate

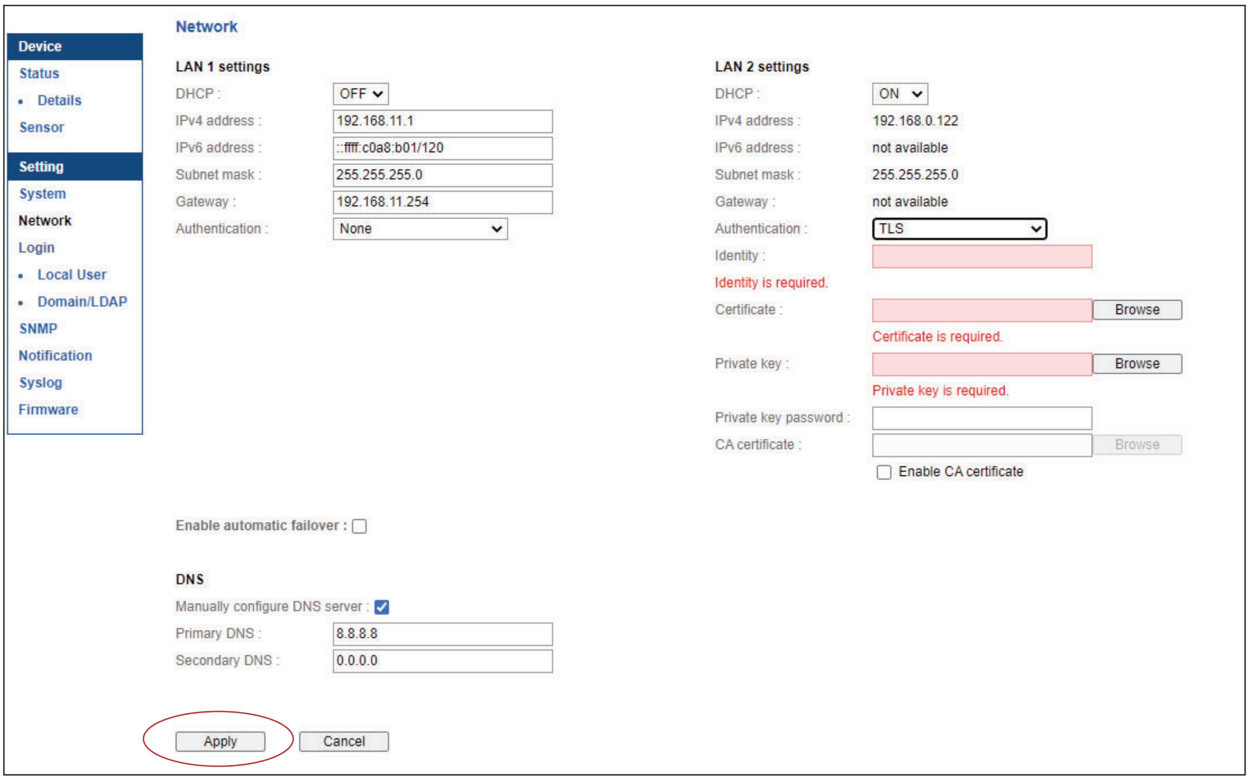
Enable automatic failover : □

DNS

Manually configure DNS server : ☑
Primary DNS : 8.8.8.8
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.



Network

LAN 1 settings

DHCP : OFF
IPv4 address : 192.168.11.1
IPv6 address : ::ffff:c0a8:b01/120
Subnet mask : 255.255.255.0
Gateway : 192.168.11.254
Authentication : None

LAN 2 settings

DHCP : ON
IPv4 address : 192.168.0.122
IPv6 address : not available
Subnet mask : 255.255.255.0
Gateway : not available
Authentication : TLS
Identity :
Identity is required.
Certificate :
Certificate is required.
Private key :
Private key is required.
Private key password :
CA certificate :
□ Enable CA certificate

Enable automatic failover : □

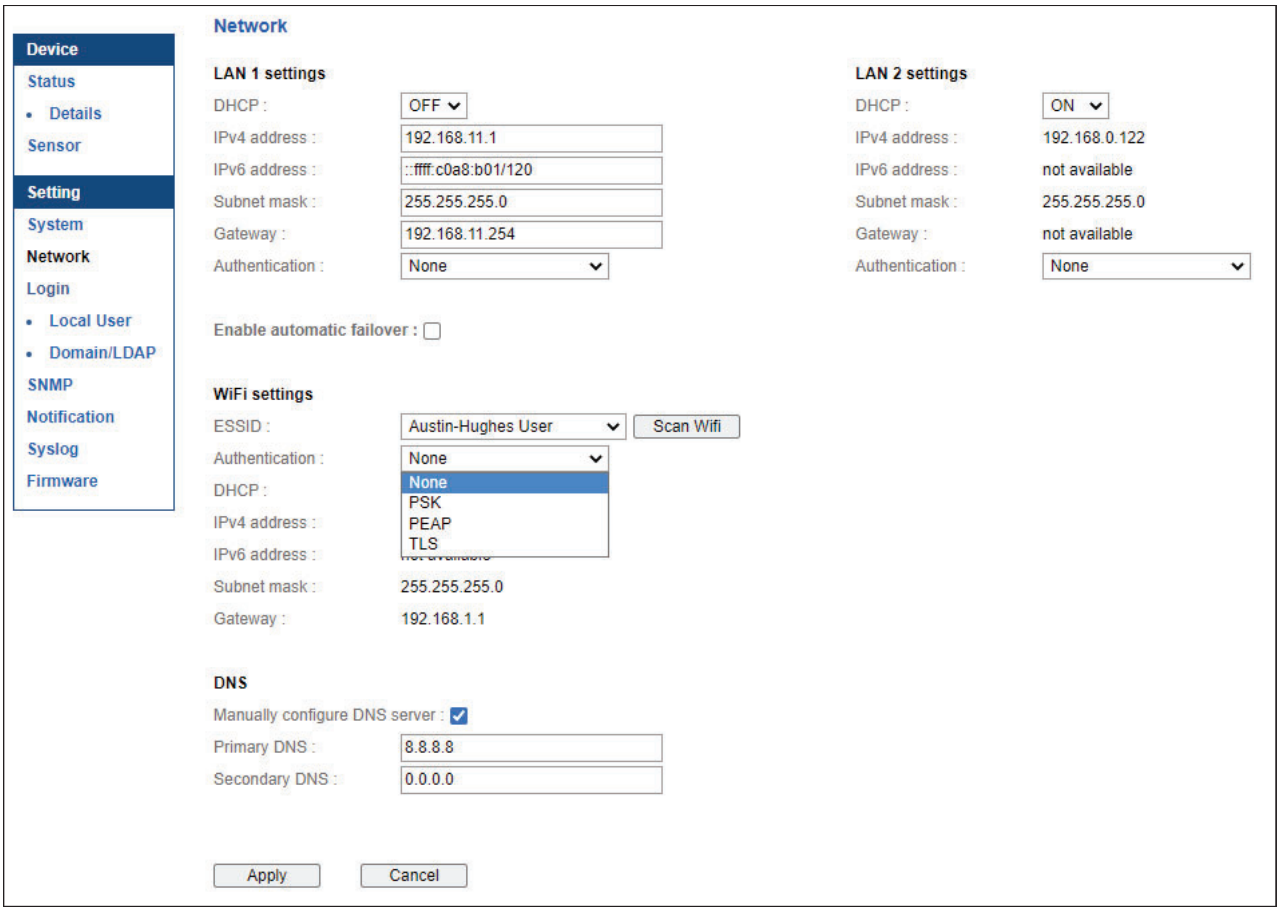
DNS

Manually configure DNS server : ☑
Primary DNS : 8.8.8.8
Secondary DNS : 0.0.0.0

< 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



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	ON
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.122
IPv6 address :	::ffff:c0a8:b01/120	IPv6 address :	not available
Subnet mask :	255.255.255.0	Subnet mask :	255.255.255.0
Gateway :	192.168.11.254	Gateway :	not available
Authentication :	None	Authentication :	None

Enable automatic failover : □

WiFi settings

ESSID :	Austin-Hughes User
Authentication :	None None PSK PEAP TLS
DHCP :	
IPv4 address :	
IPv6 address :	
Subnet mask :	255.255.255.0
Gateway :	192.168.1.1

DNS

Manually configure DNS server : ☑

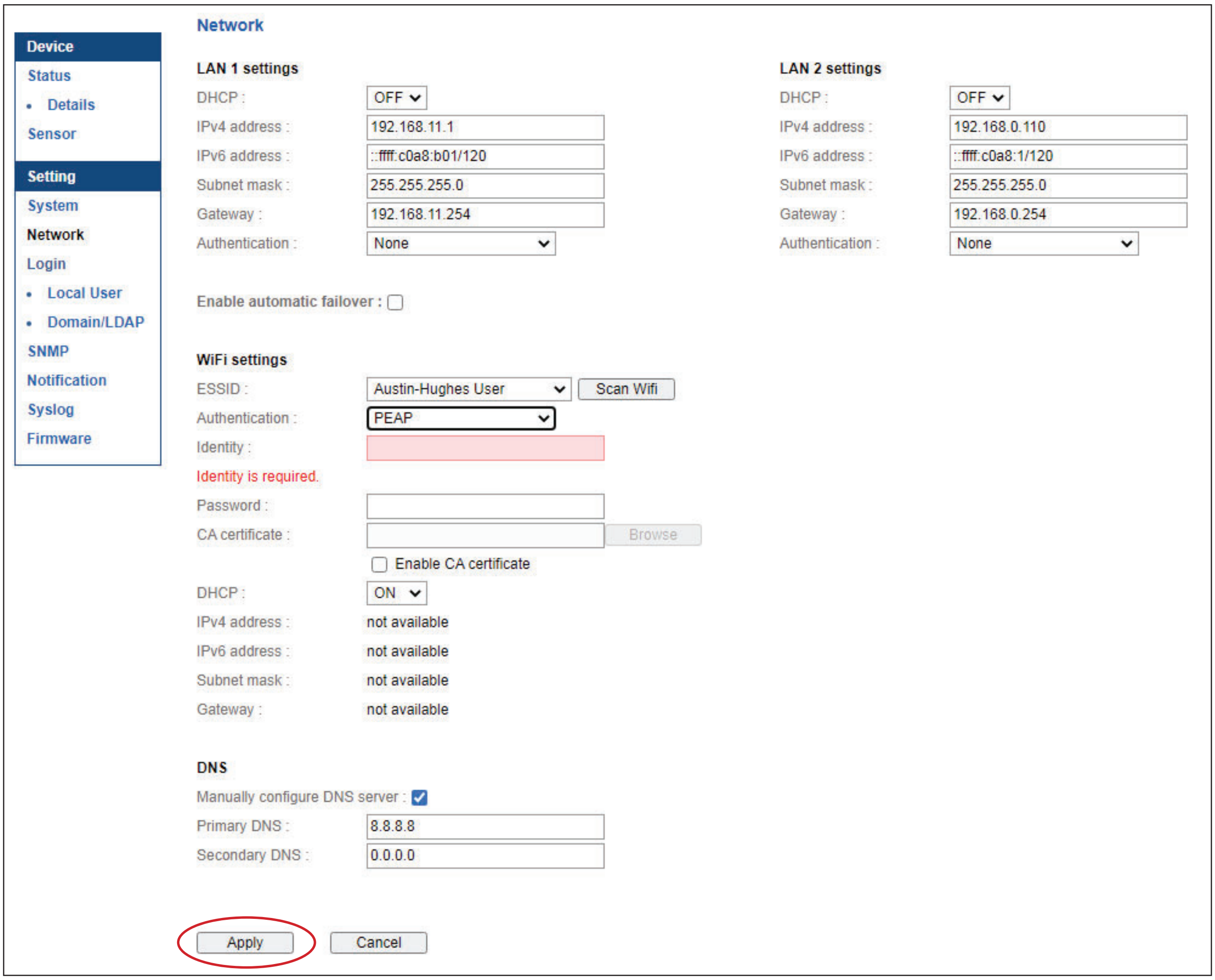
Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

< 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.



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.110
IPv6 address :	::ffff:c0a8:b01/120	IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0	Subnet mask :	255.255.255.0
Gateway :	192.168.11.254	Gateway :	192.168.0.254
Authentication :	None	Authentication :	None

Enable automatic failover : □

WiFi settings

ESSID : Austin-Hughes User

Authentication : PEAP

Identity :

Identity is required.

Password :

CA certificate :

□ Enable CA certificate

DHCP : ON

IPv4 address : not available

IPv6 address : not available

Subnet mask : not available

Gateway : not available

DNS

Manually configure DNS server : ☑

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

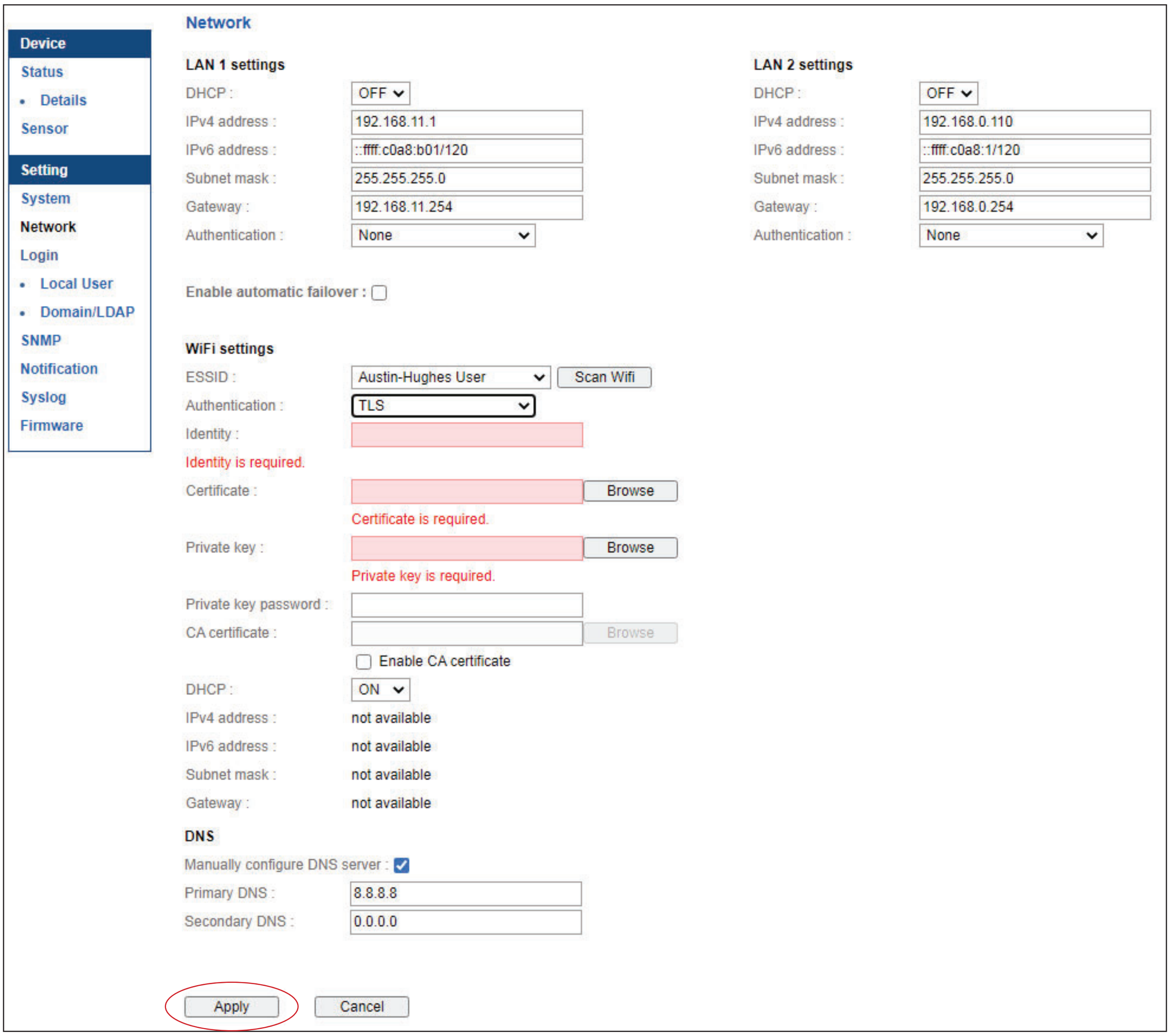
< 2.13 >   802.1X authentication

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.



Network

LAN 1 settings

DHCP :	OFF
IPv4 address :	192.168.11.1
IPv6 address :	::ffff:c0a8:b01/120
Subnet mask :	255.255.255.0
Gateway :	192.168.11.254
Authentication :	None

LAN 2 settings

DHCP :	OFF
IPv4 address :	192.168.0.110
IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0
Gateway :	192.168.0.254
Authentication :	None

Enable automatic failover : □

WiFi settings

ESSID :	Austin-Hughes User
Authentication :	TLS
Identity :	
Identity is required.	
Certificate :	
	Certificate is required.
Private key :	
	Private key is required.
Private key password :	
CA certificate :	
	□ Enable CA certificate
DHCP :	ON
IPv4 address :	not available
IPv6 address :	not available
Subnet mask :	not available
Gateway :	not available

DNS

Manually configure DNS server :	☑
Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

< 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 IP dongle 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

Intentionally
Left
Blank

Intentionally
Left
Blank

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 2024 Austin Hughes Electronics Ltd. All rights reserved.