InfraPower®

Inspired by Your Data Center

User Manual

PPS-03-S, IP dongle GUI & SNMP

InfraPower Intelligent PDU

Designed and manufactured by Austin Hughes

FC CE RoHS REACH

Legal Information

First English printing, August 2023

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 damage to other equipment or injury to persons nearby.
- ■ When the equipment is in an open position, do not cover, block or in any way obstruct the gap between it and the power supply. Proper air convection is necessary to keep it from overheating.
- ■ Arrange the equipment's power cord in such a way that others won't trip or fall over it.
- ■ If you are using a power cord that didn't ship with the equipment, ensure that it is rated for the voltage and current labelled on the equipment's electrical ratings label. The voltage rating on the cord should be higher than the one listed on the equipment's ratings label.
- ■ Observe all precautions and warnings attached to the equipment.
- ■ If you don't intend on using the equipment for a long time, disconnect it from the power outlet to prevent being damaged by transient over-voltage.
- ■ Keep all liquids away from the equipment to minimize the risk of accidental spillage. Liquid spilled on to the power supply or on other hardware may cause damage, fire or electrical shock.
- ■ Only qualified service personnel should open the chassis. Opening it yourself could damage the equipment and invalidate its warranty.
- ■ If any part of the equipment becomes damaged or stops functioning, have it checked by qualified service personnel.

What the warranty does not cover

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

Regulatory Notices Federal Communications Commission (FCC)

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

Any changes or modifications made to this equipment may void the user's authority to operate this equipment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ■ Re-position or relocate the receiving antenna.
- ■ Increase the separation between the equipment and receiver.
- ■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Contents

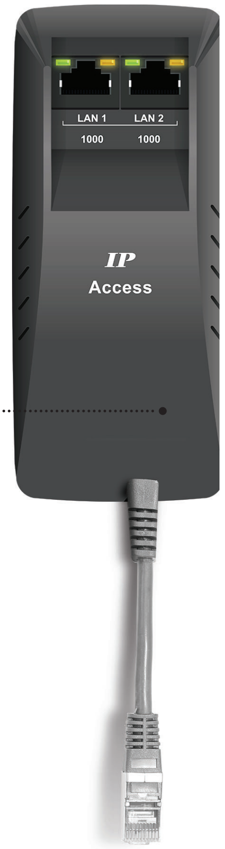
< 1.1 > IP Dongle Specification

IP Dongle Access to 32 PDU Levels

Patented IP Dongle provides IP remote access to the PDUs by a true network IP address chain. Only 1 x IP dongle allows access to max. 32 PDUs in daisy chain - which is a highly efficient application for saving not only the IP remote accessories cost, but also the true IP addresses required on the PDU management.

Hot-Pluggable design facilitates the IP dongle installation. Simply integrate the IP Dongle to the 1st PDU, then the entire daisy chain group can be remote over IP. Hence, administrator can remotely access all PDUs in the daisy chain group by one single IP via the IP Dongle.

- Press the reset button and release instantly to reboot IP dongle.
- Press and hold the reset button until Green LED off to reset IP dongle to factory default



Part no.
IPD-03-S

Reset button

InfraPower PPS-03-S

Features		
Capacity	IP Dongle Group (Just 1 for 32 PDU levels)	1
	Max PDU number per IP dongle (IPD-03-S)**	32
	Concurrent Users	1
Enhanced Features	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 Threshold Setting	✔
	Door & Smoke Sensor Monitoring	✔
	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	✔

** Data refresh speed subject to number of cascaded PDU.

< 1.1 > IP Dongle Specification

Dual LAN Network Failover

> Auto failover to a 2nd Ethernet-connection in the event of network interruption
> Ensuring 100% iPDU uptime reporting

Connectivity

> Access your iPDU on two independent networks or VLANs
> Auto-negotiable 10/100 BaseT Ethernet & 1000 BaseT Gigabit Ethernet ports
> Redundant network access to the connected iPDUs via IP

Enterprise Level IP Authentication

> Active Directory (AD), Lightweight Directory Access Protocol (LDAPv3 / LDAPS), Remote Access Dial-In User Service (RADIUS) protocol, or local credential database.
> Strong passwords and granular user/user group permissions.

Remote Management

> Significantly reduce the number of Ethernet ports used in deployment by cascading a single network connection across multiple iPDUs (up to 32)
> Simultaneous access via free management software IPM-04, web GUI & SNMP V2 / V3
> Remote level & ID setting for cascaded iPDU’s

Alerts / Alarms

> Receive alerts via SNMP, email (SMTP), and syslog when predefined thresholds are exceeded for both iPDU and environmental sensor events.
> Common SNMP MIBs (Management Information Base) across all iPDU families

USB Wifi Port

> Optionally connect via a Wifi kit (IPD-WIFI) complying with 802.11 g/n/ac

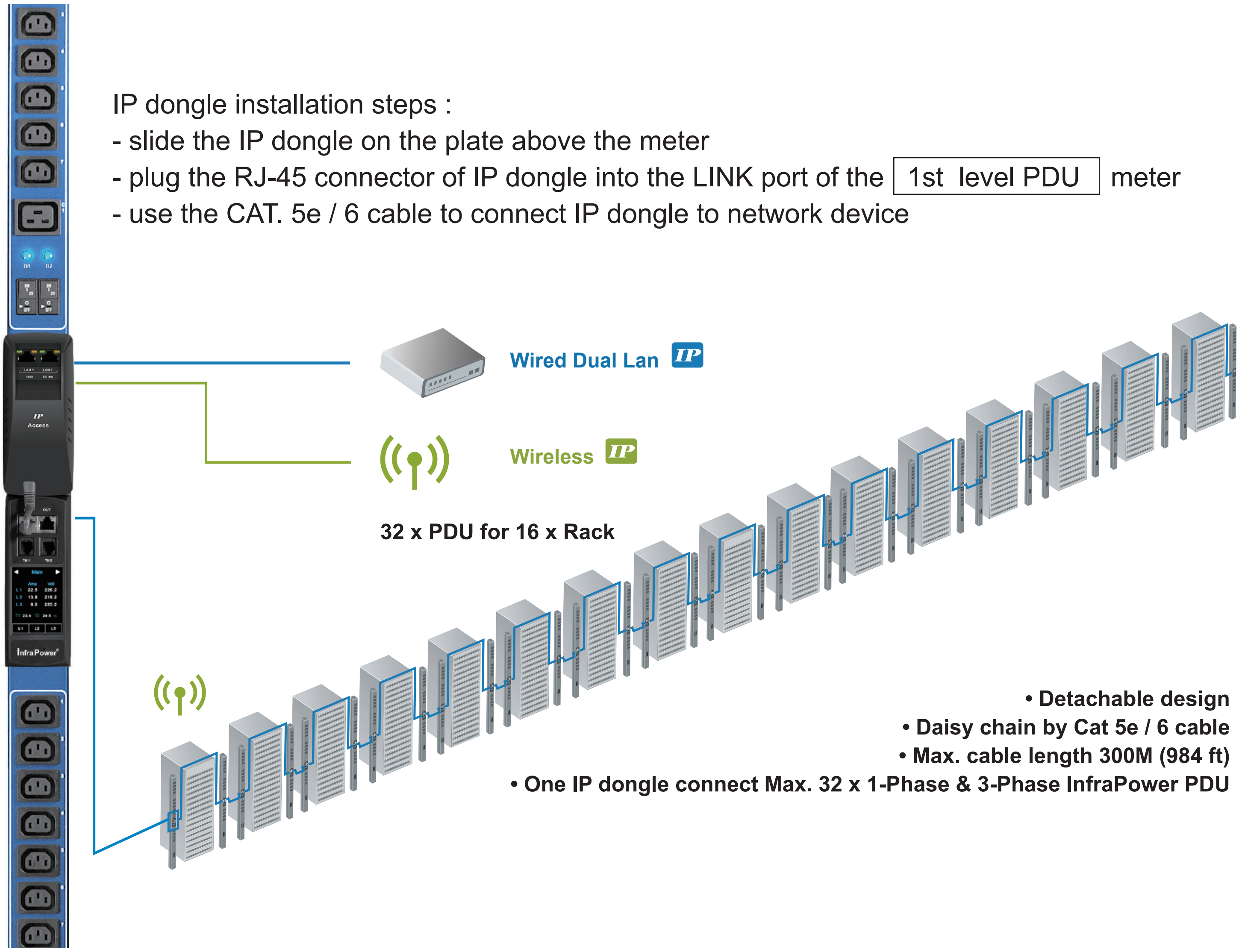
Remote Management Protocols

> HTTP(S); SSH Command Line Interface; Telnet; SMTP; IPv6/IPv4

< 1.2 > IP Dongle Installation & Meter (PDU) Cascade

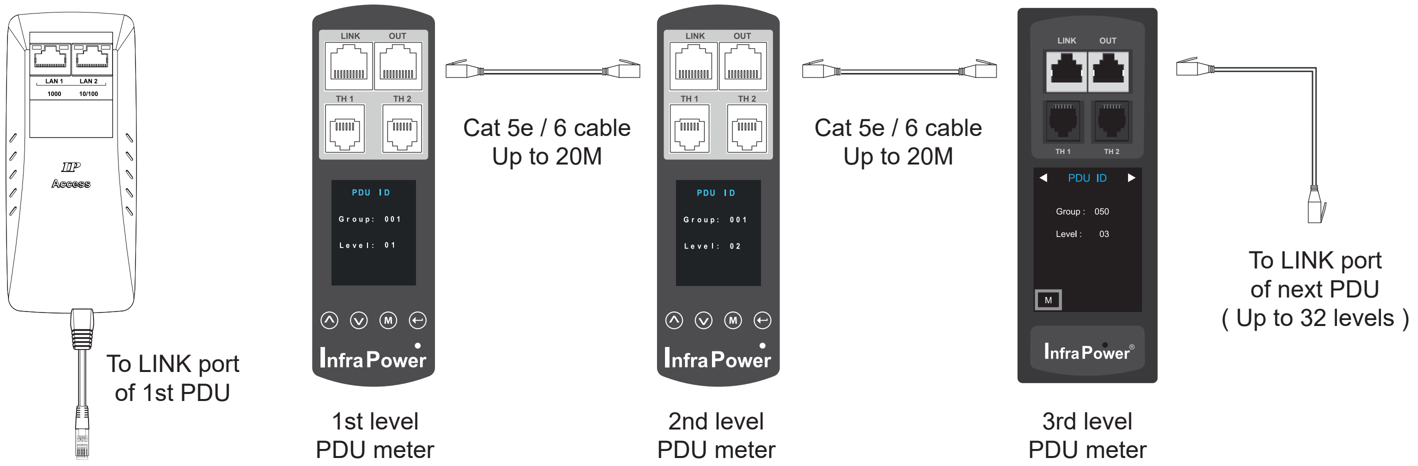
IP dongle installation steps :

- slide the IP dongle on the plate above the meter
- plug the RJ-45 connector of IP dongle into the LINK port of the 1st level PDU meter
- use the CAT. 5e / 6 cable to connect IP dongle to network device



32 x PDU for 16 x Rack

- Detachable design
- Daisy chain by Cat 5e / 6 cable
- Max. cable length 300M (984 ft)
- One IP dongle connect Max. 32 x 1-Phase & 3-Phase InfraPower PDU



To LINK port of 1st PDU

Cat 5e / 6 cable Up to 20M

Cat 5e / 6 cable Up to 20M

To LINK port of next PDU (Up to 32 levels)

1st level PDU meter

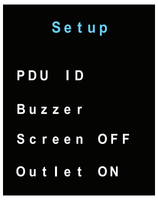
2nd level PDU meter

3rd level PDU meter

< 1.3 > Meter (PDU) Level Setting

(I) For 1.8" LCD Meter (No touchscreen function)

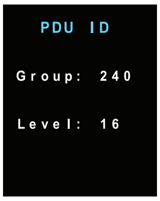
Display 9



Step 1 - Press the ∧ & ∨ button to display no.9 and press Ⓜ to confirm

Step 2 - Press the ∧ & ∨ button to PDU ID and press Ⓜ to confirm

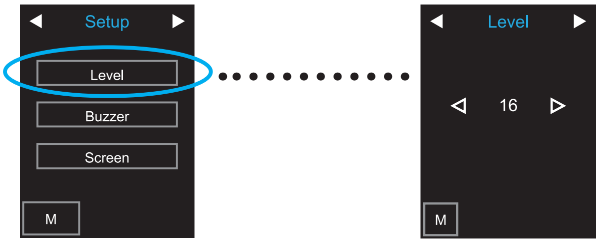
Display 9.1



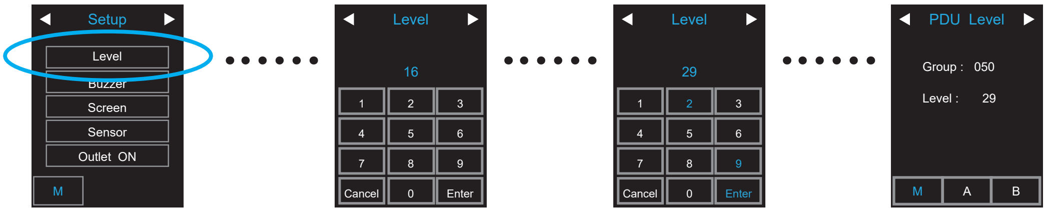
Step 3 - In display 9.1, Press the ∧ & ∨ button to select PDU level no. & press Ⓜ to confirm

Step 4 - Press ← to exit

(II) For 2.8" LCD Meter (With touchscreen function)



(III) For 2.8" LCD Meter (With touchscreen function)



⚠ For PDU with firmware version V37 or above

< 1.4 > IP Dongle Configuration

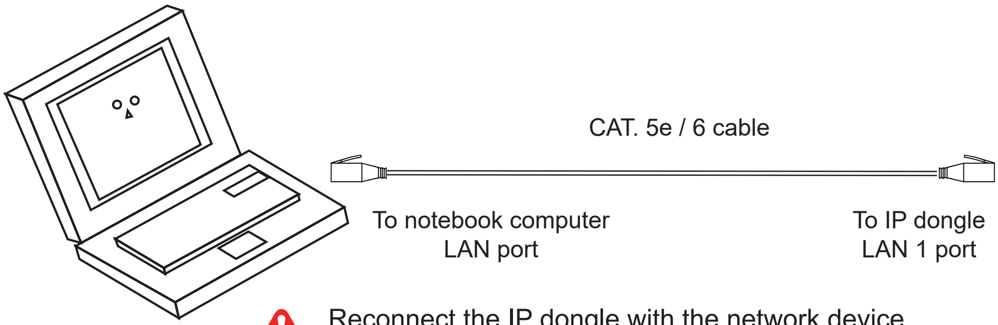
The following steps show the static IP setting only. For DHCP setting, please refer to < **1.14** > DHCP Setting

After the completion of IP dongle connection, please take the following steps to configure the IP dongle :

Step 1. Prepare a notebook computer to download the IP setup utilities from the link :
http://www.austin-hughes.com/support/utilities/infrapower/IPdongleSetup.msi

Step 2. Double Click the IPDongleSetup.msi and follow the instruction to complete the installation

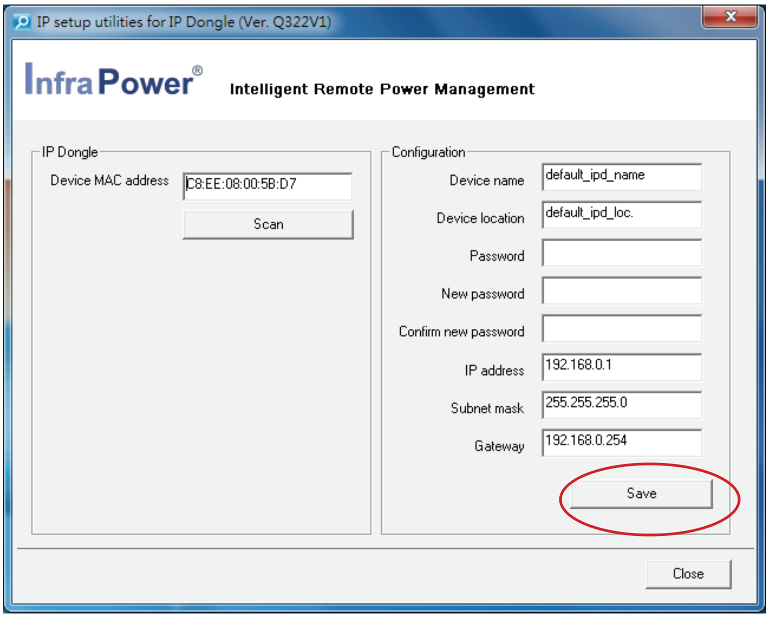
Step 3. Go to each first level PDU with the notebook computer & a piece of CAT. 5e / 6 cable to configure the **LAN 1 Port** of the IP dongle by IP setup utilities as below. Please take the procedure for all IP dongles **ONE BY ONE**



IP dongle on 1st level PDU

Ensure the PDU in power ON status

Reconnect the IP dongle with the network device (router or hub), after finish IP dongle configuration.



IP setup utilities for IP Dongle (Ver. Q322V1)

InfraPower® Intelligent Remote Power Management

IP Dongle
Device MAC address: C8:EE:08:00:5B:D7
Scan

Configuration
Device name: default_ipd_name
Device location: default_ipd_loc.
Password:
New password:
Confirm new password:
IP address: 192.168.0.1
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Save

Close

1. If the IP dongle is in factory default setting or the password is " 00000000 ", you MUST change the password for security purpose .
2. The password MUST contain at least three of the following four character groups :
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Numerals (0 through 9)
   - Non-alphabetic characters (such as !, @, #, %). [`] , [$] , ["] , [\ ] are NOT supported.
3. Device name NOT EQUAL to the Login name of IP Dongle WEBUI (PPS-03-S). To change Login name, please refer to < 1.10 > Login for details.

Step 4. Click " **Scan** " to search the connected IP dongle

Step 5. Enter device name in " **Device name** " (min. 4 char. / max. 16 char.). Default is " **default_ipd_name** "

Step 6. Enter device location in " **Device location** " (min. 4 char. / max. 16 char.). Default is " **default_ipd_loc.** "

Step 7. Enter password in " **Password** " for authentication (min. 8 char. / max. 16 char.) Default is **" 00000000 "**

Step 8. Enter new password in " **New password** " (min. 8 char. / max. 16 char.)

Step 9. Re-enter new password in " **Confirm new password** "

Step 10. Change the desired " **IP address** " / " **Subnet mask** " / " **Gateway** ", then Click **" Save "** to confirm the changes

Lan 1. The default IP setting is as below:

IP address :	192.168.11.1
Subnet mask :	255.255.255.0
Gateway :	192.168.11.254

Lan 2. The default IP setting is as below:

IP address :	192.168.0.1
Subnet mask :	255.255.255.0
Gateway :	192.168.0.254

Step 11. Repeat **Step 4 & Step 10** for **Lan 2** Port of IP dongle if you will use LAN 2 as well. Otherwise, ignore this step.

< 1.5 > Remote PDU Level & ID Setting

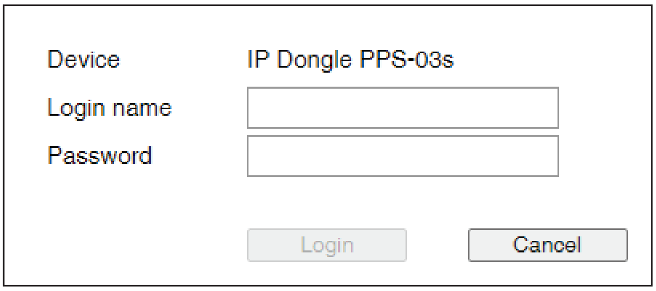
InfraPower Manager PPS-03-S provides a convenient way to set the PDU level. You can set the PDU level remotely via the IP Dongle WEBUI. Please follow the steps below to complete the Remote PDU level setting.

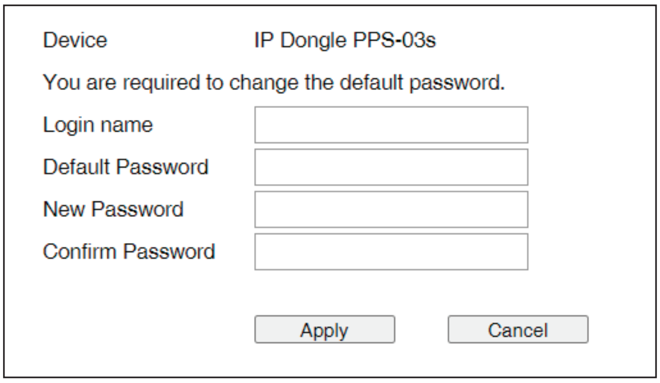
⚠ ONLY PDU with 2.8” LCD meter (firmware version V37 or above) supports this functions

⚠ You MUST have the PDU serial number onhand and know which rack the PDU is installed.

Step 1. Open MS Edge

Step 2. Enter the configured IP Dongle address into the address bar.
Default IP address of LAN 1 is “ **192.168.11.1** “
Default IP address of LAN 2 is “ **192.168.0.1** “

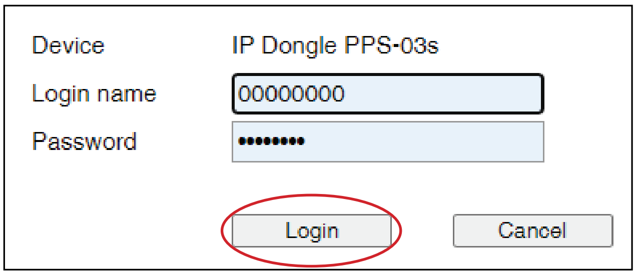

Device IP Dongle PPS-03s
Login name
Password


Device IP Dongle PPS-03s
You are required to change the default password.
Login name
Default Password
New Password
Confirm Password

⚠

- If the IP dongle is in factory default setting or the password is “ 00000000 “. This window will be shown and you MUST change the “ Password “ before you can login the IP dongle WEBUI.

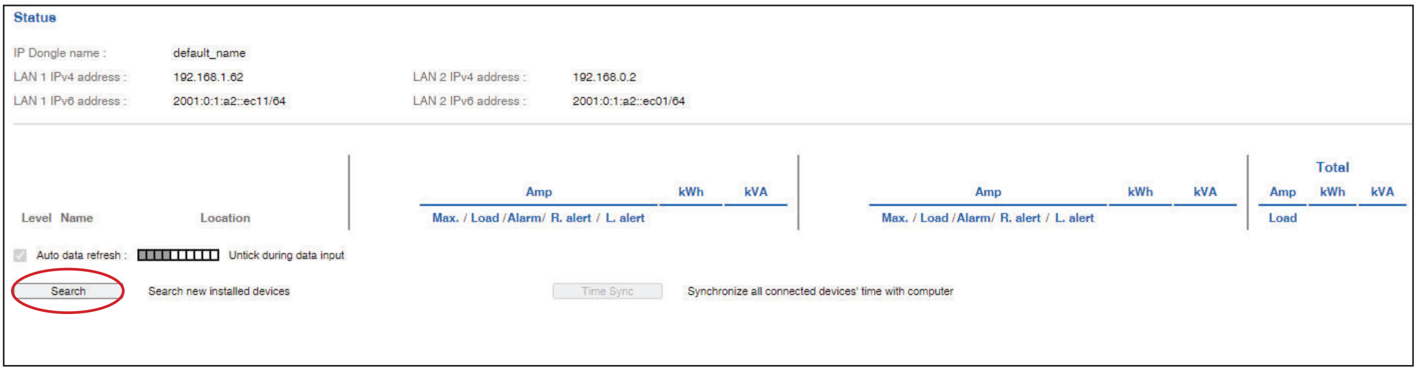
Step 3. Enter the “ **Login name** “ and “ **Password** “ & Click “ **Login** “


Device IP Dongle PPS-03s
Login name 00000000
Password ••••••••

⚠

- Default login name: 00000000
- Password: the one you set in Step 7 of < 1.4 > IP Dongle Configuration.
- The login account will be LOCKED for 5 minutes if three unsuccessful login attempts to the IP dongle WEBUI.

Step 4. In < Status >, Click “ **Search** “ to start the PDU searching


Status

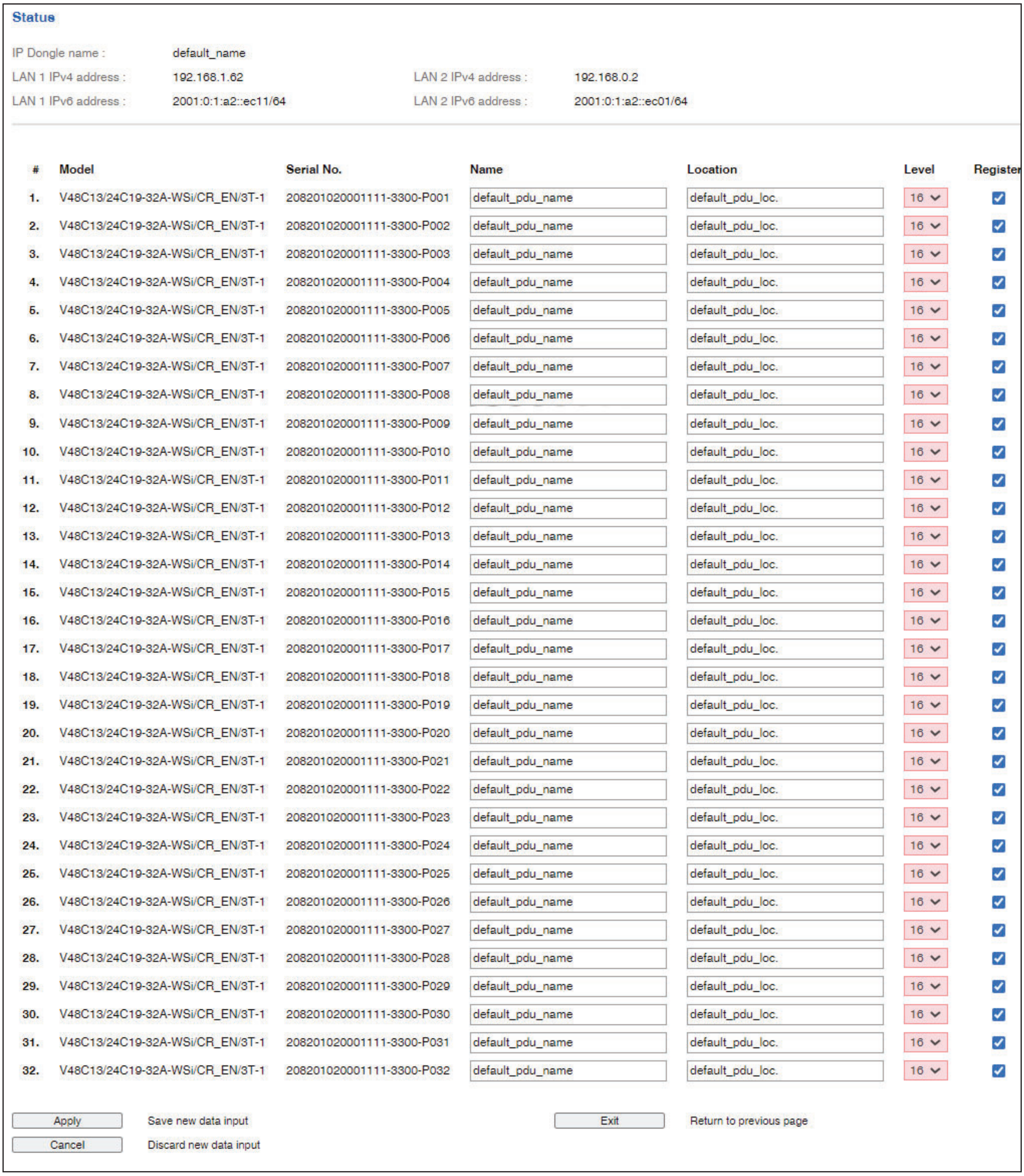
IP Dongle name : default_name
LAN 1 IPv4 address : 192.168.1.62 LAN 2 IPv4 address : 192.168.0.2
LAN 1 IPv6 address : 2001:0:1:a2::ec11/64 LAN 2 IPv6 address : 2001:0:1:a2::ec01/64

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

☑ Auto data refresh : Untick during data input
Search — Search new installed devices
Time Sync — Synchronize all connected devices' time with computer

< 1.5 > Remote PDU Level & ID Setting

Step 5. After the searching is completed, the following screen will display



Status

IP Dongle name : default_name

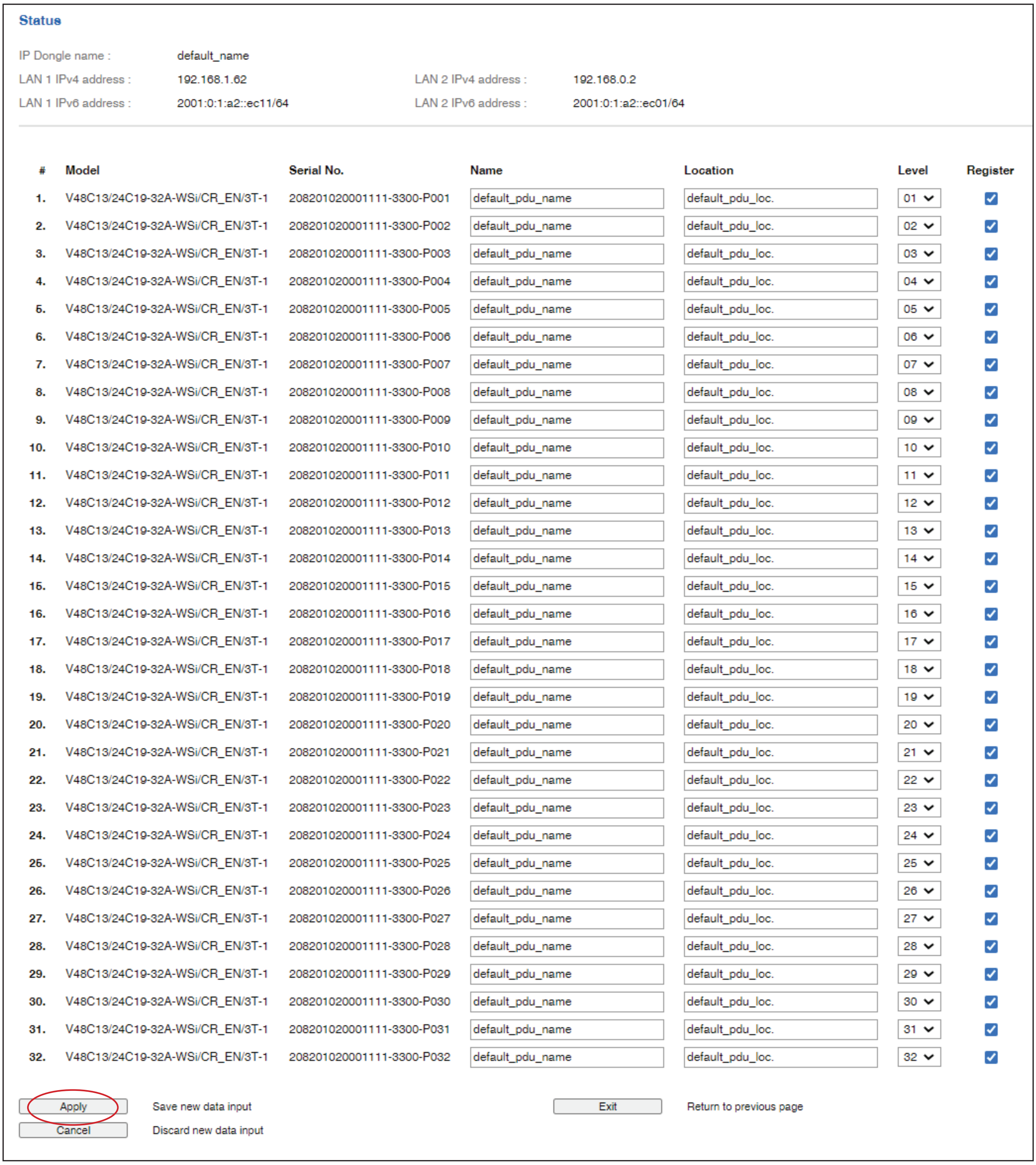
LAN 1 IPv4 address : 192.168.1.62 LAN 2 IPv4 address : 192.168.0.2

LAN 1 IPv6 address : 2001:0:1:a2::ec11/64 LAN 2 IPv6 address : 2001:0:1:a2::ec01/64

#	Model	Serial No.	Name	Location	Level	Register
1.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P001	default_pdu_name	default_pdu_loc.	16	☑
2.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P002	default_pdu_name	default_pdu_loc.	16	☑
3.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P003	default_pdu_name	default_pdu_loc.	16	☑
4.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P004	default_pdu_name	default_pdu_loc.	16	☑
5.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P005	default_pdu_name	default_pdu_loc.	16	☑
6.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P006	default_pdu_name	default_pdu_loc.	16	☑
7.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P007	default_pdu_name	default_pdu_loc.	16	☑
8.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P008	default_pdu_name	default_pdu_loc.	16	☑
9.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P009	default_pdu_name	default_pdu_loc.	16	☑
10.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P010	default_pdu_name	default_pdu_loc.	16	☑
11.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P011	default_pdu_name	default_pdu_loc.	16	☑
12.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P012	default_pdu_name	default_pdu_loc.	16	☑
13.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P013	default_pdu_name	default_pdu_loc.	16	☑
14.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P014	default_pdu_name	default_pdu_loc.	16	☑
15.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P015	default_pdu_name	default_pdu_loc.	16	☑
16.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P016	default_pdu_name	default_pdu_loc.	16	☑
17.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P017	default_pdu_name	default_pdu_loc.	16	☑
18.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P018	default_pdu_name	default_pdu_loc.	16	☑
19.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P019	default_pdu_name	default_pdu_loc.	16	☑
20.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P020	default_pdu_name	default_pdu_loc.	16	☑
21.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P021	default_pdu_name	default_pdu_loc.	16	☑
22.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P022	default_pdu_name	default_pdu_loc.	16	☑
23.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P023	default_pdu_name	default_pdu_loc.	16	☑
24.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P024	default_pdu_name	default_pdu_loc.	16	☑
25.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P025	default_pdu_name	default_pdu_loc.	16	☑
26.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P026	default_pdu_name	default_pdu_loc.	16	☑
27.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P027	default_pdu_name	default_pdu_loc.	16	☑
28.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P028	default_pdu_name	default_pdu_loc.	16	☑
29.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P029	default_pdu_name	default_pdu_loc.	16	☑
30.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P030	default_pdu_name	default_pdu_loc.	16	☑
31.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P031	default_pdu_name	default_pdu_loc.	16	☑
32.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P032	default_pdu_name	default_pdu_loc.	16	☑

< 1.5 > Remote PDU Level & ID Setting

Step 6. Assign a unique “ **Level** “ , “ **Name** “ and “ **Location** “ to each PDU and ensure to check the register box. Then Click “ **Apply** “.



Status

IP Dongle name : default_name

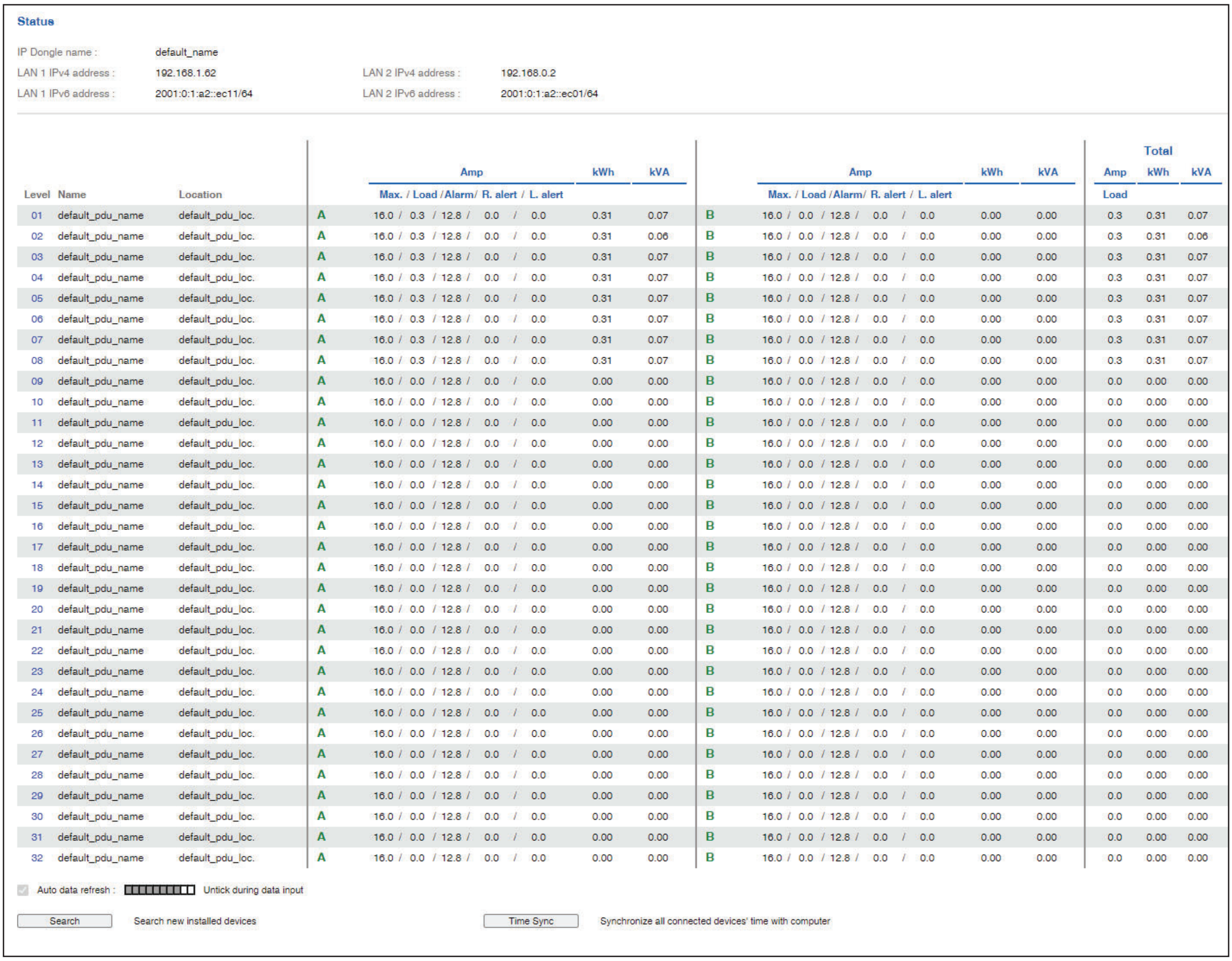
LAN 1 IPv4 address : 192.168.1.62 LAN 2 IPv4 address : 192.168.0.2

LAN 1 IPv6 address : 2001:0:1:a2::ec11/64 LAN 2 IPv6 address : 2001:0:1:a2::ec01/64

#	Model	Serial No.	Name	Location	Level	Register
1.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P001	default_pdu_name	default_pdu_loc.	01	☑
2.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P002	default_pdu_name	default_pdu_loc.	02	☑
3.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P003	default_pdu_name	default_pdu_loc.	03	☑
4.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P004	default_pdu_name	default_pdu_loc.	04	☑
5.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P005	default_pdu_name	default_pdu_loc.	05	☑
6.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P006	default_pdu_name	default_pdu_loc.	06	☑
7.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P007	default_pdu_name	default_pdu_loc.	07	☑
8.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P008	default_pdu_name	default_pdu_loc.	08	☑
9.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P009	default_pdu_name	default_pdu_loc.	09	☑
10.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P010	default_pdu_name	default_pdu_loc.	10	☑
11.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P011	default_pdu_name	default_pdu_loc.	11	☑
12.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P012	default_pdu_name	default_pdu_loc.	12	☑
13.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P013	default_pdu_name	default_pdu_loc.	13	☑
14.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P014	default_pdu_name	default_pdu_loc.	14	☑
15.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P015	default_pdu_name	default_pdu_loc.	15	☑
16.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P016	default_pdu_name	default_pdu_loc.	16	☑
17.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P017	default_pdu_name	default_pdu_loc.	17	☑
18.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P018	default_pdu_name	default_pdu_loc.	18	☑
19.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P019	default_pdu_name	default_pdu_loc.	19	☑
20.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P020	default_pdu_name	default_pdu_loc.	20	☑
21.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P021	default_pdu_name	default_pdu_loc.	21	☑
22.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P022	default_pdu_name	default_pdu_loc.	22	☑
23.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P023	default_pdu_name	default_pdu_loc.	23	☑
24.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P024	default_pdu_name	default_pdu_loc.	24	☑
25.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P025	default_pdu_name	default_pdu_loc.	25	☑
26.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P026	default_pdu_name	default_pdu_loc.	26	☑
27.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P027	default_pdu_name	default_pdu_loc.	27	☑
28.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P028	default_pdu_name	default_pdu_loc.	28	☑
29.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P029	default_pdu_name	default_pdu_loc.	29	☑
30.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P030	default_pdu_name	default_pdu_loc.	30	☑
31.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P031	default_pdu_name	default_pdu_loc.	31	☑
32.	V48C13/24C19-32A-WSi/CR_EN/3T-1	208201020001111-3300-P032	default_pdu_name	default_pdu_loc.	32	☑

< 1.5 >   Remote PDU Level & ID Setting

Step 7.   After the PDU level setting is complete, “ **Status** “ page will display the PDU with proper level.



Status

IP Dongle name : default_name

LAN 1 IPv4 address : 192.168.1.62   LAN 2 IPv4 address : 192.168.0.2

LAN 1 IPv6 address : 2001:0:1:a2::ec11/64   LAN 2 IPv6 address : 2001:0:1:a2::ec01/64

												Total	
				Amp	kWh	kVA		Amp	kWh	kVA	Amp	kWh	kVA
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.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
02	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.06	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.06
03	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
04	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
05	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
06	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
07	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
08	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
09	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
10	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
11	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
12	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
13	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
14	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
15	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
16	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
17	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
18	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
19	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
20	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
21	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
22	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
23	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
24	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
25	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
26	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
27	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
28	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
29	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
30	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
31	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
32	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00

☑ Auto data refresh : Untick during data input

Search new installed devices

Synchronize all connected devices' time with computer

< 1.6 > PPS-03-S IP Dongle GUI

Each IP dongle (IPD-03-S) provides a **FREE** built-in GUI , PPS-03-S, which allows user, via a web browser, to see PDU's data and remotely manage the PDU over a TCP / IP Ethernet network.

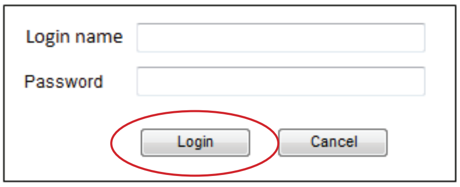
Each web browser window supports only one IP dongle (IPD-03-S). If user installs more IP dongles, multi windows will be required

PPS-03-S is a management software with very limited features. User can use more advanced software, InfraPower Manager IPM-04

Step 1. Open MS Edge

Step 2. Enter the configured IP dongle address into the address bar (Please refer to < 1.4 > IP dongle configuration)
Default IP address of LAN 1 is " **192.168.11.1** "
Default IP address of LAN 2 is " **192.168.0.1** "

Step 3. Enter " **Login name** " , " **Password** " & Click " **Login** "

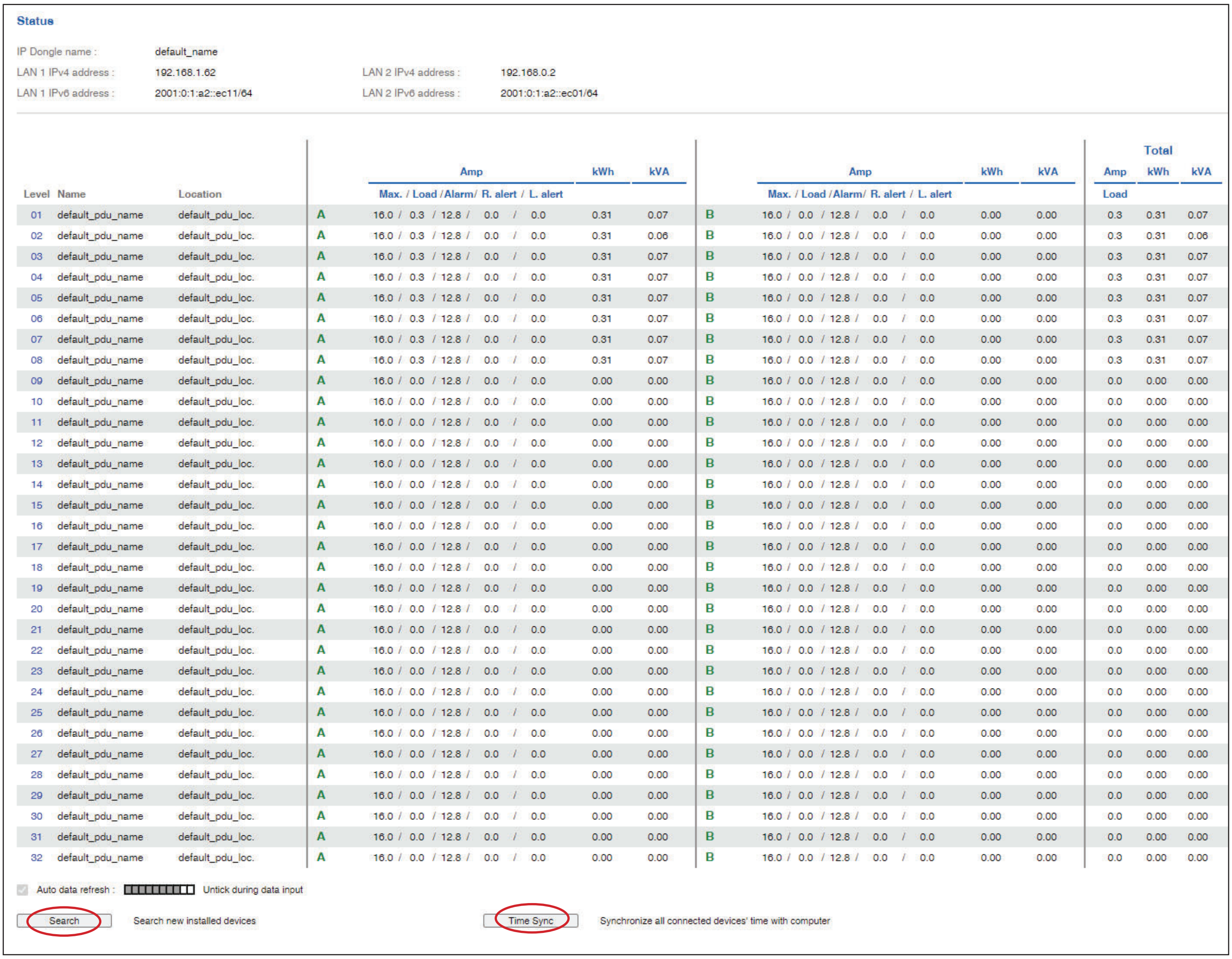


Login name
Password

- Default login name: 00000000
- Password: the one you set in Step 7 of < 1.4 > IP Dongle Configuration.

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
- View status of Door / Smoke sensors connected to each PDU
- Click " **Time Sync** " update all connected PDU's real time clock from the computer logged in the IP Dongle



Status

IP Dongle name :	default_name
LAN 1 IPv4 address :	192.168.1.62
LAN 1 IPv6 address :	2001:0:1:a2::ec11/64
LAN 2 IPv4 address :	192.168.0.2
LAN 2 IPv6 address :	2001:0:1:a2::ec01/64

				Amp	kWh	kVA		Amp	kWh	kVA	Total Amp	Total kWh	Total kVA
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.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
02	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.06	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.06
03	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
04	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
05	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
06	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
07	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
08	default_pdu_name	default_pdu_loc.	A	16.0 / 0.3 / 12.8 / 0.0 / 0.0	0.31	0.07	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.3	0.31	0.07
09	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
10	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
11	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
12	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
13	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
14	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
15	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
16	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
17	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
18	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
19	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
20	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
21	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
22	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
23	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
24	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
25	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
26	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
27	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
28	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
29	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
30	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
31	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00
32	default_pdu_name	default_pdu_loc.	A	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	B	16.0 / 0.0 / 12.8 / 0.0 / 0.0	0.00	0.00	0.0	0.00	0.00

☑ Auto data refresh : Untick during data input

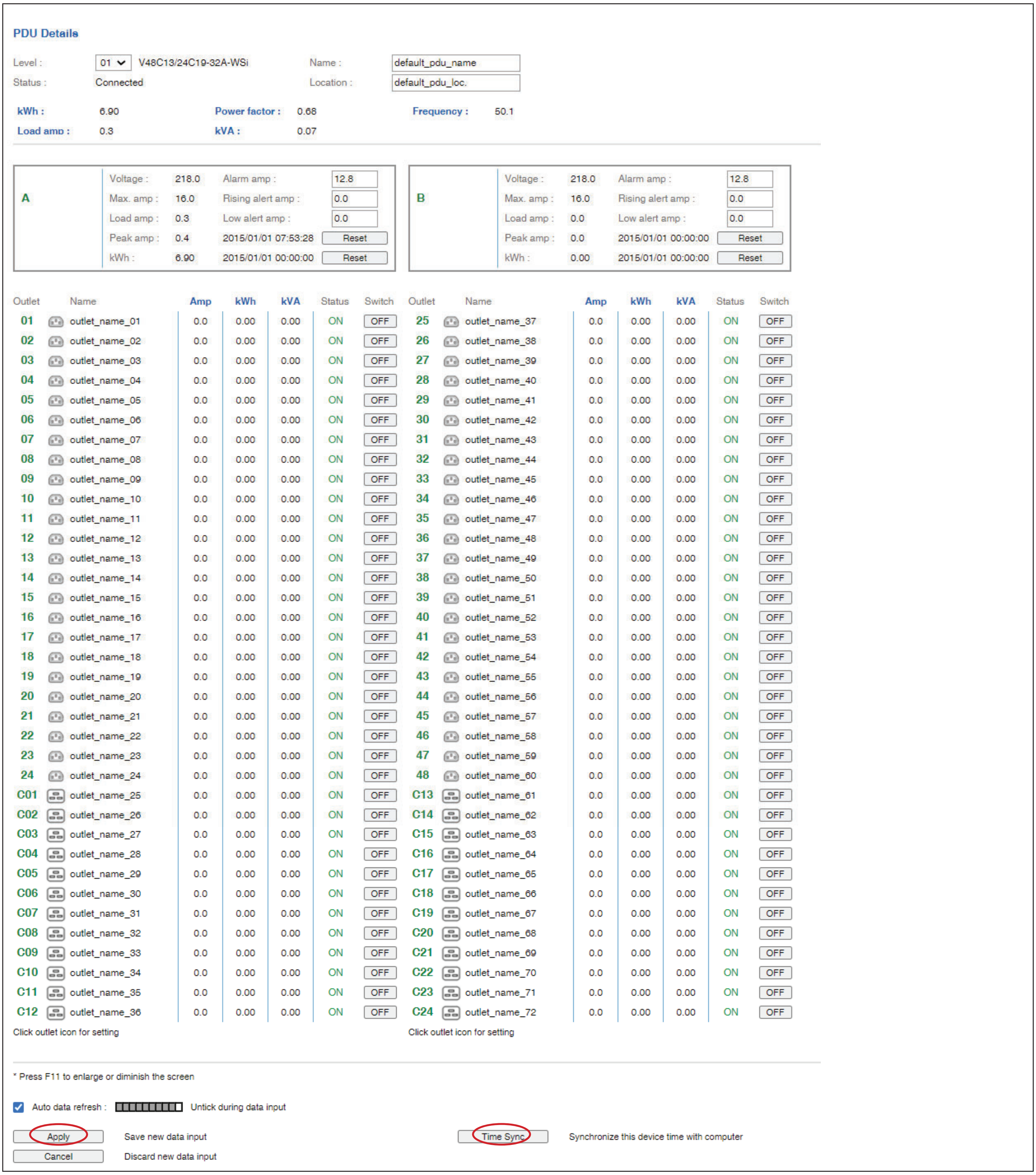
Search new installed devices

Synchronize all connected devices' time with computer

< 1.6 > PPS-03-S IP Dongle GUI

In < **Details** >,

- Change “ **Name** ” and “ **Location** ” of PDU & Click “ **Apply** ”
- Change “ **Alarm 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 logged in the IP Dongle



PDU Details

Level :	01	V48C13/24C19-32A-WSi	Name :	default_pdu_name
Status :	Connected		Location :	default_pdu_loc.

kWh :	6.90	Power factor :	0.68	Frequency :	50.1
Load amp :	0.3	kVA :	0.07		

A	Voltage :	218.0	Alarm amp :	12.8
	Max. amp :	16.0	Rising alert amp :	0.0
	Load amp :	0.3	Low alert amp :	0.0
	Peak amp :	0.4	2015/01/01 07:53:28	Reset
	kWh :	6.90	2015/01/01 00:00:00	Reset

B	Voltage :	218.0	Alarm amp :	12.8
	Max. amp :	16.0	Rising alert amp :	0.0
	Load amp :	0.0	Low alert amp :	0.0
	Peak amp :	0.0	2015/01/01 00:00:00	Reset
	kWh :	0.00	2015/01/01 00:00:00	Reset

Outlet	Name	Amp	kWh	kVA	Status	Switch	Outlet	Name	Amp	kWh	kVA	Status	Switch
01	outlet_name_01	0.0	0.00	0.00	ON	OFF	25	outlet_name_37	0.0	0.00	0.00	ON	OFF
02	outlet_name_02	0.0	0.00	0.00	ON	OFF	26	outlet_name_38	0.0	0.00	0.00	ON	OFF
03	outlet_name_03	0.0	0.00	0.00	ON	OFF	27	outlet_name_39	0.0	0.00	0.00	ON	OFF
04	outlet_name_04	0.0	0.00	0.00	ON	OFF	28	outlet_name_40	0.0	0.00	0.00	ON	OFF
05	outlet_name_05	0.0	0.00	0.00	ON	OFF	29	outlet_name_41	0.0	0.00	0.00	ON	OFF
06	outlet_name_06	0.0	0.00	0.00	ON	OFF	30	outlet_name_42	0.0	0.00	0.00	ON	OFF
07	outlet_name_07	0.0	0.00	0.00	ON	OFF	31	outlet_name_43	0.0	0.00	0.00	ON	OFF
08	outlet_name_08	0.0	0.00	0.00	ON	OFF	32	outlet_name_44	0.0	0.00	0.00	ON	OFF
09	outlet_name_09	0.0	0.00	0.00	ON	OFF	33	outlet_name_45	0.0	0.00	0.00	ON	OFF
10	outlet_name_10	0.0	0.00	0.00	ON	OFF	34	outlet_name_46	0.0	0.00	0.00	ON	OFF
11	outlet_name_11	0.0	0.00	0.00	ON	OFF	35	outlet_name_47	0.0	0.00	0.00	ON	OFF
12	outlet_name_12	0.0	0.00	0.00	ON	OFF	36	outlet_name_48	0.0	0.00	0.00	ON	OFF
13	outlet_name_13	0.0	0.00	0.00	ON	OFF	37	outlet_name_49	0.0	0.00	0.00	ON	OFF
14	outlet_name_14	0.0	0.00	0.00	ON	OFF	38	outlet_name_50	0.0	0.00	0.00	ON	OFF
15	outlet_name_15	0.0	0.00	0.00	ON	OFF	39	outlet_name_51	0.0	0.00	0.00	ON	OFF
16	outlet_name_16	0.0	0.00	0.00	ON	OFF	40	outlet_name_52	0.0	0.00	0.00	ON	OFF
17	outlet_name_17	0.0	0.00	0.00	ON	OFF	41	outlet_name_53	0.0	0.00	0.00	ON	OFF
18	outlet_name_18	0.0	0.00	0.00	ON	OFF	42	outlet_name_54	0.0	0.00	0.00	ON	OFF
19	outlet_name_19	0.0	0.00	0.00	ON	OFF	43	outlet_name_55	0.0	0.00	0.00	ON	OFF
20	outlet_name_20	0.0	0.00	0.00	ON	OFF	44	outlet_name_56	0.0	0.00	0.00	ON	OFF
21	outlet_name_21	0.0	0.00	0.00	ON	OFF	45	outlet_name_57	0.0	0.00	0.00	ON	OFF
22	outlet_name_22	0.0	0.00	0.00	ON	OFF	46	outlet_name_58	0.0	0.00	0.00	ON	OFF
23	outlet_name_23	0.0	0.00	0.00	ON	OFF	47	outlet_name_59	0.0	0.00	0.00	ON	OFF
24	outlet_name_24	0.0	0.00	0.00	ON	OFF	48	outlet_name_60	0.0	0.00	0.00	ON	OFF
C01	outlet_name_25	0.0	0.00	0.00	ON	OFF	C13	outlet_name_61	0.0	0.00	0.00	ON	OFF
C02	outlet_name_26	0.0	0.00	0.00	ON	OFF	C14	outlet_name_62	0.0	0.00	0.00	ON	OFF
C03	outlet_name_27	0.0	0.00	0.00	ON	OFF	C15	outlet_name_63	0.0	0.00	0.00	ON	OFF
C04	outlet_name_28	0.0	0.00	0.00	ON	OFF	C16	outlet_name_64	0.0	0.00	0.00	ON	OFF
C05	outlet_name_29	0.0	0.00	0.00	ON	OFF	C17	outlet_name_65	0.0	0.00	0.00	ON	OFF
C06	outlet_name_30	0.0	0.00	0.00	ON	OFF	C18	outlet_name_66	0.0	0.00	0.00	ON	OFF
C07	outlet_name_31	0.0	0.00	0.00	ON	OFF	C19	outlet_name_67	0.0	0.00	0.00	ON	OFF
C08	outlet_name_32	0.0	0.00	0.00	ON	OFF	C20	outlet_name_68	0.0	0.00	0.00	ON	OFF
C09	outlet_name_33	0.0	0.00	0.00	ON	OFF	C21	outlet_name_69	0.0	0.00	0.00	ON	OFF
C10	outlet_name_34	0.0	0.00	0.00	ON	OFF	C22	outlet_name_70	0.0	0.00	0.00	ON	OFF
C11	outlet_name_35	0.0	0.00	0.00	ON	OFF	C23	outlet_name_71	0.0	0.00	0.00	ON	OFF
C12	outlet_name_36	0.0	0.00	0.00	ON	OFF	C24	outlet_name_72	0.0	0.00	0.00	ON	OFF

Click outlet icon for setting

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

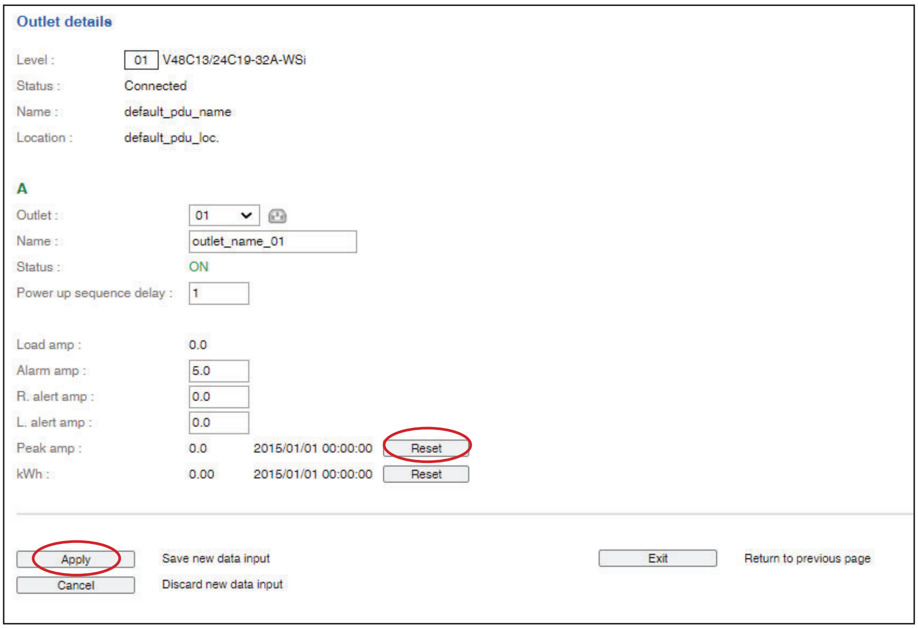
< 1.6 > PPS-03-S IP Dongle GUI

In < **Outlet setting** >,

- Change PDU's outlet name
- Change " **Power up sequence delay** " of PDU's outlet (Switched PDU only)
- Change " **Alarm amp.** ", " **Rising Alert amp.**" & " **Low alert amp.** " of PDU's outlet (Outlet Measurement PDU only)

⚠ Click " **Apply** " to finish the above settings

- Click " **Reset** " to reset peak amp. or kWh of PDU's outlet (Outlet Measurement PDU only)



Outlet details

Level : 01 V48C13/24C19-32A-WSi

Status : Connected

Name : default_pdu_name

Location : default_pdu_loc.

A

Outlet : 01

Name : outlet_name_01

Status : ON

Power up sequence delay : 1

Load amp : 0.0

Alarm amp : 5.0

R. alert amp : 0.0

L. alert amp : 0.0

Peak amp : 0.0 2015/01/01 00:00:00 Reset

kWh : 0.00 2015/01/01 00:00:00 Reset

Apply Save new data input

Cancel Discard new data input

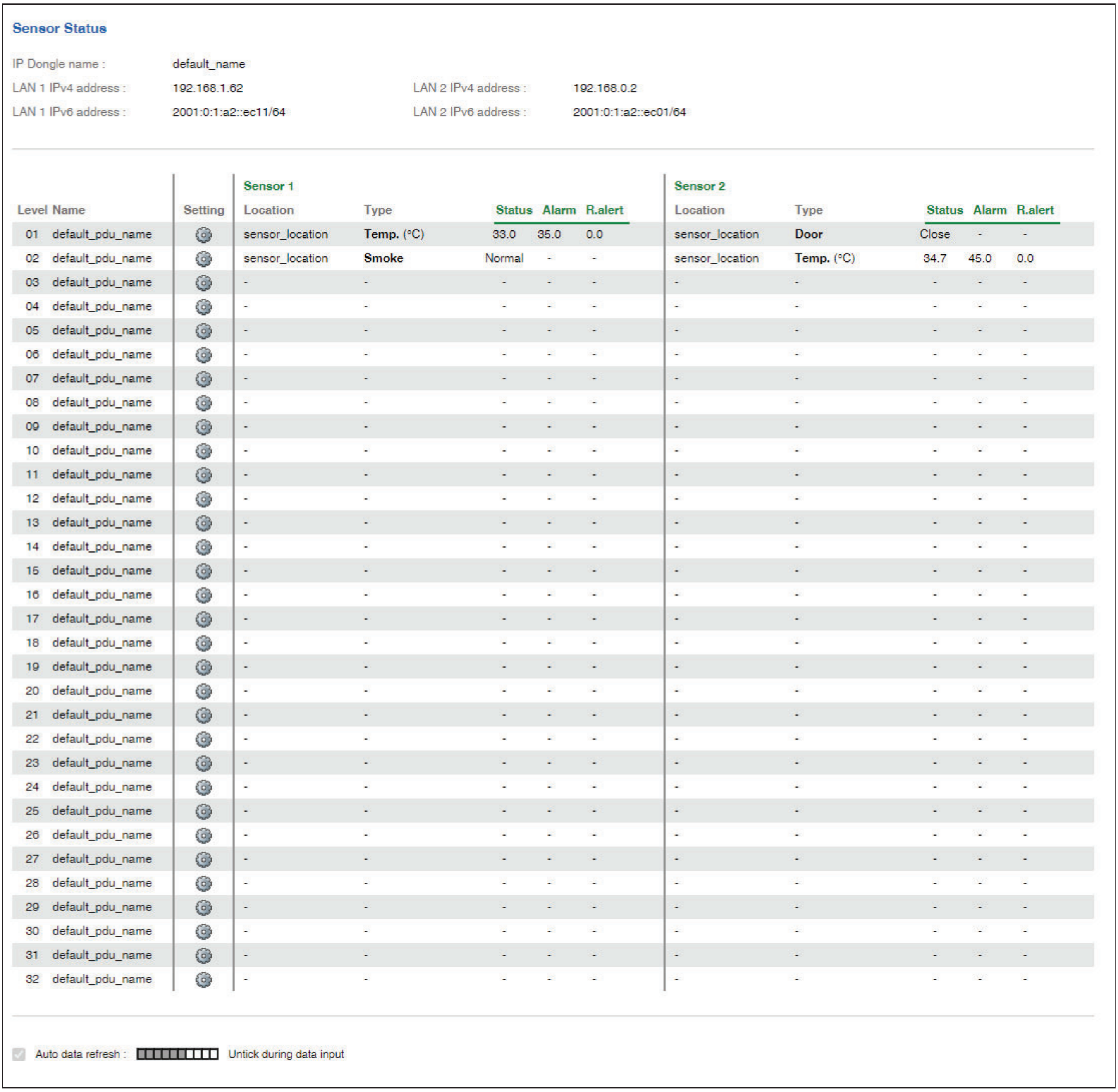
Exit Return to previous page

< 1.6 > PPS-03-S IP Dongle GUI

In < **Sensor Status** >,

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

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



Sensor Status

IP Dongle name : default_name

LAN 1 IPv4 address : 192.168.1.62 LAN 2 IPv4 address : 192.168.0.2

LAN 1 IPv6 address : 2001:0:1:a2::ec11/64 LAN 2 IPv6 address : 2001:0:1:a2::ec01/64

			Sensor 1					Sensor 2				
Level	Name	Setting	Location	Type	Status	Alarm	R.alert	Location	Type	Status	Alarm	R.alert
01	default_pdu_name	⚙	sensor_location	**Temp.** (°C)	33.0	35.0	0.0	sensor_location	**Door**	Close	-	-
02	default_pdu_name	⚙	sensor_location	**Smoke**	Normal	-	-	sensor_location	**Temp.** (°C)	34.7	45.0	0.0
03	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
04	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
05	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
06	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
07	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
08	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
09	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
10	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
11	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
12	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
13	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
14	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
15	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
16	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
17	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
18	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
19	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
20	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
21	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
22	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
23	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
24	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
25	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
26	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
27	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
28	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
29	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
30	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
31	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-
32	default_pdu_name	⚙	-	-	-	-	-	-	-	-	-	-

☑ Auto data refresh : ▮▮▮▮▮▮▮▯▯▯ Untick during data input

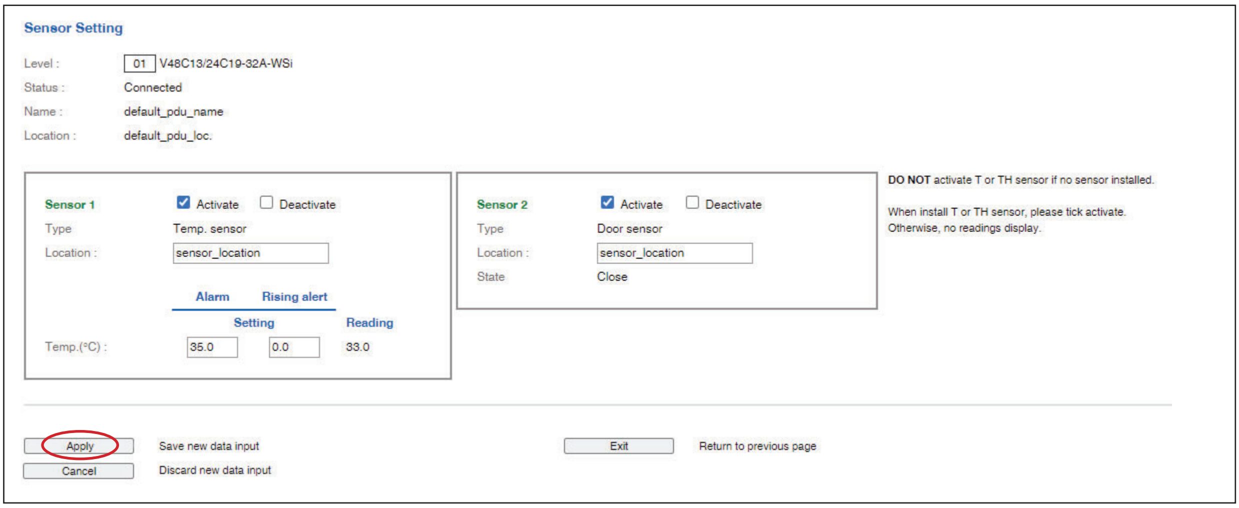
< 1.6 > PPS-03-S IP Dongle GUI

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
- Change " **Location** " of Door sensor & Smoke sensor

⚠ If no any sensor connected, NEVER activate.



Sensor Setting

Level :	01 V48C13/24C19-32A-WSi
Status :	Connected
Name :	default_pdu_name
Location :	default_pdu_loc.

Sensor 1 ☑ Activate ☐ Deactivate

Type: Temp. sensor

Location : sensor_location

	Alarm Setting	Rising alert Setting	Reading
Temp.(°C) :	35.0	0.0	33.0

Sensor 2 ☑ Activate ☐ Deactivate

Type: Door sensor

Location : sensor_location

State: Close

DO NOT activate T or TH sensor if no sensor installed.

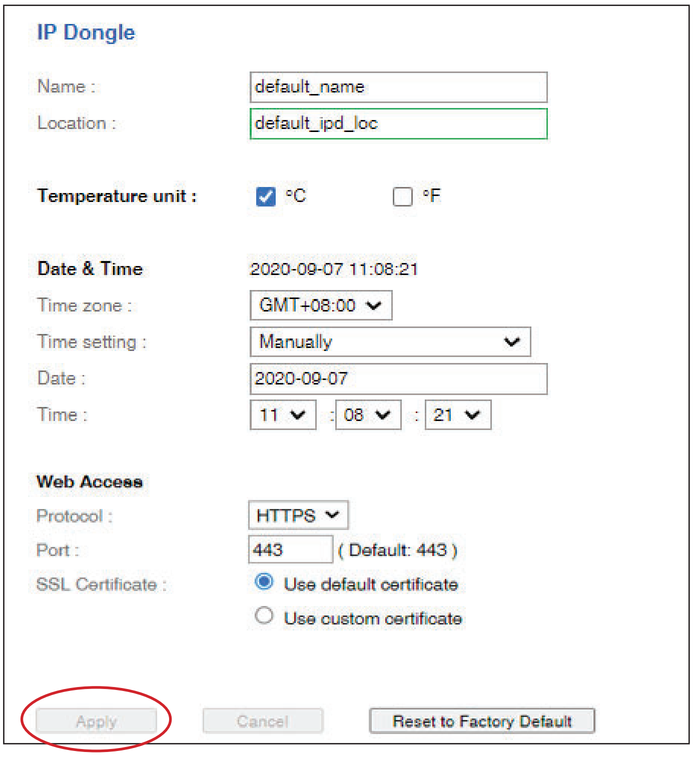
When install T or TH sensor, please tick activate. Otherwise, no readings display.

Apply	Save new data input
Cancel	Discard new data input
Exit	Return to previous page

< 1.7 > System

In < **System** >,

- Change IP dongle name & location
- Change temperature unit displayed in UI
- Set the “ **Date & Time** “ of the IP dongle (by **“ Manually “** or **“ NTP server “**). Default is **“ Manually “**
- Tick **“ Force HTTPS ”** to provide data transmission security. Default Web Access is **“ HTTP “**
- Click “ **Apply** ” to finish the above settings



IP Dongle

Name : default_name

Location : default_ipd_loc

Temperature unit : ☑ °C □ °F

Date & Time 2020-09-07 11:08:21

Time zone : GMT+08:00

Time setting : Manually

Date : 2020-09-07

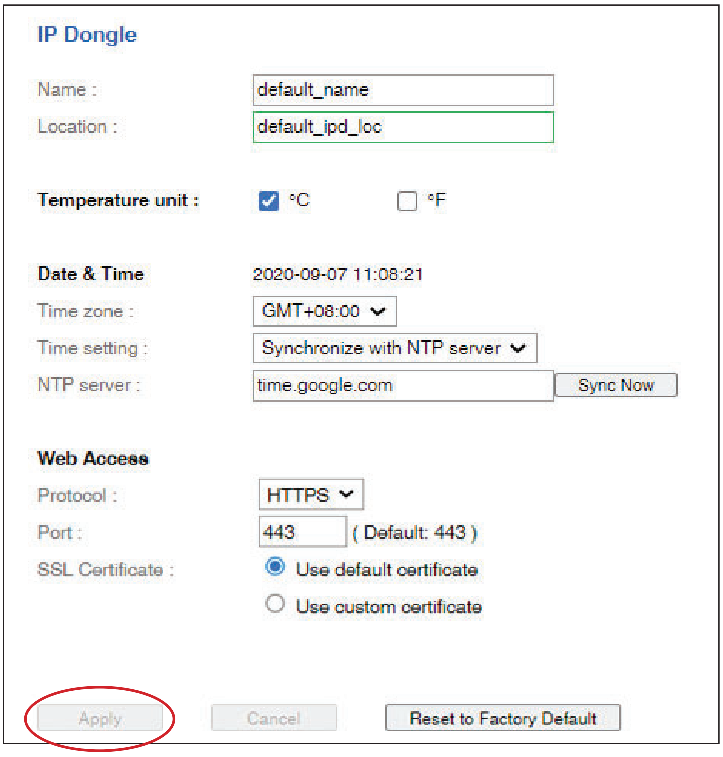
Time : 11 : 08 : 21

Web Access

Protocol : HTTPS

Port : 443 (Default: 443)

SSL Certificate : ● Use default certificate ○ Use custom certificate



IP Dongle

Name : default_name

Location : default_ipd_loc

Temperature unit : ☑ °C □ °F

Date & Time 2020-09-07 11:08:21

Time zone : GMT+08:00

Time setting : Synchronize with NTP server

NTP server : time.google.com

Web Access

Protocol : HTTPS

Port : 443 (Default: 443)

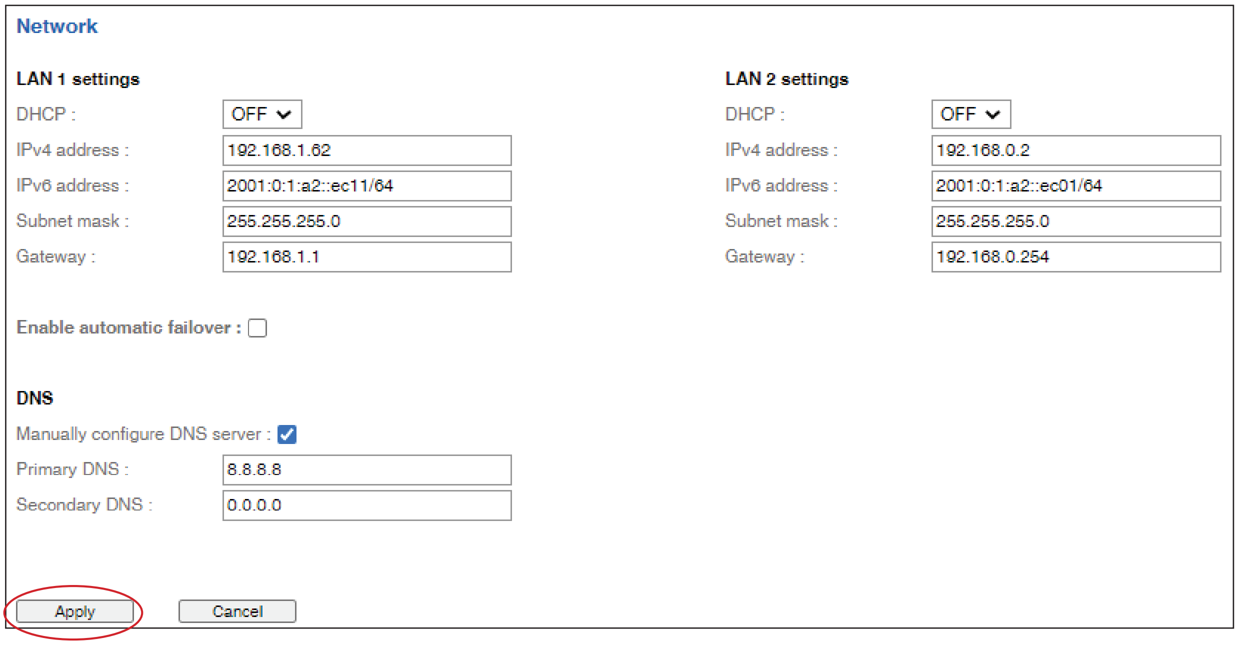
SSL Certificate : ● Use default certificate ○ Use custom certificate

< 1.8 > Network

In < **Network** >, IP dongle 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 : □

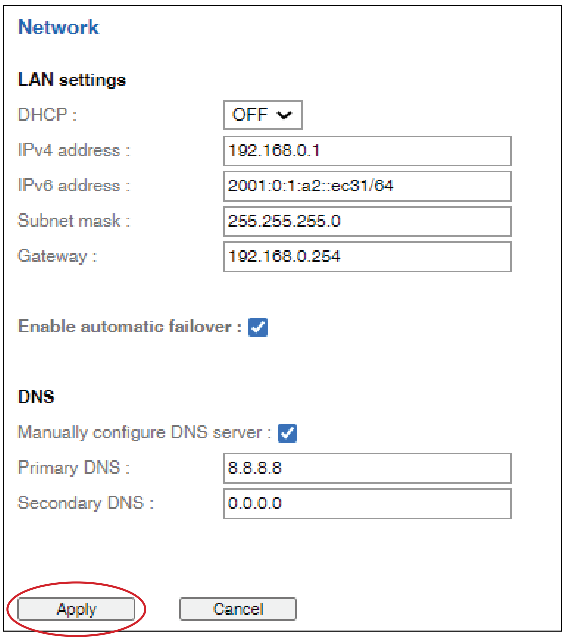
DNS

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

< 1.9 > Wifi Network Configuration

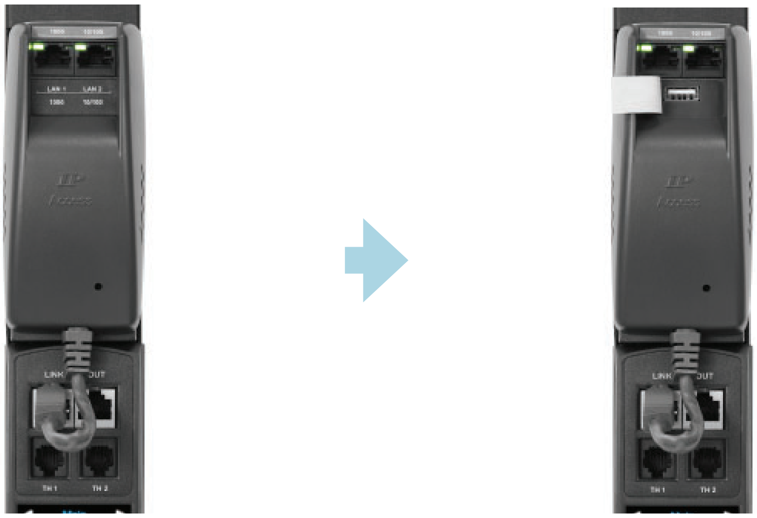
< Preparation >

- Make sure the network meet the security WPA2 - Personal or WPA2 - Enterprise.
- PDU dongle IPD-03-S is well connected to the iPDU and powered on.
- Login IPD-03-S web UI via LAN 1/ LAN 2 to configure the WIFI network.

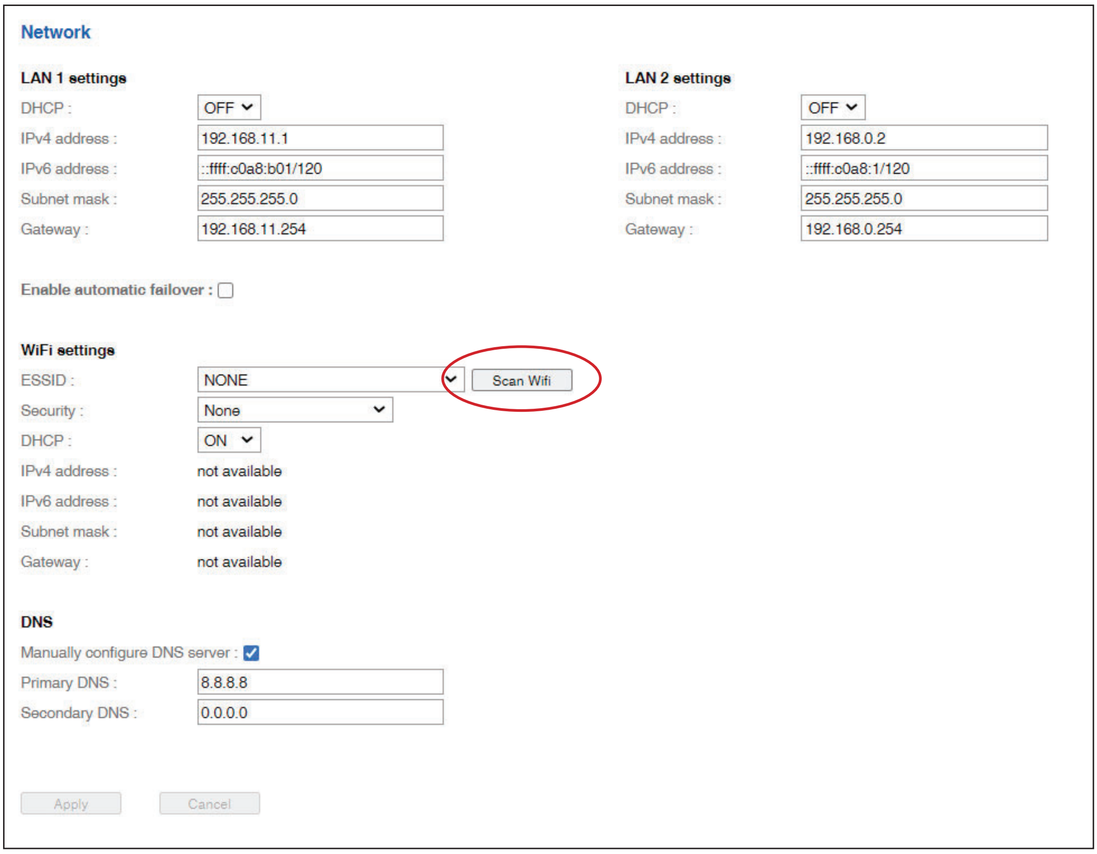
3rd party WIFI kit is not compatible to InfraPower.
Make sure IPD-WIFI has been used for the WIFI network connection.

(I) Wifi Static IP setting

Step 1. Take out the membrane from the IP dongle and the Wifi USB port will be found.
Then, connect the USB wireless adapter to the IP dongle.
(Details please refer to < 1.17 > Optional Accessories - Wifi Kit)



Step 2. Click " Scan Wifi " to search the available WiFi network



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.2
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

Enable automatic failover : □

WiFi settings

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

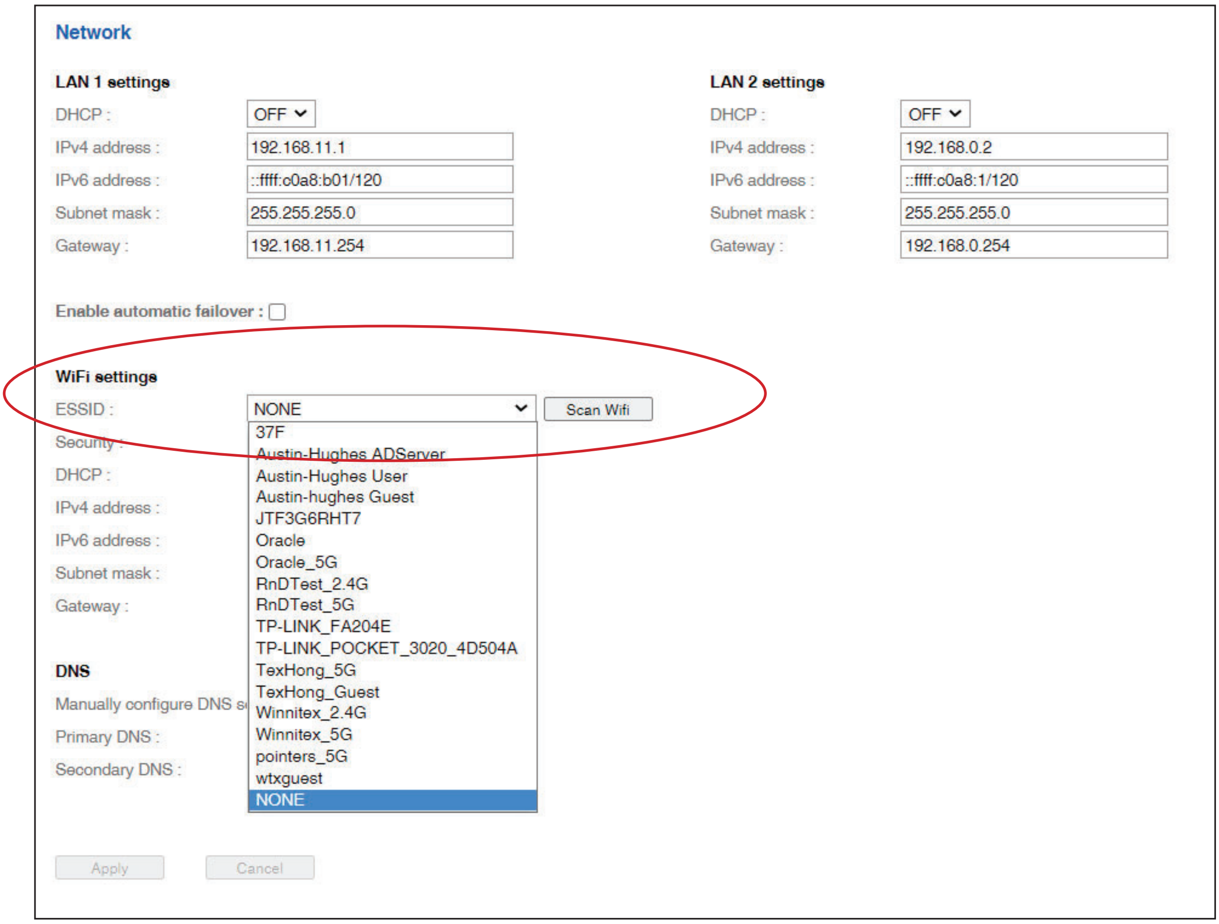
DNS

Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

< 1.9 > Wifi Network Configuration

Step 3. Select the appropriate network from the pull down menu of “ ESSID “



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.2
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

Enable automatic failover : □

WiFi settings

ESSID : NONE

Security :

DHCP :

IPv4 address :

IPv6 address :

Subnet mask :

Gateway :

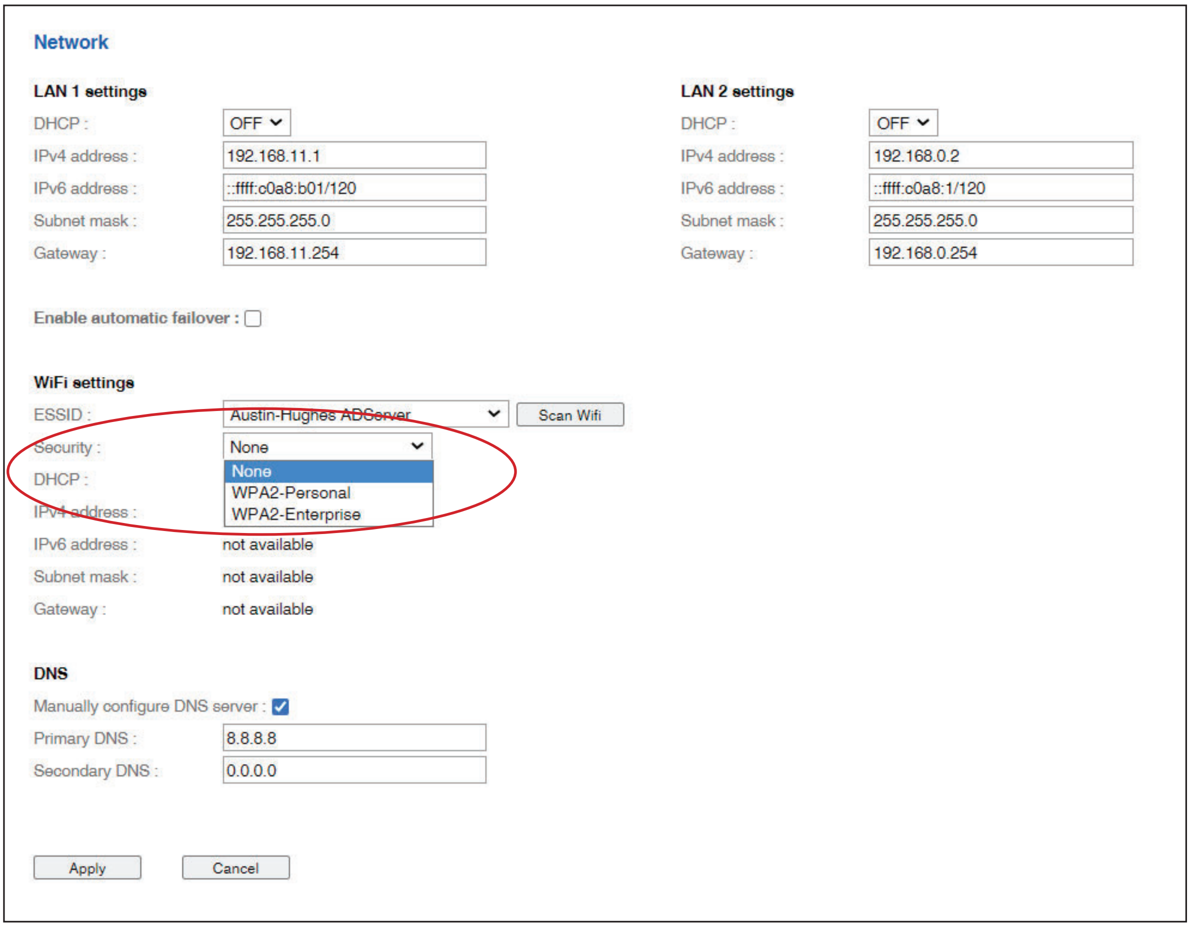
DNS

Manually configure DNS se

Primary DNS :

Secondary DNS :

Step 4. Select the security type (NONE / WPA2-Personal / WPA2-Enterprise)



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.2
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

Enable automatic failover : □

WiFi settings

ESSID : Austin-Hughes ADServer

Security : None

DHCP :

IPv4 address :

IPv6 address : not available

Subnet mask : not available

Gateway : not available

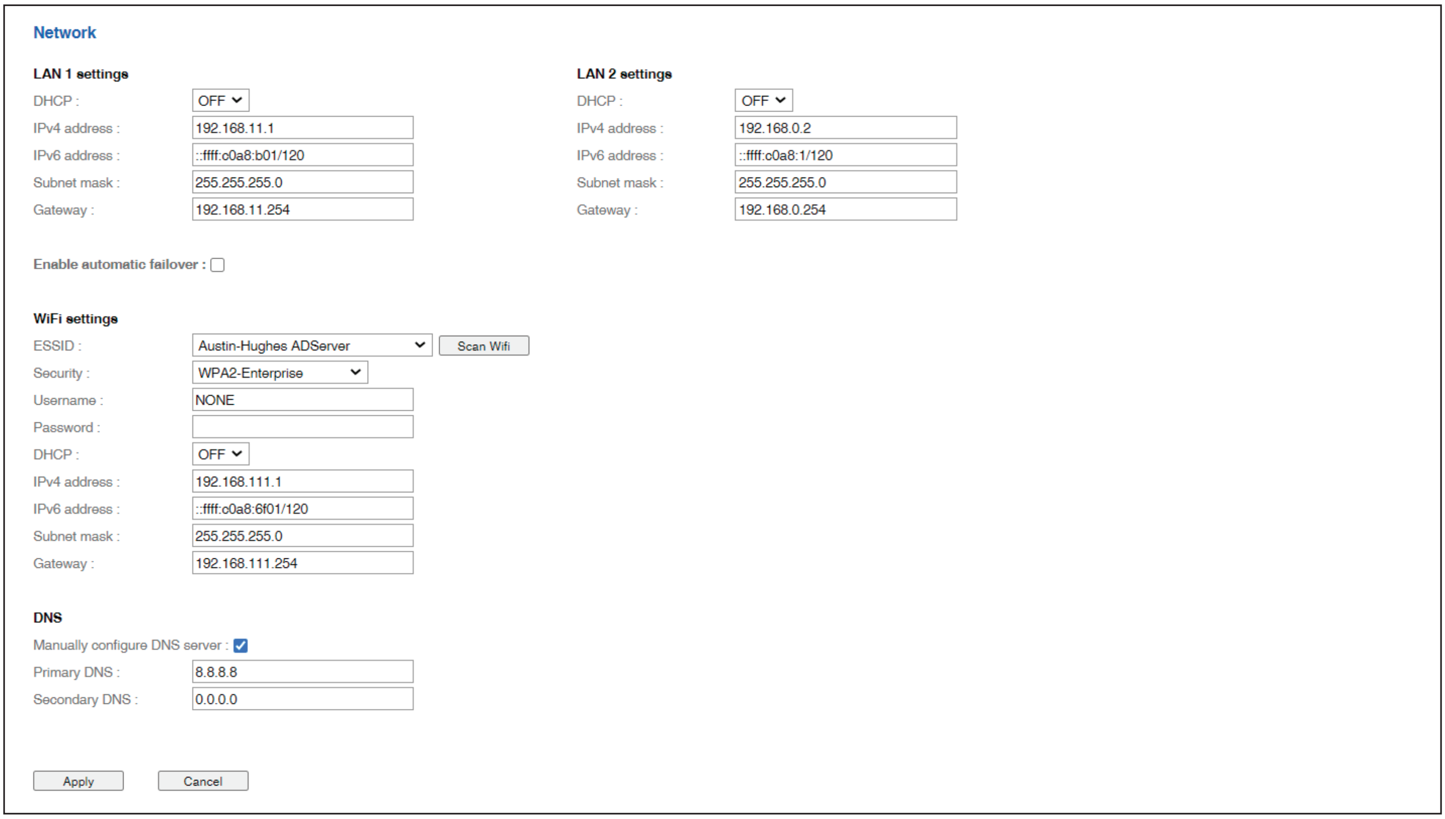
DNS

Manually configure DNS server : ☑

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Step 5. Enter “ Username “ (For security type : WPA2-Enterprise ONLY)



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.2
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

Enable automatic failover : □

WiFi settings

ESSID :	Austin-Hughes ADServer
Security :	WPA2-Enterprise
Username :	NONE
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

Step 6. Enter “ Password “

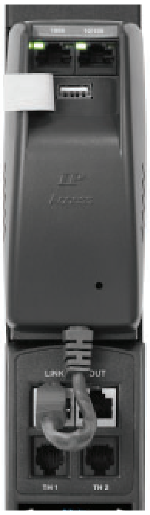
Step 7. Select “ DHCP “ to “ OFF “. Default is “ ON “

Step 8. Enter “ IPv4 address “ , “ IPv6 address “ , “ Subnet mask “ , “ Gateway “ & Click “ Apply “ to finish the above settings.

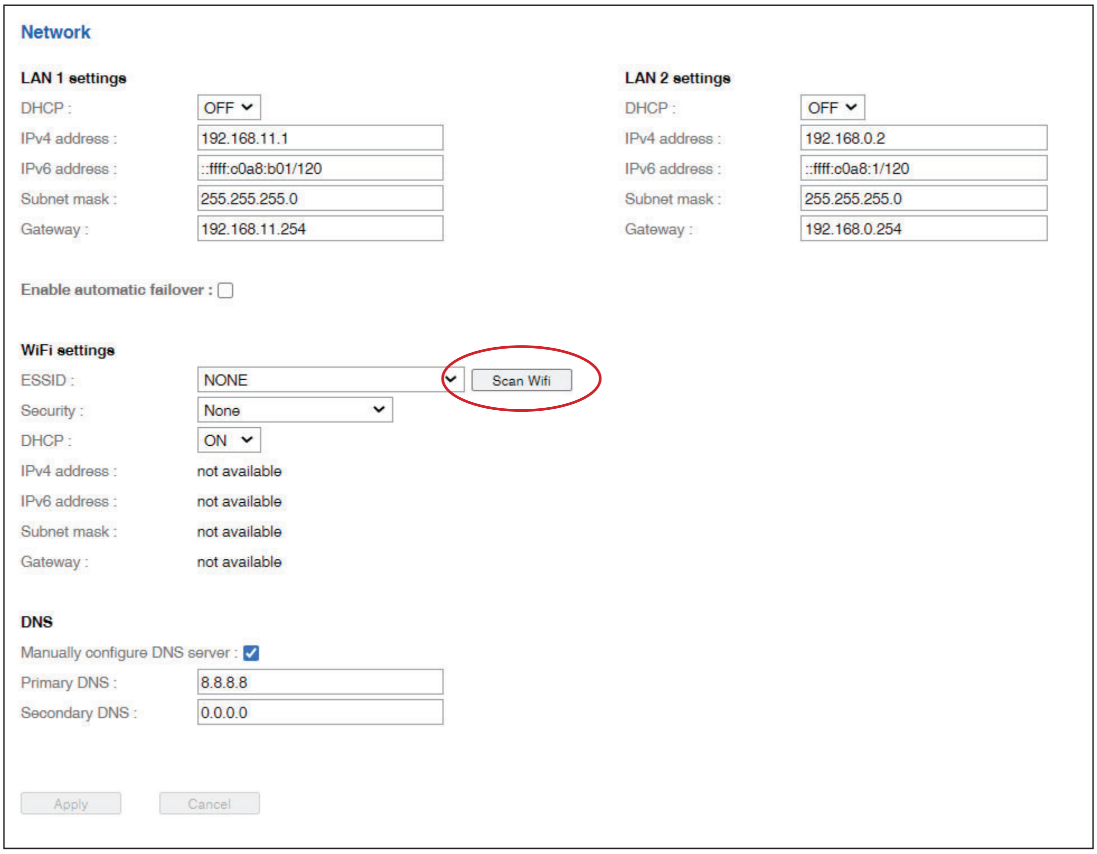
< 1.9 >   Wifi Network Configuration

(II) Wifi DHCP setting

Step 1. Take out the membrane from the IP dongle and the Wifi USB port will be found.
Then, connect the USB wireless adapter to the IP dongle.
(Details please refer to < 1.17 > Optional Accessories - Wifi Kit)



Step 2. Click “ Scan Wifi “ to search the available WiFi network



Network

LAN 1 settings		LAN 2 settings	
DHCP :	OFF	DHCP :	OFF
IPv4 address :	192.168.11.1	IPv4 address :	192.168.0.2
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

Enable automatic failover : □

WiFi settings

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

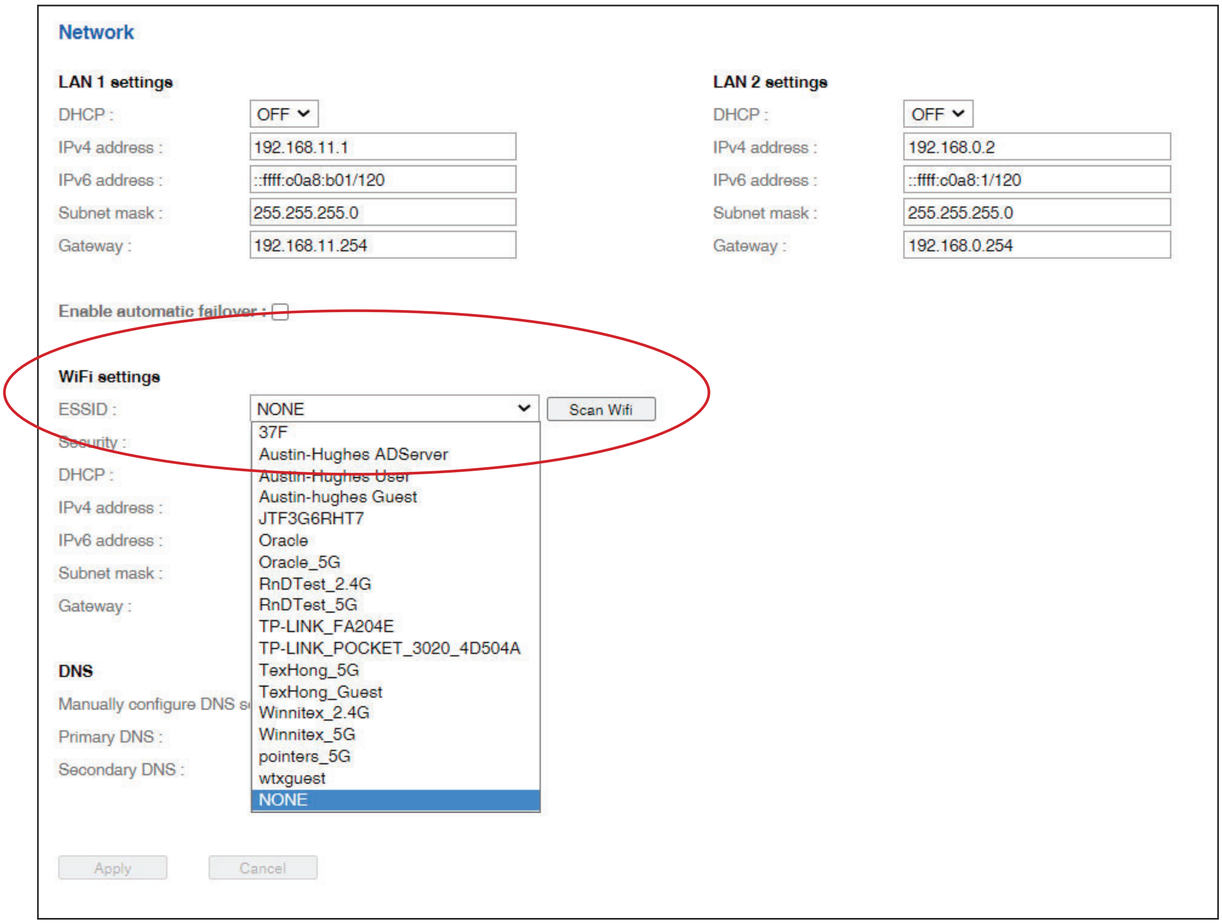
DNS

Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

< 1.9 > Wifi Network Configuration

Step 3. Select the appropriate network from the pull down menu of “ ESSID “



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

LAN 2 settings

DHCP : OFF

IPv4 address : 192.168.0.2

IPv6 address : ::ffff:c0a8:1/120

Subnet mask : 255.255.255.0

Gateway : 192.168.0.254

Enable automatic failover : □

WiFi settings

ESSID : NONE

Security :

DHCP :

IPv4 address :

IPv6 address :

Subnet mask :

Gateway :

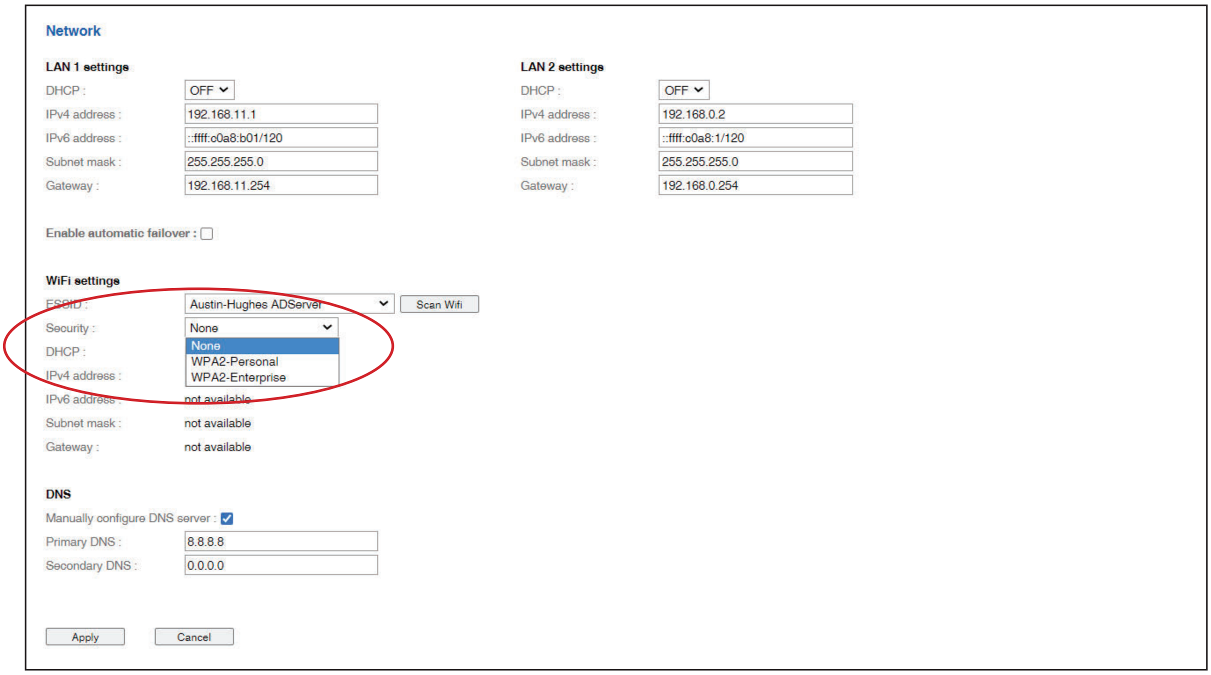
DNS

Manually configure DNS s

Primary DNS :

Secondary DNS :

Step 4. Select the security type (NONE / WPA2-Personal / WPA2-Enterprise)



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

LAN 2 settings

DHCP : OFF

IPv4 address : 192.168.0.2

IPv6 address : ::ffff:c0a8:1/120

Subnet mask : 255.255.255.0

Gateway : 192.168.0.254

Enable automatic failover : □

WiFi settings

ESSID : Austin-Hughes ADServer

Security : None

DHCP :

IPv4 address :

IPv6 address : not available

Subnet mask : not available

Gateway : not available

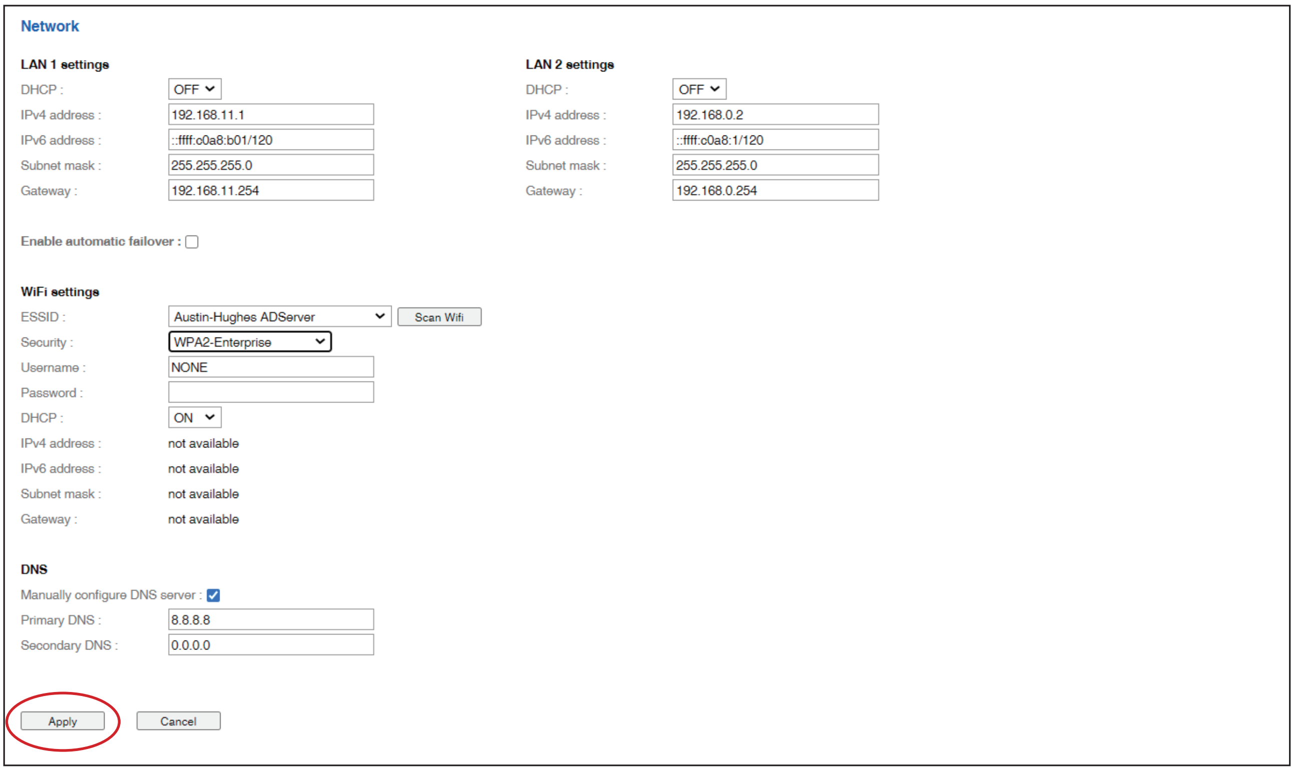
DNS

Manually configure DNS server : ☑

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Step 5. Enter “ Username “ (For security type : WPA2-Enterprise ONLY)



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

LAN 2 settings

DHCP :	OFF
IPv4 address :	192.168.0.2
IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0
Gateway :	192.168.0.254

Enable automatic failover : □

WiFi settings

ESSID :	Austin-Hughes ADServer
Security :	WPA2-Enterprise
Username :	NONE
Password :	
DHCP :	ON
IPv4 address :	not available
IPv6 address :	not available
Subnet mask :	not available
Gateway :	not available

DNS

Manually configure DNS server : ☑

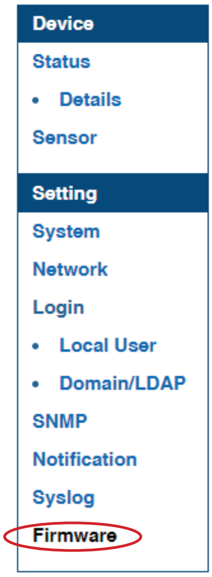
Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

Step 6. Enter “ Password “

Step 7. Select “ DHCP “ to “ ON “. Default is “ ON “

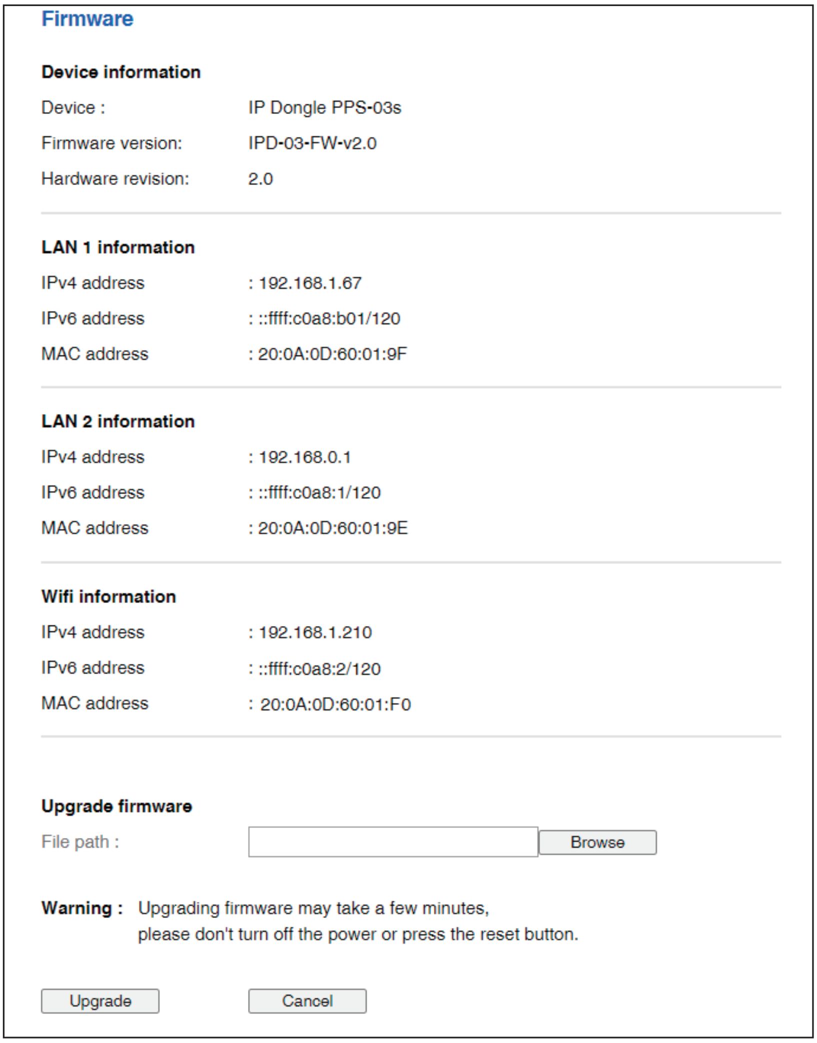
Step 8. Click “ Apply “ to finish the above settings.

Step 9. Select “ Firmware “ from the left navigation pane



< 1.9 > Wifi Network Configuration

Step 10. Record the “ MAC address “ of the Wifi kit



Firmware

Device information

Device :	IP Dongle PPS-03s
Firmware version:	IPD-03-FW-v2.0
Hardware revision:	2.0

LAN 1 information

IPv4 address	: 192.168.1.67
IPv6 address	: ::ffff:c0a8:b01/120
MAC address	: 20:0A:0D:60:01:9F

LAN 2 information

IPv4 address	: 192.168.0.1
IPv6 address	: ::ffff:c0a8:1/120
MAC address	: 20:0A:0D:60:01:9E

Wifi information

IPv4 address	: 192.168.1.210
IPv6 address	: ::ffff:c0a8:2/120
MAC address	: 20:0A:0D:60:01:F0

Upgrade firmware

File path :

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

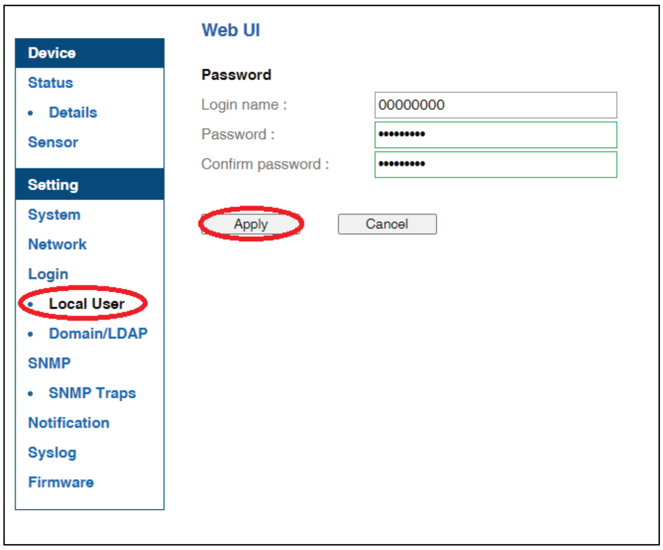
Step 11. Assign an IP address of the Wifi kit from your DHCP server.

< 1.10 > Login

In < **Login** >, you can login the IP dongle WEBUI 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



Web UI

Password

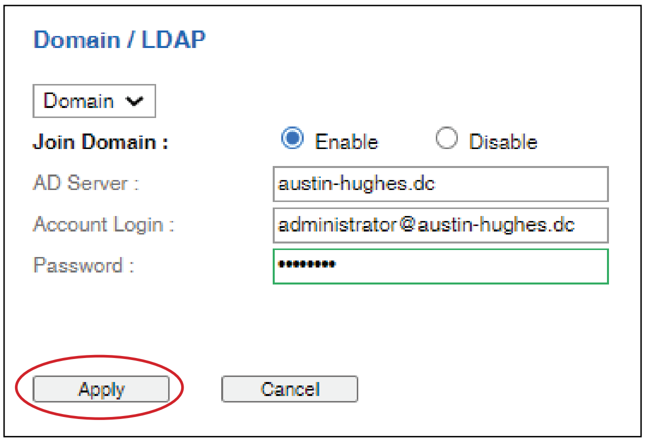
Login name : 00000000

Password : •••••••••

Confirm password : •••••••••

Domain/LDAP :

- Default Join Domain is **“ Disable “**
- Enable “ **Join Domain** ” only when you want to login the IP dongle WEBUI 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 / LDAP

Domain

Join Domain : ● Enable ○ Disable

AD Server : austin-hughes.dc

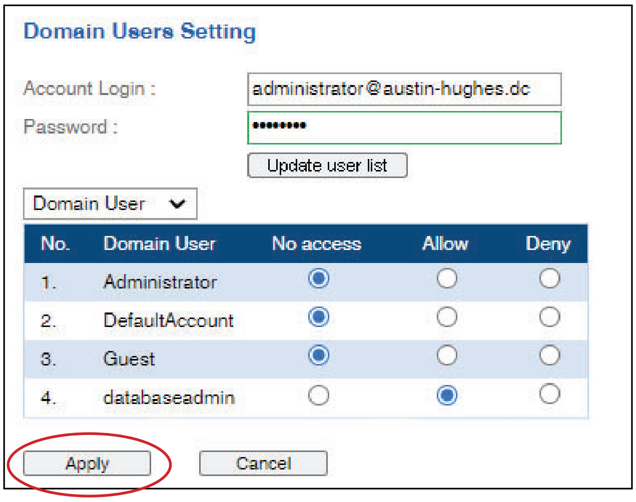
Account Login : administrator@austin-hughes.dc

Password : ••••••••

< 1.10 > 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 IP dongle WEBUI.



Domain Users Setting

Account Login : administrator@austin-hughes.dc

Password : ••••••••

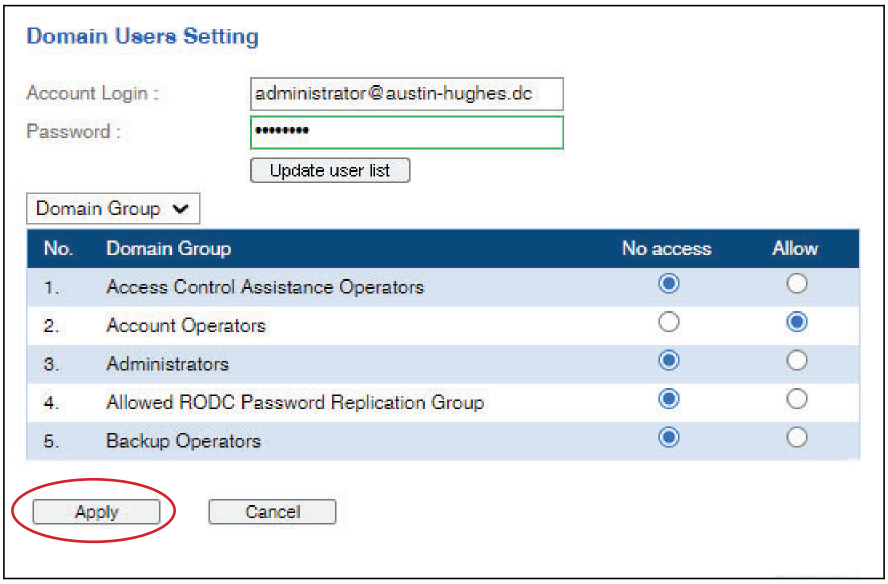
Update user list

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 IP dongle WEBUI.



Domain Users Setting

Account Login : administrator@austin-hughes.dc

Password : ••••••••

Update user list

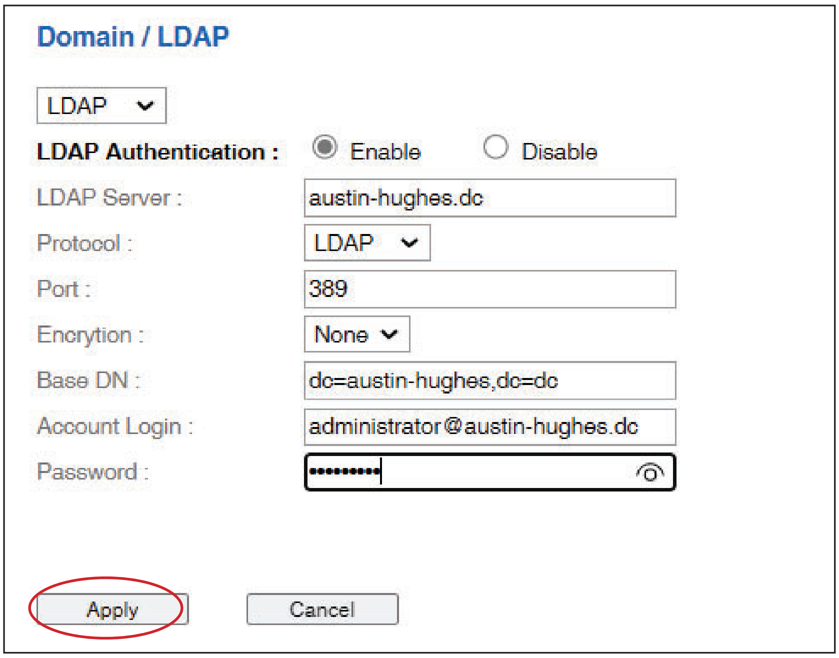
Domain Group

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	●	○

< 1.10 > Login

Domain/LDAP :

- Default LDAP Authentication is **“ Disable “**
- Enable **“ LDAP Authentication ”** only when you want to login the IP dongle WEBUI by LDAP server
- Enter “ **LDAP Server** ”,
- Select “ **Protocol** ”(LDAP / LDAPS). Default is **“ LDAP “**
- Enter **“ Port “**. Default is **“ 389 “**
- Select “ **Encrytion** ”(None / SSL). Default is **“ None “**
- Enter **“ Base DN “**.
- Enter “ **Account Login** ” & “ **Password** ”.
- Click “ **Apply** ” and “ **OK** “ on the pop up window to make changes effective
- You can now go to “ **LDAP Users** ” to assign access right to the **“ LDAP User ”** or the **“ LDAP Group ”**



Domain / LDAP

LDAP

LDAP Authentication : ● Enable ○ Disable

LDAP Server : austin-hughes.dc

Protocol : LDAP

Port : 389

Encrytion : None

Base DN : dc=austin-hughes,dc=dc

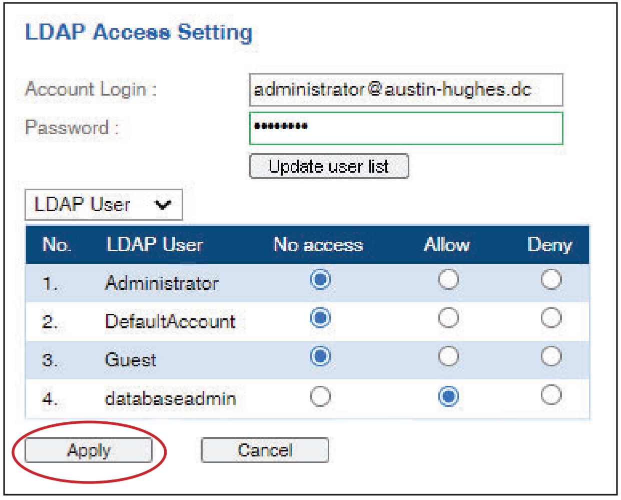
Account Login : administrator@austin-hughes.dc

Password : ••••••••••

< 1.10 > Login

In “ **LDAP Access Setting** ”,

- Click **“ Update domain data ”** to update domain user list.
- Assign access right (No access / Allow / Deny) to **“ LDAP User ”** and click **“ Apply ” .**
- The LDAP User assigned **“ Allow “** access right can login the IP dongle WEBUI.



LDAP Access Setting

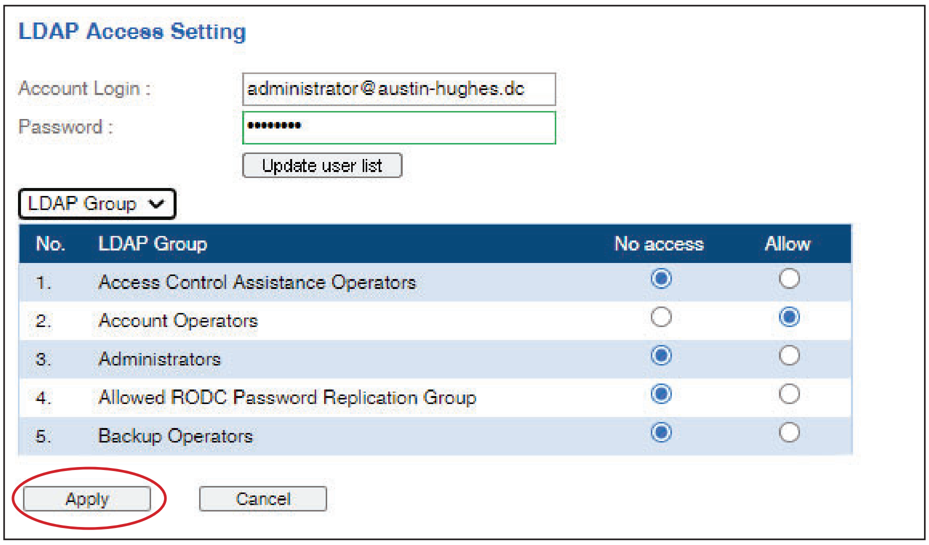
Account Login : administrator@austin-hughes.dc

Password : ••••••••

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

In “ **LDAP Access Setting** ”,

- Click **“ Update domain data ”** to update domain user list.
- Assign access right (No access / Allow / Deny) to **“ LDAP Group ”** and click **“ Apply ” .**
- The LDAP Group assigned **“ Allow “** access right can login the IP dongle WEBUI.



LDAP Access Setting

Account Login : administrator@austin-hughes.dc

Password : ••••••••

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

< 1.11 > SNMP Setup

The IP dongle 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

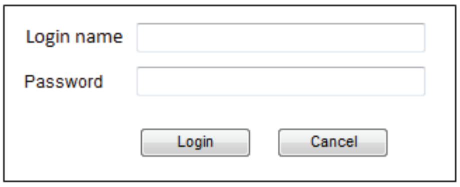
i. The following steps summarize how to enable the IP Dongle for SNMP v1 / v2 support.

Step 1. Connect the IP Dongle to a computer. (Please refer to < 1.4 > IP dongle configuration)

Step 2. Open the MS Edge

Step 3. Enter the configured IP Dongle address into the address bar.
Default IP address of LAN 1 is “ **192.168.11.1** “
Default IP address of LAN 2 is “ **192.168.0.1** “

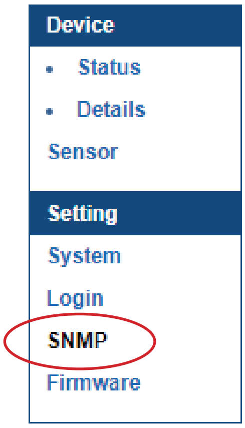
Step 4. Enter “ **Login name** “ & “ **Password** “.



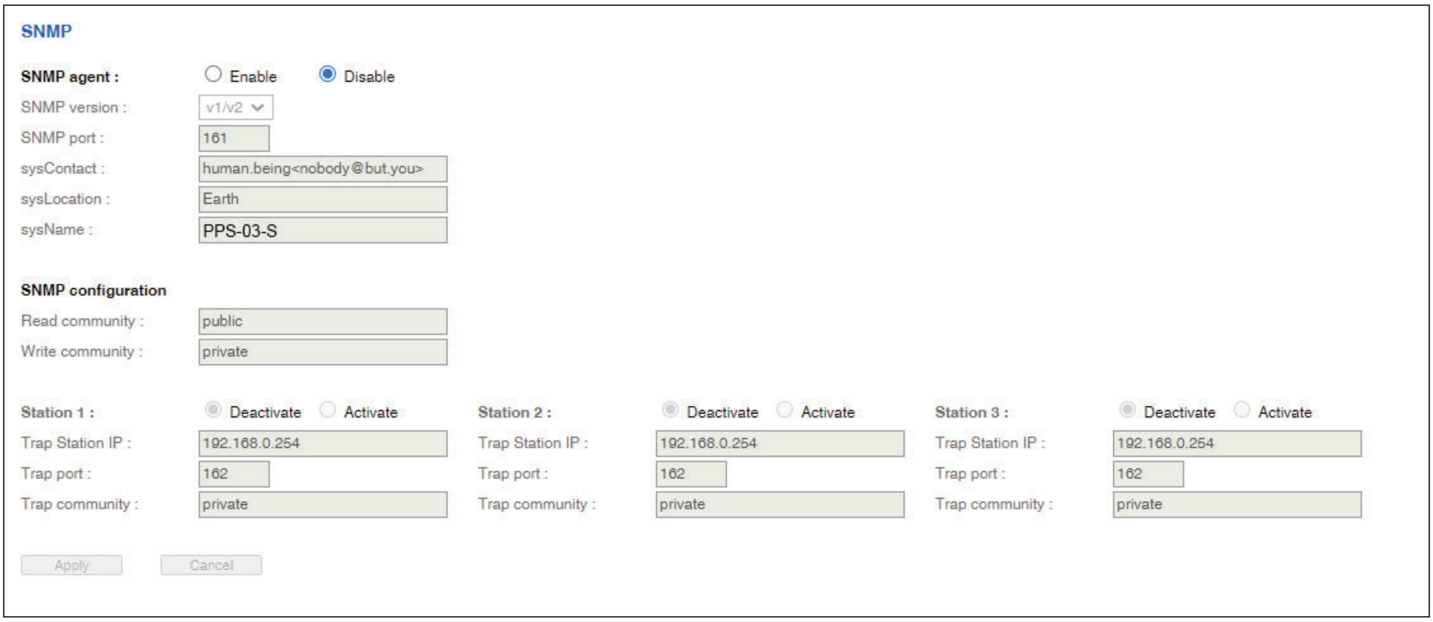
- Default login name: 00000000
- Password: the one you set in Step 7 of < 1.4 > IP Dongle Configuration.

< 1.11 > 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 A320D

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

< 1.11 > SNMP Setup

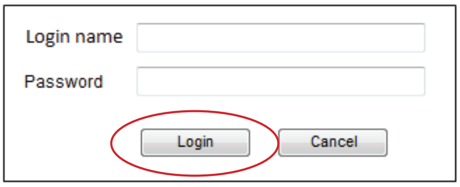
ii. The following steps summarize how to enable the IP Dongle for SNMP v3 support.

Step 1. Connect the IP dongle to a computer. (Please refer to < 1.4 > IP dongle configuration)

Step 2. Open MS Edge

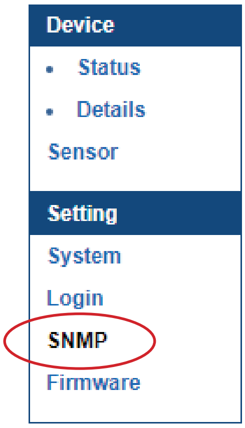
Step 3. Enter the configured IP Dongle address into the address bar.
Default IP address of LAN 1 is " **192.168.11.1** "
Default IP address of LAN 2 is " **192.168.0.1** "

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

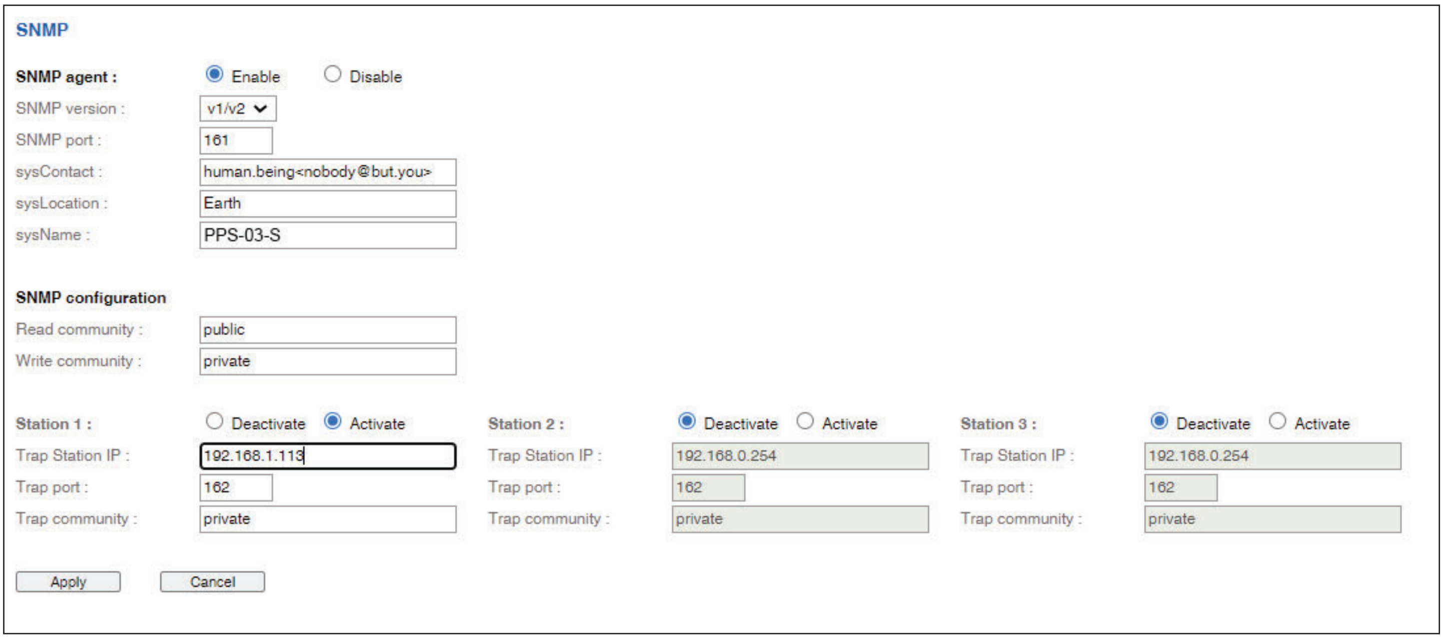

Login name
Password
Login Cancel

- Default login name: 00000000
- Password: the one you set in Step 7 of < 1.4 > IP Dongle Configuration.

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

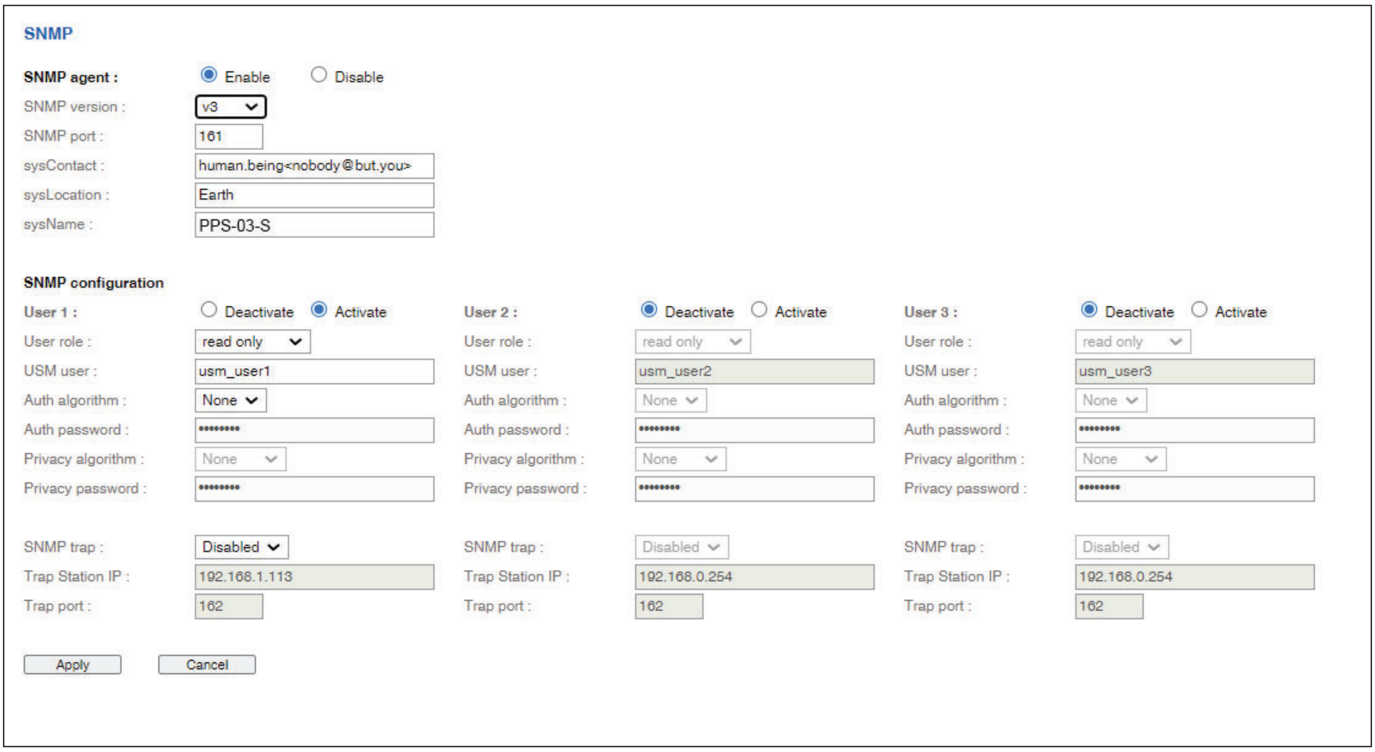
Station 1 :	○ Deactivate ● Activate	Station 2 :	● Deactivate ○ Activate	Station 3 :	● Deactivate ○ Activate
Trap Station IP :	192.168.1.113	Trap Station IP :	192.168.0.254	Trap Station IP :	192.168.0.254
Trap port :	162	Trap port :	162	Trap port :	162
Trap community :	private	Trap community :	private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

Apply Cancel

< 1.11 > 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 A320D

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** “

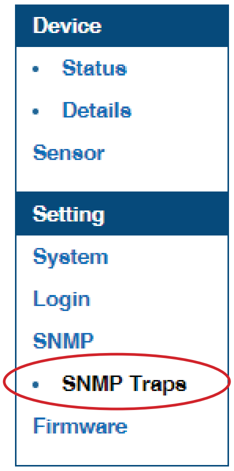
Step 22. Repeat step 12 to 20 for User 2 & 3

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

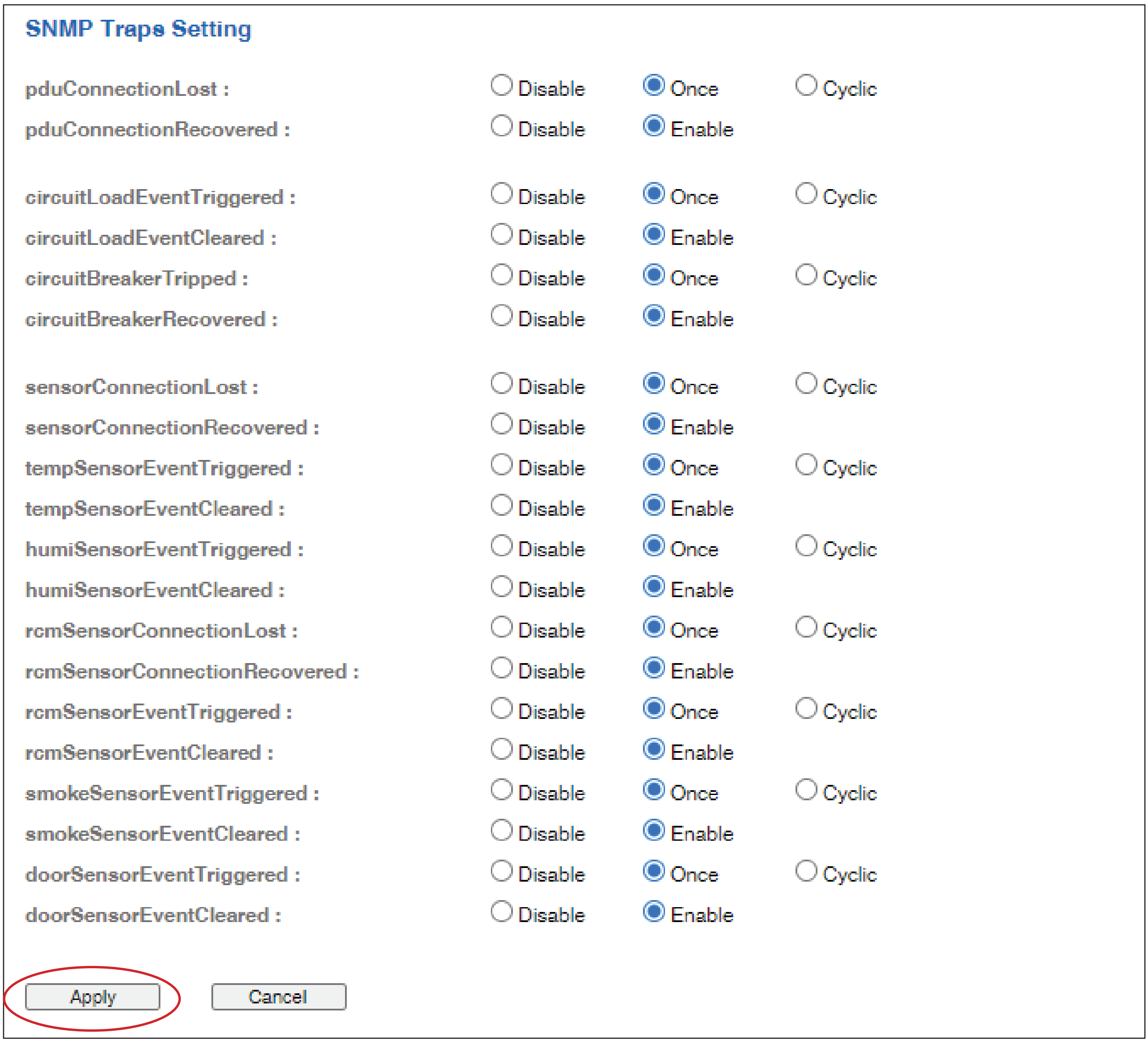
< 1.11 > SNMP Setup

(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	

< 1.12 > Notification

In **< Notification >** , you can configure the alarm email server & max. 5 email recipients to receive alarm notifications from the IP dongle.

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 ”**

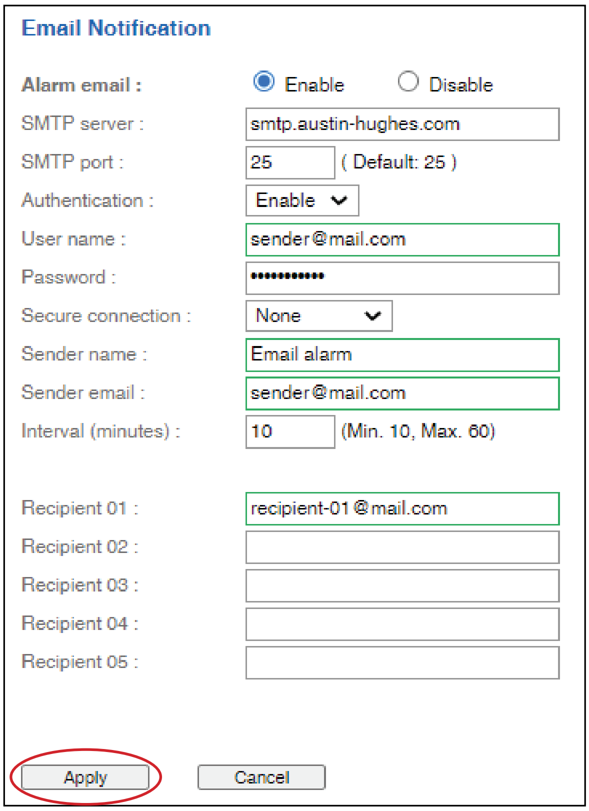
Step 6. Enter the **“ Sender Name ”** and **“ Sender Email ”**

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

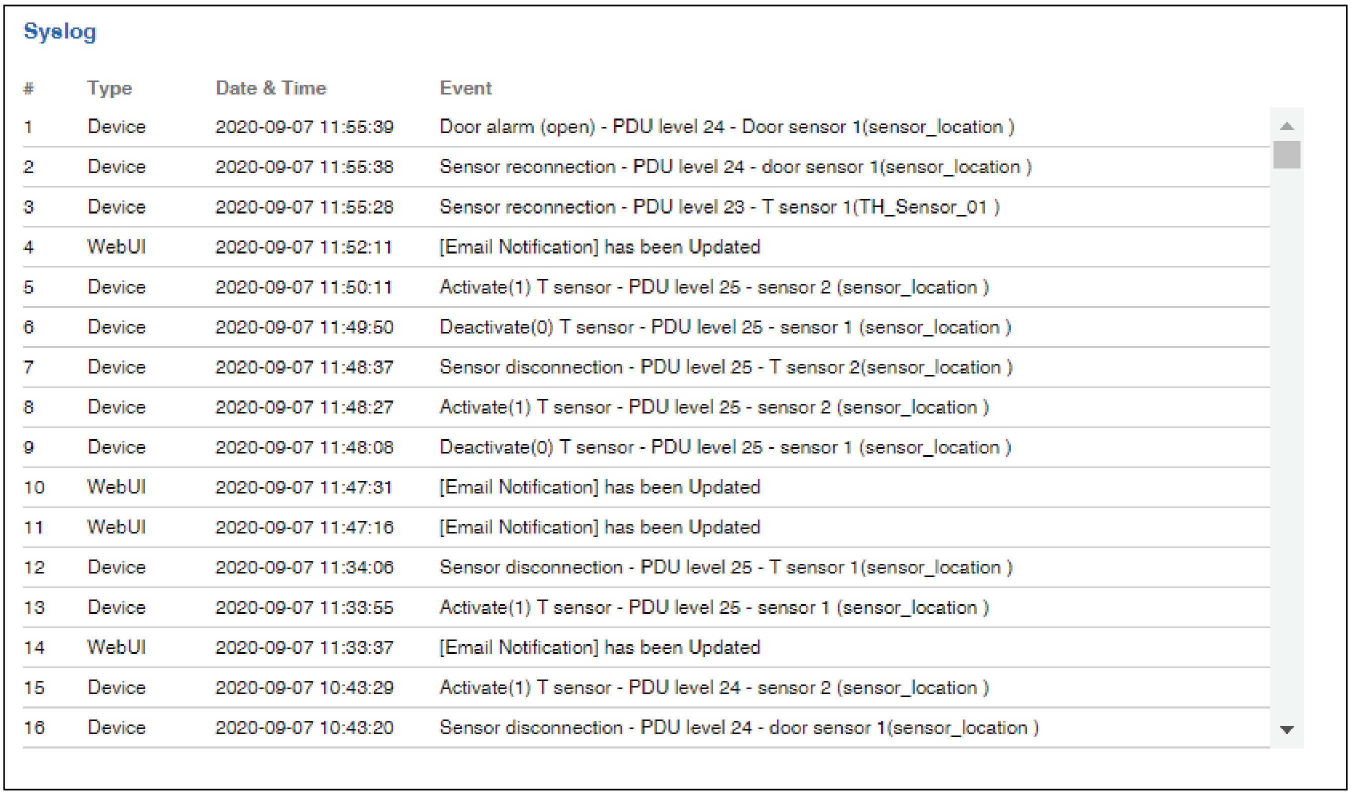


Email Notification

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 :	

< 1.13 > 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)

< 1.14 > IP Dongle Firmware Upgrade

< Firmware Upgrade >

For function enhancement of IP dongle WEBUI, please take the following steps to remotely upgrade the IP Dongle firmware :

Step 1. Click the following link to go to the mangement software download page :
http://www.austin-hughes.com/resources/infrapower/software

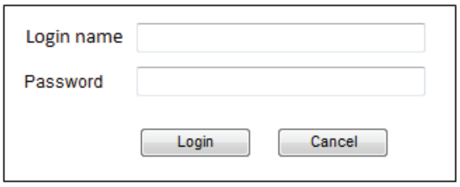
Step 2. Select the appropriate IP Dongle firmware file of the PDU series

Step 3. Connect the IP Dongle to the computer. (Please refer to < 1.4 > IP dongle configuration)

Step 4. Open the MS Edge

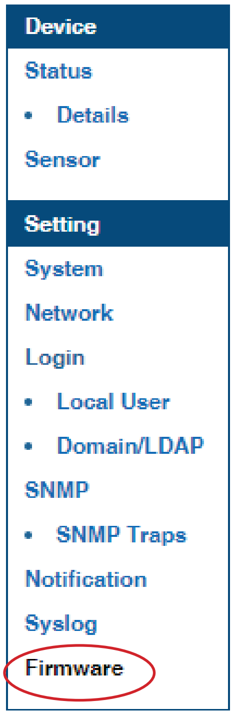
Step 5. Enter the configured IP Dongle address into the Address bar.
Default IP address of LAN 1 is “ **192.168.11.1** “
Default IP address of LAN 2 is “ **192.168.0.1** “

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



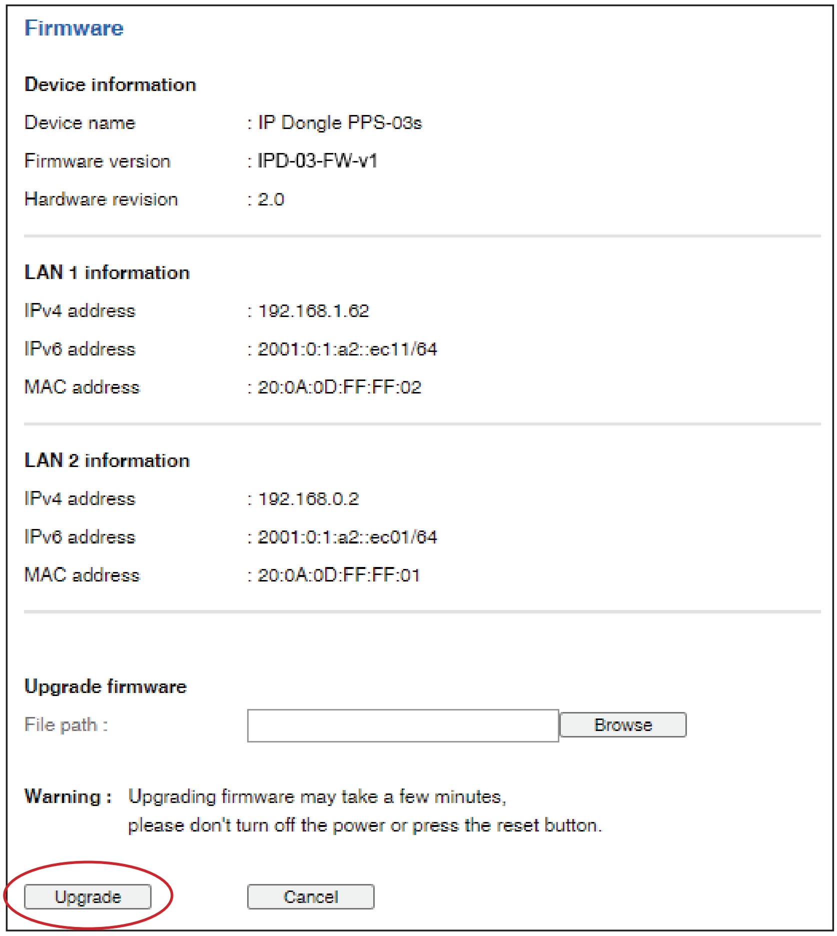
- Default login name: 00000000
- Password: the one you set in Step 7 of < 1.4 > IP Dongle Configuration.

Step 7. Select the Firmware from the left navigation pane



< 1.14 >   IP Dongle Firmware Upgrade

Step 8. The firmware upgrade window appears as below :



Firmware

Device information

Device name : IP Dongle PPS-03s

Firmware version : IPD-03-FW-v1

Hardware revision : 2.0

LAN 1 information

IPv4 address : 192.168.1.62

IPv6 address : 2001:0:1:a2::ec11/64

MAC address : 20:0A:0D:FF:FF:02

LAN 2 information

IPv4 address : 192.168.0.2

IPv6 address : 2001:0:1:a2::ec01/64

MAC address : 20:0A:0D:FF:FF:01

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 (xxx.zip for firmware version IPD-03-FW-v1 **/** xxx.enc for firmware version IPD-03-FW-V1.1 or above) 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.

< 1.15 > Bulk Firmware Upgrade

< 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 IP dongles (IPD-03-S) in the same network.

⚠
- The feature of bulk firmware upgrade via DHCP/TFTP only works on IPD-03-S 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 >

The bulk firmware upgrade feature only available for IP Dongle (IPD-03-S) firmware version v3.0 or above. Ensure the IP Dongle (IPD-03-S) firmware is v3.0 or above before you want to perform the 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
- IP Dongle firmware file 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

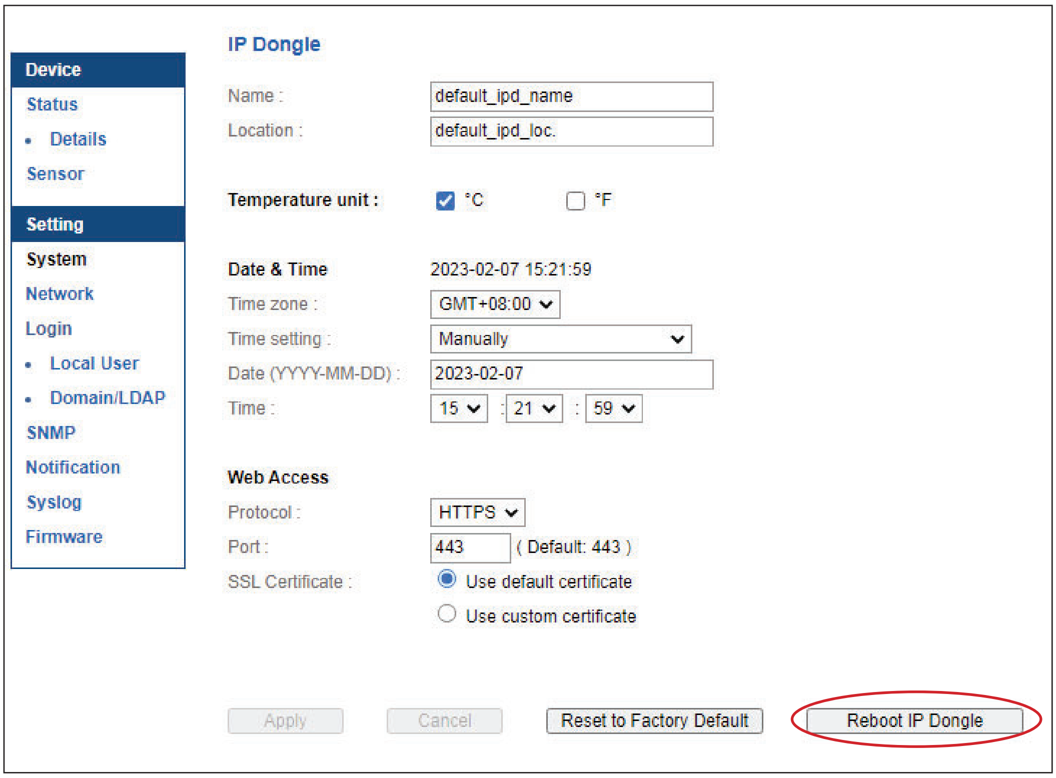
Step 4. Properly configure your DHCP server so that it refers to the file “ **fwupdate.cfg** ” on the TFTP server for your IP Dongle. See ***DHCP IPv4 Configuration in Windows***

Step 5. Make sure all of the IP Dongles use DHCP as the IP configuration method and have been directly connected to the network.

⚠ The default IP configuration of IP Dongle is “ **STATIC** ”

< 1.15 > Bulk Firmware Upgrade

Step 6. Reboot the IP Dongles. The DHCP server will execute the commands in the “ **fwupdate.cfg** ” file on the TFTP server to upgrade those IP Dongles supporting DHCP in the same network. You can Click “ **Reboot IP Dongle** ” in “ System ” of IP Dongle.



IP Dongle

Name : default_ipd_name

Location : default_ipd_loc.

Temperature unit : ☑ °C ☐ °F

Date & Time 2023-02-07 15:21:59

Time zone : GMT+08:00

Time setting : Manually

Date (YYYY-MM-DD) : 2023-02-07

Time : 15 : 21 : 59

Web Access

Protocol : HTTPS

Port : 443 (Default: 443)

SSL Certificate : ● Use default certificate

○ Use custom certificate

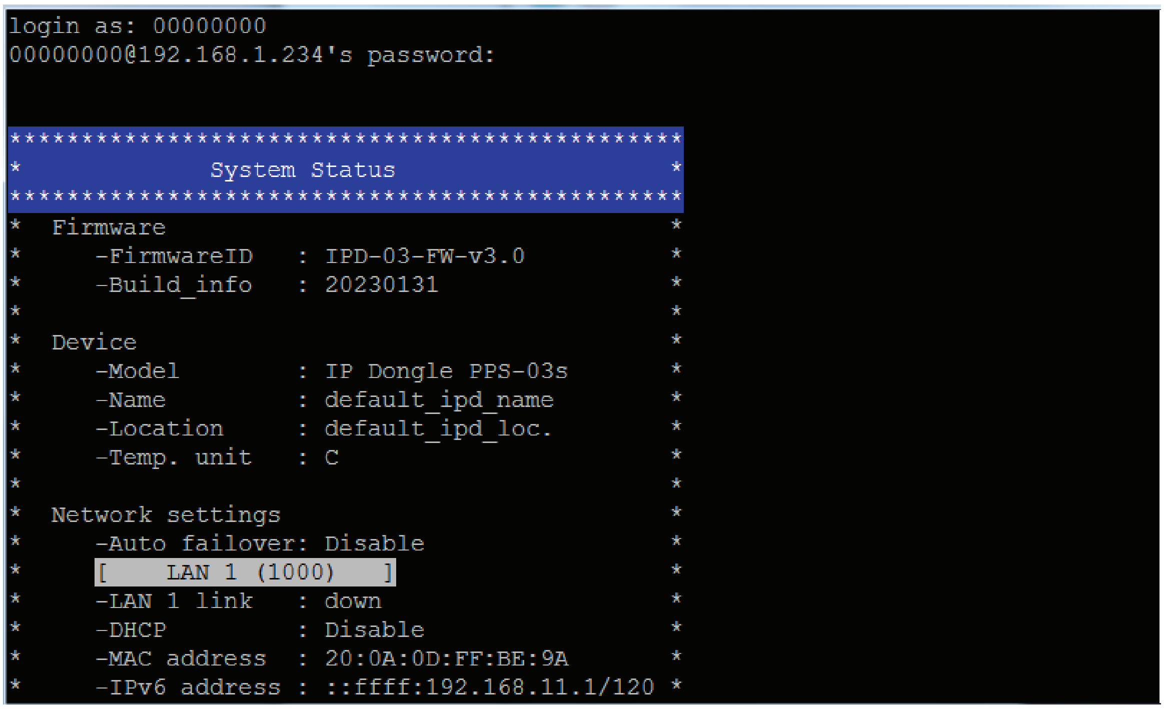
You must enable firmware upgrade via DHCP in SSH (default is ENABLED) and input the username and password for bulk firmware upgrade in the “ **fwupdate.cfg** ” file. You can change the username and password for bulk firmware upgrade via SSH. **See *Con figuration of username / password for bulk firmware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

< 1.15 > Bulk Firmware Upgrade

Configuration of username / password for bulk firmware upgrade

Step 1. Access the SSH using putty

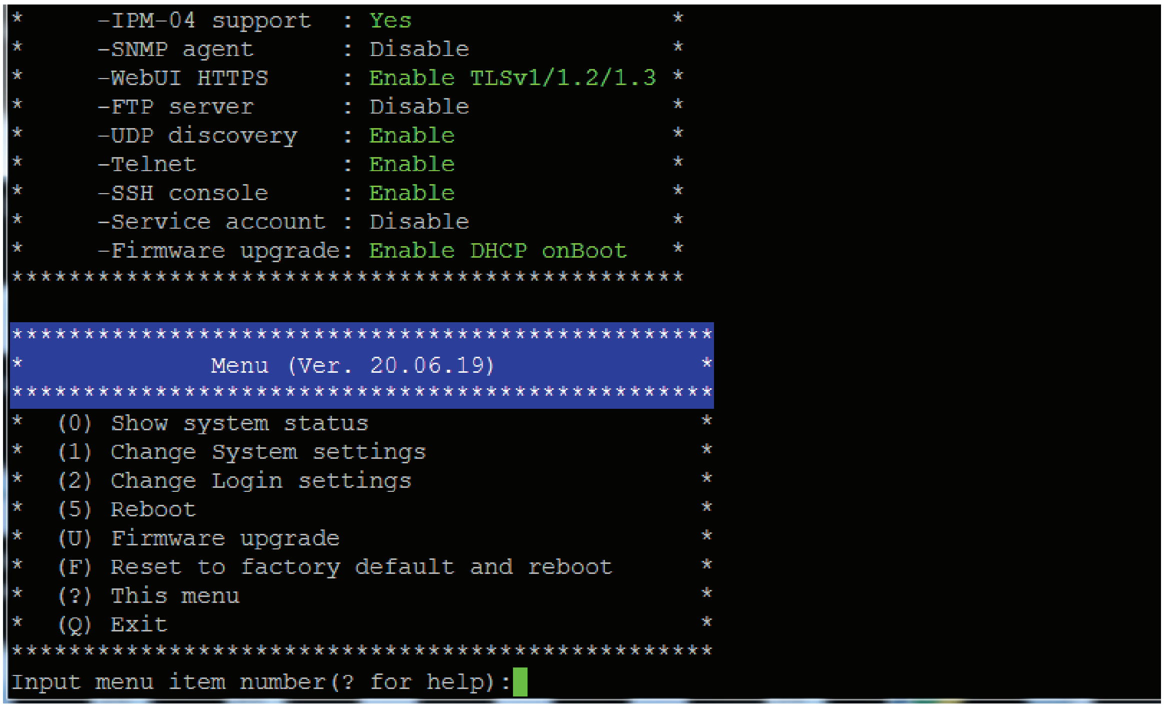
Step 2. Input the login name and password to login the CLI.



```
login as: 00000000
00000000@192.168.1.234's password:


***********************************************
*              System Status                  *
***********************************************
*  Firmware                                   *
*     -FirmwareID   : IPD-03-FW-v3.0          *
*     -Build_info   : 20230131                *
*                                             *
*  Device                                     *
*     -Model        : IP Dongle PPS-03s       *
*     -Name         : default_ipd_name        *
*     -Location     : default_ipd_loc.        *
*     -Temp. unit   : C                       *
*                                             *
*  Network settings                           *
*     -Auto failover: Disable                 *
*     [    LAN 1 (1000)    ]                  *
*     -LAN 1 link   : down                    *
*     -DHCP         : Disable                 *
*     -MAC address  : 20:0A:0D:FF:BE:9A       *
*     -IPv6 address : ::ffff:192.168.11.1/120 *
```

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

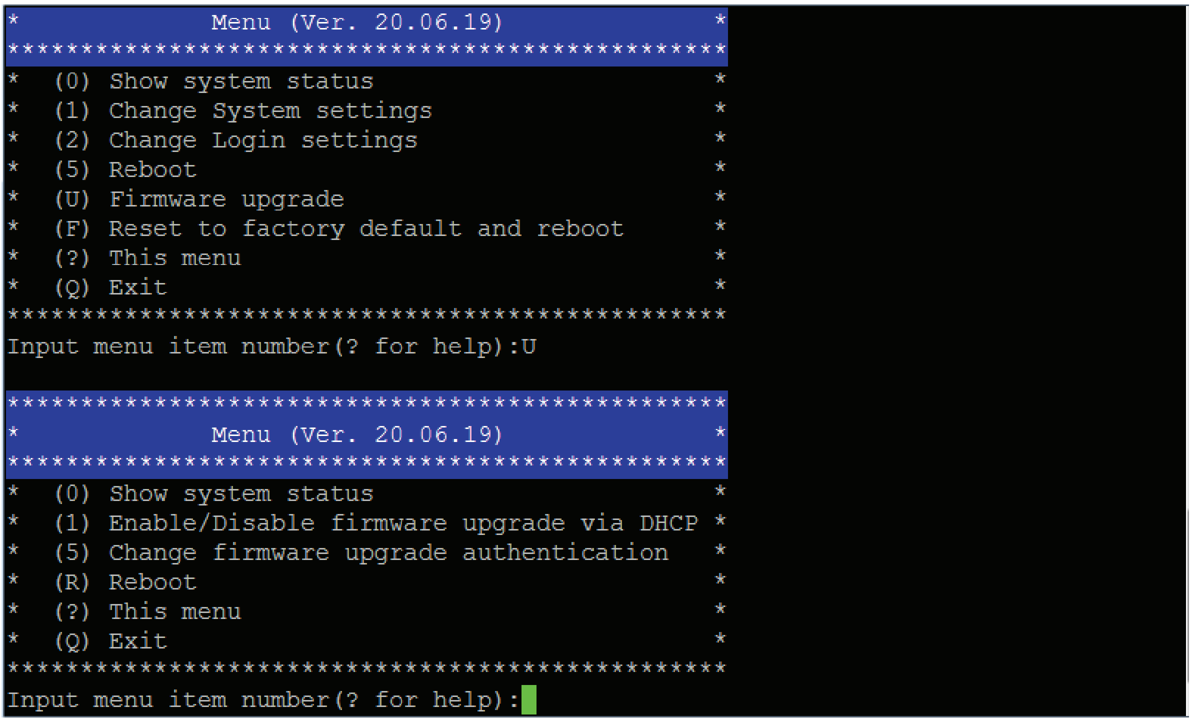


```
*     -IPM-04 support  : Yes                  *
*     -SNMP agent      : Disable              *
*     -WebUI HTTPS     : Enable TLSv1/1.2/1.3 *
*     -FTP server      : Disable              *
*     -UDP discovery   : Enable               *
*     -Telnet          : Enable               *
*     -SSH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

< 1.15 > Bulk Firmware Upgrade

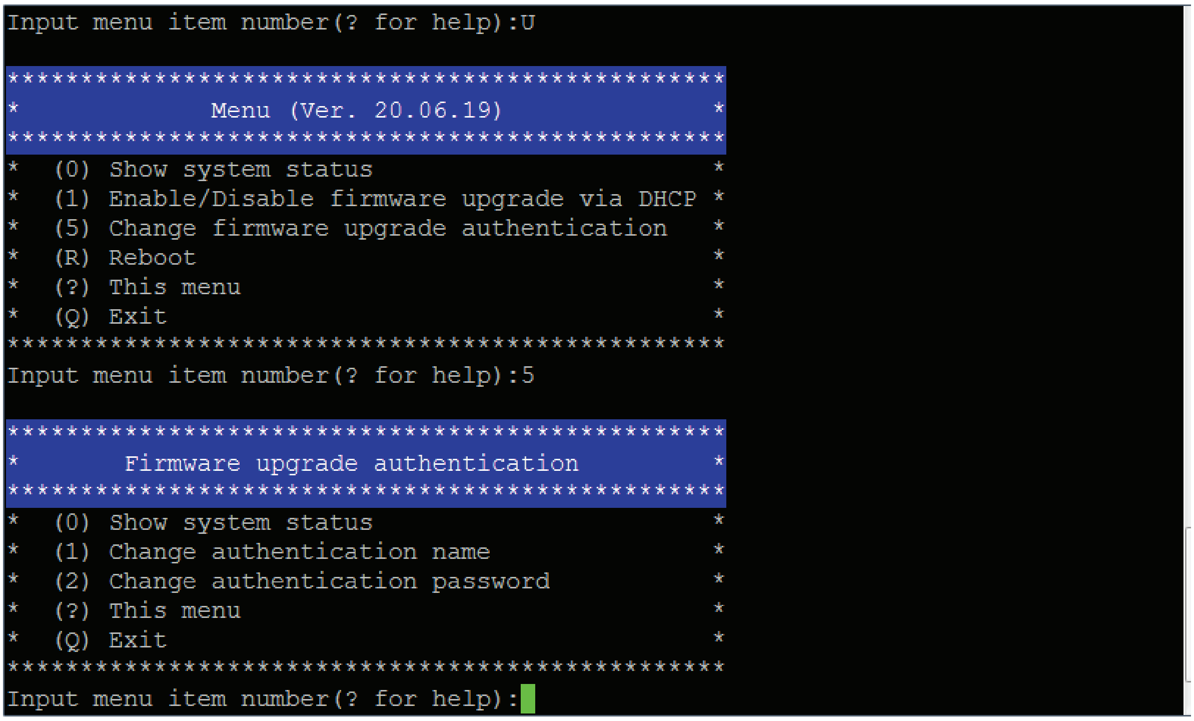
Step 4. Select “ **(5) Change firmware upgrade authentication** ” and “ **Enter** ”



```
*              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):
```

< 1.15 > Bulk Firmware Upgrade

< TFTP Requirements >

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

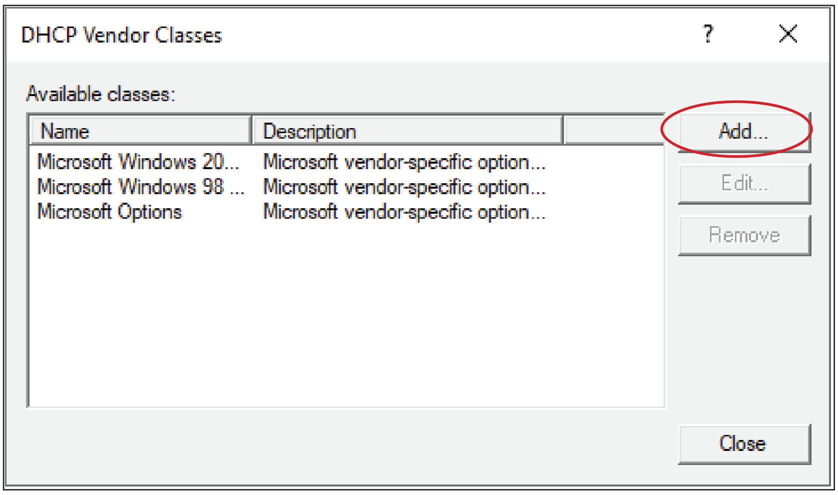
- Able to work with IPv4
- A folder containing all required files is available in the TFTP root directory. The folder name MUST be the same as the String value of the Magic code. Details please refer to DHCP IPv4 Configuration in Winodws
- The TFTP server supports the write operation including file creation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

- 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.

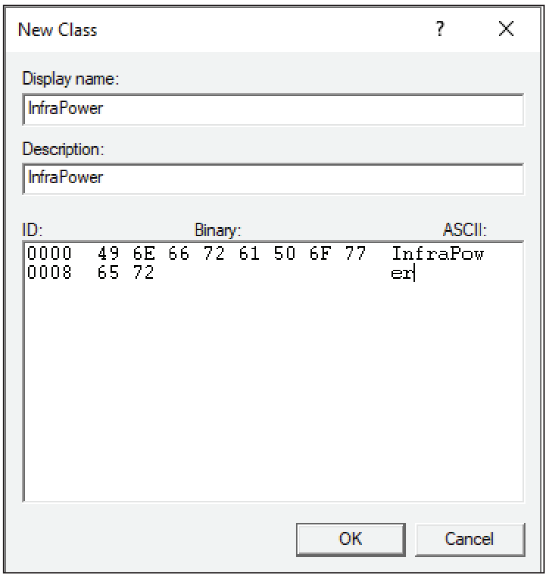


DHCP Vendor Classes

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

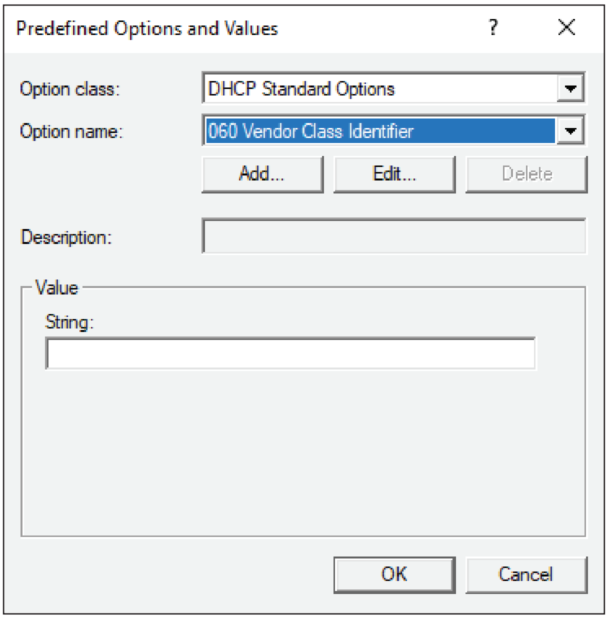
Display name: InfraPower

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

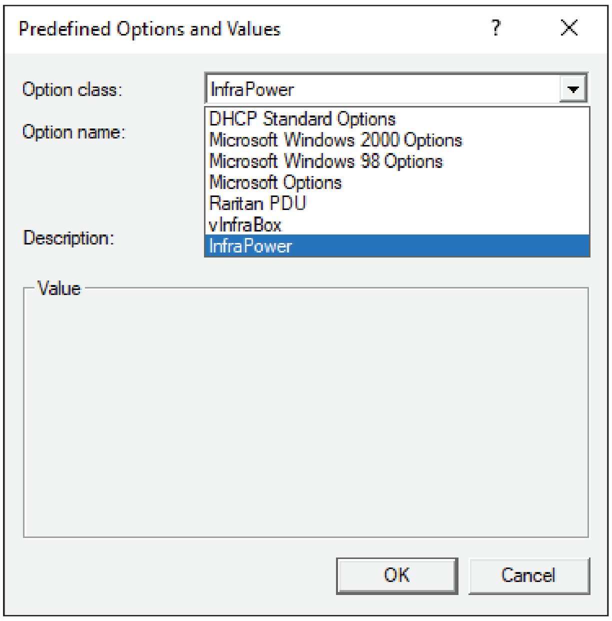
Description:

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

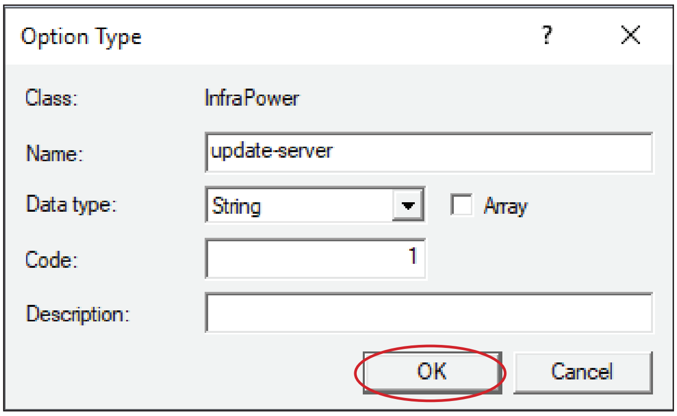
Option class: InfraPower

Option name:

Description:

Value

- 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** “.



Option Type

Class: InfraPower

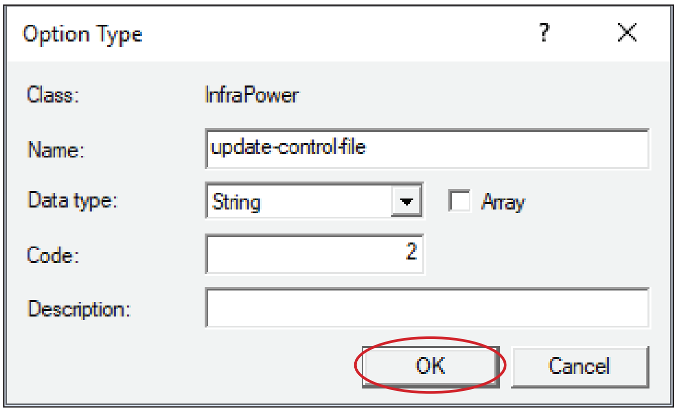
Name: update-server

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** “.



Option Type

Class: InfraPower

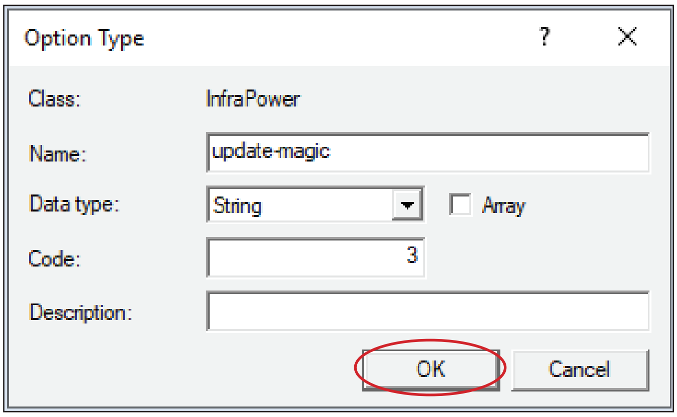
Name: update-control-file

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** “.



Option Type

Class: InfraPower

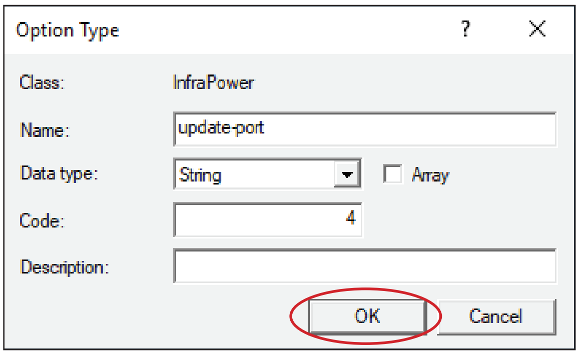
Name: update-magic

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

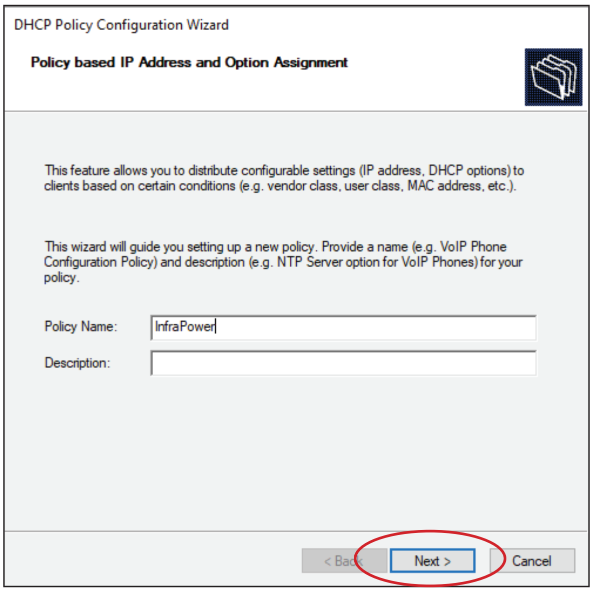
Data type: String □ Array

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

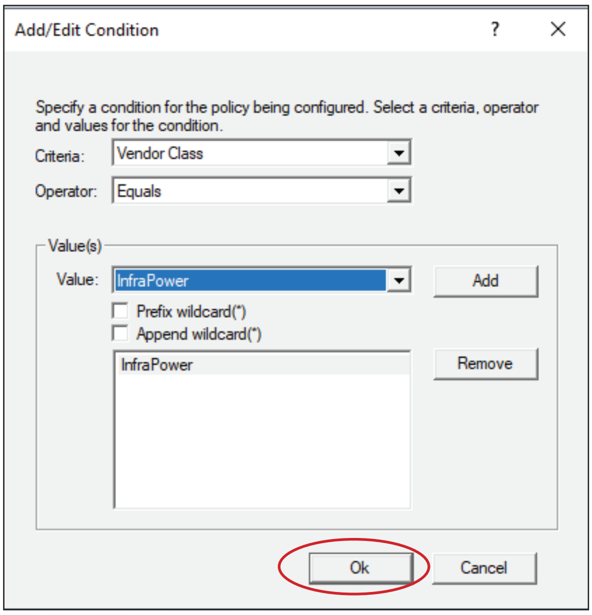
This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

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)

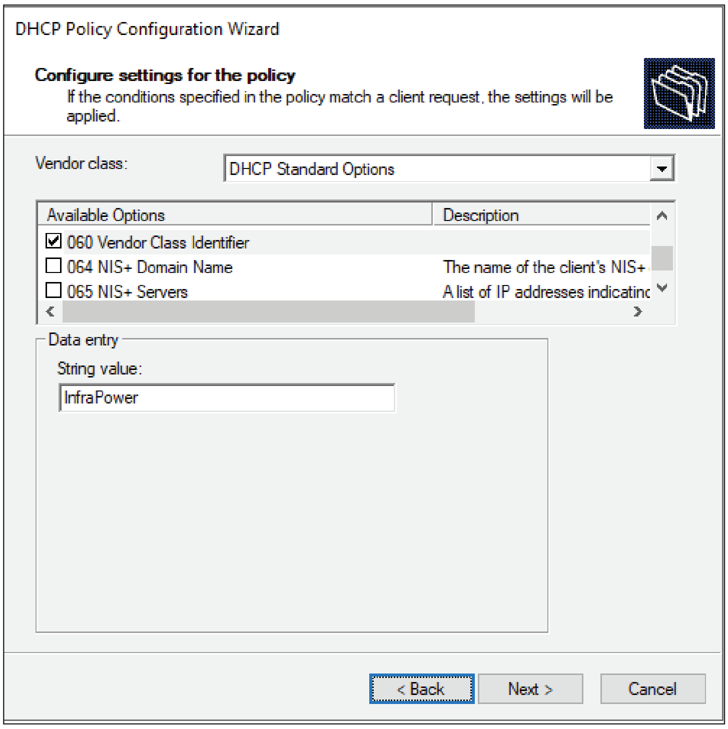
Value: InfraPower

□ Prefix wildcard(*)

□ Append wildcard(*)

InfraPower

- 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.

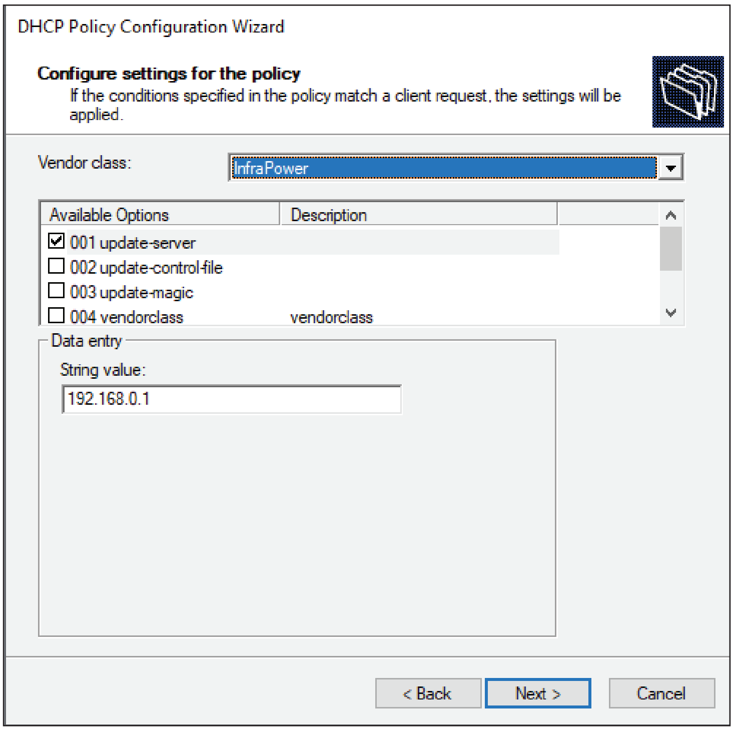
Vendor class: DHCP Standard Options

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.

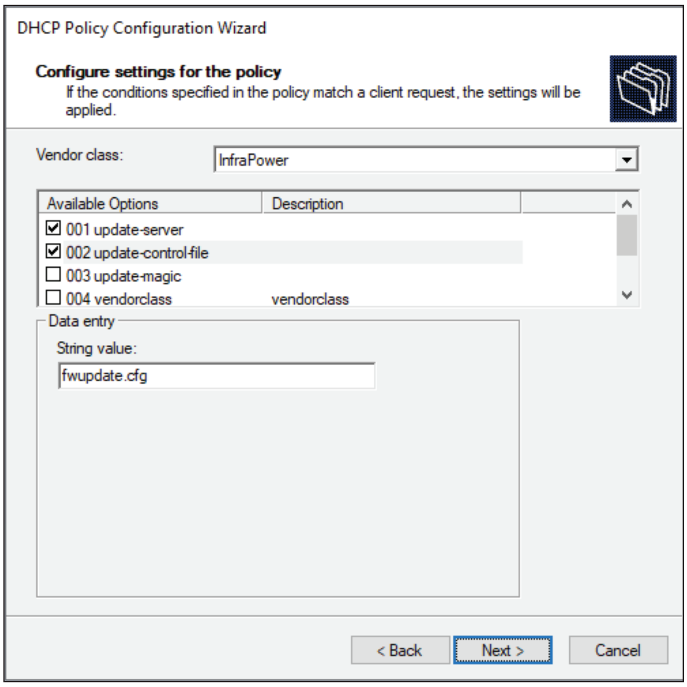
Vendor class: InfraPower

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.

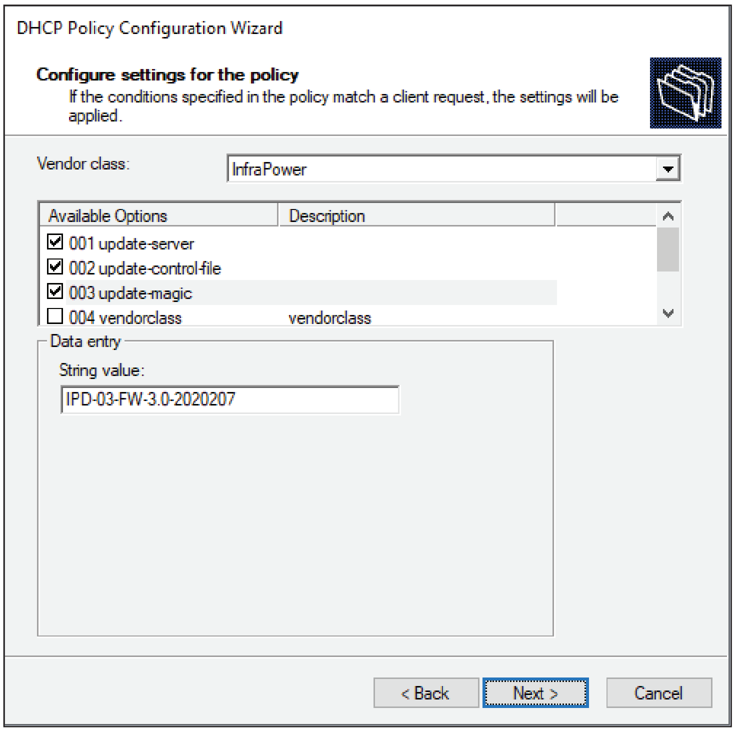
Vendor class: InfraPower

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

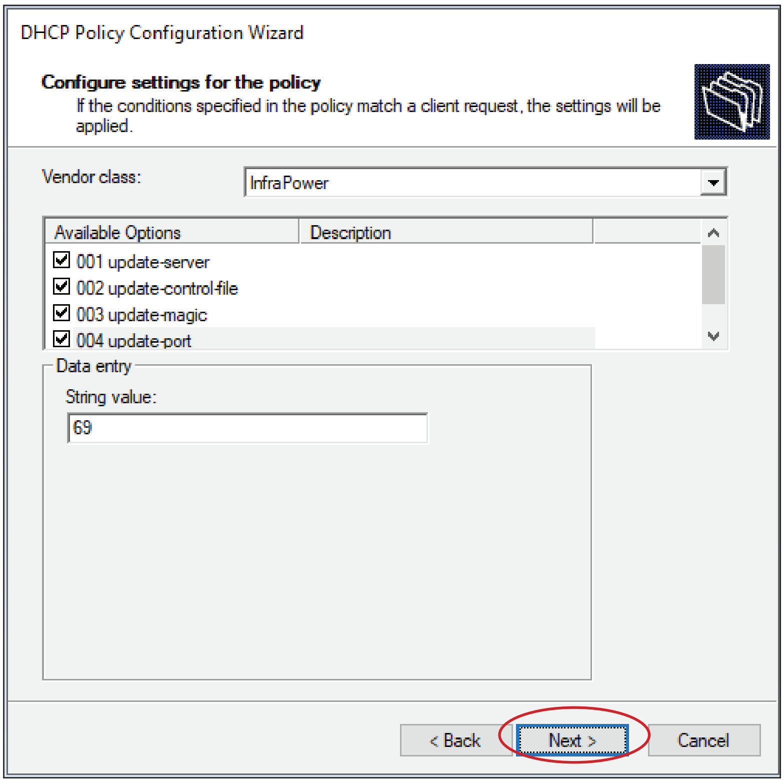
Data entry

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

⚠ The magic code is transmitted to and stored in IP Dongle 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 the IP Dongle. Therefore, you must modify the magic code’s value in DHCP when intending to execute the “ **fwupdate.cfg** ” commands next time.

< 1.15 > Bulk Firmware Upgrade

- 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.
Available Options
Description
Data entry
< Back
Next >
Cancel

Vendor class: InfraPower

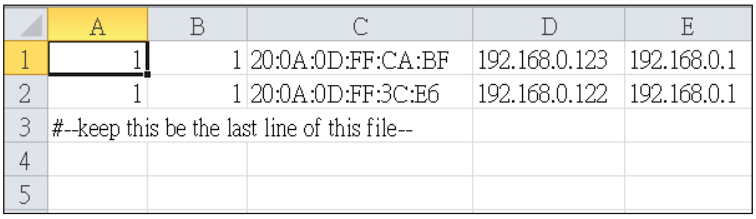
☑ 001 update-server
☑ 002 update-control-file
☑ 003 update-magic
☑ 004 update-port

String value: 69

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

< 1.15 > Bulk Firmware Upgrade

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					

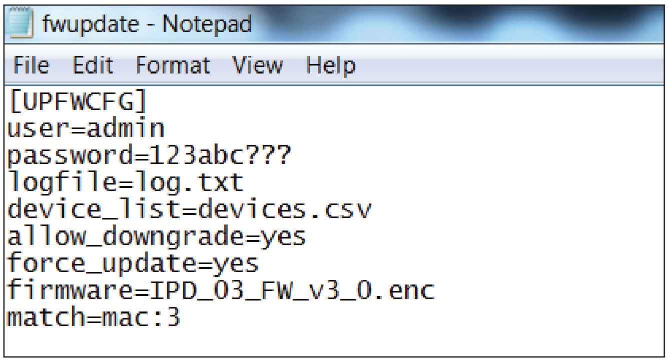
Column A & B is reserved for future use

Column C is the MAC address of the network interface of the IP Dongle. As the IP Dongle

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 IP Dongle 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 IP Dongle.

Fifth row lets IP Dongle 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.

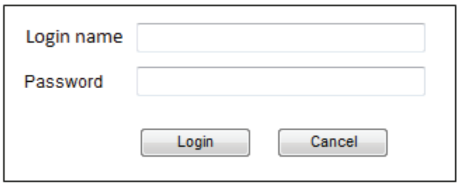
< 1.16 > DHCP Setting

Step 1. Connect the IP dongle to the computer (Please refer to < 1.4 > IP dongle configuration)

Step 2. Open the MS Edge

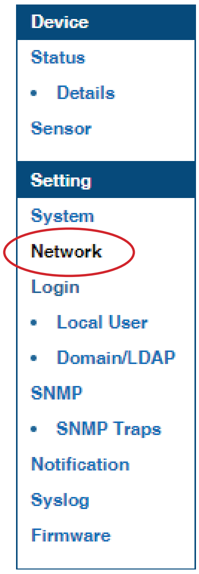
Step 3. Enter the configured IP Dongle address into the address bar.
Default IP address of LAN 1 is “ **192.168.11.1** “
Default IP address of LAN 2 is “ **192.168.0.1** “

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

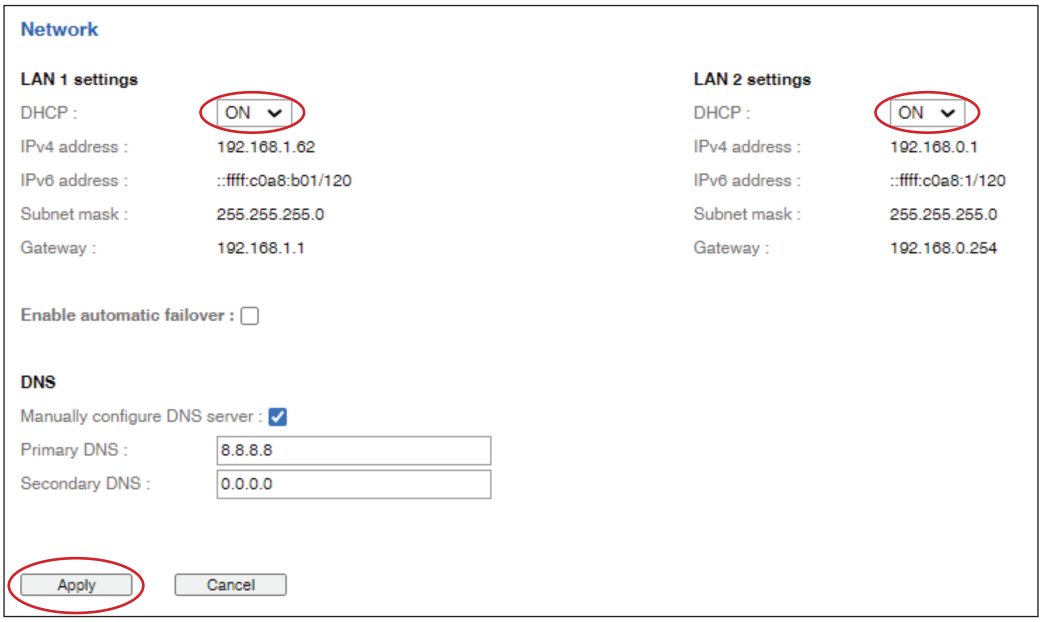


- Default login name: 00000000
- Password: the one you set in Step 7 of < 1.4 > IP Dongle Configuration.

Step 5. Select “ **Network** “ from the left navigation pane.



Step 6. Dual Lan Mode: Select “ **ON** “ from “ **DHCP** “ of LAN 1 & LAN 2.
Click “ **Apply** “ to save the settings.



Network

LAN 1 settings

DHCP :	ON
IPv4 address :	192.168.1.62
IPv6 address :	::ffff:c0a8:b01/120
Subnet mask :	255.255.255.0
Gateway :	192.168.1.1

LAN 2 settings

DHCP :	ON
IPv4 address :	192.168.0.1
IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0
Gateway :	192.168.0.254

Enable automatic failover : □

DNS

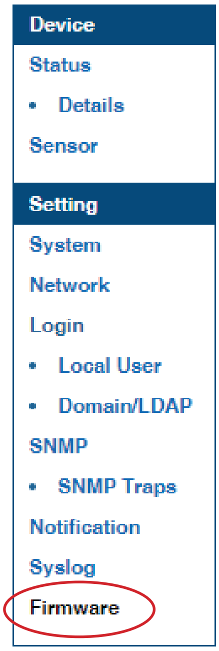
Manually configure DNS server : ☑

Primary DNS : 8.8.8.8

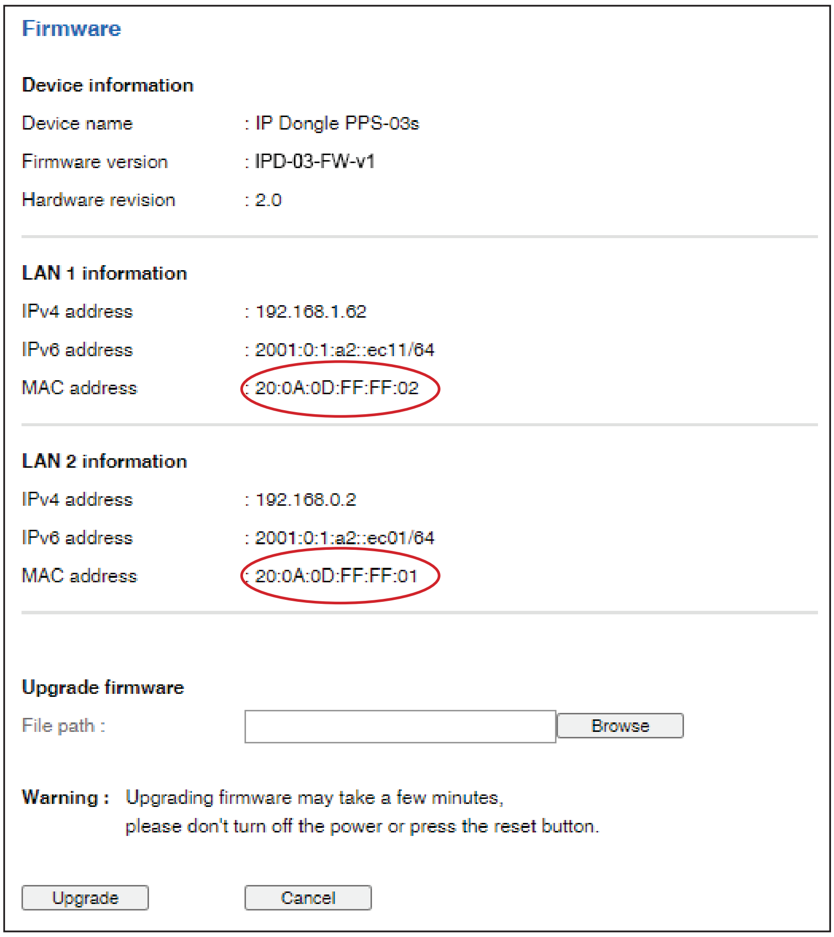
Secondary DNS : 0.0.0.0

< 1.16 > DHCP Setting

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



Step 8. Record the " **MAC address** " of LAN 1 & LAN 2.



Firmware

Device information

Device name : IP Dongle PPS-03s

Firmware version : IPD-03-FW-v1

Hardware revision : 2.0

LAN 1 information

IPv4 address : 192.168.1.62

IPv6 address : 2001:0:1:a2::ec11/64

MAC address : 20:0A:0D:FF:FF:02

LAN 2 information

IPv4 address : 192.168.0.2

IPv6 address : 2001:0:1:a2::ec01/64

MAC address : 20:0A:0D:FF:FF:01

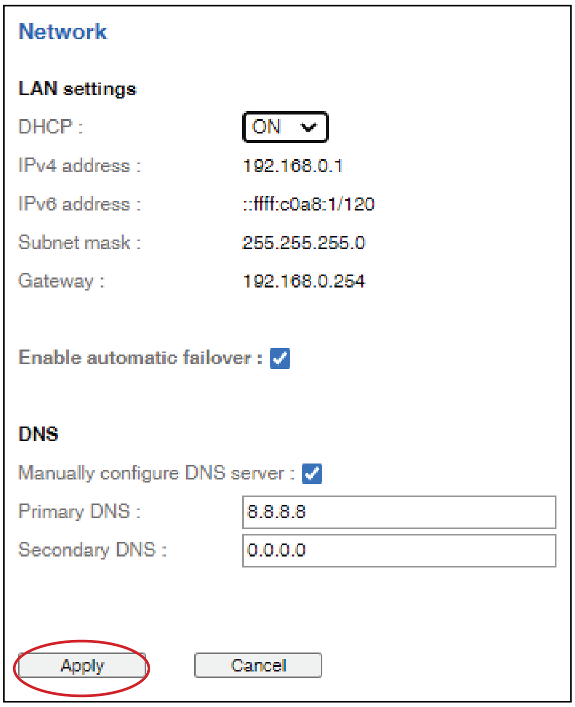
Upgrade firmware

File path :

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

Step 9. Assign an IP addressof LAN 1 & LAN 2 of to the IP Dongle from your DHCP server.

Step 10. Failover Mode: Select “ **ON** “ from “ **DHCP** “ & Click “ **Apply** “ to save the settings.



Network

LAN settings

DHCP :	ON
IPv4 address :	192.168.0.1
IPv6 address :	::ffff:c0a8:1/120
Subnet mask :	255.255.255.0
Gateway :	192.168.0.254

Enable automatic failover : ☑

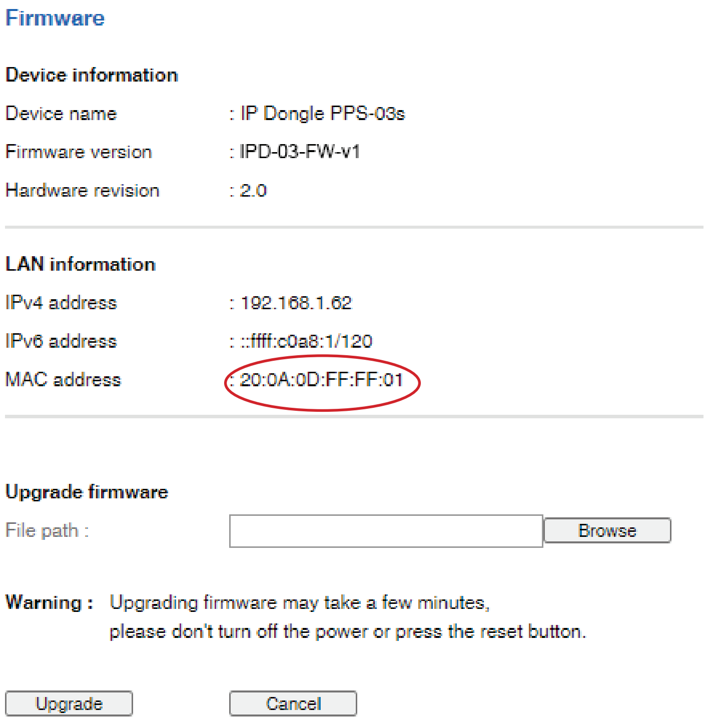
DNS

Manually configure DNS server : ☑

Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

Step 11. Select “ **Firmware** “ from the left navigation pane.

Step 12. Record the “ **MAC address** “.



Firmware

Device information

Device name	: IP Dongle PPS-03s
Firmware version	: IPD-03-FW-v1
Hardware revision	: 2.0

LAN information

IPv4 address	: 192.168.1.62
IPv6 address	: ::ffff:c0a8:1/120
MAC address	: 20:0A:0D:FF:FF:01

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 13. Assign an IP address to the IP Dongle from your DHCP server.

• **Complete**

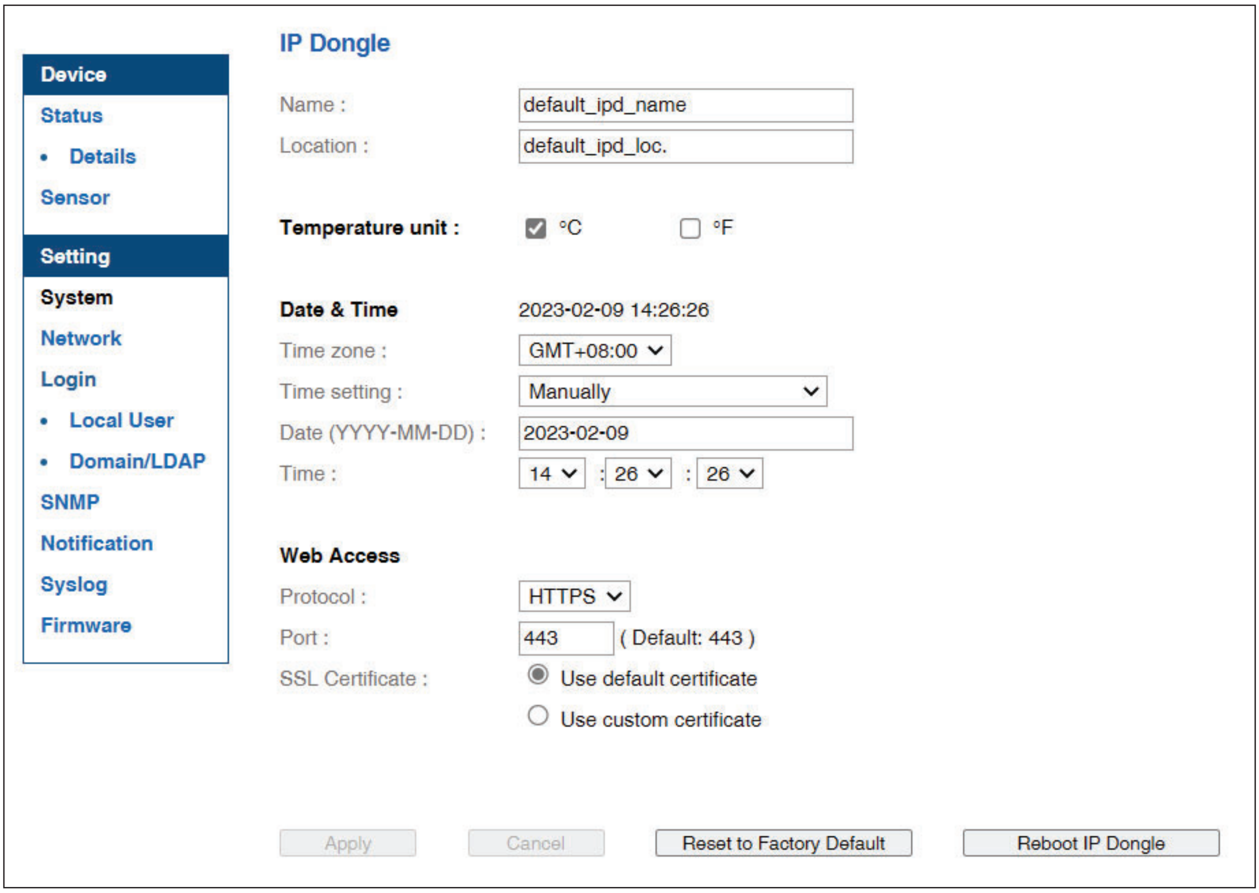
< 1.17 > 802.1X authentication

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.

802.1X authentication function ONLY available at IP Dongle firmware version v3.0 or above.

Before configure the 802.1X authentication, ensure the system clock of the IP Dongle 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 IP Dongle to set up the date and time of the IP Dongle.



IP Dongle

Name : default_ipd_name

Location : default_ipd_loc.

Temperature unit : ☑ °C □ °F

Date & Time 2023-02-09 14:26:26

Time zone : GMT+08:00

Time setting : Manually

Date (YYYY-MM-DD) : 2023-02-09

Time : 14 : 26 : 26

Web Access

Protocol : HTTPS

Port : 443 (Default: 443)

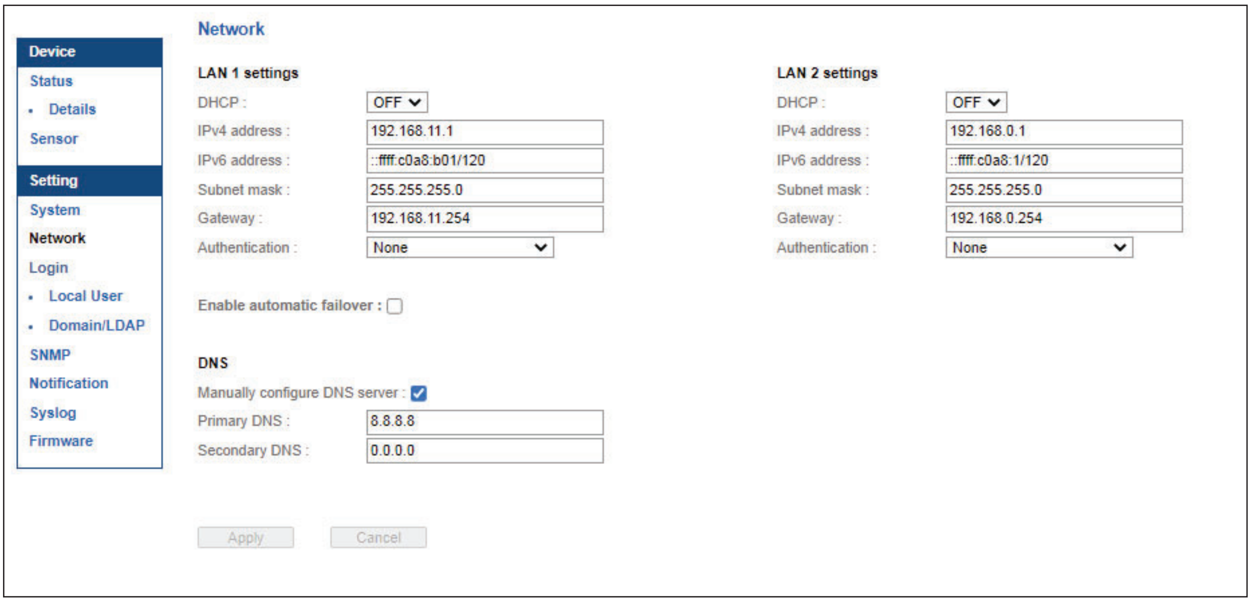
SSL Certificate : ● Use default certificate ○ Use custom certificate

< 1.17 >   802.1X authentication

Please follow the procedures below to setup the 802.1X authentication in IP Dongle.

< 802.1X authentication for Wired network >

Step 1. Login the IP Dongle WEBUI and go the Network.



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

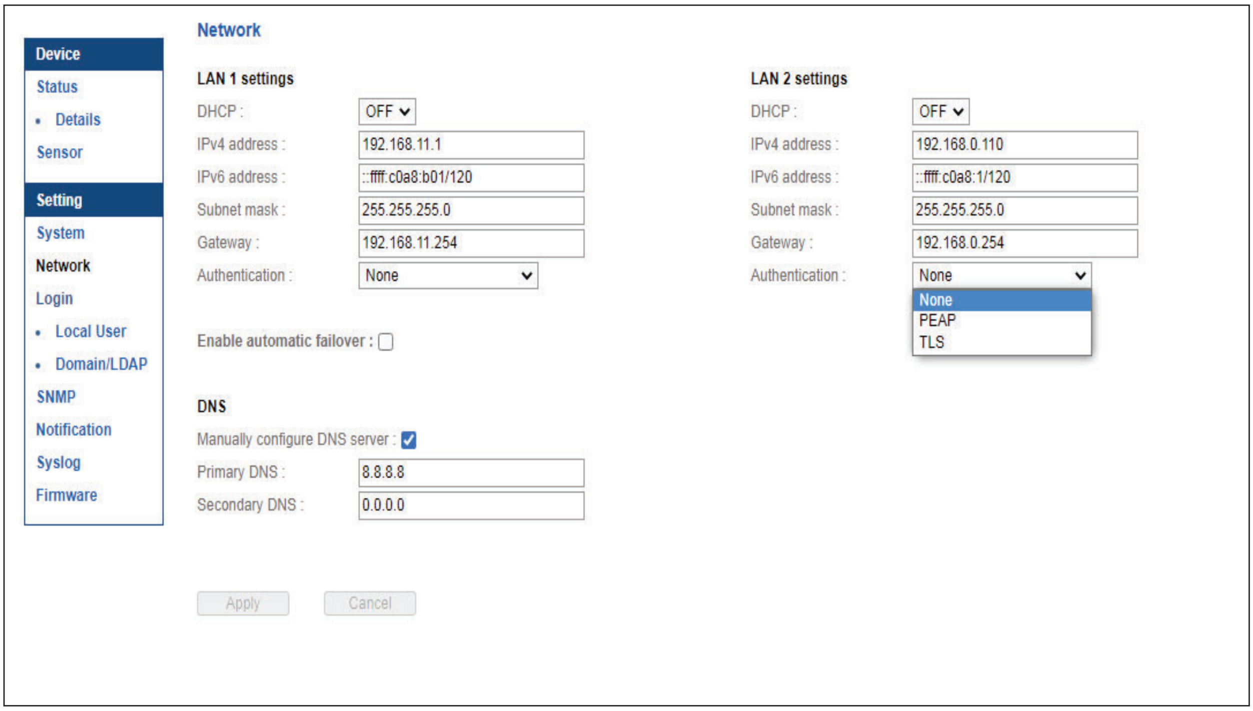
DHCP : OFF
IPv4 address : 192.168.0.1
IPv6 address : ::ffff:c0a8:1/120
Subnet mask : 255.255.255.0
Gateway : 192.168.0.254
Authentication : None

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

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

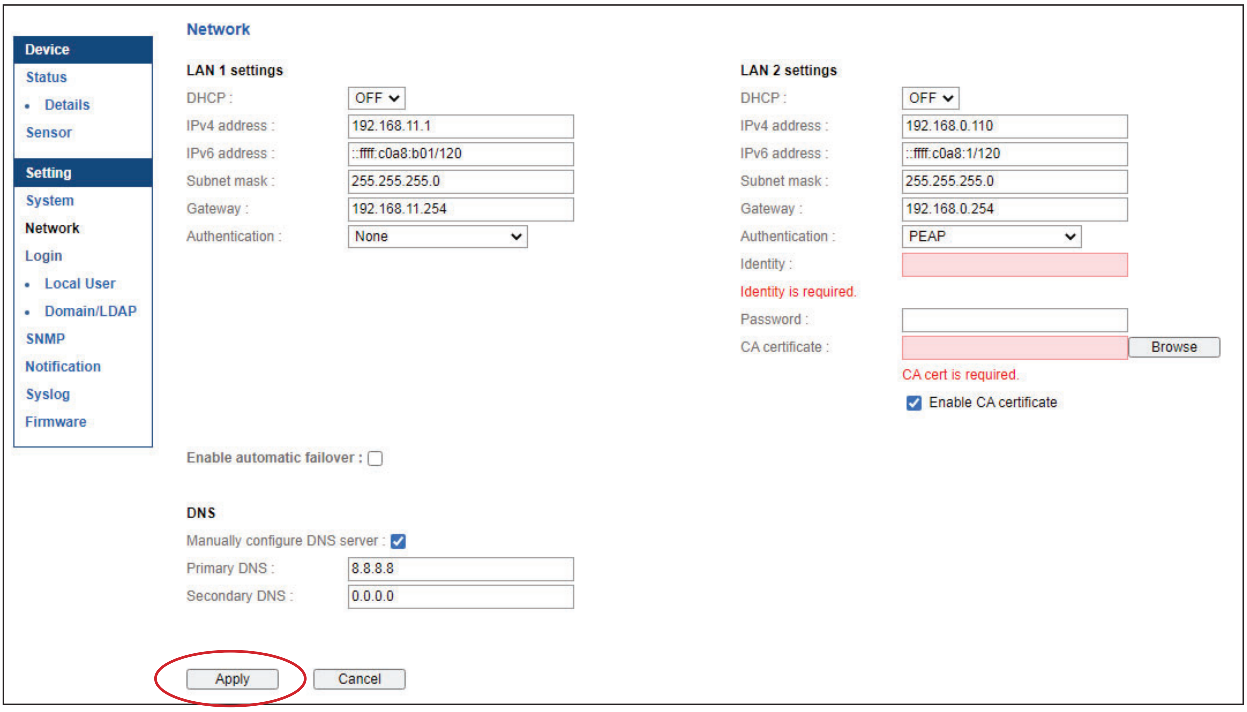
Enable automatic failover : □

DNS

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

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

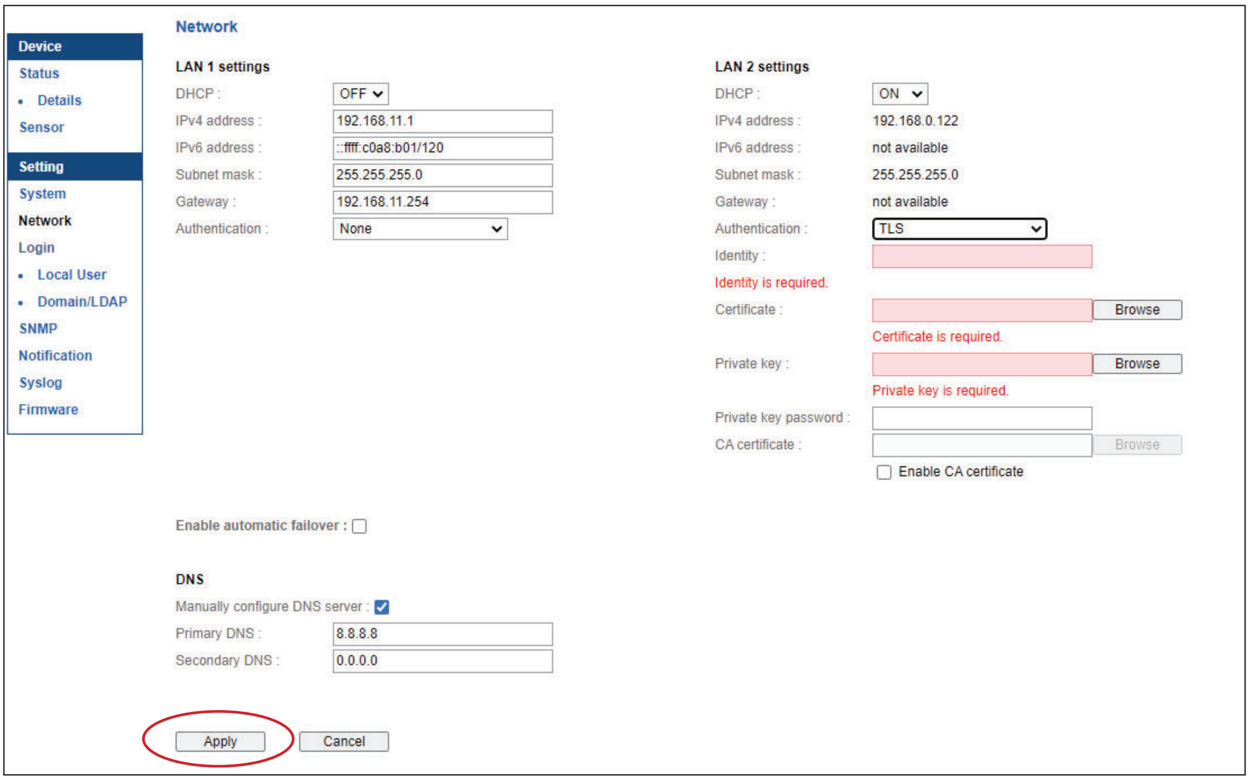
Enable automatic failover : □

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 : □

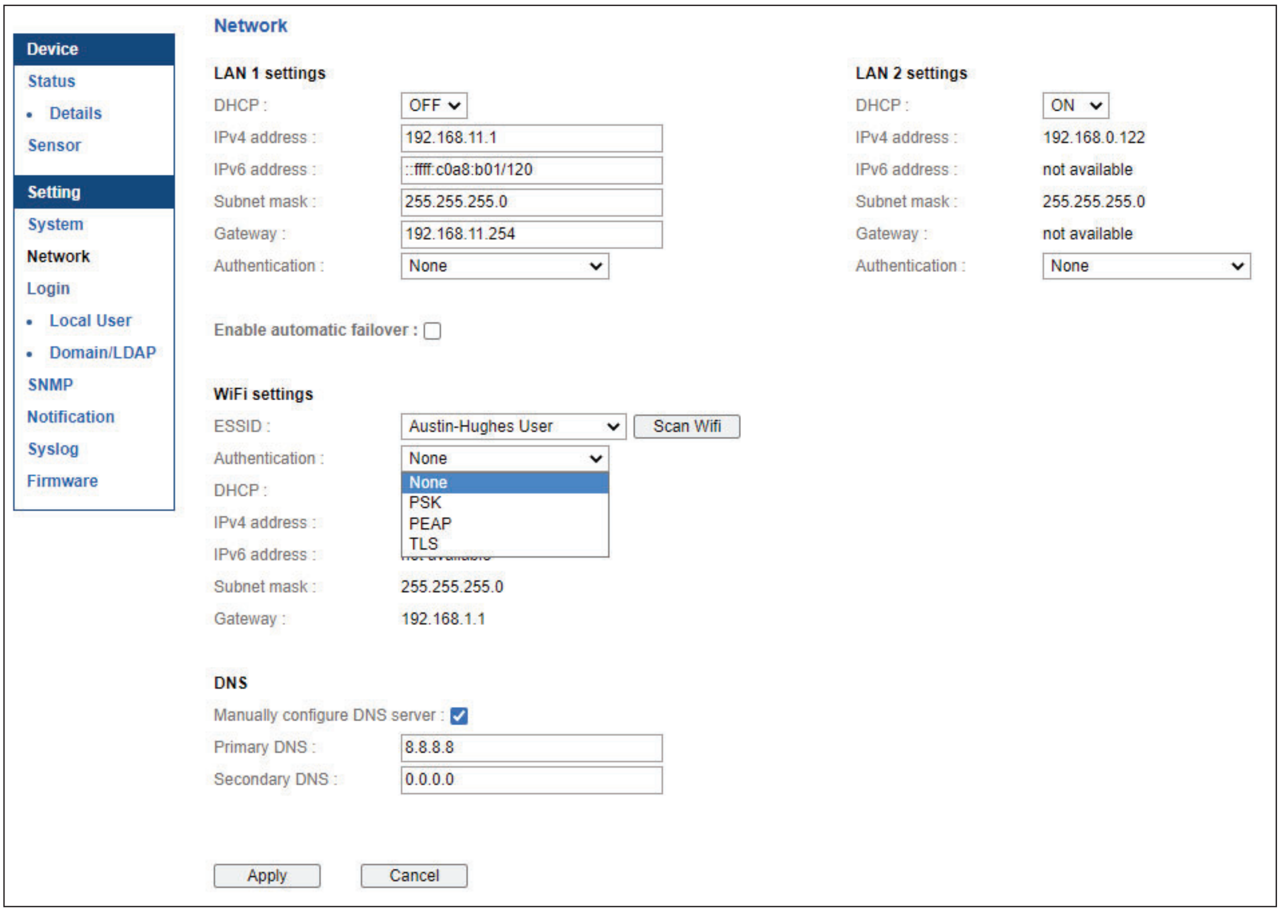
DNS

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

< 1.17 >   802.1X authentication

< 802.1X authentication for Wireless network >

Step 1. Login the IP Dongle WEBUI and go to Network. Click the Authentication pull down menu and you will see the authentication method



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 : None

Enable automatic failover : □

WiFi settings

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

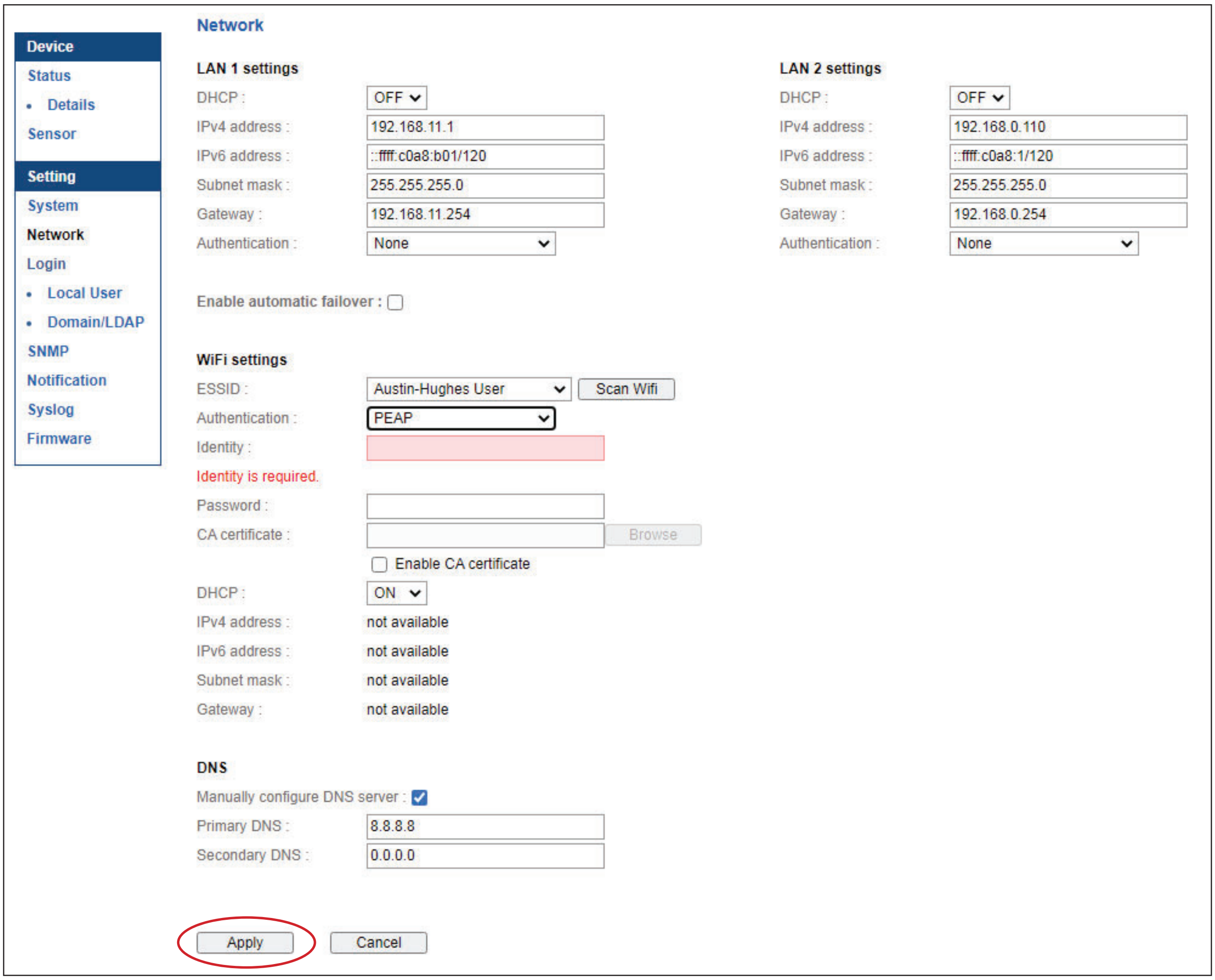
< 1.17 >   802.1X authentication

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 :	
Password :	
CA certificate :	
	□ Enable CA certificate
DHCP :	ON
IPv4 address :	not available
IPv6 address :	not available
Subnet mask :	not available
Gateway :	not available

Identity is required.

DNS

Manually configure DNS server : ☑

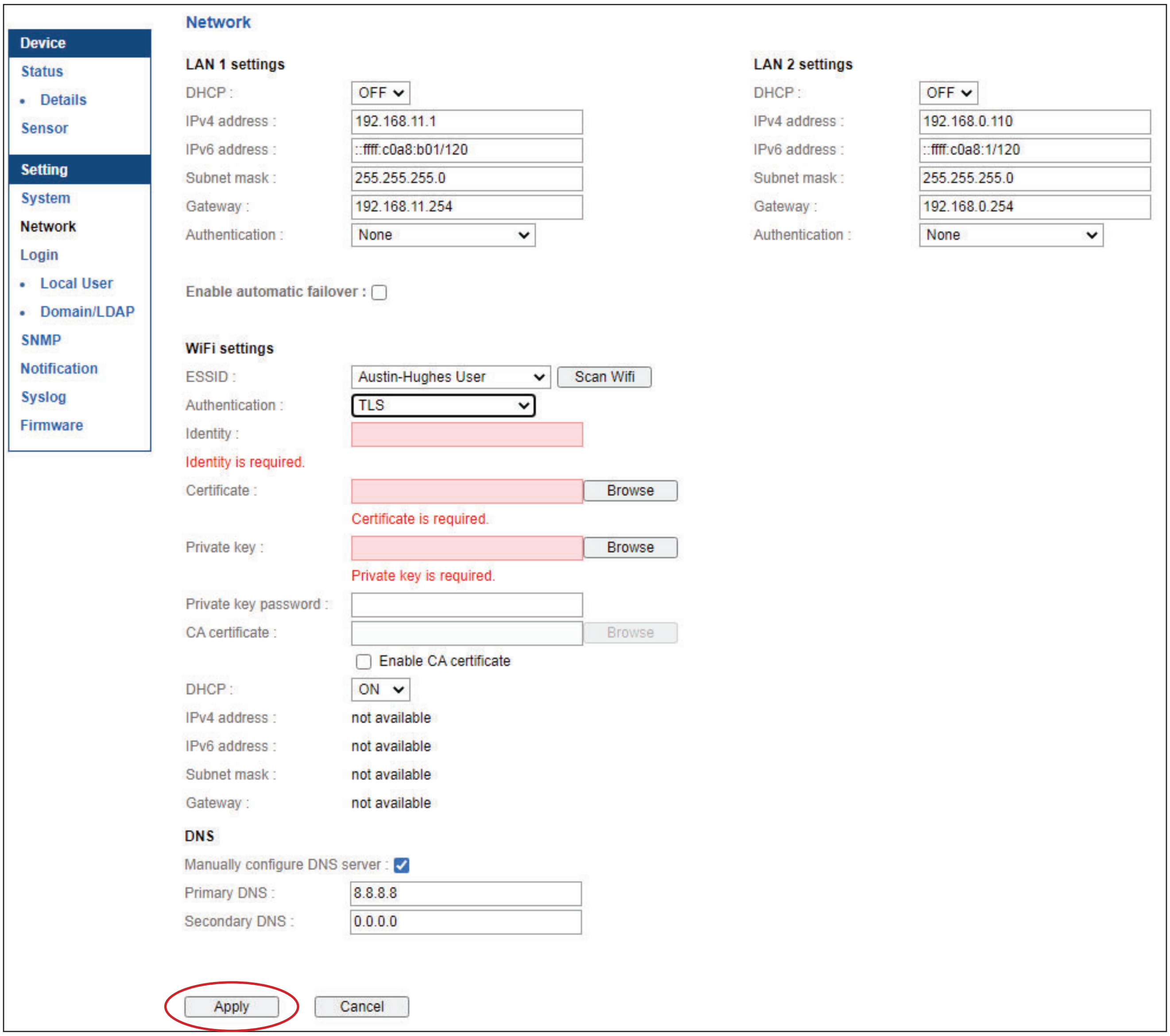
Primary DNS :	8.8.8.8
Secondary DNS :	0.0.0.0

Step 3. To use TLS as authentication method, select TLS. Select the Wireless network from " **ESSID** ", input the " **Identity** ", " **Certificate** ", " **Private key** ", " **Private key pass word** " 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

< 1.18 > Command Line Interface (CLI) Access

Command Line Interface (CLI) allows you access the IP dongle 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 IP dongle.

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

CLI and IP dongle WEBUI 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 WEBUI
   - Change system RTC date time : set the system time of the IP Dongle
   - Change network settings : change the IP settings of the IP Dongle
   - 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 (When disabled, IP dongle CANNOT be found by IP setup utilities)
     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

< 1.19 > Optional Accessories - Wifi Kit

Part I.   Package and Technical Specification

WIFI Kit (IPD-WIFI)

- Antenna x 1
- USB wireless adapter x 1
- Magnetic stand with 1M antenna wire x 1

Unpacking

The equipment comes with the standard parts shown on the package contents. Check and make sure they are included and in good condition. If anything is missing, or damage, contact the supplier immediately.

IPD-WIFI Wireless Specification	
IEEE Standards	IEEE 802.11a / b / g / n / ac
Operating Frequencies	2.4GHz~2.4835GHz / 5.15GHz~5.85GHz
Modulation	・802.11b : CCK, DQPSK, DBPSK ・802.11a/g : 64-QAM, 16-QAM, QPSK, BPSKz ・802.11n : 64-QAM, 16-QAM, QPSK, BPSK ・802.11ac : 256-QAM, 64-QAM, 16-QAM, QPSK, BPSK BT, 8DPSK, π/4DQPSK, GFSK
Wireless Date Rate	・802.11b : 1, 2, 5.5, 11 Mbps ・802.11a/g : 6, 9, 12, 18, 24, 36, 48, 54 Mbps ・802.11n : HT20 reach up to 72.2Mbps, HT40 reach up to 150Mbps ・802.11ac : VHT20 reach up to 86.7Mbps, VHT40 reach up to 200Mbps, VHT80 reach up to 433.3Mbps
Security	・WPA2 - Personal ・WPA2 - Enterprise

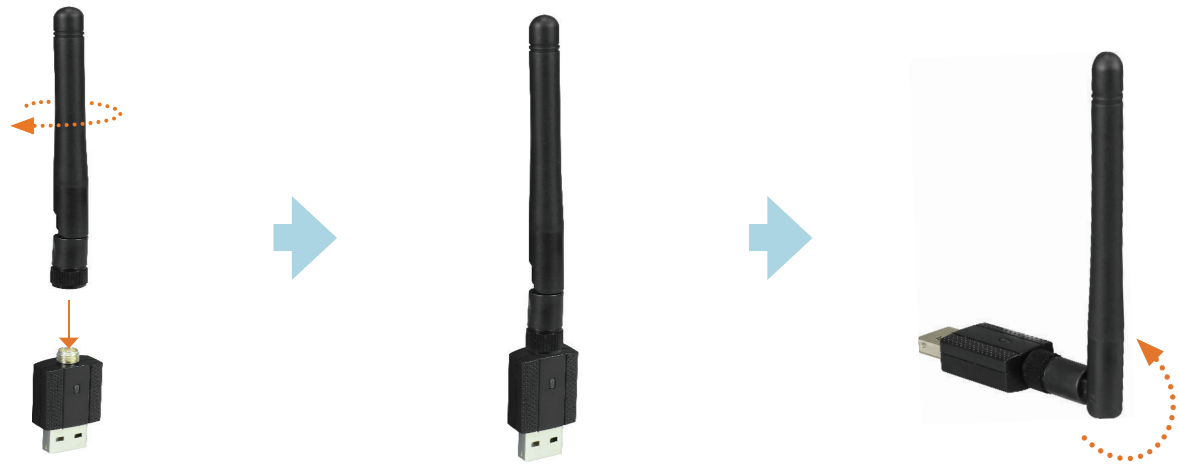
< 1.19 > Optional Accessories - Wifi Kit

Part II. Hardware Connection

Antenna + USB Wireless Adaptor

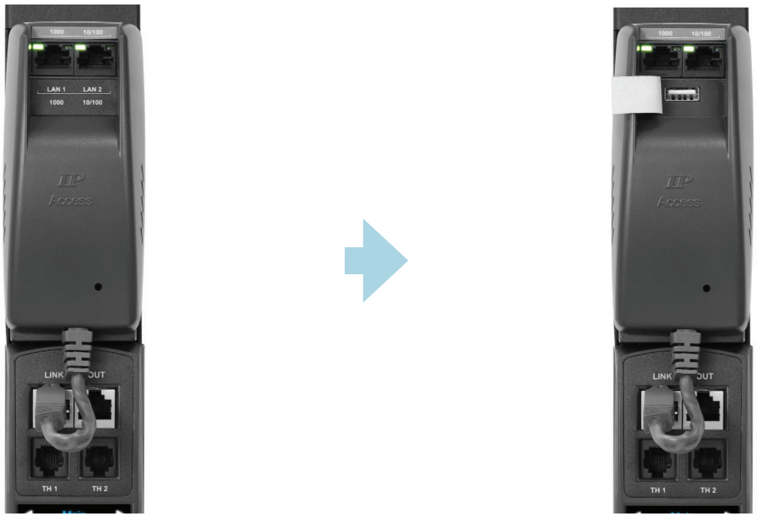
Step < 1 >

- Inset and screw the antenna to the USB wireless adapter. Fix the antenna in place & lift it up.



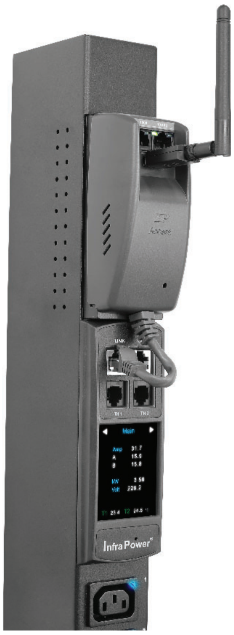
Step < 2 >

- Take out the membrane from the PDU dongle, and the WIFI USB port will be found.



Step < 3 >

- Connect the USB wireless adapter (with antenna) to PDU dongle

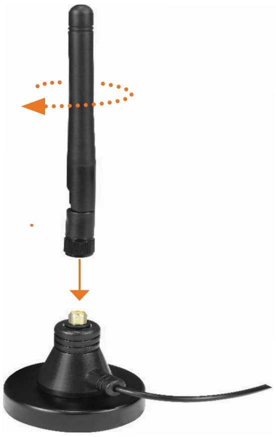


< 1.19 > Optional Accessories - Wifi Kit

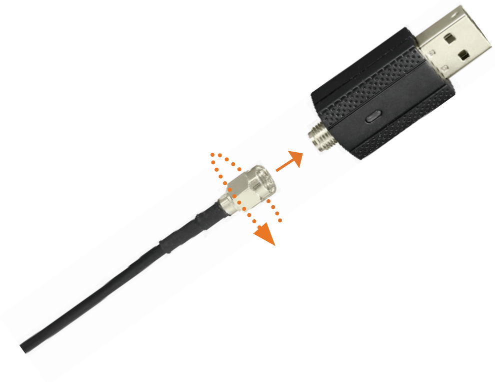
Antenna + USB Wireless Adaptor + Magnetic Stand with Antenna Wire

Step < 1 >

■ Inset and screw the antenna to the magnetic stand, and fix the antenna in place.

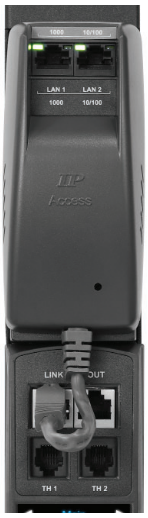


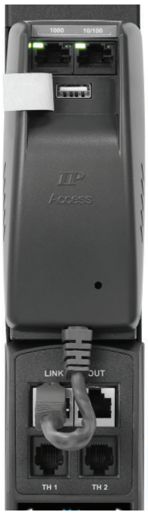
■ Inset and screw the 1M antenna wire to USB wireless adapter, and fix the adapter in place.



Step < 2 >

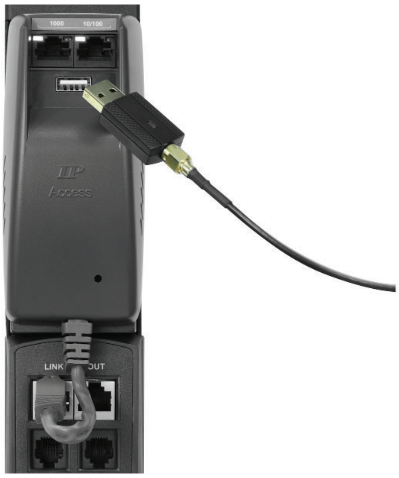
■ Take out the membrane from the PDU dongle, and the WIFI USB port will be found.





Step < 3 >

■ Connect USB wireless adapter to PDU dongle.



■ Affix the magnetic stand (with antenna) to the desirable area of rack.

Intentionally
Left
Blank

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.