Inova

User Manual

Intelligent Power Distribution Unit

Content

Part Ⅰ. General Information

Important Safety Information

Read the instructions carefully to become familiar with the equipment before trying to install, operate, service or maintain it. The following messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards.

Obey all safety messages that follow this symbol to avoid possible injury or death.

The following blocks will appear again in the following chapters. Please pay special attention to those safety notices.

DANGER

Danger indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING

Warning indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury;

CAUTION

Caution indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

NOTICE

Notice addresses practices not related to physical injury including certain environmental hazards, potential damage, or loss of data.

SAFETY NOTICE

This product has not been tested for Radio Frequency Interference. Sale of this product where Radio Frequency Interference testing is required is prohibited. This includes North America and Japan.

Part Ⅱ . Introduction

Product Features

The Power Distribution Unit (PDU) may be used as a stand-alone, network manageable power distribution device. The PDU provides real-time remote monitoring of connected loads. User-defined alarms warn of potential circuit overloads. You can manage a PDU through its Web User Interface (Web UI), Command Line Interface (CLI), or Simple Network Management Protocol (SNMP).

The PDU has these additional features:

- ✧ Monitor device power, apparent power, power factor, energy, and frequency.
- ✧ Monitor phase voltage, current, power, apparent power, power factor and energy.
- ✧ Monitor outlet status, current, voltage, power, apparent power, power factor, energy, and loads status.
- ✧ Individual outlet control and outlet group control for switched PDUs (Only for the Switch per Outlet type PDUs).
- ✧ Configurable alarm thresholds with network access to help avoid overloaded circuits.
- ✧ Email notifications for PDU and system events.
- ✧ Various levels of access: Admin User, Super User and Read Only.
- ✧ Event logging (400 events).
- ✧ SNMP traps (V1, V2c, and V3) based on the severity level or category of system event.
- ✧ Security protocols for authentication and encryption.
- ✧ Up to 32 PDUs of any type can be cascaded using the PDU In and PDU Out ports so that only the one network connection is necessary.
- ✧ USB port, Firmware upgrade and system events export.
- ✧ Synchronize the time with the SNTP Server.

NOTE: There is no Real Time Clock (RTC) battery on this device. You will need to set a SNTP server for the first log in.

Getting Started

To start the PDU:

- Install the PDU refer to the Power Distribution Unit Installation Instructions.
- Apply power and connect to your network. Follow the directions in the Power Distribution Unit Installation Instructions.
- Establish network settings (more detail refers to **Page 8**)
- Begin using the PDU by one of the following ways:
  - Web User Interface (more detail refers to **Page 14**).
  - PDU Controller (more detail refers to **Page 12**).
  - SNMP protocol (more detail refers to **Page 32**).
  - Command Line Interface (CLI) (more detail refers to **Appendix F**).

Establish Network Settings

DHCP Configuration

The default TCP/IP configuration setting, DHCP, assumes that a properly configured DHCP server is available to provide TCP/IP settings to the PDU.

Connect a Computer by Ethernet

Notices: Please use a router or other network device to get the IP address of PDU before configuring the Ethernet network.

PDU can directly connect a computer with Ethernet network:

- The computer need set to DHCP mode.
- The computer need disable wireless network.
- Find the IP address from LCD display (more detail refers to Figure 4).

Static IP Configuration

You must define three TCP/IP settings for the PDU before it can operate on the network:

- The IP address of the PDU.
- The subnet mask of the PDU.
- The IP address of the default gateway (only needed if you are going off segment).

Command Line Interface (CLI)

- Connect to Serial Port (Configure the port for 115200 bps, 8 data bits, no parity, 1 stop bit, and no flow control).

- Log on to the CLI (default account: admin/admin).
- Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the PDU.
- Use these three commands to configure network settings. (Text in italics indicates a variable.

  tcpip-i yourIPaddress tcpip-s yourSubnetMask

  tcpip-g yourdefaultgateway

  For each variable, type a numeric value that has the format xxx.xxx.xxx.xxx.

  For example, to set a system IP address of 156.205.14.141, type the following command and press ENTER: *tcpip -i 156.205.14.141*

- Type *reboot*. The PDU restarts to apply the changes.

  For detailed information on how to configure the TCP/IP settings in a PDU, refer to “IPv4” on Page 29.

Network Port Sharing (NPS)

About the Network Port Sharing Feature

You can use the NPS feature to view the status of and configure and manage up to 32 PDUs using only one network connection. This is made possible by connecting the PDUs via the In and Out ports on the PDU front panel.

Display ID

The display ID is a number, 00 to 31, used to uniquely identify the PDU in a group. After two or more PDUs are connected to one another in an NPS group, they can be identified on the various interfaces using this "Display ID". This Display ID is viewable in the left bottom of the display.

Installation Instruction

Connect to 32 PDUs via the PDU In and PDU Out ports on the PDU.

NOTE: Only one PDU in an NPS group is allowed to be the host. The Display ID for host is 00.

Specific Assignment of Display IDs

The default ID is 01. You need to define a host device and change the ID to 00.

- On the controller display, press the ⓬**Menu** button to open the main menu, press the ❸ **Scroll** button to **4-RS485ID**, then press ❹ Select button.
- Press the ❸ Scroll button to **2-DOWN** – to decrease the ID number to 00, press the ❸ **Scroll** button to **3-OK** to finish.

Use the SET ID menu to assign a unique ID to each guest device. The PDU group is now available via the Host's IP address. (see figure2)

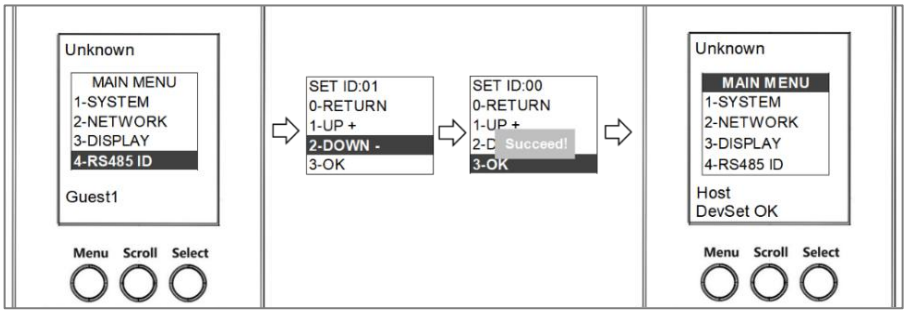


Figure 1. Set UP LCD Display ID

Reset to Defaults

Using the LCD Menu

Reset to Defaults via LCD menu even in case of forgot the password:

- On the controller display, press the ⓬Menu button to open the main menu, press the ❸ Scroll button to 1-SYSTEM, press ❹ Select button.
- Press the ❸ Scroll button to 3-Resets, press ❹ Select button.
- Press the ❸ Scroll button to 1-CPU, press ❹ Select button.
- Press the ❸ Scroll button to 1-Defalut, press ❹ Select button to finish.
- Use the default account to login into the PDU.

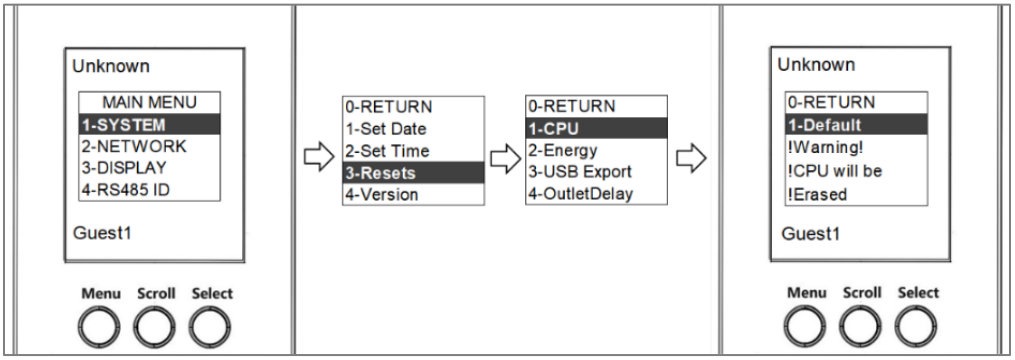


Figure 2. Rest to Defaults via LCD Menu

Using the Command Line Interface

To use a local computer (a computer that connects to the PDU or other device) through the serial port to access the Command Line Interface:

- Select a serial port at the local computer and disable any service that uses that port.
- Connect the serial cable to the selected port on the computer and to the ❺ Serial port of the PDU.
- Run a terminal program (such as Tera Term® or HyperTerminal®) and configure the selected port (115200 bps, 8 data bits, no parity, 1 stop bit, and no flow control).
- Press ENTER, repeat press, if necessary, to display the username prompt. Then use the default for the username and password.
- At the Command Line Interface, use the following commands to default the parameters *`reset [-a] Reset All parameters reset [-d] Reset Device parameters reset [-n] Reset Network parameters reset [-c] Remove Certificate`*
- Type *`reboot`* to restart the device.

NOTE: Press the Reset button on the LCD front panel only to reboot the device itself without resetting to defaults.

Part III. Controller Overview

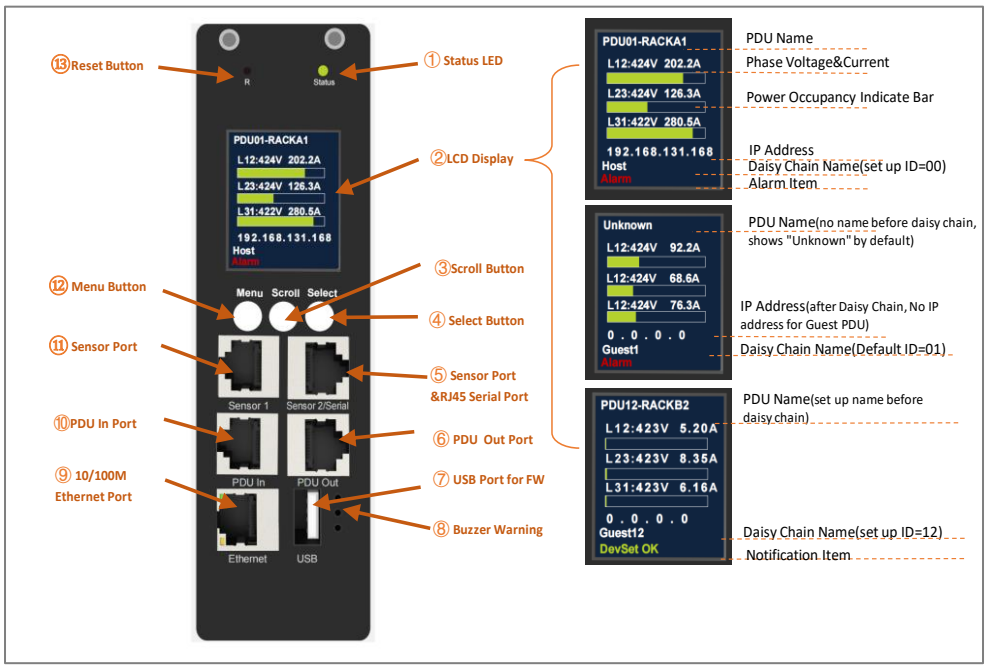


Table 1. Controller Display and Interfaces

Item	Function	Description
❶	Status Light	Solid Green:Normal operation Solid Red:Critical or Warning Alarm
❷	LCD Display	Show information about the Rack PDU.
❸	Scroll Button	Use the Scroll button to move through displayed information.
❹	Select Button	With a menu option highlighted, press the Select button to display the selected Rack PDU information.
❺	Temp/Humidity Port & RJ45 Serial Port	Temp/Humidity Sensor connection port. Serial commuication port.
❻	PDU Out Port	RS485 port for use with Network Port Sharing feature.
❼	USB Port	Connect flash drive for firmware upgrades or to download data logs.
❽	Buzzer Warning	Warning device
❾	10/100M Ethernet Port	Connect the Rack PDU to the network.
❿	PDU In Port	RS485 port for use with Network Port Sharing feature.
⓫	Temp/Humidity Port	Temp/Humidity Sensor connection port.
⓬	Menu Button	Press to view the Rack PDU electrical input.
⓭	Reset Button	Reset the Rack PDU without affecting the status of the outlets.

Connect to PDU by Ethernet Port

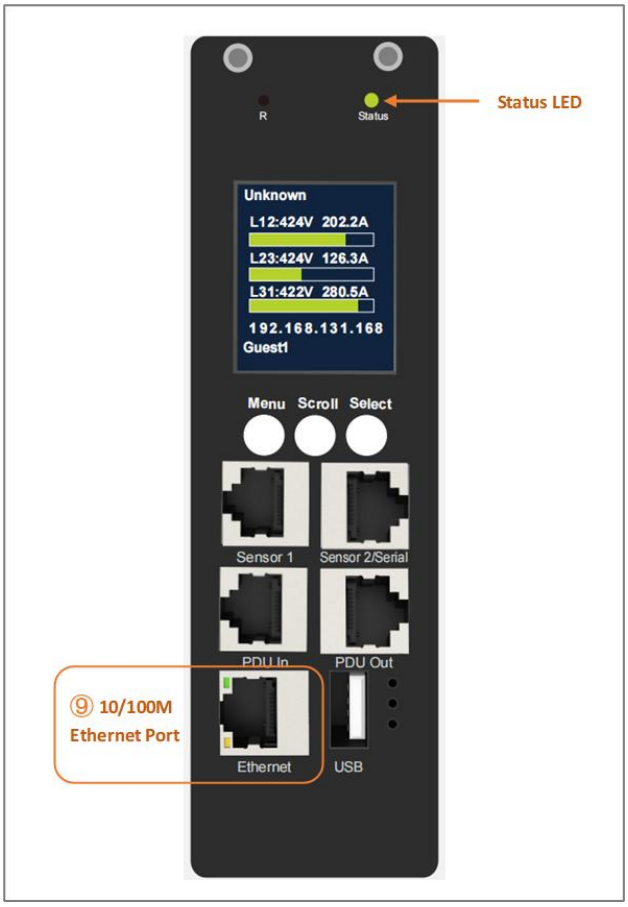


Figure 3. Ethernet Port

Connect the PDU via Ethernet or LAN to monitor and control intelligent PDU devices:

- Connect one end of the network cable to the Ethernet port of the PDU.
- Connect one end of the cable to the PDU Ethernet port. Connect the other end of the cable to an Ethernet router, switch, or other LAN port.

The PDU defaults to DHCP and HTTPS connections at the factory. If you connect to a network with a DHCP server, the PDU automatically receives the IP address and displays it on the LCD. If no DHCP server is searched after a few minutes, the LCD display shows the IP address as 0.0.0.0, unplug and re-plug the network cable and the PDU will restart the DHCP server search process.

NOTE: Ethernet port on the PDU indicates solid green light on the right and a flashing yellow light on the left. This indicates successful connectivity to the network.

Part IV. Web User Interface Configuration

In a standard web browser, enter the PDU IP address (“https://IP ADDRESS”) and proceed to configure the PDU as shown in the Web Configuration section. (IP address detail refers to **Establish Network Settings**)

Web Configuration

Supported Web Browsers

The supported Web browsers are Google Chrome (mobile and desktop), Mozilla Firefox, Microsoft Edge, and Apple Safari (mobile and desktop).

Log on the Web UI

Please use the default username and password for first login. Initial Default Username and Password: **admin**

Figure 4. Login Page

Change Password

After successful login, you are required to change the default password.

Input the current password and new password twice to confirm. Press “Apply” to complete set up new password.

NOTE: By default, password must between 8 and 32 characters.

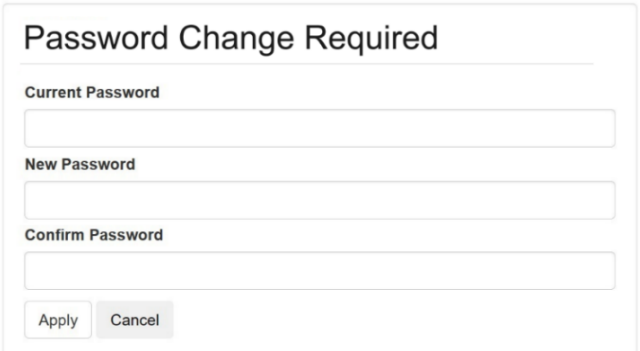


Figure 5. Password Change

Introduction for the Web GUI

Landing Page/ Home page

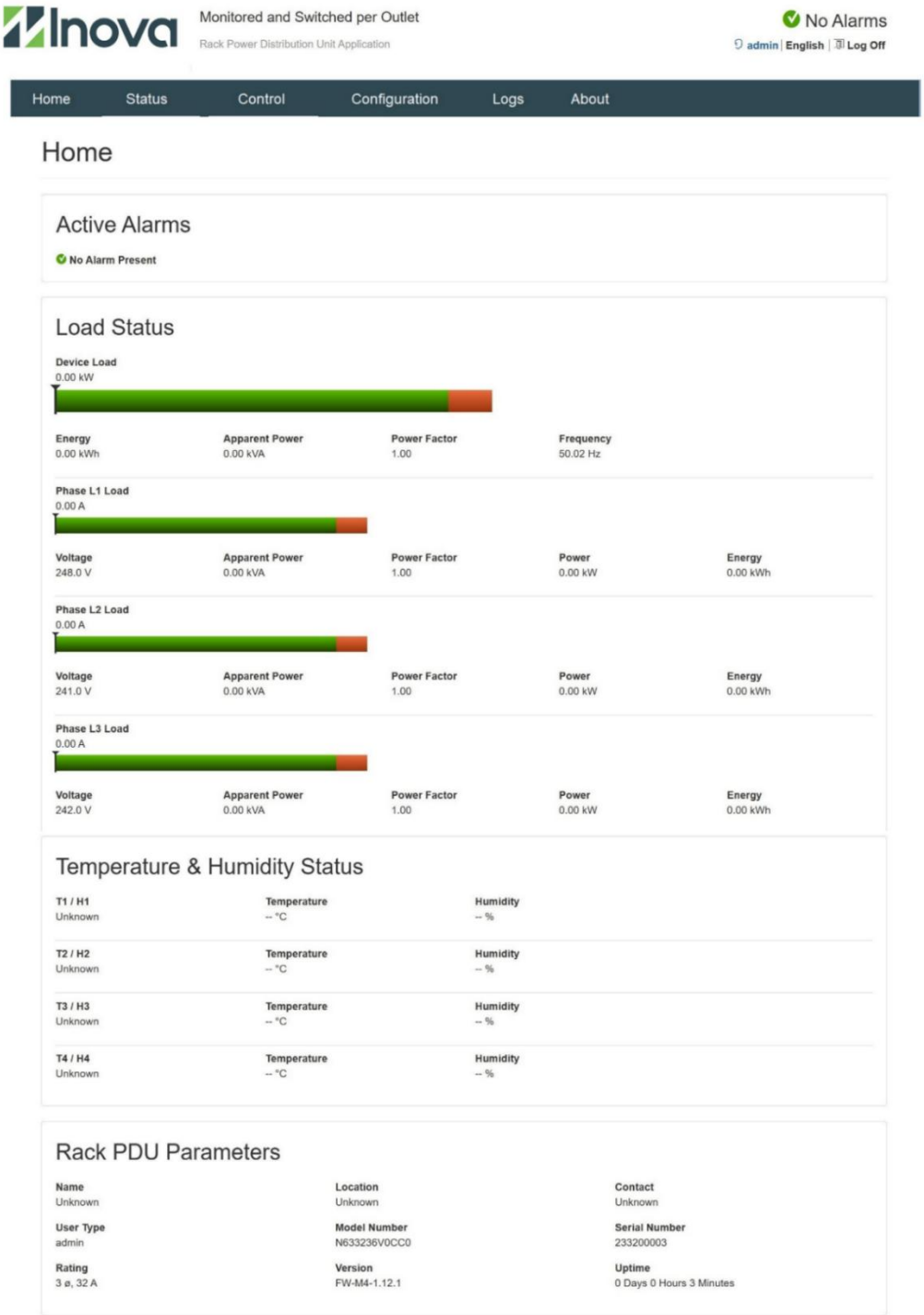


Figure 6. Landing/Home Page Overall View

Dropdown Menu Tab & Quick Link Menu

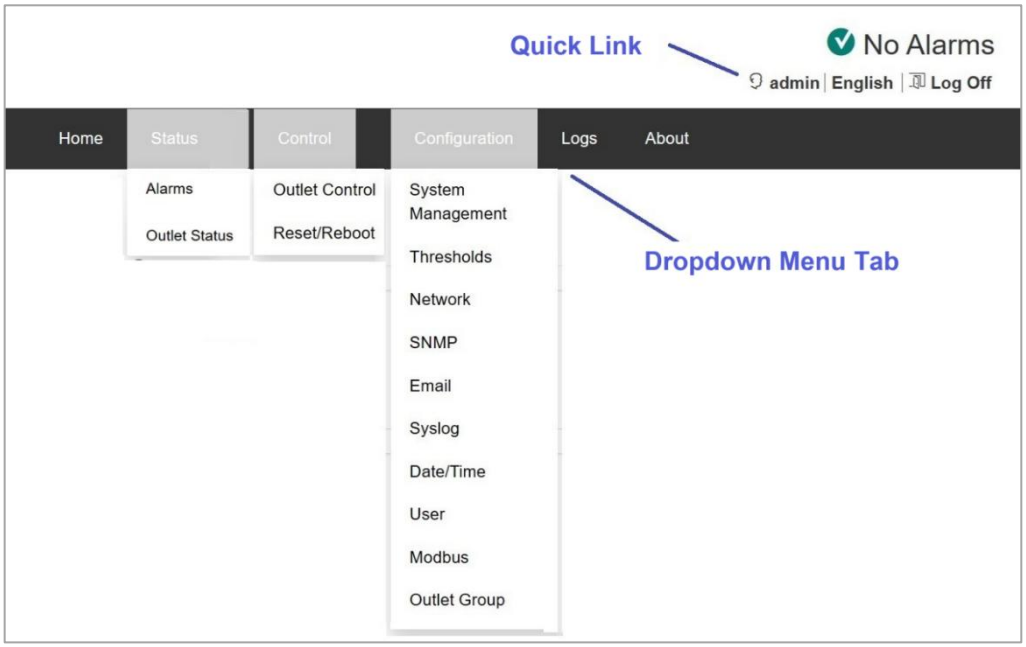


Figure 7. Dropdown Menu Tab & Quick Link Menu

Table 2. Tab Description

No	Tab	Description
1	Home	Default tab when you log on. Review active alarms, the load status of the PDU
2	Status	Provide details of the active critical alarms and active warning alarms.
3	Control	Outlet control management and Reset/Reboot
4	Configuration	Setup the System Management, Thresholds, Network, SNMP, Email, Syslog, Date/Time, User, Modbus, Outlet group.
5	Logs	Review the events and export to file
6	About	Information about the PDU
7	admin	Quick link for user configure to change user preferences
8	English	Quick link to change language preference
9	Log Off	Quick link to log the current user off from the Web UI

Device Status Icon

One or more icons and accompanying text indicates the current operating status of the PDU.

Table 3. Device Status Icon

Symbol	Description
	**Critical**: A critical alarm exists, which requires immediate action
	Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	**No Alarms**: No alarms are present, and the PDU is operating normally

At the upper right corner of every page, the Web User Interface displays the same icons currently displayed on the Home page to report PDU status:

- The No Alarms icon if no alarms exist.
- One or both other icons (Critical and Warning) if any alarms exist, and after each icon, the number of active alarms of that severity.

Quick Link Menu

There is quick link menu on the top right of the home page. Click the tab to enter to related management page immediately.

Admin

Click the admin tab to quick enter to the user management page.

More det

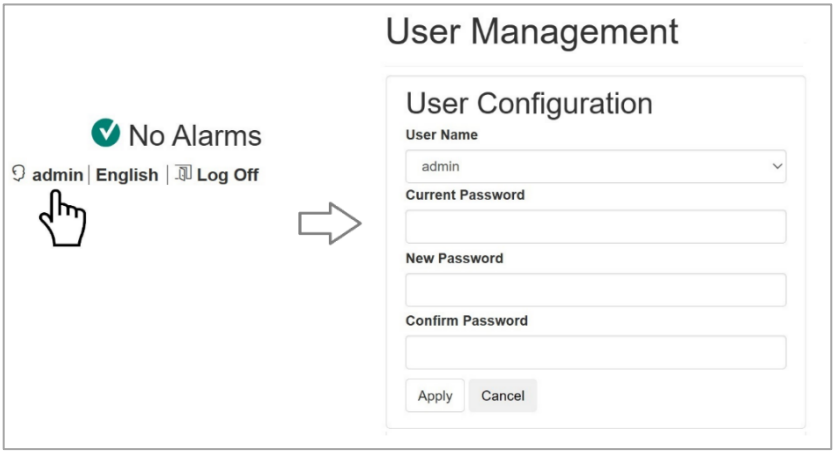


Figure 8. Quick Link to User Management

Language

Click the English tab to quick enter to the language selection page.

Figure 9. Quick Link to Language Selection

Log Off

Click the Log Off tab to exit and back to login page.

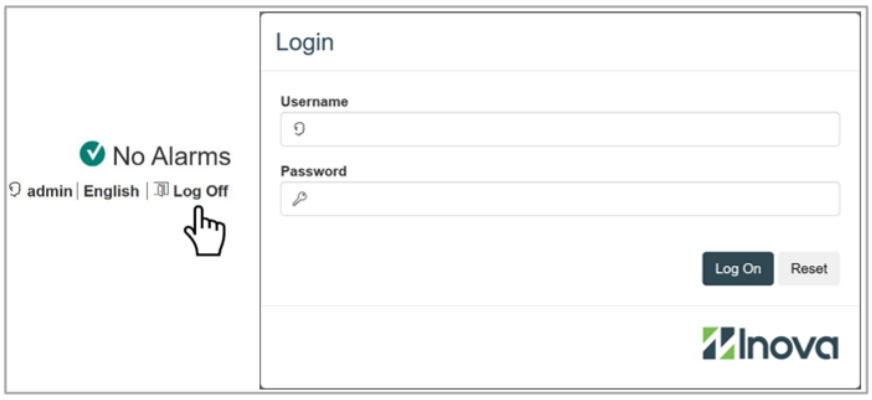


Figure 10. Quick Link to Log Off

Home Page Introduction

The **Home** page contains the following information: Active Alarms, Device Load Status, Phases Load Status, Temperature & Humidity Status, and PDU Parameters.

Active Alarms

Active Alarms will show if any alarms exist. If no alarms exist, a green check mark with the words “No Alarms Present” will be shown.

Figure 11. Active Alarms

Load Status

The Load Status shows a colored bar demonstrating the level of the Phases and Device loads. Review the basic electricity parameters for the device and for the phases, as applicable. The green, blue, and red meter shows the current load status: normal, low load, or overload.

NOTE: Blue will only appear if the optional low-load threshold is configured.

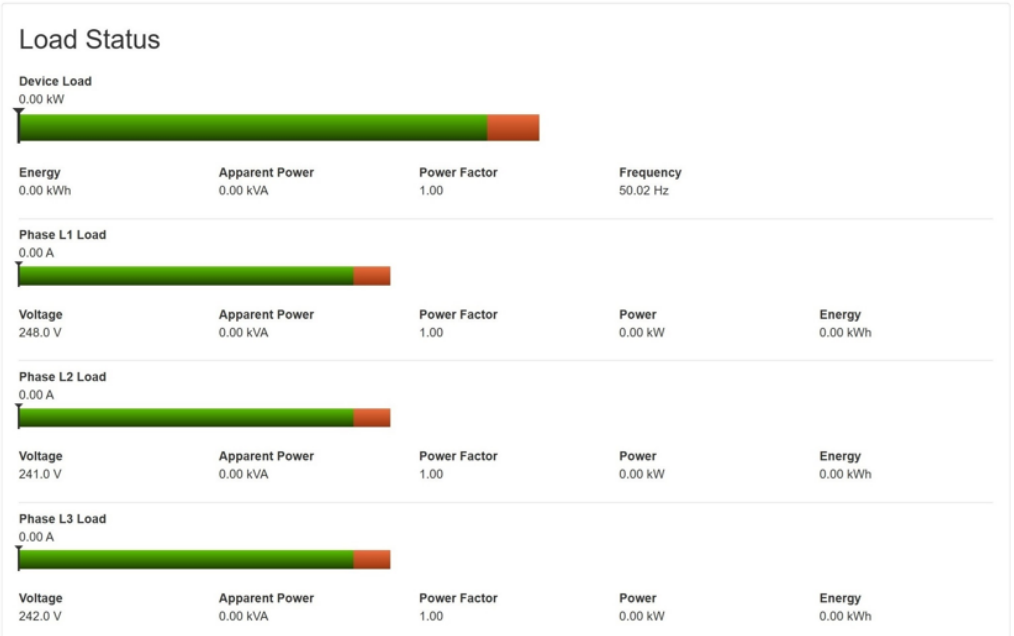


Figure 12. Load Status

Sensor Status

Sensor Status area is to show the current temperature & humidity sensor and DI sensor status.

NOTE: IO1/IO2 are defined as the leakage detection sensor status input port, which needs to be connected to the normally open passive dry contact signal.

Figure 13. Sensor Status

PDU Parameters

The **PDU Parameters** area is to show the Name, Location, Contact, Model Number, Rating, User Type (type of user account accessing the PDU), version, and Uptime (the amount of time the PDU has been operating since the l

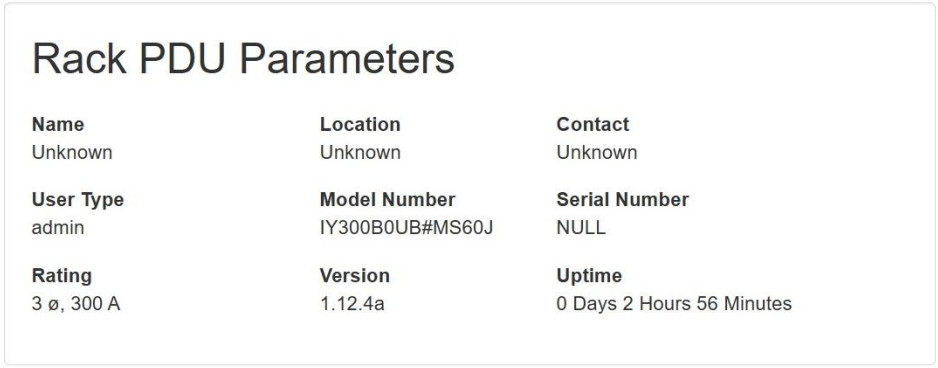


Figure 14. PDU Parameters

Status Tab Introduction

The **Status Tab** page contains the following information: Alarms, and Outlet.

Device Alarm Status

Path: Status > Alarms

To View the Alarm status for the PDU.

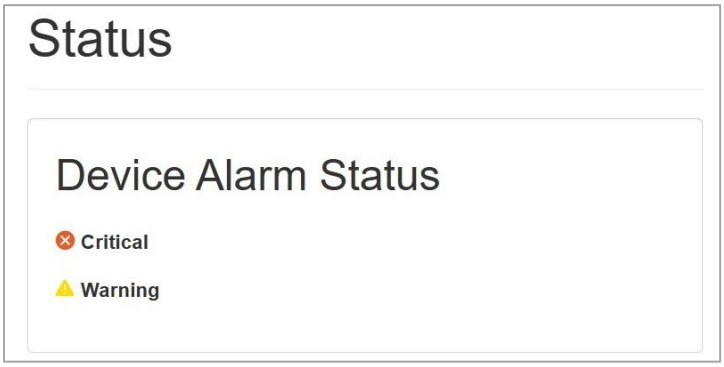


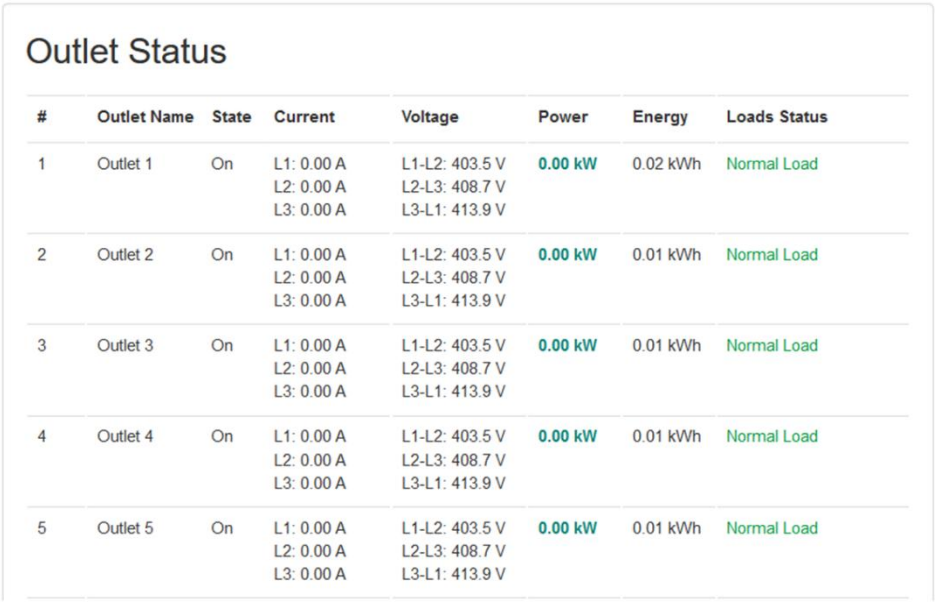
Figure 15. Device Alarm Status

Outlet Status

Path: Status > Outlet Status

To View the status for each outlet.

NOTE: The outlet status page is only available for Monitored per outlet PDU.



Outlet Status

#	Outlet Name	State	Current	Voltage	Power	Energy	Loads Status
1	Outlet 1	On	L1: 0.00 A L2: 0.00 A L3: 0.00 A	L1-L2: 403.5 V L2-L3: 408.7 V L3-L1: 413.9 V	0.00 kW	0.02 kWh	Normal Load
2	Outlet 2	On	L1: 0.00 A L2: 0.00 A L3: 0.00 A	L1-L2: 403.5 V L2-L3: 408.7 V L3-L1: 413.9 V	0.00 kW	0.01 kWh	Normal Load
3	Outlet 3	On	L1: 0.00 A L2: 0.00 A L3: 0.00 A	L1-L2: 403.5 V L2-L3: 408.7 V L3-L1: 413.9 V	0.00 kW	0.01 kWh	Normal Load
4	Outlet 4	On	L1: 0.00 A L2: 0.00 A L3: 0.00 A	L1-L2: 403.5 V L2-L3: 408.7 V L3-L1: 413.9 V	0.00 kW	0.01 kWh	Normal Load
5	Outlet 5	On	L1: 0.00 A L2: 0.00 A L3: 0.00 A	L1-L2: 403.5 V L2-L3: 408.7 V L3-L1: 413.9 V	0.00 kW	0.01 kWh	Normal Load

Figure 16. Outlet Status

Control Tab Introduction

The **Control** menu options enable you to take immediate actions affecting active user management and the security of your network.

NOTE: The **Outlet Control** is only available for Switched per Outlet PDUs.

Outlet Control

Path: Control > Outlet Control

In outlet control area, to view each outlet's State, Name, and Type or (Phase and Bank).

- Mark the check boxes for each individual outlet, outlet group or select All Outlets check box.
- Select the **Control Action** (No Action/Off/On) from dropdown menu.
- Click **Apply** or **Cancel** to complete the control action.

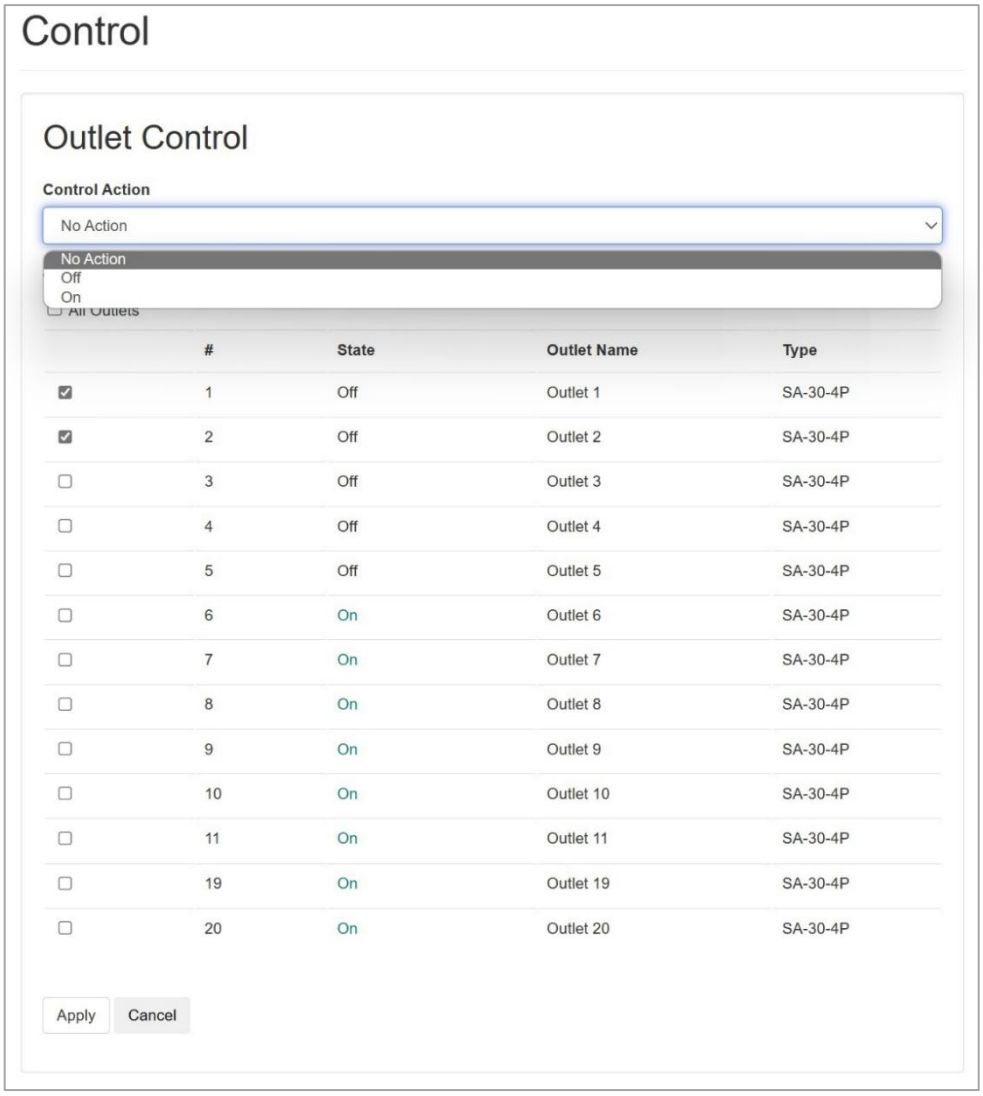


Figure 17. Outlet Control

Reset/ Reboot Network Interface

Path: Control > Reset/Reboot

This interface gives you the option to reset and reboot various components of the network interface. You also have the option to Reboot Management Interface.

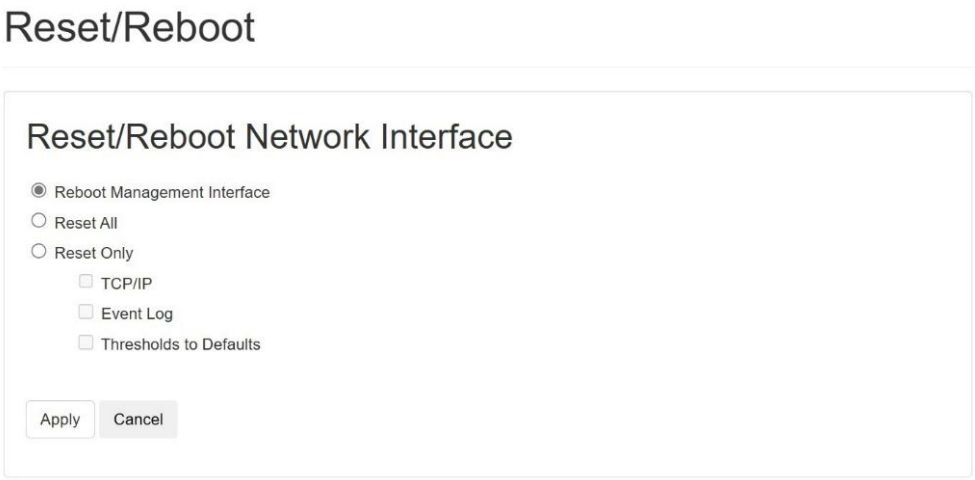


Figure 18. Reset/Reboot Network Interface

NOTE: Reboot Management Interface is only to restart the Rack PDU's Network Management Interface, which will not affect the outlet ON/OFF status.

Reset All: Reset all configuration values except for account information and the Event Log.

Reset Only: Options include:

TCP/IP: Set TCP/IP Configuration to **DHCP**, its default setting. This requires that the PDU receive its TCP/IP settings from a DHCP server.

Event Log: Reset all Event logs.

Thresholds to Default: Reset all threshold settings.

System Configuration

About the Configuration Tab

Several menu options are available to make changes to the PDU as below:

- System Management: Language selection; Set up name, location, and contact for the PDU; Set up name for the Temperature & Humidity sensor; Upgrade the firmware and certificate file.
- Set up thresholds for all connected Devices, Phases and Outlets.
- Network: IPv4, IPv6, Web configuration.
- SNMP configuration.
- Email configuration.
- Syslog
- Date and time configuration.
- Users Management.
- Modbus
- Outlet Group Management. (not available for hydro PDU)

System Management

Language Configuration

Path: Configuration >System Management>Language Configuration

The system lets you select a Language: English, Chinese.

NOTE: Click home page **English/**简体中文 can quick link to this page. (Page 18)

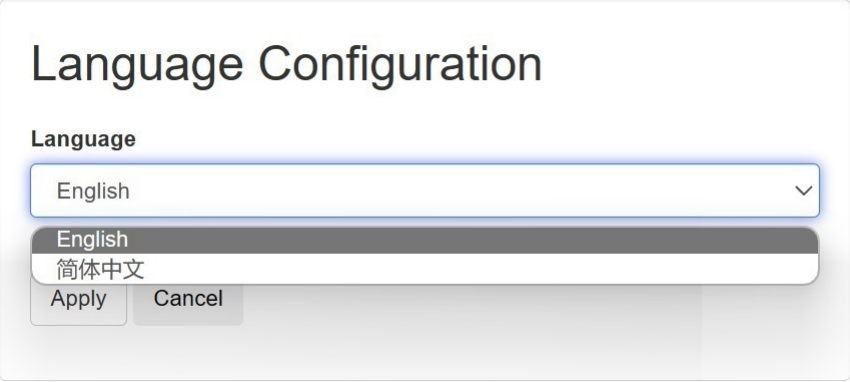


Figure 19. Language Configuration

Device Configuration

Path: Configuration >System Management>Device

The device information includes the name and location of the PDU system and information of the person to contact in case an issue arises. Follow the steps below to set up the system information:

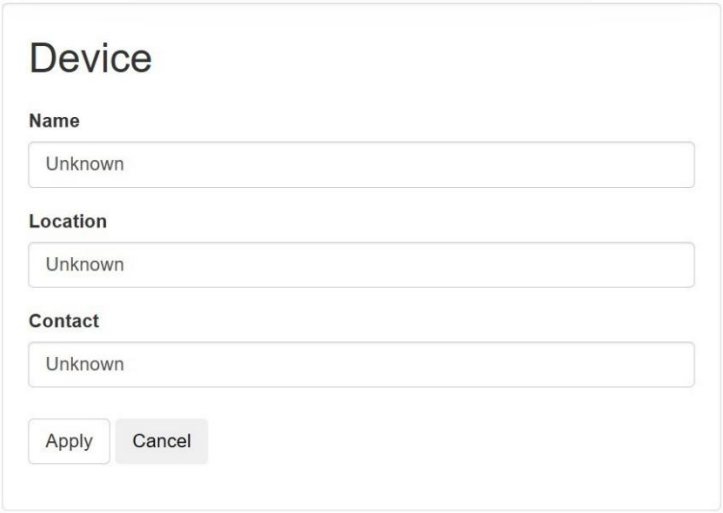


Figure 20. Device Set Up Page

- Select the **System Management** tab to define **Device Information**.
- Enter the **Device Name**, the name will appear on PDU LCD display after complete naming the device.
- Enter the location of the main PDU into Location section.
- Enter the information of who should be contacted if there is a problem with the system into the Contact section.
- Press **Apply**.
- The LCD will display individual name for each guest PDU after daisy chained if you set up the device name before daisy chain, otherwise only can display the name as same as that of host PDU.

  NOTE: PDU controller display only can shows no more than 15 characters of the device name. Naming Example: PDU01_RACK001.

Sensor Name

Path: Configuration >System Management>Sensor Name

Each rack PDU can support up to four Temperature and Humidity sensors, user can define the name of four Temperature & Humidity sensors to make a distinction.

- Enter the name of the sensor.

➢ Click Apply to complete the set up.

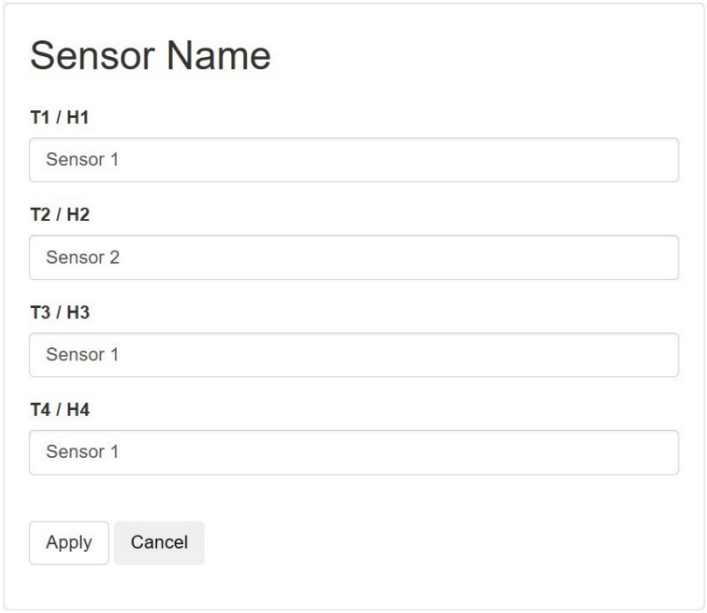


Figure 21. Sensor Name Set Up Page

Load Firmware File

Path: Configuration >System Management>File Upgrade

Each rack PDU can upgrade the firmware by Web Interface

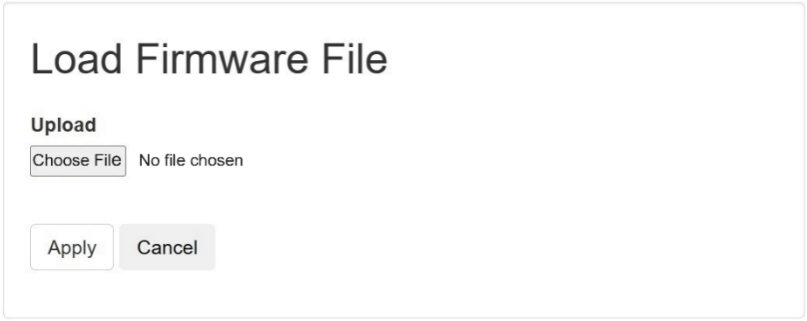


Figure 22. Load Firmware File

Please refer to AppendixA Firmware Upgrade Options> Web Interface Method

Upgrade Certificate File

Path: Configuration >System Management>Upgrade Certificate File

To add, replace, or remove a security certificate.

If user installs an invalid certificate, or if no certificate is loaded when opening web browser, the Rack PDU will generates a default certificate. User can use the default certificate for basic encryption-based security, but

a security alert message will display whenever a user logs in.

- **Add or Replace**: add or replace certificate file via web browsers.
- **Remove**: Delete the current certificate.

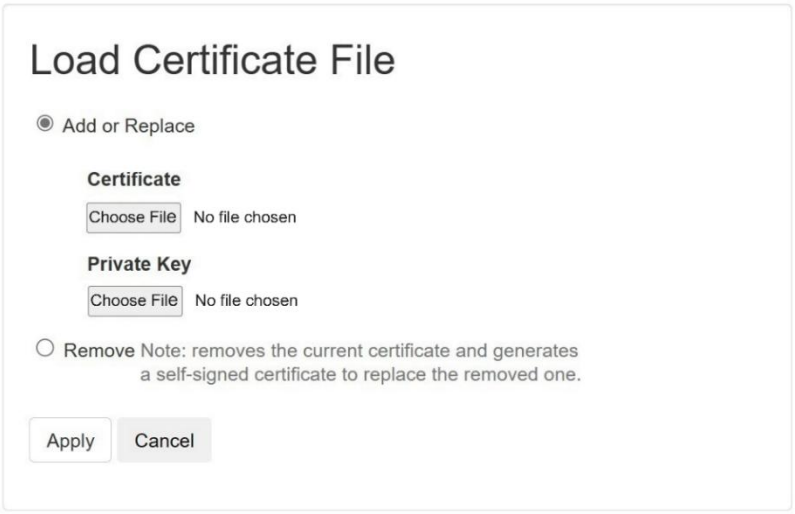


Figure 23. Upgrade Certificate File

Thresholds Configuration

Path: Configuration >Thresholds

To set up load thresholds for the Device Load, Phases Current, Phase Voltage, Banks, Outlets, Temperature Sensor, and Humidity Sensor.

PDUs will send alert notifications when the device load above or below the threshold settings for below item:

- Set the **Low Load Warning** and **Overload Alarm** thresholds for Device Load.
- Select Phase and set the **Low Current Warning** and **Over Current Alarm**.
- Select Phase and set the **Low Voltage Warning** and **Over Voltage Alarm**.
- Select Outlet and set the **Low Current Warning** and **Over Current Alarm**.
- Select Outlet and set the **Low Load Warning** and **Overload Alarm**.
- Select Sensor and set the **Temperature Over Alarm** and **Humidity Low Warning**.
- Click **Apply** to save the threshold settings.

NOTE: The Outlet Current and Load is only available for Monitored per Outlet.

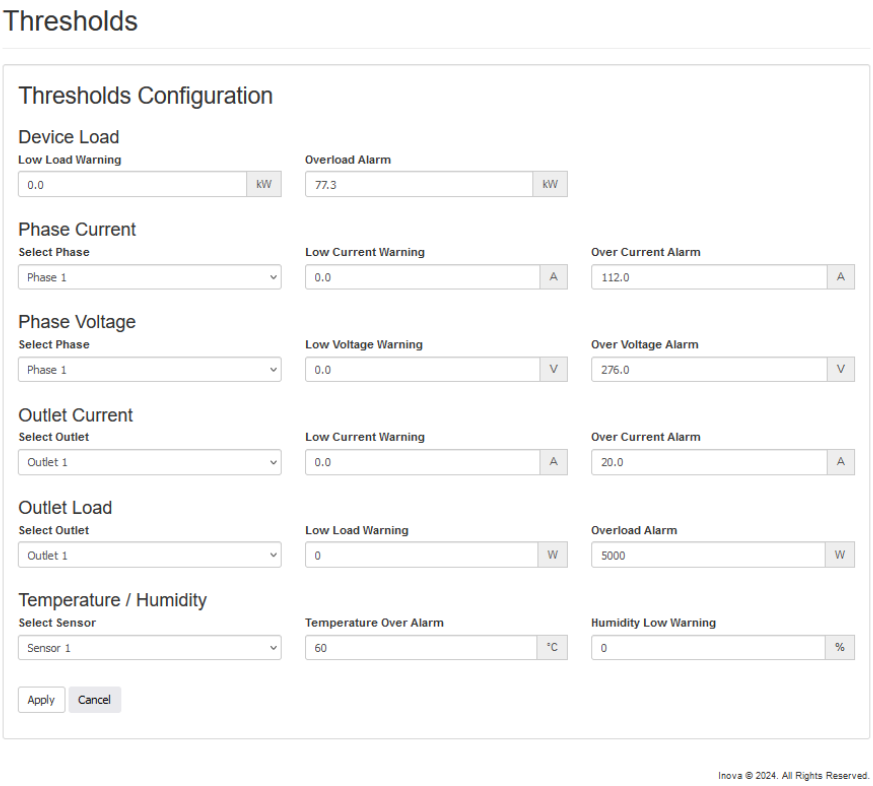


Figure 24. Thresholds Configuration Page

Network Configuration

The Network Settings allow management of IPv4, IPv6 Configuration, Web Access Configuration.

Current Settings

Path: Configuration >Network>Current Settings

Current Settings page shows the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the PDU.

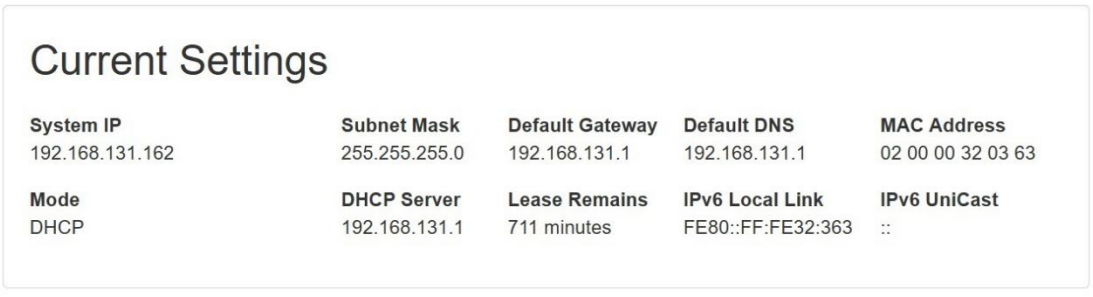


Figure 25. Current Settings Information

IPv4 Configuration

Path: Configuration > Network >IPv4 Configuration

Table 4. Mode Description

Mode	Description
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway
DHCP	Default setting. The PDU requests network assignment from any DHCP server. If the PDU finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.

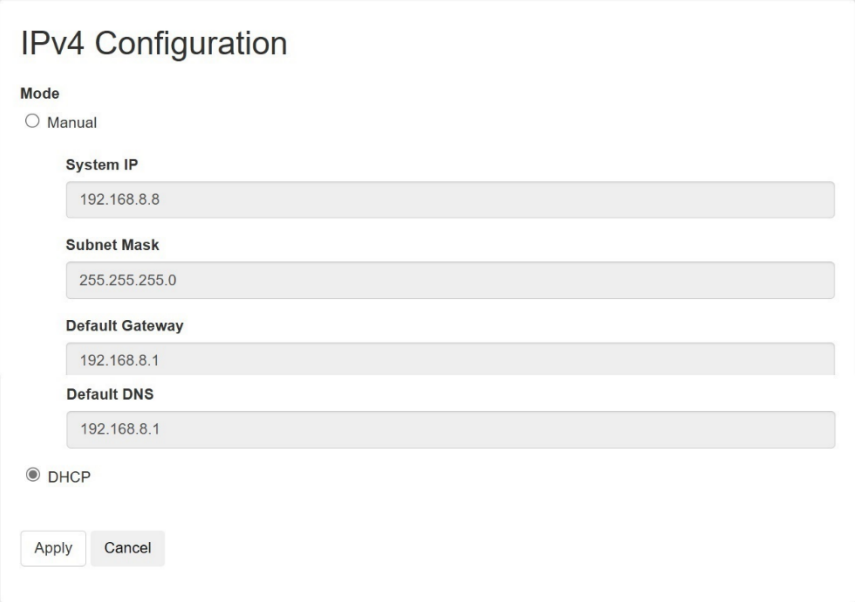


Figure 26. IPv4 Configuration

- **DHCP response options:** Each valid DHCP response contains options that provide the TCP/IP settings that the PDU needs to operate on a network, and other information that affects the operation of the PDU.
- **TCP/IP options**: The PDU uses the following options within a valid DHCP response to define its TCP/IP settings.
- **IP Address** (from the **yiaddr** field of the DHCP response): The IP address that the DHCP server is leasing to the PDU.
- **Subnet Mask** (option 1): The Subnet Mask value that the PDU needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3): The default gateway address that the PDU needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the PDU.
- **Other options**: The PDU also uses these options within a valid DHCP response.
- **Network Time Protocol Servers** (option 42): One NTP server that the Rack PDU can use.
- **Time Offset** (option 2): The offset of the Rack PDU's subnet, in seconds, from Coordinated Universal Time (UTC).

- ✧ **Domain Name Server** (option 6): One Domain Name System (DNS) server that the PDU can use.
- ✧ **Host Name** (option 12): The host name that the PDU will use (32-character maximum length).

Web Configuration

Table 5. Web Configuration

Option	Description
Access	**Enable HTTP:** Enables Hypertext Transfer Protocol (HTTP, which provides Web access by username and password, but does not encrypt usernames, passwords, and data during transmission. HTTP is disabled by default. **Enable HTTPS:** Enables Hypertext Transfer Protocol (HTTPS over Secure Sockets Layer (SSL). SSL encrypts usernames, passwords, and data during transmission, and authenticates the PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. HTTPS is enabled by default. **HTTP Port:** The TCP/IP port (80 by default) used to communicate by HTTP with the PDU. **HTTPS Port:** The TCP/IP port (443 by default) used to communicate by HTTPS with the PDU. **Minimum Protocol:** TLS 1.2.
SSL Certificate	Add, replace, or remove a security certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the PDU generates a default certificate.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File:** Use file upgrade function via web browsers to add or replace certificate file. **Remove:** Delete the current certificate.

IPv6 Configuration

Path: Configuration >Network> IPv6 Configuration

Figure 27. IPv6 Configuration

DHCPv6 is a method to assign IPv6 addresses automatically to network clients. When you enable IPv6 for a trusted or optional interface, you can enable the DHCPv6 server on the interface, to assign IPv6 addresses

to clients that connect.

You can enable a DHCPv6 client on this interface to request an IP address from a DHCPv6 server. To get IPv6 addresses, the DHCPv6 client can use a rapid two-message exchange (solicit, reply) or a four-message exchange (solicit, advertise, request, reply). By default, the DHCPv6 client uses the four-message exchange. To use the two-message exchange, enable the Rapid Commit option on the interface and on the DHCPv6 server.

- **Current Settings** displays the current IPv6 Local Link IP, UniCast IP.

Table 6. IPv6 Setting

Model	Description
Manual	Configure IPv6 manually by entering the System IP address, Default Gateway
DHCPv6	The Default Gateway setting. When you enable IPv6 for an external interface, if you do not enable IPv6 address autoconfiguration, you must specify the default IPv6 gateway. To specify the default gateway: In the Default Gateway text box, type the IPv6 address of the default gateway.

- **DHCPv6 response options**: If the Options field is configured on the DHCPv6 server, when the DHCPv6 client applies for an IPv6 address, the DHCPv6 client obtains the configuration information in the Options field through the DHCPV6 packet returned by the server.

Web Configuration

Path: Configuration >Network>Web Configuration

Web Access Configuration can be set to HTTP, HTTPS.

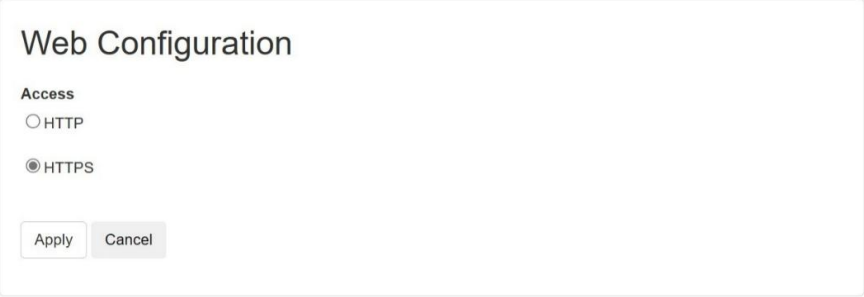


Figure 28. Web Configuration

SNMP Configuration

Path: Configuration >SNMP Configuration

All usernames, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access, or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When manage a PDU on the public network, you must have SNMP enabled in the PDU interface. Read access will allow to receive traps from the PDU, but Write access is required while you use the interface of the PDU to set the serv

Figure 29. SNMP Configuration

Set Up Trap Proxy Server

- Access the Web interface and log in.
- Set the Trap Proxy Server
- Click **Apply** to enable the Trap Proxy Server.

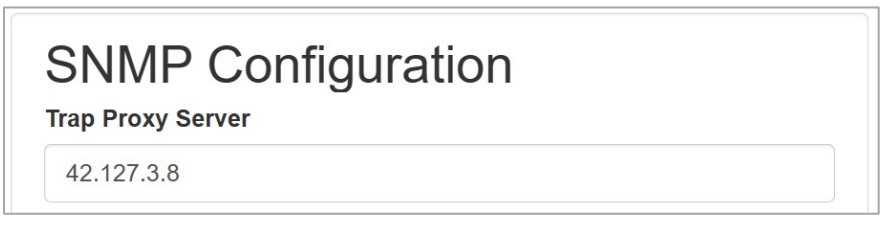


Figure 30. SNMP Configuration

.

Configuring Users for SNMP v1/v2C

- Access the Web interface and log in.
- Under SNMP Configuration, select **SNMP V1 or SNMP V2C**.
- Set the **Read Community Name and Write Community Name**.
  - **Read Community**: the read-only community string to allow an SNMP v1/v2C manager to read a SNMP object.
  - **Write Community**: the write-only community string to allow an SNMP v1/v2C manager to write a SNMP object.
- Click **Apply** to enable SNMP v1 or SNMP v2C.

NOTE: The default SNMP v1 port is 161.

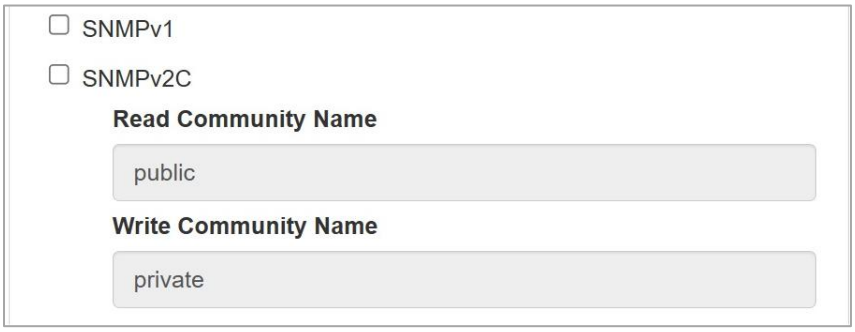


Figure 31. SNMP v1/SNMP v2C Page

Configuring Users for SNMP v3

- Access the Web interface and log in.
- Under SNMP Configuration, select **SNMP V3**.
- Configure the SNMP **Username**.
- Set the **Authentication Passphrase** and **Privacy Passphrase password**.
- Select the desired **Authentication** and **Privacy Protocol algorithm**.
- Click **Apply** to enable SNMP v3.

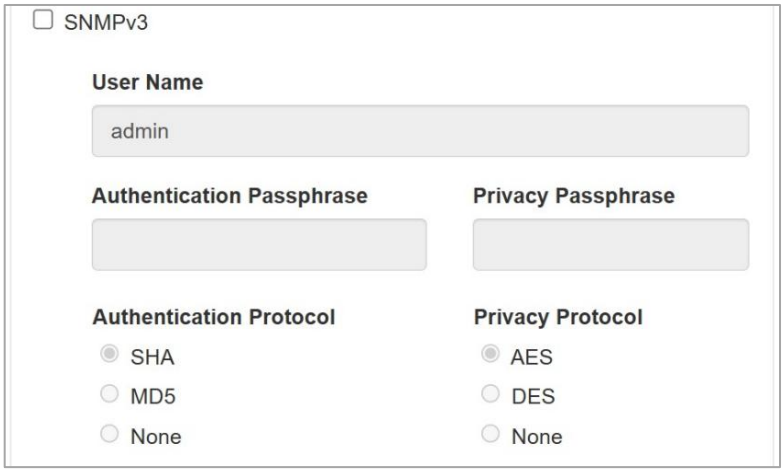


Figure 32. SNMP v3 Page

E-mail Configuration

Path: Configuration >Email

The PDU can be configured to send Emails to specific users when an event occurs. To do this, the information about the SMTP (Simple Mail Transfer Protocol) server needs to be configured.

- Set the **SMTP Server Address**, this is the IP address of SMTP which will accept the messages.
- Configuring the Port number, which is the communication endpoint on the server. The default is 25. Other common SMTP ports are 465,587 2525, 5000 to 32768.
- Select whether SMTP supports SSL by **SMTP-over-SSL**.
- If the SMTP server requires **Authentication**, enter the **Username** and **Password**. These will be determined by the configuration on the SMTP server. If the SMTP does not require authentication, a **Username** and **Password** will need to be entered, but they will not be used.
- Set the **From Address** and **To Address**. This is the email address that the email is sent from and sent to. You could use a unique email address on required PDU or the same email address across all PDUs.
- Click **Apply** to enable the settings.

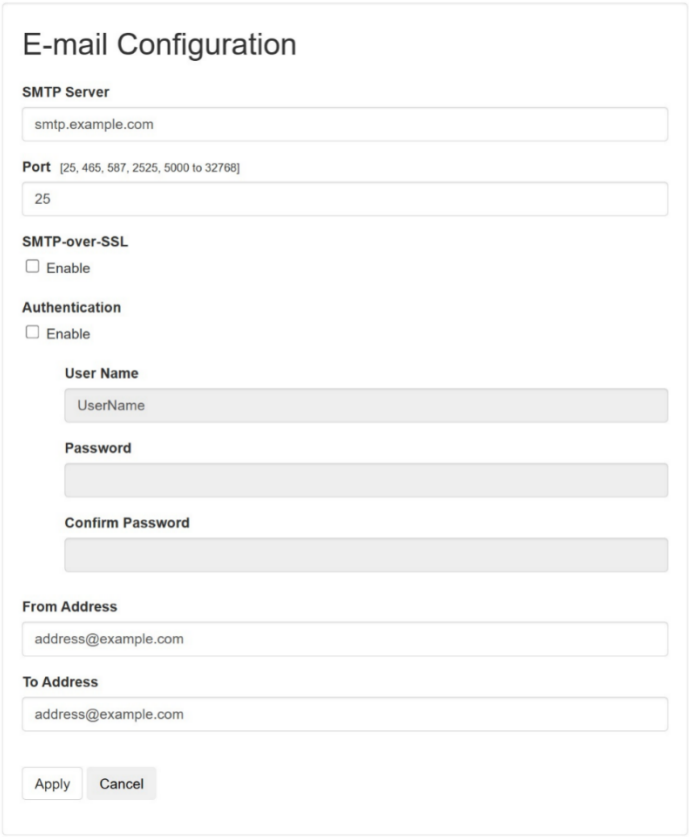


Figure 33. E-mail Configuration

Syslog

Path: Configuration >Syslog

The PDU can automatic synchronization system logs and has the function of uploading these logs to the designated server. To set up the PDU to send syslog message.

- **Enable**: Enable syslog function.
- **Server**: Set the IP address of server to receive these syslog data.
- **Port**: Set the syslog service port, the default port is 514.
- **Syslog Test**: send a test message and check if server can receive the test message.
- Click **Apply** to complete the settings.

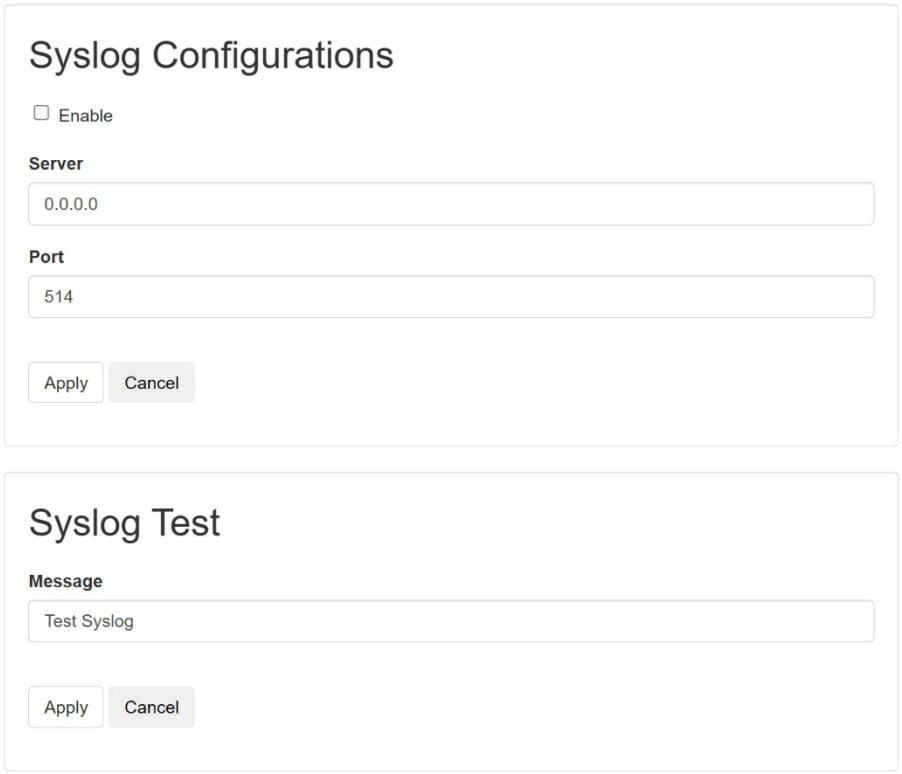


Figure 34. Syslog Configuration

Date/Time

You can set the internal clock manually or link to a Network Time Protocol (NTP) server and set the date and time.

Current Settings

Path: Configuration >Date/Time>Current Settings

To view the current Date and Time information.

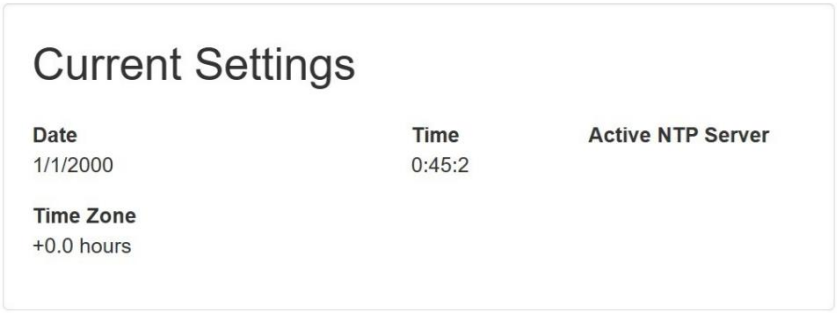


Figure 35. Data/Time Current Settings

System Time Configuration

Path: Configuration > Date/Time>System Time Configuration>Manual

Manual setting the date and time:

- Enter the **Date** using the YYYY-MM-DD format to set a date.
- Enter the **Time** using the hh/mm/ss format to set a time in 24 hours system.
- Click **Apply**.
- Or select directly **Apply Local Computer Time**.

If you select Override Manual NTP Settings, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.

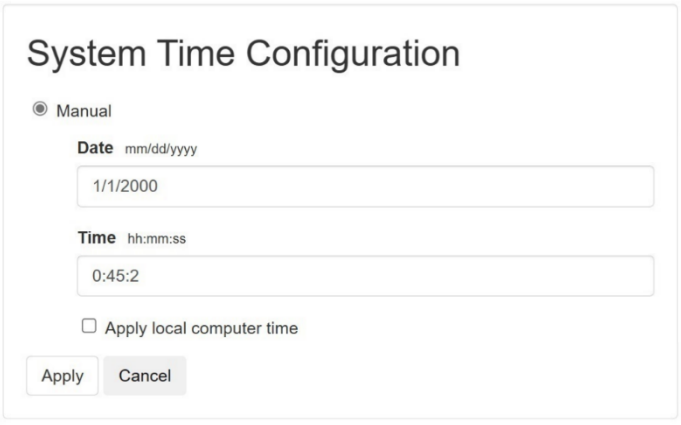


Figure 36. Manual Setting System Time

Synchronize to Network Time Protocol (NTP)

Path: Configuration > Date/Time>System Time Configuration>NTP

Synchronize with NTP Server setting the date and time:

- Select **Synchronize with NTP Server** to enable NTP.
- Select the appropriate time zone from the **Time Zone** drop-down list.
- Enter the IP address of the NTP server in the **NTP Server** field.
- Select the interval time of PDU access the NTP server zone for an update in the **Update Interval**. Minimum:1; Maximum:8760(1year).
- Click **Apply** to complete the setting.

NOTE: NTP Server must be online to test and save the settings.

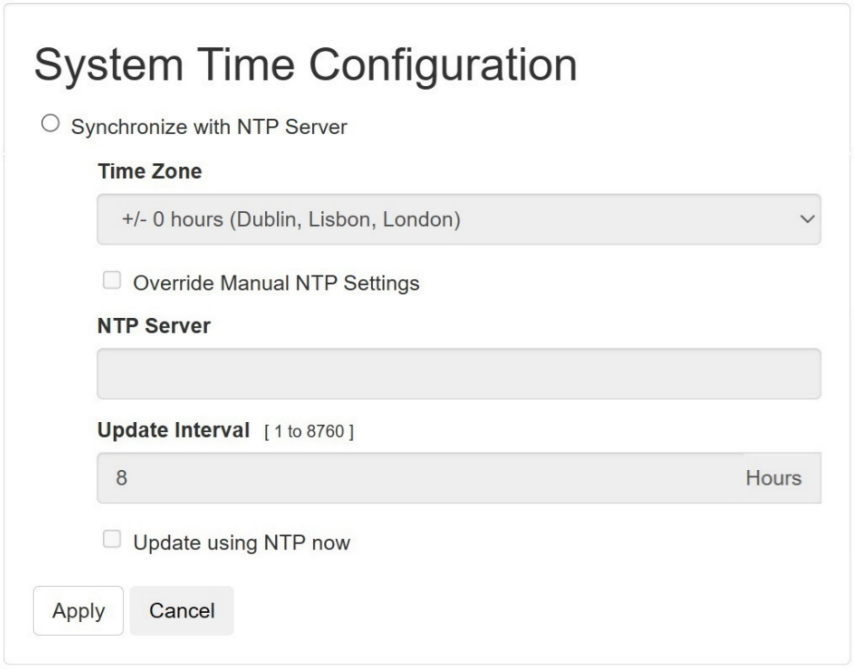


Figure 37. Synchronize With NTP Setting Time

User Management

User Configuration

The PDU has various levels of access (Administrator, Super User, and Read-Only User), which are protected by username and password requirements. Up to ten users are allowed to login to the same PDU simultaneously.

Before setting up users, determine the Roles that will be required. Each user must be given a Role. These Roles define the permissions granted to the user.

Table 7. User Role

Role	Default Permissions
Admin	Typical the system administrator and has the Administrator Privileges with full operating permissions.
Super User	Full permissions that cannot be modified or deleted.
Read Only	Read-only permissions. Can monitor the system but cannot change any configuration

By default, the User Role is a Read Only profile. All other users must be added by a user with administrator privileges. Users are defined by their unique login credentials and by their user role. The level of access privilege determines what the user will see and what actions the user can perform. The level of access privilege determines which menu items the user can access, or which fields display on individual setting and configuration dialogs.

Path: Configuration >User>User Configuration

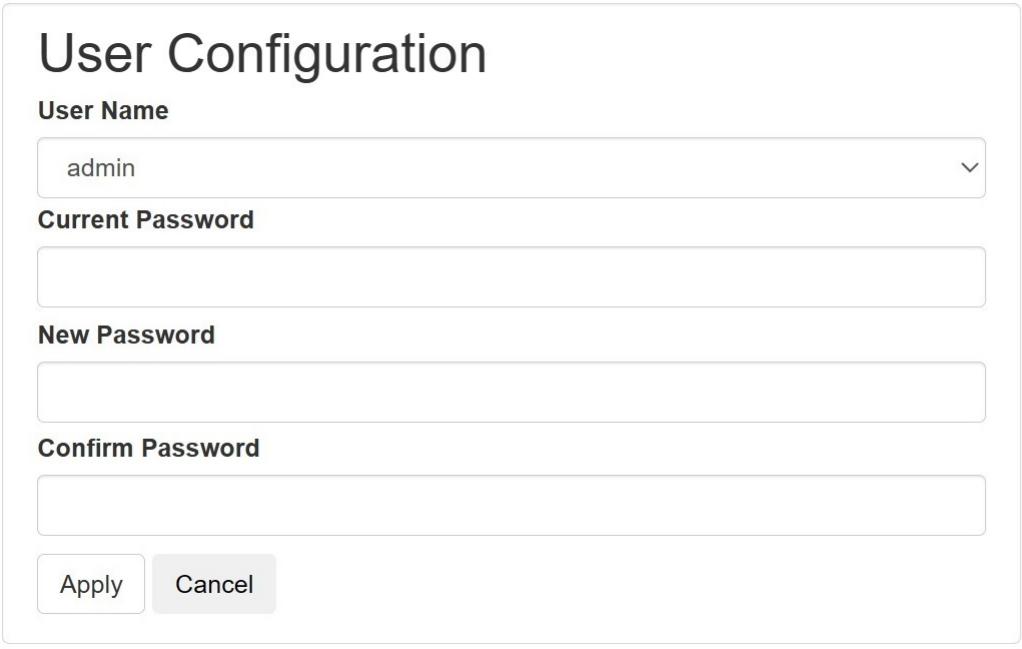


Figure 38. User Configuration

New User

Path: Configuration > User >New User

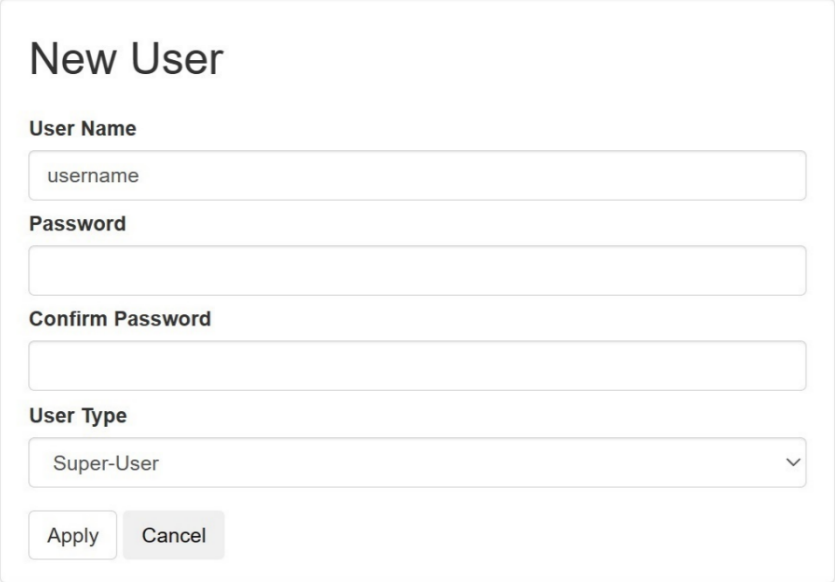


Figure 39. Add New User

To add a user with the following steps:

- Go to New User interface to add new user profile.
- Enter the following information:
  - Username (required)
  - Password (required)
  - Confirm Password (required)
  - User Type (dropdown list)
- Click **Apply** to save the new user profile.

NOTE:

1. By default, the passwords length limitation is 8-32 characters,
2. at least one numeric character, one special character is must to have.
3. Only admin user account can create the new user.

Delete User

Path: Configuration > User>Delete User

To delete user, select the Username and click Apply to complete the setting.

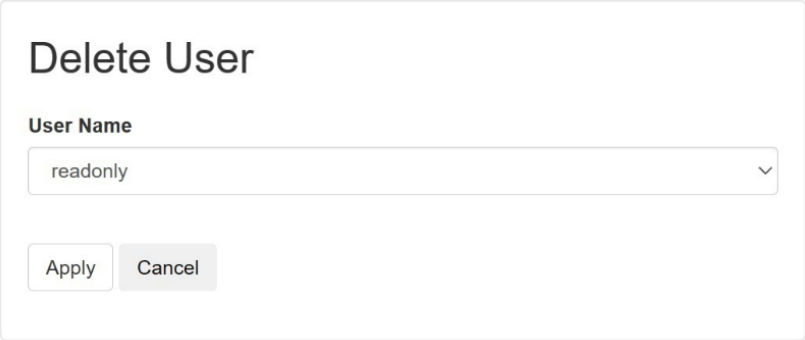


Figure 40. Delete User

Modbus

Path: Configuration >Modbus

The PDU can support Modbus -TCP protocol.

Select **Enable** and click **Apply** to complete the setting.

NOTE: Please contact PDU Tech support for the Modbus agreement.

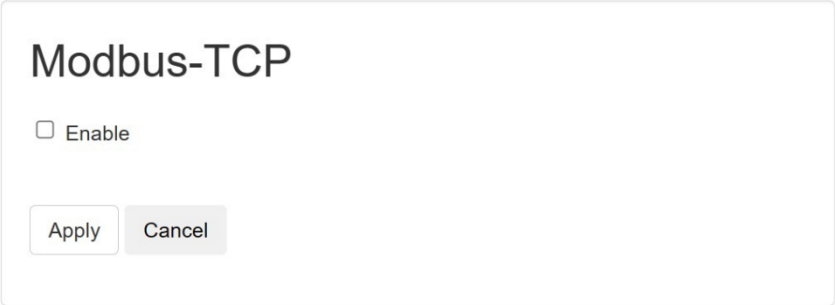


Figure 41. Modbus-TCP

Outlet Group

Path: Configuration >Outlet Group

The Switched Per Outlet Type PDU can support outlet group customization function. Outlets that in an outlet group have the synchronized manner of group turn on, group turn off, group reboot action. To configure the **Outlet Group** function, select **Outlet Group** under the configuration tab.

- Press the Outlet Group1~10 button and select the related PDU outlet;
- Press Apply to enable the current outlet group; Press Delete to disable the current outlet group.

NOTE：

1. This is only applicable to switched per outlet PDUs.
2. Each group includes a maximum of 4 units.

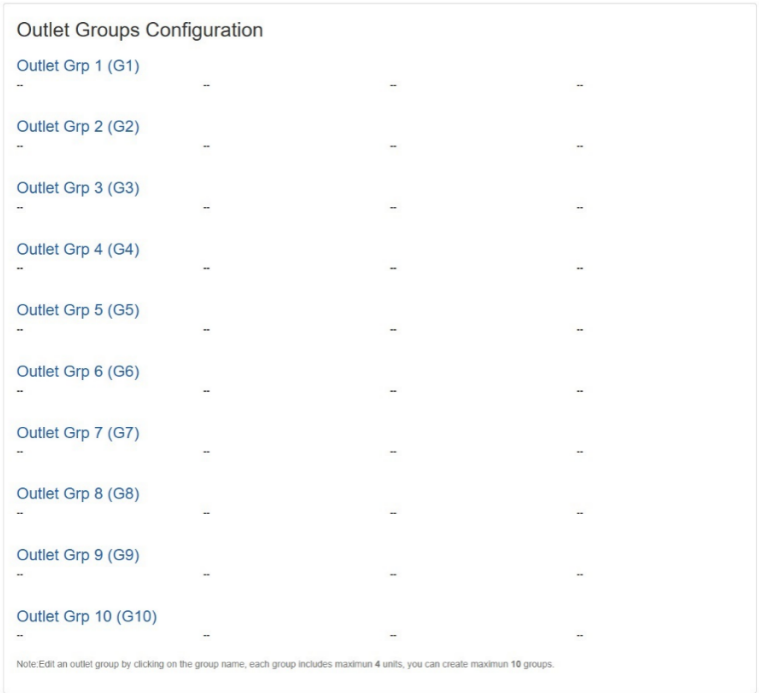


Figure 43. Outlet Group Configuration

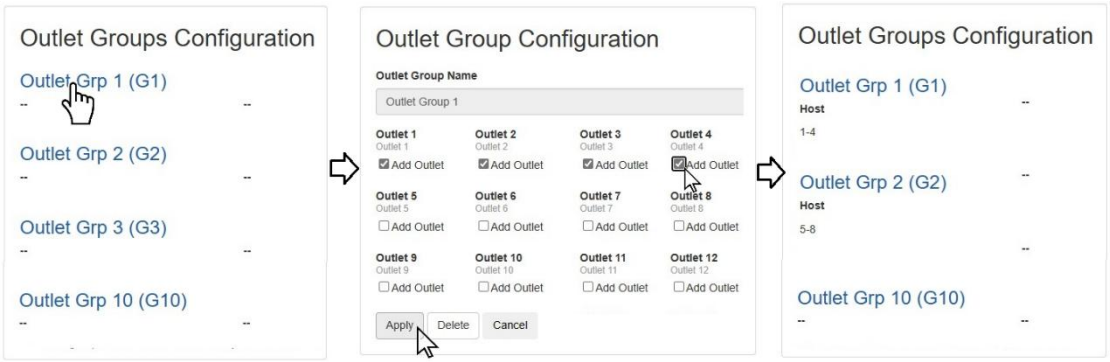


Figure 42. Outlet Group Set Up Process

Purpose and Benefits of Outlet Groups

By using groups of synchronized outlets on PDUs, you can ensure that outlets turn on, turn off, and reboot in a synchronized manner. Synchronizing control group actions through outlet groups provides the following benefits.

- Synchronized shutdown and startup of the power supplies of dual-corded servers prevents erroneous reporting of power supply failures during a planned system shutdown or reboot.
- Synchronizing outlets by using outlet groups provides more precise shutdown and restart timing than relying on the delay periods of individual outlets.

System Requirements for Outlet Groups

To set up and use synchronized outlet control groups, you need a computer that can initiate synchronized control operations through the Web UI.

Edit or Delete an Outlet Group

In the **Outlet Group Configuration** table, click on the number or name of the outlet group to edit or delete.

- When editing an outlet group, you can add or remove outlets by selecting the check boxes to mark or unmark them.
- To delete the outlet group, click **Delete**.

Event Logs

Path: Logs Tab

The log can hold maximum of 400 items, starting with the latest events. The oldest item will be deleted in case of log is full.

Not every Event Notification applies or is supported by every PDU type even though the toggle switch in the Web GUI may seem like the feature is supported.

Below is a table of PDU types and the Event Notifications that particular PDU type supports.

Table 8. Particular PDU Type Supports

Event Notifications	Monitored Input (MI Series)	Monitored Input Switched Per Outlet (MS Series)	Monitored Per Outlet (MPO Series)	Monitored Per Outlet Switched Per Outlet (MSPO Series)
Circuit Breaker Status Changed	X	✓	X	✓
Breaker Voltage	X	✓	✓	✓
Breaker/Group Current	✓	✓	✓	✓
User Activity	✓	✓	✓	✓
Outlet Power Control Status Changed	X	✓	X	✓
User Status Changed	✓	✓	✓	✓
Critical Alarm	✓	✓	✓	✓
Warning Alarm	✓	✓	✓	✓
Password/Settings Changed	✓	✓	✓	✓
Network Card Reset/Start	✓	✓	✓	✓
External Sensor Status Changed	✓	✓	✓	✓
User Role Status Changed	✓	✓	✓	✓
Firmware Updated	✓	✓	✓	✓
Communication Status Changed	✓	✓	✓	✓

Download event logs: Click **Download** to save the log as a local text file.

Delete event logs: Click **Clear** to delete all events. The deleted events cannot be retrieved.

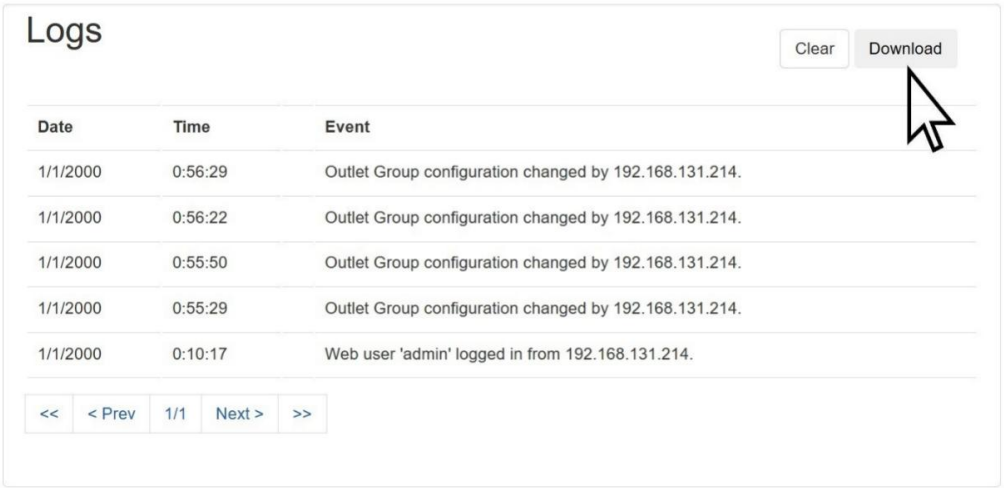


Figure 44. Event Logs

About

Path: About Tab

To view the PDU system firmware and hardware information.

The hardware information is useful to Customer Support for troubleshooting problems with the PDU. The serial number and MAC address are also available on the PDU itself.

Firmware information for the Application Module and Boot Monitor indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at the official website.

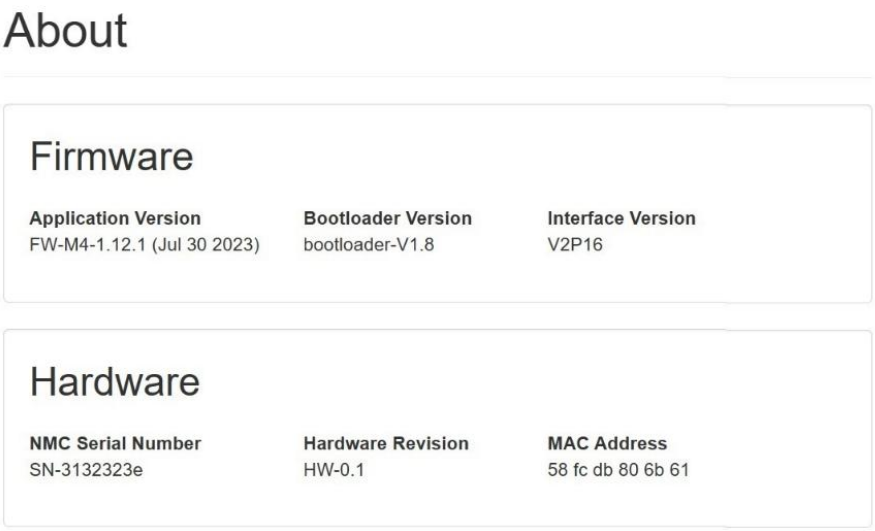


Figure 45. PDU Information

Part Ⅴ. Network Controller Display

Controller Buttons Introduction

The Onboard Display provides information about the PDU and connected devices. The PDU has a three-button, graphical Network Controller panel. Use the buttons to change the screen display and retrieve specific data.

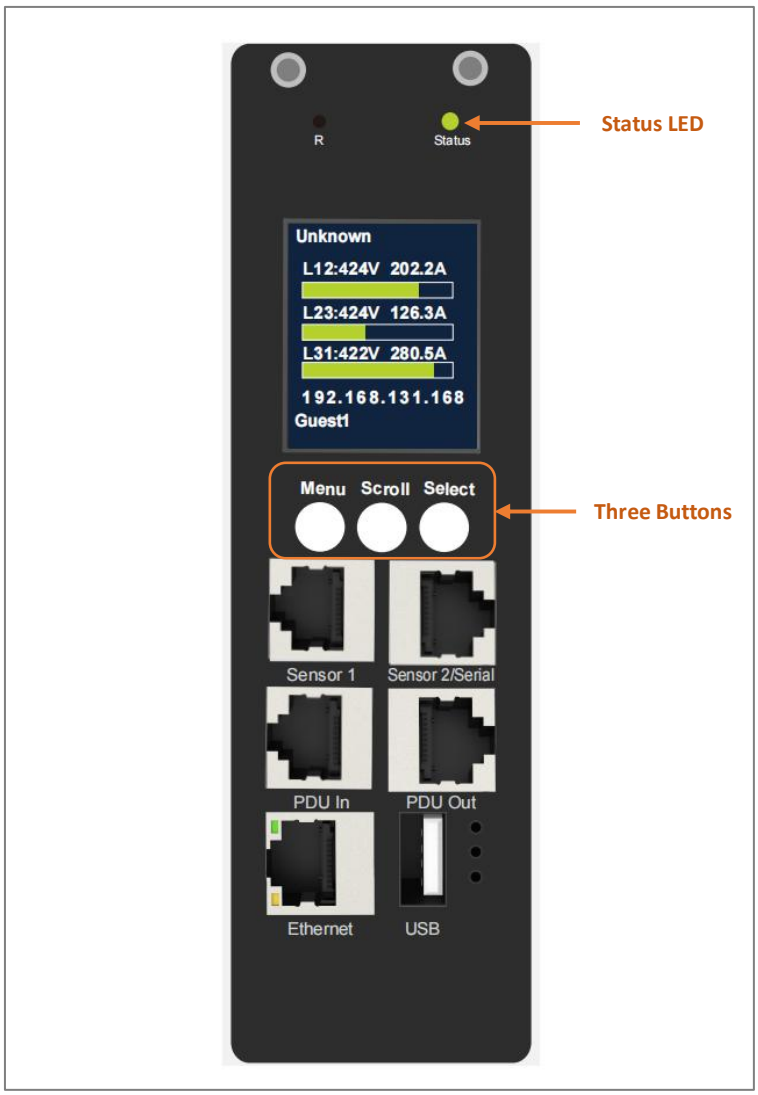


Figure 46. Network Controller Buttons

The Network Controller Display has **Two modes**:

- **Menu mode** (Network Controller Display main menu): When the PDU is powered up or when a button is pushed while in Power Save mode.
- **Power Save mode**: The PDU enters Power Save mode when it has been in Menu mode for setting time. To exit Power Save mode, press any button on the display.

Control Buttons

Summarizes how to use the control buttons on the Network Controller display.

Table 9. Control Buttons Instruction

Button	When in Menu Mode	When in Power Save Mode
Menu	Select from the four main menus.	Returns to the previous display screen before entering the power save mode.
Scroll	Scrolls down through the list of menu items. **NOTE:** A highlighted menu item is ready to be selected.	Returns to the previous display screen before entering the power save mode.
Select	Open the selected menu.	Returns to the previous display screen before entering the power save mode.

Status LED

The LED will change colors depending on the state of the PDU.

Table 10. LED State

LED State	Description
Solid Green	Normal Operation
Solid Red	Critical or Warning Alarm

Network Controller Menu Structure

Press **Scroll** button on controller to enter the PDU system navigation.

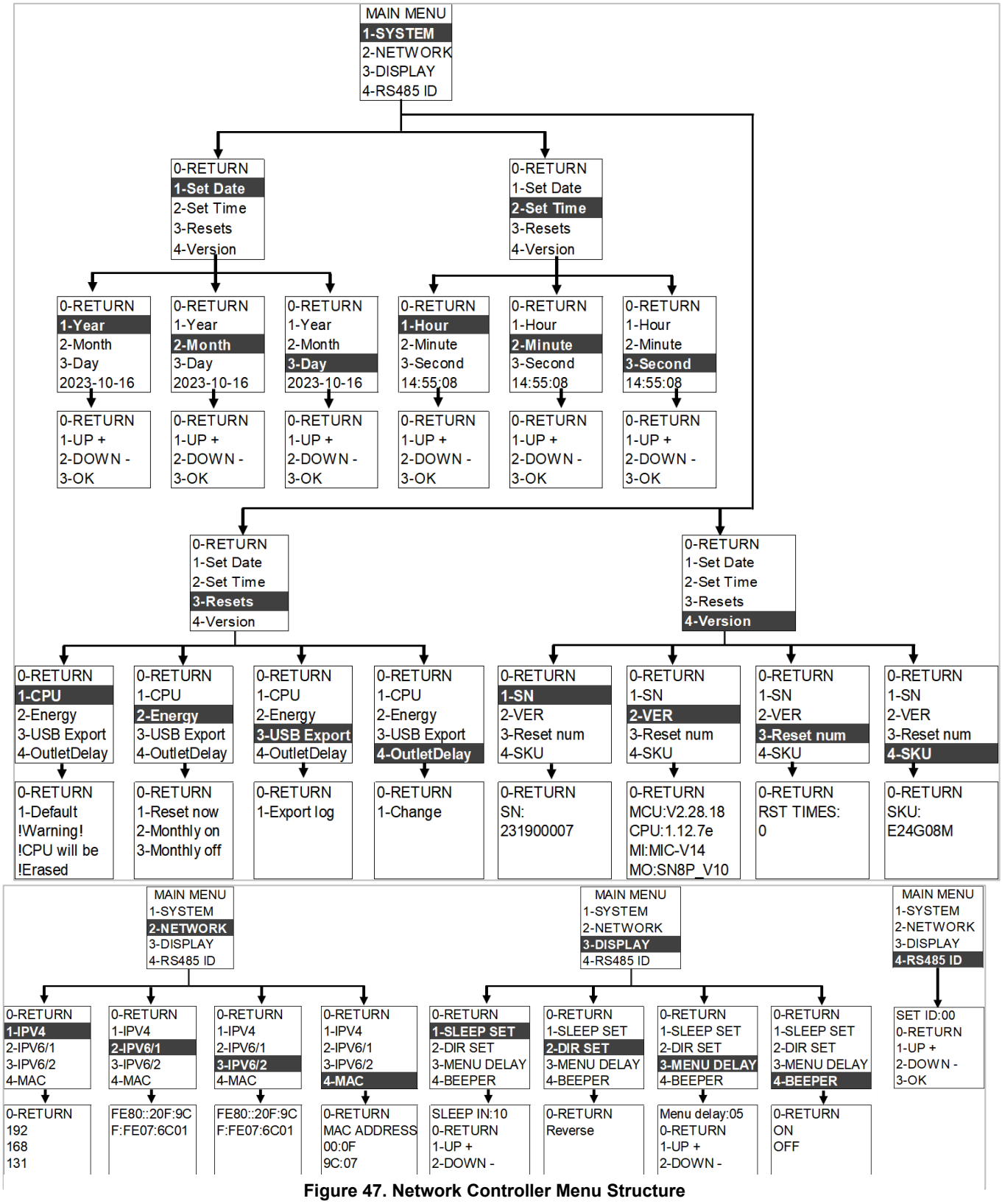


Figure 47. Network Controller Menu Structure

Main Menu Selections

- Press **MENU** button, The PDU menu selection hierarchy consists of **System, Network, Display and RS485 ID.**
- Press **Scroll** button to scroll down for selection, press Select button to enter to submenu. **Scroll** down to select a submenu and press **Select** button to display the submenu options.
- Press Select button to select the **0-RETURN** to back to previous menu.

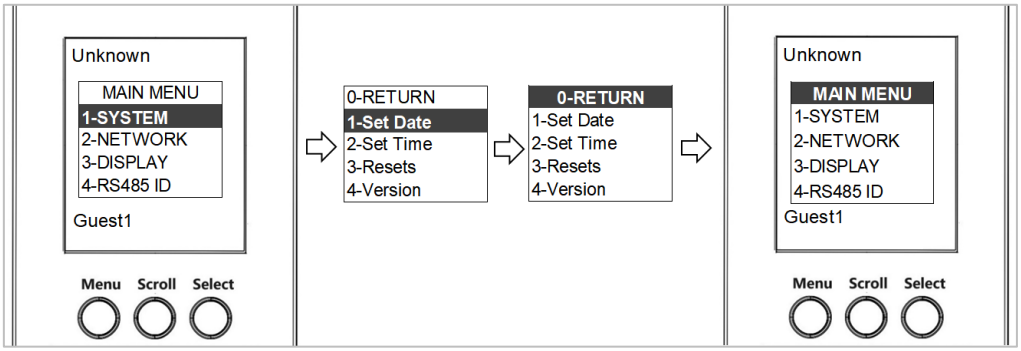


Figure 48. Main Menu

System Menu

The system menu contains: Set Date, Set time, Resets and Version.

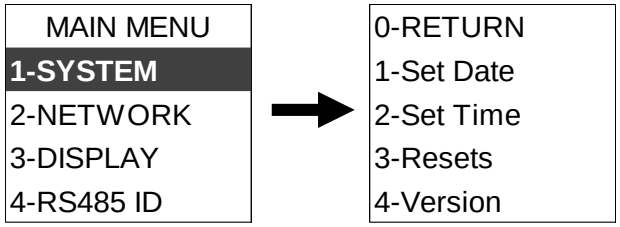


Figure 49. System Menu

Set Date Submenu

The Set Date menu allows you to view recent date and modify that.

- On the System menu, **Scroll** down to Set Date.
- Press **Select** to enter the Set Date Submenu. **Scroll** down to highlight the selected option from the submenu. Press **Select** the option.
- Press **Scroll** and **Select** to **0-RETURN**, back to the previous menu.

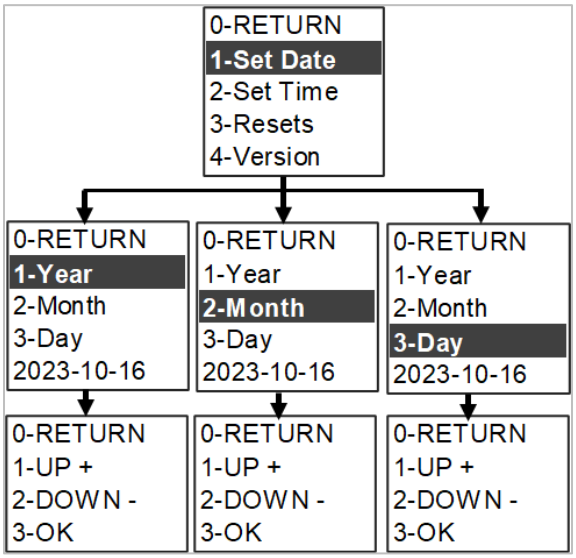


Figure 50. Set Date Submenu

Set Time Submenu

The Set Time menu allows you to view recent time and modify that.

- On the System menu, **Scroll** down to Set Time.
- Press **Select** to enter the Set Time Submenu. **Scroll** down to highlight the selected option from the submenu. Press **Select** the option.
- Press Scroll and Select to **0-RETURN**, back to the previous menu

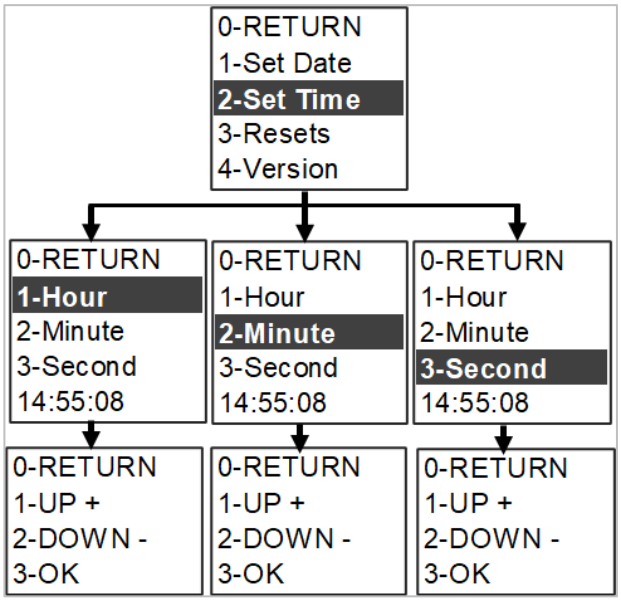


Figure 51. Set Time Submenu

Resets Submenu

The Resets menu allows you to reset configured information.

- On the System menu, **Scroll** down to Resets.
- Press **Select** to enter the Resets Submenu. **Scroll** down to highlight the selected option from the submenu. Press **Select** the option.
- Press **Scroll** and **Select** to **0-RETURN**, back to the previous menu.

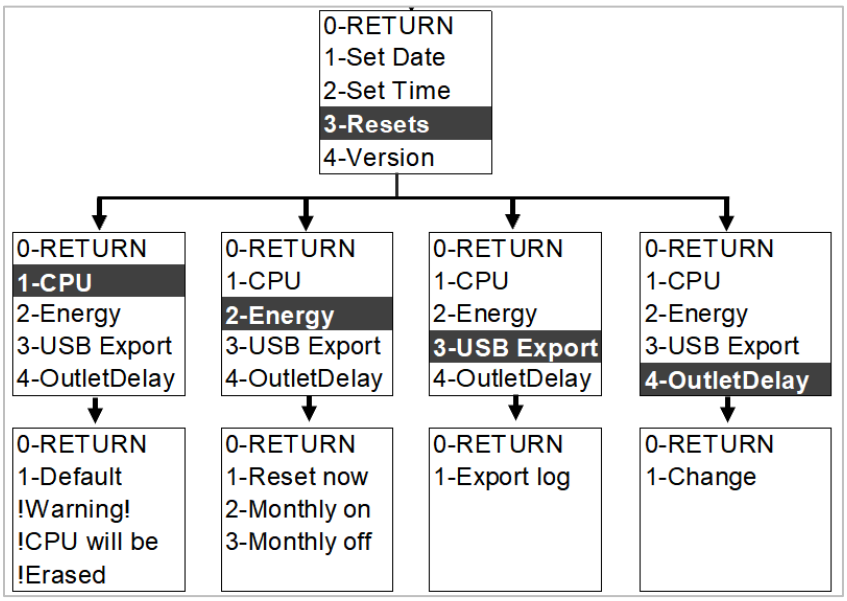


Figure 52. Reset Submenu

Version Submenu

The Version menu allows you to view recent the PDU's Serial Number and firmware version.

- On the System menu, **Scroll** down to Version.
- Press **Select** to enter the Version Submenu. **Scroll** down to highlight the selected option from the submenu. Press **Select** the option.
- Press **Scroll** and **Select** to **0-RETURN**, back to the previous menu.

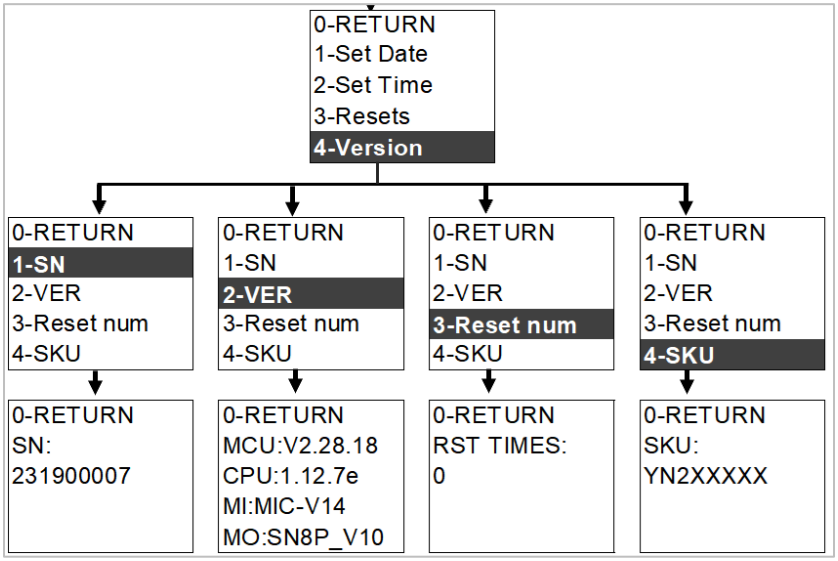


Figure 53. Version Submenu

Network Menu

The Network menu allows you to view IP address, IPv4, IPv6/1，IPv6/2, MAC.

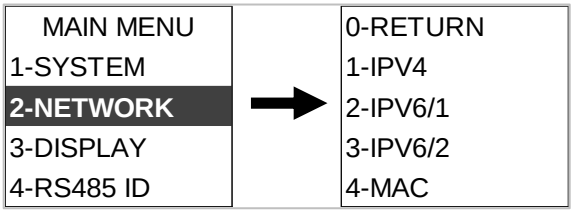


Figure 54. Network Menu

- On the Network menu, **Scroll** down to IPv4, IPv6/1, IPv6/2, MAC
- Press **Select** to enter the Submenu.
- Press **Scroll** and **Select** to **0-RETURN**, back to the previous menu.

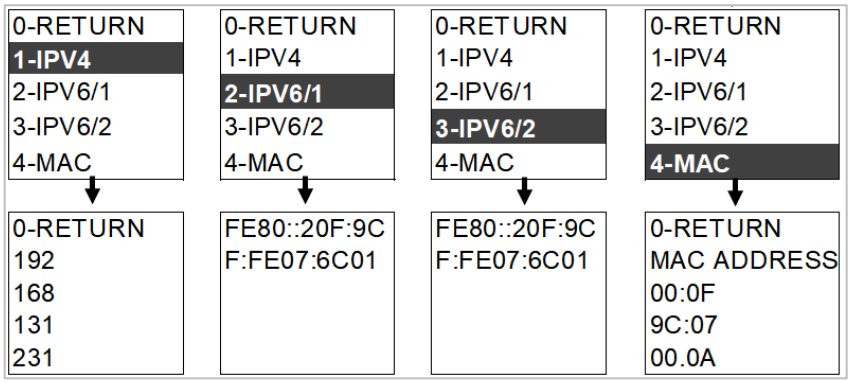


Figure 55. Network Submenu

Display Menu

The display menu allows you to view Sleep Set, Dir Set, Menu Delay & Beeper.

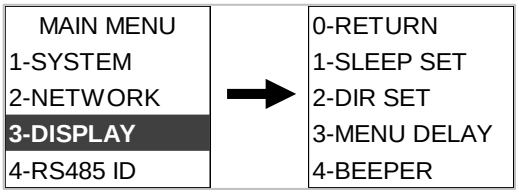


Figure 56. Display Menu

- On the Display menu, **Scroll** down to Sleep Set, Dir Set, Menu Delay & Beeper.
- Press **Select** to enter the Submenu. **Scroll** down to highlight the selected option from the submenu. Press **Select** the option.
- Press **Scroll** and **Select** to **0-RETURN**, back to the previous menu.

NOTE: Beeper default setting is off.

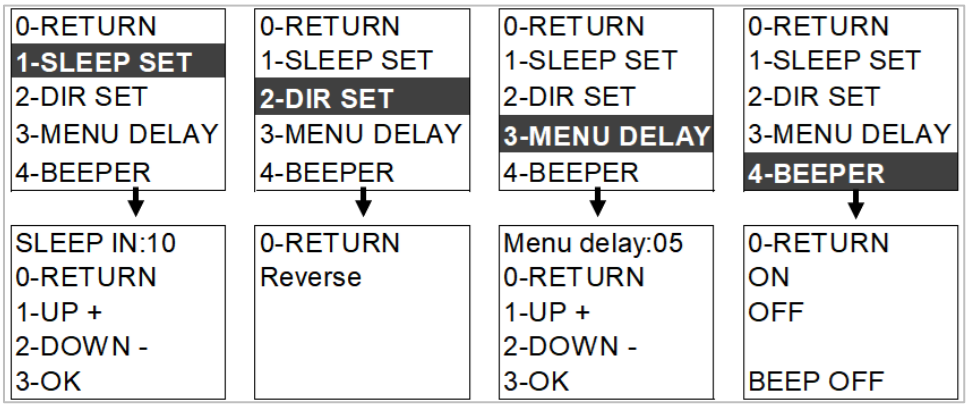


Figure 57. Display Submenu

RS485 Menu

The RS485 Menu is to manage ID of Daisy Chained PDUs (Review PartX – Daisy Chain Configuration) and allows you to view RS485 Set.

- On the Main Menu, **Scroll** down to RS485 ID.
- Press **Select** to enter the RS485 ID Submenu.
- The default is ID is 01, **Scroll** to UP+ or Down-, **Select** to required ID number.
- **Scroll** to **3-OK**, **Select** and complete the ID setting.

NOTE: The ID=00 is consider as the Host PDU.

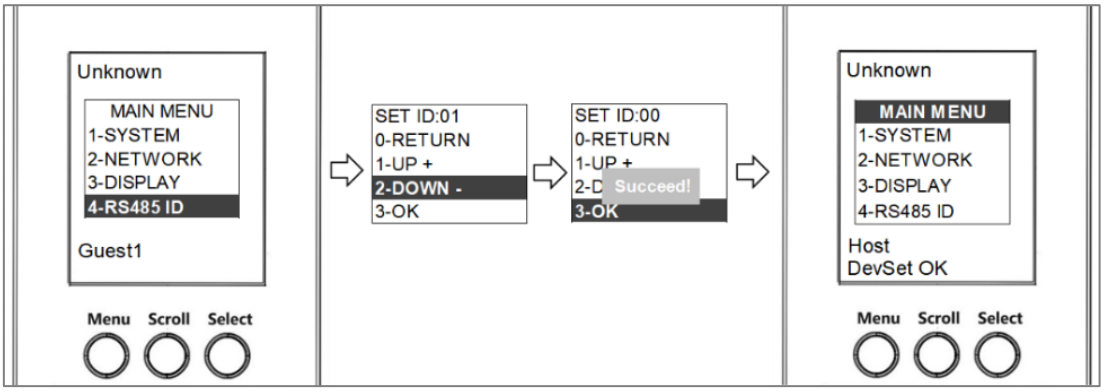


Figure 58. RS485 Menu

Power Menu

The Power menu allows you to view information of system, device, phase, bank and outlets. On the Main Menu, press **Select** to display each submenu from system to the Main menu.

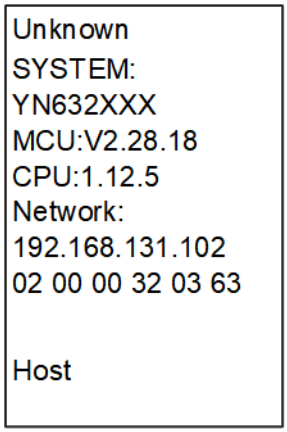


Figure 60. System Info.

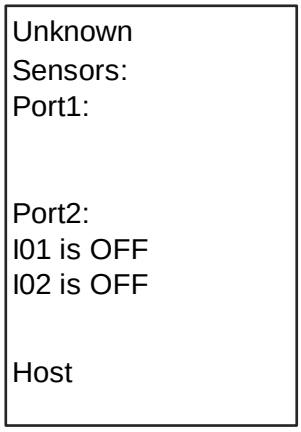


Figure 61. Sensor Info.

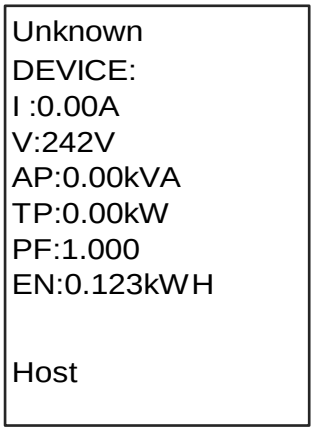


Figure 59. Device Info.

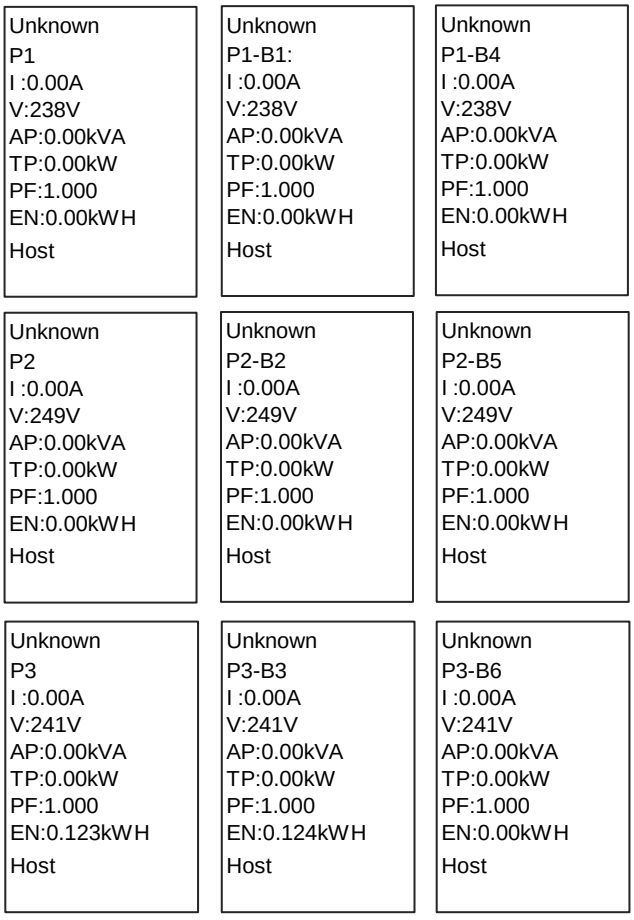


Figure 62. Phase, Bank Information

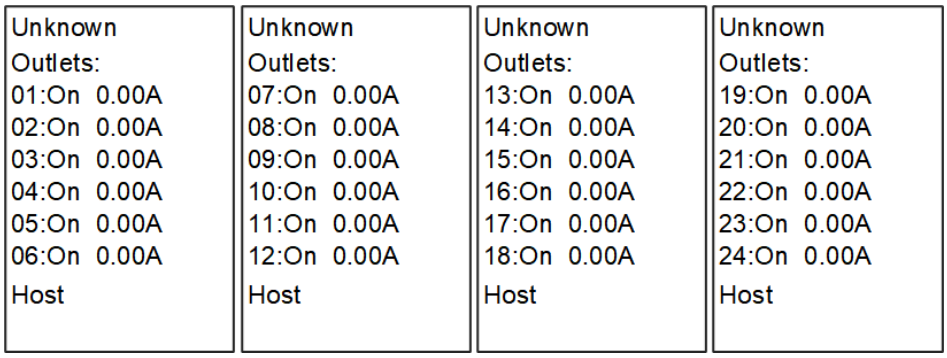


Figure 63. Outlet Information

Part Ⅵ. Daisy Chain Configuration

Daisy-Chain Overview

In daisy chain mode, up to (32) PDUs can be connected via one IP address. This allows users to gather information and data on all daisy chained PDUs from the main PDU. The daisy chain functionality reduces network cost for PDUs.

NOTE: When replacing a Daisy Chained PDU or Accessory, please 'RESTART' the Primary (main) PDU1 controller to re-synchronize the daisy chained PDUs sequence. This action will not disrupt operations (or outlet states) and can be completed remotely via Web GUI, SNMP or CLI or physically by pressing and holding the reset button on the primary controller for 10 seconds (but not more than 15 seconds).

Daisy-Chain Setup

- Select one PDU of daisy chain group as host, set its ID to 00(refer to *RS485 Menu* section)
- After the initial PDU is configured (host), connect an Ethernet cord from the **PDU Out** port on the configured PDU to the **PDU In** port on the second PDU in the daisy chain line.
- Repeat step 2, connecting PDUs from the **PDU Out** port to the **PDU In** port for up to 32 PDUs. Recommend setting the ID from 00-31, but discontinuous ID numbers will not impact system to recognize daisy chained PDU
- Go to Web User Interface to manage and control the PDUs in the daisy chain.

NOTE: The total length of the Ethernet cords connecting the PDUs must be less than 50m (164.04 ft.).

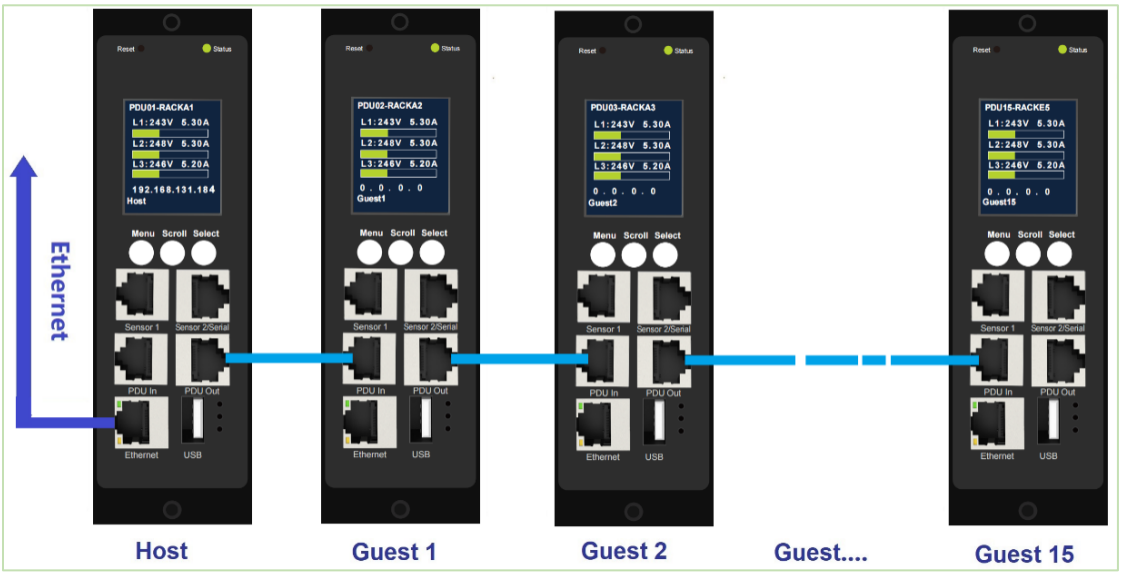


Figure 64. Daisy Chain Physical Connection Diagram

Appendix A: Firmware Upgrade Options

It's important to remain up to date on your PDU firmware as bugs are resolved and performance improves with every release. The firmware upgrade procedure verifies the image by validating the signature of the images. If the signature does not match, the firmware upgrade procedure will ignore the image and remain on the current version. Updating the firmware does not affect the configuration or outlet state of the intelligent PDU.

NOTE: If you load incompatible firmware, no damage will occur and PDU will maintain the original firmware.

Web Interface Method

- Open the User interface in a web browser by entering the PDU IP address.
- Login to with Administration credentials.
- Go to menu tap **Configuration>System Management> File Upgrade**
- In the Firmware Update dialog box, browse to (*.bin) firmware file.
- Click **Apply**, the system will update the newest firmware to the Network Controller.
- Upon the upload is finished, the system will reboot automatically.

Figure 65. Web Interface

YMODEN Method

To use YMODEM to upgrade one Rack PDU that is not on the network, you must extract the firmware files from the official website. Login to a FTPs program with a role with administration privileges.

- Select a serial port at the local computer and disable any service that uses the port.
- Connect the RJ-45 to DB-9 console cable to the serial port at the Rack PDU.
- Run a terminal program such as Tera Term® or HyperTerminal®, and configure the selected port for 115200 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
- Press the **Reset** button on the Rack PDU, then immediately press the Esc key several times until the Boot Monitor prompt displays: #>.
- Type Ymodem, then press **ENTER**.
- From the terminal program's menu, select **YMODEM**, then select the binary firmware file to transfer using YMODEM. After the YMODEM transfer is complete, the Boot Monitor prompt returns.
- Type reset or press the **Reset** button to restart the PDU's management interface.

USB Method

NOTE: Verified to work with ToshibaTM or SandiskTM up to 16GB USB Drives. Others USB drives may work as well. Before starting the transfer, make sure the USB drive is formatted in FAT32.

- Save the Firmware file ('pdu_img.bin') to a USB drive.
- Insert the USB drive into the USB port of the Network Controller.
- PDU will update the firmware automatically, waiting for about 30 seconds and check the firmware version from LCD
- When the update is complete, remove the USB.
- Press the Reset button and wait for device reboot fully.

Appendix B: NMC Firmware Update

Group Upgrade Tool

- Confirm that the PDU and the computer are in the same domain.
- Copy the new firmware file(*.bin) to "NMCFirmwareUpdate" folder.
- Upgrade firmware.

Single PDU Upgrade

- Open the NMCFirmwareUpdate tool, click the drop-down menu and select the correct firmware(*.bin).
- Select the Single Device menu and type the correct the IP address, user name and password of PDU to be upgraded.
- Click "Start Upgrade" button to upgrade the new firmware.

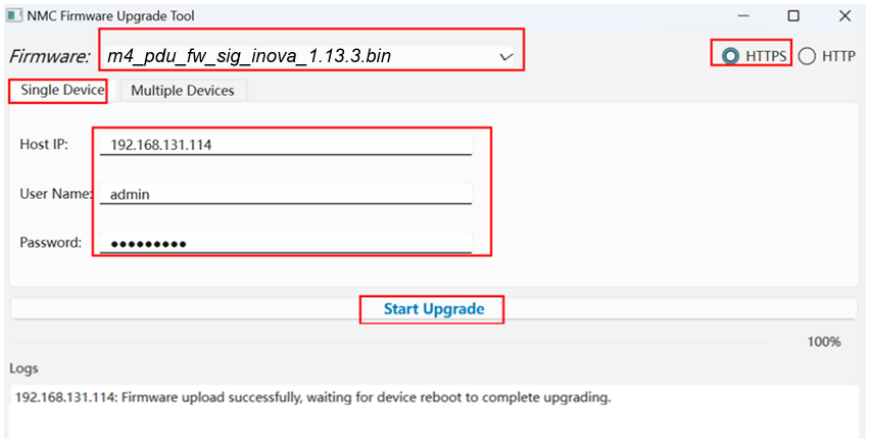


Figure 66. Single PDU Upgrade

Multiple PDU Upgrade

- Open the "Devices" file of NMCFirmwareUpdate folder, and type the correct IP address, user name and password of PDU to be upgraded, then save and close the file;
- Open the NMCFirmwareUpdate tool, and click the drop-down menu and select the correct firmware(*.bin) ;
- Select the Multiple Devices and click "Start Upgrade" button to upgrade the new firmware.

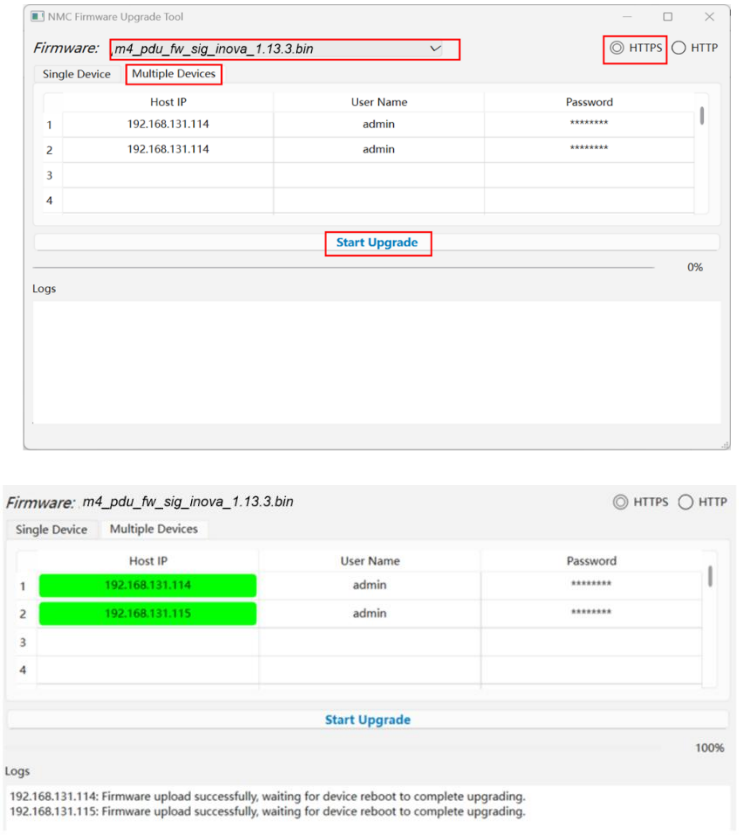


Figure 67. Multiple PDU Upgrade

Appendix C: System Reset or Password Recovery

Use Reset Button on Controller

Press and hold the Reset Button for 8 seconds to recover from an Intelligent Network Controller communication failure. This will cause a reset of the iNC controller, all configuration(s) will be retained.

To Default the controller to factory settings, press and hold the Reset Button for at least 20 seconds. This will cause a reset of the controller erasing all existing configurations, including username(s) and password(s). It does not change the Energy (kWh) value and does not affect the outlet state.

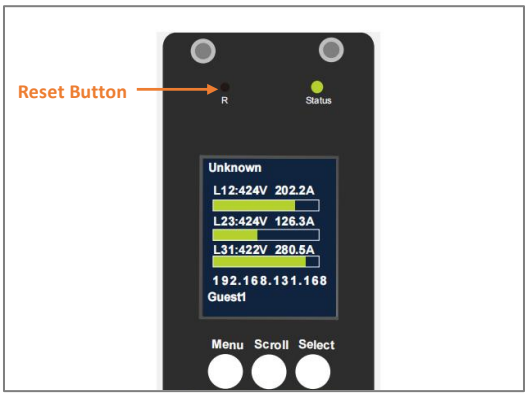


Figure 68. Use Reset Button

Resets Command from Submenu

CPU Reset

CPU reset command will cause a reset of controller erasing all existing network configurations, including username(s) and password(s), network configurations, it does not change the Energy(kWh) value and does not affect the outlet state.

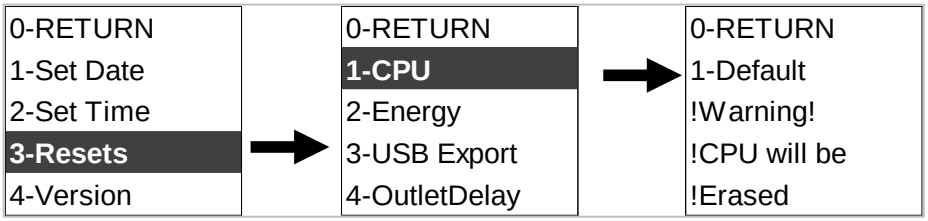


Figure 69. CPU Rest

Reset/Reboot from Web UI

The menu provides the option to reset and reboot various components of the network interface. More details refer to Page 23.

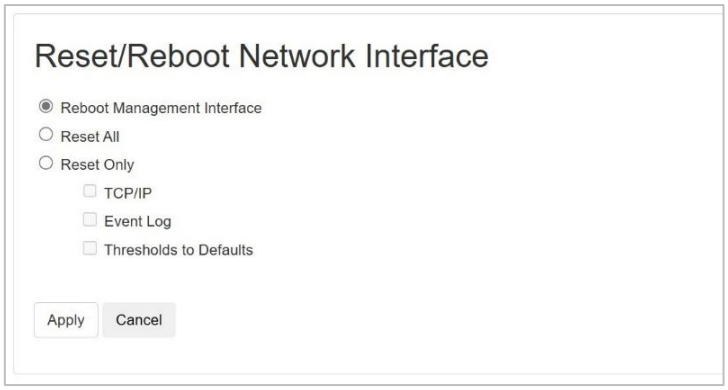


Figure 70. Reset/Reboot from Web UI

Appendix D: PDU Alarms

PDU Unit	PDU Unit Active Power Above upper warning PDU Unit Active Power Below lower warning
Input Phase	Input Phase X Current Above upper warning Input Phase X Current Below lower warning
Circuit Breaker	Circuit Breaker X Current Above upper warning Circuit Breaker X Current Below lower warning Circuit Breaker status OFF
Outlet	Outlet X Active Power Above upper warning Outlet X Active Power Below lower warning
External Sensor	External Sensor X (numerical) Above upper warning External Sensor X (numerical) Below lower warning External Sensor X (state) Alarmed External Sensor X (state) Communication Lost

Trap Class	Trap Description
Critical	The PDU unit active power is ABOVE critical threshold value.
	The PDU unit active power is BELOW critical threshold value.
	The phase (1-3) current is ABOVE critical threshold value.
	The phase (1-3) current is BELOW critical threshold value
	The outlet (1-48) active power is ABOVE critical threshold value
	The outlet (1-48) active power is BELOW critical threshold value
	The sensor (1-8) temperature/humidity is ABOVE critical threshold value
	The sensor (1-8) temperature/humidity is BELOW critical threshold value
	Input Phase (1-3) Frequency Asserted below lower critical.
	Input Phase (1-3) Frequency Asserted above upper critical
Trap Class	**Trap Description**
Warning	The PDU unit active power is ABOVE warning threshold value.
	The PDU unit active power is BELOW warning threshold value.
	The phase (1-3) current is ABOVE warning threshold value.
	The phase 1 current is BELOW warning threshold value.
	The outlet (1-48) active power is ABOVE warning threshold value.
	The outlet (1-48) active power is BELOW warning threshold value.
	The sensor (1-8) temperature/humidity is ABOVE warning threshold value.
	The sensor (1-8) temperature/humidity is BELOW warning threshold value.
Trap Class	**Trap Description**
Clear	The PDU unit active power is alarm clear.
	The phase (1-3) voltage alarm cleared
	The phase (1-3) current alarm cleared
	The outlet (1-48) active power current alarm cleared.
	The sensor (1-4) temperature/humidity alarm cleared.
	The sensor (1-4) lost communication alarm cleared.

Appendix E: Direct Connect to the PDU

NOTE: Instructions refer specifically to Windows 10. Please refer to your operating system documentation if you are not using Windows 10.

- Type **control** into Windows Search and select **Control Panel**.

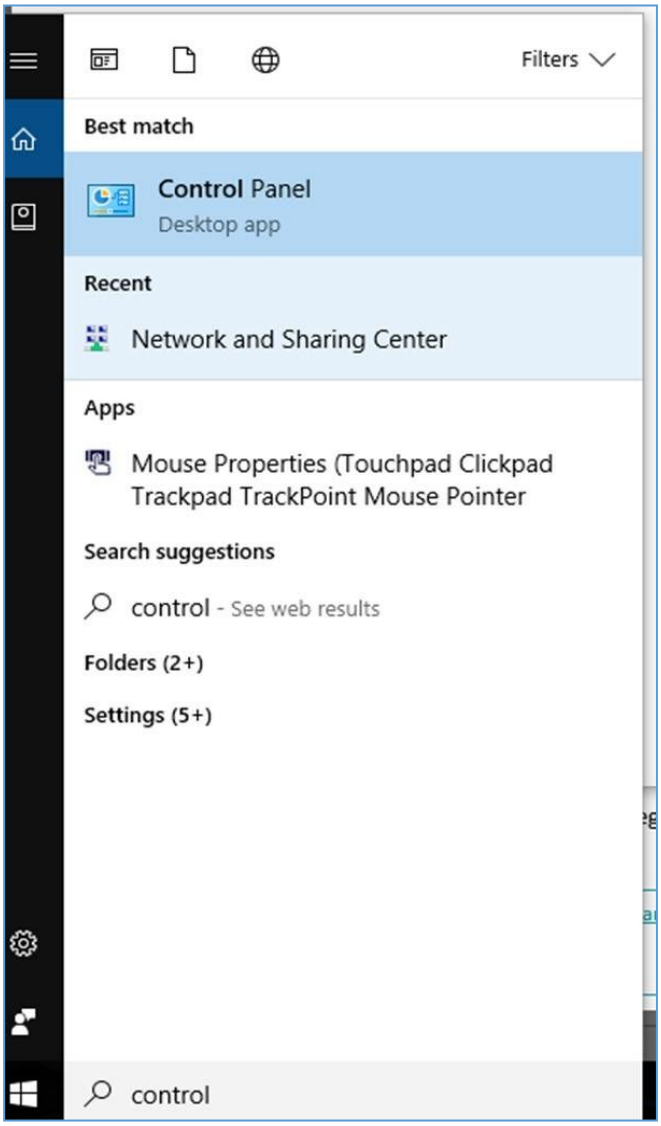


Figure 71. Control Panel

- In the Control Panel window, select **View network status and tasks** under the Network and Internet heading.

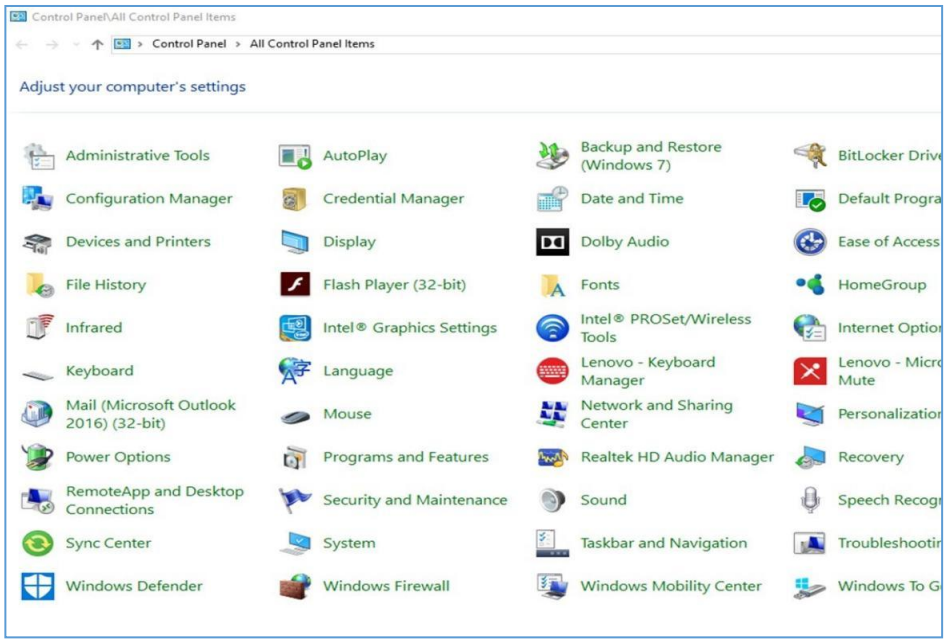


Figure 72. Control Panel Items

- Select **Change adapter settings** from the menu on the left.

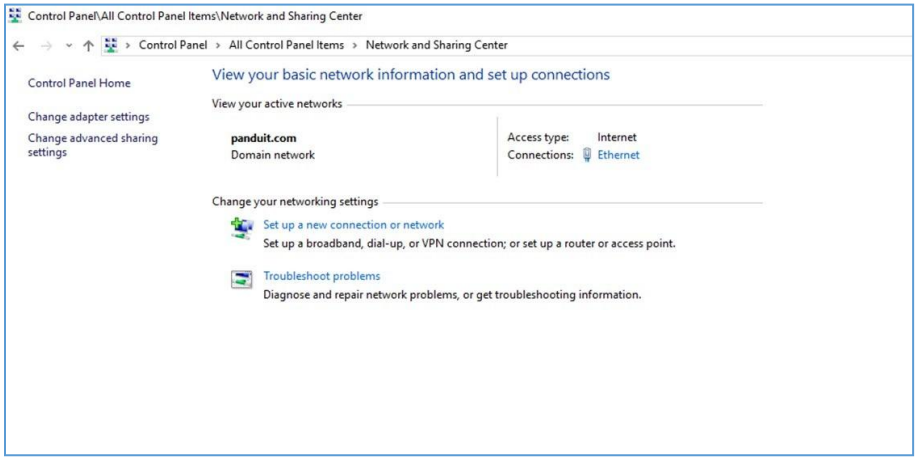


Figure 73. Network and Sharing Center

- Right-click **Ethernet** and select **Properties**.

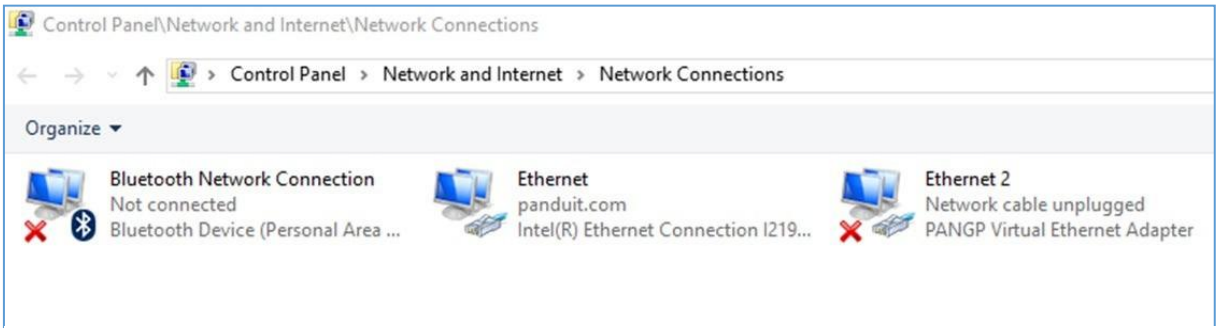


Figure 74. Network Connections

- Select **Internet Protocol (TCP/IP) Version 4** (you may need to scroll down). Then click the **Properties button**.

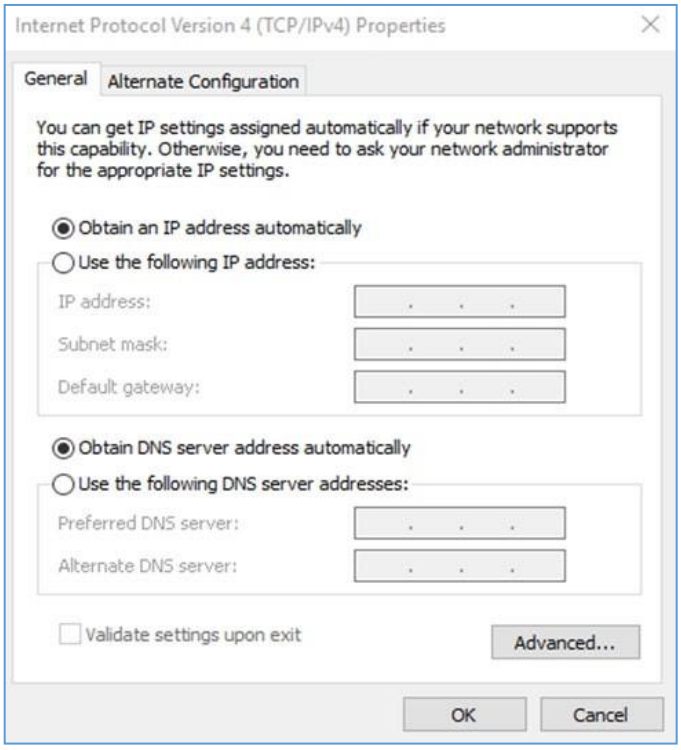


Figure 75. Internet Protocol (TCP/IP) Version 4

- Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically radio button**, enable DHCP function.
- Connect the PDU network connection directly to the PC's Ethernet card using a patch cable.
- Power the PDU unit.
- Open a web browser on the PC.
- Enter the IP address from NMC LCD display into your browse

Appendix F: Command Line Interface (CLI)

The Command Line Interface (CLI) is an alternate method used to manage and control the PDU status and parameters, as well as basic admin functions. Through the CLI a user can:

- ✧ Reset the PDU;
- ✧ Display PDU and network properties;
- ✧ Configure the PDU and network settings;
- ✧ View user information;

The CLI uses YMODEM to perform the file transfer. However, you cannot read the current file through YMODEM.

The PDU CLI command set for managing and monitoring the PDU includes the following commands:

- ✧ help command: PDU help query；
- ✧ tcpip command: Configuration and display tcpip parameters;
- ✧ web command: Configuration and display web parameters;
- ✧ version command: System version;
- ✧ reset command: System parameters reset to default;
- ✧ reboot command: System reboot;
- ✧ mac command: Configuration device mac address.

Connecting To the CLI Through the Serial Interface

An option to communicating through the serial interface is to use the specialized YOST Serial Data Cable. This cable Remaps Serial Interface to a YOST interface.

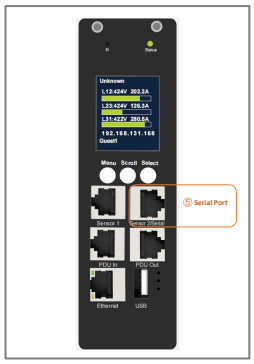


Figure 76. Connect to Serial Port

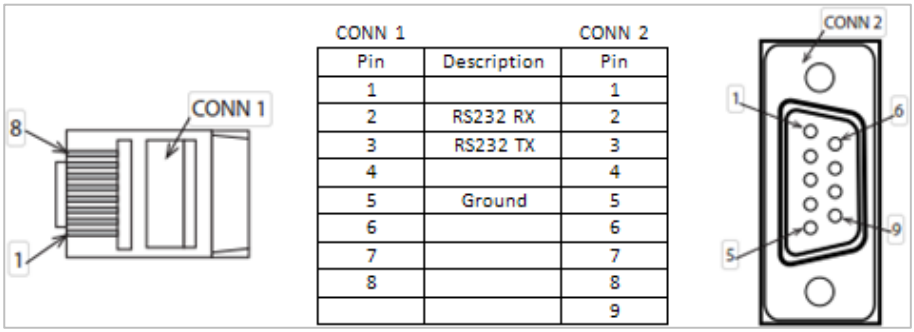
Logging in with HyperTerminal

To login through HyperTerminal, set the COM settings to the following parameters:

- ✧ Bits per second: 115200
- ✧ Date bits: 8
- ✧ Parity: None
- ✧ Stop bits: 1
- ✧ Flow control: None

Serial Cable Pinout to Create Your Own Cable

Optionally if you prefer to make your own RJ45-to-DB9 Serial cable, the connections are wired as shown:



CONN 1		CONN 2
Pin	Description	Pin
1		1
2	RS232 RX	2
3	RS232 TX	3
4		4
5	Ground	5
6		6
7		7
8		8
		9

Figure 77. Serial Cable Pinout Logging in via PuTTY

- ➢ Select a serial port at the computer and disable any service that uses that port.
- ➢ Connect the serial cable from the selected serial port on the computer to the Serial port on the Rack PDU.
- ➢ Run PuTTY (Tera Term® or HyperTerminal®) and configure the selected port (115200 bps, 8 data bits, no parity, 1 stop bit, and no flow control).
- ➢ Press Enter. It may take multiple (up to three) attempts to get a prompt to appear. At the prompt, enter your username and password.

CLI Commands

Help Commands

Table 11. Help Commands

Command	Description	Example
>help	List all available PDU CLI commands.	>help **tcpip** Configuration and display tcpip parameters. **web** Configuration and display web parameters. **Version** System version. **reset** System parameters reset to default. **Reboot** System reboot. **mac** Configuration device mac address

System Commands

Table 12. System Commands

Command	Description	Example
Version	System version	>version bootloader version: bootloader-V1.8 firmware version: FW-M4-1.9.11
Reset -c	Remove Certificate	> reset -c Remove Certificate
Reset -n	Reset Network parameters	> reset -n Reset Network parameters
Reset -d	Reset Device parameters	> reset -d Reset Device parameters
Reset -a	Reset All parameters	> reset -a Reset All parameters
Reboot	System reboot	> reboot Bootloader start

Network Commands

Table 13. Network Commands

Command	Description	Example
Web -a http	Web UI Access mode. Access Web UI with Http protocol.	> web -a http
Web -a http	Web UI Access mode. Access Web UI with https protocol.	> web -a http
Web	To view the TCP/IP port used by HTTP.	> web Http: enabled Https: disabled Http Port: 80 Https Port: 443

		Minimum Protocol: TLS1.2

Command	Description	Example
tcpip	To view the network settings of the PDU	> tcpip Active IPv4 Settings ----------
		Active IPv4 Address: 192.168.131.104 Active IPv4 Subnet Mask: 255.255.255.0 Active IPv4 Gateway: 192.168.131.1 Manually Configured IPv4 Settings ----------
		IPv4: enabled IPv4 Address: 192.168.8.8 Subnet Mask: 255.255.255.0 Gateway: 192.168.8.1 MAC Address: 58-fc-db-80-6c-1d Active IPv6 Settings ----------
		IPv6 link local address: FE80::5AFC:DBFF:FE80:6C1D IPv6 unicast address:
tcpip -i	To view the IP address of the PDU	> tcpip -i IPv4 address: 192.168.08.08 > tcpip -i 192.168.8.9 IPv4 address: 192.168.08.09 Reboot required for change to take effect
tcpip -m	Get IP address manually or with DHCP.	> tcpip -m Mode: DHCP > tcpip -m manual Mode: Manual Reboot required for change to take effect. > tcpip -m dhcp Mode: dhcp Reboot required for change to take effect.
tcpip -s	Type the subnet mask for the Rack PDU.	> tcpip -s Sub mask: 255.255.255.0
tcpip -g	Type the IP address of the default gateway. Do not use the loopback address (127.0.0.1) as the default gateway	> tcpip -g Gateway: 192.168.131.1
MAC	Configuration device mac address	> mac Mac address: 58-fc-db-80-6c-1d > mac 58fcdb806c1c

		58-fc-db-80-6c-1c

Appendix G: NMC REST API

The 'REST' API uses posts and gets to serval key URIs on the device:

- /api/login: for user authentication;
- /api/bulk/#: for querying device data in batches;
- /api/firmware/upload: for uploading and updating firmware;
- /files/config/#: for accessing or modifying the device's configuration files;
- /files/control/#: for performing control actions on the device.

NOTE: '#' is only the guest unit ID number in Network sharing mode.

Authentication

If the device is configured with a user of 'admin' and his password is '123456' login by:

Post {"username": "admin", "password":"123456"} to /api/login

The device will respond with a statusCode of 200 if accepted or a 401 (unauthorized) if the credentials are not correct.

If the device responded with 200, save csrfToken for continued use with the session. The body will contain json with the following information:


```
{
    "status":"success",
    "passwordexpired":false,
    "csrfToken":"26cAr5JmvTgV8lXD",
    "access":["admin","ctrl","base","changeOwnPass"],
    "config/sessionMgmt":{
        "signInRetriesLimited":1,
        "numRetries":3,
        "sessionTimeoutValue":"30 minutes",
        "lockoutTime":"10 minutes"
    }
}
```


If the password is expired, or was never initially changed, the body will contain the following:


```
{
    "status": "success",
    "passwordexpired": true,
    "csrfToken": "$2b$04$...",
    "access": ["changeOwnPass"]
}
```


Prior to accessing any further information, change the password by pos ng the following to /api/login:

{"username": "admin", "password":"123456", "newpassword":"newSuperPassword"}

Session

After successfully logging in, any data/functionality available to the authenticated user may be accessed/written. Each successive post must include the csrfToken in the headers as follows:

headers['X-CSRF-Token'] = prevBody[‘csrfToken’]

Every response from the device will contain a csrfToken and the most recent should be sent.

Reading Data

Data is read by posting a JSON array of queries to /api/bulk. A wildcard (*) may be used to request multiple items but must be at the end of the request item. See the data model sec on for more details.

```
{"items": [{"id": "status/phaseInput"}]}    // read phase input data
{"items": [{"id": "status/phaseInput*"}]}   // read all phase input data
{"items": [{"id": "status/outlet"}]}        // read outlet status
{"items": [{"id": "status/sensor"}]}        // read sensor data
{"items": [{"id": "status/systemInfo"}]}    // read system Infomation
```

Read example:

POST:

```
{"items": [{"id": "status/systemInfo"}]}
```

Response:


```
{
    "csrfToken":"26cAr5JmvTgV8lXD",
    "query":{
        "status/systemInfo":{
            "appVer":"1.13.3-42-gc53e57d-dirty",
            "bootVer":"bootloader-V1.8",
            "interVer":"","hardwareVer":"0.1",
            "contactName":"Unknown",
            "location":"Unknown",
            "deviceName":"Unknown"
        }
    },
    "errors":{}
}
```

Configure Data

This api supports network parameters configure, like TCP/IP, SNMP, and Modbus.

Config TCP/IP Example:

POST:

```
{
    "tcpip" {
        "bootmode": "dhcp",
        "ipv4addr": "192.168.8.8",
        "subnetmask": "255.255.255.0",
        "defaultgw": "192.168.8.1",
        "defaultdns": "192.168.8.1"
    }
}
```

Response:

```
{"csrfToken":"lvfYCVDG3wRevaJ7","updateResult":"OK"}
```

Config SNMP Example:

POST:

```
{
    "snmp" {
        "trapserver": "192.168.8.8",
        "version1": "enable",
        "readcommunity": "public",
        "writecommunity": "private"
    }
}
```

Response:

```
{"csrfToken":"lvfYCVDG3wRevaJ7","updateResult":"OK"}
```

Config Modbus Example:

POST:

```
{
    "modbus" {
        "enable": "1"
    }
}
```

Response:

```
{"csrfToken":"lvfYCVDG3wRevaJ7","updateResult":"OK"}
```

Request Errors

If there are errors in the data id, access levels or the data value is out of range, the device will add an error response for the specific id with an error.

POST:

```
{
    "items": [{
            "id": "config/systemInfo/contactPerson",
            "val": "Test Value"
        }
    ]
}
```

Response:

```
{
    "csrfToken": "$2b$04$...",
    "errors": {
        "config/systemInfo/contactPerson": "DB_INVALID_ID"
    }
}
```

Firmware Uploads

Files are uploaded both for firmware updates by pos ng a mul part/form-data stream to the respec ve URI. The device assumes the proper multipart headers are set.

For FW Uploads, post the file to:

/api/firmware/upload

After the firmware is posted, the device will return a status code ‘200’, then validate and start flashing the new firmware. While the device is writing the firmware it may be unresponsive. The device will reboot a er the new firmware is flashed. When the device responds.

This API is mainly for NMC Firmware upgrade tool for multiple devices upgrading.

Control

For control device, post the content to:

/api/control

with example: Reboot device:

POST:

```
{"action": "reboot"}
```

Response:

```
{"csrfToken":"lvfYCVDG3wRevaJ7","updateResult":"OK"}
```

With example: Turn OFF outlet 5

POST:

```
{"outlet": {"name": "outlet5", "status":"off"}
```

Response

```
{"csrfToken":"lvfYCVDG3wRevaJ7","updateResult":"OK"}
```

With example: Turn ON ALL outlets

POST:

```
{"outlet": {"name": "all", "status":"on"}
```

Response:

```
{"csrfToken":"lvfYCVDG3wRevaJ7","updateResult":"OK"}
```

Appendix G: Secure Shell (SSH)

SSH is a network security protocol, mainly used for remote login, command line control, file transfer and other operations. It protects data transmission through encryption technology to avoid the security risks caused by plain text transmission in traditional protocols (such as Telnet and FTP).

Manage The PDU

- Connect the PDU to Ethernet network and confirm that the PDU and the computer are in the same domain.
- Open Serial tool of Putty or Tera Term, type the IP address of PDU, set the connection type to SSH mode, then click Open button.

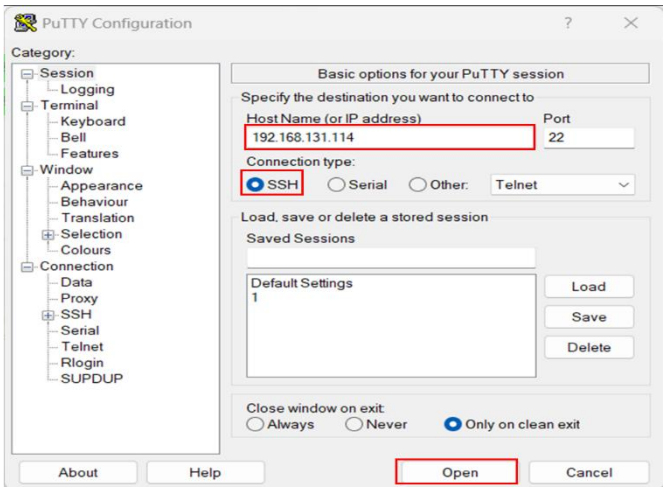


Figure 78. PuTTY Configuration

- Type the correct login account and password, then manage the PDU by CLI command.

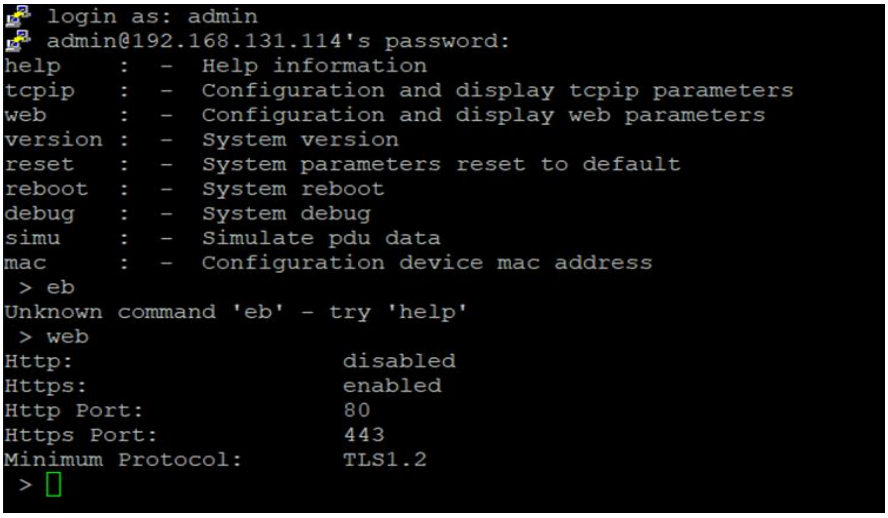


Figure 79. Login Account

Inova

Choose Us, Choose More Options

Selecting our containment solutions means choosing a partner dedicated to providing a wide array of options for your data center needs. Enjoy the benefits of efficient cooling, energy savings, and a tailored solution that evolves with your infrastructure.

For inquiries and consultation, contact sales@inovadc.com.