



The power behind competitiveness

Delta InfraSuite Power Management

Rack Power Distribution Unit (rPDU)

ViLink Series, Metered Type

User Manual

www.deltaww.com



SAVE THIS MANUAL

This manual contains important instructions and warnings that you should follow during the installation, operation, storage and maintenance of this product. Failure to heed these instructions and warnings will void the warranty.

Copyright © 2025 by Delta Electronics Inc. All Rights Reserved. All rights of this User Manual ("Manual"), including but not limited to the contents, information, and figures are solely owned and reserved by Delta Electronics Inc. ("Delta"). The Manual can only be applied to the operation or the use of this product. Any disposition, duplication, dissemination, reproduction, modification, translation, extraction, or usage of this Manual in whole or in part is prohibited without the prior written permission of Delta. Given that Delta will continuously improve and develop the product, changes may be made to the information in this Manual at any time without obligation to notify any person of such revision or changes. Delta will make all possible efforts to secure the accuracy and the integrity of this Manual. Delta disclaims any kinds or forms of warranty, guarantee, or undertaking, either expressly or implicitly, including but not limited to the completeness, faultlessness, accuracy, non-infringement, merchantability or fitness for a particular purpose of the Manual.

Table of Contents

Chapter 1 : Important Safety Instructions.....	5
1.1 Safety Precautions	5
1.2 Precautions for Rack Mounting.....	5
1.3 Precautions for Connecting to a Power Source	6
1.4 Maintenance with Input Power	6
1.5 Electromagnetic Interference	7
Chapter 2 : Introduction	8
2.1 General Overview.....	8
2.2 Package Inspection.....	8
2.3 Features & Functions	9
2.4 Circuit Breaker	11
2.5 Output Socket.....	11
Chapter 3 : rPDU Installation	12
3.1 Mounting on Delta Standard Rack.....	12
3.2 Mounting on Delta Standard Rack (Side-hung)	17
3.3 Mounting on Other Racks.....	18
Chapter 4 : rPDU Connection	19
4.1 Plug in the rPDU	19
4.2 Output Sockets.....	19
4.3 Retention Sleeves (Optional).....	21
Chapter 5 : Communication Interfaces.....	23
5.1 Remote Monitoring Controller.....	23
5.1.1 RMC General Specification	24
5.1.2 Reset the RMC.....	25
5.2 Daisy Chain Ports.....	25
5.3 LED Indicator and Display	26
5.4 Serial Port	26
5.5 Network Port	27
Chapter 6 : Web User Interface.....	28
6.1 Check IP Address from the Console	28

6.2	Login to the Web Page	29
6.3	Web Page	31
Chapter 7 : Daisy Chain		74
7.1	Connection of rPDUs in A Daisy Chain	74
7.2	Daisy Chain Web Page Initial Setup.....	75
7.3	Firmware Upgrade for Chained rPDUs.....	77
Chapter 8 : Troubleshooting		79
Chapter 9 : Optional Accessories.....		80
Appendix 1 : Warranty.....		81

Chapter 1 : Important Safety Instructions

1.1 Safety Precautions

To reduce the risk of personal injury from electric shock, you must observe the following safety precautions when placing, installing, operating, or performing maintenance on the Delta Rack Power Distribution Units (rPDU)

- The product is designed for indoor use only in a controlled environment away from excess moisture, temperature extremes, conductive contaminants, dust or direct sunlight.
- Do not connect the rPDU to an ungrounded outlet or extension cords and adapters that eliminate the connection to ground.
- Do not use the rPDU in the presence of flammable substances.
- The power requirement for each piece of equipment connected to the rPDU must not exceed the load rating of individual output sockets.
- The total power requirement for equipment connected to the rPDU must not exceed the maximum load rating for the rPDU.
- Do not drill into or attempt to open any part of the rPDU housing. There are no user serviceable parts inside.
- Do not modify the rPDU, including the input plugs and power cables.
- Do not use the rPDU if any part of it becomes damaged.
- Do not mount the rPDU to an insecure or unstable surface.
- Never install electrical equipment during a thunderstorm.
- Suitable for installation in Information Technology Rooms.
- The rPDU is not suitable for use in locations where children are likely to be present.

1.2 Precautions for Rack Mounting

- **Elevated Operating Ambient:** If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.
- **Reduced Air Flow:** Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

- **Mechanical Loading:** Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading:** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing:** Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (such as use of power strips).

1.3 Precautions for Connecting to a Power Source

- Only a certified electrician can connect the rPDU with a power source.
- Do not remove the cover. There are no internal components that a user can service.
- A certified electrician must install a circuit breaker when connecting the rPDU to a power source. This protects the rPDU against over current.
- A certified electrician must determine the type of circuit breaker required depending on the input voltage.
- Before connecting the power supply, make sure you verify the earth connection.
- The use of a detachable input power cord is prohibited.
- The plug on the power supply cord is intended to serve as the disconnect device. The outlet of power source shall be installed near the equipment and shall be easily accessible.
- The short-circuit protection device is considered to be provided external to the equipment, a circuit breaker with adequate breaking (rupturing) capacity to interrupt the maximum fault current is provided between the equipment and the building installation.

1.4 Maintenance with Input Power

Delta strongly recommends that you do not perform maintenance on the rPDU if it is receiving input power. However, if critical maintenance is required on the rPDU connected to input power, please reduce your risk of electric shock by strictly following the precautions below.

To reduce your risk of personal injury by electric shock, you must:

- Be a certified electrician trained in live electrical installation.
- Always work with another qualified person.

- Know how to disconnect electricity to the rPDU and data center in case of emergency.
- Wear the right protective equipment.
- Use double-insulated tools.
- Strictly follow local and site regulations.

1.5 Electromagnetic Interference

This is a Class A product. In a domestic environment, the product may cause radio interference in which case the user may be required to take adequate measures.

Chapter 2 : Introduction

2.1 General Overview

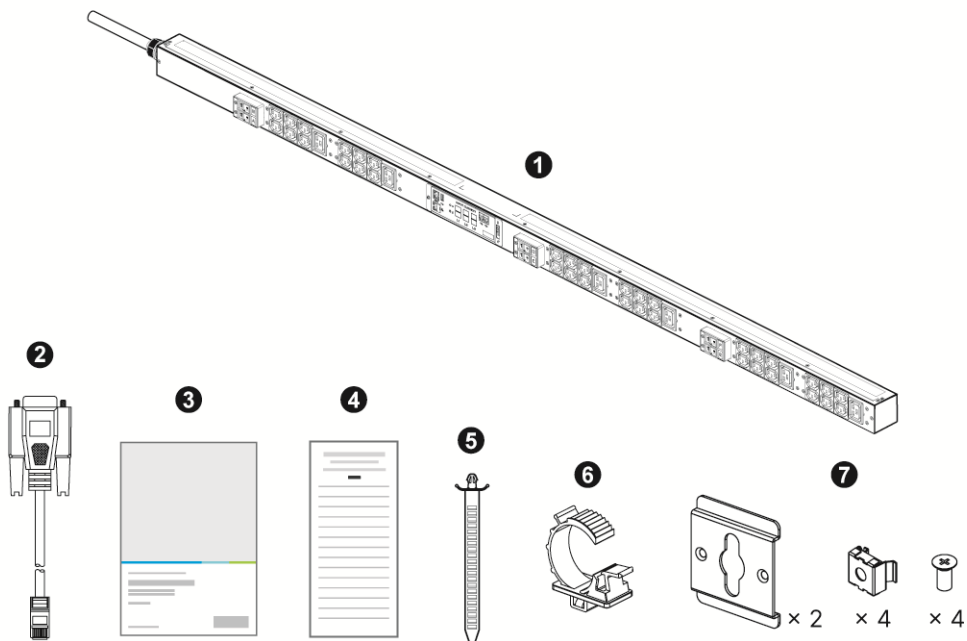
The Delta ViLink Metered Rack Power Distribution Unit (hereinafter referred to as the rPDU) is a product of the Delta intelligent rPDU family. The rPDU distributes power to equipment mounted in racks and enclosures used in data centers as well as IT and telecom installations. The rPDU installs vertically without tools in the rear of a rack and without requiring a unit space. Input to the rPDU can be either single phase or three phase America/ Taiwan or International voltages.

The rPDU features remote access to allow users to monitor its status, including input voltage, branch current, power information and environmental conditions via the Ethernet network.

Regarding detailed specifications, please refer to the individual datasheet of rPDU.

2.2 Package Inspection

The rPDU package contains the following items:



No.	Item	Quantity
❶	Power Distribution Unit	1 PC
❷	RJ45 to DB9 Cable	1 PC
❸	User Manual	1 PC
❹	Installation & Operation Quick Guide	1 PC
❺	Cable Tie	Based on the rPDU's total output socket quantity
❻	Cable Tie Fixing Holder	
❼	Mounting Bracket Kit (including two mounting brackets, four cage nuts and four screws)	1 Set

2.3 Features & Functions

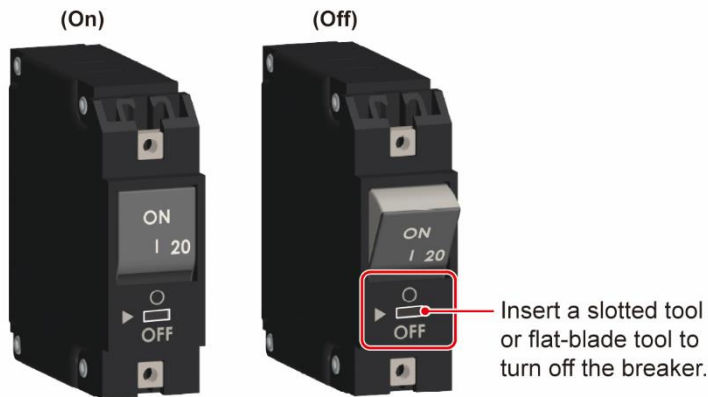
Feature	Function
 ACCESS CONTROL	Supports state-of-the-art authentication (e.g. LDAP(s), RADIUS, TACACS+) to secure rPDU access.
 ACCURACY	Independently verified by the IEC 62053-21 standard to meet 1% billing grade accuracy requirement.
 CABLE LOCKING	- Cable ties and their fixing holders are provided. - Plastic flexible retention sleeves are available (optional). - Compatible with P-locks and IEC locks (optional).
 CIRCUIT PROTECTION	Equipped with the UL489 certificated magnetic-hydraulic circuit breaker for each branch circuit protection, and the UL248 certificated fuse (optional) for each branch circuit protection.

Feature	Function
 COLOR GROUPING	• Colour options include red, blue and green. • Associates output sockets on the same phase with related breaker(s) to differentiate phase-breaker-socket groups.
 DAISY CHAIN	• Allows up to 40 rPDUs connected together to be monitored and controlled under one IP address, which reduces IP addresses.
 GIGABIT ETHERNET	• Supports 10/ 100/ 1000 Mbps Ethernet connectivity. • Provides up to 1 Gbps Ethernet connectivity in anticipation of future networking topologies.
 IPv4 & IPv6	• Supports both IPv4 and IPv6 protocols.
 LOCAL DISPLAY	• Provides local users with real-time information. • Displays input current of individual lines on an auto-flip LED for local installation and maintenance.
 METERING	• Input metering functions to measure voltage (V), current (A), power (W), energy (Wh), apparent power (VA), PF, THDv (%) and THDi (%).
 NETWORK MONITORING	• Provides multiple secured network protocols, including HTTP/HTTP(S), SSH/SSL, SNMP, IPv4, IPv6 and LDAP(S) for the management of rPDUs.
 TOOL - FREE	• An inbuilt hot-swappable and tool-free remote monitoring controller (RMC) allows users to remove, install and maintain easily.

2.4 Circuit Breaker

- Circuit Breaker with Handle Guard

The handle of circuit breaker should be in the ON position during operation. Once a slotted tool or flat-blade tool is inserted into the OFF slot manually as shown in *Figure 2-1*, the circuit breaker would be turned off.



(Figure 2-1: Circuit Breaker with Handle Guard)

- To reset the circuit breaker, its handle should be turned to the ON position.
- If the circuit breaker is tripped due to over current, please set its handle to the OFF position first and then reset back to the ON position.

2.5 Output Socket

- The C13 socket is rated 10 Amax / 200 - 240Vac.
- The C19 socket is rated 16Amax / 200 - 240 Vac
- Each branch of rPDU is rated 16 Amax / 200 - 240Vac.

Chapter 3 : rPDU Installation

You can install the rPDU into a rack using toolless mounting pegs and, if needed, mounting brackets. Once in rack, you can plug devices' power cords into the rPDU's output sockets and secure them to the rPDU's retention slots using the cable ties (provided).



NOTE:

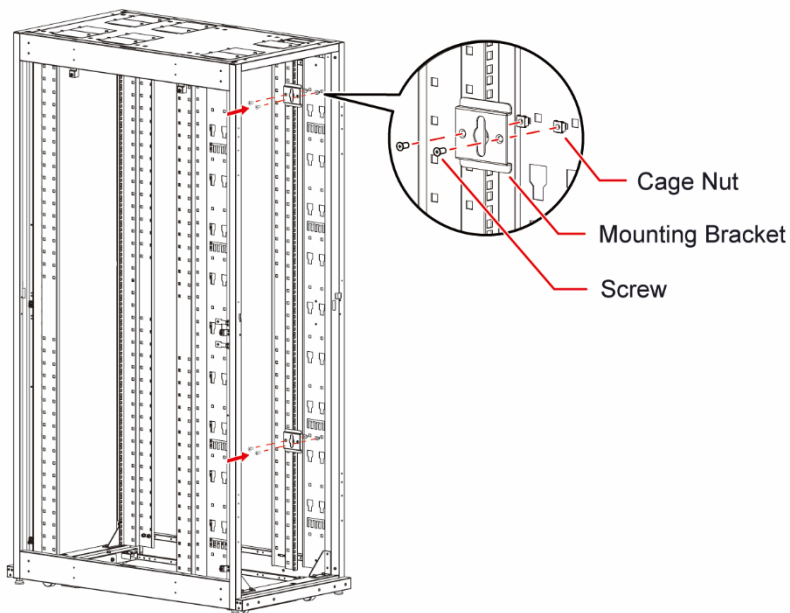
Mounting brackets varies with different racks and situations. For better feasibility, please contact Delta customer service for more information.

3.1 Mounting on Delta Standard Rack

The rPDU can be vertically installed at the rear of the rack. Mounting brackets are required for the installation of the rPDU.

Step 1

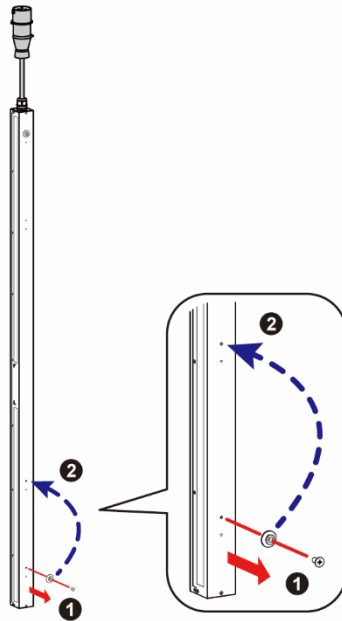
Put cage nuts into the EIA holes between 11U & 12U and 39U & 40U on the Delta Standard Rack. And fasten the mounting brackets to cage nuts with screws. We recommend you use #2 Phillip screwdriver to fasten the screws. See *Figure3-1*.



(Figure 3-1: Install the Cage Nuts and Mounting Brackets)

Step 2

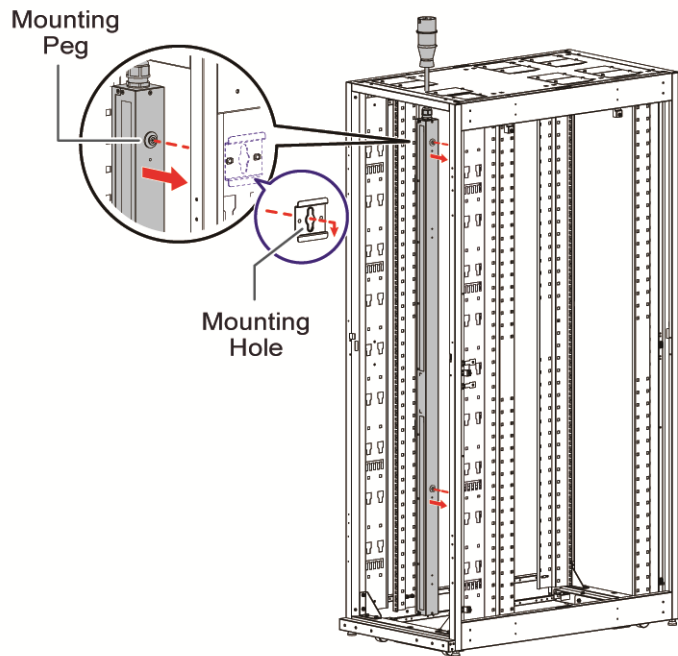
When the power cord goes up, the toolless mounting peg should be adjusted to relative position (from ① to ②) following the mounting bracket. We recommend the use of #2 Phillip screwdriver. See *Figure 3-2*.



(Figure 3-2: Adjust the Toolless Mounting Peg to Relative Position)

Step 3

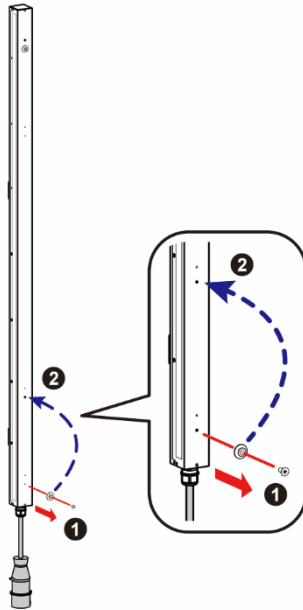
Hold the rPDU vertically and align its toolless mounting pegs with the mounting holes. See *Figure 3-3*.



(Figure 3-3: Align the Mounting Pegs with the Mounting Holes)

Step 4

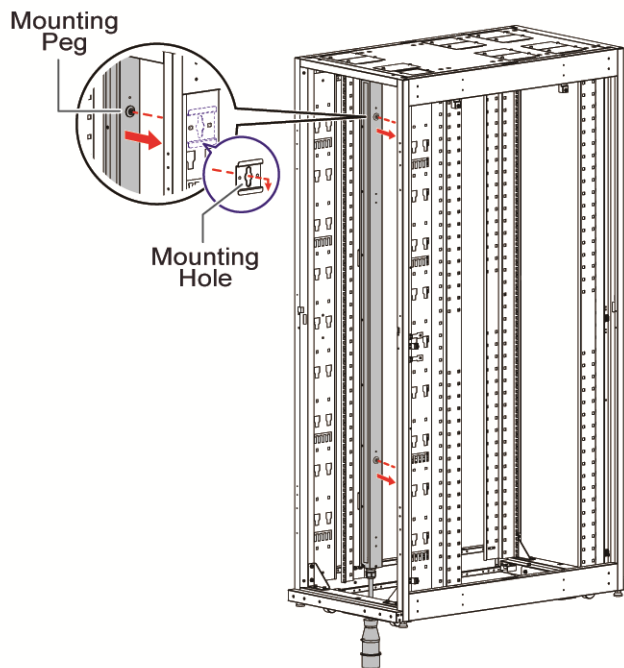
When the power cord goes down, the toolless mounting peg should be adjusted to relative position (from **1** to **2**) following the mounting bracket. We recommend the use of #2 Phillip screwdriver. See **Figure 3-4**.



(Figure 3-4: Adjust the Toolless Mounting Peg to Relative Position)

Step 5

Hold the rPDU vertically and align its toolless mounting pegs with the mounting holes. See **Figure 3-5**.



(Figure 3-5: Align the Toolless Mounting Pegs with the Mounting Holes)

3.2 Mounting on Delta Standard Rack (Side-hung)

Side-hung is also feasible on the Delta Standard Rack. All you need is to choose different mounting brackets.

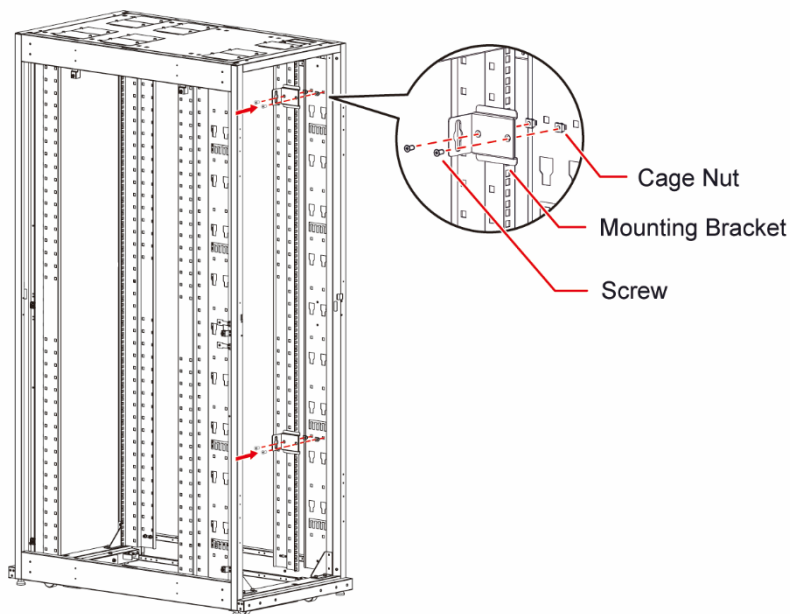


NOTE:

If you would like to perform side-hung, please contact Delta customer service for more information.

Step 1

Put cage nuts into the EIA holes between 11U & 12U and 39U & 40U on the Delta Standard Rack. And fasten the mounting brackets to cage nuts with screws. We recommend you use #2 Phillip screwdriver to fasten the screws. See *Figure3-6*.



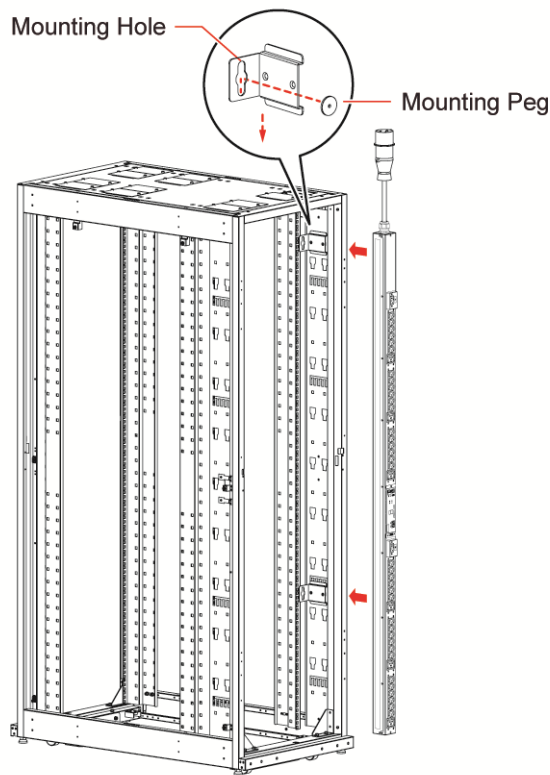
(Figure 3-6: Install the Cage Nuts and Mounting Brackets)

Step 2

Please refer to *Figure 3-2* for the positions of the toolless mounting pegs when the power cord goes up and refer to *Figure 3-4* when the power cord goes down.

Step 3

Hold the rPDU vertically and align its toolless mounting pegs with the mounting holes. See *Figure 3-7*.



(Figure 3-7: Align the Toolless Mounting Pegs with the Mounting Holes)

3.3 Mounting on Other Racks

If you choose not to use the Delta Standard Rack, please contact Delta engineers or Delta customer service for further information to find suitable mounting solution for your rack.

Chapter 4 : rPDU Connection

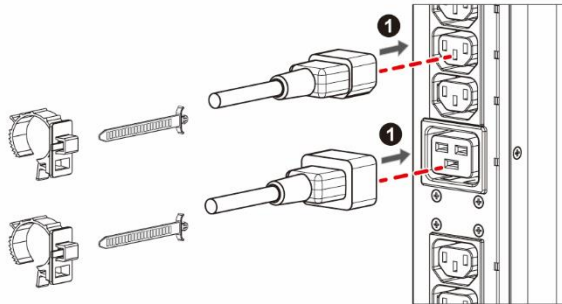
4.1 Plug in the rPDU

Plug the rPDU input power cord into a grounded outlet. Make sure the grounded outlet does not share a circuit with a heavy electrical load such as an air conditioner or a refrigerator.

4.2 Output Sockets

Step 1

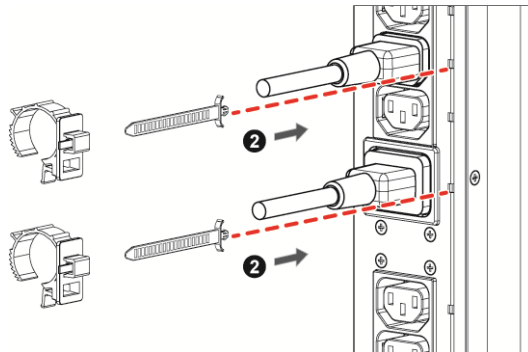
Plug the power cords into rPDU's sockets (❶). Please refer to *Figure 4-1*.



(Figure 4-1: Plug the Power Cords into rPDU's Output Sockets)

Step 2

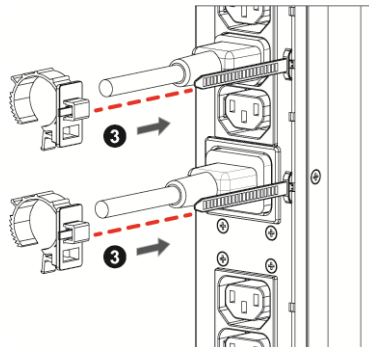
Insert the cable ties into the slots (❷). Please refer to *Figure 4-2*.



(Figure 4-2: Insert the Cable Ties into the Slots)

Step 3

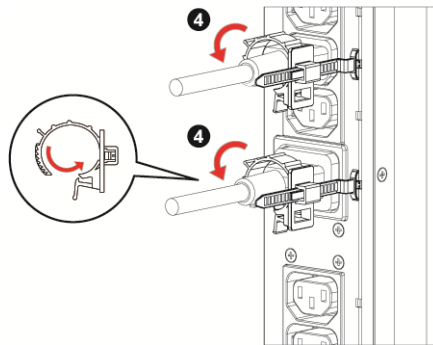
Insert the cable ties into the fixing holders (❸) and push the fixing holders toward the output sockets as close as possible. Please refer to *Figure 4-3*.



(Figure 4-3: Insert the Cable Ties into the Fixing Holders)

Step 4

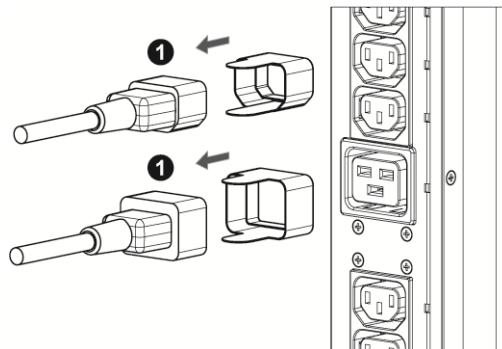
Tighten the fixing holder by pushing the end into the groove (④). Please refer to *Figure 4-4*.



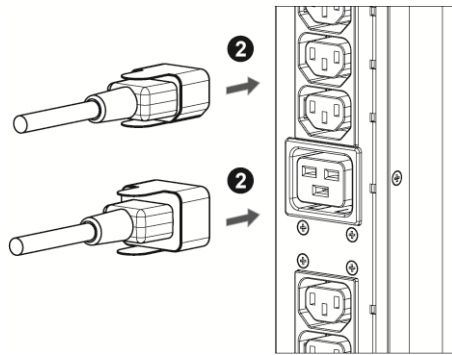
(Figure 4-4: Tighten the Fixing Holder)

4.3 Retention Sleeves (Optional)

An alternate solution for connecting the plugs strongly is retention sleeves. First, attach them to the plugs as *Figure 4-5* and then plug them into the output sockets as *Figure 4-6*.



(Figure 4-5: Attach the Retention Sleeves to the Plugs)



(Figure 4-6: Insert the Plugs into the Output Sockets)



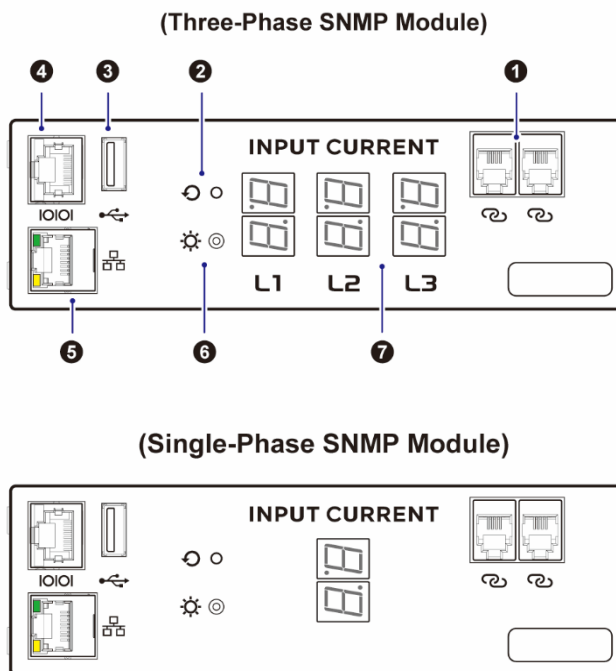
NOTE:

If you would like to use the retention sleeves, please contact Delta customer service for more information.

Chapter 5 : Communication Interfaces

5.1 Remote Monitoring Controller

The rPDU features a remote monitoring controller (RMC), which has a built-in SNMP IPv6 communication device, a RJ45 port for the RS232 console and the RS485 EMP communication. Additionally, the RMC has a USB port for downloading event log and data log, two daisy chain ports for daisy chain configuration, an alarm indicator that indicates the condition of the rPDU. Moreover, there are two-digit LED displays that show the current of each line, and a reset button.



No.	Icon	Description
①	 Daisy Chain Port	For daisy-chain connection. Refer to <i>Chapter 5: Communication Interfaces</i> for details.
②	 Reset Button	Reset of RMC, password and DHCP.
③	 USB Port	For download of event log and data log to a USB flash drive.
④	 Serial Port	For console and environmental probe connection. Refer to <i>Chapter 5: Communication Interfaces</i> for details.
⑤	 Network Port	It connects to the Ethernet network. This port allows users to access the web user interface and provides network communication service. Refer to <i>Chapter 5: Communication Interfaces</i> for details.
⑥	 System Status Indicator	Green light: The system is normal. Red light: An alarm has occurred.
⑦	L1/ L2/ L3 Auto-flip Display	It shows the current value of individual lines.

5.1.1 RMC General Specification

Items	Specification
Networking	10/100/1000 Mbps Ethernet
	IPv4, IPv6
	SNMP V1/V2c/V3
	HTTP, HTTPs, SSH, SSL
Console	Local monitoring via RS232 console
	Baud rate: 115200 bps

Items	Specification	
Measurement Accuracy	Voltage	$\pm 1\%$
	Current	$\pm 1\%$
	Power	$\pm 2\%$ (2 ~ 45A) $\pm 4\%$ (< 2A)
LED Indicator	Red	Alarm issued
	Green	RMC is in operation mode
Maintenance	Tool-less and hot swappable design.	

5.1.2 Reset the RMC

Press the reset button for 1 second to reset the RMC. This will not affect the operation of the rPDU.

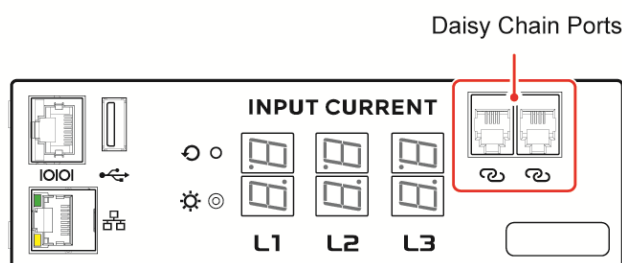


NOTE:

When the RMC requires repairs and needs to be replaced, please download the configuration file on the original RMC and transfer it to the new RMC for your use.

5.2 Daisy Chain Ports

The two ports shown below are for daisy chain application. The daisy chain function allows up to 40 rPDUs connected together to be monitored and controlled under one IP address, which reduces IP addresses. To connect one rPDU with another, a RJ11-RJ11 cable and two terminal resistors are required. If you need this service, please contact Delta customer service.



5.3 LED Indicator and Display

LED	Color	Definition	
System Status Indicator	Green/ Red (Bi-color LED)	Green	Normal
		Red	Alarm
7-segment Display	Green	2-Digit line current for L1/ L2/ L3	

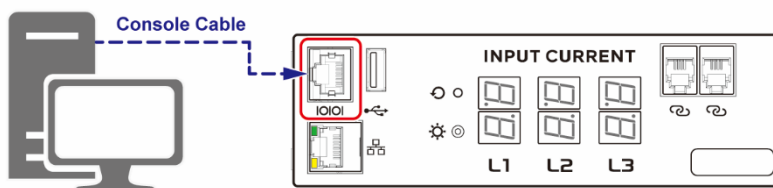
- **Invert the Numerical Display**

If you are mounting the rPDU in the rack with upside-down, the 7-segment display will rotate 180 degrees automatically.

5.4 Serial Port

The serial port serves as the RS232 port and RS485 port at the same time. It allows users to connect the serial port to a console or an environmental probe.

- **Connection to a Console**

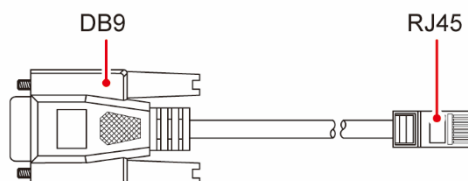


PC Tera Term Setting

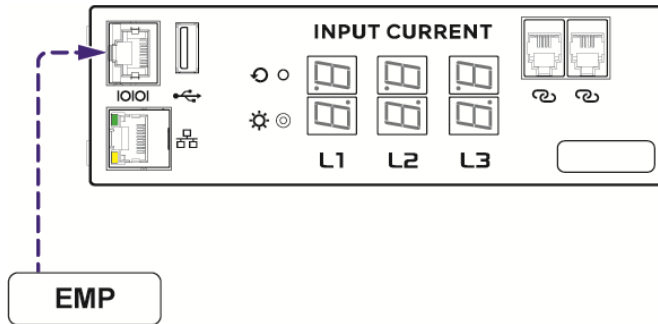
COM Port Number: Please check in your "Device Administrator".
Baud Rate: 115200 bps

For local management, users can use the console mode to control and monitor the rPDU via the RS232 port.

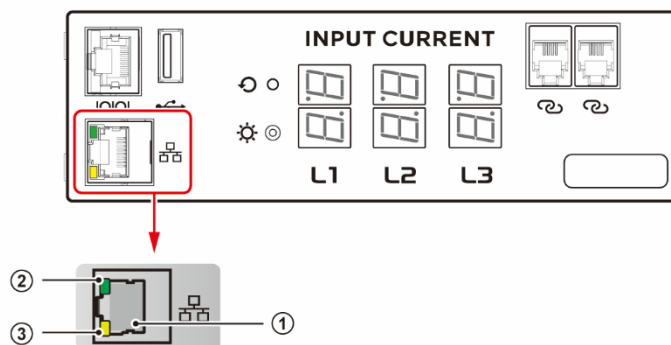
To link user's PC or notebook to the rPDU, the below accessory, a console cable shown in the figure below, is required for the communication.



- Connection to an Optional Environment Monitoring Probe (EMP) Module



5.5 Network Port



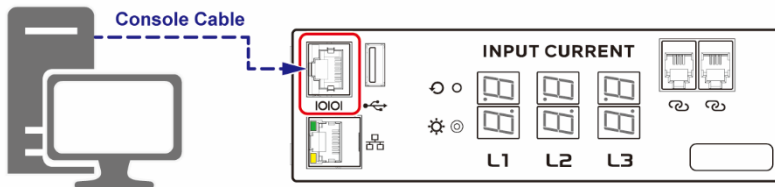
This Network port supports various protocols, e.g. HTTP(s), SSH, SSL, SNMP, IPv4 and IPv6.

No.	Item	Function
①	Network Port (RJ45)	It connects to the Ethernet network.
②	Link LED (Green)	It presents the network connection status. 1. ON: Network connection is established. 2. OFF: Network connection is not established.
③	Activity LED (Yellow)	It presents the network activity status. 1. OFF: No network activity. 2. Flashing: Active network (RX, TX) status.

Chapter 6 : Web User Interface

To remotely monitor and control the rPDU, web user interface and SNMP are available.

6.1 Check IP Address from the Console



PC Tera Term Setting

COM Port Number: Please check in your "Device Administrator".

Baud Rate: 115200 bps

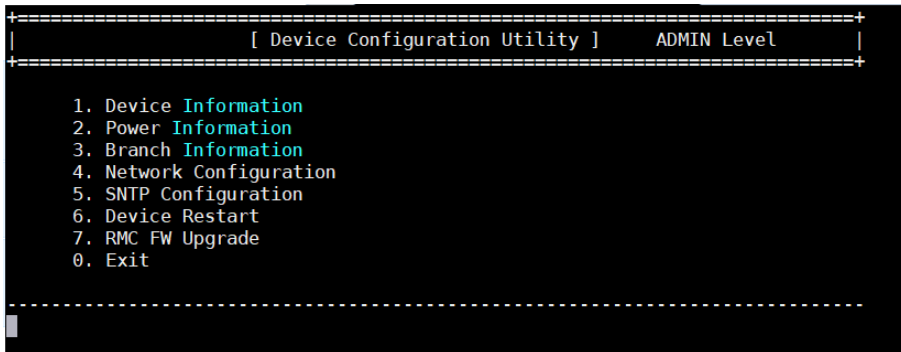
Please follow the steps in *Chapter 5.4 Serial Port* for console connection.

Step 1

Key in the information below:

Login account: **Admin**

Password: **00000000** (Default)



NOTE:

1. The default password of Admin/ User shall be changed and managed.
2. Pursuant to the California Security Law, it is mandatory that users change the password when first logging in. For the first login, users will not be able to log in with a User level account; therefore, users shall log in as Admin and change the password.

Step 2

To check the network setting, enter "1" and you will see the IP address information as below.

```
[ Device Information ]

Software Version: S1.00B18
Hardware Version: S0
Model Number: CUD-09B A
Factory Date: 2021/3/17
MAC Address: 00:18:23:0C:FB:46
System Name: DELTA iPDU (PDU A317DSA23500)
System Description: 3-P Wye IP & Branch Metered PDU C13(36)+C19(6)+CB(6)
System Datetime: 2021-05-14 16:36:06

[IPv4]
Address Auto Configure: DHCP
IP Address: 192.168.0.1
Netmask: 255.255.255.0
Gateway Address: 192.168.0.254
DNS Address:

[IPv6]
Address Auto Configure: None
Link Local Address: fe80::218:23ff:fe0c:fb46
Global Address:
Prefix: 0
Gateway Address:
DNS Address:

Hit Enter key to leave...
```



NOTE:

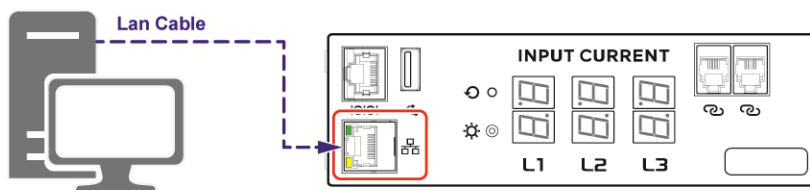
To change the network setting, please enter "4".

6.2 Login to the Web Page



NOTE:

Please use a LAN cable to connect the rPDU with your PC.



PC Lan Port Setting

Address : 192.168.0.100
Netmask : 255.255.255.0

PDU Default Network Setting

TCP/ IP Mode : Static IP
Address : 192.168.0.1
Gateway : 192.168.0.254
Netmask : 255.255.255.0

Step 1

Open the Web browser and enter the IP address **Https://192.168.0.1**, and you will see the login screen as below.



NOTE:

If you log in for the first time and cannot acquire connection, please ensure that the link (**Https://**) and rPDU's domain are correct. For web browsers, please use Microsoft Edge, Chrome or Firefox 3.0.1.

Step 2

Key in the information below:

User Name: **Admin**

Password: **00000000** (Default)



NOTE:

1. Follow the capitalization rule for the user's name.
2. The default password of Admin/ User shall be changed and managed.
3. Pursuant to the California Security Law, it is mandatory that users change their passwords when they first log in. For the first login, users will not be able to log in with a User level account; therefore, users shall log in as Admin and change their passwords.

6.3 Web Page

- Power Management



The **Overview** page under **Power Management** shows the rPDU current status, AC input, total power and environment conditions as in the above figure.

No.	Item	Description
①	Control Menu	The main control bar of the website.
②	System Status	The system status: System OK Minor Alarm Major Alarm
③	rPDU Name	The model name of the rPDU in use. Users can jump to the setting page by clicking the icon.
④	Date & Time	The current date and time on the Remote Monitoring Controller of the rPDU. Users can jump to the setting page by clicking the icon.
⑤	RMC Version	The current firmware version of the Remote Monitoring Controller. Users can jump to setting page by clicking the icon.
⑥	Logout	Click the icon to logout of the website.
⑦	Power Information	The power rating of the rPDU. The icon turns red when an overload alarm occurs.
⑧	AC Input Information	The three-phase/ single-phase voltage and current. The icon turns red when an alarm happens.
⑨	EMP Information	The individual temperature and humidity records. The icon turns red when an alarm happens.
⑩	USB Indicator	The indicator will show when rPDU detects an USB drive is inserted. For security reasons, users need to manually select 'Mount' before using the USB function. (i.e. download and access the USB drive.) Supported USB format: FTA32, NTFS and exFAT.

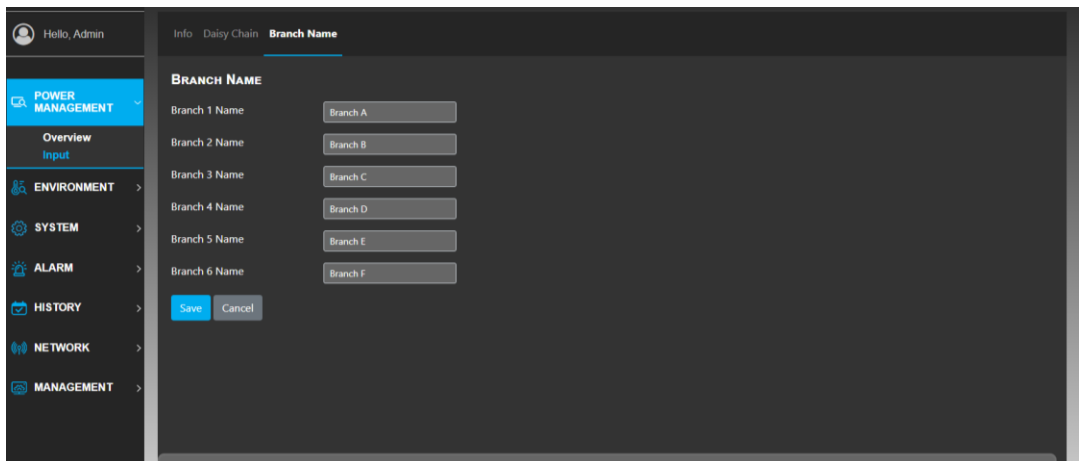
The screenshot shows the 'Input' page under 'Power Management'. The left sidebar contains navigation links: POWER MANAGEMENT, Overview, Input, ENVIRONMENT, SYSTEM, ALARM, HISTORY, NETWORK, and MANAGEMENT. The main content area has a top bar with 'Info', 'Daisy Chain', and 'Branch Name'. Below this, there are two tables: 'INPUT STATUS' and 'BRANCH STATUS'. The 'INPUT STATUS' table has columns: Line, Source, Line Voltage(V), Phase Voltage(V), Line Current(A), Power(W), Energy(Wh), Power Factor, Apparent Power(VA), Voltage THD(%), and Current THD(%). The 'BRANCH STATUS' table has columns: Branch, Name, Phase, Voltage(V), Current(A), Power(W), Energy(Wh), Power Factor, Apparent Power(VA), Voltage THD(%), and Current THD(%). Red boxes highlight the 'INPUT STATUS' and 'BRANCH STATUS' tables. Yellow boxes highlight the reset icons (a blue 'c' in a circle) for the total energy and branch energy. Numbered callouts 1-4 point to the 'INPUT STATUS' table, the 'BRANCH STATUS' table, the total energy reset icon, and the branch energy reset icon respectively.

Line	Source	Line Voltage(V)	Phase Voltage(V)	Line Current(A)	Power(W)	Energy(Wh)	Power Factor	Apparent Power(VA)	Voltage THD(%)	Current THD(%)
L1	Source 1	358.5	206.9	0.00	0	0	0.00	0	0	0
L2	Source 1	357.1	206.8	0.00	0	0	0.00	0	0	0
L3	Source 1	356.9	205.2	0.00	0	0	0.00	0	0	0
Total					0	0				

Branch	Name	Phase	Voltage(V)	Current(A)	Power(W)	Energy(Wh)	Power Factor	Apparent Power(VA)	Voltage THD(%)	Current THD(%)
A	Branch A	L1-N	206.9	0.00	0	0	0	0	0	0
B	Branch B	L2-N	206.8	0.00	0	0	0	0	0	0
C	Branch C	L3-N	205.2	0.00	0	0	0	0	0	0
D	Branch D	L1-N	201.6	0.00	0	0	0	0	0	0

On the **Input** page under **Power Management**, click **Info** to see the detailed AC input and branch status. The total energy records are also shown.

No.	Item	Description
1	AC Input Information	Display of the voltage, current, power energy, PF, apparent power, vTHD and iTHD information.
2	Branch Information	Display of the phase, voltage, current, power energy, PF, apparent power, vTHD and iTHD information of individual branches.
3	Reset Total Energy	Click the icon to reset the total energy record.  NOTE: The procedure is irreversible.
4	Reset Branch Energy	Click the icon to reset the energy record of each branch.  NOTE: The procedure is irreversible.



On the **Input** page under **Power Management**, click **Branch Name** to change the branch name. It will be easier for users to distinguish individual branches.

Hello , Admin

POWER MANAGEMENT

Overview

Input

ENVIRONMENT

SYSTEM

ALARM

HISTORY

NETWORK

MANAGEMENT

Info

Daisy Chain

Branch Name

Daisy Chain Branch Name

INPUT STATUS --- SUMMARY

System ID	Line	Source	Line Voltage(V)	Phase Voltage(V)	Line Current(A)	Power(W)	Energy(Wh)	Frequency(Hz)	Power Factor	Apparent Power(VA)	Voltage THD(%)	Current THD(%)		
1	L1	Source 1	370.3	214.6	0.00	0	0	60.0	---	0	0.0	0.0		
1	L2	Source 1	370.3	214.5	0.00	0	0	60.0	---	0	0.0	0.0		
1	L3	Source 1	370.3	214.5	0.00	0	7	60.0	---	0	0.0	0.0		
Total						0	7							
2	L1	Source 1	381.9	221.6	0.00	0	0	60.0	---	0	1.3	0.0		
2	L2	Source 1	382.0	221.7	0.00	0	0	60.0	---	0	0.0	0.0		
2	L3	Source 1	382.0	221.7	0.00	0	14	60.0	---	0	0.0	0.0		
Total						0	14							
3	L1	Source 1	0.0	0.0	0.00	0	0	---	0.00	0	0.0	0.0		
3	L2	Source 1	0.0	0.0	0.00	0	0	---	0.00	0	0.0	0.0		
3	L3	Source 1	0.0	0.0	0.00	0	0	---	0.00	0	0.0	0.0		
Total						0	0							

Hello , Admin

Info **Daisy Chain** Branch Name Daisy Chain Branch Name

BRANCH STATUS --- SUMMARY

System ID	Branch	Name	Phase	Voltage(V)	Current(A)	Power(W)	Energy(Wh)	Power Factor	Apparent Power(VA)	Voltage THD(%)	Current THD(%)	
1	A	Branch A	L1-N	214.1	0.00	0	0	---	0	0.0	0.0	C
1	B	Branch B	L2-N	214.4	0.00	0	0	---	0	0.0	0.0	C
1	C	Branch C	L3-N	214.4	0.00	0	0	---	0	0.0	0.0	C
1	D	Branch D	L1-N	214.7	0.00	0	0	---	0	0.0	0.0	C
1	E	Branch E	L2-N	214.7	0.00	0	0	---	0	0.0	0.0	C
1	F	Branch F	L3-N	214.8	0.00	0	7	---	0	0.0	0.0	C
2	A	Branch A	L1-N	220.8	0.00	0	0	---	0	0.0	0.0	C
2	B	Branch B	L2-N	220.8	0.00	0	0	---	0	1.6	0.0	C
2	C	Branch C	L3-N	221.1	0.00	0	0	---	0	0.0	0.0	C
2	D	Branch D	L1-N	220.8	0.00	0	0	---	0	0.0	0.0	C
2	E	Branch E	L2-N	220.9	0.00	0	0	---	0	1.7	0.0	C
2	F	Branch F	L3-N	221.0	0.00	0	14	---	0	0.0	0.0	C
3	A	Branch A	L1-N	0.0	0.00	0	0	0.00	0	0.0	0.0	C
3	B	Branch B	L2-N	0.0	0.00	0	0	0.00	0	0.0	0.0	C
3	C	Branch C	L3-N	0.0	0.00	0	0	0.00	0	0.0	0.0	C
3	D	Branch D	L1-N	0.0	0.00	0	0	0.00	0	0.0	0.0	C

On the **Input** page under **Power Management**, click **Daisy Chain** to see all rPDUs' detailed AC input and branch status.

Hello , Admin

Info Daisy Chain Branch Name **Daisy Chain Branch Name**

BRANCH NAME 1 ▾

Branch 1 Name

Branch 2 Name

Branch 3 Name

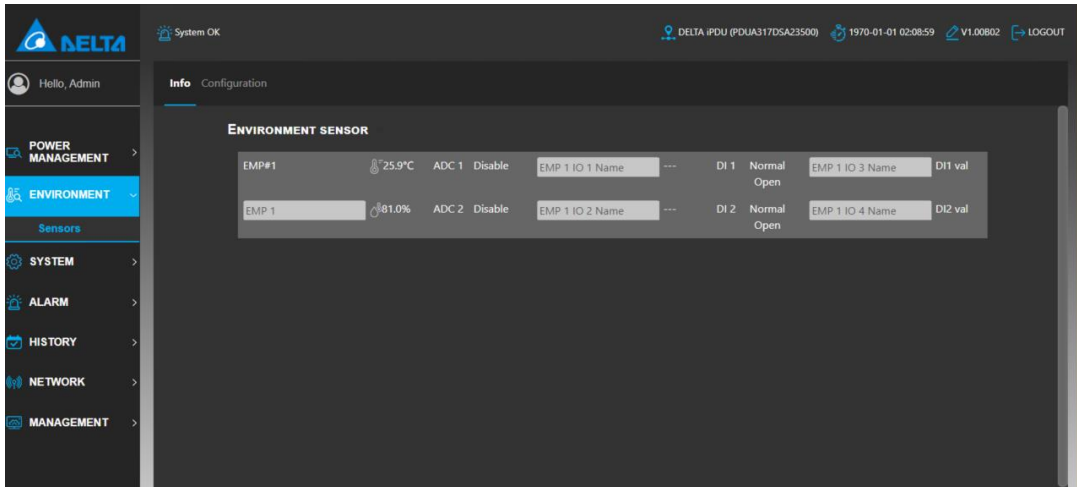
Branch 4 Name

Branch 5 Name

Branch 6 Name

On the **Input** page under **Power Management**, click **Daisy Chain Branch Name** to see every rPDU's branch name. Click the **1 ▾** button to select an rPDU and set its branch name.

- Environment

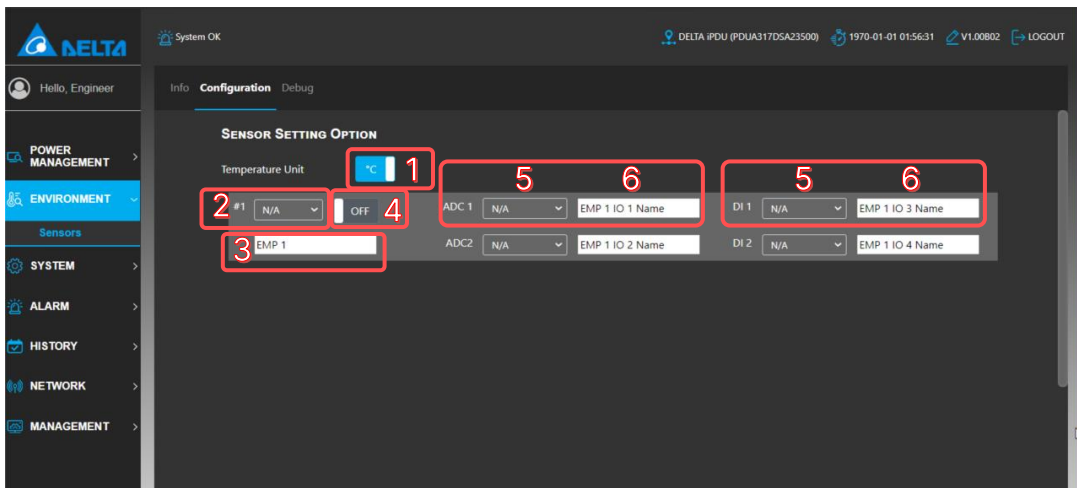


On the **Sensor** page under **Environment**, click **Info** to see the detailed temperature and humidity information in the surroundings. The maximum amount of sensor connected to the rPDU is one.



NOTE:

This function is only enabled when users connect the rPDU with the optional EMP. If you need more EMP information or EMP setup service, please contact your local dealer or Delta customer service.

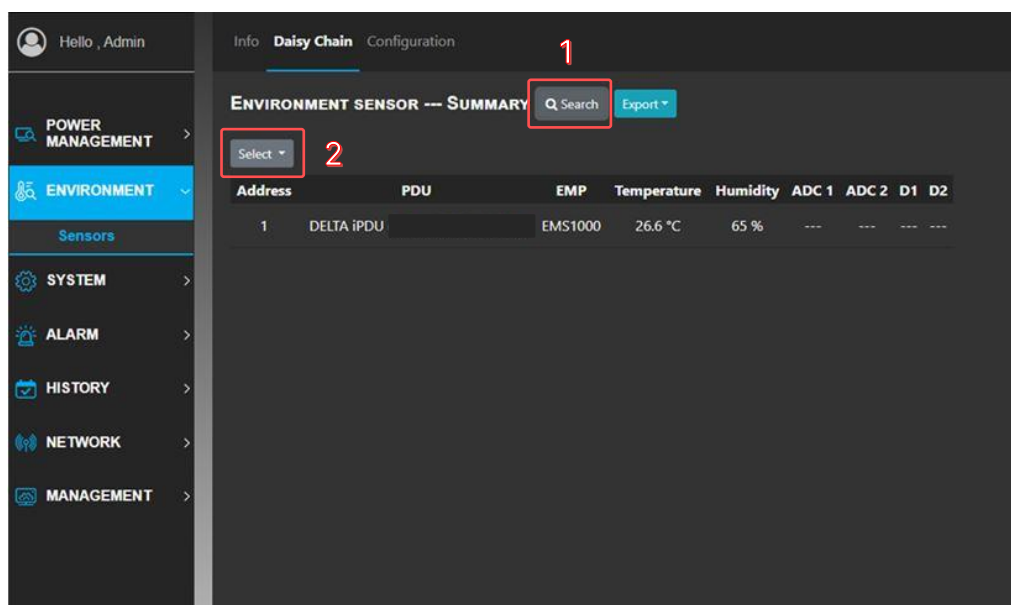


On the **Sensor** page under **Environment**, click **Configuration** to change the temperature unit and the sensor name. Moreover, users can disable the unused sensor on this page.

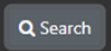
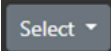
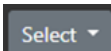
**NOTE:**

This function is only enabled when users connect the rPDU with the optional EMP. If you need more EMP information or EMP setup service, please contact your local dealer or Delta customer service.

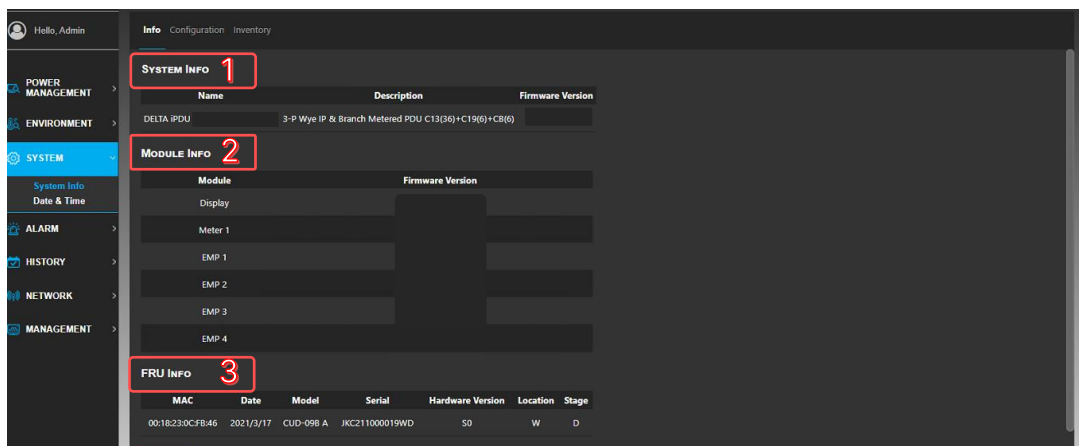
No.	Item	Description
①	Temperature Unit Switch	The temperature unit can be changed to Celsius or Fahrenheit using this switch.
②	Sensor Type	Users can change the sensor type (EMP, EMS1000) by selecting the item when unfolding the list.
③	Sensor Name	Users can change the sensor name in the space.
④	Sensor ON/OFF Switch	Users can enable/ disable the sensor connected to the rPDU by using this switch.
⑤	Analog Input/Digital Input	Various kinds of additional sensors can be connected to the EMP through these input ports.
⑥	Analog Input/Digital Input Name	Users can change the AI/ DI name in the space.



On the **Sensors** page under **Environment**, click **Daisy Chain** to see every rPDU's temperature and humidity information.

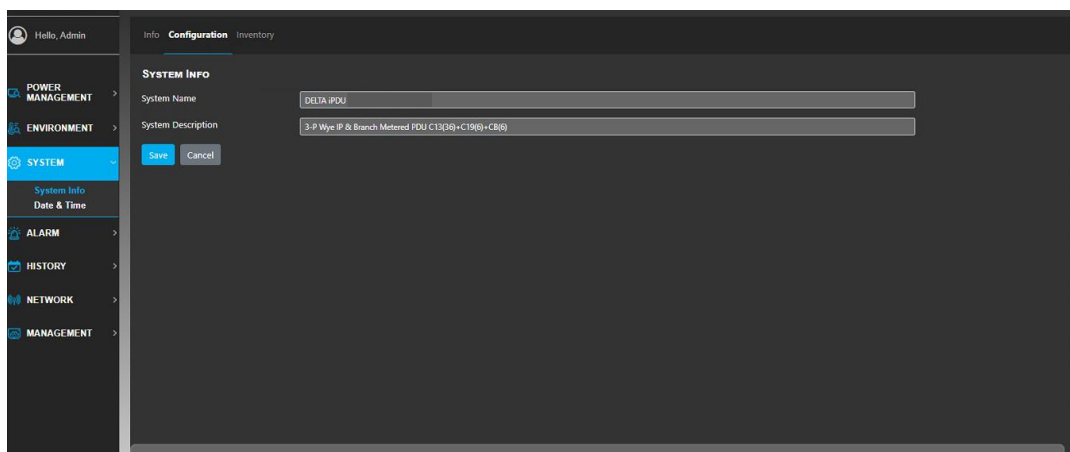
No.	Item	Description
①	Search Button	Click the  button to display the  item.
②	Select Button	Click the  button to choose a specific rPDU or all rPDUs.

- **System**

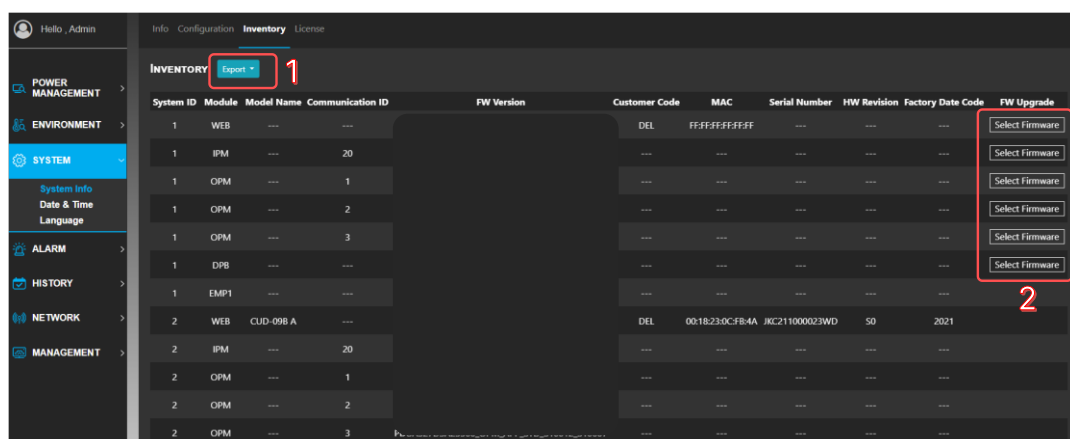


On the **System Info** page under **System**, click **Info** to see the rPDU related information (the firmware version, FRU information and serial number, etc.).

No.	Item	Description
①	System Info	The name, description and firmware version of the rPDU are shown in System Info.
②	Module Info	The firmware versions of the modules and accessories that are connected to the rPDU are specified in Module Info.
③	FRU Info	The information of the manufacture for the rPDU is specified in FRU Info.



On the **System Info** page under **System**, click **Configuration** to see the name and description of the rPDU. Users can edit the information on this page.



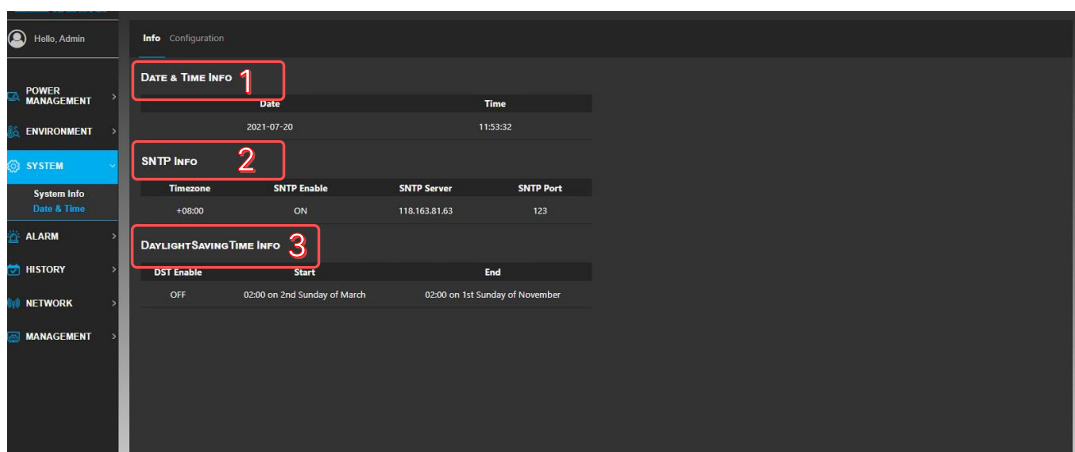
On the **System Info** page under **System**, click **Inventory** to see the inventory log. The inventory log shows detailed information of the modules that are connected to the rPDU. The information includes the firmware version and the information of the manufacturer. Firmware upgrade for each module can be performed by clicking the **Select Firmware** button.

No.	Item	Description
①	Export Button	Users can export the information of the modules that are connected to the rPDU by clicking this button. The file will be exported as an excel file.
②	Firmware Upgrade Button	Users can upgrade the firmware for each module by clicking this button. During the upgrade, the button will turn into a progress bar.



NOTE:

On this page, you can see all information of the modules that are connected to the chained rPDUs. If you need to update the firmware of the chained rPDUs, please refer to **Chapter 7.3 Firmware Upgrade for Chained rPDUs**.



On the **Date & Time** page under **System**, click **Info** to see the current date and time, the SNTP information and the DST information. Settings can be changed on the configuration page.

No.	Item	Description
①	Date & Time Info	Display of the current date and time on the rPDU.
②	SNTP Info	Display of the SNTP (Simple Network Time Protocol) information. The rPDU can synchronize the time with the SNTP server.
③	Daylight Saving Time Info	Display of the starting and ending time of DST.

On the **Date & Time** page under **System**, click **Configuration** to set the time for the rPDU. Users can enable the synchronization with the SNTP server and the DST function.

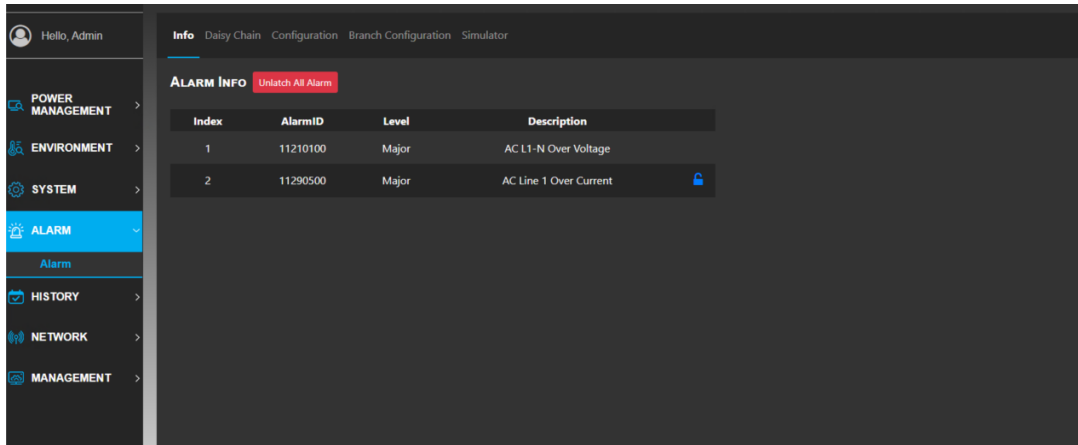
No.	Item	Description
①	Manual Time Source	Users can manually change the time for the rPDU or simply choose to synchronize the rPDU time with the time on the user PC.
②	SNTP Info	Users can enable/ disable the SNTP function, change the rPDU time zone as well as the SNTP server IP. Once the SNTP function is enabled, the rPDU will always synchronize its time with the SNTP server.
③	Daylight Saving Time	Users can enable/ disable the DST function and change the starting/ ending time of the DST.



NOTE:

When the IP address of this rPDU changes, the SNTP function will automatically enable. If this function is not needed, please go to **System**→**Date & Time**→**Configuration** and select **Disable** to avoid triggering the **SNTP Sync Fail** alarm.

- Alarm

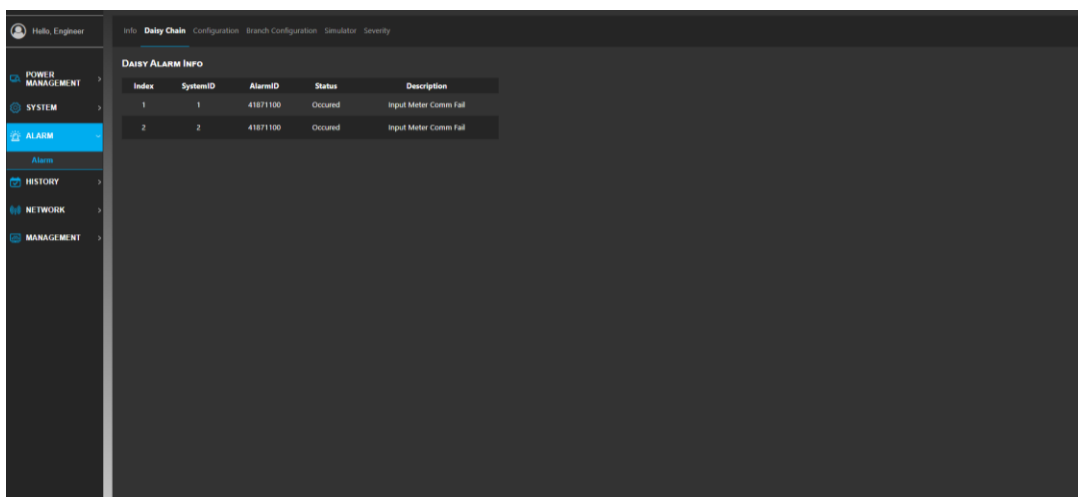


On the **Alarm** page under **Alarm**, click **Info** to see the current rPDU alarm. There are two types of alarm, ordinary alarm and latch type alarm. An ordinary alarm will disappear from the list when the alarm condition no longer exists. However, a latch type alarm will remain on the list even when the alarm condition no longer exists. Users can clear the latch type alarm by clicking  or **Unlatch All Alarm**.

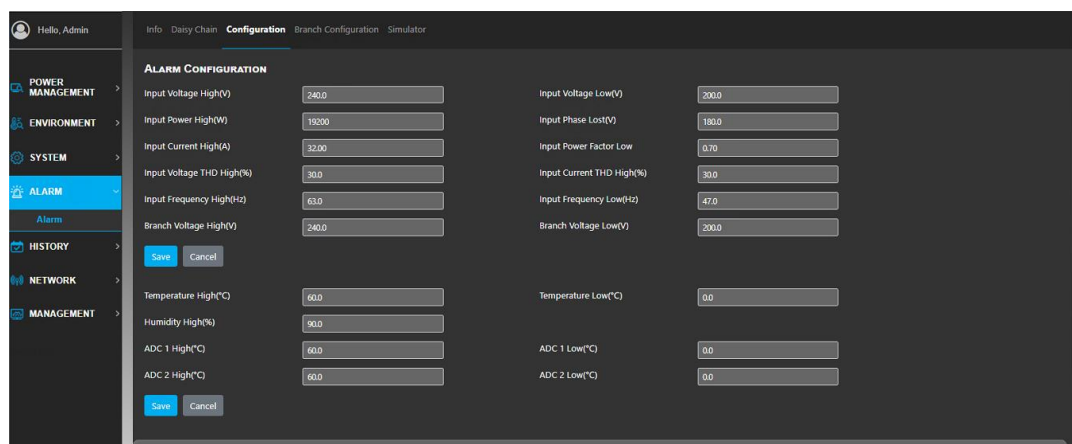


NOTE:

When any of the following alarms occurs and continues to exist, please contact Delta customer service: Input Meter Comm Fail, Input Meter IC Fail, Meter EEPROM Fail, Set Config Fail, Meter ID Collision, Daisy Chain ID Collision, Display Comm Fail, EMPx Comm Fail, EMPx Config Error.



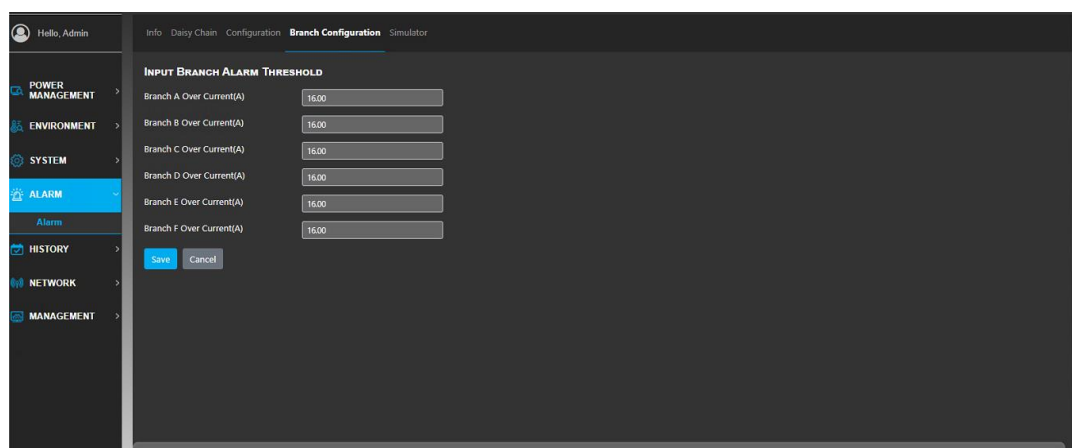
On the **Alarm** page under **Alarm**, click **Daisy Chain** to see the chained rPDU alarm. There are two types of alarm, ordinary alarm and latch type alarm. An ordinary alarm will disappear from the list when the alarm condition no longer exists. However, a latch type alarm will remain on the list even when the alarm condition no longer exists. Users can clear the latch type alarm by clicking  or **Unlatch All Alarm**.



ALARM CONFIGURATION

Input Voltage High(V)	240.0	Input Voltage Low(V)	200.0
Input Power High(W)	19200	Input Phase Lost(V)	180.0
Input Current High(A)	32.00	Input Power Factor Low	0.70
Input Voltage THD High(%)	30.0	Input Current THD High(%)	30.0
Input Frequency High(Hz)	60.0	Input Frequency Low(Hz)	47.0
Branch Voltage High(V)	240.0	Branch Voltage Low(V)	200.0
Save Cancel			
Temperature High(°C)	60.0	Temperature Low(°C)	0.0
Humidity High(%)	90.0		
ADC 1 High(°C)	60.0	ADC 1 Low(°C)	0.0
ADC 2 High(°C)	60.0	ADC 2 Low(°C)	0.0
Save Cancel			

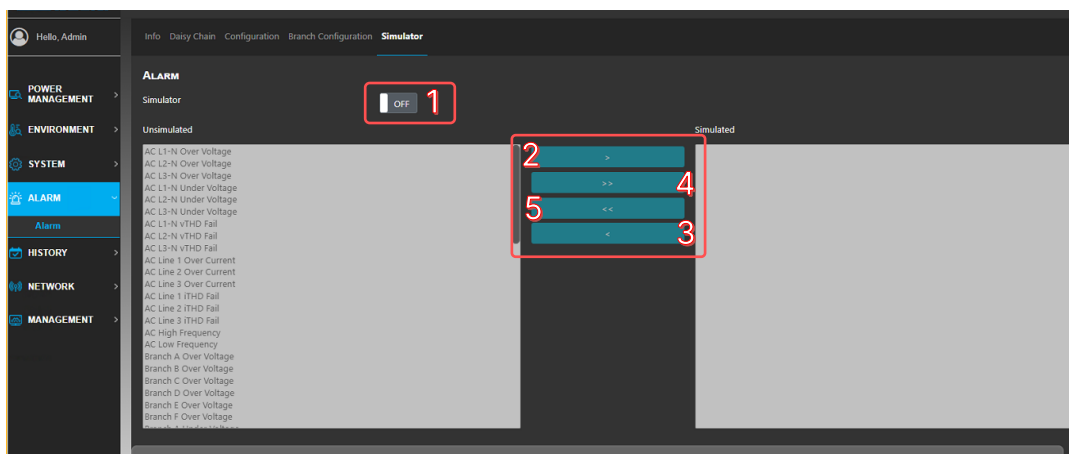
On the **Alarm** page under **Alarm**, click **Configuration** to change the threshold for triggering an alarm. The value entered must be within the range shown on the pop-up message (**Allow value in 80.0~240.0**), or the value entered will be ignored.



INPUT BRANCH ALARM THRESHOLD

Branch A Over Current(A)	16.00
Branch B Over Current(A)	16.00
Branch C Over Current(A)	16.00
Branch D Over Current(A)	16.00
Branch E Over Current(A)	16.00
Branch F Over Current(A)	16.00
Save Cancel	

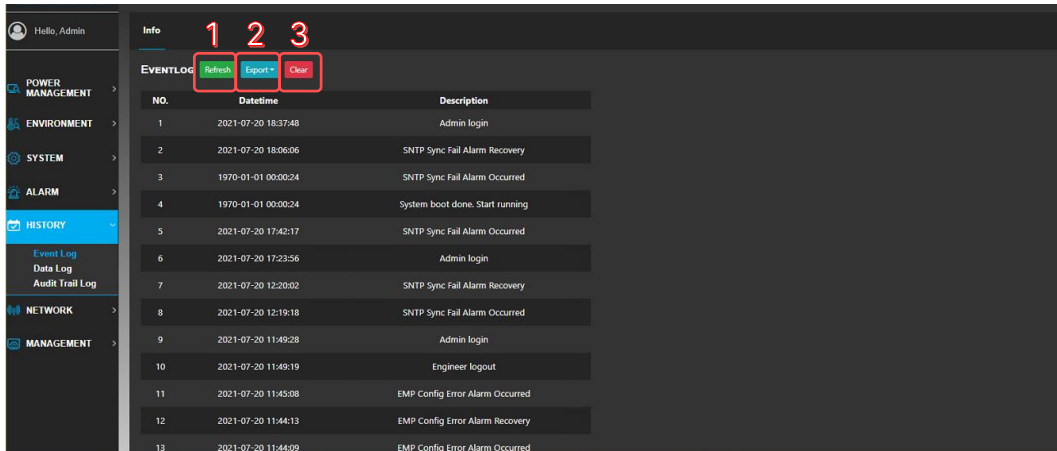
The rPDU has multiple output branches. On the **Alarm** page under **Alarm**, click **Branch Configuration** to set the current alarm threshold for individual branches. Users can set different current thresholds according to different load conditions.



The alarm simulator allows users to trigger alarms without letting actual abnormal conditions occur. Users can use the alarm simulator to choose alarm events and they will show on WEB, SNMP, Trap or SMTP interface. All alarms shown on the **Alarm Info** page and the EMP readings will vanish when the simulator is enabled. The alarms and the readings will show up again when the simulator is disabled.

No.	Item	Description
①	Alarm Simulator ON/ OFF Switch	The switch of alarm simulator. The switch must be turned on before using the function on this page.
②	Alarm Enable Button	Click the button after selecting alarms on the left to enable the selected alarms.
③	Alarm Disable Button	Click the button after selecting alarms on the right to disable the selected alarms.
④	All Alarms Enable Button	Click the button to enable all alarms on the left.
⑤	All Alarms Disable Button	Click the button to disable all alarms on the right.

- History



The **Event Log** page shows events that have happened (login & logout, alarm occurred & eliminated, simulator on & off, etc.). The maximum amount of events recorded is 10000, FIFO is applied after reaching this limit.

No.	Item	Description
①	Refresh Button	This button allows users to refresh the event log.
②	Export Button	This button allows users to export the current event log. Users can choose where to export the file to (PC or USB).
③	Clear Button	 NOTE: The procedure is irreversible.

NO.	Datetime	Input 1 ACV1(V)	Input 1 ACV2(V)	Input 1 ACV3(V)	Input 1 Frequency(Hz)	Input 1 AC1(A)	Input 1 AC2(A)	Input 1 AC3(A)	Input 1 TotalCurrent(A)	Branch1 Current(A)	Branch2 Current(A)
1	2021-07-20 18:43:21	213.6	214.0	213.0	60.0	0.00	0.00	0.00	---	0.00	0.00
2	2021-07-20 18:42:21	214.6	215.1	212.6	60.0	0.00	0.00	0.00	---	0.00	0.00
3	2021-07-20 18:41:22	214.4	214.8	212.5	60.0	0.00	0.00	0.00	---	0.00	0.00
4	2021-07-20 18:40:21	213.8	214.0	211.8	60.0	0.00	0.00	0.00	---	0.00	0.00
5	2021-07-20 18:39:21	214.2	214.8	212.4	60.0	0.00	0.00	0.00	---	0.00	0.00
6	2021-07-20 18:38:21	213.7	213.9	212.6	60.0	0.00	0.00	0.00	---	0.00	0.00
7	2021-07-20 18:37:21	214.7	215.0	212.6	60.0	0.00	0.00	0.00	---	0.00	0.00
8	2021-07-20 18:36:21	214.7	214.7	212.7	60.0	0.00	0.00	0.00	---	0.00	0.00
9	2021-07-20 18:35:21	213.8	213.7	211.7	60.0	0.00	0.00	0.00	---	0.00	0.00
10	2021-07-20 18:34:21	215.0	214.8	212.8	60.0	0.00	0.00	0.00	---	0.00	0.00

The **Data Log** page shows data readings (AC input voltage, current, frequency, etc.). The maximum number of events recorded is 10000. FIFO method will be applied after the limit is reached.

No.	Item	Description
①	Refresh Button	This button allows users to refresh the event log.
②	Export Button	This button allows users to export the current event log. Users can choose where to export the file to (PC or USB).
③	Clear Button	This button allows users to clear the current event log.  NOTE: The procedure is irreversible.
④	Page Selection	Users can proceed to the next page of log by clicking the button. Moreover, users can click on the page number and enter the page number to be displayed directly.

Info Daisy Chain Configuration

DATALOG 2+ Refresh Export Clear

No.	Date	1 ACV1(V)	Input 1 ACV2(V)	Input 1 ACV3(V)	Input 2 ACV1(V)	Input 2 ACV2(V)	Input 2 ACV3(V)	Input 1 Frequency(Hz)	Input 2 Frequency(Hz)	Input 1 AC1(A)	Input 1 AC2(A)	Input 1 AC3(A)	Input 2 AC1(A)	Input 2 AC2(A)	Input 2 AC3(A)
1	1970-01-01 01:51:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
2	1970-01-01 01:51:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
3	1970-01-01 01:51:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
4	1970-01-01 01:52:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
5	1970-01-01 01:51:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
6	1970-01-01 01:50:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
7	1970-01-01 01:49:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
8	1970-01-01 01:48:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
9	1970-01-01 01:47:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---
10	1970-01-01 01:46:17	0.0	0.0	0.0	---	---	---	0.0	---	0.00	0.00	0.00	---	---	---

<< 1 of 10 >>

The **Data Log** (Daisy Chain) page shows data readings (AC input voltage, current, frequency, etc.) of chained rPDUs.

No.	Item	Description
1	rPDU Selection	Users can select the rPDU data to be displayed.

Number of Chained rPDUs	Maximum Number of Data Log
1 ~ 16	10,000
17 ~ 32	5,000
33 ~ 40	3,000

Info Daisy Chain Configuration

Log Setting OPTION

Enable ☒ ON 1

Interval 1 Min 2

Save Cancel

The **Log Setting Option** page under **Data Log** allows users to change the record interval.

No.	Item	Description
①	Enable Button	This button allows users to enable the data log function.
②	Record Interval	Users can select the record interval of data log by changing this interval (default 1 minute per log).

The **Audit Trail Log** page shows the time a user logs in, who logs in and what the user does on the rPDU (user level, IP address, event etc.). The maximum number of events that can be recorded is 1000. The FIFO method will be applied after this limit is reached.

No.	Item	Description
①	Refresh Button	This button allows users to refresh the audit trial log.
②	Export Button	This button allows users to export the current audit trial log. Users can choose where to export the file to (PC or USB).
③	Clear Button	This button allows users to clear the current audit trial log.  NOTE: The procedure is irreversible.

- Network

The screenshot shows the 'Network' configuration page in a web interface. The left sidebar contains a menu with 'POWER MANAGEMENT', 'SYSTEM', 'ALARM', 'HISTORY', 'NETWORK' (highlighted), and 'MANAGEMENT'. The 'NETWORK' section is expanded, showing sub-items: 'TCP/IP', 'SNMP', 'HTTP', 'Remote Access', 'SMTP', 'LDAP', 'RADIUS', 'Daisy Chain', and 'SysLog'. The main content area is titled 'Info Configuration' and displays the current network settings for IPv4 and IPv6.

Mode	Address	Gateway	Netmask	DNS
dhcp	192.168.0.1	192.168.0.254	255.255.255.0	

Enable	Mode	Link Local	Address	Prefix	Gateway	DNS
ON	dhcpv6	fe80::218:23ff:fe33:c1b0		0		

On the **TCP/ IP** page under **Network**, click **Info** to see the current internet connection setting. Information regarding IPv4 and IPv6 is displayed.

This screenshot shows the same 'Network Configuration' page, but with red boxes highlighting the configuration sections for IPv4 and IPv6. A red '1' is placed next to the IPv4 section, and a red '2' is placed next to the IPv6 section.

IPv4 Configuration (1):

- Address Obtain: DHCP
- Address: 192.168.0.1
- Netmask: 255.255.255.0
- Gateway: 192.168.0.254
- DNS: (empty)
- Buttons: Save, Cancel

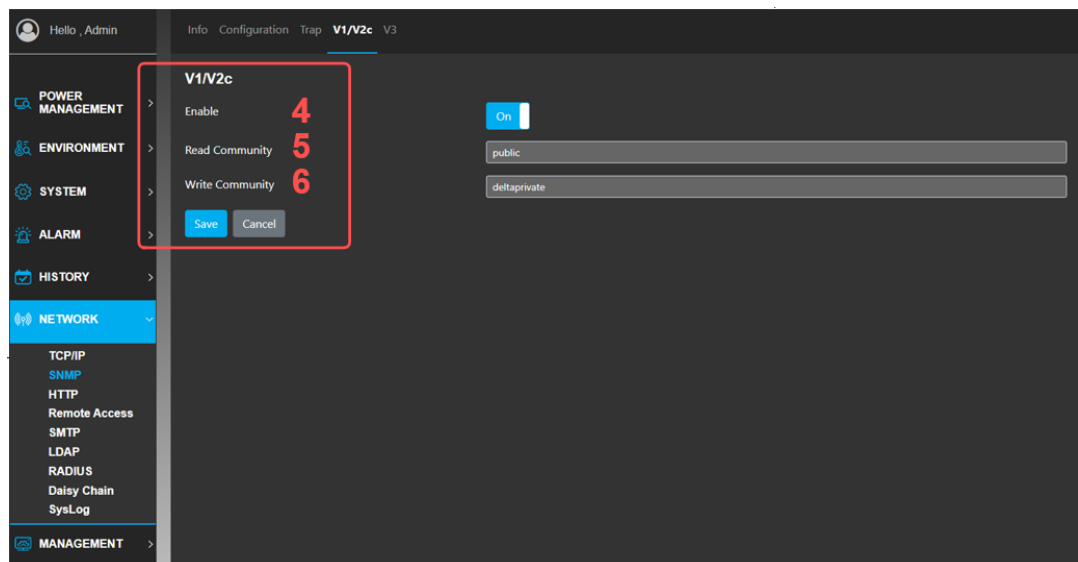
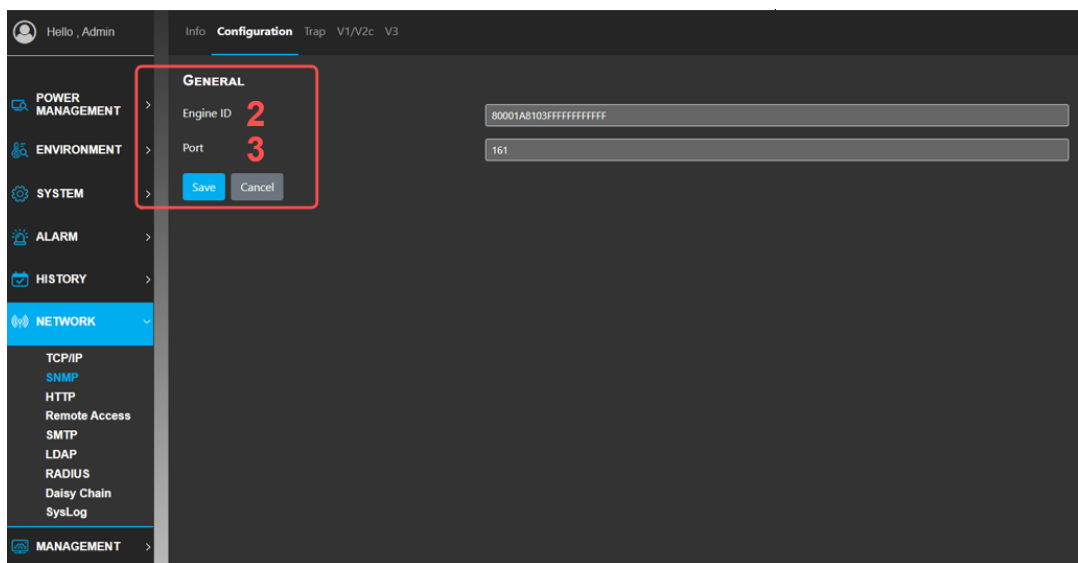
IPv6 Configuration (2):

- Enable: ON
- Address Obtain: DHCP
- Address: (empty)
- Prefix: 0
- Gateway: (empty)
- DNS: (empty)
- Buttons: Save, Cancel

The configuration of TCP/IP allows users to change the Internet setting (IP address, netmask, gateway etc.). The default IPv4 address for the rPDU is 192.168.0.1. The function of IPv6 can be enabled by turning on the IPv6 switch.

No.	Item	Description
①	IPv4 Address Obtain Button	Users can select to use DHCP or static mode to obtain the IPv4 IP address.
②	IPv6 Enable/Disable	This switch can enable or disable the function of IPv6.

The screenshot displays the configuration interface for the Delta Metered Type rPDU ViLink Series. The left sidebar contains a navigation menu with categories: POWER MANAGEMENT, ENVIRONMENT, SYSTEM, ALARM, HISTORY, NETWORK (selected), and MANAGEMENT. The NETWORK menu is expanded, showing options like TCP/IP, SNMP, HTTP, Remote Access, SMTP, LDAP, RADIUS, Daisy Chain, and SysLog. The main content area is titled 'Info Configuration Trap V1/V2c V3'. Under the 'GENERAL' section, there is a table with 'Engine ID' (80001A8103FFFFFFFF) and 'Port' (161). The 'MIB DOWNLOAD' section features a 'Download' button, which is highlighted with a red box and a large red number '1'. Below this, the 'TRAP' section shows a table with 'Read Community' (pdutrap) and 'Port' (162). The 'V1/V2c' section has a table with 'Enable' (ON), 'Read Community' (public), and 'Write Community' (deltaprivate). The 'V3' section shows a table with columns for 'Index', 'User', 'Auth Protocol', 'Priv Protocol', and 'Access'.



The **SNMP** page allows users to download the MIB file. Users then can load the MIB file using their SNMP software. Users who wish to access the rPDU by SNMP v1/v2c can use community strings on this page.

No.	Item	Description
①	MIB Download	Users can download the MIB file by clicking this button.
②	Engine ID	Users can specify their preferred engine ID according to their network environment. The default engine ID uses RFC3411 format 3.
③	SNMP Port	Users can change the SNMP port. Please make sure the configured port is available.
④	V1/ V2c Enable	Enable or disable the SNMP v1/ v2c function.
⑤	Read Community	Used by SNMP v1/ v2c. Users can specify the read community string.
⑥	Write Community	Used by SNMP v1/ v2c. Users can specify the write community string.



NOTE:

1. If SNMP cannot perform GET: Check the read (GET) community name (SNMPv1) and the user profile configuration (SNMPv3).
2. If SNMP cannot perform SET: Ensure that SNMP is enabled and SNMPv1 & SNMPv3 are enabled. Check the read/ write (SET) community name (SNMPv1) and the user profile configuration (SNMPv3).

The screenshot shows the configuration interface for the Delta Metered Type rPDU ViLink Series. The 'Trap' configuration page is displayed, showing fields for 'Read Community' (labeled 1) and 'Port' (labeled 2). The 'Read Community' field contains 'pdutrap' and the 'Port' field contains '162'. Below these fields are 'Save' and 'Cancel' buttons. The 'DESTINATION' section has a green button labeled 'Add a New Trap Address' (labeled 3). Below this is a table with columns 'Index', 'User', and 'Trap Address' (labeled 4). The table is currently empty.

The **SNMP Trap** page allows users to set a trap address that allows users to receive trap information when an alarm or event occurs. The following figure shows a trap receiver receiving alarm information via the MIB browser.

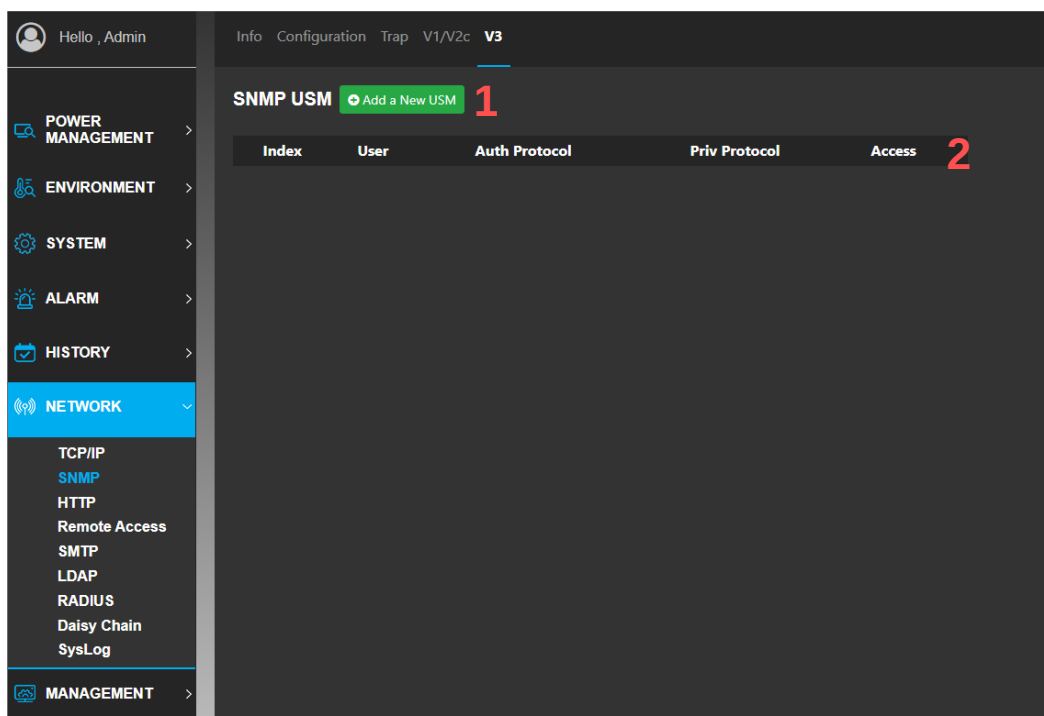
No.	Item	Description
①	Trap Community	Users can specify the trap community string via SNMP.
②	Trap Port	Users can change the trap port. Please make sure the port that needs to be configured is available.
③	Add a New Trap Address	Add a new address for the trap connection.
④	Delete Address	Delete an existing trap address.

Result Table	Trap Receiver ×	
Operations	Tools	
    		
Description	Source	Time
Input-1-Line-1-Over-Current-Happen	192.168.0.1	2021-05-21 10:08:13
Input-1-L1-N-Under-Voltage-Recovery	192.168.0.1	2021-05-21 10:08:11
Input-1-L1-N-Under-Voltage-Happen	192.168.0.1	2021-05-21 10:08:09
Input-1-L1-N-Over-Voltage-Recovery	192.168.0.1	2021-05-21 10:08:08
Input-1-L1-N-Over-Voltage-Happen	192.168.0.1	2021-05-21 10:08:06



NOTE:

The trap address can be in IPv4 or IPv6 format.



The **SNMP USM** page allows users to create/ delete SNMPv3 user accounts. The SNMP agent of the rPDU supports the user security level defined in RFC2574.

No.	Item	Description
①	Add New Users	Add a user for SNMPv3 connection.
②	Delete Address	Delete an existing SNMPv3 user.

No.	Item	Description
①	Name	Name of the user.
②	Authentication Protocol	Users can choose which authentication protocol to use. Users can choose MD5, SHA or None.
③	Authentication Password	Password used for authentication. The password can be empty if the authentication protocol is set to None.
④	Privacy Protocol	Users can choose which privacy protocol to use. Users can choose DES, AES or None.
⑤	Privacy Password	Password used for privacy setting. The password can be empty if the privacy protocol is set to None.
⑥	Access	Set the access privilege for users. The access privilege can be read only or read and write.

Hello , Admin

POWER MANAGEMENT >

ENVIRONMENT >

SYSTEM >

ALARM >

HISTORY >

NETWORK >

TCP/IP

SNMP

HTTP

Remote Access

SMTP

LDAP

RADIUS

Daisy Chain

SysLog

MANAGEMENT >

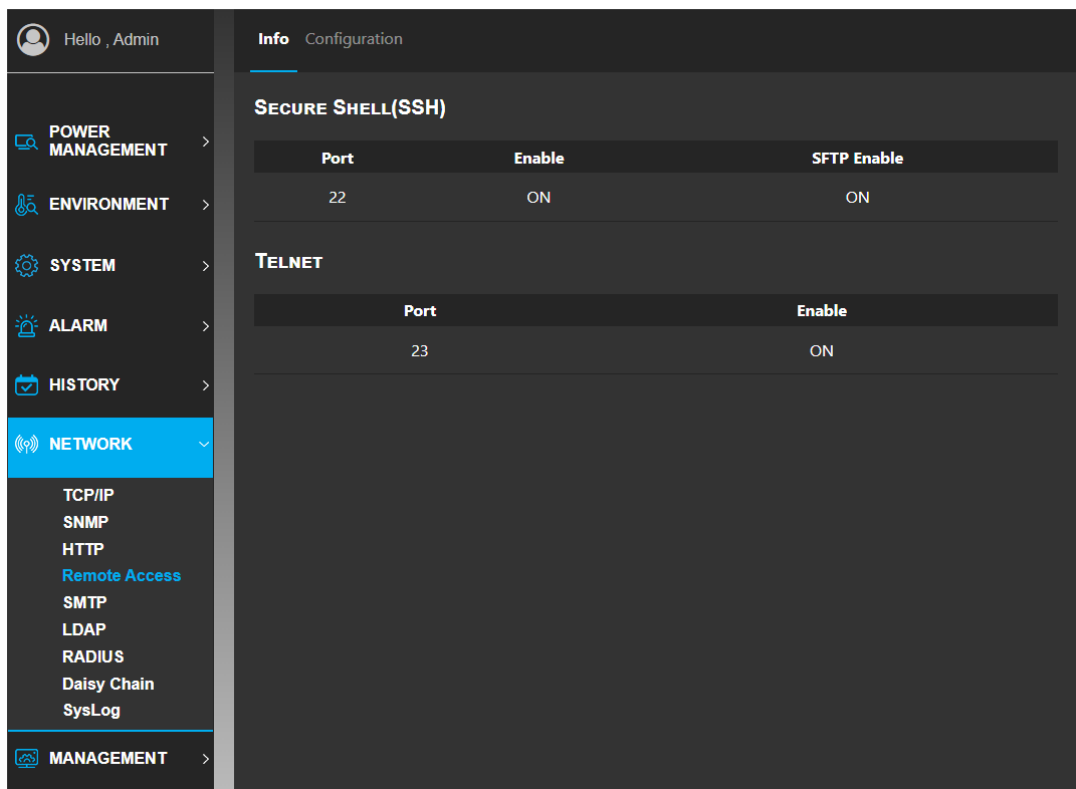
Info Configuration

HTTP

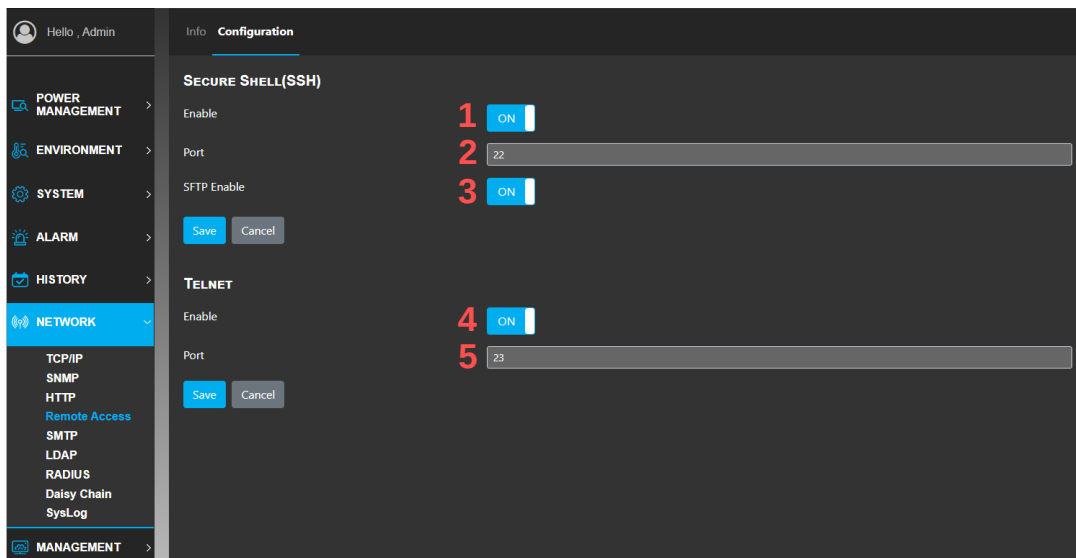
HTTP Enable	Port	HTTPS Port	Certificate
OFF	80	443	Default

This page allows users to change HTTP security related configurations, including disabling insecure connection, changing default connection ports and uploading users' desired security certificates.

No.	Item	Description
①	HTTP Enable	HTTP is an insecure way of connection. This option allows users to disable HTTP. If HTTP is disabled, user connection via HTTP port will be redirected to a secured connection – the HTTPS port.
②	HTTP Port	Users can change the HTTP connection port. Please make sure the configured port is available.
③	HTTPS Port	Users can change the HTTPS connection port. Please make sure the configured port is available.
④	Import Customized Certificate	Uploading of users' customized certificate will override rPDU's default certificate. The rPDU supports the X.509 PEM format and the certificate and private key shall be included. After a successful certificate upload, the rPDU will restart the HTTP service. The restart will cause a temporary disconnection.
⑤	Delete Customized Certificate	Deletion of users' customized certificate to use the rPDU's default certificate. If the rPDU is using the default certificate already, clicking this button will not lead to any action. After a successful certificate deletion, the rPDU will restart the HTTP service. The restart will cause a temporary disconnection.



The **Info** page of **Remote Access** under **Network** shows basic information of the secure shell and telnet.



The rPDU provides two routes for remote CLI access. The two routes are Secure Shell and Telnet. It is recommended to always use Secure Shell and turn off Telnet for security reason. The remote access configuration page allows users to turn on/ off remote access routes and change the corresponding communication port number.

No.	Item	Description
①	Secure Shell Enable	Turn on/ off the secure shell function.
②	Secure Shell Port	Set the secure shell communication port number. The number should not be the same with the telnet port number.
③	SFTP Enable	Turn on/ off the SFTP function.
④	Telnet Enable	Turn on/ off the telnet function
⑤	Telnet Port	Set the telnet communication port number. The number should not be the same with the secure shell port number.

Hello , Admin

POWER MANAGEMENT >

ENVIRONMENT >

SYSTEM >

ALARM >

HISTORY >

NETWORK >

TCP/IP

SNMP

HTTP

Remote Access

SMTP

LDAP

RADIUS

Daisy Chain

SysLog

MANAGEMENT >

Info Configuration

SMTP INFO

1 Enable

2 Address

3 Port

4 Use TLS

5 Login Auth

6 User Name

7 Password

OFF

192.168.0.1

25

OFF

OFF

MAIL INFO

8 Sender Address

9 Recipient Address

10 Subject

11 Content

SUBJECT

CONTENT

The SMTP function allows users to receive email notification when an alarm or event happens.



NOTE:

This function is only enabled when SMTP service is available to users.

No.	Item	Description
①	SMTP Service Status	Status information will be sent to users via mail.
②	SMTP Sever Address	Address of the SMTP mail server.
③	SMTP Sever Port	Port used by the mail server.
④	Use TLS	Display of the status of TLS for encrypting the SMTP connection.
⑤	SMTP Sever Authentication	When connecting to the SMTP mail server, the login authentication can be performed.
⑥	User Name for Authentication	When login authentication is enabled, user name needs to be filled in for the e-mail server.
⑦	Password for Authentication	When login authentication is enabled, password needs to be filled in for the e-mail server.
⑧	Sender Address	Display of the e-mail address of senders in the mail.
⑨	Recipient Address	The e-mail address to receive the notification.
⑩	Subject	Subject of the e-mail.
⑪	Content	Prefix text of the e-mail.

The screenshot shows the 'Configuration' page of the rPDU interface. The left sidebar contains a menu with categories: POWER MANAGEMENT, ENVIRONMENT, SYSTEM, ALARM, HISTORY, NETWORK (selected), and MANAGEMENT. Under NETWORK, sub-items include TCP/IP, SNMP, HTTP, Remote Access, SMTP (selected), LDAP, RADIUS, Daisy Chain, and SysLog. The main content area is divided into two sections: SMTP CONFIGURATION and MAIL CONFIGURATION. Red numbers 1 through 9 are overlaid on the interface to highlight specific elements: 1 points to the 'Enable' checkbox in SMTP; 2 points to the 'Address' field; 3 points to the 'Port' field; 4 points to the 'Use TLS' checkbox; 5 points to the 'Login Auth' checkbox; 6 points to the 'User Name' field; 7 points to the 'Password' field; 8 points to the 'Save' button in SMTP; and 9 points to the 'Cancel' button in SMTP.

No.	Item	Description
①	Enable	It allows the rPDU to inform users via e-mail notification.
②	Address	IP address of the e-mail server for the connection.
③	Port	E-mail port for the connection.
④	Use TLS	Users can turn on/ off the TLS function.
⑤	Login Authentication	The e-mail server may require an authentication login. If login authentication is required, enable this item and fill in the Username and Password below.
⑥	Username	Username for authentication login.
⑦	Password	Password for authentication login.
⑧	Save	It saves the current SMTP configuration.
⑨	Cancel	Cancellation of changes and reloading of the previous configuration.

The screenshot shows a configuration page with a sidebar on the left containing categories like POWER MANAGEMENT, ENVIRONMENT, SYSTEM, ALARM, HISTORY, NETWORK, and MANAGEMENT. The main area is titled 'Configuration' and contains two sections: 'SMTP CONFIGURATION' and 'MAIL CONFIGURATION'.

SMTP CONFIGURATION:

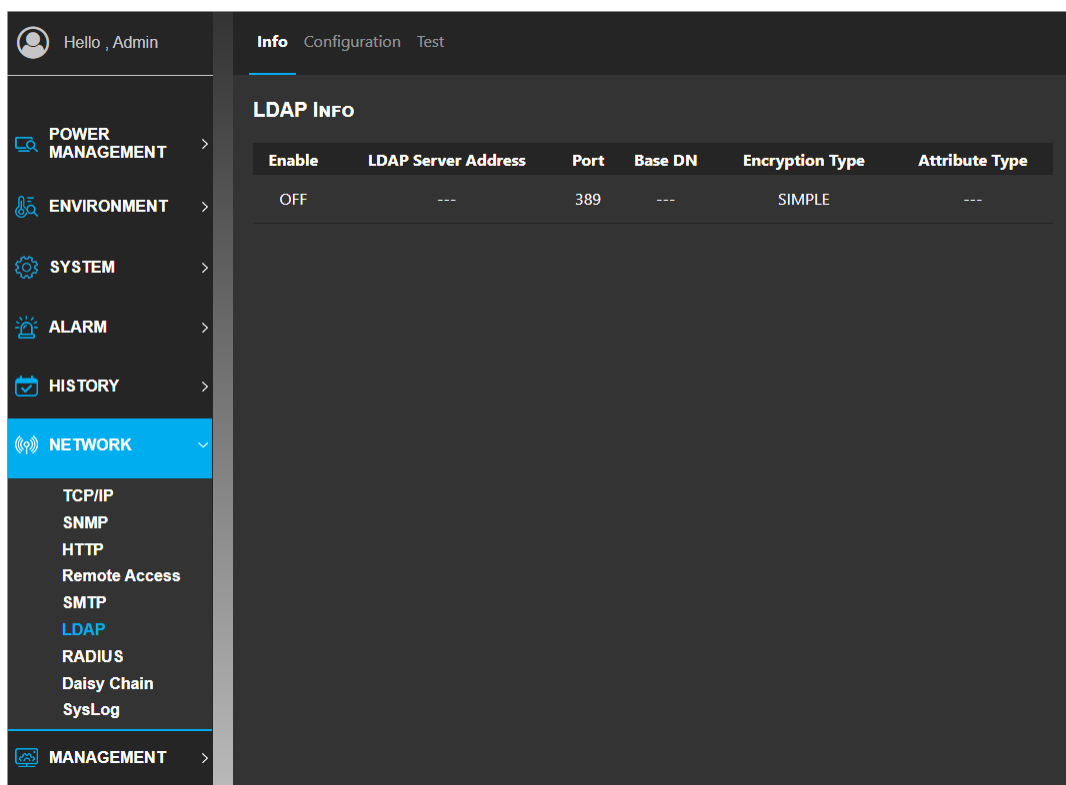
- Enable: ☐ OFF
- Address: 192.168.0.1
- Port: 25
- Use TLS: ☐ OFF
- Login Auth: ☐ OFF
- User Name: [Empty field]
- Password: [Empty field]
- Buttons: Save, Cancel

MAIL CONFIGURATION:

- Sender Address: 1
- Recipient 1 Address: 2
- Recipient 2 Address: 3
- Recipient 3 Address: 4
- Recipient 4 Address: 5
- Subject: SUBJECT
- Content: CONTENT
- Buttons: Test, Save, Cancel

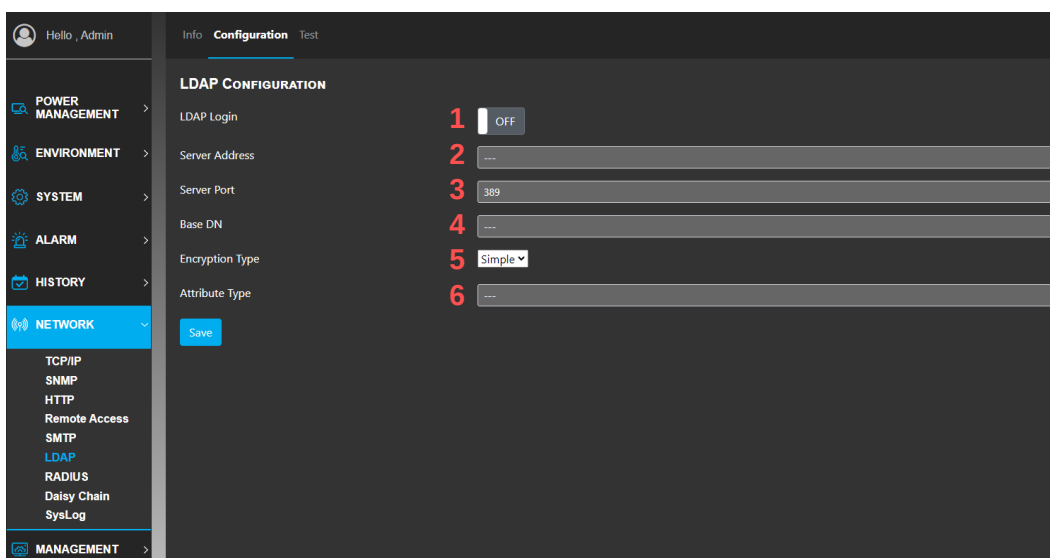
Red numbers 1 through 7 are overlaid on the interface to identify specific elements: 1 points to the Sender Address field, 2 to the Recipient 1 Address field, 3 to the Subject field, 4 to the Content field, 5 to the Test button, 6 to the Save button, and 7 to the Cancel button.

No.	Item	Description
①	Sender Address	E-mail address of the sender who sends the e-mail notification.
②	Recipient Address	Recipient's e-mail address for the mail to be sent. A maximum of 4 recipient addresses can be applied. Please fill in from Recipient 1 to Recipient 4.
③	Subject	The subject of the e-mail to be sent.
④	Content	The contents of the e-mail.
⑤	Test	Click the button to send a test e-mail with the connection configuration. Please save first.
⑥	Save	Click the button to save the current mail configuration.
⑦	Cancel	Click the button to cancel the changes and reloading of the previous configuration.



The **Info** page of **LDAP** under **Network** shows the LDAP server configured information.

- **LDAP server setup**



Three types of LDAP encryption method, simple, TLS and SSL, are described below:

1. LDAP encryption type: Simple

No.	Item	Description
①	LDAP Login	Enable or disable LDAP login.
②	Server Address	LDAP server address configuration, e.g. 192.168.0.100.
③	Server Port	Server port configuration, e.g. 389.
④	Baseline DN	LDAP Server Base DN configuration, e.g DC = delta, DC = corp.
⑤	LDAP Encryption	LDAP transmission encryption type configuration, e.g. Simple.
⑥	Attribute	LDAP server attribute configuration, e.g. empty.

2. LDAP encryption type: TLS

No.	Item	Description
①	LDAP Login	Enable or disable LDAP login.
②	Server Address	LDAP server address configuration, e.g. 192.168.0.100.
③	Server Port	Server port configuration, e.g. 389.
④	Baseline DN	LDAP Server Base DN configuration, e.g DC = delta, DC = corp.
⑤	LDAP Encryption	LDAP transmission encryption type configuration, e.g. TLS.
⑥	Attribute	LDAP server attribute configuration, e.g. sAMAccountName.

3. LDAP encryption type: SSL

No.	Item	Description
①	LDAP Login	Enable or disable LDAP login.
②	Server Address	LDAP server address configuration, e.g. 192.168.0.100.
③	Server Port	Server port configuration, e.g. 636.
④	Baseline DN	LDAP Server Base DN configuration, e.g DC = delta, DC = corp.
⑤	LDAP Encryption	LDAP transmission encryption type configuration, e.g. SSL.
⑥	Attribute	LDAP server attribute configuration, e.g. sAMAccountName.

- LDAP server Test

LDAP TEST

User Name **1**

Password **2**

Test

No.	Item	Description
1	Username	Valid user account on an LDAP server with domain name, e.g. Delta_PDU@delta.corp.
2	Password	Valid user account password.

RADIUS **1** **2** **3**

Enable	Timeout(Sec)	Retry
OFF	1	3

SERVER **4** **5**

Index	Address	Port
1	---	1812
2	---	1813

The RADIUS function allows users to login with an external identity verification.



NOTE:

This function is only enabled when RADIUS service is available to users.

No.	Item	Description
①	Enable	RADIUS function enable status.
②	Timeout	The request will be sent again when no response from the RADIUS server is received within the set time.
③	Retry	Maximum number to resend a request to the RADIUS server when no response from the RADIUS server is received.
④	Address	Address setting of the RADIUS server for the connection.
⑤	Port	Port setting of the RADIUS server for the connection.

No.	Item	Description
①	Enable	RADIUS function enable status.
②	Timeout	The request will be sent again when no response from the RADIUS server is received within the set time.

No.	Item	Description
③	Retry	Maximum number to resend a request to the RADIUS server when no response from the RADIUS server is received.
④	Server 1 Address	Address setting of RADIUS server 1 for the connection.
⑤	Server 1 Port	Port number setting of RADIUS server 1 for the connection.
⑥	Server 1 Secret	Secret key setting of RADIUS server 1 for the connection.
⑦	Server 2 Address	Address setting of RADIUS server 2 for the connection.
⑧	Server 2 Port	Port number setting of RADIUS server 2 for the connection.
⑨	Server 2 Secret	Secret key setting of RADIUS server 2 for the connection.
⑩	Save	Click the button to save the current RADIUS configuration.
⑪	Cancel	Click the button to cancel the changes and reloading of the previous configuration.

The screenshot displays the 'RADIUS TEST' configuration page. On the left, a sidebar lists various system settings, with 'NETWORK' expanded and 'RADIUS' selected. The main panel has three tabs: 'Info', 'Configuration', and 'Test'. The 'Test' tab is active, showing input fields for 'User Name' (labeled 1) and 'Password' (labeled 2). A 'Test' button (labeled 3) is positioned below the password field.

No.	Item	Description
①	Username	Account user name for testing the connection.
②	Password	Account password for testing the connection.

No.	Item	Description
3	Test	When the button is clicked, connection with RADIUS configuration starts with inputting the username and password. Connection result is shown at the right button. “Success” will show when with correct server configuration and account information. “Fail” will show when server configuration or account information has an error.

The screenshot shows the 'Daisy Chain Nodes List' in the 'Network' section. A red box highlights the 'Action' column for the first three nodes. A red line connects this box to two callout boxes. The first callout box (labeled 3) shows the context menu for the first node, and the second callout box (labeled 2) shows the context menu for the second node. The third callout box (labeled 4) shows the context menu for the third node. The fourth callout box (labeled 5) shows the context menu for the fourth node. The fifth callout box (labeled 1) shows the 'Rearrange Address' button.

Index	Status	Address	Preferred	MAC	Name	Serial	FW Version	Date & Time	Action
1	ONLINE	1	1		This PDU				[Action icons]
2	ONLINE	2	0	00:18:23:0C:FB:73	DELTA IPDU (PDU A327DSA23500)	JKC211000006WD	S1.06B02	2023-05-06 17:12:53	[Action icons]
3	ONLINE	3	0	00:18:23:0C:FB:41	DELTA IPDU (PDU A327DSA23500)	JKC211000004WD	S1.06B02	2023-05-06 17:12:53	[Action icons]
4	ONLINE	4	0	00:18:23:0C:FB:64	DELTA IPDU (PDU A327DSA23500)	JKC211000001WD	S1.06B02	2023-05-06 17:12:53	[Action icons]
5	OFFLINE	---	---	---	---	---	---	---	[Action icons]
6	OFFLINE	---	---	---	---	---	---	---	[Action icons]
7	OFFLINE	---	---	---	---	---	---	---	[Action icons]
8	OFFLINE	---	---	---	---	---	---	---	[Action icons]
9	OFFLINE	---	---	---	---	---	---	---	[Action icons]
10	OFFLINE	---	---	---	---	---	---	---	[Action icons]
11	OFFLINE	---	---	---	---	---	---	---	[Action icons]
12	OFFLINE	---	---	---	---	---	---	---	[Action icons]
13	OFFLINE	---	---	---	---	---	---	---	[Action icons]

Callout 1: Rearrange Address

Callout 2: Send RMC firmware to all nodes, Send IPM firmware to all nodes, Send Output Meter firmware to all nodes, Send Display Board firmware to all nodes, Indicate, Sync all date time from this

Callout 3: Send RMC firmware to PDU#2, Send IPM firmware to PDU#2, Send Output Meter firmware to PDU#2, Send Display Board firmware to PDU#2, Indicate

Callout 4: Send RMC firmware to PDU#2, Send IPM firmware to PDU#2, Send Output Meter firmware to PDU#2, Send Display Board firmware to PDU#2, Indicate

Callout 5: Send RMC firmware to PDU#2, Send IPM firmware to PDU#2, Send Output Meter firmware to PDU#2, Send Display Board firmware to PDU#2, Indicate

The **Daisy Chain Nodes List** in **Network** displays the network information of the chained rPDUs.

No.	Item	Function
①	Address Setup Button	User can set all rPDUs' addresses.  NOTE: 1. When setting a new address, please pay attention whether the address has already been used or not. If yes, you need to set the rPDU that has used the address to other address; otherwise, the set address will not be obtained. 2. If you enable the following functions, the rPDU's address will be changed accordingly. Restore to Factory Default Restore to User Default Import Configuration
②	Firmware Sent to All Chained rPDUs For Upgrade	Users can click the button to send this rPDU's RMC, IPM or DPB firmware to all chained rPDUs for upgrade.
③	Firmware Sent to A Specific rPDU For Upgrade	Users can click the button to send this rPDU's RMC, IPM or DPB firmware to a specific rPDU for upgrade.
④	Indicator Button	When users click the button, the assigned rPDU's system status indicator on the RMC will blink red and green five times.
⑤	Time Synchronization Button	Users can click the button to synchronize the time of this rPDU with all chained rPDUs.  NOTE: When any rPDU connected in the Daisy Chain enables the SNTP function, the rest of other chained rPDUs will also automatically synchronize their time with this rPDU.

Item	Description
RMC	Remote monitoring controller
IPM	Input meter
DPB	Display board

- **SysLog**

The screenshot shows a web interface with a dark theme. On the left is a sidebar menu with icons and labels: 'POWER MANAGEMENT', 'ENVIRONMENT', 'SYSTEM', 'ALARM', 'HISTORY', 'NETWORK' (highlighted in blue), and 'MANAGEMENT'. Under 'NETWORK', there is a list of sub-items: 'TCP/IP', 'SNMP', 'HTTP', 'Remote Access', 'SMTP', 'LDAP', 'RADIUS', 'Daisy Chain', and 'SysLog' (highlighted in blue). The main content area has a top bar with 'Info' and 'Configuration' tabs. Below this is the 'SysLog Info' section, which contains a table with three columns: 'Enable', 'Server Address', and 'Port'. The table has one row with the values 'OFF', '192.168.0.1', and '514'.

Enable	Server Address	Port
OFF	192.168.0.1	514

The **SysLog** page shows Syslog server connection settings. Users can obtain the information about event log by connecting to the Syslog server.

SysLog CONFIGURATION

Enable **1** ☐ OFF

Server Address **2**

Port **3**

Protocol **4**

No.	Item	Function
1	Enable	Enable or disable the Syslog function.
2	Server Address	Users can set up the Syslog server's IP address.
3	Port	Users can set up the Syslog server's port.
4	Protocol	Users can choose either RFC3416 or RFC5424 protocol for message encoding.

- Management**

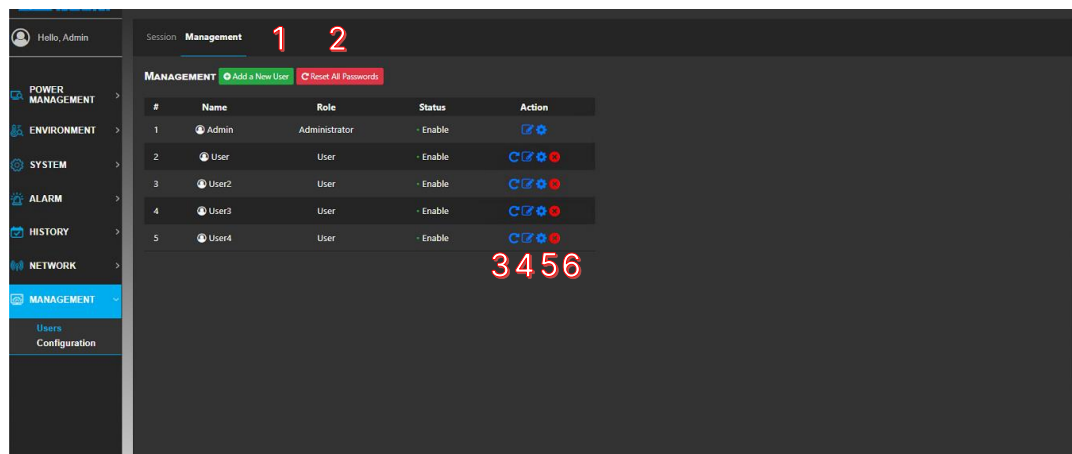
Session Management

SESSION LIST

Admin @ 10.142.33.28

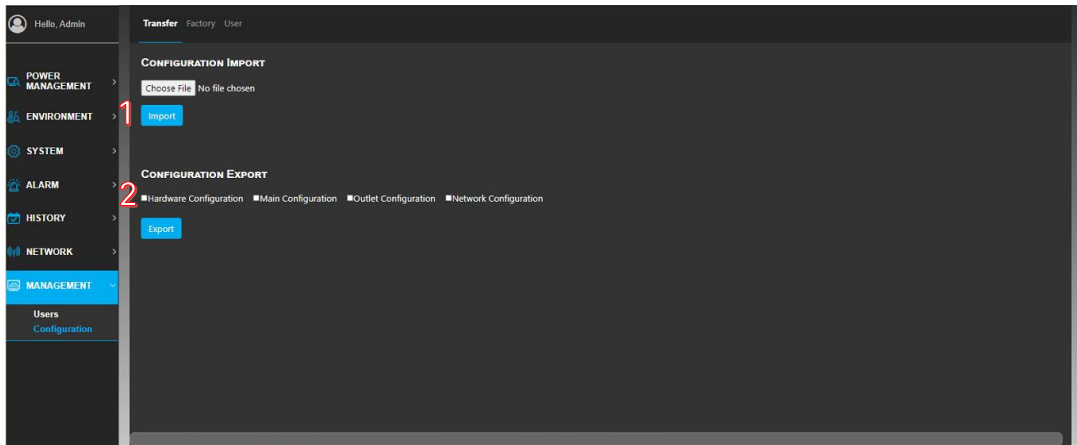
The session list displays the user who logged in and is currently using the rPDU. Users can see their own account and others accounts of other users who have lower account level than them (i.e., if you log in with an Admin account, you can see logged-in Admin and User accounts; if you log in with a User level account, you can only see logged-in User level accounts).

Users with a higher-level account can remove users who login with a lower-level account. Re-login action is needed after the removal.



The **Management** page under **Users** shows all visible accounts with their account level. Admin-level users can perform several actions on these accounts.

No.	Item	Function
①	Add New Users	Admin-level users can add a new user who is allowed to login to this rPDU by clicking this button.
②	Reset All Passwords	Admin-level users can reset passwords of all accounts displayed on the screen by clicking this button.
③	Reset Password	Admin-level users can reset the password of the selected account by clicking this button.
④	Change Password	Admin-level users can change the password of the selected account by clicking this button.
⑤	Multi Setting Option	Admin-level users can change user name and user role as well as enable or disable the selected account by clicking this button.
⑥	Delete Account	Admin-level users can delete the selected account by clicking this button.



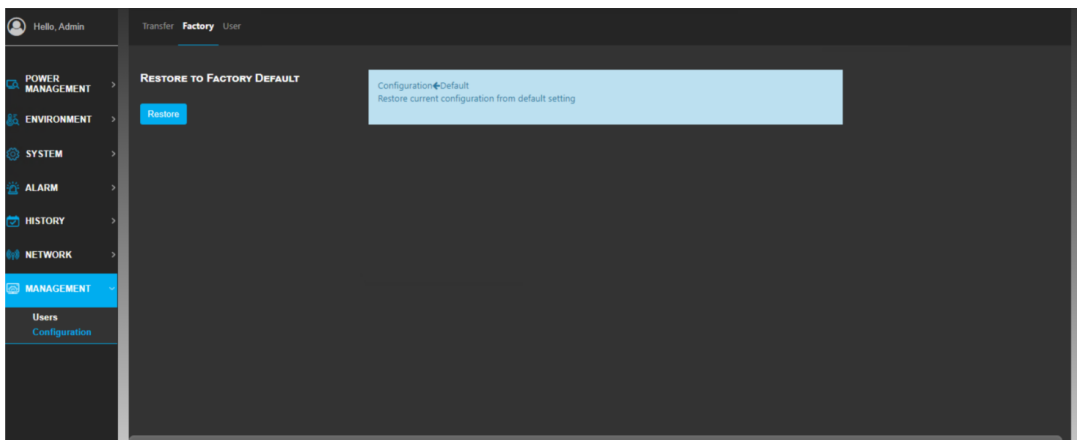
The **Transfer** page under **Configuration** allows users to import the preferred configuration to a new rPDU or export the current configuration to a configuration file. Any other rPDU can apply this configuration simply by importing data on the configuration file.

No.	Item	Function
①	Select Import File	Users can select the preferred configuration file and upload it to the rPDU by clicking this button.
②	Configuration Export	Users can select the configuration that will be packaged into the configuration file. Selection of multi-part of the configuration for the file is allowed.



NOTE:

The original set address of each chained rPDU will be saved in **Network Configuration**. After importing the configuration from other rPDU, please reset this rPDU's address according to the setup procedures mentioned in *Chapter 7.1 Connection of rPDUs in A Daisy Chain*.

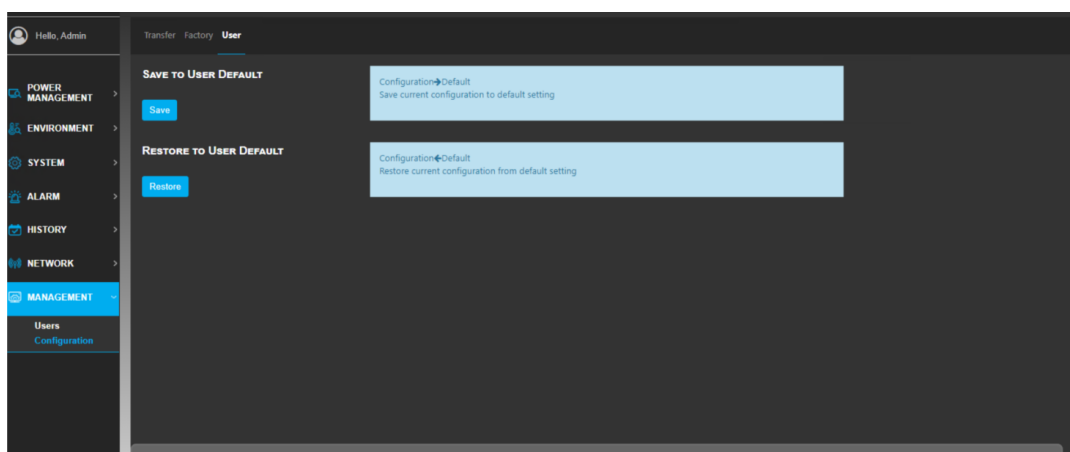


The function of restoration to factory default allows current configuration of the rPDU to go back to the initial factory setting. Be aware that this action will force unsaved configuration (including password and user account information) set by users to be overwritten.



NOTE:

1. Please restore to factory default if you don't need to use the rPDU anymore.
2. The default address of each chained rPDU is 1. Please reset this rPDU's address according to the setup procedures mentioned in ***Chapter 7.1 Connection of rPDUs in A Daisy Chain*** after clicking the restore button to **RESTORE TO FACTORY DEFAULT**.



Save to User Default lets users save the preferred configuration to rPDU storage. Saving allows the rPDU to restore to the preferred configuration as users click **Restore to User Default**.

Restore to User Default allows users to restore all configuration on the rPDU back to the user default setting. Be aware that this action will force unsaved configuration (including password and user account information) set by users to be overwritten.



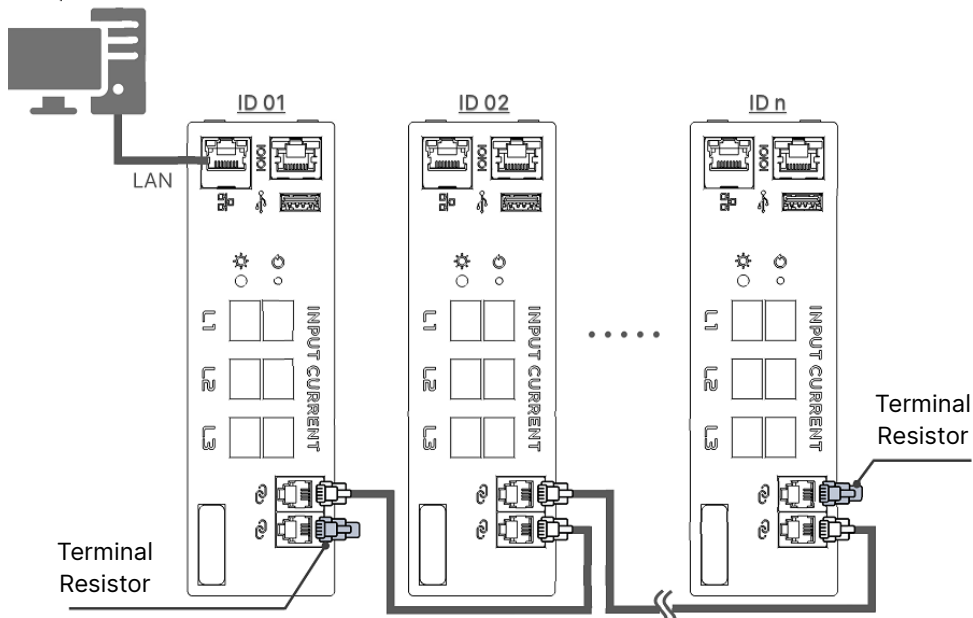
NOTE:

The original set address of each chained rPDU will be saved in **USER DEFAULT**. If you are not sure about the address set in **USER DEFAULT**, please reset this rPDU's address according to the setup procedures mentioned in ***Chapter 7.1 Connection of rPDUs in A Daisy Chain*** after clicking the restore button to **RESTORE TO USER DEFAULT**.

Chapter 7 : Daisy Chain

Users can connect up to 40 rPDUs through the daisy chain ports. With connecting to one rPDU through one IP address, users can monitor all chained rPDUs' information and status and also upgrade all chained rPDUs' firmware.

7.1 Connection of rPDUs in A Daisy Chain



(Figure 7-1: Connection of rPDUs in A Daisy Chain)

Step 1

Select one rPDU as the first unit and connect it to a PC via LAN. After that, insert a terminal resistor into one of the rPDU's daisy chain ports.

Step 2

Use a RJ11-RJ11 cable to connect the first rPDU's the other daisy chain port with the second rPDU's daisy chain port (just choose one). Repeat this step to connect all rPDUs in series.

Step 3

Insert a terminal resistor into the last rPDU's unconnected daisy chain port to complete the daisy chain hardware setup.



NOTE:

Up to 40 rPDUs can be connected in a daisy chain, and the total cable length should be within 40 meters (131.23 ft).

7.2 Daisy Chain Web Page Initial Setup

Index	Status	Address	MAC	Name	Serial	FW Version	Date & Time	Action
1	ONLINE	1		This PDU				
2	ONLINE	2	00:18:23:0C:FB:4A	DELTA iPDU	JKC211000023WD		2023-04-27 21:15:36	
3	ONLINE	3	00:18:23:0C:FB:73	DELTA iPDU	JKC211000006WD		2023-04-27 21:15:35	
4	ONLINE	4	00:18:23:0C:FB:41	DELTA iPDU	JKC211000004WD		2023-04-27 21:15:35	
5	ONLINE	5	00:18:23:0C:FB:6A	DELTA iPDU	JKC211000037WD		2023-04-27 21:15:36	
6	ONLINE	6	00:18:23:0C:FB:64	DELTA iPDU	JKC211000041WD		2023-04-27 21:15:38	
7	ONLINE	7	00:18:23:0C:FB:3B	DELTA iPDU	JKC211000011WD		2023-04-27 21:15:35	
8	ONLINE	8	00:18:23:0C:FB:50	DELTA iPDU	JKC211000030WD		2023-04-27 21:15:38	
9	ONLINE	9	00:18:23:0C:FB:4F	DELTA iPDU	JKC211000025WD		2023-04-27 21:15:38	
10	ONLINE	10	00:18:23:33:AB:8D	DELTA iPDU	JKC224900749W0		2023-04-27 21:15:36	
11	ONLINE	11	00:18:23:33:AC:47	DELTA iPDU	JKC224900719W0		2023-04-27 21:15:36	
12	ONLINE	12	00:18:23:33:AC:39	DELTA iPDU	JKC224900734W0		2023-04-27 21:15:38	
13	ONLINE	13	00:18:23:33:AB:8C	DELTA iPDU	JKC224900744W0		2023-04-27 21:15:38	

Step 1

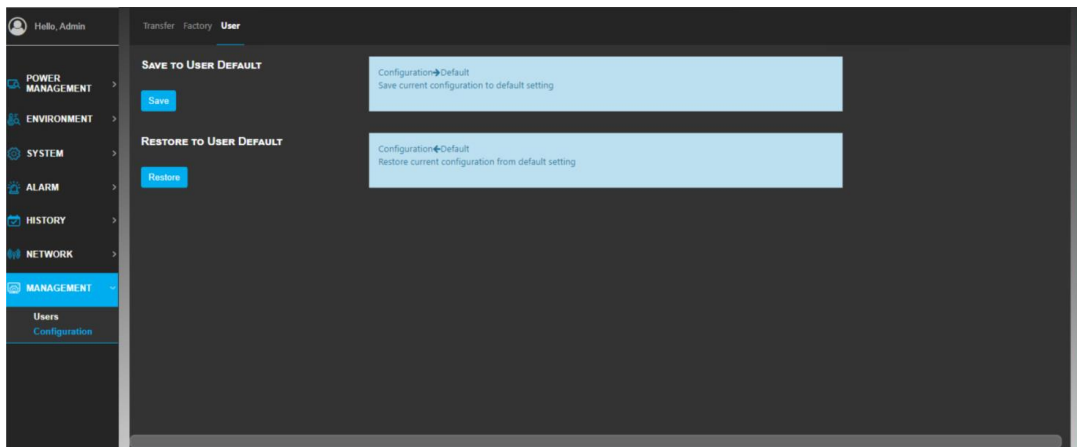
Enter the **Daisy Chain** page under **Network**, and check whether the total number of **ONLINE** units matches the actual number of the connected rPDUs.

Step 2

Follow the ID sequence of rPDUs connected in series according to *Chapter 7.1 Connection of rPDUs in A Daisy Chain* and click the **Rearrange Address** button to set up each rPDU's address in the address field. You can refer to the MAC on the RMC or click the  button to ensure the actual connection addresses of all chained rPDUs. After that, click the save button to complete the initial setup of daisy chain web page.

Step 3

Go to the **User** page under **Configuration** shown in the figure below, and click the save button to save this rPDU's address to **USER Default**. For the rest of chained rPDUs, log in to each Web Page and perform the procedures mentioned in **Step 3**.



NOTE:

1. The default address of each chained rPDU is 1. When an rPDU is connected online and finds that the set address has already been occupied, it will automatically find the next vacant address to go online. For the first time connection, the address sequence will be based on the online time of each rPDU and may be different from the ID sequence defined in the hardware configuration mentioned in ***Chapter 7.1 Connection of rPDUs in A Daisy Chain***.
2. Please confirm that all addresses are entered before clicking the save button in order to ensure that all chained rPDUs receive the new addresses at the same time.
3. After the daisy chain web page initial setup is completely done, the rPDUs will save users' setting values individually. When the rPDUs are re-connected online, they will give priority to reconnecting with the set addresses.

7.3 Firmware Upgrade for Chained rPDUs

Hello , Admin

POWER MANAGEMENT >

ENVIRONMENT >

SYSTEM >

ALARM >

HISTORY >

List

NODES LIST

Rearrange Address

Index	Status	Address	MAC	Name	Serial	FW Version	Date & Time	Action
1	ONLINE	1		This PDU				   
2	ONLINE	2	00:18:23:0C:FB:4A	DELTA iPDU	JKC211000023WD		2023-05-02 10:18:50	   
3	ONLINE	3	00:18:23:0C:FB:73	DELTA iPDU	JKC211000006WD		2023-05-02 10:18:53	   
4	ONLINE	4	00:18:23:0C:FB:41	DELTA iPDU	JKC211000004WD		2023-05-02 10:18:50	   
5	ONLINE	5	00:18:23:0C:FB:6A	DELTA iPDU	JKC211000037WD		2023-05-02 10:18:50	   

After updating the firmware of the rPDU, users can click the  button to send this rPDU's RMC, IPM or DPB firmware to all chained rPDUs for firmware upgrade, or click the  button to send this rPDU's RMC, IPM or DPB firmware to a specific rPDU for firmware upgrade.

Hello , Admin

POWER MANAGEMENT >

ENVIRONMENT >

SYSTEM >

ALARM >

HISTORY >

List

NODES LIST

Index	Status	Address	MAC	Name	Serial	FW Version	Date & Time	Action
1	0.30%							 
2	ONLINE	2	00:18:23:0C:FB:4A	DELTA iPDU	JKC211000023WD		2023-04-28 15:43:54	   
3	ONLINE	3	00:18:23:0C:FB:73	DELTA iPDU	JKC211000006WD		2023-04-28 15:43:53	   
4	ONLINE	4	00:18:23:0C:FB:41	DELTA iPDU	JKC211000004WD		2023-04-28 15:43:54	   
5	ONLINE	5	00:18:23:0C:FB:6A	DELTA iPDU	JKC211000037WD		2023-04-28 15:43:55	   

When the firmware is being sent to other rPDU(s), the **Action** icon of the original rPDU will change to . When the icon  appears, it means that the firmware is being uploaded. Users can click the  icon to terminate sending the firmware.

As for the rPDU(s) receiving the firmware, the **Action** icon will change to . After the firmware is received or upload is terminated, it will return to the original state.

9	2020-02-01 08:12:42	File sent to 39/39 PDU(s)
10	2020-02-01 07:44:38	Firmware distribution Start

After the firmware is received, users can go to the **Event Log** page under **History** to check how many rPDUs successfully receive the firmware and go to the **Inventory** page under **System** to check whether the firmware version is successfully updated.



NOTE:

1. During the process of uploading the firmware to other rPDU(s), if the web page is idle for a long time to cause logout, it will not affect the firmware upload process. Please ensure that the LAN is still connected.
2. The firmware upload process does not affect the operation of all chained rPDUs; users can switch pages to operate each rPDU normally.

Chapter 8 : Troubleshooting

Problem	Solution
The reset address cannot be saved.	1. Check if the address is set as 1 ~ 40. 2. Check if the same address is set.
The new set address is invalid.	Please make sure whether the new set address has already been occupied by other rPDU. If yes, please reset the rPDU that occupies the address to another vacant address and reset the rPDU that you originally want to set.
The chained rPDUs suddenly change their addresses.	Please reset the address according to <i>7.2 Daisy Chain Web Page Initial Setup.</i>
The rPDU cannot connect online.	1. Please check whether the first chained rPDU and the last one are connected with the terminal resistors. 2. Please replace the RJ11-RJ11 cable with a new one and check if the total cable length exceeds 40 meters (131.23 ft). If the above-mentioned solution doesn't work, please contact Delta customer service.
The Inventory page under System still shows the old version of the firmware after firmware upgrade.	The firmware upload progress bar only indicates the progress of sending the firmware to other rPDU(s). Only after the rPDU(s) completely receive(s) the firmware can the firmware be upgraded. Please wait for a few minutes and go to the Inventory page under System to confirm.
Unable to send the IPM firmware.	Please make sure that all chained rPDUs have the same input type (e.g. 1p-LN, 3p-WYE, 1p-LL or 3p-DELTA). Different input types of rPDUs will cause failure of sending the IPM firmware.
Firmware upgrade is failed.	If there are continuous failures of sending firmware to other rPDU(s), please unplug the RMC that failed to receive the firmware, re-plug the RMC, wait for the rPDU to go online and try to send the firmware again. If the firmware still cannot be upgraded, please contact Delta customer service.

Chapter 9 : Optional Accessories

No.	Item		Function
1	RJ11-RJ11 Cable	1 m (3.28 ft)	Connection with the daisy chain port for daisy chain application.
		3 m (9.84 ft)	
		5 m (16.4 ft)	
2	Terminal Resistor		Connection with the daisy chain port for daisy chain application.
3	Grounding Nut		For grounding use
4	Retention Sleeve		For stronger connection with the output socket.

Appendix 1 : Warranty

Seller warrants this product, if used in accordance with all applicable instructions, to be free from original defects in material and workmanship within the warranty period. If the product has any failure problem within the warranty period, Seller will repair or replace the product at its sole discretion according to the failure situation.

This warranty does not apply to normal wear or to damage resulting from improper installation, operation, usage, maintenance or irresistible force (i.e. war, fire, natural disaster, etc.), and this warranty also expressly excludes all incidental and consequential damages.

Maintenance service for a fee is provided for any damage out of the warranty period. If any maintenance is required, please directly contact the supplier or Seller.



WARNING:

The individual user should take care to determine prior to use whether the environment and the load characteristic are suitable, adequate or safe for the installation and the usage of this product. The User Manual must be carefully followed. Seller makes no representation or warranty as to the suitability or fitness of this product for any specific application.

Global Headquarter

Taiwan

Delta Electronics Inc.
30 Section 2, Huandong Road, Shanhua District,
Tainan City 74144, Taiwan
T +886 6 505 6565
E ups.taiwan@deltaww.com

Regional Office

EMEA

Netherlands

Delta Electronics (Netherlands) B.V.
Zandsteen 15, 2132 MZ Hoofddorp, The Netherlands
T +31 (0)20 800 3900
E info@delta-emea.com

AMERICA

U.S.A

Delta Electronics (Americas) Ltd.
46101 Fremont Blvd. Fremont, CA 94538
T +1 510 668 5100
E ups.na@deltaww.com

Colombia

Delta Electronics Colombia SAS
Cra 72 # 95 – 51 Bodega 16, Parque Empresarial Los Lagartos
Bogota DC, Colombia
T +57 317 4052794
E ups.colombia@deltaww.com

ASIA

India

Delta Electronics India Pvt. Ltd.
Plot No. 43, Sector-35, HSIDC, Gurgaon-122001,
Haryana, India
T +91 124 4874 900
E ups.india@deltaww.com

Japan

Delta Electronics (Japan), Inc.
2-1-14 Shibadai, Minato-Ku, Tokyo, 105-0012,
Japan
T +81-3-5733-1111
E jpstps@deltaww.com

Singapore

Delta Electronics Int'l (Singapore) Pte Ltd.
17 Kallang Junction, #01-01, TRION,
Singapore 339274
T +65 6747 5155
E ups.singapore@deltaww.com

Vietnam (Ho Chi Minh)

Delta Electronics (Vietnam) Co., Ltd.
10th Floor, The Galleria Office Building,
258 Nam Ky Khoi Nghia Street, Vo Thi Sau Ward,
District 3, Ho Chi Minh City, Vietnam
T +84 903 133 548
E ups.vietnam@deltaww.com

Philippines

Eltek Power Inc./ Delta
302 Orient Square Bldg
F. Ortigas JR Road, Barangay
San Antonio, Pasig City
1605 Philippines
E ups.philippines@deltaww.com

OCEANIA

Australia

Delta Electronics (Australia) Pty Ltd.
St Leonard's Corporate Centre
Unit 18/39 Herbert Street, St Leonards NSW 2065, Australia
T +61 2 9479 4200
E ups.australia@deltaww.com

UK

Delta Electronics (UK) Ltd.
Eltek House, Unit 1 Cleveland Road, Hemel Hempstead,
Hertfordshire, HP2 7EY, UK
T +44 1442 210805
E sales.gb@eltek.com

Brazil

Delta Electronics Brasil Ltda.
Estrada Velha Rio-São Paulo, 5300 – Eugênio de Melo –
CEP 12247-001 São José dos Campos-SP-Brazil
T +55 12 39322300
E ups.brazil@deltaww.com

Peru

Delta Electronics (Peru) Inc. S.R.L.
Av. Pardo y Aliaga 699 Of. 601, San Isidro Lima, Peru.
T +51 962 834 287
E ups.peru@deltaww.com

China

Delta GreenTech (China) Co., Ltd.
238 Minxia Road, Pudong, Shanghai, 201209 P.R.C
T +86 21 5863 5678
+86 21 5863 9595
E ups.china@deltaww.com

South Korea

Delta Electronics (Korea), Inc.
1511, Byucksan Digital Valley 6-cha, Gasan-dong, Geumcheon-gu,
Seoul, Korea, 153-704
T +82-2-515-5303
E ups.south.korea@deltaww.com

Thailand

Delta Electronics (Thailand) Public Co.,Ltd.
909 Soi 9, Moo 4, E.P.Z., Bangpoo Industrial Estate, Tambon Phraksa,
Amphur Muang-samutprakarn, Samutprakarn Province 10280,
Thailand
T +662 709-2800
E ups.thailand@deltaww.com

Vietnam (Hanoi)

Delta Electronics (Vietnam) Co., Ltd.
3rd Floor, Vietnam 3D Creative Center Building, No. 3 Duy Tan Street,
Dich Vong Hau Ward, Cau Giay District, Hanoi City, Vietnam
T +84 966 532 266
E ups.vietnam@deltaww.com

Indonesia

Delta Electronics International (S) Pte Ltd.
Soho Capital, 30th Fl, Unit SC3009
Jl. Letjend S. Parman kav 28. Jakarta 11470 Indonesia
T + 65 9667 4687
E ups.indonesia@deltaww.com



5013312302