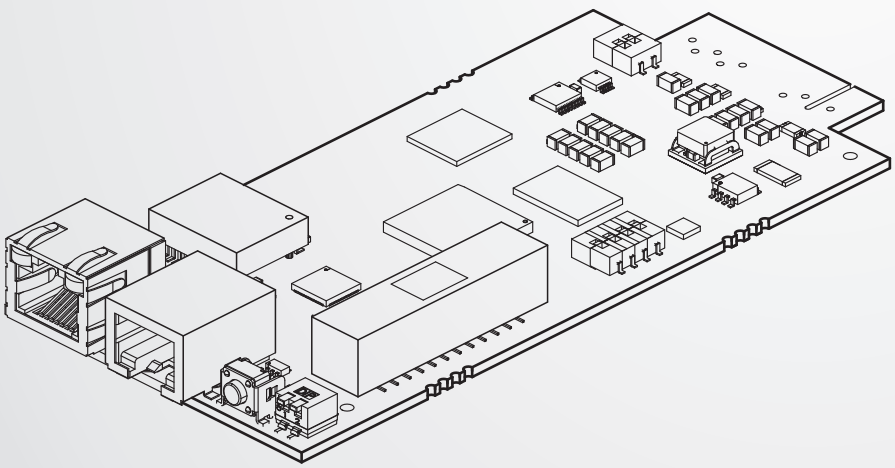


The power behind competitiveness

Delta UPS Network Management and Monitoring Solutions

Simple Network Management Protocol (SNMP) Card Gen3
IPv6

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.

Table of Contents

Chapter 1 : Important Safety Instructions

1.1 Warnings

- The Delta SNMP IPv6 Card for UPS, hereafter referred to as SNMP IPv6, is designed to work with a UPS and needs to be installed inside the UPS's SNMP slot or inside an external SNMP box. Before installation, ensure that all power sources and critical loads connected to the UPS are disconnected.
- Do not place or use this unit in the presence of flammable substances.
- Do not attempt to disassemble the unit.
- Do not attempt to perform any internal modifications on the unit.
- Do not attempt to fix/ replace internal components. When repair is needed, refer all servicing to the nearest Delta service center or authorized distributor.
- Do not allow any objects or liquids of any kind to penetrate the unit.
- Always follow this User Manual to install and operate this unit.
- Do not play the included CD on a conventional CD player. This could generate loud noise at a level that could result in permanent hearing loss.

1.2 Standard Compliance

- **IEC 62368-1**
- **EN 62368-1**
- **EN 55032: 2015+A11: 2020**

  EN 61000-3-2: 2014

  EN 61000-3-3: 2013
- **EN 55035:2017 +A11:2020**

  IEC 61000-4-2:2008

  IEC 61000-4-3:2020

  IEC 61000-4-4:2012

  IEC 61000-4-5:2014+A1:2017

  IEC 61000-4-6:2013+C1:2015

  IEC 61000-4-8:2009

  IEC 61000-4-11:2020+C1:2020+C2:2022

- UL 62368-1
- FCC

  FCC 47 CFR PART 15 SUBPART B and ANSI C63.4: 2014 Amended as per ANSI C63.4a: 2017

Chapter 2 : Introduction

2.1 Product Description

The Delta SNMP IPv6 Card for UPS, hereafter referred to as SNMP IPv6, is a device that provides an interface between an UPS and a network. It communicates with the UPS, acquires its information and remotely manages the UPS via a network system. The SNMP IPv6 supports public protocols including SNMP and HTTP. You can effortlessly configure this SNMP IPv6 using a network system and easily obtain your UPS's status and manage your UPS via the SNMP IPv6.

2.2 Features

- **Network UPS management**

Allows remote management of the UPS from any workstation through Internet or Intranet.

- **Remote UPS monitoring via SNMP & HTTP**

Allows remote monitoring of the UPS using SNMP NMS, Delta MIB (Management Information Base) or a Web Browser.

- **UPS and system function configuration from any client (password protected)**

Set the UPS and system parameters through a Web Browser.

- **Event logs & metering data keeping**

Provides a history data of the UPS's power events, power quality, status and battery conditions.

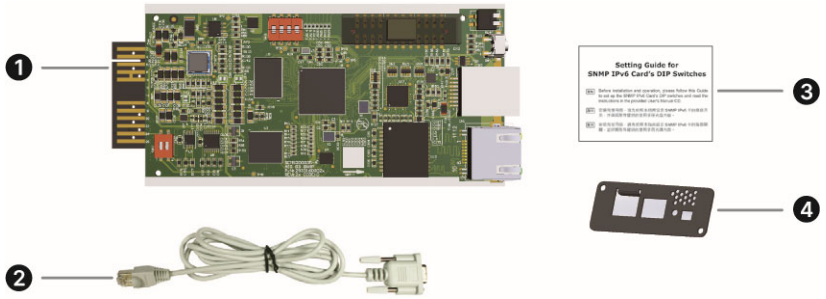
Other features and supported protocols include:

- User notification via SNMP Traps and E-mail
- Network time protocol
- Telnet configuration
- BOOTP/ DHCP
- HTTPS, SSH, SFTP and SNMPv3 security protocols
- RADIUS (Remote Authentication Dial In User Service) and LDAP (Lightweight Directory Access Protocol) authentication for login
- Local authentication

- Remote event log management through syslog
- IPv4 protocol
- IPv6 protocol

2.3 Package Contents

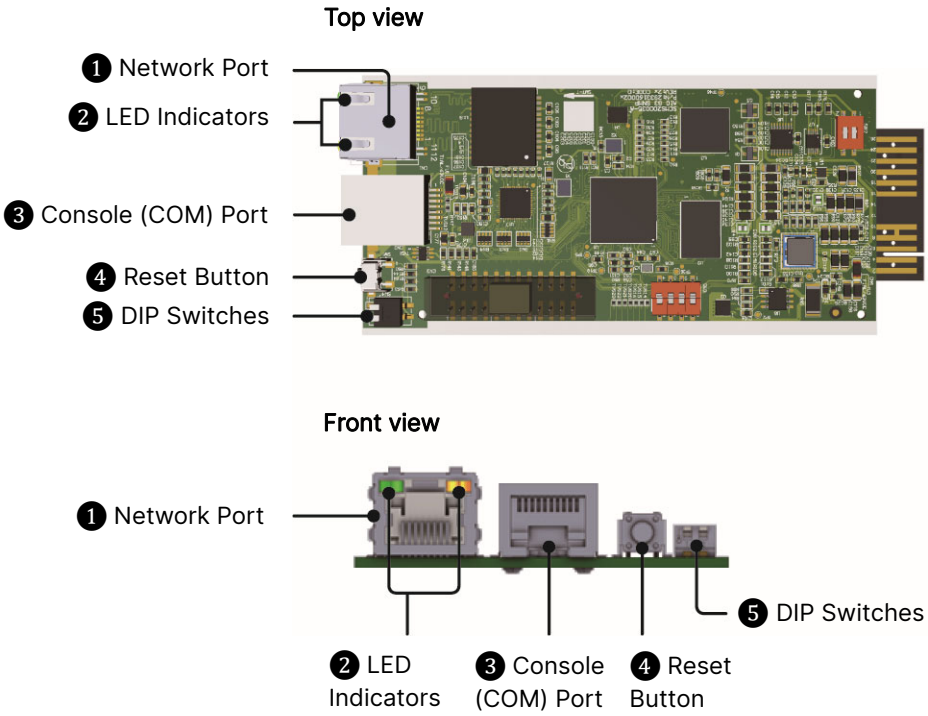
Please carefully verify the SNMP IPv6 and the included accessories. Contact your dealer if any item is missing or damaged. Should you return the items for any rea- son, ensure that they are carefully repacked using the original packing materials came with the unit.



No.	Item	Q'ty
❶	Delta SNMP IPv6 Card for UPS	1 PC
❷	RJ45 to DB9 cable	1 PC
❸	Setting Guide for SNMP IPv6 Card's DIP Switches	1 PC
❹	Cover	1 PC

2.4 Interface

The interface includes a NETWORK port, a COM port, LED indicators, a Reset button, DIP switches shown below. For their functions and indications, please refer to the table below.



No.	Item	Description
1	Network Port	Connects to the Ethernet Network.
2	LED Indicators	When the SNMP IPv6 is initializing or upgrading firmware, the two LED indicators flash simultaneously to show its status. Refer to the following: • **Rapid simultaneous flashing** (every 50ms): Initialization or firmware upgrade in progress. • **Slow simultaneous flashing** (every 500ms): Initialization failed.

<table>
<tr><th>No.</th><th>Item</th><th>Description</th></tr>
<tr><td>❷</td><td>LED Indicators (continued)</td><td>WARNING:
Do NOT remove the SNMP IPv6 or disconnect the UPS's input power during initialization or firmware upgrade! This could result in data loss or damage to the SNMP IPv6.

The green LED indicator shows the network connection status:
• ON: Network connection established and the IPv4 address is useable.
• OFF: Not connected to a network.
• Flashes slowly (every 500ms): Faulty IP address.
The yellow LED indicator shows the linking status between the SNMP IPv6 and the UPS:
• Flashes rapidly (every 50ms): UPS linked.
• Flashes slowly (every 500ms): UPS not linked.</td></tr>
<tr><td>❸</td><td>Console (COM) Port</td><td>1. Connects to a workstation with the provided RJ45 to DB9 cable to configure the system.
2. Connects to an EnviroProbe (optional) to monitor its connected environment monitoring devices.</td></tr>
<tr><td>❹</td><td>Reset Button</td><td>Resets the SNMP IPv6. This does not affect the operation of the UPS.</td></tr>
<tr><td>❺</td><td>DIP Switches</td><td>Set up operation modes.
<table>
<tr><th>DIP switches</th><th>Operation mode</th><th>Description</th></tr>
<tr><td> 
</td><td>Normal Mode</td><td>The SNMP IPv6 works with the UPS. It provides the UPS's status information and parameters through a network system.</td></tr>
<tr><td> 
</td><td>Pass Through Mode</td><td>The SNMP IPv6 stops polling the UPS but transfers the communi-cation data between the console port and the UPS.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>No.</th><th>Item</th><th>Description</th></tr>
<tr><td>❺</td><td>DIP Switches (continued)</td><td>
<table>
<tr><th>DIP switches</th><th>Operation mode</th><th>Description</th></tr>
<tr><td> 
</td><td>Sensor Mode (with EnviroProbe)</td><td>The SNMP IPv6 works with the UPS and an optional EnviroProbe. It provides not only the UPS's status information and parameter readings, but also the EnviroProbe's status information and its environmental parameters such as temperature and humidity.</td></tr>
<tr><td> 
</td><td>Configuration Mode</td><td>In this mode, the user can log in through the console port and configure the SNMP IPv6's settings. Please refer to 4.3 Configuring via COM Port.</td></tr>
</table>
</td></tr>
</table>

NOTE:

For EnviroProbe information, please refer to the Installation Guide included in the package of the EnviroProbe.

Chapter 3 : Installation

NOTE:

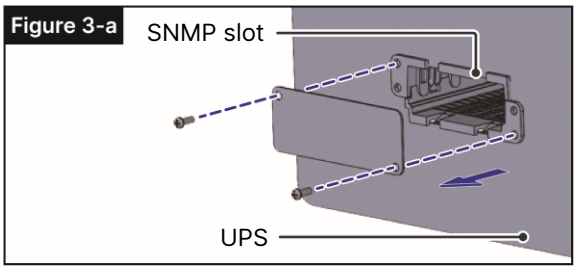
Before installation, please disconnect all power sources and critical loads connected to the UPS. Otherwise, the SNMP IPv6 might have shorting issues to cause UPS shutdown or damage.

Please install the SNMP IPv6 inside your UPS's SNMP slot. If your UPS does not have any SNMP slot, please install it in an optional external SNMP box.

- Please follow the procedures below to install the SNMP IPv6 into your UPS's SNMP slot.

  Step 1 Remove the cover and the two screws shown from the UPS's SNMP slot *(see Figure 3-a)*.

Figure 3-a

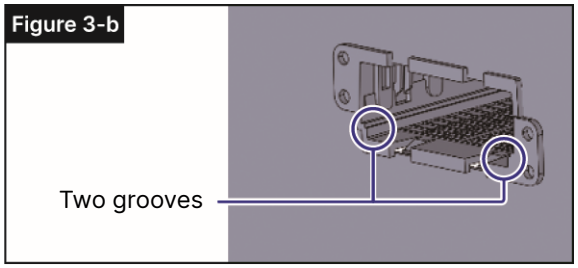


NOTE:

Please note that, due to different design, the location of screws for each UPS's SNMP slot might be different.

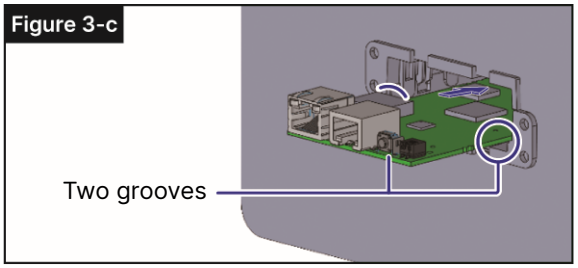
Step 2 Find the two grooves inside the SNMP slot *(see Figure 3-b)*.

Figure 3-b



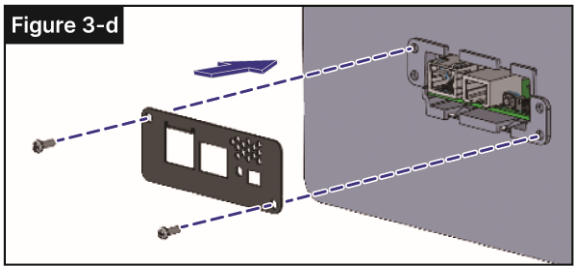
Step 3 Insert the SNMP IPv6 into the grooves ***(see Figure 3-c)***.

Figure 3-c



Step 4 One cover is provided in the SNMP IPv6's package. Please use the two screws that you just removed to fix the cover on the SNMP slot ***(see Figure 3-d)***.

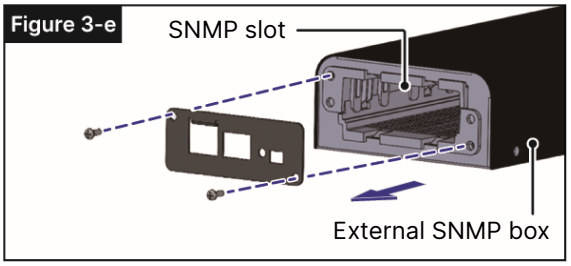
Figure 3-d



- Please follow the procedures below to install the SNMP IPv6 into an external SNMP box.

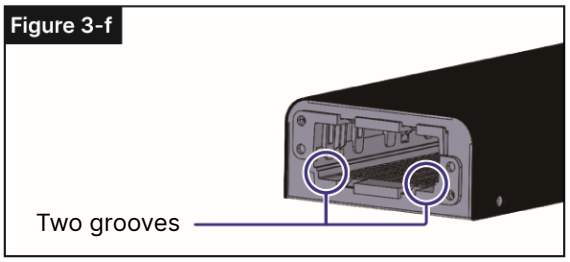
Step 1 Remove the two screws shown from the external SNMP box ***(see Figure 3-e)***.

Figure 3-e



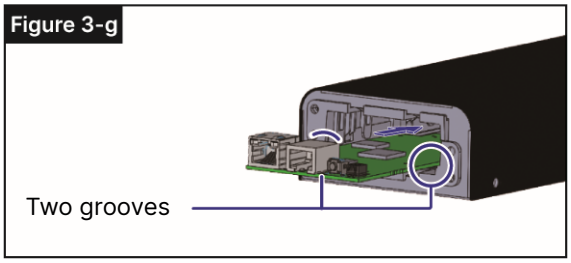
Step 2 Find the two grooves inside the external SNMP box ***(see Figure 3-f)***.

Figure 3-f



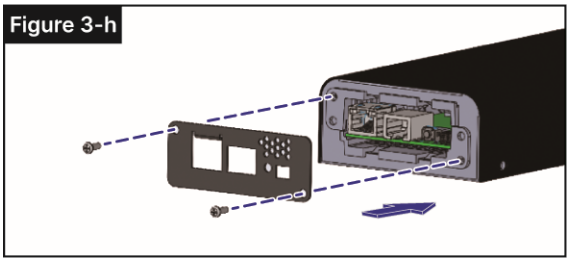
Step 3 Insert the SNMP IPv6 into the grooves ***(see Figure 3-g)***.

Figure 3-g



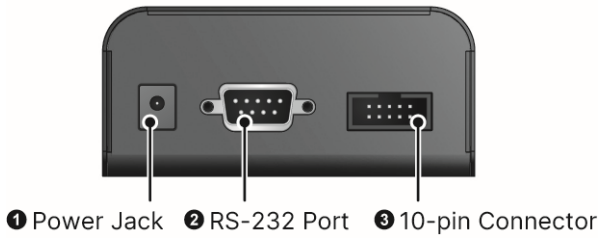
Step 4 One cover is provided in the SNMP IPv6's package. Please use the two screws that you just removed to fix the cover on the external SNMP box ***(see Figure 3-h).***

Figure 3-h



NOTE:

The backside view of the external SNMP box is shown as follows.



No.	Item	Description
❶	Power Jack	Connects your UPS's output. The input power should be 12Vdc.
❷	RS232 Port	Use the RS232 cable provided by your UPS to connect your UPS's RS232 port.
❸	10-pin Connector	Connects your UPS's PC board. Please ask qualified service personnel to execute such connection. Do not perform the connection yourself.

Please refer to the table below for the external SNMP box's specifications.

External SNMP Box Specifications	
Power Jack	Input Power 12Vdc
RS232 Port	D-Sub 9-Pin Male
10-pin Connector	Male
Size (W×D×H)	92.4 × 208 × 42 mm
Weight	540 g

Chapter 4 : System Configurations

There are different ways you can configure your SNMP IPv6. If a network connection is available at your location, the following methods can be used:

- **Web-based interface :** The InsightPower SNMP IPv6 for UPS Web offers comprehensive system management and monitoring. Please refer to *Chapter 5: InsightPower SNMP IPv6 for UPS Web*.
- **SSH mode :** Configure your SNMP IPv6 via text mode. Please refer to *4.2 Configuring via SSH*.

The above-mentioned methods require network connection. If not available, you can use direct COM port connection to set up your SNMP IPv6. Please see *4.3 Configuring via COM Port*.

NOTE:

1. To ensure system security, it is highly recommended that you change your account and password after the first login.
2. If you have multiple SNMP IPv6 units installed in your network, we highly suggest that you change the SNMP IPv6's default Host Name to avoid conflicts. Also, it is recommended that you disable BOOTP/ DHCP and manually assign a valid static IP address to the SNMP IPv6.

4.1 Configuring via InsightPower SNMP IPv6 for UPS Web

To set up the SNMP IPv6 via your web browser, please follow the instructions below:

Step 1 Use a CAT5 network cable to connect the SNMP IPv6's Network port to the network. Launch your web browser. In the address bar, enter the SNMP IPv6's default Host Name **InsightPower**, or default IP address **192.168.1.100**. If you are unable to connect, please see *Chapter 7 : Troubleshooting Q5*.

NOTE:

If you have previously changed the SNMP IPv6's Host Name or IP address, connect with the new settings.

Step 2 Log in as Administrator (default account/ password: admin/ password, case sensitive).

Step 3 Specify your preferred display language (default: English) from the drop-down menu on the top right of the page. The SNMP IPv6 remembers your language preference. In the following instructions, English is chosen as the display language.

Step 4 Click **System** → **Administration** → **User Manager**. Manage your login accounts and passwords under the 'Local Authentication' subhead. The access permission for the account types is shown as follows:

1) **Administrator :** Allowed to modify all settings.

2) **Device Manager :** Allowed to modify device-related settings.

3) **Read Only User :** Only allowed to view settings without the permission to make changes.

You can manually specify whether users are allowed to log in from other LANs. If you wish to block login attempts from external connections, select **Only in This LAN**. Otherwise, select **Allow Any**.

Step 5 Click **System** → **Administration** → **TCP/ IP** to set Host Name, IP address, Subnet Mask and Gateway IP for the SNMP IPv6.

Step 6 Click **Time Server** to manually set time and date for the system or enable automatic time synchronization between the SNMP IPv6 and the time servers.

NOTE:

To completely set up your SNMP IPv6, please refer to *Chapter 5: InsightPower SNMP IPv6 for UPS Web*.

4.2 Configuring via SSH

Step 1 Use a CAT5 network cable to connect the SNMP IPv6's Network port to the network.

Step 2 Connect the workstation to the LAN that the SNMP IPv6 is connected to.

Step 3 Utilize the SSH client tool (such as Putty) to establish the connection.

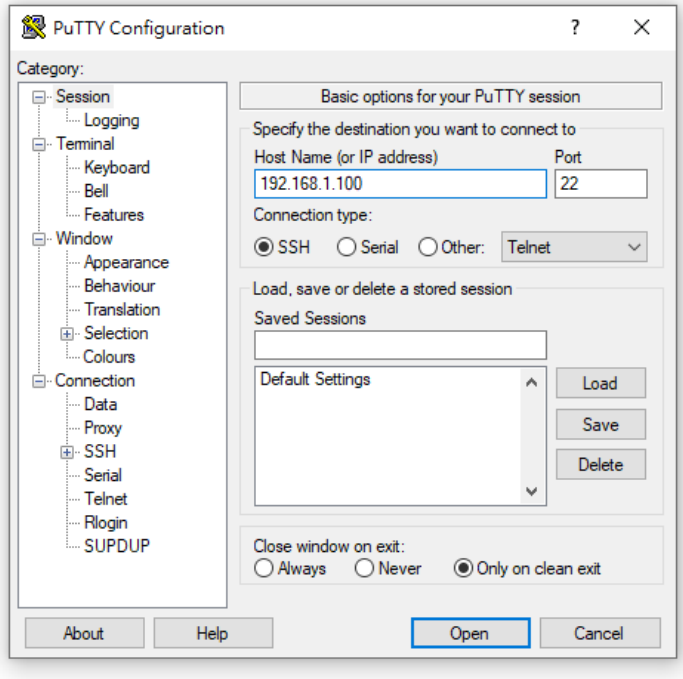
NOTE:

The Putty is a free software, it can be downloaded from http://www.putty.org.

Step 4 Enter the SNMP Card IP Address or Host Name in the '**Host Name (or IP address)**' field and enter **22** in the '**Port**' field.

Step 5 Select **SSH** for the **Connection type** and click the **Open** button to initiate SSH connection with the SNMP IPv6.

Step 6 When the connection is established, enter the Administrator's account and password (default: admin/ password, case sensitive). The Main Menu will appear on the screen. Please refer to ***4.4 Configuring via Text Mode*** for more information.



NOTE:

1. The SNMP IPv6 will terminate idle connection after 60 seconds.
2. Refer to ***Chapter 5: InsightPower SNMP IPv6 for UPS Web*** for complete configurations.

4.3 Configuring via COM Port

If a network connection is not available at your location, you can still set up the SNMP IPv6 via COM port connection. Please follow the instructions below:

NOTE:

If you are running a non-Windows system, refer to your system's user manual for Telnet clients.

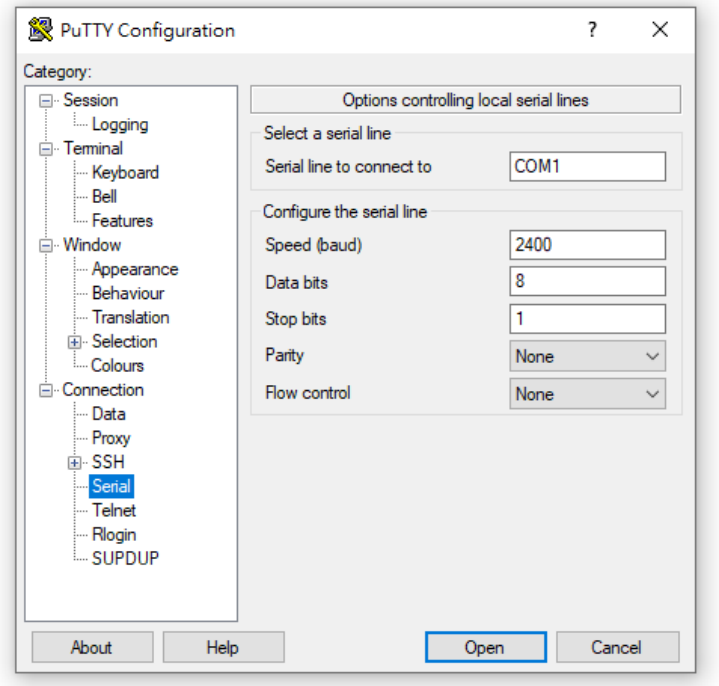
Step 1 Use the provided RJ45 to DB9 cable to connect the SNMP IPv6's COM port to the workstations' COM port.

Step 2 Make sure the two DIP switches of the SNMP IPv6 are set to the **OFF** position (Normal Mode).

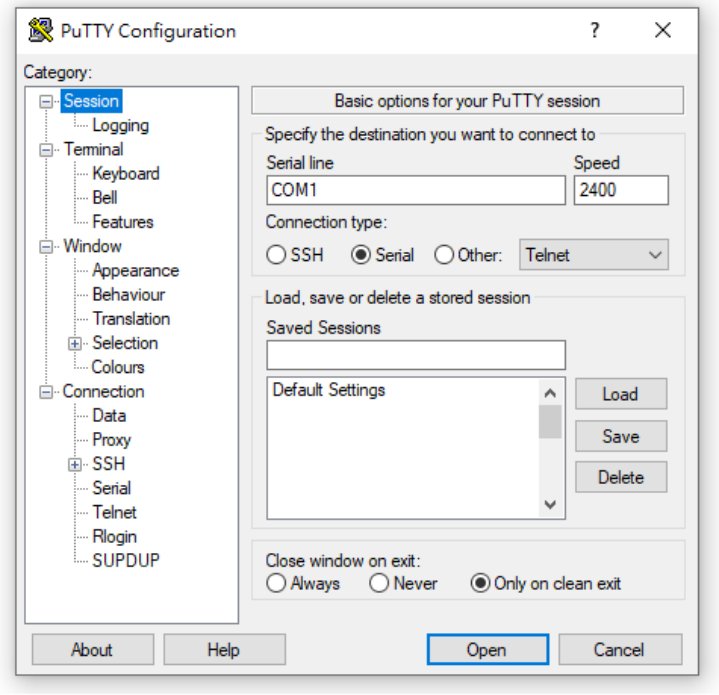
Step 3 Utilize the SSH client tool (such as Putty) to establish the connection.

Step 4 Select a COM port that is connected to the SNMP IPv6 and enter the port name in the '**Serial line to connect to**' field.

Step 5 Configure the COM port parameters as follows.



Step 6 Select **Serial** for the **Connection type** and click the **Open** button.

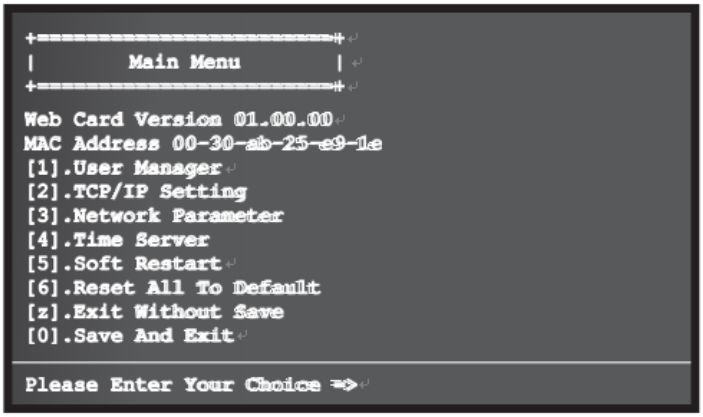


Step 7 Set the two DIP switches of the SNMP IPv6 to the ON position (Configuration Mode) and press the **Enter** key to establish the connection. When the connection is established, log in the Administrator's account/ password (default: admin/ password, case sensitive). Once you are logged in, the Main Menu appears on the screen. Please refer to *4.4 Configuring via Text Mode* for more information.

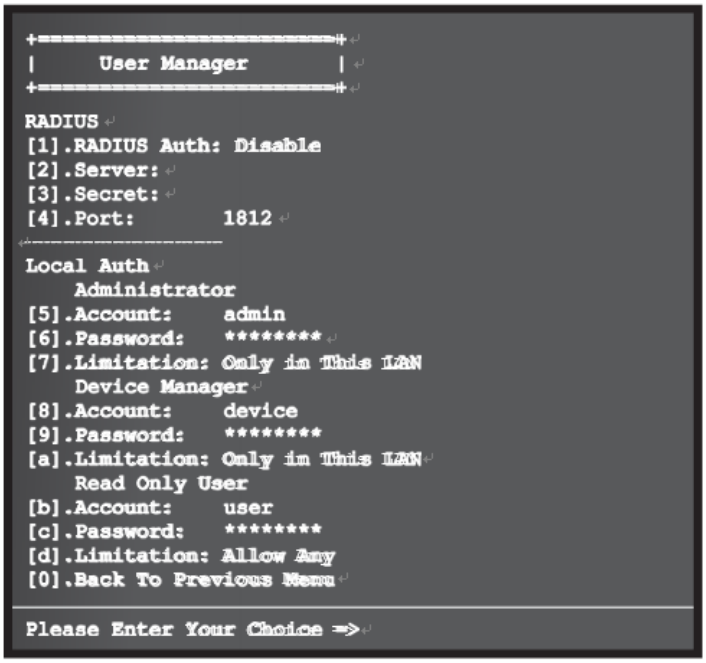
4.4 Configuring via Text Mode

You can configure the SNMP IPv6 via text mode by using SSH/ Serial client tool such as Putty. In this section, you can find descriptions and default settings.

- Main Menu



- User Manager

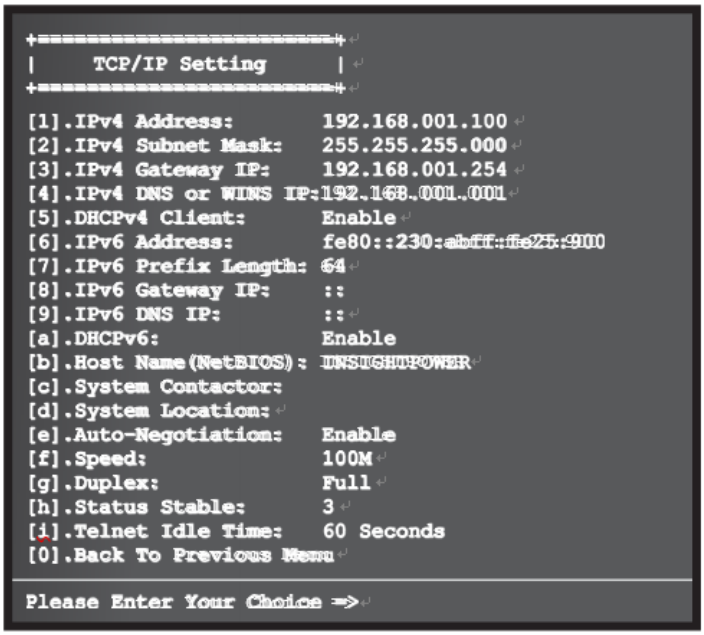


No.	Item	Description	Default
[1]	RADIUS Auth	Specify whether RADIUS login is allowed.	Disable
[2]	Server	The RADIUS server name.	
[3]	Secret	The RADIUS secret.	

No.	Item	Description	Default
[4]	Port	The RADIUS port number.	1812
[5]	Administrator Account	The default account/ password for the Administrator (case sensitive).	admin
[6]	Administrator Password		password
[7]	Administrator Limitation	Restrict Administrator login area.	Only in This LAN
[8]	Device Manager Account	The default account/ password (case sensitive) for the Device Manager. This account is only permitted to change device-related settings.	device
[9]	Device Manager Password		password

No.	Item	Description	Default
[a]	Device Manager Limitation	Restrict Device Manager login area.	Only in This LAN
[b]	Read Only User Account	The default account/ password (case sensitive) for Read Only User. This account is only allowed to view set- tings without the permission to make changes.	user
[c]	Read Only User Password		password
[d]	Read Only User Limitation	Restrict Read Only User login area.	Allow Any

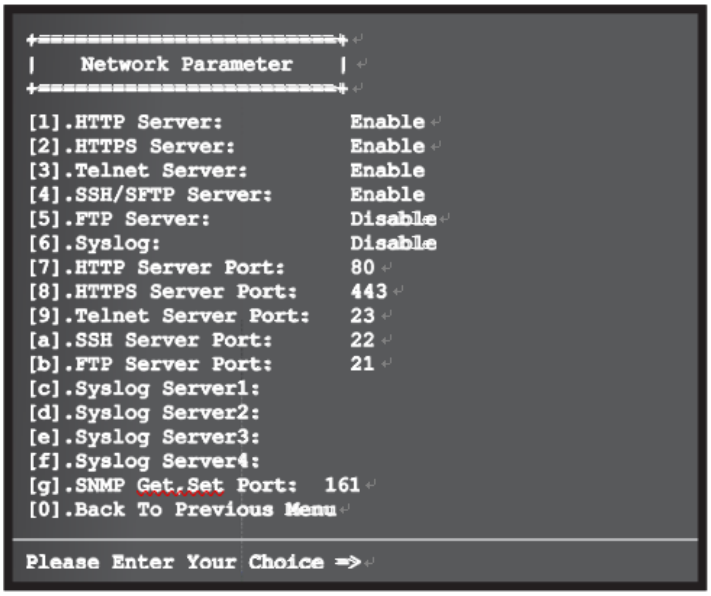
- TCP/IP Setting



No.	Item	Description	Default
[1]	IPv4 Address	The IPv4 address.	192.168.001.100
[2]	IPv4 Subnet Mask	The IPv4 subnet mask setting.	255.255.255.000
[3]	IPv4 Gateway IP	The IPv4 gateway's IP address.	192.168.001.254
[4]	IPv4 DNS or WINS IP	IPv4 Domain Name Server or WINS IP.	192.168.001.001
[5]	DHCPv4 Client	Enable/ Disable DHCPv4 protocol.	Enable
[6]	IPv6 Address	The IPv6 address.	
[7]	IPv6 Prefix Length	The IPv6 prefix length.	
[8]	IPv6 Gateway IP	The IPv6 gateway's IP address.	
[9]	IPv6 DNS IP	IPv6 Domain Name Server's IP address.	

No.	Item	Description	Default
[a]	DHCPv6	Enable/ Disable DHCPv6 protocol.	Enable
[b]	Host Name (NetBIOS)	The Host Name for the SNMP IPv6.	INSIGHTPOWER
[c]	System Contact	The System Contact information.	
[d]	System Location	The System Location information.	
[e]	Auto-Negotiation	Enable/disable automatic transfer rate (10/ 100Mbps) negotiation.	Enable
[f]	Speed	If the Auto-Negotiation is dis- abled, you can specify the transfer rate.	100M
[g]	Duplex	If the Auto-Negotiation is dis- abled, you can specify the duplex mode.	Full
[h]	Status Stable	Status change confirmation check time.	3
[i]	Telnet Idle Time	Telnet connection time-out setting.	60 Seconds

- Network Parameter

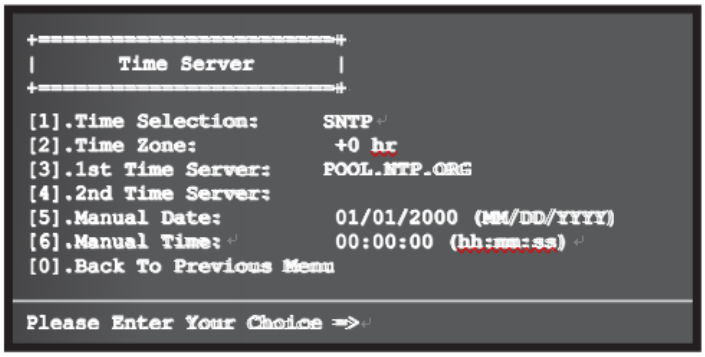


No.	Item	Description	Default
[1]	HTTP Server	Enable/ disable HTTP protocol.	Enable
[2]	HTTPS Server	Enable/ disable HTTPS protocol.	Enable
[3]	Telnet Server	Enable/ disable Telnet protocol.	Enable
[4]	SSH/ SFTP Server	Enable/ disable SSH/ SFTP protocol.	Enable
[5]	FTP Server	Enable/ disable FTP protocol.	Disable
[6]	Syslog	Enable/ disable remote Syslog.	Disable
[7]	HTTP Server Port	HTTP port.	80
[8]	HTTPS Server Port	HTTPS port.	443
[9]	Telnet Server Port	Telnet port.	23
[a]	SSH Server Port	SSH port.	22

No.	Item	Description	Default
[b]	FTP Server Port	FTP port.	21
[c]	Syslog Server 1	The Host Name of remote Syslog Server 1.	
[d]	Syslog Server 2	The Host Name of remote Syslog Server 2.	
[e]	Syslog Server 3	The Host Name of remote Syslog Server 3.	
[f]	Syslog Server 4	The Host Name of remote Syslog Server 4.	
[g]	SNMP Get, Set Port	The SNMP port.	161

- **Time Server**

  You can manually adjust time and date for the SNMP IPv6 or set up automatic time server synchronization.



No.	Item	Description	Default
[1]	Time Selection	SNTP or manual.	SNTP
[2]	Time Zone	Adjust your time zone.	+0 hr
[3]	1st Time Server	The first time server for SNTP.	POOL.NTP.ORG
[4]	2nd Time Server	The second time server for SNTP.	
[5]	Manual Date	Set the date manually.	01/01/2000
[6]	Manual Time	Set the time manually.	00:00:00

- **Soft Restart**

  Reset the SNMP IPv6. This will not affect the operation of the UPS.

- **Default Reset**

  Reset to manufacture default.

- **Exit Without Saving**

  Exit and ignore changes.

- **Save and Exit**

  Preserve your changes and exit.

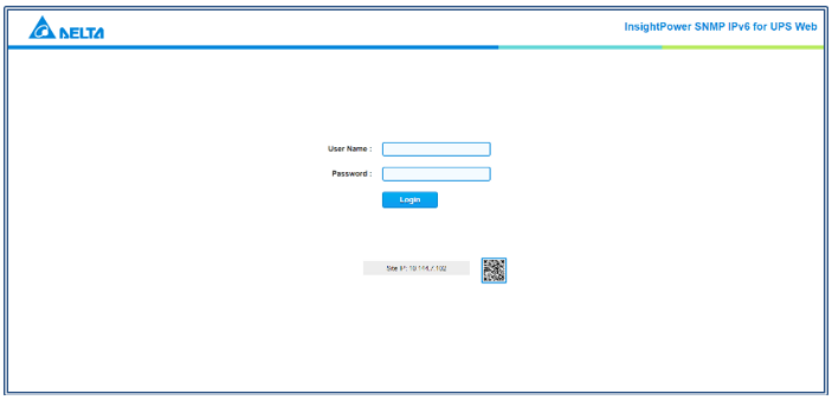
Chapter 5 : InsightPower SNMP IPv6 for UPS Web

To configure the SNMP IPv6 via the InsightPower SNMP IPv6 for UPS Web, please follow the steps below:

Step 1 Make sure that your SNMP IPv6 is connected to the LAN. Use a CAT5 network cable to connect the SNMP IPv6's Network port to the network.

Step 2 Launch your web browser. In the address bar, enter the SNMP IPv6's Host Name **http:/InsightPower/** or IP address. For encrypted connection, enter **https://InsightPower/ or https://192.168.1.100/**.

Step 3 When connection is established, the login page appears. Enter your account and password (default: admin/ password).



The **InsightPower SNMP IPv6 for UPS Web** includes the information of **Monitor, Device** and **System**. Please refer to the following sections ***5.1 Monitor~ 5.3 System*** for more information.

NOTE:

1. If you have previously changed the SNMP IPv6's Host Name or IP address, please connect with new settings.
2. If the login page is accessible, but you are unable to log in with correct account and password, additional network configuration may be needed. The cause could be the IP subnet of the computer you are logging into is different from the SNMP IPv6's. To solve this issue, please refer to *Chapter 7: Troubleshooting Q2*.
3. The SNMP IPv6 will automatically log off idle connections after 30 minutes.

5.1 Monitor

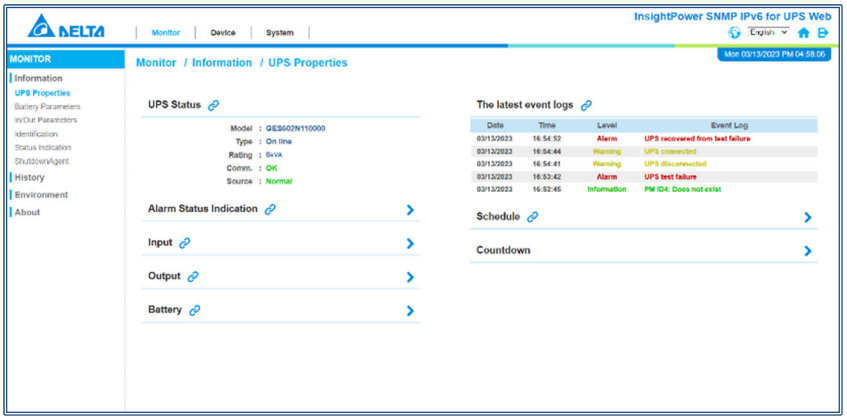
Under the Monitor category, there are Information, History and Environment these three items.

5.1.1 Information

This includes the information of UPS Properties, Battery Parameters, In/ Out Parameters, Identification, Status Indication, and ShutdownAgent. Please note that since different UPSs provide different information, the UPS that you have may not display the same web page.

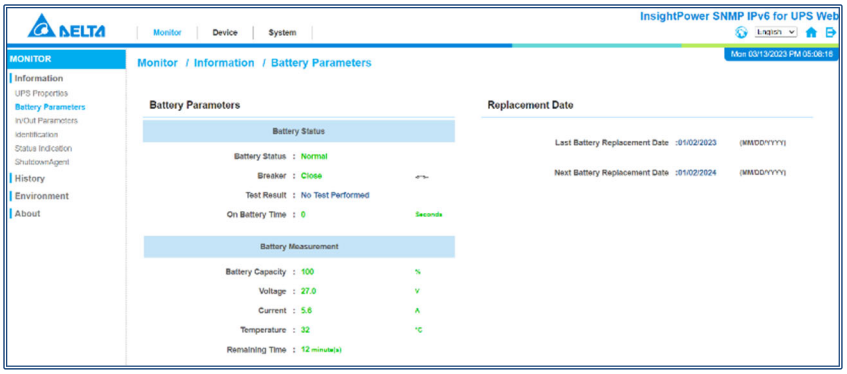
- **UPS Properties**

  Go to **Monitor** → **Information** → **UPS Properties** to see a status overview of the UPS's major parameters. The values will be updated automatically.



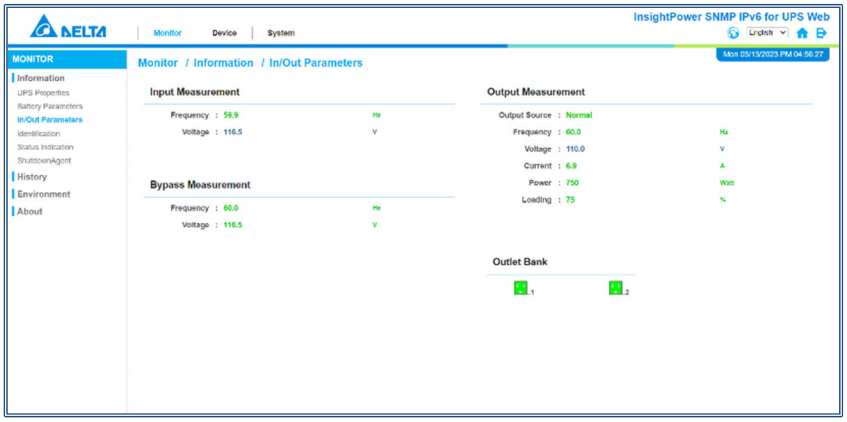
- **Battery Parameters**

  Go to **Monitor** → **Information** → **Battery Parameters** to view the information of Battery Status, Battery Measurement, Battery Replacement Date.



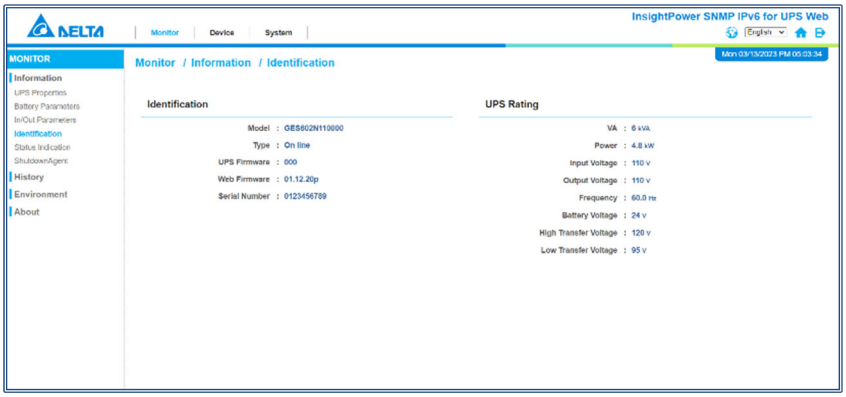
- **In/ Out Parameters**

  Go to **Monitor → Information → In/ Out Parameters** to view the information of Input Measurement, Bypass Measurement, Output Measurement and Outlet Bank.



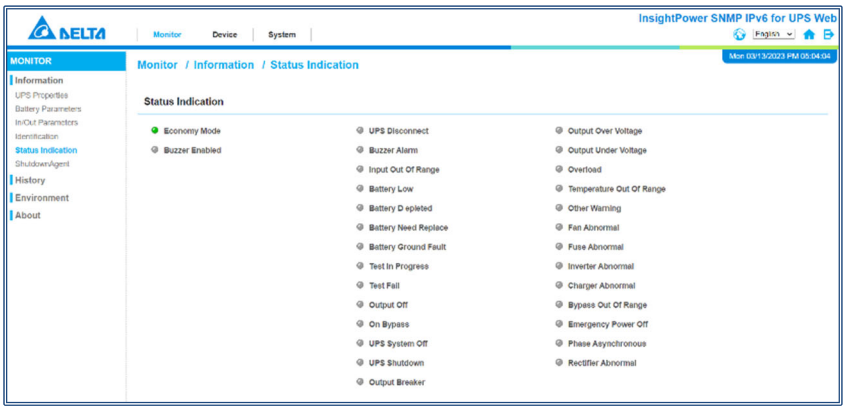
- **Identification**

  Go to **Monitor → Information → Identification** to view the information of Identification and UPS Rating.



- **Status Indication**

  Go to **Monitor** → **Information** → **Status Indication** to view the UPS's event list. When an event occurs, its according beacon lights green.

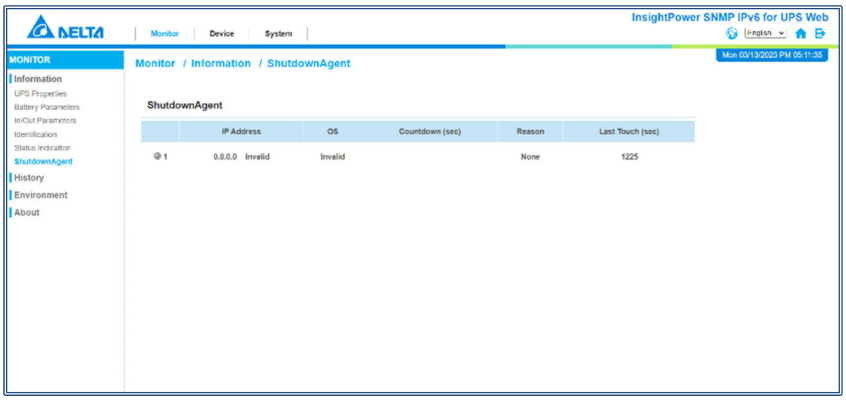


- **ShutdownAgent**

  Go to **Monitor** → **Information** → **ShutdownAgent** to view your designated PCs' shutdown information, including IP Address, OS (operation system), Countdown, Reason and Last Touch.

  Please note that the page only appears if:

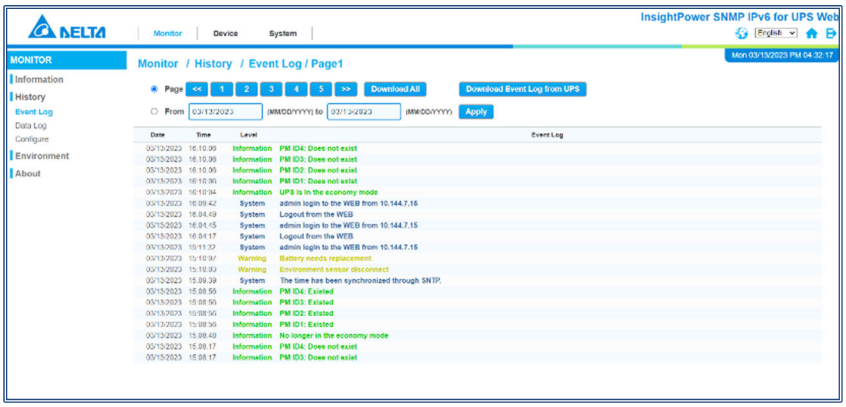
  - Your PCs have connected to a UPS using this SNMP IPv6.
  - Your PCs have installed ShutdownAgent 2012 software.
  - You have went to **System** → **Administration** → **SNMP Trap** to specify your PCs' IP Addresses in the Target IP bar and selected 'ShutdownAgent 2012' from Event Level's pull-down menu.



5.1.2 History

- **Event Log**

  Go to **Monitor** → **History** → **Event Log** → Page 1/ 2/ 3/ 4... to see events that occur. The existing ones are overwritten when the maximum number of entries (1,000) is reached. You can also download the entire event log archive (event_log.xls) recorded during an assigned period of time on your computer.

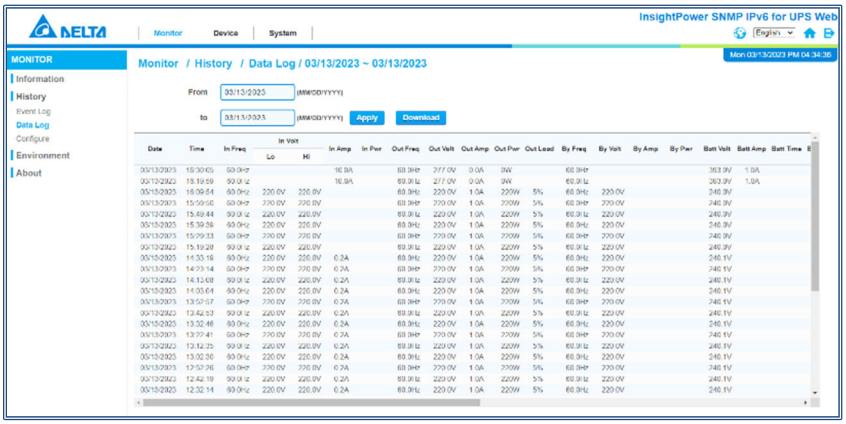


  - **Date:** The date when the event occurred.
  - **Time:** The time when the event occurred.
  - **Level:** The Event Level of the event occurred.
  - **Event Log:** The description of the event that occurred.
  - **Download Event Log from UPS**

    The SNMP IPv6 sends a request to the UPS, collects the event logs saved in the UPS, and replies to the user through network. Please note that this option only appears when the UPS supports this function, and the event logs saved in the UPS may be different from the event logs saved in the SNMP IPv6.

- **Data Log**

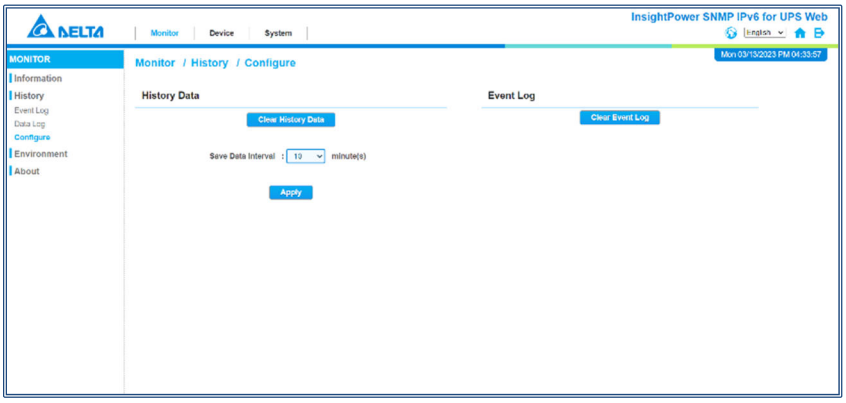
  Go to **Monitor** → **History** → **Data Log** to see all saved device data. You can also download the data archive (data_log.xls) recorded during an assigned period of time on your computer.



- **Date:** The date when the data entry is recorded.
- **Time:** The time when the data entry is recorded.

- **Configure**

  Go to **Monitor** → **History** → **Configure** to clear the history data and event log. You can also assign the Save Data Interval.



- **Clear History Data:** Empty the history data log only.
- **Clear Event Log:** Empty the event log only.
- **Save Data Interval:** The time interval after which an event/ data entry is recorded.

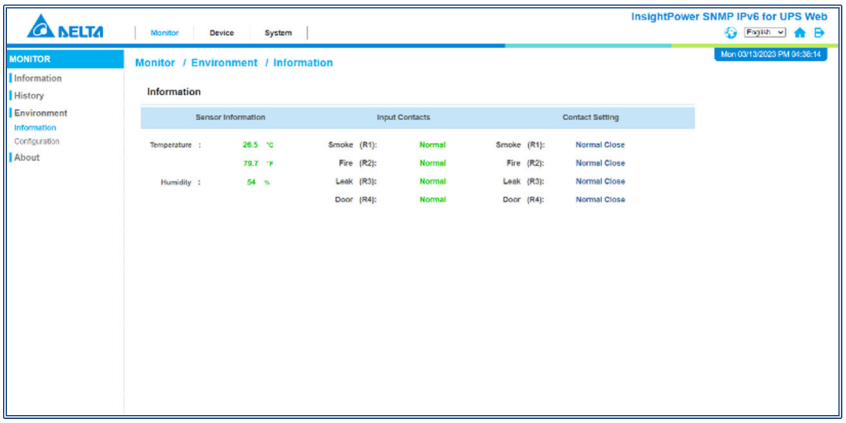
5.1.3 Environment

Only when an EnviroProbe is used can the Environment page show up. Please note that the SNMP IPv6's DIP switch 1 should be set to the **ON** position and DIP switch 2 should be set to the **OFF** position when you use an EnviroProbe.

The Environment page includes Information and Configuration these two items. You can monitor and set up your EnviroProbe via this Environment page. For EnviroProbe information, please refer to the Installation Guide included in the package of the EnviroProbe.

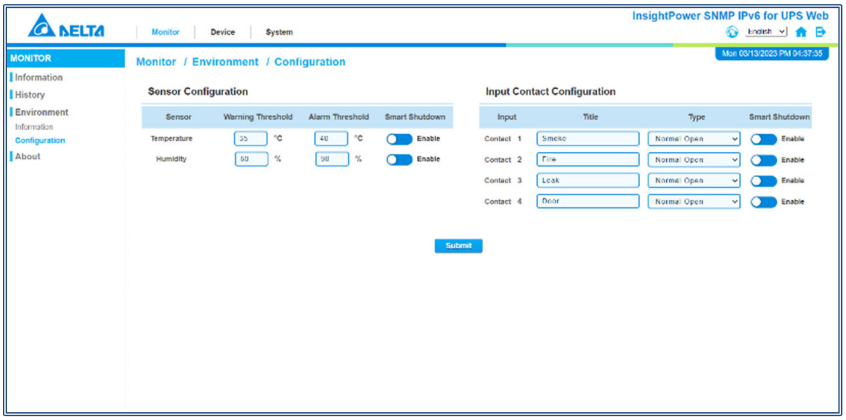
- **Information**

  Go to **Monitor** → **Environment** → **Information** to see your EnviroProbe's Sensor Information, Input Contacts and Contact Setting.



- **Configuration**

  Go to **Monitor** → **Environment** → **Configuration** to configure your EnviroPobe's Warning Threshold, Alarm Threshold, Title and Type. Please see the table below for detailed information.

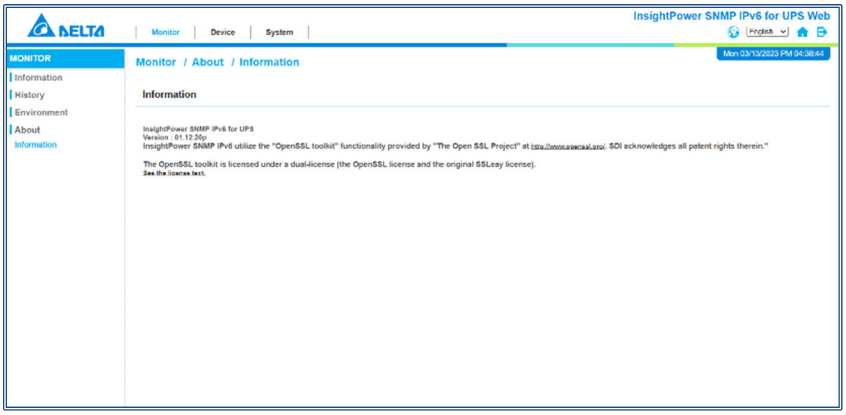


5.1.4 About

Under About category, there is only one item called Information. You can obtain your SNMP IPv6's other information via this channel.

- **Information**

  Go to **Monitor** → **About** → **Information** to see the version of your InsightPower SNMP IPv6 for UPS and other information about OpenSSL toolkit and licenses.

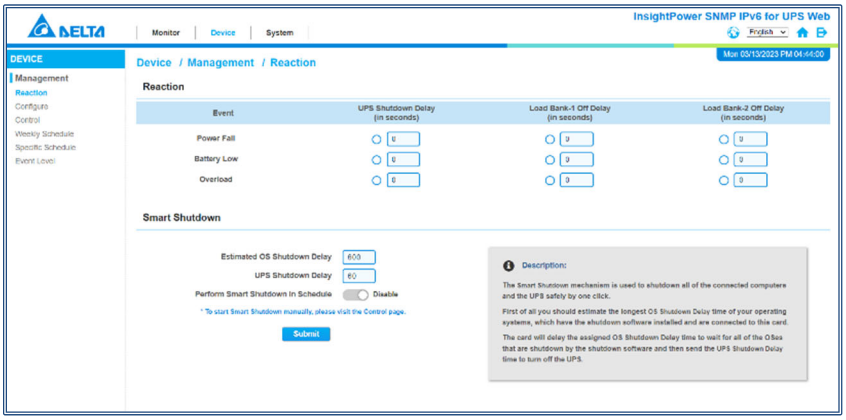


5.2 Device

5.2.1 Management

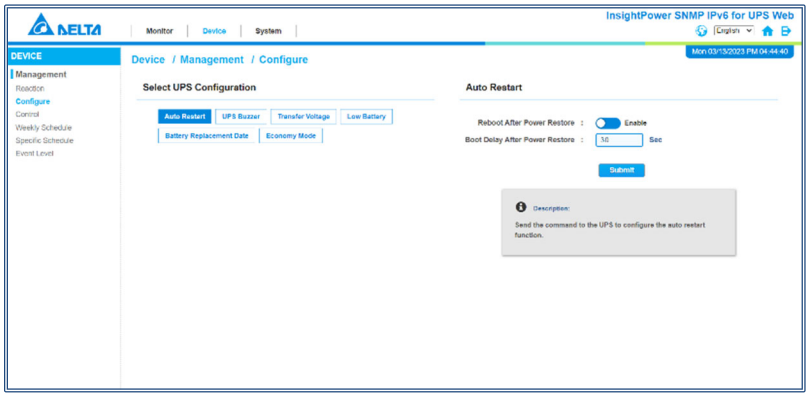
Since different UPSs have different functions, your UPS may not support the same configurations or control items stated below.

- **Reaction**



- **Configure**

  Go to **Device** → **Management** → **Configure** to configure the UPS. The configuration values are saved in the UPS or in the SNMP IPv6 and these values change UPS operation. The configuration items include the following. Please note that different UPSs may support different configuration options.



  - **Auto Restart**

    After you click **Submit** to confirm your auto restart setup, the SNMP IPv6 will send the command to the UPS to enable auto restart.

  - **UPS Buzzer**

    After you click **Submit** to confirm your buzzer setup, the SNMP IPv6 will send the command to the UPS to enable buzzer.

  - **Voltage Sensitivity**

    After you set up your voltage sensitivity (there are Normal, Reduced, and Low selections) and click **Submit**, the SNMP IPv6 will send the command to the UPS to enable the UPS's voltage sensitivity function.

  - **Transfer Voltage**

    After you click **Submit** to confirm your transfer voltage setup, the SNMP IPv6 will send the command to the UPS to enable the relevant functions.

  - **Low Battery**

    This configuration saves the setup values in the SNMP IPv6 and compares with the values received from the UPS. If the received battery level is lower than the assigned one, the SNMP IPv6 will trigger a low-battery alarm.

- **UPS Shutdown Action**

  This configuration saves your setup values in the SNMP IPv6 and compares with the values received from the UPS. If an event like power failure or low battery occurs, the SNMP IPv6 will send the assigned shutdown delay command to the UPS.

- **Smart Shutdown**

  The Smart Shutdown configuration is used to safely shutdown all of the connected computers and the UPS. First of all, you should estimate the longest OS Shutdown Delay time for your operating systems that have been in- stalled shutdown software and connected to the SNMP IPv6. The SNMP IPv6 will delay the assigned OS Shutdown Delay time and wait for all operating systems' shutdown. After that, the SNMP IPv6 will send the assigned UPS shutdown-delay command to the UPS and turn off the UPS.

- **Battery Replacement Date**

  After you set up battery replacement dates, the SNMP IPv6 will send the command to the UPS and save the information in the UPS.

- **External Battery Pack**

  After you click **Submit** to confirm your external battery pack setup, the SNMP IPv6 will send the command to the UPS and save the external battery pack quantity in the UPS.

- **Bypass Transfer Frequency**

  After you set a tolerance of bypass transfer frequency and confirm your set- up, the SNMP IPv6 will send the command to the UPS. If the UPS transfers to bypass mode and the bypass frequency is out of the tolerance, output will be turned off and critical loads will be protected.

- **Bypass Transfer Voltage**

  After you set a tolerance of bypass transfer voltage and confirm your setup, the SNMP IPv6 will send the command to the UPS. If the UPS transfers to bypass mode and the bypass voltage is out of the tolerance, output will be turned off and critical loads will be protected.

- **Periodic Auto Test**

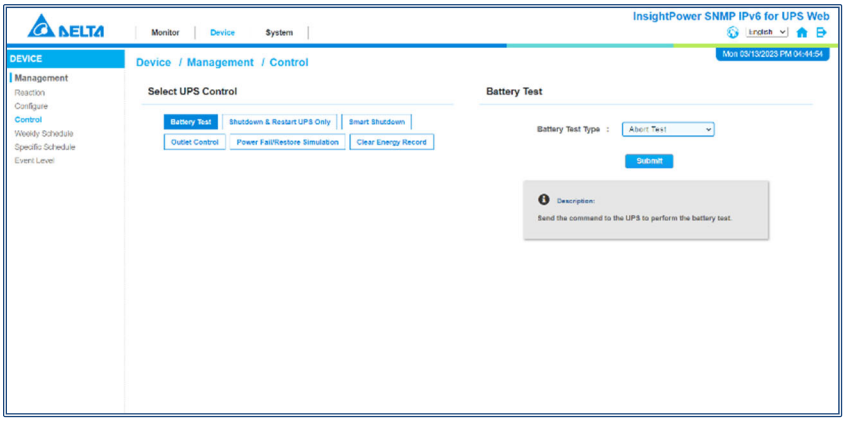
  This configuration is used to set up battery test time. After you confirm your setup, the SNMP IPv6 will send the command to the UPS and save the setup in the UPS. When the test time is due, the UPS will automatically perform the battery test.

- **Output Dry Contacts**

  After you click **Submit** to confirm your setup of output dry contacts, the SNMP IPv6 will send the command to the UPS, save the values in the UPS, and report the current UPS's status.

- **Control**

  Go to **Device** → **Management** → **Control** to configure relevant control commands. After you click **Submit**, the SNMP IPv6 will send the according commands to the UPS to enable relevant functions. The control items include the following.



- **Battery Test**

  After you select the battery test type and click **Submit**, the SNMP IPv6 will send the command to the UPS to enable the battery test accordingly.

- **Shutdown & Restart UPS Only**

  After you confirm your setup, the SNMP IPv6 will send the command to the UPS to shut down or/ and restart the UPS.

  If you want to shut down the UPS, please check the UPS Shutdown Delay box and key in delay time.

  If you want to restart the UPS, please check the UPS Restart Delay box and key in delay time.

  If you want to shut down and restart the UPS, please check both of the boxes and key in delay time.

- **Smart Shutdown**

  The Smart Shutdown configuration is used to safely shutdown all of the connected computers and the UPS. First of all, you should estimate the longest OS Shutdown Delay time for your operating systems that have been installed shutdown software and connected to the SNMP IPv6. The SNMP IPv6 will delay the assigned OS Shutdown Delay time and wait for all operating systems' shutdown. After that, the SNMP IPv6 will send the assigned UPS shutdown-delay command to the UPS and turn off the UPS.

- **Outlet Control**

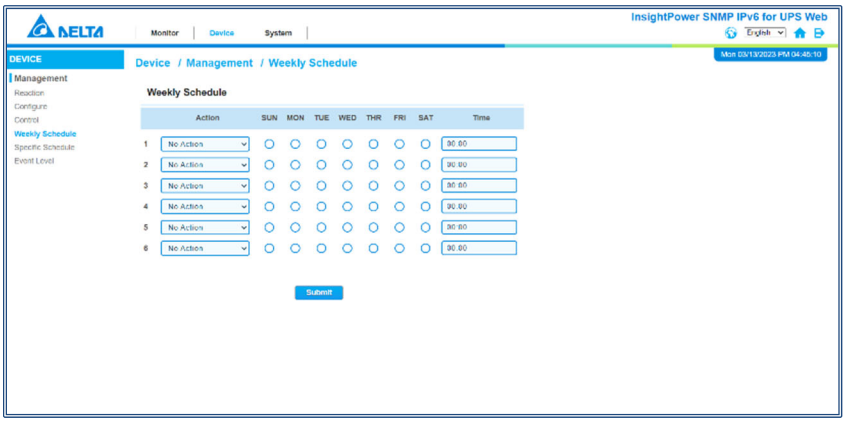
  Press the **Switch Bank** button to control the UPS output relay (on or off).

- **Power Fail/ Restore Simulation**

  Click **Power Fail Test** or **Power Restore Test** button to let the SNMP IPv6 simulate UPS power failure or power restore event. This function allows you to test all of the connected software and verify whether they work properly or not. Please note that the simulation won't influence UPS operation, the UPS remains in its original operation mode and won't transfer to battery mode.

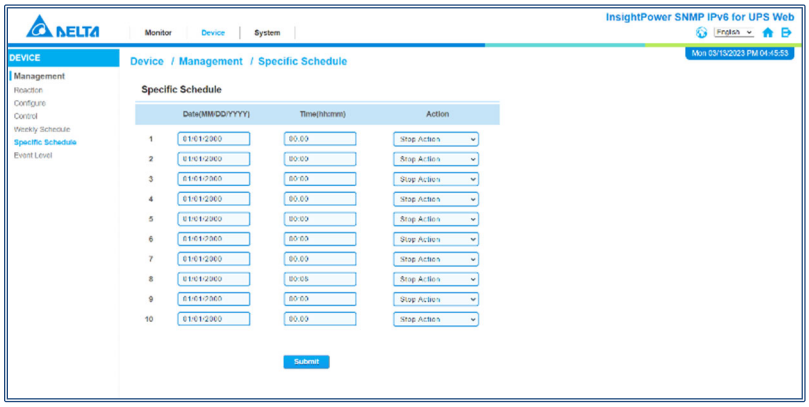
- **Weekly Schedule**

  Go to **Device → Management → Weekly Schedule** to arrange a weekly schedule for the UPS. You can select **No Action, Shutdown, Restart, 10-Second Test**, and set up what day and what time you want the action to be executed.



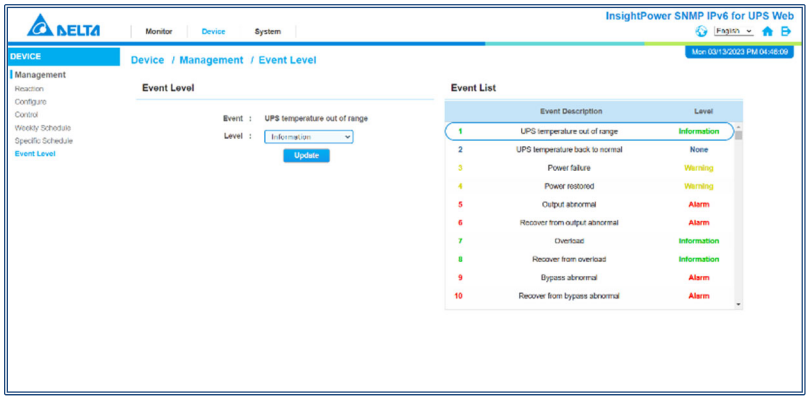
- **Specific Schedule**

  Go to **Device → Management → Specific Schedule** to arrange a specific schedule for the UPS. You can set up a specific date **(MM/ DD/ YYYY)** and time **(hh:mm)** for a specific action **(Stop Action, Shutdown, Restart, 10-Second Test and Deep Battery Test)**.



- **Event Level**

  Go to **Device → Management → Event Level** to set up a level for an event. If you want to receive an event notification, please refer to ***5.3.3 Notification - SNMP Trap*** and ***5.3.3 Notification - Mail Server***.



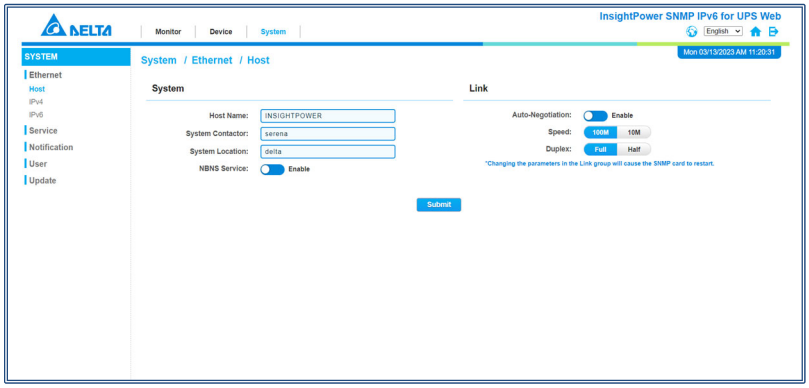
5.3 System

Only Administrator can see the System page. Under the System category, there are Ethernet, Service, Notification, User and Update these five items. You can use them to change or look up the system's relevant settings or records. Please see below for more descriptions.

5.3.1 Ethernet

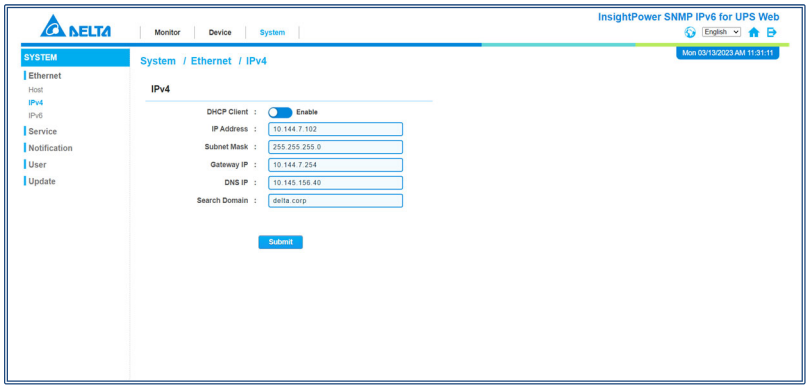
The Ethernet page includes Host, IPv4 and IPv6 these three items. It allows Administrator to configure local network parameters for the SNMP IPv6.

- Host



  - System
    1) **Host Name:** The SNMP IPv6 Host Name on the network.
    2) **System Contact:** System contact information.
    3) **System Location:** System location information.
    4) **NBNS Service:** Enable/ disable NBNS service.
  - Link
    1) **Auto-Negotiation:** Enable/ Disable automatic transfer rate (10/ 100M bps) negotiation.
    2) **Speed:** If the Auto-Negotiation is disabled, you can specify the transfer rate.
    3) **Duplex:** If the Auto-Negotiation is disabled, you can specify the duplex mode.

- **IPv4**



  - **TCP/ IP Settings for IPv4**

    1) **DHCP Client:** Enable/ Disable DHCP. If enabled, DHCP server automatically assigns an IP address to the SNMP IPv6.

    2) **IP Address:** The IP address in dotted format.

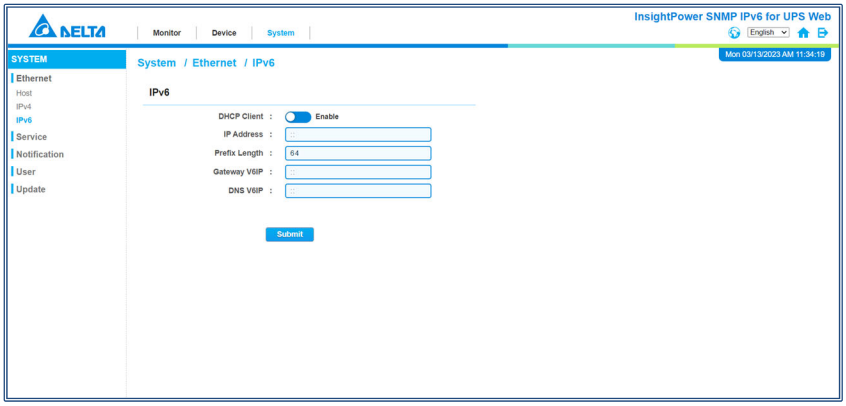
    3) **Subnet Mask:** The Subnet Mask for your network.

    4) **Gateway IP:** The IP address for network gateway in dotted format.

    5) **DNS IP:** The IP address Domain Name Server in dotted format.

    6) **Search Domain:** If the Host Name you provided cannot be found, the system appends the search domain to your Host Name.

- **IPv6**



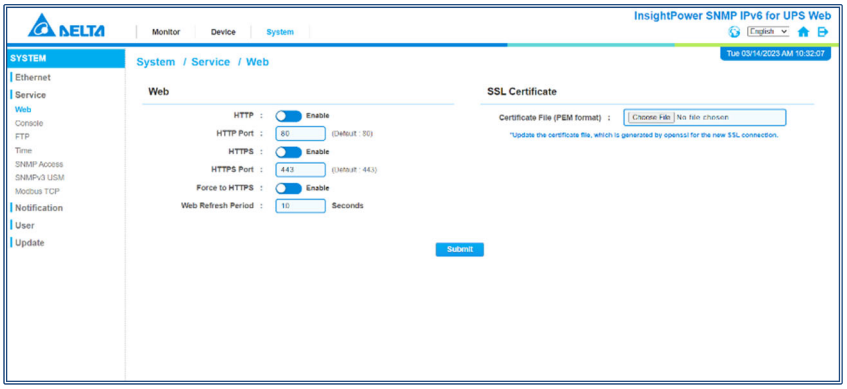
- **TCP/ IP Settings for IPv6**

  1) **DHCP Client:** Enable/ Disable DHCP. If enabled, DHCP server automatically assigns an IP address to the SNMP IPv6.
  2) **IP Address:** The IPv6 address.
  3) **Prefix Length:** The prefix length for the IPv6 address.
  4) **Gateway V6IP:** The IP address for the IPv6 network gateway.
  5) **DNS V6IP:** The IP address for the IPv6 domain name server.

5.3.2 Service

- **Web**

  The **Web** page allows Administrator to configure Web service settings.



- **Web**

  1) **HTTP:** Enable/ disable HTTP connection.
  2) **HTTP Port:** Assign a HTTP port number (default: 80).
  3) **HTTPS:** Enable/ disable HTTPS connection.
  4) **HTTP Port:** Assign a HTTP port number (default: 443).
  4) **Force to HTTPS:** Force the WEB to use HTTPS.
  5) **Web Refresh Period:** Web refresh interval.

- **SSL Certificate**

  1) To ensure connection security between the SNMP IPv6 and the connecting workstation, SSL certificate can be used to encrypt and secure the integrity of transmitting data.

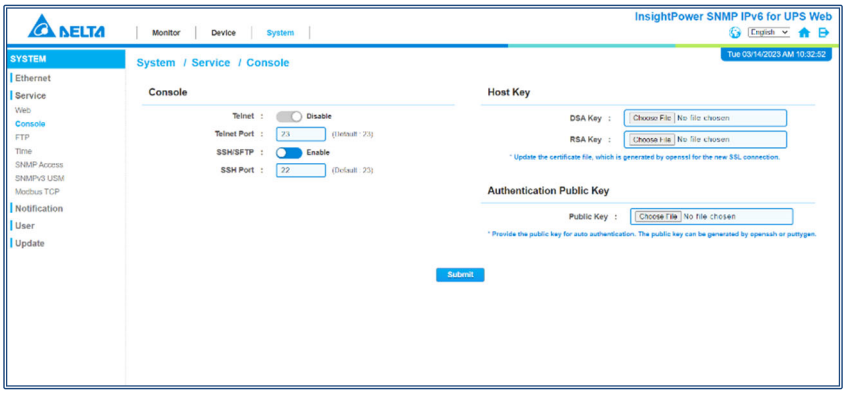
2) **Certificate File:** This allows you to replace your own SSL certificate file. The SNMP IPv6 supports PEM format which is generated by OpenSSL. Click **Choose File** to upload a certificate file.

NOTE:

For more information about generating a private SSL certificate file, please refer to *Chapter 7: Troubleshooting Q11*, or visit http://www.openssl.org/.

- **Console**

  This item allows the Administrator to enable or disable Telnet/ SSH communication protocols.



  - **Telnet:** Enable/ disable Telnet connection.
  - **Telnet Port:** Assign a Telnet port number (default: 23).
  - **SSH/ SFTP:** Enable/ disable SSH/ SFTP connection.
  - **SSH Port:** Assign an SSH protocol port number (default: 22).
  - **Host Key/ Authentication Public Key:**

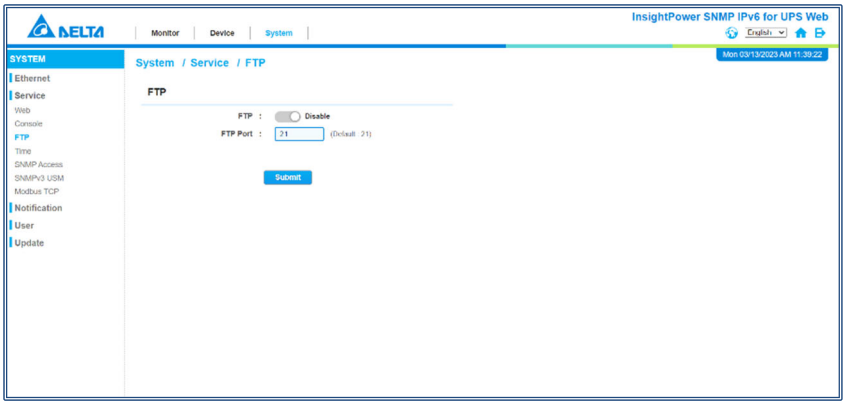
    This allows you to replace your own SSH keys. The SNMP IPv6 supports key files generated by OpenSSH, including DSA, RSA, and Authentication Public Keys. How to generate DSA, RSA, and Authentication Public keys for SSH, please refer to *Chapter 7 : Troubleshooting Q12*. You can use this page or SFTP protocol to upload key files. For detailed information, please refer to *Chapter 7 : Troubleshooting Q13*.

    NOTE:

    For cyber security considerations, it is suggested that you disable Telnet and enable SSH where possible.

- **FTP**

  The **FTP** page allows Administrator to enable/ disable FTP communication protocol.



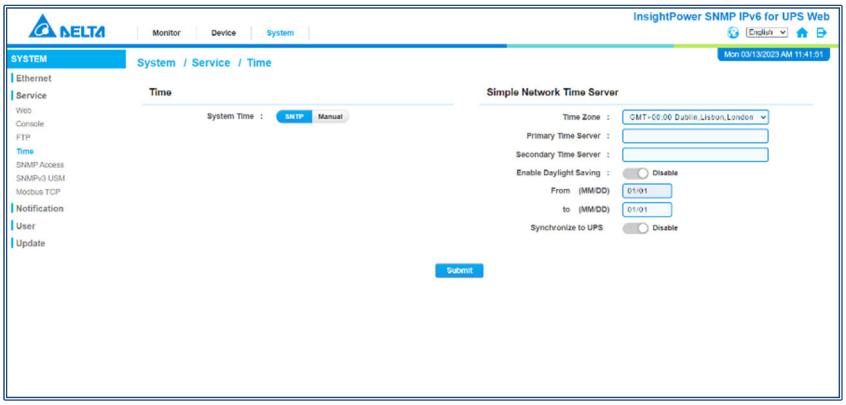
  - **FTP:** Enable/ disable FTP connection.
  - **FTP Port:** Assign an FTP port number (default: 21).

NOTE:

For cyber security considerations, it is suggested that you disable FTP and use SFTP instead.

- **Time**

  You can manually set the time and date or allow automatic time synchronization with SNTP servers. Please note that if the SNTP server is not responsive, the event and data log will not register even when SNTP is enabled.



- **Time**

  If a time server is not accessible, you can still manually set time and date. Please note that every time you restart the SNMP IPv6's network module, time and date is reinstated to previous assigned settings.

- **Simple Network Time Server**

  1) **Time Zone:** From the dropdown menu, select the time zone for the location where the SNMP IPv6 is located.

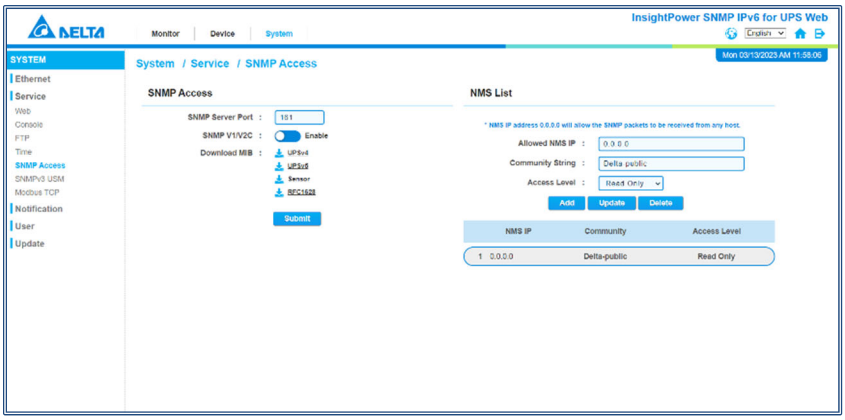
  2) **Primary/ Secondary Time Server:** Two time servers can be added. Every 60 minutes, the SNMP IPv6 synchronizes with the first responding server.

  3) **Enable Daylight Saving:** Enable or disable daylight saving time. During this period, the SNMP IPv6 adjusts time forward one hour.

  4) **Synchronize to UPS:** Enable or disable UPS automatic time synchronization with the SNMP IPv6.

- **SNMP Access**

  The SNMP IPv6 supports SNMP protocol and SNMP NMS (Network Management System), which are commonly used to monitor network devices for conditions that call for administrative attention. To prevent unauthorized access, you can specify the NMS IP addresses that are allowed to access, their community strings and access levels. The maximum number of IP entries is 256.

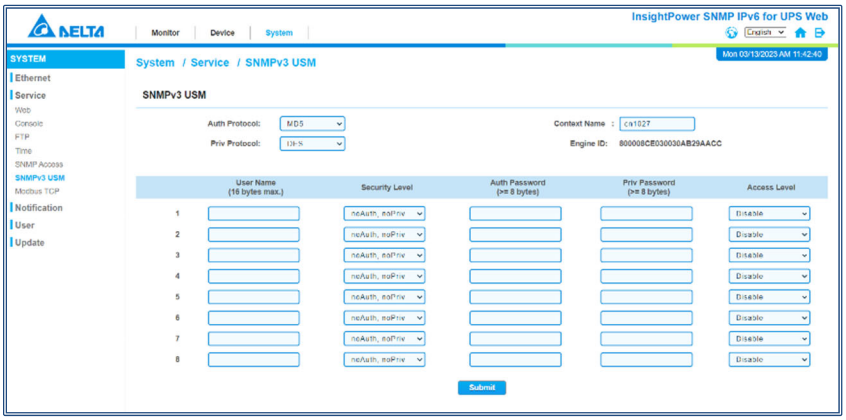


NOTE:

1. If IP address **0.0.0.0** is enlisted, the NMS IP access restriction is ignored. The SNMP IPv6 checks the community string to identify the access level and permission according to your setting.
2. For cyber security considerations, it is suggested that you disable SNMP V1/ V2C.

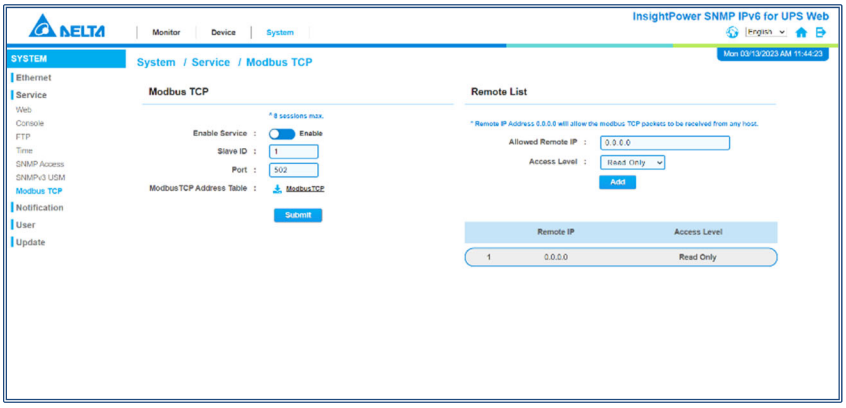
- **SNMPv3 USM**

  SNMPv3 offers features such as the encryption of packets and authentication to improve security. The SNMPv3 USM (User Session Management) allows you to assign eight User Names whose access is granted via SNMPv3 protocol. You can also define their respective Security Levels, Auth Passwords, Priv Passwords and Access Levels.



- **Modbus TCP**

  The SNMP IPv6 supports Modbus TCP service for remote monitoring.



- **Modbus TCP**

  1) **Enable Service:** Enable/ disable Modbus TCP service.
  2) **Slave ID:** The unique ID of the SNMP IPv6.
  3) **Port:** The port for Modbus TCP communication.
  4) **Modbus TCP Address Table:** The download link for the Modbus TCP address table.

- **Remote List**

  1) **Allowed Remote IP:** The remote IP that is allowed for Modbus TCP communication. The IP address 0.0.0.0 represents that it allows to receive the Modbus TCP packets from any host.

  2) **Access Level:** Disable/ Read Only/ Read Write.

  NOTE:

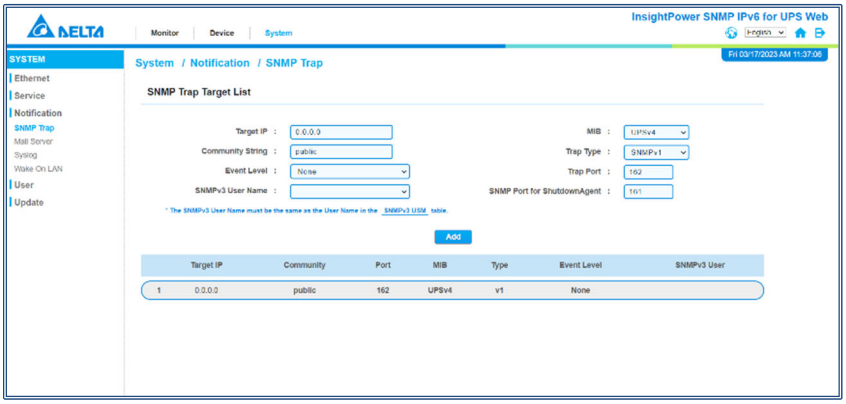
  For cyber security considerations, it is suggested that you configure the allowed remote specified IP and required access level to prevent unauthorized access.

5.3.3 Notification

The **Notification** page includes SNMP Trap, Mail Server, Syslog and Wake On LAN these four items.

- **SNMP Trap**

  SNMP Trap alerts users to event occurrences in your monitored environment. To enable SNMP Trap, you must add Target IP addresses to the Target IP list. Specify the Community String, Trap Type, MIB, SNMPv3 User Name, Trap Port, Event Level, SNMP Port for ShutdownAgent and click **Add**. If you wish to update or delete a Target IP address, specify the IP address in the Target IP list, and click **Update** or **Delete**.



NOTE:

The SNMP IPv6 supports SNMPv1, SNMPv2c and SNMPv3 traps to satisfy most of customers' environments. If you select the SNMPv3 trap, please specify an SNMPv3 USM User Name.
You can use Event Level to determine what event notifications should be sent to which Target IP Address. Five event levels are listed as follows:

None: No event notifications are sent to the target address.

Information: All event notifications are sent to the target address.

Warning: Both Warning and Alarm event notifications are sent to the target address.

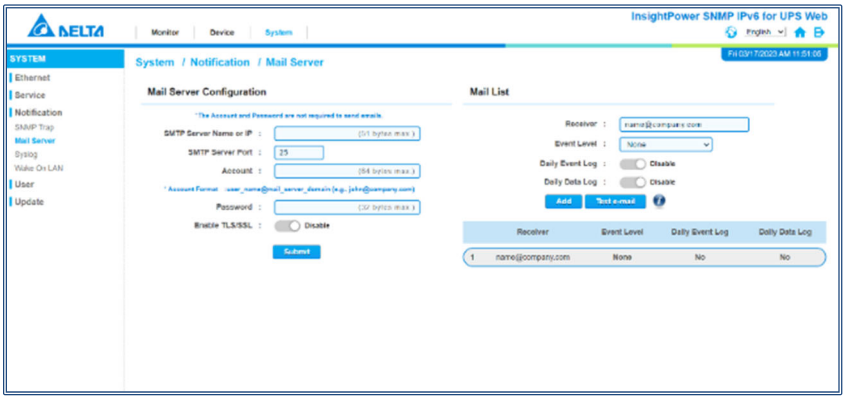
Alarm: Only Alarm event notifications are sent to the target address.

ShutdownAgent: All event notifications are sent to the target address, and you can go to **Monitor** → **Information** → **Shutdown-Agent** to review your designated PCs' shutdown information.

You can go to **Device** → **Management** → **Event Level** to change the event level.

- **Mail Server**

You can set up an SMTP Server and specify a list of E-mail recipients who will receive notifications when events occur. The maximum number of recipients is 256.



NOTE:

1. If a DNS server is not available in the network, please manually assign an SMTP server address (xxx.xxx.xxx.xxx) to enable the E-mail notification system.
2. If the SMTP service settings are complete, please click the '**Test email**' button to confirm whether the SMTP settings are correct.

- **SMTP Server Name or IP**

  If a Host Name is entered, a **DNS IP** should be added in **TCP/ IP**. Please see *5-3-1 Ethernet*.

- **SMTP Server Port**

  The port for the SMTP server.

- **Account**

  The mail server login account.

- **Password**

  The mail server login password.

- **Enable TLS/ SSL**

  Enable/ disable SMTP encryption.

- **Receiver**

  The recipients' Email addresses.

- **Event Level**

  Select the Event Level that when triggered, an E-mail notification is sent to the corresponding recipient.

  1) **Information:** All event notifications are sent to the target address.
  2) **Warning:** Warning and Alarm event notifications are sent to the target address.
  3) **Alarm:** Only Alarm event notifications are to the target address.

- **Daily Event Log**

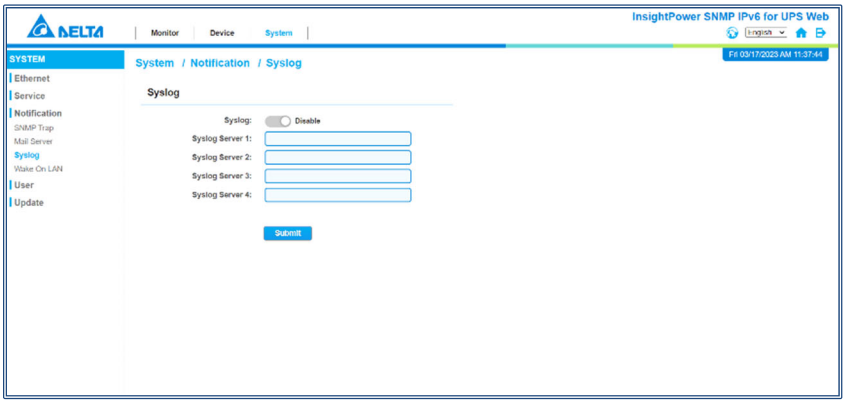
  Enable/ disable the system to send the daily event log to the recipients' E-mail addresses.

- **Daily Data Log**

  Enable/ disable the system to send the daily data log to the recipients' E-mail addresses.

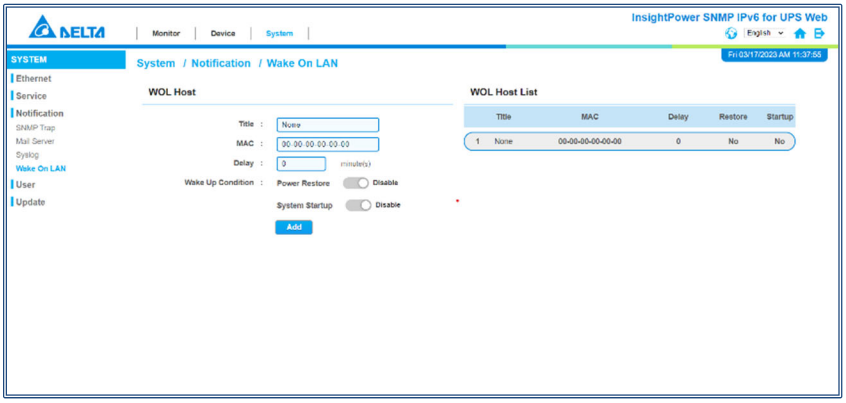
- **Syslog**

  Syslog is used to store the event log on remote Syslog servers. This will not affect the local event log. After enabling the Syslog, please set up a server IP address. You can set up at maximum four Syslog servers at a time.



- **Wake On LAN**

  Wake On LAN function can start up clients' PCs from network with MAC address, and you can set up at maximum 256 MAC addresses. The configuration can wake up clients' PCs after power restores or the SNMP IPv6 starts up.

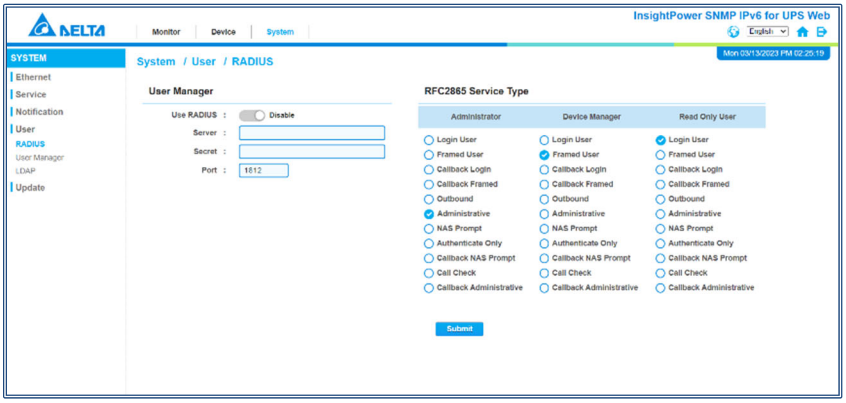


5.3.4 User

The **User** page includes RADIUS, User Manager and LDAP these three items.

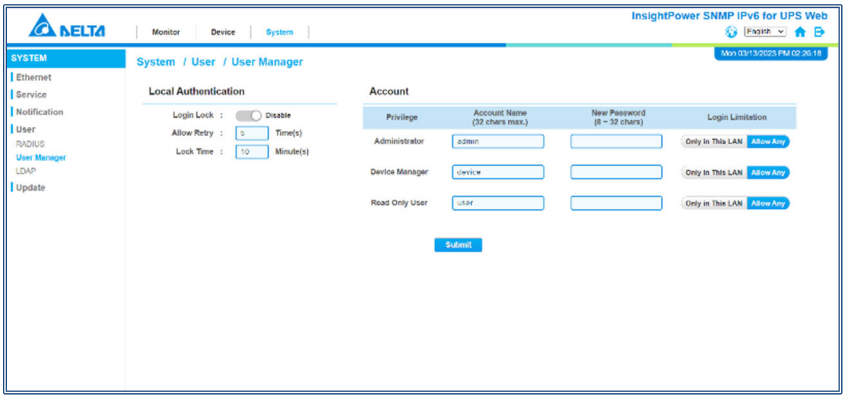
- **RADIUS**

  The SNMP IPv6 supports RADIUS. To enable the **Use RADIUS**, key in required information including **Server, Secret** and **Port** (default: 1812) and click **Submit** to enable RADIUS.



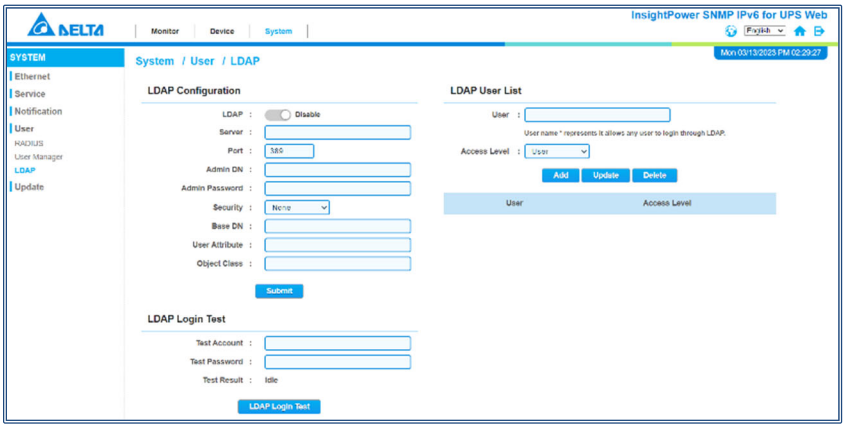
- **User Manager**

  You can manage accounts for Administrator, Device Manager and Read Only User. If RADIUS is disabled, you can still manage the Account Name, Password and Login Limitation for Local Authentication.



- **LDAP**

  The SNMP IPv6 supports LDAP authentication and provides LDAP Login Test to test the correction of LDAP configuration. The SNMP IPv6 also provides LDAP User List for defining LDAP user accounts that are allowed to log in and their access levels.



- LDAP Configuration
  1) **LDAP:** Enable/ disable LDAP authentication. If it is enabled, remote users can log in through LDAP.
  2) **Server:** The IP address or hostname of LDAP server.
  3) **Port:** The port of LDAP server (default: 389).
  4) **Admin DN:** Admin Distinguished Name (the service account used to access the LDAP server to search LDAP user accounts).
  5) **Admin Password:** Password for the service account to access the LDAP server.
  6) **Security:** Enable/ disable StartTLS/ TLS encryption.
  7) **Base DN:** Base Distinguished Name (the base path for searching LDAP user accounts, for example: *dc=test, dc=com*).
  8) **User Attribute:** Authenticate the user credentials (for example: *sAMAccountName or CN*).
  9) **Object Class:** Authenticate the user credentials (for example: *Person*)
- LDAP Login Test
  1) **Test Account:** LDAP user account for login test.
  2) **Test Password:** LDAP user password for login test.
  3) **Test Result:** Idle/ Success/ Fail/ Timeout.

- **LDAP User List**

  1) **LDAP:** LDAP user account that is allowed to log in. The mark '*' represents that it accepts all accounts to log in using the assigned access level.

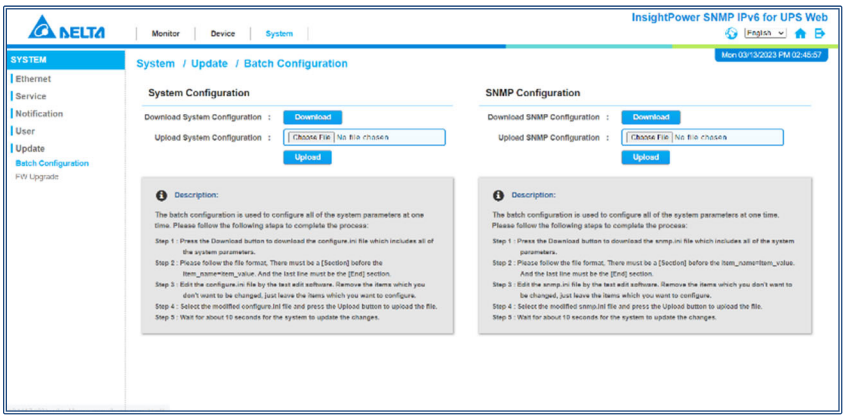
  2) **Access Level:** Access level of LDAP user account (User/ Device/ Admin).

5.3.5 Update

The **Update** page includes Batch Configuration and FW Upgrade these two items.

- **Batch Configuration**

  The SNMP IPv6 provides batch configuration to allow quick and effortless setup on multiple SNMP devices. You can duplicate settings by exporting configuration files from the SNMP IPv6 that you have successfully configured and import the configuration files on other devices.



NOTE:

If the IP address is static and you wish to copy settings to other devices on the same LAN, you must manually remove the following line **IP=xxx.xxx.xxx.xxx** under the [System] section from the exported configuration file. You can open the configuration file with text editors such as Notepad and WordPad. To modify/ assign IP address for the SNMP IPv6, please see *Chapter 4: System Configurations*.

- **System Configuration**

  The **System Configuration** includes all settings about system, Ethernet, accounts, time, etc. To download a configuration file, simply click **Download**. To upload a configuration file, click **Choose File**, select the file you wish to upload, and click **Upload**.

- **SNMP Configuration**

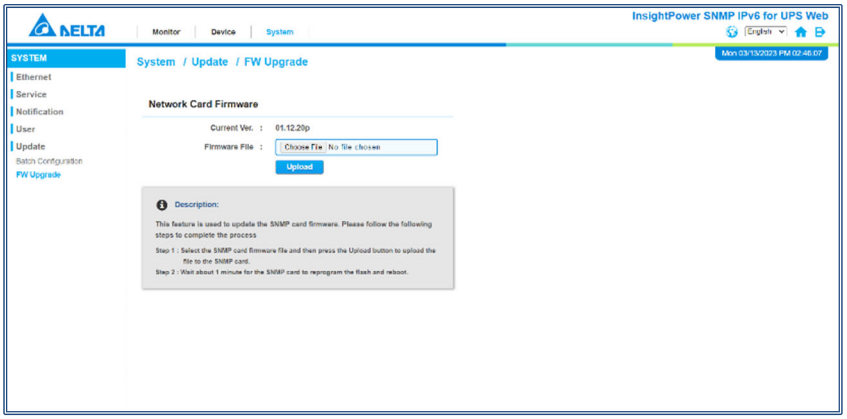
  The **SNMP Configuration** includes all settings about the SNMP protocol. To download a configuration file, simply click **Download**. To upload a configuration file, click **Choose File**, select the file you wish to upload, and click **Upload**.

  NOTE:

  If you need to modify the command lines, please do not delete the unmodified ones. They should be left intact to assure the integrity of the configuration file.

- **FW Upgrade**

  The **FW Upgrade** page shows the SNMP IPv6's current firmware version. The Administrator can use this page to update the SNMP IPv6's firmware. Click **Choose File**, select the file you wish to upload, and click **Upload**. The upgrade process should take about a few minutes.



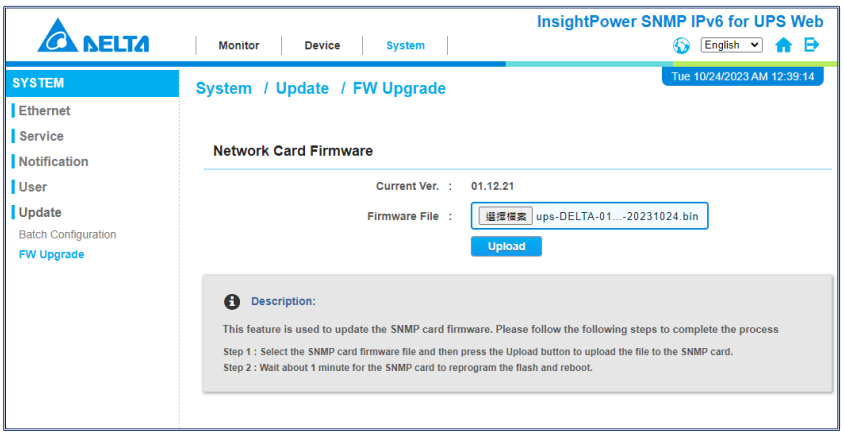
NOTE:

After the firmware file is uploaded, the system will take some time for self-upgrade and initialization. Please do not power off or restart the SNMP IPv6 to avoid unexpected problems.

Chapter 6 : SNMP Device Firmware Upgrade

Via Web or SFTP, you can effortlessly perform a firmware upgrade to your SNMP device via LAN. Please refer to the following instructions.

6.1. Firmware Upgrade via Web



Step 1

Log in to the Web as an Admin. Please refer to *Chapter 5 : InsightPower SNMP IPv6 for UPS Web*.

Step 2

Go to **System→ Update→ FW Upgrade**. This page shows current firmware version and description about updating the SNMP device firmware.

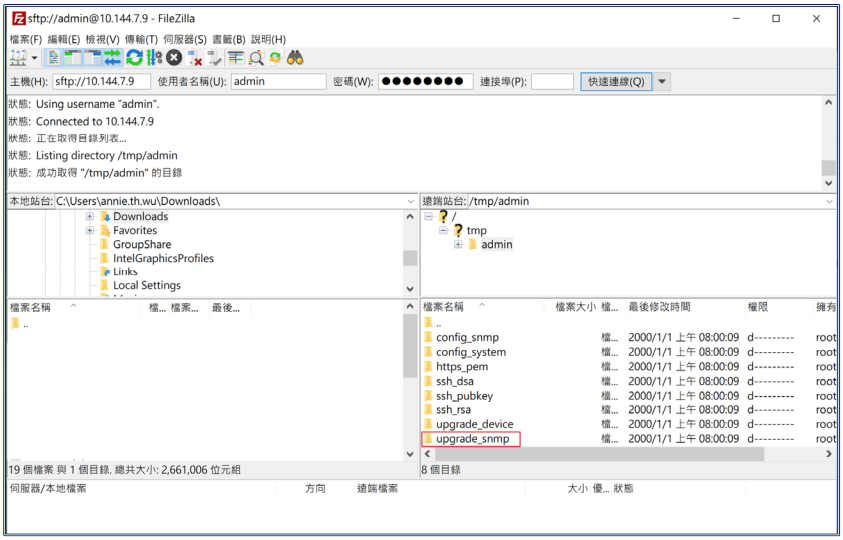
Step 3

Select a SNMP card firmware file and the file name will be displayed on the webpage. Click the **Upload** button to upload the file to the SNMP card.

Step 4

Please wait about 2 minutes until the upgrade is completed. After completion, the system will automatically reboot.

6.2 Firmware Upgrade via SFTP



Step 1

Use any SFTP client tool to log in to the SNMP card as an Admin.

Step 2

Upload a SNMP card firmware file to the ***upgrade_snmp*** folder.

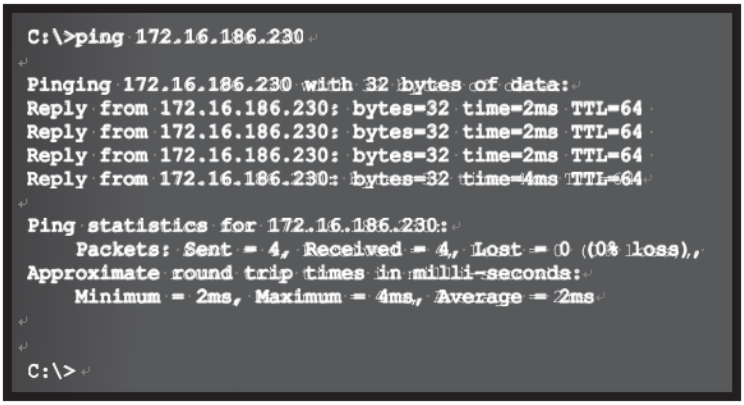
Step 3

After the upload process is finished, please wait about 2 minutes until the upgrade is completed. After completion, the system will automatically reboot.

Chapter 7 : Troubleshooting

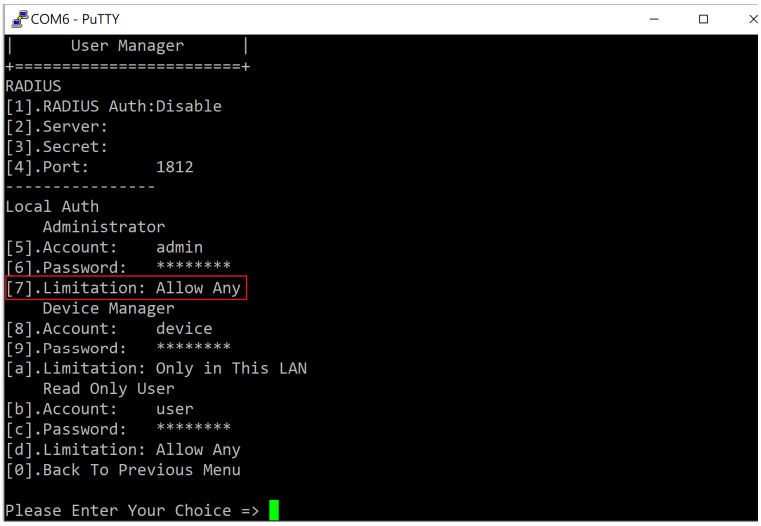
Q1. How to make sure the linking between the SNMP IPv6's and the UPS is established?

If the linking between the SNMP IPv6 and the UPS is correctly established, the yellow LED indicator should flash rapidly. If not, confirm that the device ID set- ting on the SNMP IPv6 and the UPS is consistent.



Q2. I can access the InsightPower SNMP IPv6 for UPS Web, but I cannot log in.

Please check the IP addresses of the SNMP IPv6 and the workstation where you are trying to log in. By default, they have the same LAN so you can connect via the web interface. You can use the COM port (please refer to *4.3 Configuring via COM Port*) to solve this issue. After login via COM port, please select [1]. -> User Manager -> [7]. Limitation, and change the Limitation command from **Only in This LAN** to **Allow Any** as shown below.

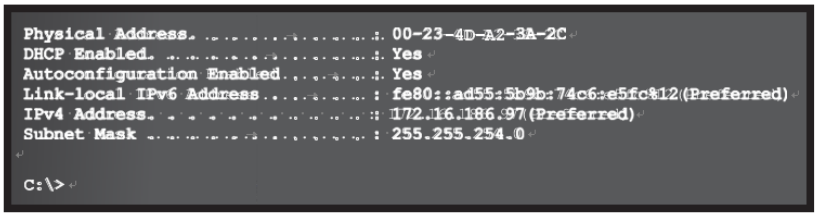


Q3. Unable to connect to the SNMP IPv6 via its Host Name?

If you just assign a new static IP address to the SNMP IPv6, you may need to refresh the NetBIOS table so that it corresponds with the new setting. Although Windows updates its NetBIOS table periodically, you can still manually force it to refresh by entering the following command **nbtstat –R** in DOS prompt mode. After that, you can now connect to the SNMP IPv6 by its Host Name. Please also ensure that the Host Name assigned to the SNMP IPv6 does not exceed 16 bytes.

Q4. How to check my workstation's IP address?

For Windows, please enter **ipconfig /all** in DOS prompt mode. For UNIX, please enter **ifconfig** in shell. You should be able to check your IP and MAC (Physical Address) now.



Q5. Unable to ping the SNMP IPv6 from my workstation?

If the SNMP IPv6 is non-responsive, check the following:

1) If the green LED indicator on the SNMP IPv6 is OFF, check if the network cable is correctly connected from the SNMP IPv6 to the router or hub.

2) If the green LED indicator is ON, the current IP address could be unreachable. Manually assign a valid IP address to the SNMP IPv6.

3) If the green LED indicator flashes and (1) your network configuration includes a DHCP server, make sure the DHCP service is working properly; (2) Otherwise, make sure the assigned IP is not already taken on the network. Please note that if the current configuration is not useable, the SNMP IPv6 will reset to default IP settings (IPv4 address: 192.168.1.100/ net mask: 255.255.255.0/ gateway: 192.168.1.254).

4) If the problem persists, use a network cable to cross link your SNMP IPv6 and the workstation. Ping the SNMP IPv6's default or static IP address, ac- cording to your configurations. If a ping response is successfully received, indicating that the SNMP IPv6 is working properly, check your network equipment. If not, contact your local dealer or service personnel for assistance.

Q6. Unable to perform an SNMP Get command?

Refer to *5-3-3 Notification* to check SNMP settings. Make sure that the work- station's IP address is added to the NMS IP list with Read or Read/ Write access. The community string on the workstation and the SNMP IPv6 must match.

Q7. Unable to perform an SNMP Set command?

Refer to *5-3-3 Notification* to check SNMP settings. Make sure that the work- station's IP address is added to the NMS IP list, with Read/ Write permission. The community string on the PC and the SNMP IPv6 must match.

Q8. Unable to receive SNMP trap?

Refer to *5.3.3 Notification* to check SNMP Trap settings. Make sure that the workstation's IP address is added to the Target IP list.

Q9. Forgot Administrator's account and password?

You can reset Administrator's account and password via text mode. Refer to *4.3 Configuring via COM Port* to establish a COM port connection with the SNMP IPv6. Please press the '**Reset Button**' of the SNMP IPv6 to restart. When the login and password information are prompted, key in **rstadmin** for each and press the **Enter** key within 60 seconds. The administrator's account and password will be reset to default (admin/ password).

Q10. How to generate a private SSL certificate file (in PEM format) for HTTPs connection?

To ensure connection security between the SNMP IPv6 and your workstation, you can create your own SSL certificate file. Please download and install OpenSSL Toolkit from http://www.openssl.org. Launch Shell or DOS prompt mode and enter the following command to create your own certificate file:

```
openssl req -x509 -nodes -days 365 -newkey
rsa:2048 -keyout cert.pem -out cert.pem
```

1) Answer the prompted questions. Proceed with the given directions. Once it is completed, a file named cert.pem is created in the current working di- rectory.
2) Upload cert.pem to the InsightPower SNMP IPv6 for UPS Web. Please refer to *5.3.2 Service – Web*.

Q11. How to generate DSA, RSA and Public keys for SSH?

For Linux:

1) Please download and install OpenSSH from http://www.openssh.org.
2) Launch Shell and enter the following commands to create your own keys (please ignore it when prompted to provide passphrase):

```
DSA Key:ssh-keygen –t dsa

RSA Key:ssh-keygen –t rsa
```

3) Upload DSA and RSA keys to the InsightPower SNMP IPv6 for UPS Web. Please refer to ***5.3.2 Service – Web*** for more information.

For Windows:

1) Please download and install Putty from http://www.putty.org.
2) Run puttygen.exe from the installed directory.
3) Select SSH-2 RSA from the Parameters area and click **Key** → **Generate key pair** to generate a RSA key.
4) Click **Conversions** → **Export OpenSSH Key** and assign a filename to the RSA key. Please ignore it when prompted to provide key passphrase.
5) Select **SSH-2 DSA** from the Parameters, click **Key** → **Generate key pair** to generate a DSA key.
6) Click **Conversions** → **Export OpenSSH Key** and assign a filename to the DSA key. Please ignore it when prompted to provide key passphrase.
7) Copy the generated key from the text box, paste in a text editor and save as a text file.

8) Upload the DSA/ RSA/ Public keys files to the InsightPower SNMP IPv6 for UPS Web. Refer to ***5.3.2 Service – Web*** for more information.

Q12. How to upload configuration / firmware / key files via SSH/ SFTP?

To quickly configure your SNMP IPv6, you can upload the files via SSH/ SFTP. The SNMP IPv6 automatically imports your settings after the files are uploaded to the designated directories. Refer to the following table:

Directory	Files
\config_snmp	snmp.ini
\config_system	configure.ini
\ssh_dsa	DSA key
\ssh_rsa	RSA key
\ssh_pubkey	Public key
\upgrade_snmp	SNMP IPv6's firmware upgrade package (binary)
\upgrade_device*	Device's firmware upgrade package (binary)

*Appears on specific devices only.

Upload files to their respective directories. Make sure the filenames do not contain non-English characters to avoid read error. Overwrite existing files if prompted by your SFTP client.

Q13. How to test SNMPv3 in Linux?

Before you can access the SNMP OID (Object Identifier) via SNMPv3 protocol, the SNMPv3 USM table must be organized. Please refer to *5.3.2 Service – SNMPv3 USM* for more information.

To test SNMPv3 in Linux, launch shell and key in the following command:

```
snmpwalk -v 3 -u <user> -l authPriv -A <pass-
word> -X <password> -n <context name> -t 3 <ip>
1.3.6.1.2.1.1.1.0
```

-v: 1 for SNMPv1, 3 for SNMPv3.

-l: Follow the security levels. They are: noAuthNoPriv, authNoPriv and authPriv.

-u: The user name which is assigned from SNMPv3 USM table.

-A: The Auth Password which is assigned from SNMPv3 USM table.

-X: The Priv Password which is assigned from SNMPv3 USM table.

-n: The Context Name which is assigned from SNMPv3 USM table.

-t: Timeout in seconds.

<ip>: The IP address of the SNMP IPv6.

<oid>: The next available SNMP OID (for example: 1.3.6.1.2.1.1.1.0). Please refer to the RFC1213 MIB.

Appendix 1 : Specifications

Model Name	InsightPower SNMP IPv6
Power Input	12 Vdc
Power Consumption	3.5 Watt (Max.)
Network Connection	RJ-45 jack connector (10M/ 100M/ 1G)
Physical	
Size (W × D)	130 × 60 mm (5.12” x 2.36”)
Weight	75 g (0.17 lb)
Environmental	
Operating Temperature	0 ~ 60℃ (32 ~140°F)
Storage Temperature	-40 ~ 125℃ (-40 ~ 257 °F)
Operating Humidity	0 ~ 90 % (Non-condensing)

NOTE:

1. Refer to the rating label for the safety rating.
2. All specifications are subject to change without prior notice.

Appendix 2 : 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.

No. : 501331510000
Version : V 0.0
Release Date : 2023_10_30

- Global Headquarter

Taiwan

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

- Regional Office

U.S.A

Delta Electronics (Americas) Ltd.
46101 Fremont Blvd. Fremont, CA 94538
T +1 510 344 2157
E ups.na@deltaww.com

Australia

Delta Energy Systems Australia Pty Ltd.
Unit 20-21, 45 Normanby Road, Notting Hill VIC 3168, Australia
T +61 3 9543 3720
E ups.australia@deltaww.com

South America

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

Thailand

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

Singapore

Delta Electronics Int'l (Singapore) Pte Ltd.
4 Kaki Bukit Ave 1, #05-04, Singapore 417939
T +65 6747 5155
E ups.singapore@deltaww.com

India

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

EMEA

Delta Electronics (Netherlands) BV
Zandsteen 15, 2132MZ Hoofddorp, The Netherlands
T +31 20 655 09 00
E ups.netherlands@deltaww.com

Japan

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

UK

Delta Electronics (UK) Ltd.
Eltek House Cleveland Road, Hemel Hempstead Industrial Estate,
Hemel Hempstead, Hertfordshire, HP2 7EY
T +44 1442 219355
E sales.gb@eltek.com

Smarter. Greener. Together.

5013315100