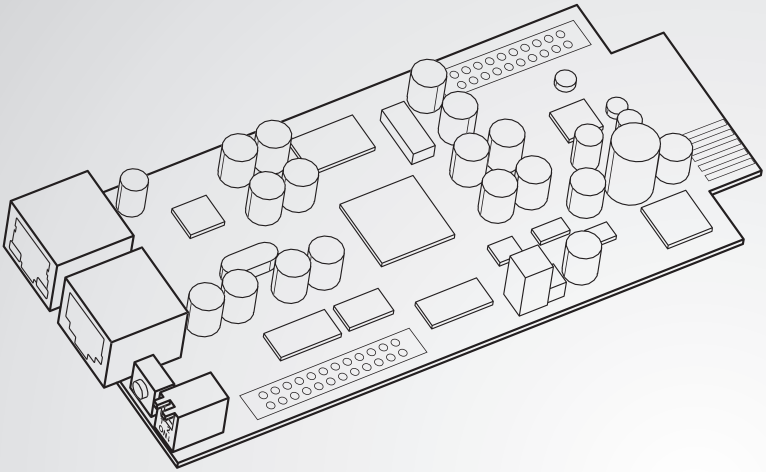


The power behind competitiveness

Delta InsightPower SNMP IPv6 for UPS

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©2011 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 ---------- 1

1-1 Warnings ---------- 1

1-2 Standard Compliance ---------- 1

Chapter 2 : Introduction ---------- 2

2-1 Product Description ---------- 2

2-2 Features ---------- 2

2-3 Package Contents ---------- 3

2-4 Interface ---------- 4

Chapter 3 : Installation ---------- 6

Chapter 4 : System Configurations ---------- 10

4-1 Configuring via InsightPower UPS Web ------- 10

4-2 Configuring with EzSetting ---------- 12

4-3 Configuring via Telnet ---------- 14

4-4 Configuring through COM Port ---------- 15

4-5 Configuring via Text Mode ---------- 17

Chapter 5 : InsightPower UPS Web ---------- 23

5-1 Monitor ---------- 24

5-1-1 Information ---------- 24

UPS Properties ---------- 24
Battery Parameters ---------- 25
In/ Out Parameters ---------- 25
Identification ---------- 26
Status Indication ---------- 26
Power Module ---------- 26

5-1-2 History ---------- 27

Event Log ---------- 27
Data Log ---------- 28
Configure ---------- 29

5-1-3 Environment ---------- 29
Information ---------- 29
Configuration ---------- 30
5-2 Device ---------- 31
5-2-1 Management ---------- 31
Configure ---------- 31
Control ---------- 33
Weekly Schedule ---------- 35
Specific Schedule ---------- 35
Event Level ---------- 36
5-3 System ---------- 37
5-3-1 Administration ---------- 37
User Manager ---------- 37
TCP/ IP ---------- 38
Web ---------- 39
Console ---------- 40
FTP ---------- 41
Time Server ---------- 42
Syslog ---------- 43
Batch Configuration ---------- 43
Upgrade ---------- 45
5-3-2 Notification ---------- 45
SNMP Access ---------- 45
SNMPv3 USM ---------- 46
SNMP Trap ---------- 47
Mail Server ---------- 48
Wake On LAN ---------- 49

Chapter 6 : SNMP Device Firmware Upgrade ---------- 50

Chapter 7 : Troubleshooting ---------- 53

Appendix A : Specifications ---------- 59

Appendix B : Warranty ---------- 60

Chapter 1 : Important Safety Instructions

1-1 Warnings

- The InsightPower SNMP IPv6 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

- **EN 55022: 2006 + A1: 2007, Class B**

  EN 61000-3-3: 1995+A1: 2001+A2: 2005
- **EN 55024: 1998 + A1: 2001 + A2: 2003**

  IEC 61000-4-2: 1995+A1: 1998+A2: 2000

  IEC 61000-4-3: 2006

  IEC 61000-4-4: 2004

  IEC 61000-4-5: 2005

  IEC 61000-4-6: 2007

  IEC 61000-4-8: 1993+A1: 2000

  IEC 61000-4-11: 2004

Chapter 2 : Introduction

2-1 Product Description

The InsightPower SNMP IPv6 for UPS 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)**

  Sets 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.

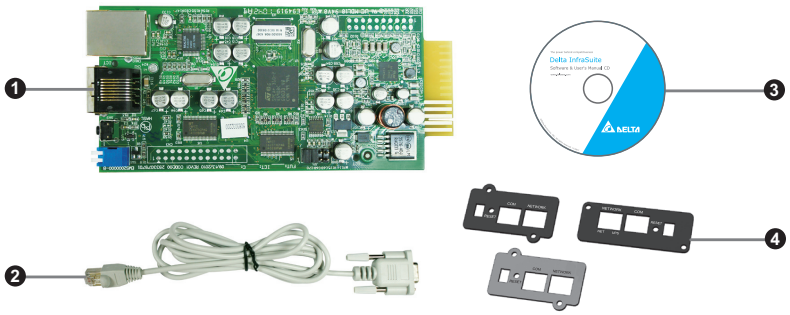
Other features and supported protocols include:

- 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) login and local authentication
- Remote event log management through syslog
- IPv4 and IPv6

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 reason, ensure that they are carefully repacked using the original packing materials came with the unit.

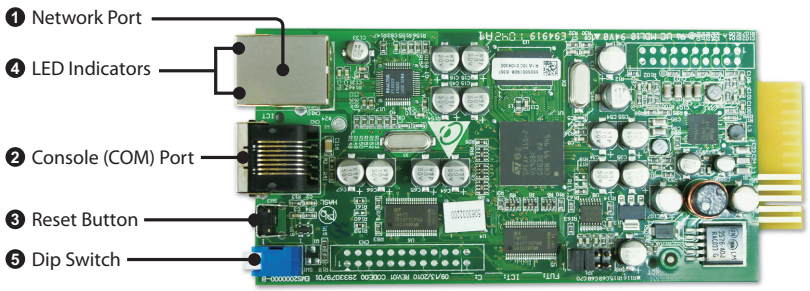


No.	Item	Quantity
❶	InsightPower SNMP IPv6 for UPS	1 PC
❷	RJ45 to DB9 cable	1 PC
❸	Software & User's Manual CD	1 PC
❹	Cover	3 PCS

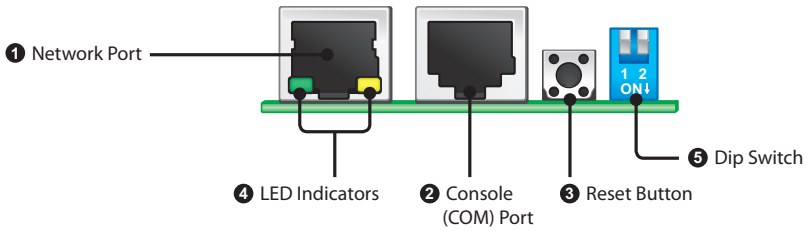
2-4 Interface

The interface includes NETWORK port, COM port, NET LED, UPS LED, RESET button and dip switch shown below. For their functions and indications, please refer to the table below.

Top view:



Front view:



No.	Item	Description
❶	Network Port	Connects to the Ethernet Network.
❷	Console (COM) Port	1. Connects to a workstation with the provided RJ45 to DB9 cable to configure the system. 2. Connects to an EnviroProbe to monitor the connected environment monitoring devices.
❸	Reset Button	Resets the SNMP IPv6. This does not affect the operation of the UPS.

No.	Item	Description
❹	LED Indicators	NET LED (Green) indicates network communication status. UPS LED (Yellow) indicates UPS communication status.

NET LED (Green)	UPS LED (Yellow)	Description
OFF	---	Hardware or network errors
---	Blinks every second	UPS disconnection
Without EnviroProbe		
ON	Blinks every 50 ms	Normal operation
With EnviroProbe		
Blinks every 50 ms	Blinks every 50 ms	Normal operation
ON	Blinks every 50 ms	EnviroProbe disconnection

❺ DIP Switch — Sets up operation mode.

Dip 1	Dip 2	Operation Mode	Description
OFF	OFF	Normal Mode	The SNMP IPv6 works with the UPS. It provides the UPS's status information and parameters through a network system.
OFF	ON	Pass Through Mode	The SNMP IPv6 stops polling the UPS but transfers the communication data between the console port and the UPS.
ON	OFF	Sensor Mode (with EnviroProbe)	The SNMP IPv6 works with the UPS and an optional EnviroProbe. It provides the UPS's information and the environmental parameters (temperature, humidity, etc).
ON	ON	Configuration Mode	In this mode, the user can login through the console port and configure the SNMP IPv6's settings. Please refer to ***4-4 Configuring through COM Port***.

NOTE

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

Chapter 3 : Installation

NOTE

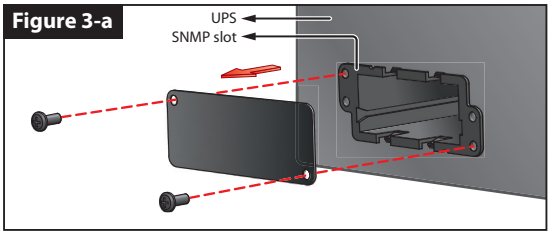
Before installation, please disconnect all power sources and critical loads connected to the UPS. Otherwise, the SNMP IPv6 might have shorting issues to cause UPS shutdown or damage.

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

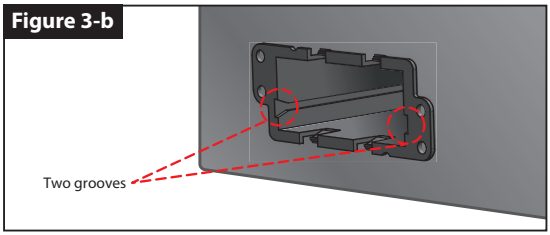


NOTE

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

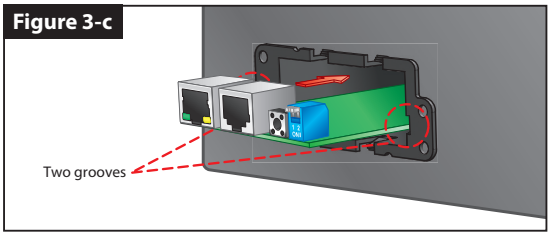
Step 2 Find the two grooves inside the SNMP slot ***(see Figure 3-b)***.

Figure 3-b



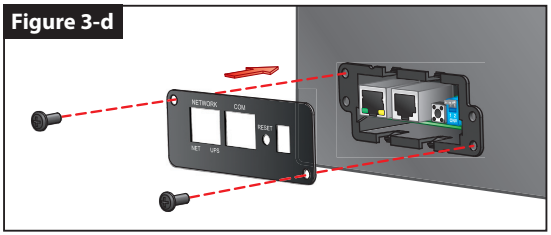
Step 3 Insert the SNMP IPv6 into the grooves ***(see Figure 3-c)***.

Figure 3-c



Step 4 There are three covers provided in the SNMP IPv6's package. Please follow the location of screw holes on the SNMP slot to select the suitable cover, and use the two screws that you just removed to fix the cover on the SNMP slot ***(see Figure 3-d)***.

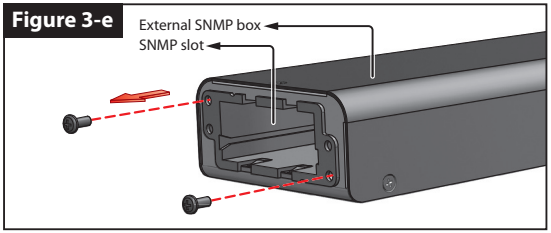
Figure 3-d



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

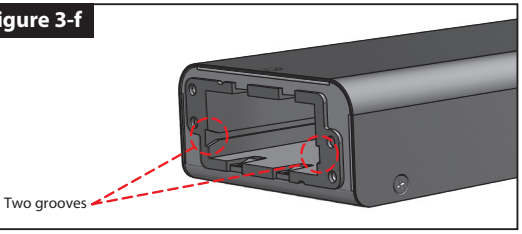
Step 1 Remove the two screws shown from the external SNMP box ***(see Figure 3-e)***.

Figure 3-e



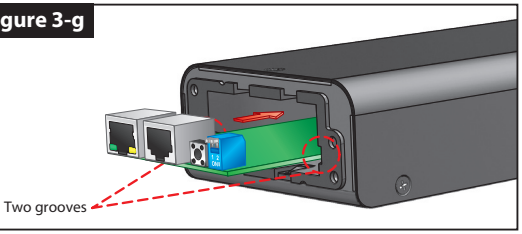
Step 2 Find the two grooves inside the external SNMP box ***(see Figure 3-f)***.

Figure 3-f



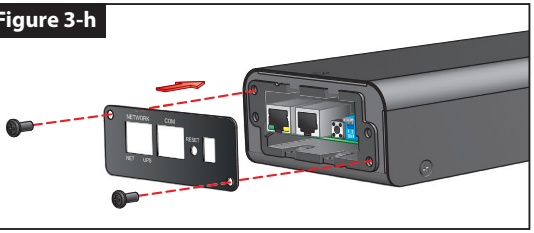
Step 3 Insert the SNMP IPv6 into the grooves ***(see Figure 3-g)***.

Figure 3-g



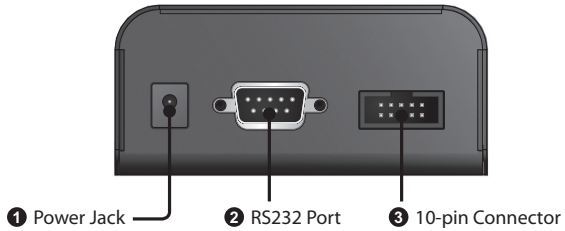
Step 4 There are three covers provided in the SNMP IPv6's package. Please follow the location of screw holes on the external SNMP box to select the suitable cover, and use the two screws that you just removed to fix the cover on the external SNMP box ***(see Figure 3-h)***.

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 x 208 x 42 mm
Weight	540 g

Chapter 4 : System Configurations

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

- Web-based **InsightPower UPS Web** (please refer to ***Chapter 5: InsightPower UPS Web***). This offers complete system management and monitoring.
- Provided program **EzSetting** (Please refer to ***4-2 Configuring with EzSetting***)
- **Telnet mode** (please refer to ***4-3 Configuring via Telnet***)

The above-mentioned methods require network connection. If it is not available at your location, you can use direct COM port connection to set up your InsightPower SNMP IPv6. Please see ***4-4 Configuring through 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 other SNMP IPv6 units connected in your network, we highly suggest that you change the SNMP IPv6's default Host Name to avoid Host Name conflicts. Also, it is recommended that you disable BOOTP/ DHCP and manually assign a valid static IP address for the SNMP IPv6.

4-1 Configuring via InsightPower UPS Web

To set up the SNMP IPv6 via the **InsightPower UPS Web**, please see the following instructions:

Step 1 Use a CAT5 cable to connect the SNMP IPv6's network port and the network. Launch your Web Browser and enter default Host Name **InsightPower** or the SNMP IPv6's default IP **192.168.1.100** in the address box. If you are unable to connect, please see ***Chapter 7: Troubleshooting Q6***.

NOTE

If you have previously changed the SNMP IPv6's Host Name or IP address, make sure to provide the correct information accordingly.

Step 2 Log in as Administrator (default account/ password: admin/ password, case sensitive). Click **System → Administration → User Manager**. Manage your login accounts and passwords under the "Local Authentication" subhead. The access permission for the account types are listed as follows:

1) Administrator: Permitted to modify all settings.
2) Device Manager: Permitted to modify device-related settings.
3) Read Only User: Only permitted to observe monitoring data.

NOTE

You can manually specify whether users are allowed to log in from external connections (from other LANs). Selecting **Only in This LAN** will block login attempts from external connections. Selecting **Allow Any** will allow these attempts.

Step 3 Click **System → Administration → TCP/ IP** to set Host Name, IP address, Subnet Mask and Gateway IP for the SNMP IPv6.

Step 4 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 configure all InsightPower SNMP IPv6's settings including system information, input/ output management, system administration, event notifications and event history, please refer to ***Chapter 5: InsightPower UPS Web – 5-1 Monitor, 5-2 Device, 5-3 System***.

4-2 Configuring with EzSetting

One of the easiest ways to configure the SNMP IPv6 is utilizing **EzSetting** (Compatible with Windows systems), a program you can find in the provided CD. You can use it to set up your InsightPower SNMP IPv6 and perform firmware upgrades on your SNMP devices.

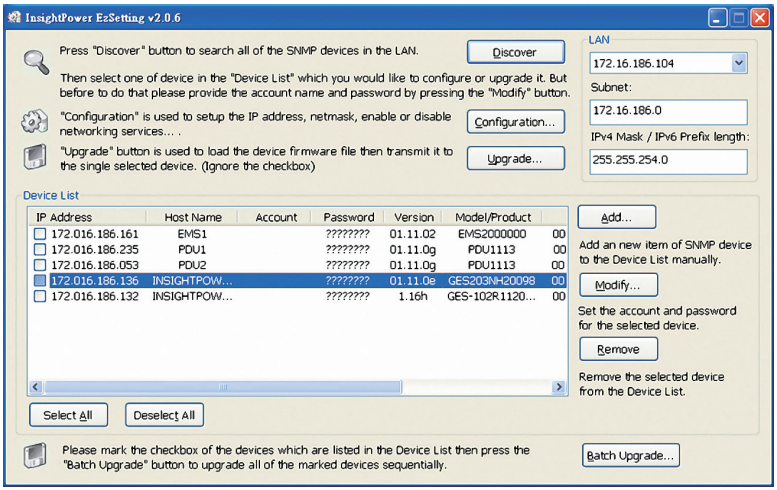
Step 1 Set up a workstation (Windows 2000/ 2003/ 2008/ XP/ Vista/ Win7 or later version).

Step 2 Use a CAT5 cable to connect the SNMP IPv6's network port and the network.

Step 3 Make sure both of the DIP switches of the SNMP IPv6 are set to the **OFF** position (normal mode) to enable network transmission, and make sure the workstation and the SNMP IPv6 are on the same LAN.

Step 4 Insert the provided CD in the CD-ROM drive. From the root directory, launch **EzSetting**.

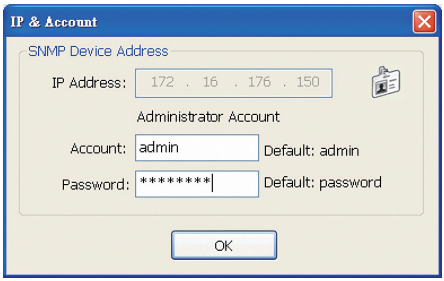
Step 5 Click **Discover** to search all SNMP devices on the LAN. A list of devices will be shown.



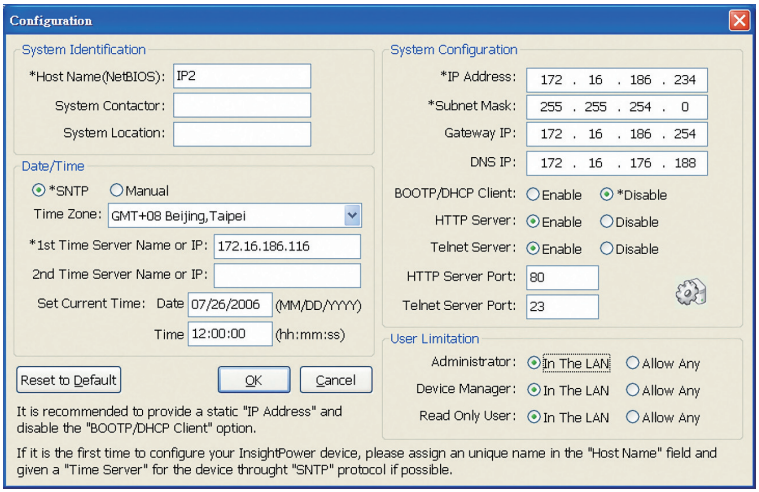
NOTE

1. If you want to search all SNMP devices in a different domain, change the **Subnet** and **IPv4/ IPv6 Prefix Length** and then click **Discover**.
2. If the SNMP IPv6 can not be found, check the networking port **UDP 3456** on the workstation you are using. Make sure it is not blocked.

Step 6 Select a device from the Device List, click **Modify**, and key in Administrator account and password. Default account/ password: admin/ password (case sensitive).



Step 7 Click **Configuration** and set up essential parameters.



NOTE

To configure all InsightPower SNMP IPv6's settings including system information, input/ output management, system administration, event notifications and event history, please refer to ***Chapter 5: InsightPower UPS Web***.

4-3 Configuring via Telnet

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

Step 2 Set up a workstation (Microsoft Windows, Max OSX or Linux). Connect the workstation to the same LAN which the SNMP IPv6 is connected to.

Step 3 Make sure both of the DIP switches of the SNMP IPv6 are set to the **OFF** position (normal mode).

Step 4 For Windows workstations, launch DOS prompt mode (**Start → Run →** key in **cmd** and press **Enter**). For Linux, launch shell.

Step 5 Enter the following command: **telnet InsightPower** to initiate telnet connection with the SNMP IPv6.

Step 6 When connection is established, enter **account** and **password** (default: admin/ password, case sensitive). The **Main Menu** will appear on the screen. Please refer to ***4-5 Configuring via Text Mode*** for more information.

NOTE

1. The SNMP IPv6 will terminate idle connections after 60 seconds.
2. To configure all InsightPower SNMP IPv6's settings including system information, input/ output management, system administration, event notifications and event history, please refer to ***Chapter 5: InsightPower UPS Web***.

4-4 Configuring through COM Port

If network connection is not available at your location, you can still manage the SNMP IPv6 by using the COM port connection. Please follow the instructions below.

NOTE

If you are running on a non-Windows system, refer to your system's User Manual for Telnet clients.

Step 1 Set up a workstation (Microsoft Windows 2000, 2003, 2008, XP, Vista or 7).

Step 2 Use the provided RJ45 to D89 cable to connect the SNMP IPv6's COM port and the workstations' COM port.

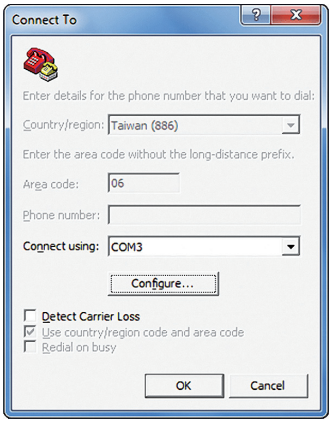
Step 3 Make sure both of the DIP switches of the SNMP IPv6 are set to the **OFF** position (normal mode).

Step 4 For workstations running Windows 2000, 2003, 2008 or XP, go to **Start → Programs → Accessories → Communications** and select **HyperTerminal**.

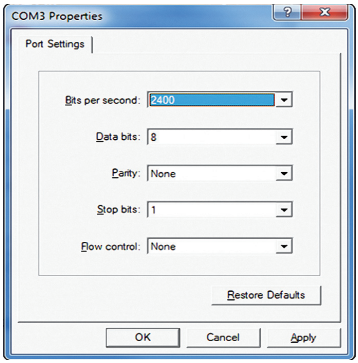
NOTE

Microsoft has removed HyperTerminal from Windows Vista and later versions. For workstations running these systems, you can still download a free Telnet/ SSH client 'PuTTY' from http://www.putty.org.

Step 5 Enter a name and choose an icon for the connection. Click **OK** to continue. From the dropdown list **Connect using**, select the **COM port** that is connected to the SNMP IPv6.



Step 6 Click **Configure** and set up COM port parameters as follows:



Step 7 Click **OK** to continue and set both of the DIP switches of the SNMP IPv6 to the **ON** position (configuration mode). HyperTerminal will automatically connect to the SNMP IPv6. If it does not connect, click the telephone icon **call** from the icon list. When connection is established, log in with account/ password. (Default: admin/ password, case sensitive). Once you are logged in, the **Main Menu** appears on the screen. Please refer to ***4-5 Configuring via Text Mode*** for more information.

4-5 Configuring via Text Mode

You can configure the SNMP IPv6 via text mode by using Telnet/ SSH clients such as HyperTerminal and PuTTy. In this section, you can find descriptions and default values for each item in the table.

Main Menu

```
+=======================+
|        Main Menu      |
+=======================+
Web Card Version 01.00.00
MAC Address 00-30-ab-25-e9-1e
[1].User Manager
[2].TCP/IP Setting
[3].Network Parameter
[4].Time Server
[5].Soft Restart
[6].Reset All To Default
[z].Exit Without Save
[0].Save And Exit

Please Enter Your Choice =>
```

User Manager

```
+=======================+
|     User Manager      |
+=======================+
RADIUS
[1].RADIUS Auth: Disable
[2].Server:
[3].Secret:
[4].Port:       1812
---------------
Local Auth
    Administrator
[5].Account:    admin
[6].Password:   ********
[7].Limitation: Only in This LAN
    Device Manager
[8].Account:    device
[9].Password:   ********
[a].Limitation: Only in This LAN
    Read Only User
[b].Account:    user
[c].Password:   ********
[d].Limitation: Allow Any
[0].Back To Previous Menu

Please Enter Your Choice =>
```

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	
[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 who is only permitted to change device-related settings	device
[9]	Device Manager Password		password
[a]	Device Manager Limitation	Restrict login area of the Device Manager	Only in This LAN
[b]	Read Only User Account	The default account/ password (case sensitive) for Read Only User who can only observe settings	user
[c]	Read Only User Password		password
[d]	Read Only User Limitation	Restrict login area of the Read Only User	Allow Any

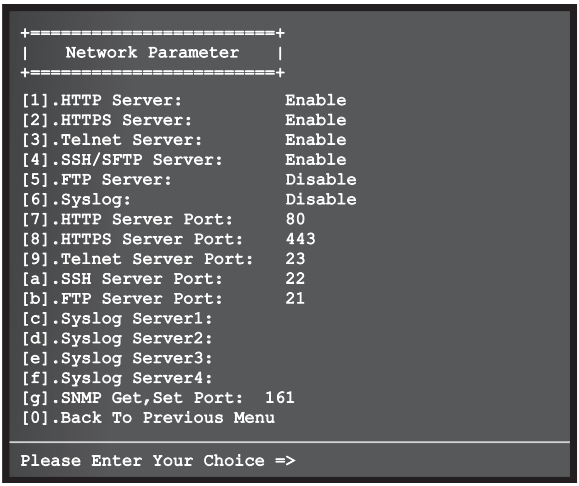
TCP/IP Setting

```
+=========================+
|     TCP/IP Setting      |
+=========================+
[1].IPv4 Address:        192.168.001.100
[2].IPv4 Subnet Mask:    255.255.255.000
[3].IPv4 Gateway IP:     192.168.001.254
[4].IPv4 DNS or WINS IP:192.168.001.001
[5].DHCPv4 Client:       Enable
[6].IPv6 Address:        fe80::230:abff:fe25:900
[7].IPv6 Prefix Length:  64
[8].IPv6 Gateway IP:     ::
[9].IPv6 DNS IP:         ::
[a].DHCPv6:              Enable
[b].Host Name(NetBIOS):  INSIGHTPOWER
[c].System Contact:
[d].System Location:
[e].Auto-Negotiation:    Enable
[f].Speed:               100M
[g].Duplex:              Full
[h].Status Stable:       3
[0].Back To Previous Menu

Please Enter Your Choice =>
```

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 network gateway	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 network default gateway	
[9]	IPv6 DNS IP	IPv6 Domain Name Server IP address	
[a]	DHCPv6	Enable/ Disable DHCPv6 protocol	Enable

No.	Item	Description	Default
[b]	Host Name (NetBIOS)	The Host Name for the SNMP IPv6	INSIGHTPOWER
[c]	System Contactor	The System Contactor information	
[d]	System Location	The System Location information	
[e]	Auto-Negotiation	Enable/ Disable automatic transfer rate (10/ 100M bps) negotiation	Enable
[f]	Speed	If the Auto-Negotiation is disabled, you can specify the transfer rate	100M
[g]	Duplex	If the Auto-Negotiation is disabled, you can specify the duplex mode	Full
[h]	Status Stable	Status change confirmation check time	3

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 networking port	80
[8]	HTTPS Server Port	HTTPS networking port	443
[9]	Telnet Server Port	Telnet networking port	23
[a]	SSH Server Port	SSH networking port	22
[b]	FTP Server Port	FTP networking port	21
[c]	Syslog Server1	The remote syslog Host Name	
[d]	Syslog Server2	The remote syslog Host Name	
[e]	Syslog Server3	The remote syslog Host Name	
[f]	Syslog Server4	The remote syslog Host Name	
[g]	SNMP Get, Set Port	The SNMP networking port	161

Time Server

You can manually adjust time and date for the SNMP IPv6 or set up automatic time server synchronization. The SNMP IPv6, Windows XP and later versions work with SNTP (Simple Network Time Protocol). If you need to start up a time server service on your workstation, please refer to ***Chapter 7: Troubleshooting Q1***.

```
+========================+
|       Time Server      |
+========================+
[1].Time Selection:     SNTP
[2].Time Zone:           +0 hr
[3].1st Time Server:    POOL.NTP.ORG
[4].2nd Time Server:
[5].Manual Date:         01/01/2000 (MM/DD/YYYY)
[6].Manual Time:         00:00:00 (hh:mm:ss)
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Item	Description	Default
[1]	Time Selection	SNTP or manual	SNTP
[2]	Time Zone	Select the 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.

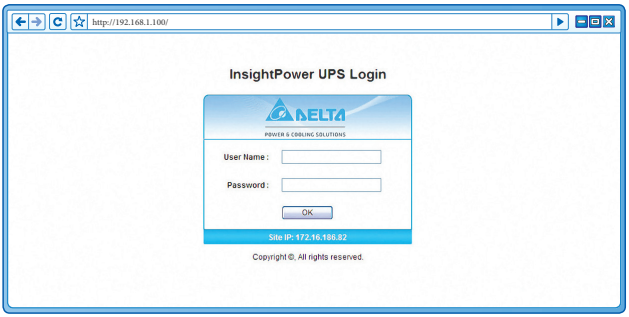
Chapter 5 : InsightPower UPS Web

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

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

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

Step 3 When connection is established, the **InsightPower UPS Login** page appears. Enter your account and password. (Default: admin/ password).



NOTE

1. If you have previously changed the SNMP IPv6's Host Name or IP address, make sure to provide the correct information accordingly.
2. If the login page is accessible, but you are unable to log in with correct **account** and **password**, additional network configuration is needed. The cause could be the IP subnet of the computer you are logging in to is different from the SNMP IPv6's. To solve this issue, please refer to ***Chapter 7: Troubleshooting Q3***.
3. The SNMP IPv6 will automatically log off idle connections after 30 minutes.

The **InsightPower UPS Web** includes the information of **Monitor, Device** and **System**. Please refer to the following sections ***5-1~5-3*** for more information.

5-1 Monitor

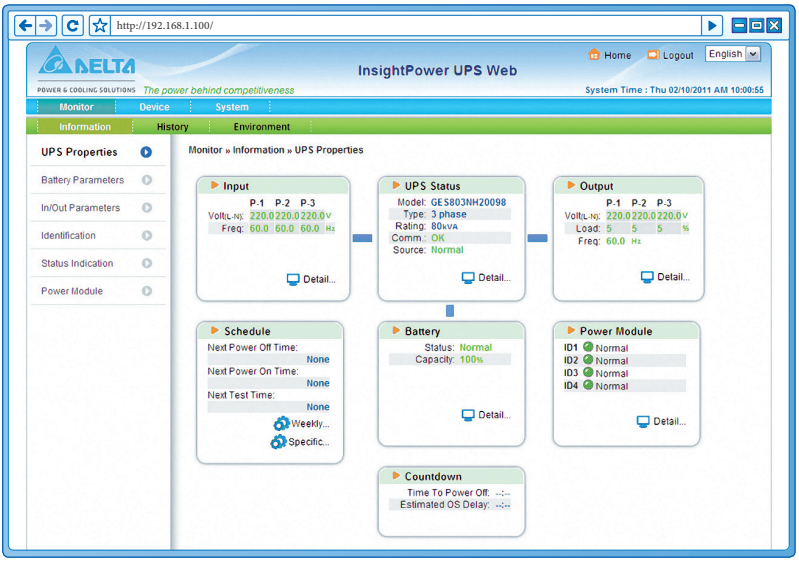
Under the Monitor category, there are Information, History and Environment these three items.

5-1-1 Information

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

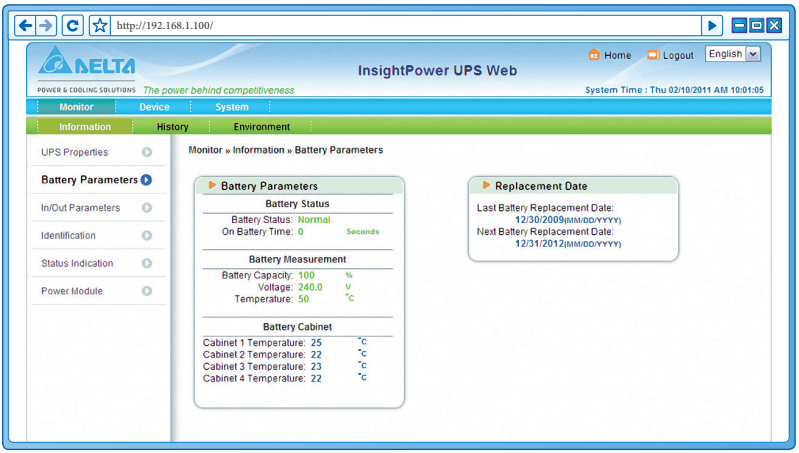
UPS Properties

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



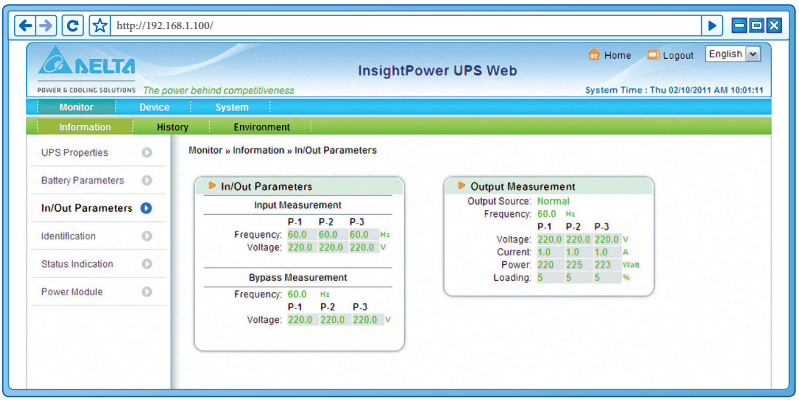
Battery Parameters

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



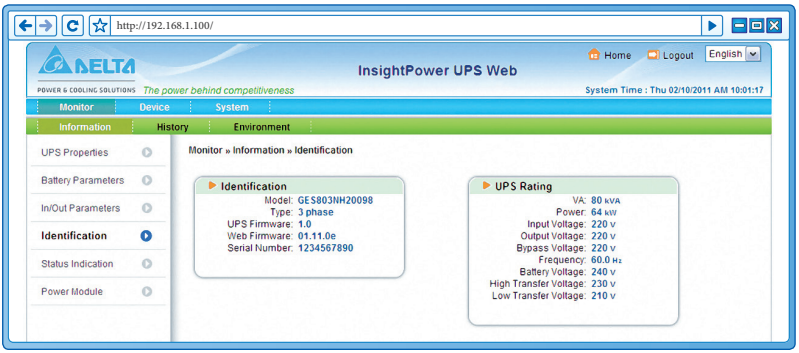
In/ Out Parameters

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



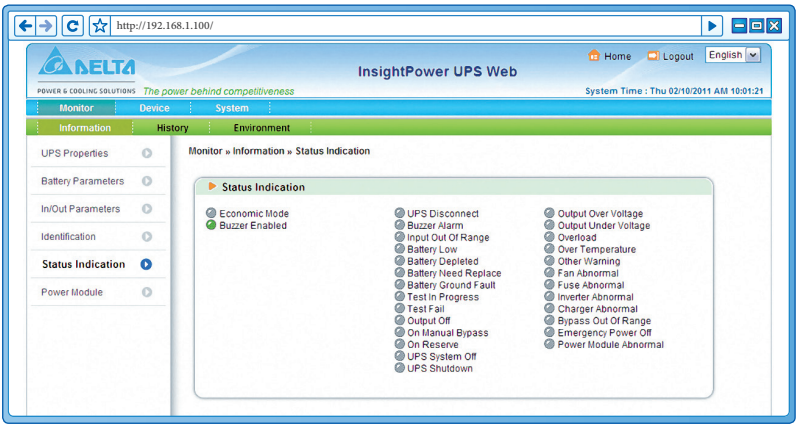
Identification

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



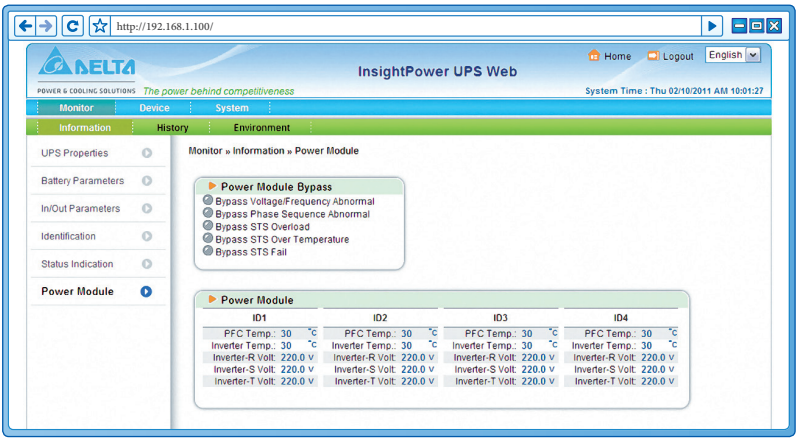
Status Indication

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



Power Module

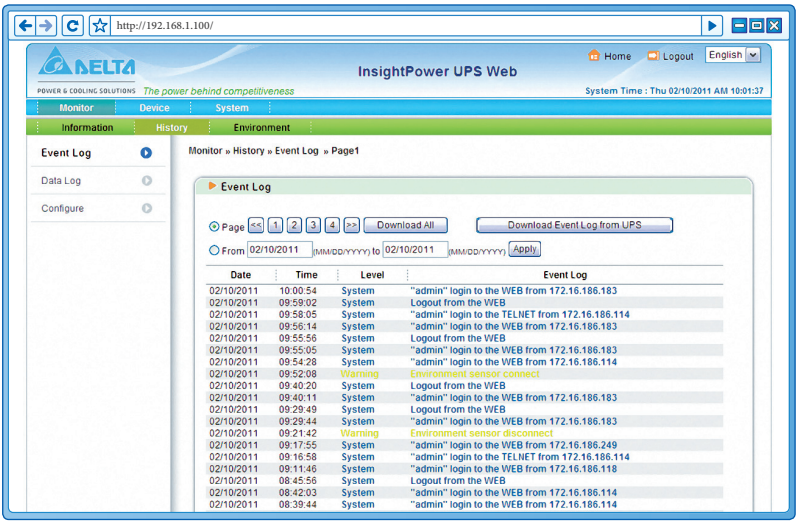
Go to **Monitor → Information → Power Module** to view the information of Power Module Bypass and Power Module ID1/ 2/ 3/ 4. Please note that this page only appears when your UPS has designated power modules.



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.

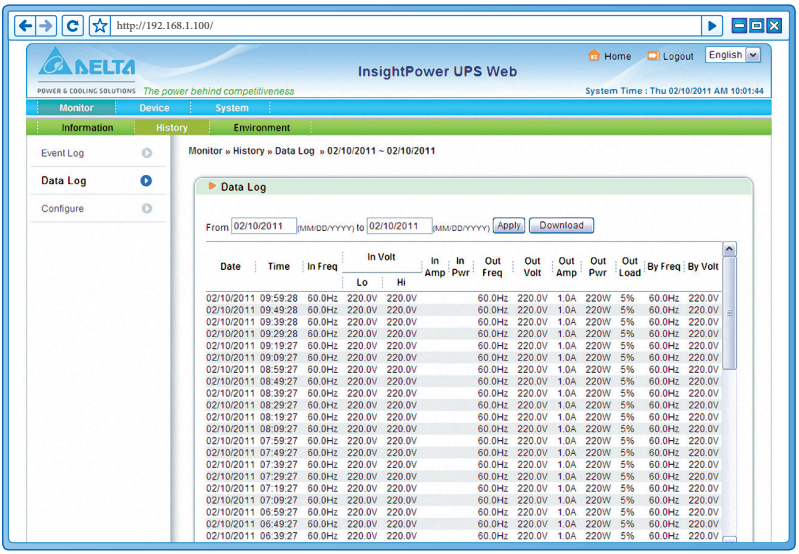


- **Date:** The date when the event occurred.
- **Time:** The time when the event occurred.
- **Level:** The Event Level of the event occurred.
- **Event Log:** The description of the event that occurred.
- **Download Event Log from UPS**

  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

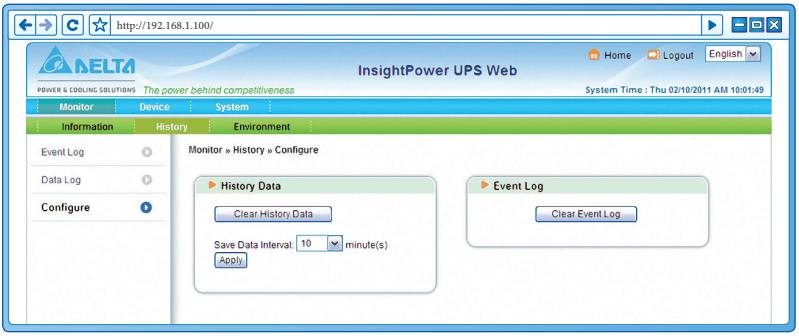
Go to **Monitor → History → Data Log** to see all saved device data. You can also download the data archive (data_log.xls) recorded during an assigned period of time on your computer.



- **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 logs and event logs. You can also assign the Save Data Interval.

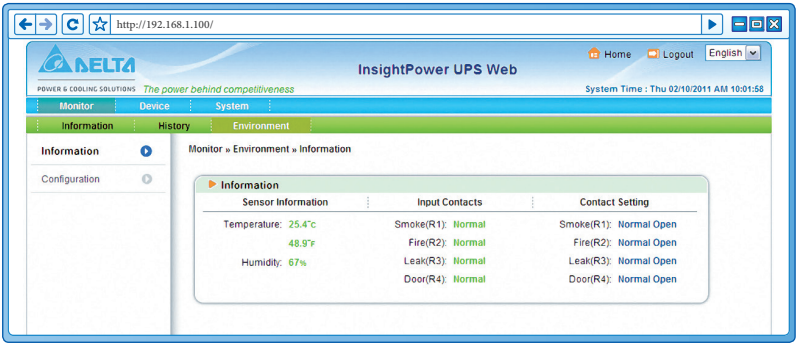


- **Clear History Data:** Empty history data logs.
- **Clear Event Log:** Empty event logs.
- **Save Data Interval:** The time interval after which an event/ data entry is recorded.

5-1-3 Environment

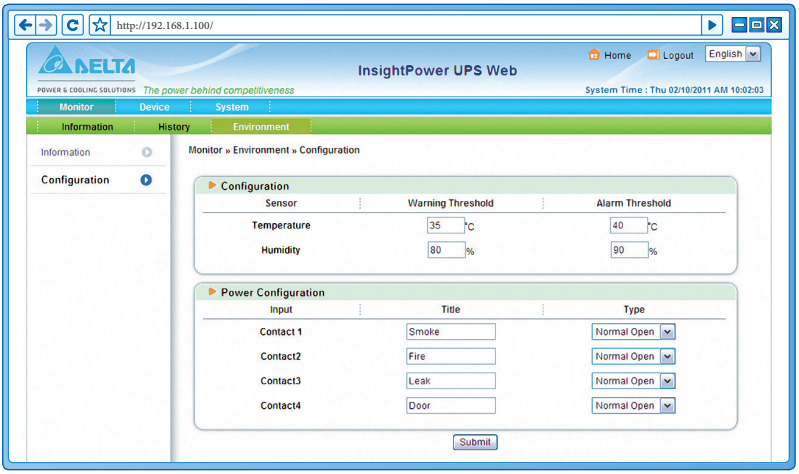
Information

Go to **Monitor → Environment → Information** to see the information of Sensor, Input Contacts and Contact Setting.



Configuration

Go to **Monitor → Environment → Configuration** to configure the Warning Threshold, Alarm Threshold, Title and Type. Please note that you can use the two dip switches to set different operation modes. Please see the table below for detail information.



Dip 1	Dip 2	Opeation Mode	Description
OFF	OFF	Normal Mode	The SNMP IPv6 works with the UPS. It provides the UPS's status information and parameters through a network system.
OFF	ON	Pass Through Mode	The SNMP IPv6 stops polling the UPS but transfers the communication data between the console port and the UPS.
ON	OFF	Sensor Mode (with EnviroProbe)	The SNMP IPv6 works with the UPS and an optional EnviroProbe. It provides the UPS's information and the environmental parameters (temperature, humidity, etc).
ON	ON	Configuration Mode	In this mode, the user can login through the console port and configure the SNMP IPv6's settings. Please refer to ***4-4 Configuring through COM Port.***

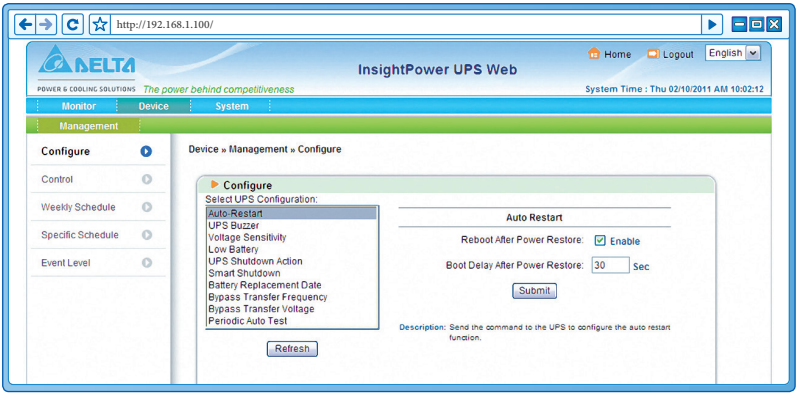
5-2 Device

5-2-1 Management

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

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 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.

- **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 setup, 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**

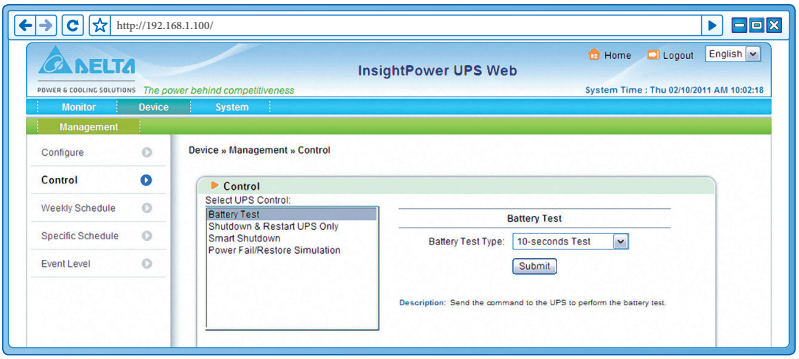
  This configuration is used to set up battery test time. After you confirm your setup, the SNMP IPv6 will send the command to the UPS and save the setup in the UPS. When the test time is due, the UPS will automatically perform the battery test.

- **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 shutdown 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 shutdown and restart the UPS, please check both of the boxes and key in according 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**

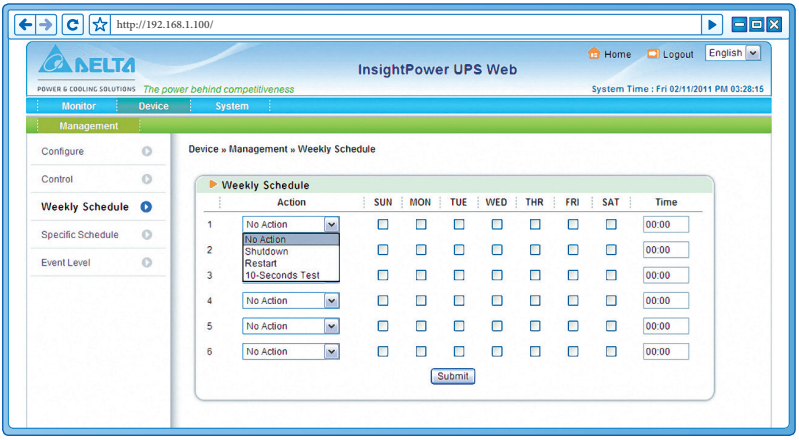
  Press the **Switch Bank** button to control the UPS output relay (on or off).

- **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.

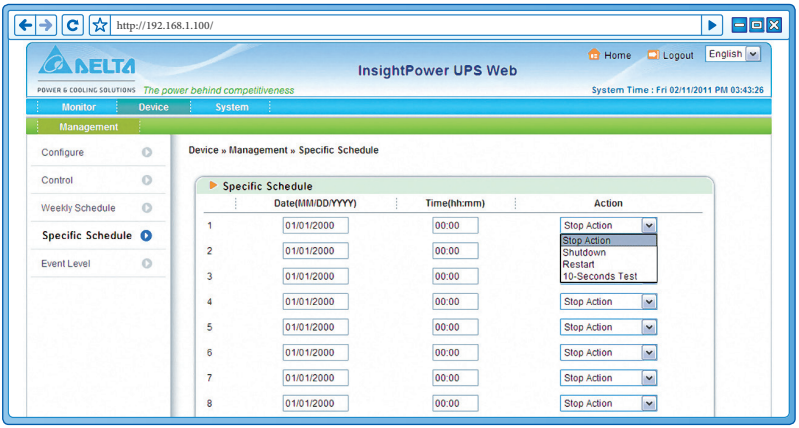
Weekly Schedule

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.



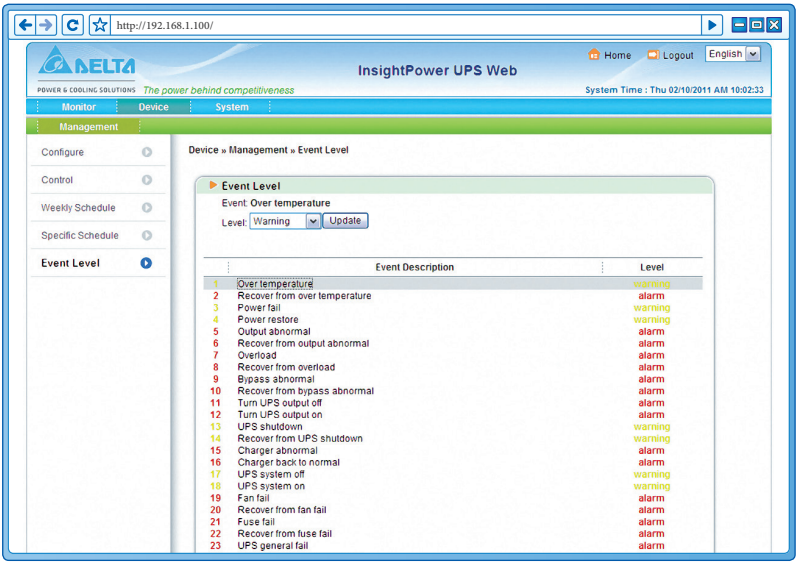
Specific Schedule

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)**.



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 ***5-3-2 Notification - SNMP Trap*** and ***5-3-2 Notification - Mail Server***.



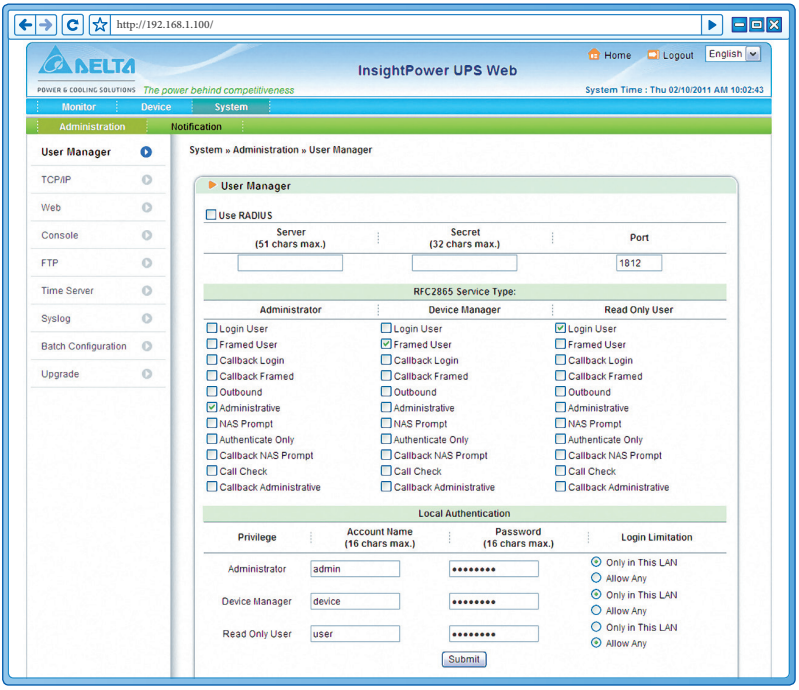
5-3 System

Under the System category, there are Administration and Notification these two items.

5-3-1 Administration

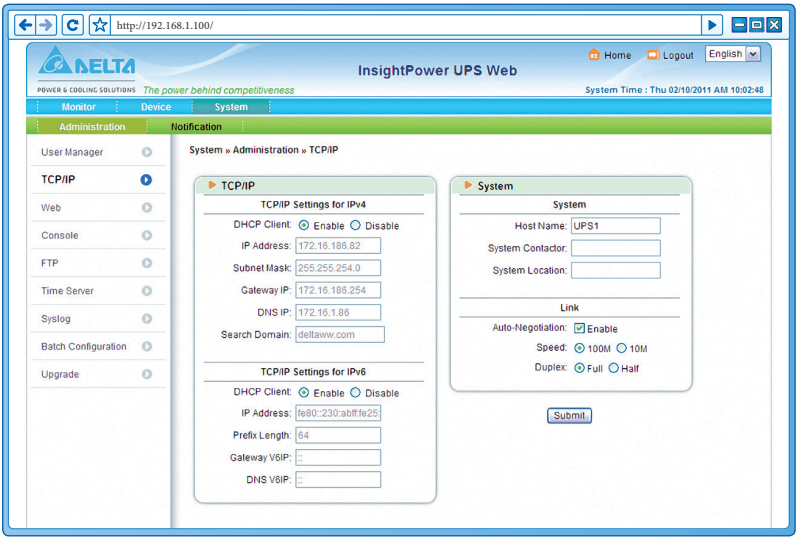
User Manager

The SNMP IPv6 supports RADIUS. Check the **Use RADIUS** box, key in required information including Server, Secret and Port (default: 1812) and click **Submit** to enable RADIUS. You can define service types 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.



TCP/ IP

This allows Administrator to configure local network parameters for the SNMP IPv6.



- **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 (e.g. 192.168.1.100).

  3) **Subnet Mask:** The Subnet Mask for your network (e.g. 255.255.255.0).

  4) **Gateway IP:** The IP address for network gateway in dotted format (e.g. 192.168.1.254).

  5) **DNS IP:** The IP address Domain Name Server in dotted format (e.g. 192.168.1.1).

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

- **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.

- **System**

1) **Host Name:** The SNMP IPv6 Host Name on the network.

2) **System Contact:** System contactor information.

3) **System Location:** System location information.

- **Link**

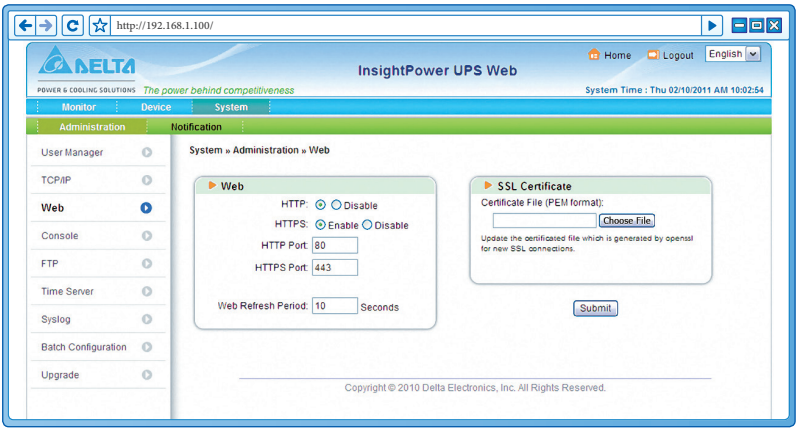
1) **Auto-Negotiation:** Enable/ Disable automatic transfer rate (10/ 100M bps) negotiation.

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.

Web

This allows Administrator to enable/ disable HTTP/ HTTPS communication protocols.



- **Web**

  1) **HTTP:** Enable/ disable HTTP connection.

  2) **HTTPS:** Enable/ disable HTTPS connection.

  3) **HTTP Port:** Assign an HTTP port number (default: 80).

  4) **HTTPS Port:** Assign an HTTPS port number (default: 443).

  5) **Web Refresh Period:** Web refresh update 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.

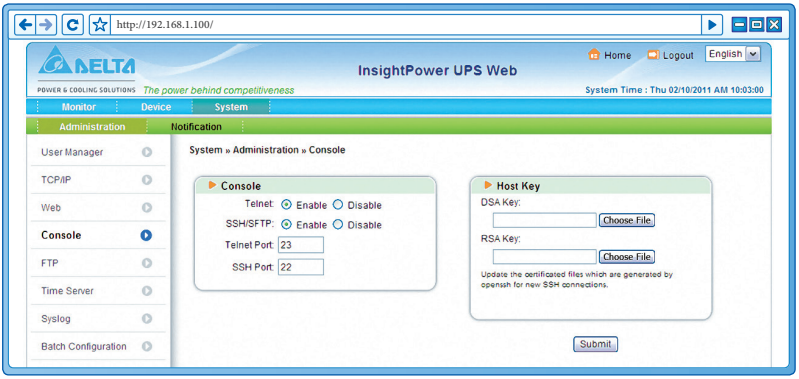
  2) **Certificate File:** This allows you to replace your own SSL certificate file. The SNMP IPv6 supports PEM format which is generated by OpenSSL. Click **Choose File** to upload a certificate file.

NOTE

For more information regarding generating a private SSL certificate file, please refer to ***Chapter 7: Troubleshooting Q12***, or visit http://www.openssl.org/.

Console

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

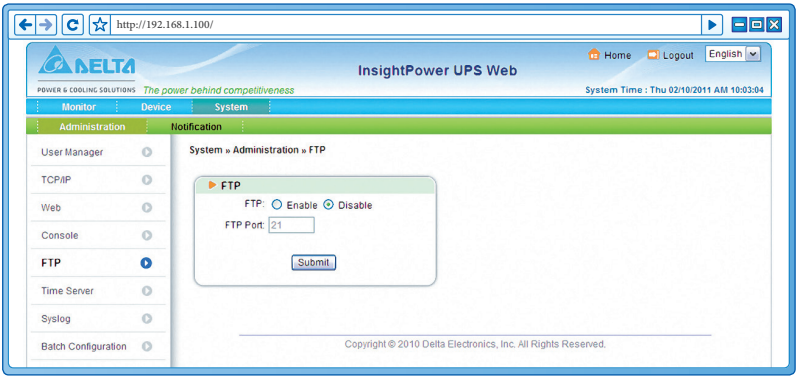


- **Telnet:** Enable/ disable Telnet connection.
- **SSH/ SFTP:** Enable/ disable SSH/ SFTP connection.
- **Telnet Port:** Assign a Telnet port number (default: 23).
- **SSH Port:** Assign an SSH protocol port number (default: 22).
- **Host Key:**

  DSA/ RSA Key: This allows you to replace your own SSH keys. The SNMP IPv6 supports key files generated by OpenSSH. Please refer to ***Chapter 7: Troubleshooting Q13***.

FTP

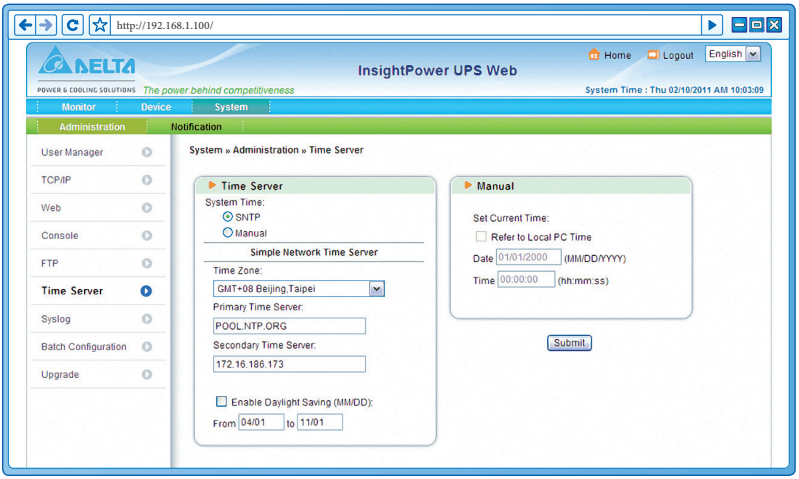
This allows Administrator to enable/ disable FTP communication protocol.



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

Time Server

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.



- **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.

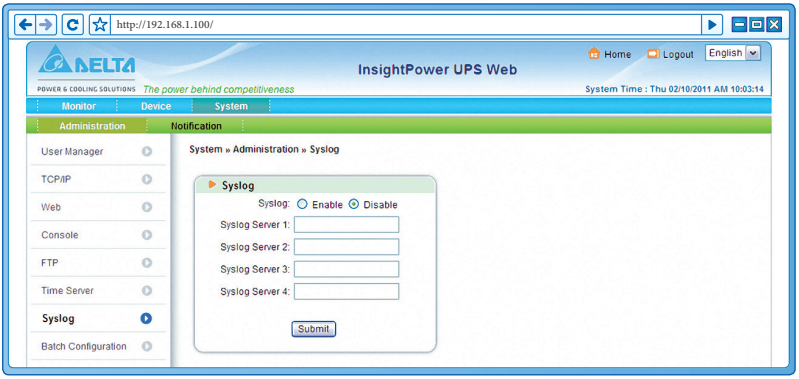
  3) **Enable Daylight Saving:** Check to enable daylight saving time. During this period, the SNMP IPv6 adjusts time forward one hour.

- **Manual**

  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.

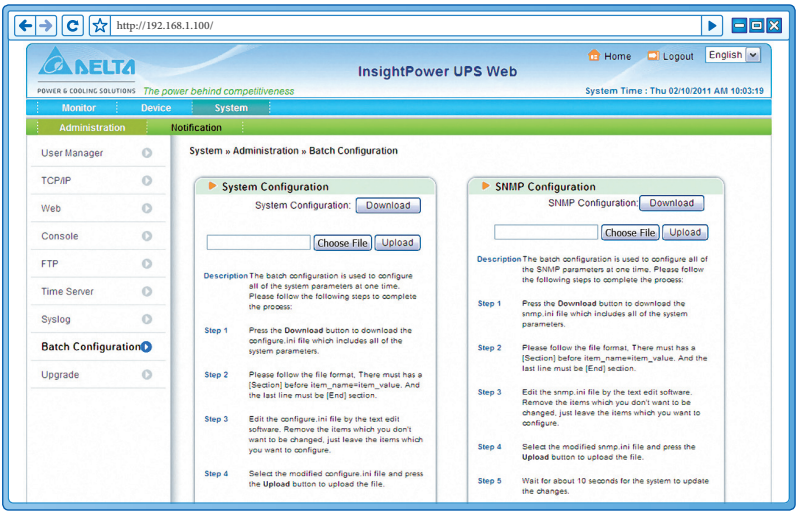
Syslog

Syslog is used to store event logs on remote syslog servers. This will not affect the local event logs.



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.



- **System Configuration**

  The **System Configuration** includes settings saved in the **Management** and **Administration** tabs. 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 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***.

- **SNMP Configuration**

  The **SNMP Configuration** includes settings in the **Notification** tab. 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

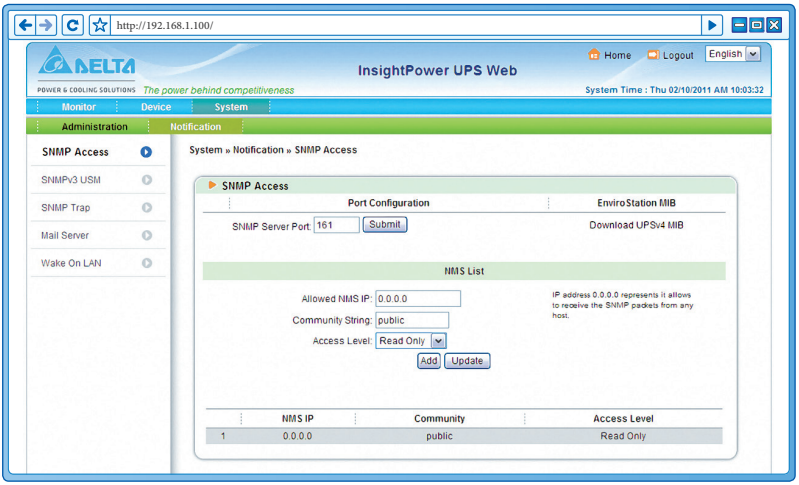
If you need to modify the command lines, please do not delete the unmodified ones. They should be left intact to assure the integrity of the configuration file.

Upgrade

This menu allows the Administrator to update the SNMP IPv6's firmware.

5-3-2 Notification

SNMP Access



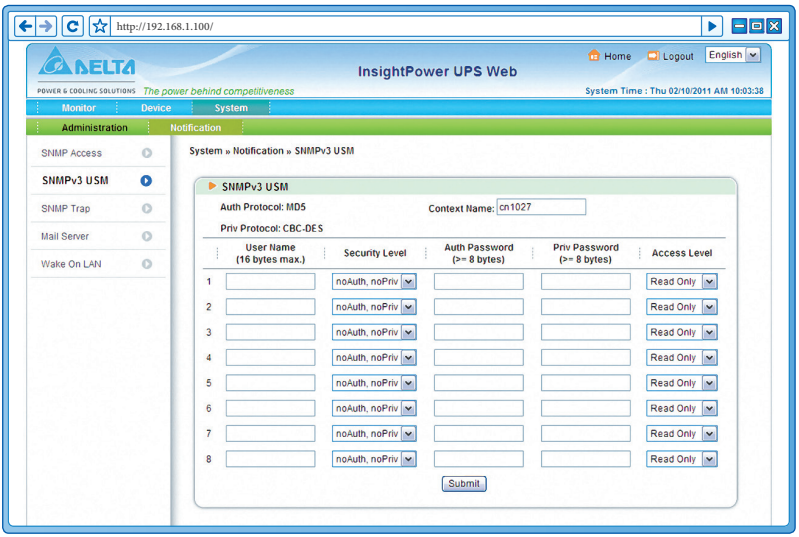
The SNMP IPv6 supports SNMP protocol and SNMP NMS (Network Management System), which are commonly used to monitor network devices for conditions that call for administrative attention. To prevent unauthorized access, you can specify the NMS IP addresses that are allowed to access, their community strings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

NOTE

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.

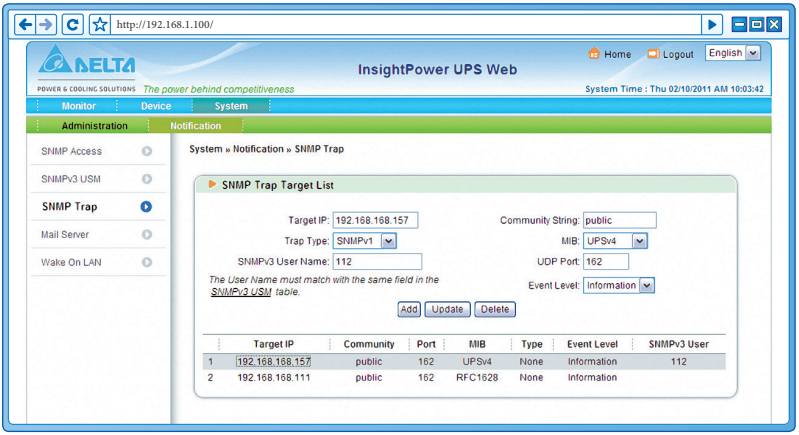
SNMPv3 USM

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.



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, UDP port, and Event Level, 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 provides SNMPv1, v2c and v3 traps to satisfy most of customers' environments. If you use the SNMPv3 trap, please provide one of the user names in the SNMPv3 USM table.

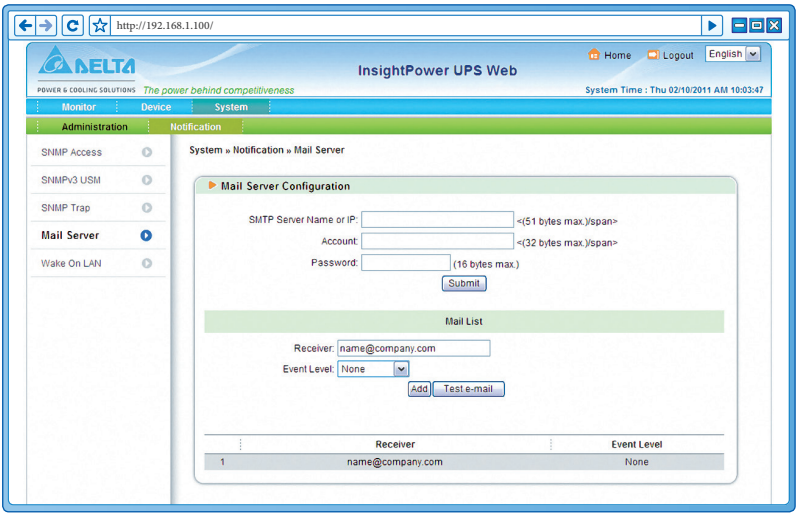
You can determine what event notifications should be sent to the Target IP(s) from **Event Level**. Three Event Levels are listed as follows:

- **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.

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

If a DNS server is not available in the network, you need to manually assign an SMTP server address to enable the E-mail notification system.

- **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 Administration – TCP/ IP***.

- **Account**

  The mail server login account.

- **Password**

  The mail server login password.

- **Receiver**

  The recipients' E-mail addresses.

- **Event Level**

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

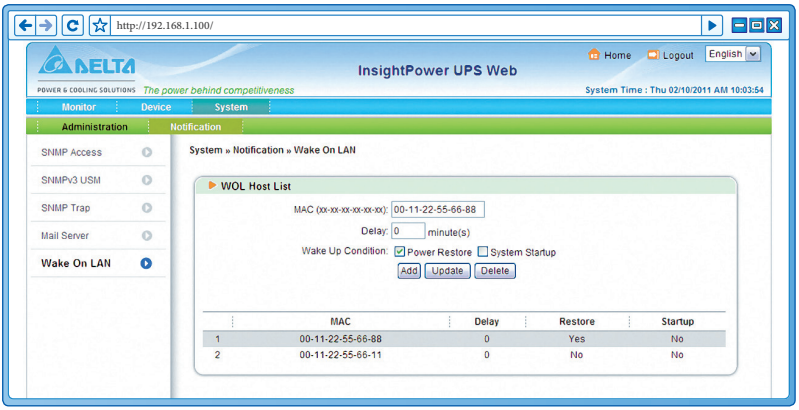
  1) **Information:** All event notifications are sent to the target address.

  2) **Warning:** Warning and Alarm event notifications are sent to the target address.

  3) **Alarm:** Only Alarm event notifications are to the target address.

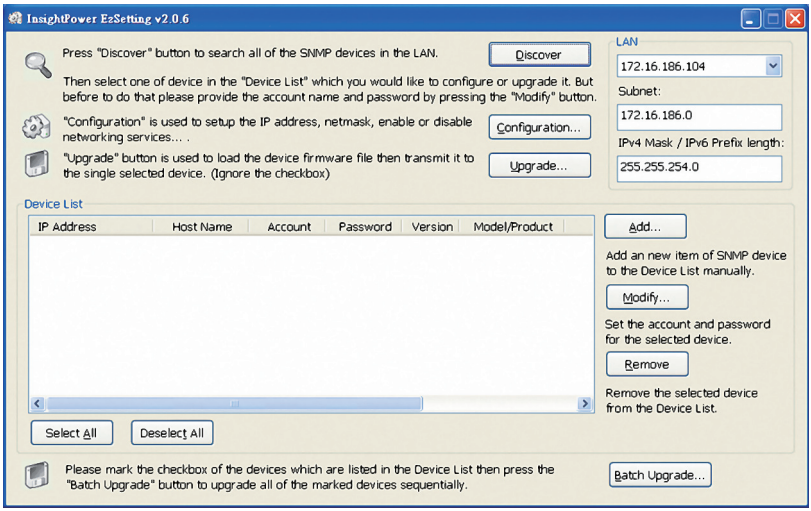
Wake On LAN

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.



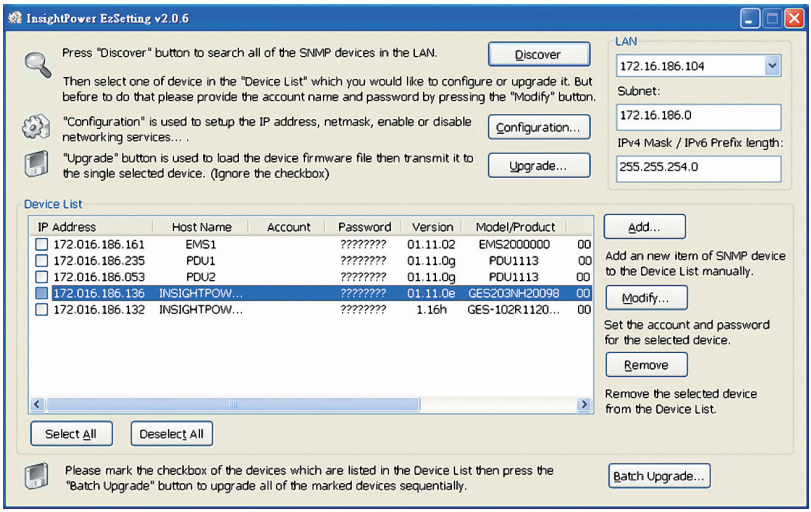
Chapter 6 : SNMP Device Firmware Upgrade

With the provided program EzSetting, you can effortlessly perform a firmware upgrade for SNMP devices discoverable on the LAN. Please refer to the following instructions to upgrade your devices.

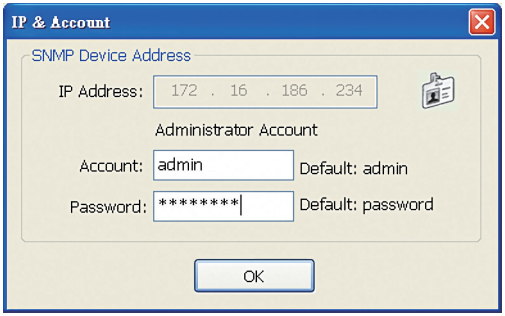


Step 1 The subnet mask allows you to refine the device discovery range in the specified subnets. Make sure the SNMP device you wish to upgrade is in the subnet that is specified. If it is not, please modify the subnet and subnet mask.

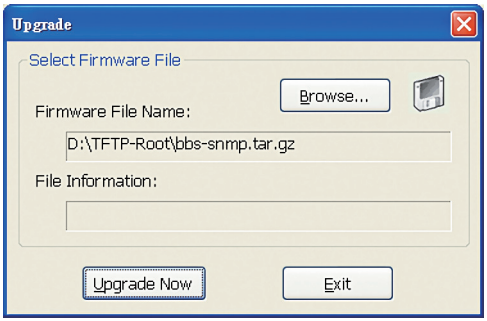
Step 2 Click **Discover**. A list of SNMP devices on the specified subnet is shown.



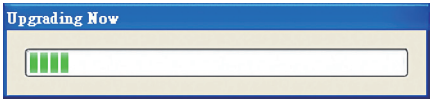
Step 3 Select a device from the Device List, click **Modify**, and key in Administrator account and password.



Step 4 Click **Upgrade**. The upgrade dialog box pops up. Click **Browse** to select a valid SNMP IPv6 firmware binary file. Verify the firmware version listed under File Information, and then click **Upgrade Now** to continue.



Step 5 The upgrade process should take about 20 seconds.



Step 6 When the upgrade is completed, the following dialog box appears. It takes about 1 minute for the device to reboot.

Chapter 7 : Troubleshooting

Q1. How to set up a SNTP server on my workstation for the SNMP IPv6 to synchronize?

To enable SNTP services in Windows XP, go to **Start → Control Panel → Add/ Remove Programs → Add/ Remove Windows Components → Networking Services →** check **Simple TCP/ IP Services → OK**. To enable time synchronization, you need to set SNTP time server addresses in **Time Server**. Please refer to ***Chapter 4: System Configurations***.

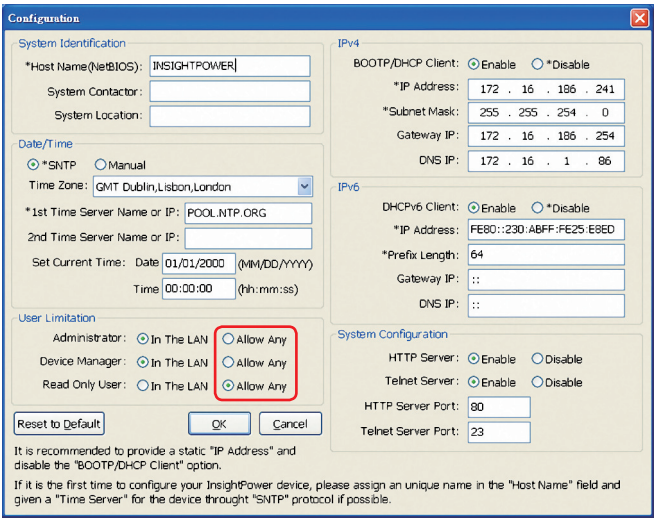
Q2. How to make sure that network connection is established between my workstation and the SNMP IPv6?

To check connection between the SNMP IPv6 and workstation, in Windows please launch DOS prompt mode (**Start → Run →** key in **cmd** and press **Enter**). In Linux, launch Shell. Enter the following command: **ping Host Name** (default: InsightPower). If the connection is correctly established, you should be able to receive replies from the SNMP IPv6.

```
C:\>ping 172.16.186.230

Pinging 172.16.186.230 with 32 bytes of data:
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=4ms TTL=64

Ping statistics for 172.16.186.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms


C:\>
```

Q3. I can access the login page, but cannot log in the InsightPower UPS Web.

Please check the IP addresses of the SNMP IPv6 and the workstation you are trying to log in. The cause could be they are not connected to the same LAN. In that case, launch **EzSetting** and change **User Limitation** settings to **Allow Any**. Please see the following figure.



Q4. How to refresh the NetBIOS table in Windows Systems?

If you 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 one. 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 or shell. After that, you can now connect to the SNMP IPv6 by its Host Name.

Q5. How to obtain the IP address and MAC address from my workstation?

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.

```
Physical Address. . . . . . . . . : 00-23-4D-A2-3A-2C
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ad55:5b9b:74c6:e5fc%12(Preferred)
IPv4 Address. . . . . . . . . . . : 172.16.186.97(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.254.0

C:\>
```

Q6. Unable to ping or connect to the SNMP IPv6?

Check connection by following the measures below.

1) Ensure that your workstation and the SNMP IPv6 are on the same LAN.

2) You can connect to the SNMP IPv6 only when the IP addresses of your workstation and the SNMP IPv6 are from the same address block. Normally, private LANs use IP Addresses from one of the following blocks:

   10.0.0.0~10.255.255.255

   172.16.0.0~172.31.255.255

   192.168.0.0~192.168.255.255

The default IP address (192.168.1.100) for the SNMP IPv6 is on the 192.168.1.1~ 192.168.1.254 block. If your workstation's IP is on a different address block, you will not be able to connect to the SNMP IPv6. To solve this problem, you can either:

1) Use the COM port connection to change the SNMP IPv6's IP address. Please see ***4-4 Configuring through COM port***.

2) Change the workstation's IP address so that they are on the same block. (192.168.1.0~192.168.1.255)

Q7. Unable to perform an SNMP Get operation?

Check the SNMP settings of the SNMP IPv6. Please see ***5-3-2 Notification***. Make sure that the workstation's IP address is added on the NMS IP list with Read or Read/ Write access. The community string on the PC and the SNMP IPv6 must match.

Q8. Unable to perform an SNMP Set operation?

Check the SNMP settings of the SNMP IPv6. Please see ***5-3-2 Notification***. Make sure that the workstation's IP address is added on the NMS IP list, with Read/ Write permission. The community string on the PC and the SNMP IPv6 must match.

Q9. Unable to receive SNMP traps?

Check the SNMP Trap settings of the SNMP IPv6. Please see ***5-3-2 Notification***. Make sure that the workstation's IP address is added on the Target IP list.

Q10. Forgot Administrator account and password?

To reset account and password, connect the RJ45 to DB9 serial cable to the console port. Start Text Mode (Please refer to ***4-4 Configuring through COM Port***), when the login information is prompted, key in **rstadmin** within 30 seconds and then press enter. The Administrator account and password are now reset to default (admin/ password).

Q11. How to enable IPv6 on the SNMP IPv6?

If you are operating in Windows XP, please enable IPv6 first (click **START → RUN**, and enter **ipv6 install**). The SNMP IPv6 supports IPv6, therefore, no additional configuration is required. However, please note that IPv6 is automatically disabled if an identical LLA (Local-link Address) already exists in the LAN. Also, when the IPv4 and IPv6 settings coexist, IPv4 is used as the primary IP address for the SNMP IPv6.

To learn more information regarding IPv6 compatibility, please visit **IETF** (http://tools.ietf.org/html), or **IPv6 Ready Logo Program** (http://www.ipv6ready.org).

Q12. How to generate a private SSL (Secure Socket Layer) certificate file (in PEM format) for HTTP connection?

To ensure connection security between the SNMP IPv6 and your browser, you can create your own SSL certificate file on Linux. Please download and install OpenSSL from http://www.openssl.org. Launch shell and enter the following command to create your own certificate file:

```
Openssl req -x509 -nodes -days 3650 -newkey
rsa:1024 -keyout cert.pem -out cert.pem
```

1) Answer the prompted questions. Proceed as directed by the messages. Once it is completed, a file named **cert.pem** is created in the current working directory.

2) Upload **cert.pem** on the InsightPower UPS Web. Please refer to ***5-3-1 Administration – Web***.

Q13. How to generate DSA and RSA keys for SSH?

For Linux:

1) Please download and install OpenSSH from http://www.openssh.org.

2) Launch shell and enter the following command 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 key files on the InsightPower UPS Web. Please refer to ***5-3-1 Administration – Console*** 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) Select **Conversions → Export OpenSSH Key** and assign a file name to the RSA key. Please ignore it when prompted to provide key passphrase.
5) Select **SSH-2 DSA** from the Parameters area and select **Key → Generate key pair** to generate a DSA key.
6) Select **Export OpenSSH Key** from **Conversions** and assign a file name to the DSA key. Please ignore it when prompted to provide key passphrase.
7) Upload the DSA and RSA key files to the InsightPower UPS Web. Please refer to ***5-3-1 Administration – Console*** for more information.

Q14. 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 Notification – 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 A : Specifications

Model Name	InsightPower SNMP IPv6
Power Input	12 Vdc
Power Consumption	2 Watt (Max.)
Network Connection	RJ-45 jack connector (10/ 100M)
Physical	
Size (W x D)	130 mm x 60 mm
Weight	75 g
Environmental	
Operating Temperature	0 ~ 60℃
Storage Temperature	-40 ~ 125℃
Operating Humidity	0 ~ 90 % (Non-condensing)

NOTE

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

Appendix B : 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.UMEN3915100924-S35111129