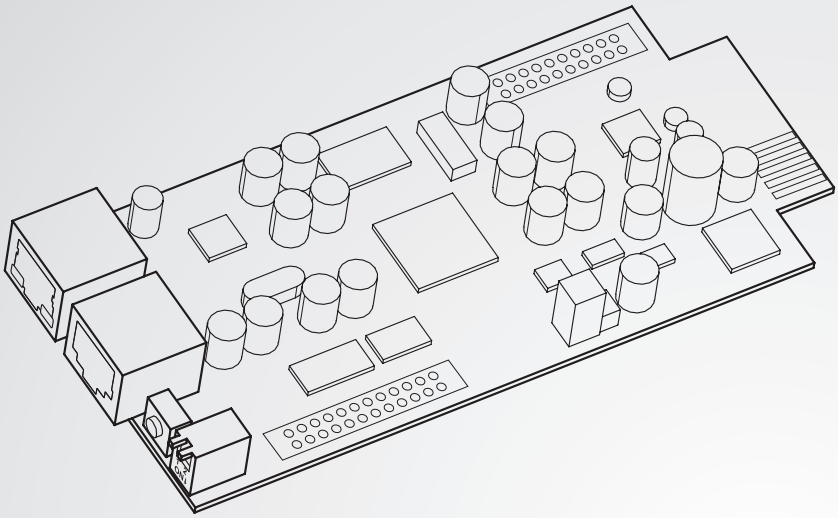


The power behind competitiveness

Delta Infrasuite Power SNMP IPv6 for rSTS

User Manual

www.deltapowersolutions.com

Smarter. Greener. Together.

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.

Electromagnetic Interference

This is a Class A product. In a domestic environment, this product might cause radio interference in which case the user is required to take adequate precaution.

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

  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

Table of Contents

Chapter 1 : Overview

The InsightPower SNMP IPv6 for rSTS (rack static transfer switch), hereafter referred to as SNMP IPv6, is built in the rSTS and is a device that provides an interface between the rSTS and a network. It communicates with the rSTS, acquires its information and remotely manages the rSTS 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. With a network system, you are able to obtain your rSTS's status and manage your rSTS via the SNMP IPv6 easily.

1.1 Features

- **Network rSTS management**

  Allow remote management of the rSTS from any workstation through Internet or Intranet.

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

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

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

  Set the rSTS and system parameters through a Web Browser.

- **Event logs & metering data keeping**

  Provide a history data of the rSTS's power events, power quality and status.

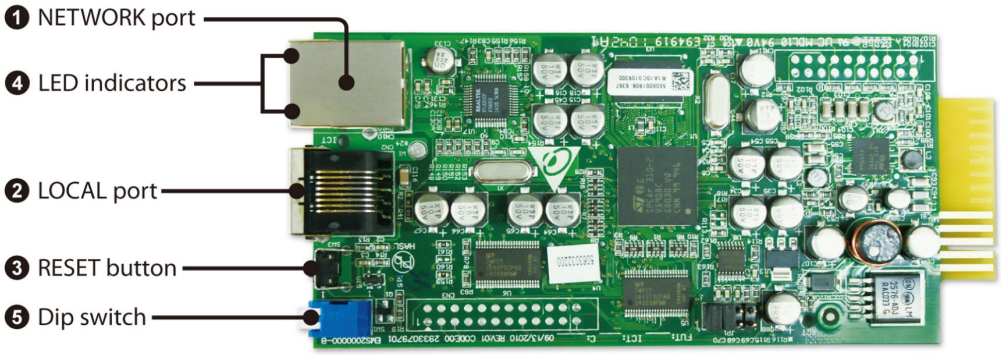
- **Other features and supported protocols include:**

  - 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
  - IPv6 Ready Logo certified (ID ***02-C-000624***)

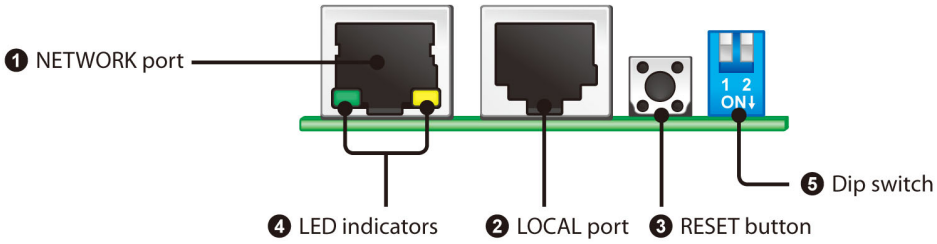
Chapter 2 : Description

The components of SNMP IPv6 are described as below.

- **Top View**



- **Front View**



2.1 Ports

Item	Description	
Network Port	Connect to the Ethernet Network.	
LOCAL Port	1. Connect to a VT100 terminal to configure the system. 2. Connect to an EnviroProbe to monitor the environmental parameter.	
Green LED Indicator	ON	Network connection established and the IP address is usable.
	OFF	Not connected to a network.
	Slow Flash	Faulty IP address.

<table>
<tr><th>Item</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">Yellow LED Indicator</td><td>Rapid Flash</td><td>Normal MODBUS communication.</td></tr>
<tr><td>Slow Flash</td><td>rSTS is now in bootloader mode or can't be communicated with MODBUS.</td></tr>
<tr><td>DIP Switch</td><td colspan="2">Set up the operation mode. Please refer to the following table.
<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 provides rSTS’s status information and parameters through a network system.</td></tr>
<tr><td> 
</td><td>Pass Through Mode</td><td>The SNMP IPv6 stops the communication with rSTS but transfers communication data between its LOCAL port and the rSTS.</td></tr>
<tr><td> 
</td><td>Sensor Mode (with EnviroProbe)</td><td>The SNMP IPv6 works with rSTS and an optional EnviroProbe. It provides not only the rSTS’s status information and parameters, 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 login through the LOCAL port and configure the SNMP IPv6’s settings.</td></tr>
</table></td></tr>
<tr><td>Reset</td><td colspan="2">Reset the InsightPower SNMP IPv6 only. Resetting the SNMP IPv6 does not affect the operation of rSTS.</td></tr>
</table>

NOTE:

During the firmware upgrade period, two LED indicators will both blink rapidly.

Chapter 3 : Initial Configuration

Check your network environment and follow the steps below.

- LAN with **BOOTP/ DHCP** support

  1. Connect the SNMP IPv6 to a network with a networking cable.
  2. Open a Web Browser and link the SNMP IPv6 by using the default host name '**InsightPower**' in the address bar.
  3. Login as an administrator with '**admin**' for default account name and '**password**' for default password.
  4. Open the **User Manager** page to manage your account and password.
  5. On the **User Manager** page, select whether to restrict login users from using different LAN. Select '**Only in this LAN**' to restrict this login account from using different LAN, or select '**Allow Any**' to allow this login account to login from anywhere.
  6. Switch to the **System Configuration** page and change the default host name.
  7. Configure the IP address, Subnet Mask, Gateway IP for the SNMP IPv6. If there is no DNS server and you want to be notified by an e-mail, you need to assign an IP address to the mail server.
  8. We recommend you to disable the '**BOOTP/ DHCP**' option and assign a valid static IP address to the SNMP IPv6.
  9. Open the **Time Server** page to synchronize the SNMP IPv6 and the time server. Please refer to ***3.1 Troubleshooting*** to learn more about how to construct your SNTP server.

- LAN without **BOOTP/ DHCP** support

  1. Prepare a workstation (Microsoft Windows 2000, 2003, 2008, XP, Vista, or 7).
  2. Use the provided RJ45 to DB9 serial cable to connect the SNMP IPv6's COM port with the workstation's COM port.
  3. Set both DIP switches of SNMP IPv6 to '**Normal Mode**' (switched up, refer to ***2.1 Ports***) to enable the network transmission.
  4. For the workstation running Windows 2000, 2003, 2008, or XP, please click the '**HyperTerminal**' icon in '**Accessories Program Group**'. For the workstation running Windows Vista or 7, please download the **Putty** software from the internet to execute the configuration
  5. Set up the COM port's parameters- 2400 bps, 8 data bits, no parity, 1 stop bit and no flow control.

6. Set both of the DIP switches of the SNMP IPv6 to '**Configuration Mode**' (switched down, refer to ***2.1 Ports***). After a message shows up on the screen, key in the **account** (default account name '**admin**') and **password** (default password '**password**'). After that, the SNMP IPv6 Main Menu will show on the screen. Please refer to ***4.4 Configure* the SNMP IPv6 via Text Mode** for more information.

3.1 Troubleshooting

1. How to provide an SNTP (Simple Network Time Protocol) server for SNMP IPv6?

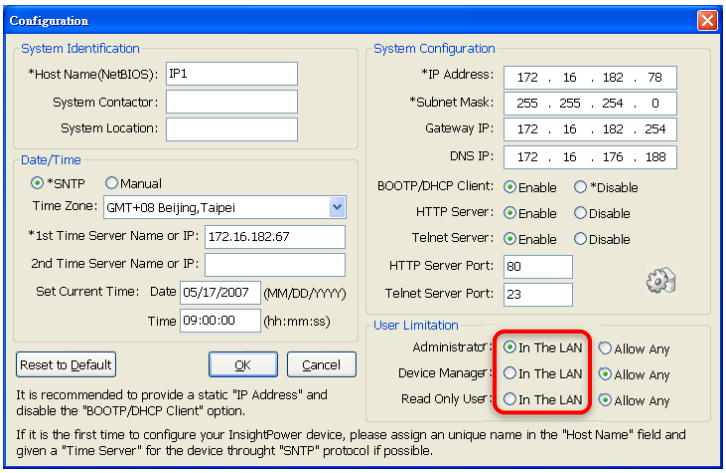
   Answer: In Windows XP operating system, click '**Start**' → select '**Control Panel**' → choose '**Add/ Remove Programs**' → click the '**Add/ Remove Windows Components**' button → click '**Networking Services**' →select the '**Simple TCP/ IP Services**' check box→ and then click **'OK'** to finish the installation of **Simple TCP/ IP Services**. After that, key in the host's IP address on the **Time Server** page.

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

   Answer: Check the network connection by typing the following command '**ping HostName or IP**' at your workstation.

3. In the Web Browser, I see the login page but I cannot login.

   Answer: Please check the IP addresses of the SNMP IPv6 and the PC you try to login. If both IP addresses are not on the same LAN, please run the **EzSetting** to configure the **User Limitation** to '**Allow Any**'. Please refer to ***Figure 3-1***.



(Figure 3-1)

4. How to refresh the NetBIOS table in Windows operating system?

   Answer: Sometimes the IP address of the SNMP IPv6 will change but the host name will remain the same. Although Windows will update its NetBIOS table periodically, you can force it to purge its cache immediately by typing command '**nbtstat –R**' in the shell. After that, you can connect to the SNMP IPv6 by its host name.

5. How to get the IP address and MAC address from my computer?

   Answer: For Windows system, please type '**ipconfig /all**' in DOS prompt. For UNIX system, please key in '**ifconfig**' in the shell.

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

   Answer: Follow the measures below.

   1) Check all network connections.
   2) Ensure that your PC and the SNMP IPv6 are in the same network segment. If you don't have a router, they must be in the same network segment.
   3) You can connect to the SNMP IPv6 only when your PC and SNMP IPv6 use IP Addresses from the same address block. Normally, private LANs use the 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 SNMP IPv6's default IP Address (192.168.1.100) is from the last block. If your LAN is using a different address block, you will not be able to connect to the SNMP IPv6 via the LAN.

      Under such condition, you can choose to:

      - Use the **Terminal Mode** to reset the SNMP IPv6's IP Address.
      - Change your PC's IP Address to allow connection via the LAN.

7. Unable to perform SNMP Get operation?

   Answer: Check the SNMP settings stored in the SNMP IPv6. The IP Address of the PC you are using must be entered in one of the SNMP Access Control NMS IP fields, with Read or Read/Write permission. The community string on the PC and the SNMP IPv6 must match.

8. Unable to perform SNMP Set operation?

   Answer: Check the SNMP settings stored in the SNMP IPv6. The IP Address of the PC you are using must be entered in one of the SNMP Access Control NMS IP fields, with Read/Write permission. The community string on the PC and the SNMP IPv6 must match.

9. Unable to receive traps at my management station?

   Answer: Check the SNMP Trap settings on the SNMP IPv6. The IP Address of the PC you are using must be entered in one of the Target IP fields.

10. Forgot the administrator's account and password?

    Answer: Connect the RJ45 to DB9 serial cable to the console port and set both of the DIP switches of the SNMP IPv6 to '**Configuration Mode**' (switched down, refer to ***Chapter 2.1 Ports***). Key in '**rstadmin**' within 30 seconds while the **account** and **password** are prompted. After that, the administrator's account and password are now reset to default.

11. About IPv6 support?

    Answer:

    1) For every device that supports IPv6, you will find a LLA (Link Local Address) generated according to its own MAC address and the EUI-64 standard algorithm. For example, if the MAC address is **00:11:22:33:44:55**, the according LLA will be fe80::**211**:**22**ff:fe**33**:**4455**. As this SNMP IPv6 can support IPv6, you can directly link the SNMP IPv6 via LLA without any additional configuration. You should note that, according to RFC-4862, the IPv6 interface will automatically shutdown if the same LLA has already existed on the LAN.
    2) If the IPv4 and IPv6 DNS configurations co-exist, the IPv4 DNS configuration becomes the top priority.
    3) If your operating system is Windows XP, please enable IPv6 first (select '**RUN**' from '**START**' and enter '**ipv6 install**').
    4) To know more about IPv6 compatibility information, please refer to RFC documents (1981, 2460, 4861, 4862, and 4443) on the **IETF** website (http://tools.ietf.org/html), or refer to IPv6 Ready Logo website (http://www.ipv6ready.org).

12. How to generate a private SSL certificate file (PEM format) for HTTPS?

Answer:

1) Please download the openssl from http://www.openssl.org and install it in the Linux.
2) Open the command shell and key in the following command to create your own certificate file:

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

3) Answer to the questions. Once it is completed, the cert.pem will be created in the current working directory.
4) Upload the cert.pem file to the SNMP IPv6 through the web page, please refer to the ***Chapter 5.3.3***.

13. How to generate the SSH DSA and RSA keys for SSH?

Answer: Refer to ***Appendix C. Key Generation for SSH***.

Chapter 4 : Configuration Methods

The easiest way to configure the SNMP IPv6 is to run the **EzSetting** software, which you can find in the CD. If you have configured the essential network parameters successfully, you can launch a Web Browser or telnet to the SNMP IPv6 to execute more detailed configuration. The first thing is to open the User Manager page to change your account and password.

4.1 Configure the SNMP IPv6 by EzSetting

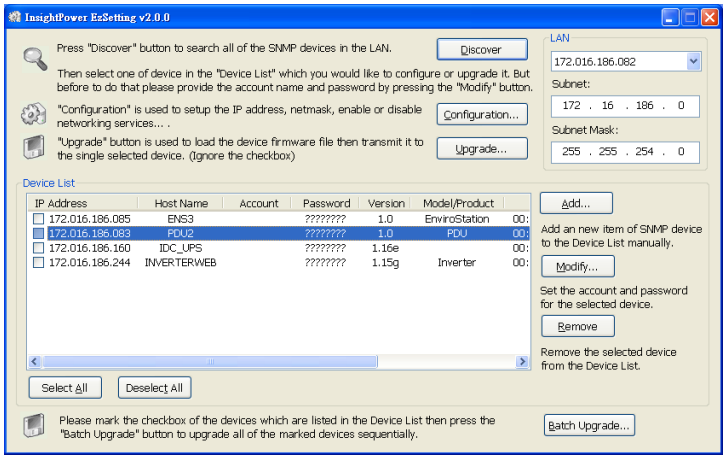
1. Prepare a workstation (Microsoft Windows 2000, 2003, 2008, XP, Vista, Win7 or later installed).

2. Make sure both of the DIP switches of the SNMP IPv6 are set to '**Normal Mode**' (switched up, refer to ***Chapter 2.1 Ports***) to enable a network transmission.

3. Make sure the workstation and the SNMP IPv6 are on the same LAN.

4. Go to link **http://datacenter-softwarecenter.deltaww.com** to launch the **EzSetting** software.

5. Press the '**Discover**' button to search all of the InsightPower devices on the LAN, and then all of the InsightPower devices will be listed on the **Device List** as shown in ***Figure 4-1***.

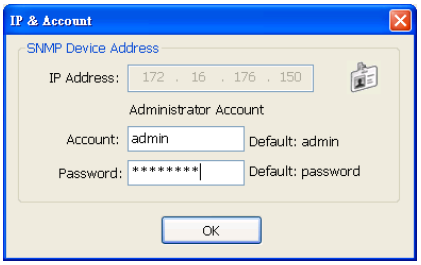


(Figure 4-1)

6. If you want to search all of the InsightPower devices in a different domain network, just change the '**Subnet**' and '**Subnet Mask**' addresses and then press the '**Discover**' button to list them.

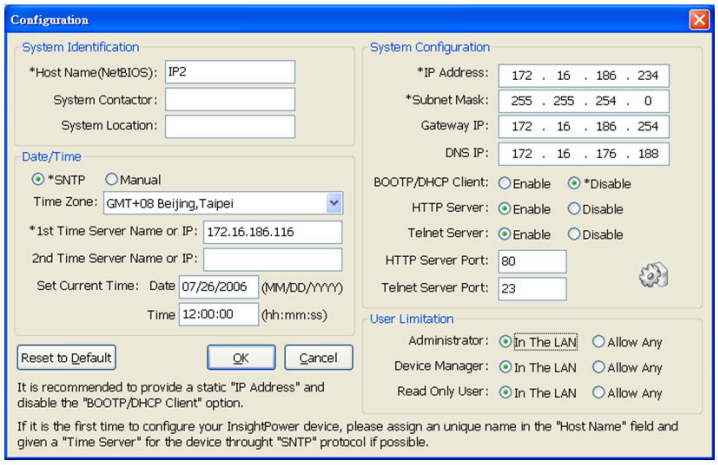
7. If the SNMP IPv6 cannot be found, check the networking port UDP 3456 in the OS. Open it if it is blocked.

8. Select ‘**SNMP IPv6**’ device in the **Device List** to configure the network parameters and then click the ‘**Modify**’ button to key in your ‘account’ and ‘**password**’. The default account and password are ‘admin’ and ‘**password**’ respectively. Please see ***Figure 4-2***.



(Figure 4-2)

9. Click the ‘**Configuration**’ button and set up the essential network parameters as shown in ***Figure 4-3***.



(Figure 4-3)

4.2 Configure the SNMP IPv6 through LOCAL Port

The easiest way to configure the SNMP IPv6 is to run the **EzSetting** software, which you can find via the link: **http://datacenter-softwarecenter.deltaww.com**. If you have configured the essential network parameters successfully, you can launch a Web Browser or telnet to the SNMP IPv6 to execute more detailed configuration. The first thing is to open the User Manager page to change your account and password.

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

2. Use a Delta Model #301814175 RJ45 to DB9 serial cable to connect the SNMP IPv6’s LOCAL port with the workstation’s COM port.

3. Set both of the DIP switches of the SNMP IPv6 to **'Normal Mode'** (switched up, refer to ***Chapter 2.1 Ports***) to enable a network transmission.

4. For the workstation running Windows 2000, 2003, 2008, or XP, please click the '**HyperTerminal**' icon in the '**Accessories Program Group**'. For the workstation running Windows Vista or 7, please download the **Putty** software from the internet to execute the configuration.

5. Set up the COM port's parameters- 2400 bps, 8 data bits, no parity, 1 stop bit and no flow control.

6. Set both DIP switches of the SNMP IPv6 to '**Configuration Mode**' (switched down, refer to ***Chapter 2.1 Ports***). After a message displays on the screen, key in the **account** (default account is 'admin') and password (default password is '**password**'). After that, the **SNMP IPv6 Main Menu** will show on the screen. Please refer to ***Chapter 4.3 Configure the SNMP IPv6 via Text Mode*** for more information.

4.2.1 Cable Specification

- Only Delta Model #30814175 cables can be used because they have been custom-specified to have pin #1 disconnected. You can buy these cables from Delta using the following information:

  Model: 30814175

  Specification: Cable

  Minimum Order Quantity is 201 pcs. Quantity ordered should be a multiple of 3.

  DEI Logistics (USA) Corporation 4405 Cushing Parkway Fremont,
  CA 94538 USA Telephone: 1-510-668-5188

- Why is it important that pin 1 is disconnected?

  Pin 1 on the RJ45 port provides access to 12V power from the rSTS, but it is not needed for console management. If a cable that allows pin 1 connection is used, too much current may be drawn through pin 1. And this will cause the 1-ohm resistor inside the rSTS to become overheated. The overheat can lead to a cracking damage that blocks the current and ultimately a shutting down of the SNMP IPv6 (see "**Delta rSTS Series User Manual**" ***Chapter 7: Troubleshooting***).

4.3 Configure the SNMP IPv6 via Text Mode

You can configure the SNMP IPv6 via text mode by using a Telnet utility or through the LOCAL port. Please see below for **SNMP IPv6 Main Menu** description.

4.3.1 SNMP IPv6 Main Menu

```
+========================+
|   Web Card Main Menu   |
+========================+
Web Card Version 01.12.14e
MAC Address 00-18-23-1f-72-81
[1].User Manager
[2].TCP/IP Setting
[3].Network Parameter
[4].Time Server
[5].Soft Restart
[6].Reset All To Default
[d].Device Communication
[z].Exit Without Save
[0].Save And Exit

Please Enter Your Choice => _
```

Items in this **SNMP IPv6 Main Menu** are described in the following pages.

4.3.1.1 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:  Allow Any
    Device Manager
[8].Account:     device
[9].Password:    ********
[a].Limitation:  Allow Any
    Read Only User
[b].Account:     user
[c].Password:    ********
[d].Limitation:  Allow Any
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Function	Description	Default
❶	RADIUS Auth	Obtain the login authentication from a RADIUS server.	Disable
❷	Server	The RADIUS server name.	
❸	Secret	The RADIUS secret.	
❹	Port	The RADIUS port number.	1812
❺	Administrator Account	The Administrator has the sole right to modify the InsightPower settings.	admin
❻	Administrator Password		password
❼	Administrator Limitation	Restrict the login area for the administrator.	Only in this LAN
❽	Device Account	Device Manager is not permitted to change network settings but has the right to configure device settings.	device
❾	Device Password		password
a	Device Limitation		Only in this LAN
b	User Account	Read Only. User can observe the DEVICE information only.	user
c	User Password		password
d	User Limitation	Restrict login area for the user.	Allow Any

4.3.1.2 TCP/ IP Setting

```
+=========================+
|     TCP/IP Setting      |
+=========================+
[1].IPv4 Address:          10.0.10.186
[2].IPv4 Subnet Mask:      255.255.255.0
[3].IPv4 Gateway IP:       10.0.10.254
[4].IPv4 DNS or WINS IP:10.0.10.254
[5].DHCPv4 Client:         Disable
[6].IPv6 Address:          fe80::230:abff:feaa:ff09
[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:      Disable
[f].Speed:                 100M
[g].Duplex:                Full
[i].Telnet Idle Time:      60 Seconds
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Function	Description	Default
1	IPv4 Address	The InsightPower IPv4 address	192.168.001.100
2	IPv4 Subnet Mask	The IPv4 sub-net mask setting	255.255.255.000
3	IPv4 Gateway IP	The IPv4 network default gateway	192.168.001.254
4	IPv4 DNS IP	IPv4 Domain Name Server IP address	
5	DHCPv4 Client	Enable/ Disable DHCPv4 protocol	Enable
6	IPv6 Address	The InsightPower IPv6 address	
7	IPv6 Subnet Mask	The IPv6 sub-net mask setting	
8	IPv6 Gateway IP	The IPv6 network default gateway	
9	IPv6 DNS IP	IPv6 Domain Name Server IP address	
a	DHCPv6 Client	Enable/ Disable DHCPv6 protocol	Enable
b	Host Name	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	The network link operation.	Enable
f	Speed		100M
g	Duplex		Full
i	Telnet Idle Time	Timeout for telnet.	

4.3.1.3 Network Parameter

```
+=======================+
|   Network Parameter    |
+=======================+
[1].HTTP Server:          Enable
[2].HTTPS Server:         Enable
[3].Telnet Server:        Disable
[4].SSH/SFTP Server:      Enable
[5].FTP Server:           Enable
[6].Syslog:               Disable
[7].HTTP Server Port:     80
[8].HTTPS Server Port:    443
[9].Telnet Server Port:   23
[a].SSH Server Port:      22
[b].FTP Server Port:      21
[c].Syslog Server1:
[d].Syslog Server2:
[e].Syslog Server3:
[f].Syslog Server4:
[g].SNMP Get,Set Port:    161
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Function	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	Disable
4	SSH/SFTP Server	Enable/ Disable SSH/SFTP protocol	Enable
5	FTP Server	Enable/ Disable FTP protocol	Enable
6	syslog	Enable/ Disable remote syslog	Disable
7	HTTP Server Port	HTTP networking port	80
8	HTTPS Server Port	HTTP 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

4.3.1.4 Time Server

There are two ways to set the SNMP IPv6's current time and date. One is to set the system time manually, but this is not the best way. The ideal way is to set up a time server for the SNMP IPv6. The SNMP IPv6 can support SNTP, which is supported by MS Windows XP.

To configure a Windows PC to act as a time server, please install the '**Simple TCP/IP Services**' from the **Add/Remove Windows Components**.

```
+=======================+
|        Time Server     |
+=======================+
[1].Time Selection:      SNTP
[2].Time Zone:           +0 hr
[3].1st Time Server:
[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.	Function	Description	Default
1	Time Selection	Select SNTP or manually	SNTP
2	Time Zone	Select time zone	+0 hr
3	1st Time Server	The first time server for SNTP	
4	2nd Time Server	The second time server for SNTP	
5	Manual Date	Assign the date manually if the Time Selection is selected to Manual	01/ 01/ 2000
6	Manual Time	Assign the time manually if the Time Selection is selected to Manual	00:00:00

4.3.1.5 Device Communication

Enter rSTS Command Mode.

4.3.1.6 Soft Restart

Simply restart the SNMP IPv6 and it will not affect the rSTS.

4.3.1.7 Reset All To Default

Set all of the settings back to the original default settings.

4.3.1.8 Exit Without Save

Exit and disregard any change.

4.3.1.9 Save And Exit

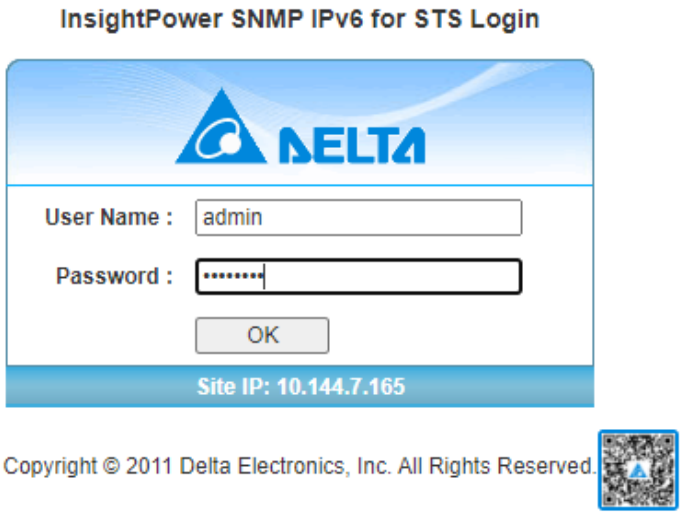
Save your change(s) and exit.

Chapter 5 : Web Interface

5.1 Run a Web Browser

1. Make sure that you have a **TCP/ IP** network installed already.

2. Start your Web Browser. Enter '**http: //host_name**' or '**http: //ip_address**' in the address bar for the plain text web transmission and '**https: //host_name**' or '**https: //ip_address**' for the encrypted web transmission. The SNMP IPv6 will then ask your account and password. After keying in the correct account and password, the **SNMP IPv6 Management Home Page** will appear on the screen.



3. If the login page can be displayed but you are unable to login with the correct account and password, it might be because that the IP address where you login is different from the SNMP IPv6's IP address subnet. Please refer to ***3.1 Troubleshooting*** Point 3 to solve this issue.

NOTE:

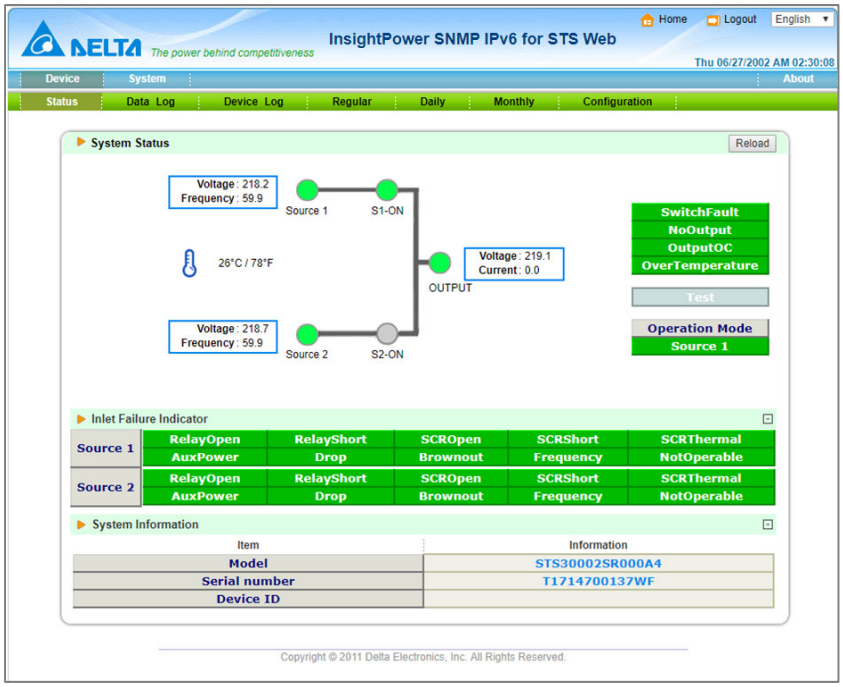
The SNMP IPv6 will logout the user automatically if there is no any data transmission through HTTP/HTTPS for more than **30** minutes.

5.2 Device Management

This category includes most usable information of the rSTS. You can also configure some specific rSTS parameters here.

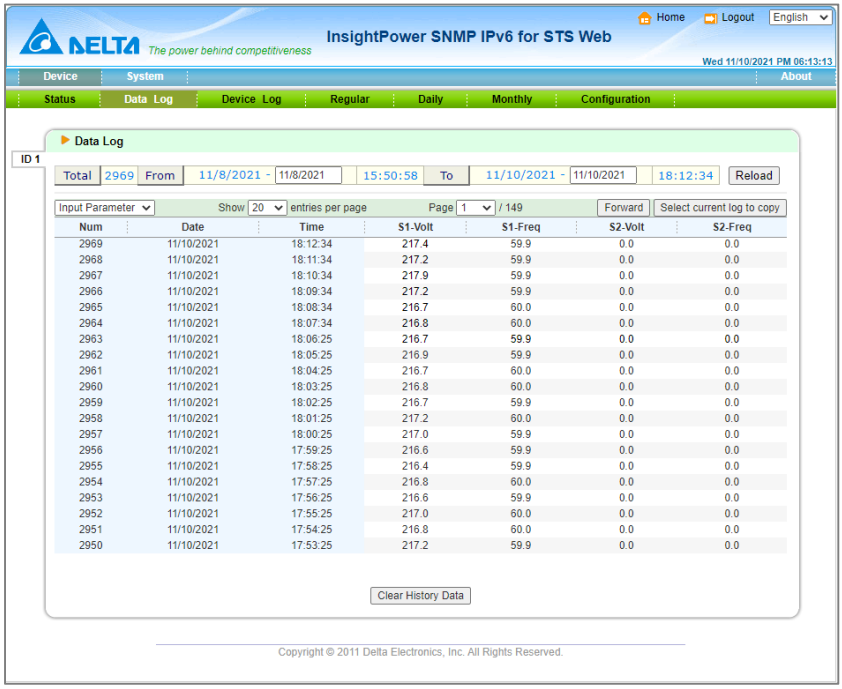
5.2.1 rSTS Status

This page reports the summary information of rSTS.



5.2.2 Data Log

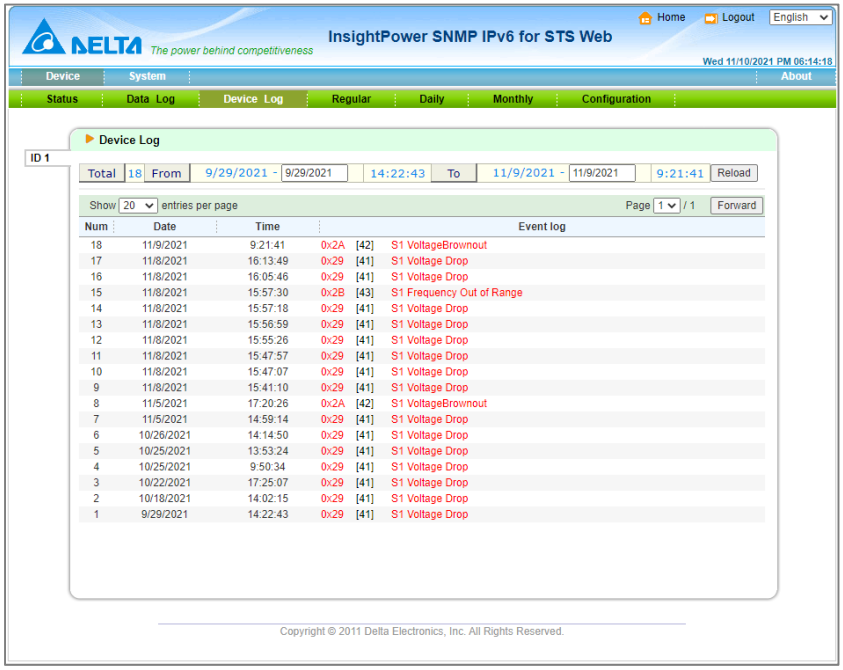
This page shows all recorded parameters, including flow information, measured data and configurations. The built-in memory can record 8000 data logs at maximum.



Num	Date	Time	S1-Volt	S1-Freq	S2-Volt	S2-Freq
2969	11/10/2021	18:12:34	217.4	59.9	0.0	0.0
2968	11/10/2021	18:11:34	217.2	59.9	0.0	0.0
2967	11/10/2021	18:10:34	217.9	59.9	0.0	0.0
2966	11/10/2021	18:09:34	217.2	59.9	0.0	0.0
2965	11/10/2021	18:08:34	216.7	60.0	0.0	0.0
2964	11/10/2021	18:07:34	216.8	60.0	0.0	0.0
2963	11/10/2021	18:06:25	216.7	59.9	0.0	0.0
2962	11/10/2021	18:05:25	216.9	59.9	0.0	0.0
2961	11/10/2021	18:04:25	216.7	60.0	0.0	0.0
2960	11/10/2021	18:03:25	216.8	60.0	0.0	0.0
2959	11/10/2021	18:02:25	216.7	59.9	0.0	0.0
2958	11/10/2021	18:01:25	217.2	60.0	0.0	0.0
2957	11/10/2021	18:00:25	217.0	59.9	0.0	0.0
2956	11/10/2021	17:59:25	216.6	59.9	0.0	0.0
2955	11/10/2021	17:58:25	216.4	59.9	0.0	0.0
2954	11/10/2021	17:57:25	216.8	60.0	0.0	0.0
2953	11/10/2021	17:56:25	216.6	59.9	0.0	0.0
2952	11/10/2021	17:55:25	217.0	60.0	0.0	0.0
2951	11/10/2021	17:54:25	216.8	60.0	0.0	0.0
2950	11/10/2021	17:53:25	217.2	59.9	0.0	0.0

5.2.3 Device Log

This page shows the inner rSTS log information. Built-in memories record at maximum 1000 device logs.



Num	Date	Time			Event log
18	11/9/2021	9:21:41	0x2A	[42]	S1 VoltageBrownout
17	11/8/2021	16:13:49	0x29	[41]	S1 Voltage Drop
16	11/8/2021	16:05:46	0x29	[41]	S1 Voltage Drop
15	11/8/2021	15:57:30	0x2B	[43]	S1 Frequency Out of Range
14	11/8/2021	15:57:18	0x29	[41]	S1 Voltage Drop
13	11/8/2021	15:56:59	0x29	[41]	S1 Voltage Drop
12	11/8/2021	15:55:26	0x29	[41]	S1 Voltage Drop
11	11/8/2021	15:47:57	0x29	[41]	S1 Voltage Drop
10	11/8/2021	15:47:07	0x29	[41]	S1 Voltage Drop
9	11/8/2021	15:41:10	0x29	[41]	S1 Voltage Drop
8	11/5/2021	17:20:26	0x2A	[42]	S1 VoltageBrownout
7	11/5/2021	14:59:14	0x29	[41]	S1 Voltage Drop
6	10/26/2021	14:14:50	0x29	[41]	S1 Voltage Drop
5	10/25/2021	13:53:24	0x29	[41]	S1 Voltage Drop
4	10/25/2021	9:50:34	0x29	[41]	S1 Voltage Drop
3	10/22/2021	17:25:07	0x29	[41]	S1 Voltage Drop
2	10/18/2021	14:02:15	0x29	[41]	S1 Voltage Drop
1	9/29/2021	14:22:43	0x29	[41]	S1 Voltage Drop

5.2.4 Essential Log

Show outlet parameters and temperature history.

- **Regular**

  Every 5 minutes record one data and a record of 31 days at maximum will be kept.

Date	Time	Max-V	Avg-V	Min-V	Max-I	Avg-I	Min-I	Max-TC	Avg-TC	Min-TC
11/23/2015	19:20:00	219.1	219.1	219.1	0.0	0.0	0.0	32	32	32
11/23/2015	19:18:15	219.5	218.9	218.2	0.0	0.0	0.0	32	32	32
11/23/2015	19:10:00	219.9	219.9	219.9	0.0	0.0	0.0	32	32	32

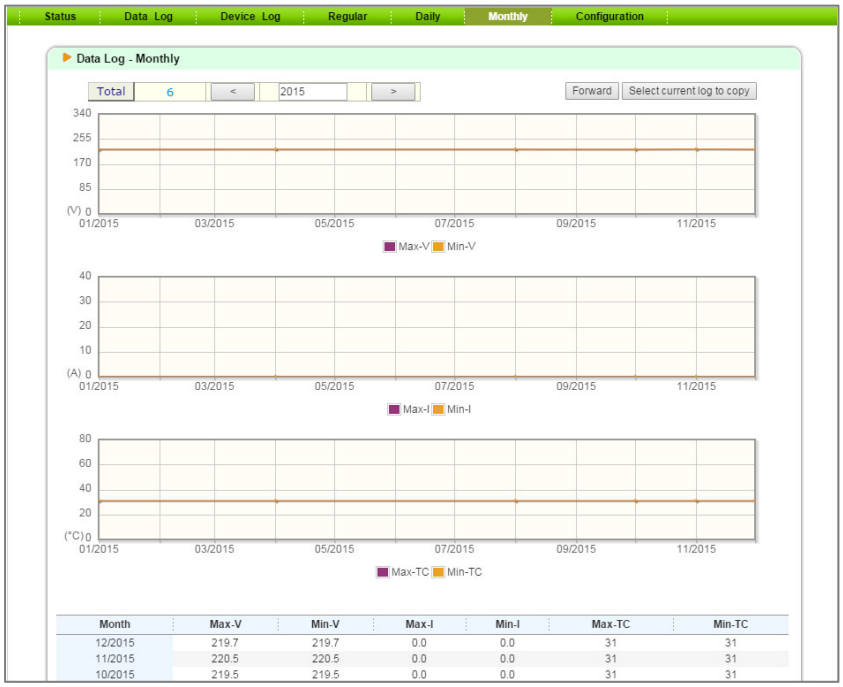
- **Daily**

It records maximum and minimum data of each day, up to 12 months.

Date	Max-V	Min-V	Max-I	Min-I	Max-TC	Min-TC
11/25/2015	220.5	220.5	0.0	0.0	31	31
11/23/2015	220.7	215.9	0.0	0.0	33	31
11/22/2015	220.5	220.5	0.0	0.0	31	31

- **Monthly**

  It record maximum and minimum data of each month, up to 10 years.

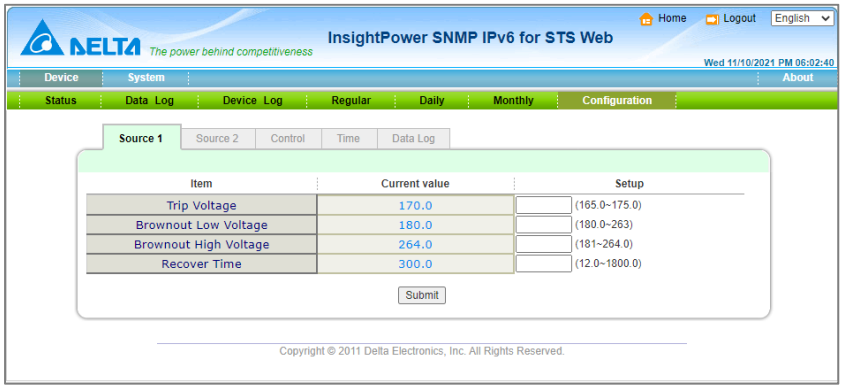


Month	Max-V	Min-V	Max-I	Min-I	Max-TC	Min-TC
12/2015	219.7	219.7	0.0	0.0	31	31
11/2015	220.5	220.5	0.0	0.0	31	31
10/2015	219.5	219.5	0.0	0.0	31	31

5.2.5 Configuration

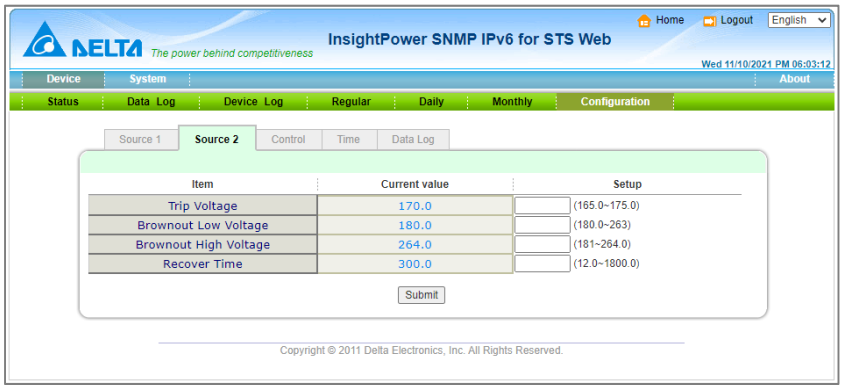
Select **Configuration** from the green bar to configure rSTS parameters. This includes source configuration, flow control, local time and data log.

- **Source 1 Configuration**



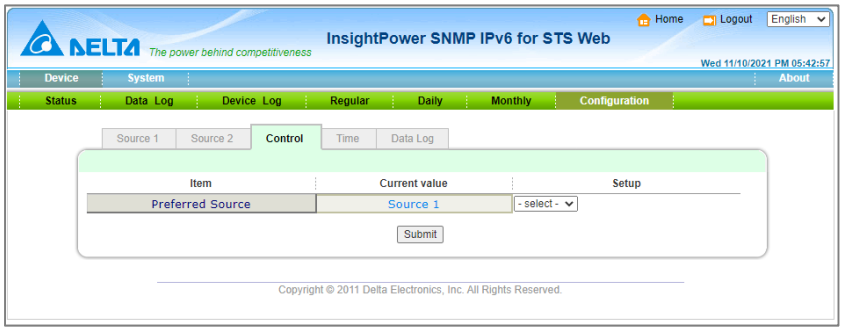
Item	Default Setting Value	Setting Range	Description
Trip Voltage	170	165-175	S1 Voltage Dropout ≤ setting value, rSTS will transfer to S2.
Brownout Low Voltage	180	180-263	S1 Voltage Brownout ≤ setting value, rSTS will transfer to S2.
Brownout High Voltage	264	181-264	S1 Voltage Brownout ≥ setting value, rSTS will transfer to S2.
Recover Time	300	12~1800	S1 High/ Low Voltage Recover Time

- **Source 2 Configuration**



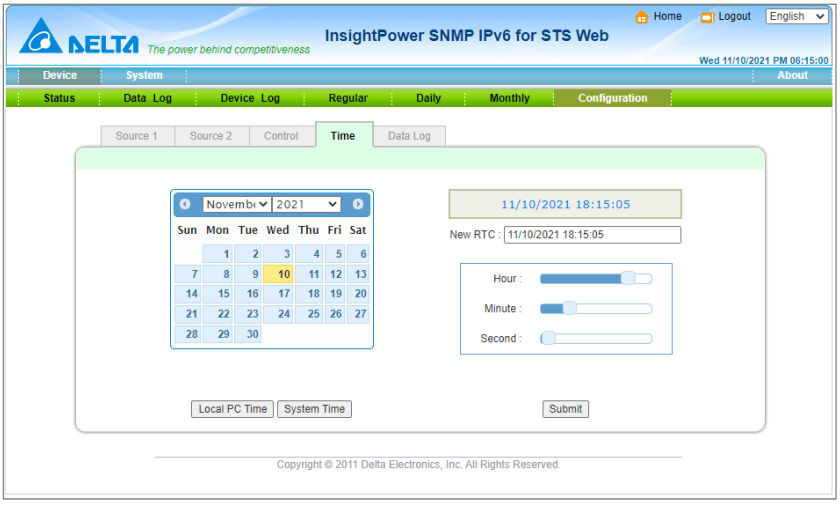
Item	Default Setting Value	Setting Range	Description
Trip Voltage	170	165-175	S2 Voltage Dropout ≤ setting value. rSTS will Transfer to S1
Brownout Low Voltage	180	180-263	S2 Voltage Brownout ≤ setting value, rSTS will Transfer to S1
Brownout High Voltage	264	181-264	S2 Voltage Brownout ≥ setting value, rSTS will transfer to S1
Recover Time	300	12~1800	S2 High/ Low Voltage Recover Time

- **Flow Control**



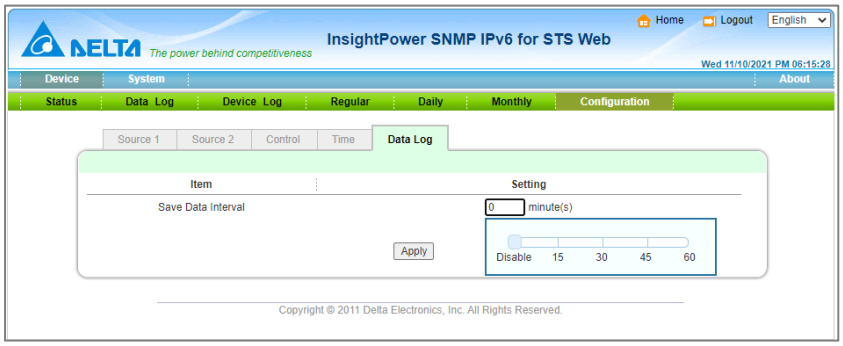
Item	Description	Default Setting Value
Preferred Source	Select priority source	Source 1

- **Local Time**



- **Data Log**

The built-in memory can record 8000 data logs at maximum.

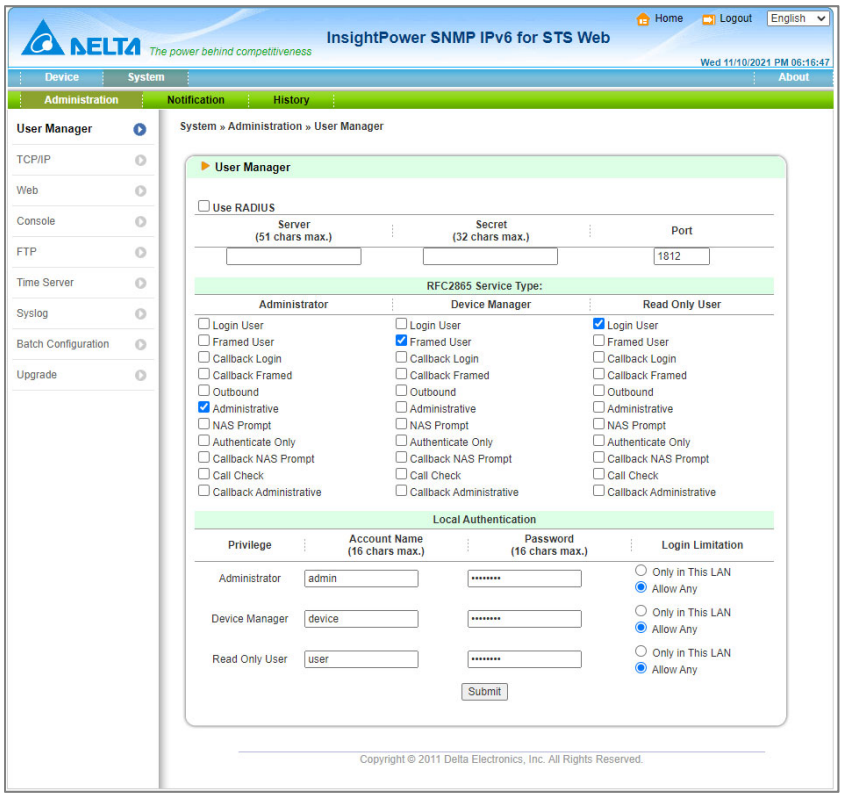


Item	Description	Default Setting Value
Save Data Interval	This value is used to set the time interval for saving the rSTS measuring data in the data log.	0 minutes (Disable)

5.3 System Administration

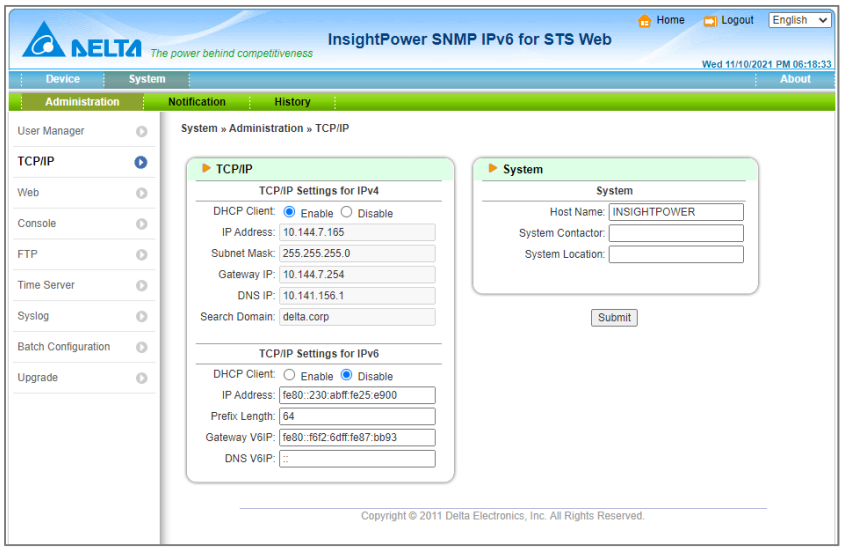
5.3.1 User Manager

The SNMP IPv6 supports the RADIUS. You can assign your RADIUS server to the card for login authentication through HTTP, Telnet, SSH, FTP, SFTP and EzSetting. If the RADIUS option is disabled, you can still manage the login authentication locally by assigning 3 different levels of users' account and password.



5.3.2 TCP/ IP

This menu allows the administrator to set the local network configuration parameters in SNMP IPv6.



5.3.2.1 IPv4

DHCP Client: Enable/ Disable DHCP to get the IP address from DHCP server.

IP Address: The IP address of the card in dotted format (e.g. 192.168.1.100).

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

Gateway IP: The IP address of the network gateway in dotted format (e.g. 192.168.1.254).

DNS IP: The IP address of the domain name server in dotted format (e.g. 192.168.1.1).

Search Domain: The system domain name. If the host name you provide cannot be searched, then the system will append the search domain to your host name.

5.3.2.2 IPv6

DHCP Client: Enable/ Disable DHCP to get the IP address from DHCP server.

IP Address: The IPv6 address of the card.

Prefix Length: The prefix length used for the IPv6 network.

Gateway V6IP: The IP address of the IPv6 network gateway.

DNS V6IP: The IP address of the IPv6 domain name server.

5.3.2.3 System

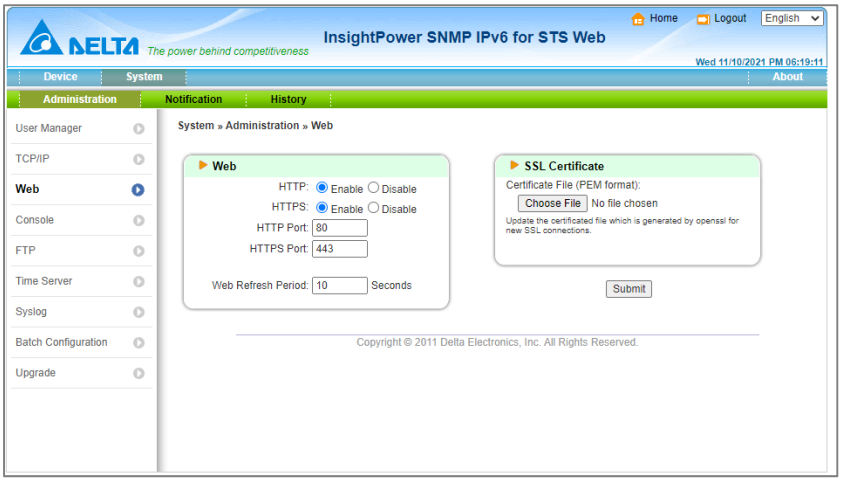
Host Name: The SNMP host name in the network.

System Contact: The system contactor information for SNMP network administration string.

System Location: The system installed location for SNMP network administrator string.

5.3.3 WEB

This menu allows the administrator to enable or disable the HTTP/ HTTPS communication protocols available in the SNMP IPv6



5.3.3.1 Web

HTTP: Enabling or disabling the HTTP connection with the SNMP IPv6.

HTTPS: Enabling or disabling the HTTPS connection with the SNMP IPv6.

HTTP Port: Users may configure HTTP protocol to use a port number other than standard HTTP port (80).

HTTPS Port: Users may configure HTTPS protocol to use a port number other than the standard HTTPS port (443).

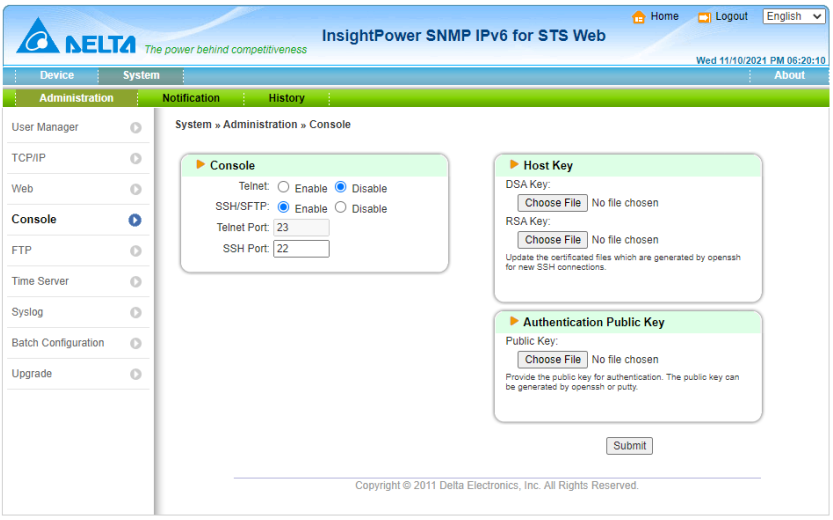
Web Refresh Period: The period of time to update web pages.

5.3.3.2 SSL Certificate

Certificate File: This option is used to replace your own SSL certificate file. The SNMP IPv6 supports the PEM format that is generated by OpenSSL. Please refer to item12 in ***Chapter 3.1 Trouble Shooting***.

5.3.4 Console

This menu allows the administrator to enable or disable the Telnet/SSH communication protocols available in SNMP IPv6.



5.3.4.1 Console

Telnet: Enabling or disabling the Telnet connection with the SNMP IPv6.

SSH/ SFTP: Enabling or disabling the SSH/SFTP connection with the SNMP IPv6.

Telnet Port: Users may configure the Telnet protocol to use a port number other than the standard Telnet port (23).

SSH Port: Users may configure the SSH protocol to use a port number other than the standard SSH port (22).

5.3.4.2 Host Key

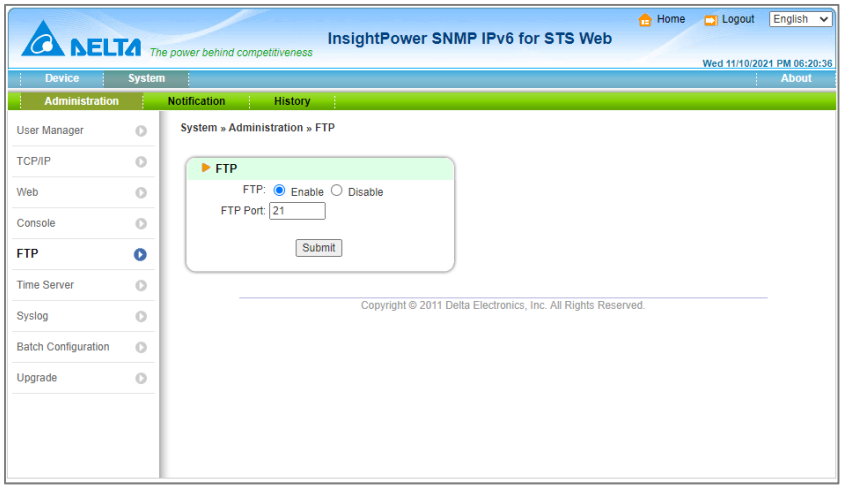
DSA/ RSA Key: These options are used for the replacement of your own SSH keys. The SNMP IPv6 supports the key files that are generated by the OpenSSH. Please refer to item 13 in ***Chapter 3.1 Trouble Shooting***.

5.3.4.3 Authentication Public Key

Public Key: The SNMP IPv6 supports login without entering password via the SSH.

5.3.5 FTP

This menu allows the administrator to enable or disable the FTP communication protocols available in the SNMP IPv6.



5.3.5.1 FTP

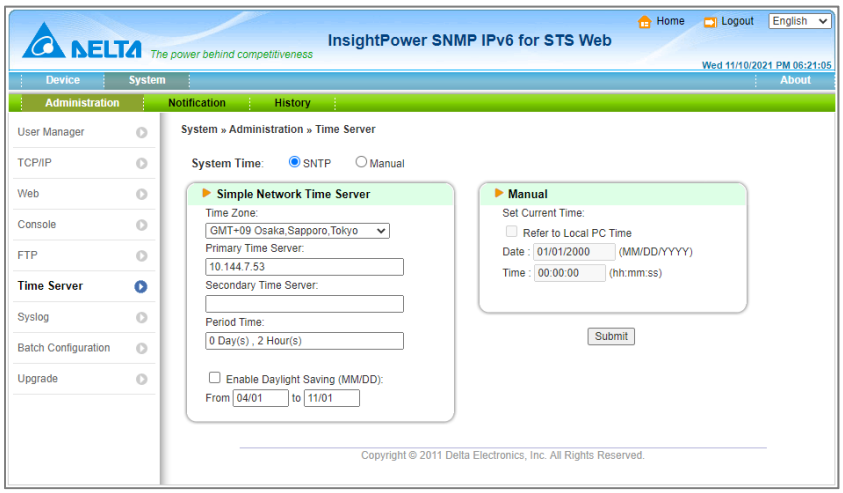
FTP: Enabling or disabling the FTP connection with the SNMP IPv6.

FTP Port: Users may configure the FTP protocol to use a port number other than the standard FTP port (21).

5.3.6 Time Server

This menu allows you to set the SNMP IPv6 internal date and time. There are 2 ways to set the date and time: synchronization with the SNTP server or manually setup for the date and time.

Please note that if the SNTP is enabled but no reply is received from the assigned time server, the event log and data log will not work.



5.3.6.1 Simple Network Time Server

Time Zone: Select the time zone where the SNMP IPv6 is installed.

Primary/ Secondary Time Server: The SNMP IPv6 searches both time servers and follows time of the server that replies first. The card synchronizes with the time server every two hours by default.

Period Time: The time interval that the SNMP IPv6 synchronizes with the SNTP server.

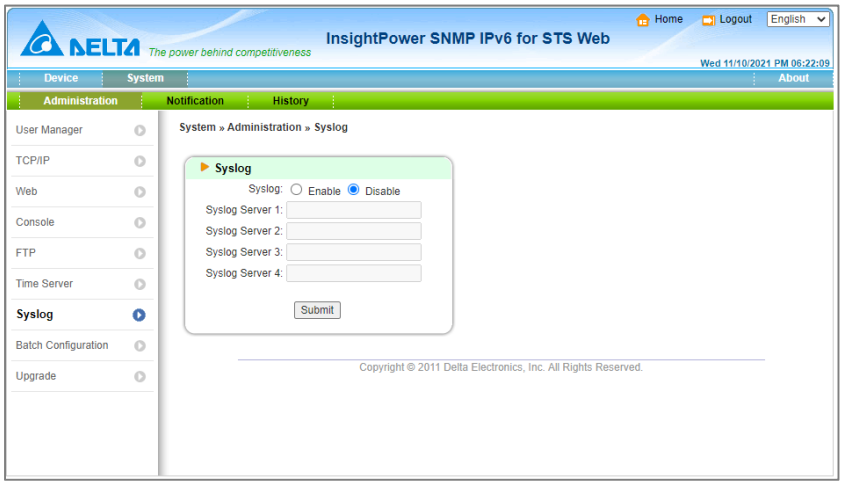
Enable Daylight Saving: This option is used to setup a daylight saving time. During the period of daylight saving time, the SNMP IPv6 will add 1 hour automatically.

5.3.6.2 Manual

If time servers are unreachable, the only way to adjust the system time is to configure date and time manually. Please note that the system date and time will synchronize with the assigned date/ time if the SNMP IPv6 is restarted.

5.3.7 Syslog

This menu allows administrator to set the SNMP IPv6 syslog. The syslog features the storage of event logs on the remote syslog servers. This feature does not affect the storage of local event logs.



5.3.8 Batch Configuration

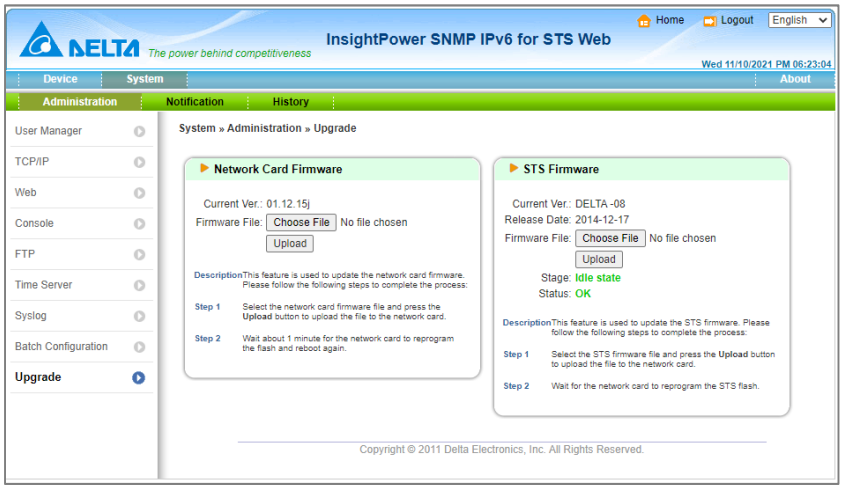
If you are an administrator and you have configured one site of the SNMP IPv6, you can copy the same configuration to the other SNMP IPv6s by distributing the configuration files.

Please note that you should only delete the lines which you don't want to distribute and if the IP address is static then you must delete the line of IP= xxx.xxx.xxx in the (System) section.

The batch configuration can work through the FTP, too.

5.3.9 Upgrade

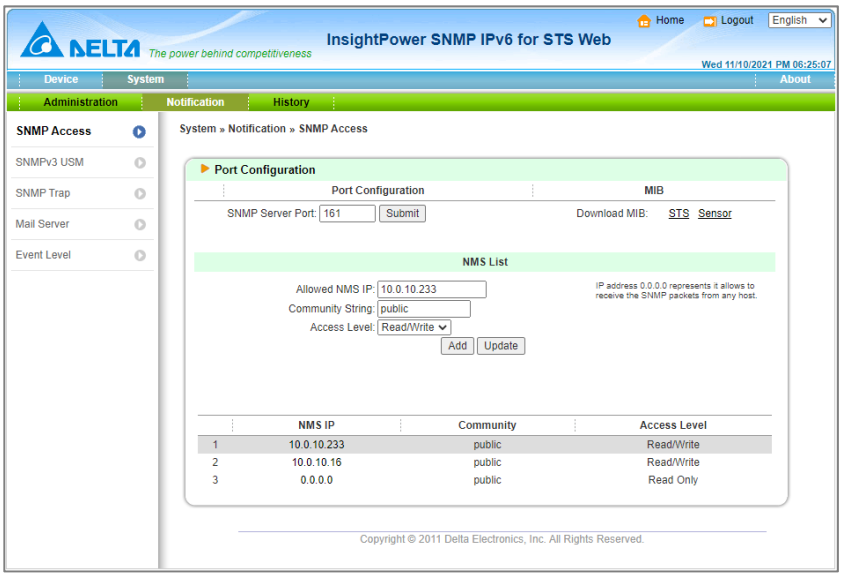
SNMP IPv6 provides the easiest way to upgrade the SNMP IPv6 firmware and rSTS firmware through the web interface. The users just need to assign the firmware file from your local disk then press the Upload button to transmit the specific firmware file to the SNMP IPv6 for upgrading.



5.4 Notification

5.4.1 SNMP Access

The SNMP IPv6 supports the SNMP protocol. You can use the SNMP NMS to manage the device through a network. You must enter the IP address of the workstation in the **SNMP Access Table** to prevent any unauthorized users from configuring the SNMP IPv6 via SNMP protocol. The maximum number of IP is 256.



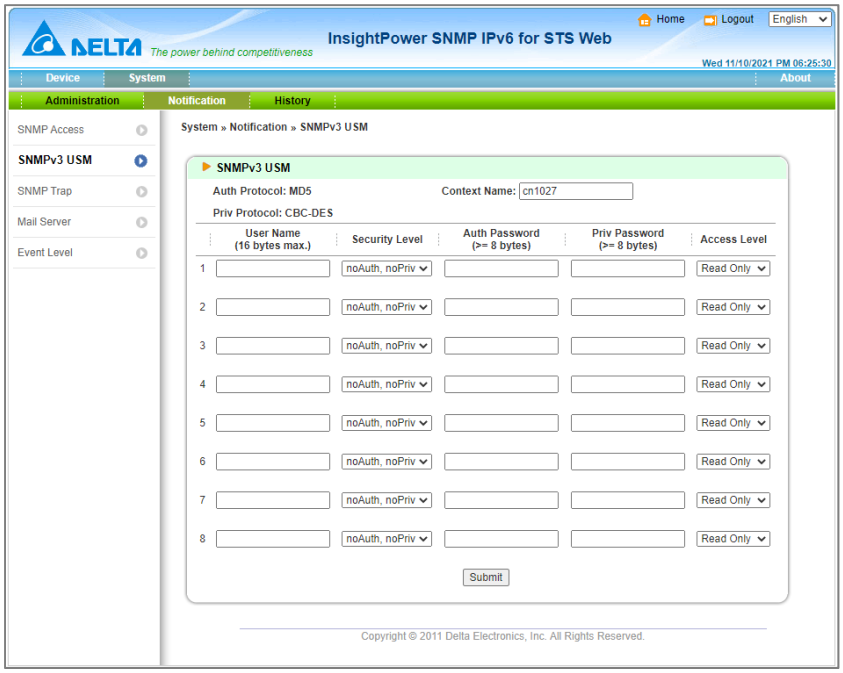
If you wish to use a workstation with SNMP Manager installed, or if you wish to set a more restrictive access to the **SNMP IPv6**, you can use the **SNMP Access** to add the IP address of the PC of which you wish to modify the access permission.

The IP address can be ignored when it is set as 0.0.0.0. The SNMP IPv6 will first check the community string to identify whether the incoming packet is Read Only or not. If the packet can be identified, the SNMP IPv6 will respond the inquiry.

The NMS IP can be a net. This means the form x.x.x.x/ prefix can be used to specify a net like 10.0.10.0/ 24.

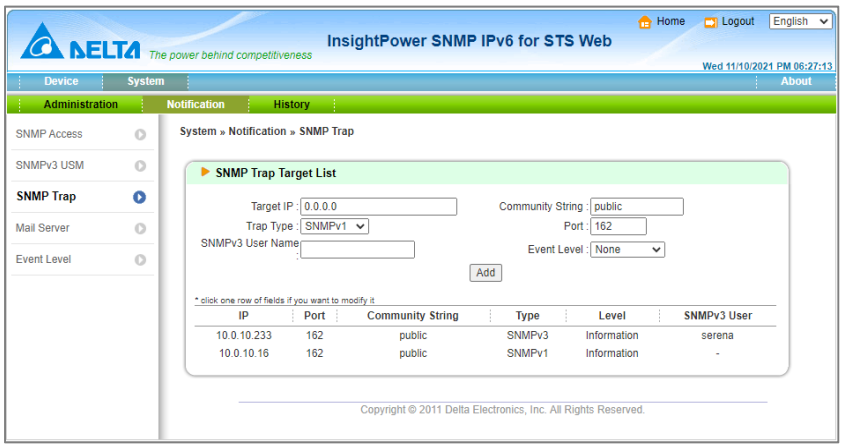
5.4.2 SNMPv3 USM (User Based Management)

The SNMP IPv6 supports access via SNMPv3 USM model for 8 users. After configuring the account parameters, you can access the card through the SNMPv3 protocol. The user table below is related to the SNMPv3 Trap.



5.4.3 SNMP Trap

If you want to use a PC and perform the SNMP Manager '**Trap**' function to manage the device through SNMP IPv6, you must add the IP address of the PC to the SNMP Trap list. The maximum number of SNMP trap target is 256.

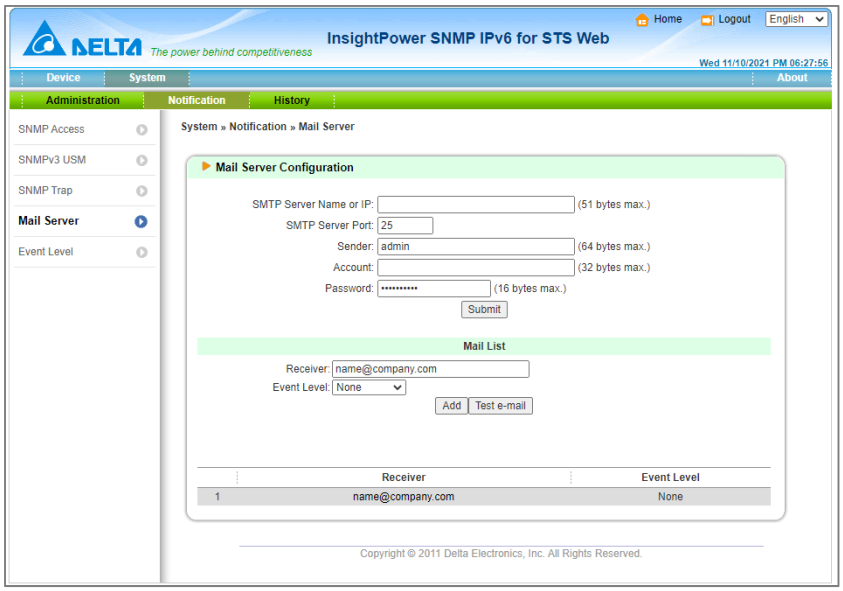


The **Event Level** field is used to decide what kind of power event's notification should be sent to the target address. There are 3 levels of power events: **Information**, **Warning and Alarm**. If you select **Information**, the notification of all power events will be sent to the target address; if you select **Warning**, the notification of Warning event as well as Alarm event will be sent to the target address; if you choose **Alarm**, only the notification of Alarm event will be sent to the target address.

The SNMP IPv6 provides SNMPv1, v2c and v3 trap to satisfy most of customer's environment. If you select to use the SNMPv3 trap then please provide one of the user names in the SNMPv3 USM table

5.4.4 Mail Server

The administrator can set up the SMTP Server and the e-mail recipient so the designated recipient can receive the e-mail notification from the SNMP IPv6 whenever a power event occurs. The maximum number of e-mail recipient can be filled out is 256.



1. **SMTP Server Name or IP**

   This is the hostname of a SMTP Mail Server used to send the email message from the SNMP IPv6. When entering a hostname, you are also required to enter the **DNS IP** in the **TCP/ IP**.

2. **Sender**

   The sender's E-mail address.

3. **Account**

   The Mail Server's login account.

4. **Password**

   The Mail Server's login password.

5. **Receiver**

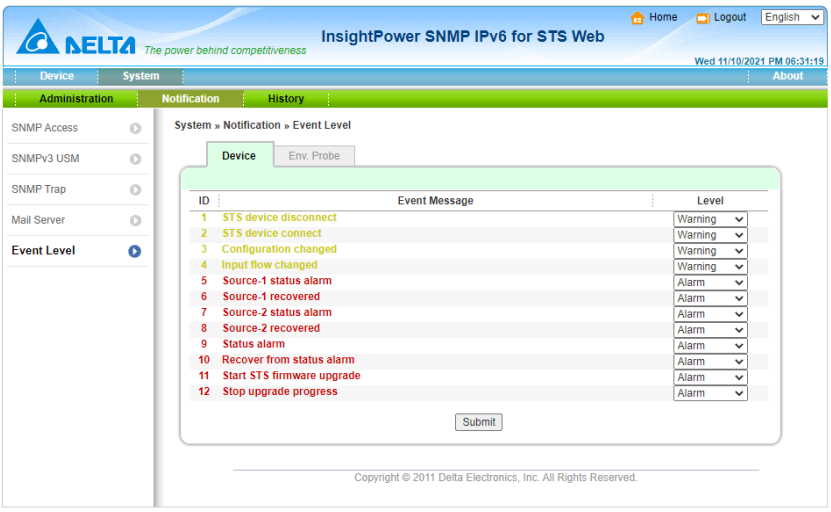
   Enter the email address that you wish the SNMP IPv6 to send an e-mail to.

6. **Event Level**

   Select the event level that you wish to send the corresponding e-mail notification to the recipient. If you select **Information**, the notification of all power events will be sent to the target address. If you select **Warning**, the notification of Warning event as well as Alarm event will be sent to the target address. If you choose **Alarm**, only the notification of Alarm event will be sent to the target address.

5.4.5 Event Level

The level of events can be configured here. The selection of Env. Probe will be shown if the dip switch is configured as probe mode.



5.5 History

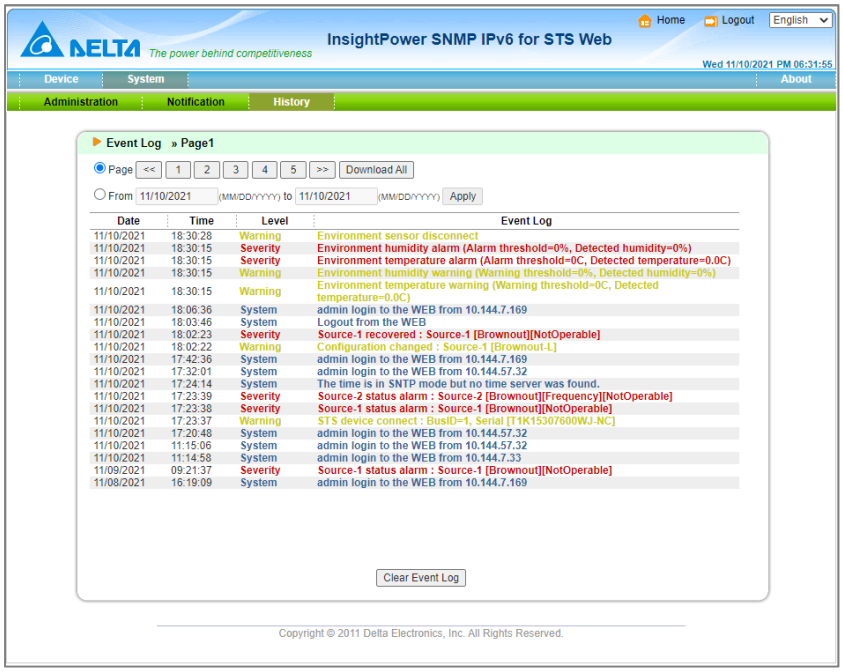
This table lists all the events that have occurred. The existing values are overwritten when the maximum number of entries (rows) has been reached. You can also download all event logs to your computer.

1. **Date:** The date when the event occurred

2. **Time:** The time when the event occurred

3. **Level:** The event level of the event occurred

4. **Event Log:** The description of the event occurred



Chapter 6 : SNMPv3

SNMPv3 is an encryption version of the SNMP protocol. Before you can access the SNMP OID from the SNMP IPv6 through SNMPv3 protocol, you have to maintain the SNMPv3 USM table. Please refer to ***Chapter 5.12*** for more detailed information.

To test the SNMPv3, please find a Linux operating system and open the terminal shell. After that, key in the following command to get the reply.

snmpwalk -v 3 -u <user> -l authPriv -A <password> -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 level, there are noAuthNoPriv, authNoPriv and authPriv.

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

-A: Follow an Auth Password which is assigned in the SNMPv3 USM table.

-X: Follow a Priv Password which is assigned in the SNMPv3 USM table.

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

-t: Timeout in second.

<ip>: IP address of the SNMP IPv6.

<oid>: The available SNMP OID, please refer to the MIB file. For example: 1.3.6.1.2.1.1.1.0

Chapter 7 : Upgrade SNMP IPv6 & rSTS

7.1 Prepare

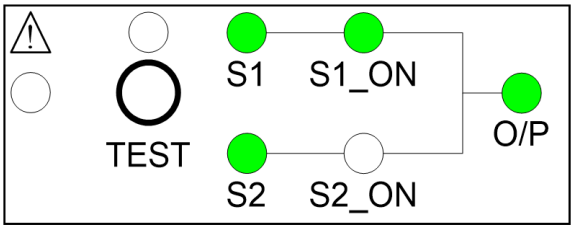
SNMP IPv6 provides several methods to upgrade itself and the connected rSTS. The procedures are as follows:

1. Check all DIP switches (Can't be ***pass-through*** mode)
2. Check unit's IP address from LOCAL port or **EzSetting**.

   default IP address: **192.168.1.100** with mask 255.255.255.0
3. Upload firmware file through -
   a. Web
   b. FTP / SFTP
   c. EzSetting (SNMP IPv6 only)
4. Wait for SNMP IPv6 to complete the remaining procedure. **During this process, two LED indicators will flash rapidly**.

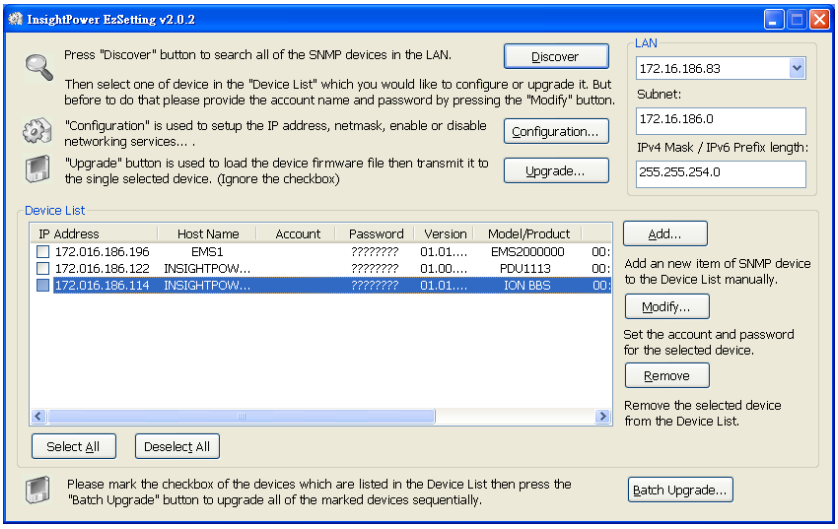
NOTE:

S1 is required for the upgrade of the rSTS firmware.



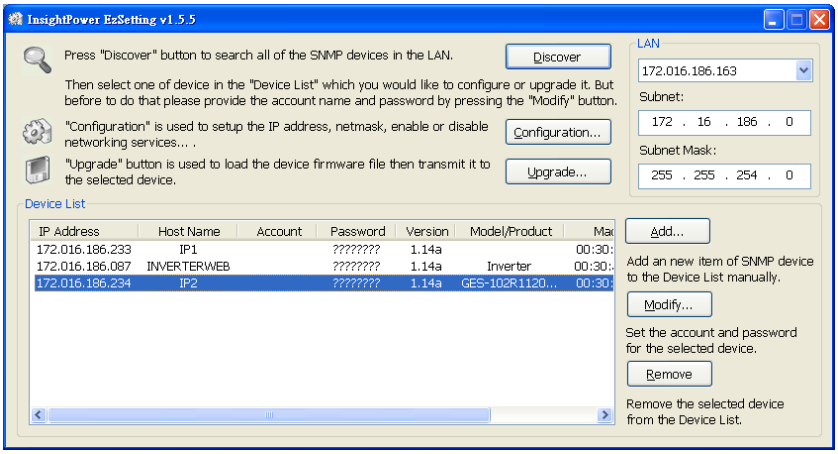
7.2 Upgrade via EzSetting

To perform a firmware upgrade (***SNMP IPv6 only***), please use the **EzSetting** software. The **EzSetting** program is compatible with the Windows operating system.

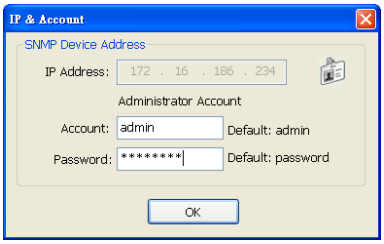


1. Make sure the SNMP IPv6 is in the “Subnet” that has been specified. If it is not in the specified subnet network please edit the subnet and subnet mask to the correct network that the SNMP IPv6 is located.

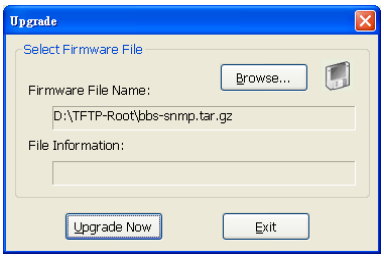
2. Press the ”Discover” button to search all of the SNMP IPv6 in the specified subnet.



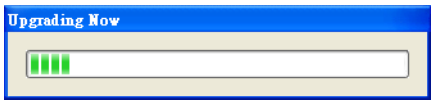
3. Select one device in the “Device List” then press the “Modify” button to key in the account and password of admin user’s level.



4. Back to the main window and press the “Upgrade” button. The upgrade window pops up to guide you to select a valid SNMP IPv6 firmware binary file. Verify the firmware version number listed in the “File Information” field and press the “Upgrade Now” button.



5. The SNMP IPv6 will respond to the upgrade request in 20 seconds.

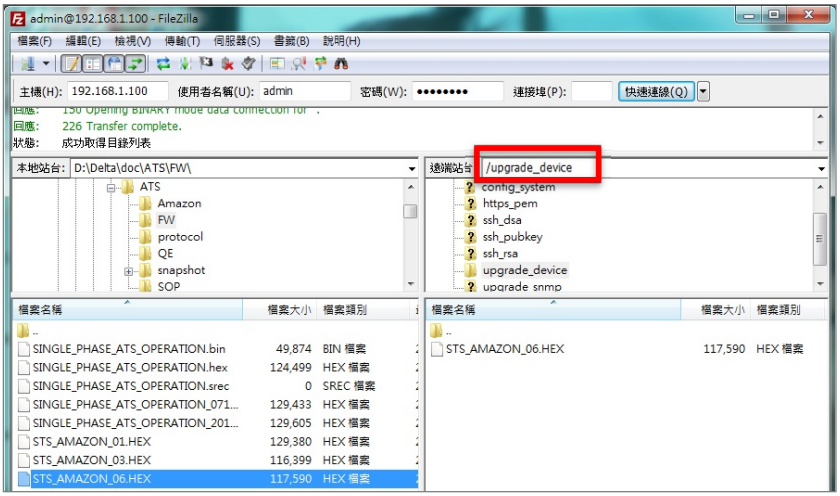


6. After finishing the upgrade procedure, the following window will be pop up. Please wait for 1 minute for the SNMP IPv6 to reboot.

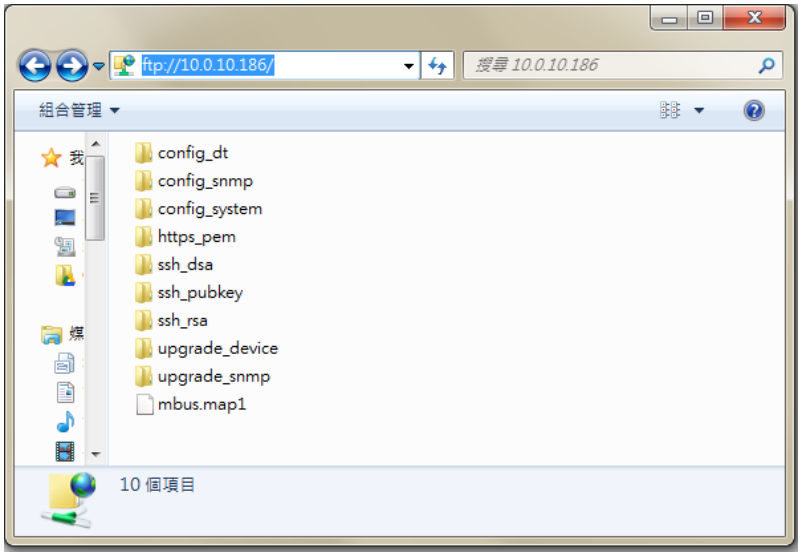
7.3 Upgrade via FTP or SFTP

The SNMP IPv6 supports the upload of firmware image through FTP or SFTP. After login, it will upload an image to the folder ***upgrade_snmp (SNMP IPv6 *.bin)*** or ***upgrade_device (STS *.hex)***. The SNMP IPv6 will perform the upgrade within 10 seconds.

Example to put file for the upgrade of rSTS. (folder /upgrade_device)

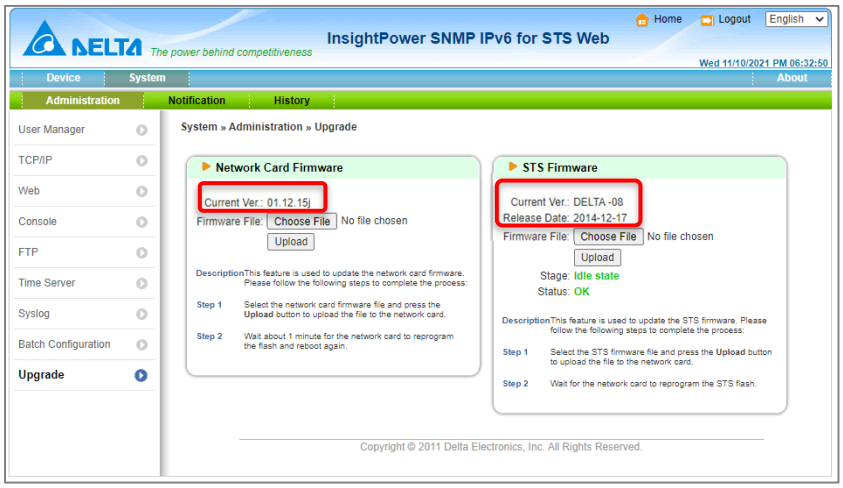


Use File Manager as the FTP client (under Miscrosoft Windows only) and drag a firmware file to the right folder.

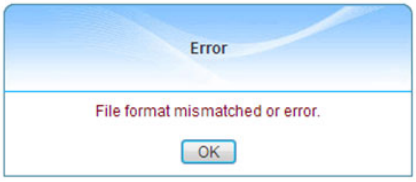


7.4 Upgrade via Web

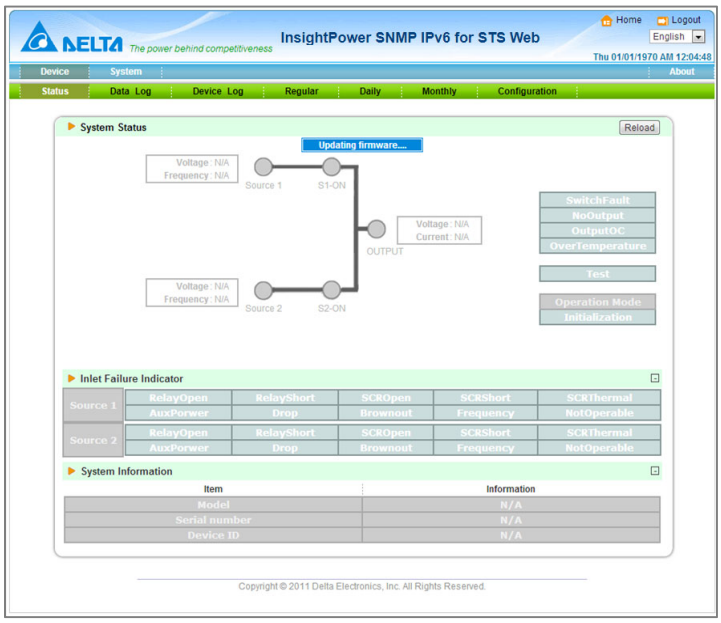
It's recommended to check the current version first. If rSTS can't be connected (may be in bootloader mode due to faulty upgrade before), the rSTS FW information will be kept empty.



SNMP IPv6 will check the format of the upgrade file. If the window below pops up, please check whether your upgrade file is correct.



During process, the status page will be shown as



Step comparison

	SNMP IPv6 (Left)	rSTS FW (Right)
DIP Switch	No setting is required	**Normal Mode**
Source	No setting is required	**S1**
Proxy OFF	**Turn off proxy function**	
Check HTTP	Check if the HTTP service is enabled through the **LOCAL** port	
Select File	*.BIN	*.HEX
Upload	Click "Upload" to send a file	
Check LED	Two LEDs will flash rapidly during upgrade process	
Check Web	Shutdown	1. Check FileID 2. Auth 3. Program 4. Read comparison 5. Finish
Complete	Reset	Try to estsalish a MODBUS communication
Normal Operation	Yellow LED should flash rapidly	

Appendix A : rSTS Command Set

The SNMP IPv6 provides a command interface for users to get device information via the LOCAL port. Users can also use telnet and SSH to configure the command mode and use it instead of the configuration menu (manufacturer settings).

Command	Description	Parameter	Response
Info	Report summary information.	N/A	<Report>
TempF	Report internal rSTS Fahrenheit temperature.	N/A	#
TempC	Report internal rSTS Celsius temperature.	N/A	#
Age	Report internal rSTS age.	N/A	# days hh:mm:ss
Time	Report present time.	N/A	hh:mm:ss MM/DD/YYYY
XCount	Report number of times that rSTS has transferred.	N/A	#
FWVer	Report rSTS FW version	N/A	<Version string>
FWDate	Report rSTS FW release data	N/A	YYYY-MM-DD
AgentVer	Report SNMP IPv6 version	N/A	AA.BB.XXX
Model	Report the model name.	N/A	<Model name string>
Serial	Report the unit's serial number.	N/A	<Device serial string>
DevID	Report the unit's device ID.	N/A	<Device ID string>
Prefer	Report the preferred source.	N/A	S1 or S2
Sens	Report the sensitivity.	N/A	hi or low
Mode	Report the operation mode.	N/A	Initialization Diagnosis Off S1 S2 Safe Fault
Link	Check current MODBUS connection	N/A	1 - normal/ 2 - abnormal/ 3- upgrading
Input / Output Parameters			
Vout	Report the output voltage.	N/A	#.#
Iout	Report the output current.	N/A	#.#

Command	Description	Parameter	Response
Vs1	Report the primary voltage.	N/A	#.#
Vs2	Report the secondary voltage.	N/A	#.#
Fs1	Report the primary frequency.	N/A	#.#
Fs2	Report the secondary frequency.	N/A	#.#
Configuration			
Vtp2s	Report the primary to secondary trip voltage.	N/A	#.#
Vts2p	Report the secondary to primary trip voltage.	N/A	#.#
Vbp2s	Report the primary to secondary brownout voltage.	N/A	#.#
Vbs2p	Report the secondary to primary brownout voltage.	N/A	#.#
Tdp2s	Report the recover time of transfer from primary to secondary.	N/A	#.#
Tds2p	Report the recover time of transfer from secondary to primary.	N/A	#.#
Mvs1	Report the max voltage of comparing cycles for primary AC blackout.	N/A	#
Mvs2	Report the max voltage of comparing cycles for secondary AC blackout.	N/A	#
Mts1	Report the max time of comparing cycles for primary AC blackout.	N/A	#.#
Mts2	Report the max time of comparing cycles for secondary AC blackout.	N/A	#.#
Device Log			
Log	Report the event code and time of prior transfers.	[Index] [# to show] # = 1 - 20	STS> Log 10 STS> Log 1 15:33:59 03/20/2016 0x29 STS> Log 3 5 Index Time Date Event

Command	Description	Parameter	Response
			3) 13:07:42 07/12/2011 0x29 4) 13:07:54 07/12/2011 0x2D 5) 15:19:00 06/20/2011 0x2B 6) 15:19:00 06/20/2011 0x2E 7) 15:19:00 06/20/2011 0x2B
Tprev[1..9]	Report the time of prior transfer/event. Tprev1 is the most recent time.	N/A	hh:mm:ss MM/DD/YYYY
Event[1..9]	Report the event code for prior transfer. Event1 is the most recent event.	N/A	0x#
Essential Log			
LogR	Report regular log.	[Index | Date] [1-288]	<List of regular log>
LogD	Report daily log.	[Index | Date | Month] [1-200]	<List of daily log>
LogM	Report monthly log.	[Index | Month] [1-200]	<List of monthly log>
Setting			
SetTime	Set the present time.	hh:mm:ss [MM/DD/YYYY]	[Message]
SetDate	Set the present date.	MM/DD/YYYY	[Message]
SetPrefer	Set the preferred source.	1 or 2	[Message]
SetDevID	Set the unit device ID.	<20 characters> alphanumeric only	[Message]
SetVtp2s	Set the primary to secondary trip voltage.	165.0 ~ 175.0	[Message]
SetVts2p	Set the secondary to primary trip voltage.	165.0 ~ 175.0	[Message]
SetVbp2s	Set the primary to secondary brownout voltage.	180.0 ~ 264.0	[Message]
SetVbs2p	Set the secondary to primary brownout voltage.	180.0 ~ 264.0	[Message]
SetTdp2s	Set the recover time of transfer from primary to secondary.	12.0 ~ 1800.0	[Message]
SetTds2p	Set the recover time of transfer from secondary to	12.0 ~ 1800.0	[Message]

Command	Description	Parameter	Response
	primary.		
SetMvs1	Set the max voltage of comparing cycles for primary AC blackout.	30 ~ 50	[Message]
SetMvs2	Set the max voltage of comparing cycles for secondary AC blackout.	30 ~ 50	[Message]
SetMts1	Set the max time of comparing cycles for primary AC blackout.	2.0 ~ 4.0	[Message]
SetMts2	Set the max time of comparing cycles for secondary AC blackout.	2.0 ~ 4.0	[Message]
Upgrade Status			
UpProcess	Status of upgrade progress	N/A	Idle/ Run/ Error
UpStep	Stage of upgrade progress	N/A	Init/ FileID/ Auth/ Addr/ Erase / Program/ Read
UpPercentage	Percentage of upgrade progress	N/A	#.#
UpResult	Result of upgrade progress	N/A	OK/ No response/ File ID fail/ Authenticate fail/ Erase fail/ Flash fail/ Read fail/ Upgrade complete
UpDate	Report time of each FW upgrade	[Index] [# to show] # = 1 - 20	STS> UpDate 3 STS> UpDate 1 13:43:15 04/10/2013 STS> UpDate 1 20 Index Time Date 1) 13:43:15 04/10/2013 2) 13:28:26 04/10/2013 3) 13:27:37 04/10/2013
AgentVer	Report SNMP IPv6 version	N/A	AA.BB.XXX
Link	Check current MODBUS connection	N/A	1 - normal/ 2 - abnormal/ 3- upgrading
Other			
Bye | Exit	Terminate remote connection	N/A	

NOTE:

For SNMP firmware version existing before the version of 01.12.11f (inc.), the response format is ‘sec’.

For SNMP firmware version existing after the version of 01.12.14e (inc.), the response format is ‘day(s) hh:mm:ss.

- **Interaction and Response**

Generally, users can use commands as:

Get Parameter: <Command>

```
STS> Age
10 days 8:02:46
STS>
```

Set Parameter: <Command> <Argument1> <Argument2>

```
STS> SetTdp2s 300
OK
STS>
```

Get Log: <Command> <Argument1> <Argument2>

```
STS> Log
10
STS> Log 2 5
Index Time     Date       Event
   2) 13:08:09 07/12/2011 0x2D - S2 Voltage Brownout
   3) 15:19:00 06/20/2011 0x2E - S2 Frequency out of range
   4) 15:19:00 06/20/2011 0x2B - S1 Frequency out of range
   5) 15:19:00 06/20/2011 0x2E - S2 Frequency out of range
```

Positive Response:

a. Report is defined as command specific.

b. OK

```
STS> SetTdp2s 300
OK
STS>
```

Negative responses:

a. Invalid Command

```
STS> SetTdp2s
Invalid Command
STS> SeTdp2s 300
Invalid Command
ATS>
```

b. Invalid Range or Value

```
STS> SetTdp2s 10
Invalid Range or Value
STS>
```

c. Failed to Set

```
STS> SetTdp2s 300
Failed to Set
STS>
```

- **Essential Log**

User can get outlet parameters and temperature history by using LogR/LogD/LogM.

LogR - Regular Log

Argument 1: empty or index or date

Argument 2: empty or quantity

a. Report today log

```
STS> LogR
Index Time     Date       Voltage           Current           Temperaute(C)
  24) 16:25:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  25) 16:20:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  26) 16:15:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  27) 16:10:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  28) 16:05:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  29) 16:00:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  30) 15:55:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  31) 15:50:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  32) 15:45:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
  33) 15:40:00 07/03/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
```

b. Report regular log of a specific date

```
STS> LogR 2014/6/28
Index Time     Date       Voltage            Current            Temperaute(C)
1375) 23:55:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
1376) 23:50:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
1377) 23:45:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
     ....................................
1647) 01:15:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
1648) 01:10:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
1649) 01:05:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
1650) 01:00:00 06/28/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
```

c. Report regular log of a specific date and quantity

```
STS> LogR 2014/6/30 20
Index Time     Date       Voltage            Current            Temperaute(C)
 800) 23:55:00 06/30/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
 801) 23:50:00 06/30/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
 802) 23:45:00 06/30/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
 803) 23:40:00 06/30/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
 804) 23:35:00 06/30/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
 805) 23:30:00 06/30/2014 220.8/220.8/220.8 -   0.0/  0.0/  0.0 - 39/39/39
```

LogD - Daily Log

Argument 1: empty or index or date or month

Argument 2: empty or quantity

a. Report daily log of this month

```
STS> LogD
Index Date       Voltage       Current       Temperaute(C)
   1) 07/03/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   2) 07/02/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   3) 07/01/2014 220.8/220.8 -   0.0/  0.0 - 39/39
```

b. Report daily log of a specific month

```
STS> LogD 2014/6
Index Date       Voltage       Current       Temperaute(C)
   4) 06/30/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   5) 06/29/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   6) 06/28/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   7) 06/27/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   8) 06/26/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   9) 06/25/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  10) 06/24/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  11) 06/23/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  12) 06/22/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  13) 06/21/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  14) 06/20/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  15) 06/19/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  16) 06/18/2014 220.8/220.8 -   0.0/  0.0 - 39/39
```

c. Report daily log from a specific month with a given quantity

```
STS> LogD 2014/6/28 5
Index Date      Voltage      Current      Temperaute(C)
   6) 06/28/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   7) 06/27/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   8) 06/26/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   9) 06/25/2014 220.8/220.8 -   0.0/  0.0 - 39/39
  10) 06/24/2014 220.8/220.8 -   0.0/  0.0 - 39/39
```

LogM - Monthly Log

Argument 1: empty or index or month

Argument 2: empty or quantity

a. Report monthly log of this year

```
STS> LogM
Index Month   Voltage      Current      Temperaute(C)
   1) 07/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   2) 06/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   3) 05/2014 220.8/220.8 -   0.0/  0.0 - 39/39
```

b. Report monthly log from a specific month

```
STS> LogM 2014/6
Index Month   Voltage      Current      Temperaute(C)
   2) 06/2014 220.8/220.8 -   0.0/  0.0 - 39/39
   3) 05/2014 220.8/220.8 -   0.0/  0.0 - 39/39
```

Appendix B : SNMP TRAP

rSTS MIB

Trap OID: .1.3.6.1.4.1.2254.2.80.20.0.1

Generic: EnterpriseSpcific

Name	OID	Description	Variable Bindings
stsTrapCommLost	.1.3.6.1.4.1.2254.2.80.20.0.1	Communication with the STS failed.	**[Name]** 1.3.6.1.4.1.2254.2.80.1.3.2.0 **[Value]** Bus ID
stsTrapCommEstablished	.1.3.6.1.4.1.2254.2.80.20.0.2	Communication with the STS reestab-lished.	**[Name]** 1.3.6.1.4.1.2254.2.80.1.3.2.0 **[Value]** Bus ID
stsTrapConfigChange	.1.3.6.1.4.1.2254.2.80.20.0.3	The STS configuration has been changed.	
stsTrapFlowChange	.1.3.6.1.4.1.2254.2.80.20.0.4	The Input flow status has been changed.	**[Name]** 1.3.6.1.4.1.2254.2.80.4.1.0 (stsInputFlowIndicator) **[Value]** Bit Map bit0: source 1 relay bit1: source 1 SCR bit2: source 1 parallel relay bit8: source 2 relay bit9: source 2 SCR bit10: source 2 parallel relay
stsTrapInput1Alarm	.1.3.6.1.4.1.2254.2.80.20.0.5	Alarm of source-1 failure(s).	**[Name]** 1.3.6.1.4.1.2254.2.80.4.3.0 (stsInputFailureIndicator) **[Value]** Bit Map bit0: relay open bit1: relay short bit2: SCR open bit3: SCR short bit4: Over thermal of SCR bit5: aux power bit6: voltage drop bit7: voltage brownout bit8: frequency out of range bit9: not operable

Name	OID	Description	Variable Bindings
stsTrapInput1AlarmRecover	.1.3.6.1.4.1.2254.2.80.20.0.6	Recover from source-1 failure(s).	**[Name]** 1.3.6.1.4.1.2254.2.80.4.3.0 (stsInputFailureIndicator) **[Value]** Bit Map bit0: relay open bit1: relay short bit2: SCR open bit3: SCR short bit4: Over thermal of SCR bit5: aux power bit6: voltage drop bit7: voltage brownout bit8: frequency out of range bit9: not operable
stsTrapInput2Alarm	.1.3.6.1.4.1.2254.2.80.20.0.7	Alarm of source-2 failure(s).	**[Name]** 1.3.6.1.4.1.2254.2.80.4.3.0 (stsInputFailureIndicator) **[Value]** Bit Map bit16: relay open bit17: relay short bit18: SCR open bit19: SCR short bit20: Over thermal of SCR bit21: aux power bit22: voltage drop bit23: voltage brownout bit24: frequency out of range bit25: not operable
stsTrapInput2AlarmRecover	.1.3.6.1.4.1.2254.2.80.20.0.8	Recover from source-2 failure(s).	**[Name]** 1.3.6.1.4.1.2254.2.80.4.3.0 (stsInputFailureIndicator) **[Value]** Bit Map bit16: relay open bit17: relay short bit18: SCR open bit19: SCR short bit20: Over thermal of SCR bit21: aux power bit22: voltage drop bit23: voltage brownout bit24: frequency out of range bit25: not operable

Name	OID	Description	Variable Bindings
stsTrapAlarm	.1.3.6.1.4.1.2254.2.80.20.0.9	Alarm of failure(s).	**[Name]** 1.3.6.1.4.1.2254.2.80.4.5.0 (stsFailureIndicator) **[Value]** Bit Map bit0: switch fault bit1: no output bit2: output over current bit3: over temperature bit4: environment fault
stsTrapAlarmRecover	.1.3.6.1.4.1.2254.2.80.20.0.10	Recover from failure(s).	**[Name]** 1.3.6.1.4.1.2254.2.80.4.5.0 (stsFailureIndicator) **[Value]** Bit Map bit0: switch fault bit1: no output bit2: output over current bit3: over temperature bit4: environment fault
stsTrapUpgradeBegin	.1.3.6.1.4.1.2254.2.80.20.0.11	Start to upgrade STS firmware.	
stsTrapUpgradeEnd	.1.3.6.1.4.1.2254.2.80.20.0.12	End of upgrade progress.	**[Name]** 1.3.6.1.4.1.2254.2.80.7.1.0 (stsUpgradeProcess) **[Value]** 0: N/A 1: Idle 2: Run 3: Erro **[Name]** 1.3.6.1.4.1.2254.2.80.7.2.0 (stsUpgradeStep) **[Value]** 0:N/A 1:Init 2:FileID 3:Auth 4:Addr 5:Erase 6:Program 7:Read

Sensor MIB

Trap OID: .1.3.6.1.4.1.2254.2.50.20.0.1

Generic: EnterpriseSpcific

Name	OID	Description	Variable Bindings
dsensorNoLongerOverAlarmTemperature	.1.3.6.1.4.1.2254.2.500.20.0.1	WARNING: Communication with the environmental sensor failed.	
dsensorOverWarningHumidity	.1.3.6.1.4.1.2254.2.500.20.0.2	INFORMATION: Communication with the environmental sensor reestablished.	
dsensorNoLongerOverWarningHumidity	.1.3.6.1.4.1.2254.2.500.20.0.3	SEVER: The environment over warning temperature.	
dsensorOverAlarmHumidity	.1.3.6.1.4.1.2254.2.500.20.0.4	INFORMATION: The environment recovered from over warning temperature.	
dsensorNoLongerOverAlarmHumidity	.1.3.6.1.4.1.2254.2.500.20.0.5	SEVER: The environment over alarm temperature.	
dsensorRelay1Alarm	.1.3.6.1.4.1.2254.2.500.20.0.6	INFORMATION: The environment recovered from over alarm temperature.	
dsensorRelay1Normal	.1.3.6.1.4.1.2254.2.500.20.0.7	SEVER: The environment over warning humidity.	
dsensorRelay2Alarm	.1.3.6.1.4.1.2254.2.500.20.0.8	INFORMATION: The environment recovered from over warning humidity.	
dsensorRelay2Normal	.1.3.6.1.4.1.2254.2.500.20.0.9	SEVER: The environment over alarm humidity.	
dsensorRelay3Alarm	.1.3.6.1.4.1.2254.2.500.20.0.10	INFORMATION: The environment recovered from over alarm humidity.	

Name	OID	Description	Variable Bindings
dsensorRelay3Normal	.1.3.6.1.4.1.2254.2.500.20.0.11	INFORMATION: The environment relay1 is not in normal state.	
dsensorRelay4Alarm	.1.3.6.1.4.1.2254.2.500.20.0.12	INFORMATION: The environment relay1 is in normal state.	
dsensorRelay4Norma	.1.3.6.1.4.1.2254.2.500.20.0.13	INFORMATION: The environment relay2 is not in normal state.	
dsensorNoLongerOverAlarmTemperature	.1.3.6.1.4.1.2254.2.500.20.0.14	INFORMATION: The environment relay2 is in normal state.	
dsensorOverWarningHumidity	.1.3.6.1.4.1.2254.2.500.20.0.15	INFORMATION: The environment relay3 is not in normal state.	
dsensorNoLongerOverWarningHumidity	.1.3.6.1.4.1.2254.2.500.20.0.16	INFORMATION: The environment relay3 is in normal state.	
dsensorOverAlarmHumidity	.1.3.6.1.4.1.2254.2.500.20.0.17	INFORMATION: The environment relay4 is not in normal state.	
dsensorNoLongerOverAlarmHumidity	.1.3.6.1.4.1.2254.2.500.20.0.18	INFORMATION: The environment relay4 is in normal state.	

Appendix C : Device Logs

Environmental faults						
Decimal	**Hexade cimal**	**Meaning**	**Action**	**Reset**	**Change in LED**	**SNMP Trap OID**
E01	0x01	Output Over Current	Alarm	Clear automatically (the load is less than 95%)	Red LED Blink	1.3.6.1.4.1.2254.2.80.20.0.9 (bit 2)
E02	0x02	Over temperature (due to detection of ambient temperature)	Alarm (ambient temperature rises above 50 ℃)	Clear automatically (ambient temperature falls below 45℃)	Red LED Blink	1.3.6.1.4.1.2254.2.80.20.0.9 (bit 3)
E03	0x03	Over temperature warning (due to detection of S1 heat-sink temperature)	Transfer to S2 if S2 is available. Once the temperature recovers, return to S1 automatically	Clear automatically (the thermal switch is reset)	Red LED Blink	NO
E04	0x04	Over temperature warning (due to detection of S2 heat-sink temperature)	Transfer to S1 if S1 is available. Once the temperature recovers, return to S2 automatically	Clear automatically (the thermal switch is reset)	Red LED Blink	NO

Warnings						
Decimal	Hexade cimal	Meaning	Action	Reset	Change in LED	SNMP Trap OID
E41	0x29	S1 Voltage Drop	Transfer to S2	Clear automatically (S1 Voltage is in the range)	Red LED Blink S1 LED dark	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 6 or bit 7,8,9 are 1)
E42	0x2A	S1 Voltage Brownout	Transfer to S2	Clear automatically (S1 Voltage is in the range)	Red LED Blink S1 LED dark	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 7)
E43	0x2B	S1 Frequency Out of Range	Transfer to S2	Clear automatically (S1 Frequency is in the range)	Red LED Blink S1 LED dark	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 8)
E44	0x2C	S2 Voltage Drop	Transfer to S1	Clear automatically (S2 Voltage is in the range)	Red LED Blink S2 LED dark	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 21 or bit 22,23,24 are 1)
E45	0x2D	S2 Voltage Brownout	Transfer to S1	Clear automatically (S2 Voltage is in the range)	Red LED Blink S2 LED dark	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 22)
E46	0x2E	S2 Frequency Out of Range	Transfer to S1	Clear automatically (S2 Frequency is in the range)	Red LED Blink S2 LED dark	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 23)

Internal Faults						
Decimal	Hexade cimal	Meaning	Action	Reset	Change in LED	SNMP Trap OID
E11	0x0B	Over temperature (due to detection of S1 heat-sink temperature)	Transfer to S2 path if S2 is available.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 4)
E12	0x0C	Over temperature (due to detection of S2 heat-sink temperature)	Transfer to S1 path if S1 is available.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 20)
E13	0x0D	Auxiliary power 1 circuit is fail	Alarm	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 5)

Internal Faults						
Decimal	Hexade cimal	Meaning	Action	Reset	Change in LED	SNMP Trap OID
E14	0x0E	Auxiliary power 2 circuit is fail	Alarm	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 21)
E21	0x15	Input relay of S1 is open	Transfer to S2.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 0)
E22	0x16	Input relay of S1 is short	At diagnosis mode, rSTS keep at S1. At S2 mode, rSTS transfer to S1.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 1)
E23	0x17	Input relay of S2 is open	Transfer to S1.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 16)
E24	0x18	Input relay of S2 is short	At diagnosis mode, rSTS keep at S2. At S1 mode, rSTS transfer to S2.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 17)
E25	0x19	Input SCR of S1 is open	At S1 mode, rSTS transfer to S2. During transferring from S2 path to S1 path, rSTS keep at S1 path.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.5 (bit 2)
E27	0x1B	Input SCR of S2 is open	At S2 mode, rSTS transfer to S1. During transferring from S1 path to S2 path, rSTS keep at S2 path.	Can't be reset auto-matically. Can only be reset by turning off the rSTS.	Red LED Solid ON	1.3.6.1.4.1.2254.2.80.20.0.7 (bit 18)

Appendix D : System History Event Logs

Message	Level
System startup	System
Soft reboot	System
Upgrade firmware	System
Test message	System
The administrator account and password are reset	System
[Account] login to the WEB from [IP Address]	System
Logout from the WEB	System
[Account] login to the TELNET from [IP Address]	System
Logout from the TELNET	System
[Account] login to the CONSOLE	System
Logout from the CONSOLE	System
[Account] login to the FTP from [IP Address]	System
Logout from the FTP	System
The time is in manual mode, please synchronize it to the local time.	System
The time is in SNTP mode but no time server was found.	System
The time has been synchronized through SNTP.	System
[Device Name] device disconnect : BusID=[Bus ID]	Warning
[Device Name] device connect : BusID=[Bus ID], Serial [Serial Number]	Warning
Configuration changed : Source-[1 or 2] [Configuration Type]	Warning
Input flow changed : Source-[1 or 2] [Relay/SCR/ParallelRelay]	Warning
Source-1 status alarm : Source-[1 or 2] [Relay-Open/Relay-Short/SCR-Open/ SCR-Sharot/SCR-Thremal/AuxPower/Drop/Brownout/Frequency/ NotOperable]	Alarm
Source-1 recovered : Source-[1 or 2] [Relay-Open/Relay-Short/SCR-Open/ SCR-Sharot/SCR-Thremal/AuxPower/Drop/Brownout/Frequency/ NotOperable]	Alarm
Source-2 status alarm : Source-[1 or 2] [Relay-Open/Relay-Short/SCR-Open/ SCR-Sharot/SCR-Thremal/AuxPower/Drop/Brownout/Frequency/ NotOperable]	Alarm

Message	Level
Source-2 recovered : Source-[1 or 2] [Relay-Open/Relay-Short/SCR-Open/ SCR-Sharot/SCR-Thremal/AuxPower/Drop/Brownout/Frequency/ NotOperable]	Alarm
Status alarm : [Fault/NoOutput/OutputOC/OverTemperature/Upgrade]	Alarm
Recover from status alarm : [Fault/NoOutput/OutputOC/OverTemperature/Upgrade]	Alarm
Start [Device Name] firmware upgrade : begin time [Time]	Alarm
Stop upgrade progress : end time [Time], process [Idle/Run/Error], stage [Init/FileID/Auth/Addr/Erase/Program/Read]	Alarm
Environment sensor disconnect	Warning
Environment sensor connect	Warning
Environment temperature warning (Warning threshold=[Data]C, Detected temperature=[Data]C)	Warning
Environment temperature recovered from warning (Warning threshold=[Data]C, Detected temperature=[Data]C)	Warning
Environment humidity warning (Warning threshold=[Data]%, Detected humidity=[Data]%)	Warning
Environment humidity recovered from warning (Warning threshold=[Data]%, Detected humidity=[Data]%)	Warning
Environment temperature alarm (Alarm threshold=[Data]C, Detected temperature=[Data]C)	Alarm
Environment temperature recovered from alarm (Alarm threshold=[Data]C, Detected temperature=[Data]C)	Alarm
Environment humidity alarm (Alarm threshold=[Data]%, Detected humidity=[Data]%)	Alarm
Environment humidity recovered from alarm (Alarm threshold=[Data]%, Detected humidity=[Data]%)	Alarm
Environment R1 [Title] alarm	Alarm
Environment R1 [Title] normal	Alarm
Environment R2 [Title] alarm	Alarm
Environment R2 [Title] normal	Alarm
Environment R3 [Title] alarm	Alarm
Environment R3 [Title] normal	Alarm
Environment R4 [Title] alarm	Alarm
Environment R4 [Title] normal	Alarm

Appendix E : Key Generation for SSH

- **For Linux Version:**

  1. Please download the openssh from http://www.openssh.org and install it in the Linux.
  2. Open the command shell and key in the following command to create your own keys: Please ignore the request when asked to provide the key passphrase.

     DSA Key: ssh-keygen – t dsa

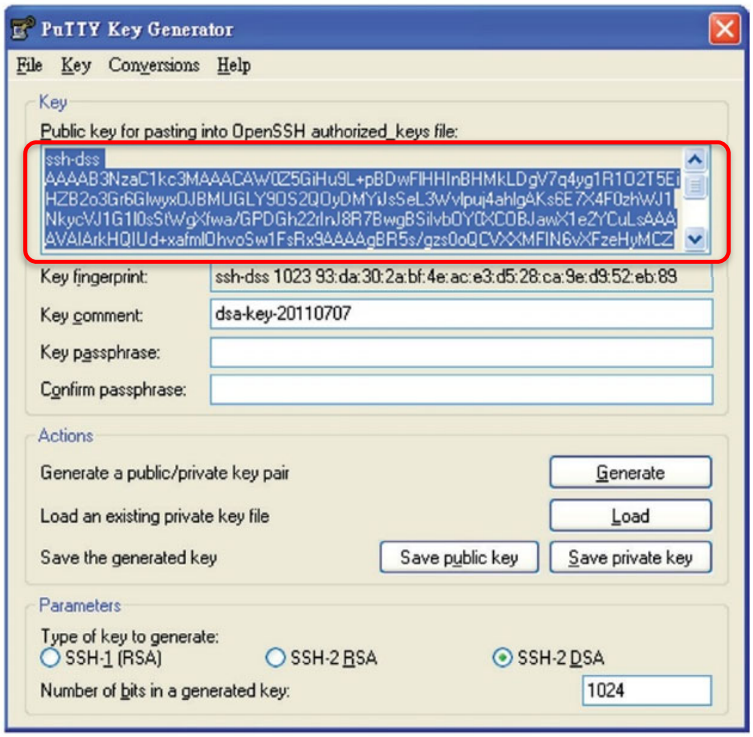
     RSA Key: ssh-keygen – t rsa
  3. To upload the DSA and RSA key files to the SNMP IPv6 through the web page, please refer to the ***Chapter 5.3.4 Console***.

- **For Windows Version:**

  1. Please download the Putty from http://www.putty.org and install it in the Windows.
  2. Run the **puttygen.exe** in the putty installed directory.
  3. Select **SSH-2 RSA** from the Parameters area and select the **Generate key pair** from the **Key** menu to generate the RSA key.
  4. Select **Export OpenSSH Key** from the **Conversions** menu and assign a file name for the RSA key. Please ignore the request when asked to provide the key passphrase.
  5. Select **SSH-2 DSA** from the Parameters area and select the **Generate key pair** from the **Key** menu to generate the DSA key.
  6. Select **Export OpenSSH Key** from the **Conversions** menu and assign a file name for the DSA key. Please ignore the request when asked to provide the key passphrase.
  7. To upload the DSA and RSA key files to the SNMP IPv6 through the web page, please refer to the ***Chapter 5.3.4 Console***.

NOTE:

You can also copy the marked block below and save it to a public key file for login without entering password via SSH.



Appendix F : Specifications

8.1 Technical Specifications

SNMP IPv6 provides several methods for the upgrade and the connection to the rSTS. The specifications are listed as below:

Network Connection	RJ - 45 connector
Operating Temperature	0 ~ 40° C
Operating Humidity	10 ~ 80 %
Power Input	9 ~ 24 VDC
Power Consumption	2 Watt Maximum
Size	130 mm × 60 mm (L × W)
Weight	75 g

Appendix G : 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. : 501330150000
Version : V 0.0
Release Date : 2022_02_22

- 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

The United States

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 Bairro Eugenio de Melo
12247-001 - São José dos Campos - SP - Brasil
T +55 12 3935-2300
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 Power Solutions (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 Europe Limited
1 Redwood Court, Peel Park, East Kilbride,G74 5PF,
Scotland, United Kingdom
T +44 1355 588 888
E sales.gb@eltek.com

Smarter. Greener. Together.

5013301500