

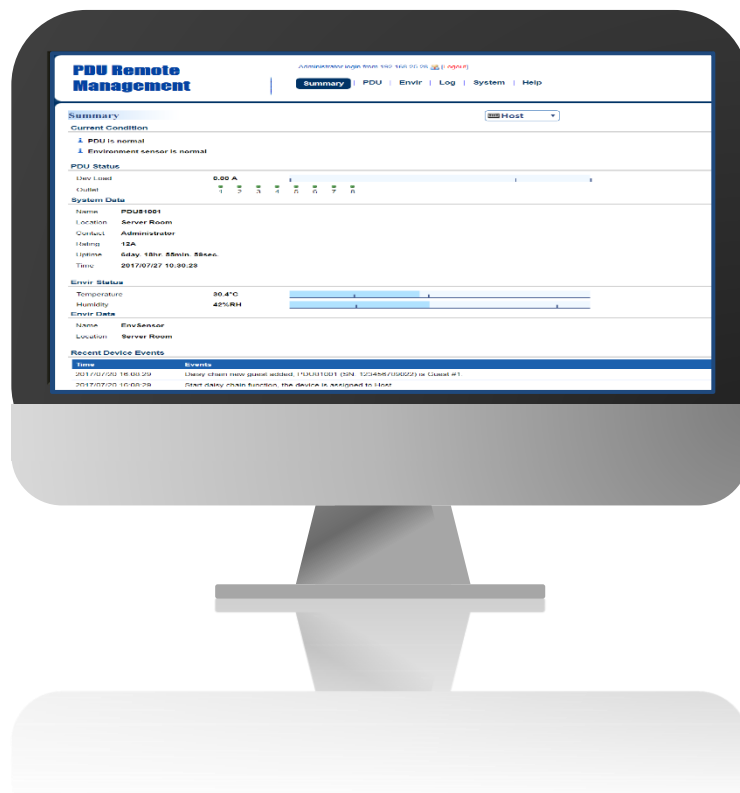
## Intelligent PDU User Guide

PDU31xxx

PDU41xxx

PDU71xxx

PDU81xxx



# Table of Contents

---

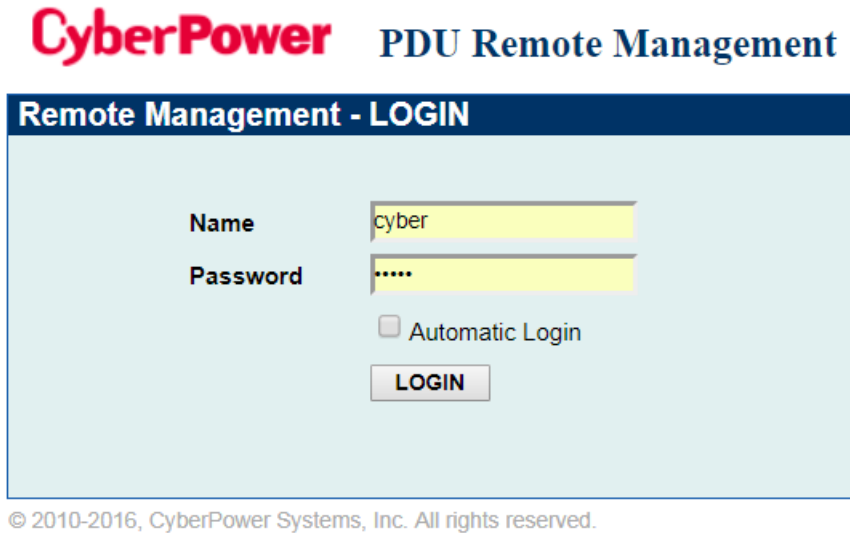
<b>Web Interface .....</b>	<b>1</b>
Introduction .....	1
Advanced Power Management.....	10
Outlet Management .....	38
Security.....	56
Network Service.....	67
PDU Information .....	79
<b>Command Line Interface .....</b>	<b>81</b>
Introduction .....	81
Command Lists.....	83
<b>Save and Restore Configuration Settings.....</b>	<b>106</b>
<b>PDU Network Daisy Chain.....</b>	<b>110</b>
<b>Firmware Upgrade.....</b>	<b>114</b>

# Web Interface

## Introduction

CyberPower’s Intelligent Power Distribution Unit (PDU) Web Interface gives users all the features they need to configure, manage, and monitor the Intelligent PDU Series via a Web browser. With this easy-to-navigate interface, users can perform real-time monitoring of each outlet, control individual outlet, set power alerts, and complete many other tasks in an intuitive manner.

## How to Log in



1. Open a Web browser.
2. Enter the IP address of the CyberPower PDU in the Browser Address Bar, and then press ENTER.  
 Note: To look up the IP address, please refer to the LCD screen of the PDU.
3. Enter the information for the User Name and Password fields.  
 There are two types of user accounts.

Account Type	Default User Name	Default Password	Authorization
Administrator	cyber	cyber	View, access, and control all settings.
Viewer	device	cyber	View all settings.

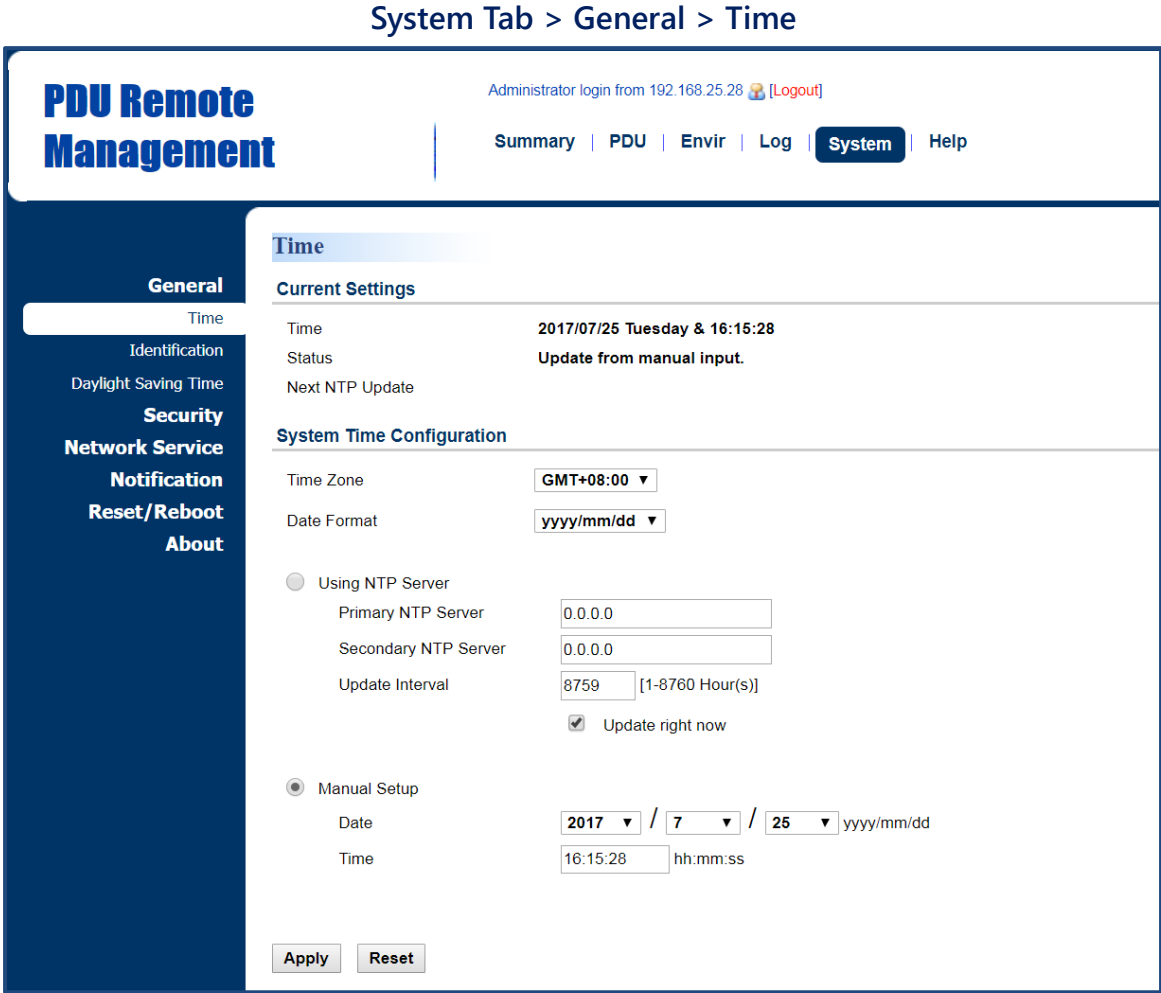
4. Click LOGIN to open the [Summary Tab](#).

### General Settings

These are the basic settings for the PDU.

#### 1. Date and Time Settings

The date and time can be set manually or synchronized with a Network Time Protocol (NTP) server. All time-related configurations are based on this setting. See [System Tab > General > Time](#).



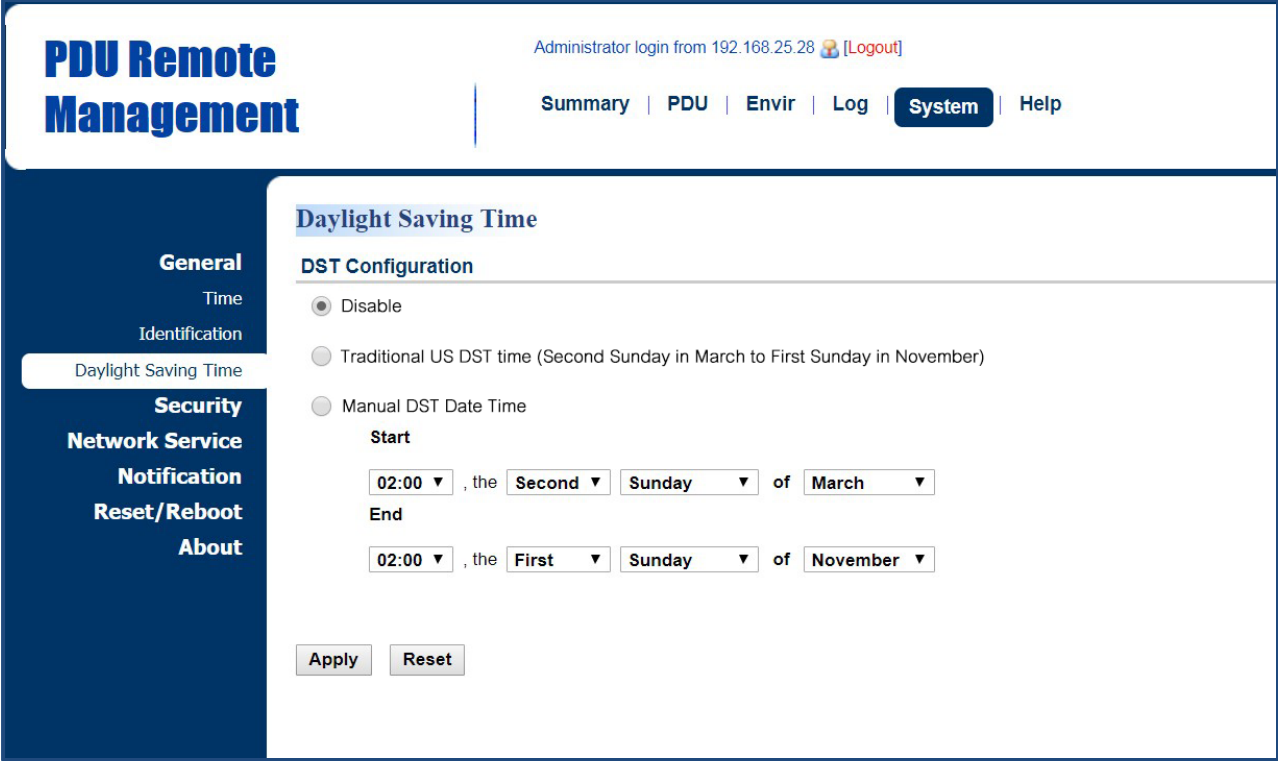
Item	Definition
<b>Current Settings</b>	
Time	The current date and time.
Status	Show whether the date and time setting is updated by manual setup or by the NTP (Network Time Protocol) server.
Next NTP Update	Synchronize with <i>Update Interval</i> .

Item	Definition
<b>System Time Configuration</b>	
Time Zone	The options for time zone selection.
Date Format	The options for date format selection.
Using NTP Server	<p><b>*Primary NTP Server:</b> Users enter the IP address/domain name of the NTP server and choose local time zone based on their location.</p> <p><b>*Secondary NTP Server:</b> Users enter the IP address/domain name of the NTP server and choose local time zone based on their location.</p> <p><b>*Update Interval:</b> The frequency for updating the date and time from the NTP server. Select the <b>Update right now</b> option to update immediately.</p>
Manual Setup	<p><b>*Date:</b> Enter the date in the designated format.</p> <p><b>*Time:</b> Enter the time in the designated format.</p>

2. Daylight Saving Time

Users adjust the daylight saving time according to their location. See [System Tab > General > Daylight Saving Time](#).

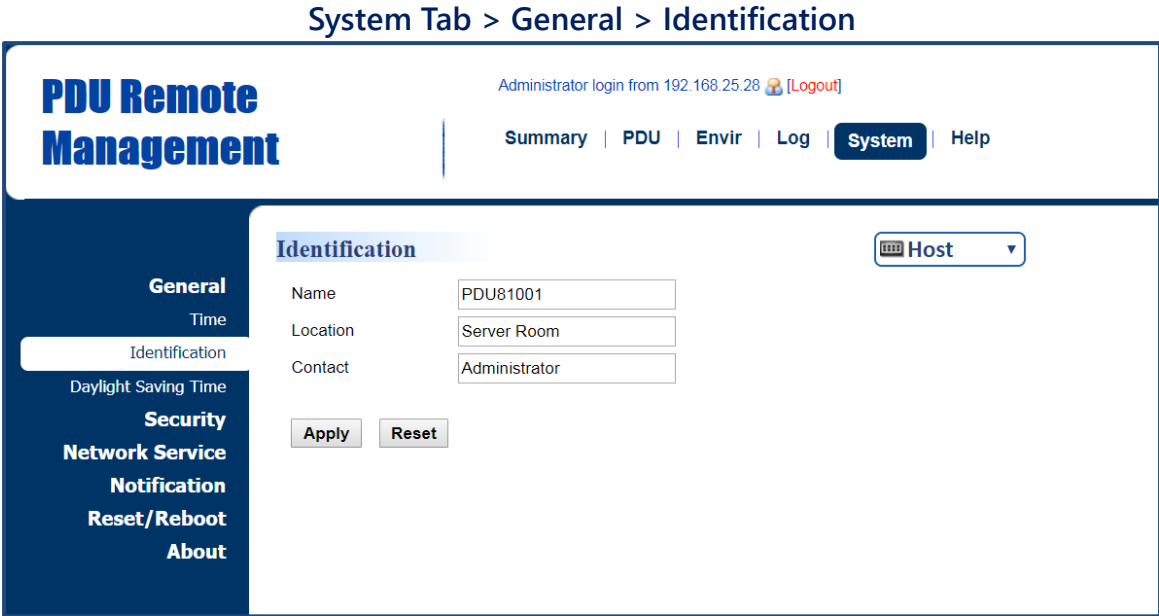
System Tab > General > Daylight Saving Time



Item	Definition
<b>DST Configuration</b>	
Disable	Disable the DST function.
Traditional US DST Time	Start from the second Sunday in March to the first Sunday in November.
Manual DST Date Time	Select the start/end time using the dropdown menu.

3. Device Identification

Users assign the device’s name, location, and the person to contact about issues. See **System Tab > General > Identification**.

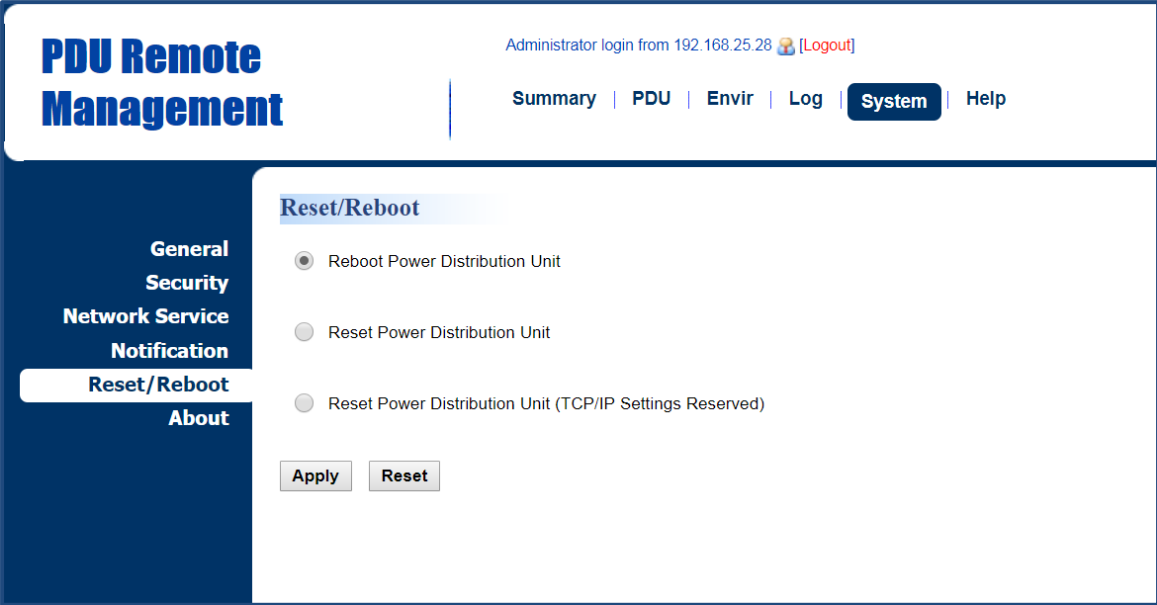


Item	Definition
HOST/GUEST#	Select the role of the PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Name	The name entered by the user to identify the PDU.
Location	The PDU location entered by the user.
Contact	The person to be contacted about issues. Entered by the user.

4. Device Reset/Reboot

Users can reboot the PDU or reset all the settings to defaults. See [System Tab > Reset/Reboot](#).

System Tab > Reset/Reboot



Item	Definition
Reboot Power Distribution Unit	Restart the PDU without power cycling any outlet.
Reset Power Distribution Unit	Reset the PDU to its factory default setting and restart it. This action will power cycle any outlet.
Reset Power Distribution Unit (TCP/IP Settings Reserved)	Reset the PDU to its factory default setting while reserving the TCP/IP settings, and restart the PDU. This action will power cycle any outlet.



5. Environmental Monitoring

PDU with CyberPower ENVIROSENSOR can provide remote monitoring of temperature and humidity in a server closet and/or datacenter. You can set temperature and humidity threshold for event action warning. See [Envir Tab > Status](#) & [Envir Tab > Configuration](#). Note that Envir Tab **only** appears when an ENVIROSENSOR is connected to the PDU.

Envir Tab > Status

The screenshot shows the 'Envir Tab > Status' page in the 'PDU Remote Management' interface. At the top, it indicates 'Administrator login from 192.168.27.126' with a [Logout] link. The navigation menu includes Summary, PDU, **Envir**, Log, System, and Help. The left sidebar has 'Status' and 'Configuration' options. The main content area is titled 'Status' and contains the following sections:

- Information:** Name: EnvSensor, Location: Server Room.
- Temperature:** Current Value: **23.1 °C**; Maximum: 24.1 °C (at 02/15/2017 11:10:55); Minimum: 20.5 °C (at 02/16/2017 07:45:25). Includes a 'Reset' button.
- Humidity:** Current Value: **51 %RH**; Maximum: 56 %RH (at 02/16/2017 09:32:10); Minimum: 42 %RH (at 02/15/2017 13:12:40). Includes a 'Reset' button.
- Contact:** Contact#1: Normal; Contact#2: Normal; Contact#3: Normal; Contact#4: Normal.

Item	Definition
Information	Display the name and location of the ENVIROSENSOR.
<b>Temperature</b>	
Current Value	The real-time reading of temperature.
Maximum	The highest temperature recorded and the time of occurrence.
Minimum	The lowest temperature recorded and the time of occurrence. Click <b>Reset</b> to reset the highest and lowest value to zero.
<b>Humidity</b>	
Current Value	The real-time reading of humidity.

Item	Definition
Maximum	The highest humidity recorded and the time of occurrence.
Minimum	The lowest humidity recorded and the time of occurrence. Click <b>Reset</b> to reset the highest and lowest value to zero.
Contact	Display the current status of each input dry contact relay.

Envir Tab > Configuration

**PDU Remote Management** Administrator login from 192.168.25.32 [Logout]

Summary | PDU | **Envir** | Log | System | Help

**Configuration**

**Information**

Name: EnvSensor  
Location: Server Room

**Temperature**

High Threshold: 32 °C [1-70]  
Low Threshold: 15 °C [1-70]  
Hysteresis: 2 °C [1-10]  
Rate of Change: 10 °C per 5 minutes [1-70]  
Unit: °C

**Humidity**

High Threshold: 80 %RH [10-90]  
Low Threshold: 20 %RH [10-90]  
Hysteresis: 5 %RH [1-20]  
Rate of Change: 20 %RH per 5 minutes [1-80]

**Contact**

#1 Name & State: Contact#1, Normally Open  
#2 Name & State: Contact#2, Normally Open  
#3 Name & State: Contact#3, Normally Open  
#4 Name & State: Contact#4, Normally Open

Apply Reset

Item	Definition
<b>Information</b>	
Name	The name entered by user to identify the ENVIROSENSOR.
Location	The location of the ENVIROSENSOR, entered by the user.
<b>Temperature</b>	
High Threshold	Set the highest temperature value for a high temperature warning.
Low Threshold	Set the lowest temperature value for a low temperature warning.

Item	Definition
Hysteresis	<p>The point where the environmental state changes from abnormal to normal and users receive a clearing event notification. The function of Hysteresis is to avoid receiving multiple event notifications.</p> <p>*For high threshold, the point is the threshold minus the Hysteresis value; for low threshold, the point is the threshold plus the Hysteresis value.</p> <p>For example: The high threshold is 32°C, and hysteresis is 2°C. The temperature rises to 33°C, you will get a warning. Then it goes down to 31°C and up to 33°C repeatedly. No clearing events and warnings will occur while the temperature readings are within the Hysteresis. You will not get a clearing event until it drops to 30°C.</p>
Rate of Change	<p>Define the abnormal change of temperature per 5 minutes.</p> <p>For example: The current temperature is 23°C, and rate of change is 10°C. If it goes up to 33°C or down to 13°C within 5 minutes, you will get a warning.</p>
Unit	Select the unit of temperature.
<b>Humidity</b>	
High Threshold	Set the highest humidity value for a high humidity warning.
Low Threshold	Set the lowest humidity value for a low humidity warning.
Hysteresis	Same as <i>Hysteresis</i> under temperature.
Rate of Change	Same as <i>Hysteresis</i> under temperature.
<b>Contact</b>	Enter the name of each input dry contact relay and use the dropdown menu to define the normal status of each one.

# Advanced Power Management

## Remote Monitoring

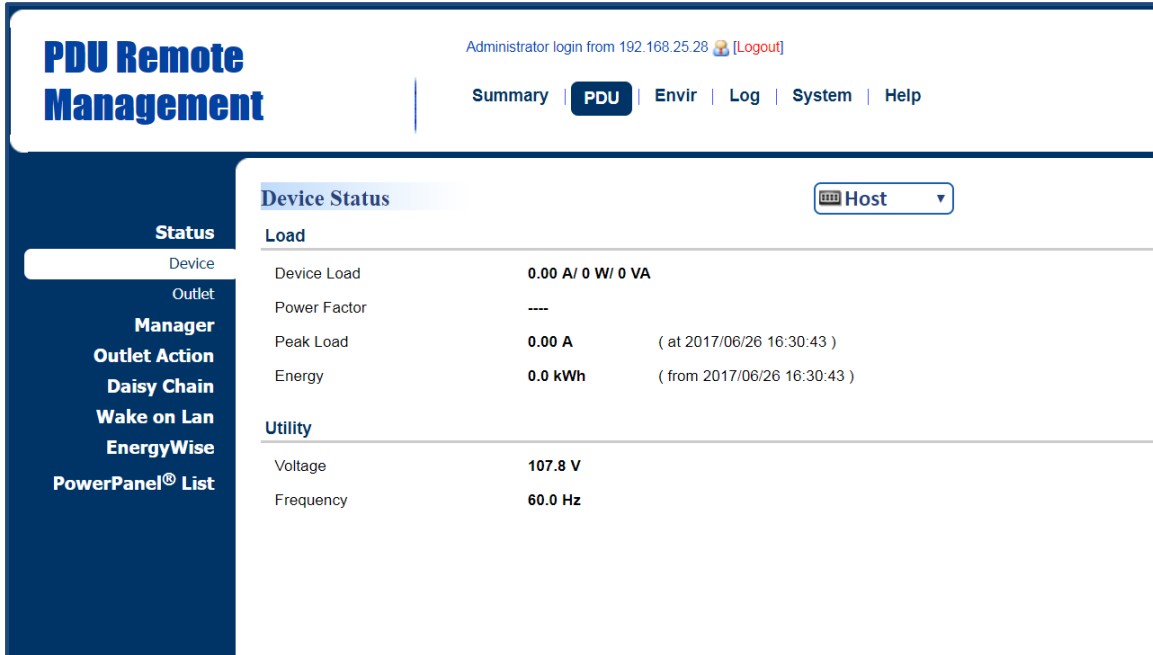
Users can see real-time readings of PDU vitals such as device load, power consumption, and outlet status for an overview of current PDU status. See [Summary Tab](#), [PDU Tab > Status](#), and [PDU Tab > Status > Outlet](#).

### Summary Tab

Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Current Condition	Operating condition of the PDU and ENVIROSENSOR.
<b>PDU Status</b>	
Dev Load	Total load current of all connected devices, measured in Amps.
Outlet	The on/off status of each outlet. The green light icon indicates that the outlet is on and providing power. This light will go off when the outlet turns

Item	Definition
	off. Outlet Tooltip Function: move the cursor to an individual outlet, Outlet name and its ON/OFF status will be shown.
<b>System Data</b>	
Name	The name of the PDU. For configuration, see <a href="#">System Tab &gt; General &gt; Identification</a> .
Location	The location of the PDU. For configuration, see <a href="#">System Tab &gt; General &gt; Identification</a> .
Contact	The person accountable for the maintenance of the PDU. For configuration, see <a href="#">System Tab &gt; General &gt; Identification</a> .
Rating	UL current rating of the PDU, measured in Amps.
Uptime	The amount of time the system has been working for since it was last restarted.
Time	System time of the PDU. For configuration, see <a href="#">System Tab &gt; General &gt; Time</a> .
<b>Envir Status</b>	
Temperature	Display temperature reading when the ENVIROSENSOR is connected to the PDU.
Humidity	Display humidity reading when the ENVIROSENSOR is connected to the PDU.
<b>Envir Data</b>	
Name	The name of the ENVIROSENSOR. For configuration, see <a href="#">Envir Tab &gt; Configuration</a> .
Location	The location of the ENVIROSENSOR. For configuration, see <a href="#">Envir Tab &gt; Configuration</a> .
<b>Recent Device Events</b>	A list of the five most recent device events. All events are related to configuration changes.

## PDU Tab &gt; Status &gt; Device



**PDU Remote Management**

Administrator login from 192.168.25.28 [Logout]

Summary | **PDU** | Envir | Log | System | Help

**Device Status** Host

**Status**

- Device
- Outlet
- Manager
- Outlet Action
- Daisy Chain
- Wake on Lan
- EnergyWise
- PowerPanel® List

**Load**

Device Load	0.00 A / 0 W / 0 VA
Power Factor	---
Peak Load	0.00 A ( at 2017/06/26 16:30:43 )
Energy	0.0 kWh ( from 2017/06/26 16:30:43 )

**Utility**

Voltage	107.8 V
Frequency	60.0 Hz

Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
<b>Load</b>	
Device Load	Load current of the connected device(s), measured in Amps. Load power of the connected device(s), measured in Kilowatts and Kilovolt-Amps.
Bank Load*	Load current of the bank, measured in Amps.
Power Factor	Power factor of the connected device(s).
Peak Load	Maximum load current recorded and the time of occurrence. Users can reset the value to zero at Power Restore in <a href="#">PDU Tab &gt; Manager &gt; Device</a> .
Energy	Total energy consumed by the connected device(s) from the reset date, measured in kWh. Users can reset the value to zero at Power Restore in <a href="#">PDU Tab &gt; Manager &gt; Device</a> .
<b>Utility</b>	
Voltage	Voltage of the utility power.
Frequency	Frequency of the utility power.

\*Only available in select models.

PDU Tab > Status > Outlet\*

The screenshot shows the 'PDU Remote Management' interface. At the top, it says 'Administrator login from 192.168.25.28 [Logout]'. Below that are navigation tabs: Summary, PDU, Envir, Log, System, Help. The main content area is titled 'Outlet Status' and has a dropdown menu set to 'Host'. Below this is a table with the following data:

#	Name	Status	Load (A)	Load (W)	Peak Load(W)	Energy(kWh)
1	Outlet1	ON	0.90	0	10 ( at 2017/06/27 04:07:56 )	0.0 ( from 2017/06/26 16:30:43 )
2	Outlet2	ON	1.68	30	60 ( at 2017/06/27 03:23:15 )	16.5 ( from 2017/06/26 16:30:43 )
3	Outlet3	ON	2.84	0	0 ( at 2017/06/26 16:30:43 )	0.0 ( from 2017/06/26 16:30:43 )
4	Outlet4	ON	3.17	0	0 ( at 2017/06/26 16:30:43 )	0.0 ( from 2017/06/26 16:30:43 )
5	Outlet5	ON	0.83	0	10 ( at 2017/06/26 22:48:32 )	0.0 ( from 2017/06/26 16:30:43 )
6	Outlet6	ON	1.96	30	70 ( at 2017/06/27 01:31:11 )	18.0 ( from 2017/06/26 16:30:43 )
7	Outlet7	ON	2.94	0	0 ( at 2017/06/26 16:30:43 )	0.0 ( from 2017/06/26 16:30:43 )
8	Outlet8	ON	3.22	0	0 ( at 2017/06/26 16:30:43 )	0.0 ( from 2017/06/26 16:30:43 )

\*The above Outlet Status Page is available for Switched Metered by Outlet Series only.

Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Status	The on/off status of each outlet.
Load (A)	Load current of each outlet, measured in Amps.
Load (kW)	Load power of each outlet, measured in Kilowatts.
Peak Load (kW)	The maximum load current recorded and the time of occurrence. Users can reset the value to zero at Power Restore in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a> .
Energy (kWh)	Total energy consumed by connected equipment of each outlet since the last reset. The reset can be set in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a> .

## Visible Power Consumption

With comprehensive energy measurement data, users can gain more visibility to the total power usage of a PDU, as well as estimate the energy cost and CO2 emissions. The energy-trend report also helps users analyze their power utilization and to review the history of power conditions. See [Log Tab > Status Records](#), [Log Tab > Graphing](#), [Log Tab > Energy Records](#), and [Log Tab > Maintenance](#).

### Log Tab > Status Records

PDU Remote Management		Administrator login from 192.168.25.28 <a href="#">[Logout]</a>						
		Summary	PDU	Envir	Log	System	Help	
Event Logs <b>Status Records</b> Energy Records Graphing Syslog Maintenance		<b>Status Records</b> <span>Host</span>						
Time	Device max (A)	Device (A)	Voltage (V)	Temp. (°C)	Hum. (%RH)	Outlet 1 max (W)	Outlet 1 (W)	
2017/07/25 13:34:28	0.00	0.00	107.8	30.0	38	0	0	
2017/07/25 12:34:29	0.00	0.00	107.8	30.0	40	0	0	
2017/07/25 11:34:29	0.00	0.00	107.8	29.8	38	0	0	
2017/07/25 10:34:29	0.00	0.00	107.8	29.9	39	0	0	
2017/07/25 09:34:29	0.00	0.00	107.8	29.6	41	0	0	
2017/07/25 08:34:29	0.00	0.00	107.8	30.7	40	0	0	
2017/07/25 07:34:29	0.00	0.00	107.8	30.8	45	0	0	
2017/07/25 06:34:29	0.00	0.00	107.8	30.6	45	0	0	
2017/07/21 00:34:37	0.00	0.00	107.8	29.8	44	0	0	
2017/07/20 23:34:37	0.00	0.00	107.8	29.5	45	0	0	
2017/07/20 22:34:37	0.00	0.00	107.8	29.0	46	0	0	

Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Device Max (A)	The maximum load current of the connected device(s) or bank during a specific time interval, measured in Amps. This interval can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Device (A)	Load current of the connected device(s) or bank, measured in Amps.
Voltage (V)	Voltage of the utility power.
Temp. (°C)	Temperature reading when the ENVIROSENSOR is connected to the PDU.
Hum. (%RH)	Humidity reading when the ENVIROSENSOR is connected to the PDU.
Outlet # Max (kW)*	The maximum load power of a specific outlet during a specific time interval, measured in Kilowatts. This interval can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Outlet # (kW)*	Load power of a specific outlet, measured in Kilowatts.



\*For Switched Metered by Outlet Series only.

## Log Tab &gt; Graphing

Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Graph Period	The time period is used to create a retroactive graph of the status records. A large time period will require more time to render the graph.
Graph Data	The data used to create a graph of the status records. Up to five data points can be selected. A large number of data selected will require more time to render the graph.
Graph Node	Select the <b>Display All Nodes in Detail</b> option to display the selected data points along the graph. When the cursor is moved to an individual data point, information about that point will be shown. If this option is not selected, the graph will show only the line (without the points), so less time is needed to render.
Draw	A graph of the status records will be created.
Reset	Reset the <i>Graph Period</i> to default (1 day).
Launch Graph in New Window	A detailed view of the graph opens in a new browser window.

### Log Tab > Energy Records

PDU Remote Management

Administrator login from 192.168.25.28 [Logout](#)  
[Summary](#) | [PDU](#) | [Environ](#) | [Log](#) | [System](#) | [Help](#)

Energy Records

Host

Time	Interval Energy(kWh)	Interval Cost(units)	Interval CO2(kg)	Energy (kWh)	Cost (units)	CO2 (kg)	Outlet # (kWh)
2017/07/25 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/24 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/23 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/22 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/21 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/20 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/19 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/18 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/07/01 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0
2017/06/30 00:00:00	0.0	0.00	0.000	0.0	0.00	0.000	0.0

Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Interval Energy (kWh)	Energy consumed by connected device(s) during a specific time interval, measured in kWh. This interval can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Interval Cost (units)	Cost of the energy consumed by the connected device(s) during a specific time interval, equal to <i>Electricity Rate</i> multiplied by <i>Interval Energy</i> . The interval and electricity rate can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Interval CO2 (kg)	Equivalent CO2 emission of the connected device(s) during a specific time interval, equal to <i>CO2 Emissions</i> multiplied by <i>Interval Energy</i> . The interval and CO2 emissions can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Energy (kWh)	Accumulated <i>Interval Energy</i> since the last reset. The reset can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Cost (units)	Accumulated <i>Interval Cost</i> since the last reset. The reset can be set in <a href="#">Log Tab &gt; Maintenance</a> .
CO2 (kg)	Accumulated <i>Interval CO2</i> since the last reset. The reset can be set in <a href="#">Log Tab &gt; Maintenance</a> .
Outlet # (kWh)*	Accumulated <i>Interval Energy</i> of a specific outlet since the last reset. The reset can be set in <a href="#">Log Tab &gt; Maintenance</a> .

\*For Switched Metered by Outlet Series only.

### Log Tab > Maintenance

PDU Remote Management

Administrator login from 192.168.25.28 [\[Logout\]](#)

Summary | PDU | Envir | **Log** | System | Help

Event Logs  
 Status Records  
 Energy Records  
 Graphing  
 Syslog  
**Maintenance**

#### Maintenance

---

##### Event Logs

Clear All Logs  No  Yes, right now.

The Number of Events 111 / 1024

Save Event Logs

---

##### Status Records

Recording Interval

Clear All Records  No  Yes, right now.

Remaining Time 56day 11hour / 85day 8hour

Save Status Records

---

##### Energy Records

Recording Interval

Clear All Records  No  Yes, right now.

Electricity Rate  units / kWh [0.00-600]

CO2 Emissions  kg / kWh [0.00-600]

Save Energy Records

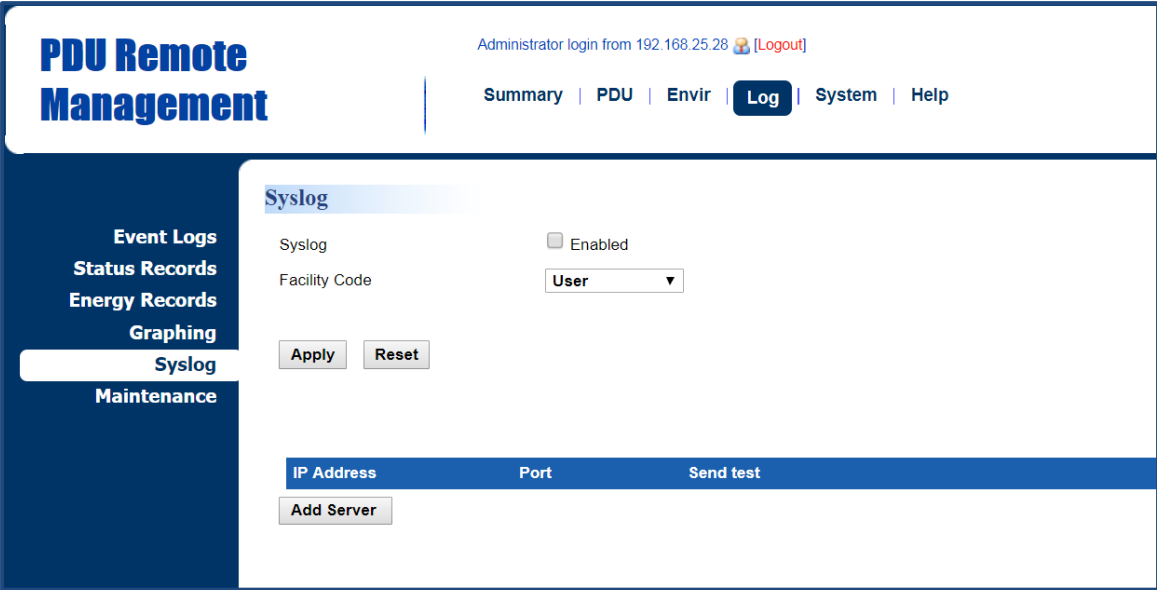
Item	Definition
<b>Event Logs</b>	
Clear All Logs	Clear the existing event logs.
The Number of Events	The number of the existing event logs and the maximum number of the event logs that can be recorded. Once the maximum number is reached, new events overwrite oldest events in memory.
Save Event Logs	Save the existing event logs as a text file.
<b>Status Records</b>	
Recording Interval	The frequency to record the status data. A smaller interval will provide more recordings, but the recordings are overwritten in a shorter period of time. A larger interval will provide fewer recordings, but the recordings are overwritten in a longer period of time.
Clear All Records	Clear the existing status records.

Item	Definition
Remaining Time	The time that records have been kept. A smaller recording interval leads to less remaining time while a larger recording interval leads to more remaining time. Once the maximum number is reached, new status records overwrite oldest status records in memory.
Save Status Records	Save the status records as a text file.
<b>Energy Records</b>	
Recording Interval	The frequency to record the energy data.
Clear All Records	Clear the existing energy records.
Electricity Rate	The cost (units) of energy per unit of energy consumed (kWh). Unit is a monetary value.
CO2 Emissions	The equivalent CO2 emission (kg) per unit of energy consumed (kWh).
Save Energy Records	Save the existing energy records as a text file.

### Event Logging

Users can view all the events, including log in/out records and configuration changes. The timestamp is recorded in a 24-hour format. See [Log Tab > Syslog](#) and [Log Tab > Event Logs](#). For event logs, Users can clear the existing event logs in [Log Tab > Maintenance](#)

### Log Tab > Syslog



Item	Definition
Syslog	Check this box to enable Syslog function.
Facility Code	Classify syslog message

Click Add Server to enter [Syslog Server Page](#).

## Syslog Server Page

PDU Remote Management

Administrator login from 192.168.25.28 [\[Logout\]](#)

[Summary](#) | [PDU](#) | [Envir](#) | [Log](#) | [System](#) | [Help](#)

Event Logs

Status Records

Energy Records

Graphing

Syslog

Maintenance

### Syslog Server

Server IP

Server Port

Item	Definition
Server IP	The IP address of Syslog server.
Server Port	The port number that Syslog server uses to communicate.

## Logs Tab > Event Logs

PDU Remote Management

Administrator login from 192.168.25.28 [\[Logout\]](#)

[Summary](#) | [PDU](#) | [Envir](#) | [Log](#) | [System](#) | [Help](#)

Event Logs

Status Records

Energy Records

Graphing

Syslog

Maintenance

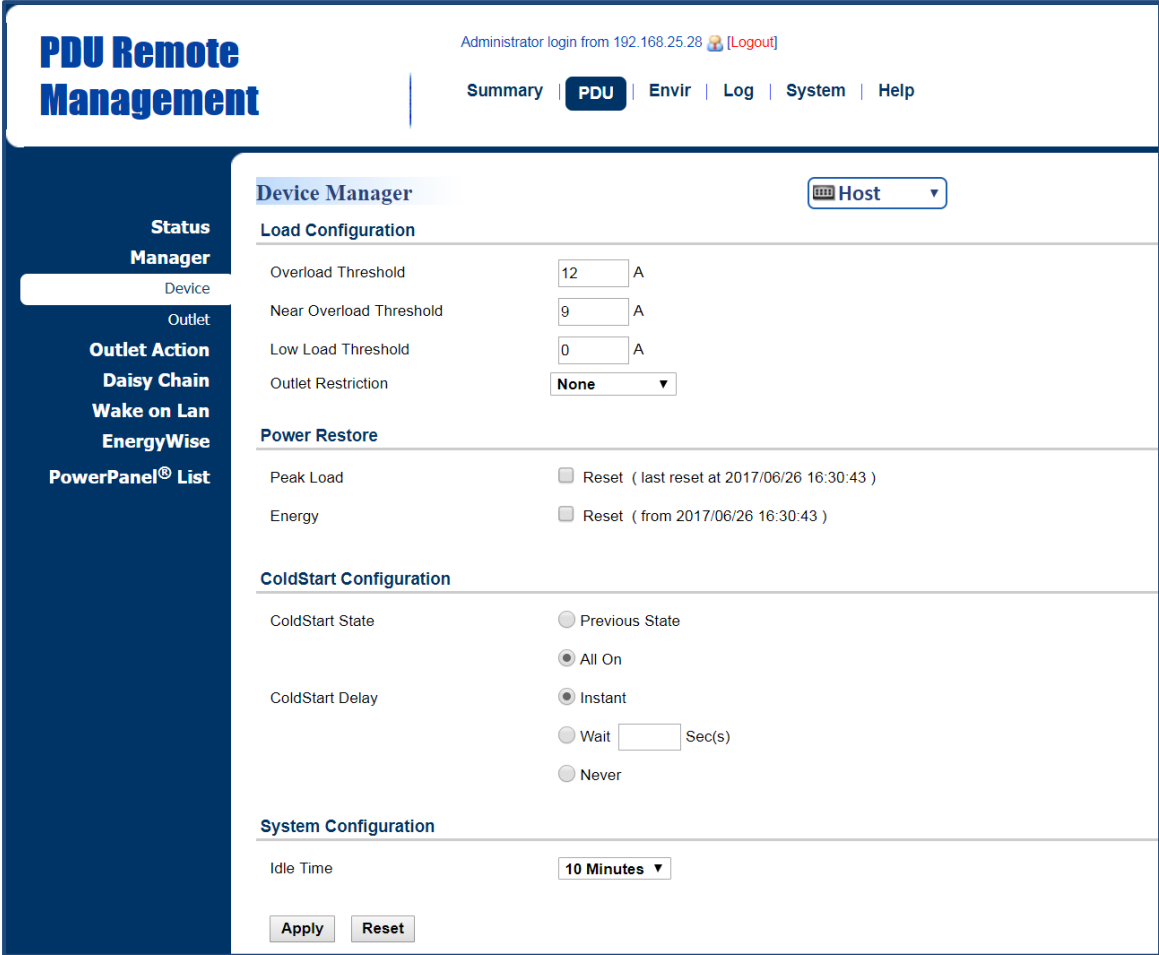
### Event Logs

Time	Events
2017/07/25 16:12:48	Admin user login from 192.168.25.28.
2017/07/25 14:49:49	Admin user logout from 192.168.25.28.
2017/07/25 14:37:51	Admin user login from 192.168.25.28.
2017/07/25 14:31:57	Admin user logout from 192.168.25.28.
2017/07/25 14:21:53	Admin user login from 192.168.25.28.
2017/07/25 14:14:13	Admin user logout from 192.168.25.28.
2017/07/25 13:53:25	Admin user login from 192.168.25.28.
2017/07/25 13:53:14	Login authorization failure via HTTP from 192.168.25.28.
2017/07/25 13:30:36	Admin user logout from 192.168.25.28.
2017/07/25 13:20:33	Admin user login from 192.168.25.28.
2017/07/25 11:12:15	Admin user logout from 192.168.25.28.
2017/07/25 10:59:48	Admin user login from 192.168.25.28.
2017/07/24 22:03:10	Admin user logout from 192.168.25.28.
2017/07/24 21:44:02	Admin user login from 192.168.25.28.
2017/07/24 21:29:47	Admin user logout from 192.168.25.28.

### Power Protection

The configurable load threshold can be set to prevent an overload condition. Coldstart and system configurations are also offered for different user needs. See [PDU Tab > Device Manager](#).

#### PDU Tab > Manager > Device



Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
<b>Load Configuration</b>	
Overload Threshold	Set the value for the total current on the PDU that will signal an overload warning. Must be higher than <i>Near Overload Threshold</i> and equal to or lower than the PDU <i>Rating</i> in the <a href="#">Summary Tab</a> .
Near Overload Threshold	Set the value for the total current on the PDU that will signal a near overload warning. Must be between <i>Overload Threshold</i> and <i>Low Load Threshold</i> .



Item	Definition
Low Load Threshold	Set the value for the total current on the PDU that will signal a low load warning. Must be lower than <i>Near Overload Threshold</i> .
Outlet Restriction**	<p>When load current exceeds the corresponding threshold, no outlets will be allowed to turn on.</p> <p>*None: Users can turn on an outlet even if the device is in Near Overload or Overload state.</p> <p>*On Near Overload: Users cannot turn on an outlet when the device is in Near Overload or Overload state.</p> <p>*On Overload: Users cannot turn on an outlet when the device is in Overload state.</p>
<b>Power Restore</b>	
Peak Load	Reset the peak load to zero.
Energy	Reset the energy to zero.
<b>ColdStart Configuration</b>	
ColdStart State	<p>*Previous State: Outlets will return to the same state (on or off) they were in prior to the PDU turning off. The <i>ColdStart Delay</i> setting will apply when the PDU resumes power.</p> <p>*All On: All outlets will turn on when power is restored to the PDU.</p>
ColdStart Delay	<p>*Instant: Outlets will be turned on immediately when power is restored to the PDU.</p> <p>*Wait: Outlets will be turned on according to this setting when power is restored to the PDU.</p> <p>*Never: Outlets will not be turned on when power is restored to the PDU.</p>
<b>System Configuration</b>	
Idle Time	The PDU LCD screen will turn off automatically after it remains idle for the selected period of time.

\*\*For some models, the Outlet Restriction only shows in the [Bank Manager Page](#).

## Event Action Notification

Users decide the event actions for which they receive notifications. When a certain event happens, an automatic notification will be sent to users so that they can make timely decisions to prevent potential problems. See [System Tab > Notification](#).

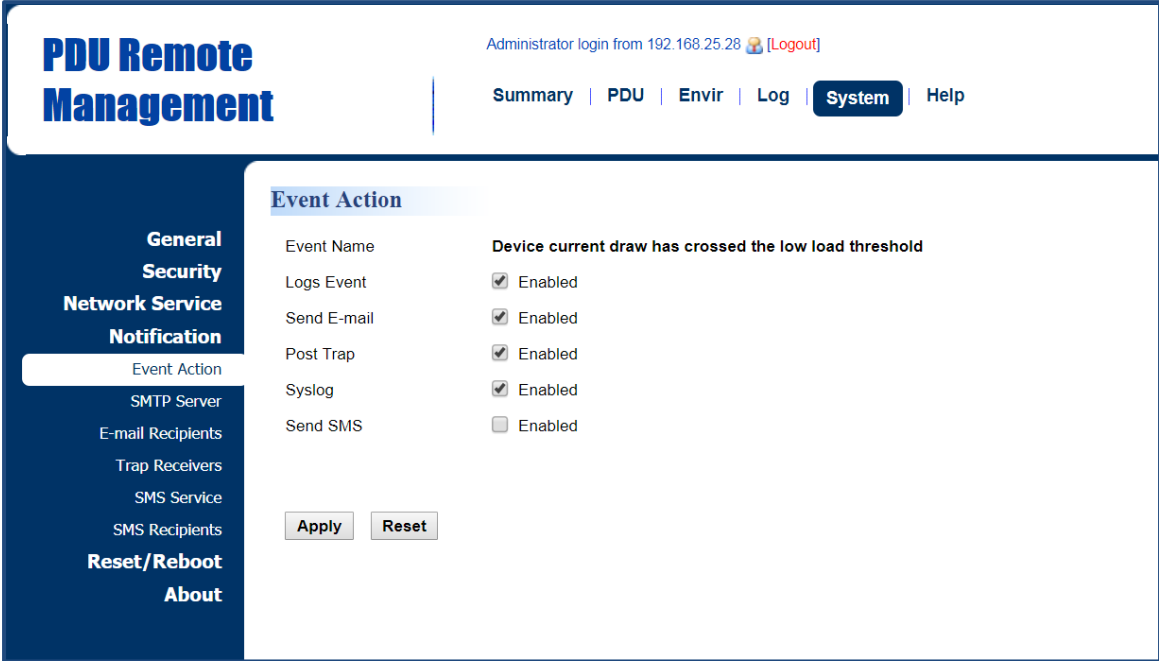
### System Tab > Notification > Event Action

The screenshot shows the 'Event Action' configuration page in the PDU Remote Management web interface. The page is titled 'Event Action' and is part of the 'System' tab. It features a navigation menu on the left with categories like General, Security, Network Service, Notification, and About. The main content area is divided into 'Device Events' and 'System Events' sections. Below these sections is a table with columns for 'Event', 'Log', 'E-mail', 'Trap', 'Syslog', and 'SMS'. The first two rows of the table are highlighted with a red box, indicating the events that have been selected for notification.

Event	Log	E-mail	Trap	Syslog	SMS
Device current draw has crossed the low load threshold	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
The low load condition on a PDU has been cleared	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device current draw has cross the near overload threshold	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
The near overload condition on a PDU has been cleared	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device current draw has crossed the overload condition	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
The overload condition on a PDU has been cleared	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Click the Event field to enter the [Event Action Page](#).

### Event Action Page



The Event Action Page enables users to modify the notification method.

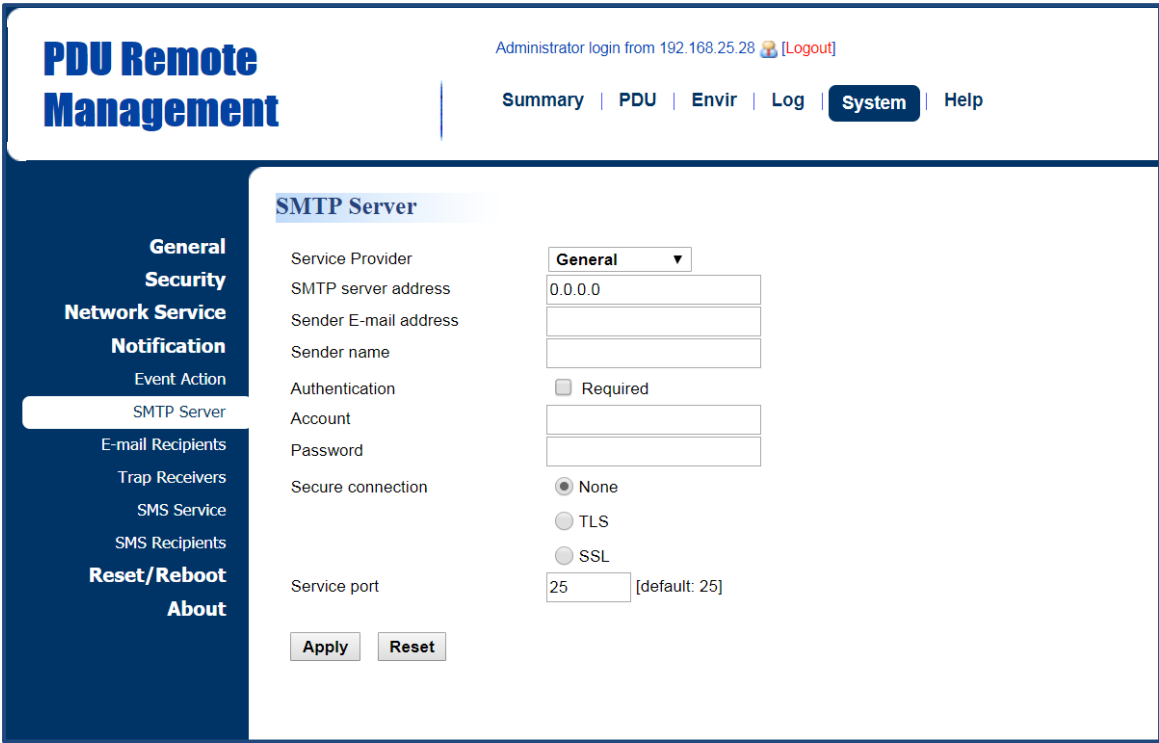
Item	Definition
Logs Event	Record the device event in the <i>Event Logs</i> .
Send E-mail	Send an email to a specific user. An available SMTP server is necessary.
Post Trap	Send a SNMP trap to a specific IP address.
Syslog	Record the device event in Syslog server.
Send SMS	Send a short message to a specific mobile phone number. An available Short Message Service (SMS) provider is needed.

# Event Action Recipient Settings

## 1. E-mail Notification

Set the proper SMTP server settings so that users can receive an email when a specific event occurs. See [System Tab > Notification > SMTP Server](#).

### System Tab > Notification > SMTP Server



Item	Definition
Service Provider	The service provider of e-mail account. There are two options: Other and Gmail.
Other	Select other as service provider. Complete all field settings and click <b>Apply</b> to save.
Gmail	Select Gmail as the service provider. Click <b>Authorize</b> for an authorization to send a mail notification. Then complete the sender name and click <b>Apply</b> to save the settings.
SMTP server address	The IP or host Name of SMTP server used to notify users by e-mail.
Sender E-mail Address	The From field shown in the e-mail message.
Sender Name	The name of the sender.
Authentication	Select this option if the SMTP server requires Authentication.

Item	Definition
Account	Account used for Authentication.
Password	Password used for Authentication.
Secure connection	Enable/Disable TLS or SSL to encrypt the SMTP connection.
Service Port	The port number that the PDU uses to communicate with SMTP server.

Users can set up to five e-mail recipients in designated email address format.  
See [System > Notification > E-mail Recipients](#).

### System > Notification > E-mail Recipients

The screenshot displays the 'E-mail Recipients' configuration page in the PDU Remote Management web interface. The page title is 'E-mail Recipients'. It features a table with columns for 'E-mail', 'Status', 'Send test', and 'Result'. One recipient is listed with the email address 'ted\_mosby@cyberpower.com' and a status of 'Enabled'. A 'TEST' button is visible next to the recipient. A 'New Recipient' button is located below the table. The left sidebar shows navigation options like 'General', 'Security', 'Network Service', 'Notification', 'E-mail Recipients', 'Trap Receivers', 'SMS Service', 'SMS Recipients', 'Reset/Reboot', and 'About'. The top navigation bar includes 'Summary', 'PDU', 'Envir', 'Log', 'System', and 'Help'.

Item	Definition
E-mail	Click the e-mail address of the recipient to enter the <a href="#">Configure E-mail Recipient Page</a> . Users can modify the e-mail address, change its status, check test result, and delete an existing recipient.
TEST	Click this button to check if the SMTP setting and the email recipients are set correctly.
New Recipient	Click this button to enter the <a href="#">Add New E-mail Recipient Page</a> . Users can add a new recipient.

### Configure E-mail Recipient Page

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

**General**  
**Security**  
**Network Service**  
**Notification**  
Event Action  
SMTP Server  
**E-mail Recipients**  
Trap Receivers  
SMS Service  
SMS Recipients  
**Reset/Reboot**  
**About**

#### Configure E-mail Recipient

Activate  Enabled

E-mail

**Apply** **Reset** **Delete**

### Add New E-mail Recipient Page

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

**General**  
**Security**  
**Network Service**  
**Notification**  
Event Action  
SMTP Server  
**E-mail Recipients**  
Trap Receivers  
SMS Service  
SMS Recipients  
**Reset/Reboot**  
**About**

#### Add New E-mail Recipient

Activate  Enabled

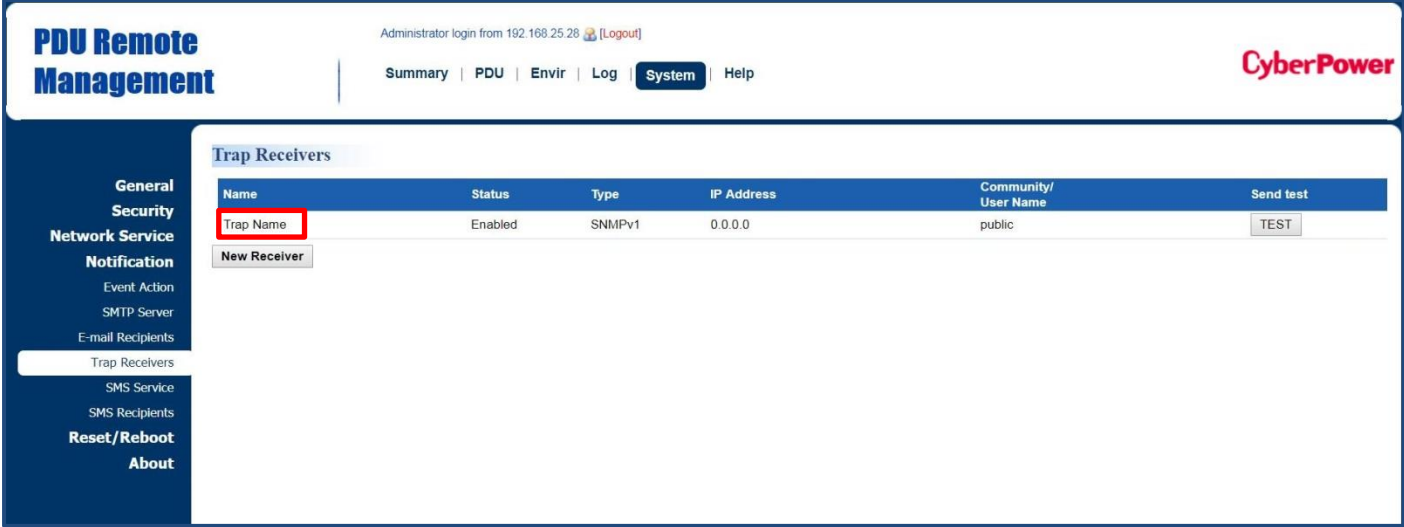
E-mail

**Apply** **Reset**

2. SNMP Trap Notification

Set up to 10 SNMP trap receivers to be notified when an event occurs. See [System > Notification > Trap Receivers](#).

System > Notification > Trap Receivers



Item	Definition
Name	Click on the trap name to enter the <a href="#">Configure Trap Receiver Page</a> . Users can modify or delete an existing receiver.
TEST	Click this button to check if the trap can be sent.
New Receiver	Click this button to enter the <a href="#">Add New Trap Receiver Page</a> . Users can add a new recipient.

### Configure Trap Receiver Page

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

- General
- Security
- Network Service
- Notification
  - Event Action
  - SMTP Server
  - E-mail Recipients
  - Trap Receivers**
  - SMS Service
  - SMS Recipients
- Reset/Reboot
- About

#### Configure Trap Receiver

Active  Enabled

Name

IP Address

SNMPv1

Community

SNMPv3

User Name

### Add New Trap Receiver Page

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

- General
- Security
- Network Service
- Notification
  - Event Action
  - SMTP Server
  - E-mail Recipients
  - Trap Receivers**
  - SMS Service
  - SMS Recipients
- Reset/Reboot
- About

#### Add New Trap Receiver

Active  Enabled

Name

IP Address

SNMPv1

Community

SNMPv3

User Name



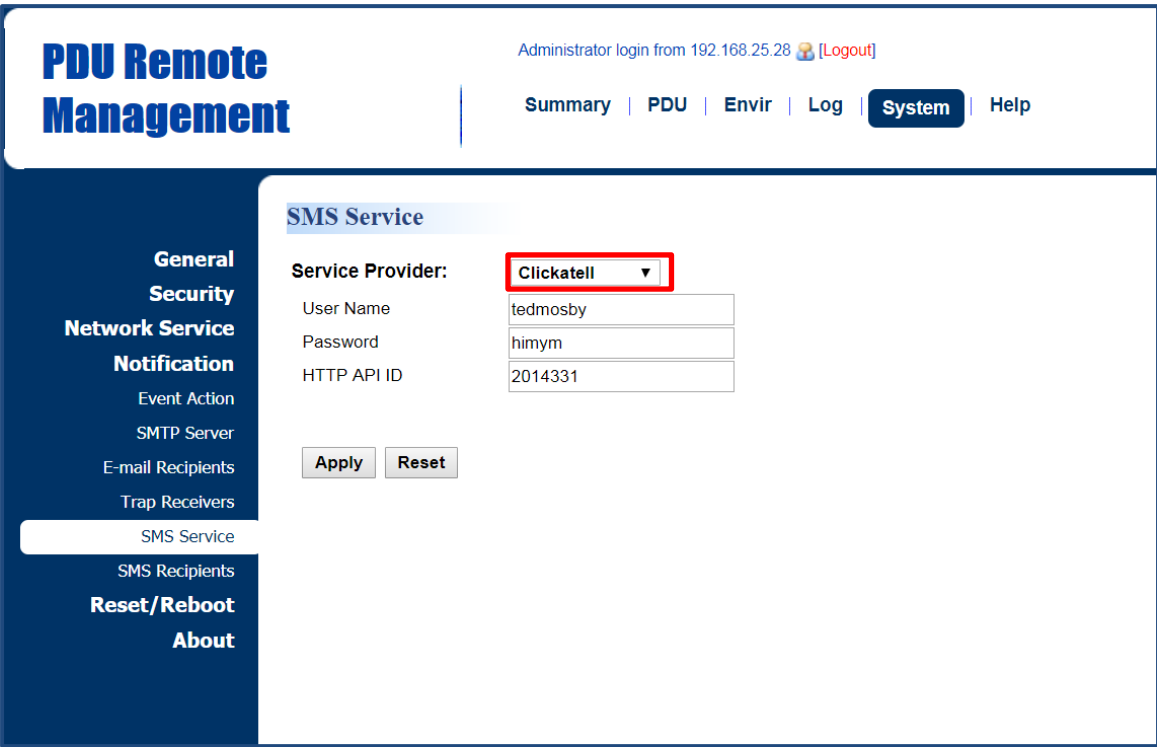
Item	Definition
Name	The name of trap receiver.
IP Address	The IP address of the trap receiver.
SNMPv1	If choosing the <b>SNMPv1</b> option as the trap type for a trap receiver, select the corresponding community. See <a href="#">System Tab &gt; Network Service &gt; SNMPv1 Service</a> .
SNMPv3	If choosing the <b>SNMPv3</b> option as the trap type for a trap receiver, select the corresponding user name. See <a href="#">System Tab &gt; Network Service &gt; SNMPv3 Service</a> .

### 3. SMS Notification

Short Message Service (SMS) is used by mobile communication systems to send a short message to a specific mobile phone number. Standardized communication protocols allow the exchange of short text messages between mobile devices.

The system provides four methods for users to choose how they want to send a message. See [System > Notification > SMS Service](#).

#### System > Notification > SMS Service

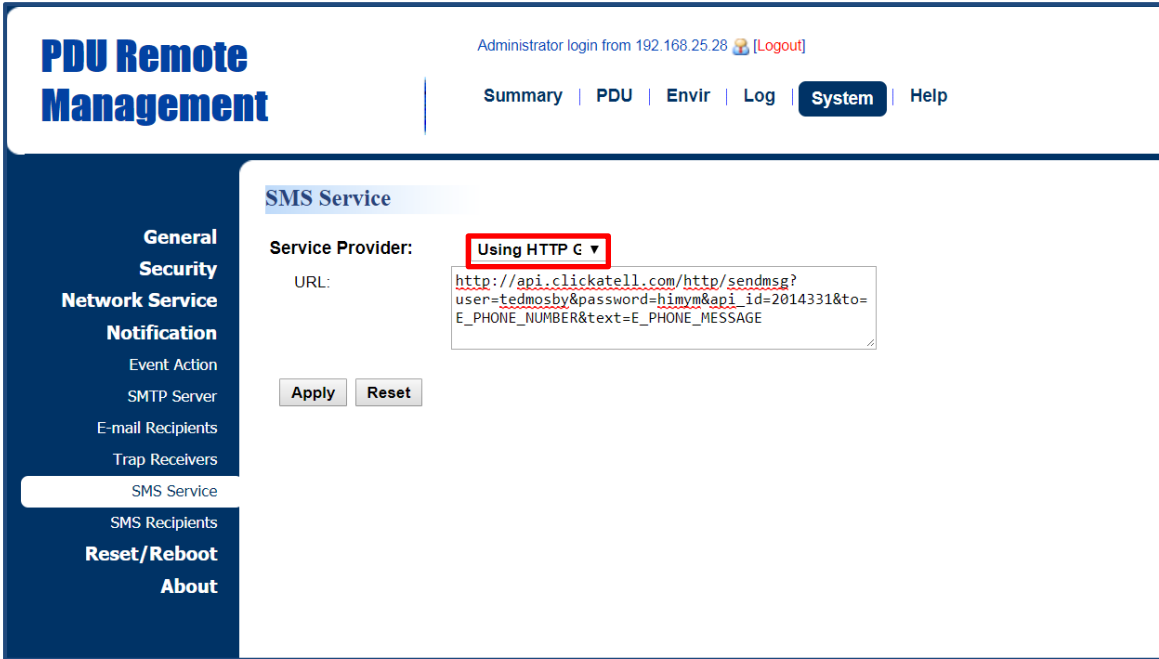


**Clickatell method:**

Clickatell is one of the supported SMS service providers. Go to the Clickatell website to sign up and get an API ID.

Item	Definition
User name	The account username created on Clickatell website.
User password	The user password created on Clickatell website.
HTTP API ID	The API ID acquired on Clickatell website.

System > Notification > SMS Service



Using HTTP GET:

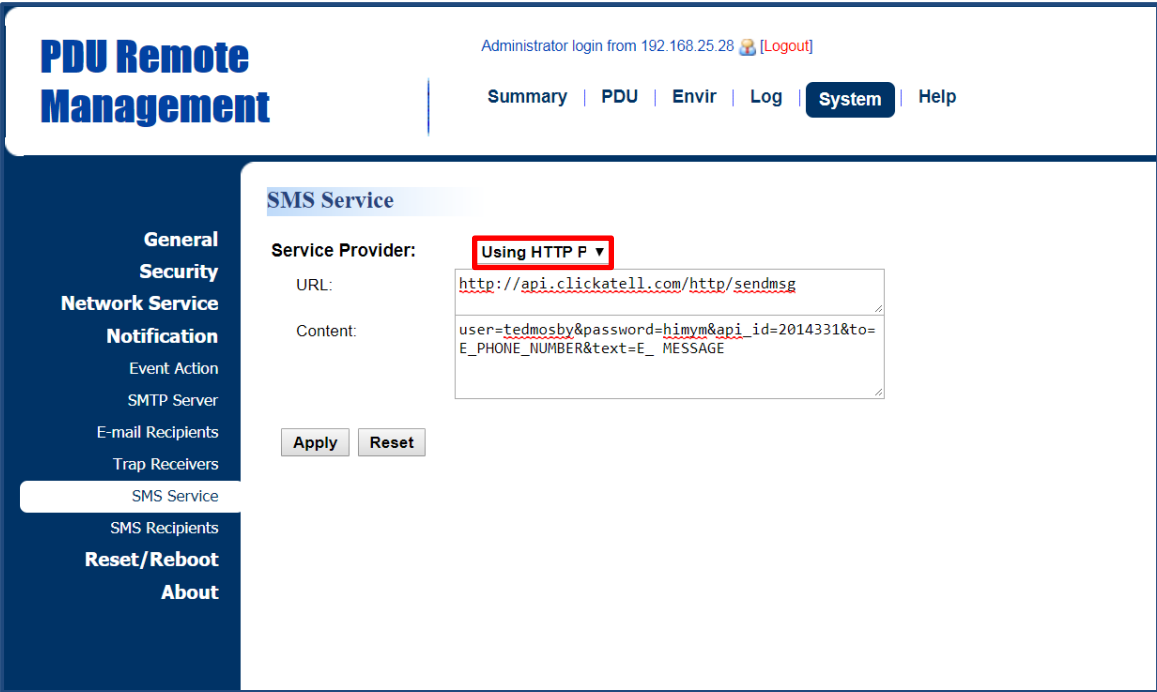
Use the example where Clickatell is the SMS provider.

The basic form of URL using the HTTP GET method is:

http://api.clickatell.com/http/sendmsg?user=tedmosby&password=himym&api\_id=2014331&to=E\_PHONE\_NUMBER&text=E\_PHONE\_MESSAGE

Query String in the URL	Definition
user=tedmosby	Replace “tedmosby” with the user name created at the Clickatell website.
password=himym	Replace “himym” with the password created at the Clickatell website.
api_id=2014331	Replace “2014331” with the API ID acquired at the Clickatell website.
to=E_PHONE_NUMBER	Do not replace this information. It refers to the receiver phone number entered in <a href="#">System Tab &gt; Notification &gt; SMS Recipients</a> .
text=E _MESSAGE	Do not replace this information. It refers to the event action sent by the SMS service provider. For configurations, see <a href="#">System Tab &gt; Notification &gt; Event Action</a> .

System > Notification > SMS Service



Using HTTP POST:

Use the example where Clickatell is the SMS provider.

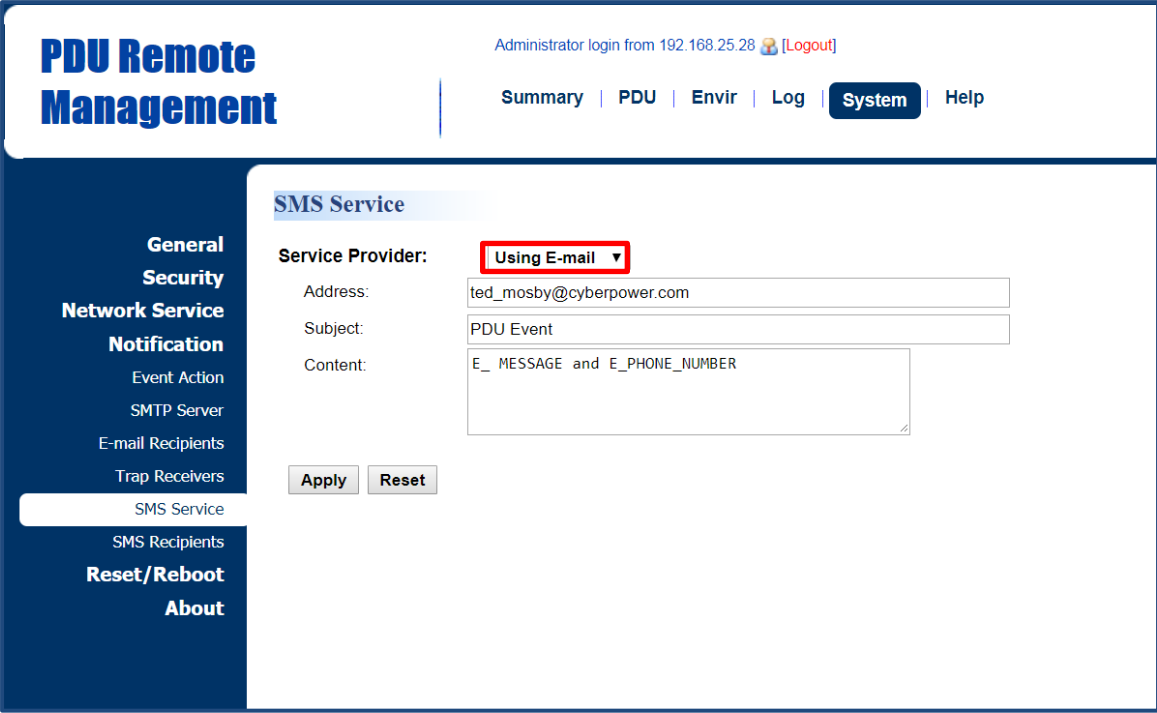
The basic form of URL is: http://api.clickatell.com/http/sendmsg

The basic form of body is:

user=tedmosby&password=himym&api\_id=2014331&to=E\_PHONE\_NUMBER&text=E\_MESSAGE

Query String in Body	Definition
user=tedmosby	Replace “tedmosby” with the user name created at the Clickatell website.
password=himym	Replace “himym” with the password created at the Clickatell website.
api_id=2014331	Replace “2014331” with the API ID acquired at the Clickatell website.
to=E_PHONE_NUMBER	Do not replace this information. It refers to the receiver phone number entered in <a href="#">System Tab &gt; Notification &gt; SMS Recipients</a> .
text=E_MESSAGE	Do not replace this information. It refers to the event action sent by SMS service provider. For configurations, see <a href="#">System Tab &gt; Notification &gt; Event Action</a> .

System > Notification > SMS Service



Using Mail:

Users set the SMTP server in [System Tab > Notification > SMTP Server](#) first, and then enter the following information.

Item	Definition
Address	Enter the e-mail of the recipient.
Subject	The Subject field shown in the e-mail message, entered by user.
Content	
E_ MESSAGE	Do not replace this information. It refers to the event action sent by SMS service provider. For configurations, see <a href="#">System Tab &gt; Notification &gt; Event Action</a> .
E_PHONE_NUMBER	Do not replace this information. It refers to the receiver phone number entered in <a href="#">System Tab &gt; Notification &gt; SMS Recipients</a> .

Users can set up to 10 mobile phone numbers as SMS recipients who will receive a short message notification when a specific event occurs. See [System Tab > Notification > SMS Recipients](#).

### System Tab > Notification > SMS Recipients

Item	Definition
Recipient Name	Click the name of the recipient to open the <a href="#">Configure SMS Receiver Page</a> . Users can modify or delete an existing receiver.
TEST	Click this button to check whether the test message is correctly sent.
New Recipient	Click this button to open the <a href="#">Add New SMS Receiver Page</a> . Users can add a new recipient.

### Configure SMS Receiver Page

**PDU Remote Management** Administrator login from 192.168.25.28 [\[Logout\]](#)

Summary | PDU | Envir | Log | **System** | Help

- General
- Security
- Network Service
- Notification**
  - Event Action
  - SMTP Server
  - E-mail Recipients
  - Trap Receivers
  - SMS Service
  - SMS Recipients
- Reset/Reboot
- About

#### Configure SMS Recipient

Active  Enabled

Recipient Name

Mobile Number

### Add New SMS Receiver Page

**PDU Remote Management** Administrator login from 192.168.25.28 [\[Logout\]](#)

Summary | PDU | Envir | Log | **System** | Help

- General
- Security
- Network Service
- Notification**
  - Event Action
  - SMTP Server
  - E-mail Recipients
  - Trap Receivers
  - SMS Service
  - SMS Recipients
- Reset/Reboot
- About

#### Add New SMS Recipient

Active  Enabled

Recipient Name

Mobile Number

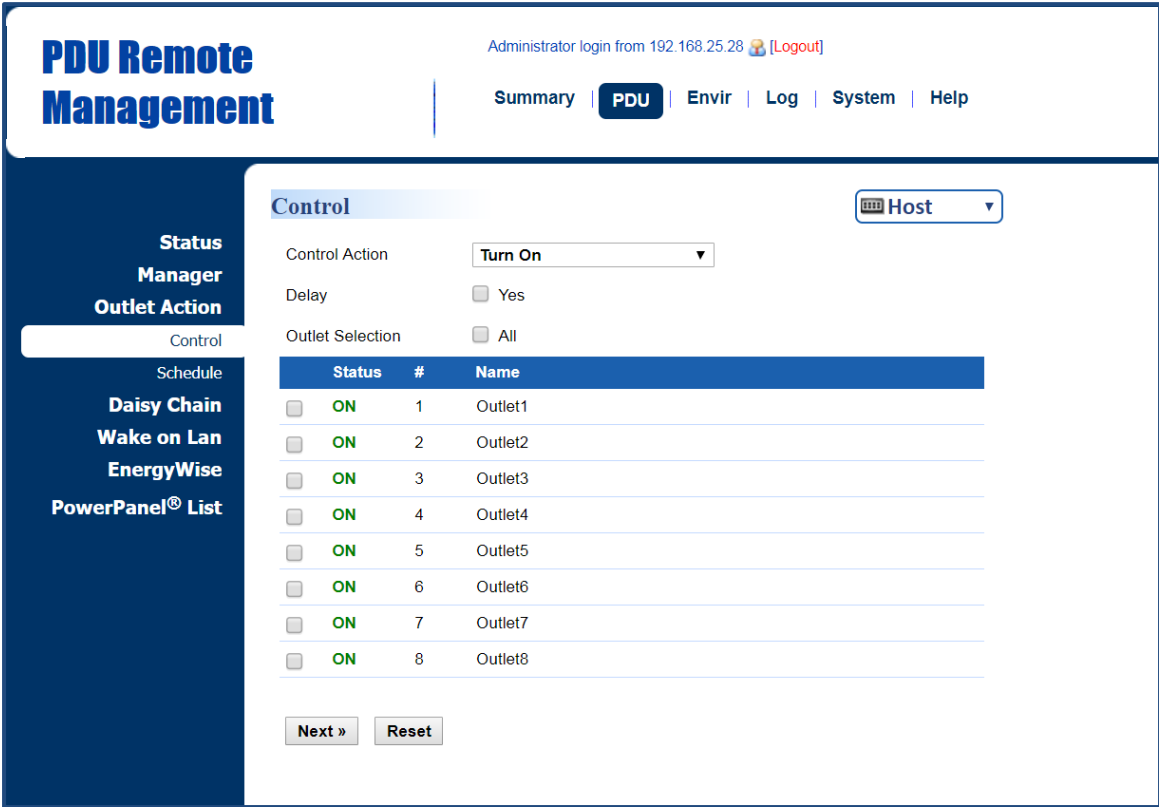
# Outlet Management

The following provides the outlet configurations to meet different application scenarios.

## Remote Outlet On/Off/Reboot

Users can turn on, turn off, or reboot individual outlet. See [PDU Tab > Outlet Action > Control](#). (For Switched Metered by Outlet Series and Switched Series only.)

### PDU Tab > Outlet Action > Control



Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
<b>Control Action</b>	
Turn On	Selected outlets will be immediately turned on.
Turn On + Delay	Selected outlets will be turned on according to each outlet's <i>Power On Delay</i> in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a> .
Turn Off	Selected outlets will be immediately turned off.

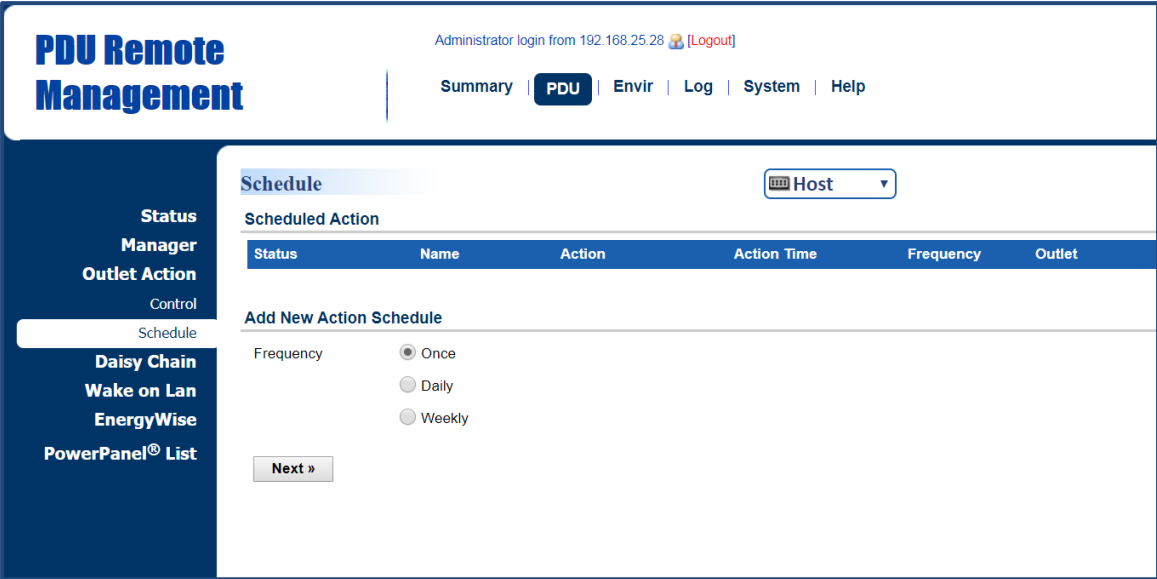


Item	Definition
Turn Off + Delay	<p>Selected outlets will be turned off according to each outlet's <i>Power Off Delay</i> in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a>.</p> <p>This action could signal a computer to shut down, if PowerPanel® Business Edition Client software is installed on it.</p>
Reboot	<p>Selected outlets will be immediately turned off and then be turned on again according to each outlet's <i>Reboot Duration</i> in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a>.</p>
Reboot + Delay	<p>Selected outlets will be turned off according to each outlet's <i>Power Off Delay</i>. They will be synchronized with the longest <i>Power Off Delay</i> and the longest <i>Reboot Duration</i> of the selected outlets. Then they will be turned on according to each outlet's <i>Power On Delay</i> in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a>.</p>
Cancel Pending Command	<p>Any pending commands of the selected outlet(s) will be cancelled. Any outlet in a pending command state will be notated with an asterisk (*).</p>
Outlet Selection	<p>Outlets selected for action.</p>

### Scheduled Outlet On/Off/Reboot

Outlet(s) can be set to automatically turn on, turn off, or reboot at scheduled times. See [PDU Tab > Outlet Action > Schedule](#). (For Switched Metered by Outlet Series and Switched Series only.)

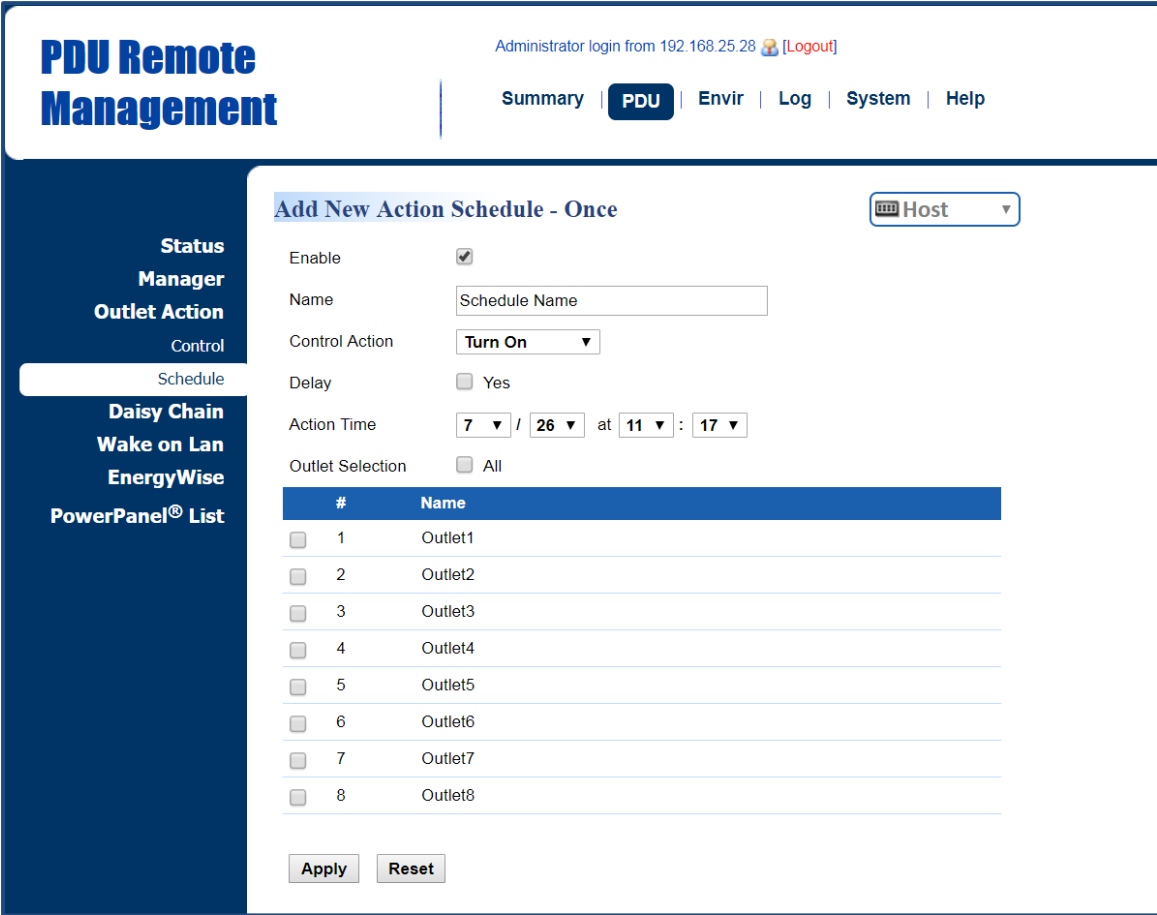
#### PDU Tab > Outlet Action > Schedule



Select the role of PDU (HOST or GUEST#) first if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU. Select the **Once**, **Daily** or **Weekly** option, and then click the **Next** button to enter the [Add New Action Schedule Page](#).

Item	Definition
<b>Frequency</b>	
Once	Scheduled action takes place once at the configured date and time.
Daily	Scheduled action takes place daily at the configured time.
Weekly	Scheduled action takes place once a week for the configured day and time.

### Add New Action Schedule Page



Up to 10 scheduled settings are allowed.

Item	Definition
Enable	Check this box to activate the scheduled action function.
Name	The name entered by the user to identify the specific scheduled event.
Control Action	The action will be performed when the scheduled event takes place. For reboot action, selected outlets will be immediately turned off and then be turned on again according to outlet's <i>Reboot Duration</i> in <a href="#">PDU Tab &gt; Manager &gt; Outlet</a> . The duration is within 5 to 60 seconds.
Delay	Click this box to activate outlet delay function. For configurations, see <a href="#">PDU Tab &gt; Manager &gt; Outlet</a>
Action Time	The time at which the scheduled event takes place.
Outlet Selection	Outlets selected for the scheduled event.

### Sequencing Power On/Off

Enable users to turn on, turn off, or reboot the outlets in sequence. When powering on the connected devices, the sequential power-on method is recommended to avoid high inrush current. See [PDU Tab > Manager > Outlet](#). (For Switched Metered by Outlet Series and Switched Series only.)

### PDU Tab > Manager > Outlet

The screenshot shows the 'Outlet Manager' configuration page in the PDU Remote Management web interface. The page title is 'Outlet Manager' and it includes a dropdown menu set to 'Host'. Below the title is an 'Outlet Selection' section with an 'All' checkbox. The main content is a table with the following columns: #, Outlet Name, On Delay, Off Delay, Reboot Duration, Overload Threshold, Near Overload Threshold, and Low Load Threshold. The table lists 8 outlets, each with a checkbox in the first column. A 'Next »' button is located at the bottom left of the table area.

#	Outlet Name	On Delay	Off Delay	Reboot Duration	Overload Threshold	Near Overload Threshold	Low Load Threshold
<input type="checkbox"/> 1	Outlet1	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 2	Outlet2	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 3	Outlet3	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 4	Outlet4	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 5	Outlet5	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 6	Outlet6	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 7	Outlet7	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)
<input type="checkbox"/> 8	Outlet8	3 sec.	3 sec.	5 sec.	1440 (W)	1080 (W)	0 (W)

Select the role of PDU (HOST or GUEST#) first if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU. Click the box to select one outlet or multiple outlets for power sequencing and then click Next to open the [Outlet Configuration Page](#) for configuration.

## Outlet Configuration Page

PDU Remote Management

Administrator login from 192.168.25.28 [Logout](#)

Summary | PDU | Envir | Log | System | Help

Status Manager

Device

Outlet

Outlet Action

Daisy Chain

Wake on Lan

EnergyWise

PowerPanel® List

Configuration
Host

Name

**Action Configuration**

Power On Delay  Instant  
 Delay  Sec(s) [1-7200]  
 Never

Power Off Delay  Instant  
 Delay  Sec(s) [1-7200]  
 Never

Reboot Duration  Sec(s) [5-60]

**Load Configuration**

Overload Threshold  W

Near Overload Threshold  W

Low Load Threshold  W

**Power Restore**

Peak Load  Reset

Energy  Reset

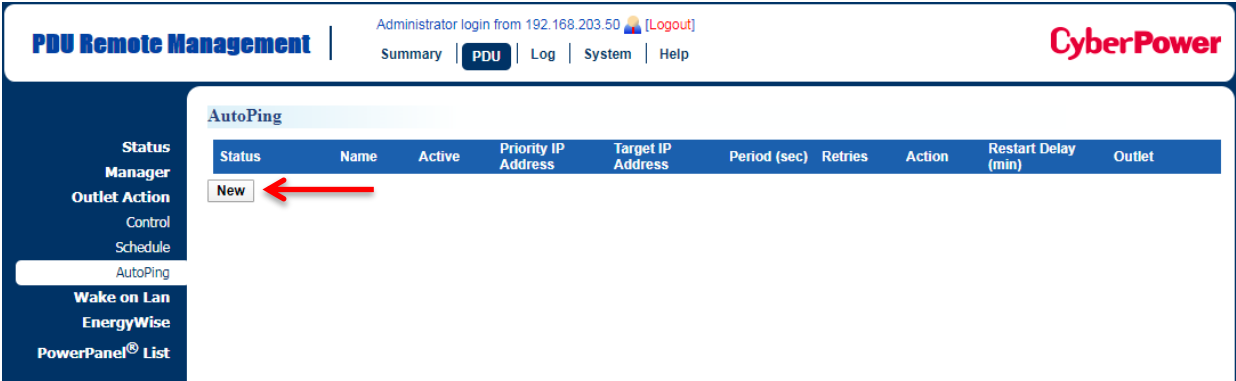
Item	Definition
Name	The name entered by the user to identify the selected outlet or multiple outlet configuration.
<b>Action Configuration</b>	
Power On/Off Delay	<p><b>*Instant:</b> Turn on/off the outlet immediately.</p> <p><b>*Delay:</b> Delay time before turning on/off the outlet. Valid values are within the range of 1 to 7,200 seconds.</p> <p><b>*Never:</b> Never turn on/off the outlet.</p>
Reboot Duration	The length of time the outlet will remain off during a Reboot action. Valid values are within the range of 5 to 60 seconds.
<b>Load Configuration</b>	
Overload Threshold	Set the value for individual outlet that will signal an overload warning in Watts. Must be higher than <i>Near Overload Threshold</i> .
Near Overload Threshold	Set the value for individual outlet that will signal a near overload warning in Watts. Must be between <i>Overload Threshold</i> and <i>Low Load Threshold</i> .

Item	Definition
Low Overload Threshold	Set the value for individual outlet that will signal a low overload warning in Watts. Must be lower than <i>Near Overload Threshold</i> .
<b>Power Restore</b>	
Peak Load	Restore the peak load of each outlet to zero.
Energy	Restore the energy of each outlet to zero.

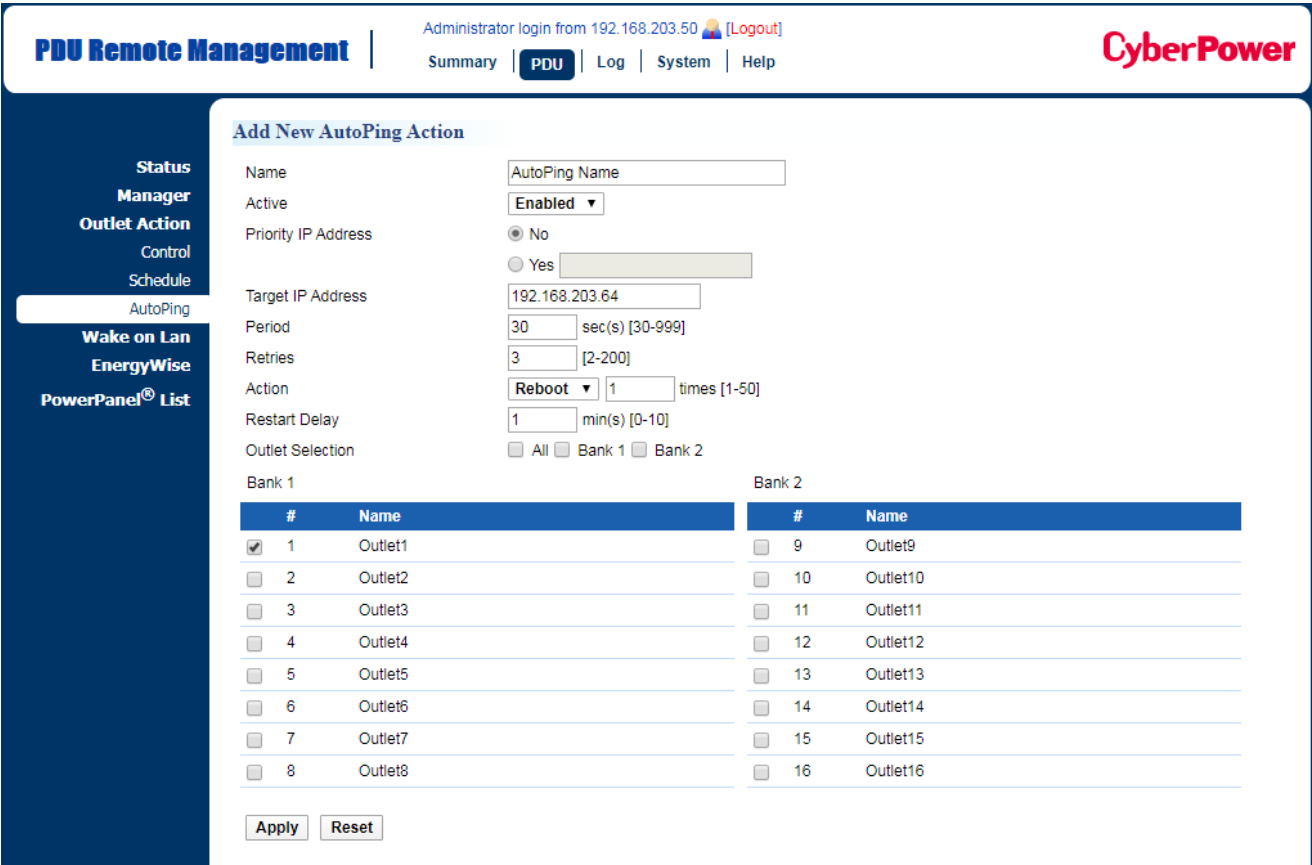
### AutoPing

The AutoPing feature allows the PDU to detect if a target device becomes unresponsive to IP pings and automatically reboot the device. If the device gets back to normal operation after reboot, network connection could be restored at the same time.

To utilize the function, See **PDU Tab > Outlet Action > AutoPing**. (For Switched Metered by Outlet Series and Switched Series only.)



AutoPing configuration is shown as below. For example, the AutoPing function is enabled on Outlet 1 with 192.168.203.64 as “Target IP address”. The PDU sends IP pings to the target device every 30 seconds. Outlet1 reboots once only if ping tests fail 3 times in a row, which takes 90 seconds for the PDU to detect the failure and trigger the action. After Outlet1 reboots, no pings are sent to the target device until 1 minute of “Restart Delay” is reached.

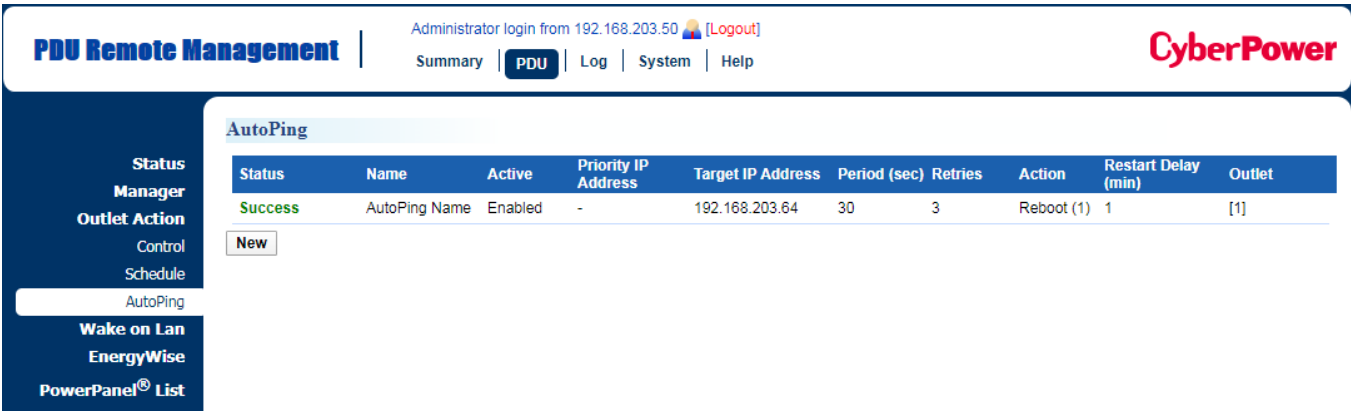


Up to 10 AutoPing settings are allowed.

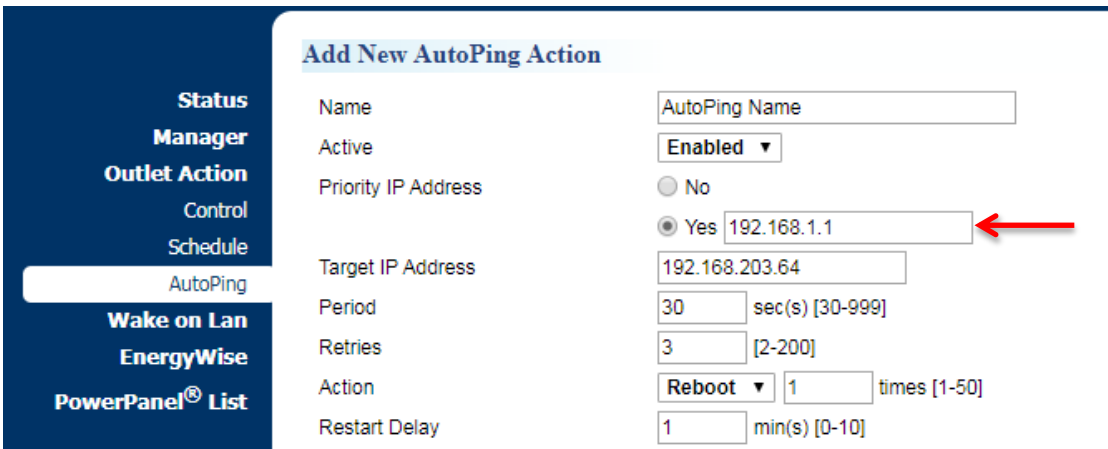
Item	Definition
Active	Enable/Disable the AutoPing function.
Priority IP Address	When “Yes” is selected, sets the IP address of the priority to utilize the function. Pings will only be sent to the target device when receiving a successful ping response from the priority. For example, the target device is connected to a router, which is set to be the priority. The PDU sends IP pings to the target device only if the router is responsive to IP pings. In this way, the PDU can verify network connection by sending IP pings to the priority first and determine if target IP ping test is performed accordingly.
Target IP Address	The IP address of the target device.
Period	The time interval between successive pings to the target device, in second.
Retries	The number of failed ping tests that must be consecutively detected before the action is triggered.
Action	The action on specific outlet if the PDU continuously receives no response from the target device. When “Reboot” is selected, sets the maximum number of times to be triggered.
Restart Delay	Length of time after an action is triggered before beginning to restart ping tests. This allows a proper time for the device to get back to normal operation. During this time interval, no pings are sent to the target device.



After confirming the AutoPing configuration and pressing “Apply” button, find your preferred configuration and AutoPing status on AutoPing Webpage.



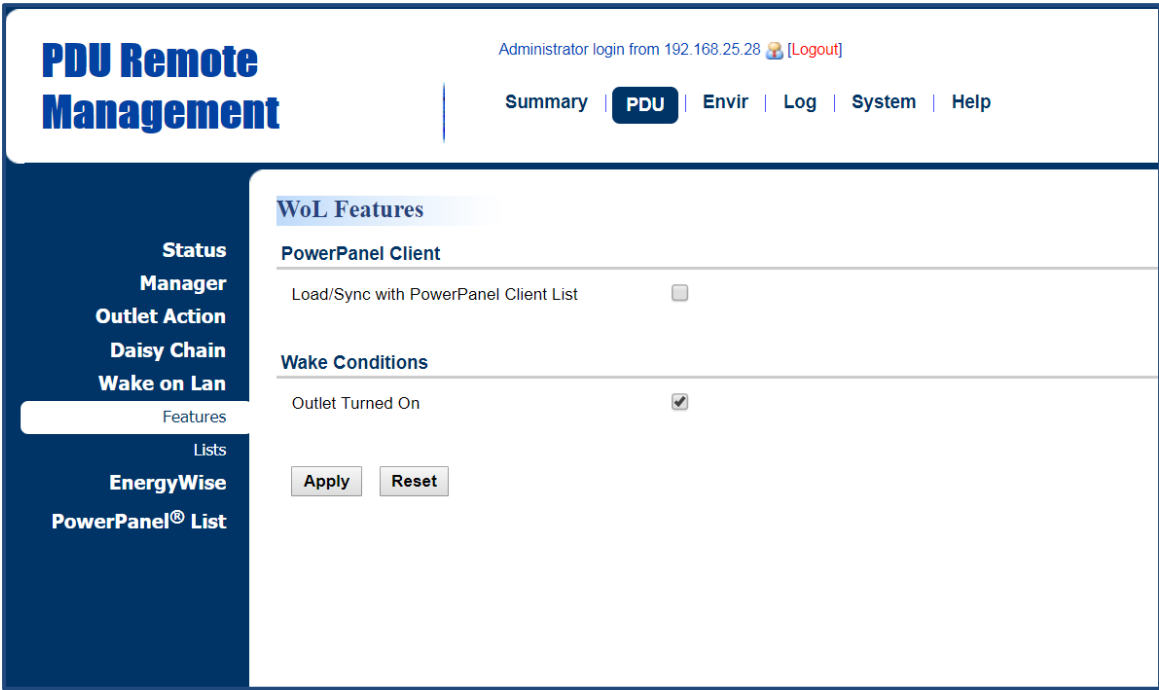
Besides, set the IP address of the priority when “Yes” is selected. For example, the target device is connected to a router, which is set to be the priority. The PDU sends IP pings to the target device only if the router is responsive to IP pings. In this way, the PDU can verify network connection by sending IP pings to the priority first and determine if target IP ping test is performed accordingly.



**Wake on LAN (WoL)**

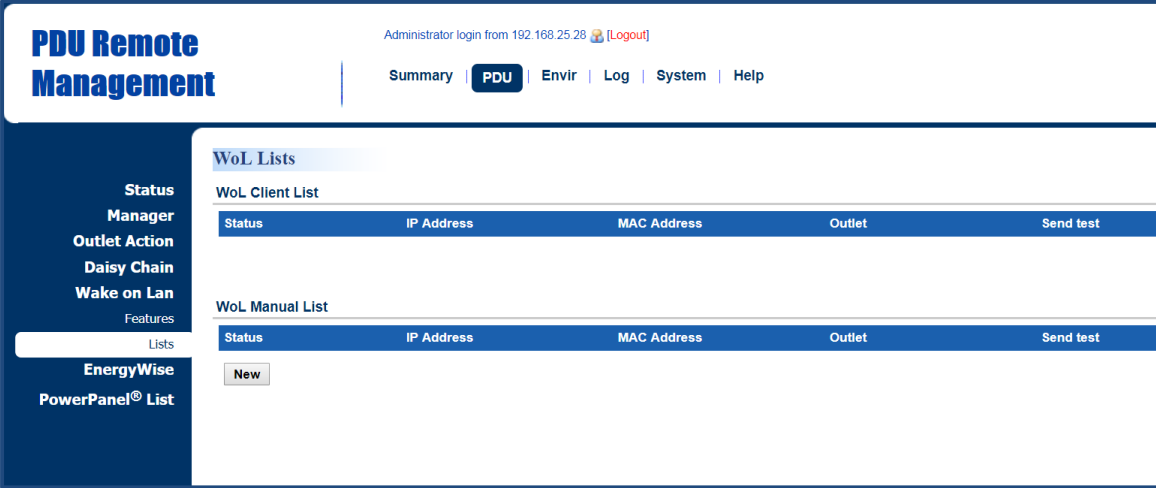
When turning on an outlet, a Wake on LAN packet can be sent to the connected computer to awaken it. It is necessary for the computer to support this function and is configured as "Enabled" in its BIOS settings. See [PDU Tab > Wake on LAN > Features](#) and [PDU Tab > Wake on LAN > Lists](#). (For Switched Metered by Outlet Series and Switched Series only.)

**PDU Tab > Wake on LAN > Features**



Item	Definition
PowerPanel Client	Load/Sync with PowerPanel Client List. To achieve synchronization, make sure the PDU has established communication with PowerPanel® Business Edition Client software. See <a href="#">System Tab &gt; Security &gt; Authentication</a> .
Wake Conditions	Enable or disable the Wake on LAN function.

PDU Tab > Wake on LAN > Lists



Item	Definition
WoL Client List	If the PowerPanel Client option in <a href="#">PDU Tab &gt; Wake on LAN &gt; Features</a> is selected, the PowerPanel® List will be automatically added to the WoL Client list.
WoL Manual List	Click New to enter the <a href="#">Add Wake on LAN Receiver Page</a> . Users can manually add WoL receivers.

### Add Wake on LAN Receiver Window

The screenshot shows the 'Add Wake on Lan Receiver' configuration window in the PDU Remote Management web interface. The top navigation bar includes the logo and user information: 'Administrator login from 192.168.25.28 [Logout]'. The main navigation menu on the left lists 'Status Manager', 'Outlet Action', 'Daisy Chain', 'Wake on Lan', 'Features', 'Lists', 'EnergyWise', and 'PowerPanel® List'. The configuration area contains the following elements:

- Active:** A checkbox labeled 'Enabled' which is checked.
- IP Address:** A text input field containing '0.0.0.0'.
- Outlet:** A table with 8 rows, each representing an outlet. The first row is selected with a radio button.

#	Name
<input checked="" type="radio"/>	1 Outlet1
<input type="radio"/>	2 Outlet2
<input type="radio"/>	3 Outlet3
<input type="radio"/>	4 Outlet4
<input type="radio"/>	5 Outlet5
<input type="radio"/>	6 Outlet6
<input type="radio"/>	7 Outlet7
<input type="radio"/>	8 Outlet8

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

Item	Definition
Active	Enable/Disable the Wake on LAN function.
IP Address	The IP address of the computer. This IP must be within the same subnet as the PDU. Up to 50 IP addresses are supported.
Outlet	Select the outlet that provides power to the computer.

### Graceful Computer Shutdown

After the connected computer is installed with PowerPanel Business Edition Client or Center and establishes communication with the PDU, its IP address will be automatically displayed in the PowerPanel® List shown below. This computer can perform a safe shutdown before the outlet powering the computer turns off, thus avoiding data loss. To achieve communication between the computer and PDU, see [System > General > Security](#).

Up to 50 computers having PPBE Client or Center installed can be listed. A Client or Center computer will be removed when it has been disconnected from the PDU for an hour. See [PDU Tab > PowerPanel® List](#). (For Switched Metered by Outlet Series and Switched Series only.)

#### PDU Tab > PowerPanel® List

The screenshot shows the 'PDU Remote Management' web interface. At the top right, it indicates 'Administrator login from 192.168.25.28 [Logout]'. Below this is a navigation menu with 'Summary', 'PDU' (selected), 'Envir', 'Log', 'System', and 'Help'. On the left side, there is a sidebar menu with options: 'Status Manager', 'Outlet Action', 'Daisy Chain', 'Wake on Lan', 'EnergyWise', and 'PowerPanel® List' (highlighted). The main content area displays the 'PowerPanel® List' table with the following data:

IP Address	Type	Outlet	Name	Location	Contact
192.168.26.107	Client	1	Lab03	Lab03	admin

Click the IP address of a client to access configuration settings.

## Cisco EnergyWise

Users can manage and control all Cisco EnergyWise entities and configure settings. See [PDU Tab > EnergyWise > Configuration](#) and [PDU Tab > EnergyWise > Children List](#).

### PDU Tab > EnergyWise > Configuration

The screenshot shows the 'PDU Remote Management' web interface. At the top right, it indicates 'Administrator login from 192.168.25.28' with a [Logout] link. Below this is a navigation bar with 'Summary', 'PDU' (selected), 'Envir', 'Log', 'System', and 'Help'. The left sidebar contains a menu with 'Status Manager', 'Outlet Action', 'Daisy Chain', 'Wake on Lan', 'EnergyWise', 'Configuration' (highlighted), 'Children List', and 'PowerPanel® List'. The main content area is titled 'EnergyWise Configuration' and contains the following fields:

- Version: 1.2.0
- EnergyWise:  Enable
- Service port: 43440
- Domain Name:
- Off-State Cache:
- Secure Mode:
- Shared Secret:

At the bottom of the form are 'Apply' and 'Reset' buttons.

Item	Definition
Version	The version of EnergyWise supported.
EnergyWise	Enable/Disable EnergyWise support.
Service Port	The port number is used to communicate with EnergyWise. This number must be the same as that of a Cisco switch that the PDU connects to.
Domain Name	The EnergyWise domain name. This must be the same as that of a Cisco switch that the PDU connects to.
Off-State Cache	Enable/Disable endpoint to cache EnergyWise list in the Cisco switch after the PDU has rebooted.
Secure Mode	Enable EnergyWise use of a shared secret.
Shared Secret	The secret for the EnergyWise domain.

### PDU Tab > EnergyWise > Children List

**PDU Remote Management**

Administrator login from 192.168.25.28 [Logout]

Summary **PDU** | Envir | Log | System | Help

#### EnergyWise Children List

**Parent**

#	Name	Role	Keywords	importance
1	PDU_Base	base,role	endpoint,child,base	1

**Children**

#	Name	Role	Keywords	importance
1	Outlet1	outlet,role	endpoint,child,outlet	1
2	Outlet2	outlet,role	endpoint,child,outlet	1
3	Outlet3	outlet,role	endpoint,child,outlet	1
4	Outlet4	outlet,role	endpoint,child,outlet	1
5	Outlet5	outlet,role	endpoint,child,outlet	1
6	Outlet6	outlet,role	endpoint,child,outlet	1
7	Outlet7	outlet,role	endpoint,child,outlet	1
8	Outlet8	outlet,role	endpoint,child,outlet	1
9	Bank1	bank,role	endpoint,child,bank	1

Click the Name field in parent and/or children list to enter the [EnergyWise Parent Configuration Page](#) and [EnergyWise Child Configuration Page](#).

### EnergyWise Parent Configuration Page

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | **PDU** | Envir | Log | System | Help

**EnergyWise Parent Configuration**

Name:

Role:

Keywords:

importance:

**Status Manager**  
**Outlet Action**  
**Daisy Chain**  
**Wake on Lan**  
**EnergyWise**  
 Configuration  
 Children List  
**PowerPanel® List**

### EnergyWise Child Configuration Page

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | **PDU** | Envir | Log | System | Help

**EnergyWise Child Configuration**

Name:

Role:

Keywords:

importance:

**Status Manager**  
**Outlet Action**  
**Daisy Chain**  
**Wake on Lan**  
**EnergyWise**  
 Configuration  
 Children List  
**PowerPanel® List**

Item	Definition
Name	The name entered by the user to identify an EnergyWise entity. The maximum length is 31 characters.
Role	This parameter is a string entered by the user to describe the function of



Item	Definition
	the entity. Maximum length is 31 characters.
Keywords	This parameter is a string entered by the user to describe the entity. Maximum length is 31 characters.
Importance	This parameter, entered by the user, shows the value of an entity's importance and must be between 1 and 100.

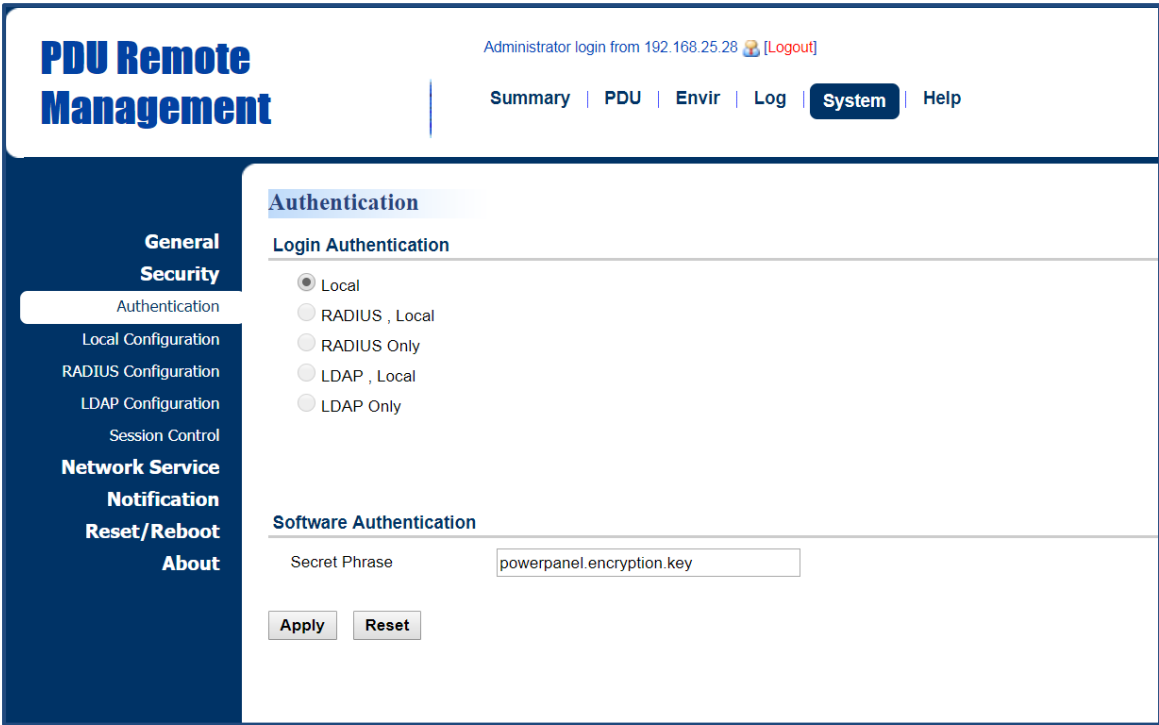
# Security

The following provides account configurations to protect against unauthorized entry.

## Login Authentication

There are five options for login authentication. Only one user can log in to the web interface at a time.

### System Tab > Security > Authentication

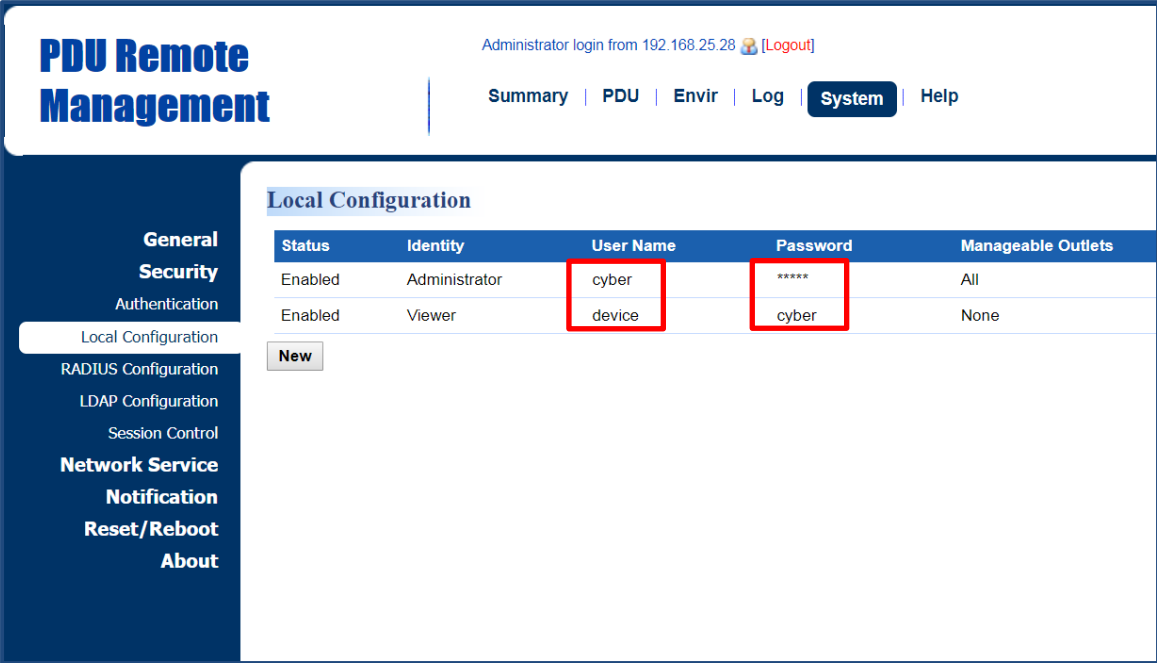


Item	Definition
<b>Login Authentication</b>	
Local	Log in with user name and password configured in Local Account. See <a href="#">System Tab &gt; Security &gt; Local Configuration</a> .
RADIUS, Local	Log in with user name and password to authenticate with RADIUS server first. If the RADIUS server fails to respond, then the user name and password configured in Local Configuration can be used. See <a href="#">System Tab &gt; Security &gt; RADIUS Configuration</a> .

Item	Definition
RADIUS Only	Log in with user name and password to authenticate with RADIUS server only. See <a href="#">System Tab &gt; Security &gt; RADIUS Configuration</a> .
LDAP, Local	Log in with user name and password to authenticate with LDAP server first. If the LDAP server fails to respond, then the user name and password configured in Local Configuration can be used. See <a href="#">System Tab &gt; Security &gt; LDAP configuration</a> .
LDAP Only	Log in with user name and password to authenticate with LDAP server only. See <a href="#">System Tab &gt; Security &gt; LDAP configuration</a> .
<b>Software Authentication</b>	
Secret Phrase	The authentication phrase is used to communicate with PowerPanel® Business Edition software. This phrase should be the same <b>Secret Phrase</b> as the field on PowerPanel® Business Edition software interface.

1. Using Local Configuration for Authentication

System Tab > Security > Local Configuration



There are two types of account: administrator and viewer. Click User Name or Password field to enter Administrator Page or Viewer Page. Users can also click NEW to enter Add Outlet User Page to create an outlet account.

### Administrator Page

# PDU Remote Management

Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

- General
- Security**
- Authentication
- Local Configuration
- RADIUS Configuration
- LDAP Configuration
- Session Control
- Network Service
- Notification
- Reset/Reboot
- About

## Administrator

User Name	<input type="text" value="cyber"/>
Current Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
Admin Manager IP	
<input checked="" type="checkbox"/> Enabled	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> Enabled	<input type="text" value="0.0.0.0"/>

### Viewer Page

# PDU Remote Management

Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

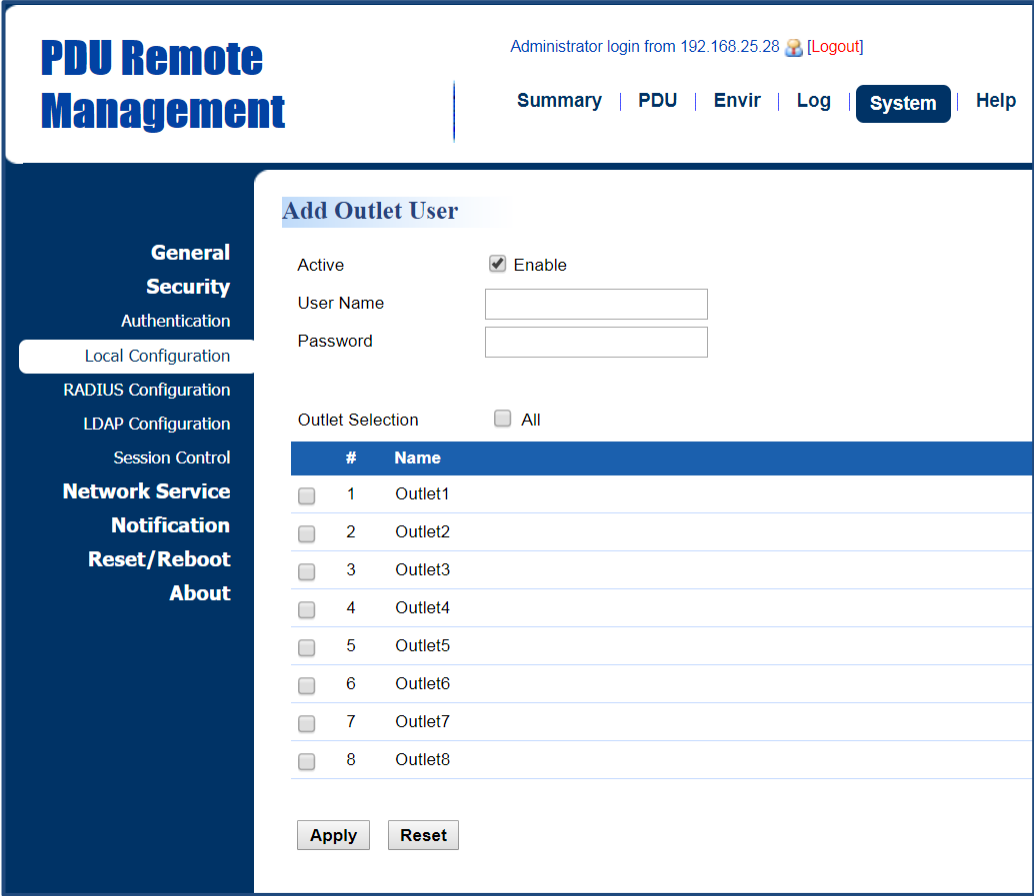
- General
- Security**
- Authentication
- Local Configuration
- RADIUS Configuration
- LDAP Configuration
- Session Control
- Network Service
- Notification
- Reset/Reboot
- About

## Viewer

Allow Access	<input checked="" type="checkbox"/> Enabled
User Name	<input type="text" value="device"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
Viewer Manager IP	
<input checked="" type="checkbox"/> Enabled	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/> Enabled	<input type="text" value="0.0.0.0"/>

Item	Definition
<b>Administrator</b>	The administrator can access all functions, including Enable/Disable the Viewer account. For login configuration, users can only create one administrator account.
User Name	Enter the new user name.
Current Password	Enter the current password for authentication.
New Password	Enter the new password.
Confirm Password	Enter the new password again to confirm it.
Admin Manager IP (optional)	Set the Admin IP which is allowed to access. If you want access from any IP address, you can set one of them as 0.0.0.0 or 255.255.255.255. <b>Note:</b> You can also set a range of IP addresses to access, for example, 192.168.16.1/24.
<b>Viewer</b>	The viewer can view the settings but cannot control or change any settings.
Allow Access	Check this box to enable view account.
Viewer Manager IP(optional)	Set the Viewer IP which is allowed to access. If you want access from any IP address, you can set one of them as 0.0.0.0 or 255.255.255.255. <b>Note:</b> You can also set a range of IP addresses to access, for example, 192.168.16.1/24.

### Add Outlet User Page\*

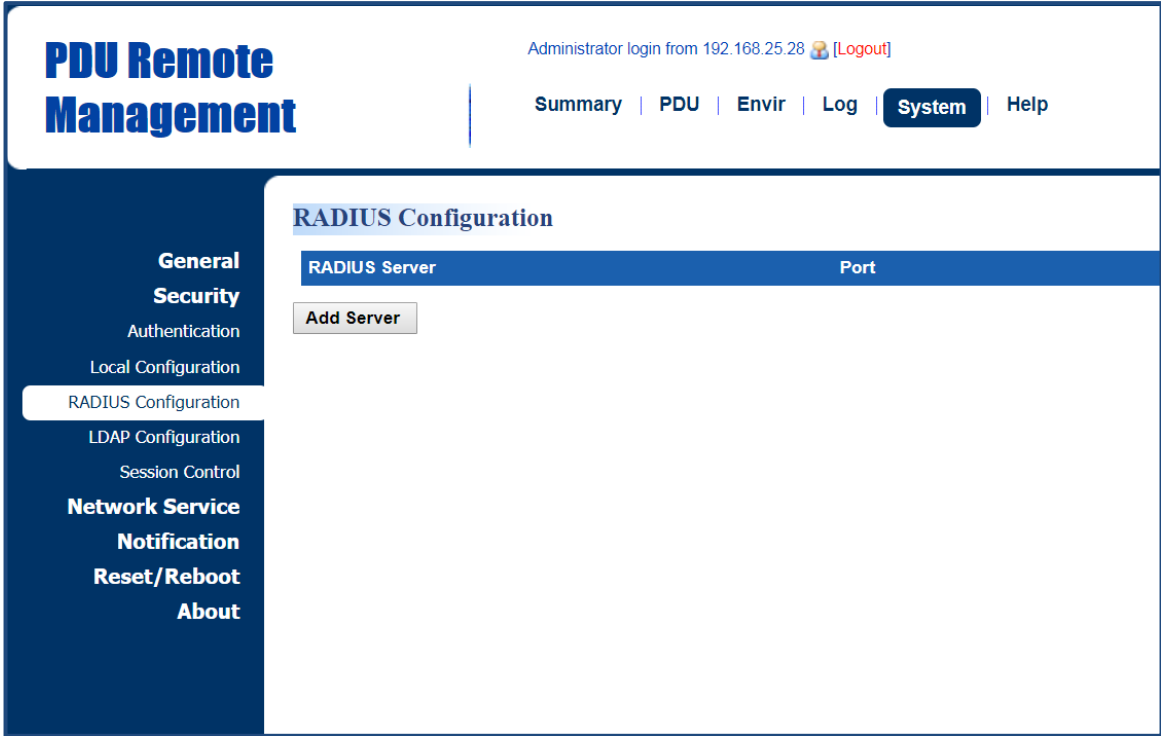


\*The above **Add Outlet User Page** is available for Switched Metered by Outlet Series and Switched Series only.  
 Users can create an outlet account that is allowed to control assigned outlet(s).

Item	Definition
Active	Enable or disable the user account.
User Name	Set a name for the user account.
Password	Set the user password.
Outlets Selection	Outlets that the user can control.

2. Using RADIUS Configuration for Authentication

System Tab > Security > RADIUS Configuration



Click Add Server to enter Radius Server Configuration Page to create a server.



### Radius Server Configuration Page

**PDU Remote Management**

Administrator login from 192.168.25.28 [Logout](#)

Summary | PDU | Envir | Log | **System** | Help

**General**  
**Security**  
Authentication  
Local Configuration  
**RADIUS Configuration**  
LDAP Configuration  
Session Control  
**Network Service**  
**Notification**  
Reset/Reboot  
About

#### RADIUS Server Configuration

Server IP:

Shared Secret:

Server Port:  [default:1812]

Test Setting

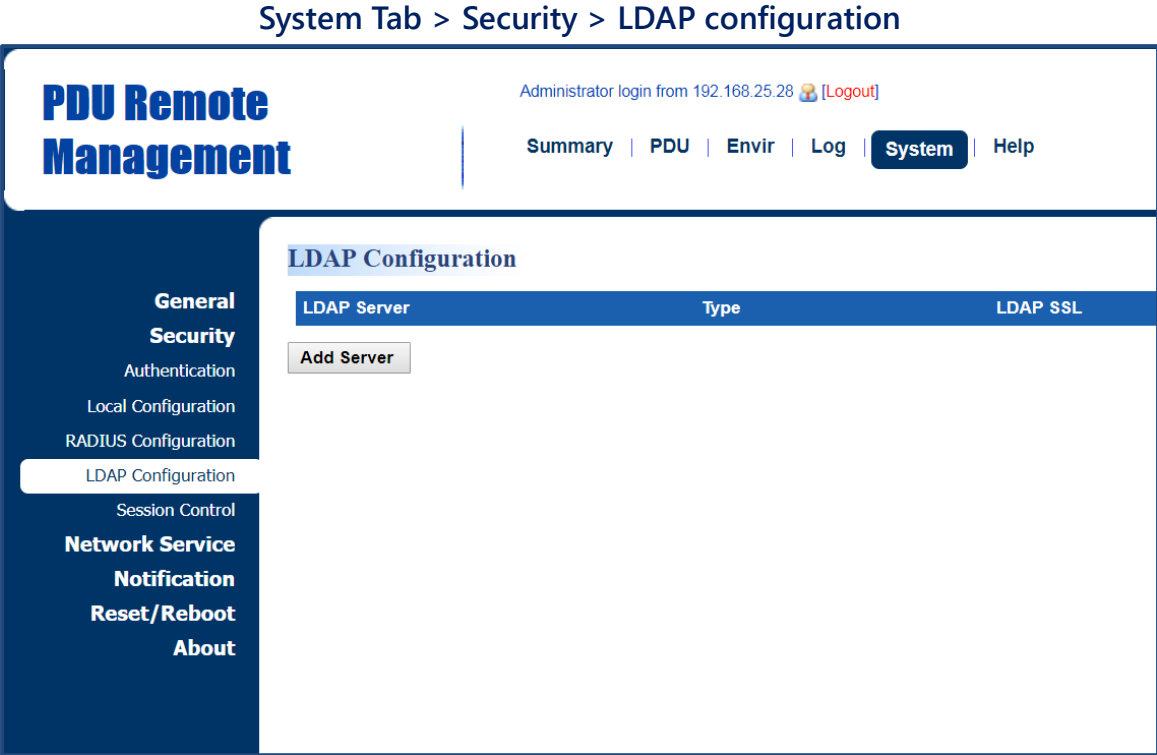
User Name:

Password:

Skip Test

Item	Definition
Server IP	The IP address of RADIUS server.
Shared Secret	The shared secret of RADIUS server.
Server Port	The UDP port used by the RADIUS server.
Test Setting	Use user name and password to authenticate with RADIUS server, and save information of RADIUS server if authentication succeeds.
Skip Test	Save information of the RADIUS server without test.

3. Using LDAP Configuration for Authentication



Click Add Server to enter LDAP Server Configuration Page to create a server.

### LDAP Server Configuration Page

PDU Remote Management

Administrator login from 192.168.25.28 [Logout]

[Summary](#) | [PDU](#) | [Envir](#) | [Log](#) | [System](#) | [Help](#)

General  
 Security  
   Authentication  
   Local Configuration  
   RADIUS Configuration  
 LDAP Configuration  
   Session Control  
 Network Service  
 Notification  
 Reset/Reboot  
 About

#### LDAP Server Configuration

LDAP Server

LDAP SSL  Enable

Port  [default:389]

Base DN

Login Attribute

Generic LDAP Server  
 Active Directory  
   AD Domain

Test Setting  
   User Name   
   Password

Skip Test

Item	Definition
LDAP Server	The IP address of LDAP server.
LDAP SSL	To communicate with LDAP server by LDAPS.
Port	The TCP port used by the LDAP(S) server.
Base DN	The base DN of LDAP server.
Login Attribute	The login attribute of LDAP user entry. (ex: cn or uid)
Generic LDAP Server	The type of LDAP server.
Active Directory	Select LDAP server type as Windows AD
AD Domain	The AD Domain of the Active Directory server.
Test Setting	Use user name and password to authenticate with LDAP server, and save information of LDAP server if authentication succeeds.
Skip Test	Save information of the RADIUS server without test.

### Timeout Setting

Configure the idle login sessions. See [System > Security > Session Control](#).

[System > Security > Session Control](#)



Item	Definition
<b>Login Session</b>	
Timeout	The time in minutes that the system waits before automatically logging off.

## Network Service

The following provides the network configurations.

### TCP/IPv4 Setting

Display the current TCP/IPv4 settings and allow users to select the option to obtain TCP/IP settings by DHCP. See [System > Network Service > TCP/IPv4](#).

[System > Network Service > TCP/IPv4](#)

**PDU Remote Management** Administrator login from 192.168.25.28 [Logout]

Summary | PDU | Envir | Log | **System** | Help

**General**  
**Security**  
**Network Service**  
TCP/IPv4  
TCP/IPv6  
SNMPv1 Service  
SNMPv3 Service  
Web Service  
Console Service  
FTP Service  
**Notification**  
**Reset/Reboot**  
**About**

**TCP/IPv4**

**Current Configuration**

IP Address	192.168.26.21
Subnet Mask	255.255.255.0
Gateway	192.168.26.254
DNS Server	0.0.0.0

**DHCP**

Enable DHCP

Obtain DNS Address from DHCP

**Manual**

IP Address	<input type="text" value="192.168.26.21"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.26.254"/>
DNS Server	<input type="text" value="0.0.0.0"/>

Item	Definition
<b>Current Configuration</b>	Display the current TCP/IP settings: IP Address, Subnet Mask, Gateway, and DNS server.
<b>DHCP</b>	<p>*<b>Enable DHCP:</b> Select this option to get IP address, Subnet Mask, and Gateway from DHCP.</p> <p>*<b>Obtain DNS Address from DHCP:</b> Select this option to get DNS by DHCP if DHCP is enabled.</p>
<b>Manual</b>	<p>Unselect <b>Enable DHCP</b> first.</p> <p>Enter the TCP/IP settings manually and click <b>Apply</b>.</p>

## TCP/IPv6 Setting

Display the current TCP/IPv6 settings and allow users to assign the IPv6 address either by router control or manually. See [System > Network Service > TCP/IPv6](#).

### System > Network Service > TCP/IPv6

The screenshot shows the PDU Remote Management web interface. At the top right, it indicates 'Administrator login from 192.168.25.28' with a [Logout] link. A navigation bar contains links for Summary, PDU, Envir, Log, System (highlighted), and Help. The left sidebar lists various services under categories: General, Security, Network Service (with TCP/IPv4 and TCP/IPv6 selected), SNMPv1 Service, SNMPv3 Service, Web Service, Console Service, FTP Service, Notification, Reset/Reboot, and About. The main content area is titled 'TCP/IPv6' and contains the following sections:

- IPv6 Interfaces:** A table with columns 'Type' and 'IPv6 Address'.
- IPv6 Gateway:** Displays 'N/A'.
- IPv6 Configuration:** Includes three checkboxes: 'Access' (unchecked), 'Router Control' (unchecked), and 'Manual' (unchecked).
- Manual IPv6 Address:** A text input field labeled 'System IP Address' with a placeholder '::'.

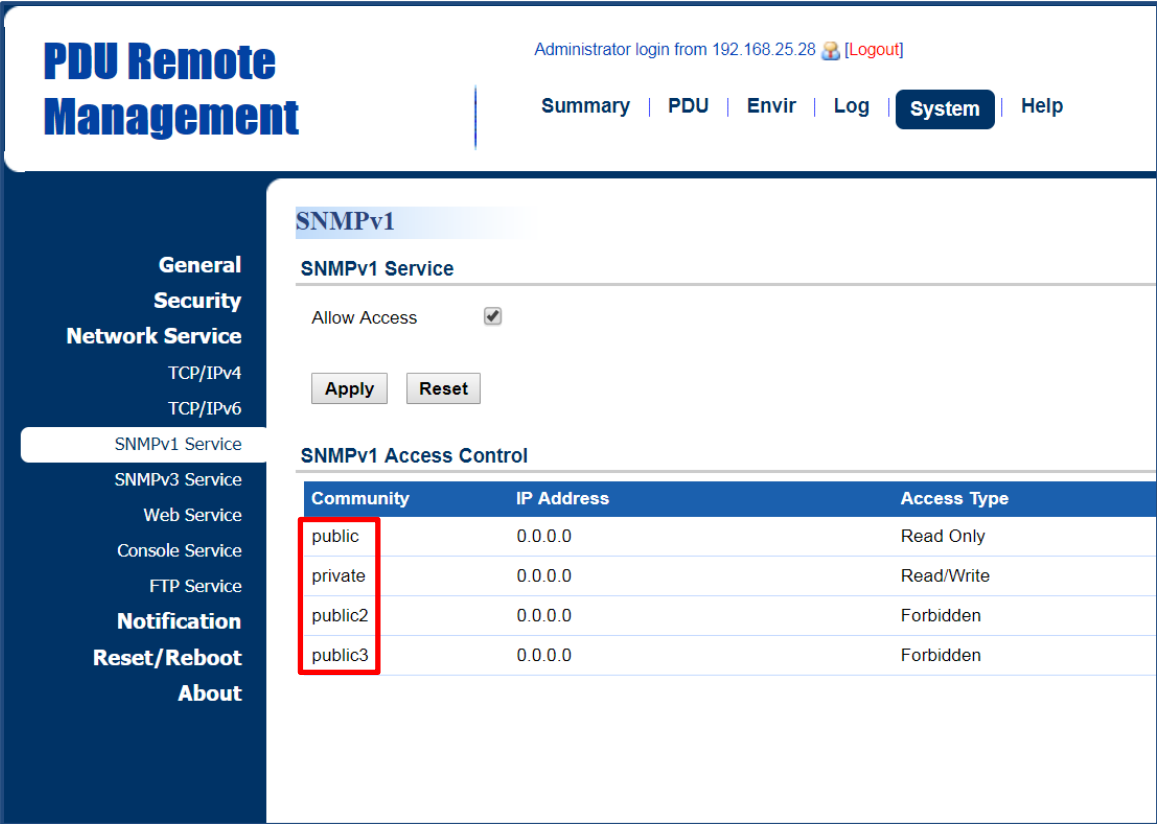
At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

Item	Definition
IPv6 Interface	Displays the current IPv6 address.
IPv6 Gateway	Displays the current IPv6 gateway.
<b>IPv6 Configuration</b>	
Allow Access	Enable/Disable IPv6 service.
Address Mode: Router Control	The IPv6 address is assigned through the method (Stateless Address Auto configuration, Stateless DHCPv6, or Stateful DHCPv6) determined by the router's configuration.
Address Mode: Manual	The IPv6 address is assigned manually.
Manual IPv6 Address	Enter the IPv6 address manually and click <b>Apply</b> when the <b>Address Mode: Manual</b> option is selected.

### SNMPv1 Service Setting

Allow users to perform SNMPv1 configurations. See [System Tab > Network Service > SNMPv1 Service](#).

System Tab > Network Service > SNMPv1 Service



Item	Definition
<b>SNMPv1 Service</b>	
Allow Access	Enable or disable the SNMPv1 service.

Click the **SNMP Trap Community** field to enter the [SNMPv1 Page](#). Users can configure the SNMPv1 settings.

### SNMPv1 Page

The screenshot shows the 'SNMPv1' configuration page in the PDU Remote Management web interface. At the top left is the logo 'PDU Remote Management'. At the top right, it says 'Administrator login from 192.168.25.28 [Logout]'. Below that is a navigation bar with links for 'Summary', 'PDU', 'Envir', 'Log', 'System' (highlighted), and 'Help'. On the left side, there is a dark blue sidebar menu with the following items: 'General', 'Security', 'Network Service' (expanded), 'TCP/IPv4', 'TCP/IPv6', 'SNMPv1 Service' (highlighted), 'SNMPv3 Service', 'Web Service', 'Console Service', 'FTP Service', 'Notification', 'Reset/Reboot', and 'About'. The main content area is titled 'SNMPv1' and contains three input fields: 'Community' with the value 'public', 'IP Address' with the value '0.0.0.0', and 'Access Type' with a dropdown menu set to 'Read Only'. Below these fields are two buttons: 'Apply' and 'Reset'.

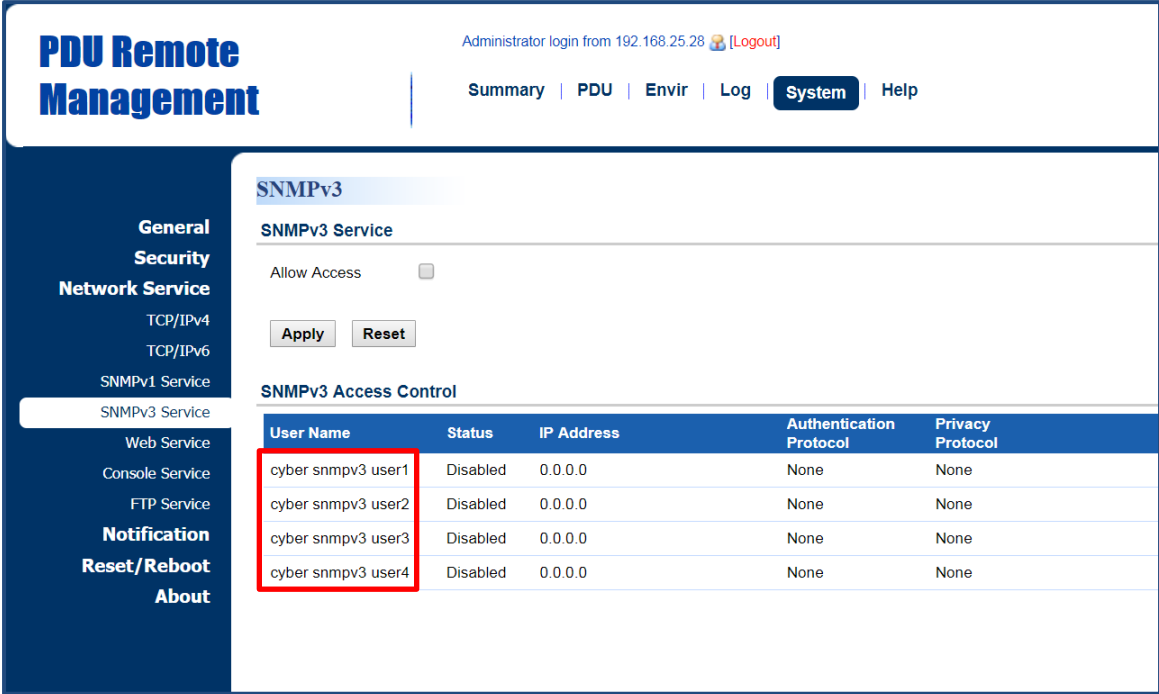
Item	Definition
Community	The name used to access the SNMP community from a Network Management System (NMS). Its maximum length is 15 characters.
IP Address (IPv6 Support)	The IP address or IP address mask can be accessed by the NMS. A specific IP address allows access only by the NMS with the specified IP Address. The “255” is regarded as the subnet mask and the rules are as follows: *192.168.20.255: Access only by an NMS on the 192.168.20.0 segment. *192.255.255.255: Access only by an NMS on the 192.0.0.0 segment. *0.0.0.0 (the default setting) or 255.255.255.255: Access by any NMS on any segments.
Access Type	The allowable action for the NMS through the community and IP address. *Read Only: GET at any time but cannot SET. *Write/Read: GET at any time. SET at any time unless someone logs in to the Web interface. *Forbidden: No GET or SET.



### SNMPv3 Service Setting

Users can perform SNMPv3 configurations. Authentication type or privacy type are provided to strengthen security. See [System Tab > Network Service > SNMPv3 Service](#).

[System Tab > Network Service > SNMPv3 Service](#)



Item	Definition
<b>SNMPv3 Service</b>	
Allow Access	Enable or disable the SNMPv3 service.

Click the **User Name** field to enter the [SNMPv3 Page](#). Users can configure SNMPv3 settings.

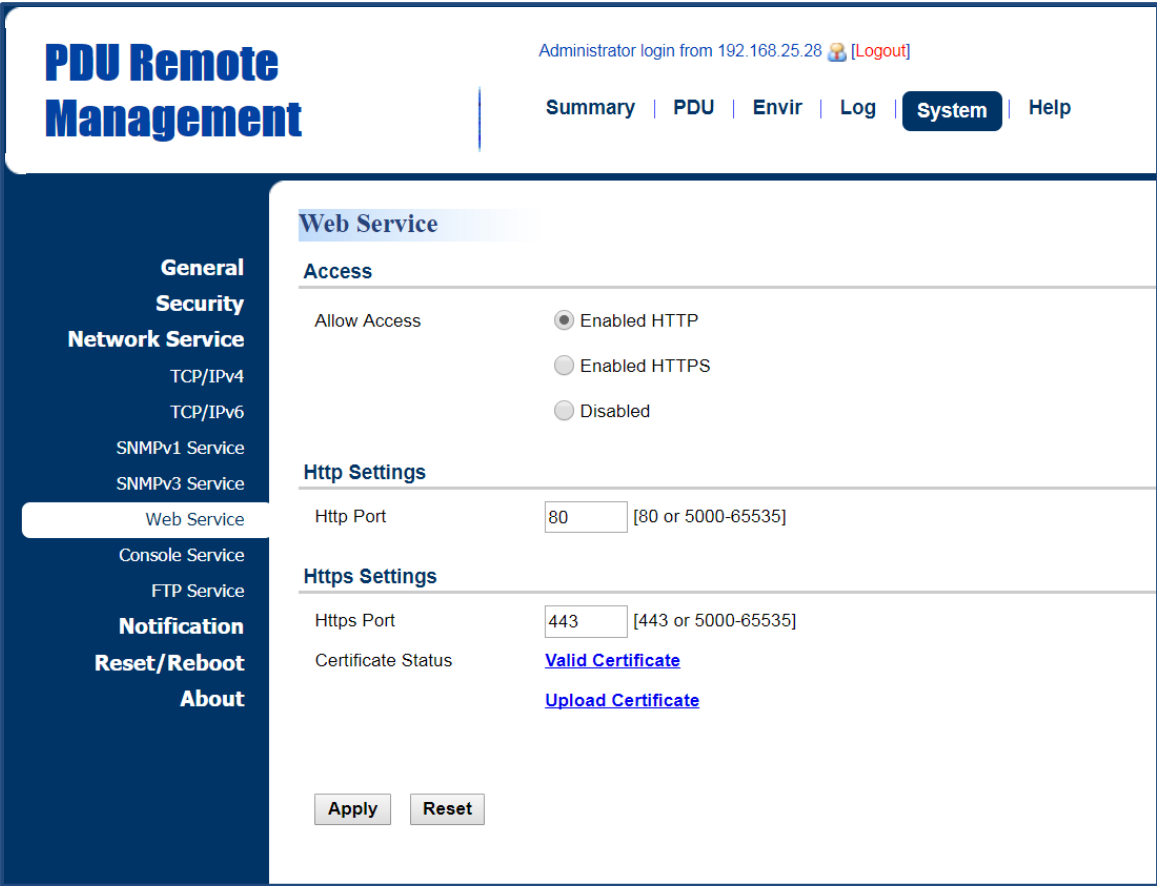
### SNMPv3 Page

Item	Definition
Access	Enable or disable the SNMPv3 service.
User Name	The name that identifies the SNMPv3 user. It must be 1 to 31 characters long.
Authentication Password	The password used to generate the key for authentication. It must be 16 to 31 characters long.
Privacy Password	The password used to generate the key for encryption. It must be 16 to 31 characters long.
IP Address (IPv6 Support)	The IP address or IP address mask that can be accessed by the NMS. A specific IP address allows access only by the NMS with the specified IP Address. The “255” is regarded as the subnet mask and the rules are as follows: *192.168.20.255: Access only by an NMS on the 192.168.20.0 segment. *192.255.255.255: Access only by an NMS on the 192.0.0.0 segment. *0.0.0.0 (the default setting) or 255.255.255.255: Access by any NMS on any segments.
Authentication Key	The hash type for authentication.
Privacy Key	The privacy type for encrypting and decrypting data.

### Web Service

Select the Enable HTTP/HTTPS option to access the HTTP/HTTPS Service and configure HTTP/HTTPS port settings. See [System Tab > Network Service > Web Service](#).

System Tab > Network Service > Web Service



Item	Definition
<b>Access</b>	
Allow Access	Enable or disable HTTP/HTTPS service. HTTPS supports the following encryption algorithms: <ul style="list-style-type: none"> <li>● AES (256/128 bits)</li> <li>● Camellia (256/128 bits)</li> <li>● 3DES (168 bits)</li> <li>● DES (168 bits)</li> <li>● RC4 SHA (128)</li> <li>● RC4 MD5 (128)</li> </ul>
<b>Http Settings</b>	

Item	Definition
HTTP Port	<p>The TCP/IP port of the Hypertext Transfer Protocol (HTTP); 80 is the default value.</p> <p>Users can also change the port setting to any unused port from 5000 to 65535 to enhance security.</p>
<b>Https Settings</b>	
Https Port	<p>The TCP/IP port of the Hypertext Transfer Protocol Secure (HTTPS); 443 is the default value.</p> <p>Users can also change the port setting to any unused port from 5000 to 65535 to enhance security.</p>
Certificate Status	<p><b>*Valid Certificate:</b> Display the detailed certificate information.</p> <p><b>*Upload Certificate:</b> Upload a certificate and replace the current one. The certificate must be uploaded in standard PEM (Privacy Enhanced Mail) format.</p>

Click the Valid Certificate link, and the Installed Certificate Page will appear.

### Installed Certificate Page

The screenshot shows the 'Installed Certificate' page. At the top left is the 'PDU Remote Management' logo. At the top right, it says 'Administrator login from 192.168.25.28 [Logout]'. Below that are navigation links: 'Summary | PDU | Envir | Log | System | Help'. On the left is a dark blue sidebar with menu items: 'General', 'Security', 'Network Service' (with sub-items: 'TCP/IPv4', 'TCP/IPv6', 'SNMPv1 Service', 'SNMPv3 Service', 'Web Service', 'Console Service', 'FTP Service'), 'Notification', 'Reset/Reboot', and 'About'. The main content area is titled 'Installed Certificate' and contains the following information:

Issue to	
Common Name(CN)	Power Distribution Unit
Organization(O)	CyberPower Systems, Inc.
Organization Unit(OU)	PDU
Locality(L)	Unknown
Country	Unknown
Serial Number	11:1C:76:14

Issue by	
Common Name(CN)	Power Distribution Unit
Organization(O)	CyberPower Systems, Inc.
Organization Unit(OU)	PDU

Validity	
Issued from	2013/05/28
Expires on	2023/05/26

Fingerprints	
SHA	44 C0 C5 CF 64 41 A0 A5 98 DF 0A B9 B1 BA 2F 3E FD 2B 84 CF
MD5	DD 84 A4 A3 38 3C BE 3E D9 09 FF 73 6D 53 3E 5C

At the bottom left of the main content area is a '« Back' button.

Click the Upload Certificate link, and the Change Certificate Page will appear.

### Change Certificate Page

The screenshot shows the 'Change Certificate' page. It has the same header and sidebar as the previous page. The main content area is titled 'Upload and Replace' and contains the following elements:

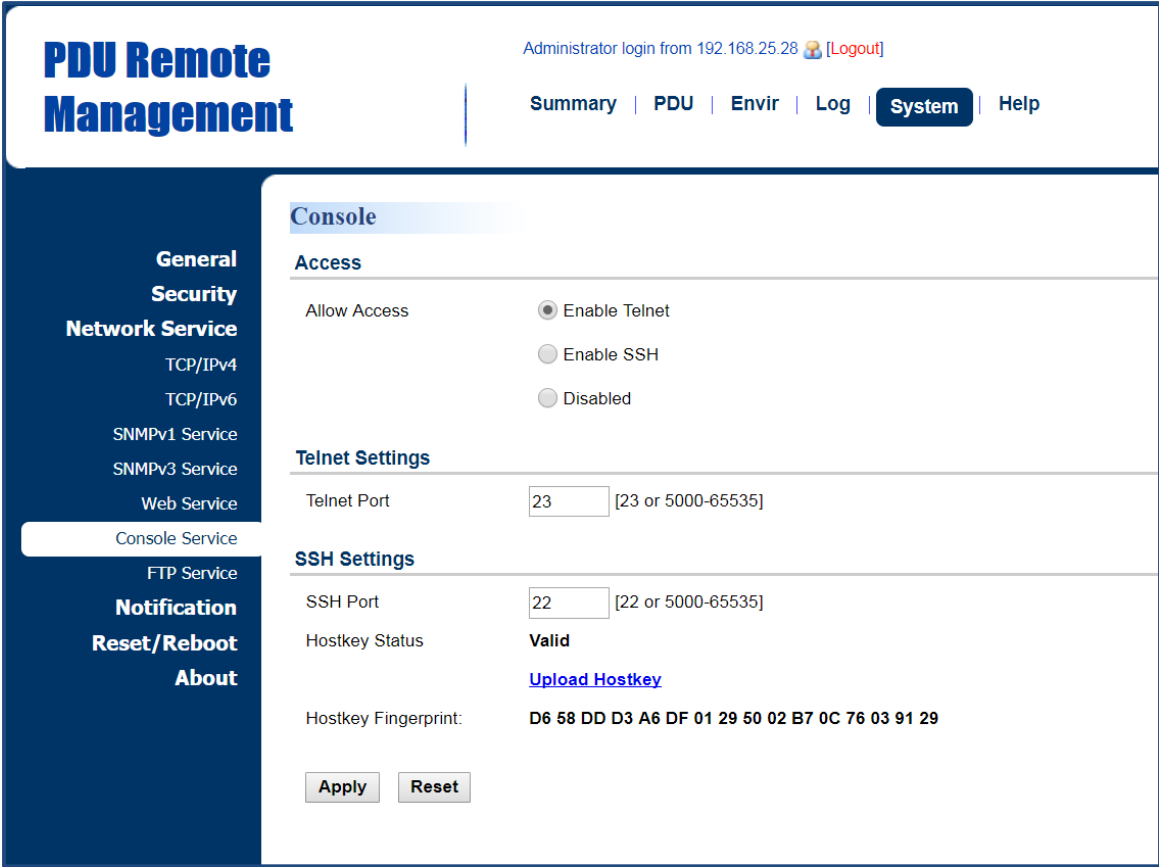
Upload Certificate

« Back

### Console Service

Select the Enable options to allow access using Telnet/SSH service and configure Telnet/SSH port settings. See System Tab > Network Service > Console Service.

System Tab > Network Service > Console Service

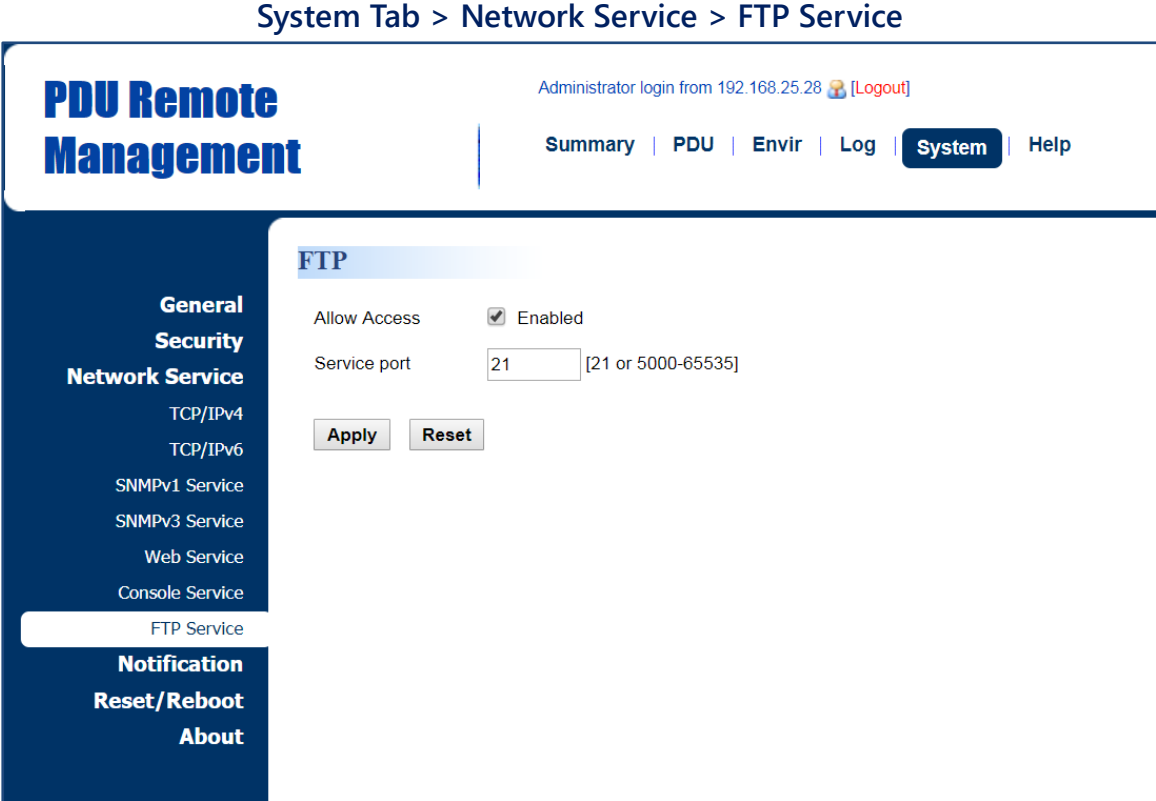


Item	Definition
<b>Access</b>	
Allow Access	Enable access using Telnet or SSH version 2, which transmits user names, passwords, and data in an encrypted format.
<b>Telnet Settings</b>	
Telnet Port	<p>The TCP/IP port that Telnet uses to communicate; 23 is the default value.</p> <p>Users can change the port setting to any unused port from 5000 to 65535 to enhance security.</p> <p><b>Note:</b> Telnet Client requires users to enter a space and the port number after the PDU IP address on the command line to access the control console.</p>

Item	Definition
<b>SSH Settings</b>	
SSH Port	The TCP/IP port that SSH uses to communicate; 22 is the default value. Users can change port setting to any unused port from 5000 to 65535 to enhance security.
Hostkey Status	Display the status of hostkey fingerprint to show whether it is valid or invalid. Click <b>Upload Hostkey</b> to upload or change hostkey.
Hostkey Fingerprint	The hostkey fingerprint uploaded by users will be displayed in this field.

### FTP Service

Allow users to enable/disable the FTP server service and configure the TCP/IP port of the FTP server. The FTP server is used for upgrading Firmware. See [System Tab > Network Service > FTP Service](#).

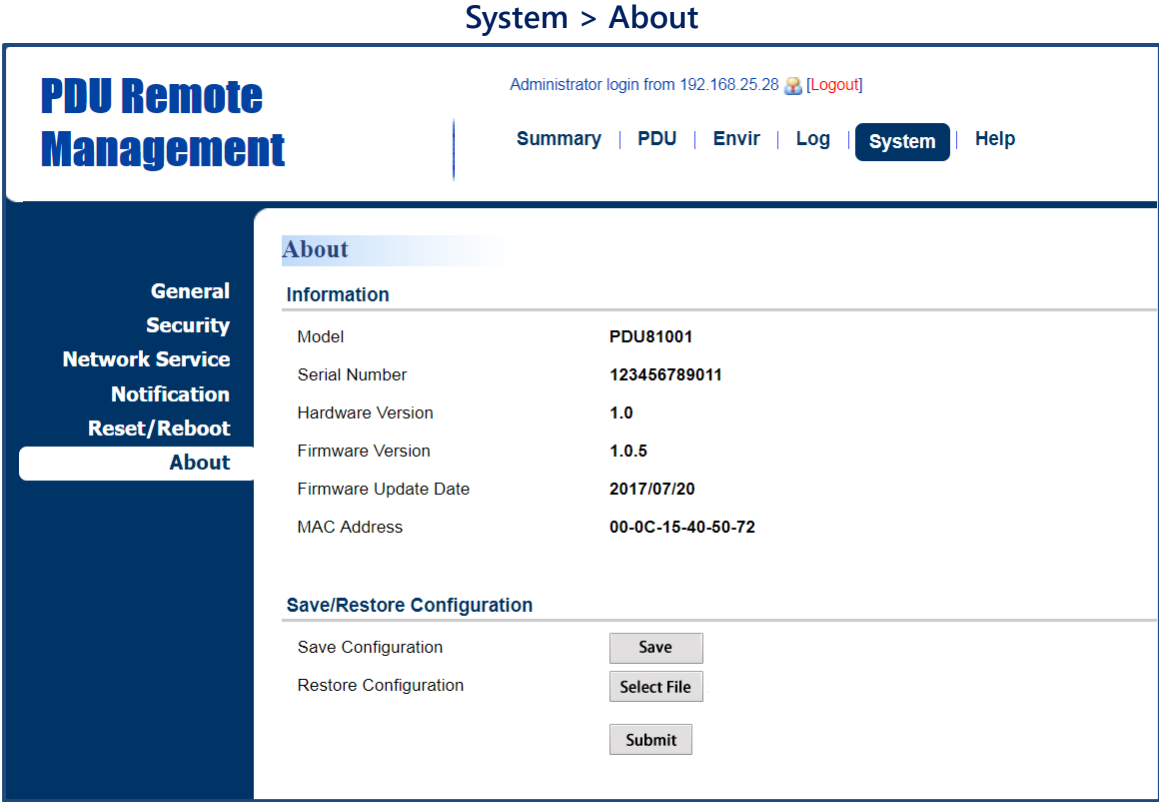


Item	Definition
Allow Access	Enable FTP server access.
Access Port	The TCP/IP port of the FTP server; 21 is the default value. Users can change port setting to any unused port from 5000 to 65535 to enhance security.



# PDU Information

Display the system information of the PDU. See [System > About](#).



Item	Definition
<b>Information</b>	
Model Name	Model name of the PDU.
Serial Number	Serial Number of the PDU.
Hardware Version	The hardware version of the PDU.
Firmware Version	The current firmware version installed on the PDU.
Firmware Updated Date	The date the firmware was last updated.
MAC Address	MAC address of the PDU. <b>Note:</b> The MAC address is shown on the label on the back of the PDU and via the LCD screen on the PDU.
<b>Save/Restore Settings</b>	
Save Configuration	Click <b>Save</b> to save the PDU configuration file to local computer. The text file name will have a default format of YYYY_MM_DD_HHMM.txt.

Restore Configuration	To restore a configuration that has been saved earlier. Click <b>Select File</b> to import an existing configuration file and then click <b>Submit</b> .
-----------------------	---

## Command Line Interface

### Introduction

#### How to log on

Users can log on to the command line interface through either console network access (Telnet or SSH) or local access (Serial port).

##### 1. Network access to the command line interface

When user logs in with the admin username and admin password through Telnet or SSH, there are two types of interfaces available. One is the command line interface (CLI) and the second is a menu interface. The default is CLI. If the user wants to change to the menu interface, type in the [menumode] command. To switch back to CLI, it is necessary to logout and login to the PDU.

##### 2. Local access to the command line interface

To log on via serial connection, the PC/server must be connected directly to the Universal port of the PDU using the included RJ45/DB9 Serial Port Connection Cable, and perform the following steps.

Step 1: Open Hyper Terminal software (eg. PuTTY, HyperTerminal, or Tera Term) on your PC and select a name and icon for the connection.

Step 2: Setup the COM port settings using the following values

- \*Bits per second: 9600

- \*Data bits: 8

- \*Parity: None

- \*Stop bits: 1

- \*Flow control: None

Step 3: Press Enter to enter the Authentication menu.

Step 4: Enter the user name and password of the PDU at the Authentication menu.

**Note:** Serial connection can only access Command Line Mode and cannot support Menu Mode.

#### How to use telnet access command line interface

Step 1: Need to make sure the computer has access to the PDU installed network. At a command prompt, type telnet and the IP address for the PDU (for example, telnet 139.225.6.133, when the PDU uses the default Telnet port of 23), and press Enter.

Step 2: Enter the user name and password (by default, user name: cyber, password: cyber)

#### How to use SSH access command line interface

SSH is highly recommended for using to access the command line interface. SSH encrypts user names, passwords, and transmitted data. To use SSH you must first configure SSH and install an SSH

client program (eg. PuTTY, HyperTerminal, or Tera Term) on your computer.

**Note:** If using PuTTY to configure SSH access, please configure Line discipline of Terminal to “Force off”, as shown in Figure 5.

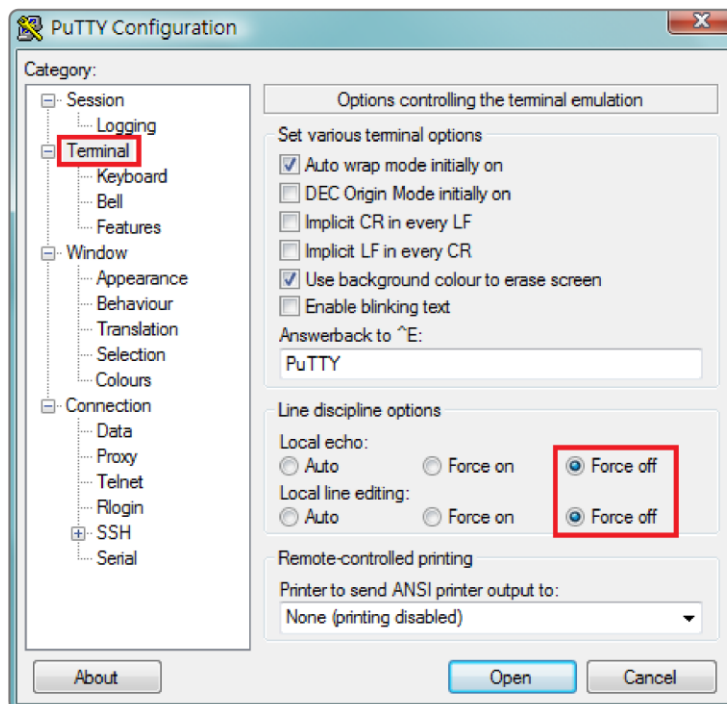


Figure 5. The PuTTY Configuration window.

### How to use the Command Line Interface

While using the command line interface, you can also do the following:

1. To close the connection to the command line interface → Type “**exit**” and press Enter
2. To switch mode as Menu Mode → Type “**menumode**” and press Enter
3. To view a list of available commands or arguments → Type “?” (Eg. date ?).
4. To view the command that was typed most recently in the session → Press the UP/DOWN arrow key. (The session can remember up to ten previous commands.)
5. A command can support multiple options → To define the date as March 21, 2015 (Eg. date yyyy 2015 mm 3 dd 21)

### Command Response Codes

When the command or arguments is not recognized or is incorrect, the console interface will display [^] underneath the wrong command or argument. The following error message will be displayed:

Command not found	PDU doesn't know this command. Console interface display the list of available commands.
Parameter Error	The parameter type or format is not allowed. Console interface display the list of available value or format.

## Command Lists

### oltloadcfgdevsta

Description: Show device status of load and utility.

Option	Argument	Description
show		Show information of system device load and utility status.
guest	1   2   3	Set daisy chain index.

Example 1:

To display device status

CyberPower > **devsta show**

### devcfg

Description: Show and set device load threshold, reset power parameters in device level, set cold start status and delay.

Option	Argument	Description
show		Show information of device configuration.
guest	1   2   3	Set daisy chain index.
overload	<overload threshold value>	Set device overload threshold value.
nearover	<near overload threshold value>	Set device near overload threshold value.
lowload	<low load threshold value>	Set device low load threshold value.
pwrrest	peakload   energy	Reset the peak load or energy of device.
coldstasta	previous   allon	Set the cold start state of device.
coldstadly	-1   0   1   2   ...   300	Set the cold start delay of device.
idletime	1   2   3   5   10   never	Set idle time of device.

Example 1:

To display load configuration of the device

CyberPower > **devcfg show**

Example 2:

To set overload threshold at 7500W

CyberPower > **devcfg overload 7500**

Example 3:

To set near overload threshold at 5000W

CyberPower > **devcfg nearover 5000**

Example 4:

To set cold start delay at 0  
 CyberPower > **devcfg coldstably 0**

Example 5:

To set idle time of the device at 10 minutes  
 CyberPower > **devcfg idletime 10**

**bankcfg**

Description: Show and set bank load configuration.

Option	Argument	Description
show		Show information of bank load threshold.
guest	1   2   3	Set daisy chain index.
index	b1   b2   all	Select bank index.
overload	<overload threshold value>	Set bank overload threshold value.
nearover	<near overload threshold value>	Set bank near overload threshold value.
lowload	<low load threshold value>	Set bank low load threshold value.
restriction	none   onnear   onover	Set outlet restriction of bank

Example 1:

To display bank load configuration  
 CyberPower > **bankcfg show**

Example 2:

To set overload threshold of bank 1 at 15A  
 CyberPower > **bankcfg index b1 overload 15**

Example 3:

To set near overload threshold of bank 2 at 10A  
 CyberPower > **bankcfg index b2 nearover 10**

**oltsta**

Description: Show information of outlet status.

Option	Argument	Description
show		Show information of outlet status.
guest	1   2   3	Set daisy chain index.
index	1   2  ...  outlet number	Select outlet index.

Example 1:

To display all outlet status

CyberPower > **oltsta show**

Example 2:

To display status of outlet #5

CyberPower > **oltsta index 5 show**

### oltctrl

Description: Control the action of outlet.

Option	Argument	Description
Index	1   2  ...  outlet number   b1   b2   all	Select outlet index.
guest	1   2   3	Set daisy chain index.
act	on   off   reboot   delayon   delayoff   delayreboot   cancel	Control the action of outlet.

Example 1:

To turn on outlet #1 immediately

CyberPower > **oltctrl index 1 act on**

Example 2:

To turn on outlet #2 with turn on delay

CyberPower > **oltctrl index 2 act delayon**

### oltcfg

Description: Show and set configuration of outlet action.

Option	Argument	Description
show		Show information of outlet delay time.
guest	1   2   3	Set daisy chain index.
index	1   2  ...  outlet number   all	Select outlet index.
name	<outlet name>	Modify outlet name.
td_on	-1   0   1   2  ...  7200	Set outlet on delay time.
td_off	-1   0   1   2  ...  7200	Set outlet off delay time.
td_reboot	<reboot duration time>	Set outlet reboot duration time.
set	<1   2  ...  outlet number  all> <Outlet Name> <0   1   2  ...  7200> <0   1   2  ...  7200> <5   6  ...  60>	Modify outlet configuration

Example 1:

To display all outlet configuration

CyberPower > **oltcfg index all show**

Example 2:

To name outlet #1 as test\_1

CyberPower > **oltcfg index 1 name test\_1**

Example 3:

To set turn on delay of outlet #2 as 3 seconds

CyberPower > **oltcfg index 2 td\_on 3**

Example 4:

To set turn off delay of outlet #3 as 3 seconds

CyberPower > **oltcfg index 3 td\_off 3**

Example 5:

To set reboot duration of outlet #4 as 5 seconds

CyberPower > **oltcfg index 4 td\_reboot 5**

Example 6:

To name outlet #1 as test\_1, set turn on delay as 3 seconds, set turn off delay as 4 seconds and set reboot duration as 5 seconds with a single command

CyberPower > **oltcfg set 1 test\_1 3 4 5**

### oltloadcfg

Description: Show and set outlet load threshold, reset power parameters in outlet level.

Option	Argument	Description
show		Show information of outlet load threshold.
guest	1   2   3	Set daisy chain index.
index	1   2  ... outlet number   all	Select outlet index.
name	<outlet name>	Modify outlet name.
overload	<overload threshold value>	Set outlet overload threshold value.
nearover	<near overload threshold value>	Set outlet near overload threshold value.
lowload	<low load threshold value>	Set outlet low load threshold value.
pwrrest	peakload   energy	Reset the peak load or energy of outlet.

Example 1:

To display outlet load configuration

CyberPower > **oltloadcfg show**

Example 2:



To set overload threshold of outlet #1 at 1800W

```
CyberPower > oltloadcfg index 1 overload 1800
```

Example 3:

To set near overload threshold of outlet #2 at 1000W

```
CyberPower > oltloadcfg index 2 nearover 1000
```

Example 4:

To set low load threshold of outlet #10 at 100W

```
CyberPower > oltloadcfg index 10 lowload 100
```

## schedule

Description: Show and configure the outlet schedule of device.

Option	Argument	Description
show		Show information of schedule.
guest	1   2   3	Set daisy chain index.
index	1   2   ...   schedule number   10	Select schedule index.
add	once   daily   weekly	<p>Add outlet schedule with a schedule name and follow the settings step by step.</p> <p>The parameters of <b>status</b> enable   disable</p> <p>The parameters of <b>action</b> on   off   reboot   delayon   delayoff   delayreboot</p> <p>The parameters of <b>outlet</b> 1   2   ...   outlet number</p> <p>The parameters of <b>frequency</b> once   daily   weekly</p> <p>The Parameters of <b>hour</b> 1   2   3   .....   24</p> <p>The Parameters of <b>minutes</b> 1   2   3   .....   59</p> <p>The Parameters of day of <b>week</b> Mon   Tue   Wed   Thu   Fri   Sat   Sun</p> <p>The parameters of <b>month</b> 1   2   .....   12</p> <p>The Parameters of <b>day</b></p>

		1  2  3  .....  31
status	enable   disable	Modify schedule status
name	<schedule name>	Modify shedule name.
act	on   off   reboot   delayon   delayoff   delayreboot	Control the action of outlet.
time	<hh:mm>	Set schedule time.
date	<mm/dd>	Set schedule date.
week	Mon   Tue   Wed   Thu   Fri   Sat   Sun	Set schedule week.
oltnum	1   2   ...   outlet number  b1  b2   all	Set the outlet number of schedule.
delete		Delete the schedule.

Example 1:

To display schedules of the device  
 CyberPower > **schedule show**

**date**

Description: Show and configure timezone, date format, date, time.

Option	Argument	Description
show		Display system date information
timezone	<time zone offset>	Choose the time zone in GMT (Greenwich Mean Time).
format	mm/dd/yyyy   yyyy/mm/dd   dd.mm.yyyy   mmm-dd-yy   dd-mmm-yy   yyyy-mm-dd	Set system date format
yyyy	<number of year>	Set year of system date by AD.
mm	<number of month>	Set month of system date.
dd	<number of date>	Set day of month.
time	<hh:mm:ss>	Set system time.

Example 1:

To define timezone offset as +08:00  
 CyberPower > **date timezone +0800**

Example 2:

To define the date as March 21, 2015  
 CyberPower > **date yyyy 2015 mm 3 dd 21**

Example 3:

To define the time as 13:45:12

CyberPower > **date time 13:45:12**

## ntp

Description: Show and configure NTP server IP, NTP update interval time.

Option	Argument	Description
show		Display all NTP information
access	enable   disable	If enable was set, System will set date and time from NTP server.
priip	<primary ntp server ip>	Set the IP address/domain name of primary NTP servers
secip	<secondary ntp server ip>	Set the IP address/domain name of secondary NTP servers
update	now   1-8760	<b>now</b> – Choose <i>Update right now</i> to update immediately. <b>1-8760</b> – Set the frequency to update the date and time from NTP server.

### Example 1:

To enable NTP server define date and time

CyberPower > **ntp access enable**

### Example 2:

To setup primary NTP server IP as “192.168.26.22”

CyberPower > **ntp priip 192.168.26.22**

### Example 3:

To update time by NTP immediately

CyberPower > **ntp update now**

## sys

Description: Show and configure identification of the device.

Option	Argument	Description
show		Display all system information
name	<system name>	Set name of the equipment.
location	<system location>	Set the location of power equipment.
contact	<system contact>	Set the person to contact about this equipment.

reset	reboot   notcpip   all	<p><b>Reboot</b> – Reboot the device</p> <p><b>notcpip</b> – Reset the System to default setting but reserving TCP/IP settings, and restart it.</p> <p><b>all</b> – Set all to reset the System to default setting and restart it.</p>
-------	------------------------	--

Example 1:

To view all information of system

CyberPower > **sys show**

Name: PDU81001  
 Location: Server Room  
 Contact: Administrator  
 Model: PDU81001  
 Hardware Version: 1.1  
 Firmware Version: 1.0.3  
 Firmware Update Date: 03/08/2015  
 Serial Number: TALGY2001975  
 MAC Address: 00-0C-15-00-B9-42

Example 2:

To reset the device to default parameter.

CyberPower > **sys reset all**

**dst**

Description: Show and configure type of Daylight Saving Time.

Option	Argument	Description
show		Display all DST information
mode	disable   us   manual	<p><b>disable</b> – Disable DST.</p> <p><b>us</b> – Tradition US DST</p> <p><b>manual</b> – Manual DST date time rules.</p> <p>After finish this command, input start and end time step by step.</p> <p>The parameters of <b>Week of month</b>:                      first   second   third   forth   last</p> <p>The Parameters of <b>day of week</b>:                      Mon   Tue   Wed   Thu   Fri   Sat   Sun</p> <p>The parameters of <b>month</b>:                      Jan   Feb   Mar   Apr   May   Jun   Jul   Aug   Sep   Oct  </p>

		Nov   Dec
--	--	-----------

Example 1:

Manual set Daylight Saving Time  
 CyberPower > **dst mode manual**  
 Start time (0~23): **2**  
 Start week of month: **second**  
 Start day of week: **Sun**  
 Start month: **Mar**  
 End time (0~23): **2**  
 End week of month: **first**  
 End day of week: **Sun**  
 End month: **Nov**

Example 2:

To view DST setting  
 CyberPower > **dst show**  
 DST: Manual DST Date Time  
 Start: 02:00, the second Sunday of Mar  
 End: 02:00, the first Sunday of Nov

login

Description: Show and configure authentication for login.

Option	Argument	Description
show		Display all login information
type	local   radiuslocal   radiusonly   ldaplocal   ldaponly	<p><b>local</b> – User to login Remote Management Card with user name and password that configured in Local Account.</p> <p><b>radiuslocal</b> – User to login Remote Management Card with user name and password for authenticate with RADIUS server first. If the RADIUS server fails to respond, the user name and password that configured in Local Account will be used.</p> <p><b>radiusonly</b> – User to login Remote Management Card with user name and password for authenticate with RADIUS server only.</p>

		<p><b>Idaplocal</b> – User to login Remote Management Card with user name and password for authenticate with LDAP server first. If the LDAP server fails to respond, the user name and password that configured in Local Account will be used.</p> <p><b>Idaponly</b> – User to login Remote Management Card with user name and password for authenticate with LDAP server only.</p>
secretphrase	<Authentication Phrase>	The Authentication Phrase used to communicate with PowerPanel Business Edition Client
timeout	1~10	The period (in minutes) that the system waits before auto logging off. The range of argument is from 1 to 10 (in minutes).

Example 1:

To change authentication type to Radius, Local Account  
 CyberPower > **login type radiuslocal**

**admin**

Description: Show and configure administrator account and manager IP.

Option	Argument	Description
show		Display all admin information
primip	<primary manager IP>	Set primary manager IP of admin
secmipac	enable   disable	Enable or disable secondary manager IP of admin
secmip	<secondary manager IP>	Set secondary manager IP of admin
name	<administrator account>	Set user name of admin
passwd	<administrator password>	Set user password of admin
secacctac	enable   disable	<p><b>enable</b> – Secondary administrator account active.</p> <p><b>disable</b> – Secondary administrator account inactive.</p>
secname	<secondary administrator account name>	Modify secondary administrator account name
secpasswd	<secondary administrator account password>	Modify secondary administrator account password

Example 1:

To change the primary administrator account information with a single command (need current password)

```
CyberPower > admin name pri_name passwd pri_pass
Input admin password : cyber
pass
```

### device

Description: Show and configure viewer account and manager IP.

Option	Argument	Description
show		Display all viewer account information
access	enable   disable	Enable or disable viewer account
primip	<primary manager IP>	Set primary manager IP of viewer account
secmipac	enable   disable	Enable or disable secondary manager IP of viewer account
secmip	<secondary manager IP>	Set secondary manager IP of viewer account
name	<user name>	Set user name of viewer account
passwd	<user password>	Set user password of viewer account

Example 1:

To define primary viewer manager IP as 192.168.26.0/24  
 CyberPower > **device primip 192.168.26.0/24**

### oltuser

Description: Show and configure the outlet user.

Option	Argument	Description
show		Show information of outlet user.
index	1   2   .....outlet user number	Select user index.
add		Add outlet user then input user name/ password/ outlet number appear later on.
status	enable   disable	Enable of disable the status of outlet user.
name	<outlet user name>	Set the name of outlet user.
passwd	<outlet user password>	Set the password of outlet user.
oltnum	1   2  ...  outlet number   b1   b2   all	Seth the outlet number of outlet user.
delete		Delete the outlet user.

Example 1:

To display configuration of outlet users

CyberPower > **oltuser show**

Example 2:

To disable the outlet user #1

CyberPower > **oltuser index 1 status disable**

Example 3:

To delete the outlet user #1

CyberPower > **oltuser index 1 delete**

## radius

Description: Show and configure information of RADIUS server.

Option	Argument	Description
show		Display all Radius server information
pri sec	show	Display primary/secondary Radius server information.
add		Add radius server then input radius server IP/Secret/Port appear later on.
add	<server IP> <server secret> <server port>	Add radius server information including server IP/Secret/Port at one time.
priip secip	<radius server IP>	Set the IP address of primary/secondary RADIUS server.
priport secport	<radius server port>	Set the UDP port which is used by the primary/secondary Radius server.
prisecret secsecret	<radius server secret>	Set the shared secret of primary/secondary Radius server.
priptype sectype	<radius server authentication type>	Set the authentication type of primary/secondary Radius server.
pridel secdel		Delete primary/secondary Radius server

Example 1:

To view primary radius server information

CyberPower > **radius pri show**

Server IP: 192.168.26.33

Server Secret: testsecret

Server Port: 1826

Example 2:



To view secondary radius server information

```
CyberPower > radius sec show
```

```
Server IP: 192.168.30.58
```

```
Server Secret: testsecret2
```

```
Server Port: 1508
```

Enter the following command to add Radius server information configuration with a single command:

```
radius add <Server IP> <Share Secret> <Server Port><Authentication Type>
```

For example:

```
CyberPower > radius add 192.168.203.55 testsecret 150 pap
```

**Note:** This single command could not be executed successfully if there are two Radius servers to be set already.

## Ldap

Description: Show and configure information of LDAP server.

Option	Argument	Description
show		Display all LDAP server information
add		Add LDAP server then input information for requirements appear later on.
pritype sectype	openldap   ad	Set the type of LDAP server.
priip secip	<LDAP server IP>	Set the IP address of primary/secondary LDAP server.
prissl secssl	enable   disable	Enable or disable using LDAPS.
priport secport	<LDAP server port>	Set the TCP port which is used by the primary/secondary LDAP server.
priidn secdn	< LDAP server base DN>	Set the Base DN of primary/secondary LDAP server.
priaddomain secaddomain	< LDAP server AD domain>	Set the AD Domain of the primary/secondary Active Directory server.
priattr secattr	< LDAP server login attribute>	Set the Login Attribute of primary/secondary LDAP user entry.
pridel secdel		Delete primary/secondary LDAP server.

Example 1:

```
To add LDAP Server
CyberPower > ldap add
Input LDAP Server Type [openldap | ad]: ad
Input IP address: 192.168.26.33
Use SSL [enable | disable]: disable
Input LDAP port: 389
Input base DN: dc=cyber,dc=com
Input login attribute: cn
Input AD Domain: cyber.com
```

Example 2:

```
To view information about LDAP Server
CyberPower > ldap show
Primary LDAP Server
  Type: Windows AD
  LDAP Server: 192.168.26.33
  LDAP SSL: Disable
  Port: 389
  Base DN: dc=cyber,dc=com
  Login Attribute: cn
  AD Domain: cyber.com
```

tcpip

Description: Show and configure IPv4 IP, netmask, gateway, DNS.

Option	Argument	Description
show		Display all IPv4 information
dhcp	enable   disable	Enable or disable DHCP
dns	manual   auto	<b>Auto</b> — Obtain DNS Address from DHCP when DHCP enable <b>Manual</b> — Obtain DNS Address by manual when DHCP enable.
ip	<system IP>	Set IP Address of system
netmask	<system netmask>	Set netmask of system
gateway	<system gateway>	Set gateway of system
dnsip	<system dns>	Set DNS of system

Example 1:

```
To disable DHCP and define IP address to 192.168.26.33
```

CyberPower > **tcpip dhcp disable ip 192.168.26.33**

### tcpip6

Description: Show and configure status of IPv6 router control, IPv6 manual IP.

Option	Argument	Description
show		Display all IPv6 information
access	enable   disable	Enable or disable IPv6 service.
routerctrl	enable   disable	The IPv6 address is assigned through the method (Stateless Address Autoconfiguration, Stateless DHCPv6 or Stateful DHCPv6) which is decided by router setting.
manual	enable   disable	Enable or disable IPv6 manual ip.
ip	<manual IPv6 IP>	Set manual IPv6 ip.

Example 1:

To define IPv6 manual IP address then show the information of IPv6

CyberPower > **tcpip6 ip 2001:cdba:0:0:0:0:3257:9652 show**

Access: Enable

Router Control: Enable

Manual: Enable

Manual IPv6 Address: [2001:cdba::3257:9652]

### snmpv1

Description: Show and configure status of SNMPv1.

Option	Argument	Description
show		Display SNMPv1 status.
index	1   2   3   4	Select SNMPv1 community index.
set	<1   2   3   4> <Community> <IP Address> <readonly   readwrite   forbidden>	Modify SNMPv1 community information.
access	enable   disable	Enable or disable SNMPv1.
community	<Community>	Modify SNMPv1 community name.
ip	<IP Address>	Modify SNMPv1 community IP address.
type	readonly   readwrite   forbidden	Modify SNMPv1 community type.

Example 1:

To view the second SNMPv1 community information

CyberPower > **snmpv1 index 2 show**

Community: private

IP Address: 192.169.203.20

Type: Read/Write

Example 2:

To change the community name of first SNMPv1 community to Public1

CyberPower > **snmpv1 index 1 community Public1**

Example 3:

To change the IP address of third SNMPv1 community to 192.168.203.88

CyberPower > **snmpv1 index 3 ip 192.168.203.88**

Example 4:

To change the community type of forth SNMPv1 community to read/write

CyberPower > **snmpv1 index 4 type readwrite**

Enter the following command to perform all parameters configuration with a single command:

**snmpv1 set <1 | 2 | 3 | 4> <Community> <IP Address> <readonly | readwrite | forbidden>**

For example:

CyberPower > **snmpv1 set 3 CyberPower 192.168.203.91 readonly**

### snmpv3

Description: Show and configure status of SNMPv3.

Option	Argument	Description
Show		Display SNMPv3 status.
Index	1   2   3   4	Select SNMPv3 user index.
Set	<1   2   3   4> <Community> <IP Address> <readonly   readwrite   forbidden>	Modify SNMPv3 user information.
Access	enable   disable	Enable or disable SNMPv3.
Name	<User Name>	Modify SNMPv3 user name.
Status	<enable   disable>	Enable or disable SNMPv3 user.
Ip	<IP Address>	Modify IP address of SNMPv3 user.
Auth	md5   sha   none	Modify authentication protocol of SNMPv3 user.
Authkey	<Auth Key>	Modify authentication password of SNMPv3 user.
Priv	aes   des   none	Modify privacy protocol of SNMPv3 user.
Privkey	<Priv Key>	Modify privacy password of SNMPv3 user.

Example 1:

To view the first SNMPv3 user information

```
CyberPower > snmpv3 index 1 show
```

```
User Name: CyberPower
```

```
Status: Enable
```

```
IP Address: 192.169.30.58
```

```
Auth Protocol: MD5
```

```
Priv Protocol: aes
```

Example 2:

To change the user name of second SNMPv3 user to CyberPower

```
CyberPower > snmpv3 index 2 name CyberPower
```

Example 3:

To enable the-third SNMPv3 user

```
CyberPower > snmpv3 index 3 status enable
```

Example 4:

To change the IP address of forth SNMPv3 user to 192.168.203.66

```
CyberPower > snmpv3 index 4 ip 192.168.203.66
```

Example 5:

To change the authentication protocol of second SNMPv3 user to md5 and set its authentication password as **test\_authkey\_123456**

```
CyberPower > snmpv3 index 2 auth md5 authkey test_authkey_123456
```

Example 6:

To change the authentication password of first SNMPv3 user to **test\_authkey\_123456**

```
CyberPower > snmpv3 index 1 authkey test_authkey_123456
```

Example 7:

To change the authentication protocol of third SNMPv3 user to none

```
CyberPower > snmpv3 index 3 auth none
```

Example 8:

To change the privacy protocol of second SNMPv3 user to aes and set its privacy password as **test\_privkey\_123456**

```
CyberPower > snmpv3 index 2 priv aes privkey test_privkey_123456
```

Example 9:

To change the privacy password of first SNMPv3 user to **test\_privkey\_123456**

```
CyberPower > snmpv3 index 1 privkey test_privkey_123456
```

Example 10:

To change the privacy protocol of third SNMPv3 user to none

CyberPower > **snmpv3 index 3 priv none**

Enter the following command to perform all parameters configuration with a single command:

snmpv3 set <1 | 2 | 3 | 4> <User Name> <IP Address> <md5 | sha | none> <Auth Key>  
<aes | des | none> <Priv Key>

For example.:

CyberPower > **snmpv3 set 1 CyberPower 192.168.203.90 sha test\_authkey\_123456 des test\_privkey\_123456**

**trap**

Description: Show and configure information of SNMP trap receiver.

Option	Argument	Description
show		Display trap receiver information.
add		Add trap receiver.
index	1   2   ...   10	Select trap receiver index.
name	<Trap Receiver Name>	Modify trap name of trap receiver.
ip	<Trap Receiver IP>	Modify IP address of trap receiver.
ver	v1   v3	Modify SNMP version of trap receiver.
status	enable   disable	Enable or disable trap receiver.
community	<Trap Receiver Community>	Modify SNMPv1 community name of trap receiver.
user	1   2   3   4	Select SNMPv3 user of trap receiver.
test		Trap receiver send test
delete		Delete trap receiver.

Example 1:

To view sixth trap receiver information

CyberPower > **trap index 6 show**

Trap Name: CyberPower

Status: Enable

IP Address: 192.168.203.68

Type: SNMPv1

Community: test\_community

Example 2:

To change the trap name of second trap receiver to test

CyberPower > **trap index 2 name test**

Example 3:

To change the IP address of third trap receiver to 192.168.30.85

CyberPower > **trap index 3 ip 192.168.30.85**

Example 4:

To change the SNMP version of forth trap receiver to SNMPv3

CyberPower > **trap index 4 ver v3**

Example 5:

To change the fifth trap receiver

CyberPower > **trap index 5 status enable.**

Example 6:

To change the community name of second trap receiver to CyberPower with the condition that the SNMP version of trap receiver must be SNMPv1.

CyberPower > **trap index 2 community CyberPower**

Example 7:

To change the SNMPv3 user of tenth trap receiver to SNMPv3 user2 with the condition that the SNMP version of trap receiver must be SNMPv3

CyberPower > **trap index 10 user 2**

Example 8:

To delete the fifth trap receiver

CyberPower > **trap index 5 delete**

Enter the following command to add trap receiver configuration with a single command:

For SNMPv1: **trap add <Trap Name> <Trap Receiver IP> v1 <Community>**

For example:

CyberPower > **trap add CyberPower 192.168.203.16 v1 test**

For SNMPv3: **trap add <Trap Name> <Trap Receiver IP> v3 <1 | 2 | 3 | 4>**

For example:

CyberPower > **trap add cyberpower 192.168.203.12 v3 3**

## web

Description: Show and configure web access type, http port and https port.

Option	Argument	Description
show		Display all web information

access	http   https   disable	<b>http</b> – Enable the access to http service. <b>https</b> – Enable the access to https service. <b>disable</b> – Disable web service
httpport	<http port>	The TCP/IP port of the Hypertext Transfer Protocol (HTTP) (80 by default)
httpsport	<https port>	The TCP/IP port of the Hypertext Transfer Protocol Secure (HTTPS) (443 by default)

Example 1:

To change the HTTP server port to 5000  
CyberPower > **web httpport 5000**

### console

Description: Show and configure console network access type, telnet port and SSH port.

Option	Argument	Description
show		Display all console information.
access	telnet   ssh   disable	<b>telnet</b> – Enable the access to Telnet. <b>ssh</b> – Enable the access to SSH. <b>disable</b> – Disable console service.
telnet	enable   disable	<b>enable</b> – Enable Telnet. <b>disable</b> – Disable Telnet.
ssh	enable   disable   reset_hostkey	<b>enable</b> – Enable SSH. <b>disable</b> – Disable SSH. <b>reset_hostkey</b> – Reset SSH Hostkey to default.
telnetport	<telnet port>	The TCP/IP port (23 by default) that Telnet uses to communicate.
sshport	<ssh port>	The TCP/IP port (22 by default) that SSH uses to communicate.

Example 1:

To enable Telnet as console type  
CyberPower > **console telnet enable**

Example 2:

To disable SSH as console type  
CyberPower > **console ssh disable**

**Note:** The telnet and the ssh modes are options for switching between each other. For example, the



telnet will be automatically disabled once ssh is enabled as console type and vice versa.

Example 3:

To reset SSH Hostkey to default

CyberPower > **console ssh reset\_hostkey**

**Note:** The system will reboot after the SSH Hostkey is reset to default.

**ftp**

Description: Show and configure FTP access type and TCP/IP port of FTP.

Option	Argument	Description
show		Display all FTP information
access	enable   disable	Enable or disable FTP server
port	<ftp port>	The TCP/IP port of the FTP server (21 by default).

Example 1:

To enable FTP service

CyberPower > **ftp access enable**

**eventlog**

Description: View and clear the eventlog of the device.

Option	Argument	Description
show		Displays the list of events and a brief description of each event along with the date and time stamp.
clear		Clear the existing event logs.

Example 1:

CyberPower > **eventlog show**

12/11/2015 03:32:08 Admin login from 192.168.26.33.

.....

Then use the following keys to navigate the event log.

Key	Description
SPACE	View the next page of event log.
Q	Close the event log and return to command line interface.

Example 2:

To clear all event logs.

CyberPower > **eventlog clear**

Do you want to clear all eventlog [yes / no]: **yes**

**syslog**

Description: Show and configure information of SYSLOG server.

Option	Argument	Description
show		Display all syslog information.
s1 s2 s3 s4	show	Display syslog server information for 1 to 4 servers.
add		Add syslog server then input syslog server IP /Port appear later on.
add	<server IP> <server port>	Add syslog server information including server IP/Port at one time.
access	enable   disable	Enable or disable syslog.
facility	kernel   user   mail   system   auth1   syslog   link   news   uucp   clock1   auth2   ftp   ntp   logaudit   logalert   clock2   local0   local1   local2   local3   local4   local5   local6   local7	Set Syslog facility.
s1test s2test s3test s4test		Send test message to Syslog server for 1 to 4 servers.
lp1 lp2 lp3 lp4	<SYSLOG server IP>	Set the IP address of Syslog server for 1 to 4 servers.
port1 port2 port3 port4	<SYSLOG server port>	Set the UDP port which is used by the Syslog server 1 to 4 servers.
s1del s2del s3del s4del		Delete Syslog server for 1 to 4 servers.

Example 1:

To view syslog information of server 1

```
CyberPower > syslog s1 show  
IP: 192.168.26.33  
Port: 514
```

Example 2:

To view syslog information of server 2

```
CyberPower > syslog s2 show  
IP: 192.168.203.89  
Port: 268
```

Example 3:

To view syslog information of server 3

```
CyberPower > syslog s3 show  
IP: 192.168.30.15  
Port: 101
```

Example 4:

To view syslog information of server 4

```
CyberPower > syslog s4 show  
IP: 192.168.26.93  
Port: 358
```

Enter the following command to perform all parameters configuration with a single command:

```
syslog add <Server IP address> <Server Port>
```

For example:

```
CyberPower > syslog add 192.168.203.65 180
```

**Note:** This single command could not be executed successfully if there are four Syslog servers to be set already.

### menumode

Description: Switch mode as Menu Mode.

### exit

Description: Close the connection to the command line interface.

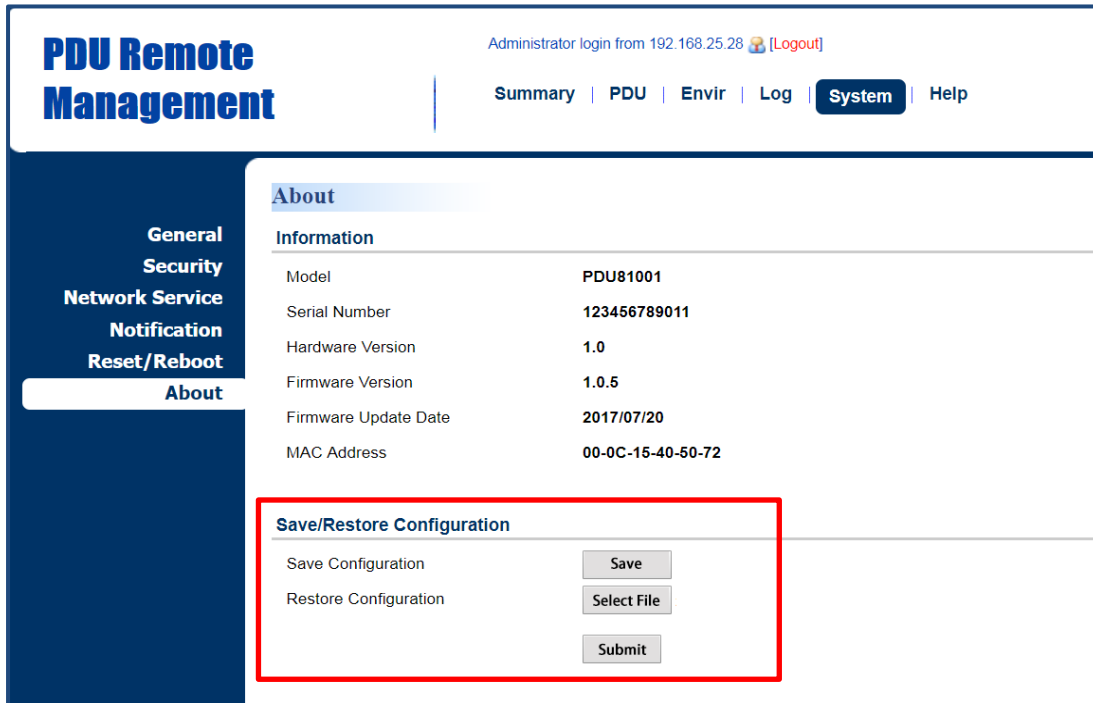
### clear

Description: Clear the console screen

## Save and Restore Configuration Settings

### Option 1: via Web interface

You can easily save and restore the device configuration to your local PC on **System > About**.



To save the configuration file, click “Save” to save the configuration to your local PC. The text file will have a default format of YYYY\_MM\_DD\_HHMM.txt. To restore configuration, click “Browse” to the location of the saved configuration file and click “Submit” to restore a configuration that has been saved earlier.

### Option 2: via File Transfer Protocol (FTP)

**Note:** Only firmware version 1.2.6 and above supports the functionality to download configuration file via FTP.

Use the following steps to save configuration via FTP.

1. Open a command prompt window and navigate to “C:\”.
2. Login to the PDU with FTP command, type
  - C:\>ftp
  - ftp> open 192.168.22.126 21 (for example: 192.168.22.126 is the current IP of the PDU and 21 is the default ftp port for the PDU)
  - Connected to 192.168.22.126.

- 220 CyberPower FTP Server Ready.
  - User (192.168.22.126:(none)):cyber
  - 331 User name okay, need password.
  - Password:
  - 230 User logged in, proceed.
  - ftp>
3. Download the configuration file, type
    - ftp> get <filename>
  4. Download is complete, type
    - ftp> quit

**Note:** <filename> is the configuration file with format of .TXT. Maximum length of filename is 32 characters, excluding the file extension(.TXT).

For example:

```
-ftp> get YYYY_MM_DD_HHMM.txt
```

YYYY\_MM\_DD\_HHMM.txt is the configuration file to be saved.

Use the following steps to restore configuration via FTP.

1. Open a command prompt window and navigate to "C:\".
2. Login to the PDU with FTP command, type
  - C:\>ftp
  - ftp> open 192.168.22.126 21 (for example: 192.168.22.126 is the current IP of the PDU and 21 is the default ftp port for the PDU)
  - Connected to 192.168.22.126.
  - 220 CyberPower FTP Server Ready.
  - User (192.168.22.126:(none)):cyber
  - 331 User name okay, need password.
  - Password:
  - 230 User logged in, proceed.
  - ftp>
3. Upload the configuration file, type
  - ftp> put <filename>
4. Upload is complete, type
  - ftp> quit
5. The system will reboot after you type "quit".

**Option 3: Use Secure Copy (SCP) command**

Use the following steps to restore configuration via SCP.

**Note:** Only firmware version 1.1.2 and above supports the functionality to restore configuration via SCP.

**For Windows Users:**

1. Download any PuTTY Secure Copy client (PSCP) utility.
2. Save the configuration file and the PSCP Utility in the same folder.
3. Open the Command Line Interface and change the path to where the configuration file and the PSCP Utility are saved.
4. Enter the following command to restore configuration:

```
pscp -scp <filename> <user>@<IP address of PDU>:
```

**Note:**

- (1) The SSH setting on the PDU must be Enabled.
- (2) <filename> is the filename of the configuration file with a default format of YYYY\_MM\_DD\_HHMM.txt.
- (3) <user> is the username of the SSH account on the PDU.
- (4) Ensure to add “:” after the IP address.

For example:

```
pscp -scp YYYY_MM_DD_HHMM.txt cyber@192.168.1.100:
```

**Note:** YYYY\_MM\_DD\_HHMM.txt is the configuration file to be restored.

5. After executing the command, a message may appear asking if you trust the host. To continue type “y” for yes within 10 seconds.
6. On the next screen enter the PDU password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

**For Linux, MacOS and Unix Users:**

1. Install the related distribution of an SSH or SCP client, for example OpenSSH client.
2. Open the Terminal and change the path to where the configuration files are saved.
3. Enter the following Command to restore configuration:

```
scp <filename> <user>@< IP address of PDU>:
```

**Note:**

- (1) The SSH setting on the PDU must be Enabled.
- (2) <filename> is the filename of the configuration file with a default format of

YYYY\_MM\_DD\_HHMM.txt.

- (3) <user> is the username of the SSH account on the PDU.
- (4) Ensure to add ":" after the IP address.

For example:

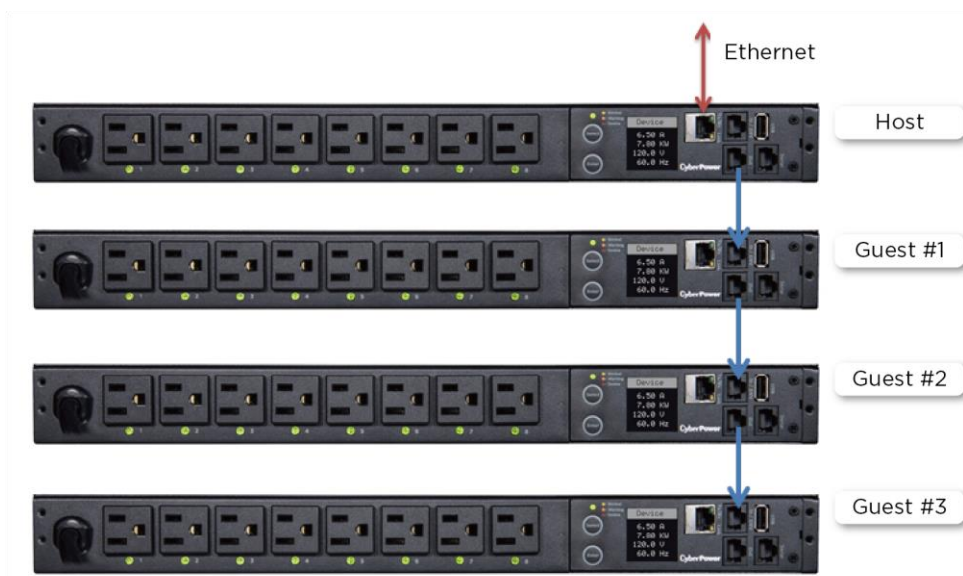
```
scp YYYY_MM_DD_HHMM.txt cyber@192.168.1.100:
```

**Note:** YYYY\_MM\_DD\_HHMM.txt is the configuration file to be restored.

- 4. After executing the command, a message may appear asking if you trust the host. To continue type "y" for yes within 10 seconds.
- 5. On the next screen enter the PDU password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

## PDU Network Daisy Chain

The daisy-chain function allows up to four PDUs to be connected together to be monitored and controlled from one IP address.

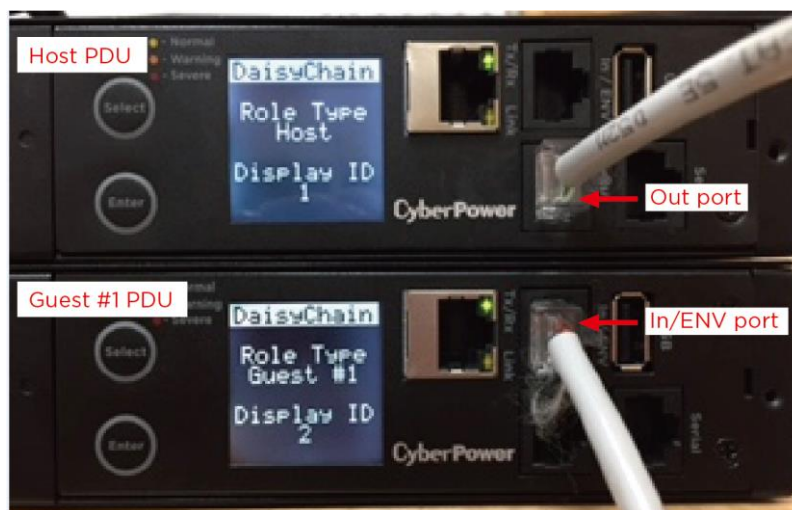


When PDUs are connected, two roles are defined: Host and Guest. Up to three Guest PDUs can be connected to one Host PDU. The Guest PDUs will be recognized by serial number and their order within the daisy-chain.

**Note:** To perform the daisy-chain function, the firmware version of the connected PDUs needs to be the same (v1.08 or above).

### How to connect the PDUs together?

Use one Ethernet cable and connect one end of it to the daisy-chain (Out) port on the Host PDU and the other end to the daisy-chain (In/ENV) port on the Guest 1 PDU to connect the PDUs (as shown below).





## What remote management protocols are supported in PDU daisy-chains?

Currently users can monitor and control daisy-chained PDUs through Web interface (HTTP/HTTPS) or SNMP protocols.

## What functions on the Web pages does daisy-chain support?

Please find in below table:

Summary	
PDU	Device Status
	Outlet Status
	Device Manager
	Outlet Manager
	Outlet Control
	Outlet Schedule
Log	Status Records
	Energy Records
	Graphing
System	Identification

## How to switch between Host and Guest PDUs on the Web interface?

Functionality supported by daisy-chained PDUs will have the Host/ Guest # drop down menu displayed on the Web interface (as shown below).

The screenshot shows the 'PDU Remote Management' web interface. At the top, there is a navigation bar with 'Summary', 'PDU', 'Envir', 'Log', 'System', and 'Help'. The 'PDU' tab is selected. On the left, there is a sidebar menu with options like 'Status', 'Device', 'Outlet', 'Manager', 'Outlet Action', 'Daisy Chain', 'Wake on Lan', 'EnergyWise', and 'PowerPanel® List'. The main content area displays 'Device Status' with a dropdown menu for selecting between 'Host' and 'Guest #1'. A red arrow points to the dropdown menu. The 'Device Status' section shows the following data:

Device Status	
Load	
Device Load	0.00 A / 0 W / 0 VA
Power Factor	----
Peak Load	0.00 A ( at 2017/06/26 16:30:43 )
Energy	0.0 kWh ( from 2017/06/26 16:30:43 )
Utility	
Voltage	105.1 V
Frequency	60.0 Hz

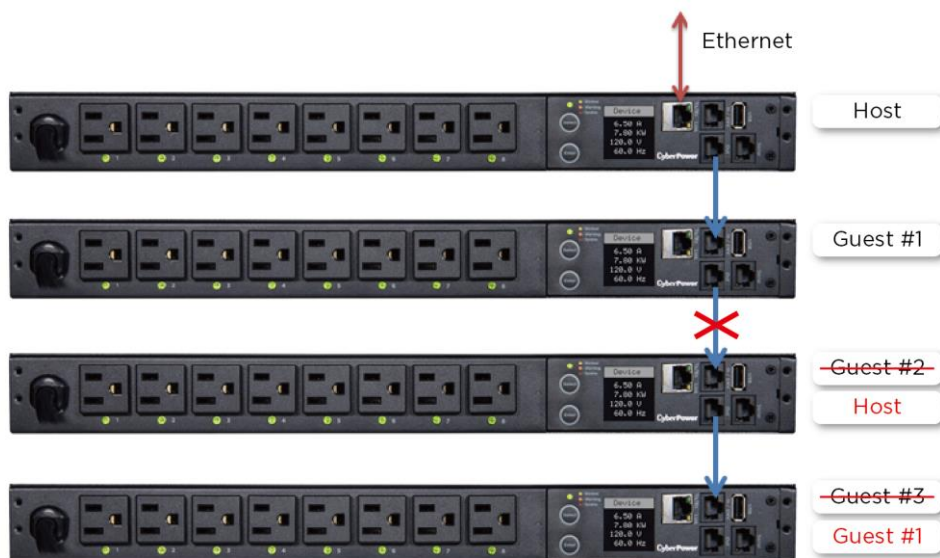
## Can I upgrade the firmware version of the Guest PDUs through the Host PDU?

Yes, you can upgrade the firmware using the Upgrade and Configuration Utility, FTP (network connection required), or USB port. Once the Host completes the PDU firmware upgrade, it will trigger its Guest PDUs to upgrade the firmware automatically. It takes about 5 minutes for the Guest PDUs to upgrade, regardless of the number of PDUs in the series.

### What will happen if an Ethernet cable is disconnected in the PDU daisy-chain?

For example, if four PDUs are connected and the cable connecting Guest 1 and 2 is disconnected, then Guest 2 and 3 will no longer be detected by the Host PDU.

An event showing that Guest 2 and 3 are removed will be recorded in the Host PDU. Meanwhile, Guest 2 and 3 will create a new daisy-chain where Guest 2 becomes a Host and Guest 3 becomes Guest 1 to the new Host.



In the above example, if the disconnected Ethernet cable is re-connected, will the role of the PDUs stay the same?

Yes, when the disconnected cable between Guest 1 and 2 is re-connected, Guest 2 and 3 will revert to their previous roles.

### What happens if one PDU in the daisy-chain is powered off?

For example, if four PDUs are connected and Guest 1 is powered off, an event showing that Guest 1, 2 and 3 are removed will be recorded in the Host PDU. Guest 2 and 3 will not create another daisy-chain.

### Does the Host PDU record the logs of the Guest PDUs and itself?

Yes, the Host PDU records the logs from all Guest PDUs daisy-chained to it.

### Will the Logs of the Guest PDUs recorded in the Host PDU be cleared if the Guest PDUs are removed from the Host PDU?

No, the Logs of the Guest PDUs will remain even after the Guest PDUs are removed.

### Does the Host PDU record the Status Records of the Guest PDUs and itself?

Yes, the Host PDU records the Status Records for all the PDUs in the daisy-chain.

### Will the Status Records of the Guest PDUs logged in the Host PDU be cleared if the Guest PDUs are disconnected from the Host PDU?

Yes, once the Guest PDUs are removed, the Status Records logged in the Host PDU will be cleared. As long as the Host PDU does not connect to other PDUs, the Status Records of the disconnected PDU can be displayed when it is re-connected to the Host PDU. If the Host PDU connects to different PDUs, the Status Records of the removed PDU will be entirely cleared.

### Are the Guest PDUs able to connect to the network when they are daisy-chained?

Yes, even when the PDUs are daisy-chained, the Guest PDUs are able to connect to the network directly. Note that a Guest PDU will require having its own Ethernet cable connected to the network.

### What will happen if a 5th PDU is added to a daisy-chain?

The maximum number of PDUs that can be connected in one daisy-chain is 4. The daisy-chain functionality will not work until the fifth PDU is removed.

### What is the maximum recommended length of the Ethernet cable to daisy-chain the PDUs?

50 ft (15 m)

## Troubleshooting

Problem	Possible Cause	Solution
The PDUs are connected but the daisy chain function is not working.	-The firmware version does not support daisy chain. -The PDUs have different firmware version.	Check the firmware version of each PDU and upgrade to v1.08 or above.
I cannot set the EnergyWise configuration for Guest PDUs.	Only the Host PDU supports this function.	N/A
I cannot set the WoL for Guest PDUs.	Only the Host PDU supports this function.	N/A

## Firmware Upgrade

By upgrading the Firmware, you can obtain new features and updates/improvements to existing functionality. To ensure the firmware is kept up to date, please regularly visit our website to see if there is any updated firmware version available. There are three methods for upgrading the PDU firmware. Please follow the instructions below for the method that is appropriate for your application. There are two files to update in order to upgrade the firmware version:

- \* cpsmpdumadata\_XXX.bin
- \* cpsmpdumafw\_XXX.bin

Note that the XXX is not part of the file name but is where the version number in the filename is given. Prior to performing a firmware update, please:

- Download the latest firmware from [www.cyberpower.com](http://www.cyberpower.com)
- Extract the downloaded firmware file to your local "C:\\" drive

### Note:

1. The FTP service needs to be enabled before attempting to execute a firmware upgrade. Please refer to 5.7 FTP Service to make sure that FTP is enabled.
2. Please do not turn the PDU off when processing the Firmware upgrade. PDU outlets will remain powered on while the firmware update takes place. Only the PDU LCD screen will reboot.
3. The PDU LCD screen will reboot during the firmware update process. This DOES NOT cause the PDU outlets to reboot.

### Option 1: Single Device Upgrade via FTP

Use the following steps to upgrade the firmware.

1. Open a command prompt window and navigate to "C:\\".
2. Login to the PDU with FTP command, type
  - C:\>ftp
  - ftp> open 192.168.22.126 21 (for example: 192.168.22.126 is the current IP of the PDU and 21 is the default ftp port for the PDU)
  - Connected to 192.168.22.126.
  - 220 CyberPower FTP Server Ready.
  - User (192.168.22.126:(none)):cyber
  - 331 User name okay, need password.
  - Password:
  - 230 User logged in, proceed.
  - ftp>

3. Upload the cpsmpdumadata\_XXX.bin, type
  - ftp > bin
  - ftp > put cpsmpdumadata\_XXX.bin
4. Upgrade complete, type
  - ftp > quit
5. The system will reboot after you type "quit". This reboot will take approx. 30 seconds.
6. Login to the PDU via FTP again, type
  - C:\>ftp
  - ftp> open 192.168.22.126 21 (for example: 192.168.22.126 is the current IP of the PDU and 21 is the default ftp port for the PDU)
  - Connected to 192.168.22.126.
  - 220 CyberPower FTP Server Ready.
  - User (192.168.22.126:(none)):cyber
  - 331 User name okay, need password.
  - Password:
  - 230 User logged in, proceed.
  - ftp>
7. Upload cpsmpdumafw\_XXX.bin, type
  - ftp > bin
  - ftp > put cpsmpdumafw\_XXX.bin
8. Upgrade complete, type
  - ftp > quit
9. The system will reboot after you type "quit".

## Option 2: Single or Multiple Device Upgrade (recommended)

Use the following steps to upgrade the firmware.

1. Download the **Upgrade and Configuration Utility** from [www.cyberpower.com](http://www.cyberpower.com)
2. Open the **Upgrade and Configuration Utility** from Start > All Programs > CyberPower Upgrade and Configuration Utility.
3. Wait for search to finish (shown in Figure 1).

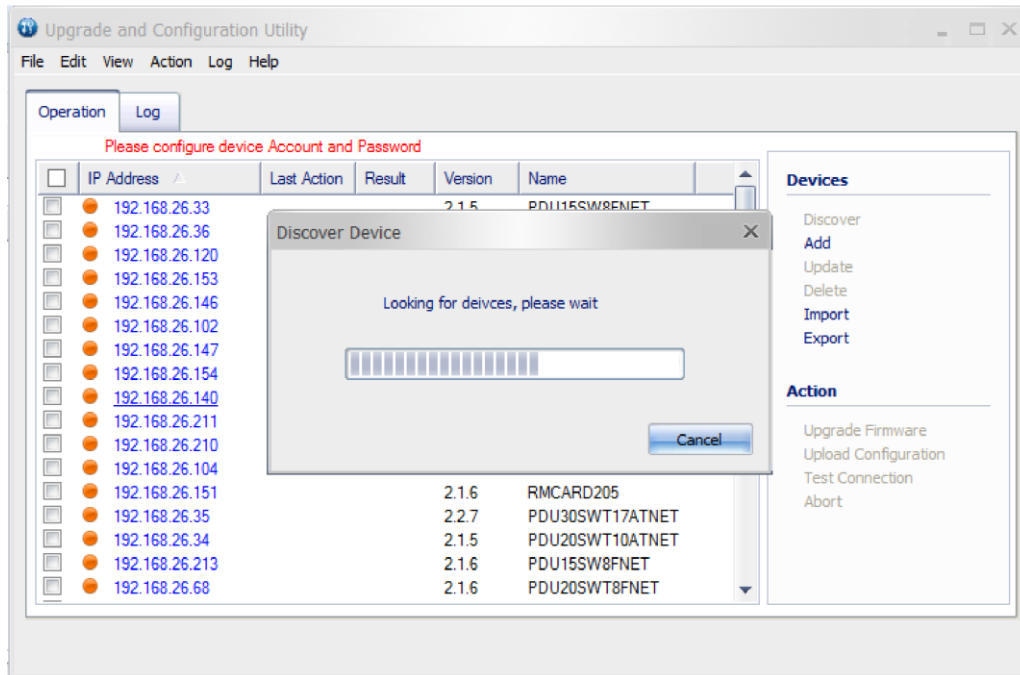


Figure 1.

4. Check the checkbox to select devices listed in the **Operation View** (Shown in Figure 2).

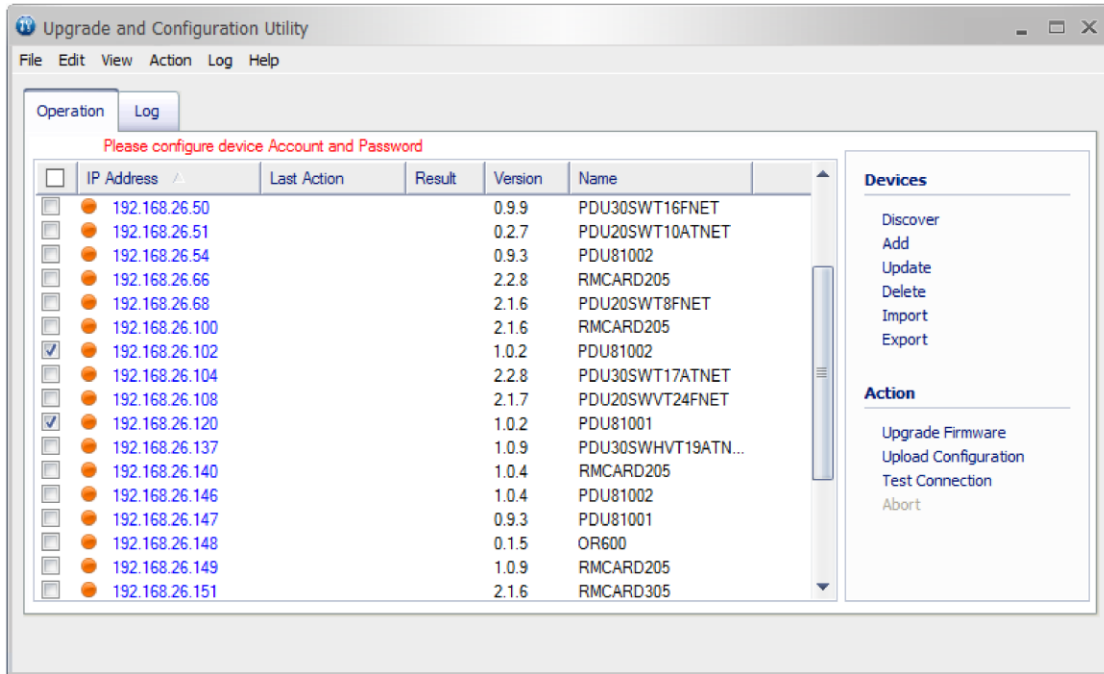


Figure 2

5. Make sure **Account** and **Password** are valid on selected devices (Shown in Figure 3).

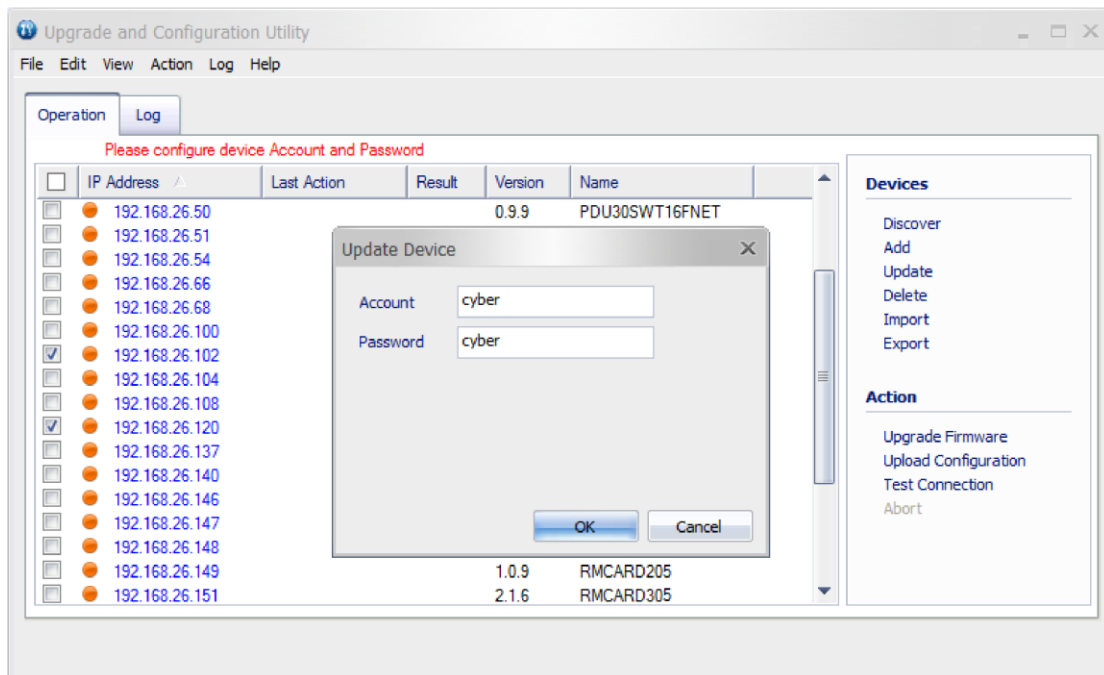


Figure 3.

6. Select **Upgrade Firmware**.

7. Click **Browse** to locate and select the firmware and data file to be updated (Shown in Figure 4).

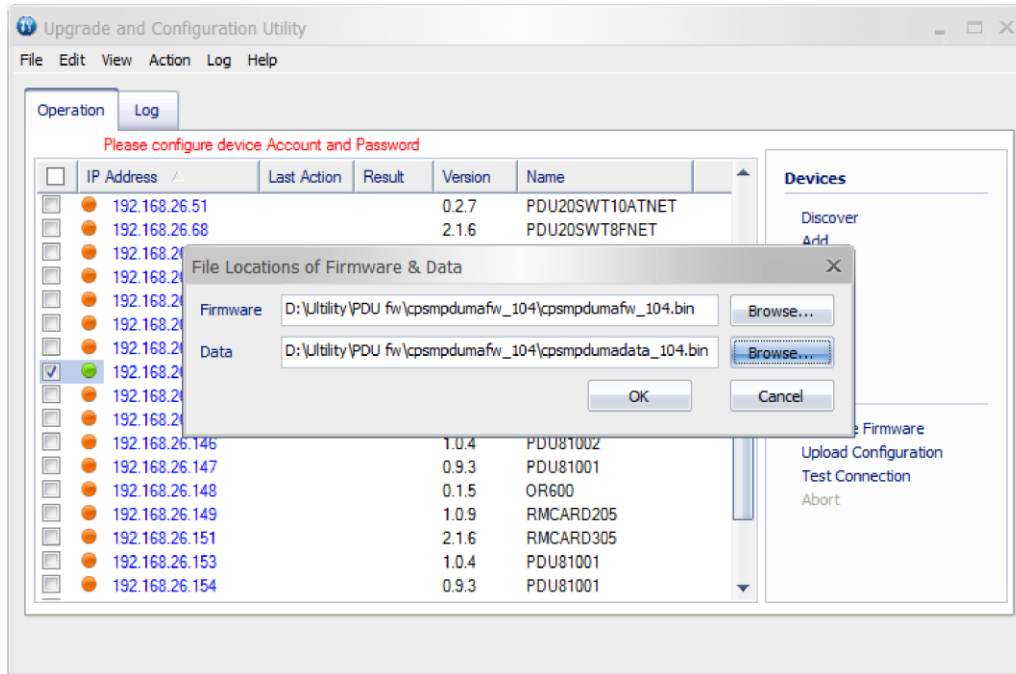


Figure 4.

8. Click **OK** in the **Upgrade Firmware** confirmation window (Shown in Figure 5).

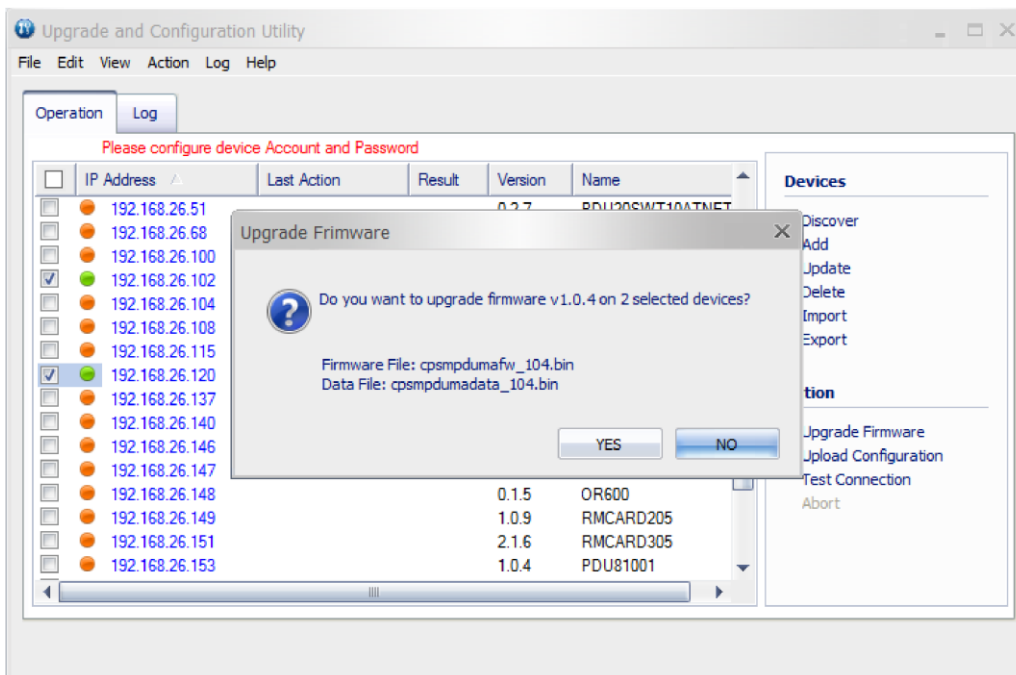


Figure 5.



9. The upgrade progress bar will show in **Last Action** column (Shown in Figure 6).

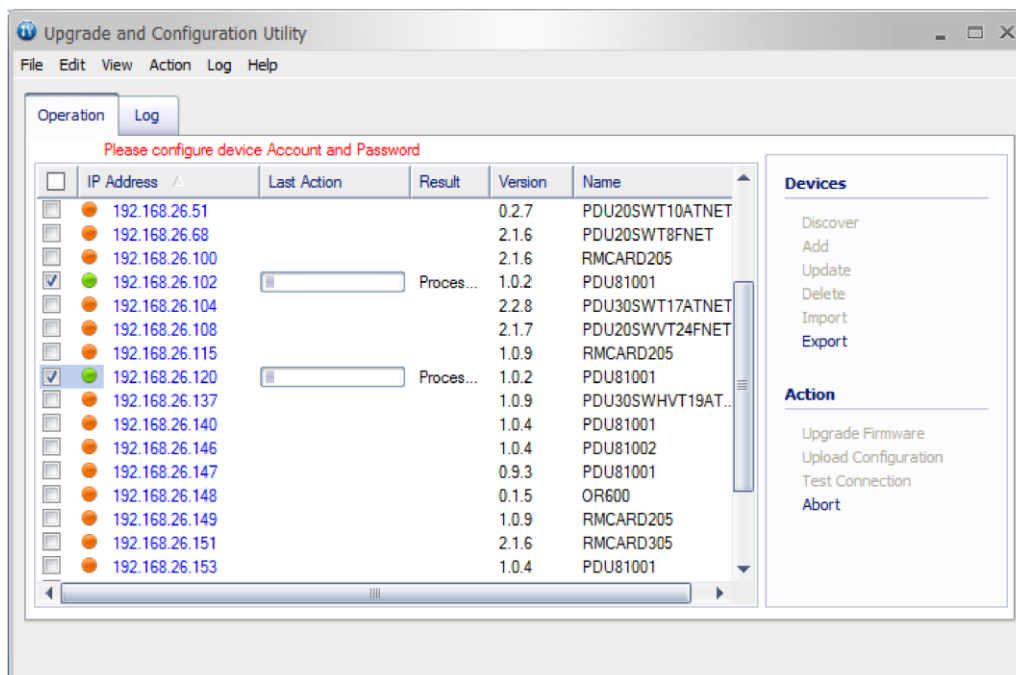


Figure 6.

10. The result of firmware upgrade will show in **Result** column (Shown in Figure 7).

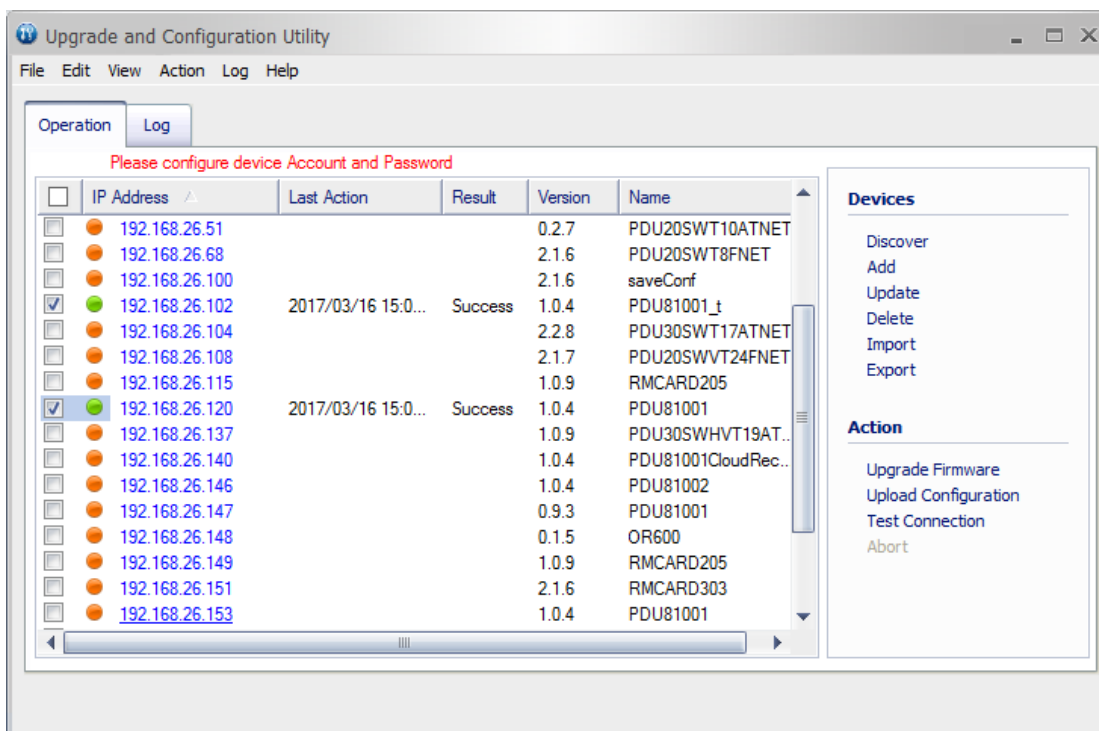


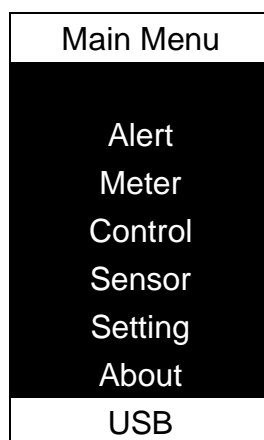
Figure 7.

**Note:** If you don't want to wait for the firmware upgrade, you can stop the process by clicking **Abort** in the **Action** menu. However, this is not recommended because the **Abort** action may cause the device to malfunction.

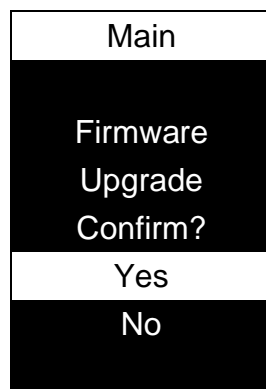
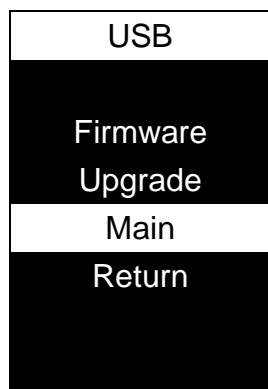
### Option 3: Use a USB Flash Drive

Use the following steps to upgrade the firmware.

1. Download the latest firmware from [www.cyberpower.com](http://www.cyberpower.com)
2. Extract the file to the root directory of a USB flash drive with **FAT32 formatting**. Please note that the two files below should be available in order to complete the firmware upgrade process:
  - \*cpsmpdumadata\_xxx.bin
  - \*cpsmpdumafw\_xxx.bin
3. Plug the USB drive into the PDU USB port and press **Enter** on the PDU LCD screen to enter **Main Menu**. The **USB** option will be displayed.



4. Select **USB** and press **Enter** button to enter **Firmware Upgrade** menu.
5. Select **Main** and **Yes** to start the upgrade process.



6. The PDU will reboot after the process is completed.

**Note:** You can check to see if the firmware upgrade is successful by checking the “Firmware version” on the [System->About] webpage. You can also check Firmware Version on LCD screen. Press **Enter** on the LCD screen to enter **Main Menu**. Select **About** and press **Enter** to see the PDU information. Select **Firmware Version** to check the PDU Firmware Version.

### Option 4: Use Secure Copy (SCP) command

Use the following steps to update the firmware via SCP.

**Note:** Only firmware version 1.10 and above supports the functionality to update firmware via SCP.

### For Windows Users:

1. Download any PuTTY Secure Copy client (PSCP) utility.
2. Save the firmware files and the PSCP Utility in the same folder.
3. Open the Command Line Interface and change the path to where the firmware files and the PSCP Utility are saved.
4. Enter the following command to perform the firmware update:  

```
pscp -scp <filename> <user>@<IP address of PDU>:
```

### Note:

- (5) The SSH setting on the PDU must be Enabled.
- (6) <filename> is the filename of the firmware file. There are two firmware files to upload: `cpsmpdumadata_XXX.bin` and `cpsmpdumafw_XXX.bin`. In order to upgrade the firmware version both files need to be uploaded. Only one firmware file can be uploaded at a time, it is recommended to upload the data file `cpsmpdumadata_XXX.bin` first followed by the firmware file `cpsmpdumafw_XXX.bin`.
- (7) <user> is the username of the SSH account on the PDU.
- (8) Ensure to add “:” after the IP address.

For example:

```
pscp -scp cpsmpdumafw_XXX.bin cyber@192.168.1.100:
```

**Note:** `cpsmpdumafw_XXX.bin` is the firmware file of the version being updated.

5. After executing the command, a message may appear asking if you trust the host. To continue type “y” for yes within 10 seconds.
6. On the next screen enter the PDU password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.
7. Repeat steps 4 through step 6 to upload the firmware file `cpsmpdumafw_XXX.bin` to complete the firmware update process.
8. If the firmware file transfer is unsuccessful you will see an error message. Attempt to retype the command and execute it again.

### For Linux, MacOS and Unix Users:

1. Install the related distribution of an SSH or SCP client, for example Openssh client.
2. Open the Terminal and change the path to where the firmware files are saved.
3. Enter the following Command to perform firmware update:  

```
scp <filename> <user>@< IP address of PDU>:
```

**Note:**

- (1) The SSH setting on the PDU must be Enabled.
- (2) <filename> is the filename of the firmware file. There are two firmware files to upload: `cpsmpdumadata_XXX.bin` and `cpsmpdumafw_XXX.bin`. In order to upgrade the firmware version both files need to be uploaded. Only one firmware file can be uploaded at a time, it is recommended to upload the data file `cpsmpdumadata_XXX.bin` first followed by the firmware file `cpsmpdumafw_XXX.bin`.
- (3) <user> is the username of the SSH account on the PDU.
- (4) Ensure to add ":" after the IP address.

For example:

```
scp cpsmpdumafw_XXX.bin cyber@192.168.1.100:
```

**Note:** `cpsmpdumafw_XXX.bin` is the firmware file of the version being updated.

4. After executing the command, a message may appear asking if you trust the host. To continue type "y" for yes within 10 seconds.
5. On the next screen enter the PDU password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.
6. Repeat steps 3 through step 5 to upload the firmware file `cpsmpdumafw_XXX.bin` to complete the firmware update process.
7. If the firmware file transfer is unsuccessful you will see an error message. Attempt to retype the command and execute it again.

## **Contact Information**

Feel free to contact our Tech Support department with installation, troubleshooting, or general product questions.

### **Cyber Power Systems, Inc.**

Web: [www.cyberpower.com](http://www.cyberpower.com)

#### **For USA and Canada:**

4241 12th Ave East, Suite 400 Shakopee, MN55379

Toll-free: (877) 297-6937

#### **For all other regions:**

Please visit our website for local contact information.