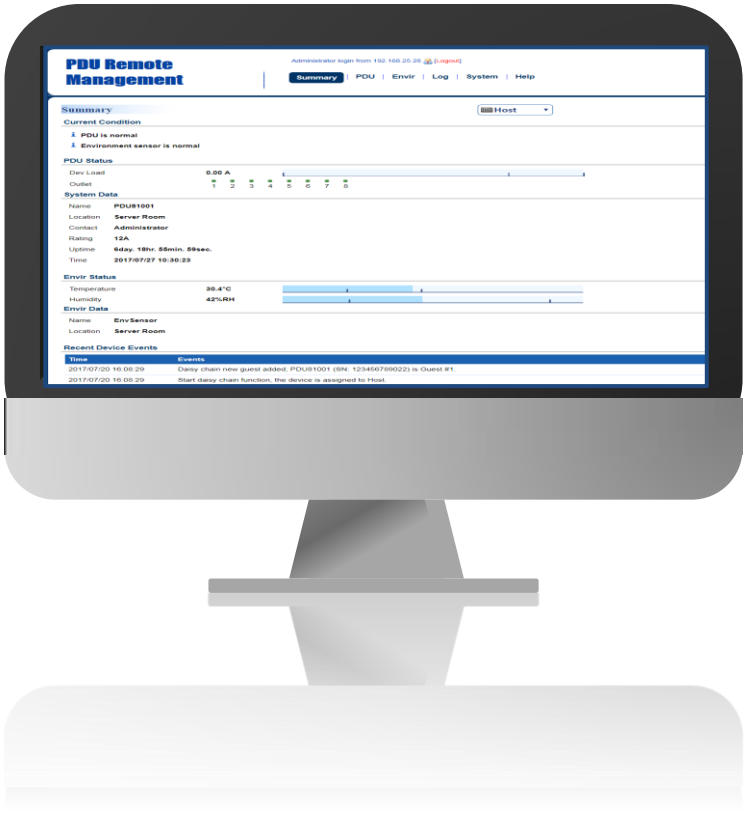
CyberPower®

USER'S MANUAL

Intelligent PDU Web Interface

PDU31xxx
PDU41xxx
PDU71xxx
PDU81xxx



Copyright © 2018 Cyber Power Systems, Inc. All rights reserved.

Table Of Contents

1. Introduction 1
1.1 Brief Introduction to the Web Interface 1
1.2 How to Log in 1
1.3 General Settings 2
1.3.1 Date and Time Settings 2
1.3.2 Daylight Saving Time 4
1.3.3 Device Identification 5
1.3.4 Device Reset/Reboot 6
1.3.5 Environmental Monitoring 7
2. Advanced Power Management 10
2.1 Remote Monitoring 10
2.2 Visible Power Consumption 14
2.3 Event Logging 20
2.4 Power Protection 22
2.5 Event Action Notification 24
2.5.1 Event Action Recipient Settings 26
2.5.1.1 E-mail Notification 26
2.5.1.2 SNMP Trap Notification 29
2.5.1.3 SMS Notification 32
3. Outlet Management 38
3.1 Remote Outlet On/Off/Reboot 38
3.2 Scheduled Outlet On/Off/Reboot 40
3.3 Sequencing Power On/Off 42
3.4 Wake on LAN (WoL) 45
3.5 Graceful Computer Shutdown 48
3.6 Cisco EnergyWise 49
4. Security 53
4.1 Login Authentication 53
4.1.1 Using Local Configuration for Authentication 55
4.1.2 Using RADIUS Configuration for Authentication 59
4.1.3 Using LDAP Configuration for Authentication 61
4.2 Timeout Setting 63
5. Network Service 64
5.1 TCP/IPv4 Setting 64
5.3 SNMPv1 Service Setting 66
5.4 SNMPv3 Service Setting 68

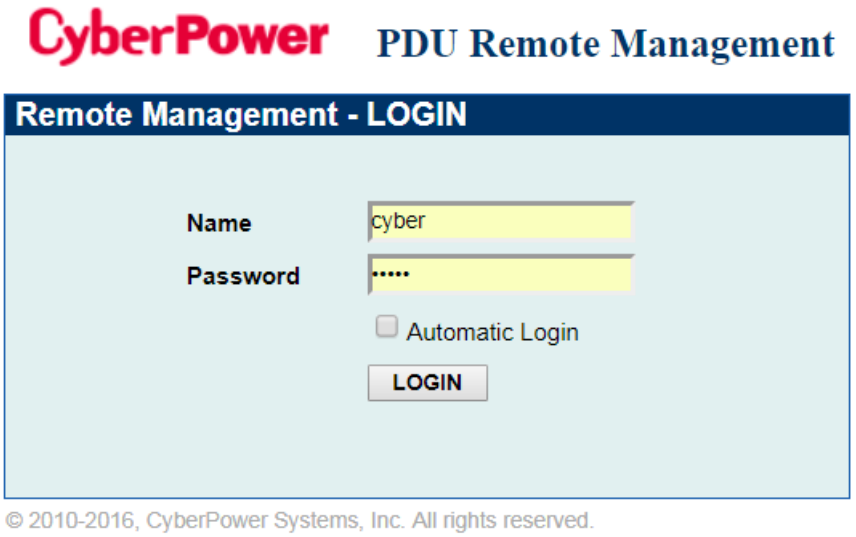
5.5 Web Service.....70
5.6 Console Service.....73
5.7 FTP Service.....75
6. PDU Information.....76
Appendix A: PDU Network Daisy Chain.....78
Appendix B: Firmware Upgrade.....82

1. Introduction

1.1 Brief Introduction to the Web Interface

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.

1.2 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.

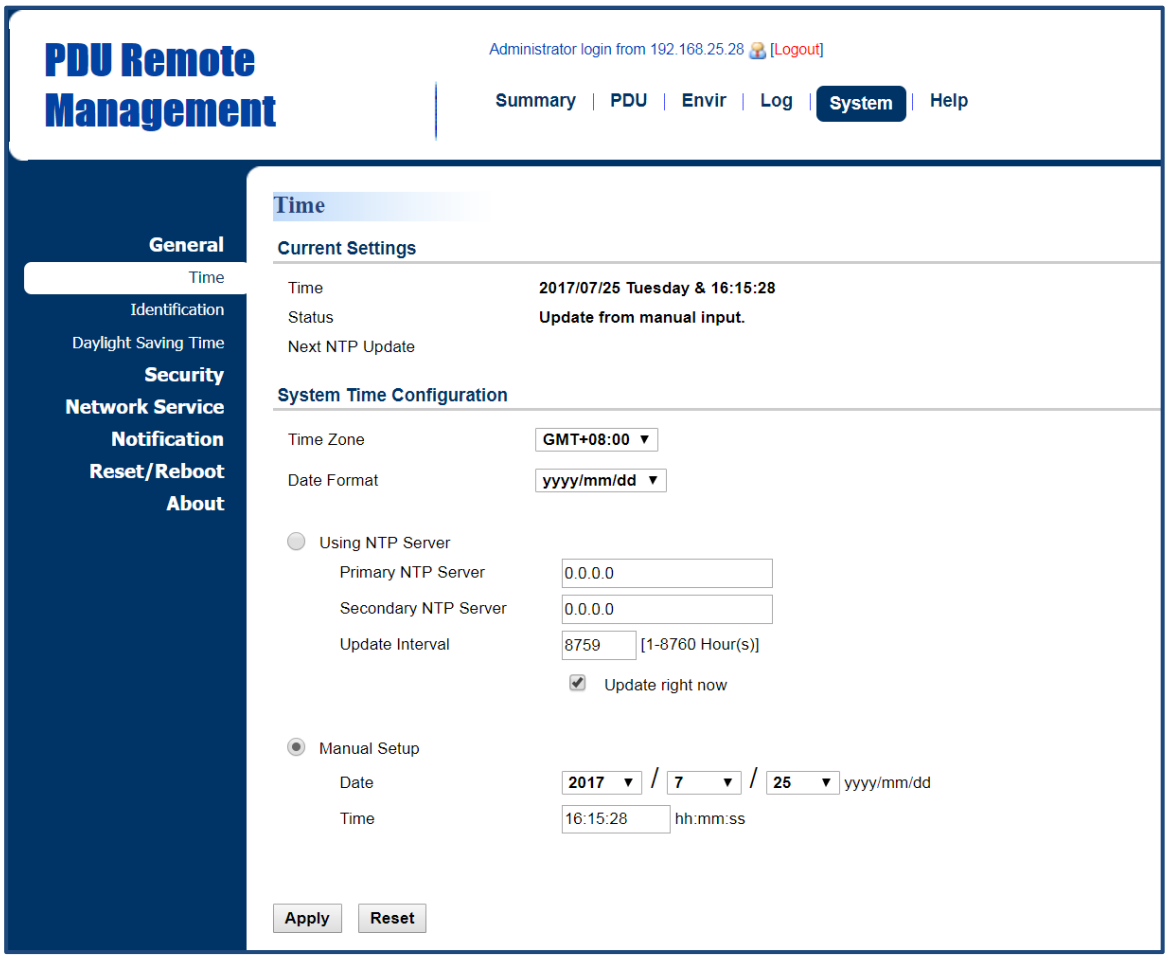
1.3 General Settings

These are the basic settings for the PDU.

1.3.1 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**.

System Tab > General > Time



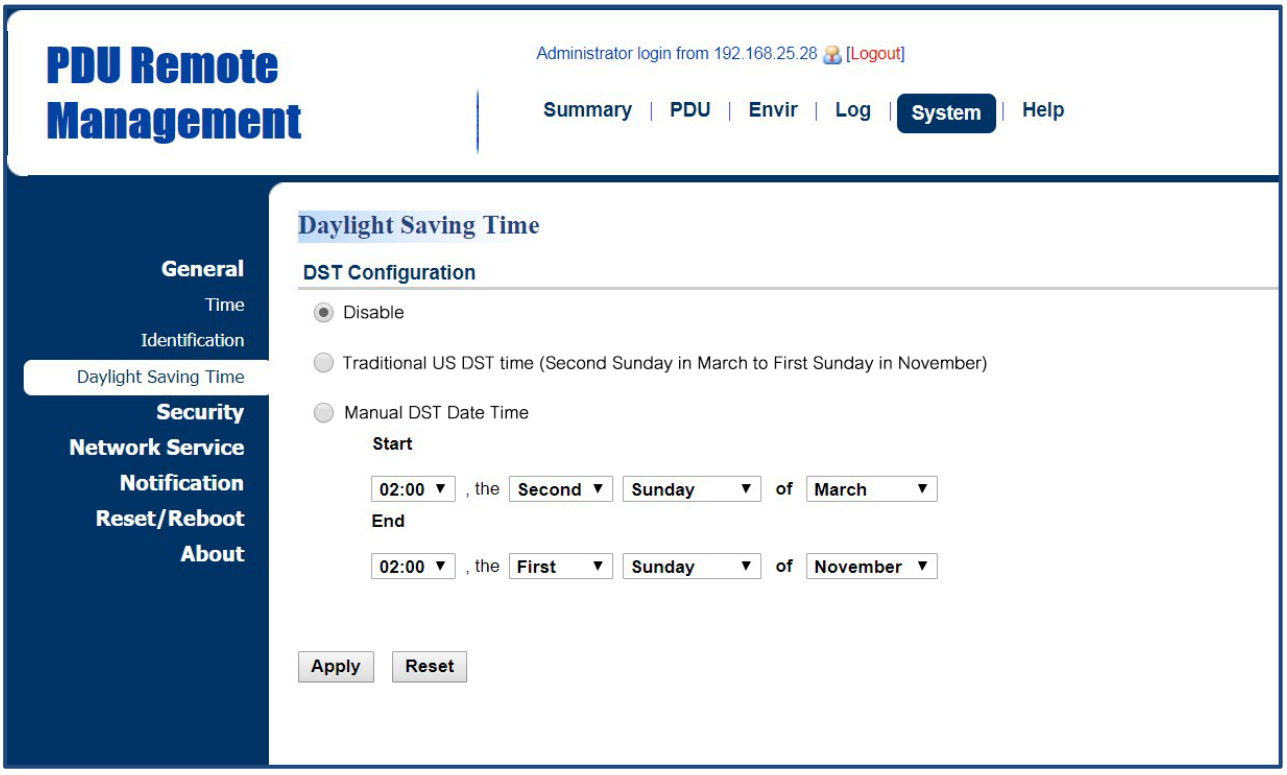
Item	Definition
Current Settings	
Time	The current date and time.
Status	Show whether the date and time setting is updated by manual setup or by the NTP (Network Time Protocol) server.
Next NTP Update	Synchronize with *Update Interval*.

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

1.3.2 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

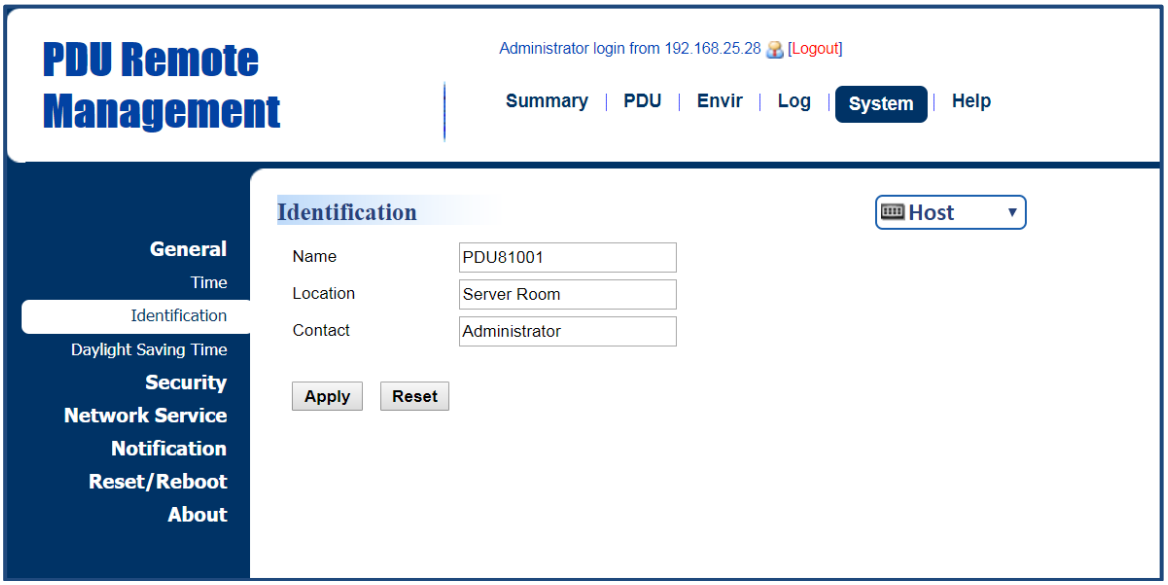


Item	Definition
DST Configuration	
Disable	Disable the DST function.
Traditional US DST Time	Start from the second Sunday in March to the first Sunday in November.
Manual DST Date Time	Select the start/end time using the dropdown menu.

1.3.3 Device Identification

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

System Tab > General > Identification

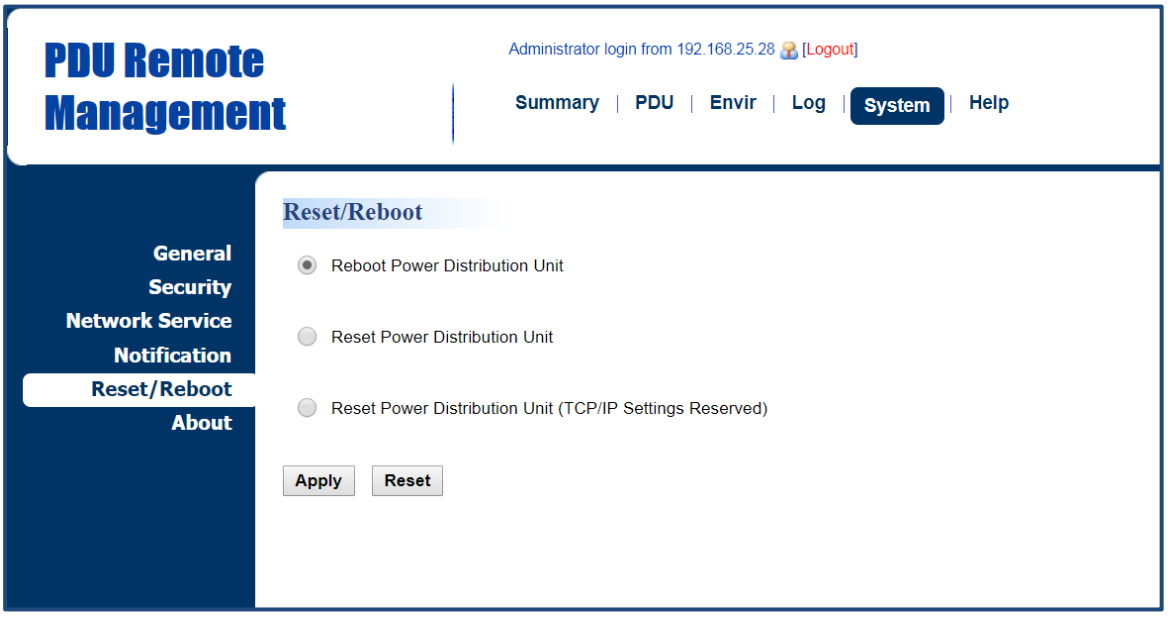


Item	Definition
HOST/GUEST#	Select the role of the PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Name	The name entered by the user to identify the PDU.
Location	The PDU location entered by the user.
Contact	The person to be contacted about issues. Entered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

1.3.4 Device Reset/Reboot

Users can reboot the PDU or reset all the settings to defaults. See **System Tab > Reset/Reboot.**

System Tab > Reset/Reboot

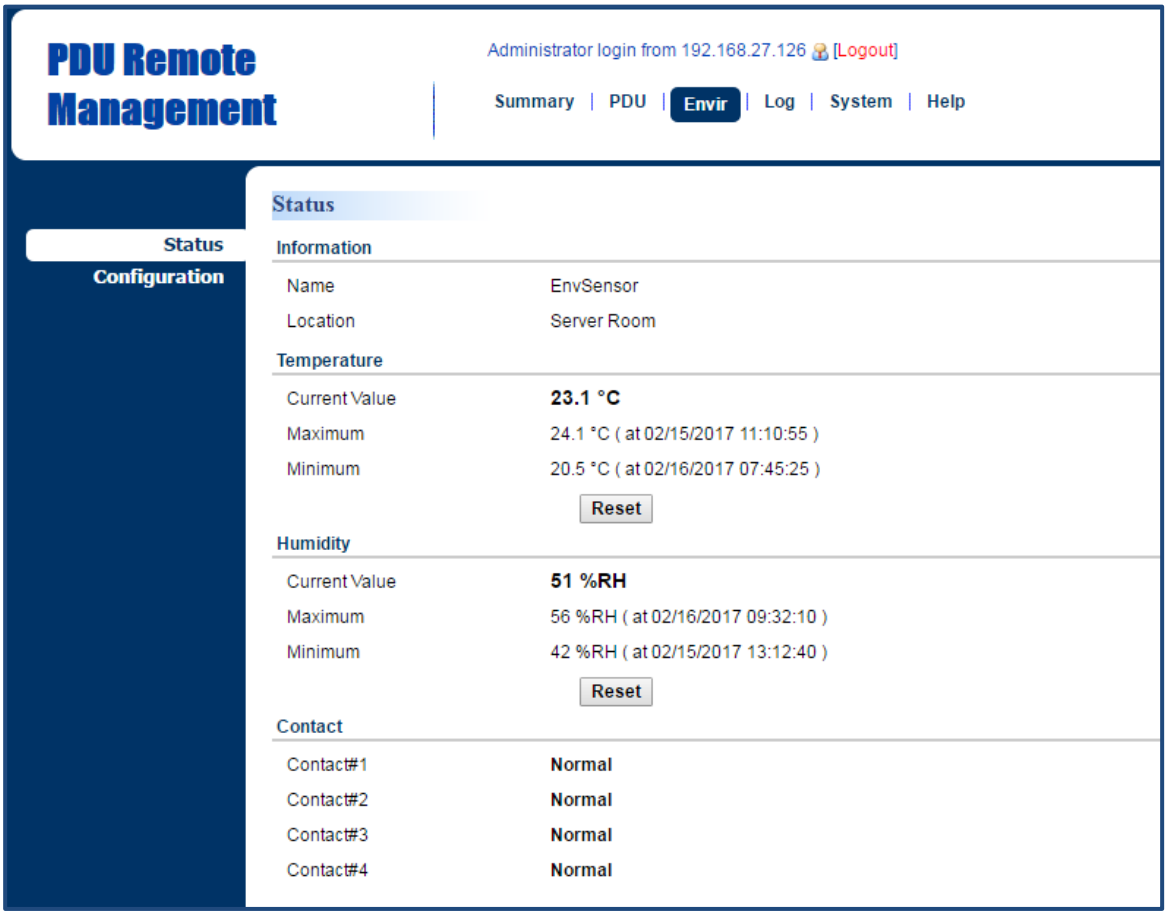


Item	Definition
Reboot Power Distribution Unit	Restart the PDU without power cycling any outlet.
Reset Power Distribution Unit	Reset the PDU to its factory default setting and restart it. This action will power cycle any outlet.
Reset Power Distribution Unit (TCP/IP Settings Reserved)	Reset the PDU to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

1.3.5 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.

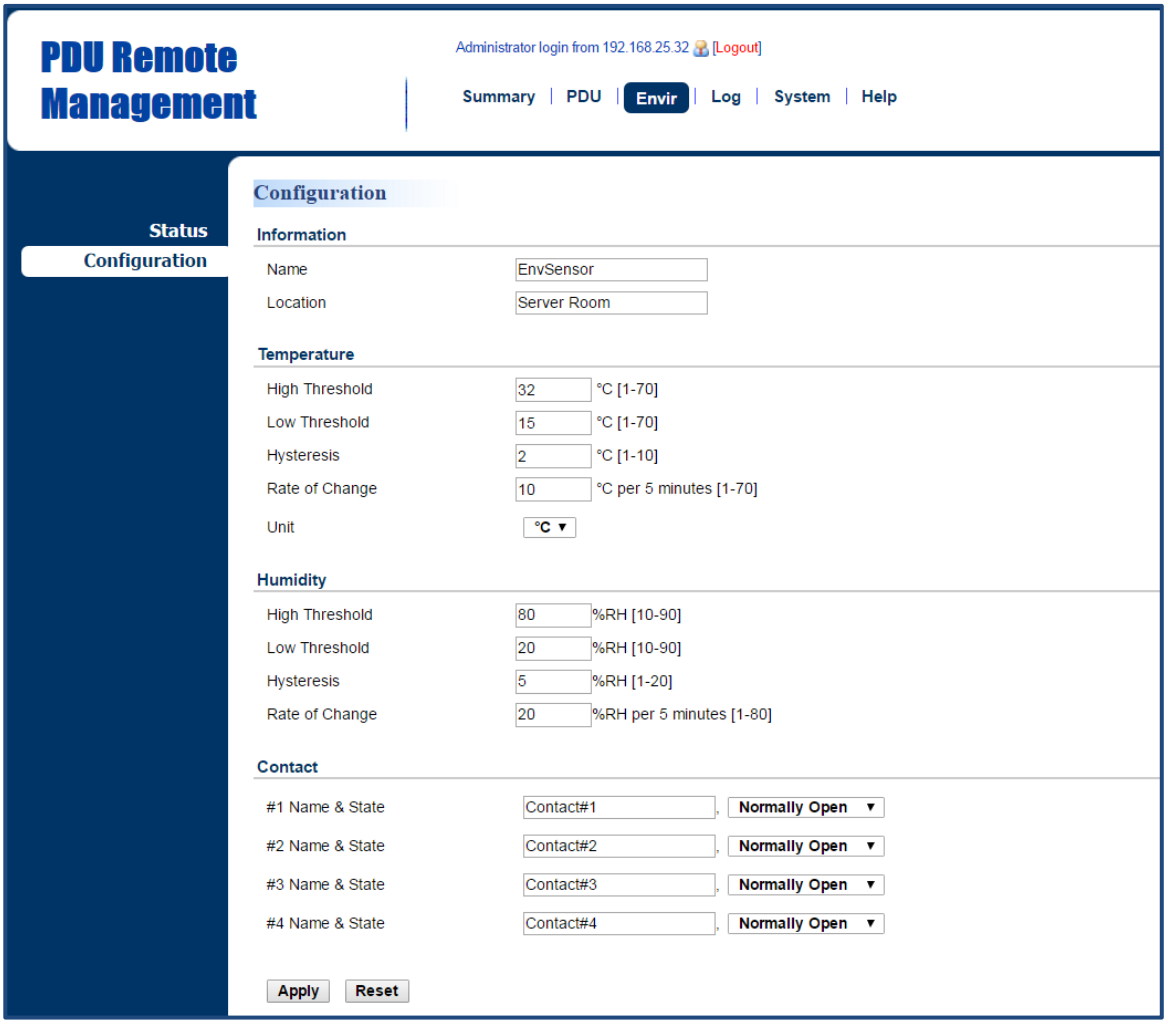
Envir Tab > Status



Item	Definition
Information	Display the name and location of the ENVIROSENSOR.
Temperature	
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 **Reset** to reset the highest and lowest value to zero.
Humidity	

Item	Definition
Current Value	The real-time reading of humidity.
Maximum	The highest humidity recorded and the time of occurrence.
Minimum	The lowest humidity recorded and the time of occurrence. Click **Reset** to reset the highest and lowest value to zero.
Contact	Display the current status of each input dry contact relay.

Envir Tab > Configuration



Item	Definition
Information	
Name	The name entered by user to identify the ENVIROSENSOR.
Location	The location of the ENVIROSENSOR, entered by the user.
Temperature	

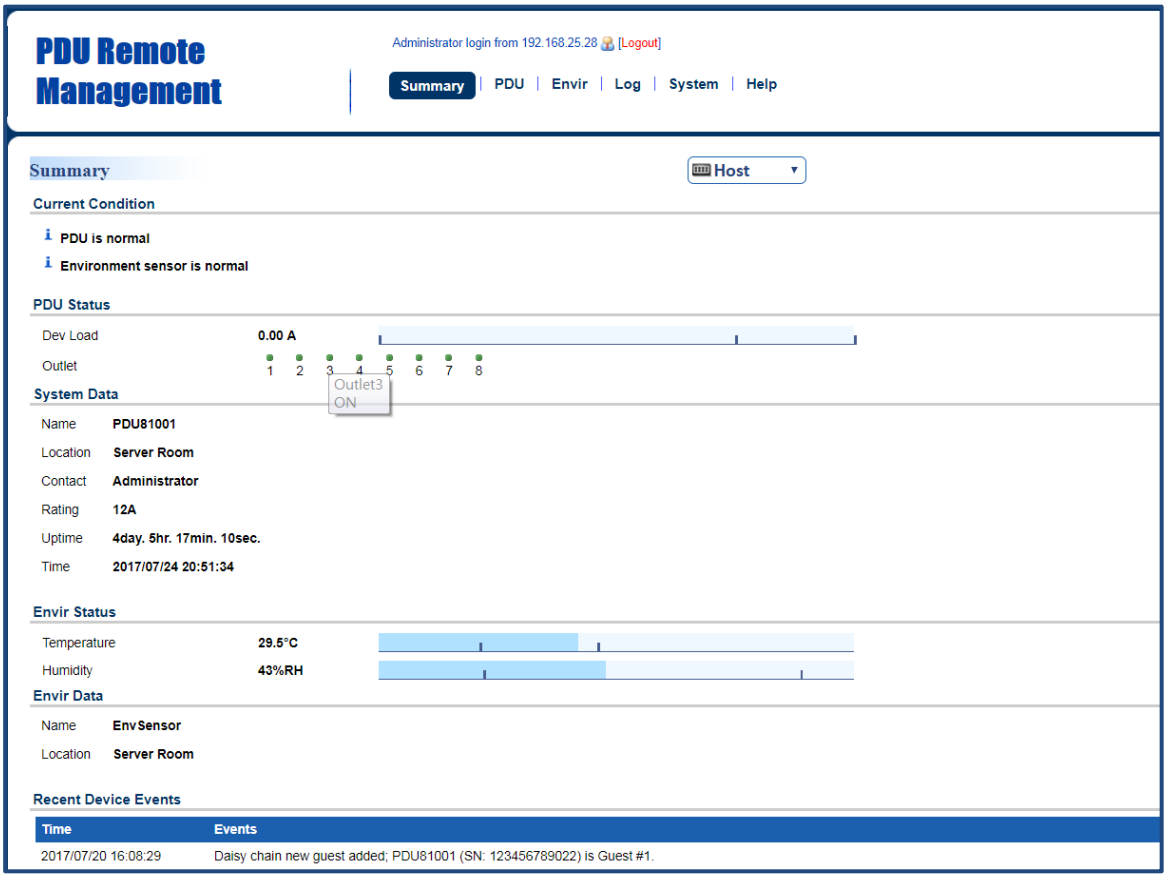
Item	Definition
High Threshold	Set the highest temperature value for a high temperature warning.
Low Threshold	Set the lowest temperature value for a low temperature warning.
Hysteresis	The point where the environmental state changes from abnormal to normal and users receive a clearing event notification. The function of Hysteresis is to avoid receiving multiple event notifications. *For high threshold, the point is the threshold minus the Hysteresis value; for low threshold, the point is the threshold plus the Hysteresis value. 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.
Rate of Change	Define the abnormal change of temperature per 5 minutes. 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.
Unit	Select the unit of temperature.
Humidity	
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 *Hysteresis* under temperature.
Rate of Change	Same as *Hysteresis* under temperature.
Contact	Enter the name of each input dry contact relay and use the dropdown menu to define the normal status of each one.

2. Advanced Power Management

2.1 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**.

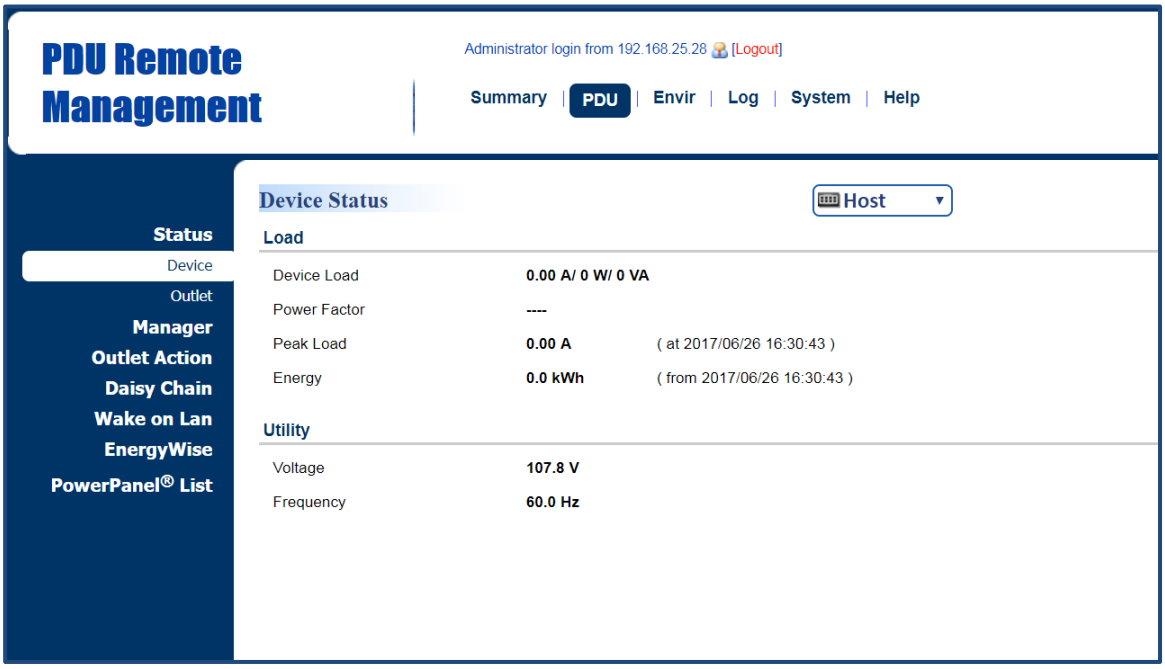
Summary Tab



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.
PDU Status	
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

Item	Definition
	when the outlet turns off. Outlet Tooltip Function: move the cursor to an individual outlet, Outlet name and its ON/OFF status will be shown.
System Data	
Name	The name of the PDU. For configuration, see System Tab > General > Identification.
Location	The location of the PDU. For configuration, see System Tab > General > Identification.
Contact	The person accountable for the maintenance of the PDU. For configuration, see System Tab > General > Identification.
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 System Tab > General > Time.
Envir Status	
Temperature	Display temperature reading when the ENVIROSENSOR is connected to the PDU.
Humidity	Display humidity reading when the ENVIROSENSOR is connected to the PDU.
Envir Data	
Name	The name of the ENVIROSENSOR. For configuration, see Envir Tab > Configuration.
Location	The location of the ENVIROSENSOR. For configuration, see Envir Tab > Configuration.
Recent Device Events	A list of the five most recent device events. All events are related to configuration changes.

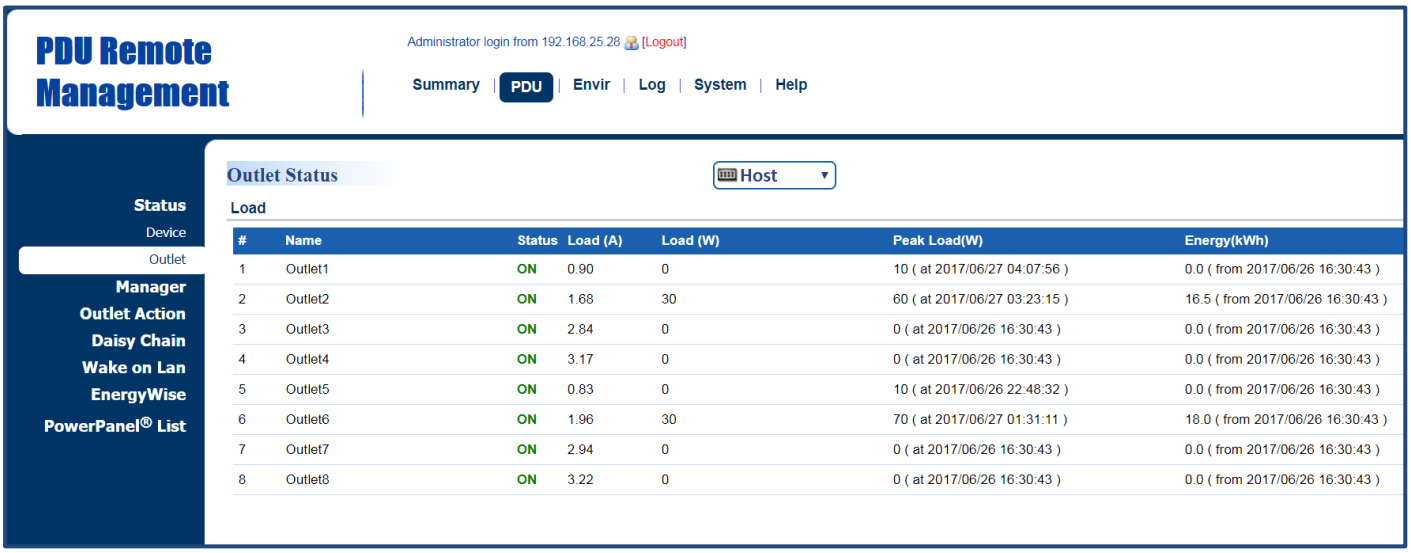
PDU Tab > Status > Device



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.
Load	
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 PDU Tab > Manager > Device.
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 PDU Tab > Manager > Device.
Utility	
Voltage	Voltage of the utility power.
Frequency	Frequency of the utility power.

*Only available in select models.

PDU Tab > Status > Outlet*



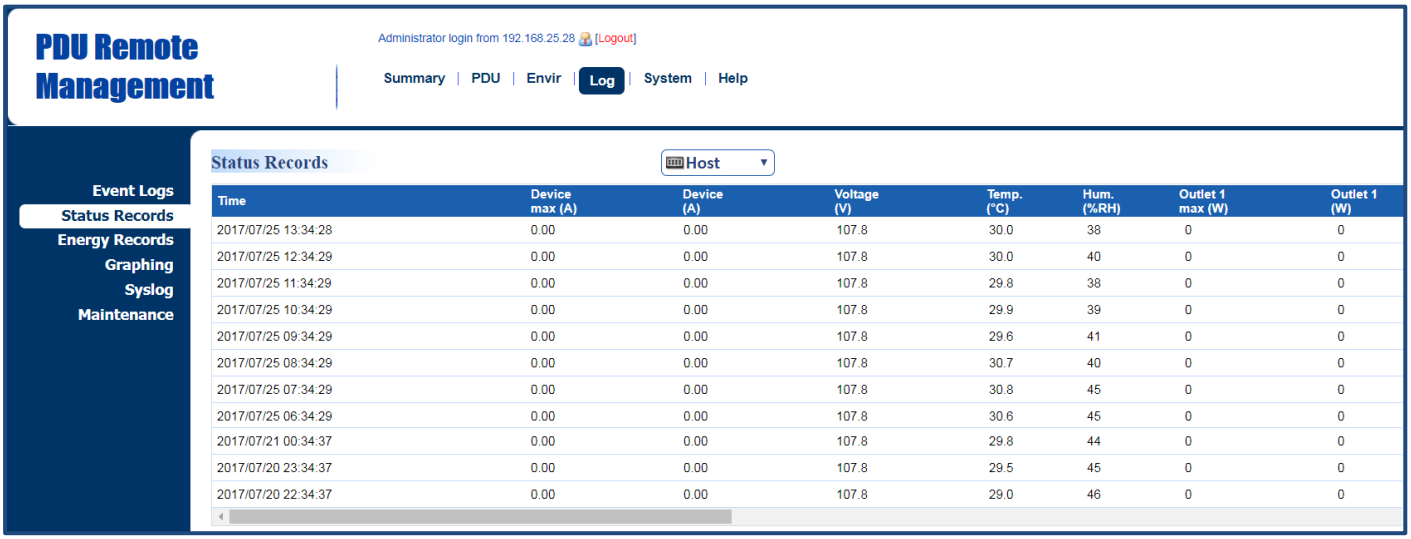
*The above **Outlet Status Page** is available for Switched Metered by Outlet Series only.

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 PDU Tab > Manager > Outlet.
Energy (kWh)	Total energy consumed by connected equipment of each outlet since the last reset. The reset can be set in PDU Tab > Manager > Outlet.

2.2 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

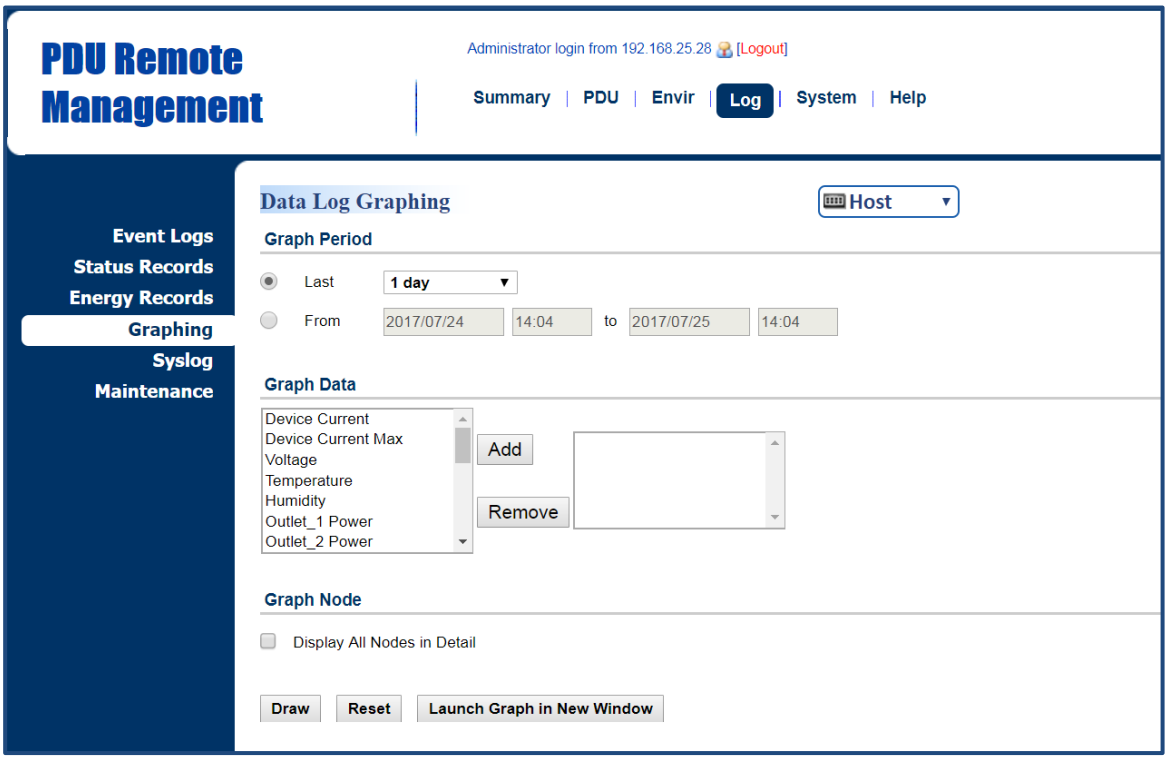


Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Device Max (A)	The maximum load current of the connected device(s) or bank during a specific time interval, measured in Amps. This interval can be set in Log Tab > Maintenance.
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 Log Tab > Maintenance.

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.
Outlet # (kW)*	Load power of a specific outlet, measured in Kilowatts.

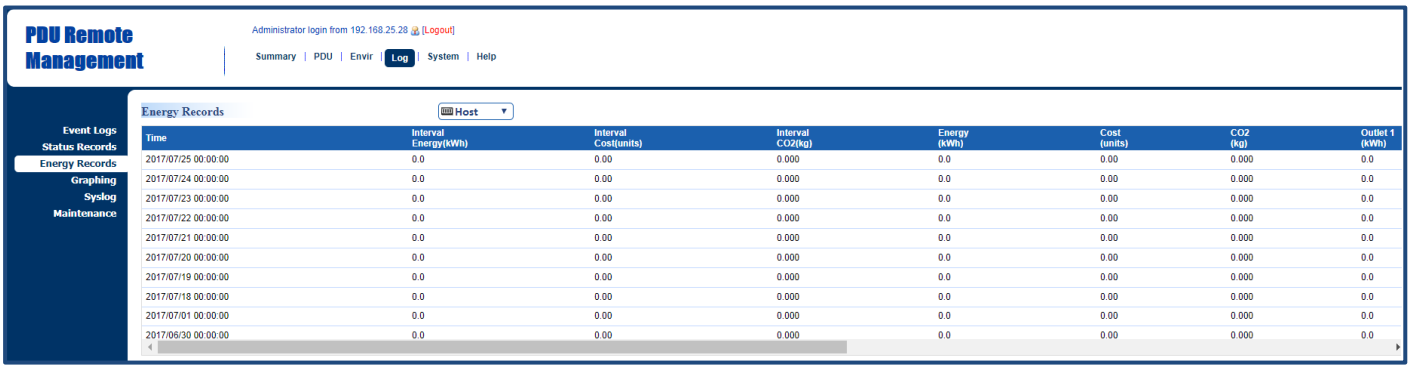
*For Switched Metered by Outlet Series only.

Log Tab > 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 **Display All Nodes in Detail** 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 *Graph Period* to default (1 day).
Launch Graph in New Window	A detailed view of the graph opens in a new browser window.

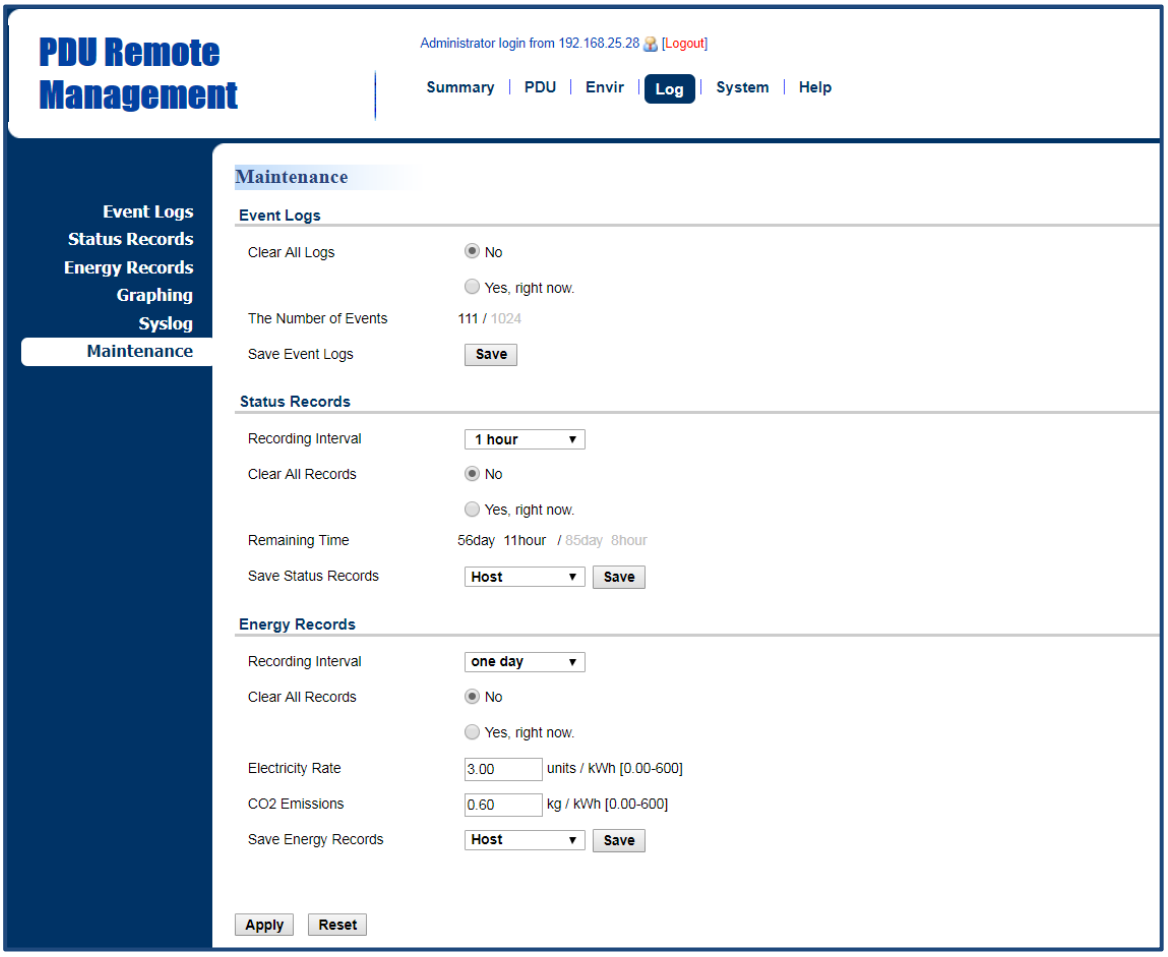
Log Tab > Energy Records



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 Log Tab > Maintenance.
Interval Cost (units)	Cost of the energy consumed by the connected device(s) during a specific time interval, equal to *Electricity Rate* multiplied by *Interval Energy*. The interval and electricity rate can be set in Log Tab > Maintenance.
Interval CO2 (kg)	Equivalent CO2 emission of the connected device(s) during a specific time interval, equal to *CO2 Emissions* multiplied by *Interval Energy*. The interval and CO2 emissions can be set in Log Tab > Maintenance.
Energy (kWh)	Accumulated *Interval Energy* since the last reset. The reset can be set in Log Tab > Maintenance.
Cost (units)	Accumulated *Interval Cost* since the last reset. The reset can be set in Log Tab > Maintenance.
CO2 (kg)	Accumulated *Interval CO2* since the last reset. The reset can be set in Log Tab > Maintenance.
Outlet # (kWh)*	Accumulated *Interval Energy* of a specific outlet since the last reset. The reset can be set in Log Tab > Maintenance.

*For Switched Metered by Outlet Series only.

Log Tab > Maintenance



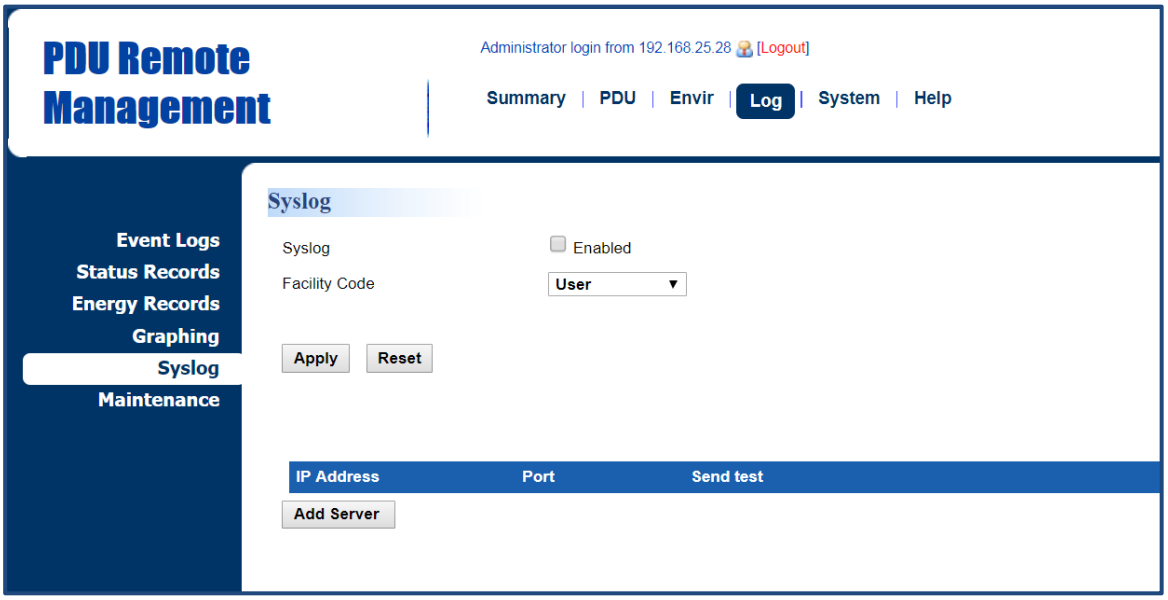
Item	Definition
Event Logs	
Clear All Logs	Clear the existing event logs.
The Number of Events	The number of the existing event logs and the maximum number of the event logs that can be recorded. Once the maximum number is reached, new events overwrite oldest events in memory.
Save Event Logs	Save the existing event logs as a text file.
Status Records	
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.

Item	Definition
Clear All Records	Clear the existing status records.
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.
Energy Records	
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.

2.3 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

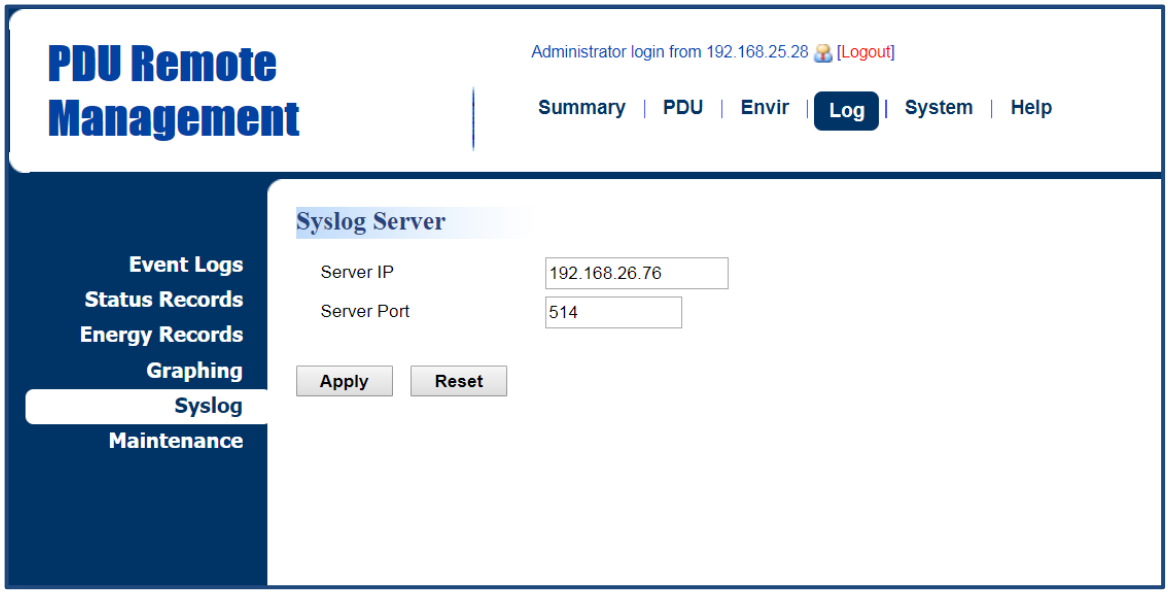
Log Tab > Syslog



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

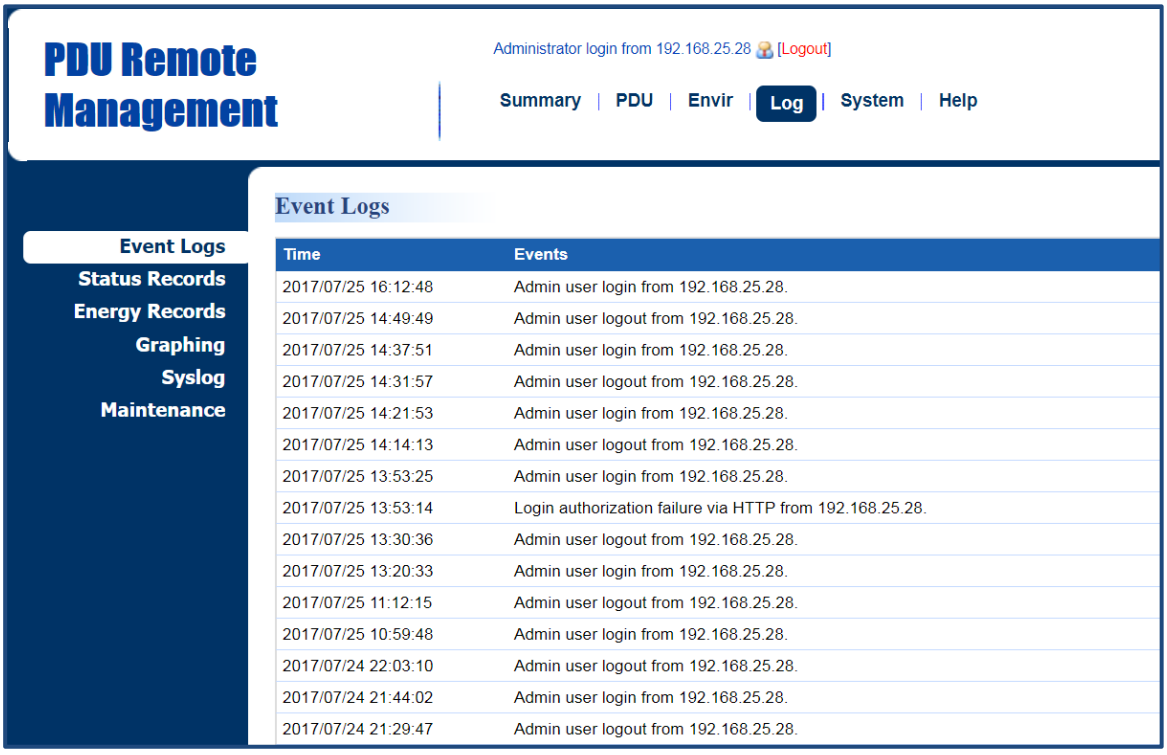
Click **Add Server** to enter **Syslog Server Page**.

Syslog Server Page



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

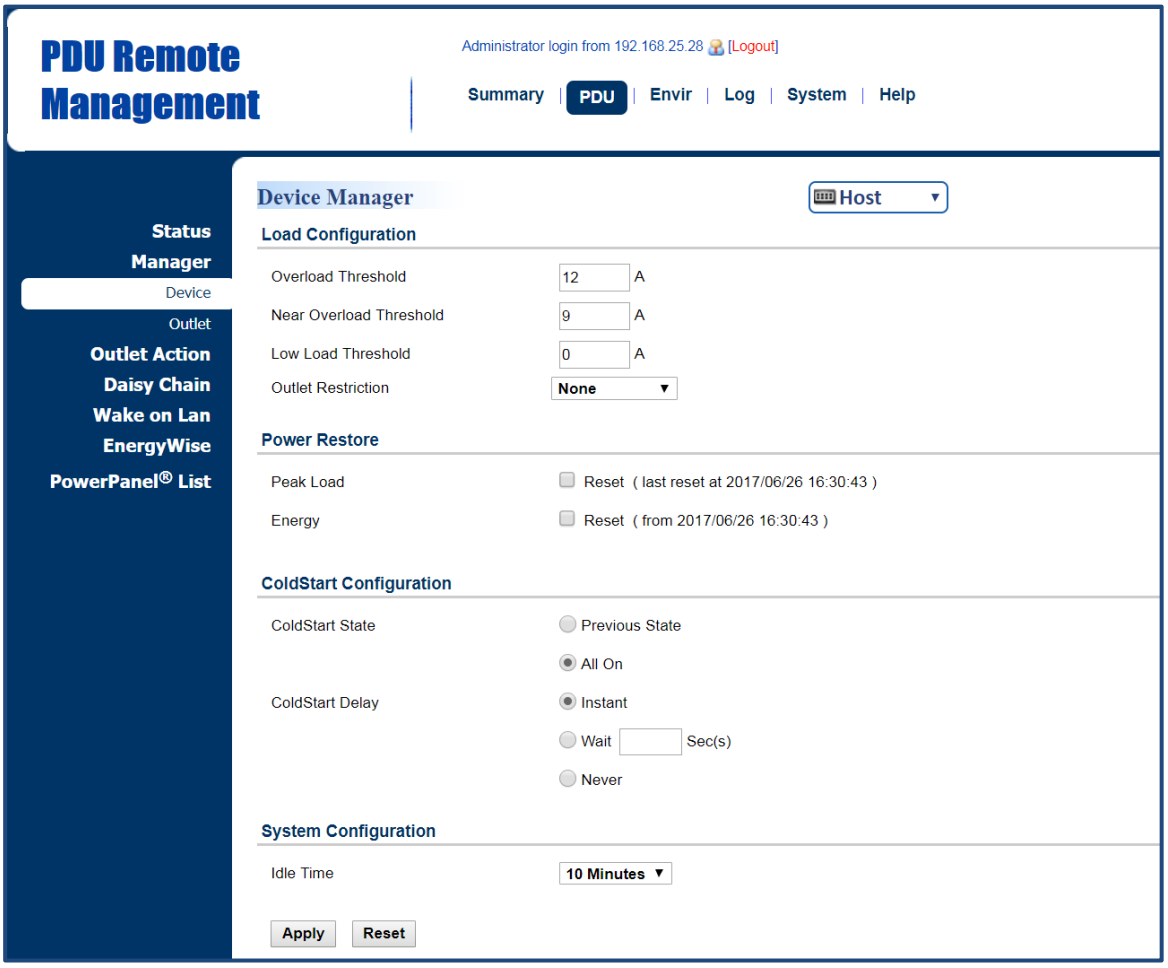
Logs Tab > Event Logs



2.4 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.
Load Configuration	
Overload Threshold	Set the value for the total current on the PDU that will signal an overload warning. Must be higher than *Near Overload Threshold* and equal to or lower than the PDU *Rating* in the Summary Tab.

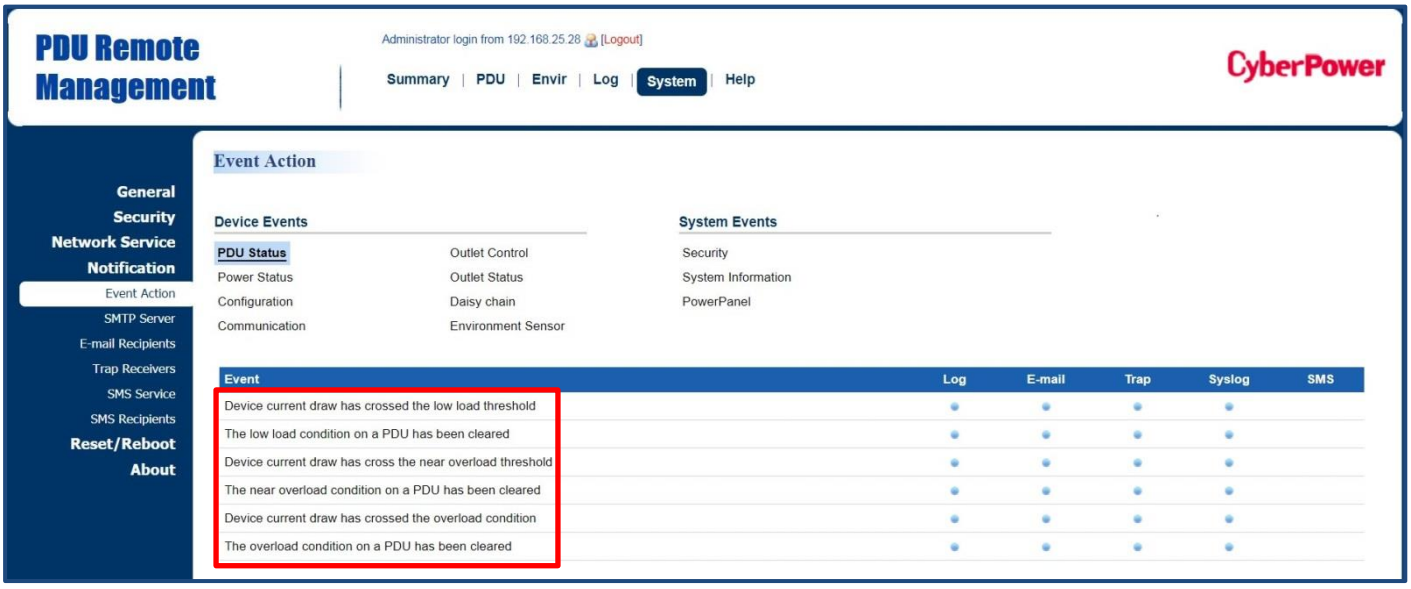
Item	Definition
Near Overload Threshold	Set the value for the total current on the PDU that will signal a near overload warning. Must be between *Overload Threshold* and *Low Load Threshold*.
Low Load Threshold	Set the value for the total current on the PDU that will signal a low load warning. Must be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

2.5 Event Action Notification

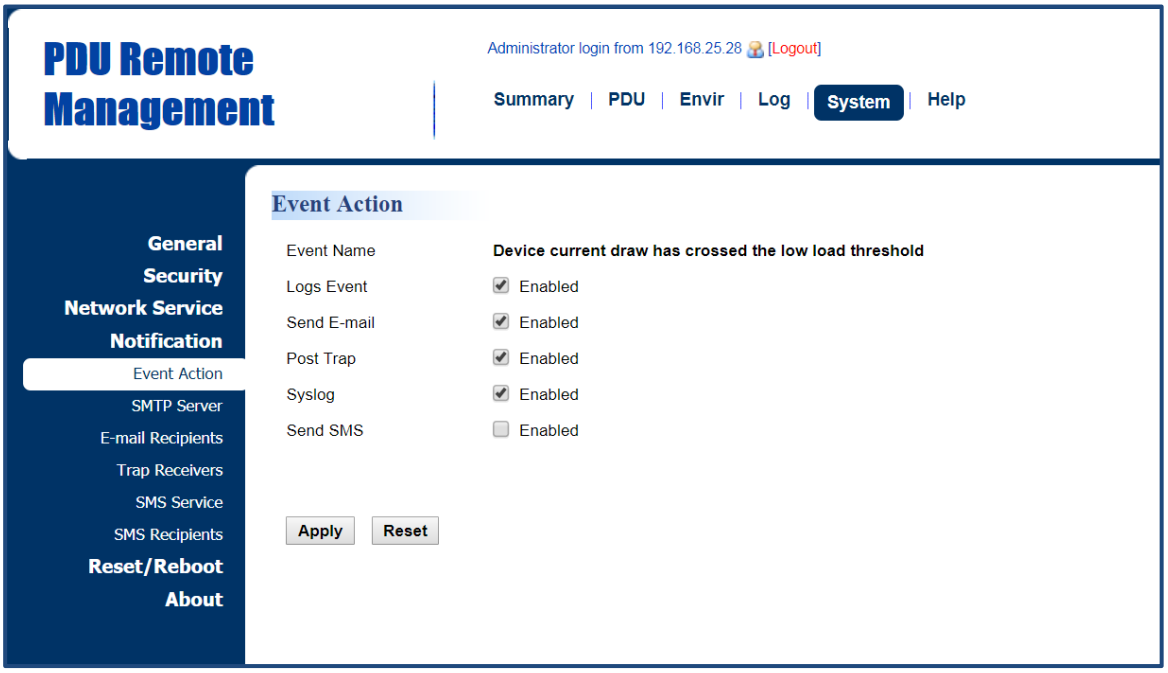
Users decide the event actions for which they receive notifications. When a certain event happens, an automatic notification will be sent to users so that they can make timely decisions to prevent potential problems. See **System Tab > Notification**.

System Tab > Notification > Event Action



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 *Event Logs*.
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.

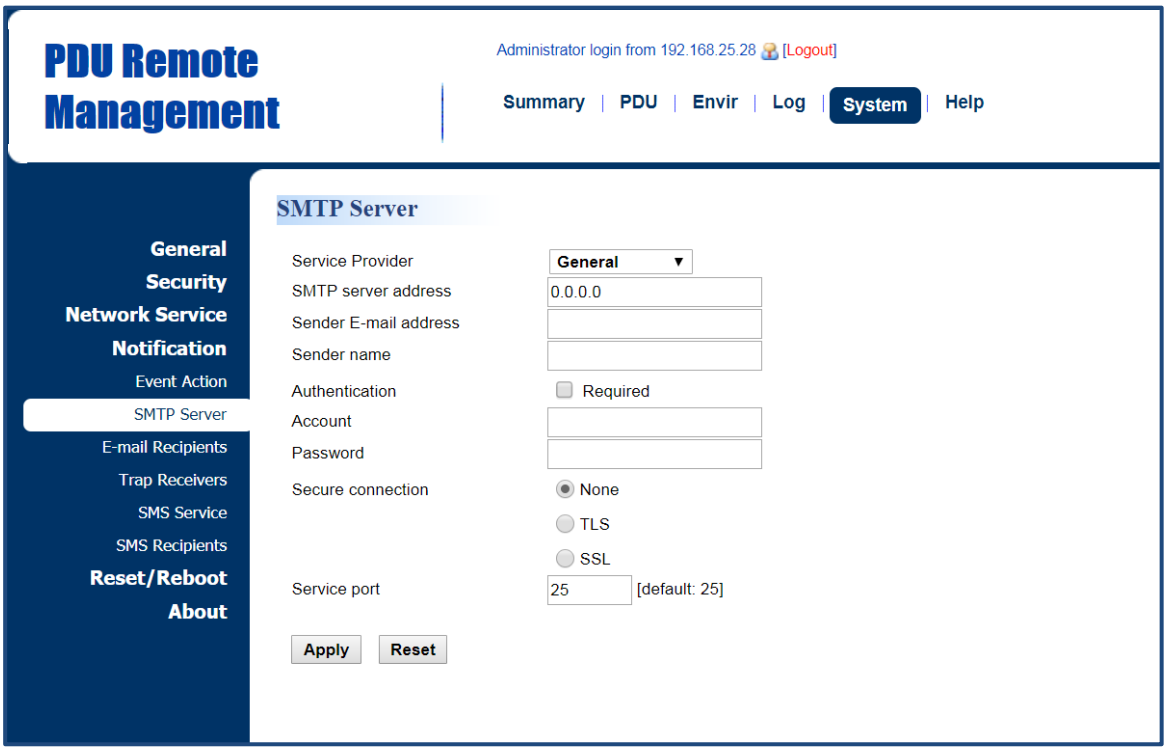
2.5.1 Event Action Recipient Settings

The following provides e-mail receiver configurations.

2.5.1.1 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

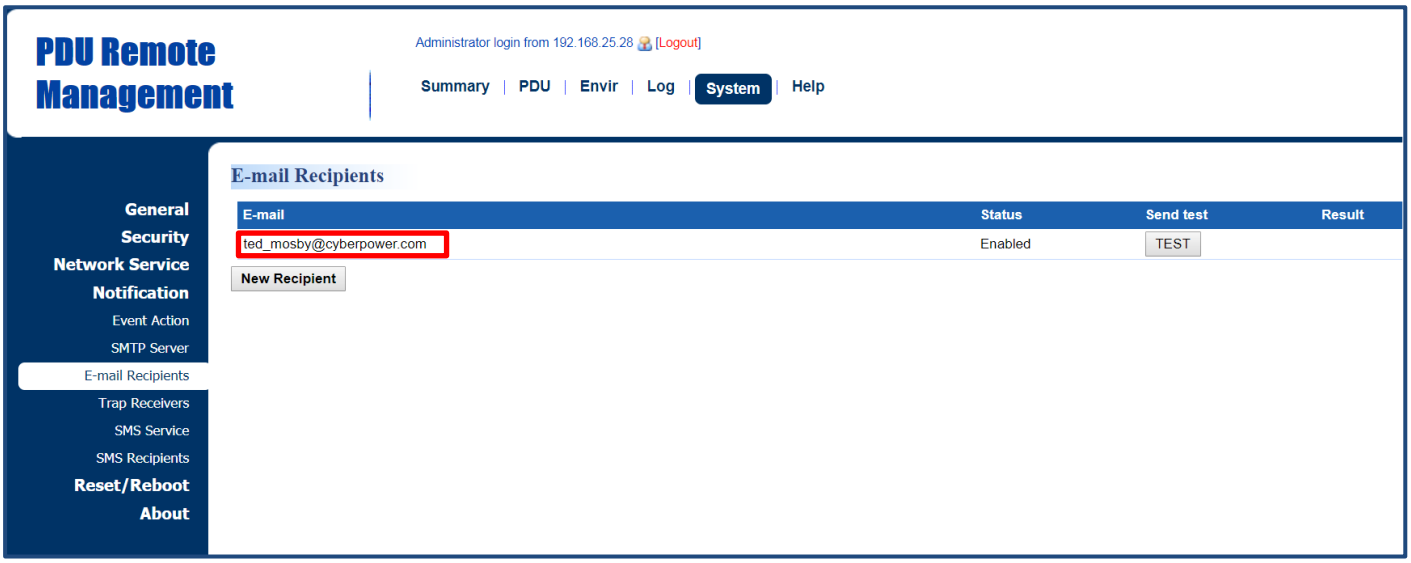


Item	Definition
Service Provider	The service provider of e-mail account. There are two options: Other and Gmail.
Other	Select other as service provider. Complete all field settings and click **Apply** to save.
Gmail	Select Gmail as the service provider. Click **Authorize** for an authorization to send a mail notification. Then complete the sender name and click **Apply** 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.

Item	Definition
Authentication	Select this option if the SMTP server requires Authentication.
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.

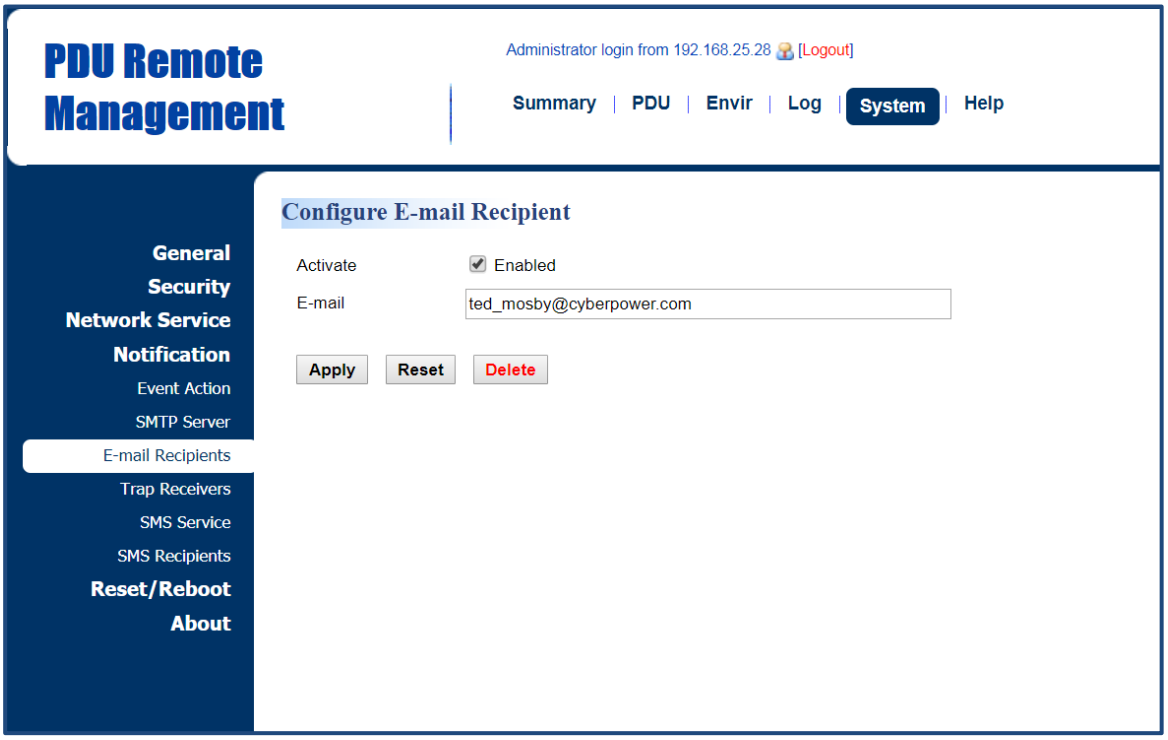
Users can set up to five e-mail recipients in designated email address format. See **System > Notification >E-mail Recipients**.

System > Notification > E-mail Recipients

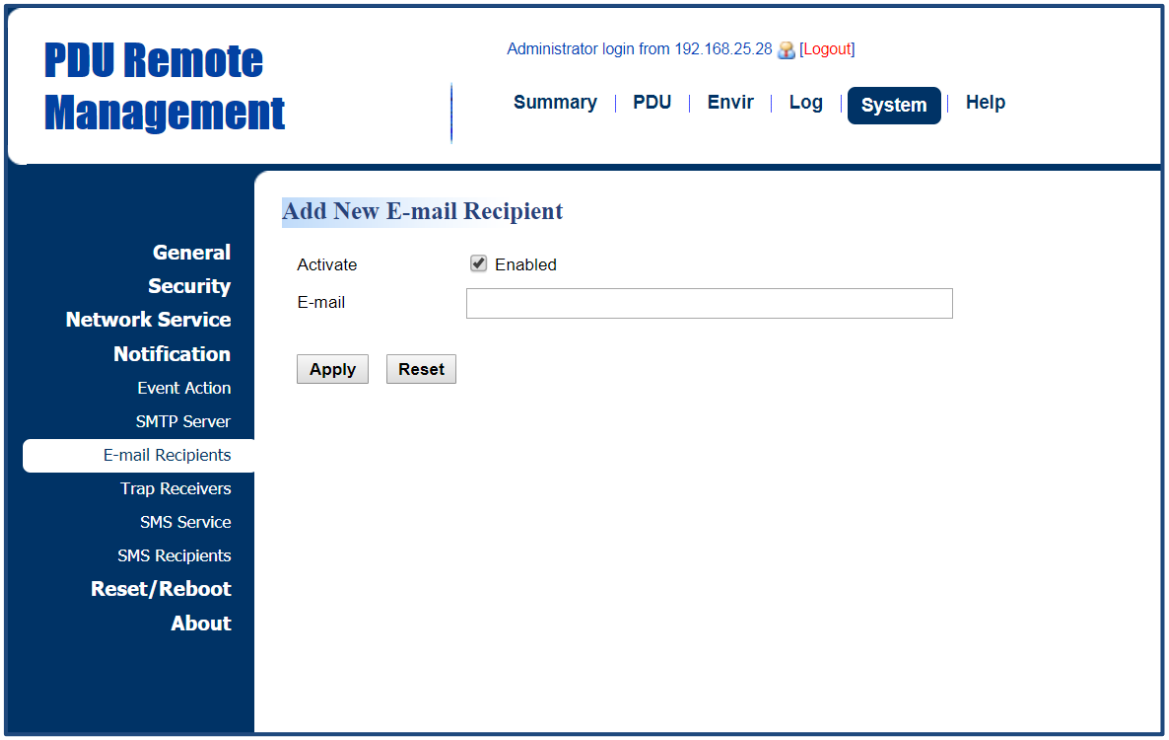


Item	Definition
E-mail	Click the e-mail address of the recipient to enter the **Configure E-mail Recipient Page**. Users can modify the e-mail address, change its status, check test result, and delete an existing recipient.
TEST	Click this button to check if the SMTP setting and the email recipients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

Configure E-mail Recipient Page



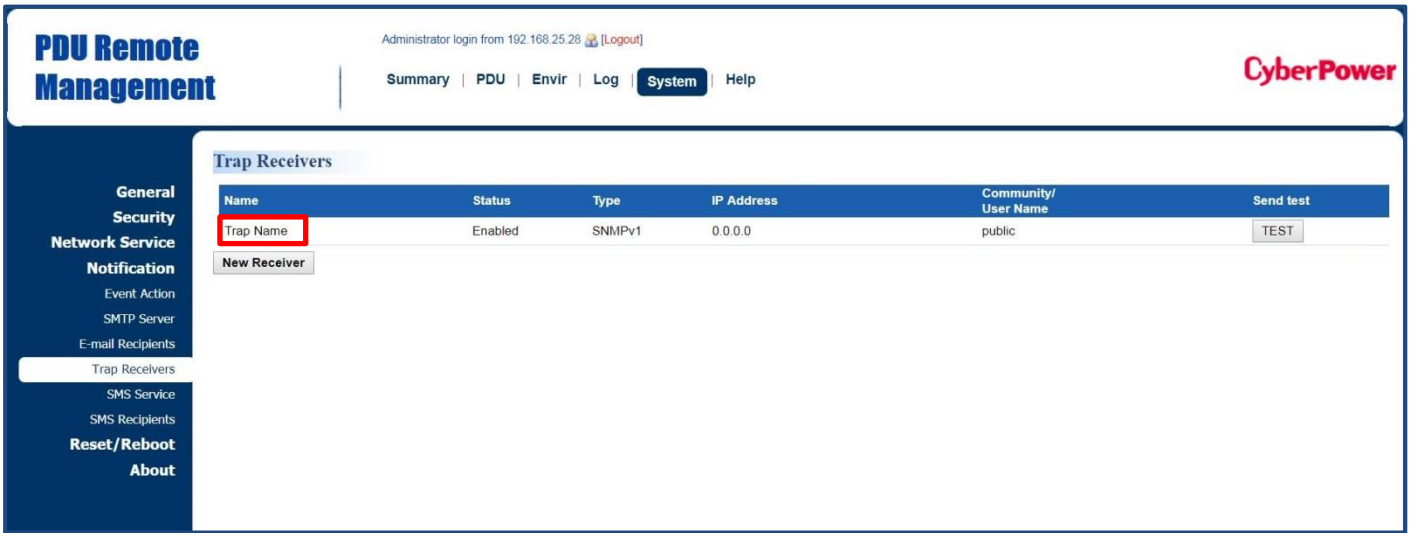
Add New E-mail Recipient Page



2.5.1.2 SNMP Trap Notification

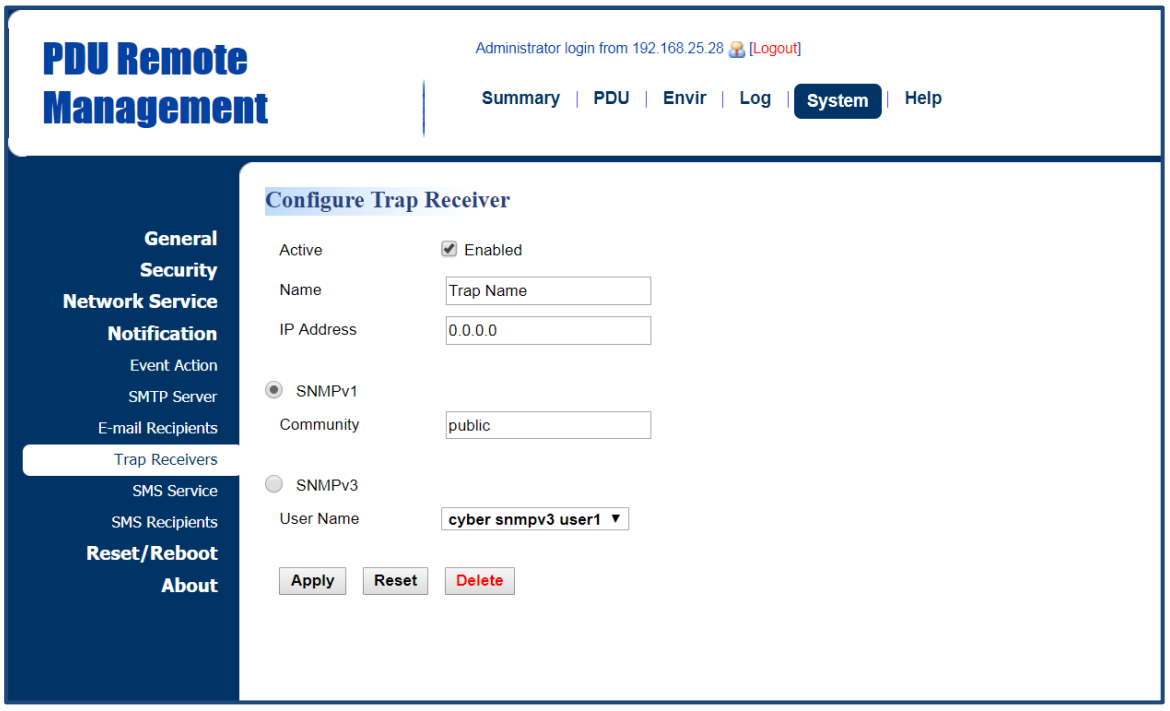
Set up to 10 SNMP trap receivers to be notified when an event occurs. See **System > Notification > Trap Receivers**.

System > Notification > Trap Receivers

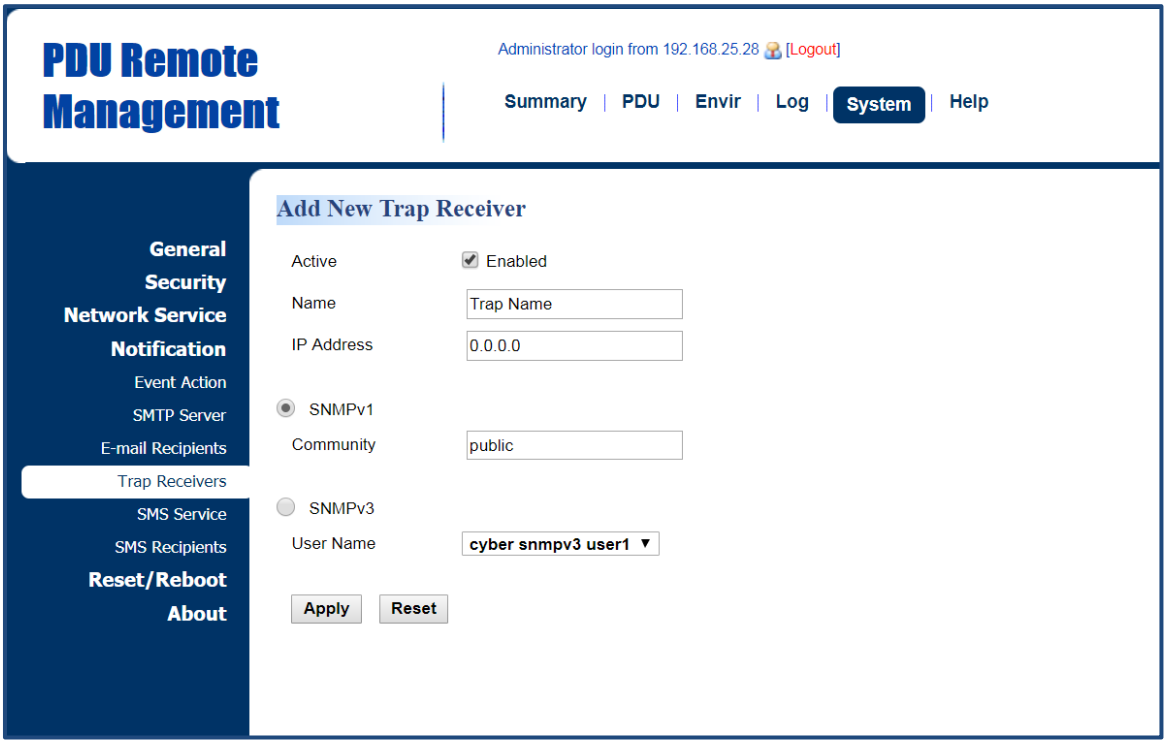


Item	Definition
Name	Click on the trap name to enter the **Configure Trap Receiver Page**. Users can modify or delete an existing receiver.
TEST	Click this button to check if the trap can be sent.
New Receiver	Click this button to enter the **Add New Trap Receiver Page**. Users can add a new recipient.

Configure Trap Receiver Page



Add New Trap Receiver Page

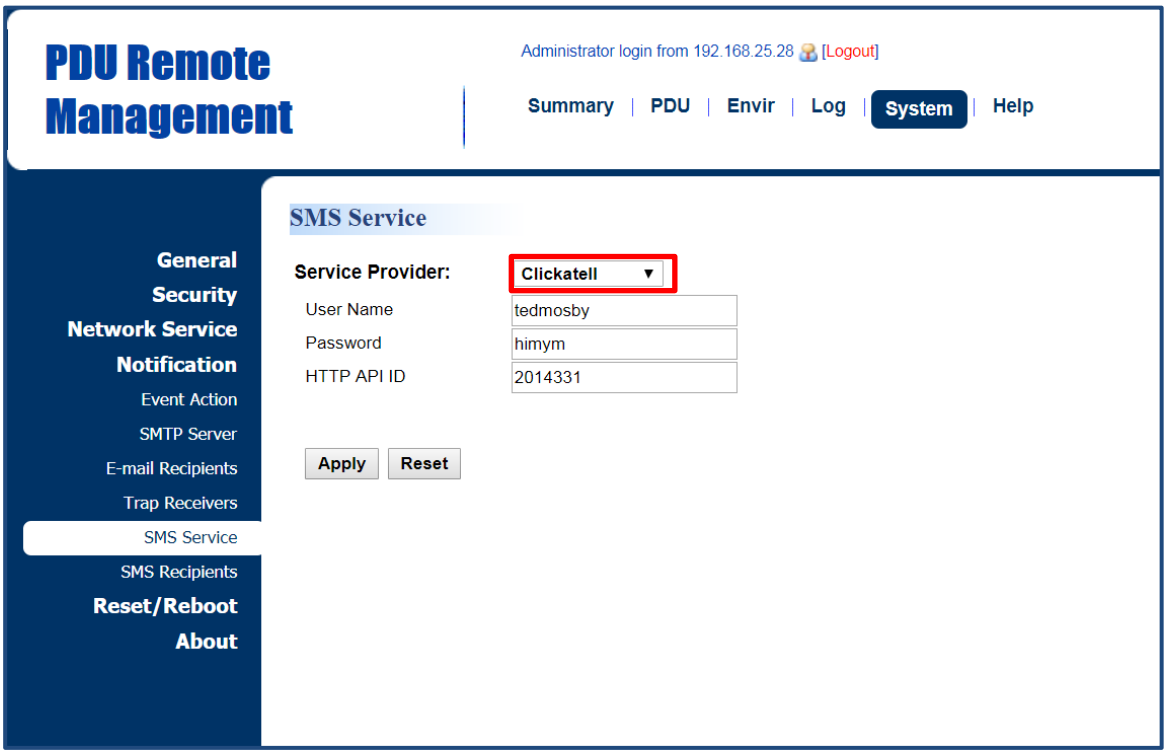


Item	Definition
Name	The name of trap receiver.
IP Address	The IP address of the trap receiver.
SNMPv1	If choosing the **SNMPv1** option as the trap type for a trap receiver, select the corresponding community. See System Tab > Network Service > SNMPv1 Service.
SNMPv3	If choosing the **SNMPv3** option as the trap type for a trap receiver, select the corresponding user name. See System Tab > Network Service > SNMPv3 Service.

2.5.1.3 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

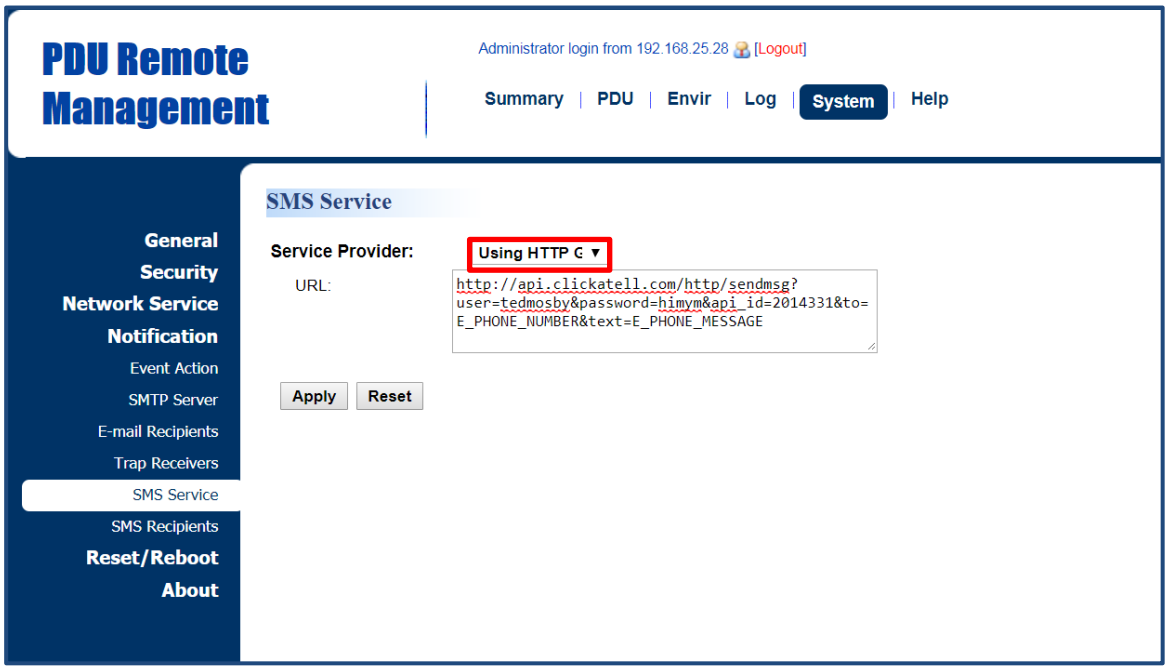


Clickatell method:

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:

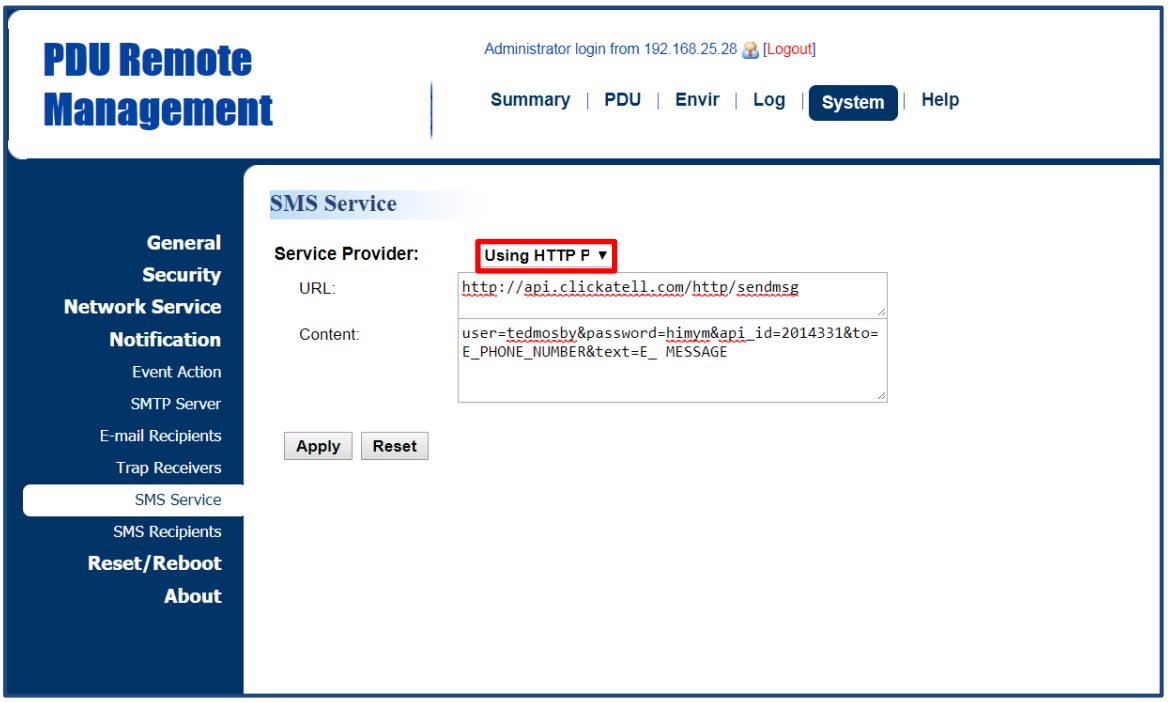
Use the example where Clickatell is the SMS provider.

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 System Tab > Notification > SMS Recipients.
text=E _MESSAGE	Do not replace this information. It refers to the event action sent by the SMS service provider. For configurations, see System Tab > Notification > Event Action.

System > Notification > SMS Service



Using HTTP POST:

Use the example where Clickatell is the SMS provider.

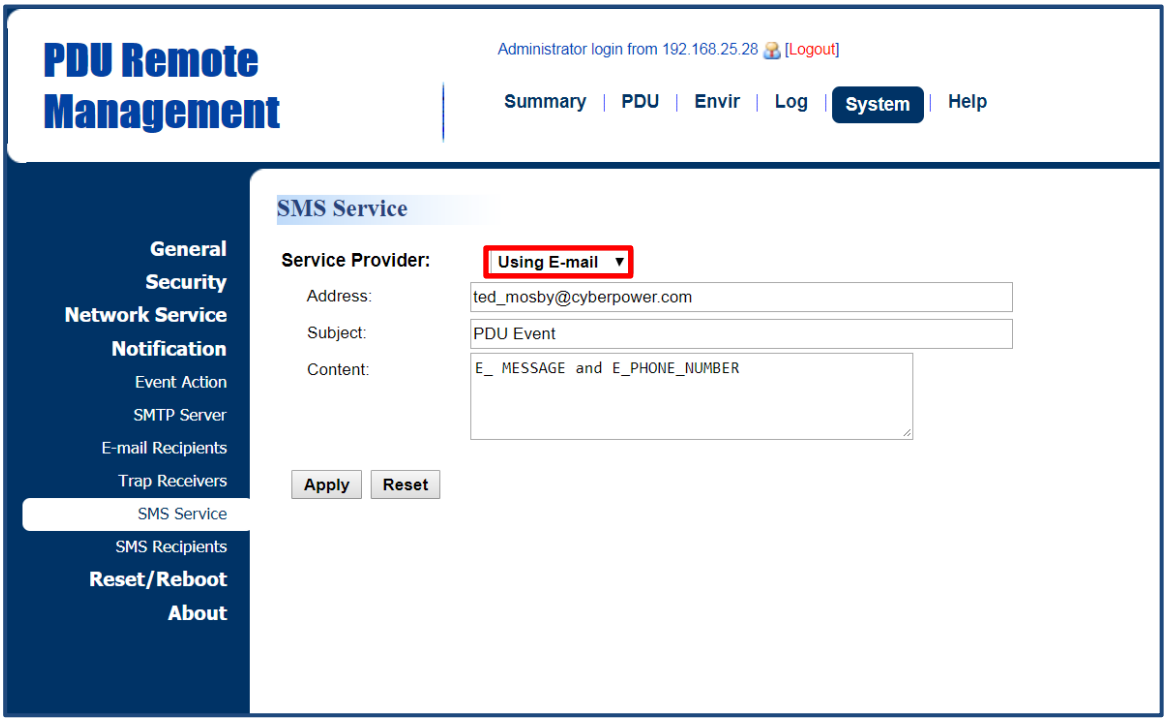
The basic form of URL is: http://api.clickatell.com/http/sendmsg

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 System Tab > Notification > SMS Recipients.
text=E_ MESSAGE	Do not replace this information. It refers to the event action sent by SMS service provider. For configurations, see System Tab > Notification > Event Action.

System > Notification > SMS Service



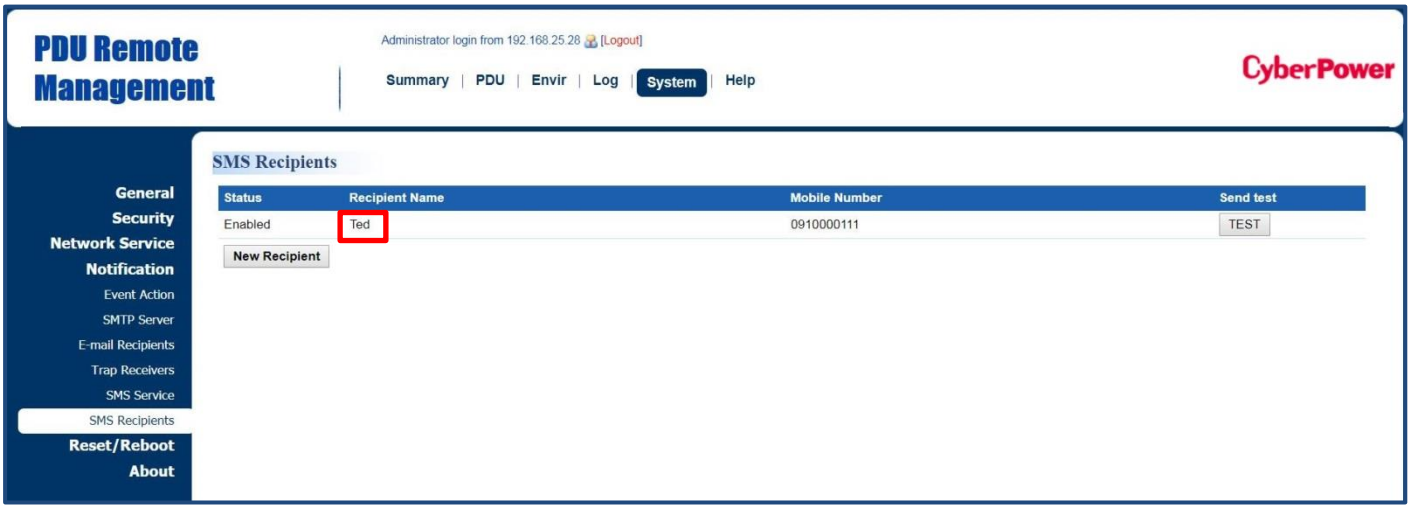
Using Mail:

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 System Tab > Notification > Event Action.
E_PHONE_NUMBER	Do not replace this information. It refers to the receiver phone number entered in System Tab > Notification > SMS Recipients.

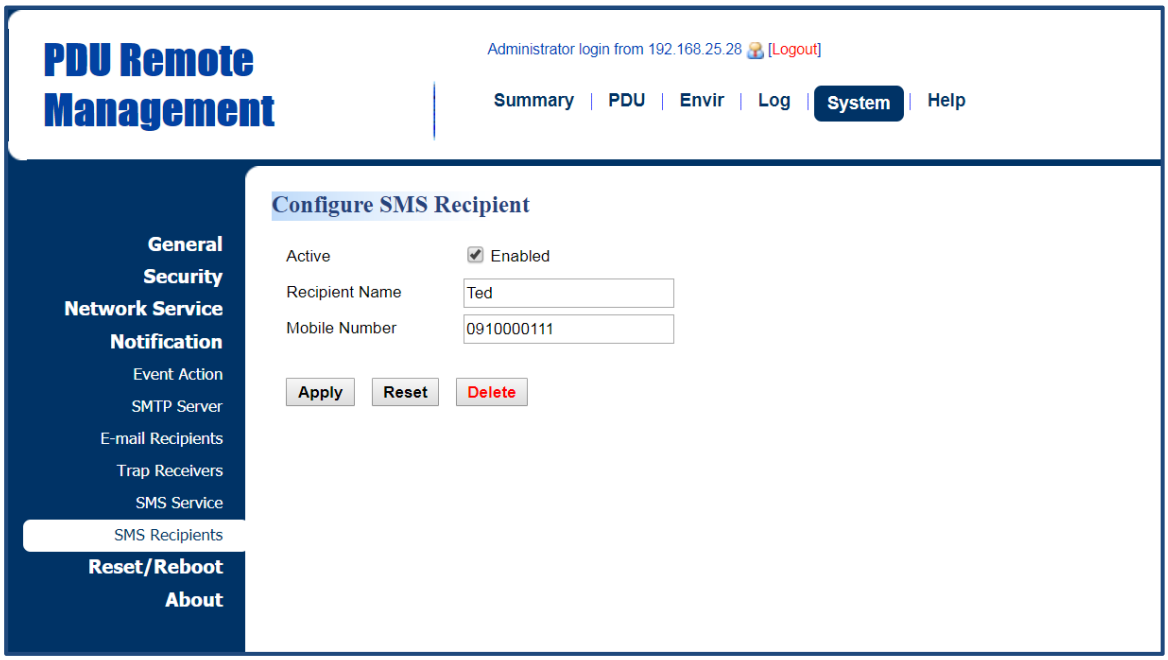
Users can set up to 10 mobile phone numbers as SMS recipients who will receive a short message notification when a specific event occurs. See **System Tab > Notification > SMS Recipients**.

System Tab > Notification > SMS Recipients

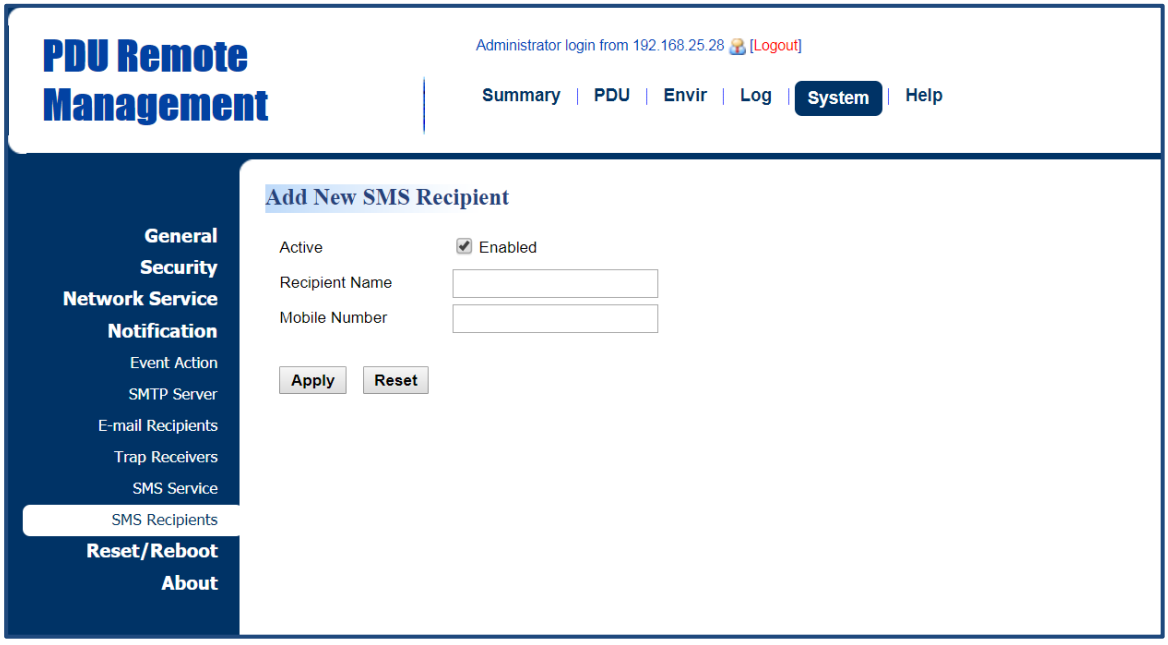


Item	Definition
Recipient Name	Click the name of the recipient to open the **Configure SMS Receiver Page**. Users can modify or delete an existing receiver.
TEST	Click this button to check whether the test message is correctly sent.
New Recipient	Click this button to open the **Add New SMS Receiver Page**.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

Configure SMS Receiver Page



Add New SMS Receiver Page



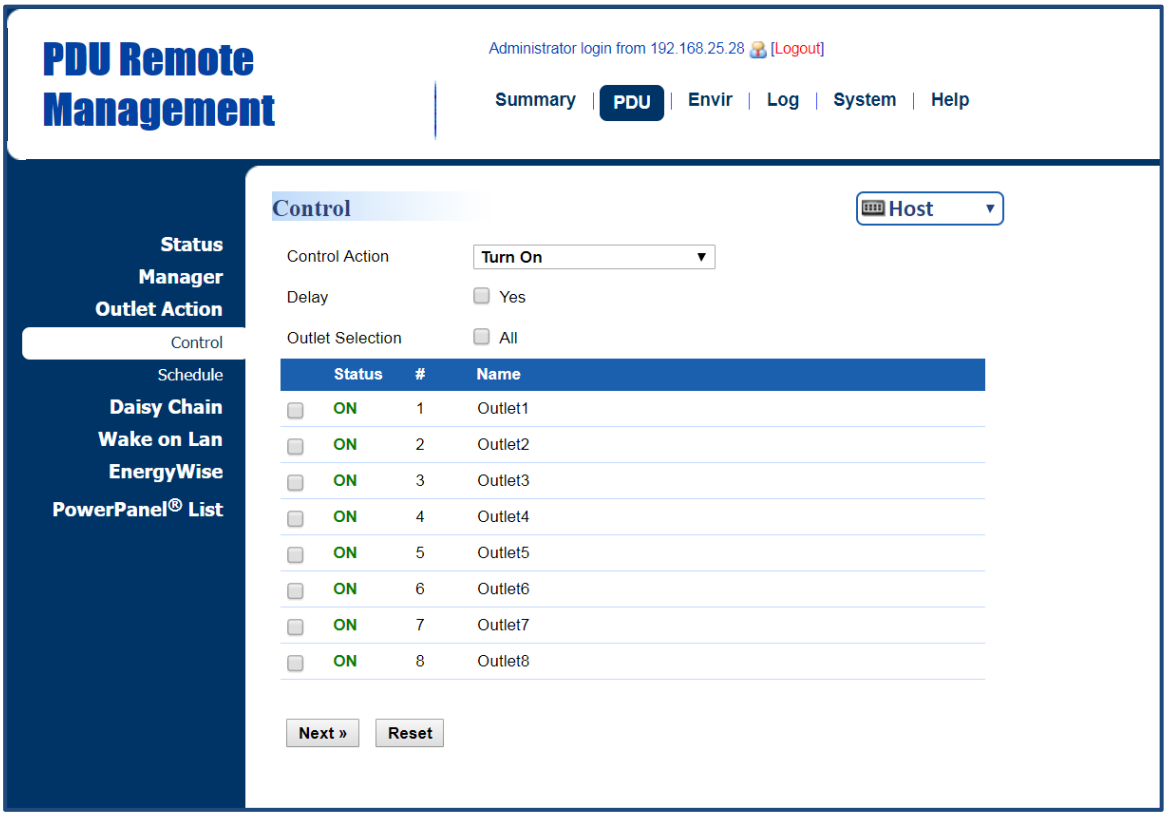
3. Outlet Management

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

3.1 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



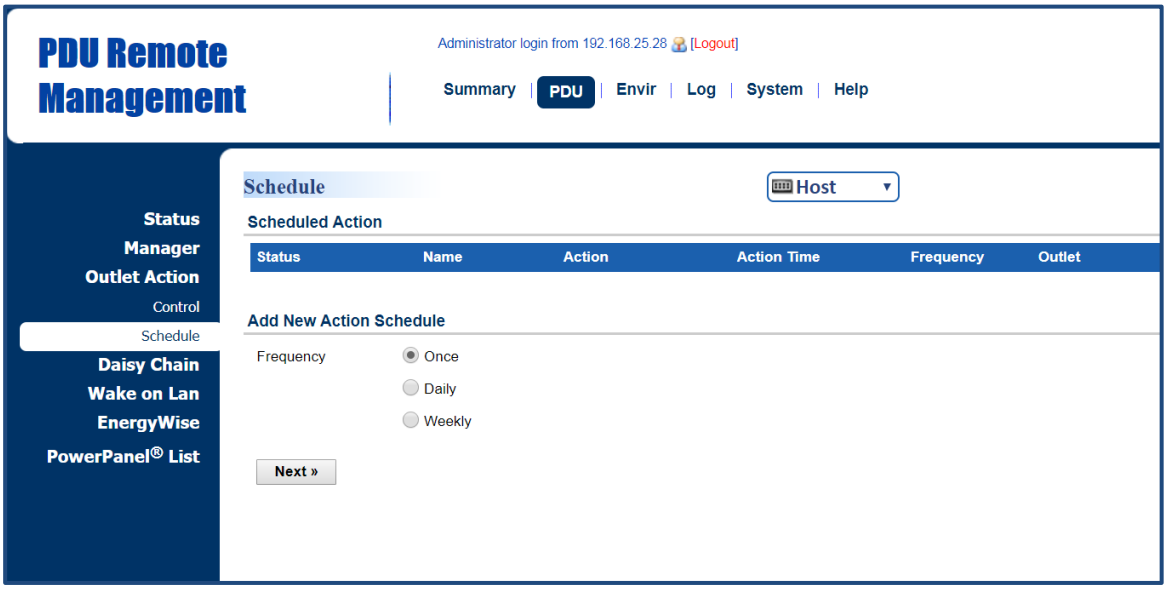
Item	Definition
HOST/GUEST#	Select the role of PDU (HOST or GUEST#) if PDUs are daisy chained. Up to 3 GUEST PDUs can connect to 1 HOST PDU.
Control Action	
Turn On	Selected outlets will be immediately turned on.
Turn On + Delay	Selected outlets will be turned on according to each outlet's *Power On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

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

3.2 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.)

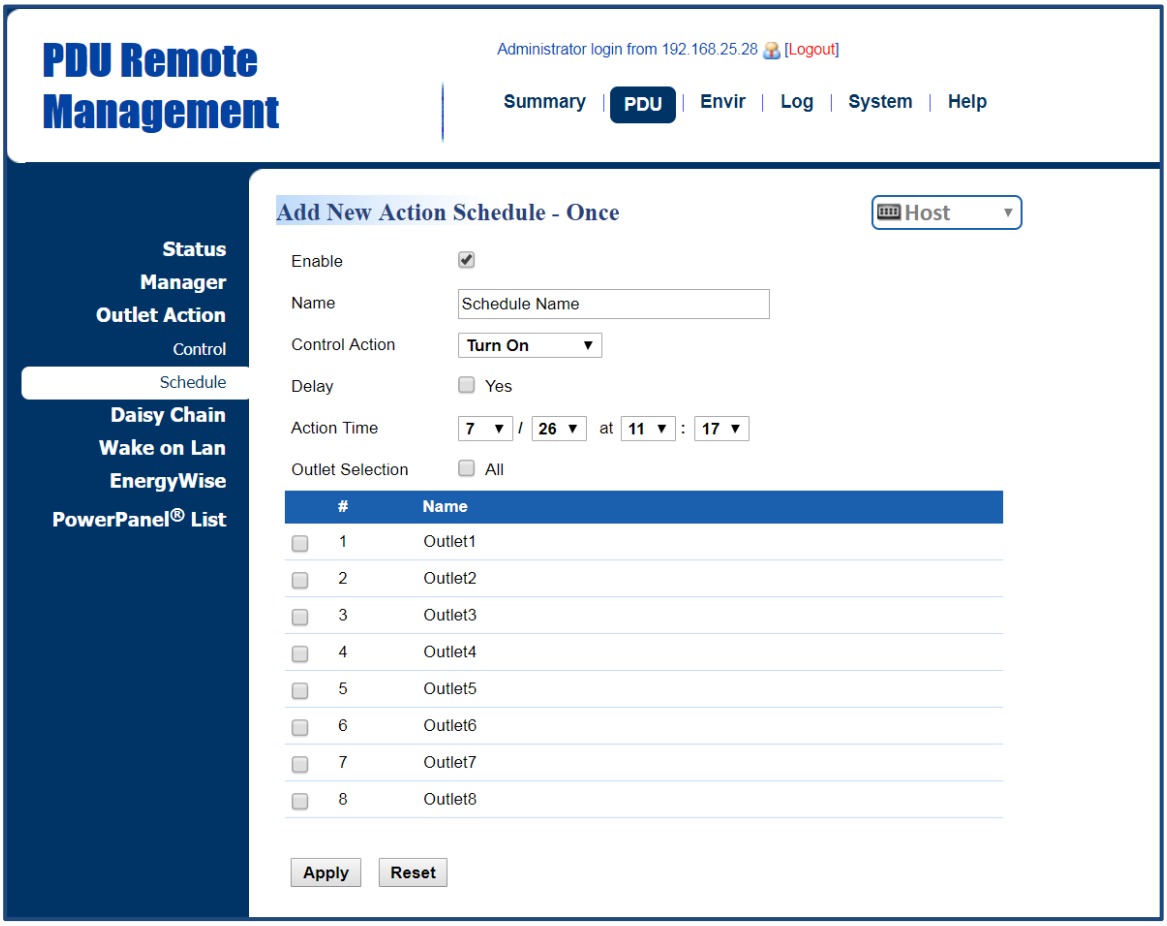
PDU Tab > Outlet Action > Schedule



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
Frequency	
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



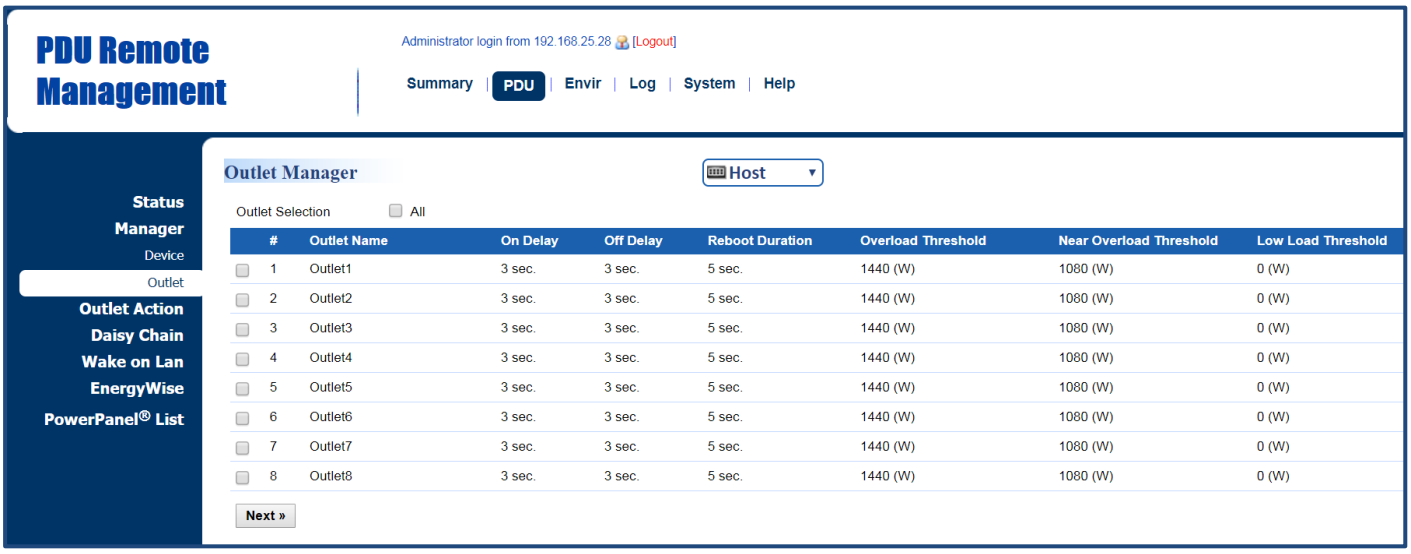
Up to 10 scheduled settings are allowed.

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 *Reboot Duration* in PDU Tab > Manager > Outlet. The duration is within 5 to 60 seconds.
Delay	Click this box to activate outlet delay function. For configurations, see PDU Tab > Manager > Outlet
Action Time	The time at which the scheduled event takes place.
Outlet Selection	Outlets selected for the scheduled event.

3.3 Sequencing Power On/Off

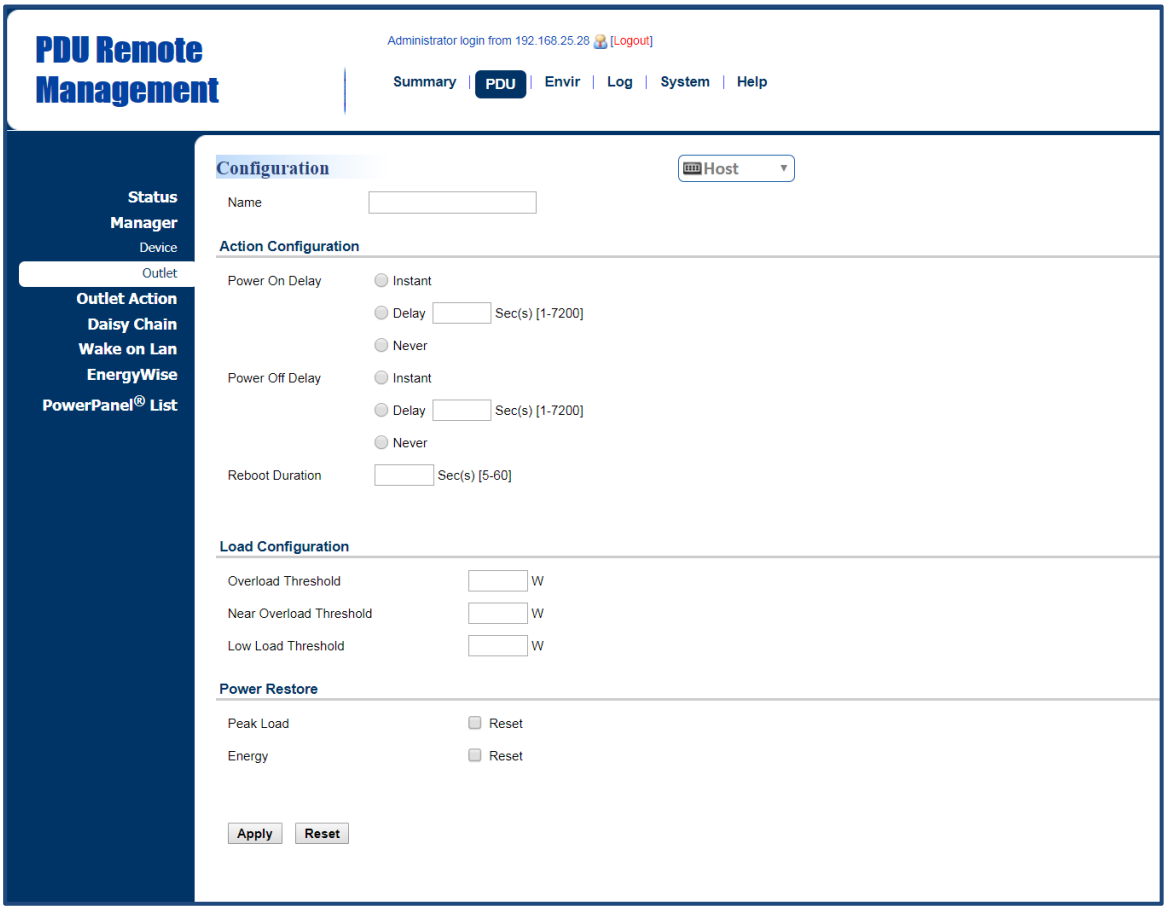
Enable users to turn on, turn off, or reboot the outlets in sequence. When powering on the connected devices, the sequential power-on method is recommended to avoid high inrush current. See **PDU Tab > Manager > Outlet**. (For Switched Metered by Outlet Series and Switched Series only.)

PDU Tab > Manager > Outlet



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



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

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

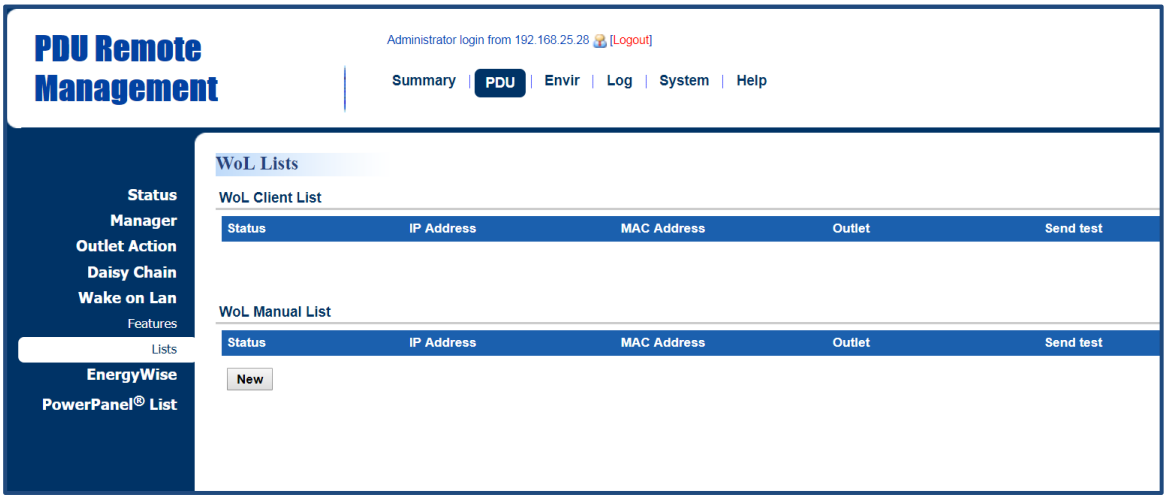
3.4 Wake on LAN (WoL)

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

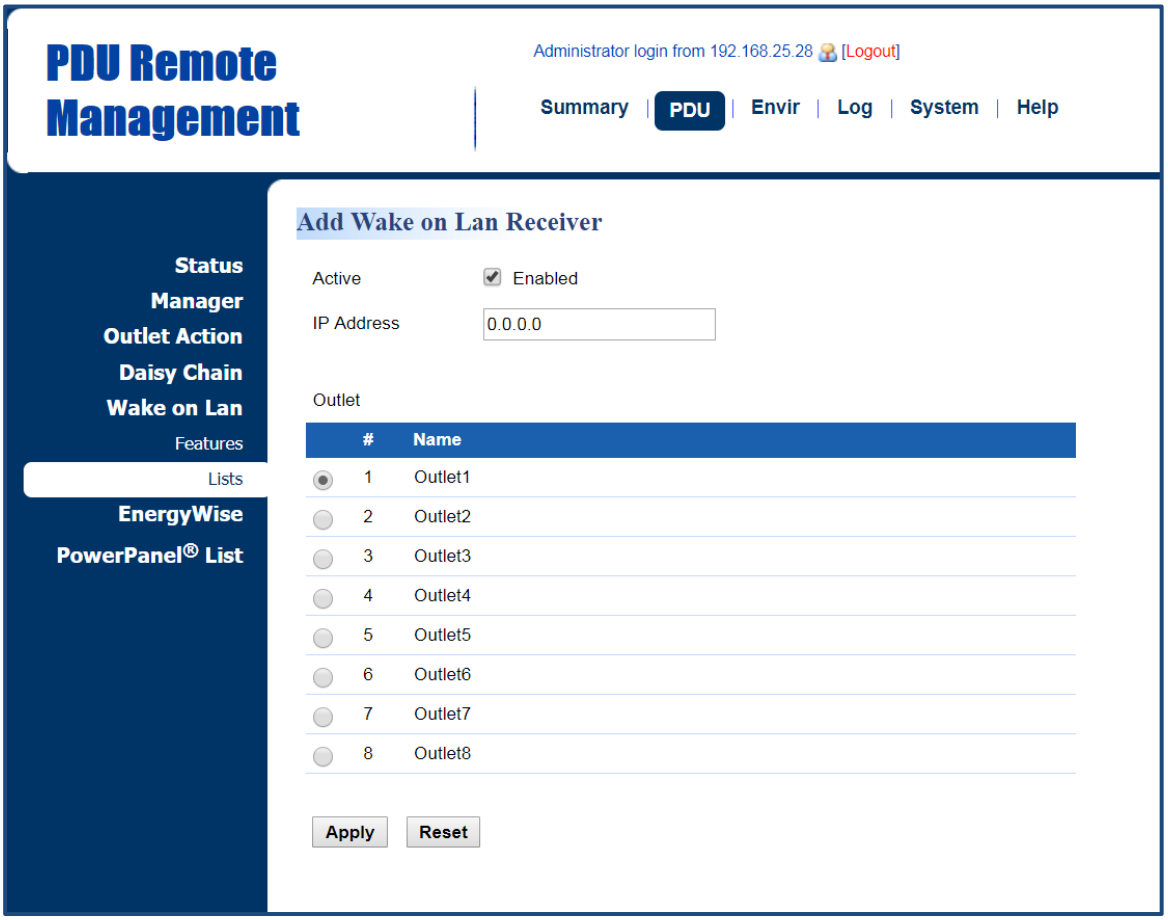
Item	Definition
PowerPanel Client	Load/Sync with PowerPanel Client List. To achieve synchronization, make sure the PDU has established communication with PowerPanel® Business Edition Client software. See System Tab > Security > Authentication.
Wake Conditions	Enable or disable the Wake on LAN function.

PDU Tab > Wake on LAN > Lists



Item	Definition
WoL Client List	If the **PowerPanel Client** option in PDU Tab > Wake on LAN > Features is selected, the PowerPanel® List will be automatically added to the WoL Client list.
WoL Manual List	Click **New** to enter the **Add Wake on LAN Receiver Page**. Users can manually add WoL receivers.

Add Wake on LAN Receiver Window



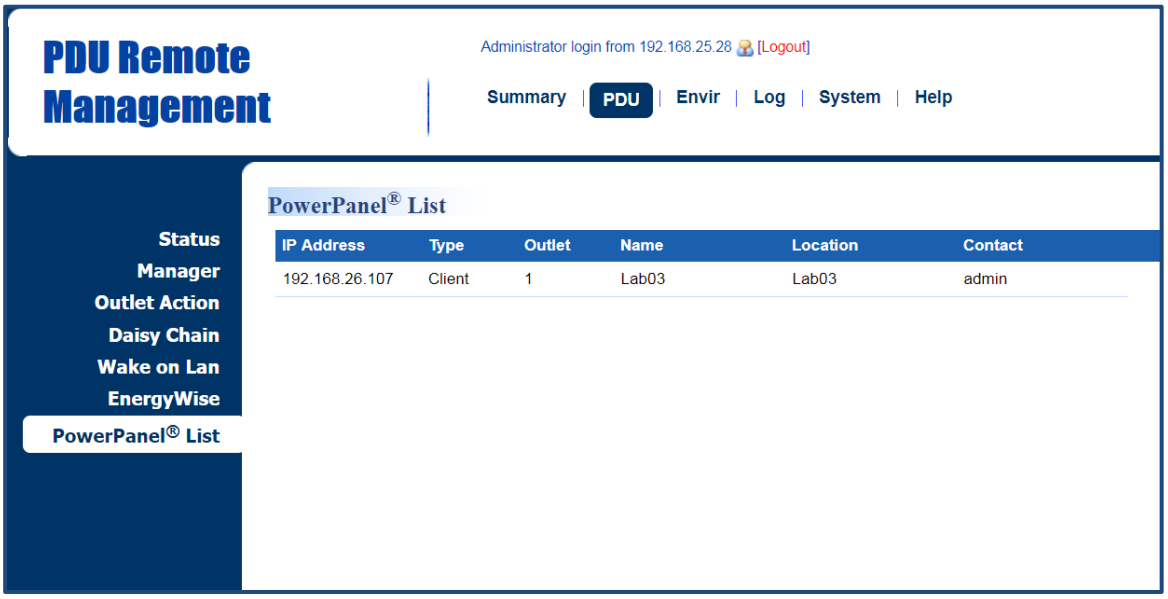
Item	Definition
Active	Enable/Disable the Wake on LAN function.
IP Address	The IP address of the computer. This IP must be within the same subnet as the PDU. Up to 50 IP addresses are supported.
Outlet	Select the outlet that provides power to the computer.

3.5 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

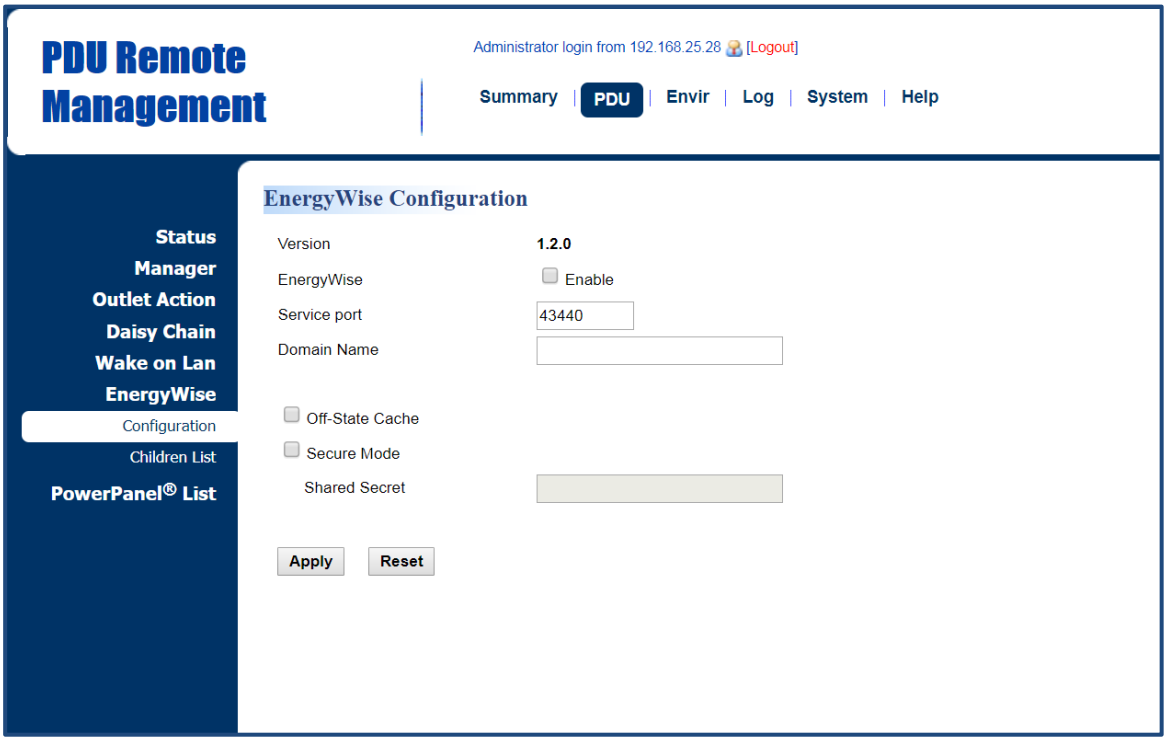


Click the IP address of a client to access configuration settings.

3.6 Cisco EnergyWise

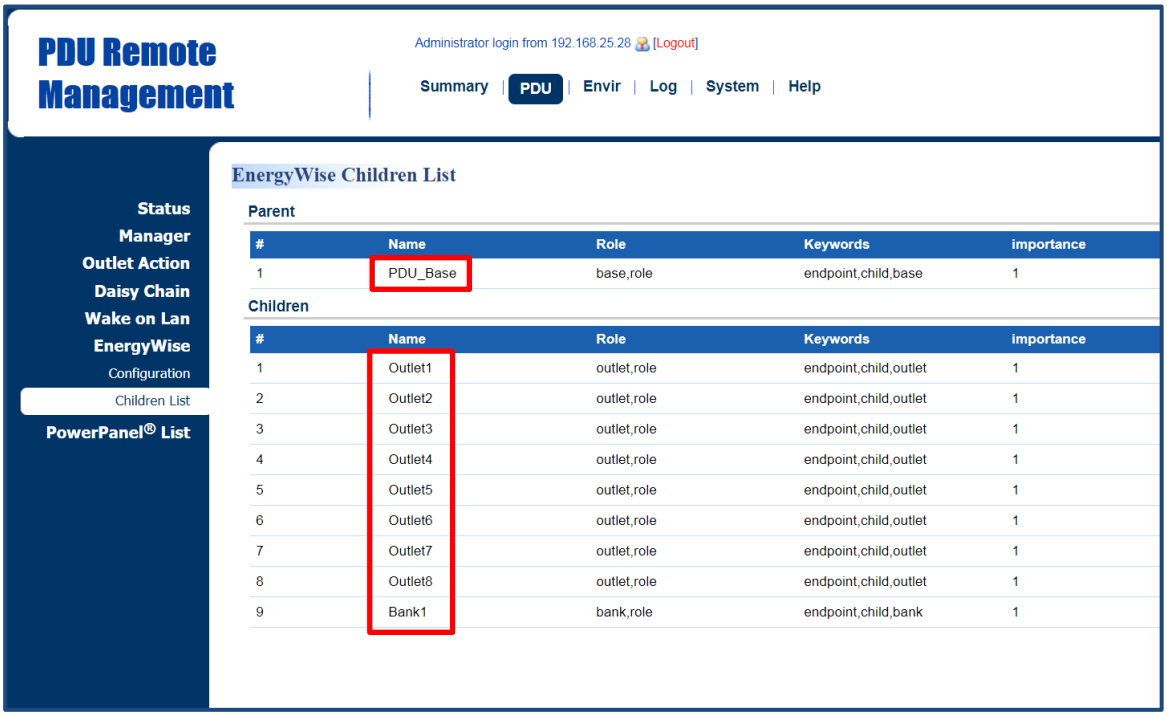
Users can manage and control all Cisco EnergyWise entities and configure settings. See **PDU Tab > EnergyWise > Configuration** and **PDU Tab > EnergyWise > Children List.**

PDU Tab > EnergyWise > Configuration



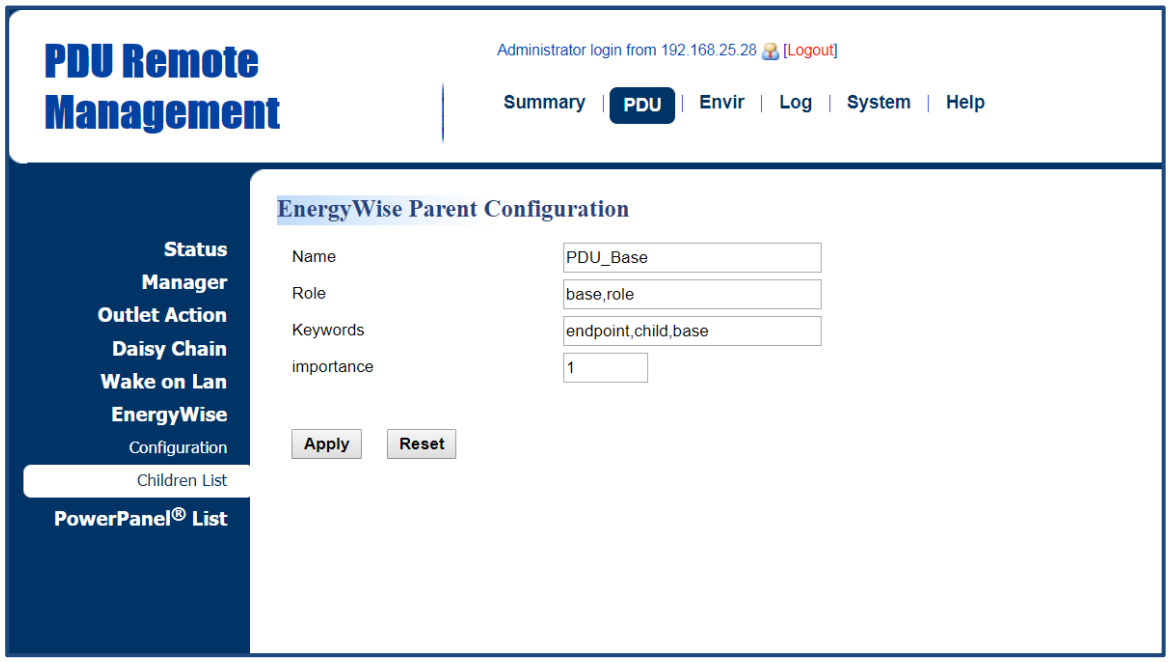
Item	Definition
Version	The version of EnergyWise supported.
EnergyWise	Enable/Disable EnergyWise support.
Service Port	The port number is used to communicate with EnergyWise. This number must be the same as that of a Cisco switch that the PDU connects to.
Domain Name	The EnergyWise domain name. This 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



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



EnergyWise Child Configuration Page

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

Item	Definition
	function of 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.

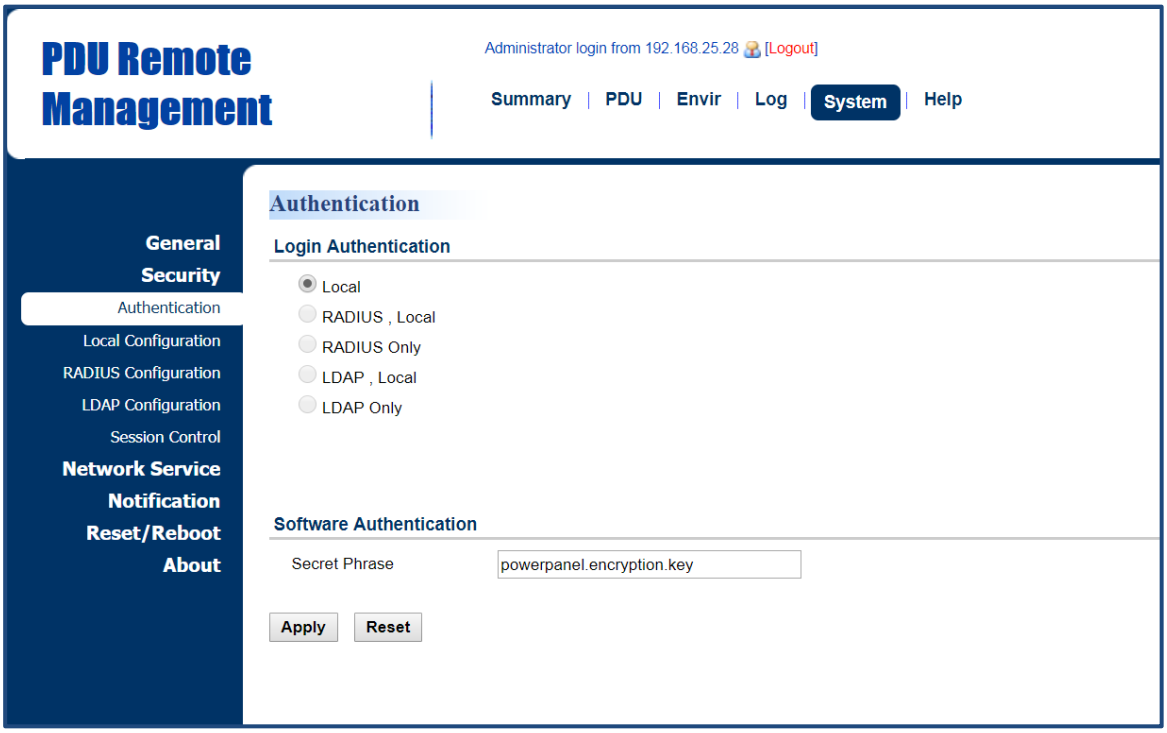
4. Security

The following provides account configurations to protect against unauthorized entry.

4.1 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

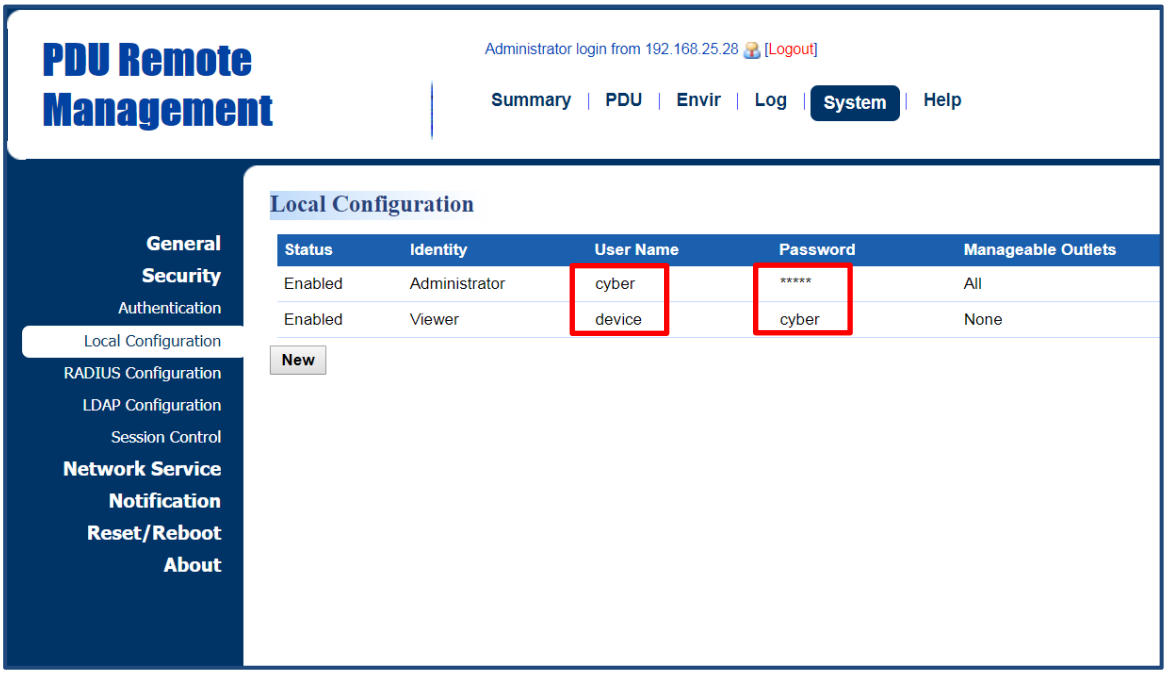


Item	Definition
Login Authentication	
Local	Log in with user name and password configured in Local Account. See System Tab > Security > Local Configuration.
RADIUS, Local	Log in with user name and password to authenticate with RADIUS server first. If the RADIUS server fails to respond, then the user name and password configured in Local Configuration can be used. See System Tab > Security > RADIUS Configuration.

Item	Definition
RADIUS Only	Log in with user name and password to authenticate with RADIUS server only. See System Tab > Security > RADIUS Configuration.
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 System Tab > Security > LDAP configuration.
LDAP Only	Log in with user name and password to authenticate with LDAP server only. See System Tab > Security > LDAP configuration.
Software Authentication	
Secret Phrase	The authentication phrase is used to communicate with PowerPanel® Business Edition software. This phrase should be the same **Secret Phrase** as the field on PowerPanel® Business Edition software interface.

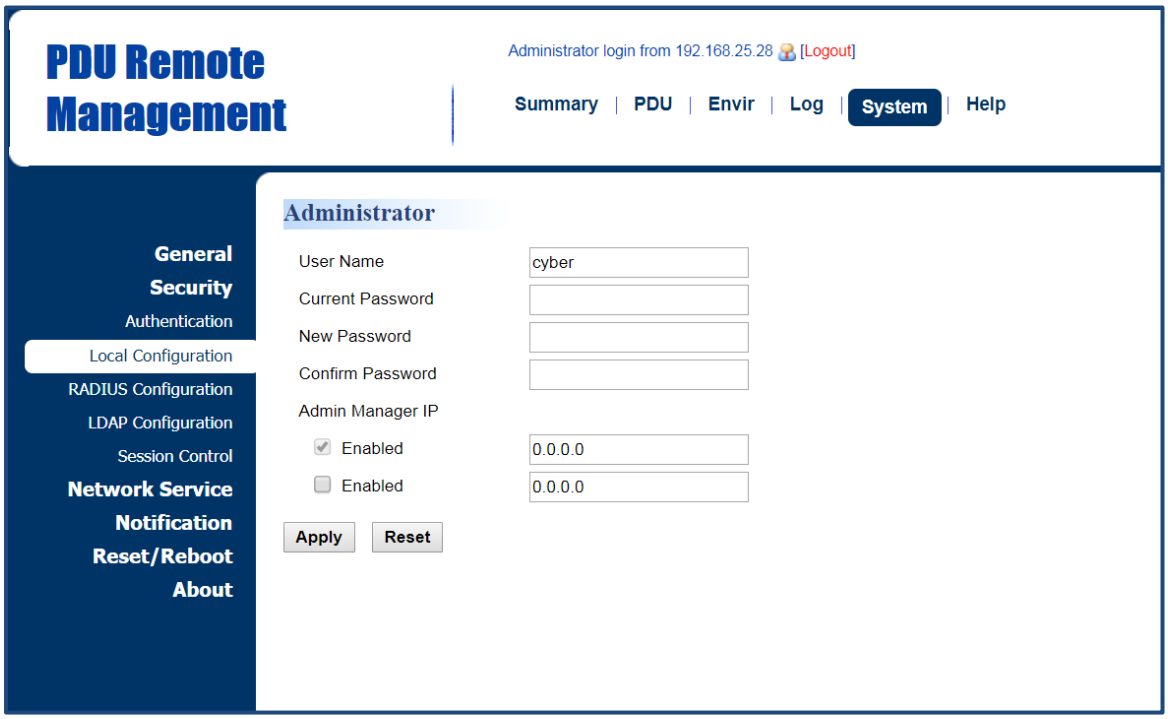
4.1.1 Using Local Configuration for Authentication

System Tab > Security > Local Configuration

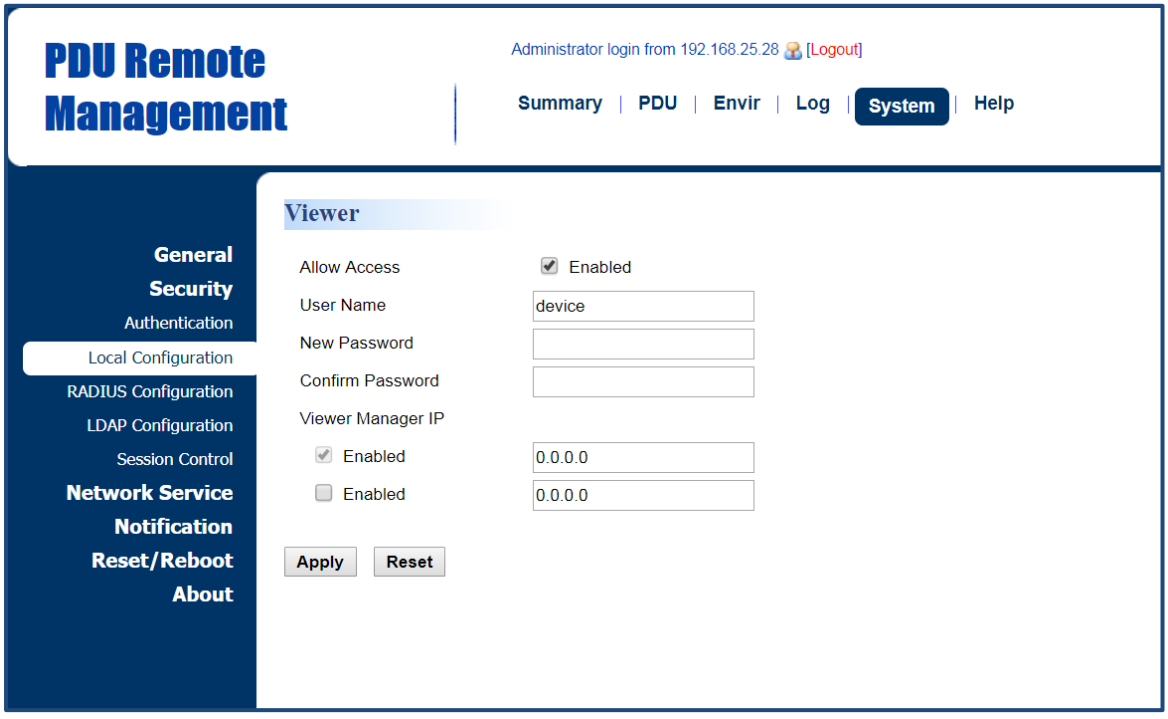


There are two types of account: administrator and viewer. Click **User Name** or **Password** field to enter **Administrator Page or Viewer Page**. Users can also click **NEW** to enter **Add Outlet User Page** to create an outlet account.

Administrator Page

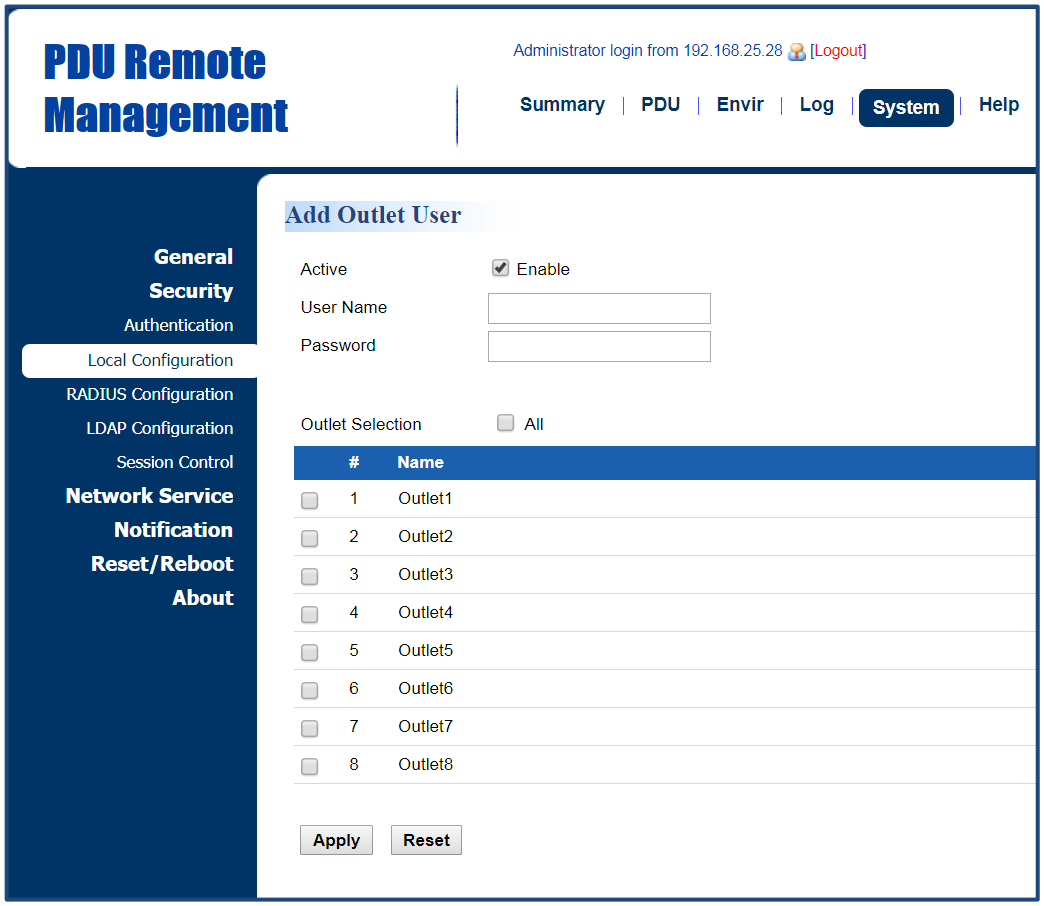


Viewer Page



Item	Definition
Administrator	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. **Note**: You can also set a range of IP addresses to access, for example, 192.168.16.1/24.
Viewer	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. **Note**: You can also set a range of IP addresses to access, for example, 192.168.16.1/24.

Add Outlet User Page*

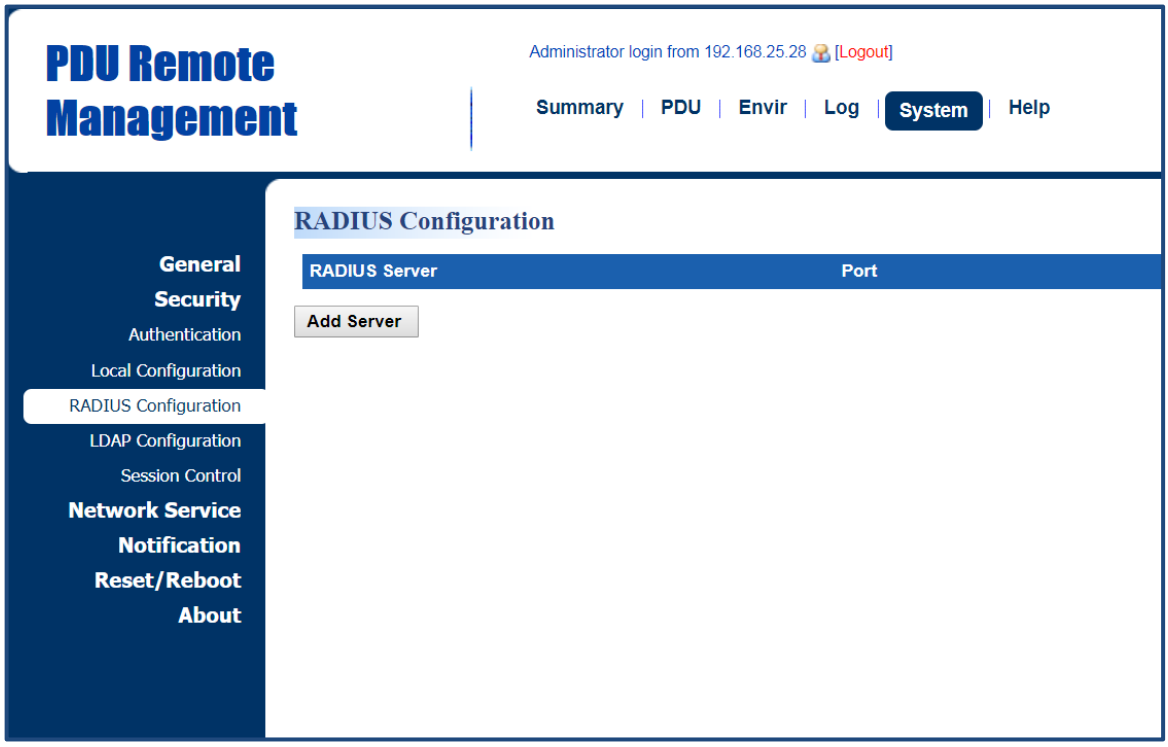


*The above **Add Outlet User Page** is available for Switched Metered by Outlet Series and Switched Series only.
Users can create an outlet account that is allowed to control assigned outlet(s).

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.

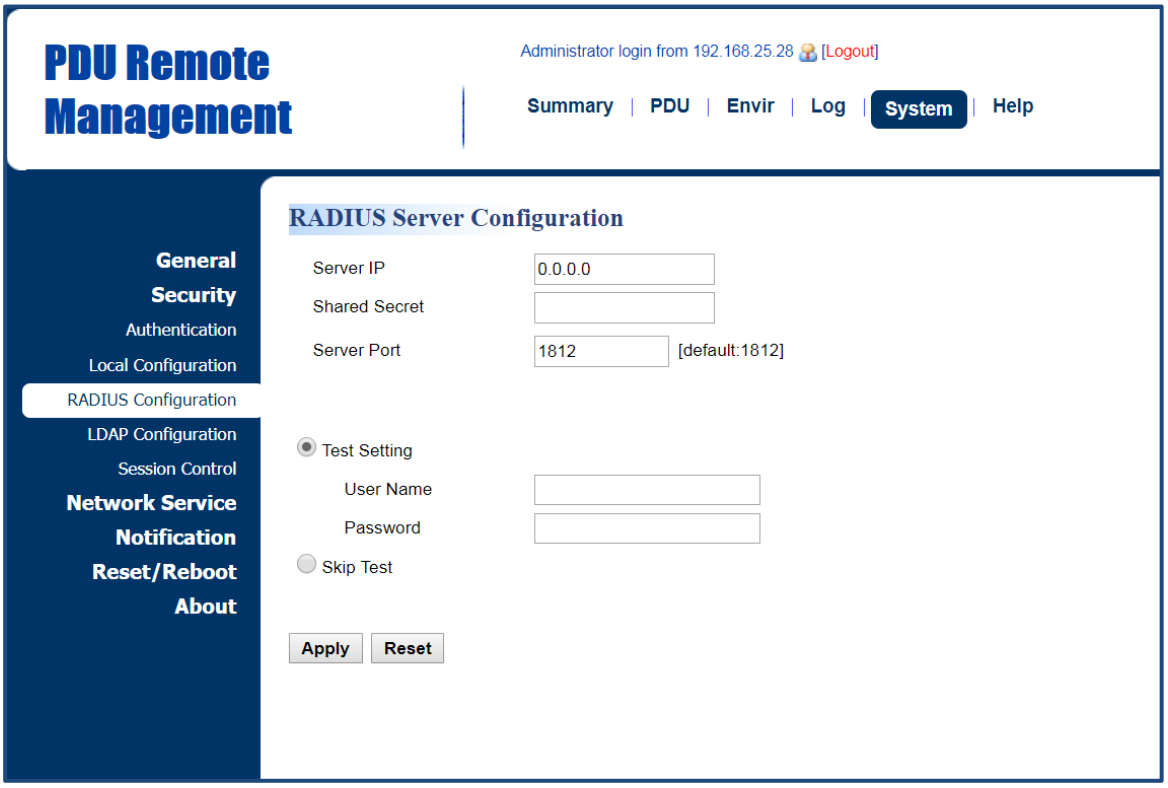
4.1.2 Using RADIUS Configuration for Authentication

System Tab > Security > RADIUS Configuration



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

Radius Server Configuration Page



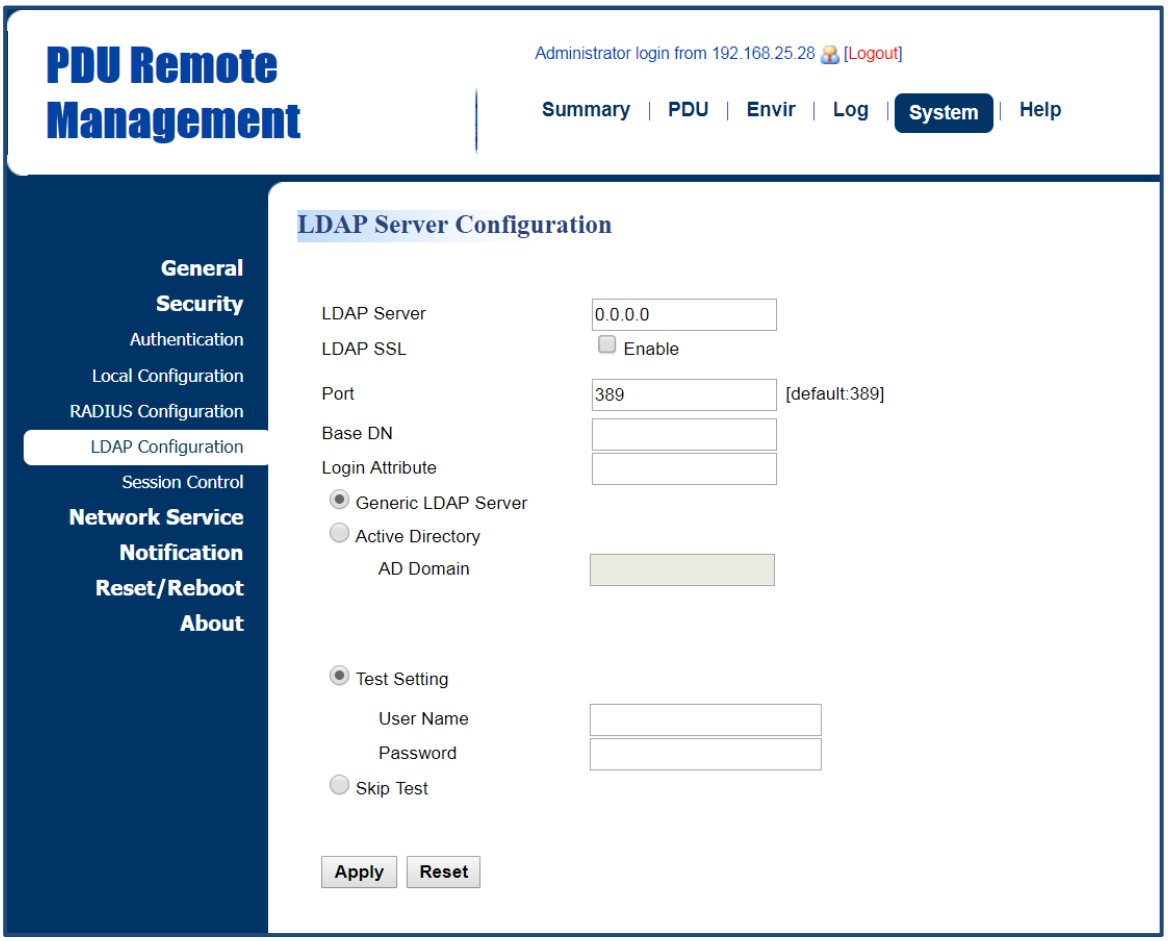
Item	Definition
Server IP	The IP address of RADIUS server.
Shared Secret	The shared secret of RADIUS server.
Server Port	The UDP port used by the RADIUS server.
Test Setting	Use user name and password to authenticate with RADIUS server, and save information of RADIUS server if authentication succeeds.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

4.1.3 Using LDAP Configuration for Authentication

System Tab > Security > LDAP configuration

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

LDAP Server Configuration Page



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.

4.2 Timeout Setting

Configure the idle login sessions. See **System > Security > Session Control**.

System > Security > Session Control

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

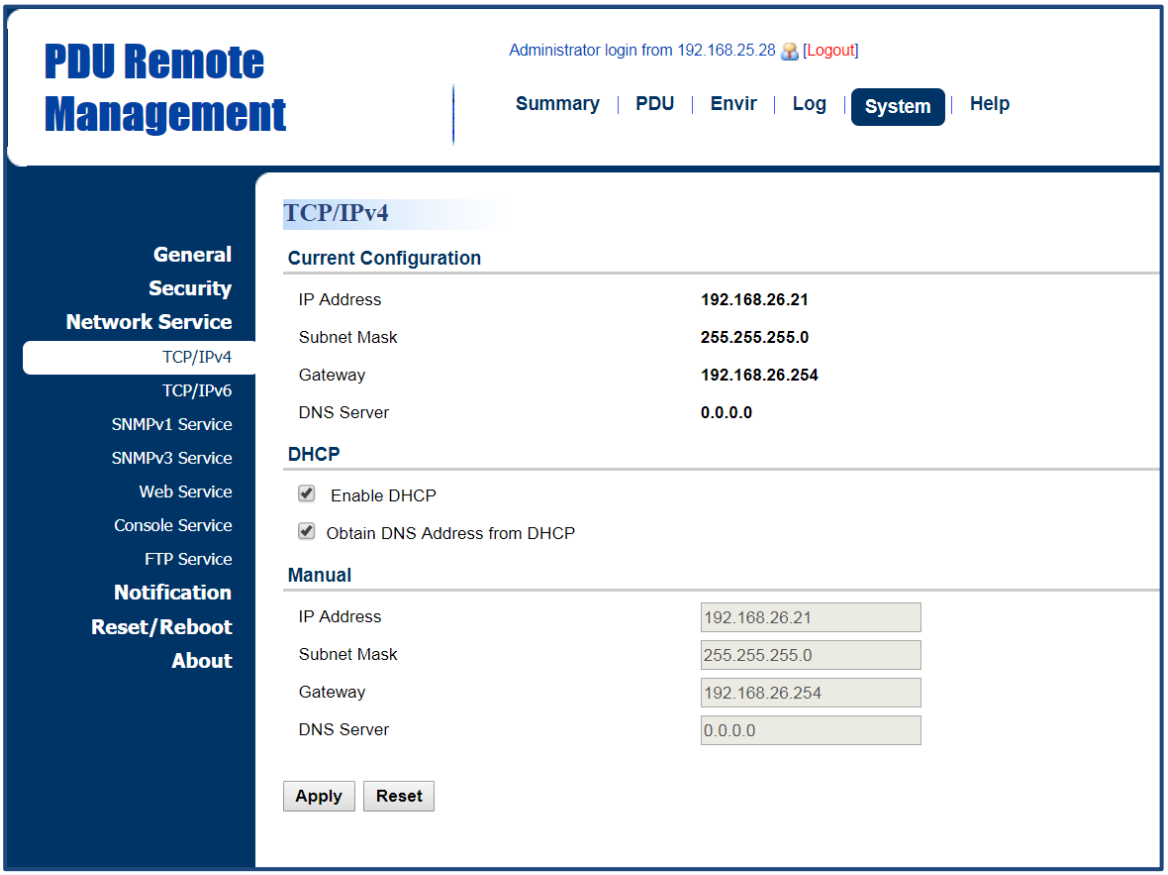
5. Network Service

The following provides the network configurations.

5.1 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

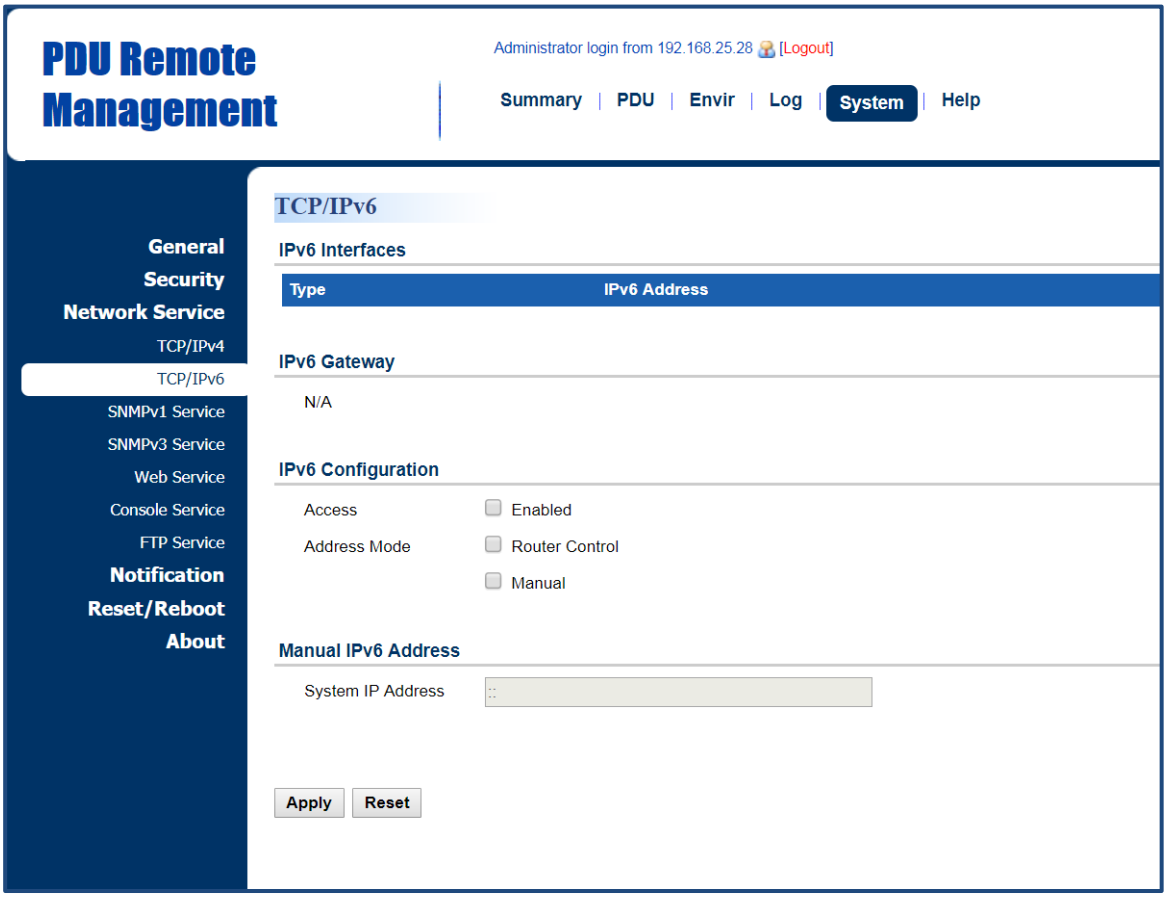


Item	Definition
Current Configuration	Display the current TCP/IP settings: IP Address, Subnet Mask, Gateway, and DNS server.
DHCP	***Enable DHCP**: Select this option to get IP address, Subnet Mask, and Gateway from DHCP. ***Obtain DNS Address from DHCP**: Select this option to get DNS by DHCP if DHCP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

5.2 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

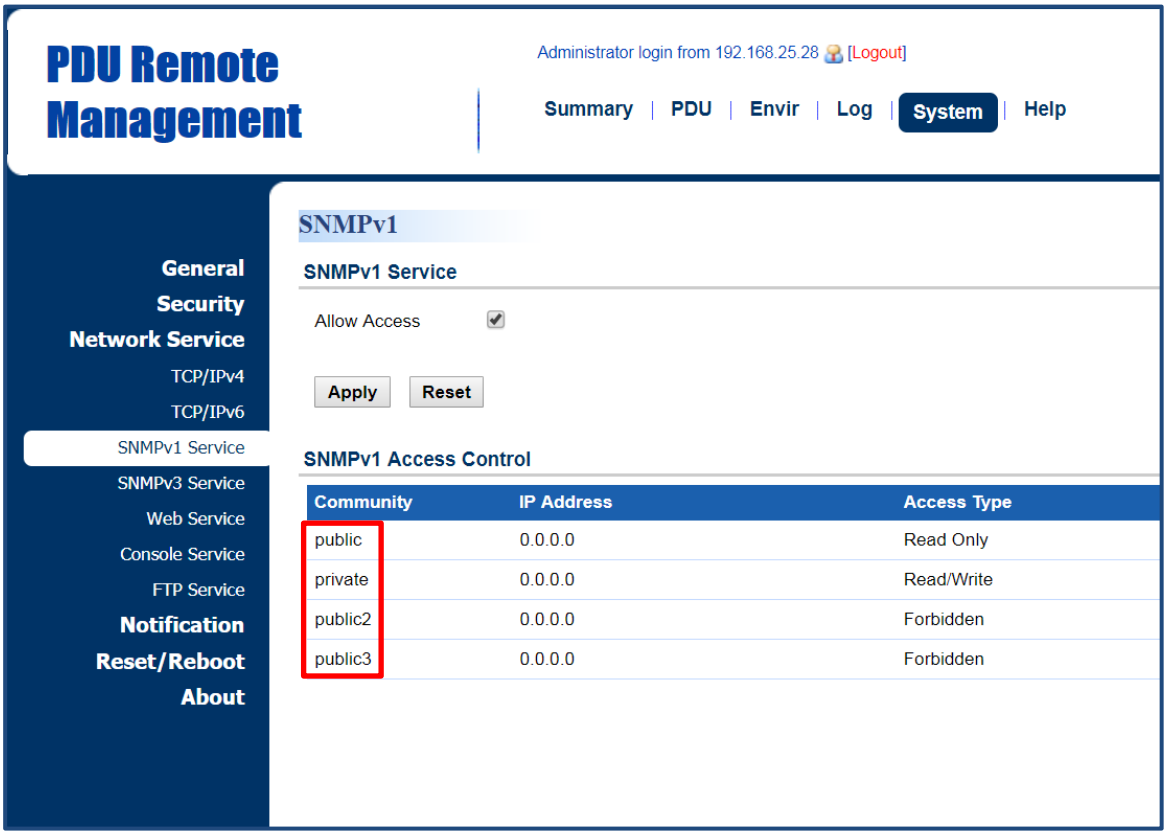


Item	Definition
IPv6 Interface	Displays the current IPv6 address.
IPv6 Gateway	Displays the current IPv6 gateway.
IPv6 Configuration	
Allow Access	Enable/Disable IPv6 service.
Address Mode: Router Control	The IPv6 address is assigned through the method (Stateless Address Auto configuration, Stateless 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 **Apply** when the **Address Mode: Manual** option is selected.

5.3 SNMPv1 Service Setting

Allow users to perform SNMPv1 configurations. See **System Tab > Network Service > SNMPv1 Service.**

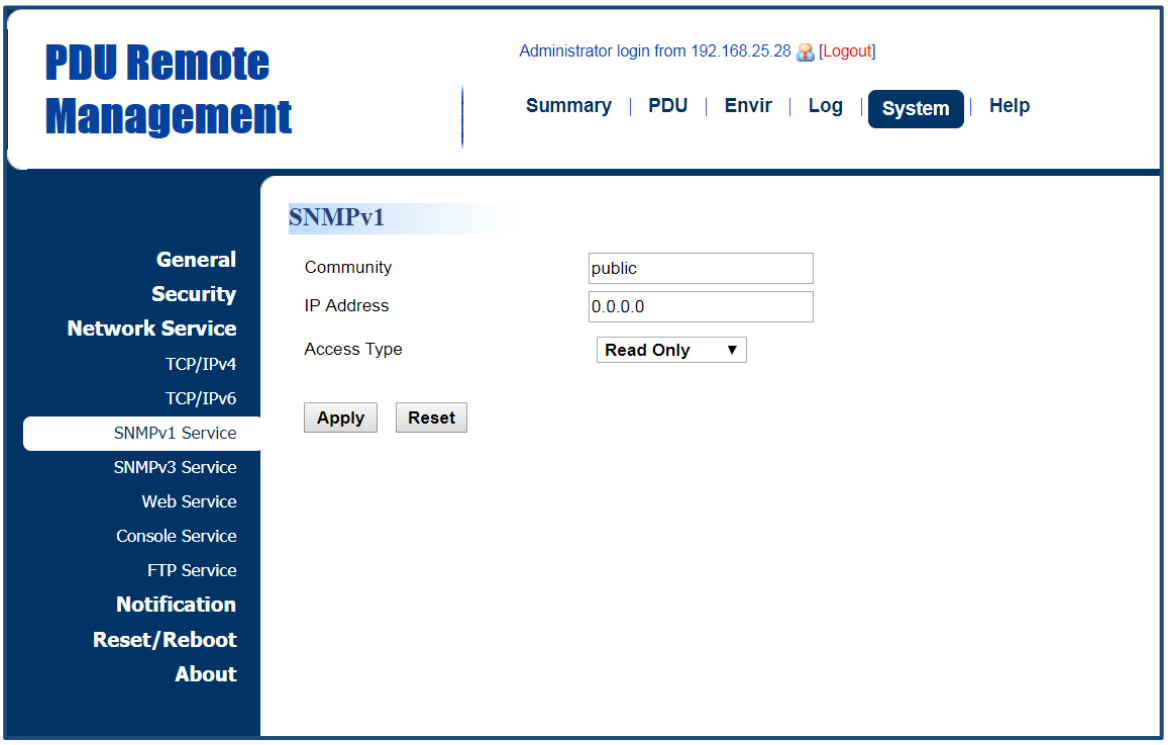
System Tab > Network Service > SNMPv1 Service



Item	Definition
SNMPv1 Service	
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

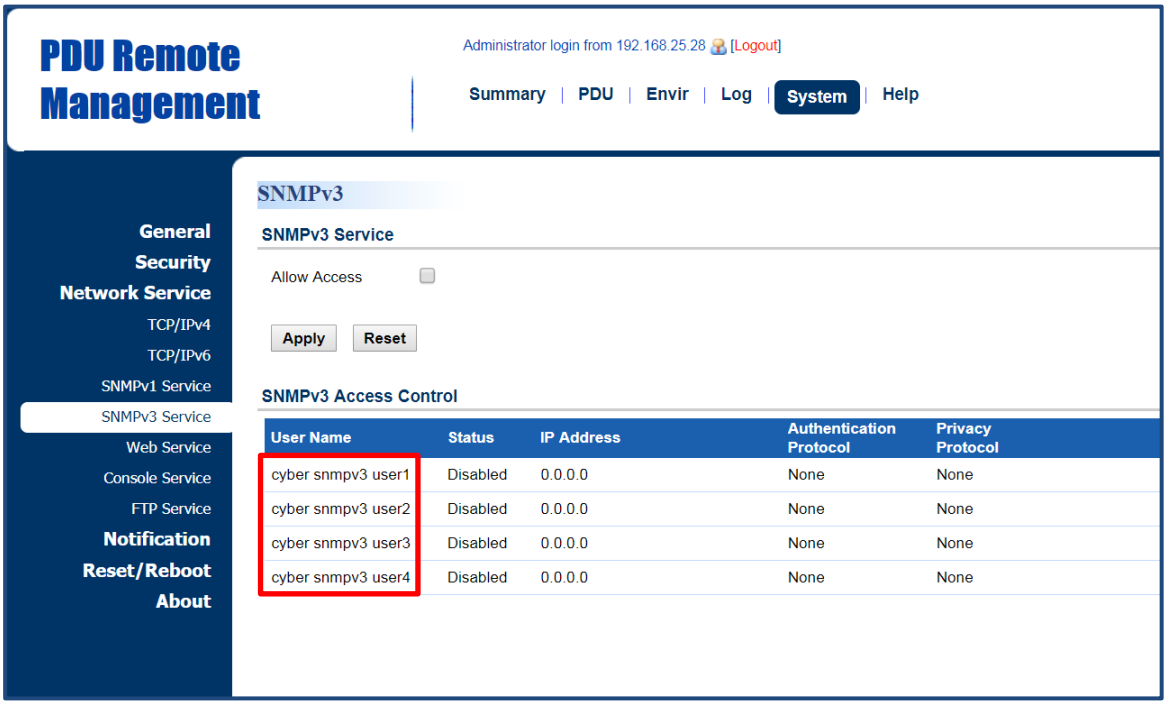


Item	Definition
Community	The name used to access the SNMP community from a Network Management System (NMS). Its maximum length is 15 characters.
IP Address (IPv6 Support)	The IP address or IP address mask can be accessed by the NMS. A specific IP address allows access only by the NMS with the specified 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.

5.4 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**.

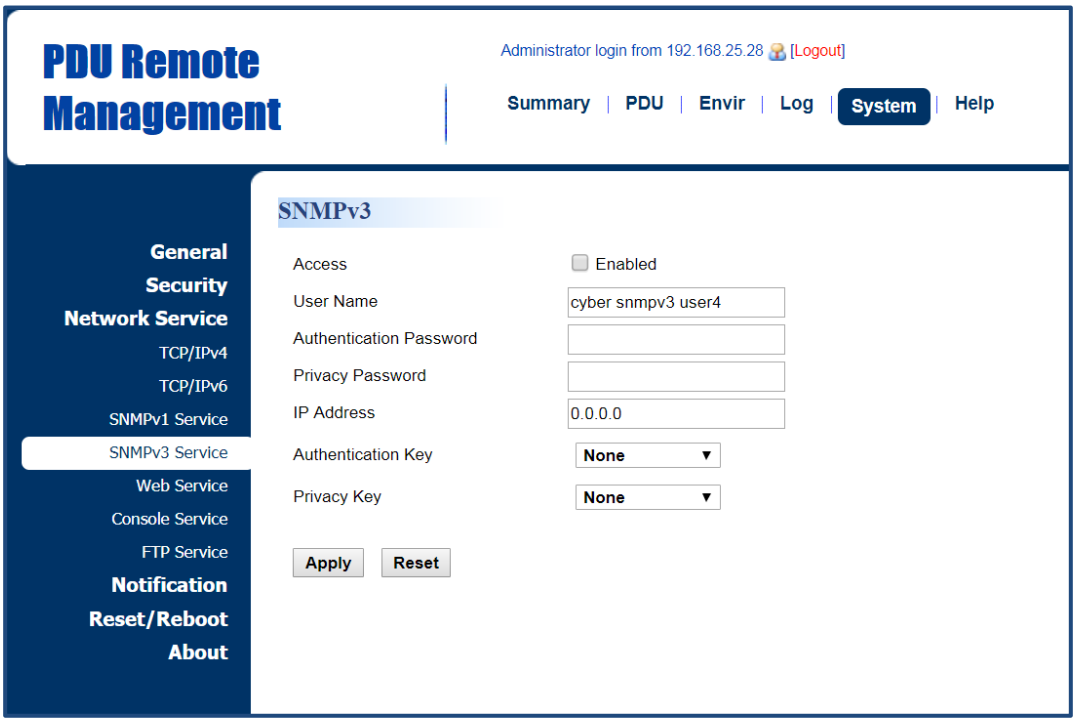
System Tab > Network Service > SNMPv3 Service



Item	Definition
SNMPv3 Service	
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.

5.5 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**.

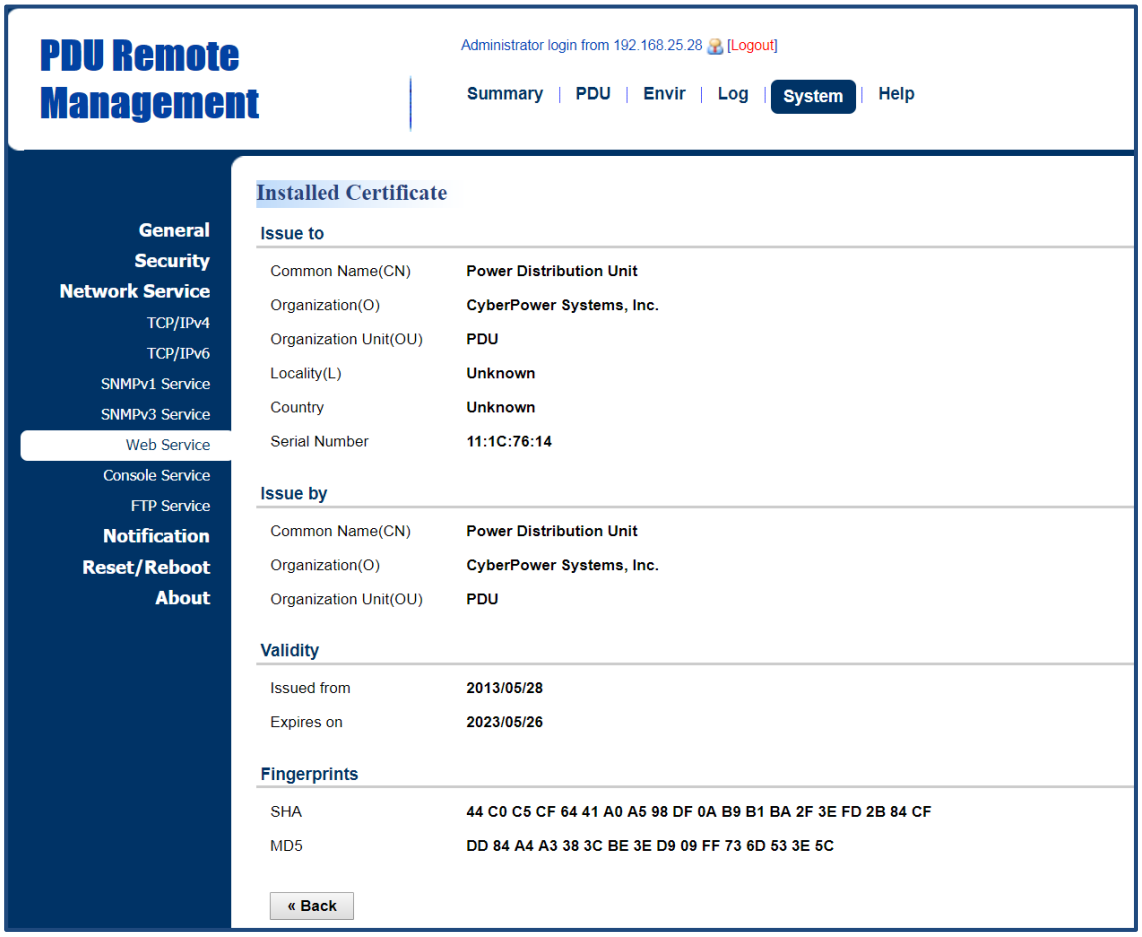
System Tab > Network Service > Web Service

Item	Definition
Access	
Allow Access	Enable or disable HTTP/HTTPS service. HTTPS supports the following encryption algorithms: ● AES (256/128 bits) ● Camellia (256/128 bits) ● 3DES (168 bits) ● DES (168 bits) ● RC4 SHA (128) ● RC4 MD5 (128)
Http Settings	

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

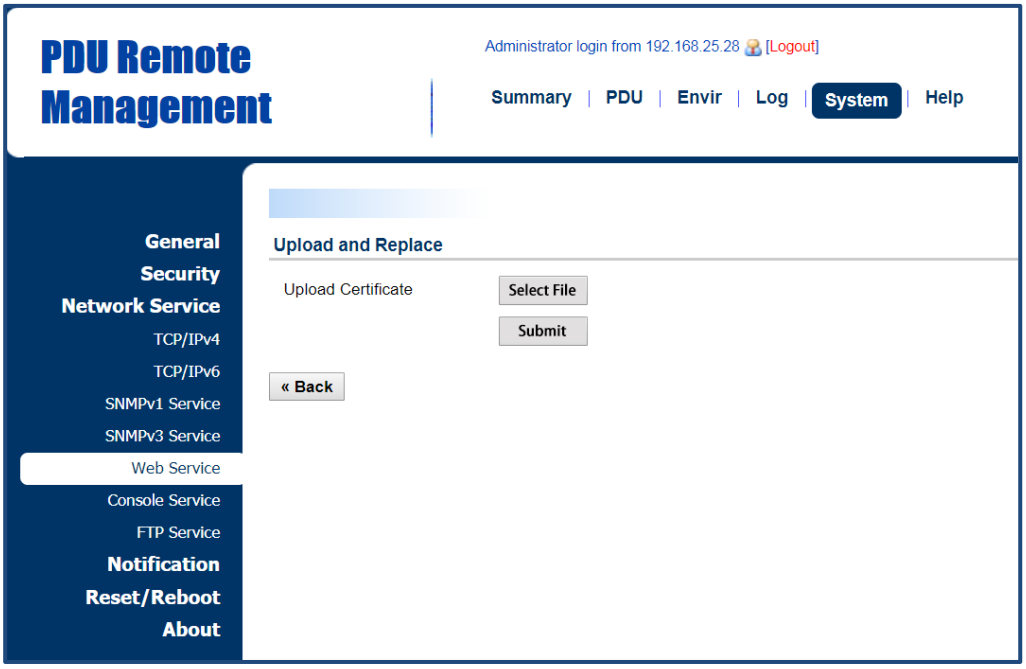
Click the **Valid Certificate** link, and the **Installed Certificate Page** will appear.

Installed Certificate Page



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

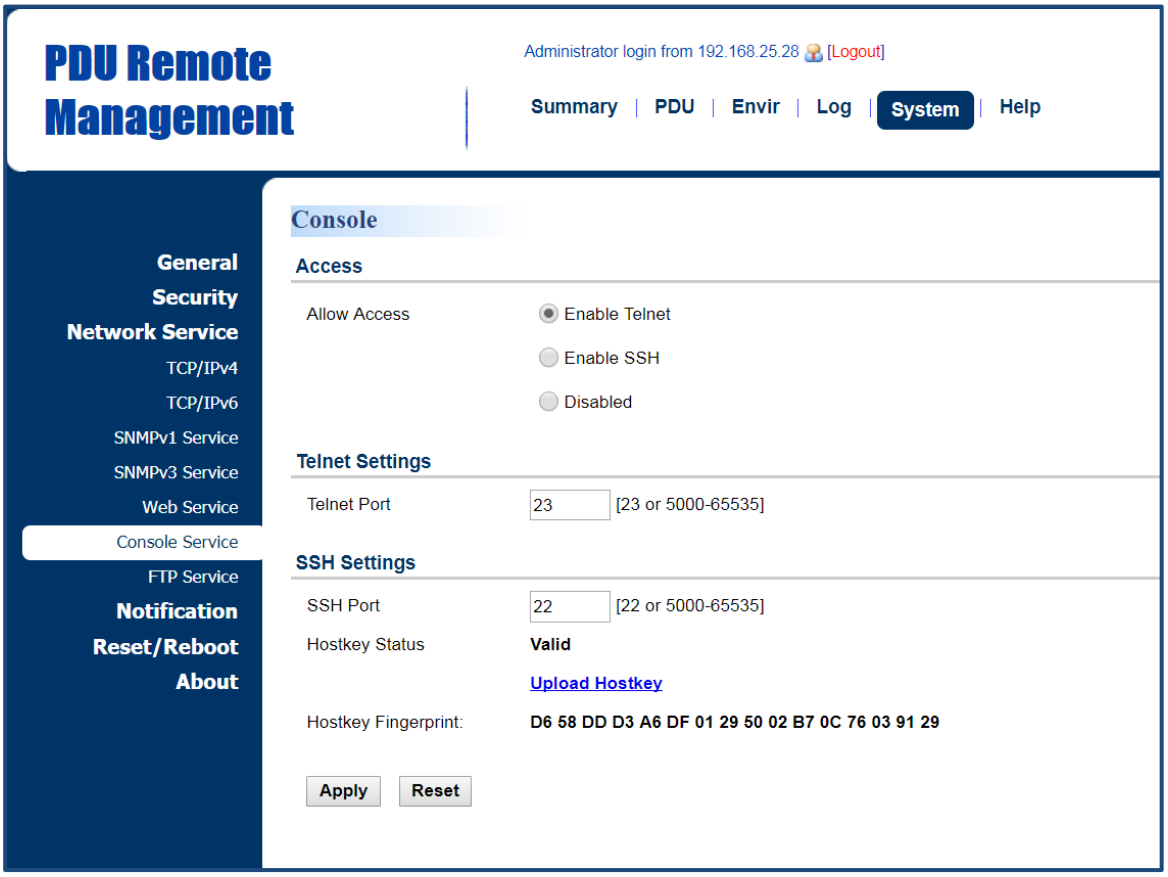
Change Certificate Page



5.6 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



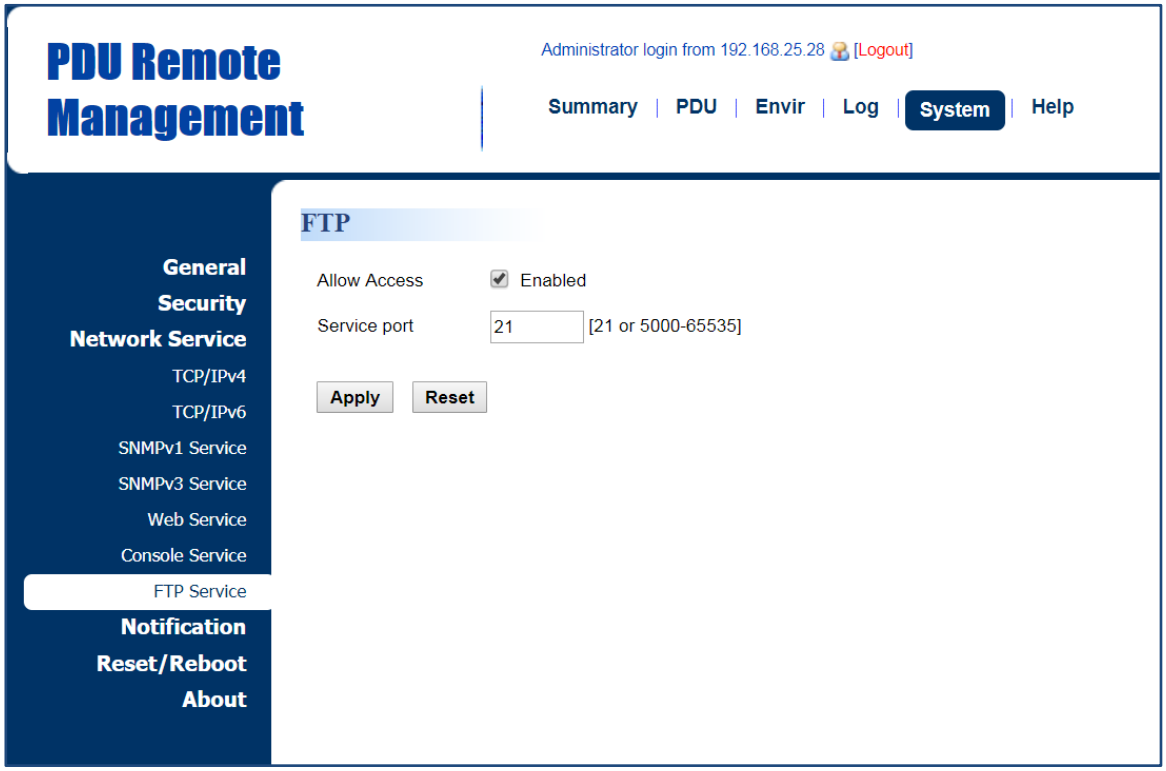
Item	Definition
Access	
Allow Access	Enable access using Telnet or SSH version 2, which transmits user names, passwords, and data in an encrypted format.
Telnet Settings	
Telnet Port	The TCP/IP port that Telnet uses to communicate; 23 is the default value. Users can change the port setting to any unused port from 5000 to 65535 to enhance security. **Note**: 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.

Item	Definition
SSH Settings	
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 **Upload Hostkey** to upload or change hostkey.
Hostkey Fingerprint	The hostkey fingerprint uploaded by users will be displayed in this field.

5.7 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**.

System Tab > Network Service > FTP Service

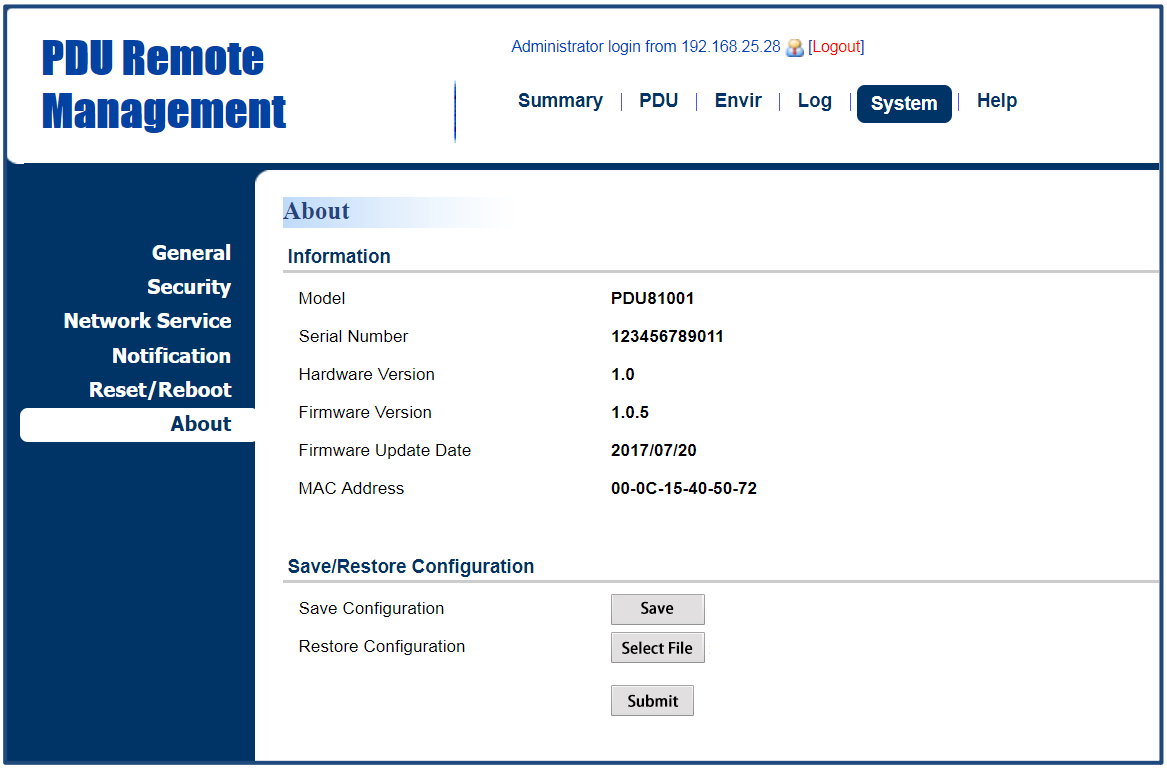


Item	Definition
Allow Access	Enable FTP server access.
Access Port	The TCP/IP port of the FTP server; 21 is the default value. Users can change port setting to any unused port from 5000 to 65535 to enhance security.

6. PDU Information

Display the system information of the PDU. See **System > About.**

System > About

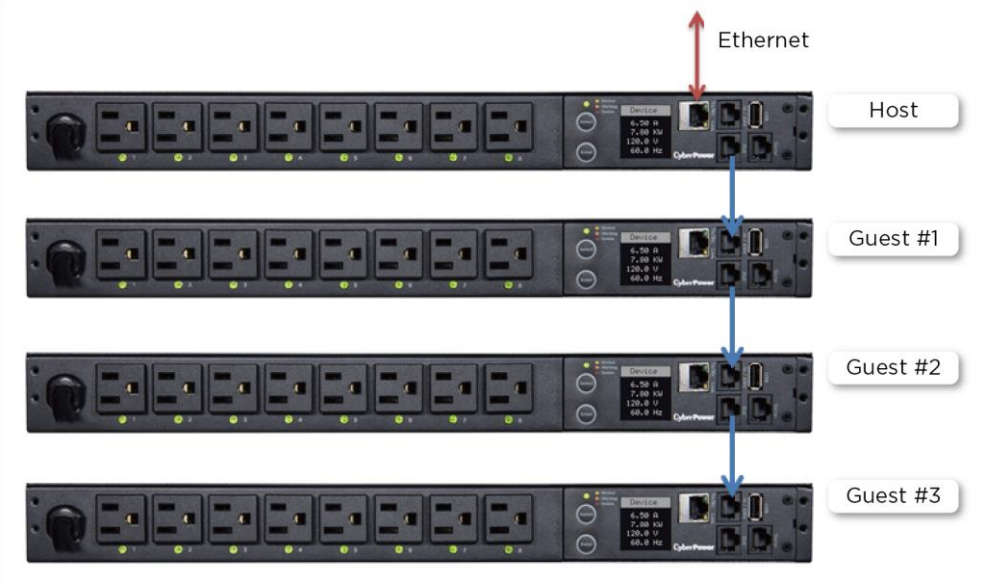


Item	Definition
Information	
Model Name	Model name of the PDU.
Serial Number	Serial Number of the PDU.
Hardware Version	The hardware version of the PDU.
Firmware Version	The current firmware version installed on the PDU.
Firmware Updated Date	The date the firmware was last updated.
MAC Address	MAC address of the PDU. **Note**: The MAC address is shown on the label on the back of the PDU and via the LCD screen on the PDU.
Save/Restore Settings	
Save Configuration	Click **Save** 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 **Select File** to import an existing configuration file and then click **Submit**.

Appendix A: 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.

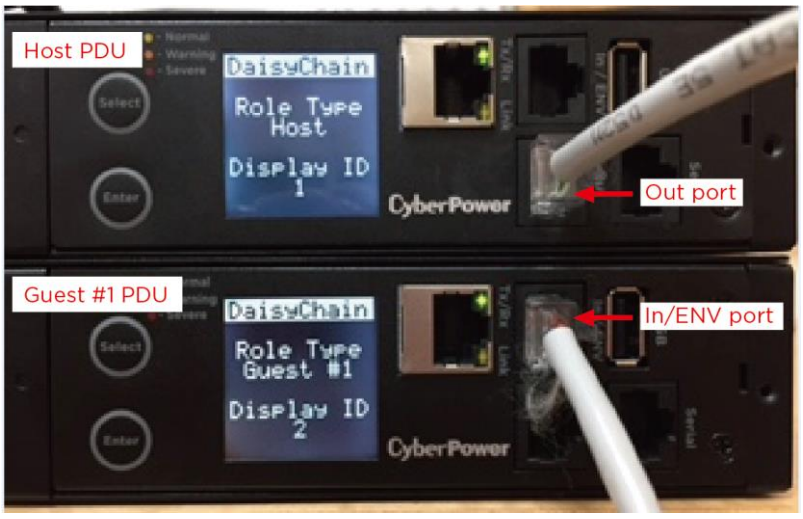


When PDUs are connected, two roles are defined: Host and Guest. Up to three Guest PDUs can be connected to one Host PDU. The Guest PDUs will be recognized by serial number and their order within the daisy-chain.

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.

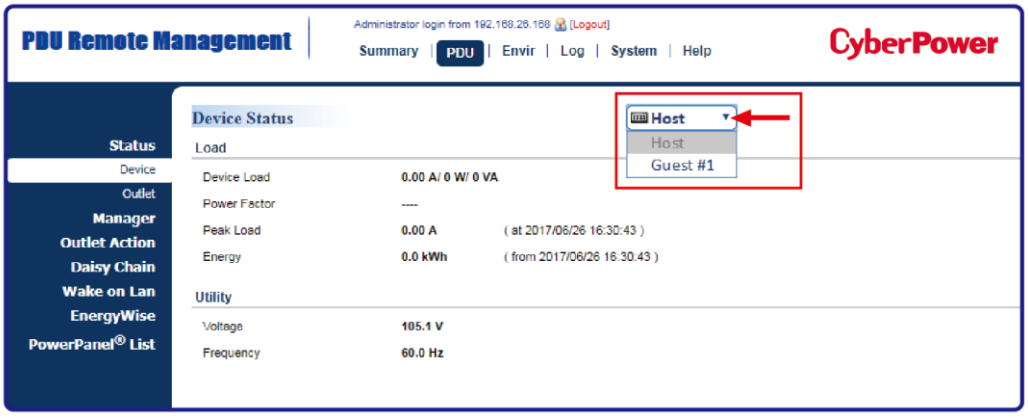
What functions on the Web pages does daisy-chain support?

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).

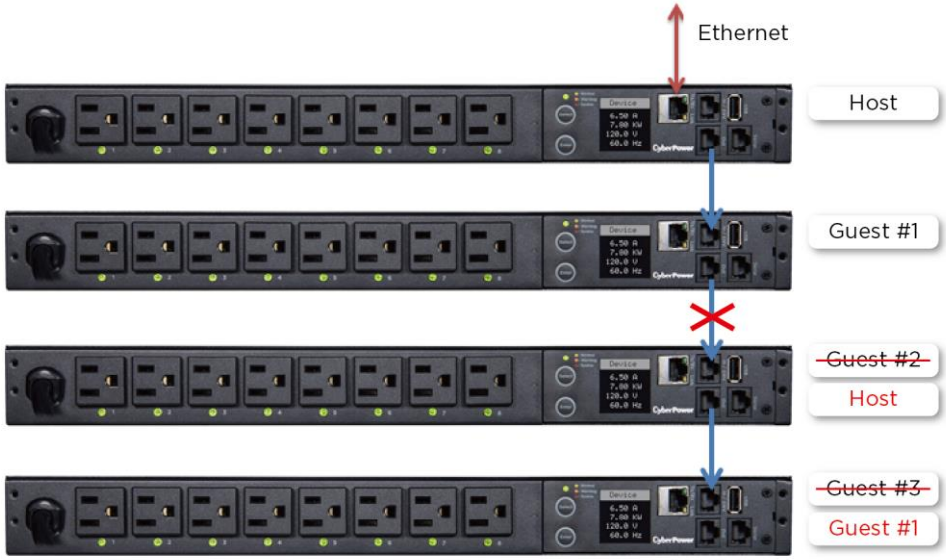


Can I upgrade the firmware version of the Guest PDUs through the Host PDU?

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

Appendix B: 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:

* cpsmpdumafw_XXX.bin
* cpsmpdumadata_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
- 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 cpsmpdumafw_XXX.bin, type
   - `ftp > bin`
   - `ftp > put cpsmpdumafw_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 cpsmpdumadata_XXX.bin, type
   - `ftp > bin`
   - `ftp > put cpsmpdumadata_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
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).

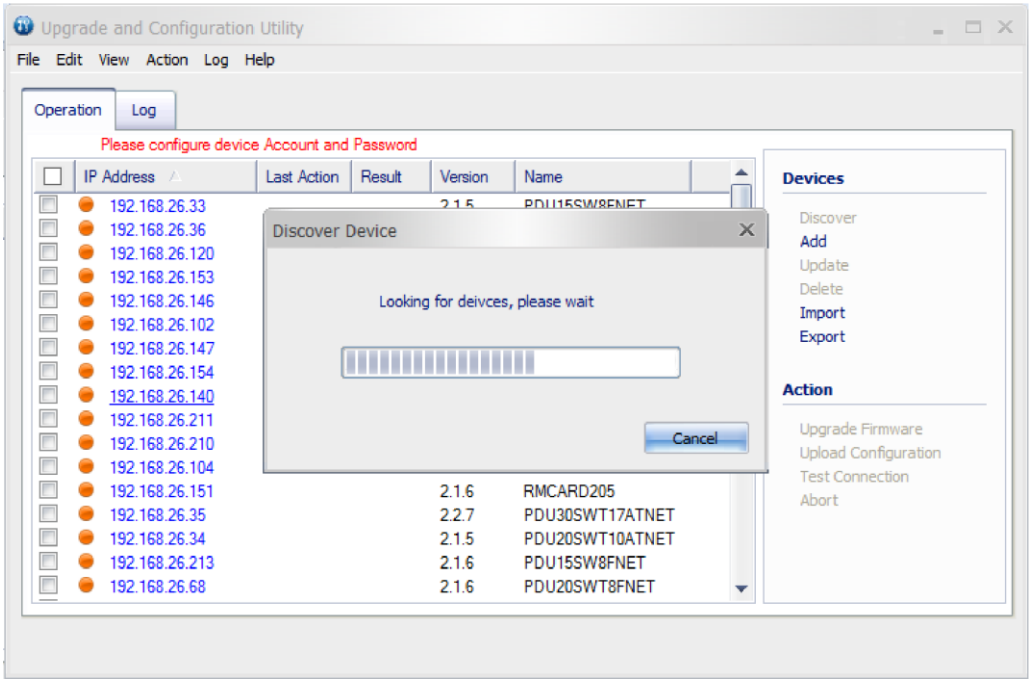


Figure 1.

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

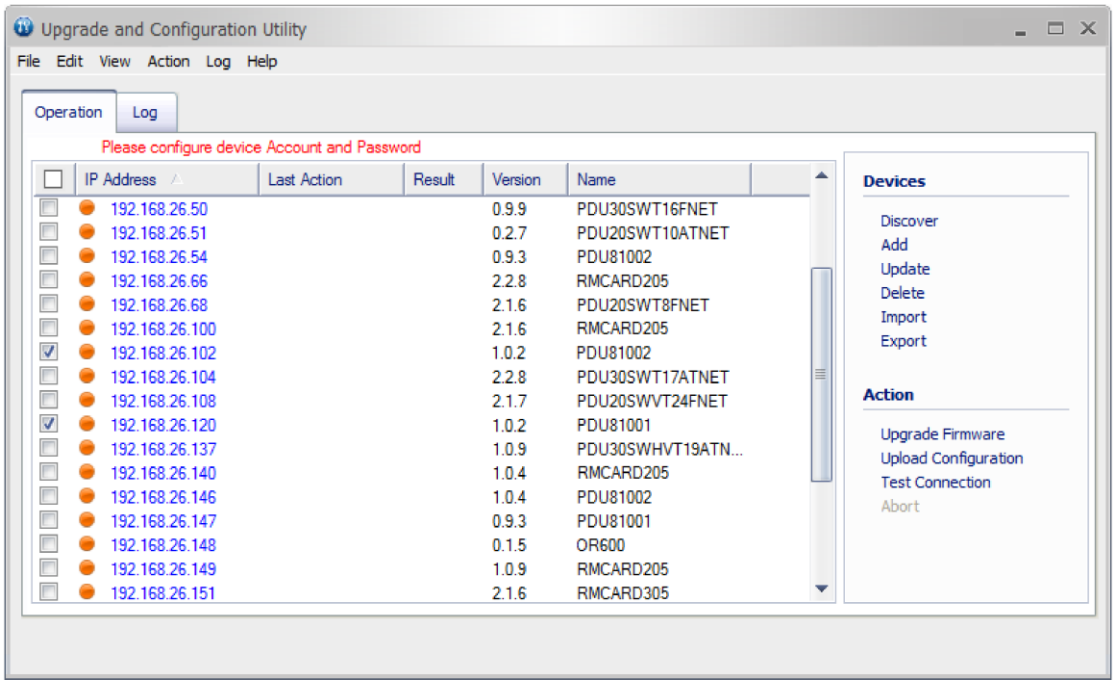


Figure 2

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

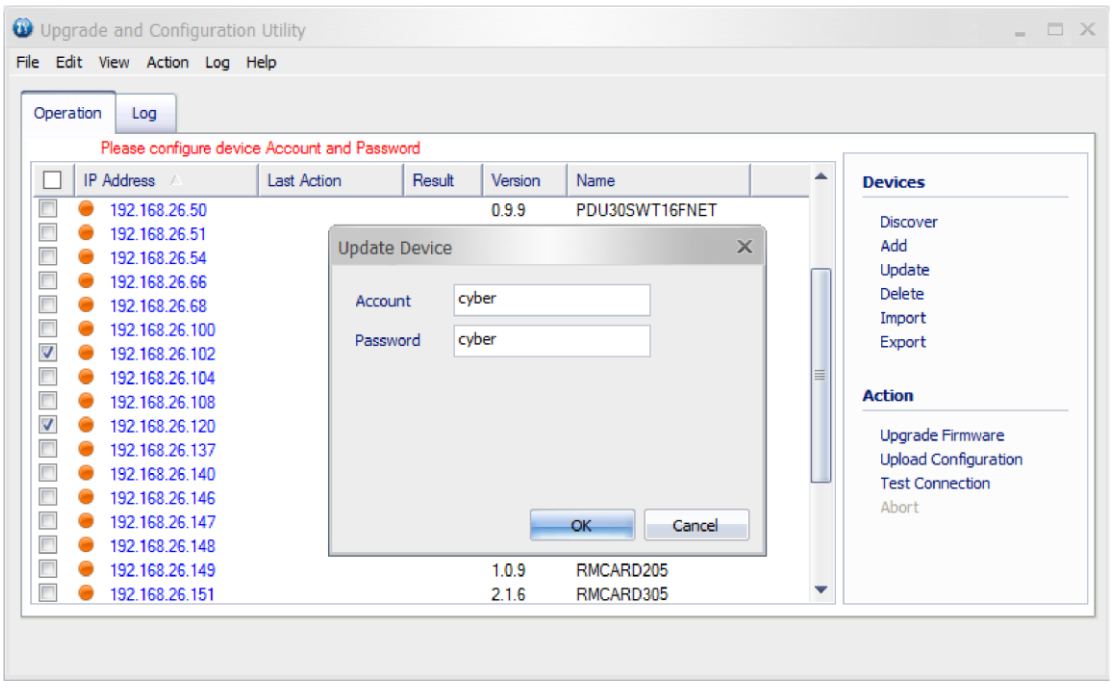


Figure 3.

6. Select **Upgrade Firmware**.

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

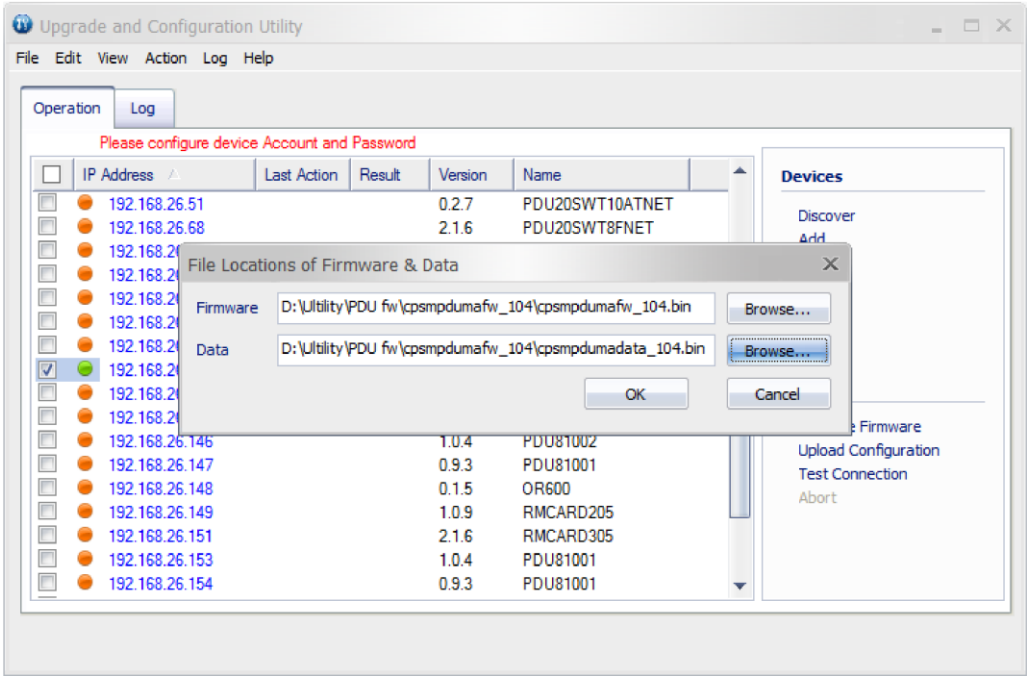


Figure 4.

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

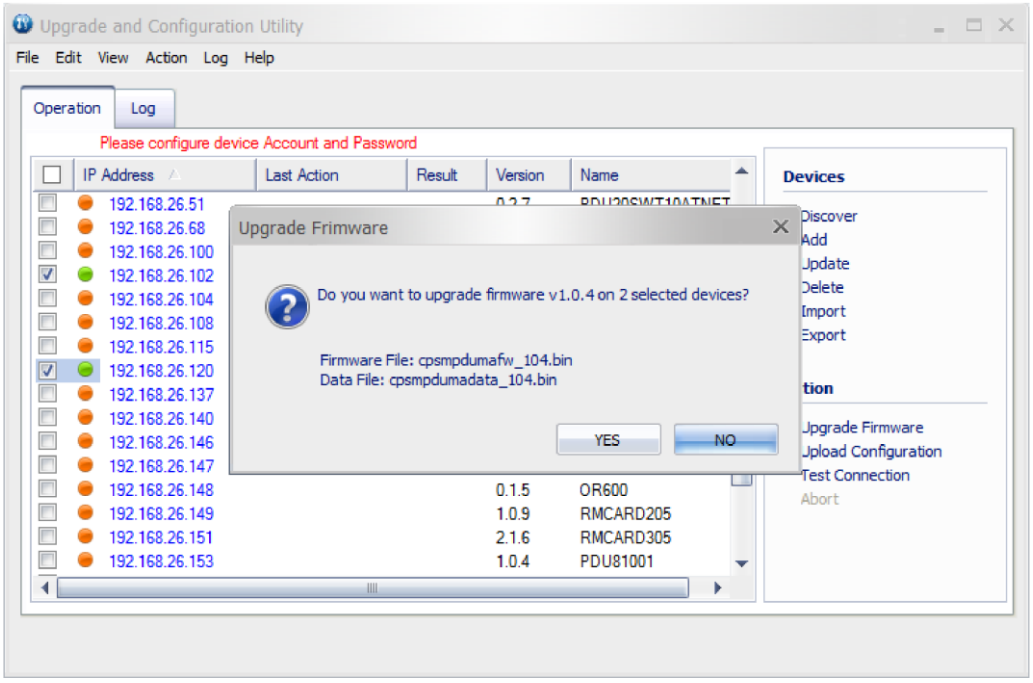


Figure 5.

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

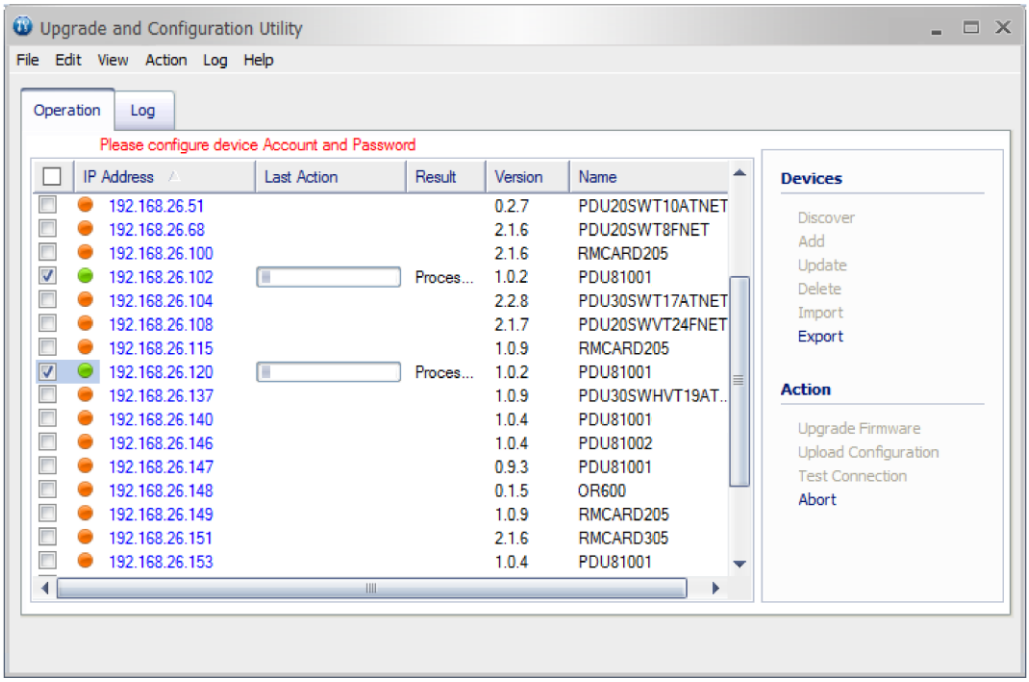


Figure 6.

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

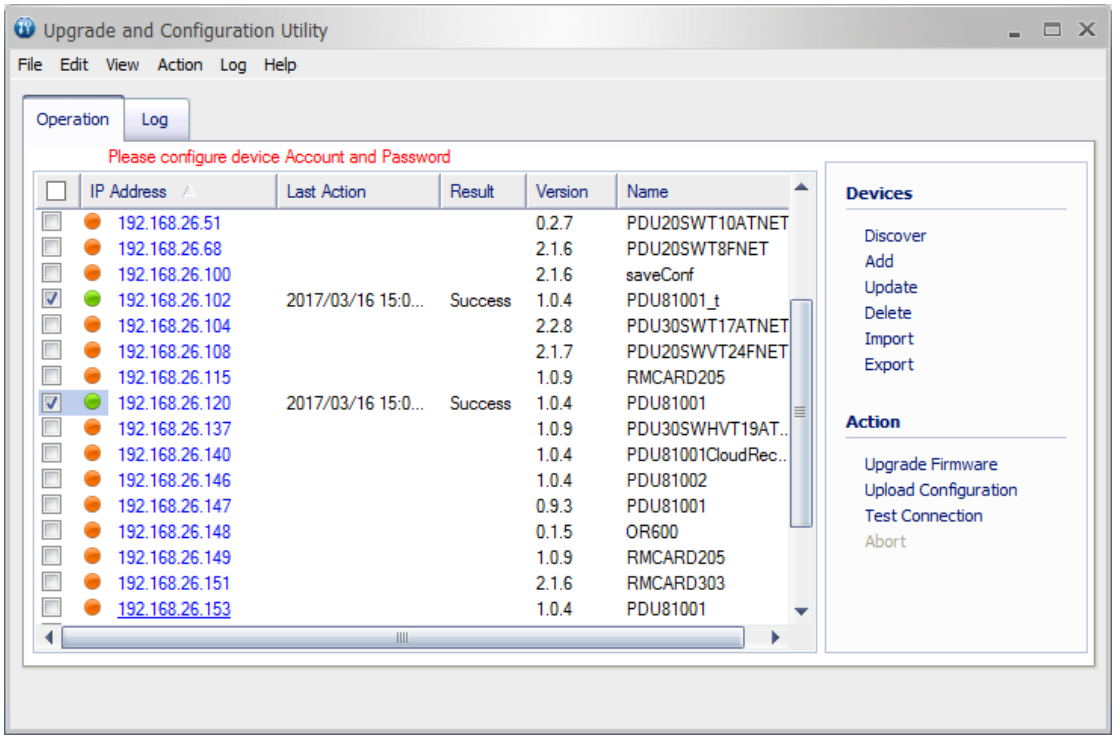


Figure 7.

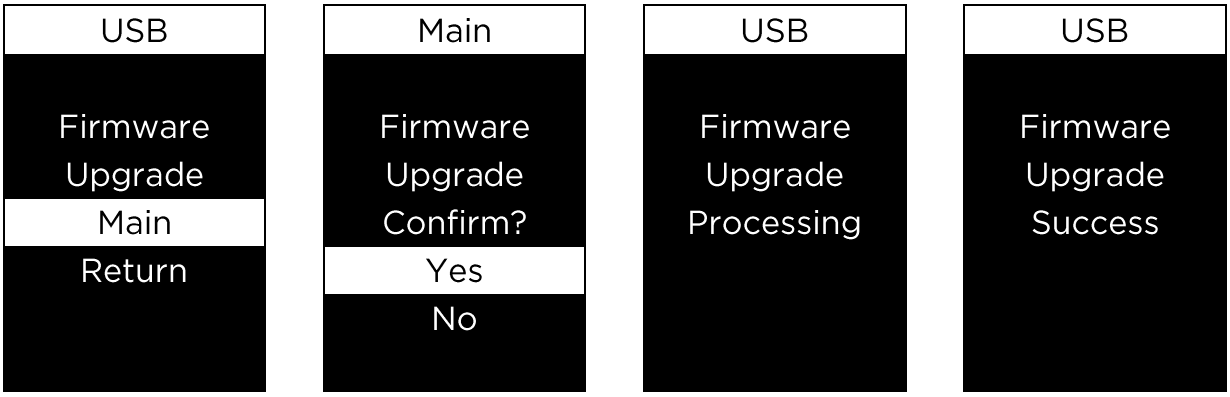
Note: If you don't want to wait for the firmware upgrade, you can stop the process by clicking **Abort** in the **Action** menu. However, this is not recommended because the **Abort** action may cause the device to malfunction.

Option 3: Use a USB Flash Drive

Use the following steps to upgrade the firmware.

1. Download the latest firmware from www.cyberpower.com
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:

(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: `cpsmpdumafw_XXX.bin` and `cpsmpdumadata_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 firmware file `cpsmpdumafw_XXX.bin` first followed by the data file `cpsmpdumadata_XXX.bin`.

(3) `<user>` is the username of the SSH account on the PDU.

(4) 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. The firmware file transfer may take a couple minutes to complete. 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 data file `cpsmpdumadata_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: `cpsmpdumafw_XXX.bin` and `cpsmpdumadata_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 firmware file `cpsmpdumafw_XXX.bin` first followed by the data file `cpsmpdumadata_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. The firmware file transfer may take a couple minutes to complete. 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 data file `cpsmpdumadata_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

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.