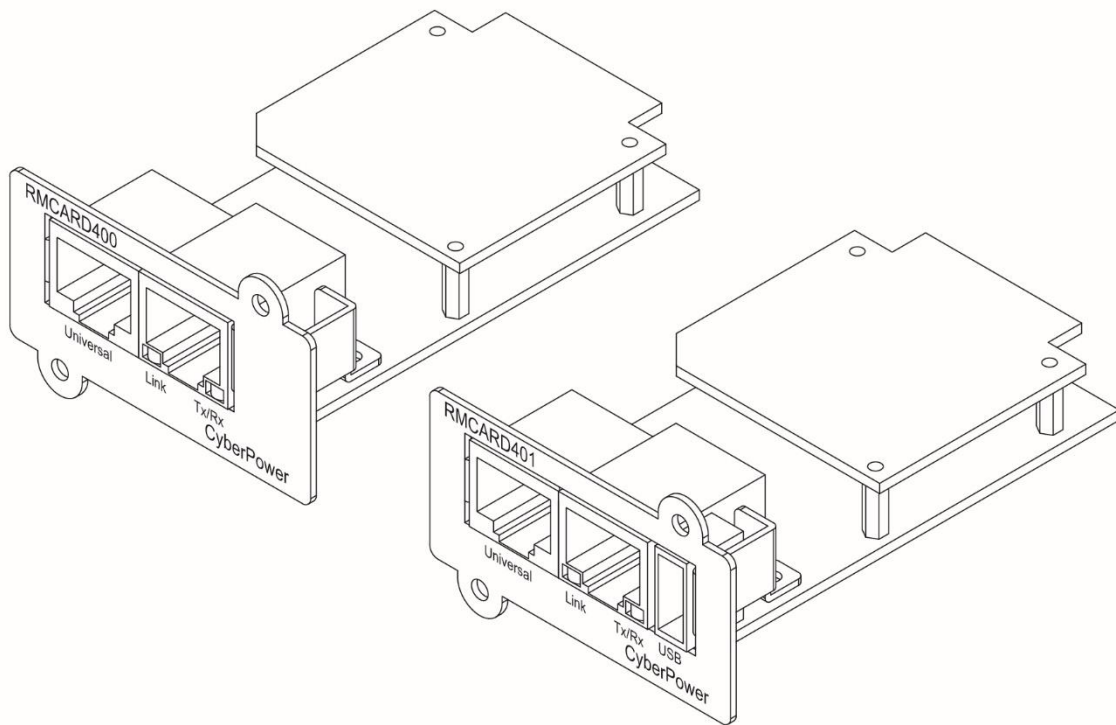**CyberPower**

Remote Management Card

RMCARD400
RMCARD401

The Remote Management Card allows a UPS system and environmental sensor to be managed, monitored, and configured.

TABLE OF CONTENTS

Introduction

Overview

The CyberPower Remote Management Card allows for remote monitoring and management of a UPS attached to a network. After installing the hardware and configuring an IP address, the user can access, monitor, and control the UPS from anywhere in the world! Simply use a web browser, command line interface or SSH client to access your UPS. Servers and workstations can be protected by the UPS utilizing PowerPanel® Business Remote to gracefully shutdown when signaled by the Remote Management Card.

Features

- Real time UPS monitoring
- Remote management and configuration of the UPS via Web Browser, NMS or Command Line Interface (SSH and Telnet)
- Local management and configuration of the UPS via serial connection
- Trigger servers/workstations to shutdown during a power event to prevent data loss or corruption
- Schedule shutdown/start-up/reboot of the UPS remotely
- Event logging to trace UPS operational history
- Graphic data logging to analyze power conditions
- Save and restore configuration settings including current UPS parameter configuration.
- Event notifications via Email, SNMP traps, Syslog, and SMS
- Remote UPS Firmware Upgrade via Web Interface and FTP in Select UPS Models
- Support IPv4/v6, SNMPv1/v3, HTTP/HTTPs, TCP/IP, UDP, DHCP, NTP, DNS, SMTP, SMTPS, SSH, Telnet, FTP and Syslog protocol
- Support Email Secure Authentication Protocols: SSL, TLS
- Support External Authentication Protocols: RADIUS, LDAP, LDAPS, 802.1X, Windows AD
- SNMP MIB available for free download
- User upgradeable firmware via FTP, CyberPower Upgrade and Configuration Utility and Secure Copy Protocol (SCP)
- Upgrade firmware and upload configuration files to multiple units at once
- Multi-language user interface
- Quick installation
- Hot-swappable
- Support Environmental Sensor (ENVIROSENSOR/SNEV001)
- RMCARD400 supports the CyberPower's UPS models which have smart slot. (RMCARD401 supports the new specific UPS models)

System Requirements

- A 10/100/1000Mbps Ethernet connection to an existing network
- Web Browser or SSH client
- (Optional) NMS (Network Management System) compliant with SNMP

Application with PowerPanel® Business
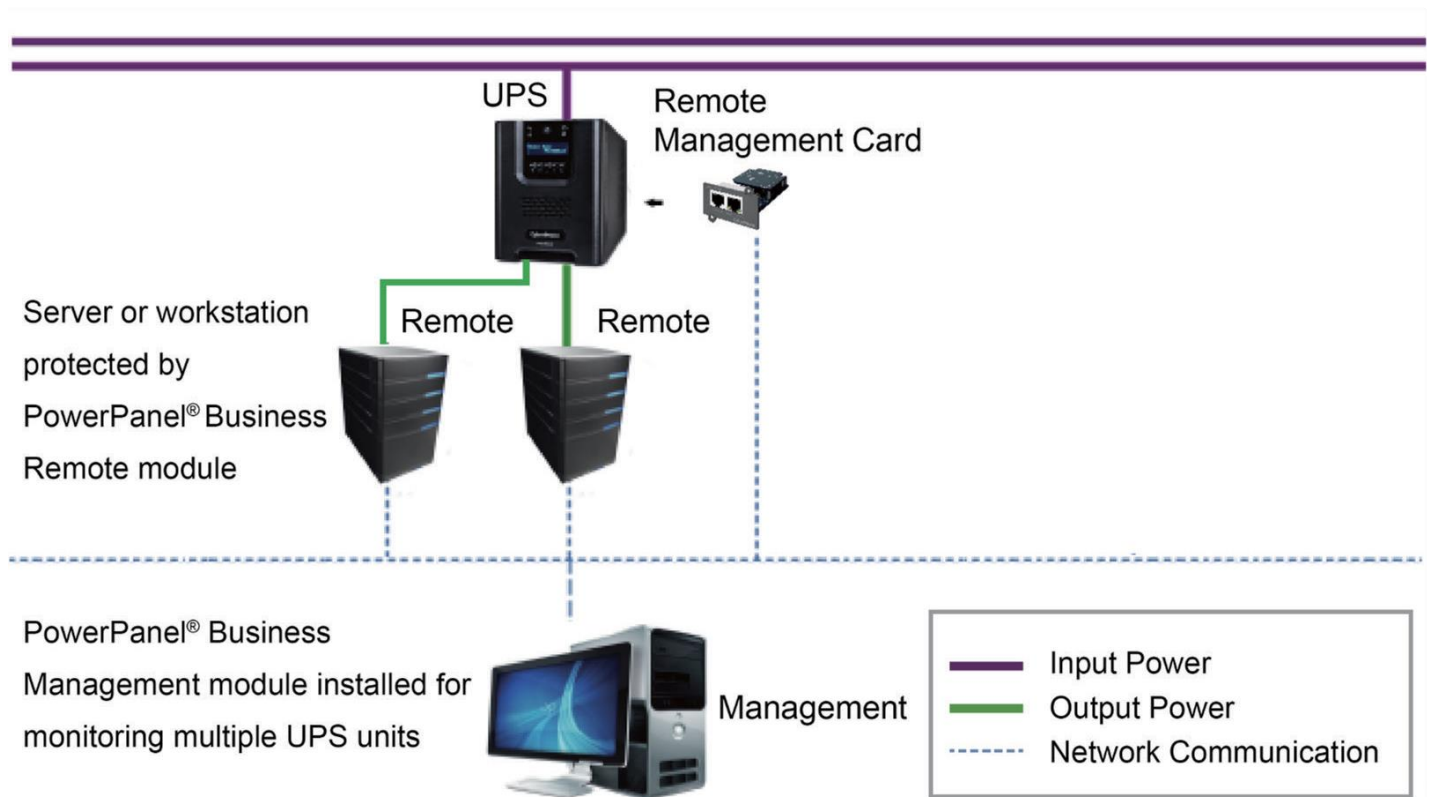
Unpacking

Inspect the Remote Management Card upon receipt. The package should contain the following:

- CyberPower Remote Management Card
- RJ45/DB9 Serial Port Connection Cable
- Quick Start Guide
- Spare Jumper

Front Panel

RMCARD400
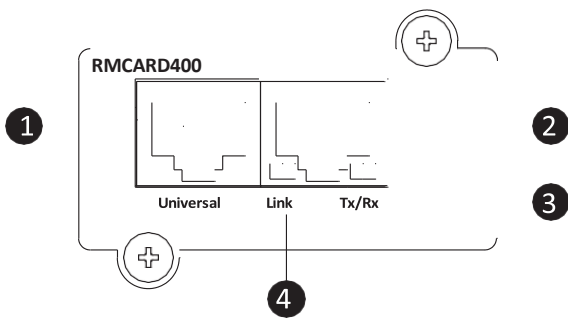
1. Universal Port

2. Ethernet Port

3. Tx/Rx Indicator

4. Link Indicator

5. USB Port

RMCARD401
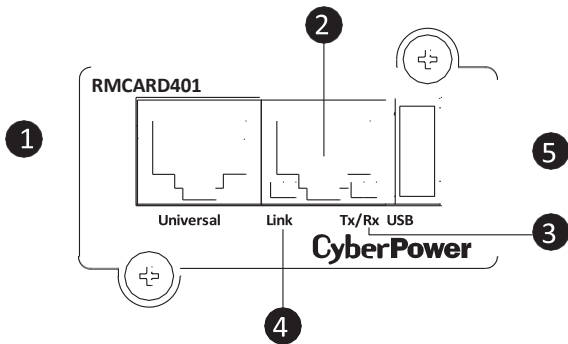
LED Status Indicators

Link LED	Condition
Off	The Remote Management Card is not connected to the Network/ or the Remote Management Card power is off
On (Yellow)	The Remote Management Card is connected to the Network (Up to 10/100Mbps Speed)
On (Green)	The Remote Management Card is connected to the Network (Up to 1000Mbps Speed)
Tx/Rx LED	
Off	The Remote Management Card power is off
On (Green)	The Remote Management Card power is on
Flashing (Green)	- Receiving/transmitting data packet - Reset finished

Installation Guide

Step 1. Hardware Installation

Note: The CyberPower Remote Management Card is hot-swappable, so you do not need to turn off the UPS to install it.

Note: Please do not remove or modify SDCARD on the back. CyberPower is not responsible for any unauthorized modification to RMCARD400/401.

1. Remove the two retaining screws from the expansion slot and remove the cover.

2. Install the CyberPower Remote Management Card into the expansion slot.

3. Insert and tighten the retaining screws.

4. Connect an Ethernet cable to the Ethernet port of the CyberPower Remote Management Card.

5. *(Optional)* To connect an environmental sensor, use a RJ45 Ethernet cable. Connect one end to the Universal port on the RMCARD and the other end into the sensor. For more information, please see the ENVIROSENOR/SNEV001 user's manual.

Note: Please only connect a CyberPower ENVIROSENOR/SNEV001 or the supplied RJ45/DB9 Serial Connection Cable to the Universal port on the RMCARD.

RMCARD400/401
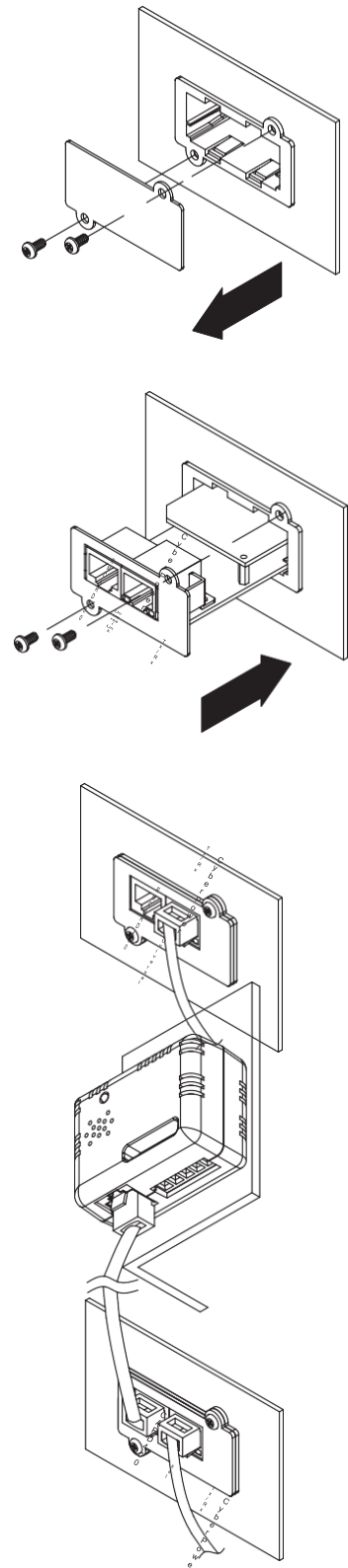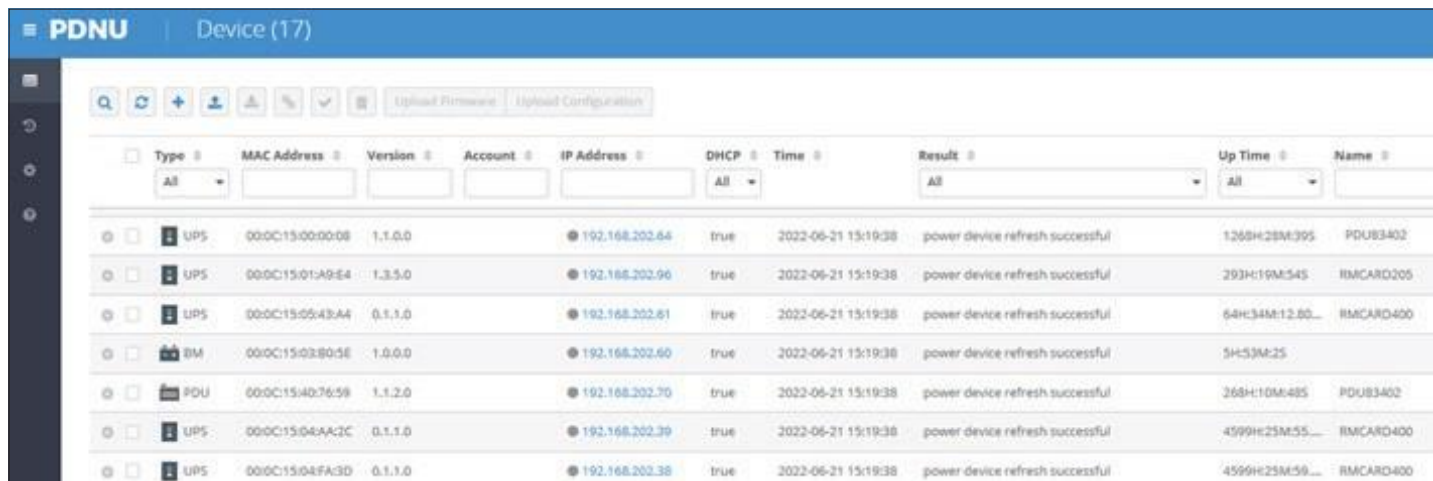
Step 2. Configure the IP address for the CyberPower Remote Management Card

Note: These instructions are for Windows OS. For other OS please refer to Appendix 4.

Method 1: Using the Power Device Network Utility 2

1. Install the Power Device Network Utility available for download at www.cyberpower.com.

2. After installation completes, run the "Power Device Network Utility 2".

3. The main window of the Power Device Network Utility program is shown in Figure 1. The configuration tool will display all CyberPower Remote Management devices present on the local network subnet. The "Refresh" button is used to search the local network subnet again.

Figure 1. The main window of the "Power Device Network Utility 2" program.

4. Select the Remote Management Card you are setting up. Click on the Tools menu and select the Remote Management Card you want to configure. Then, click the "Connection" button on the top tools list to set up.
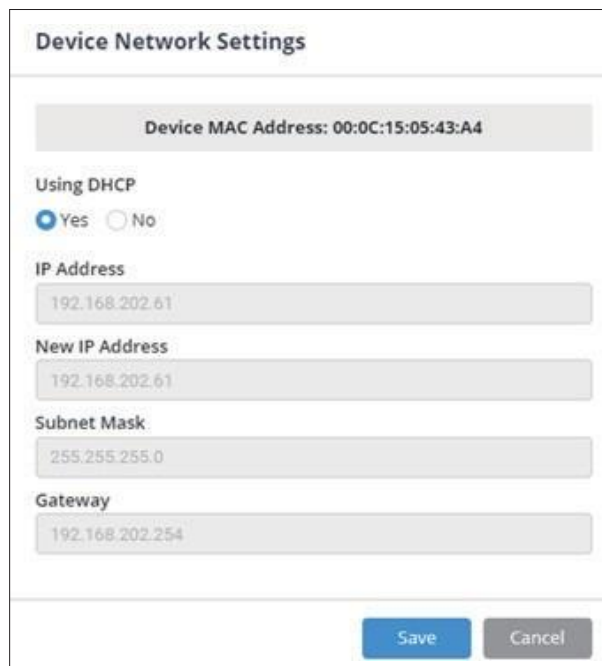
5. You will need to enter a User Name and Password for the Remote Management Card in the authentication window, as shown in Figure 2.
   - Default user name: cyber
   - Default password: cyber

Connection Information

Account

Password

Save   Cancel

Figure 2. The Device Network setting window.

6. You can modify the IP Address, Subnet Mask, and Gateway address for the Device MAC Address listed in the Device Network Settings window, as shown in Figure 3. The factory default IP Address is 192.168.20.177 and the default Subnet Mask is 255.255.255.0.

Device Network Settings

Device MAC Address: 00:0C:15:05:43:A4

Using DHCP
◉ Yes ○ No

IP Address
192.168.202.61

New IP Address
192.168.202.61

Subnet Mask
255.255.255.0

Gateway
192.168.202.254

Save   Cancel

Figure 3. Authentication window.

7. Modify the IP, subnet mask or gateway address. Enter the new addresses into the corresponding fields and then click "Save".

8. In case the change is not successful, for example, if the IP address change is unsuccessful you will see a warning message. Attempt to make the desired changes again. If the problem persists, please see the Troubleshooting section for help.

Web Interface

Login User Account

You will need to enter a User Name and Password to login to the interface, and can select a preferred language after login. There are two user account types.

1. Administrator
   - Default user name: cyber
   - Default password: cyber

2. View only
   - Default username: device
   - Default password: cyber

You will be asked to reset a password upon the first login. The administrator can access all functions, including enable/disable the view only account. The viewer can access read only features but cannot change any settings.

Note: 1 . The Administrator account User Account Authentication HyperText Transfer Protocol (HTTP) HTTP and HyperText Transfer Protocol over Secure Sockets Layers (HTTPS) is also used for the FTP login, Power Device Network Utility, and Upgrade and Configuration Utility.

   2. Up to 15 users can log in and access the device at a time.

Web Content

Note: English is the default language and you can change to a preferred language.

[Summary] Provide an overview of the system operation and the items that are auto refreshed; however, different UPS system models may have different items displayed.

Item	Definition
Current Condition	Display the current operating condition of the UPS and environmental sensor.
UPS Status	
Battery Capacity	Graph of the percentage of the current UPS battery capacity.
Load	Graph of the load of UPS as a percentage of available Watts.
Remaining Runtime	Length of time the UPS can support its load on battery power.
System Data	
Name	The name given to the UPS.
Location	Location description given to the UPS.
Contact	The person to contact about this UPS.
Uptime.	Length of time the system has been working continuously
Envir Status	
Temperature	Graph of the current temperature reading of the environmental sensor.
Humidity	Graph of the current humidity reading of the environmental sensor.

Item	Definition
Envir Data	
Name	The name of the environmental sensor.
Location	The location of the environmental sensor.
Recent Device Events	A list of device events that recently occurred. The maximum number of events is 5.

[UPS] The following items can be displayed/configured through the UPS page; however, different UPS models may have different items displayed/configured.

[UPS->Status] Display the basic information about the current UPS status. Items displayed are auto refreshed.

Item	Definition
Input	
Status	The current status of the utility power supplied to the UPS.
Voltage	The current input voltage of the utility power supplied to the UPS.
Frequency	The current frequency of the utility power supplied to the UPS.
Current	The current of the utility power supplied to the UPS.
Power Factor	The ratio of the real power flowing to the UPS, to the apparent power of utility power.
Bypass	
Status	Displays the present status of bypass circuit.
Voltage	The voltage of the bypass supplied to the UPS.
Frequency	The frequency of the bypass supplied to the UPS.
Current	The current of the bypass supplied to the UPS.
Power Factor	The ratio of the real power flowing to the bypass, to the apparent power of bypass.
Output	
Status	The current status of the output power the UPS is supplying to connected equipment.
Voltage	The output voltage the UPS is supplying to the connected equipment.
Frequency	The output frequency the UPS is supplying to the connected equipment.
Load	The power draw of the connected equipment expressed as a percentage of the total UPS load capacity. This is displayed as watts on some UPS models.
Current	The output current the UPS is supplying to the connected equipment.
Power Factor	The radio of the active power flowing to the load, to the apparent power in the circuit.
Active Power	The capacity of the circuit for performing work in a particular time.
Apparent Power	The product of the current and voltage of the circuit.
Reactive Power	The portion of power flow that is temporarily stored in the form of magnetic or electric fields, due to inductive and capacitive network elements, and then returned to source, is known as reactive power.

Item	Definition
Non-Critical Load (NCL)	The present status of NCL outlets.
Energy	Device energy meter reading in units of kWh. *Click "Reset" will clear Energy value to zero.
Battery	
Status	The present status of the UPS battery.
Charge Mode	SBM Mode: Using Smart Battery Management (SBM) mode to charge the batteries, which helps extend overall battery life, and Fast Charge Technology. Normal Mode: Using normal charge method to charge the batteries.
Charge Check	In SBM Mode: Displays the 3 operation stages (Charge Float Rest Mode) of Smart Battery Management (SBM). In Normal Mode: Displays charger work in Normal Mode.
Remaining Capacity	The present capacity of the batteries, expressed as a percentage of full charge.
Remaining Runtime	The amount of estimated time that the UPS can supply power to its load.
Voltage	The present voltage of the UPS battery.
System	
Status	The present operating status of the UPS.
Temperature	The operating temperature of the UPS.
Maintenance Breaker	Displays the present operating status of maintenance break.

[UPS->Battery Status] Display the information of the built-in battery and the Extended Battery Modules (EBM) including battery pack temperature, voltage of each battery within its pack and battery pack equalization status.

Item	Definition
Last Update Date	The last date that the battery status is updated. Update: Use this function to get the latest battery status.
Pack	The current number of UPS/EBM battery pack.
Temperature	The current temperature reading of UPS/EBM battery pack.
Voltage	The current voltage reading of each UPS/EBM battery.
Equalization Status	Display the current battery voltage equalization status of UPS/EBM battery pack. Active: The battery pack equalization function is active. Inactive: The battery pack equalization function is not active.

[UPS->Information] Display the technical specifications of the UPS.

Information	Description
Model	The model name of the UPS.
Serial Number	The serial number of the UPS.
Voltage Rating	The nominal output voltage rating (Volts) of the UPS.
Working Frequency	The operating frequency of the UPS output power.
Power Rating	The Volt-Amp rating of the UPS.
Current Rating	The output current rating (Amps) of the UPS.
Load Power	The power rating (Watts) of the UPS.
Battery Voltage Rating	The operating DC voltage rating of the battery power.
Firmware Version	The revision number of the UPS firmware. Update: Use this function to upgrade the UPS firmware. For further information, please refer to Appendix 3.
USB Firmware Version	The revision number of the UPS USB firmware
LCD Firmware Version	The revision number of the UPS LCD firmware
Battery Replacement Date	The date that the batteries were last replaced. This must be set manually after the batteries have been replaced or when the unit is first installed. If this date has not been set, it is recommended that it be set immediately.
NCL	The amount of Non-Critical Load banks.
Extended Battery Pack	The amount of the external battery modules connected to the UPS. The number of modules is configured manually, and the configurations will vary by model.
Installation Place	When clicking the "Find it" button, either the alarm will beep or the indicators will flash on the UPS to alert users of the specific location. This helps users to identify a specific UPS in lots of UPS.

[UPS->Configuration] Configure the parameters of the UPS.

Item	Definition
Supplied Power	
Voltage	Set the UPS output voltage that is supplied to the connected equipment. Note: On some models belong to Paragon Tower series, this setting becomes configurable in Bypass Mode and the changes require a restart to activate.
Utility Power Failure Condition	
High/Low Input (or Output) Voltage Threshold	When the utility power voltage or output voltage (depending on UPS model) is higher/lower than the threshold, the UPS will supply battery power to the connected equipment.

Item	Definition
Utility Sensitivity	When the UPS detects the utility voltage is out of range, the UPS will switch to battery mode to protect the equipment plugged into the UPS. Low sensitivity has a looser voltage range and the supplied power may vary more widely. The power from fuel generator may cause the UPS to switch to battery mode more frequently, and the low sensitivity is recommended. The UPS switches to battery mode rarely and also saves more battery power. High sensitivity allows the UPS to supply more stable power to equipment and switches to battery mode frequently.
Frequency Tolerance	Sets the acceptable range of the input frequency. The UPS will supply battery power to the connected equipment if it is out of tolerance.
Operation	
Normal	Normal operating mode of the UPS.
Generator Mode	If the UPS uses generator as its input power, this option should enable the UPS to function normally. If this option is selected, the UPS will be forbidden to enter Bypass Mode or ECO Mode to protect the connected equipment.
ECO Mode	Economy mode. The UPS will enter Bypass Mode when the input voltage/frequency is within the configured threshold. Once the utility voltage/frequency exceeds thresholds, the UPS will switch to Normal operation. This mode will significantly increase UPS system efficiency.
Manual Bypass	Determines whether to allow the UPS to enter Manual Bypass Mode. If this option is enabled, the UPS will be forced to enter Bypass Mode.
Bypass	Note: The UPS may automatically enter Bypass Mode per these configured settings.
Bypass Condition	No Bypass: If this option is selected, the UPS will not enter Bypass Mode and will stop supplying output power. Check Volt/Freq: If the utility voltage is in the range of the voltage thresholds and the utility frequency is in range of the frequency tolerance, the UPS will enter Bypass Mode. Otherwise, the UPS will stop supplying output power. Check Volt Only: Only if the utility voltage is in the range of the voltage thresholds, the UPS will enter Bypass Mode. Otherwise, the UPS will stop supplying output power.
Bypass When UPS Off	When the UPS turn off, the UPS switch to Bypass Mode.
Power Restore	After utility power is restored, the UPS turns on automatically and supplies power to the connected equipment. The following settings are used to configure the UPS restore behavior:
Automatic Restore	When this option is enabled, the UPS will restore output immediately when the utility power restores. When this option is disabled, the UPS will not restore output until it is turned on manually at a later time.
Recharged Delay	When utility power restores, the UPS will start to recharge until the specified time has elapsed before restoring output power.
Recharged Capacity	When utility power restores, the UPS will start to recharge until the specified battery capacity is met before restoring output power.
Returned Delay	The Returned Delay will take effect every time when the UPS is turned on.

Item	Definition
Line Stable Delay	When the UPS is in Battery Mode and utility power is restored, the UPS will wait for the specific delay time to change Battery Mode to Line Mode. When the UPS battery is lower than the Low Battery Threshold and utility power is restored, the UPS will return to Line Mode immediately.
Battery	
External Battery Set	Number of parallel sets and the battery capacity.
Low Battery Threshold	When the UPS supplies battery power and the remaining capacity is lower than this threshold, the UPS will sound an alarm.
External Battery Modules	Set the amount of external battery modules. This allows for an accurate runtime estimation based upon the total number of batteries connected to the UPS.
Periodical Battery Test	The UPS will cyclically perform the battery test automatically to ensure the batteries have full functional. Note: Only Online (OL) series support the Smart Battery Management (SBM) feature. SBM carries out battery tests, even if Periodical Battery Test setting is disabled.
Charge Mode	Normal Mode: Using normal charge method to charge the batteries. SBM Mode: Activating the Smart Battery Management to charge the batteries.
Charge Check	Sets Enabled/Disabled to constantly monitor the charger function.
Self-Test On UPS Startup	When this option is enabled, the UPS will perform the self-test automatically when the UPS is turned on. Note: The self-test will not be triggered when the UPS is having an Auto-Restart.
System	
Cold Start	Set the ability of the UPS to start in the absence of input power. When this option is enabled, the UPS can be turned on with battery power.
Audible Alarm	If this option is enabled, the UPS will issue an audible alarm when supplying battery power, when output is overloaded, or other conditions are present (varies by UPS model).
Dry Relay Function	This configures the UPS dry relay to function when the selected condition occurs. Refer to the UPS manual for further information about advanced UPS dry relay functions. The Dry Relay Function can be configured to be activated under the following power conditions: (1) Utility Failure: The utility power fails and the UPS is using battery power. (2) Low Battery: The battery capacity is too low to support the connected computers to shut down. (3) Alarm: The UPS is issuing the audible alarm due to the occurrence of warning events, such as overload. (4) Bypass: The UPS has switched to Bypass Mode. (5) UPS Fault: The UPS could be malfunctioning due to hardware fault.

Item	Definition
Screen Save Time	When no UPS button is pressed and no power event occurs during this time, the LCD screen will go to sleep.
Wiring Fault Detecting	If this option is enabled, the UPS will detect if the input wiring is not grounded or is reversed. It is recommended to ensure the UPS wiring has a ground connection first.
Over Discharge Protection	When the UPS is in Battery Mode with 0% for the time configured, the RMCARD will switch the UPS to Sleep Mode and the output will be turned off.
Enter Sleep Mode After All Remote Shutdown	If this option is enabled, the UPS will enter sleep mode after all PowerPanel® Remote shutdown +2 minutes. Note: For PowerPanel® Business Edition Clients, if this option is enabled, the UPS will enter sleep mode after utility power fails and remaining MSDT+2 minutes. For more information about MSDT please reference the help page in UPS -> PowerPanel List.
Non-Critical Outlet Bank	
Turn Off Threshold	When supplying battery power, the UPS will power off this NCL outlet bank if the remaining battery capacity is lower than this threshold.
Turn off Delay	When supplying battery power, the UPS will power off this NCL outlet bank after this delay time is met.
Turn On Delay	When utility power is restored, the UPS will restore the output of this NCL outlet bank after the delay time is met. This prevents excessive power consumption caused by all the connected equipment starting at the same time.

[UPS->Master Switch] Switch the output power of the UPS to be on or off.

Item	Definition
Reboot UPS	Turns the UPS off and back on.
Turn UPS Off	Turns the UPS off.
UPS Sleep	This command is available in Utility Power Failure Mode. It puts the UPS in sleep mode until power is restored. Note: Some UPS models may not support this command.
Reset	Resets the pending action to turn the UPS off.
Turn UPS On	Turns the UPS on.

Item	Definition
Shutdown/Sleep Delay	Amount of time the UPS waits before it turns off in response to a "Reboot UPS", "Turn UPS off" or "UPS Sleep" command.
Reboot Duration	After the UPS is turned off, Reboot Duration defines how long the UPS waits before it turns back on response to "Reboot UPS" command.
Signal PowerPanel® Remote to Shutdown	Select this option to warn PowerPanel® Business Remote before turning the UPS off. The Shutdown Delay (MST, Max Clients Shutdown Time) for the UPS can be changed to insure a graceful shutdown.

[UPS->Bank Control] Display the current state of each outlet Bank, and it provides on/off control for the Critical/Non-Critical Outlet Bank. Outlet Number and Device Name displays the device name associated with the specific outlet.

Item	Definition
Bank Control Options	
ON	Turns critical/non-critical bank on immediately.
OFF	Turns critical/non-critical bank off immediately.
Device Name Identification	
Outlet #	UPS outlet number as designated by the outlet configuration (varies by UPS model).
Device Name	Device Name assigned to this outlet.

Note: Only Critical Outlet Bank switchable UPS support on/off control for the Critical Outlet Bank.

[UPS->Diagnostics] The **UPS/Diagnostics** page provides the ability to verify UPS batteries are in adequate working conditions. You can also complete a runtime calibration to insure an accurate estimation for the connected load.

Item	Definition
Battery Test	The Battery Test will force the UPS to switch to battery power for 10 seconds. This allows the user to verify the battery conditions and provides information about the battery, including the results and date of the last battery test. Click the "Start" button to begin a battery test. The information will be reported after a battery test completes. Note: "N/A" means the UPS model does not have this function.
Start	Execute the battery test immediately.
Last Test Result	The results of the most recent battery test. Passed: The battery performed normally during the test. Failed: The battery test did not pass. Follow the steps below if the battery test fails: Repeat the battery test and replace the batteries if the test fails again. Contact CyberPower for assistance if the battery test fails after the batteries have been replaced.

Item	Definition
Last Test Date	The date of the most recent battery test.
Runtime Estimation	The Runtime Estimation function discharges the UPS batteries from the battery capacity, at the time the estimate is requested, to near zero capacity with the current load. The results of the runtime estimation show the runtime, status of estimation, and the date of the last estimation. When the runtime estimation is initiated, the connected equipment will be run on battery power until the batteries are discharged to near zero capacity. Once the batteries are discharged to this point, the connected equipment will run on utility power. The batteries will then be recharged automatically after the estimation is done. Note: This estimated runtime may vary based on the load and the level of charge on the batteries when the runtime estimation is initiated. The batteries will be recharged then automatically after the estimation is done. Users can click the "Start" button to initiate the runtime estimation. Click the "Abort" button to interrupt the runtime estimation. The result will be reported after the runtime estimation is finished or canceled:
Estimated Runtime	The estimated runtime of the batteries with the current load.
Last Estimation Result	The results of the last Runtime Estimation. Passed: The runtime estimation was completed and the batteries are good. Canceled: The runtime estimation was interrupted.
Last Estimation Date	The date the last runtime estimation was performed.

[UPS->Schedule]: Sets the UPS to automatically shutdown and restart at scheduled times (Once/Daily/Weekly). The Schedule page manages scheduled shutdowns and lists all configured schedules. Each schedule row displays the details of when the schedule will take effect.

[Once]: The user may set one time event for the UPS to shutdown/restart. [Daily]: Set a daily re-occurrence for the UPS to shutdown/restart. [Weekly]: Set a weekly re-occurrence for the UPS to shutdown/restart.

1. Click [Once], [Daily] or [Weekly] option and Click "Next>>", Enter the date and time to shut down the UPS. Select [Never], [Instant], or the date and time for the UPS to turn back on. Select the bank to be controlled, and click "Shutdown Clients" to set all clients to perform a graceful shutdown. You can enter a "Name" for this Schedule.

2. Click "Apply" to add the item to the Schedule. Click "Reset" to return to default settings..

3. Saved settings are listed in [Schedule] menu.

4. If you want to delete the scheduled action, simply click the Name of the item listed in [Schedule] menu, and click "Delete".

Note: The management system allows up to 10 schedule entries.

[UPS->Wake on Lan] This function is used to wake a computer through the network. Enter the IP address of that computer when it is on and the system will search its MAC address accordingly. The maximum number of IP addresses that can be set is 50.

Item	Definition
PowerPanel® Remote	
Load/Sync with PowerPanel® Remote List	Enable this option to Load and Synchronize WoL Client List with PowerPanel® Remote List.
Wake Conditions	
UPS Turn On	When selected, this option will enable the RMCARD to send the WoL signal to the connected PowerPanel® Remote computers when the UPS turns on.
Utility Power Restore and Output is Supplied	When selected, this option will enable the RMCARD to send the WoL signal to the connected PowerPanel® Remote computers when utility power is restored and UPS output is on.
WoL Lists	
WoL Remote List	When the option "Load/Sync with PowerPanel® Remote List" is enabled, it will list PPB Remote PC IP/MAC here.
WoL Manual List	Wake on Lan manual list.

Note: The PowerPanel® Remote computer's BIOS settings need to support WoL and be configured accordingly.

[UPS->PowerPanel® List] Display the Information of the connected PowerPanel® Business. The connection is established by PowerPanel® Business. The listed will be removed if disconnected for 1 hour.

Item	Definition
Configuration	
Max Remote Shutdown Time (MST)	The max time that all the connected Remote require to shutdown.
Max Remote Shutdown Delay Time (MSDT)	The max value required from the moment utility power fails until all the clients gracefully shutdown.
List	
Type	The type of PowerPanel® Business • Remote • Management
Shutdown Condition	The shutdown condition of PowerPanel® Business • None • Power Failure • Low Battery • Runtime Insufficient
The status of PowerPanel® Business	The status of PowerPanel® Business • Connecting • Normal • Shutdown is processing • Shutdown is complete

Note: It is not suggested to have the PowerPanel® Business Edition or PowerPanel® Business connection to the RMCARD at the same time.

[Envir] Following items can be displayed/configured through the Envir page. Note that Envir Tab only appears when an ENVIROSENSOR is connected to the RMCARD.

[Envir->Status] Display the basic information of the environmental sensor and contact closure inputs.

Item	Definition
Information	
Name	The name of the environmental sensor.
Location	The location of the environmental sensor.
Temperature	
Current Value	The current environmental temperature.
Maximum	The highest temperature and time detected by the environmental sensor.
Minimum	The lowest temperature and time detected by the environmental sensor.
Humidity	
Current Value	The current environmental humidity.
Maximum	The highest humidity and time detected by the environmental sensor.
Minimum	The lowest humidity and time detected by the environmental sensor.
Contact	Display the name and status (Normal/Abnormal) of each input dry relay contact.

[Envir->Configuration] Configure the parameters of the environmental sensor.

Item	Definition
Information	
Name	The name used to identify the environmental sensor.
Location	The place where the environmental sensor is located.
Temperature	
High Threshold	Upper limit for normal temperature.
Low Threshold	Lower limit for normal temperature.
Hysteresis	The point at which the difference between the High and Low temperature threshold changes from abnormal to normal.
Rate of Change	The rate used to define an abnormal change in temperature.
Unit	The unit of temperature measurement.
Humidity	
High Threshold	Upper limit for normal humidity.
Low Threshold	Lower limit for normal humidity.
Hysteresis	The point at which the difference between the High and Low humidity threshold changes from abnormal to normal.
Rate of Change	The rate used to define an abnormal change in humidity.
Contact	Enter the name of each input dry contact relay and use the dropdown menu to define the normal status of each one.

[Accessory] Following items can be displayed/configured through the Accessory page.　Note that Accessory Tab only appears when a new version of the environmental sensor (SNEV001) is connected to the RMCARD.

[Accessory->Status->ENV Basic Status] Display the basic information of the environmental sensor.

Item	Definition
Information	
Name	The name of the environment sensor.
Location	The location of the environment sensor.
Temperature	
Current Value	The current temperature of the environment.
Maximum	The highest temperature as well as the time of occurrence is detected by the environment sensor.
Minimum	The lowest temperature as well as the time of occurrence is detected by the environment sensor.
Humidity	
Current Value	The current humidity of the environment.
Maximum	The highest humidity as well as the time of occurrence is detected by the environment sensor.
Minimum	The lowest humidity as well as the time of occurrence is detected by the environment sensor.

[Accessory->Status->ENV Contact Status] Display the basic information of the contact closure inputs.

Item	Definition
Information	
Contact	Display the name and status (Normal/Abnormal) of each input dry contact.

[Accessory->Information] Display the basic information of the accessory device.

Item	Definition
Information	
Position	The position of the accessory device.
Model	The model name of the accessory device.
Serial Number	The serial number of the accessory device.
Hardware Version	The hardware version of the accessory device.
Firmware Version	The firmware version of the accessory device.
Firmware Update	
Update the firmware of the accessory de vice. Click Browse to the location of the accessory binary file and click Submit to upload the file.	

[Accessory->Configuration->ENV Basic Configuration] Configure the parameters of the environmental sensor.

Item	Definition
Information	
Name	The name used to identify the environmental sensor.
Location	The place where the environmental sensor is located.
Temperature	
High Threshold	The upper limit for normal temperature.
Low Threshold	The lower limit for normal temperature.
Hysteresis	The difference between High/Low Threshold and the point where the temperature state is from abnormal to normal.
Rate of Change	The rate is used to define an abnormal change in temperature.
Unit	The unit of temperature.
Humidity	
High Threshold	The upper limit for normal humidity.
Low Threshold	The lower limit for normal humidity.
Hysteresis	The difference between High/Low Threshold and the point where the humidity state is from abnormal to normal.
Rate of Change	The rate is used to define abnormal changes in humidity.

[Accessory->Configuration-> ENV Contact Configuration] Configure the parameters of the contact closure inputs.

Item	Definition
Contact	Enter the name of each input dry contact relay and use the dropdown menu to define the normal status of each one.
Name	The name is used to identify the contact.
Status	The state is used to define the normal condition of the contact.

[Logs->Event Logs] Display the list of events and a brief description of each event along with the date and time stamp.

Note: 1. The recordable events are listed under "System->Notifications->Event Action."
　　　2. The recorded time is using the 24-hour clock format.

[Logs->Status Records] This page is used to view the logs of the UPS status and environment status; however, different products may have different items displayed.

All items have the same definition as they are in the UPS status or environmental status.

- Input min (V): The minimum input voltage of the utility power from the previous record.
- Input max (V): The maximum input voltage of the utility power from the previous record.
- Input (Hz): The current frequency of the utility power supplied to the UPS.
- Output (V): The output voltage of the UPS supplying to the connected equipment.
- Output (Hz): The output frequency of the UPS supplying to the connected equipment.
- Load (%): The percentage of the total UPS power being supplied to the connected equipment.
- Capacity (%): The percentage of the current UPS battery capacity.

- Remaining Runtime: The estimated duration of time that the UPS can support the connected load in battery mode.
- Temperature (°C or °F): The current temperature of the environmental sensor.
- Humidity (%RH): The current humidity of the environmental sensor.

[Logs->Energy Records] Energy Records page displays a list of energy records along with a date and time stamp.

Item	Definition
Energy	Energy used by the device during a specific interval, measured in kWh.
Cost	Cost of the energy used by the device during a specific interval.
CO2	CO2 emissions of the device during a specific interval.
Accumulated Energy	Cumulative energy used by the device since the last reset, measured in kWh.
Accumulated Cost	Cumulative cost of the energy used by the device since the last reset.
Accumulated CO2	Cumulative CO2 emissions from the device since the last reset.

[Logs->Graphing] This page is used to display the data of the Status Record. The graphing function makes the status records easier to view.

Item	Definition
Graph Period	The period used to draw the graph. Longer periods will require more time to be displayed.
Graph Data	The data used to draw the graph. The more data selected, the more graphing time is needed.
Graph Node	Selecting "Display All Nodes in Detail" will display all the points along the line; moving the cursor on the data point will show the information of that point.
Launch Graph in New Window	Checking this box will open the graph in detail in a new page.

[Logs->Maintenance] This page is used to select "Event Logs" and "Status Records" settings. The application provides information on how many events are recorded before it is full.

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	Set the frequency status data is recorded. A smaller interval will provide more frequent recordings but exhaust available memory quicker. A larger interval will provide less frequent recordings, but save data for a longer period of time.
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 for recording the energy data.
Clear Entire Records	Clear the existing energy records
Electricity Rate	The ratio of energy cost to energy.
CO2 Emissions	The ratio of CO2 emissions to energy.
Save Energy Records	Save the existing event logs as a text file.

Note: Event Logs and Status Records use a First In First Out memory. Oldest data will be rewritten once memory is full.

[Logs->Syslog] Allow users to set syslog server and send test message.

Item	Definition
Syslog Servers	
Server IP	The IP address of Syslog server.
Server Port	The UDP port used by the Syslog server.
Syslog Setting	
Syslog	Enable or disable Syslog function.
Facility Code	Select Syslog facility.
Syslog Test	
Severity	Select Syslog Severity with this message.
Syslog Message	Type the message that will send to Syslog server.

[System->General->Time] Display the system date and time and allow users to set it manually or by using the NTP (Network Time Protocol) server.

Item	Definition
Current Settings	Displays the current date and time on the card status and time until the next Network Time Protocol (NTP) update. To set the date and time, users can choose to set it manually or by using the NTP (Network Time Protocol) server.
System Time Configuration	
Time Zone	Choose the RMCARD time zone in GMT (Greenwich Mean Time).
DST Configuration	Enable or disable the daylight-saving time function.
Date Format	Choose the different kind of date format.
Using NTP server	Enter the IP address/domain name of NTP servers, and set the frequency to update the date and time from NTP server. Click "Update right now" to update immediately.
Manual Setup	Enter the date and time in the designated format.

[System->General->Identification] Assign the system's name, contact, and location.

Item	Definition
Name	The name of the equipment.
Synchronization with Host Name	Allow the host name to be synchronized with the identification name so both fields automatically contain the same value. Note: When enabling this feature, the identification name can only contain numbers (0-9), letters (a-z, A-Z), hyphen and decimal point. Allow the identification name to be synchronized with the host name so both fields automatically contain the same value.
Location	Where the power equipment is located.
Contact	The person to contact about this equipment.

[System->Security->Management] Set for login authentication and software authentication.

Item	Definition
Login Authentication	
Local Account	Use local account Administrator or Viewer settings to log in.
RADIUS, Local Account	Use RADIUS configuration settings to log in. If RADIUS authentication fails then Local Account settings will be used to log in.
RADIUS Only	Use RADIUS configuration settings to log in.
LDAP, Local Account	Use LDAP configuration settings to log in. If LDAP authentication fails then Local Account settings will be used to log in.
LDAP Only	Use LDAP configuration settings to log in.
Software Authentication	
Secret Phrase	The Authentication Phrase used to communicate with PowerPanel® Business Remote. Note: For more information, please refer to Appendix 4.
Admin/Viewer Manager IP	This setting determines what IP address is allowed to access the device using either Admin or Viewer accounts. If you want to access Remote Management Card from any IP address, you can set one of them as 0.0.0.0 or 255.255.255.255. Note: A range of IP addresses can be allowed by entering the subnet mask. For example, 192.168.20.0/16 means the IP which has subnet of 192.168.0.0 can be allowed to access.

[System->Security->Local Account] This page is used to configure the login account.

Item	Definition
Administrator	Administrator has full access to read/write configuration settings.
Viewer	Viewer has restricted access to read only.

Change Administrator account:

1. Enter User Name

2. Enter Current Password

3. Set the Manager IP (optional)

4. Enter New Password

5. Enter Confirm Password

6. Click "Apply"

Note: The maximum length of both User Name and Password is 63 characters.

Change Viewer account:

1. Select "Allow Access" to enable the Viewer account

2. Enter the User Name

3. Set the Manager IP (optional)

4. Enter New Password

5. Enter Confirm Password

6. Click "Apply"

Note: The maximum length of both User Name and Password is 15 characters.

[System->Security->RADIUS Configuration] After setting the proper RADIUS server, the Remote Management Card can use user name and password set on the RADIUS server to login.

Item	Definition
Server IP	The IP address/domain of RADIUS server.
Shared Secret	The shared secret of RADIUS server.
Server Port	The UDP port used by the RADIUS server.
Authentication Type	The authentication protocol type for RADIUS Server. • Password authentication protocol (PAP) • Challenge-Handshake Authentication Protocol (CHAP)
Timeout	The time of waiting to login Radius server.
Test Setting	Test RADIUS server using user name and password settings. If authentication is successful the settings will be saved.
Skip Test	Save RADIUS server settings without testing.

Note: Please refer to Appendix 2 for the account configuration in RADIUS servers.

[System->Security->LDAP Configuration] After setting the proper LDAP server, the Remote Management Card can use user name and password that set on the LDAP server to login.

Item	Definition
LDAP Server	
LDAP Server	The IP address/domain of LDAP server.
LDAP SSL	Enable to communicate with LDAP server by LDAPS.
Port	The TCP port used by the LDAP(S) server.
User Base DN	The Base DN of LDAP server.
Login Attribute	The Login Attribute of LDAP user entry (for example: cn or uid).
LDAP Authentication	
Authentication Mode	Identifies the method to use for authentication. • Anonymous: Bind Request using Simple Authentication with a zero-length bind DN and a zero-length password. • Accredited User: Bind Request using Simple Authentication with a Bind DN and Bind Password. • By Logon User: Bind Request using Simple Authentication with a User Base DN and login Password.
LDAP Authorization	
Authorization Mode	Identifies the method to use for authorization. • By User Attribute: Determine access level by User Attribute and User Attribute Value. • By Group: Determine access level by group witch search DN information such as the following Group Base DN, Group Attribute and Group Attribute Value.
LDAP Server Type	
Generic LDAP Server	Select LDAP server type as OPENLDAP.
Active Directory	Select LDAP server type as Windows AD.
AD Domain	The AD Domain of the Active Directory server.
LDAP Test	
Test Setting	Test LDAP(S) server using user name and password settings. If authentication is successful the settings will be saved.
Skip Test	Save LDAP(S) server settings without testing.

Note: Please refer to Appendix 2 for the account configuration in LDAP & Windows AD servers.

[System->Security->Session Control] Set for timeout setting for open sessions to automatically log off.

Item	Definition
Timeout	The period (in minutes) that the system waits before automatically logging off.

[System->Security->802.1X] In an EAPoL (Extensible Authentication Protocol over LAN) architecture used in IEEE 802.1X port- based network access control, the RMCARD acts as a supplicant. The RMCARD supports EAP-TLS for authentication, requiring users to upload 3 client-side certificates. Private keys are stored encrypted. A valid passphrase is needed to enable 802.1X security access.

Item	Definition
Information	
Enable	Used to enable or disable 802.1X Security Access.
Supplicant Identifier	Allows the users to set their own supplicant identifier (up to 32 characters including whitespace).
CA Root	
CA Root Status	Successfully upload or not.
CA Root upload	Upload/replace or remove a CA root certificate.
Certificate	
Certificate Status	Successfully upload or not.
Certificate upload	Upload/replace or remove a certificate.
Private Key	
Private Key Status	Successfully upload or not.
Private Key upload	Upload/replace or remove a Private Key.
Passphrase	Provide the passphrase to decrypt the encrypted private. Note: The maximum length of passphrase is 64 characters.

[System->Network Service->TCP/IPv4] Display the current TCP/IPv4 settings. Set DHCP and DNS server settings.

Item	Definition
Current Configuration	Displays the current TCP/IP settings: IP address, subnet mask, gateway, and DNS server, Active Host Name, and Active Domain Name
DHCP	Select the "Enable DHCP" option and click "Apply" to get IP address, Subnet Mask, and Gateway from DHCP server. Select the "Obtain DNS Address from DHCP" and click "Apply" to get the IP of DNS from the DHCP server.
Manual	Enter the TCP/IP settings directly and click "Apply".
Host Name	Register host name to DNS Server. Host Name - Configure a host name. Synchronization with Identification Name - Allow the identification name to be synchronized with the host name so both fields automatically contain the same value. Note: When enabling this feature, the identification name can only contain numbers (0-9), letters (a-z, A-Z), hyphen and decimal point. Allow the identification name to be synchronized with the host name so both fields automatically contain the same value.

[System->Network Service->TCP/IPv6] Display and configure the current IPv6 settings.

Item	Definition
IPv6 Interface	Displays the current IPv6 address.
IPv6 Gateway	Displays the current IPv6 gateway.
IPv6 Configuration	
Access	Set the IPv6 service to either Enable or Disable.
Address Mode	
Router Control	The IPv6 address is assigned through one of the following methods as configured in the router settings: Stateless Address Auto-configuration, Stateless DHCPv6 or Stateful DHCPv6.
Manual	The IPv6 address is assigned manually.
Manual IPv6 Address	Enter the IPv6 address directly when the Manual setting is selected

[System->Network Service->SNMPv1 Service] Allow users to use a NMS and configure the appropriate SNMPv1 settings.

Item	Definition
SNMPv1 Service	
Allow Access	Set the SNMP service to either Enable or Disable.
SNMPv1 Access Control	
Community	The name used to access this community from a Network Management System (NMS). The field must be 1 to 15 characters in length.
IP Address	NMS access can be restricted by entering a specific IP address or an IP network subnet mask. The following subnet mask rules apply: • 192.168.20.255: Access only by an NMS on the 192.168.20 segment. • 192.255.255.255: Access only by an NMS on the 192 segment. • 0.0.0.0 (the default setting) or 255.255.255.255: Access by any NMS on any segment.
Access Type	The allowable action for the NMS through the community and IP address. • Read Only: GET command allowed any time; SET command restricted. • Write/Read: GET command allowed any time; SET command allowed anytime unless a user session is active. • Forbidden: GET and SET commands are restricted.

[System->Network Service->SNMPv3 Service] Allow users to use a NMS and configure the appropriate SNMPv3 settings.

Item	Definition
SNMPv3 Service	
Allow Access	Set the SNMPv3 service to either Enable or Disable.
SNMPv3 Access Control	
User Name	The name to identify SNMPv3 user. The field must be 1 to 31 characters in length.
Authentication Protocol	The hash type for authentication.
Authentication Password	The password used to generate the key used for authentication. The field must be 16 to 31 characters in length.
Privacy Protocol	The type of data encryption/decryption.
Privacy Password	The password used to generate the key used for encryption. The field must be 16 to 31 characters in length.
IP Address	- NMS access can be restricted by entering a specific IP address or an IP network subnet mask. The following subnet mask rules apply: 192.168.20.255: Access only by an NMS on the 192.168.20 segment. 192.255.255.255: Access only by an NMS on the 192 segment. 0.0.0.0 (the default setting) or 255.255.255.255: Access by any NMS on any segment.

Note: The privacy protocol cannot be selected if no authentication protocol is selected.

[System->Network Service->Web Service] Select Enable to allow access to the HTTP or HTTPS Service and configures the TCP/IP port for them.

Item	Definition
Access	
Allow Access	Enable the access to HTTP or HTTPS service. The HTTPS supports encryption algorithm list as follow: • AES (256/128 bits) • Camellia (256/128 bits) • DES (168 bits) Note: HTTP and HTTPS are both enabled by default.
Http Settings	
Http Port	The TCP/IP port of the Hypertext Transfer Protocol (HTTP) (80 by default)
Https Settings	
Https Port	The TCP/IP port of the Hypertext Transfer Protocol Secure (HTTPS) (443 by default)
Certificate Status	• Valid Certificate (or Invalid Certificate): Click to view Certificate detailed information. • Upload Certificate: Click to upload a certificate and replace the current one. Note: The format of uploading certificate must in a standard PEM (Privacy Enhanced Mail).

[System->Network Service->Console Service] Select Enable to allow access to the Telnet or SSH Service and configures the TCP/IP port that Telnet or SSH uses to communicate.

Item	Definition
Access	
Allow Access	Enable the access to Telnet or SSH version 2, which encrypts transmission of user names, passwords and data.
Telnet Port	The TCP/IP port (23 by default) that Telnet uses to communicate.
SSH Settings	
SSH Port	The TCP/IP port (22 by default) that SSH uses to communicate.
Hostkey Status	• Display the status of hostkey fingerprint to show whether it is valid or invalid. • Upload Hostkey: Click to upload a Hostkey and replace the current one. • Export Hostkey: Click to export a current Hostkey.

Note: To enhance security, users can change port setting to any unused port from 5000 to 32768. Users must then specify the non-default port to obtain access. Telnet clients require users to append either a space and the port number or a colon and the port number to the command line to access the control console.

[System->Network Service->FTP Service] Allow users to Enable/Disable the FTP server service and configure the TCP/IP port of the FTP server (21 by default).

Item	Definition
Allow Access	Enable the access to FTP server.
Service Port	The TCP/IP port of the FTP server (21 by default). Users can change port setting to any unused port from 5000 to 32768 to enhance security.

Note: The FTP server is used for upgrading Firmware. For more details about the upgrade process, please refer to "Firmware Upgrade" section.

[System->Notifications->Event Action] Configure notification settings for every Device Event. Events are categorized for ease of management.

• Log: Record the event in the "Event Logs".
• E-mail: Send an email to a specific user (An available SMTP server is necessary).
• Trap: A SNMP trap sent to a specific IP address.
• Syslog: Sent syslog message to specific syslog server. (An available Syslog server is necessary).
• SMS: Send a short message to a specific mobile phone number (An available SMS service provider is needed).
• Delay: The event will be sent if the condition persists for at least x seconds.
  Note: Delay configuration currently for UPS utility power event only.

[System->Notifications->SMTP Server] After setting the proper SMTP server, event notification email can be sent to recipients when specific events occur.

Item	Definition
SMTP server address	The IP address or Host Name of the SMTP server used to send email notifications.
Sender's E-mail Address	Email address used to send the email notification.
Authentication	Select this option if the SMTP server requires to authenticate the user.
User Name	Account used for Authentication with a maximum length of 63 characters.
Password	Password used for Authentication with a maximum length of 63 characters. For public SMTP Servers like Gmail and Office 365, please type the App Password provided by the SMTP Server for Authentication.
Secure connection	Enable TLS or SSL security.

Item	Definition
Service port	The port number used to communicate with the SMTP server.

[System->Notifications->E-mail Recipients] Set up to five email recipients to receive notifications when configured Events occur.
To add a new recipient, click "New Recipient". To modify or delete an existing Recipient, click the e-mail address of that recipient. To check if SMTP setting and the email recipients are set correctly, click "TEST" button to send a test message.

[System->Notifications->Trap Receivers] Setup up to 10 SNMP TRAP receivers by IP address (IPv6 supported). SNMPv1 and v3 is supported. The listed TRAP receivers will be notified when device Events occur.
To add a new receiver, click "New Receiver". To modify or delete an existing receiver, click the IP address or name of that receiver. To check if the traps can be received correctly, click "TEST" button.

[System->Notifications->SMS Service] Short Message Service (SMS) is a communication service used by mobile communication systems. Using standardized communication protocols will allow the interchange of short text messages between mobile devices. The system provides 4 methods for users to choose how they want to send the messages.

Item	Definition
Service provider is Clickatell	Select the Clickatell option in the SMS Method field. Complete all the account details including Username, Password and HTTP API ID fields. For example: Clickatell (accout before 2016/11) User Name Name Password Passwd HTTP API ID 3234599 Clickatell (account after 2016/11) HTTP API ID 3234599
Service provider accepts HTTP GET	This specification from the SMS provider is required before using the HTTP GET method. Select the Using HTTP GET option in the SMS Method field. Insert the E_PHONE_ NUMBER as recipient's mobile phone number and the E_ PHONE_MESSAGE as event message, described by the SMS provider specification, and fill in the URL field. The expressions will be replaced by relevant content before the message is sent by the SMS provider. For example: URL http://ServiceProviderURL?user=Name&password=Passwd&api_id=3234599&to=E_PHONE_NUMBER&text=E_ MESSAGE

Item	Definition
Service provider accepts HTTP POST	This specification from the SMS provider is required before using the HTTP POST method to deliver messages via SMS providers. Select the Using HTTP POST option in the SMS Method field. Insert E_PHONE_NUMBER as recipient's mobile phone number and E_PHONE_MESSAGE as the event message, described by the SMS provider specification, and fill in the POST URL and POST BODY fields. The expressions will be replaced by the relevant content before the message is sent by the SMS provider. For example: URL http://ServiceProviderURL Content user=Name&password=Passwd&api_id=3234599&to=E_PHONE_NUMBER&text=E_MESSAGE
Service provider accepts E-mail (SMTP)	This specification from a SMS provider is required before using the E-mail to deliver the messages via SMS providers. Select the Using E-mail option in the Service Provider field. Insert E_PHONE_NUMBER as recipient's mobile phone number and the E_PHONE_MESSAGE as event message, described by the SMS provider specification. Fill in the Recipient's Address, Subject and Content. The expressions will be replaced by the relevant content before the message is sent by the SMS provider. For example: Address sample@cyberpower.com Subject TestSubject Content E_PHONE_NUMBER&text=E_MESSAGE

[System->Notifications->SMS Recipients] Users can set up to 10 mobile phone numbers as SMS recipients. The Recipients will receive a short message notification when configured events occur.

To add a new recipient, click "New Recipient". To modify or delete an existing Recipient, click the mobile number or Name of that recipient. To test SMS settings, click "TEST" button and see if the test message is correctly received.

[System->Reset/Reboot] Reset or reboot the RMCARD system.

Item	Definition
Reboot System	Restart the system without turning off and restarting the UPS.
Reset System	Reset the system to factory default setting. The system will restart. This action will not turn off or restart the UPS.
Reset System (TCP/IP Settings Reserved)	Reset the system to factory default setting but reserving TCP/IP. The system will restart This action will not turn off or restart the UPS.

[System->About] Display system information for the Remote Management Card.

Item	Definition
Model Name	Model name of the Remote Management Card.
Hardware Version	The hardware version of the Remote Management Card.
Kernel Version	The current kernel version installed on the Remote Management Card.
Firmware Version	The current firmware version installed on the Remote Management Card.
Firmware Updated Date	The last date the firmware was updated.
Serial Number	Serial number of the Remote Management Card.
MAC Address	MAC address of the Remote Management Card. NOTE: MAC address is also listed on the top of Product.
System Software Update	Use this function to upload the software. Click Browse to go to the location of the file and click Submit.
Save Configuration	Click "Save" to save the RMCARD configuration file. The text file name will have a default format of CONFIG_YYYY_MM_DD_XXXXXX.tar.gz
Restore Configuration	Use this function to restore a configuration that had been previously saved. Click "Choose File" to select the location of the saved configuration file and click "Submit". Note: The saved Configuration file includes security information such as user name and password. After you complete the Restore Configuration, its suggested that you delete the file to keep sensitive information safe and secure.
Diagnostic Information	Click the "Save" button to save all diagnostic information to a file. The saved information includes Event Logs, Status Records and other RMCARD/UPS/ information. It's suggested to have this information saved when contacting CyberPower Technical Support for assistance.

Command Line Interface

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

   How to use telnet access command line interface

   Step 1: Need to make sure the computer has access to the RMCARD installed network.
   Open a command prompt, type telnet and the IP address for the RMCARD (for example, telnet 192.168.20.177, when the RMCARD uses the default Telnet port of 23), and press Enter.

   Step 2: Enter the user's 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 4.
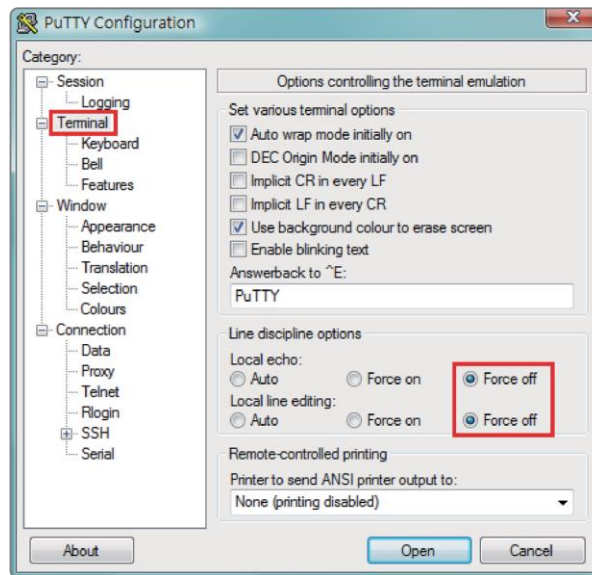

Figure 4. The PuTTY Configuration window.

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 RMCARD 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's name and password of the RMCARD at the Authentication menu.

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 view a list of available commands or arguments → Type "help" and press Enter.

3. 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.)

Command Response Codes

When the command or arguments is not recognized or is incorrect, the following error message will be displayed:

Command not found	RMCARD 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 Descriptions

ups
Description: Show the information about UPS, input, output. And use master switch to control UPS.

Option	Argument	Description
info	show	Display UPS information
input	show	Display UPS input information
output	show	Display UPS output information

Example 1:

```
To view UPS information
CyberPower > ups info show
UPS information
      Model: OL1000XL
      Voltage Rating: 100V
      Working Frequency: 40~70 Hz
      Power Rating: 1000 VA
      Current Rating: 10 Amp
      Load Power: 900 Watts
      Battery Voltage Rating: 36 V
      USB Version: 0.1B
      Next Battery Replacement Date: 10/08/2018
      NCL Bank: 1
      Extended Battery Pack: 4
```

upsctrl
Description: Enable to use UPS Master Switch.

Option	Argument	Description
reboot	off delay / reboot duration (eg. 10/10) off delay: 0 | 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600 reboot duration: 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600	Turns the UPS off and back on. There is one string include off delay (in seconds) and reboot duration (in seconds) , ex: 10/10 means off delay in 10 seconds and reboot duration in 10 seconds.
on		Turns the UPS on.
off	0 | 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600	Turns the UPS off. Argument means Turn Off Delay in seconds.
sleep	0 | 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600	This command is available in Utility Power Failure Mode. It can make UPS in sleep mode until power restore. The argument means Sleep Delay in seconds.

Example 1:

To reboot UPS turn off delay 10sec and reboot duration 20sec.
```
CyberPower > upsctrl reboot 10/20
```

upscfg

Description: Show and configure UPS supply power, UPS sensitivity, UPS high voltage threshold, UPS low voltage threshold, UPS bypass condition, UPS bypass high threshold, UPS bypass low threshold, UPS recharge delay, UPS recharge capacity, UPS working mode, and UPS return delay.

Option	Argument	Description
show		
outpwr	<output power in VAC>	Sets the output voltage which is supplied to the connected equipment.
sen	high | medium | low	Low sensitivity has a looser voltage range and the supplied power may vary more widely. The power from fuel generator may cause the UPS to switch to battery mode more frequently, and the low sensitivity is recommended. The UPS switches to battery mode rarely and also saves more battery power. High sensitivity allows the UPS to supply the more stable power to equipment and switches to battery mode frequently.
hvlimit	<high threshold in VAC>	When the utility voltage (or output voltage) exceeds the threshold, the UPS will supply battery power to the connected equipment.
lvlimit	<low threshold in VAC>	When the utility voltage (or output voltage) exceeds the threshold, the UPS will supply battery power to the connected equipment.
bypasscond	nobypass | freqvolt | voltonly	No Bypass-If this option is selected, the UPS will not enter Bypass mode and will stop supplying output power. Check Volt/Freq-If the utility voltage is in the range of the High/Low Bypass Voltage and the utility frequency is in the range of the Frequency Tolerance, the UPS will enter Bypass mode. Otherwise, the UPS will stop supplying output power. Check Volt Only-Only if the utility voltage is in the range of the High/Low Bypass Voltage, the UPS will enter Bypass mode. Otherwise, the UPS will stop supplying output power.
bypasshvlimit	10 | 15	Set high bypass voltage in percentage. If the utility voltage exceeds thresholds, the UPS will be forbidden to enter Bypass mode.
bypasslvlimit	10 | 15 | 20	Set low bypass voltage in percentage. If the utility voltage exceeds thresholds, the UPS will be forbidden to enter Bypass mode.

Option	Argument	Description
rechargedelay	0 | 60 | 120 | 180 | 300 | 600 | 1200 | 1800 | 3600	Set the recharge delay in seconds. When the utility power restores, the UPS will start to recharge until the specified delay is expired before restoring output power.
rechargecap	0 | 15 | 30 | 45 | 60 | 75 | 90	Set the recharge capacity in percentage. When the utility power restores, the UPS will start to recharge until the specified battery capacity is met before restoring output power.
workmode	normal | eco10% | eco15% | generator | bypass	normal-Normal working mode of the UPS. eco10%-On-line UPS enters Economy 10% mode. eco15%-On-line UPS enters Economy 15% mode. generator-If the UPS uses generator as its input power, this option should enable the UPS to function normally. If this option is selected, the UPS will be forbidden to enter Bypass mode to protect the powered equipment. bypass-Determines whether to allow the UPS to enter Manual Bypass mode. If this option is enabled, the UPS will be forced to enter Bypass mode.
returndelay	0 ~ 600	When the utility power restores, the UPS will start to recharge until the specified delay is expired before restoring output power. The numbers in the range 1 to 600 seconds are numbers divisible by 5.

Example 1:

To view the available value voltage this UPS output power can be set. CyberPower >

```
upscfg supply?
100
110
115
```

Example 2:

To define bypass condition as check utility voltage only
CyberPower > **upscfg bypasscond voltonly**

Example 3:

To define UPS recharge delay as 2 minutes CyberPower >
upscfg rechargedelay 120

Example 4:

To set On-line UPS mode to generator mode
CyberPower > **upscfg mode generator**

upsbatt
Description: Show information of battery, and execute the battery test and battery runtime calibration.

Option	Argument	Description
show		Display all battery information for this UPS
test		Execute the battery test immediately.
cal	start | stop	Start or stop Runtime calibration.
rdyyyy	<number of year>	Set year of battery replacement date by AD.
rdmm	<number of month>	Set month of battery replacement date.
rddd	<number of date>	Set day of month.

Example 1:

  To execute battery selftest.
  CyberPower > **upsbatt test**

Example 2:

  To start battery runtime calibration
  CyberPower > **upsbatt cal start**

Example 3:

  To set the battery replacement date as May 29, 2018.
  CyberPower > **upsbatt rdyyyy 2018 rdmm 5 rddd 29**

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

Option	Argument	Description
show		Display system date information for RMCARD
timezone	<city>	Choose the RMCARD 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	<00:00:00>	Set system time.

Example 1:

  To define timezone offset as Central Standard Time
  CyberPower > `datectl timezone Central`

Example 2:

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

Example 3:

  To define the time as 13:45:12
  CyberPower > `datectl time 13:45:12`

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

Option	Argument	Description
show		Display all NTP information for RMCARD
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	**now**-Choose Update right now to update immediately. **1-8760**-Set the frequency to update the date and time from NTP server.

Example 1:

  To enable NTP server define date and time of RMCARD
  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 RMCARD, reset RMCARD.

Option	Argument	Description
show		Display all system information for RMCARD
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.

Example 1:

To view all information of system

```
CyberPower > sys show
Name: RMCARD400
Location: Server Room
Contact: Admainistrator
Model: RMCARD400
Hardware Version: 1.1
Firmware Version: 1.0.3
Firmware Update Date: 03/08/2020
Serial Number: TALGY2001975
MAC Address: 00-0C-15-00-B9-42
```

auth

Description: Show and configure authentication for login.

Option	Argument	Description
show		Display all login information for RMCARD
type	local | radiuslocal | radiusonly | ldaplocal | ldaponly	local-User to login Remote Management Card with user name and password that configured in Local Account. radiuslocal-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. radiusonly-User to login Remote Management Card with user name and password for authenticate with RADIUS server only. ldaplocal-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. ldaponly-User to login Remote Management Card with user name and password for authenticate with LDAP server only.
secretphrase	<Authentication Phrase>	The Authentication Phrase used to communicate with PowerPanel® Business Remote.
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 > **auth type radiuslocal**

mgrip
Description: Show and configure the primary/secondary manager IP, username, password of admin/device user.

Option	Argument	Description
show		Display all admin or device information for this RMCARD
pri	<primary manager IP>	Set primary manager IP of admin/device
sec	<secondary manager IP>	Set secondary manager IP
secacc	enable | disable	Enable or disable secondary manager IP of admin/device

Example 1:

To define primary admin manager IP as 192.168.26.0/24

```
CyberPower > mgrip pri 192.168.26.0/24
Input admin password: cyber
Pass
```

radius
Description: Show and configure information of radius server.

Option	Argument	Description
show		Display all Radius server information for RMCARD
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.
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>
```

For example:
```
CyberPower > radius add 192.168.203.55 testsecret 150
```

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 for RMCARD
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.
pridn 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 for RMCARD
dhcp	enable | disable	Enable or disable DHCP
dns	manual | auto	Auto-Obtain DNS Address from DHCP when DHCP enable Manual-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 for RMCARD
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**
  manual enable 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 for RMCARD
index	<1 | 2 | 3 | 4>	Select SNMPv1 community index.
set	<1 | 2 | 3 | 4>	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 for RMCARD
index	<1 | 2 | 3 | 4>	Select SNMPv3 user index.
set	<1 | 2 | 3 | 4>	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 for RMCARD.
add		Add trap receiver for RMCARD.
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.
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 for RMCARD
http	<enable | disable>	Enable or disable HTTP Server
https	<enable | disable>	Enable or disable HTTPS Server
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 for RMCARD
telnet	<enable | disable>	enable-Enable Telnet. disable-Disable Telnet.
ssh	<enable | disable | reset_hostkey>	enable-Enable SSH. disable-Disable SSH. reset_hostkey-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: Telnet is disabled by default, and SSH is enabled by default.

Example 3:
    To reset SSH Hostkey to default
```
CyberPower > console ssh reset_hostkey
```

Note: The system will reboot after the SSH Hostkey of RMCARD 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 for RMCARD
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 RMCARD and UPS.

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 inter-face.

Example 2:
To clear all event logs.
```
CyberPower > eventlog clear
```

syslog

Description: Show and configure information of SYSLOG server.

Option	Argument	Description
show		Display all syslog information for RMCARD
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
ip1 ip2 ip3 ip4	<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.

user
Description: Show and configure the username, password of admin/device user.

Option	Argument	Description
Show		Show information of User Account
Add		Add User Account
Delete	<user name to modify>	Delete User Account
Passwd	< user password>	Modify User Account Password
Access	<enable | disable>	Modify User Account Access
type	<admin | device>	Modify User Account Type

Example 1:
  To delete user name
  `CyberPower > `**`user name XXX delete`**

accy
Description: Show accessory information.

Option	Argument	Description
show		Show information of accessory.

Example 1:
  To display general information of accessory
  `CyberPower > `**`accy show`**

```
      Model          Serial number      HW version   FW version
  ------------------------------------------------------------------
  1  SENV001         TBLMV2000001       1.0          1.0.4
  2  SENV001         TBLMV2000002       1.0          1.0.4
```

envsta
Description: Show environmental sensor status.

Option	Argument	Description
show		Show information of environmental sensor.
index	1 | 2 | 3|…| 8	Select environmental sensor index.

Example 1:
    To display general status of environment sensor
        CyberPower > **envsta show**
```
          Name                 Location                    Temp        Humid
        ----------------------------------------------------------------------
        1  Name1                Location1                   77.21 F     54.00 %RH
        2  Name2                Location2                   76.33 F     53.00 %RH
```

envcfg

Description: Show and set environment sensor configuration.

Option	Argument	Description
show		Show configuration of environmental sensor.
index	1 | 2 | 3|...| 8	Select environmental sensor index.
name	< environment sensor name>	Modify environmental sensor name.
location	< environment sensor location>	Set environmental sensor location.
temphthres	<high threshold value>	Set high temperature threshold.
templthres	<low threshold value>	Set low temperature threshold.
temphyster	<hysteresis value>	Set temperature hysteresis.
tempchange	<rate of change value>	Set temperature rate of change.
humhthres	<high threshold value>	Set high humidity threshold.
humlthres	<low threshold value>	Set low humidity threshold.
humhyster	<hysteresis value>	Set humidity hysteresis.
humchange	<rate of change value>	Set humidity rate of change.
maxminreset	<temp | humid>	Reset maximum and minimum record of temperature or humidity.
unit	<celcius | fahrenheit>	Set temperature unit

Example 1:
    To display general configuration of environment sensor
        CyberPower > **envcfg show**
```
                                        Temperature(F)      Humidity(%RH)
          Name              Location    [HTH|LTH|HYS|CAG] [HTH|LTH|HYS|CAG]
        ----------------------------------------------------------------------
        1  Name1             Location1   [158|33 |3  |18 ] [80 |50 |5   |20 ]
        2  Name2             Location2   [158|33 |3  |18 ] [80 |50 |5   |20 ]

        *HTH = High Threshold *LTH = Low Threshold
        *HYS = Hysteresis     *CAG = Change Rate(per 5min)
```

Example 2:
    To set accessory#1's name as envirname1
        CyberPower > **envcfg index 1 name envirname1**

Example 3:
    To set high temperature threshold of the accessory#1 at 70
        CyberPower > **envcfg index 1 temphthres 70**

Example 4:
    To reset maximum and minimum record of accessory#1 temperature
        CyberPower > **envcfg index 1 maxminreset temp**

Example 5
    To set temperature unit as celcius
    CyberPower > **envcfg unit celcius**

contactsta
Description: Show contact status.

Option	Argument	Description
show		Show status of contact.
index	1 | 2 | 3|...| 8	Select contact index.

Example 1:
    To display general status of contact
    CyberPower > **contactsta show**
```
      name            |name          |name          |name          |status
      contact1        |contact2      |contact3      |contact4      |[#1|#2|#3|#4]
    ----------------|-------------|-------------|-------------|-------------
  1   contact1-1      | contact1-2  | contact1-3  | contact1-4  |[ X| X| X| X]
  2   contact2-1      | contact2-2  | contact2-3  | contact2-4  |[ X| X| X| X]

    *O = Normal *X = Abnormal
```

contactcfg
Description: Show and set contact configuration.

Option	Argument	Description
show		Show configuration of contact.
index	1 | 2 | 3|...| 8	Select contact index.
contact1name	<contact name>	Modify contact 1 name.
contact1state	<open | closed>	Set contact 1 state
contact2name	<contact name>	Modify contact 2 name.
contact2 state	<open | closed>	Set contact 2 state
contact3name	<contact name>	Modify contact 3 name.
contact3 state	<open | closed>	Set contact 3 state
contact4name	<contact name>	Modify contact 4 name.
contact4 state	<open | closed>	Set contact 4 state

Example 1:
    To display general configuration of contact
    CyberPower > **contactcfg show**

Example 2:
    To set envirsensor#1's contact 2 name as contact1-2
   CyberPower > **contactcfg index 1 contact2name contact1-2**

clear
Description: Clear the console screen.

exit
Description: Close the connection to the command line interface.

Reset to Factory Default Setting / Recover from a Lost Password

To reset the CyberPower Remote Management Card to its factory default setting (including web log-in user name and password), please following these steps:

RESET JUMPER

RMCARD400/401
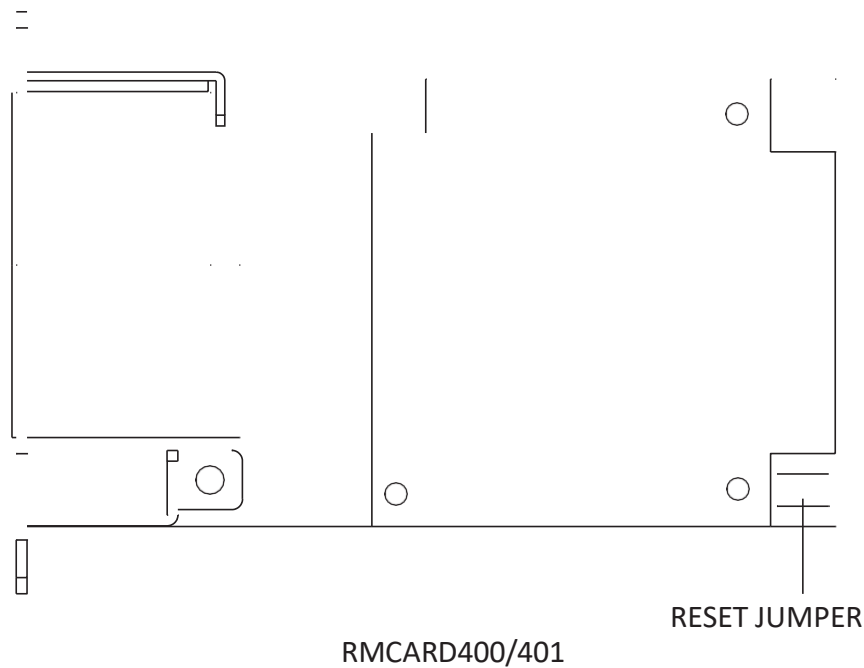
1. Remove the card from the UPS without turning the UPS off.

2. Remove the jumper from the reset pins as illustrated. Do not dispose of the jumper.

3. Insert the card into the expansion port on the UPS.

4. Wait until the green Tx/Rx LED is flashing (the frequency of the ON/OFF flashing is once per second).

5. Remove the card again.

6. Place the jumper back onto the Reset pins.

7. Install card into the expansion port again and tighten the retaining screws.

RMCARD Firmware Upgrade

By upgrading the firmware, you can obtain both the new features and updates/ improvements to existing functionality. FTP service needs to be Enabled before attempting to execute a Firmware Upgrade. You can check the "Firmware version" on the
[System->About] page on the web user interface of the RMCARD. There is one file to update in order to upgrade the firmware version.

- cpsrm4safw_XXX

Note: To ensure keeping RMCARD firmware up to date, please visit CyberPower website every 3 months to see if there is any updated firmware version available.

Note: Please do not turn the UPS off when processing the Firmware upgrade.

Note: To update the RMCARD firmware successfully, please check whether the connections to Port 20 and 21 in firewall are not blocked.

Method 1: Using FTP command

Use the following steps to upgrade the firmware:

1. Download the latest firmware

2. Extract the downloaded files to "C:\"

3. Open a command prompt window

4. Login to the CyberPower Remote Management Card with FTP command, in the command prompt type:

    (1) `ftp`

    (2) `ftp> open`

    (3) `To [current IP address of RMCARD] [port]; EX: To 192.168.22.126 21`

    (4) `Input USER NAME and PASSWORD (same as the administrator account in web user interface, see page 6 for default factory settings)`

5. Upload file :
   `ftp > put cpsrm4safw_XXX`

6. Upload is now complete, type:
   `ftp > quit`

7. The system will reboot after you type "quit"

Method 2: Using Power Device Network Utility 2

Install the CyberPower Power Device Network Utility 2 available for download at www. CyberPower.com.

1. After installation completes, run the "Power Device Network Utility 2".

2. The main window of the Power Device Network Utility 2 program is shown in Figure 5. The configuration tool will display all CyberPower Remote Management devices present on the local network subnet. The "Scan" button is used to search the local network subnet again.
Note: You can click "Scan" and select the items you want to view.

	Type	MAC Address	Version	Account	IP Address	DHCP	Time	I Up Time
	All					All		All
PDU	00:0C:15:11:11:13	0.1.1.0		192.168.202.31	true	2022-07-12 11:59:36	240H:37M:35S
UPS	00:0C:15:01:3E:17	0.1.3.0		192.168.202.41	true	2022-07-12 11:59:36	2H:44M:11S
PDU	00:0C:15:40:76:59	1.1.2.0		192.168.202.70	true	2022-07-12 11:59:36	240H:36M:54S
BM	00:0C:15:03:B0:5E	1.0.0.0		192.168.202.80	true	2022-07-12 11:59:36	1H:13M:39S
ATS	00:0C:15:40:E2:D4	1.2.4.0		192.168.202.39	true	2022-07-12 11:59:36	3H:38M:52S
UPS	00:0C:15:05:43:51	1.0.0.0		192.168.202.38	true	2022-07-12 11:59:36	64H:35M:23.20...

Figure 5. The main window of the "Power Device Network Utility 2" program.

3. Check the boxes to select the devices you wish to upgrade, and select "Connection" on to connect the device user account and password. Once the connection is confirmed the status icon next to the IP Address will change from grey to green.
Note: You must connect to the device by entering user account and password credentials before firmware upgrade.

4. Select the devices you wish to upgrade by checking their respective checkbox and select "Upload Firmware".
Note: You can upload the firmware of multiple devices that use the same firmware files

5. Select the Firmware and click "OK" to implement firmware upgrade, as shown in Figure 6.
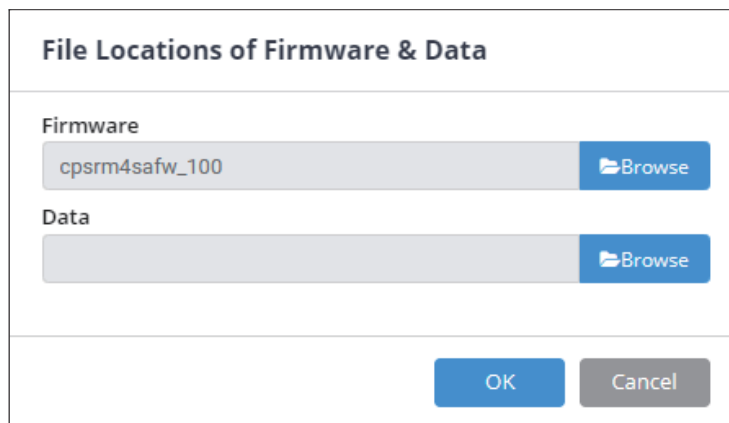

Figure 6. The File Locations of Firmware & Data window.

6. If the firmware upgrade is implemented, you will see the Result in the main window, as shown in Figure 7.

Figure 7. Firmware upgrade success in the main window.

Method 3: Using Secure Copy (SCP) command Use the

following steps 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 file and the PSCP Utility are saved.

4. Enter the following command to perform the firmware update: pscp –scp <filename> <user>@<IP address of RMCARD>:

Note:

   (1) The SSH setting on the RMCARD must be Enabled.

   (2) `<filename>` is the filename of the firmware file. There is one firmware file to upload:
        `cpsrm4safw_XXX`

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

   (4) Ensure to add "`:`" after the IP address. For
        example:
        `pscp  –scp cpsrm4safw_XXX cyber@192.168.1.100:`

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 RMCARD password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

7. 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 file is saved.

3. Enter the following Command to perform firmware update:
   `scp <filename> <user>@< IP address of RMCARD>:`

Note:

   (1) The SSH setting on the RMCARD must be Enabled.

   (2) `<filename>` is the filename of the firmware file. There is one firmware file to upload: `cpsrm4safw_XXX`

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

   (4) Ensure to add ":" after the IP address. For example:
   `scp  cpsrm4safw_XXX cyber@192.168.1.100:`
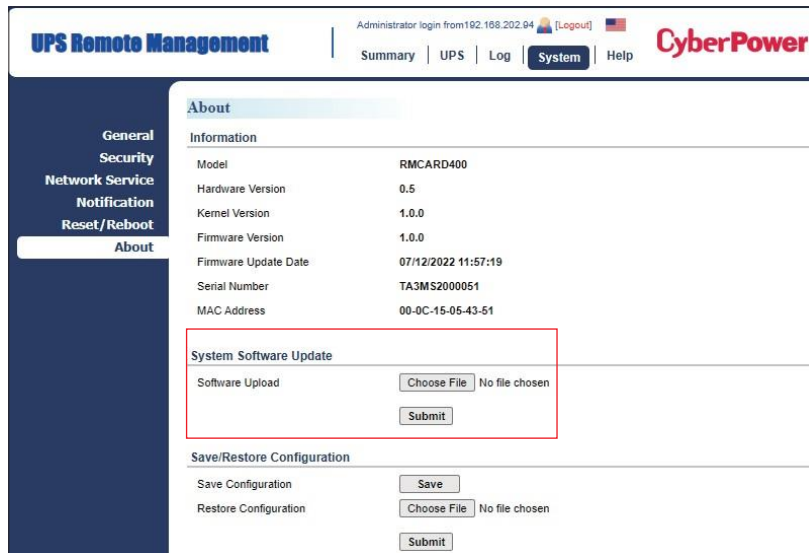
4. After executing the command, a message may appear asking if you trust the host. To continue type "y" for yes within 10 seconds.

5. On the next screen enter the RMCARD password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

6. If the firmware file transfer is unsuccessful you will see an error message. Attempt to retype the command and execute it again.

Method 4: Using Web Interface

Use the following steps to upgrade the firmware via Web Interface

1. Go to About page via the [System->About].

2. Select the Firmware and click "Submit" to implement firmware upgrade, as shown in Figure 8.

Figure 8. Firmware Update in the main window.

3. If the firmware upgrade is implemented, you will see the Result in the main window, as shown in Figure 9.
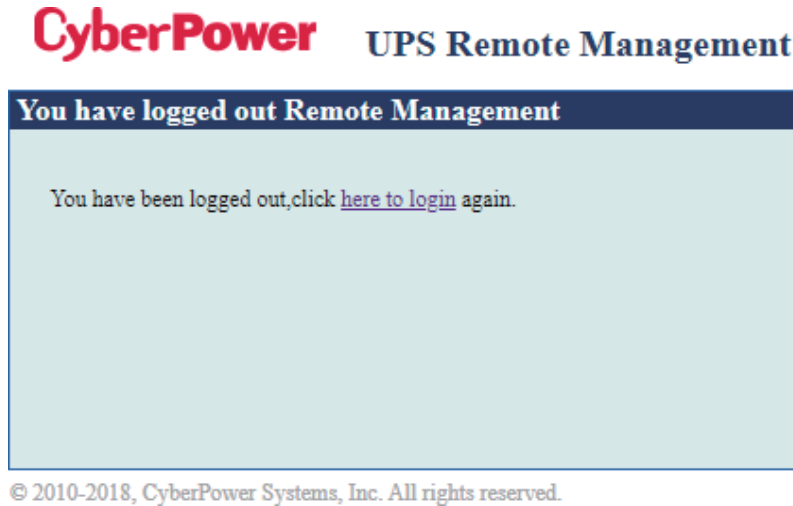

Figure 9. Firmware upgrade success in the main window.

Save and Restore Configuration Settings

Method 1: Using Web Interface
You can easily save and restore the device configuration to your local PC on [System->About]
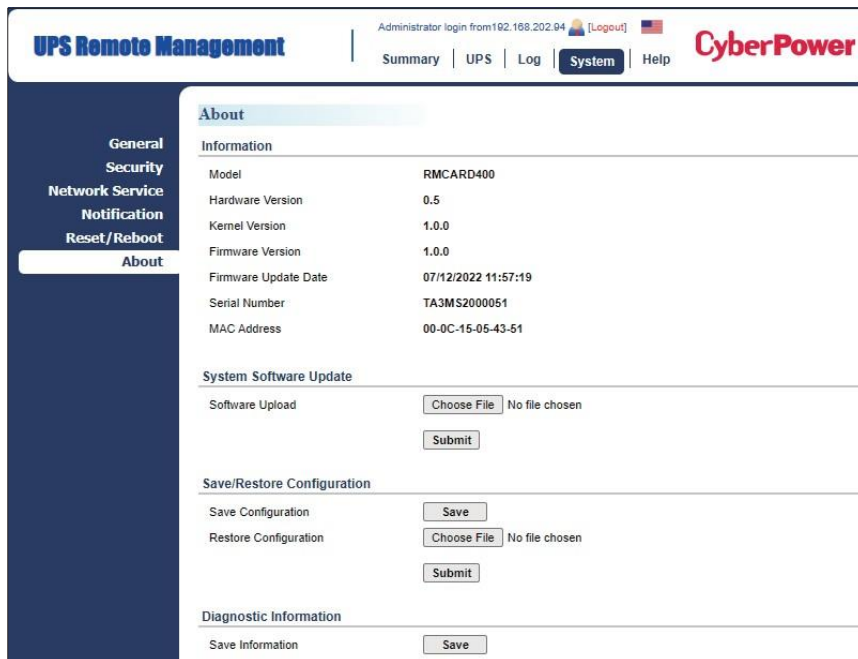

Figure 10. Save/Restore Configuration in the main window.

You can easily save and restore the device configuration to your local PC on the [System->About], as shown in Figure 10.

To save the configuration file, click "Save" to save the configuration to your local PC. The text file will have a default format of CONFIG_YYYY_MM_DD_XXXXXX.tar.gz

To restore a configuration, click "Browse" to the location of the saved configuration file and click "Submit" to restore a configuration that has been saved earlier.

Method 2: Using File Transfer Protocol (FTP)

Use the following steps to save configuration via FTP.

Note: Only firmware version 1.0.3 and above supports the functionality to download
configuration file via FTP.

1. Open a command prompt window and navigate to "C:\".

2. Login to the RMCARD with FTP command, type

    (1) `C:\>ftp`

    (2) `ftp> open 192.168.22.126`

    (3) `Connected to 192.168.22.126.`

    (4) `220 CyberPower FTP Server Ready.`

    (5) `User (192.168.22.126:(none)): cyber`

    (6) `331 User name okay, need password.`

    (7) `Password:`

    (8) `230 User logged in, proceed.`

    (9) `ftp>`

3. Download the configuration file, type

    `ftp> get download/config.tar.gz`

4. Download is complete, type

    `ftp> quit`

Use the following steps to restore configuration via FTP.

1. Open a command prompt window and navigate to "C:\".

2. Login to the RMCARD with FTP command, type

    (1) `C:\>ftp`

    (2) `ftp> open 192.168.22.126`

    (3) `Connected to 192.168.22.126.`

    (4) `220 CyberPower FTP Server Ready.`

    (5) `User (192.168.22.126:(none)): cyber`

    (6) `331 User name okay, need password.`

    (7) `Password:`

    (8) `230 User logged in, proceed.`

    (9) `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".

   Note: `<filename>` is the filename of the configuration file.

   - `<CONFIG_YYYY_MM_DD_XXXXXX.tar.gz>` is the configuration file to be saved via Web Interface.
   - `<config.tar.gz>` is the configuration file to be saved via File Transfer Protocol (FTP).

Method 3: Using Secure Copy (SCP) command

Use the following steps 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 RMCARD>:`

Note:

   (1) The SSH setting on the RMCARD must be Enabled.

   (2) `<filename>` is the filename of the configuration file with a default format of `CONFIG_YYYY_MM_DD_XXXXXX.tar.gz`

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

   (4) Ensure to add ":" after the IP address. For example:
        `pscp  -scp CONFIG_YYYY_MM_DD_XXXXXX.tar.gz cyber@192.168.1.100:`
        Note: `CONFIG_YYYY_MM_DD_XXXXXX.tar.gz 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 RMCARD 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 RMCARD>:
   ```

Note:

    (1)   The SSH setting on the RMCARD must be Enabled.

    (2)   `<filename>` is the filename of the configuration file with a default format of
         CONFIG_YYYY_MM_DD_XXXXXX.`tar.gz`

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

    (4)   Ensure to add ":" after the IP address. For
         example:
         `scp  CONFIG_YYYY_MM_DD_XXXXXX.tar.gz cyber@192.168.1.100:`
         Note: CONFIG_YYYY_MM_DD_XXXXXX.`tar.gz` 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 RMCARD password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete

Save Event Logs and Status Records via File Transfer Protocol (FTP)

Use the following steps to save event logs file and status records file via FTP.

 Note: Only firmware version 1.0.3 and above supports the functionality to download configuration file via FTP

1. Open a command prompt window and navigate to "C:\".

2. Login to the RMCARD with FTP command, type

    (1) `C:\>ftp`

    (2) `ftp> open 192.168.22.126`

    (3) `Connected to 192.168.22.126.`

    (4) `220 CyberPower FTP Server Ready.`

    (5) `User (192.168.22.126:(none)):cyber`

    (6) `331 User name okay, need password.`

    (7) `Password:`

    (8) `230 User logged in, proceed.`

    (9) `ftp>`

3. Download the event logs file, type

    `ftp> get download/log.txt`

4. Download the status records file, type

    `ftp> get download/status_rec.txt`

5. Download is complete, type

    `ftp> quit`

Upload SSH Host key via Secure Copy (SCP)

A SSH HOST Key can be uploaded to RMCARD with Secure Copy commands.

Please make sure the uploaded filename contains the start string of "ssh_hostkey_" .

Some examples of acceptable file name are as following:

  ssh_hostkey_sample1.pem

  ssh_hostkey_1024.pem

  ssh_hostkey_type100.***

Example of Upload Process

1. Download PuTTY Secure Copy client (PSCP) utility.

2. Have the SSH Host key file and the PSCP Utility in the same folder.

3. Open the Command Prompt and change the path to SSH Host key file and the PSCP Utility are saved.

4. Enter the following command

   `pscp –scp  <filename> <admin_account>@<IP address of RMCARD>:`

   Ex：`pscp -scp ssh_hostkey_xxx.xxx cyber@192.168.203.66:`

5. After executing the command, a message may appear asking if you trust the host. Please type "y" for yes within 10 seconds.

6. On the next screen enter the admin password. The 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.

Host-Key Requirement

SSH that are created with 2048-bit or 4096-bit RSA k

Troubleshooting

Problem	Solution
Unable to configure the Remote Management Card using method 1 or method 2	1. Check the LED status, it is normal when the yellow and green LEDs are both on. If green LED is off : ► Check if the Remote Management Card is properly seated in the device and the device has power. If yellow LED is off : ► Ensure the network connection is good. 2. Ensure the PC being used is on the same local network subnet as the CyberPower device you are trying to communicate with. 3. Ensure the Jumper on the Reset Pin is correctly installed.
Unable to ping the Remote Management Card	1. Use method 1 and/or method 2 to get/set a correct IP address for the Remote Management Card. 2. If the PC being used is on a different network subnet from the Remote Management Card, verify the setting of subnet mask and the IP address of gateway.
Lost the user's name and password	Please refer to the "Reset to Factory Default Set-ting / Recover from a Lost Password" section.
Default Network Setting	IP: 192.168.20.177 Subnet mask: 255.255.255.0 DHCP: On
Unable to access the Web Interface	1. Ensure you can ping the RMCARD. 2. Ensure you are specifying the correct URL. 3. Ensure the HTTP/HTTPS access is enabled by logging in to the card via CLI (Telnet or SSH client).
Unable to operate a SNMP get/set	SNMPv1: Verify the community's name. SNMPv3: Verify the user profile configuration.
Unable to receive traps	1. Ensure the trap types (SNMPv1/SNMPv3) and trap receiver are configured correctly. 2. Ensure the IP address of gateway is configured correctly if the RMCARD and NMS are on a different network.

Conformance Approvals

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Any special accessories needed for compliance must be specified in the instruction.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

> The Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.
>
> Cet appareil numerique de la class A respecte toutes les exigencies du Reglement sur le materiel brouilleur du Canada.

European Union

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

⚠ WARNING: This product can expose you to chemicals including Styrene, which is known to the State of California to cause cancer, and Bisphenol-A, which is known to
the State of California to cause birth defects or other reproductive harm. For more
information go to www.P65Warnings.ca.gov.

Appendix 1: IP Address Identification for CyberPower Remote Management Card

Overview

All devices on a computer network need to have an IP address. Each device's IP address is unique. The same address cannot be used twice. In order to assign an IP address to the CyberPower Remote Management Card, you must determine the range of the available IP addresses, and then choose an unused IP address to assign to the Remote Management Card.

Note: You may need to contact your network administrator to obtain an available IP address.

Procedures to find an IP address:

1. Locate the subnet of the CyberPower Remote Management Card.
   One way to determine the range of possible IP addresses is to view the network configuration on a workstation. Click on [Start] and select [Run]. Type "command" into the open box and click [OK]. At the command prompt type "ipconfig /all" and press [Enter]. The computer will display network information as listed below:

   ```
   Ethernet adapter

   Connection-specific DNS Suffix………: xxxx.com
        Description………………...: D-Link DE220 ISA PnP LAN adapter
        Physical Address………………: 00-80-C8-DA-7A-C0
        DHCP Enabled…………………..…: Yes
        Autoconfiguration Enabled…: Yes
        IP Address…………………..……: 192.168.20.102
        Subnet Mask…………………..…..…: 255.255.255.0
        Default Gateway……………..…: 192.168.20.1
        DHCP Server…………………..…..…: 192.168.20.1
        DNS Servers…………………...…..…: 211.20.71.202
                                 168.95.1.1
   ```

2. Select an IP Address for the CyberPower Remote Management Card
   Verify the IP Addresses for the computer and the Remote Management Card belong to the same subnet. Refer to the above network information, the possible IP Address for the Remote Management Card could be 192.168.20.* (* hereafter represents any number between 1 and 255). Similarly, if the Subnet Mask is 255.255.0.0, the IP Address for Remote Management Card could be set up as 192.168.*.* to reach the same subnet with the computer.

   To verify there is no other equipment connected to the network using the same IP Address, run "Ping 192.168.20.240" at the DOS Mode prompt when the IP Address you would like to set is 192.168.20.240. If the response is presented as below, the IP address is most likely not used and may be available for the CyberPower Remote Management Card.

   ```
   Pinging 192.168.20.240 with 32 bytes of data:
   Request timed out.
   Request timed out.
   Request timed out.
   Request timed out.
   ```

If the response is shown as below, the IP address is in use. Try another IP address until an available address is found.

```
Pinging 192.168.20.240 with 32 bytes of data:
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
```

Appendix 2: How to Configure a RMCARD User Account in Authentication Servers

RADIUS

1. Add a new attribute to RADIUS Dictionary as the Cyber vendor:
    3808 – Vendor

2. Add two new specific attributes to RADIUS server interface under the vendor:

    (1) Cyber-Service-Type (integer variable)

    Cyber-Service-Type can accept three integer parameter values:
    1 – Administrator
    2 – Viewer
    3 – Outlet User

    (2) Cyber-Outlets (string variable)
    Cyber-Outlets can accept a string describing outlet numbers. This attribute will let the outlet user access and control the designated outlets. For example, Cyber- Outlets="1,2,5" allows the user to control outlets 1, 2 and 5.

The example of the Dictionary File:

```
VENDOR        Cyber           3808
BEGIN-VENDOR  Cyber
ATTRIBUTE     Cyber-Service-Type    1      integer
ATTRIBUTE     Cyber-Outlets          2       string
VALUE         Cyber-Service-Type    Admin     1
VALUE         Cyber-Service-Type    Viewer    2
VALUE         Cyber-Service-Type    Outlet    3
END-VENDOR      Cyber
```

LDAP & Windows AD

Add one of the attributes below to description on the OpenLDAP or Windows AD interface for indicating the user account type and authentication:

1. cyber_admin (Administrator)

2. cyber_viewer (Viewer)

3. cyber_outlet="string" (Outlet user)

The string entered in cyber_outlet designates what outlets the Outlet User can access and control. For example, cyber_outlet="1,2,5" allows the user to control outlets 1, 2 and 5.

Appendix 3: UPS Firmware Upgrade

You can check the "Firmware version" on the [UPS->Information] page on the web user interface of the RMCARD.

Method 1: Using Web Interface

1. Turn off the UPS via the [UPS->Master Switch].

2. Go to Firmware Version page via the [UPS->Information->Firmware Version].

3. Upload the UPS firmware by clicking Update then Choose File to select the location of the UPS firmware file.

4. Click Submit to implement the update, and an upgrade success window will show up after upgrade has completed.

5. Turn on the UPS via [UPS->Master Switch].

Method 2: Using FTP Command

FTP service needs to be Enabled before attempting to execute a Firmware Upgrade. Use the following steps to upgrade the firmware via FTP:

1. Turn off the UPS.

2. Extract the update file to "C:\"

3. Open a command prompt window

4. Login to the CyberPower Remote Management Card with FTP command, in the command prompt type:

   (1) `ftp`

   (2) `ftp > open`

   (3) To [current IP address of RMCARD] [port]; EX: To `192.168.22.126 21`

   (4) Input USER NAME and PASSWORD (same as the administrator account in web user interface, see page 6 for default factory settings)

5. Upload the file, type:
   `ftp > bin`
   `ftp > put XXX.bin`

6. Upload is now complete, type:
   `ftp > quit`

7. Turn on the UPS.

Note: 1. It may take about 5 mins to complete the update. Please do not carry out any other actions or pull out the RMCARD during the UPS firmware update process.

Note: 2.The update progress can only display in web interface.

Note: 3. If you see a message "Uploaded an invalid UPS firmware" after uploading the UPS Firmware file via Web interface, please check:

(1) The file is Binary file for UPS firmware.
(2) The UPS firmware file is supporting the UPS Model.

Appendix 4: Software Support

PowerPanel® Business Remote is used to perform a graceful operating system shutdown when protected by a UPS with a remote management card installed. PowerPanel® Business software is available on CyberPower Systems official website. Please visit www. CyberPower.com and go to the software section for free download.

Communicate with PowerPanel® Business Remote

The remote management card requires to authenticate with PowerPanel® Business Remote via a shared secret phrase, as shown in Figure 9.

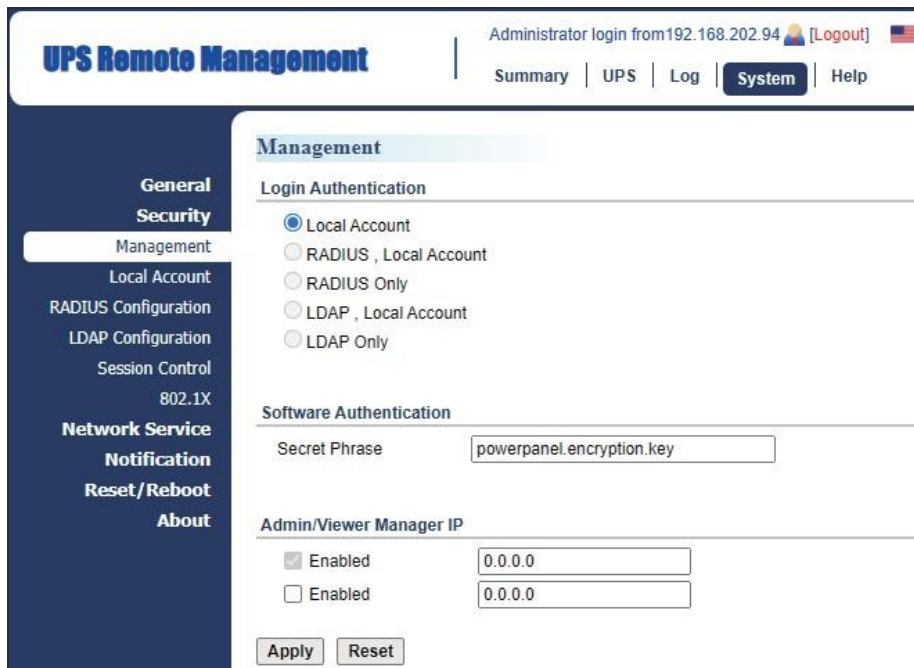Note: The default secret phrase is 'powerpanel.encryption.key'.

Figure 11. RMCARD System>Authentication web UI.

Note: PowerPanel® Business software supports automated graceful shutdown of VMware ESX/ESXi hosts as well as other virtualization platforms such as Microsoft Hyper-V and Citrix.

Obtain IP Address for Linux Operating System

The instructions in 'Configure the IP address for the CyberPower Remote Management Card' section is for Windows OS. For Linux Operating System, please use PowerPanel® Business Remote software to scan and obtain the IP address. To do this, go to
[Power->Configuration] on the PowerPanel® Business Remote web interface, as shown in Figure 10. For more information, please refer to PowerPanel® Business User's Manual.
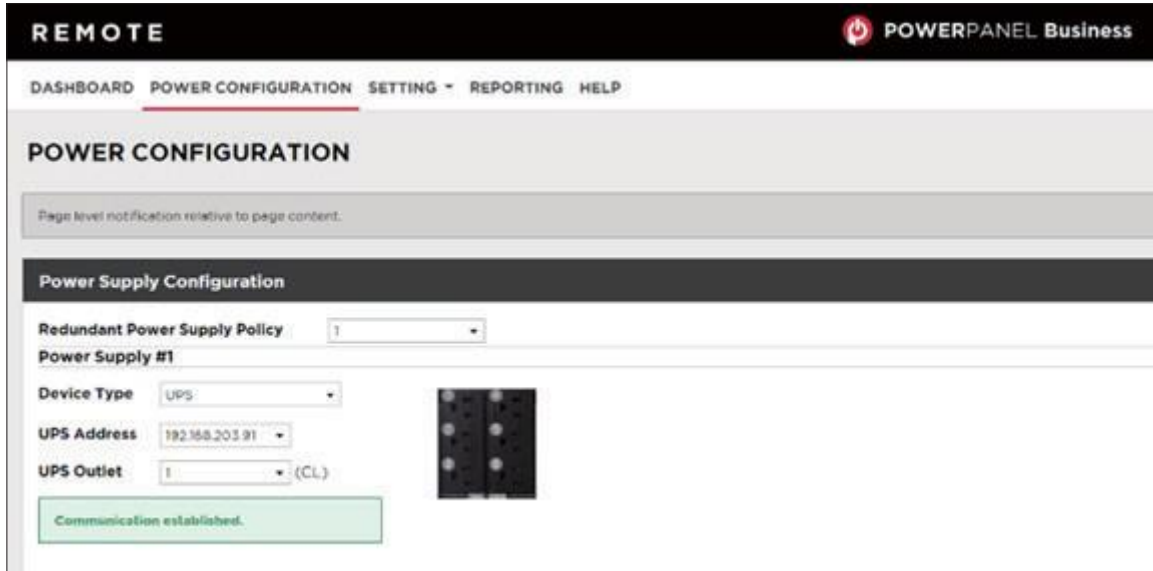

Figure 12. The PowerPanel® Business Remote web interface

Appendix 5: How to Update Kernel version

You can check the "Kernel Version" on the **[System->About]** page on the web user interface of the RMCARD. There is one file to update in order to upgrade the kernel version.

- cpsrkernel_XXX

Note: To ensure keeping RMCARD kernel up to date, please visit CyberPower website every 3 months to see if there is any updated kernelversion available.

1. Change operation mode via serial connection

   Change operation mode via serial connection, the PC/server must be connected directly to the Universal port of the RMCARD 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: 115200
   *Data bits: 8
   *Parity: None
   *Stop bits: 1
   *Flow control: None

2. Change Remote Management Card from Normal Operation to Backup Operation

   After connect to the Terminal, please reboot the RMCARD. Enter "2" on the Terminal to change to Backup Mode operation.

   Note: You need to enter choice within 2 seconds. Otherwise, the Terminal will enter "1" automatically and remain in Normal Operation.

```
1:          Normal Operation
2:          Backup Operation
Enter choice: 2
2:          Backup Operation

Starting kernel ...
```

3. Upload kernel file with FTP command

   Use the following steps to update the kernel:

   1. Download the latest kernel file

   2. Extract the downloaded files to "C:\"

   3. Open a command prompt window

   4. Login to the CyberPower Remote Management Card with FTP command, in the command prompt type:

      - ftp

      - ftp> open

      - To [current IP address of RMCARD] [port]; EX: To 192.168.22.126 21

      - Input USER NAME and PASSWORD (same as the administrator account in web user interface, see page 6 for default factory settings)

   5. Upload file :
      ftp > put cpskernel_XXX

   6. Upload is now complete, type:
      ftp > quit

   7. The system will reboot after you type "quit"

CyberPower

Cyber Power Systems, Inc.
www.cyberpower.com

For USA and Canada:
4241 12th Ave East, Suite 400
Shakopee, MN 55379
Toll-free: (877) 297-6937

For all other regions:
Please visit our website for local contact information.

CE

K01-E0000043-03