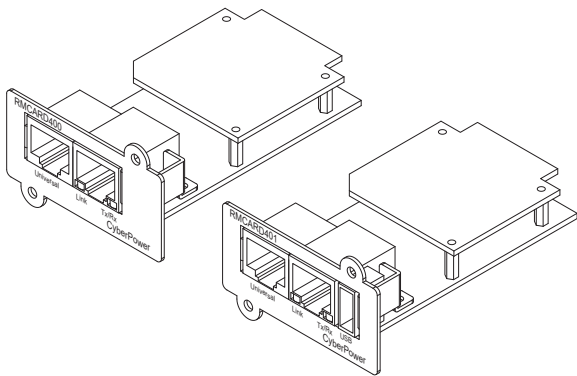# CyberPower

QUICK START GUIDE

Remote Management Card

RMCARD400
RMCARD401

SAVE THESE INSTRUCTIONS
Please read this guide and follow the instructions for installation and use.

Table of Contents

INTRODUCTION

Overview

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

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
- RMCARD400 supports the CyberPower's UPS models which have smart slot.
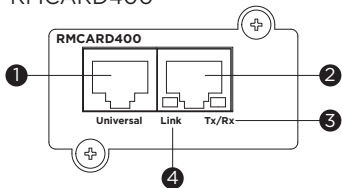 (RMCARD401 supports the new specific UPS models)

Unpacking

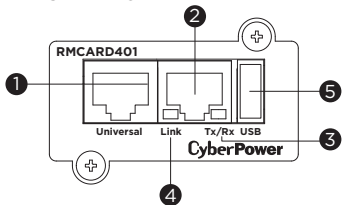Inspect the Remote Management Card upon receipt. The package should contain the following:

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

Front Panel

RMCARD400

RMCARD401

1. Universal Port
2. Ethernet Port
3. Tx/Rx Indicator
4. Link Indicator
5. USB Port

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 (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

Step 1. Hardware Installation

NOTE: The CyberPower Remote Management Card is hot-swappable, so you do not need to turn off the device 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 of the expansion slot, and then 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 user's manual.
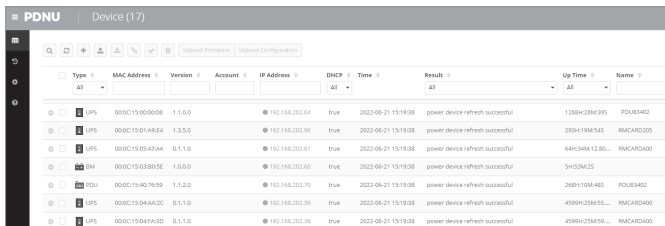
RMCARD400/401
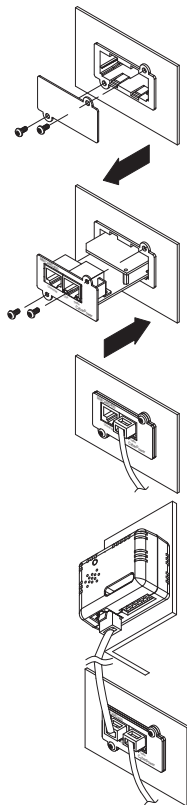
Step 2. Configure the IP Address for the CyberPower Remote Management Card

Method 1: Using the Power Device Network Utility 2

1. Install the Power Device Network Utility 2 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 2 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.
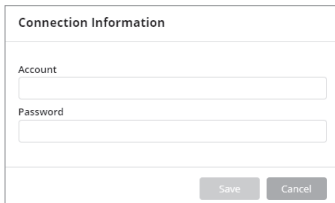

Figure 1. The main window of the "Power Device Network Utility 2" program

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. Authentication 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. The Device Network setting window

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

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 username: **cyber**
   - Default password: **cyber**

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

You will be asked to reset a username and 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. For detailed descriptions and explanations of the Web UI, please refer to RMCARD User's Manual.

FIRMWARE UPGRADE

By upgrading the firmware, you can obtain both the new features and updates/improvements to existing functionality. To ensure the RMCARD firmware is kept up to date, please visit our website every 3 months to see if there is any updated firmware version available. 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.
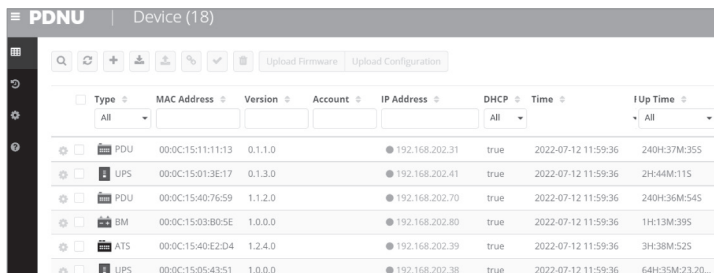
- cpsrm4safw_XXX

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

Using Power Device Network Utility

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 4. 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 4. 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

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

File Locations of Firmware & Data

Firmware

| cpsrm4safw_100 | 📂Browse |

Data

| | 📂Browse |

OK   Cancel

Figure 5. The File Locations of Firmware & Data window.

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

	Type	MAC Address	Version	Account	IP Address	DHCP	Time	I Up Time	Name	Location	Sub
	All ▾					All ▾	▾ All ▾				
⚙ ☐	PDU	00:0C:15:11:11:13	0.1.1.0		● 192.168.202.31	true	2022-07-12 09:17:15	237H:55M:14S	PDU83105	Server Room	
⚙ ☐	UPS	00:0C:15:01:3E:17	0.1.3.0		● 192.168.202.41	true	2022-07-12 09:17:15	0H:1M:51S	RMCARD205	Server Room	
⚙ ☐	BM	00:0C:15:03:80:5E	1.0.0.0		● 192.168.202.60	true	2022-07-12 09:17:15	237H:54M:52S	BM100	Server Room	
⚙ ☐	PDU	00:0C:15:40:76:59	1.1.2.0		● 192.168.202.70	true	2022-07-12 09:17:15	237H:54M:33S	PDU83402	Server Room	
⚙ ☐	ATS	00:0C:15:40:E2:D4	1.2.4.0		● 192.168.202.39	true	2022-07-12 09:17:15	0H:56M:31S	PDU84002	Server Room	
⚙ ☑	UPS	00:0C:15:05:43:51	1.0.0.0	admin	● 192.168.203.38	true	2022-07-12 09:17:15	64H:35M:22.82...	RMCARD400	Server Room	

Figure 6. Firmware upgrade success in the main window.

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 follow these steps:
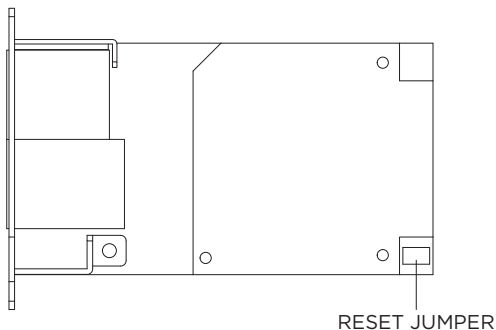
RESET JUMPER

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.

NOTE: RMCARD400/401 is designed for the 43x18mm (1.69x0.71 inch) SNMP card expansion port of CyberPower PR, OR, and 1-3kVA OL series UPS.

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 7.

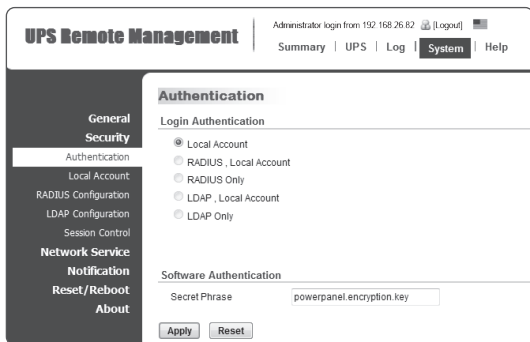**NOTE:** The default secret phrase is 'powerpanel.encryption.key'.

Figure 7. 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.

TROUBLESHOOTING

Problem	Solution
Unable to configure the Remote Management Card IP Address 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 name and password	Please refer to the "Reset to Factory Default Setting / 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 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.

For warranty and additional information, please visit:
www.cyberpower.com.

Disposal

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to contribute to sustainable production and consumption by contributing to the efficient use of resources and the retrieval of secondary raw materials through re-use, recycling and other forms of recovery. The symbol on this product and/or its packaging indicates that the product must be disposed of separately from ordinary household wastes at its end of life. Contact your related WEEE management authority, local office, or your household waste disposal service about information on the recycling drop off site.

CyberPower

www.cyberpower.com

Europe, Northern Ireland
Cyber Power Systems B.V.

Flight Forum 3545, 5657DW Eindhoven, The Netherlands
Tel: +31 40 2348170 | Fax: +31 40 2340314
Email: eu.service@cyberpower.com

Austria, Germany, Switzerland
Cyber Power Systems GmbH

Edisonstrasse 16, 85716 Unterschleissheim, Germany
Telefon: +49 89 1 222 166 0 | Fax: +49 89 1 222 166 29
Email: de.service@cyberpower.com

France
Nitram S.A.

Z.I. Saint-Séverin, 28220 CLOYES, FRANCE
Tél : +33 2 37 98 61 50 | Fax: +33 2 37 98 60 04
E-mail: infos@nitram.fr

United States, Canada
Cyber Power Systems (USA), Inc.

4241 12th Avenue East, Suite 400, Shakopee, MN 55379
Toll-free: +1 877 297 6937
Email: sales@cpsww.com

Taiwan, United Kingdom
Cyber Power Systems, Inc.

11F., No.26, Jinzhuang Rd., Neihu Dist., Taipei City 114, Taiwan
Tel: +886 2 8792 9510 | Fax: +886 2 8792 9621
Email: tw.service@cyberpower.com, uk.service@cyberpower.com

All Other Regions
Please visit our website for local contact information.

CE UK CA EAC