

Remote Netzwerk-Karte RMCARD205 / RMCARD305

Benutzerhandbuch

Die Remote Management Card ermöglicht die Verwaltung, Überwachung und Konfiguration eines USV-Systems und eines Umgebungssensors.

INHALTSVERZEICHNIS

Einführung	3
Installationsanleitung.....	6
Web-Schnittstelle	9
Befehlszeilenschnittstelle	39
Zurücksetzen auf Werkseinstellungen / Wiederherstellen eines verlorenen Passworts	64
RMCARD Firmware Upgrade.....	65
Speichern und Wiederherstellen von Konfigurationseinstellungen	71
SSH-Host-Schlüssel über Secure Copy (SCP) hochladen	75
Fehlersuche	76
Anhang 1 : IP-Adressen-Identifizierung für CyberPower Remote Management Card.....	78
Anhang 2 : Wie man ein RMCARD-Benutzerkonto in Authentifizierungsservern konfiguriert	80
Anhang 3 : USV Firmware Upgrade.....	81
Anhang 4: Software-Unterstützung	82
Anhang 5: RMCARD Adapter Anleitung.....	84

Einführung

Übersicht

Die CyberPower Remote Management Card ermöglicht die Fernüberwachung und -verwaltung einer an ein Netzwerk angeschlossenen USV. Nach der Installation der Hardware und der Konfiguration einer IP-Adresse kann der Benutzer von überall auf der Welt auf die USV zugreifen, sie überwachen und steuern! Verwenden Sie einfach einen Webbrowser, eine Befehlszeilenschnittstelle oder einen SSH-Client, um auf Ihre USV zuzugreifen. Server und Workstations können durch die USV geschützt werden, indem PowerPanel® Business Remote verwendet wird, um sich ordnungsgemäß herunterzufahren, wenn ein Signal von der Remote Management Card kommt.

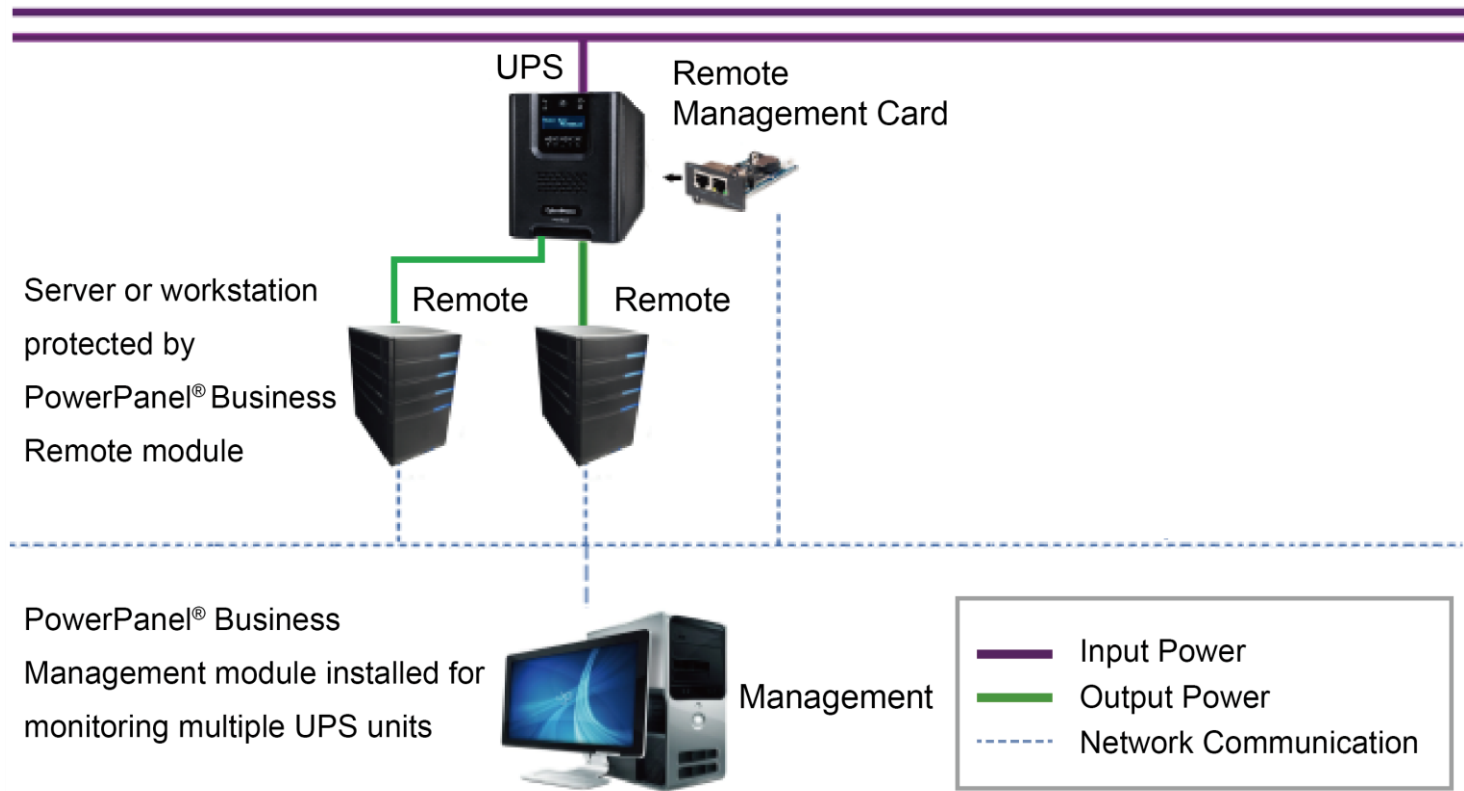
Eigenschaften

- USV-Überwachung in Echtzeit
- Remote Verwaltung und -konfiguration der USV über Webbrowser, NMS oder Command Line Interface (SSH und Telnet)
- Lokale Verwaltung und Konfiguration der USV über eine serielle Verbindung
- Auslösen des Herunterfahrens von Servern/Workstations während eines Stromausfalls, um Datenverlust oder -beschädigung zu verhindern
- Planen Sie Shutdown/Startup/Reboot der USV aus der Ferne
- Ereignisprotokollierung zur Rückverfolgung der USV-Betriebsgeschichte
- Grafische Datenaufzeichnung zur Analyse der Leistungsbedingungen
- Speichern und Wiederherstellen von Konfigurationseinstellungen, einschließlich der aktuellen USV- und ATS-Parameter-Konfiguration.
- Ereignisbenachrichtigungen per E-Mail, SNMP-Traps, Syslog und SMS
- Remote-Upgrade der USV-Firmware über Web-Interface und FTP bei ausgewählten USV-Modellen
- Unterstützung von IPv4/v6, SNMPv1/v3, HTTP/HTTPS, DHCP, NTP, DNS, SMTP, SSH, Telnet, FTP, Syslog und Modbus TCP Protokoll
- Unterstützung von sicheren E-Mail-Authentifizierungsprotokollen: SSL, TLS
- Unterstützung externer Authentifizierungsprotokolle: RADIUS, LDAP, LDAPS, Windows AD
- SNMP MIB zum kostenlosen Download verfügbar
- Vom Benutzer aktualisierbare Firmware über FTP, CyberPower Upgrade and Configuration Utility und Secure Copy Protocol (SCP)
- Aktualisieren der Firmware und Hochladen von Konfigurationsdateien auf mehrere Geräte gleichzeitig
- Mehrsprachige Benutzeroberfläche
- Schnelle Installation
- Hot-swap-fähig
- Cisco EnergyWise-kompatibel
- Unterstützung Umweltsensor (ENVIROSENSOR/SNEV001)

Systemanforderungen

- Eine 10/100-Mbps-Ethernet-Verbindung zu einem bestehenden Netzwerk
- Web-Browser oder SSH-Client
- (Optional) NMS (Network Management System), das mit SNMP kompatibel ist

Anwendung mit PowerPanel® Business

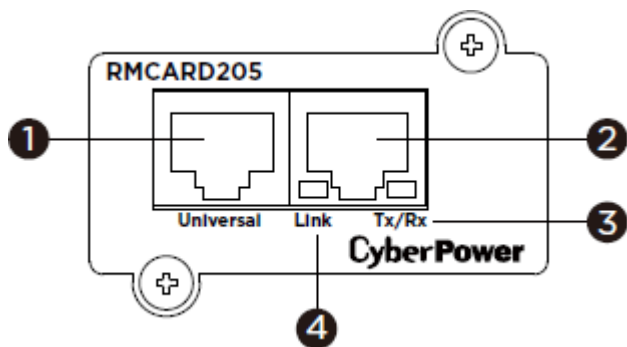


Auspacken

Überprüfen Sie die Remote Management Card bei Erhalt. Die Verpackung sollte Folgendes enthalten:

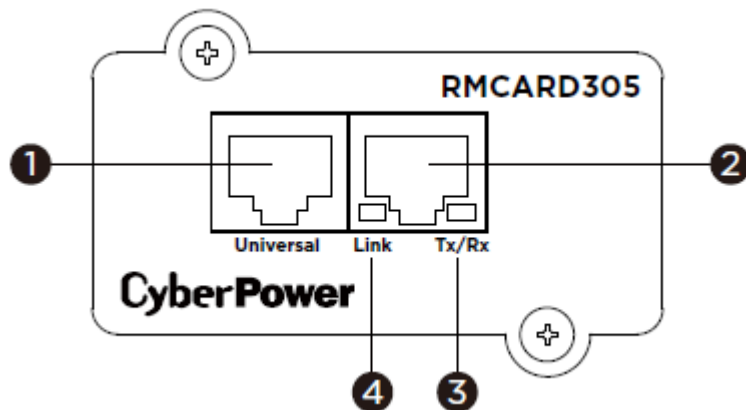
- CyberPower Remote Management Card
- RJ45/DB9 Verbindungskabel zum seriellen Port
- Schnellstart-Anleitung
- Ersatz-Jumper
- RMCARD205 Frontplatte (nur mit RMCARD305)

Frontplatte RMCARD205



1. Universal Port
2. Ethernet-Anschluss
3. Tx/Rx-Anzeige
4. Link-Indikator

RMCARD305



LED-Status-Anzeigen

Link-LED	Zustand
Aus	Die Remote Management Card ist nicht mit dem Netzwerk verbunden und/oder die Remote Management Card ist ausgeschaltet
Ein (Gelb)	Die Remote Management Card ist mit dem Netzwerk verbunden
Tx/Rx-LED	
Aus	Die Remote Management Card ist ausgeschaltet
Ein (Grün)	Die Remote Management Card ist eingeschaltet
Blinken (grün)	- Empfangen/Senden von Datenpaketen - Reset beendet

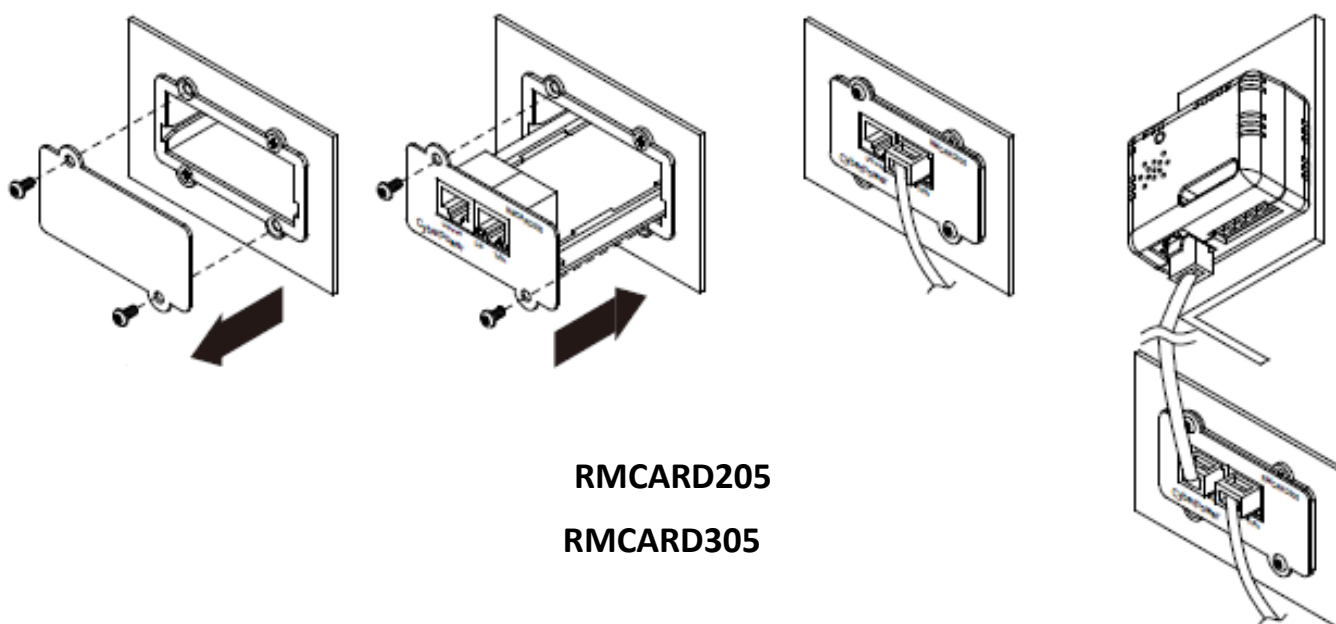
Installationsanleitung

Schritt 1. Hardware-Installation

Hinweis: Die CyberPower Remote Management Card **ist im laufenden Betrieb austauschbar**, so dass Sie die USV nicht ausschalten müssen, um sie zu installieren.

1. Entfernen Sie die beiden Befestigungsschrauben des Erweiterungssteckplatzes und nehmen Sie die Abdeckung ab.
2. Stellen Sie die CyberPower Remote Management Card in den Erweiterungssteckplatz ein.
3. Stellen Sie die Befestigungsschrauben ein und ziehen Sie sie fest.
4. Schließen Sie ein Ethernet-Kabel an den Ethernet-Port der CyberPower Remote Management Card an.
5. *(Optional)* Um einen Umgebungssensor anzuschließen, verwenden Sie ein RJ45-Ethernet-Kabel. Verbinden Sie ein Ende mit dem Universal-Port der RMCARD und das andere Ende mit dem Sensor. Weitere Informationen finden Sie im Benutzerhandbuch des ENVIROSENSOR/SNEV001.

Hinweis: Bitte schließen Sie nur einen CyberPower ENVIROSENSOR/SNEV001 oder das mitgelieferte RJ45/DB9 Serielle Verbindungskabel an den Universal Port der RMCARD an.



Schritt 2. Konfigurieren Sie die IP-Adresse für die CyberPower Remote Management Card

Hinweis: Diese Anweisungen gelten für das Betriebssystem Windows. Für andere Betriebssysteme lesen Sie bitte Anhang 4.

Methode 1: Verwendung des Power Device Network Utility 2

1. Installieren Sie "Power Device Network Utility 2", die Sie unter [Power Device Network Utility V2 - Software | CyberPower](#) herunterladen können.
2. Führen Sie nach Abschluss der Installation die "Power Device Network Utility 2" aus.

3. Das Hauptfenster der "Power Device Network Utility 2" ist in Abbildung 1 dargestellt. Das Konfigurationsprogramm zeigt alle CyberPower Remote Management-Geräte an, die sich im lokalen Netzwerk-Subnetz befinden. Mit der Schaltfläche "Scan" wird das lokale Netzwerk-Subnetz erneut durchsucht.

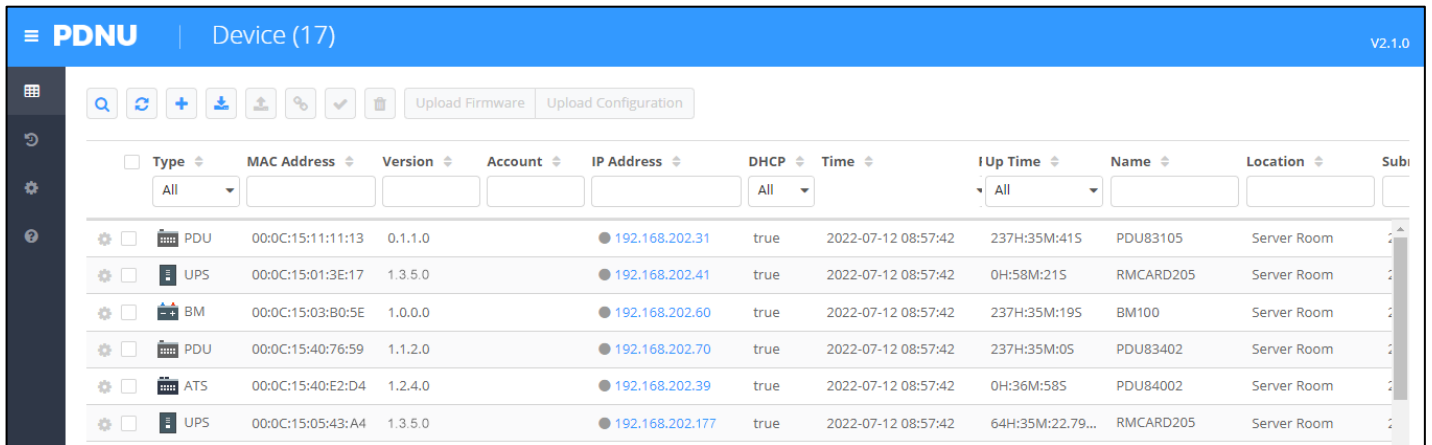


Abbildung 1. Das Hauptfenster des Programms "Power Device Network Utility 2".

4. Wählen Sie die Remote Management Card aus, die Sie einrichten möchten. Klicken Sie auf das Menü Tools und wählen Sie die Remote Management Card aus, die Sie konfigurieren möchten. Klicken Sie dann auf die Schaltfläche "Verbindung" in der oberen Werkzeugliste, um die Einrichtung vorzunehmen.

5. Sie müssen einen Benutzernamen und ein Kennwort für die Remote Management Card in das Authentifizierungsfenster eingeben, wie in Abbildung 2 dargestellt.

- Standardkonto: **cyber**
- Standard-Passwort: **cyber**

Connection Information

Account

Password

Abbildung 2. Fenster "Authentifizierung".

6. Sie können die IP-Adresse, die Subnetzmaske und die Gateway-Adresse für die MAC-Adresse des Geräts ändern, die im Fenster Netzwerkeinstellungen des Geräts aufgeführt sind (siehe Abbildung 3). Die werkseitige Standard-IP-Adresse ist 192.168.20.177 und die Standard-Subnetzmaske ist 255.255.0.0.

Device Network Settings

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

Using DHCP
 Yes No

IP Address
 192.168.20.177

New IP Address
 192 . 168 . 10 . 134

Subnet Mask
 255 . 255 . 0 . 0

Gateway
 192 . 168 . 26 . 254

Save Cancel

Abbildung 3. Das Fenster der Gerätenetzeinstellungen.

7. Ändern Sie die IP, die Subnetzmaske oder die Gateway-Adresse. Geben Sie die neuen Adressen in die entsprechenden Felder ein und klicken Sie dann auf "Speichern".
8. Wenn die Änderung nicht erfolgreich ist, z. B. wenn die Änderung der IP-Adresse nicht erfolgreich war, wird eine Warnmeldung angezeigt. Versuchen Sie erneut, die gewünschten Änderungen vorzunehmen. Wenn das Problem weiterhin besteht, lesen Sie bitte den Abschnitt "Fehlerbehebung", um Hilfe zu erhalten.

Methode 2: Verwendung einer Eingabeaufforderung

1. Ermitteln Sie die MAC-Adresse auf dem Etikett der Remote Management Card. Jede Verwaltungskarte hat eine eindeutige MAC-Adresse.

Hinweis: Die MAC-Adresse ist auf der Karte vermerkt.

2. Verwenden Sie den ARP-Befehl, um die IP-Adresse festzulegen.

Beispiel:

Um der Remote Management Card mit der MAC-Adresse 00-0C-15-00-FF-99 die IP-Adresse 192.168.10.134 zuzuweisen, geben Sie Folgendes in die Eingabeaufforderung eines PCs ein, der mit demselben Netzwerk wie die Remote Management Card verbunden ist.

- (1) Geben Sie `arp -s 192.168.10.134 00-0C-15-00-FF-99` für Windows OS ein; geben Sie `arp -s 192.168.10.134 00:0c:15:00:ff:99` für Mac OS ein, und drücken Sie die Eingabetaste.

3. Verwenden Sie den Ping-Befehl, um der IP eine Größe von 123 Byte zuzuweisen.

- (1) Geben Sie `ping 192.168.10.134 -l 123` ein und drücken Sie die Eingabetaste.

- (2) Wenn die Antworten empfangen werden, kann Ihr Computer mit der IP-Adresse kommunizieren.

Informationen zur Auswahl einer verfügbaren IP-Adresse für die Remote Management Card finden Sie in Anhang 1.

Web-Schnittstelle

Anmeldung Benutzerkonto

Sie müssen einen Benutzernamen und ein Passwort eingeben, um sich bei der Schnittstelle anzumelden, und können nach der Anmeldung eine bevorzugte Sprache auswählen. Es gibt zwei Arten von Benutzerkonten.

1. Verwalter

- Standard-Benutzername: **cyber**
- Standard-Passwort: **cyber**

2. Nur Ansicht

- Standard-Benutzername: **device**
- Standard-Passwort: **cyber**

Bei der ersten Anmeldung werden Sie aufgefordert, einen Benutzernamen und ein Passwort neu zu vergeben. Der Administrator kann auf alle Funktionen zugreifen, einschließlich der Aktivierung/Deaktivierung des Nur-Ansicht-Kontos. Der Betrachter kann nur auf Lesefunktionen zugreifen, kann aber keine Einstellungen ändern.

- Hinweis:** 1. der Administrator acco Benutzerkonto-Authentifizierung HyperText Transfer Protocol (HTTP) HTTP und HyperText Transfer Protocol over Secure Sockets Layers (HTTPS) und wird auch für die FTP-Anmeldung, Power Device Network Utility 2 und Upgrade and Configuration Utility verwendet.
2. Es kann sich jeweils nur ein Benutzer anmelden und auf das Gerät zugreifen.

Web-Inhalt

Hinweis: Englisch ist die Standardsprache, Sie können aber auch eine andere Sprache wählen.

[Zusammenfassung] Bietet einen Überblick über den Systembetrieb und die Elemente, die automatisch aktualisiert werden; bei verschiedenen USV-Systemmodellen können jedoch unterschiedliche Elemente angezeigt werden.

Artikel	Definition
Aktueller Zustand	Anzeige des aktuellen Betriebszustands der USV und des Umgebungssensors.
USV-Status	
Batteriekapazität	Graphische Darstellung des Prozentsatzes der aktuellen USV-Batteriekapazität.
Last (%)	Graphische Darstellung der USV-Auslastung als Prozentsatz der verfügbaren Wattzahl.
Verbleibende Laufzeit	Zeitspanne, in der die USV ihre Last mit Batteriestrom versorgen kann.
Systemdaten	
Name	Der Name, der der USV gegeben wurde.
Ort	Standort Beschreibung für den USV.
Kontakt	Die Kontaktperson für diesen USV.
Betriebszeit.	Dauer des ununterbrochenen Betriebs des Systems
Umgebungsstatus	
Temperatur	Grafische Darstellung der aktuellen Temperaturmessung des Umgebungssensors.
Luftfeuchtigkeit	Grafische Darstellung des aktuellen Feuchtigkeitsmesswerts des Umgebungssensors.

Artikel	Definition
Umgebungsdaten	
Name	Der Name des Umgebungssensors.
Ort	Der Standort des Umgebungssensors.
Aktuelle Geräteereignisse	Eine Liste der fünf jüngsten Geräteereignisse. Alle Ereignisse beziehen sich auf Konfigurationsänderungen.

[USV] Die folgenden Elemente können auf der USV-Seite angezeigt/konfiguriert werden; bei verschiedenen USV-Modellen können jedoch unterschiedliche Elemente angezeigt/konfiguriert werden.

[USV->Status] Anzeige der grundlegenden Informationen über den aktuellen USV-Status. Die angezeigten Elemente werden automatisch aktualisiert.

Artikel	Definition
Eingang	
Status	Den aktuellen Status der Netzversorgung an die USV
Spannung	Stromeingangsspannung der Netzversorgung.
Frequenz	Die aktuelle Frequenz des Netzs, der an die USV geliefert wird.

Strom	Die Stromstärke des Netzstroms, der an die USV geliefert wird.
Leistungsfaktor	Das Verhältnis von Wirkleistung, welche die USV erreicht, und Scheinleistung des Netzstroms.
Bypass	
Status	Zeigt den aktuellen Status des Bypass-Schaltung an.
Spannung	Die an die USV gelieferte Spannung des Bypasses.
Frequenz	Die an die USV gelieferte Frequenz des Bypasses.
Strom	Die an die USV gelieferte Stromstärke des Bypasses.
Leistungsfaktor	Das Verhältnis von Wirkleistung, welche den Bypass erreicht, und Scheinleistung des Bypasses.
Ausgang	
Status	Zeigt den aktuellen Status der Ausgangsleistung, den die USV an die angeschlossenen Geräte liefert.
Spannung	Die Ausgangsspannung, die die USV an die angeschlossenen Geräte liefert.
Frequenz	Die Ausgangsfrequenz, die die USV an die angeschlossenen Geräte liefert.
Last (%)	Die Leistungsaufnahme des angeschlossenen Gerätes, ausgedrückt als Prozentsatz der Gasamtlastkapazität. Dies wird bei einigen USV-Modellen als Wattangabe angezeigt.
Strom	Die USV-Ausgangsstrom in Ampere.
Leistungsfaktor	Das Verhältnis von Wirkleistung, welche die Last erreicht, und Scheinleistung der Schaltung.
Wirkleistung	Die Kapazität der Schaltung zum Arbeiten in einer bestimmten Zeit.
Scheinbare Leistung	Das Produkt von Stromstärke und Spannung im Schaltkreis.
Blindleistung	Der durch induktive und kapazitive Netzwerkelemente temporär in Form von magnetischen oder elektrischen Feldern gespeichert und dann an die Quelle zurückgegeben wird, auch als Blindleistung bekannt.
NCL	Zeigt den aktuellen Status des NCL Ausgangs anzeigen.

Artikel	Definition
Energiewert(kWh)	Energiezählerstand des Geräts in kWh-Einheiten. *Klicken Sie auf "Zurücksetzen", um den Energiewert auf null zu setzen.
Batterie	
Status	Der aktuelle Status der USV-Batterie.
Lademodus	SBM-Modus: Verwenden des Smart Battery Management (SBM) -Modus zum Aufladen der Batterien, wodurch die Gesamtdauer der Batterie verlängert wird, und der Schnellladungs-technologie. Normaler Modus: Verwenden Sie die normale Ladeart, um die Batterien aufzuladen.
Ladezustand	Im SBM-Modus: Zeigt die 3 Betriebsphasen (Lade-Float-Ruhe-Modus) von Smart Battery Management (SBM) an.

	Im Normalmodus: Zeigt das Ladegerät im Normalmodus an.
Verbleibende Kapazität	Die derzeitige Kapazität der Batterie(n) als Prozentsatz der vollen Ladung ausgedrückt.
Verbleibende Laufzeit	Die Länge der Zeit, für die die USV-Strom an ihre Last liefern kann.
Spannung	Die aktuelle Spannung der USV-Batterie.
System	
Status	Zeigt den aktuellen Betriebszustand der USV.
Temperatur	Die aktuelle interne Temperatur der USV. Wird in (°C) und Fahrenheit(°F) angezeigt.
Wartung Unterbrecher	Zeigt den aktuellen Betriebszustand der Wartungspause.

[USV->Batteriestatus Zeigt die Informationen der integrierten Batterie und der Erweiterten Batteriemodule (EBM) einschließlich der Akkutemperatur an, Spannung jeder Batterie innerhalb ihres Batterie- und Batteriepack-Ausgleichszustands.

Artikel	Definition
Datum des letzten Updates	Das letzte Datum, an dem der Batteriestatus aktualisiert wird. Update: Verwenden Sie diese Funktion, um den aktuellen Batteriestatus abzurufen.
Aktualisieren	Verwenden Sie diese Funktion, um den neuesten Batteriestatus zu erhalten.
Temperatur	Die aktuelle Temperaturanzeige des UPS / EBM-Akkupacks.
Spannung	Der aktuelle Spannungswert jeder USV / EBM-Batterie.
Ausgleichsstatus	Zeigt den aktuellen Batteriespannungsausgleichsstatus des UPS / EBM-Akkus an. Aktiv: Die Akku-Ausgleichsfunktion ist aktiv. Inaktiv: Die Akku-Ausgleichsfunktion ist nicht aktiv.

[USV->Information] Anzeige der technischen Daten der USV.

Informationen	Beschreibung
Modell	Die Modellbezeichnung der USV.
Informationen	Beschreibung
Spannungsbereich	Der Ausgabe Nennspannung (Volt) der USV.
Betriebsfrequenz	Die Frequenz der USV-Ausgangsleistung.
Nennleistung	Die Volt/Ampere Angabe der USV.
Stromwert	Der Ausgangsnennstrom (Ampere) der USV.
Last	Die Leistungsangabe (Watt) der USV
Batterie(n)pannung	Die Gleichspannungsangabe der Batterie(n)atzes
Firmware Version	Die Revisionsnummer der USV-Firmware. Aktualisieren: Verwenden Sie diese Funktion, um die USV-Firmware zu aktualisieren. Klicken Sie auf Durchsuchen Sie den Speicherort der UPS-

	Binardatei und klicken Sie auf Senden.
USB-Firmware-Version	Die Revisionsnummer der USV USB Firmware
LCD-Firmware-Version	Die Revisionsnummer der USV LCD-Firmware
Austauschdatum Batterien	Das Datum, zu dem die Batterie(n) zuletzt ersetzt wurden; es kann nur zum Zeitpunkt des Batteriewechsels eingestellt werden. Dieses Datum sollte nach dem Batteriewechsel eingestellt werden. Falls dieses Datum nicht eingestellt ist, sollte dieses Datum sofort eingestellt werden.
NCL	Die Anzahl der nicht kritischen Last.
Externe	Die Anzahl an externen Batteriepacks, die an die USV angeschlossen sind.
Installationsort	Durch Anklicken von Suchen werden Nutzer mit Hilfe des akustischen Alarms oder blinkender Anzeigen informiert. Dies hilft Nutzern bei der Identifizierung der spezifischen USV, wenn mehrere USVen vorhanden sind.

[USV->Konfiguration] Konfigurieren Sie die Parameter der USV.

Artikel	Definition
Eingangsversorgung	
Spannung	Legt die Ausgabespannung, die dem angeschlossenen Gerät geliefert wird, fest. Hinweis: Bei einigen Modellen, die zur Paragon Tower Serie gehören, ist diese Einstellung im Bypass Modus konfigurierbar und die Änderungen erfordern einen Neustart zur Aktivierung.
Netzversorgung ausgefallen	
Hohen Eingangs (oder Ausgangs) Spannungsschwellwert	Wenn die USV feststellt, dass die Versorgungsspannung außerhalb des zulässigen Bereichs liegt, schaltet die USV auf Batteriebetrieb um, um die an die USV angeschlossenen Geräte zu schützen. Bei niedriger Empfindlichkeit ist der Spannungsbereich kleiner und die Versorgungsspannung kann stärker schwanken. Die Stromversorgung durch den Kraftstoffgenerator kann dazu führen, dass die USV häufiger in den Batteriebetrieb schaltet, weshalb die niedrige Empfindlichkeit empfohlen wird. Die USV schaltet seltener in den Batteriebetrieb und spart außerdem mehr Batteriestrom. Mit einer hohen Empfindlichkeit kann die USV die Geräte stabiler mit Strom versorgen und schaltet häufiger in den Batteriebetrieb.
Geringen Eingangs (oder Ausgangs) Spannungsschwellwert	Wenn die Netzspannung oder die Ausgangsspannung (je nach USV-Modell) über/unter dem Schwellenwert liegt, versorgt die USV die angeschlossenen Geräte mit Batteriestrom.

Artikel	Definition
Frequenztoleranz	Legt den akzeptablen Bereich der Eingangsfrequenz fest. Falls sich der Wert außerhalb dieser Toleranz befindet, befindet sich das Gerät im Stromausfallzustand.
Betrieb	
Normal	Normaler Betriebsmodus der USV.
Generatormodus	Falls die USV einen Generator zur Leistungsaufnahme nutzt, sollte diese Option aktiviert werden, damit die USV normal funktioniert. Falls diese Option ausgewählt ist, darf die USV den Bypass Modus zum Schutz der mit Energie versorgten Geräte nicht aufrufen.
Energiesparmodus	Online USV ruft Energiesparmodus auf. Die USV ruft den Bypass Modus auf, wenn die Eingangsspannung/ Frequenz innerhalb des Bereichs der Schwellwerte liegt. Sobald die Netzspannung/ Frequenz die Schwellwerte übersteigt, versorgt die USV ihre Lasten mit Strom.
Manueller Bypass	Legt fest, ob die USV den manuellen Bypass Modus aufrufen darf. Falls diese Option aktiviert ist, wird die USV gezwungen, den Bypass Modus aufzurufen.
Bypass	Hinweis: Die USV kann automatisch in den Bypass-Modus wechseln, wenn diese Einstellungen vorgenommen werden.
Bypass-Bedingungen	<p>Kein Bypass: Wenn diese Option ausgewählt wird, wird die USV nicht in den Bypass Modus wechseln und aufhören, eine Ausgabeleistung zu liefern.</p> <p>Volt/Freq. prüfen: Falls die Netzspannung im Bereich von Hohen/Geringe Bypass Spannung und die Netzfrequenz im Bereich der Frequenztoleranz liegt, ruft die USV den Bypass Modus auf. Andernfalls stoppt die USV die Versorgung mit Ausgangsleistung.</p> <p>Nur Volt prüfen: Nur wenn die Netzspannung im Bereich von Hohen/Geringe Bypass Spannung liegt, ruft die USV den Bypass Modus auf. Andernfalls stoppt die USV die Versorgung mit Ausgangsleistung.</p>
ByPass aktivieren, wenn USV aus ist	Bei Abschaltung der USV wechselt die USV in den Bypass Modus.
Wiederkehr Versorgung	Nachdem Wiederherstellung der Netzversorgung schaltet sich die USV automatisch ein und versorgt den Computer mit Strom. Falls das Computer BIOS darauf eingestellt ist, das System bei Wiederherstellung der Netzversorgung hochzufahren, startet der Computer automatisch neu. Die folgenden Einstellungen werden verwendet, um das USV-Wiederherstellungsverhalten zu konfigurieren:
Automatische Wiederkehr	Wenn diese Option aktiviert ist, setzt die USV die Ausgabe bei Wiederherstellung der Netzversorgung sofort fort. Wenn diese Option deaktiviert ist, setzt die USV die Ausgabe zu diesem Zeitpunkt nicht fort und der Nutzer muss sie zu einem späteren Zeitpunkt manuell einschalten.
Verzögerung Aufladung	Bei Wiederherstellung der Netzversorgung beginnt die USV mit dem Wiederaufladen, bis die angegebene Verzögerung abgelaufen ist, bevor sie die Ausgabe fortsetzt.

Aufgeladene Kapazität	Bei Wiederherstellung der Netzversorgung beginnt die USV mit dem Wiederaufladen, bis die angegebene Batteriekapazität erreicht ist, bevor sie die Ausgabe fortsetzt.
Verzögerung Rückkehr	Die Wiederherstellungsverzögerung tritt bei jedem Einschalten der USV in Kraft. Dies beinhalten auch die Planung und Nutzersteuerungsaufgabe.
Stabile Linienverzögerung	Wenn sich die USV im Batteriemodus befindet und die Netzversorgung wiederhergestellt wird, wartet die USV die spezifische Verzögerungszeit zum Wechseln vom Batteriemodus in den Netzmodus ab. Wenn die Kapazität des USV-Batterie(n) bereits unterhalb des Batterie(n)stand gering Schwellwertes liegt und die Netzversorgung wiederhergestellt wird, kehrt die USV sofort in den Netzmodus zurück.
Artikel	Definition
Batterie	
Externe Batterieerweiterung(en)	Anzahl der Batterieerweiterungen und Kapazität
Schwellwert Batterie schwach	Wenn die USV-Batterie(n) trom bereitstellt und die verbleibende Kapazität unter dieser Schwelle liegt, gibt die USV einen Alarm aus.
Externe Batterieerweiterung	Legen Sie die Anzahl der externen Batteriepacks fest. Dies ermöglicht eine exakte Ermittlung der Laufzeit basierend auf der Gesamtanzahl Batterie(n).
Regelmäßiger Batterietest	Die USV führt in zyklischen Abständen einen automatischen Batterietest durch, um sicherzustellen, dass die Batterie(n) voll funktionsfähig sind. Hinweis: Nur online (OL) -Reihe der Smart Battery Management (SBM) Funktion unterstützen. SBM führt Batterietests, auch wenn Periodische Batterietest Einstellung deaktiviert ist.
Ladungsmodus	Normaler Modus: Verwenden Sie die normale Ladeart, um die Batterien aufzuladen. SBM-Modus: Aktivieren des Smart Battery Managements zum Laden der Batterien.
Gebührenkontrolle	Aktiviert/Deaktiviert, um die Ladefunktion ständig zu überwachen.
Selbsttest beim Start der USV	Wenn diese Option aktiviert ist, führt die USV den Selbsttest automatisch durch, wenn die USV eingeschaltet wird. Hinweis: Der Selbsttest wird nicht ausgelöst, wenn die USV einen Auto-Neustart durchführt.
System	
Kaltstart	Legen Sie die Fähigkeit der USV fest, ohne Aufnahmeleistung zu starten. Wenn diese Option aktiviert ist, kann die USV ohne Aufnahmeleistung gestartet werden.
Akustischer Alarm	Wenn diese Option aktiviert ist, gibt die USV bei Versorgung mit Batterie(n) trom oder einer Ausgangs Überlast einen akustischen Alarm aus.
Relais-Kontakt Funktion	Dies konfiguriert den Betriebszustand des potenzialfreien USV-Relais, wenn

	<p>der ausgewählte Zustand auftritt. Weitere Informationen über die Nutzung des fortschrittlichen potenzialfreien USV-Relais erhalten Sie in der USV Anleitung. Die Funktion des potenzialfreien Relais bietet folgende Betriebszustände:</p> <p>Netzausfall: Der Netz fällt aus und die USV nutzt Batterie(n)trom.</p> <p>Batterie schwach: Die Batteriekapazität ist zu gering, als dass die angeschlossenen Computer herunterfahren könnten.</p> <p>Alarm: Die USV gibt aufgrund von Warnereignissen, wie einer Überlast, einen akustischen Alarm aus.</p> <p>Bypass: Die USV ist aufgrund einer Überlast oder eines USV Fehlers in den Bypass Modus gewechselt.</p> <p>USV Fehler: Die USV funktioniert aufgrund eines Hardwarefehlers, wie z. B. eines Inverter Fehlers, Busfehlers oder einer Überhitzung, möglicherweise nicht richtig.</p>
Zeit Bildschirmschoner	Wenn keine USV-Schaltfläche gedrückt wird oder sich kein Stromausfall während dieser Verzögerung ereignet, wird der LCD Bildschirm ausgeschaltet.

Artikel	Definition
Ruhezustand nach Abschaltung aller Remote einleiten	Wenn diese Option aktiviert ist, wechselt die USV nach allen PowerPanel® Remote-Shutdown +2 Minuten in den Ruhemodus. Hinweis: Für PowerPanel® Business Edition-Clients, wenn diese Option aktiviert ist, ruft die USV den Ruhemodus auf, nachdem das Netz ausgefallen ist und die verbleibende Zeit MSDT+2 Minuten beträgt. Weitere Informationen über MSDT erhalten Sie auf der Hilfeseite der USV > PowerPanel Liste.
Erkennung Verkabelungsfehler	Falls diese Option aktiviert ist, erkennt die USV, ob die USV-Verkabelung geerdet oder vertauscht ist. Sie sollten zunächst sicherstellen, dass die USV-Verkabelung geerdet ist. Diese Option sollte aktiviert sein, wenn die USV-Verkabelung geerdet ist.
Tiefentladeschutz	Wenn sich die USV im Batteriemodus mit 0 % Last befindet und der Status für die konfigurierte Dauer aufrechterhalten bleibt, Die Fernverwaltungskarte versetzt die USV in den Standby-Modus und der Ausgang wird ausgeschaltet.
Nicht kritische Ausgangsreihe NCL	
Abschaltung Schwellwert	Bei Bereitstellung von Batterie(n)trom wird die USV diesen NCL-Ausgang ausschalten, wenn die verbleibende Batteriekapazität unter diesem Schwellwert liegt.
Abschaltverzögerung (nach einem Stromausfall)	Bei Bereitstellung von Batterie(n)trom wird die USV den NCL-Ausgang ausschalten, nachdem diese Verzögerungszeit erreicht ist.

Einschaltverzögerung (nach Wiederherstellung des Versorgungsnetzes)	Bei Wiederherstellung des Netzes setzt die USV die Ausgabe seines NCL Ausgangs nach Ablauf der Verzögerungszeit fort. Dies verhindert übermäßigen Stromverbrauch, der bei gleichzeitigem Einschalten aller angeschlossenen Geräte auftritt.
---	---

[USV->Hauptschalter] Schalten Sie die Ausgangsleistung der USV ein oder aus.

Artikel	Definition
Neustart USV	Schaltet die USV aus und wieder ein
USV ausschalten	Schaltet die USV aus.
USV-Ruhezustand (Verfügbar, wenn Netzversorgung ausgefallen ist)	Dieser Befehl ist im Stromausfallmodus verfügbar. Er kann die USV in den Ruhezustand versetzen, bis die Netzversorgung wiederhergestellt ist. (Einige USV unterstützen diesen Befehl möglicherweise nicht) Hinweis: Einige USV-Modelle unterstützen diesen Befehl möglicherweise nicht.
Zurücksetzen	Bricht eine ausstehende Aktion zum Abschalten der USV ab.
USV einschalten	Schaltet die USV ein.
Herunterfahren/Verzögerung	Wie lange die USV wartet, bevor Sie sich in Folge eines der Befehle USV neu starten, USV ausschalten und USV-Ruhezustand abschaltet.
Ruhezustand	
Dauer Wiederstart	Nach Abschaltung der USV-Neustartdauer legt fest, wie lange die USV wartet, bevor sie sich in Folge eines USV neu starten Befehls wieder einschaltet.
PowerPanel® Remote Shutdown Befehl senden	Wählen Sie diese Option, wenn die PowerPanel Business Remote vor der USV-Abschaltung gewarnt werden sollen. Die Abschaltverzögerung (MST, Max. Remote Shutdown Time) für die USV kann zur Sicherstellung einer ordnungsgemäßen Abschaltung geändert werden.

[USV->Verwaltung Ausgangsreihe] Die Seite Ausgangsreihesteuerung zeigt den aktuellen Status der Ausgangsreihe und bietet Ein /Abschaltsteuerung für die nicht kritische Ausgangsreihe. Ausgangsindex und Gerätenamen zeigen den Gerätenamen, der Strom über den spezifischen Ausgang bereitstellt.

Artikel	Definition
Verwaltung Ausgangsreihe Optionen	
An	Schaltet die nicht kritische Band sofort ein.
AUS	Schaltet die nicht kritische Bank sofort aus.
Identifizierung des Gerätenamens	
Ausgang #	Der Index des Ausgangs.
Gerätenamen	Gerätenamen an diesem Ausgang.

Hinweis: Nur umschaltbare USVs der Critical Outlet Bank unterstützen die Ein/Aus-Steuerung der Critical Outlet Bank.

[USV->Diagnose] Die Seite **USV/Diagnose** bietet die Fähigkeit zur Verifizierung, ob die USV eine angemessene Batterielaufzeit zur ordnungsgemäßen Abschaltung angeschlossener Computer bereitstellen kann. Führen Sie eine vollständige Laufzeitkalibrierung zur Gewährleistung und exakten Ermittlung der Laufzeit für die angeschlossene Last durch. Summer und Anzeige der USV können auf ihre Funktionstüchtigkeit hin getestet werden. Die Informationen werden nach Abschluss eines Batterietests gemeldet.

Artikel	Definition
Batterietest	Der Batterietest prüft, ob die Batterie(n) in einem guten Zustand sind, Auf diese Weise kann der Benutzer den Batteriezustand überprüfen und Informationen über die Batterie bereitstellen, einschließlich der Ergebnisse und des Datums des letzten Batterietests. Klicken Sie zum Starten eines Batterietests auf die Starten Schaltfläche. Die Informationen werden nach Abschluss eines Batterietests gemeldet. Hinweis: „N / A“ bedeutet, dass das USV-Modell diese Funktion nicht hat.
Starten	Batterietest sofort ausführen.
Letztes Testergebnis	Das Datum des zuletzt ausgeführten Batterietests.
Letzter Testdatum	Das Ergebnis des letzten Batterietests.
Kalibrierung Laufzeit	Die Laufzeitschätzung entlädt die Batterien unter der aktuellen Belastung von der aktuellen Batteriekapazität auf nahezu Null. Die Ergebnisse der Laufzeitschätzung zeigen den Status der Schätzung, das Datum der letzten Schätzung und die geschätzte Laufzeit. Wenn die Laufzeitschätzung gestartet wird, wird das angeschlossene Gerät von der USV über den Batteriestrom betrieben, bis die Batterien fast vollständig entladen sind. Bitte beachten Sie, dass die geschätzte Laufzeit variieren kann, da sie abhängig von der Belastung und dem Ladezustand der Batterien ist, wenn die Laufzeitschätzung eingeleitet wird. Nachdem die Schätzung durchgeführt wurde, werden die Batterien automatisch wieder aufgeladen. Benutzer können auf die Schaltfläche Start klicken, um die Laufzeitschätzung zu beginnen. Klicken Sie auf die Schaltfläche Abbrechen, um die Laufzeitschätzung zu unterbrechen. Das Ergebnis wird angezeigt, nachdem die Laufzeitschätzung beendet oder abgebrochen wurde :
Artikel	Definition
Geschätzte Laufzeit	Die geschätzte Laufzeit im Batteriebetrieb.
Geschätzte Laufzeit	Die geschätzte Laufzeit der Batterien mit der aktuellen Last.
Ergebnis letzten Kalibrierung	Die Ergebnisse der letzten Laufzeitschätzung. Bestanden: Die Laufzeitschätzung wurde abgeschlossen und die Batterien sind in Ordnung. Abgebrochen: Die Laufzeitschätzung wurde unterbrochen.
Datum letzten Kalibrierung	Das Datum, an dem die letzte Laufzeitabschätzung durchgeführt wurde.

[USV->Zeitplan]: Stellt die USV so ein, dass sie zu geplanten Zeiten automatisch herunterfährt und neu startet (einmal/täglich/wöchentlich). Die Seite **Zeitplan** verwaltet die geplanten Shutdowns und listet alle konfigurierten Zeitpläne auf. Jede Zeitplanzeile zeigt die Details an, wann der Zeitplan in Kraft treten wird.

[Einmal]: Der Benutzer kann ein Zeitereignis für das Herunterfahren/Neustarten der USV festlegen.

[Täglich]: Legen Sie fest, wie oft die USV täglich heruntergefahren/neu gestartet werden soll.

[Wöchentlich]: Legen Sie eine wöchentliche Wiederholung für das Herunterfahren/Wiedereinschalten der USV fest.

1. Klicken Sie auf die Option [Einmal], [Täglich] oder [Wöchentlich] und klicken Sie auf "Weiter>>", geben Sie das Datum und die Uhrzeit für das Herunterfahren der USV ein. Wählen Sie [Nie], [Sofort] oder das Datum und die Uhrzeit, zu der die USV wieder eingeschaltet werden soll. Wählen Sie die zu steuernde Bank aus und klicken Sie auf " Remote herunterfahren", um alle Clients für ein sanftes Herunterfahren zu konfigurieren. Sie können einen "Namen" für diesen Zeitplan eingeben.
2. Klicken Sie auf "Übernehmen", um das Element zum Zeitplan hinzuzufügen. Klicken Sie auf "Zurücksetzen", um zu den Standardeinstellungen zurückzukehren.
3. Gespeicherte Einstellungen werden im Menü [Zeitplan] aufgelistet.
4. Wenn Sie die geplante Aktion löschen möchten, klicken Sie einfach auf den Namen des Elements im Menü [Zeitplan] und dann auf "Löschen".

Hinweis: Das Managementsystem erlaubt bis zu 10 Zeitplaneinträge.

[USV->Wake on Lan] Mit dieser Funktion kann ein Computer über das Netzwerk aufgeweckt werden. Geben Sie die IP-Adresse des eingeschalteten Computers ein, und das System sucht seine MAC-Adresse entsprechend. Die maximale Anzahl der IP-Adressen, die eingestellt werden können, beträgt 50.

Artikel	Definition
PowerPanel® Remote	
Aufnehmen/Sync mit PowerPanel Remote Liste	Laden und mit PowerPanel Remote Liste synchronisieren. PowerPanel Remote Netzwerkgerät bei Netzversorgungsereignis aufwecken.
Bedingungen Aufwecken	
USV-Einschalten	Durch Aktivieren der Option können Sie ein registrierten Netzwerkgerät bei einem Betriebsereignis aufwecken: USV-Einschaltung.
Artikel	Definition
Netzversorgung wiederhergestellt und Ausgang wird versorgt	Durch Aktivieren der Option können Sie ein registrierten Netzwerkgerät bei einem Betriebsereignis aufwecken: USV-Netzwiederherstellung und Ausgang wird versorgt.
WoL-Listen	
WoL Remote Liste	When the option Load/Sync with PowerPanel® Remote List is enabled, PPB Remote PC IP/MAC shows here.
WoL-Handbuch Liste	Wake on Lan manual list.

Hinweis: Die BIOS-Einstellungen des PowerPanel® Remote-Computers müssen WoL unterstützen und entsprechend konfiguriert sein.

[USV->EnergyWise] Die EnergyWise-Initiative konzentriert sich auf die Reduzierung des Energieverbrauchs aller mit einem Cisco-Netzwerk verbundenen Geräte. Durch diese Kompatibilität ist die CyberPower Remote Management Card für die Zusammenarbeit mit anderen EnergyWise-fähigen Geräten anerkannt und kann leicht überwacht und gesteuert werden, um die beste Energieleistung im Rahmen des EnergyWise-Betriebsrahmens zu erzielen.

Artikel	Definition
Konfiguration	
Version	Aktivieren Sie die CISCO EnergyWise Unterstützung.
EnergyWise	Aktivieren Sie die Unterstützung von CISCO EnergyWise.
Service Port	Die für die Kommunikation mit der EnergyWise Lösung genutzte Portnummer. (Muss mit Switch identisch sein)
Domainname	Der Domainname der EnergyWise Lösung. (Muss mit Switch identisch sein)
Off State-Cache	Aktivieren/deaktivieren Sie den Endpunkteintrag zum Zwischenspeichern in der Switch EnergyWise Liste nach dem Neustart.
Abgesicherter Modus	Aktivieren Sie die EnergyWise Nutzung eines gemeinsamen Geheimnisses.
Gemeinsames Geheimnis	Das Geheimnis der EnergyWise Domain.
Liste Netzknoten	
EnergyWise Parent/Children List zeigt alle EnergyWise Entitäten und erlaubt Benutzern, EnergyWise Entitätsattribute zu konfigurieren.	
Name	Der zur Identifikation jedes einzelnen Ausgangs verwendete Name.
Rolle	Dieser Parameter ist ein zum Beschreiben der Funktion des Eintrags verwendeter String. (Max. Länge von 31 Zeichen)
Schlüsselbegriffe	Dieser Parameter ist ein zum Beschreiben des Eintrags verwendeter String. (Max. Länge von 31 Zeichen).
Wichtigkeit	Dieser Parameter ist ein Wert zwischen 1 und 100, der die Wichtigkeit des Eintrags (hoch oder gering) anzeigt.

[USV->PowerPanel® Liste] Zeigt die Informationen der verbundenen PPB (PowerPanel Business) Remote. Die Verbindung wird durch PPB Remote ausgeführt und der aufgelistete Remote wird bei 1 stündiger Trennung entfernt.

Hinweis: Es wird nicht empfohlen, die PowerPanel® Business Edition- oder PowerPanel® Business-Verbindung gleichzeitig mit der Remote-Management-Karte herzustellen

Artikel	Definition
Konfiguration	
Max. Remote Abschaltzeit (MST)	Die maximale Zeit, die alle angeschlossenen Remote zum Herunterfahren benötigen.
Max. Remote Abschaltverzögerungszeit (MSDT)	Der maximale Zeitwert ab einem Stromausfall, bis alle Remote heruntergefahren sind.
Liste	
Typ	Die Art des PowerPanel® Business <ul style="list-style-type: none"> • Remote • Management
Abschaltbedingung	Der Abschaltzustand von PowerPanel® Business <ul style="list-style-type: none"> • Keine • Stromausfall • Schwache Batterie • Laufzeit unzureichend
Status	Der Status von PowerPanel® Business <ul style="list-style-type: none"> • Anschließen • Normal • Herunterfahren wird ausgeführt • Herunterfahren ist abgeschlossen

[Umgebung] Die folgenden Punkte können auf der Envir-Seite angezeigt/konfiguriert werden. Beachten Sie, dass die Registerkarte Envir nur erscheint, wenn ein ENVIROSENSOR/SNEV001 an die RMCARD angeschlossen ist.

[Umgebung ->Status] Zeigt die grundlegenden Informationen des Umgebungssensors und der Kontaktschließeingänge an.

Artikel	Definition
Informationen	
Name	Der Name des Umgebungssensors.
Ort	Der Ort des Umgebungssensors.
Temperatur	
Aktueller Wert	Die aktuelle Umgebungstemperatur.

Maximum	Die höchste vom Umgebungssensor erkannte Temperatur und die Zeit des Auftretens.
Minimum	Die niedrigste vom Umgebungssensor erkannte Temperatur und die Zeit des Auftretens.
Feuchtigkeit	
Aktueller Wert	Die aktuelle Umgebungsfeuchtigkeit.
Maximum	Die höchste vom Umgebungssensor erkannte Feuchtigkeit und die Zeit des Auftretens.
Minimum	Die geringste vom Umgebungssensor erkannte Feuchtigkeit und die Zeit des Auftretens.
Kontakt	Zeigt den Namen und den Status (normal/normal) (Normal / Abnormal) jedes trockenen Eingangskontakts an.

[Umgebung ->Konfiguration] Konfigurieren Sie die Parameter des Umweltsensors.

Artikel	Definition
Informationen	
Name	Der zur Identifikation des Umgebungssensors verwendete Name.
Ort	Der Ort, an dem sich der Umgebungssensor befindet.
Temperatur	
Hoher Schwellenwert	Obergrenze der normalen Temperatur.
Niedriger Schwellenwert	Untergrenze der normalen Temperatur.
Hysterese	Der Unterschied zwischen dem oberen/unteren Schwellwert und dem Punkt, an dem der Temperaturstatus von unnormal zu normal wechselt.
Änderungsrate	Die zur Bestimmung einer ungewöhnlichen Temperaturänderung verwendete Geschwindigkeit.
Einheit	Die Einheit der Temperaturmessung.
Feuchtigkeit	
Hoher Schwellenwert	Obergrenze der normalen Feuchtigkeit.
Niedriger Schwellenwert	Untergrenze der normalen Feuchtigkeit.
Hysterese	Der Punkt, an dem der Unterschied zwischen dem Schwellenwert für hohe und niedrige Luftfeuchtigkeit von anormal zu normal wechselt.
Änderungsrate	Der Unterschied zwischen dem oberen/unteren Schwellwert und dem Punkt, an dem der Feuchtigkeitsstatus von unnormal zu normal wechselt.
Kontakt	Der zur Identifikation des Kontakts verwendete Name.

[Accessory] Die folgenden Punkte können auf der Accessory Seite angezeigt/konfiguriert werden. Beachten Sie, dass die Registerkarte "Accessory" nur erscheint, wenn eine neue Version des Umweltsensors (SNEV001) an die RMCARD angeschlossen ist.

[Accessory->Status->ENV Basic Status] Anzeige der Basisinformationen des Umweltsensors.

Artikel	Definition
Informationen	
Name	Der Name des Umgebungssensors.

Ort	Der Standort des Umgebungssensors.
Temperatur	
Aktueller Wert	Die aktuelle Temperatur der Umgebung.
Maximum	Die höchste Temperatur sowie der Zeitpunkt des Auftretens wird vom Umgebungssensor erfasst.
Minimum	Die niedrigste Temperatur sowie der Zeitpunkt des Auftretens, der vom Umgebungssensor erfasst wird.
Feuchtigkeit	
Aktueller Wert	Die aktuelle Luftfeuchtigkeit in der Umgebung.
Maximum	Die höchste Luftfeuchtigkeit sowie der Zeitpunkt des Auftretens wird vom Umgebungssensor erfasst.
Minimum	Die niedrigste Luftfeuchtigkeit sowie der Zeitpunkt des Auftretens werden vom Umgebungssensor erfasst.

[Accessory->Status->ENV Kontakt Status] Zeigt die grundlegenden Informationen der Kontaktschlusseingänge an.

Artikel	Definition
Informationen	
Kontakt	Zeigt den Namen und den Status (Normal / Abnormal) jedes trockenen Eingangskontakts an.

[Zubehör->Information] Zeigt die grundlegenden Informationen des Zubehörgeräts an.

Artikel	Definition
Informationen	
Position	Die Position des Zusatzgeräts.
Modell	Der Modellname des Zubehörgeräts.
Seriennummer	Die Seriennummer des Zubehörgeräts.
Hardware-Version	Die Hardware-Version des Zubehörgeräts.
Firmware-Version	Die Firmware-Version des Zubehörgeräts.
Firmware-Aktualisierung	
Aktualisieren Sie die Firmware des Zubehörgeräts. Klicken Sie auf Durchsuchen, um den Speicherort der Zubehör-Binärdatei zu finden, und klicken Sie auf Senden, um die Datei hochzuladen.	

[Accessory->Konfiguration-> ENV Basic Konfiguration] Konfigurieren Sie die Parameter des Umgebungssensors.

Artikel	Definition
Informationen	
Name	Der Name, der zur Identifizierung des Umgebungssensors verwendet wird.
Ort	Der Ort, an dem sich der Umgebungssensor befindet.
Temperatur	
Hoher Schwellenwert	Der obere Grenzwert für die normale Temperatur.
Niedriger Schwellenwert	Der untere Grenzwert für die Normaltemperatur.
Hysterese	Die Differenz zwischen dem oberen/unteren Schwellwert und dem Punkt, an dem der Temperaturzustand von anormal zu normal wechselt.
Rate der Veränderung	Die Rate wird verwendet, um anormale Temperaturänderungen zu definieren.
Einheit	Die Einheit der Temperatur.
Feuchtigkeit	
Hoher Schwellenwert	Der obere Grenzwert für die normale Luftfeuchtigkeit.
Niedriger Schwellenwert	Der untere Grenzwert für die normale Luftfeuchtigkeit.
Hysterese	Die Differenz zwischen dem oberen/unteren Schwellwert und dem Punkt, an dem der Zustand der Luftfeuchtigkeit von abnormal zu normal wechselt.
Rate der Veränderung	Die Rate wird verwendet, um anormale Änderungen der Luftfeuchtigkeit zu definieren.

[Zubehör->Konfiguration-> ENV-Kontakt Konfiguration] Konfigurieren Sie die Parameter der Kontaktschlusseingänge.

Artikel	Definition
Kontakt	Geben Sie den Namen jedes Eingangsrelais mit potenzialfreiem Kontakt ein und verwenden Sie das Dropdown-Menü, um den Normalzustand jedes Relais zu definieren.
Name	Der Name wird zur Identifizierung des Kontakts verwendet.
Status	Der Zustand wird verwendet, um den normalen Zustand des Kontakts zu definieren.

[Log Daten ->Ereignisprotokolle] Zeigt die Liste von Ereignissen und eine kurze Beschreibung jedes Ereignisses sowie Datum und Zeitstempel.

Hinweis: 1. Die aufnehmbaren Ereignisse werden unter "System > Benachrichtigungen > Ereignisaktion" aufgelistet und die Aufzeichnungszeit wird im 24 Stunden Format angegeben.

2. Die aufgezeichnete Zeit wird im 24-Stunden-Format angezeigt.

[Auf dieser Seite werden die Protokolle des USV-Status und des Umgebungsstatus angezeigt; bei verschiedenen Produkten können jedoch unterschiedliche Elemente angezeigt werden.

Alle Positionen haben die gleiche Definition wie im USV-Status oder Umweltstatus.

- **Eingang min. (V)** Die minimale Eingangsspannung der Netzversorgung von der vorherigen Aufzeichnung.
- **Eingang max. (V)** Die maximale Eingangsspannung der Netzversorgung von der vorherigen Aufzeichnung.
- **Eingang (Hz)** Die aktuelle Frequenz des Netzes, der an die USV geliefert wird.
- **Ausgang (V)** Die Ausgangsspannung der USV, der Strom an die angeschlossenen Geräte liefert.
- **Ausgang (Hz)** Die Ausgangsfrequenz der USV, der Strom an die angeschlossenen Geräte liefert.
- **Last (%)** Der Prozentsatz der gesamten USV-Last, die Strom an die angeschlossenen Geräte liefert.
- **Kapazität (%)** Der Prozentsatz der aktuellen USV-Batteriekapazität.
- **Verbleibende Laufzeit** Wie lange die USV ihre Last im Batteriemodus mit Strom versorgen kann.
- **Temperatur (°C oder °F)** Die aktuelle Temperatur der Umgebung.
- **Feuchtigkeit (% relative Luftfeuchte)** Die aktuelle Feuchtigkeit der Umgebung.

Auf der Seite [Log Daten -> Aufzeichnungen Energiewerte] Energieaufzeichnungen wird eine Liste der Energieaufzeichnungen mit einem Datums- und Zeitstempel angezeigt.

Artikel	Definition
Energie	Vom Gerät während eines bestimmten Zeitraums verbrauchte Energie, gemessen in kWh.
Kosten	Kosten für die vom Gerät während eines bestimmten Zeitraums verbrauchte Energie.
CO2	CO2-Emissionen des Geräts während eines bestimmten Zeitraums.
Kumulierte Energie	Kumulierter Energieverbrauch des Geräts seit dem letzten Zurücksetzen, gemessen in kWh.
Kumulierte Kosten	Kumulative Kosten der vom Gerät verbrauchten Energie seit dem letzten Zurücksetzen.
Kumuliertes CO2	Kumulative CO2-Emissionen des Geräts seit dem letzten Zurücksetzen.

[Log Daten ->Grafisch darstellen] Diese Seite dient zur Anzeige der Daten des Status Records. Die Diagrammfunktion erleichtert die Anzeige der Statusaufzeichnungen.

Artikel	Definition
Grafikzeitraum	Die Dauer zur Darstellung der Grafik ab dem heutigen Tag rückwärts. Je länger die Dauer, desto mehr Zeit wird zur grafischen Darstellung benötigt.
Grafikdaten	Die zur Darstellung der Grafik verwendeten Daten. Je mehr Daten, desto mehr Zeit wird zur grafischen Darstellung benötigt.
Graph Knoten	Durch Auswahl von Knoten im Detail anzeigen werden alle Punkte entlang der Linie ab diesem Punkt angezeigt. Wird der Cursor an den Punkt bewegt, werden die Informationen angezeigt Falls das Kästchen nicht ausgewählt ist, zeigt die Grafik nur die Linie, es wird jedoch weniger Zeit zur grafischen Darstellung benötigt.
Grafik in neuem Fenster zeigen	Durch Anklicken des Kästchens öffnet sich eine neue Seite, die die Grafik im Detail anzeigt.

[Log Daten ->Wartung] Auf dieser Seite werden die Einstellungen für "Ereignisprotokolle" und "Statusaufzeichnungen" ausgewählt. Die Anwendung liefert Informationen darüber, wie viele Ereignisse aufgezeichnet werden, bevor sie voll sind.

Artikel	Definition
Ereignisprotokoll	
Alle Protokolle löschen	Löschen Sie die bestehenden Ereignisprotokolle.
Anzahl Ereignisse	Die Anzahl bestehender Ereignisprotokolle / die max. Anzahl Ereignisprotokolle.
Ereignisprotokoll speichern	Speichern Sie die bestehenden Ereignisprotokolle als txt Datei.
Statusmeldungen	
Intervall Aufzeichnungen	Legen Sie die Frequenz zur Aufzeichnung der Statusdaten fest. Ein kleineres Intervall sorgt für häufigere Aufzeichnungen, die jedoch kürzere Zeit aufbewahrt werden. Ein größeres Intervall sorgt für seltenere Aufzeichnungen, die jedoch längere Zeit aufbewahrt werden.
Alle Aufzeichnungen löschen	Löschen Sie die bestehenden Statusaufzeichnungen.
Restzeit	Die verbleibende Aufzeichnungsdauer basierend auf dem Aufzeichnungsintervall. Ein kleineres Aufzeichnungsintervall führt zu einer geringeren Restzeit, ein größeres Aufzeichnungsintervall zu einer längeren Restzeit. Sobald die maximale Anzahl erreicht ist, überschreiben neue Statussätze die ältesten Statussätze im Speicher.
Statusaufzeichnungen speichern	Speichern Sie die Statusaufzeichnungen als TXT-Datei.

Aufzeichnungen Energiewerte	
Intervall Aufzeichnungen	Die Häufigkeit der Aufzeichnung der Energiedaten.
Alle Aufzeichnungen löschen	Löschen Sie die vorhandenen Energieaufzeichnungen
Stromtarifkosten	Das Verhältnis von Energiekosten zu Energie.
CO2-Emissionen	Das Verhältnis von CO2-Emissionen zu Energie.
Energieaufzeichnungen speichern	Speichern Sie die vorhandenen Ereignisprotokolle als Textdatei.

Hinweis: Ereignisprotokolle und Statusaufzeichnungen verwenden einen First-In-First-Out-Speicher. Einige alte Ereignisprotokolle/Statusaufzeichnungen werden automatisch gelöscht, wenn es keinen Platz zur Aufzeichnung gibt.

[Log Daten ->Syslog] Benutzer können Syslog-Server einstellen und Testnachrichten senden.

Artikel	Definition
Syslog Server	
Server-IP	Die IP-Adresse des Syslog-Servers.
Server-Port	Der UDP-Port des Syslog Servers.
Syslog Einstellung	
Syslog	Aktivieren das Ereignisprotokolle and den Syslog Server gesendet werden.
Code der Einrichtung	Werks Code
Syslog Test	
Priorisierung	Wählen Sie die Syslog Gewichtung der Meldung.
Syslog Nachricht	Geben Sie die Nachricht an, die an den Syslog Server gesendet wird.

[System->Allgemein->Zeit] Zeigt das Systemdatum und die Systemzeit an und ermöglicht es dem Benutzer, sie manuell oder über den NTP-Server (Network Time Protocol) einzustellen.

Artikel	Definition
Aktuelle Einstellungen	Zeigt das aktuelle Datum und die Uhrzeit auf der Karte sowie die Zeit bis zur nächsten Aktualisierung des Network Time Protocol (NTP) an. Das Datum und die Uhrzeit können entweder manuell oder über den NTP-Server (Network Time Protocol) eingestellt werden.
Konfiguration der Systemzeit	
Zeitzone	Wählen Sie die Zeitzone der Remote Management Card in GMT (Greenwich Mean Time).
NTP-Server verwenden	Geben Sie die IP-Adresse/den Domainnamen der NTP Server ein, wählen Sie die Zeitzone und stellen Sie die Frequenz zur Aktualisierung von Datum und Uhrzeit vom NTP Server ein. Wählen Sie zur sofortigen Aktualisierung Jetzt aktualisieren .
Manuelle	Geben Sie Datum und Zeit im benannten Format ein.

Einrichtung	
-------------	--

[System->Allgemein->Identifizierung] Weisen Sie dem System einen Namen, einen Kontakt und einen Ort zu.

Artikel	Definition
Name	Der Name des Geräts.
Synchronisierung mit Hostnamen	Ermöglichen Sie, die Synchronisierung des Hostnamens mit dem Identifikationsnamen, sodass beide Felder automatisch denselben Wert enthalten. Hinweis: Wenn diese Funktion aktiviert ist, darf der Identifikationsname nur Zahlen (0-9), Buchstaben (a-z, A-Z) und Bindestriche enthalten. Außerdem sollte der Identifikationsname nicht mit einem Bindestrich beginnen.
Ort	Der Ort, an dem sich das Stromgerät befindet.
Kontakt	Die Person, die bezüglich dieses Gerätes kontaktiert werden soll.

[System->Allgemein->Sommerzeit] Stellen Sie die Uhr auf Sommerzeit um.

Artikel	Definition
Sommerzeitkonfiguration	
Deaktivieren	Sommerzeit deaktivieren.
Traditionelle US	Legen Sie die traditionellen US-Sommerzeiteinstellungen fest Start: 2:00, zweiter Sonntag im März. Ende: 2:00 Uhr, erster Sonntag im November.
Manuelle Sommerzeit	Manuelle Regeln zur Festlegung der Sommerzeit.

[System->Sicherheit->Management] Für die Anmeldeauthentifizierung und die Software-Authentifizierung einstellen.

Artikel	Definition
Anmeldung Authentifizierung	
Lokales Konto	Anmeldung bei der Remote Management Karte mit dem Benutzername und Passwort das im lokalen Konto festgelegt wurde.
RADIUS, Lokales Konto	Anmeldung bei der Remote Management Karte mit Benutzername und Passwort mit Authentifizierung über den RADIUS Server. Wenn der RADIUS Server nicht reagiert, werden der Benutzername und das Kennwort aus dem lokalen Konto verwendet.
Nur RADIUS	Anmeldung bei der Remote Management Karte mit Benutzername und Passwort zur Authentifizierung über den RADIUS Server.
LDAP, Lokales Konto	Anmeldung bei der Remote Management Karte mit Benutzername und Passwort mit Authentifizierung über den LDAP-Server. Wenn der LDAP-

	Server nicht reagiert, werden der Benutzername und das Kennwort aus dem lokalen Konto verwendet.
Nur LDAP	Anmeldung bei der Remote Management Karte mit Benutzername und Passwort zur Authentifizierung über den LDAP-Server.
Software-Authentifizierung	
Geheimes Kennwort	Die zur Kommunikation mit dem PowerPanel Business Remote verwendete Authentifizierungsphrase Hinweis: Weitere Informationen finden Sie in Anhang 4 .
Manager IP	Diese IP-Einstellungen dienen der Festlegung bestimmter IP Adressen. Nutzer, die sich als Administrator (Betrachter) anmelden, können auf die Remote-Management-Karte Webseiten zugreifen, falls es sich bei ihrer IP Adresse um eine der Administrator (Betrachter) Manager IPs handelt. Wenn Sie von einer anderen IP-Adresse aus auf die Fernverwaltungskarte zugreifen möchten, können Sie eine von ihnen auf 0.0.0.0 oder 255.255.255.255 festlegen. Hinweis: Ein Bereich von IP-Adressen kann durch Eingabe der Subnetzmaske zugelassen werden. Zum Beispiel 192.168.20.0/16 bedeutet, dass der Zugriff auf die IP-Adresse mit dem Subnetz 192.168.0.0 erlaubt werden kann.

[System->Sicherheit->Lokales Konto] Diese Seite dient zur Konfiguration des Anmeldekontos.

Informationen	Beschreibung
Administrator	Der Administrator kann auf alle Funktionen zugreifen, einschließlich der Aktivierung/Deaktivierung des Viewers Kontos.
Viewer	Der Viewer kann auf die Lesen Funktion zugreifen, jedoch keine Einstellungen steuern oder ändern.

Ändern Sie das Administratorkonto:

1. Geben Sie den aktuellen Benutzernamen ein.
2. Geben Sie das aktuelle Kennwort zur Authentifizierung ein.
3. Legen Sie die Manager IP fest (optional)
4. Geben Sie das neue Kennwort ein.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.
6. Klicken Sie auf Übernehmen

Hinweis: Die maximale Länge von Benutzername und Passwort des Administrators beträgt 63 Zeichen.

Viewer-Konto ändern:

1. Wählen Sie zum Aktivieren des Betrachter Kontos Zugriff erlauben.
2. Geben Sie den Benutzernamen ein.
3. Legen Sie die Manager IP fest (optional)
4. Geben Sie das neue Kennwort ein.
- 5 Geben Sie das Kennwort zur Bestätigung erneut ein.

6. Klicken Sie auf Übernehmen

Hinweis: Die maximale Länge von Benutzername und Passwort des Viewers beträgt 15 Zeichen.

[System->Sicherheit->RADIUS-Konfiguration] Nach der Einstellung des richtigen RADIUS-Servers kann sich die Remote Management Card mit dem auf dem RADIUS-Server eingestellten Benutzernamen und Kennwort anmelden.

Artikel	Definition
Server-IP	Die IP-Adresse/Domäne des RADIUS-Servers.
Gemeinsames Geheimnis	Die Sicherheitsphrase des RADIUS-Servers.
Server- Port	Der UDP-Port der von dem Radius Server verwendet wird.
Authentifizierungsart	Der Authentifizierungsprotokolltyp für RADIUS-Server. <ul style="list-style-type: none"> • Passwort-Authentifizierungsprotokoll (PAP) • Challenge-Handshake-Authentifizierungsprotokoll (CHAP)
Zeitüberschreitung	Die Wartezeit für die Anmeldung beim Radius-Server.
Einstellung testen	Verwendung von Benutzername und Kennwort zur Authentifizierung mit RADIUS Server und Speicherung der Einstellung, wenn die Authentifizierung erfolgreich war.
Test überspringen	Speichert die Informationen zum RADIUS Servers ohne Prüfung.

Hinweis: Informationen zur Konfiguration von Konten in RADIUS-Servern finden Sie in [Anhang 2](#).

[System->Sicherheit->LDAP-Konfiguration] Nach der Einstellung des richtigen LDAP-Servers kann die Remote Management Card den Benutzernamen und das Kennwort verwenden, die auf dem LDAP-Server für die Anmeldung festgelegt wurden.

Artikel	Definition
LDAP-Server	
LDAP-Server	Die IP-Adresse / der Domänenname des LDAP-Servers.
LDAP SSL	Kommunikation des LDAP-Server über LDAPS.
Port	Verwendete TCP Port des LDAP(S) Server.
Benutzerbasis DN	Der Basis-DN des LDAP-Servers.
Attribute Anmeldung	Login Werte des LDAP-Benutzereintrags (zum Beispiel: cn oder uid).
LDAP-Authentifizierung	
Authentifizierungsmodus	Gibt die Methode an, die für die Authentifizierung verwendet werden soll. <ul style="list-style-type: none"> • Anonym: Bind-Anfrage mit einfacher Authentifizierung mit einem Bind-DN der Länge Null und einem Passwort der Länge Null. • Akkreditierter Benutzer: Anfrage mit einfacher Authentifizierung mit Bind-DN und Bind-Passwort binden. • Nach Anmeldebenutzer: Anfrage mit einfacher Authentifizierung mit einem Benutzerbasis-DN und einem Anmeldekennwort verbinden.
LDAP-Autorisierung	
Autorisierungsmodus	Gibt die Methode an, die für die Autorisierung verwendet werden soll.

	<ul style="list-style-type: none"> Nach Benutzerattribut: Bestimmen Sie die Zugriffsstufe nach Benutzerattribut und Benutzerattributwert.
Artikel	Definition
Autorisierungsmodus	<ul style="list-style-type: none"> Nach Gruppe: Ermitteln Sie die Zugriffsebene nach Gruppen mit Quellen-UND-Informationen wie dem folgenden Gruppen-Basis-DN, Gruppenattribut und Gruppenattributwert.
LDAP-Servertyp	
Generic LDAP-Server	Wählen Sie den LDAP-Servertyp als OpenLDAP aus
Active Directory	Select LDAP server type as windows AD
AD Domain	AD Domain des Active Directory server.
LDAP-Test	
Einstellung testen	Verwendung von Benutzername und Kennwort zur Authentifizierung mit LDAP-Server und Speicherung der Einstellung, wenn die Authentifizierung erfolgreich war.
Test überspringen	Speichert die Informationen zum LDAP-Server ohne Prüfung.

Hinweis: Informationen zur Konfiguration von Konten auf LDAP- und Windows AD-Servern finden Sie in [Anhang 2](#).

[System->Sicherheit-> Überwachung Sitzungen] Einstellung für die Zeitüberschreitung für offene Sitzungen zur automatischen Abmeldung.

Artikel	Definition
Zeitüberschreitung	Die Dauer (in Minuten), nach der sich das System automatisch abmeldet.

[System->Netzwerkdienst ->TCP/IPv4] Anzeige der aktuellen TCP/IPv4-Einstellungen. DHCP- und DNS-Server-Einstellungen festlegen.

Artikel	Definition
Aktuelle Konfiguration	Zeigt die aktuellen TCP/IP Einstellungen: IP-Adresse, Subnetzmaske, Gateway, DNS-Server, aktiver Hostname und aktiver Domänenname.
DHCP verwenden	<p>Wählen Sie die Option und klicken Sie zum Beziehen der TCP/IP Einstellungen über DHCP auf <i>Übernehmen</i>.</p> <ul style="list-style-type: none"> DHCP aktivieren Wählen Sie die Option zum Beziehen von IP-Adresse, Subnetzmaske und Gateway über DHCP. DNS-Adresse per DHCP beziehen Wählen Sie die Option zum Beziehen des DNS per DHCP, wenn DHCP aktiviert ist.
Per Manuell	Geben Sie die TCP/IP Einstellungen direkt ein und klicken Sie auf <i>Übernehmen</i> .
Hostname	<p>Registrieren Sie den Hostname beim DNS-Server.</p> <ul style="list-style-type: none"> Hostname: Konfigurieren Sie einen Hostnamen. Synchronisierung mit Identifikationsname: Konfigurieren Sie einen Domännennamen.

	Hinweis: Wenn diese Funktion aktiviert ist, darf der Identifikationsname nur Zahlen (0-9), Buchstaben (a-z, A-Z) und Bindestriche enthalten. Außerdem sollte der Identifikationsname nicht mit einem Bindestrich beginnen.
--	---

[System->Netzwerkdienst ->TCP/IPv6] Anzeige und Konfiguration der aktuellen IPv6-Einstellungen.

Artikel	Definition
IPv6-Schnittstelle	Zeigt die aktuelle IPv6-Adresse.
IPv6-Gateway	Zeigt das aktuelle IPv6-Gateway.
IPv6-Konfiguration	
Zugriff	Stellen Sieden IPv6-Service entweder auf Aktivieren oder Deaktivieren.
Routersteuerung	Die IPv6 Adresse wird über die Methode (Stateless Address Auto Konfiguration, Stateless DHCPv6 oder Stateful DHCPv6) zugewiesen, die durch die Routereinstellung festgelegt wird.
Manuell	Die IPv6 Adresse wird durch manuelle Einstellung zugewiesen.
Manuelle IPv6-Adresse	Geben Sie die IPv6 Adresse direkt ein und klicken Sie auf Übernehmen, wenn das Manuell Kästchen ausgewählt ist.

[System->Netzwerkdienst ->SNMPv1-Service] Erlaubt Benutzern die Verwendung eines NMS und die Konfiguration der entsprechenden SNMPv1-Einstellungen.

Artikel	Definition
SNMPv1-Service	
Zugriff erlauben	Stellen Sie den SNMPv1 Service auf Aktivieren oder Deaktivieren ein.
SNMPv1 Zugriffskontrolle	
Gruppe	Der zum Zugreifen auf diese Community durch ein Network Management System (NMS) verwendete Name. Das Feld muss 1 bis 15 Zeichen enthalten.
IP/Hostname	Die IP-Adresse oder IP-Adressmaske ist per NMS zugänglich. Eine spezifische IP-Adresse erlaubt Zugriff nur durch den NMS mit der angegebenen IP-Adresse. 255 gilt als Maske und die Regel ist wie folgt: <ul style="list-style-type: none"> • 192.168.20.255: Zugriff nur durch ein NMS im 192.168.20 Segment. • 192.255.255.255: Zugriff nur durch ein NMS im 192. Segment. • 0.0.0.0 (die Standardeinstellung) oder 255.255.255.255: Zugriff durch jedes NMS in jedem Segment.
Zugriff styp	Die zulässige Aktion für das NMS über die Community und die IP-Adresse. <ul style="list-style-type: none"> • Nur lesen: GET-Befehl jederzeit erlaubt; SET-Befehl eingeschränkt. • Schreiben/Lesen: GET-Befehl jederzeit erlaubt; SET-Befehl jederzeit erlaubt, es sei denn, eine Benutzersitzung ist aktiv. • Verboten: Die Befehle GET und SET sind eingeschränkt.

[System->Netzwerkdienst->SNMPv3-Service] Erlaubt den Benutzern die Verwendung eines NMS und die Konfiguration der entsprechenden SNMPv3-Einstellungen.

Artikel	Definition
SNMPv3-Service	
Zugriff erlauben	Stellen Sie den SNMPv3 Dienst auf Aktivieren oder Deaktivieren ein.
SNMPv3 Zugriff Steuerung	
Benutzername	Der Name zur Identifizierung des SNMPv3 Benutzers. Das Feld muss 1 bis 31 Zeichen enthalten.
Authentifizierung Protokoll	Der Hash Typ für die Authentifizierung.
Authentifizierungskennwort	Das zum Generieren des für die Authentifizierung verwendeten Schlüssels genutzte Kennwort. Das Feld muss 16 bis 31 Zeichen enthalten.
Privatsphäre Protokoll	Der Typ für die Verschlüsselung und Entschlüsselung von Daten. Hinweis: Das Privatsphärenprotokoll kann nicht ausgewählt werden, falls kein Authentifizierungsprotokoll ausgewählt ist,
Datenschutzkennwort	Das zum Generieren des für die Verschlüsselung verwendeten Schlüssels genutzte Kennwort. Das Feld muss 16 bis 31 Zeichen enthalten.
IP/Hostname (IPv6 Unterstützung)	Die IP-Adresse oder IP-Adressmaske ist per NMS zugänglich. Eine spezifische IP-Adresse erlaubt Zugriff nur durch den NMS mit der angegebenen IP-Adresse.255 gilt als Maske und die Regel ist wie folgt: <ul style="list-style-type: none"> • 192.168.20.255: Zugriff nur durch ein NMS im 192.168.20 Segment. • 192.255.255.255: Zugriff nur durch ein NMS im 192. Segment. • 0.0.0.0 (die Standardeinstellung) oder 255.255.255.255: Zugriff durch jedes NMS auf jedem Segment.

[System->Netzwerkdienst ->Web] Wählen Sie Aktivieren, um den Zugriff auf den HTTP- oder HTTPS-Service zu erlauben und konfigurieren Sie den TCP/IP-Port für diese Service e.

Artikel	Definition
Zugriff	
Zugriff erlauben	<ul style="list-style-type: none"> • Zugriff auf HTTP oder HTTPS Dienst aktivieren. HTTPS unterstützt eine Verschlüsselungsalgorithmus Liste wie folgt: • AES (256/128 Bits) • Kamelie (256/128 Bits) • DES (168 Bits)
Http-Einstellungen	
Http-Port	Der TCP/IP-Port des Hypertext Transfer Protocol (HTTP) (standardmäßig 80)
Https-Port	Der TCP/IP-Port des Hypertext Transfer Protocol Secure (HTTPS) (standardmäßig 443)
Zertifikatstatus	<p>Gültiges Zertifikat (oder ungültiges Zertifikat): Klicken Sie hier, um detaillierte Informationen zum Zertifikat anzuzeigen.</p> <p>Zertifikat hochladen: Klicken Sie auf, um ein Zertifikat hochzuladen und das aktuelle zu ersetzen.</p> <p>Hinweis: Das hochgeladene Zertifikat muss sich im Standard PEM (Privacy</p>

	Enhanced Mail) Format befinden.
Chiffrier-Suiten	Stellen Sie die Cipher Suite entweder auf Aktivieren oder Deaktivieren ein.

System->Netzwerkdienst ->Konsole] Wählen Sie Aktivieren, um den Zugriff auf den Telnet- oder SSH-Service zu erlauben, und konfigurieren Sie den TCP/IP-Port, den Telnet oder SSH für die Kommunikation verwenden.

Artikel	Definition
Zugriff	
Zugriff erlauben	Aktivieren Sie den Zugriff zu Telnet oder SSH-Version 2, das die Übertragung von Benutzernamen, Passwörtern und Daten verschlüsselt.
Telnet-Port	Der TCP/IP-Port (standardmäßig 23), das Telnet für die Kommunikation verwendet.
SSH-Einstellungen	
SSH-Port	Der TCP/IP-Port (standardmäßig 22), den SSH für die Kommunikation verwendet.
Hostkey Status	Zeigt den Status des Hostkey-Fingerabdrucks an, um anzuzeigen, ob er gültig oder ungültig ist. <ul style="list-style-type: none"> Hostkey hochladen: Klicken Sie hier, um einen Hostkey hochzuladen und den aktuellen zu ersetzen. Hostkey exportieren: Klicken Sie hier, um einen aktuellen Hostschlüssel zu exportieren.

Hinweis: Um die Sicherheit zu erhöhen, können Benutzer die Porteinstellung auf einen beliebigen nicht verwendeten Port zwischen 5000 und 65535 ändern. Die Benutzer müssen dann den nicht standardmäßigen Port angeben, um Zugriff zu erhalten. Bei Telnet-Clients müssen Benutzer entweder ein Leerzeichen und die Portnummer oder einen Doppelpunkt und die Portnummer an die Befehlszeile anhängen, um auf die Steuerkonsole zuzugreifen.

[System->Netzwerkdienst ->FTP-] Ermöglicht es dem Benutzer, den FTP-Server Service zu aktivieren/deaktivieren und den TCP/IP-Port des FTP-Servers zu konfigurieren (standardmäßig 21).

Artikel	Definition
Zugriff erlauben	Aktivieren Sie den Zugriff auf den FTP-Server.
Service-Port	Der TCP/IP-Port des FTP-Servers (standardmäßig 21). Benutzer können die Porteinstellung auf einen beliebigen unbenutzten Port zwischen 5000 und 65535 ändern, um die Sicherheit zu erhöhen.

Hinweis: Der FTP-Server wird zur Aktualisierung der FW verwendet. Details zu den Verfahren entnehmen Sie bitte der Bedienungsanleitung. "Firmware-Upgrade".

[System->Netzwerkdienst ->Modbus TCP] Diese Seite zeigt den aktuellen Modbus TCP Kommunikationsstatus und die Konfiguration.

Artikel	Definition
Host-IP-Adresse	Modbus TCP Host-IP-Adresse
Verbindungsstatus	Modbus TCP Kommunikationsstatus

Zugriff erlauben	Einstellung Modbus TCP aktivieren oder nicht.
Zugriff auf IP-Adresse	Diese Einstellung bestimmt, welche IP-Adresse über Modbus TCP auf das Gerät zugreifen darf. Wenn Sie von einer beliebigen IP-Adresse aus auf das Gerät zugreifen möchten, können Sie den Wert 0.0.0.0 festlegen
Modbus TCP-Port	Richten Sie den Modbus TCP-Port ein (Standard: 502).

[System->Benachrichtigungen->Ereignisaktion] Ereignisaktionen für jedes Ereignis anzeigen. Klicken Sie auf ein Ereignis zur Änderung seiner Aktion. Wenn das spezifische Ereignis auftritt, kann der Benutzer durch die entsprechende Methode gemäß dieser Liste benachrichtigt werden.

- **Protokoll:** Ereignis unter "Ereignisprotokolle" aufzeichnen.
- **E-Mail:** Eine E-Mail wird an einen spezifischen Benutzer gesendet. (Ein verfügbarer SMTP-Server ist erforderlich.)
- **Trap:** Eine SNMP-Trap wird an eine spezifische IP-Adresse gesendet.
- **Syslog:** Gesendete Syslog-Nachricht an einen bestimmten Syslog-Server gesendet. (Ein verfügbarer Syslog-Server ist erforderlich). SMS: Eine Kurzmitteilung an eine spezifische Mobilfunknummer senden. (Ein verfügbarer SMS-Serviceanbieter ist erforderlich.)
- **Verzögerung:** Das Ereignis wird ausgeführt, wenn der Zustand mindestens für x Sekunden besteht.

Hinweis Die Einstellung Verzögerung ist derzeit nur für das Ereignis Stromausfall verfügbar.

[System->Benachrichtigungen->SMTP-Server] Nach der Einstellung des richtigen SMTP-Servers können E-Mail-Benachrichtigungen bei bestimmten Ereignissen an die Empfänger gesendet werden.

Artikel	Definition
Adresse des SMTP-Servers	Die IP-Adresse oder der Hostname des SMTP-Servers, der für den Versand von E-Mail-Benachrichtigungen verwendet wird.
Absender-E-Mail	E-Mail-Adresse, die für den Versand der E-Mail-Benachrichtigung verwendet wird.
Absender Name	Konfigurieren Sie die Absender Informationen für die E-Mail.
Authentifizierung	Wählen Sie diese Option, falls der SMTP-Server eine Authentifizierungsprüfung benötigt.
Benutzername	Für die Authentifizierung verwendetes Konto mit einer maximalen Länge von 63 Zeichen.
Passwort	Für die Authentifizierung verwendetes Kennwort mit einer maximalen Länge von 63 Zeichen. Bei öffentlichen SMTP-Servern wie Gmail und Office 365 geben Sie bitte das App-Passwort ein, das vom SMTP-Server für die Authentifizierung bereitgestellt wird.
Sichere Verbindung	TLS oder SSL zur Verschlüsselung der SMTP-Verbindung aktivieren.
Service -Port	Die Portnummer, die für die Kommunikation mit dem SMTP-Server verwendet wird.

[System->Benachrichtigungen->E-Mail-Empfänger] Legt bis zu fünf E-Mail-Empfänger im zugewiesenen E-Mail-Adressformat fest. Die Empfänger erhalten eine E-Mail-Benachrichtigung, wenn Ereignisse auftreten. Klicken Sie zum Hinzufügen eines neuen Empfängers auf Neuer Empfänger. Zum Ändern oder Löschen eines vorhandenen Empfängers klicken Sie auf die E-Mail-Adresse dieses Empfängers. Sie können prüfen, ob die

SMTP-Einstellungen (System > Benachrichtigungen > SMTP Server) und die E-Mail Empfänger richtig eingerichtet sind, indem Sie den Empfangsstatus durch Anklicken von TEST prüfen.

[System->Benachrichtigungen->Trap-Empfänger] Richten Sie bis zu 10 SNMP-TRAP-Empfänger nach IP-Adresse ein (IPv6 wird unterstützt). SNMPv1 und v3 werden unterstützt. Die aufgelisteten TRAP-Empfänger werden benachrichtigt, wenn Geräteereignisse auftreten.

Klicken Sie zum Hinzufügen eines neuen Empfängers auf Neuer Empfänger. Zum Ändern oder Löschen eines vorhandenen Empfängers klicken Sie auf die IP-Adresse oder den Namen des entsprechenden Empfängers. Prüfen Sie, ob die Traps richtig empfangen werden können, indem Sie auf TEST klicken.

[System->Benachrichtigungen->SMS-Service] Short Message Service (SMS) ist ein Kommunikation Service , der von mobilen Kommunikationssystemen verwendet wird. Die Verwendung standardisierter Kommunikationsprotokolle ermöglicht den Austausch von kurzen Textnachrichten zwischen mobilen Geräten. Das System bietet 4 Methoden, aus denen der Benutzer wählen kann, wie er die Nachrichten versenden möchte.

Artikel	Beschreibung
Service Anbieter ist Clickatell	<p>Wählen Sie im Feld SMS-Methode die Option Clickatell. Füllen Sie alle Kontodetails aus, einschließlich der Felder Benutzername, Passwort und HTTP-API-ID.</p> <p>Zum Beispiel:</p> <p>Clickatell (Konto vor 2016/11)</p> <p>Name des Benutzers Name</p> <p>Passwort Passwd</p> <p>HTTP API ID 3234599</p> <p>Clickatell (Konto nach 2016/11)</p> <p>HTTP API ID 3234599</p>

Artikel	Beschreibung
Der Service Anbieter akzeptiert HTTP GET	<p>Diese Angabe des SMS-Anbieters ist erforderlich, bevor Sie die HTTP-GET-Methode verwenden können. Wählen Sie im Feld SMS-Methode die Option HTTP GET verwenden. Geben Sie die E_PHONE_NUMBER als Handynummer des Empfängers und die E_PHONE_MESSAGE als Ereignismeldung ein, die in der Spezifikation des SMS-Providers beschrieben sind, und füllen Sie das URL-Feld aus. Die Ausdrücke werden durch entsprechende Inhalte ersetzt, bevor die Nachricht vom SMS-Anbieter versendet wird.</p> <p>Zum Beispiel:</p> <p>URL http://ServiceProviderURL?user=Name&password=Passwd&api_id=3234599&to=E_PHONE_NUMBER&text=E_MESSAGE</p>
Der Service Anbieter akzeptiert HTTP POST	<p>Diese Angabe des SMS-Anbieters ist erforderlich, bevor Sie die HTTP POST-Methode für die Zustellung von Nachrichten über SMS-Anbieter verwenden. Wählen Sie im Feld SMS-Methode die Option HTTP POST verwenden. Geben Sie E_PHONE_NUMBER als Mobiltelefonnummer des Empfängers und</p>

	<p>E_PHONE_MESSAGE als Ereignismeldung ein, die durch die Spezifikation des SMS-Providers beschrieben wird, und füllen Sie die Felder POST URL und POST BODY aus. Die Ausdrücke werden durch den entsprechenden Inhalt ersetzt, bevor die Nachricht vom SMS-Provider versendet wird.</p> <p>Zum Beispiel: URL http://ServiceProviderURL Inhalt user=Name&password=Passwd&api_id=3234599&to=E_PHONE_NUMBER&text=E_MESSAGE</p>
Service Anbieter akzeptiert E-Mail (SMTP)	<p>Diese Angabe eines SMS-Providers ist erforderlich, bevor Sie die E-Mail für die Zustellung der Nachrichten über SMS-Provider verwenden können. Wählen Sie im Feld Service anbieter die Option E-Mail verwenden. Geben Sie E_PHONE_NUMBER als Handynummer des Empfängers und E_PHONE_MESSAGE als Ereignismeldung ein, wie in der Spezifikation des SMS-Providers beschrieben. Geben Sie die Adresse des Empfängers, den Betreff und den Inhalt ein. Die Ausdrücke werden durch den entsprechenden Inhalt ersetzt, bevor die Nachricht vom SMS-Provider versendet wird.</p> <p>Zum Beispiel: Adresse sample@cyberpower.com Thema TestSubjekt Inhalt E_PHONE_NUMBER&text=E_MESSAGE</p>

[System->Benachrichtigungen->SMS-Empfänger] Benutzer können bis zu 10 Mobiltelefonnummern als SMS-Empfänger festlegen. Die Empfänger erhalten eine Kurzmitteilung, wenn konfigurierte Ereignisse auftreten.

Um einen neuen Empfänger hinzuzufügen, klicken Sie auf "Neuer Empfänger". Um einen bestehenden Empfänger zu ändern oder zu löschen, klicken Sie auf die Handynummer oder den Namen des Empfängers. Um die SMS-Einstellungen zu testen, klicken Sie auf die Schaltfläche "TEST" und sehen Sie, ob die Testnachricht korrekt empfangen wird.

[System->Reset/Reboot] Zurücksetzen oder Neustarten des RMCARD-Systems.

Artikel	Definition
System neu starten	Starten Sie das System neu, ohne die USV auszuschalten und neu zu starten.
System zurücksetzen	Stellen Sie das System auf die Werkseinstellung zurück. Das System wird neu gestartet. Diese Aktion schaltet die USV nicht aus oder startet sie neu.
System zurücksetzen (TCP/IP-Einstellungen beibehalten)	Stellen Sie das System auf die Werkseinstellungen zurück, behalten Sie jedoch TCP/IP vor. Das System wird neu gestartet Diese Aktion schaltet die USV nicht aus oder startet sie neu.

[System->Über] Zeigt Systeminformationen für die Remote Management Card an.

Artikel	Definition
Name des Modells	Modellname der Remote Management Card.
Hardware-Version	Die Hardware-Version der Remote Management Card.

Firmware-Version	Die aktuelle Firmware-Version, die auf der Remote Management Card installiert ist.
Firmware Aktualisierungsdatum	Das letzte Datum, an dem die Firmware aktualisiert wurde.
Seriennummer	Seriennummer der Remote Management Card.
MAC-Adresse	MAC-Adresse der Remote Management Card. HINWEIS: Die MAC Adresse wird auch an der Oberseite des Produktes angegeben.
System-Firmware-Update	Verwenden Sie diese Funktion, um die Firmware und Daten hochzuladen. Klicken Sie auf Durchsuchen, um zum Speicherort der Datei zu gelangen, und klicken Sie auf Senden.
Konfiguration speichern	Zum Speichern der Konfiguration auf dem lokalen PC Speichern anklicken. Die Textdatei erhält einen Standardnamen im Format JJJ_MM_TT_HHMM.txt.
Konfiguration wiederherstellen	Nutzen Sie diese Funktion zum Wiederherstellen einer zuvor gespeicherten Konfiguration. Klicken Sie zur Suche nach der gespeicherten Konfigurationsdatei auf Durchsuchen und klicken Sie auf Übernehmen. Hinweis: Die gespeicherte Konfigurationsdatei enthält Sicherheitsinformationen wie Benutzername und Kennwort. Nachdem Sie die Konfiguration wiederhergestellt haben, wird empfohlen, die Datei zu löschen, um vertrauliche Informationen sicher zu verwahren.
Diagnoseinformationen	Klicken Sie auf die Schaltfläche "Speichern", um alle Diagnoseinformationen in einer Datei zu speichern. Die gespeicherten Informationen umfassen Ereignisprotokolle, Statusaufzeichnungen und andere Geräteinformationen. HINWEIS: Es wird empfohlen, diese Informationen zu speichern, wenn Sie sich an den technischen Support von CyberPower wenden, um Unterstützung zu erhalten

Befehlszeilenschnittstelle

Wie man sich anmeldet

Benutzer können sich an der Befehlszeilenschnittstelle entweder über einen Konsolennetzzugang (Telnet oder SSH) oder einen lokalen Zugriff (serieller Port) anmelden.

1. Netzwerkzugriff auf die Befehlszeilenschnittstelle

Wenn sich ein Benutzer mit dem Benutzernamen admin und dem Passwort admin über Telnet oder SSH anmeldet, stehen zwei Arten von Schnittstellen zur Verfügung. Eine ist die Befehlszeilenschnittstelle (CLI) und die zweite ist eine Menüschnittstelle. Die Standardeinstellung ist CLI. Wenn der Benutzer zur Menüschnittstelle wechseln möchte, gibt er den Befehl [Menu Mode] ein. Um zurück zur CLI zu wechseln, ist es notwendig, sich abzumelden und bei der RMCARD anzumelden.

So verwenden Sie die Befehlszeilenschnittstelle für den Telnet-Zugriff

Schritt 1: Stellen Sie sicher, dass der Computer Zugriff auf das installierte RMCARD-Netzwerk hat. Geben Sie an einer Eingabeaufforderung Telnet und die IP-Adresse für die RMCARD ein (z.B. Telnet 139.225.6.133, wenn die RMCARD den Standard-Telnet-Port 23 verwendet), und drücken Sie Enter.
Schritt 2: Geben Sie den Benutzernamen und das Passwort ein (Standard: Benutzername: cyber, Passwort: cyber)

So verwenden Sie die SSH-Zugriffs-Befehlszeilenschnittstelle

SSH wird für den Zugriff auf die Befehlszeilenschnittstelle dringend empfohlen. SSH verschlüsselt Benutzernamen, Kennwörter und übertragene Daten. Um SSH zu verwenden, müssen Sie zunächst SSH konfigurieren und ein SSH-Client-Programm (z. B. PuTTY, HyperTerminal oder Tera Term) auf Ihrem Computer installieren.

Hinweis: Wenn Sie PuTTY verwenden, um den SSH-Zugriff zu konfigurieren, konfigurieren Sie die Zeilendisziplin des Terminals bitte auf "Force off", wie in Abbildung 4 gezeigt.

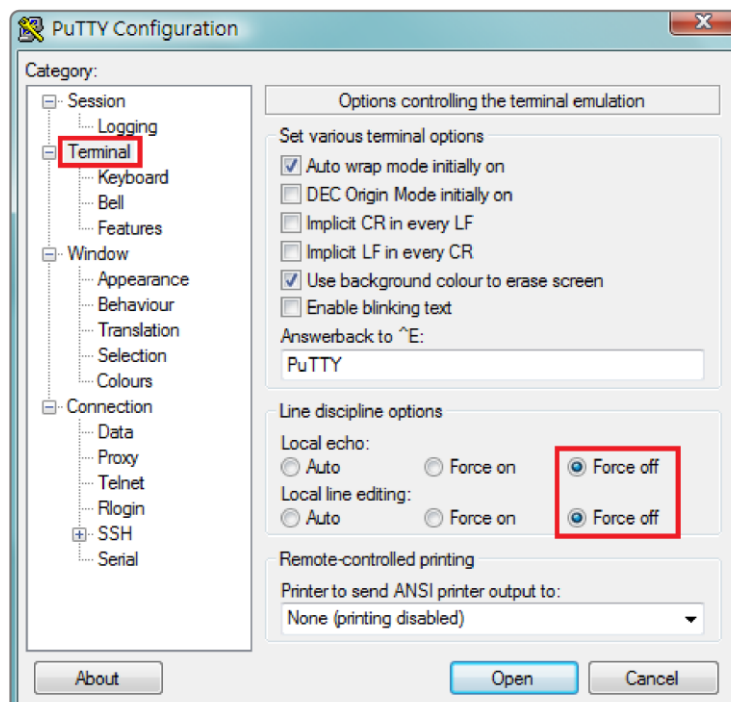


Abbildung 4. Das PuTTY-Konfigurationsfenster.

2. Lokaler Zugriff auf die Befehlszeilenschnittstelle

Um sich über eine serielle Verbindung anzumelden, muss der PC/Server über das mitgelieferte RJ45/DB9-Verbindungskabel für den seriellen Port direkt mit dem Universal-Port der RMCARD verbunden werden.

Schritt 1. Öffnen Sie die Software Hyper Terminal (z. B. PuTTY, HyperTerminal oder Tera Term) auf Ihrem PC und wählen Sie einen Namen und ein Symbol für die Verbindung.

Schritt 2. Richten Sie die COM-Port-Einstellungen mit den folgenden Werten ein

*Bits pro Sekunde: 9600

*Datenbits: 8

*Parität: Keine

*Stoppbits: 1

*Durchflusskontrolle: Keine

Schritt 3. Drücken Sie die Eingabetaste, um das Menü Authentifizierung aufzurufen.

Schritt 4. Geben Sie im Menü Authentifizierung den Benutzernamen und das Passwort der RMCARD ein.

Hinweis: Die serielle Verbindung kann nur auf den Befehlszeilenmodus zugreifen und unterstützt nicht den Menümodus.

Verwendung der Befehlszeilenschnittstelle

Bei Verwendung der Befehlszeilenschnittstelle können Sie auch Folgendes tun:

1. So schließen Sie die Verbindung zur Befehlszeilenschnittstelle → Geben Sie "**exit**" ein und drücken Sie die Eingabetaste
2. So wechseln Sie in den Menümodus → Geben Sie "**Menu Mode**" ein und drücken Sie die Eingabetaste
3. So zeigen Sie eine Liste der verfügbaren Befehle oder Argumente an → Geben Sie "?" ein (z. B. Datum ?).
4. So zeigen Sie den Befehl an, der zuletzt in der Sitzung → eingegeben wurde: Drücken Sie die Pfeiltaste AUF/AB. (Die Sitzung kann sich bis zu zehn vorherige Befehle merken).
5. Ein Befehl kann mehrere Optionen unterstützen → So definieren Sie das Datum als 21. März 2015 (z. B. Datum jjjj 2015 mm 3 tt 21)

Befehlsantwort-Codes

Wenn der Befehl oder die Argumente nicht erkannt werden oder falsch sind, zeigt die Konsolenschnittstelle [^] unterhalb des falschen Befehls oder Arguments an. Die folgende Fehlermeldung wird angezeigt:

Befehl nicht gefunden	RMCARD kennt diesen Befehl nicht. Die Konsolenschnittstelle zeigt die Liste der verfügbaren Befehle an.
Parameter Fehler	Der Typ oder das Format des Parameters ist nicht zulässig. Die Konsolenschnittstelle zeigt die Liste der verfügbaren Werte oder Formate an.

Befehlsbeschreibungen

USV

Beschreibung: Zeigen Sie die Informationen über USV, Eingang, Ausgang. Und verwenden Sie den Hauptschalter zur Steuerung der USV.

Option	Argument	Beschreibung
Infos	anzeigen	USV-Informationen anzeigen
Eingabe	anzeigen	Anzeige der USV-Eingangsinformationen
Ausgabe	anzeigen	Anzeige der USV-Ausgangsinformationen

Beispiel 1:

So zeigen Sie USV-Informationen an
 CyberPower > **USV info anzeigen**
 USV Informationen
 Modell: OL1000XL
 Nennspannung: 100V
 Arbeitsfrequenz: 40~70 Hz
 Nennleistung: 1000 VA
 Nennstrom: 10 Ampere
 Lastleistung: 900 Watt
 Batteriespannung: 36 V
 USB-Version: 0.1B
 Datum des nächsten Batteriewechsels: 10/08/2018
 NCL Bank: 1
 Erweiterter Akku-Pack: 4

USVctrl

Beschreibung: Aktivieren Sie die Verwendung von USV Master Switch.

Option	Argument	Beschreibung
Neustart	Ausschaltverzögerung / Neustartdauer (z.B. 10/10) Ausschaltverzögerung: 0 10 20 30 60 120 180 300 600 Dauer des Neustarts: 10 20 30 60 120 180 300 600	Schaltet die USV aus und wieder ein. Es gibt einen String mit Ausschaltverzögerung (in Sekunden) und Neustartdauer (in Sekunden), z.B.: 10/10 bedeutet Ausschaltverzögerung in 10 Sekunden und Neustartdauer in 10 Sekunden.
auf		Schaltet die USV ein.
aus	0 10 20 30 60 120 180 300 600	Schaltet die USV aus. Das Argument bedeutet Ausschaltverzögerung in Sekunden.

Option	Argument	Beschreibung
schlafen	0 10 20 30 60 120 180 300 600	Dieser Befehl ist im Utility Power Failure Mode verfügbar. Er kann die USV bis zur Wiederherstellung der Stromversorgung in den Ruhezustand versetzen. Das Argument bedeutet Sleep Delay in Sekunden.

Beispiel 1:

Zum Neustart der USV schalten Sie die Ausschaltverzögerung auf 10 Sekunden und die Neustartdauer auf 20 Sekunden.

CyberPower > **USVctrl-Neustart 10/20**

USVcfg

Beschreibung: Anzeigen und Konfigurieren der USV-Versorgungsleistung, der USV-Empfindlichkeit, des USV-Hochspannungsschwellenwerts, des USV-Niederspannungsschwellenwerts, des USV-Bypass-Zustands, des USV-Bypass-Hochschwellenwerts, des USV-Bypass-Niederschwellenwerts, der USV-Aufladeverzögerung, der USV-Aufladekapazität, des USV-Arbeitsmodus und der USV-Rückkehrverzögerung.

Option	Argument	Beschreibung
anzeigen		
outpwr	<Ausgangsleistung in VAC>	Stellt die Ausgangsspannung ein, die an die angeschlossenen Geräte geliefert wird.
sen	hoch mittel niedrig	Die niedrige Empfindlichkeit hat einen geringeren Spannungsbereich und die eingespeiste Leistung kann stärker schwanken. Die Stromversorgung durch den Kraftstoffgenerator kann dazu führen, dass die USV häufiger in den Batteriemodus wechselt, und es wird eine niedrige Empfindlichkeit empfohlen. Die USV schaltet seltener in den Batteriebetrieb und spart außerdem mehr Batteriestrom. Durch die hohe Empfindlichkeit kann die USV die Geräte stabiler mit Strom versorgen und häufig in den Batteriebetrieb wechseln.
hvlimit	<hoher Schwellenwert in VAC>	Wenn die Netzspannung (oder Ausgangsspannung) den Schwellenwert überschreitet, versorgt die USV die angeschlossenen Geräte mit Batteriestrom.
lvlimit	<untere Schwelle in VAC>	Wenn die Netzspannung (oder Ausgangsspannung) den Schwellenwert überschreitet, versorgt die USV die angeschlossenen Geräte mit Batteriestrom.

Option	Argument	Beschreibung
--------	----------	--------------

bypasscond	nobypass freqvolt voltonly	Kein Bypass - Wenn diese Option ausgewählt ist, geht die USV nicht in den Bypass-Modus über und stellt die Ausgangsleistung ein. Spannung/Frequenz prüfen - Wenn die Netzspannung im Bereich der <i>hohen/niedrigen Bypass-Spannung</i> und die Netzfrequenz im Bereich der <i>Frequenztoleranz liegt</i> , geht die USV in den Bypass-Modus über. Andernfalls stellt die USV die Ausgangsleistung ein. Nur Volt prüfen - Nur wenn die Versorgungsspannung im Bereich der <i>hohen/niedrigen Bypass-Spannung</i> liegt, geht die USV in den Bypass-Modus über. Andernfalls stellt die USV die Ausgangsstromversorgung ein.
bypassvlimit	10 15	Stellen Sie die hohe Bypass-Spannung in Prozent ein. Wenn die Netzspannung die Schwellenwerte überschreitet, darf die USV nicht in den Bypass-Modus wechseln.
bypassvlimit	10 15 20	Stellen Sie die niedrige Bypass-Spannung in Prozent ein. Wenn die Netzspannung die Schwellenwerte überschreitet, darf die USV nicht in den Bypass-Modus wechseln.
wiederaufgeladenVerzögerung	0 60 120 180 300 600 1200 1800 3600	Stellen Sie die Wiederaufladeverzögerung in Sekunden ein. Wenn die Stromversorgung wiederhergestellt wird, beginnt die USV mit dem Aufladen, bis die angegebene Verzögerung abgelaufen ist, bevor die Ausgangsleistung wiederhergestellt wird.
rechargecap	0 15 30 45 60 75 90	Stellen Sie die Auflade Kapazität in Prozent ein. Wenn die Stromversorgung wiederhergestellt wird, beginnt die USV mit dem Aufladen, bis die angegebene Batteriekapazität erreicht ist, bevor die Ausgangsleistung wiederhergestellt wird.

Option	Argument	Beschreibung
--------	----------	--------------

Arbeitsmodus	normal eco10% eco15% generator bypass	<p>normal - Normaler Betriebsmodus der USV.</p> <p>eco10% - Die Online-USV wechselt in den Economy-10%-Modus.</p> <p>eco15% - Die Online-USV wechselt in den Modus Economy 15%.</p> <p>Generator - Wenn die USV einen Generator als Eingangsspannung verwendet, sollte diese Option den normalen Betrieb der USV ermöglichen. Wenn diese Option ausgewählt ist, ist es der USV untersagt, in den Bypass-Modus zu wechseln, um die gespeisten Geräte zu schützen.</p> <p>bypass - Legt fest, ob die USV in den manuellen Bypass-Modus wechseln darf. Wenn diese Option aktiviert ist, wird die USV gezwungen, in den Bypass-Modus zu wechseln.</p>
Rückgabeverzögerung	0 ~ 600	Wenn die Stromversorgung wiederhergestellt ist, beginnt die USV mit dem Wiederaufladen, bis die angegebene Verzögerung abgelaufen ist, bevor die Ausgangsleistung wiederhergestellt wird. Die Zahlen im Bereich von 1 bis 600 Sekunden sind durch 5 teilbare Zahlen.

Beispiel 1:

Um den verfügbaren Spannungswert anzuzeigen, kann die USV-Ausgangsleistung eingestellt werden.

CyberPower > **USVcfg Versorgung?**

100

110

115

Beispiel 2:

So definieren Sie die Bypass-Bedingung nur als Prüfung der Versorgungsspannung

CyberPower > **USVcfg bypasscond voltonly**

Beispiel 3:

So definieren Sie die USV-Aufladeverzögerung als 2 Minuten

CyberPower > **USVcfg rechargedelay 120**

Beispiel 4:

So stellen Sie den Online-USV-Modus auf den Generatormodus ein

CyberPower > **USVcfg Modus Generator**

USVbatt

Beschreibung: Zeigt Informationen über die Batterie an und führt den Batterietest und die Kalibrierung der Batterielaufzeit durch.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Batterieinformationen für diese USV
Test		Führen Sie den Batterietest sofort durch.
cal	Start Stopp	Starten oder beenden Sie die Laufzeitkalibrierung.
rdyyyy	<Nummer des Jahres>	Legen Sie das Jahr des Batterieaustauschdatums durch AD fest.
rdmm	<Nummer des Monats>	Legen Sie den Monat des Batteriewechseldatums fest.
rddd	<Nummer des Datums>	Tag des Monats einstellen.

Beispiel 1:

Zur Durchführung des Selbsttests der Batterie.

CyberPower > **USVbatt test**

Beispiel 2:

So starten Sie die Kalibrierung der Akkulaufzeit

CyberPower > **USVbatt cal start**

Beispiel 3:

Das Datum für den Batteriewechsel auf den 29. Mai 2018 festzulegen.

CyberPower > **USVbatt rdyyyy 2018 rdmm 5 rddd 29**

atsoltsta

Beschreibung: Zeigt Informationen zum Status der ATS-Steckdose an.

Option	Argument	Beschreibung
anzeigen		Informationen zu ATS Outlet Status anzeigen
Index	<1 2 ... Nummer der Steckdose alle>	ATS-Ausgangsindex auswählen

Beispiel 1:

So zeigen Sie den Status aller Steckdosen an

CyberPower > **atsoltsta index alle anzeigen**

atsoltcfg

Beschreibung: Anzeigen und Konfigurieren von Informationen über den ATS-Ausgang.

Option	Argument	Beschreibung
anzeigen		Informationen über die ATS-Ausgangskonfiguration anzeigen
Index	<1 2 ... Nummer der Steckdose alle>	ATS-Ausgangsindex auswählen
Name	<Ausgangsname>	ATS-Ausgangsname festlegen
td_an	<-1 0 1 2 ... 7200 >	ATS-Einschaltverzögerung einstellen
td_aus	<-1 0 1 2 ... 7200 >	ATS-Ausschaltverzögerung einstellen

td_reboot	<5 6 ... 60>	Dauer des Neustarts der ATS-Steckdose festlegen
einstellen.	<1 2 ... Nummer der Steckdose alle> <Ausgangsname> <-1 0 1 2 ... 7200 > <-1 0 1 2 ... 7200 > <5 6 ... 60>	Ändern der ATS-Ausgangsconfiguration

Beispiel 1:

So zeigen Sie die gesamte Ausgangskonfiguration an
CyberPower > **atsoltcfg index all show**

Beispiel 2:

Benennen der Steckdose Nr. 1 als test_1
CyberPower > **atsoltcfg index 1 name test_1**

Beispiel 3:

Einschaltverzögerung der Steckdose Nr. 2 auf 3 Sekunden einstellen
CyberPower > **atsoltcfg index 2 td_on 3**

Beispiel 4:

So stellen Sie die Ausschaltverzögerung der Steckdose Nr. 3 auf 3 Sekunden ein
CyberPower > **atsoltcfg index 3 td_off 3**

Beispiel 5:

So stellen Sie die Ausschaltverzögerung der Steckdose Nr. 4 auf "nie ausschalten" ein
CyberPower > **atsoltcfg index 4 td_off -1**

Beispiel 6:

So legen Sie die Dauer des Neustarts von Ausgang Nr. 5 auf 5 Sekunden fest
CyberPower > **atsoltcfg index 5 td_reboot 5**

Beispiel 7:

So benennen Sie den Ausgang Nr. 1 als test_1, setzen die Einschaltverzögerung auf 3 Sekunden, die Ausschaltverzögerung auf 4 Sekunden und die Neustartdauer auf 5 Sekunden mit einem einzigen Befehl
CyberPower > **atsoltcfg set 1 test_1 3 4 5**

atsoltctrl

Beschreibung: Konfigurieren Sie den Status der ATS-Steckdose.

Option	Argument	Beschreibung
Index	<1 2 ... Ausgangsnummer alle>	ATS-Ausgangsindex auswählen
handeln	<Ein Aus Neustart td_on td_off td_reboot>	Steuerung ATS-Ausgang

Beispiel 1:

So schalten Sie die Steckdose Nr. 1 sofort ein
 CyberPower > **atsoltctrl index 1 act on**

Beispiel 2:

Einschalten der Steckdose Nr. 2 mit Einschaltverzögerung
 CyberPower > **atsoltctrl index 2 act td_on**

atssrccfg

Beschreibung: Anzeigen und Konfigurieren der bevorzugten ATS-Quelle.

Option	Argument	Beschreibung
anzeigen		Informationen von ATS Prefer Source anzeigen
lieber	<a b keine >	ATS-Quelle bevorzugen einstellen

Beispiel 1:

So zeigen Sie Informationen zu ATS Prefer Source an
 CyberPower > **atssrccfg show**

Beispiel 2:

So legen Sie die von ATS bevorzugte Quelle als Quelle A fest
 CyberPower > **atssrccfg vorziehen a**

Datum

Beschreibung: Anzeige und Konfiguration von Zeitzone, Datumsformat, Datum und Uhrzeit.

Option	Argument	Beschreibung
anzeigen		Anzeige des Systemdatums für RMCARD
Zeitzone	<Zeitzone-Offset>	Wählen Sie die RMCARD-Zeitzone in GMT (Greenwich Mean Time).
Format	mm/dd/yyyy yyyy/mm/dd dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	Datumsformat des Systems einstellen
jjjj	<Nummer des Jahres>	Jahr des Systemdatums nach AD einstellen.
Option	Argument	Beschreibung
mm	<Nummer des Monats>	Monat des Systemdatums einstellen.
dd	<Nummer des Datums>	Tag des Monats einstellen.
Zeit	<00:00:00>	Systemzeit einstellen.

Beispiel 1:

So definieren Sie die Zeitverschiebung als +08:00
 CyberPower > **Datum Zeitzone +0800**

Beispiel 2:

Den 21. März 2015 als Datum festlegen
 CyberPower > **Datum jjjj 2015 mm 3 tt 21**

Beispiel 3:

Die Zeit als 13:45:12 zu definieren

CyberPower > **Datum Uhrzeit 13:45:12**

ntp

Beschreibung: Anzeige und Konfiguration der NTP-Server-IP, NTP-Aktualisierungsintervallzeit.

Option	Argument	Beschreibung
anzeigen		Anzeige aller NTP-Informationen für RMCARD
Zugriff	aktivieren deaktivieren	Wenn diese Option aktiviert ist, stellt das System Datum und Uhrzeit vom NTP-Server ein.
Priip	<primärer ntp-Server ip>	Legen Sie die IP-Adresse/Domänennamen der primären NTP-Server fest.
secip	<sekundärer ntp-Server ip>	Legen Sie die IP-Adresse/Domänennamen der sekundären NTP-Server fest.
Update	jetzt 1-8760	now - Wählen Sie <i>Update right now</i> , um sofort zu aktualisieren. 1-8760 - Legt die Häufigkeit der Aktualisierung von Datum und Uhrzeit vom NTP-Server fest.

Beispiel 1:

Um den NTP-Server zu aktivieren, definieren Sie Datum und Uhrzeit der RMCARD

CyberPower > **ntp-Zugriff aktivieren**

Beispiel 2:

So richten Sie die IP des primären NTP-Servers als "192.168.26.22" ein

CyberPower > **ntp priip 192.168.26.22**

Beispiel 3:

Um die Zeit per NTP sofort zu aktualisieren

CyberPower > **ntp jetzt aktualisieren**

sys

Beschreibung: Anzeigen und Konfigurieren der Identifikation der RMCARD, Zurücksetzen der RMCARD.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Systeminformationen für RMCARD
Name	<Systemname>	Legen Sie den Namen des Geräts fest.
Ort	<SystemOrt >	Legen Sie den Ort der Stromversorgungsgeräte fest.
Kontakt	<Systemkontakt>	Legen Sie die Kontaktperson für dieses Gerät fest.

zurücksetzen	reboot notcpip all	<p>Neustart-Reboot RMCARD</p> <p>notcpip - Setzt das System auf die Standardeinstellungen zurück, behält aber die TCP/IP-Einstellungen bei und startet es neu.</p> <p>all-Set all, um das System auf die Standardeinstellungen zurückzusetzen und neu zu starten.</p>
--------------	------------------------	---

Beispiel 1:

So zeigen Sie alle Informationen des Systems an

CyberPower > **sys zeigen**

Name: RMCARD205 (305)

Ort : Serverraum

Kontakt: Administrator

Modell: RMCARD205 (305)

Hardware-Version: 1.1

Firmware Version: 1.0.3

Firmware Update Datum: 03/08/2015

Seriennummer: TALGY2001975

MAC-Adresse: 00-0C-15-00-B9-42

Beispiel 2:

Um die RMCARD auf die Standardparameter zurückzusetzen.

CyberPower > **sys reset all**

dst

Beschreibung: Anzeigen und Konfigurieren der Art der Sommerzeit.

Option	Argument	Beschreibung
anzeigen		Anzeige aller DST-Informationen für RMCARD
Modus	deaktivieren us manuell	disable - Deaktiviert die Sommerzeit. us-Tradition US DST manuell - Manuelle Regeln für die Sommerzeit. Nach Beendigung dieses Befehls geben Sie Schritt für Schritt die Start- und Endzeit ein. Die Parameter von Woche des Monats : erste zweite dritte vierte letzte Die Parameter des Wochentags : Mo Di Mi Do Fr Sa So Die Parameter des Monats : Jan Feb Mär Apr Mai Jun Jul Aug Sep Okt Nov Dez

Beispiel 1:

Manuell eingestellte Sommerzeit
CyberPower > **dst typ handbuch**
Startzeit (0~23): **2**
Anfangswoche des Monats: **zweite**
Starttag der Woche: **So**
Startmonat: **März**
Endzeit (0~23): **2**
Ende Woche des Monats: **erste**
Letzter Tag der Woche: **So**
Ende Monat: **Nov.**

Beispiel 2:

So zeigen Sie die Sommerzeiteinstellung an
CyberPower > **dst anzeigen**
Sommerzeit: Manuelle Sommerzeit Datum Uhrzeit
Beginn: 02:00, der zweite Sonntag im März
Ende: 02:00, der erste Sonntag im November

Anmeldung

Beschreibung: Anzeige und Konfiguration der Authentifizierung für die Anmeldung.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Anmeldeinformationen für RMCARD
Typ	lokal radiuslokal radiusonly ldaplokal ldaponly	local-Benutzer zur Anmeldung bei der Remote Management Card mit dem Benutzernamen und dem Kennwort, die unter Lokales Konto konfiguriert wurden. radiuslocal-Benutzer, um die Remote Management Card mit Benutzernamen und Kennwort anzumelden, um sich zuerst beim RADIUS-Server zu authentifizieren. Wenn der RADIUS-Server nicht antwortet, werden der Benutzername und das Kennwort, die unter Lokales Konto konfiguriert wurden, verwendet. radiusonly-Benutzer, um die Remote Management Card mit Benutzernamen und Kennwort anzumelden, nur für die Authentifizierung mit dem RADIUS-Server. ldaplokal-Benutzer für die Anmeldung an der Remote Management Card mit Benutzername und Kennwort für die erste Authentifizierung beim LDAP-Server. Wenn der LDAP-Server nicht antwortet, werden der Benutzername und das Kennwort, die unter Lokales Konto konfiguriert wurden, verwendet. ldaponly-Benutzer zur Anmeldung an der Remote Management Card mit Benutzernamen und Kennwort nur für die Authentifizierung mit dem LDAP-Server.
Geheimsprache	<Authentifizierungsphrase>	Die für die Kommunikation mit PowerPanel [®] Business Remote verwendete Authentifizierungsphrase.
Timeout	1~10	Der Zeitraum (in Minuten), den das System wartet, bevor es sich automatisch abmeldet. Der Bereich des Arguments reicht von 1 bis 10 (in Minuten).

Beispiel 1:

So ändern Sie den Authentifizierungstyp in Radius, Lokales Konto
CyberPower > **Anmeldeart radiuslokal**

admin / Gerät

Beschreibung: Zeigt und konfiguriert die primäre/sekundäre Manager-IP, den Benutzernamen und das Passwort des Admin/Gerätebenutzers.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Admin- oder Geräteinformationen für diese RMCARD
Zugriff	aktivieren deaktivieren	Aktivieren oder deaktivieren Gerät
primip	<primäre Manager-IP>	Festlegen der primären Manager-IP von admin/device
secmipac	aktivieren deaktivieren	Aktivieren oder Deaktivieren der sekundären Manager-IP von admin/device
secmip	<sekundäre Manager-IP>	Festlegen der sekundären Manager-IP von admin/device
Name	<Benutzername>	Benutzernamen von admin/device festlegen
passwd	<Benutzerpasswort>	Benutzerpasswort von admin/device festlegen

Beispiel 1:

So definieren Sie die primäre Admin-Manager-IP als 192.168.26.0/24

CyberPower > **admin primip 192.168.26.0/24**

Admin-Passwort eingeben: **cyber**

Pass

Radius

Beschreibung: Anzeigen und Konfigurieren von Informationen zum Radius-Server.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Radius-Server-Informationen für RMCARD
pri sec	anzeigen	Anzeige von primären/sekundären Radius-Server-Informationen.
hinzufügen.		Fügen Sie den Radius-Server hinzu und geben Sie später die IP/Secret/Port des Radius-Servers ein.
hinzufügen.	<Server IP> <Server Geheimnis> <Server Port>	Fügen Sie Radius-Server-Informationen einschließlich Server-IP/Secret/Port auf einmal hinzu.
Priip secip	<Radius-Server-IP>	Legen Sie die IP-Adresse des primären/sekundären RADIUS-Servers fest.
priport secpport	<Radius-Server-Port >	Legen Sie den UDP-Port fest, der von dem primären/sekundären Radius-Server verwendet wird.
prisecret Sicherheitsge heimnis	<Geheimnis des Radius- Servers>	Legen Sie das gemeinsame Geheimnis des primären/sekundären Radius-Servers fest.
pridel secdel		Primären/sekundären Radius-Server löschen

Beispiel 1:

So zeigen Sie Informationen zum primären Radius-Server an
CyberPower > **radius pri anzeigen**
Server-IP: 192.168.26.33
Server-Geheimnis: testsecret
Server-Port : 1826

Beispiel 2:

So zeigen Sie Informationen zum sekundären Radius-Server an
CyberPower > **radius sec anzeigen**
Server-IP: 192.168.30.58
Server-Geheimnis: testsecret2
Server-Port : 1508

Geben Sie den folgenden Befehl ein, um die Konfiguration der Radius-Serverinformationen mit einem einzigen Befehl hinzuzufügen:

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

Zum Beispiel:

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

Hinweis: Dieser einzelne Befehl kann nicht erfolgreich ausgeführt werden, wenn bereits zwei Radius-Server eingerichtet sind.

ldap

Beschreibung: Anzeigen und Konfigurieren von Informationen zum LDAP-Server.

Option	Argument	Beschreibung
anzeigen		Anzeige aller LDAP-Server-Informationen für RMCARD
hinzufügen.		Fügen Sie den LDAP-Server hinzu, und geben Sie die Informationen für die Anforderungen später ein.
pritype sectype	openldap ad	Legen Sie den Typ des LDAP-Servers fest.
Priip secip	<LDAP-Server-IP>	Legen Sie die IP-Adresse des primären/sekundären LDAP-Servers fest.
prissl secssl	aktivieren deaktivieren	Aktivieren oder deaktivieren Sie die Verwendung von LDAPS.
priport secport	<LDAP-Server-Port >	Legen Sie den TCP-Port fest, der vom primären/sekundären LDAP-Server verwendet wird.
pridn secdn	<LDAP-Server-Basis-DN>	Legen Sie den Basis-DN des primären/sekundären LDAP-Servers fest.
priaddomain secaddomain	< LDAP-Server AD-Domäne>	Legen Sie die AD-Domäne des primären/sekundären Active Directory-Servers fest.
Option	Argument	Beschreibung

priattr secattr	<Anmeldungsattribut des LDAP-Servers>	Legen Sie das Login-Attribut des primären/sekundären LDAP-Benutzereintrags fest.
pridel secdel		Löschen Sie den primären/sekundären LDAP-Server.

Beispiel 1:

So fügen Sie einen LDAP-Server hinzu
 CyberPower > **ldap hinzufügen**
 LDAP-Servertyp eingeben [openldap | ad]: **ad**
 IP-Adresse eingeben: **192.168.26.33**
 SSL verwenden [aktivieren | deaktivieren]: **deaktivieren**
 LDAP-Port eingeben: **389**
 Eingabe Basis-DN: **dc=cyber,dc=com**
 Login-Attribut eingeben: **cn**
 Eingabe AD-Domäne: **cyber.com**

Beispiel 2:

So zeigen Sie Informationen zum LDAP-Server an
 CyberPower > **ldap anzeigen**
 Primärer LDAP-Server
 Typ: **Windows AD**
 LDAP-Server: **192.168.26.33**
 LDAP SSL: **Deaktivieren**
 Port : **389**
 Basis-DN: **dc=cyber,dc=com**
 Login-Attribut: **cn**
 AD-Bereich: **cyber.com**

tcpip

Beschreibung: Anzeigen und Konfigurieren von IPv4 IP, Netzmaske, Gateway, DNS.

Option	Argument	Beschreibung
anzeigen		Anzeige aller IPv4-Informationen für RMCARD
dhcp	aktivieren deaktivieren	Aktivieren oder Deaktivieren von DHCP
dns	manuell automatisch	Automatischer Bezug der DNS-Adresse von DHCP, wenn DHCP aktiviert ist Manuell - Bezieht die DNS-Adresse manuell, wenn DHCP aktiviert ist.
ip	<System-IP>	IP-Adresse des Systems einstellen
Netzmaske	<System-Netzmaske>	Netzmaske des Systems festlegen
Gateway	<System-Gateway>	Gateway des Systems einstellen
dnsip	<system dns>	DNS des Systems einstellen

Beispiel 1:

So deaktivieren Sie DHCP und legen die IP-Adresse auf 192.168.26.33 fest
CyberPower > **tcpip dhcp disable ip 192.168.26.33**

tcpip6

Beschreibung: Anzeigen und Konfigurieren des Status der IPv6-Routersteuerung, IPv6 Manual IP.

Option	Argument	Beschreibung
anzeigen		Anzeige aller IPv6-Informationen für RMCARD
Zugriff	aktivieren deaktivieren	Aktivieren oder deaktivieren Sie den IPv6-Service .
routerctrl	aktivieren deaktivieren	Die IPv6-Adresse wird durch die Methode (Stateless Address Autoconfiguration, Stateless DHCPv6 oder Stateful DHCPv6) zugewiesen, die durch die Routereinstellung bestimmt wird.
Handbuch	aktivieren deaktivieren	Aktivieren oder deaktivieren Sie IPv6 manual ip.
ip	<manuelle IPv6-IP>	Manuelle IPv6-IP einstellen.

Beispiel 1:

So definieren Sie eine manuelle IPv6-Adresse und zeigen dann die IPv6-Informationen an
CyberPower > **tcpip6 manual enable ip 2001:cdba:0:0:0:0:3257:9652 show**
Zugriff : Aktivieren Sie
Router-Steuerung: Aktivieren
Manuell: Aktivieren Sie
Manuelle IPv6-Adresse: [2001:cdba::3257:9652]

snmpv1

Beschreibung: Zeigt und konfiguriert den Status von SNMPv1.

Option	Argument	Beschreibung
anzeigen		Anzeige des SNMPv1-Status für RMCARD
Index	<1 2 3 4>	Wählen Sie den SNMPv1-Community-Index.
einstellen.	<1 2 3 4>	Ändern der SNMPv1-Community-Informationen.
Zugriff	aktivieren deaktivieren	Aktivieren oder deaktivieren Sie SNMPv1.
Gemeinschaft	<Gemeinschaft>	Ändern Sie den SNMPv1-Community-Namen.
ip	<IP-Adresse>	Ändern Sie die IP-Adresse der SNMPv1-Community.
Typ	<nur Lesen Lesen/Schreiben Verboten>	Ändern Sie den SNMPv1-Community-Typ.

Beispiel 1:

So zeigen Sie die zweite SNMPv1-Community-Information an
CyberPower > **snmpv1 index 2 show**
Gemeinschaft: privat
IP-Adresse: 192.169.203.20
Typ: Lesen/Schreiben

Beispiel 2:

So ändern Sie den Community-Namen der ersten SNMPv1-Community in Public1
CyberPower > **snmpv1 index 1 Gemeinschaft Public1**

Beispiel 3:

So ändern Sie die IP-Adresse der dritten SNMPv1-Community in 192.168.203.88
CyberPower > **snmpv1 index 3 ip 192.168.203.88**

Beispiel 4:

So ändern Sie den Community-Typ der vierten SNMPv1-Community in Lesen/Schreiben
CyberPower > **snmpv1 index 4 type readwrite**

Geben Sie den folgenden Befehl ein, um die Konfiguration aller Parameter mit einem einzigen Befehl durchzuführen:

```
snmpv1 set <1 | 2 | 3 | 4> <Gemeinschaft> <IP-Adresse> <readonly | readwrite  
| forbidden>
```

Zum Beispiel:

```
CyberPower > snmpv1 set 3 CyberPower 192.168.203.91 readonly
```

snmpv3

Beschreibung: Zeigt und konfiguriert den Status von SNMPv3.

Option	Argument	Beschreibung
anzeigen		Anzeige des SNMPv3-Status für RMCARD
Index	<1 2 3 4>	Wählen Sie den SNMPv3-Benutzerindex.
einstellen.	<1 2 3 4>	Ändern Sie SNMPv3-Benutzerinformationen.
Zugriff	aktivieren deaktivieren	Aktivieren oder Deaktivieren von SNMPv3
Name	<Benutzername>	Ändern Sie den SNMPv3-Benutzernamen.
Status	<Aktivieren Deaktivieren>	Aktivieren oder deaktivieren Sie SNMPv3- Benutzer.
ip	<IP-Adresse>	Ändern Sie die IP-Adresse des SNMPv3- Benutzers.
Autorisierung	<md5 sha keine>	Ändern Sie das Authentifizierungsprotokoll des SNMPv3-Benutzers.
Authentifizierungsschlüssel	<Auth-Schlüssel>	Ändern Sie das Authentifizierungspasswort des SNMPv3-Benutzers.
privat	<aes des none>	Ändern Sie das Datenschutzprotokoll des SNMPv3-Benutzers.
Privatschlüssel	<Privater Schlüssel>	Ändern Sie das Passwort für die Privatsphäre des SNMPv3-Benutzers.

Beispiel 1:

So zeigen Sie die ersten SNMPv3-Benutzerinformationen an
CyberPower > **snmpv3 index 1 show**

Name des Benutzers: CyberPower
Status: Aktivieren
IP-Adresse: 192.169.30.58
Authentifizierungsprotokoll: MD5
Privates Protokoll: aes

Beispiel 2:

So ändern Sie den Benutzernamen des zweiten SNMPv3-Benutzers in CyberPower
CyberPower > **snmpv3 index 2 Name CyberPower**

Beispiel 3:

So aktivieren Sie den dritten SNMPv3-Benutzer
CyberPower > **snmpv3 index 3 status enable**

Beispiel 4:

So ändern Sie die IP-Adresse des vierten SNMPv3-Benutzers auf 192.168.203.66
CyberPower > **snmpv3 index 4 ip 192.168.203.66**

Beispiel 5:

So ändern Sie das Authentifizierungsprotokoll des zweiten SNMPv3-Benutzers auf md5 und setzen sein Authentifizierungspasswort auf **test_authkey_123456**
CyberPower > **snmpv3 index 2 auth md5 authkey test_authkey_123456**

Beispiel 6:

So ändern Sie das Authentifizierungspasswort des ersten SNMPv3-Benutzers in **test_authkey_123456**
CyberPower > **snmpv3 index 1 authkey test_authkey_123456**

Beispiel 7:

So ändern Sie das Authentifizierungsprotokoll eines dritten SNMPv3-Benutzers auf none
CyberPower > **snmpv3 index 3 auth keine**

Beispiel 8:

So ändern Sie das Datenschutzprotokoll des zweiten SNMPv3-Benutzers auf aes und setzen sein Datenschutzpasswort auf **test_privkey_123456**
CyberPower > **snmpv3 index 2 priv aes privkey test_privkey_123456**

Beispiel 9:

So ändern Sie das Datenschutzpasswort des ersten SNMPv3-Benutzers in **test_privkey_123456**
CyberPower > **snmpv3 index 1 privkey test_privkey_123456**

Beispiel 10:

So ändern Sie das Datenschutzprotokoll eines dritten SNMPv3-Benutzers auf none
CyberPower > **snmpv3 index 3 priv keine**

Geben Sie den folgenden Befehl ein, um die Konfiguration aller Parameter mit einem einzigen Befehl durchzuführen:

```
snmpv3 set <1 | 2 | 3 | 4> <Benutzername> <IP-Adresse> <md5 | sha | none>  
<Auth Key> <aes | des | none> <Priv Key>
```

Zum Beispiel:

```
CyberPower > snmpv3 set 1 CyberPower 192.168.203.90 sha test_authkey_123456 des test_privkey_123456
```

Falle

Beschreibung: Anzeigen und Konfigurieren von Informationen über SNMP-Trap-Empfänger.

Option	Argument	Beschreibung
anzeigen		Anzeige von Trap-Empfänger-Informationen für RMCARD.
hinzufügen.		Trap-Empfänger für RMCARD hinzufügen.
Index	<1 2 ... 10>	Wählen Sie den Trap-Empfänger-Index.
Name	<Name des Trap-Empfängers>	Ändern Sie den Trap-Namen des Trap-Empfängers.
ip	<Trap-Empfänger-IP>	Ändern Sie die IP-Adresse des Trap-Empfängers.
ver	<v1 v3>	Ändern Sie die SNMP-Version des Trap-Empfängers.
Status	<aktivieren deaktivieren>	Aktivieren oder deaktivieren Sie den Trap-Empfänger.
Gemeinschaft	<Trap Receiver Community>	Ändern Sie den SNMPv1-Community-Namen des Trap-Empfängers.
Benutzer	<1 2 3 4>	Wählen Sie den SNMPv3-Benutzer des Trap-Empfängers.
löschen		Trap-Empfänger löschen.

Beispiel 1:

So zeigen Sie die Informationen zum sechsten Trap-Empfänger an

```
CyberPower > Trap-Index 6 anzeigen
```

Name der Falle: CyberPower

Status: Aktivieren

IP-Adresse: 192.168.203.68

Typ: SNMPv1

Gemeinschaft: test_community

Beispiel 2:

So ändern Sie den Trap-Namen des zweiten Trap-Empfängers in Test

```
CyberPower > Trap-Index 2 Namenstest
```

Beispiel 3:

So ändern Sie die IP-Adresse des dritten Trap-Empfängers in 192.168.30.85

```
CyberPower > Trap-Index 3 ip 192.168.30.85
```

Beispiel 4:

So ändern Sie die SNMP-Version des vierten Trap-Empfängers auf SNMPv3

```
CyberPower > Trap-Index 4 ver v3
```

Beispiel 5:

So ändern Sie den fünften Trap-Empfänger

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

Beispiel 6:

So ändern Sie den Community-Namen des zweiten Trap-Empfängers in CyberPower mit der Bedingung, dass die SNMP-Version des Trap-Empfängers SNMPv1 sein muss.

```
CyberPower > Fallenindex 2 Gemeinschaft CyberPower
```

Beispiel 7:

So ändern Sie den SNMPv3-Benutzer des zehnten Trap-Empfängers in SNMPv3-Benutzer2 unter der Bedingung, dass die SNMP-Version des Trap-Empfängers SNMPv3 sein muss

```
CyberPower > Trap-Index 10 Benutzer 2
```

Beispiel 8:

So löschen Sie den fünften Trap-Empfänger

```
CyberPower > Trap-Index 5 löschen
```

Geben Sie den folgenden Befehl ein, um die Konfiguration des Trap-Empfängers mit einem einzigen Befehl hinzuzufügen:

```
Für SNMPv1: trap add <Trap Name> <Trap Receiver IP> v1 <Community>
```

Zum Beispiel:

```
CyberPower > trap add CyberPower 192.168.203.16 v1 test
```

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

Zum Beispiel:

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

Web

Beschreibung: Anzeigen und Konfigurieren von Webzugriffstyp, http-Port und https-Port.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Webinformationen für RMCARD
Zugriff	http https deaktivieren	http - Aktiviert den Zugriff auf den http-Service . https - Aktiviert den Zugriff auf den https-Service . disable - Webservice deaktivieren
httpport	<http-Port>	Der TCP/IP-Port für das Hypertext Transfer Protocol (HTTP) (standardmäßig 80)
httpsport	<https-Port>	Der TCP/IP-Port des Hypertext Transfer Protocol Secure (HTTPS) (standardmäßig 443)

Beispiel 1:

So ändern Sie den HTTP-Server-Port auf 5000

```
CyberPower > web httpport 5000
```

Konsole

Beschreibung: Zeigt und konfiguriert den Typ des Konsolennetzwerkzugriffs, den Telnet-Port und den SSH-Port.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Konsoleninformationen für RMCARD
Zugriff	telnet ssh deaktivieren	telnet - Aktiviert den Zugriff zu Telnet ssh - Aktiviert den Zugriff zu SSH disable - Deaktiviert den KonsolenService
telnet	<aktivieren deaktivieren>	aktivieren - Telnet aktivieren . disable - Deaktiviert Telnet.
ssh	<aktivieren deaktivieren reset_hostkey>	aktivieren - SSH aktivieren . disable - Deaktiviert SSH. reset_hostkey - Setzt den SSH-Hostkey auf die Standardwerte zurück .
telnetport	<Telnet-Port >	Der TCP/IP-Port (standardmäßig 23), den Telnet für die Kommunikation verwendet.
sshport	<ssh port>	Der TCP/IP-Port (standardmäßig 22), den SSH für die Kommunikation verwendet.

Beispiel 1:

Um Telnet als Konsole zu aktivieren, geben Sie ein
CyberPower > **Konsole telnet aktivieren**

Beispiel 2:

Um SSH als Konsole zu deaktivieren, geben Sie ein
CyberPower > **Konsole ssh deaktivieren**

Hinweis: Die Modi telnet und ssh sind Optionen zum Umschalten zwischen den beiden Modi. Zum Beispiel wird telnet automatisch deaktiviert, sobald ssh als Konsolentyp aktiviert wird und umgekehrt.

Beispiel 3:

So Stellen Sieden SSH-Hostkey auf die Standardeinstellungen zurück
CyberPower > **Konsole ssh reset_hostkey**

Hinweis: Das System wird neu gestartet, nachdem der SSH-Hostkey der RMCARD auf die Standardeinstellungen zurückgesetzt wurde.

ftp

Beschreibung: Zeigt und konfiguriert FTP-Zugriff styp und TCP/IP-Port von FTP.

Option	Argument	Beschreibung
anzeigen		Anzeige aller FTP-Informationen für RMCARD
Zugriff	aktivieren deaktivieren	Aktivieren oder Deaktivieren des FTP-Servers
Hafen	<ftp-Port >	Der TCP/IP-Port des FTP-Servers (standardmäßig 21).

Beispiel 1:

So aktivieren Sie den FTP-Service

CyberPower > **ftp-Zugriff aktivieren**

Ereignisprotokoll

Beschreibung: Anzeigen und Löschen des Ereignisprotokolls von RMCARD und USV.

Option	Argument	Beschreibung
anzeigen		Zeigt die Liste der Ereignisse und eine kurze Beschreibung jedes Ereignisses zusammen mit dem Datum und dem Zeitstempel an.
klar		Löschen Sie die vorhandenen Ereignisprotokolle.

Beispiel 1:

CyberPower > **Ereignisprotokoll anzeigen**

12/11/2015 03:32:08 Admin-Anmeldung von 192.168.26.33.

.....

Verwenden Sie dann die folgenden Tasten, um im Ereignisprotokoll zu navigieren.

Schlüssel	Beschreibung
SPACE	Zeigen Sie die nächste Seite des Ereignisprotokolls an.
Q	Schließen Sie das Ereignisprotokoll und kehren Sie zur Befehlszeilenschnittstelle zurück.

Beispiel 2:

So löschen Sie alle Ereignisprotokolle.

CyberPower > **Ereignisprotokoll löschen**

Möchten Sie das gesamte Ereignisprotokoll löschen [ja / nein]: ja

syslog

Beschreibung: Anzeigen und Konfigurieren von Informationen über den SYSLOG-Server.

Option	Argument	Beschreibung
anzeigen		Anzeige aller Syslog-Informationen für RMCARD
s1 s2 s3 s4	anzeigen	Anzeige der Syslog-Server-Informationen für 1 bis 4 Server.
hinzufügen.		Fügen Sie den Syslog-Server hinzu und geben Sie später die IP/Port des Syslog-Servers ein.
hinzufügen.	<Server-IP> <Server-Port>	Fügen Sie Syslog-Server-Informationen einschließlich Server-IP/Port auf einmal hinzu.
Zugriff	aktivieren deaktivieren	Aktivieren oder deaktivieren Sie Syslog.
Einrichtung	kernel user mail system auth1 syslog link news uucp clock1 auth2 ftp ntp logaudit logalert clock2 local0 local1 local2 local3 local4 local5 local6 local7	Syslog-Einrichtung einstellen.
s1test s2test s3test s4test		Senden Sie eine Testnachricht an den Syslog-Server für 1 bis 4 Server.
ip1 ip2 ip3 ip4	<SYSLOG-Server-IP>	Stellen Sie die IP-Adresse des Syslog-Servers für 1 bis 4 Server ein.
Hafen1 Hafen2 Port 3 Hafen4	<SYSLOG-Server-Port >	Legen Sie den UDP-Port fest, der vom Syslog-Server 1 bis 4 Server verwendet wird.
s1del s2del s3del s4del		Löschen Sie den Syslog-Server für 1 bis 4 Server.

Beispiel 1:

So zeigen Sie die Syslog-Informationen von Server 1 an

```
CyberPower > syslog s1 show
```

```
IP: 192.168.26.33
```

```
Port: 514
```

Beispiel 2:

So zeigen Sie die Syslog-Informationen von Server 2 an

```
CyberPower > syslog s2 show
```

```
IP: 192.168.203.89
```

```
Port: 268
```

Beispiel 3:

So zeigen Sie die Syslog-Informationen von Server 3 an

```
CyberPower > syslog s3 show
```

```
IP: 192.168.30.15
```

```
Hafen: 101
```

Beispiel 4:

So zeigen Sie die Syslog-Informationen von Server 4 an

```
CyberPower > syslog s4 show
```

```
IP: 192.168.26.93
```

```
Hafen: 358
```

Geben Sie den folgenden Befehl ein, um die Konfiguration aller Parameter mit einem einzigen Befehl durchzuführen:

```
syslog add <Server IP-Adresse> <Server Port>
```

Zum Beispiel:

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

Hinweis: Dieser einzelne Befehl kann nicht erfolgreich ausgeführt werden, wenn bereits vier Syslog-Server eingestellt sind.

menumode

Beschreibung: Modus als Menümodus umschalten.

klar

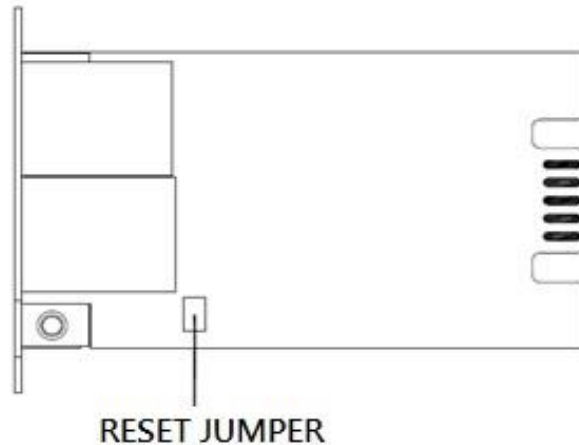
Beschreibung: Löscht den Konsolenbildschirm.

Ausgang

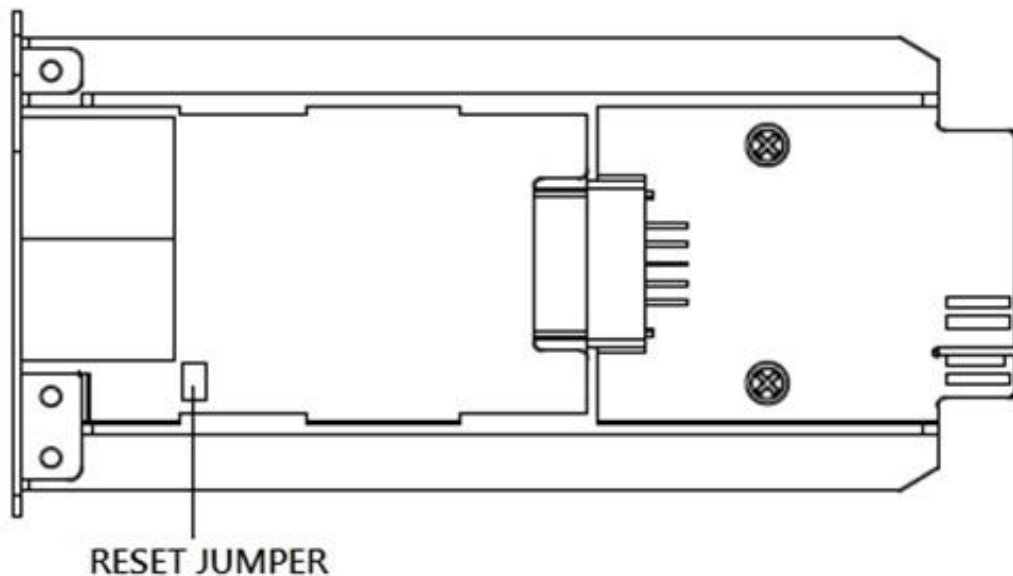
Beschreibung: Schließt die Verbindung zur Befehlszeilenschnittstelle.

Zurücksetzen auf Werkseinstellungen / Wiederherstellen eines verlorenen Passworts

Führen Sie die folgenden Schritte aus, um die CyberPower Remote Management Card auf die werkseitigen Standardeinstellungen zurückzusetzen (einschließlich Benutzername und Kennwort für die Webanmeldung):



RMCARD205



RMCARD305

1. Entfernen Sie die Karte aus der USV, ohne die USV/ATS PDU auszuschalten.
2. Entfernen Sie den Jumper von den Reset-Stiften wie abgebildet. Entsorgen Sie die Steckbrücke nicht.
3. Stecken Sie die Karte in den Erweiterungsport der USV/ATS-PDU.
4. Warten Sie, bis die grüne Tx/Rx-LED blinkt (die Frequenz des ON/OFF-Blinkens ist einmal pro Sekunde).
5. Nehmen Sie die Karte wieder heraus.
6. Stecken Sie den Jumper wieder auf die Reset-Stifte.
7. Stellen Sie die Karte wieder in den Erweiterungsport ein und ziehen Sie die Befestigungsschrauben fest.

RMCARD Firmware Upgrade

Durch ein Firmware-Upgrade können Sie sowohl neue Funktionen als auch Aktualisierungen/Verbesserungen der bestehenden Funktionen erhalten. Der FTP-Service muss aktiviert sein, bevor Sie versuchen, ein Firmware-Upgrade durchzuführen. Sie können die "Firmware Version" auf der **[System->About]** Seite auf der Web-Benutzeroberfläche der RMCARD überprüfen. Es gibt zwei Dateien, die aktualisiert werden müssen, um die Firmware-Version zu aktualisieren.

- A. cpsrm2scdata_XXX.bin
- B. cpsrm2scfw_XXX.bin

Hinweis: Um sicherzustellen, dass die RMCARD-Firmware auf dem neuesten Stand ist, besuchen Sie bitte alle 3 Monate die CyberPower-Website, um zu sehen, ob es eine aktualisierte Firmware-Version gibt.

Hinweis: Bitte schalten Sie die USV nicht aus, wenn Sie die Firmware-Aktualisierung durchführen.

Hinweis: Um die RMCARD-Firmware erfolgreich zu aktualisieren, überprüfen Sie bitte, ob die Verbindungen zu Port 20 und 21 in der Firewall nicht blockiert sind.

Methode 1: FTP-Befehl verwenden

Führen Sie die folgenden Schritte aus, um die Firmware zu aktualisieren:

1. Laden Sie die neueste Firmware herunter
2. Entpacken Sie die heruntergeladenen Dateien nach "C:\".
3. Öffnen Sie ein Fenster der Eingabeaufforderung
4. Melden Sie sich bei der CyberPower Remote Management Card mit dem FTP-Befehl an und geben Sie in die Eingabeaufforderung ein:
 - (1) ftp
 - (2) ftp> open
 - (3) An [aktuelle IP-Adresse der RMCARD] [Port]; EX: An 192.168.22.126 21
 - (4) Geben Sie den BENUTZERNAMEN und das PASSWORT ein (das gleiche wie das Administratorkonto in der Web-Benutzeroberfläche, siehe Seite 6 für die werkseitigen Standardeinstellungen)
5. Datei A hochladen, Typ:

```
ftp > bin
ftp > put cpsrm2scdata_XXX.bin
```
6. Das Hochladen ist nun abgeschlossen, geben Sie ein:

```
ftp > Beenden
```
7. Das System wird neu gestartet, nachdem Sie "quit" eingegeben haben.
8. Melden Sie sich erneut beim FTP an wie in Schritt 4.
9. Datei B hochladen, Typ:

```
ftp > bin
ftp > put cpsrm2scfw_XXX.bin
```
10. Das Hochladen ist nun abgeschlossen, geben Sie ein:

```
ftp > Beenden
```
11. Das System wird neu gestartet, nachdem Sie "quit" eingegeben haben.

Methode 2: mit Power Device Network Utility 2

1. Installieren Sie das CyberPower Power Device Network Utility 2, das Sie unter www.CyberPower.com herunterladen können.
2. Führen Sie nach Abschluss der Installation das "Power Device Network Utility 2" aus.
3. Das Hauptfenster des Programms Power Device Network Utility 2 ist in Abbildung 5 dargestellt. Das Konfigurationstool zeigt alle CyberPower Remote Management-Geräte an, die im lokalen Netzwerk-Subnetz vorhanden sind. Mit der Schaltfläche "Scan" wird das lokale Netzwerk-Subnetz erneut durchsucht .

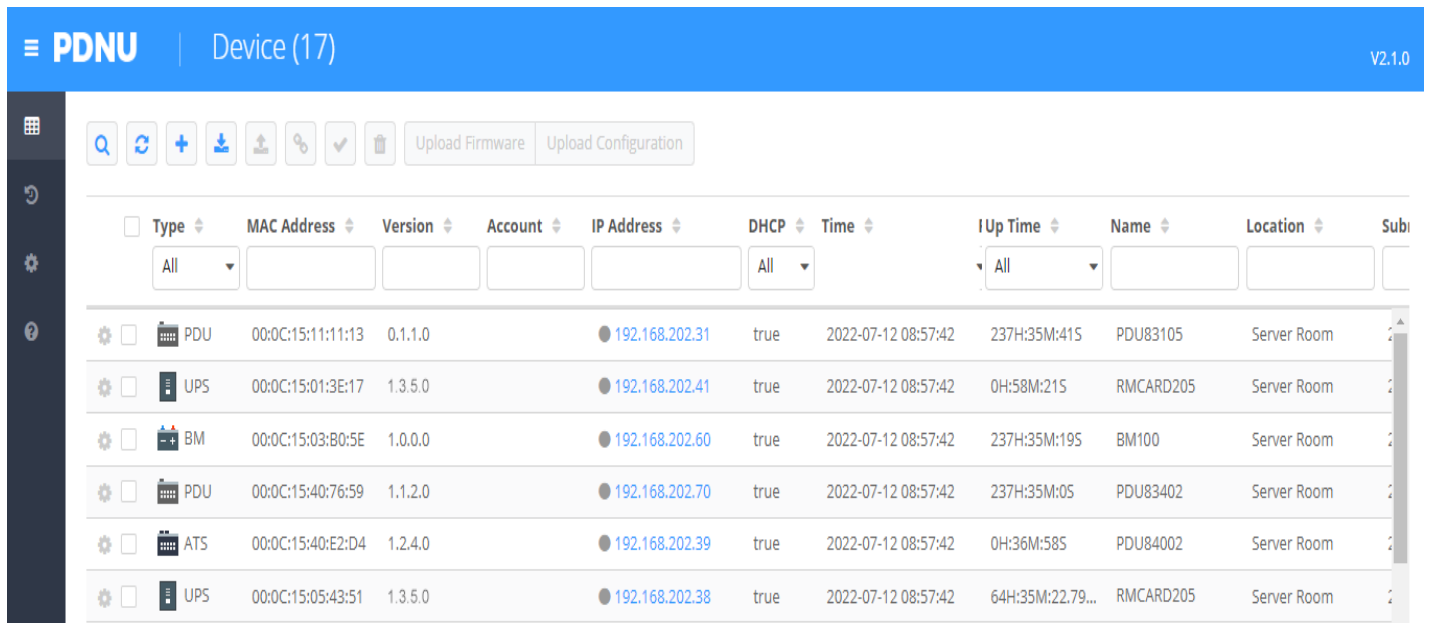


Abbildung 5. Das Hauptfenster des Programms "Power Device Network Utility 2".

4. Markieren Sie die Kästchen, um die Geräte auszuwählen, die Sie aktualisieren möchten, und klicken Sie in der oberen Werkzeugliste auf "Verbindung", um das Benutzerkonto und das Passwort des Geräts einzugeben. Sobald die Verbindung bestätigt ist, wechselt das Statussymbol neben der IP-Adresse von grau auf grün.

Hinweis: Vor der Aktualisierung der Firmware müssen Sie eine Verbindung zum Gerät herstellen, indem Sie die Anmeldedaten für das Benutzerkonto und das Passwort eingeben.

5. Wählen Sie die Geräte aus, die Sie aktualisieren möchten, indem Sie das entsprechende Kontrollkästchen aktivieren, und wählen Sie "Firmware hochladen".

Hinweis: Sie können die Firmware von mehreren Geräten hochladen, die dieselben Firmware-Dateien verwenden.

6. Wählen Sie die Firmware- und Datendateien aus und klicken Sie auf "OK", um das Firmware-Upgrade durchzuführen (siehe Abbildung 6).

File Locations of Firmware & Data

Protocol
 FTP SCP SCP/FTP

Firmware
 cpsrm2scfw_136.bin Browse

Data
 cpsrm2scdata_136.bin Browse

OK Cancel

Abbildung 6. Das Fenster Dateispeicherorte von Firmware & Daten.

7. Wenn das Firmware-Upgrade durchgeführt wurde, sehen Sie das Ergebnis im Hauptfenster, wie in Abbildung 7 dargestellt.

Type	MAC Address	Version	Account	IP Address	DHCP	Time	Up Time	Name	Location	Sub
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	1.3.5.0		192.168.202.41	true	2022-07-12 09:17:15	0H:1M:51S	RMCARD205	Server Room	
BM	00:0C:15:03:B0:5E	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	1.3.6.0	admin	192.168.202.38	true	2022-07-12 09:17:15	64H:35M:22.82...	RMCARD205	Server Room	

Abbildung 7. Erfolgreiches Firmware-Upgrade im Hauptfenster.

Methode 3: Verwendung des Befehls Secure Copy (SCP)

Führen Sie die folgenden Schritte aus, um die Firmware über SCP zu aktualisieren.

Hinweis: Nur Firmware-Version 1.1.2 und höher unterstützt die Funktion zur Aktualisierung der Firmware über SCP.

Für Windows-Benutzer:

1. Laden Sie ein beliebiges PuTTY Secure Copy Client (PSCP) Service Programm herunter.
2. Speichern Sie die Firmware-Dateien und das PSCP-Service Programm im selben Ordner.
3. Öffnen Sie die Befehlszeilenschnittstelle und ändern Sie den Pfad, in dem die Firmware-Dateien und das PSCP-Service Programm gespeichert sind.
4. Geben Sie den folgenden Befehl ein, um das Firmware-Update durchzuführen:
`pscp -scp <Dateiname> <Benutzer>@<IP-Adresse der RMCARD>:`

Anmerkung:

- (1) Die SSH-Einstellung auf der RMCARD muss auf Enabled stehen.
- (2) <Dateiname> ist der Dateiname der Firmware-Datei. Es gibt zwei hochzuladende Firmware-Dateien: `cpsrm2scdata_XXX.bin` und `cpsrm2scfw_XXX.bin`. Um die Firmware-Version zu aktualisieren, müssen beide Dateien hochgeladen werden. Es wird empfohlen, zuerst die Datendatei `cpsrm2scdata_XXX.bin` und dann die Firmware-Datei `cpsrm2scfw_XXX.bin` hochzuladen.
- (3) <user> ist der Benutzername des SSH-Kontos auf der RMCARD.
- (4) Achten Sie darauf, nach der IP-Adresse ein ":" einzufügen.

Zum Beispiel:

```
pscp -scp cpsrm2scdata_XXX.bin cyber@192.168.1.100:
```

Hinweis: `cpsrm2scdata_XXX.bin` ist die Datendatei der zu aktualisierende Version.

5. Nach der Ausführung des Befehls wird möglicherweise eine Meldung angezeigt, in der Sie gefragt werden, ob Sie dem Host vertrauen. Um fortzufahren, geben Sie innerhalb von 10 Sekunden "y" für Ja ein.
6. Geben Sie auf dem nächsten Bildschirm das RMCARD-Passwort ein. Der Datentransfer kann einige Minuten dauern, bis er abgeschlossen ist. Bitte warten Sie, bis die Fortschrittsanzeige 100% anzeigt. Das System meldet sich automatisch ab und startet neu, nachdem die Übertragung abgeschlossen ist.
7. Wiederholen Sie die Schritte 4 bis 6, um die Firmware-Datei `cpsrm2scfw_XXX.bin` hochzuladen und den Firmware-Aktualisierungsprozess abzuschließen.
8. Wenn die Übertragung der Firmware-Datei nicht erfolgreich war, erhalten Sie eine Fehlermeldung. Versuchen Sie, den Befehl neu einzugeben und erneut auszuführen.

Für Linux-, MacOS- und Unix-Benutzer:

1. Installieren Sie die entsprechende Distribution eines SSH- oder SCP-Clients, z. B. Openssh-Client.
2. Öffnen Sie das Terminal und ändern Sie den Pfad, in dem die Firmware-Dateien gespeichert sind.
3. Geben Sie den folgenden Befehl ein, um ein Firmware-Update durchzuführen:

```
scp <Dateiname> <Benutzer>@< IP-Adresse der RMCARD>:
```

Anmerkung:

- (1) Die SSH-Einstellung auf der RMCARD muss auf Enabled stehen.
- (2) <Dateiname> ist der Dateiname der Firmware-Datei. Es gibt zwei hochzuladende Firmware-Dateien: cpsrm2scdata_XXX.bin und cpsrm2scfw_XXX.bin. Um die Firmware-Version zu aktualisieren, müssen beide Dateien hochgeladen werden. Es wird empfohlen, zuerst die Datendatei cpsrm2scdata_XXX.bin und dann die Firmware-Datei cpsrm2scfw_XXX.bin hochzuladen.
- (3) <user> ist der Benutzername des SSH-Kontos auf der RMCARD.
- (4) Achten Sie darauf, nach der IP-Adresse ein ":" einzufügen.

Zum Beispiel:

```
scp cpsrm2scdata_XXX.bin cyber@192.168.1.100:
```

Hinweis: cpsrm2scdata_XXX.bin ist die Datendatei der zu aktualisierende Version.

4. Nach der Ausführung des Befehls wird möglicherweise eine Meldung angezeigt, in der Sie gefragt werden, ob Sie dem Host vertrauen. Um fortzufahren, geben Sie innerhalb von 10 Sekunden "y" für Ja ein.
5. Geben Sie auf dem nächsten Bildschirm das RMCARD-Passwort ein. Der Datentransfer kann einige Minuten dauern, bis er abgeschlossen ist. Bitte warten Sie, bis die Fortschrittsanzeige 100% anzeigt. Das System meldet sich automatisch ab und startet neu, nachdem die Übertragung abgeschlossen ist.
6. Wiederholen Sie die Schritte 3 bis 5, um die Firmware-Datei cpsrm2scfw_XXX.bin hochzuladen und den Firmware-Aktualisierungsprozess abzuschließen.
7. Wenn die Übertragung der Firmware-Datei nicht erfolgreich war, erhalten Sie eine Fehlermeldung. Versuchen Sie, den Befehl neu einzugeben und erneut auszuführen.

Methode 4: Verwendung der Webschnittstelle


Gehen Sie wie folgt vor, um die Firmware über die Webschnittstelle zu aktualisieren

Hinweis: Nur die Firmware-Version 1.3.4 und höher unterstützt die Funktion zur Aktualisierung der Firmware über die Web-Schnittstelle.

1. Gehen Sie über **[System->About]** zur Seite About.
2. Wählen Sie die Firmware- und Datendateien aus und klicken Sie auf "Senden", um das Firmware-Upgrade durchzuführen (siehe Abbildung 8).

Abbildung 8. Firmware-Update im Hauptfenster.

USV Fernverwaltung

Administratoranmeldung von 192.188.188.100 [Abmelden] 

Übersicht | USV | Protokoll | **System** | Hilfe

Allgemein
Sicherheit
Netzwerkdienst
Benachrichtigung
Reset/Neustart
Über

Über

Information

Modell	RMCARD305 (205)
Hardware Version	1.1
Firmware Version	1.4.1
Firmware Aktualisierungsdatum	04/29/2024
Seriennummer	TAMHT2000746
MAC Adresse	00-0C-15-02-04-DC

System-Firmware-Update

Firmware-Upload (cpsrm2scfw_XXX.bin) No file chosen

Daten hochladen
(cpsrm2sodata_XXX.bin) No file chosen

Konfiguration speichern/wiederherstellen

Konfiguration speichern

Konfiguration wiederherstellen No file chosen

3. Wenn das Firmware-Upgrade durchgeführt wurde, sehen Sie das Ergebnis im Hauptfenster, wie in Abbildung 9 dargestellt.

CyberPower UPS Remote Management

Warning:

Warning:
Success firmware upgrade, click [here to login](#) again.

© 2010, CyberPower Systems, Inc. All rights reserved.

Abbildung 9. Erfolgreiches Firmware-Upgrade im Hauptfenster.

Speichern und Wiederherstellen von Konfigurationseinstellungen

Methode 1: Verwendung der Webschnittstelle

Sie können die Gerätekonfiguration einfach auf Ihrem lokalen PC unter [System->About] speichern und wiederherstellen.

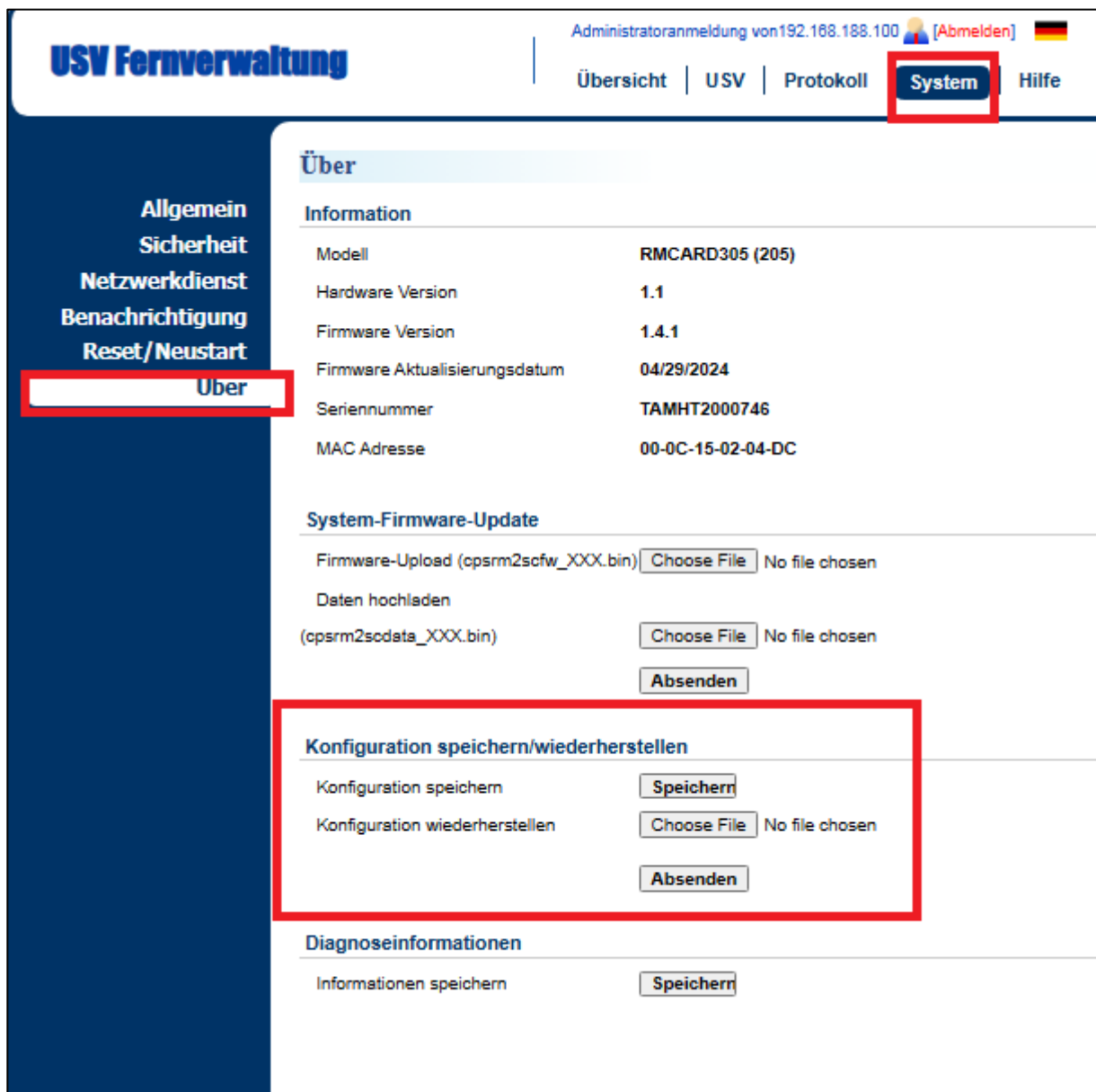


Abbildung 10. Speichern/Wiederherstellen der Konfiguration im Hauptfenster.

Sie können die Gerätekonfiguration einfach auf Ihrem lokalen PC unter [System->About] speichern und wiederherstellen, wie in Abbildung 10 dargestellt.

Um die Konfigurationsdatei zu speichern, klicken Sie auf "Speichern", um die Konfiguration auf Ihrem lokalen PC zu speichern. Die Textdatei hat das Standardformat JJJJ_MM_DT_HHMM.txt. Um eine Konfiguration wiederherzustellen, klicken Sie auf "Durchsuchen", um den Speicherort der Konfigurationsdatei zu finden, und klicken Sie auf "Senden", um eine zuvor gespeicherte Konfiguration wiederherzustellen.

Hinweis: Nur Firmware-Version 1.1.5 und höher unterstützen die Funktion zum Speichern und

Wiederherstellen der Konfiguration mit der aktuellen USV- und ATS-Parameterkonfiguration.

Methode 2: File Transfer Protocol (FTP) verwenden

Gehen Sie wie folgt vor, um die Konfiguration über FTP zu speichern.

Hinweis: Nur die Firmware-Version 1.4.0 und höher unterstützt die Funktion zum Herunterladen der Konfigurationsdatei über FTP.

1. öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zu "C:\".
2. Melden Sie sich bei der RMCARD mit dem FTP-Befehl an, geben Sie
 - C:\>ftp
 - ftp> open 192.168.22.126 21 (Beispiel: 192.168.22.126 ist die aktuelle IP der PDU und 21 ist der Standard-ftp-Port für die PDU)
 - Verbunden mit 192.168.22.126.
 - 220 CyberPower FTP-Server bereit.
 - Benutzer (192.168.22.126:(keine)):cyber
 - 331 Benutzername okay, Passwort erforderlich.
 - Kennwort:
 - 230 Benutzer eingeloggt, weiter.
 - ftp>
3. Laden Sie die Konfigurationsdatei herunter, geben Sie
 - ftp> get <Dateiname>
4. Wenn der Download abgeschlossen ist, geben Sie
 - ftp> Beenden

Hinweis: <Dateiname> ist die Konfigurationsdatei mit dem Format .TXT. Die maximale Länge des Dateinamens beträgt 32 Zeichen, ohne die Dateierweiterung (.TXT).

Zum Beispiel:

```
-ftp> get JJJJ_MM_DT_HHMM.txt  
JJJJ_MM_DT_HHMM.txt ist die zu speichernde Konfigurationsdatei.
```

Gehen Sie wie folgt vor, um die Konfiguration über FTP wiederherzustellen.

1. öffnen Sie ein Eingabeaufforderungsfenster und navigieren Sie zu "C:\".
2. Melden Sie sich bei der RMCARD mit dem FTP-Befehl an, geben Sie
 - C:\>ftp
 - ftp> open 192.168.22.126 21 (Beispiel: 192.168.22.126 ist die aktuelle IP der PDU und 21 ist der Standard-ftp-Port für die PDU)
 - Verbunden mit 192.168.22.126.
 - 220 CyberPower FTP-Server bereit.
 - Benutzer (192.168.22.126:(keine)):cyber

- 331 Benutzername okay, Passwort erforderlich.
 - Kennwort:
 - 230 Benutzer eingeloggt, weiter.
 - ftp>
3. Laden Sie die Konfigurationsdatei hoch, geben Sie
 - ftp> put <Dateiname>
 4. Das Hochladen ist abgeschlossen, geben Sie
 - ftp> Beenden
 5. Das System wird neu gestartet, nachdem Sie "quit" eingegeben haben.

Methode 3: Verwendung des Befehls Secure Copy (SCP)

Gehen Sie wie folgt vor, um die Konfiguration über SCP wiederherzustellen.

Hinweis: Nur die Firmware-Version 1.1.2 und höher unterstützt die Funktion zur Wiederherstellung der Konfiguration über SCP.

Für Windows-Benutzer:

1. Laden Sie ein beliebiges PuTTY Secure Copy Client (PSCP) Service Programm herunter.
2. Speichern Sie die Konfigurationsdatei und das PSCP-Service Programm in demselben Ordner.
3. Öffnen Sie die Befehlszeilenschnittstelle und ändern Sie den Pfad, in dem die Konfigurationsdatei und das PSCP-Service Programm gespeichert sind.
4. Geben Sie den folgenden Befehl ein, um die Konfiguration wiederherzustellen:


```
pscp -scp <Dateiname> <Benutzer>@<IP-Adresse der RMCARD>:
```

Anmerkung:

- (1) Die SSH-Einstellung auf der RMCARD muss auf Enabled stehen.
- (2) <Dateiname> ist der Dateiname der Konfigurationsdatei mit dem Standardformat JJJJ_MM_DT_HHMM.txt.
- (3) <user> ist der Benutzername des SSH-Kontos auf der RMCARD.
- (4) Achten Sie darauf, nach der IP-Adresse ein ":" einzufügen.

Zum Beispiel:

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

Hinweis: YYYY_MM_DD_HHMM.txt ist die Konfigurationsdatei, die wiederhergestellt werden soll.

5. Nach der Ausführung des Befehls wird möglicherweise eine Meldung angezeigt, in der Sie gefragt werden, ob Sie dem Host vertrauen. Um fortzufahren, geben Sie innerhalb von 10 Sekunden "y" für Ja ein.
6. Auf dem nächsten Bildschirm geben Sie das RMCARD-Passwort ein. Bitte warten Sie, bis die Fortschrittsanzeige 100% anzeigt. Das System meldet sich automatisch ab und startet neu, nachdem die Übertragung abgeschlossen ist.

Für Linux-, MacOS- und Unix-Benutzer:

1. Installieren Sie die entsprechende Distribution eines SSH- oder SCP-Clients, z. B. OpenSSH-Client.
2. Öffnen Sie das Terminal und ändern Sie den Pfad, in dem die Konfigurationsdateien gespeichert sind.
3. Geben Sie den folgenden Befehl ein, um die Konfiguration wiederherzustellen:
`scp <Dateiname> <Benutzer>@< IP-Adresse der RMCARD>:`

Anmerkung:

- (1) Die SSH-Einstellung auf der RMCARD muss auf Enabled stehen.
- (2) <Dateiname> ist der Dateiname der Konfigurationsdatei mit dem Standardformat JJJJ_MM_DT_HHMM.txt.
- (3) <user> ist der Benutzername des SSH-Kontos auf der RMCARD.
- (4) Achten Sie darauf, nach der IP-Adresse ein ":" einzufügen.

Zum Beispiel:

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

Hinweis: YYYY_MM_DD_HHMM.txt ist die Konfigurationsdatei, die wiederhergestellt werden soll.

4. Nach der Ausführung des Befehls wird möglicherweise eine Meldung angezeigt, in der Sie gefragt werden, ob Sie dem Host vertrauen. Um fortzufahren, geben Sie innerhalb von 10 Sekunden "y" für Ja ein.
5. Auf dem nächsten Bildschirm geben Sie das RMCARD-Passwort ein. Bitte warten Sie, bis die Fortschrittsanzeige 100% anzeigt. Das System meldet sich automatisch ab und startet neu, nachdem die Übertragung abgeschlossen ist.

SSH-Host-Schlüssel über Secure Copy (SCP) hochladen

Ein SSH HOST Key kann mit Secure Copy Befehlen auf die RMCARD205 hochgeladen werden.

Bitte stellen Sie sicher, dass der hochgeladene Dateiname die Anfangszeichenfolge "ssh_hostkey_" enthält.

Einige Beispiele für akzeptable Dateinamen sind die folgenden:

`ssh_hostkey_sample1.pem`

`ssh_hostkey_1024.pem`

`ssh_hostkey_type100.***`

Beispiel für einen Upload-Prozess

1. Laden Sie das Service Programm PuTTY Secure Copy Client (PSCP) herunter.
2. Die SSH-Host-Schlüsseldatei und das PSCP-Service Programm müssen sich im selben Ordner befinden.
3. Öffnen Sie die Eingabeaufforderung und ändern Sie den Pfad zur SSH-Host-Schlüsseldatei und zum PSCP-Service Programm auf
gerettet.
4. Geben Sie den folgenden Befehl ein
`pscp -scp <Dateiname> <admin_account>@<IP-Adresse der RMCARD>:`
Beispiel: `pscp -scp ssh_hostkey_xxx.xxx cyber@192.168.203.66:`
5. Nach der Ausführung des Befehls wird möglicherweise eine Meldung angezeigt, in der Sie gefragt werden, ob Sie dem Host vertrauen. Bitte geben Sie innerhalb von 10 Sekunden "y" für Ja ein.
6. Geben Sie auf dem nächsten Bildschirm das Admin-Passwort ein. Die Dateiübertragung kann einige Minuten in Anspruch nehmen. Bitte warten Sie, bis die Fortschrittsanzeige 100% anzeigt. Das System meldet sich automatisch ab und startet neu, nachdem die Übertragung abgeschlossen ist.

Host-Schlüssel-Anforderung

SSH, die mit 2048-Bit oder 4096-Bit RSA k erstellt werden

Fehlersuche

Problem	Lösung
Die Remote Management Card kann weder mit Methode 1 noch mit Methode 2 konfiguriert werden.	<ol style="list-style-type: none"> Überprüfen Sie den LED-Status. Es ist normal, wenn die gelbe und die grüne LED beide leuchten. Wenn die grüne LED aus ist: Überprüfen Sie, ob die Remote Management Card richtig im Gerät sitzt und das Gerät mit Strom versorgt wird. Wenn die gelbe LED aus ist: Vergewissern Sie sich, dass die Netzwerkverbindung gut ist. Vergewissern Sie sich, dass sich der verwendete PC im selben lokalen Netzwerk-Subnetz befindet wie das CyberPower-Gerät, mit dem Sie zu kommunizieren versuchen. Stellen Sie sicher, dass der Jumper am Reset-Pin korrekt installiert ist.
Die Remote Management Card kann nicht angefunkt werden	<ol style="list-style-type: none"> Verwenden Sie Methode 1 und/oder Methode 2, um eine korrekte IP-Adresse für die Remote Management Card zu erhalten/einzustellen. Wenn sich der verwendete PC in einem anderen Netzwerk-Subnetz befindet als die Remote Management Card, überprüfen Sie die Einstellung der Subnetzmaske und die IP-Adresse des Gateways.
Den Benutzernamen und das Passwort verloren	Bitte lesen Sie den Abschnitt "Zurücksetzen auf die Werkseinstellungen / Wiederherstellen nach einem verlorenen Passwort".
Standard-Netzwerkeinstellung	IP: 192.168.20.177 Subnetz-Maske: 255.255.255.0 DHCP: Ein
Zugriff auf die Webschnittstelle nicht möglich	<ol style="list-style-type: none"> Stellen Sie sicher, dass Sie die RMCARD anpingen können. Vergewissern Sie sich, dass Sie die richtige URL angeben. Stellen Sie sicher, dass der HTTP/HTTPS-Zugriff aktiviert ist, indem Sie sich über CLI (Telnet oder SSH-Client) bei der Karte anmelden.
SNMP get/set kann nicht ausgeführt werden	SNMPv1: Überprüfen Sie den Community-Namen. SNMPv3: Überprüfen Sie die Konfiguration des Benutzerprofils.
Traps können nicht empfangen werden	<ol style="list-style-type: none"> Stellen Sie sicher, dass die Trap-Typen (SNMPv1/SNMPv3) und der Trap-Empfänger korrekt konfiguriert sind. Stellen Sie sicher, dass die IP-Adresse des Gateways korrekt konfiguriert ist, wenn sich die RMCARD und das NMS in einem anderen Netzwerk befinden.

Konformität Genehmigungen

FCC-Warnung

Dieses Gerät wurde getestet und entspricht den Grenzwerten für ein digitales Gerät der Klasse A gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte sollen einen angemessenen Schutz gegen schädliche Störungen bei der Installation in Wohngebieten bieten. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese ausstrahlen. Wenn es nicht gemäß den Anweisungen installiert und verwendet wird, kann es schädliche Störungen im Funkverkehr verursachen. Der Betrieb dieses Geräts in einem Wohngebiet kann schädliche Störungen verursachen, die der Benutzer auf eigene Kosten beheben muss.

Eventuell erforderliches Sonderzubehör muss in der Gebrauchsanweisung angegeben werden.

Dieses Gerät erfüllt die Anforderungen von Teil 15 der FCC-Bestimmungen. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Interferenzen verursachen, und (2) dieses Gerät muss alle empfangenen Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb verursachen können.

Das digitale Gerät der Klasse A erfüllt alle Anforderungen der kanadischen Verordnung über störanfällige Geräte (Canadian Interference-Causing Equipment Regulation).

Dieses numerische Gerät der Klasse A erfüllt die Anforderungen der kanadischen Stromverbraucher-Verordnung (Reglement sur le materiel brouilleur du Canada).

Europäische Union

Dies ist ein Produkt der Klasse A. In einer häuslichen Umgebung kann dieses Produkt Funkstörungen verursachen; in diesem Fall kann der Benutzer aufgefordert werden, angemessene Maßnahmen zu ergreifen.



WARNUNG: Dieses Produkt kann Sie Chemikalien aussetzen, einschließlich Styrol, das dem Staat Kalifornien als krebserregend bekannt ist, und Bisphenol-A, von dem bekannt ist, dass es für den Staat Kalifornien, Geburtsfehler oder andere Fortpflanzungsschäden zu verursachen. Weitere Informationen finden Sie unter www.P65Warnings.ca.gov.

Anhang 1 : IP-Adressen-Identifizierung für CyberPower Remote Management Card

Übersicht

Alle Geräte in einem Computernetz müssen eine IP-Adresse haben. Die IP-Adresse eines jeden Geräts ist eindeutig. Dieselbe Adresse kann nicht zweimal verwendet werden. Um der CyberPower Remote Management Card eine IP-Adresse zuzuweisen, müssen Sie den Bereich der verfügbaren IP-Adressen bestimmen und dann eine ungenutzte IP-Adresse auswählen, die Sie der Remote Management Card zuweisen.

Hinweis: Möglicherweise müssen Sie sich an Ihren Netzwerkadministrator wenden, um eine verfügbare IP-Adresse zu erhalten.

Verfahren zur Ermittlung einer IP-Adresse:

1. Suchen Sie das Subnetz der CyberPower Remote Management Card.

Eine Möglichkeit, den Bereich möglicher IP-Adressen zu ermitteln, besteht darin, die Netzwerkkonfiguration auf einer Arbeitsstation anzuzeigen. Klicken Sie auf [Start] und wählen Sie [Ausführen]. Geben Sie "command" in das geöffnete Feld ein und klicken Sie auf [OK]. Geben Sie in der Eingabeaufforderung "ipconfig /all" ein und drücken Sie [Enter]. Der Computer zeigt nun die unten aufgeführten

Netzwerkinformationen an:

```
Ethernet-Adapter
Verbindungsspezifischer DNS-Suffix.....: xxxx.com
Beschreibung.....: D-Link DE220 ISA PnP LAN-Adapter
Physische Adresse.....: 00-80-C8-DA-7A-C0
DHCP Aktiviert.....: Ja
Autokonfiguration Aktiviert...: Ja
IP-Adresse.....: 192.168.20.102
Teilnetzmaske.....: 255.255.255.0
Standard-Gateway.....: 192.168.20.1
DHCP-Server.....: 192.168.20.1
DNS-Server.....: 211.20.71.202
168.95.1.1
```

2. Wählen Sie eine IP-Adresse für die CyberPower Remote Management Card

Vergewissern Sie sich, dass die IP-Adressen für den Computer und die Fernwartungskarte zum selben Subnetz gehören. Anhand der obigen Netzwerkinformationen könnte die mögliche IP-Adresse für die Fernwartungskarte 192.168.20.* lauten (* steht im Folgenden für eine beliebige Zahl zwischen 1 und 255). Wenn die Subnetzmaske 255.255.0.0 lautet, könnte die IP-Adresse für die Fernmanagement-Karte 192.168.*.* lauten, um das gleiche Subnetz wie der Computer zu erreichen.

Um sicherzustellen, dass keine anderen Geräte mit dem Netzwerk verbunden sind, die dieselbe IP-Adresse verwenden, führen Sie "Ping 192.168.20.240" an der DOS-Eingabeaufforderung aus, wenn die IP-Adresse, die Sie einstellen möchten, 192.168.20.240 lautet. Wenn die Antwort wie unten dargestellt ist, wird die IP-Adresse höchstwahrscheinlich nicht verwendet und kann für die CyberPower Remote Management Card verfügbar sein.

```
Pinging 192.168.20.240 mit 32 Byte Daten:
```

```
Anfrage wurde abgebrochen.
```

```
Anfrage wurde abgebrochen.
```

```
Anfrage wurde abgebrochen.
```

```
Anfrage wurde abgebrochen.
```

Wenn die Antwort wie unten angezeigt wird, ist die IP-Adresse in Gebrauch. Versuchen Sie eine andere IP-Adresse, bis eine verfügbare Adresse gefunden wird.

```
Pinging 192.168.20.240 mit 32 Byte Daten:
```

```
Antwort von 192.168.20.240: bytes=32 time<10ms TTL=64
```

```
Antwort von 192.168.20.240: bytes=32 time<10ms TTL=64
```

```
Antwort von 192.168.20.240: bytes=32 time<10ms TTL=64
```

```
Antwort von 192.168.20.240: bytes=32 time<10ms TTL=64
```

Anhang 2 : Wie man ein RMCARD-Benutzerkonto in Authentifizierungsservern konfiguriert

RADIUS

1. Fügen Sie dem RADIUS-Wörterbuch ein neues Attribut als Cyber-Anbieter hinzu:

3808 - Verkäufer

2. Fügen Sie zwei neue spezifische Attribute zur RADIUS-Server-Schnittstelle unter dem Anbieter hinzu:

(1) **Cyber-Service-Typ** (ganzzahlige Variable)

Der Cyber-Service-Typ kann drei ganzzahlige Parameterwerte annehmen:

1 - Verwalter

2 - Betrachter

3 - Auslass Benutzer

(2) **Cyber-Outlets** (String-Variable)

Cyber-Outlets können eine Zeichenkette akzeptieren, die die Nummern der Ausgänge beschreibt. Mit diesem Attribut kann der Benutzer auf die bezeichneten Ausgänge zugreifen und sie kontrollieren. Beispiel: Cyber-Outlets="1,2,5" ermöglicht dem Benutzer die Steuerung der Ausgänge 1, 2 und 5.

Das Beispiel der Wörterbuchdatei:

```
VENDOR Cyber 3808
BEGIN-VENDOR Cyber
ATTRIBUTE Cyber-Service-Typ 1 Ganzzahl
ATTRIBUTE Cyber-Outlets 2 string
VALUE Cyber-Service-Typ Admin 1
VALUE Cyber-Service-Type Viewer 2
VALUE Cyber-Service-Typ Steckdose 3
ENDVERKÄUFER Cyber
```

LDAP und Windows AD

Fügen Sie eines der nachstehenden Attribute zur **Beschreibung** auf der OpenLDAP- oder Windows AD-Schnittstelle hinzu, um den Typ des Benutzerkontos und die Authentifizierung anzugeben:

1. **cyber_admin** (Verwalter)

2. **cyber_viewer** (Betrachter)

3. **cyber_outlet="string"** (Outlet-Benutzer)

Die in cyber_outlet eingegebene Zeichenfolge gibt an, auf welche Ausgänge der Outlet-Benutzer zugreifen und diese steuern kann. Zum Beispiel erlaubt cyber_outlet="1,2,5" dem Benutzer die Kontrolle über die Ausgänge 1, 2 und 5.

Anhang 3 : USV Firmware Upgrade

Sie können die "Firmware-Version" auf der Seite **[USV->Information]** auf der Web-Benutzeroberfläche der RMCARD überprüfen.

Methode 1: Verwendung der Webschnittstelle

1. Schalten Sie die USV über den [USV->Hauptschalter] aus.
2. Gehen Sie über [USV->Informationen->Firmware-Version] zur Seite Firmware-Version.
3. Laden Sie die USV-Firmware hoch, indem Sie auf Aktualisieren und dann auf Datei auswählen klicken, um den Speicherort der USV-Firmwaredatei auszuwählen.
4. Klicken Sie auf Absenden, um die Aktualisierung durchzuführen. Nach Abschluss der Aktualisierung wird ein Fenster mit der Meldung "Upgrade erfolgreich" angezeigt.
5. Schalten Sie die USV über [USV->Hauptschalter] ein.

Methode 2: FTP-Befehl verwenden

Der FTP-Service muss aktiviert sein, bevor Sie versuchen, ein Firmware-Upgrade durchzuführen.

Führen Sie die folgenden Schritte aus, um die Firmware per FTP zu aktualisieren:

1. Schalten Sie die USV aus.
2. Entpacken Sie die Update-Datei nach "C:\".
3. Öffnen Sie ein Fenster der Eingabeaufforderung
4. Melden Sie sich bei der CyberPower Remote Management Card mit dem FTP-Befehl an und geben Sie in die Eingabeaufforderung ein:
 - (1) ftp
 - (2) ftp > öffnen
 - (3) An [aktuelle IP-Adresse der RMCARD] [Port]; EX: An 192.168.22.126 21
 - (4) Geben Sie den BENUTZERNAMEN und das PASSWORT ein (das gleiche wie das Administratorkonto in der Web-Benutzeroberfläche, siehe Seite 6 für die werkseitigen Standardeinstellungen)
5. Laden Sie die Datei hoch, geben Sie sie ein:

```
ftp > bin
ftp > put XXX.bin
```
6. Das Hochladen ist nun abgeschlossen, geben Sie ein:

```
ftp > Beenden
```
7. Schalten Sie die USV ein.

Hinweis: 1. es kann etwa 5 Minuten dauern, bis die Aktualisierung abgeschlossen ist. Bitte führen Sie während der Aktualisierung der USV-Firmware keine anderen Aktionen durch und ziehen Sie die RMCARD nicht heraus.

Hinweis: (2) Der Aktualisierungsfortschritt kann nur im Webinterface angezeigt werden.

Hinweis: 3. wenn Sie nach dem Hochladen der USV-Firmware-Datei über die Webschnittstelle die Meldung "Uploaded an invalid USV firmware" sehen, überprüfen Sie bitte:

- (1) Die Datei ist eine Binärdatei für USV-Firmware.
- (2) Die USV-Firmware-Datei unterstützt das USV-Modell.

Anhang 4: Software-Unterstützung

PowerPanel® Business Remote wird verwendet, um ein sanftes Herunterfahren des Betriebssystems durchzuführen, wenn es durch eine USV/ATS-PDU mit einer installierten Remote Management Card geschützt ist. Die PowerPanel® Business-Software ist auf der offiziellen Website von CyberPower Systems erhältlich. Bitte besuchen Sie www.CyberPower.com und gehen Sie zum kostenlosen Download in den Software-Bereich.

Kommunizieren Sie mit PowerPanel® Business Remote

Die Remote-Verwaltungskarte muss sich bei PowerPanel® Business Remote über einen gemeinsamen Geheimcode authentifizieren, wie in Abbildung 11 dargestellt.

Hinweis: Die Standardgeheimnisformel lautet "powerpanel.encryption.key".

The screenshot displays the 'USV Fernverwaltung' web interface. At the top, it shows the user is logged in as an administrator from IP 192.168.188.100, with options to log out and a German flag. The navigation menu includes 'Übersicht', 'USV', 'Protokoll', 'System' (highlighted with a red box), and 'Hilfe'. The left sidebar contains a menu with 'Allgemein', 'Sicherheit', 'Management' (highlighted with a red box), 'Lokal Konto', 'RADIUS Konfiguration', 'LDAP Konfiguration', 'Überwachung Sitzungen', 'Netzwerkdienst', 'Benachrichtigung', 'Reset/Neustart', and 'Über'. The main content area is titled 'Management' and contains the following sections:

- Anmeldung Authentifizierung**: Radio buttons for 'Lokal Konto' (selected), 'RADIUS , Lokal Konto', 'Nur RADIUS', 'LDAP , Lokal Konto', and 'Nur LDAP'.
- Software Authentifizierung**: A text input field for 'Geheimes Kennwort' containing 'powerpanel.encryption.key' with a character count of '[1-31 zeichen]'.
- Admin Manager IP**: Two rows, each with a checked 'Aktiviert' checkbox and an IP input field set to '0.0.0.0'.
- Betrachter Manager IP**: Two rows, each with a checked 'Aktiviert' checkbox and an IP input field set to '0.0.0.0'.

At the bottom of the configuration area, there are two buttons: 'Übernehmen' and 'Zurücksetzen'.

Abbildung 11. RMCARD System>Authentifizierung Web UI.



Hinweis: Die Software PowerPanel® Business unterstützt das automatische Herunterfahren von VMware ESX/ESXi-Hosts sowie von anderen Virtualisierungsplattformen wie Microsoft Hyper-V und Citrix.

IP-Adresse für Linux-Betriebssystem abrufen

Die Anweisungen im Abschnitt "Konfigurieren Sie die IP-Adresse für die CyberPower Remote Management Card" gelten für Windows-Betriebssysteme. Bei Linux-Betriebssystemen verwenden Sie bitte die PowerPanel® Business Remote-Software, um die IP-Adresse zu scannen und zu erhalten. Gehen Sie dazu auf der Weboberfläche von PowerPanel® Business Remote zu **[Power->Konfiguration]**, wie in Abbildung 12 dargestellt. Weitere Informationen finden Sie im PowerPanel® Business User's Manual.

REMOTE

DASHBOARD **POWER CONFIGURATION** SETTING ▾ REPORTING HELP

POWER CONFIGURATION

Page level notification relative to page content.

Power Supply Configuration

Redundant Power Supply Policy

Power Supply #1

Device Type

Hover over an IP Address for more device information. ✕

UPS Address

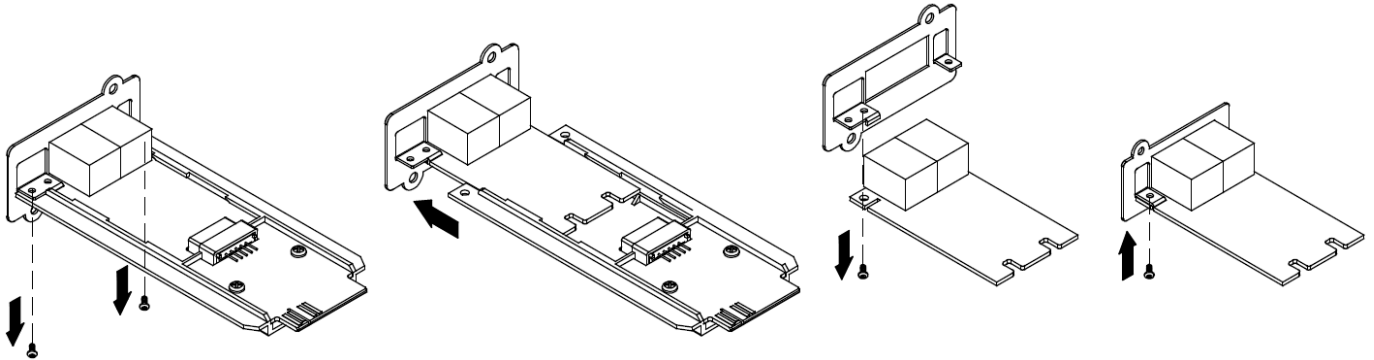
UPS Outlet

Communication established.

Abbildung 12. Die Weboberfläche von PowerPanel® Business Remote.

Anhang 5: RMCARD Adapter Anleitung

Entfernen Sie den Adapter, um eine RMCARD305 in eine RMCARD205 umzuwandeln



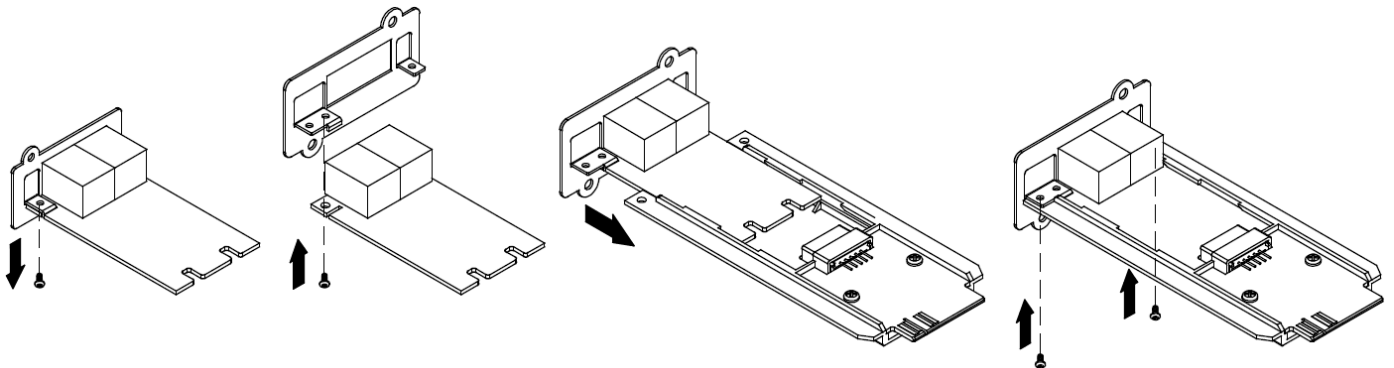
Schritt 1. Entfernen Sie die beiden Schrauben am Adapter, mit denen die Karte befestigt ist.

Schritt 2. Entfernen Sie die Karte aus dem Adapter.

Schritt 3. Entfernen Sie die Schraube, mit der die Frontplatte der RMCARD305 an der Karte befestigt ist.

Schritt 4. Bringen Sie die Frontplatte der RMCARD205 an der Karte an.

Fügen Sie den Adapter hinzu, um eine RMCARD205 in eine RMCARD305 umzuwandeln



Schritt 1. Entfernen Sie die Schraube, mit der die Frontplatte an der Karte befestigt ist, und nehmen Sie die Frontplatte der RMCARD205 ab.

Schritt 2. Schrauben Sie die Frontplatte der RMCARD305 auf die Karte.

Schritt 3. Stellen Sie die Karte in den Adapter ein. Vergewissern Sie sich, dass die Karte sicher an ihrem Platz sitzt.

Schritt 4. Befestigen Sie die Karte mit den beiden Adapterschrauben.

Hinweis: Das RMCARD Adapter Kit ist nicht im Lieferumfang der RMCARD205 enthalten. Bitte kontaktieren Sie CyberPower für Bestellinformationen oder technischen Support.

Hinweis: RMCARD205 ist für den 43x18mm (1.69x0.71inch) SNMP-Kartenerweiterungsport der CyberPower PR, OR und 1-3kVA OL Serie USV, und ATS PDU konzipiert.

RMCARD305 ist für die 57x23mm (2.24x0.91inch) SNMP-Kartenerweiterung konzipiert
Port der CyberPower-USV-Serie OL6-10kVA.



CyberPower

[CyberPower | USV Systeme, PDU, Überspannungsschutz |
Professionelle Stromversorgung Lösungen](#)

CyberPower Systems GmbH
Edisonstr. 16
85716 Unterschleissheim
Germany

T: +49-89-1 222 166 -0 F: +49-89-1 222 166 -29

E: sales@cyberpower.de

Web: www.cyberpower.de

[Home | CyberPower Wiki \(cyberpowersystems.de\)](#)

