Remote Netzwerk-Karte

RMCARD400

Security Guide

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

Einführung

Dieses Dokument bietet einen Leitfaden für die Sicherheitsfunktionen für die Firmware-Version V1.0.4 und höher der RMCARD400.
Die folgenden Teile sind enthalten.

- Benutzerkonto-Typen
- Authentifizierung von Benutzerkonten
- HyperText Transfer Protocol (HTTP) HTTP und HyperText Transfer Protocol over Secure Sockets Layers (HTTPS)
- SNMPv1 und SNMPv3
- Telnet und Secure SHell v2 (SSH)
- Dateiübertragungsprotokolle (FTP) und Secure CoPy (SCP)
- Anschluss für Kommunikation

Benutzerkonto-Typen

Die RMCARD400 bietet zwei Arten von Benutzerkonten für die Anmeldung.

- Administrator: Zugriff auf alle Elemente der Webschnittstelle und alle Befehle der Befehlszeilenschnittstelle.
- Viewer: Zugriff auf die Lesefunktionen der Webschnittstelle.

Anmerkung:

1. Bei der ersten Anmeldung wird der Benutzer aufgefordert, einen neuen Benutzernamen und ein neues Passwort festzulegen.
2. Das Administratorkonto wird auch für die FTP-Anmeldung, die CLI-Schnittstelle, das Power Device Network Utility und das Upgrade and Configuration Utility verwendet.
3. Das CyberPower Switched PDU-Gerät verfügt über ein zusätzliches "Steckdosenbenutzerkonto". Für mehr Kontoinformationen entnehmen Sie bitte der Hilfedatei des Geräts.

Authentifizierung von Benutzerkonten

Die RMCARD400 ermöglicht die Authentifizierung von lokalen und entfernten Benutzerkonten.

- **Lokal**: der Benutzername und das Passwort werden von RMCARD400 verwaltet und überprüft.

- **Remote**: Der Benutzername und das Passwort werden von einem zentralen RADIUS- (Remote Authentication Dial-In User Service) oder LDAP-Server (Lightweight Directory Access Protocol) verwaltet und überprüft.

Konfigurieren Sie die Authentifizierungsmethode **auf der Web-Seite von [**System->Sicherheit-> Verwaltung].

Einstellungen	Definition
Lokales Konto	Verwenden Sie zur Anmeldung die Einstellungen des lokalen Kontos Administrator oder Viewer.
RADIUS, Lokales Konto	Verwenden Sie die RADIUS-Konfigurationseinstellungen für die Anmeldung. Wenn die RADIUS-Authentifizierung fehlschlägt, werden die Einstellungen des lokalen Kontos für die Anmeldung verwendet.
Nur RADIUS	Verwenden Sie die RADIUS-Konfigurationseinstellungen, um sich anzumelden.
LDAP, Lokales Konto	Verwenden Sie die LDAP-Konfigurationseinstellungen für die Anmeldung. Wenn die LDAP-Authentifizierung fehlschlägt, werden die Einstellungen des lokalen Kontos für die Anmeldung verwendet.
Nur LDAP	Verwenden Sie die LDAP-Konfigurationseinstellungen für die Anmeldung.

- Die "Admin/Viewer Manager IP" definiert die zulässige Anmelde-IP für den Zugriff auf RMCARD400. Folgende Beispiele:
  - Wenn Sie einer beliebigen IP-Adresse den Zugang zur RMCARD400 erlauben, können Sie 0.0.0.0 oder 255.255.255.255 einstellen.
  - Wenn Sie jeder IP mit dem Subnetz 192.168.0.0 den Zugriff auf RMCARD400 erlauben, können Sie 192.168.20.0/16 einstellen.

Lokales Konto

Konfigurieren Sie die Parameter des lokalen Kontos auf der Seite **[System->Sicherheit->Lokales Konto].**

- Die maximale Länge des Benutzernamens und des Passworts für den Administrator beträgt 64 Zeichen.
- Die maximale Länge des Benutzernamens und des Passworts für den Viewer beträgt 64 Zeichen.

RADIUS

Wenn sich ein Benutzer bei der RMCARD anmeldet, wird eine Authentifizierungsanfrage an den RADIUS-Server gesendet, um die Berechtigungsstufe des Benutzers zu bestimmen, wenn die RADIUS-Funktion aktiviert ist.

Unterstützte RADIUS-Server

RMCARD400 unterstützt FreeRADIUS v2.x 、Microsoft Server 2008、2012、2019 Network policy Server (NPS). Andere RADIUS können funktionieren, sind aber nicht vollständig getestet worden.

RMCARD400 konfigurieren

Konfigurieren Sie die RADIUS-Parameter auf der Web-Seite [System->Sicherheit->RADIUS-Konfiguration]**.**

Einstellungen	Definition
Server-IP	Die IP-Adresse/Domäne des RADIUS-Servers.
Gemeinsames Geheimnis	Das gemeinsame Geheimnis des RADIUS-Servers.
Server-Anschluss	Der vom RADIUS-Server verwendete UDP-Port.
Test Einstellung	Testen Sie den RADIUS-Server mit den Einstellungen für Benutzernamen und Passwort. Wenn die Authentifizierung erfolgreich ist, werden die Einstellungen gespeichert.
Test überspringen	Speichern Sie die RADIUS-Servereinstellungen ohne Test.

Konfigurieren Sie den RADIUS-Server

Sie müssen Ihren RADIUS-Server so konfigurieren, dass er mit RMCARD400 funktioniert.

Beispiel:

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

Wenn sich ein Benutzer bei der RMCARD anmeldet, wird eine Authentifizierungsanfrage an den LDAP-Server gesendet, um die Berechtigungsstufe des Benutzers zu bestimmen, wenn die LDAP-Funktion aktiviert ist.

Unterstützte LDAP-Server
RMCARD400 unterstützt OpenLDAP v2.x、Windows AD Server 2008、2012、2019.

RMCARD400 konfigurieren
Konfigurieren Sie die LDAP-Parameter auf der Webseite von [System->Sicherheit->LDAP-Konfiguration] **.**

Artikel	Definition
LDAP-Server	
LDAP-Server	Die IP-Adresse/Domäne des LDAP-Servers.
LDAP SSL	Aktivieren Sie die Kommunikation mit dem LDAP-Server über LDAPS.
Hafen	Der vom LDAP(S)-Server verwendete TCP-Port.
Benutzerbasis DN	Der Basis-DN des LDAP-Servers.
Login-Attribut	Das Login-Attribut des LDAP-Benutzereintrags (zum Beispiel: cn oder uid).
LDAP-Authentifizierung	
Authentifizierungsmodus	Gibt die Methode an, die für die Authentifizierung verwendet werden soll. • Anonym: Bindungsanforderung unter Verwendung der einfachen Authentifizierung mit einem Bindungs-DN von Null-Länge und einem Passwort von Null-Länge. • Akkreditierter Benutzer: Bindungsanfrage unter Verwendung der einfachen Authentifizierung mit einem Bind-DN und einem Bindungskennwort. • Nach Anmeldebenutzer: Bindungsanforderung mit einfacher Authentifizierung mit einem Benutzer-Basis-DN und einem Anmeldekennwort.
LDAP-Autorisierung	
Autorisierungsmodus	Gibt die Methode an, die für die Autorisierung verwendet werden soll.

	• Nach Benutzerattribut: Bestimmen Sie die Zugriffsstufe nach Benutzerattribut und Benutzerattributwert. • Nach Gruppe: Bestimmen Sie die Zugriffsebene nach Gruppe, die DN-Informationen wie den folgenden Gruppen-Basis-DN, das Gruppenattribut und den Gruppenattributwert sucht.
LDAP-Server-Typ	
Generischer LDAP-Server	Wählen Sie als LDAP-Servertyp OPENLDAP.
Aktives Verzeichnis	Wählen Sie als LDAP-Servertyp Windows AD.
AD-Bereich	Die AD-Domäne des Active Directory-Servers.
LDAP-Test	
Test Einstellung	Testen Sie den LDAP(S)-Server mit den Einstellungen für Benutzernamen und Kennwort. Wenn die Authentifizierung erfolgreich ist, werden die Einstellungen gespeichert.
Test überspringen	Speichern Sie die Einstellungen des LDAP(S)-Servers ohne Test.

Konfigurieren Sie den LDAP-Server

Sie müssen Ihren RADIUS-Server so konfigurieren, dass er mit RMCARD400 funktioniert.

Fügen Sie eines der folgenden Attribute zur **Beschreibung** auf dem **LDAP-Server** 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.

Sicherheitsmerkmale

Die RMCARD400 bietet grundlegende Sicherheit und hohe Sicherheit für die Zugriffsprotokolle. Das Basissicherheitsprotokoll überträgt die Authentifizierung und Daten mit Klartext ohne Verschlüsselung, und das Hochsicherheitsprotokoll überträgt die Authentifizierung und Daten mit Verschlüsselung. Es wird empfohlen, das Hochsicherheitsprotokoll zu wählen und zu aktivieren, um auf das Basissicherheitsprotokoll zuzugreifen und es zu deaktivieren.

Zusammenfassung der Protokolle

Web-Server

HTTP	HTTPS
Grundlegender Sicherheitszugang • Nutzername und Passwort. (Übertragung im Klartext ohne Verschlüsselung) • Konfigurierbarer Server Port • Dienst kann aktiviert oder deaktiviert werden • Zugänglicher IP-Filter	Hochsicherheitszugang • TLS-Unterstützung. • Nutzername und Passwort. (TLS-Verschlüsselung übertragen) • Konfigurierbarer Server Port. • Dienst kann aktiviert oder deaktiviert werden • Zugänglicher IP-Filter

SNMP-Dienst

SNMPv1	SNMPv3
Grundlegender Sicherheitszugang • Community-Name (Übertragung im Klartext ohne Verschlüsselung) • Dienst kann aktiviert oder deaktiviert werden • 4 Zugang Gemeinschaft • Zugänglicher IP-Filter • Lese-/Schreib-/Verboten-Fähigkeit für die spezifische Gemeinschaft	Hochsicherheitszugang • 4 Benutzerprofile • Authentifizierung durch eine Authentifizierungspassphrase mit SHA- oder MD5-Hash-Algorithmus • Verschlüsselung durch eine private Passphrase mit AES- oder DES-Verschlüsselungsalgorithmus • Zugänglicher IP-Filter

Befehlszeilenschnittstelle

Telnet	SSH
Grundlegender Sicherheitszugang • Nutzername und Passwort. (Übertragung im Klartext ohne Verschlüsselung) • Konfigurierbarer Server Port	Hochsicherheitszugang • Nutzername und Passwort. (Übertragung mit SSH-Verschlüsselung) • Konfigurierbarer Server Port

• Dienst kann aktiviert oder deaktiviert werden • Zugänglicher IP-Filter	• Dienst kann aktiviert oder deaktiviert werden • Zugänglicher IP-Filter

Dateiübertragungsprotokoll

FTP	SCP
Grundlegender Sicherheitszugang • Nutzername und Passwort. (Übertragung im Klartext ohne Verschlüsselung) • Konfigurierbarer Server Port • Dienst kann aktiviert oder deaktiviert werden	Hochsicherheitszugang • Nutzername und Passwort. (Übertragung mit SSH-Verschlüsselung) • Konfigurierbarer Server Port • SCP ist aktiviert, wenn SSH aktiviert ist • Zugänglicher IP-Filter

Web-Server

HTTP und HTTPS

HyperText Transfer Protocol (HTTP) bietet einen grundlegenden Sicherheitszugang mit Benutzernamen、Passwort、konfigurierbarem Port und zugänglicher IP, aber der Benutzername、Passwort und die übertragenden Daten sind nicht verschlüsselt. HyperText Transfer Protocol over Secure Sockets Layers (HTTPS) überträgt den Benutzernamen, das Passwort und die Daten verschlüsselt und bietet eine Authentifizierung von RMCARD400 über digitale Zertifikate.

Konfigurieren Sie die HTTP/HTTPS-Parameter auf der Web-Seite von **[System->Netzwerkdienst->Webdienst].**

Artikel	Definition
Zugang	
Zugriff zulassen	Aktivieren Sie den Zugriff auf den HTTP- oder HTTPS-Dienst. HTTPS unterstützt die folgende Liste von Verschlüsselungsalgorithmen: • AES (256/128 Bits) • Kamelie (256/128 Bits) • DES (168 Bits)
Http-Einstellungen	
Http-Anschluss	Der TCP/IP-Port für das Hypertext Transfer Protocol (HTTP) (standardmäßig 80)
Https-Einstellungen	
Https-Anschluss	Der TCP/IP-Port des Hypertext Transfer Protocol Secure (HTTPS) (standardmäßig 443)

Zertifikat Status	• Gültiges Zertifikat (oder ungültiges Zertifikat): Klicken Sie hier, um detaillierte Informationen zum Zertifikat anzuzeigen. • Zertifikat hochladen: Klicken Sie auf , um ein Zertifikat hochzuladen und das aktuelle zu ersetzen.

Anmerkung: 1. Das Format des hochgeladenen digitalen Zertifikats muss ein Standard-PEM (Privacy Enhanced Mail) sein.

2. RMCARD400 unterstützt Transport Layer Sicherheit (TLS) V1.2 und V1.3 .

Nachfolgend ein Beispiel für die Erstellung des Zertifikats mit OpenSSL und das Hochladen des Zertifikats.

1. Erstellen Sie einen Ordner "CA" und kopieren Sie openssl.cnf dorthin.

```
kevin@ubuntu:~$ mkdir CA
kevin@ubuntu:~$ cd CA
kevin@ubuntu:~/CA$ sudo cp /usr/lib/ssl/openssl.cnf ./
kevin@ubuntu:~/CA$ ls -l
total 12
-rw-r--r-- 1 root root 10845 Sep  4 17:03 openssl.cnf
kevin@ubuntu:~/CA$
```

2. Geben Sie "openssl genrsa -des3 -out rootca.key 2048" und das Passwort des Schlüssels ein.

```
kevin@ubuntu:~/CA$ openssl genrsa -des3 -out rootca.key 2048
Generating RSA private key, 2048 bit long modulus
..............+++
.....................................+++
e is 65537 (0x10001)
Enter pass phrase for rootca.key:
Verifying - Enter pass phrase for rootca.key:
kevin@ubuntu:~/CA$
```

3. Geben Sie "openssl req -new -key rootca.key -out rootca.req" ein und geben Sie die Informationen des RootCA-Zertifikats ein.

```
kevin@ubuntu:~/CA$ openssl req -new -key rootca.key -out rootca.req
Enter pass phrase for rootca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Minnesota
Locality Name (eg, city) []:shakopee
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cyberpower
Organizational Unit Name (eg, section) []:firmware
Common Name (e.g. server FQDN or YOUR name) []:wr.frdistilling.com
Email Address []:test@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
kevin@ubuntu:~/CA$ _
```

4. Geben Sie "openssl x509 -req -days 7305 -sha1 -extfile openssl.cnf -extensions v3_ca -signkey rootca.key -in rootca.req -out rootca.crt" ein, um das RootCA-Zertifikat zu erstellen.

```
kevin@ubuntu:~/CA$ openssl x509 -req -days 3650 -sha1 -extfile openssl.cnf -extensions v3_ca -signke
y rootca.key -in rootca.req -out rootca.crt
Signature ok
subject=/C=US/ST=Minnesota/L=shakopee/O=cyberpower/OU=firmware/CN=wr.frdistilling.com/emailAddress=t
est@gmail.com
Getting Private key
Enter pass phrase for rootca.key:
kevin@ubuntu:~/CA$ ls -l
total 24
-rw-r--r-- 1 root  root  10845 Sep  4 17:03 openssl.cnf
-rw-rw-r-- 1 kevin kevin  1456 Sep  4 17:15 rootca.crt
-rw-rw-r-- 1 kevin kevin  1743 Sep  4 17:06 rootca.key
-rw-rw-r-- 1 kevin kevin  1074 Sep  4 17:12 rootca.req
kevin@ubuntu:~/CA$ _
```

5. Geben Sie "openssl genrsa -out server.key 2048" ein, um den Serverschlüssel zu erstellen.

```
kevin@ubuntu:~/CA$ openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.........+++
............+++
e is 65537 (0x10001)
kevin@ubuntu:~/CA$ _
```

6. Geben Sie "openssl req -new -key server.key -out server.req" ein und geben Sie die Informationen zum Zertifikat ein.

```
kevin@ubuntu:~/CA$ openssl req -new -key server.key -out server.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Minnesota
Locality Name (eg, city) []:shakopee
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cyberpower
Organizational Unit Name (eg, section) []:firmware
Common Name (e.g. server FQDN or YOUR name) []:chups01.wr.frdistilling.com
Email Address []:test@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
kevin@ubuntu:~/CA$ ls -l
total 32
-rw-r--r-- 1 root  root  10845 Sep  4 17:03 openssl.cnf
-rw-rw-r-- 1 kevin kevin  1456 Sep  4 17:15 rootca.crt
-rw-rw-r-- 1 kevin kevin  1743 Sep  4 17:06 rootca.key
-rw-rw-r-- 1 kevin kevin  1074 Sep  4 17:12 rootca.req
-rw-rw-r-- 1 kevin kevin  1679 Sep  4 17:18 server.key
-rw-rw-r-- 1 kevin kevin  1082 Sep  4 17:21 server.req
kevin@ubuntu:~/CA$
```

7. Geben Sie "openssl x509 -req -days 3650 -sha1 extfile openssl.cnf -extensions v3_req -CA rootca.crt -CAkey rootca.key -CAserial rootca.srl -CAcreateserial -in server.req -out server.crt" ein, um das Serverzertifikat zu erstellen.

```
kevin@ubuntu:~/CA$ openssl x509 -req -days 3650 -sha1 -extfile openssl.cnf -extensions v3_req -CA ro
otca.crt -CAkey rootca.key -CAserial rootca.srl -CAcreateserial -in server.req -out server.crt
Signature ok
subject=/C=US/ST=Minnesota/L=shakopee/O=cyberpower/OU=firmware/CN=chups01.wr.frdistilling.com/emailA
ddress=test@gmail.com
Getting CA Private Key
Enter pass phrase for rootca.key:
kevin@ubuntu:~/CA$
```

8. Sie sehen dann die folgenden drei Dateien.

```
-rw-r--r-- 1 root  root  10845 Sep  4 17:03 openssl.cnf
-rw-rw-r-- 1 kevin kevin  1456 Sep  4 17:15 rootca.crt
-rw-rw-r-- 1 kevin kevin  1743 Sep  4 17:06 rootca.key
-rw-rw-r-- 1 kevin kevin  1074 Sep  4 17:12 rootca.req
-rw-rw-r-- 1 kevin kevin    17 Sep  4 17:26 rootca.srl
-rw-rw-r-- 1 kevin kevin  1395 Sep  4 17:26 server.crt
-rw-rw-r-- 1 kevin kevin  1679 Sep  4 17:18 server.key
-rw-rw-r-- 1 kevin kevin  1082 Sep  4 17:21 server.req
kevin@ubuntu:~/CA$
```

9. Erstellen Sie eine Datei mit dem Namen RMC.crt und fügen Sie den Inhalt der drei Dateien in diese Datei ein.

10. Laden Sie die Datei "RMC.crt" auf der Webseite von **[System->Netzwerkdienst->Webdienst]** hoch**.**

SNMPv1 und SNMPv3

SNMPv1 bietet einen grundlegenden Sicherheitszugang mit Community、Access type und zugänglicher IP, aber die Community、 und die übermittelten Daten werden nicht verschlüsselt. SNMPv3 überträgt Daten mit Verschlüsselung und bietet Authentifizierung mit Passphrase.

Konfigurieren Sie die SNMPv1-Parameter auf der Webseite von **[System->Netzwerkdienst->SNMPv1-Dienst].**

Artikel	Definition
SNMPv1-Dienst	
Zugriff zulassen	Setzen Sie den SNMPv1-Dienst entweder auf Aktivieren oder Deaktivieren.
SNMPv1 Zugriffskontrolle	
Gemeinschaft	Der Name, der für den Zugriff auf diese Gemeinschaft von einem Netzwerkmanagementsystem (NMS) aus verwendet wird. Das Feld muss zwischen 1 und 15 Zeichen lang sein.
IP-Adresse	Der NMS-Zugang kann durch Eingabe einer bestimmten IP-Adresse oder einer IP-Netzwerk-Subnetzmaske eingeschränkt werden. Es gelten die folgenden Regeln für Subnetzmasken: • 192.168.20.255: Zugriff nur durch ein NMS auf das Segment 192.168.20. • 192.255.255.255: Zugriff nur durch ein NMS im Segment 192. • 0.0.0.0 (die Standardeinstellung) oder 255.255.255.255: Zugriff durch jedes NMS auf jedem Segment.
Zugangstyp	Die zulässige Aktion für das NMS über die Community und die IP-Adresse. • Nur lesen: GET-Befehl jederzeit erlaubt; SET-Befehl eingeschränkt. • Schreiben/Lesen: GET-Befehl jederzeit zulässig; SET-Befehl jederzeit zulässig, es sei denn, eine Benutzersitzung ist aktiv. • Verboten: Die Befehle GET und SET sind eingeschränkt.

Konfigurieren Sie die SNMPv3-Parameter auf der Webseite von **[System->Netzwerkdienst->SNMPv3-Dienst].**

Artikel	Definition
SNMPv3-Dienst	
Zugriff zulassen	Setzen Sie den SNMPv3-Dienst entweder auf Aktivieren oder Deaktivieren.
SNMPv3-Zugangskontrolle	
Name des Benutzers	Der Name zur Identifizierung des SNMPv3-Benutzers. Das Feld muss zwischen 1 und 31 Zeichen lang sein.

Authentifizierungsprotokoll	Der Hash-Typ für die Authentifizierung. MD5/SHA kann ausgewählt werden.
Authentifizierungs-Passwort	Das Passwort, mit dem der für die Authentifizierung verwendete Schlüssel generiert wird. Das Feld muss zwischen 16 und 31 Zeichen lang sein.
Datenschutz-Protokoll	Die Art der Datenverschlüsselung/-entschlüsselung. DES/AES kann ausgewählt werden.
Datenschutz Passwort	Das Passwort, das zur Generierung des Schlüssels für die Verschlüsselung verwendet wird. Das Feld muss zwischen 16 und 31 Zeichen lang sein.
IP-Adresse	Der NMS-Zugang kann durch Eingabe einer bestimmten IP-Adresse oder einer IP-Netzwerk-Subnetzmaske eingeschränkt werden. Es gelten die folgenden Regeln für Subnetzmasken: • 192.168.20.255: Zugriff nur durch ein NMS auf das Segment 192.168.20. • 192.255.255.255: Zugriff nur durch ein NMS im Segment 192. • 0.0.0.0 (die Standardeinstellung) oder 255.255.255.255: Zugriff durch jedes NMS auf jedem Segment.

Telnet und Secure Shell (SSH)

Telnet bietet einen grundlegenden Sicherheitszugang mit Benutzernamen、Passwort、konfigurierbarem Port und zugänglicher IP, aber der Benutzername、Passwort und die übermittelten Daten sind nicht verschlüsselt. Secure Shell (SSH) überträgt den Benutzernamen, das Passwort und die Daten mit Verschlüsselung.

Konfigurieren Sie die Telnet- und SSH-Parameter auf der Web-Seite von **[System->Netzwerkdienst->Konsolendienst]**

Artikel	Definition
Zugang	
Zugriff zulassen	Aktivieren Sie den Zugriff auf Telnet oder SSH-Version 2, das die Übertragung von Benutzernamen, Passwörtern und Daten verschlüsselt.
Telnet-Einstellungen	
Telnet-Anschluss	Der TCP/IP-Port (standardmäßig 23), den Telnet für die Kommunikation verwendet.
SSH-Einstellungen	
SSH-Anschluss	Der TCP/IP-Port (standardmäßig 22), den SSH für die Kommunikation verwendet.
Host-Taste Status	Zeigt den Status des Hostkey-Fingerabdrucks an, um anzuzeigen, ob er

	gültig oder ungültig ist. • Hostschlüssel hochladen: Klicken Sie darauf, um einen Hostkey hochzuladen und den aktuellen zu ersetzen. • Hostschlüssel exportieren: Klicken Sie darauf, um den aktuellen Hostschlüssel zu exportieren.
Host-Schlüssel Fingerabdruck	Der von den Benutzern hochgeladene Fingerabdruck des Host-Schlüssels wird in diesem Feld angezeigt.

Anmerkung: 1. Wenn Sie den Zugriff auf SSH aktivieren, wird der SCP-Dienst automatisch aktiviert.

2. RMCARD400 unterstützt die folgenden SSH-Algorithmen:
   - SSH-Version: SSHv2
   - Kex-Austausch:
     - ecdh-sha2-nistp521
     - ecdh-sha2-nistp384
     - ecdh-sha2-nistp256
     - diffie-hellman-group14-sha256
   - Chiffren:
     - aes256-ctr
     - aes128-ctr
   - Unterschriften:
     - ssh-dss
     - ssh-rsa (RSA-Schlüssellänge 2048 Bit oder 4096 Bit)
     - ssh-ed25519
   - MAC:
     - hmac-sha2-256
3. Erreichbare IP-Einstellung entsprechend der Einstellung in **[System->Sicherheit->Lokales Konto]**.

FTP und SCP

FTP bietet einen grundlegenden Sicherheitszugang mit Benutzername、Passwort und konfigurierbarem Port, aber der Benutzername、Passwort und die übertragenden Daten werden nicht verschlüsselt. Secure CoPy (SCP) überträgt den Benutzernamen, das Passwort und die Daten mit Verschlüsselung.

Konfigurieren Sie die FTP-Parameter auf der Web-Seite von **[System->Netzwerkdienst->FTP-Dienst]**

Artikel	Definition
Zugriff zulassen	Aktivieren Sie den Zugriff auf den FTP-Server.
Service-Anschluss	Der TCP/IP-Port des FTP-Servers (standardmäßig 21). Die Benutzer können die Port-Einstellung auf einen beliebigen, nicht verwendeten Port

	zwischen 5000 und 65535 ändern, um die Sicherheit zu erhöhen.

Anmerkung:

1. Der SCP wird aktiviert, wenn Sie SSH aktivieren.
2. Wenn Sie sich für SCP entscheiden, sollten Sie aus Sicherheitsgründen den Zugriff auf den FTP-Server deaktivieren.
3. Erreichbare IP-Einstellung entsprechend der Einstellung in **[System->Sicherheit->Lokales Konto].**

Anschluss für Kommunikation

RMCARD400 ermöglicht den Netzwerkzugang, um die Kommunikation mit anderen Geräten in den Systemen und der Konfiguration zu unterstützen. Bitte beachten Sie die folgenden Informationen zur Konfiguration der Firewalls, um den erforderlichen Zugang für die reibungslose Funktion der RMCARD zu ermöglichen.

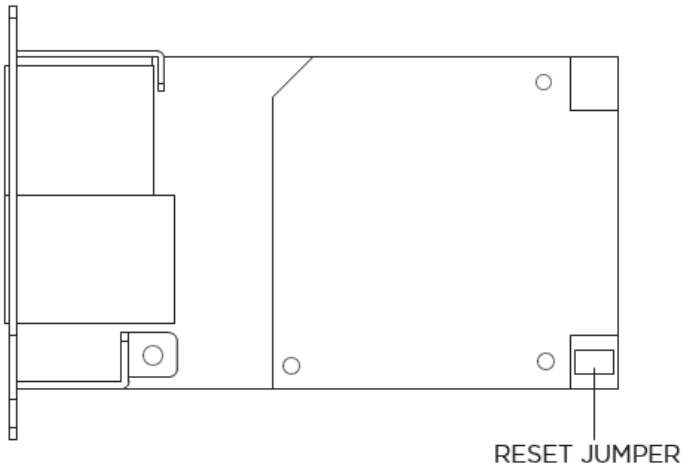
Dienst	Protokoll	Hafen-Nummer	Rolle	Standard	Umschaltbar
HTTP	TCP	80	Server	ON	Ja
HTTPS	TCP	443	Server	ON	Ja
Telnet	TCP	23	Server	AUS	Ja
SSH	TCP	22	Server	ON	Ja
FTP	TCP	20/21	Server	ON	Ja
PPB*	TCP	3052	Server	ON	Nein
SNMP	UDP	161	Server	AUS	Ja
PDNU2*	UDP	53566	Server	ON	Nein
DHCP	UDP	68	Server	ON	Nein
Produktionseinstellungen	UDP	53565	Server	ON	Nein
LDAP	TCP	389/636	Kunde	AUS	--
SMTP	TCP	25/587/465	Kunde	AUS	--
DNS	UDP	53	Kunde	ON	--
NTP	UDP	123	Kunde	AUS	--
RADIUS	UDP	1812	Kunde	AUS	--
Falle	UDP	162	Kunde	AUS	--
Syslog	UDP	514	Kunde	AUS	--
PPB	UDP	3052	Kunde	AUS	--
WOL	UDP	4999	Kunde	AUS	--

* PPB: PowerPanel® Business

* PDNU2: Power Device Network Utility 2

Anhang 1 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):



RMCARD400

1. Nehmen Sie die Karte aus der USV, **ohne die USV 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.
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. Setzen Sie die Karte wieder in den Erweiterungsport ein und ziehen Sie die Befestigungsschrauben fest.

Anhang 2 Beispiel für die Aktualisierung der Firmware mit dem Befehl Secure Copy (SCP)

Für Windows-Benutzer:

1. Laden Sie ein beliebiges PuTTY Secure Copy Client (PSCP) Dienstprogramm herunter.
2. Speichern Sie die Firmware-Dateien und das PSCP-Dienstprogramm im selben Ordner.
3. Öffnen Sie die Befehlszeilenschnittstelle und ändern Sie den Pfad, in dem die Firmware-Dateien und das PSCP-Dienstprogramm 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 nur eine Firmware-Datei zum Hochladen: cpsrm4safw_XXX.

(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 cpsrm4safw_xxx cyber@192.168.1.100:

Hinweis: cpsrm4safw_xxx ist die Firmware-Datei der zu aktualisierenden Version.

5. Nach dem Ausführen 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. Die Übertragung der Firmware-Datei kann ein paar 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.
7. 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 nur eine Firmware-Datei zum Hochladen: cpsrm4safw_XXX.

(3) <user> ist der Benutzername des SSH-Kontos auf der RMCARD.

(4) Achten Sie darauf, nach der IP-Adresse ein ":" einzufügen.

Zum Beispiel:
scp cpsrm4safw_xxx cyber@192.168.1.100:

Hinweis: cpsrm4safw_xxx ist die Firmware-Datei der zu aktualisierenden 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. Die Übertragung der Firmware-Datei kann ein paar 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.
7. Wenn die Übertragung der Firmware-Datei nicht erfolgreich war, erhalten Sie eine Fehlermeldung. Versuchen Sie, den Befehl neu einzugeben und erneut auszuführen.

Anhang 3 Beispiel für das Speichern und Wiederherstellen von Konfigurationseinstellungen mit dem Befehl Secure Copy (SCP)

Für Windows-Benutzer:

1. Laden Sie ein beliebiges PuTTY Secure Copy Client (PSCP) Dienstprogramm herunter.
2. Speichern Sie die Konfigurationsdatei und das PSCP-Dienstprogramm in demselben Ordner.
3. Öffnen Sie die Befehlszeilenschnittstelle und ändern Sie den Pfad, in dem die Konfigurationsdatei und das PSCP-Dienstprogramm 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 CONFIG_YYYY_MM_DD_HHMM.tar.gz.

(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 CONFIG_JJJJ_MM_DD_HHMM.tar.gz cyber@192.168.1.100:

Hinweis: CONFIG_YYYY_MM_DD_HHMM.tar.gz 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 CONFIG_YYYY_MM_DD_HHMM.tar.gz.
(3) <user> ist der Benutzername des SSH-Kontos auf der RMCARD.
(4) Achten Sie darauf, nach der IP-Adresse ein ":" einzufügen.

Zum Beispiel:
scp CONFIG_JJJJ_MM_DD_HHMM.tar.gz cyber@192.168.1.100:

Hinweis: CONFIG_YYYY_MM_DD_HHMM.tar.gz 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.

Anhang 4 Beispiel für das Hochladen des SSH-Host-Schlüssels mit dem Befehl Secure Copy (SCP)

Ein SSH HOST Key kann mit Secure Copy Befehlen auf die RMCARD hochgeladen werden. Bitte vergewissern Sie sich, 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 Dienstprogramm PuTTY Secure Copy Client (PSCP) herunter.
2. Die SSH-Host-Schlüsseldatei und das PSCP-Dienstprogramm müssen sich im selben Ordner befinden.
3. Öffnen Sie die Eingabeaufforderung und ändern Sie den Pfad zur SSH-Host-Schlüsseldatei und zum PSCP-Dienstprogramm 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-Schlüsseln erstellt werden.

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)

K01-E000095-01