Remote Management Card

RMCARD205 / RMCARD305

Security Guide

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

K01-E000018-06

Introduction

This document provides a guide for the security features for firmware version V1.4.0 above of RMCARD205/305(In the following content, RMCARD205 is referred to as RMCARD205 / 305.). Following parts would be included.

- User Account Types
- User Account Authentication
- HyperText Transfer Protocol (HTTP) HTTP and HyperText Transfer Protocol over Secure Sockets Layers(HTTPS)
- SNMPv1 and SNMPv3
- Telnet and Secure SHell v2 (SSH)
- File transfer protocols (FTP) and Secure CoPy(SCP)
- Port For Communication

User Account Types

The RMCARD205 provide two user account types for login.

- Administrator: be able to access all items in Web interface and all commands in the command line interface.
- Viewer: be able to access read features in Web interface.

Note: 1.The user will be asked to set a new username and password upon the first login.

2. The Administrator account is also used for the FTP login, CLI interface, Power Device Network Utility, and Upgrade and Configuration Utility.
3. Only one user can log in and access the device at a time.
4. CyberPower Switched PDU device has addition “outlet user” account. For more account information, please refer to device’s help file.
5. The viewer account is disabled by default.

User Account Authentication

The RMCARD205 provides local and remote user account authentication.

- Local: the username and password are managed and verified by RMCARD205.
- Remote: the username and password are managed and verified by a central Remote Authentication Dial-In User Service (RADIUS) or Lightweight Directory Access Protocol(LDAP) Server.

Configure authentication method on the Web page of [System->Security-> Management]

Settings	Definition
Local Account	Use local account Administrator or Viewer settings to log in.
RADIUS, Local Account	Use RADIUS configuration settings to log in. If RADIUS authentication fails then Local Account settings will be used to log in.
RADIUS Only	Use RADIUS configuration settings to log in.
LDAP, Local Account	Use LDAP configuration settings to log in. If LDAP authentication fails then Local Account settings will be used to log in.
LDAP Only	Use LDAP configuration settings to log in.

- The “Admin/Viewer Manager IP” defines the allowable login IP to access RMCARD205. Following samples:
  - If you allow any IP address to access RMCARD205, you can set as 0.0.0.0 or 255.255.255.255.
  - If you allow any IP with subnet of 192.168.0.0 to access RMCARD205, you can set as 192.168.20.0/16.

Local Account

Configure the Local Account parameters on the Web page of **[System->Security->Local Account]**

- The maximum length of both User Name and Password of Administrator is 63 characters.
- The maximum length of both User Name and Password of Viewer is 15 characters.

RADIUS

When a user logs in the RMCARD, an authentication request will be sent to the RADIUS server to determine the permission level of the user with the RADIUS function enabled.

Supported RADIUS Servers

RMCARD205 supports FreeRADIUS v2.x, Microsoft Server 2008 and 2012 Network policy Server (NPS). Other RADIUS may work but not have been fully tested.

Configure RMCARD205

Configure the RADIUS parameters on the Web page of **[System->Security->RADIUS Configuration].**

Settings	Definition
Server IP	The IP address/domain of RADIUS server.
Shared Secret	The shared secret of RADIUS server.
Server Port	The UDP port used by the RADIUS server.
Test Setting	Test RADIUS server using user name and password settings. If authentication is successful the settings will be saved.
Skip Test	Save RADIUS server settings without testing.

Configure the RADIUS Server

You have to configure your RADIUS server to make it work with RMCARD205.

Sample:

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

   3808 – Vendor

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

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

   Cyber-Service-Type can accept three integer parameter values:

   1 – Administrator

   2 – Viewer

   3 – Outlet User

   (2) **Cyber-Outlets** (string variable)

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

The example of the Dictionary File:

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

LDAP

When a user logs in the RMCARD, an authentication request will be sent to the LDAP server to determine the permission level of the user with the LDAP function enabled.

Supported LDAP Servers

RMCARD205 supports OpenLDAP v2.x、Windows AD Server 2008、2012.

Configure RMCARD205

Configure the LDAP parameters on the Web page of **[System->Security->LDAP Configuration] .**

Item	Definition
LDAP Server Type	
Generic LDAP Server	Select LDAP server type as OPENLDAP.
Active Directory	Select LDAP server type as Windows AD.
AD Domain	The AD Domain of the Active Directory server.
LDAP Server	
LDAP Server	The IP address/domain of LDAP server.
LDAP SSL	Enable to communicate with LDAP server by LDAPS.
Port	The TCP port used by the LDAP(S) server.
User Base DN	The Base DN of LDAP server.
Login Attribute	The Login Attribute of LDAP user entry (for example:cn or uid).
LDAP Authentication	
Authentication Mode	Identifies the method to use for authentication. • Anonymous : Bind Request using Simple Authentication with a zero-length bind DN and a zero-length password. • Accredited User : Bind Request using Simple Authentication with a Bind DN and Bind Password. • By Logon User : Bind Request using Simple Authentication with a User Base DN and login Password. Note: The Authentication Mode selector will be disabled when LDAP Server Type is set to Active Directory.
LDAP Authorization	
Authorization Mode	Identifies the method to use for authorization. • By User Attribute : Determine access level by User Attribute and User Attribute Value. • By Group : Determine access level by group which search DN information such as the following Group Base DN, Group Attribute and Group Attribute Value.

Configure the LDAP Server

You have to configure your RADIUS server to make it work with RMCARD205.

Add one of the attributes below to **description** on the **LDAP Server** for indicating the user account type and authentication:

1. **cyber_admin** (Administrator)
2. **cyber_viewer** (Viewer)
3. **cyber_outlet="string"** (Outlet user)

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

Security Features

The RMCARD205 provides basic security and high security for the access protocols. The basic security protocol transmits the authentication and data with plain text without encryption, and the high security protocol transmits the authentication and data with encryption. It is recommended that choose and enable the high security protocol to access and disable the basic security protocol.

Summary of the protocols

Web Server

HTTP	HTTPS
Basic Security Access • User Name and Password.(transmit with plain text without encryption) • Configurable server Port • Service can be enabled or disabled • Accessible IP filter	High Security Access • Support TLS. • User Name and Password.(transmit TLS encryption) • Configurable server Port. • Service can be enable or disable • Accessible IP filter

SNMP Service

SNMPv1	SNMPv3
Basic Security Access • Community name (transmit with plain text without encryption) • Service can be enabled or disabled • 4 access Community • Accessible IP filter • Capability of read/write/forbidden to the specific Community	High Security Access • 4 User Profiles • Authentication by an authentication passphrase with SHA or MD5 hash algorithm • Encryption by a privacy passphrase with AES or DES encryption algorithm • Accessible IP filter

Command line interface

Telnet	SSH
Basic Security Access • User Name and Password. (transmit with plain text without encryption) • Configurable server Port • Service can be enabled or disabled • Accessible IP filter	High Security Access • User Name and Password. (transmit with SSH encryption) • Configurable server Port • Service can be enabled or disabled (you can only choose Telnet or SSH to be enabled at the time) • Accessible IP filter

File Transfer protocol

FTP	SCP
Basic Security Access • User Name and Password. (transmit with plain text without encryption) • Configurable server Port • Service can be enabled or disabled	High Security Access • User Name and Password. (transmit with SSH encryption) • Configurable server Port • Service can be enabled or disabled (Enable SSH and disable FTP if you choose SCP) • Accessible IP filter

Web Server

HTTP and HTTPS

HyperText Transfer Protocol (HTTP) provides basic security access with user name、password、configurable port and accessible IP, but the user name、password and transmitting data are not encrypted. HyperText Transfer Protocol over Secure Sockets Layers (HTTPS) transmits the user name, password, and data with encryption and provides authentication of RMCARD205 via digital certificates.

Configure the HTTP/HTTPS parameters on the Web page of **[System->Network Service->Web Service]**.

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

Note: 1. The format of uploading digital certificate must be a standard PEM (Privacy Enhanced Mail).

2.RMCARD205 supports Transport Layer Security (TLS) V1.2.

Following is the example to create the certificate with OpenSSL and upload the certification.

1. Create a folder “CA” and copy openssl.cnf into it.

```
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. Type “openssl genrsa -des3 -out rootca.key 2048” and input password of key.

```
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. Type “openssl req -new -key rootca.key -out rootca.req” and input information of RootCA certificate.

```
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. Type “openssl x509 -req -days 7305 -sha1 -extfile openssl.cnf -extensions v3_ca -signkey rootca.key -in rootca.req -out rootca.crt” to create RootCA certificate.

```
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. Type “openssl genrsa -out server.key 2048” to create server key.

```
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. Type “openssl req -new -key server.key -out server.req” and input information of certificate.

```
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. Type “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” to create server certificate.

```
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. Then you can see the following three files.

```
-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. Create a file which name RMC.crt and past the content of three files into it.

Upload the file “RMC.crt” on the web page of **[System->Network Service->Web Service]**.

NOTE**:** The above procedure describes the workflow for generating RSA certificates. RSA remains supported. Starting from firmware v1.6.0, ECDSA certificates are also supported. For ECDSA certificate generation, refer to the next section.

Following is the example to provides the necessary steps and the accompanying shell script to **generate a self-signed Root Certificate Authority (CA) key and certificate** using OpenSSL. This Root CA can be used for internal testing or securing private networks.

Compatibility Note:
The Elliptic Curve Digital Signature Algorithm (ECDSA) used in this script relies on the OpenSSL command-line utility.
This functionality is explicitly supported on versions RMCARD v1.6.0 and later.
Please verify your RMCARD version before running the script.

1. Shell Script: **generate_rootca.sh**
   This script automates the process of generating an Elliptic Curve Digital Signature Algorithm (ECDSA) private key and a corresponding self-signed X.509 certificate for a Root CA.

```
#!/bin/bash

# Configuration Variables
KEY_FILE="rootca.key"
CRT_FILE="rootca.crt"
DAYS_VALID=3650  # Validity period is 10 years

# Generate an ECDSA private key using the secp256r1 curve
openssl ecparam -name prime256v1 -genkey -noout -out "$KEY_FILE"

# Generate the self-signed certificate (Root CA)
# -x509: Self-signed certificate
# -new: New certificate request
# -nodes: No encryption for the private key
# -sha256: Use SHA-256 for the signature
# -days 3650: Set validity period
# -subj: Subject information (Common Name, Organization, Location, etc.)
# -extensions v3_ca: Apply the 'v3_ca' extensions block
# -config <(...): Dynamically inject the v3_ca extensions for CA purpose
openssl req -x509 -new -nodes -key "$KEY_FILE" -sha256 -days "$DAYS_VALID" -out "$CRT_FILE"   -
subj "/CN=RMCARD/OU=RMCARD Team/O=CyberPower/L=Skakopee/ST=Minnesota/C=US"   -extensions v3_ca
-config <(cat /etc/ssl/openssl.cnf <(printf "\n[ v3_ca ]\nbasicConstraints =
critical,CA:TRUE\nkeyUsage = keyCertSign, cRLSign"))

echo "Root CA key: $KEY_FILE"
echo "Root CA cert: $CRT_FILE"
```

2. Save the Script: Save the content above into a file named **generate_rootca.sh**.
3. Run the Script: Execute the script from your terminal: **./generate_rootca.sh**

4. Shell Script: **generate_device_cert.sh**
   This script takes the device name as an argument and generates the necessary cryptographic files, including a private key, a certificate signed by the Root CA, and a combined file for deployment.

```
#!/bin/bash

# Check if the device name argument is provided
if [ -z "$1" ]; then
  echo "Usage: sh generate_device_cert.sh <device_name>"
  exit 1
fi

# Set folder and file names
DEVICE_NAME="$1"
DEVICE_DIR="$DEVICE_NAME"
DEVICE_KEY="${DEVICE_DIR}/device.key"
DEVICE_CSR="${DEVICE_DIR}/device.csr"
DEVICE_CRT="${DEVICE_DIR}/device.crt"
DEVICE_COMBINED="${DEVICE_DIR}/ecdsa_${DEVICE_NAME}.crt" # Note: This combines key and cert
CONFIG_FILE="${DEVICE_DIR}/san_only.cnf"

# Create directory for device files
mkdir -p "$DEVICE_DIR"

# Create config file with Subject Alternative Name (SAN) only
cat <<EOF > "$CONFIG_FILE"
[req]
default_bits      = 2048
prompt            = no
default_md        = sha256
distinguished_name = dn
req_extensions    = req_ext

[dn]
C  = US
ST = Minnesota
L  = Skakopee
O  = CyberPower
OU = RMCARD Team
CN = $DEVICE_NAME

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = $DEVICE_NAME
EOF

# Generate ECDSA device key (secp256r1 curve)
openssl ecparam -name prime256v1 -genkey -noout -out "$DEVICE_KEY"

# Create CSR (Certificate Signing Request)
openssl req -new -key "$DEVICE_KEY" -out "$DEVICE_CSR" -config "$CONFIG_FILE"

# Sign CSR using the rootca key and cert to generate the device cert
# -CAcreateserial creates the 'rootca.srl' file to track serial numbers
openssl x509 -req -in "$DEVICE_CSR" -CA rootca.crt -CAkey rootca.key -CAcreateserial \
  -out "$DEVICE_CRT" -days 3650 -sha256 \
  -extfile "$CONFIG_FILE" -extensions req_ext

# Concatenate the device key and certificate into a single PEM file
cat "$DEVICE_KEY" "$DEVICE_CRT" > "$DEVICE_COMBINED"

# Clean up temporary files
rm -f "$CONFIG_FILE"
rm -f "rootca.srl"
```

```
rm -f "$DEVICE_CSR"

# Display results
echo "Done: "
echo " - Private Key   : $DEVICE_KEY"
echo " - Certificate   : $DEVICE_CRT"
echo " - Combined File : $DEVICE_COMBINED"
```

5. Prerequisite: Ensure the rootca.key and rootca.crt files are in the same directory as this script.
6. Save the Script: Save the content above into a file named **generate_device_cert.sh**.
7. Run the Script: Execute the script, replacing **MyDeviceName** with the actual device identifier: **./generate_device_cert.sh <MyDeviceName>**
8. The script will generate a file named **MyDeviceName.crt**, which **combines the device's private key (**device.key**) and its certificate (**device.crt**)** into a single PEM file.

9. Upload the file **MyDeviceName.crt** on the web page of **[System->Network Service->Web Service]**.

SNMPv1 and SNMPv3

SNMPv1 provides basic security access with community、Access type and accessible IP, but the community、and transmitting data are not encrypted. SNMPv3 transmits data with encryption and provides authentication with passphrase.

Configure the SNMPv1 parameters on the Web page of **[System->Network Service->SNMPv1 Service]**.

Item	Definition
SNMPv1 Service	
Allow Access	Set the SNMPv1 service to either Enable or Disable.

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

Configure the SNMPv3 parameters on the Web page of **[System->Network Service->SNMPv3 Service]**.

Item	Definition
SNMPv3 Service	
Allow Access	Set the SNMPv3 service to either Enable or Disable.
SNMPv3 Access Control	
User Name	The name to identify SNMPv3 user. The field must be 1 to 31 characters in length.
Authentication Protocol	The hash type for authentication. MD5/SHA can be selected.
Authentication Password	The password used to generate the key used for authentication. The field must be 16 to 31 characters in length.
Privacy Protocol	The type of data encryption/decryption. DES/AES can be selected.
Privacy Password	The password used to generate the key used for encryption. The field must be 16 to 31 characters in length.
IP Address	NMS access can be restricted by entering a specific IP address or an IP network subnet mask. The following subnet mask rules apply: • 192.168.20.255: Access only by an NMS on the 192.168.20 segment. • 192.255.255.255: Access only by an NMS on the 192 segment. • 0.0.0.0 (the default setting) or 255.255.255.255: Access by any NMS on any segment.

Telnet and Secure Shell (SSH)

Telnet provides basic security access with user name、password、configurable port and accessible IP, but the user name、password and transmitting data are not encrypted. Secure Shell (SSH)transmits the user name, password, and data with encryption.

Configure the Telnet and SSH parameters on the Web page of **[System->Network Service->Console Service]**

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

Note: 1. If you enable the access of SSH, the SCP service would be enabled automatically.

2.RMCARD205 support the following SSH Algorithm(s):

- SSH Version: SSHv2
- Kex exchange:
  - diffie-hellman-group-exchange-sha256
  - diffie-hellman-group14-sha256
- Ciphers:
  - aes256-ctr
  - aes128-ctr
- Signatures:
  - ssh-rsa (RSA Key length 2048-bit or 4096-bit)
  - ssh-ed25519
- MAC:
  - hmac-sha2-512
  - hmac-sha2-256

3. Accessible IP setting following the setting in **[System->Security->Local Account]**.

FTP and SCP

FTP provides basic security access with user name、password and configurable port, but the user name、password and transmitting data are not encrypted. Secure CoPy (SCP) transmits the user name, password, and data with encryption.

Configure the FTP parameters on the Web page of **[System->Network Service->FTP Service]**

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

Note: 1. The SCP is enabled when you enable SSH.
2. If SCP is chosen, recommend to disable the access of FTP server for security.
3. Accessible IP setting following the setting in **[System->Security->Local Account].**

Port For Communication

RMCARD205 enables network access to support communication with other devices in the systems and configuration. Please refer to the following information for configuring the firewalls to allow needed access for RMCARD to function smoothly.

Service	Protocol	Port Number	Role	Default	Switchable
HTTP	TCP	80	Server	OFF	Yes
HTTPS	TCP	443	Server	ON	Yes
Telnet	TCP	23	Server	OFF	Yes
SSH	TCP	22	Server	ON	Yes
Modbus TCP	TCP	502	Server	OFF	Yes
FTP	TCP	20/21	Server	OFF	Yes
PPB*	TCP	3052	Server	ON	No
SNMP	UDP	161	Server	OFF	Yes
PDNU2*	UDP	53566	Server	ON	No
Production Settings	UDP	53565	Server	ON	No
LDAP	TCP	389/636	Client	OFF	--
SMTP	TCP	25/587/465	Client	OFF	--
DNS	UDP	53	Client	ON	--
NTP	UDP	123	Client	OFF	--
RADIUS	UDP	1812	Client	OFF	--

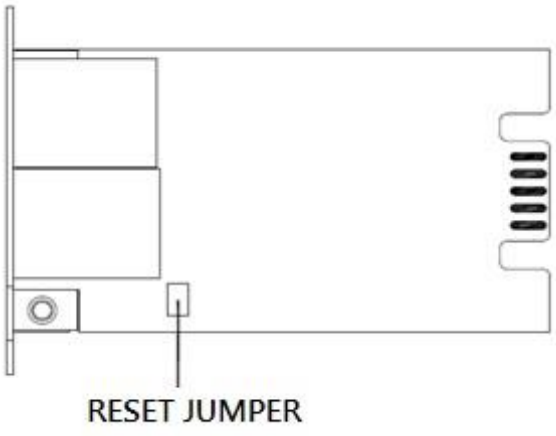
Service	Protocol	Port Number	Role	Default	Switchable
Trap	UDP	162	Client	OFF	--
Syslog	UDP	514	Client	OFF	--
PPB	UDP	3052	Client	OFF	--
WOL	UDP	4999	Client	OFF	--
EnergyWise	UDP	43440	Cilent	OFF	--

* PPB: PowerPanel® Business

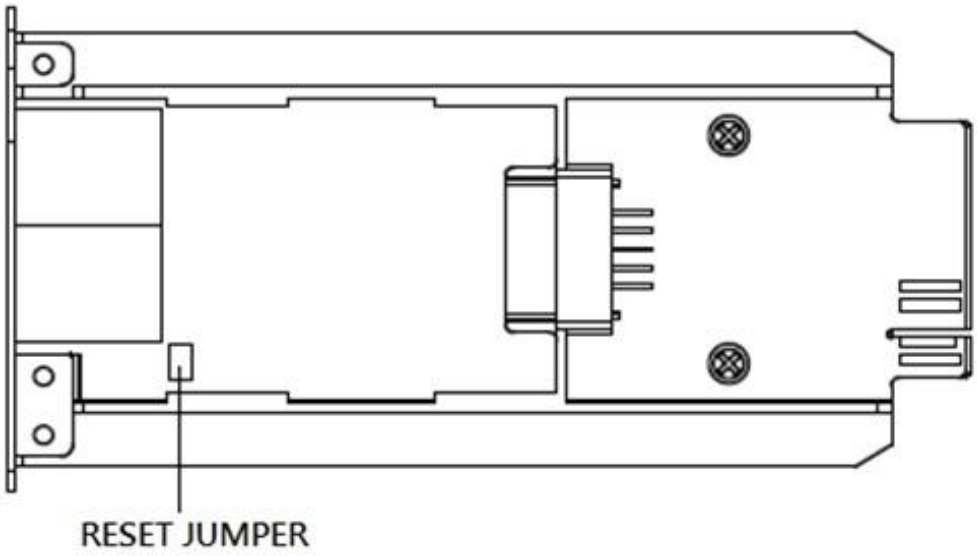
* PDNU2: Power Device Network Utility 2

Appendix 1 Reset to Factory Default Setting / Recover from a Lost Password

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



RMCARD205



RMCARD305

1. Remove the card from the UPS without turning the UPS/ATS PDU off.
2. Remove the jumper from the reset pins as illustrated. Do not dispose of the jumper.
3. Insert the card into the expansion port on the UPS/ATS PDU.
4. Wait until the green Tx/Rx LED is flashing (the frequency of the ON/OFF flashing is once per second).
5. Remove the card again.
6. Place the jumper back onto the Reset pins.
7. Install card into the expansion port again and tighten the retaining screws.

Appendix 2 Example of upgrade firmware with Secure Copy (SCP) command

Note: Only firmware version 1.1.2 and above supports the functionality to update firmware via SCP.

For Windows Users:

1. Download any PuTTY Secure Copy client (PSCP) utility.
2. Save the firmware files and the PSCP Utility in the same folder.
3. Open the Command Line Interface and change the path to where the firmware files and the PSCP Utility are saved.
4. Enter the following command to perform the firmware update:

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

Note:

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

(2) `<filename>` is the filename of the firmware file. There are two firmware files to upload: `cpsrm2scdata_XXX.bin` and `cpsrm2scfw_XXX.bin`. In order to upgrade the firmware version both files need to be uploaded. Only one firmware file can be uploaded at a time, it is recommended to upload the firmware file `cpsrm2scdata_XXX.bin` first followed by the data file `cpsrm2scfw_XXX.bin`.

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

(4) Ensure to add "`:`" after the IP address.

For example:

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

Note: `cpsrm2scdata_XXX.bin` is the firmware file of the version being updated.

5. After executing the command, a message may appear asking if you trust the host. To continue type "**y**" for yes within 10 seconds.
6. On the next screen enter the RMCARD password. The firmware file transfer may take a couple minutes to complete. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.
7. Repeat steps 4 through step 6 to upload the data file `cpsrm2scfw_XXX.bin` to complete the firmware update process.
8. If the firmware file transfer is unsuccessful you will see an error message. Attempt to retype the command and execute it again.

For Linux, MacOS and Unix Users:

1. Install the related distribution of an SSH or SCP client, for example Openssh client.
2. Open the Terminal and change the path to where the firmware files are saved.
3. Enter the following Command to perform firmware update:

   `scp <filename> <user>@< IP address of RMCARD>:`

Note:

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

(2) `<filename>` is the filename of the firmware file. There are two firmware files to upload: `cpsrm2scdata_XXX.bin` and `cpsrm2scfw_XXX.bin`. In order to upgrade the firmware version both files need to be uploaded. Only one firmware file can be uploaded at a time, it is recommended to upload the firmware file `cpsrm2scdata_XXX.bin` first followed by the data file `cpsrm2scfw_XXX.bin`.

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

(4) Ensure to add "`:`" after the IP address.

For example:

`scp cpsrm2scdata_XXX.bin cyber@192.168.1.100:`

Note: `cpsrm2scdata_XXX.bin` is the firmware file of the version being updated.

4. After executing the command, a message may appear asking if you trust the host. To continue type "**y**" for yes within 10 seconds.
5. On the next screen enter the RMCARD password. The firmware file transfer may take a couple minutes to complete. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.
6. Repeat steps 3 through step 5 to upload the data file `cpsrm2scfw_XXX.bin` to complete the firmware update process.
7. If the firmware file transfer is unsuccessful you will see an error message. Attempt to retype the command and execute it again.

Appendix 3 Example of save and restore configuration settings with Secure Copy (SCP) command

Note: Only firmware version 1.1.2 and above supports the functionality to restore configuration via SCP.

For Windows Users:

1. Download any PuTTY Secure Copy client (PSCP) utility.
2. Save the configuration file and the PSCP Utility in the same folder.
3. Open the Command Line Interface and change the path to where the configuration file and the PSCP Utility are saved.
4. Enter the following command to restore configuration:
   pscp –scp <filename> <user>@<IP address of RMCARD>:

Note:

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

(2) `<filename>` is the filename of the configuration file with a default format of YYYY_MM_DD_HHMM.txt.

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

(4) Ensure to add "`:`" after the IP address.

For example:

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

Note: `YYYY_MM_DD_HHMM.txt` is the configuration file to be restored.

5. After executing the command, a message may appear asking if you trust the host. To continue type "y" for yes within 10 seconds.
6. On the next screen enter the RMCARD password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

For Linux, MacOS and Unix Users:

1. Install the related distribution of an SSH or SCP client, for example OpenSSH client.
2. Open the Terminal and change the path to where the configuration files are saved.
3. Enter the following Command to restore configuration:
   scp <filename> <user>@< IP address of RMCARD>:

Note:

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

(2) `<filename>` is the filename of the configuration file with a default format of YYYY_MM_DD_HHMM.txt.

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

(4) Ensure to add "`:`" after the IP address.

For example:

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

Note: `YYYY_MM_DD_HHMM.txt` is the configuration file to be restored.

4. After executing the command, a message may appear asking if you trust the host. To continue type "y" for yes within 10 seconds.
5. On the next screen enter the RMCARD password. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

Appendix 4 Example of upload SSH Host key with Secure Copy (SCP) command

A SSH HOST Key can be uploaded to RMCARD205 with Secure Copy commands.
Please make sure the uploaded filename contains the start string of “ssh_hostkey” .
Some examples of acceptable file name are as following:

ssh_hostkey_sample1.pem
ssh_hostkey_1024.pem
ssh_hostkey_type100.***

Example of Upload Process

1. Download PuTTY Secure Copy client (PSCP) utility.
2. Have the SSH Host key file and the PSCP Utility in the same folder.
3. Open the Command Prompt and change the path to SSH Host key file and the PSCP Utility are saved.
4. Enter the following command

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

   Ex: **pscp -scp ssh_hostkey_xxx.xxx cyber@192.168.203.66:**
5. After executing the command, a message may appear asking if you trust the host. Please type "**y**” for yes within 10 seconds.
6. On the next screen enter the admin password. The file transfer may take a couple minutes to complete. Please wait until the progress indicator displays 100%. The system will automatically log out and reboot after the transfer is complete.

Host-Key Requirement

SSH that are created with 2048-bit or 4096-bit RSA keys.

CyberPower

CyberPower Systems, Inc.
www.cyberpowersystems.com

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

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

K01-E000018-06