Carte de gestion à distance

RMCARD205 / RMCARD305

Manuel d'utilisation

La carte de gestion à distance permet de gérer, de surveiller et de configurer un onduleur et un capteur d'environnement.

K01-E000025-00

Table des matières

Introduction

Présentation

La carte de gestion à distance CyberPower permet de surveiller et de gérer à distance un onduleur connecté à un réseau. Après l'installation du matériel et la configuration d'une adresse IP, l'utilisateur peut accéder à l'onduleur, le surveiller et le contrôler dans le monde entier ! Il vous suffit d'utiliser un navigateur Web, une interface de ligne de commande ou un client SSH pour accéder à votre onduleur. L'onduleur peut protéger les serveurs et les stations de travail en utilisant PowerPanel® Business Remote pour les arrêter correctement lorsqu'il reçoit un signal de la carte de gestion à distance.

Caractéristiques

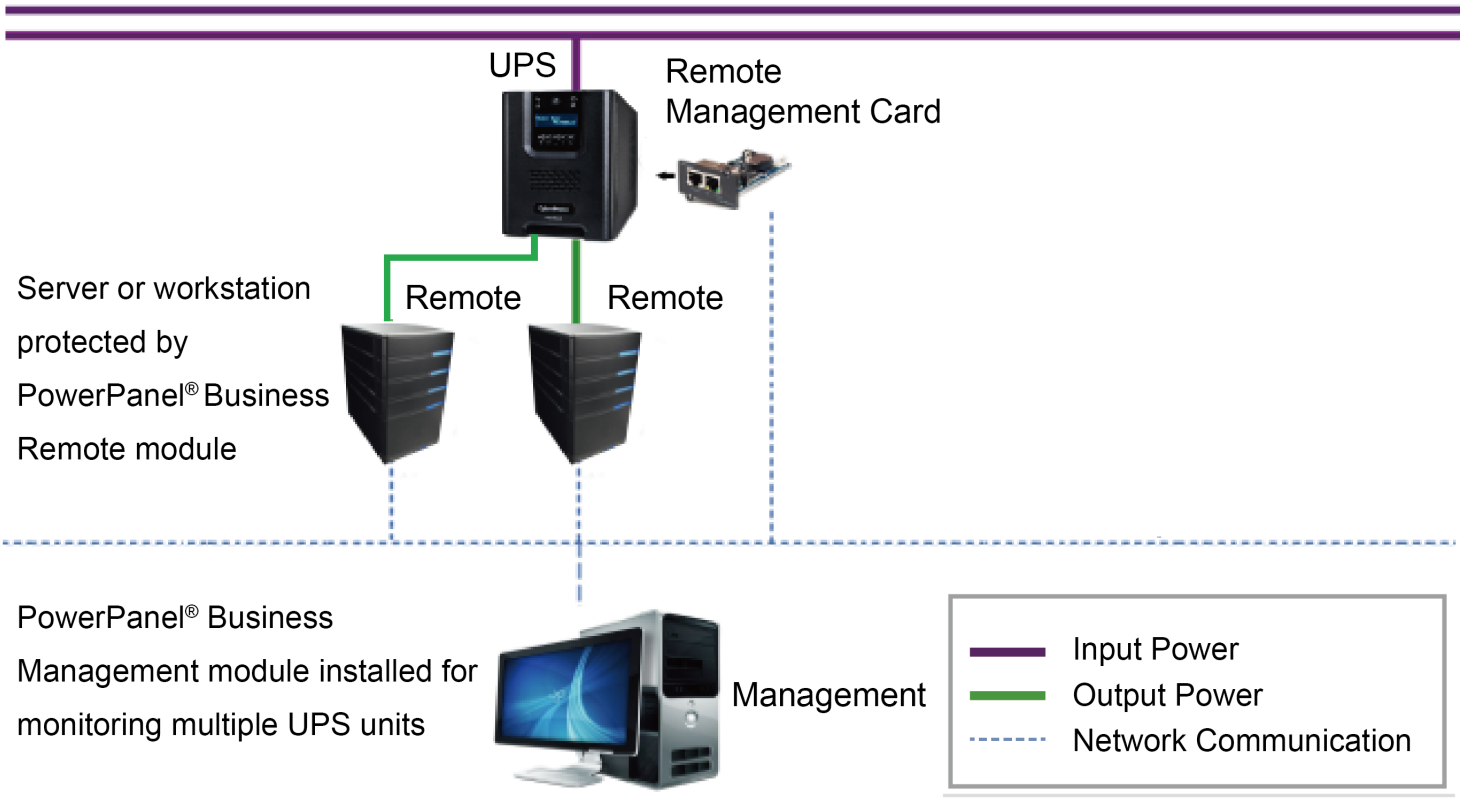
- Surveillance en temps réel de l'onduleur
- Gestion et configuration à distance de l'onduleur par le biais d'un navigateur Web, d'un système de gestion de réseau (NMS) ou d'une interface de ligne de commande (SSH et Telnet)
- Gestion et configuration en local de l'onduleur par le biais d'une connexion série
- Déclenchement des arrêts des serveurs/postes de travail en cas de panne de secteur, pour éviter toute perte ou corruption des données
- Planification de l'arrêt/du redémarrage/de la réinitialisation à distance de l'onduleur
- Journalisation des événements pour suivre l'historique de fonctionnement de l'onduleur
- Journalisation des données graphiques pour analyser les conditions électriques
- Enregistrement et restauration des paramètres de configuration, y compris ceux de l'onduleur et du commutateur de transfert automatique
- Notifications d'événements par e-mail, traps SNMP, Syslog et SMS
- Mise à niveau à distance du firmware de l'onduleur via l'interface Web et FTP sur certains modèles d'onduleur
- Prise en charge des protocoles IPv4/v6, SNMPv1/v3, HTTP/HTTPs, DHCP, NTP, DNS, SMTP, SSH, Telnet, FTP et Syslog
- Prise en charge des protocoles d'authentification sécurisée des e-mails : SSL, TLS
- Prise en charge des protocoles d'authentification externe : RADIUS, LDAP, LDAPS, Windows AD
- Protocole SNMP MIB téléchargeable gratuitement
- Mise à niveau du firmware par l'utilisateur via FTP, l'utilitaire de mise à niveau et de configuration CyberPower et le protocole de copie sécurisée (SCP, Secure Copy Protocol)
- Mise à niveau du firmware et chargement des fichiers de configuration sur plusieurs unités simultanément
- Interface utilisateur multilingue
- Installation rapide

- Échangeable à chaud
- Compatible Cisco EnergyWise
- Prise en charge du capteur d'environnement (ENVIROSENSOR)

Configuration système requise

- Connexion Ethernet 10/100 Mbit/s à un réseau existant
- Navigateur Web ou client SSH
- *(Facultatif)* Système de gestion de réseau (NMS, Network Management System) compatible SNMP

Application avec PowerPanel® Business



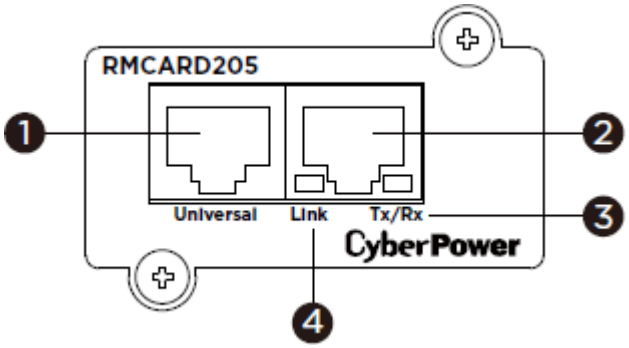
Déballage

Inspectez la carte de gestion à distance dès la réception. Le carton doit contenir les éléments suivants :

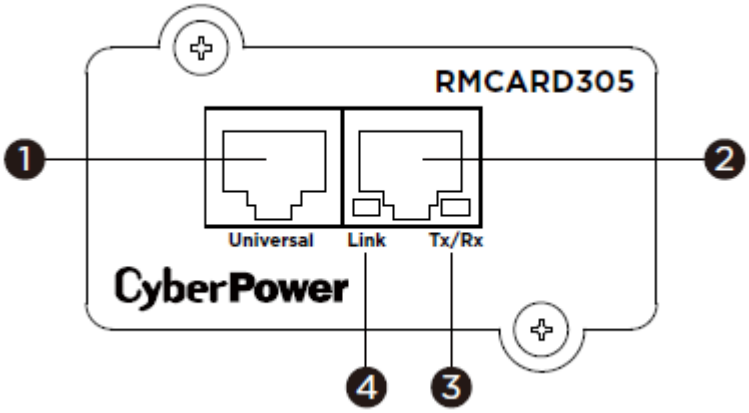
- Carte de gestion à distance CyberPower
- Câble de connexion au port série RJ45/DB9
- Guide de démarrage rapide
- Cavalier de rechange
- Panneau avant RMCARD205 (uniquement avec RMCARD305)

Panneau avant

RMCARD205



RMCARD305



1. Port universel
2. Port Ethernet
3. Voyant Tx/Rx
4. Voyant de liaison

Voyants d'état LED

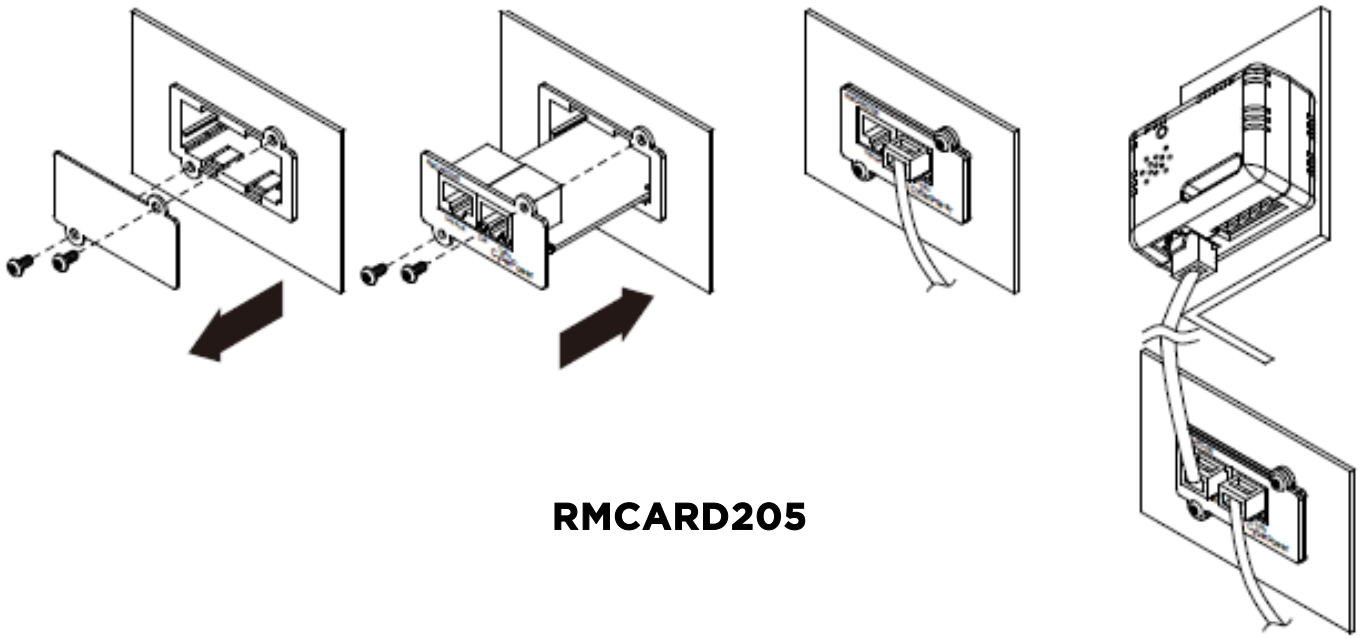
LED de liaison	Condition
Éteint	La carte de gestion à distance n'est pas connectée au réseau ou n'est pas sous tension.
Allumé (jaune)	La carte de gestion à distance est connectée au réseau.
LED Tx/Rx	
Éteint	La carte de gestion à distance est hors tension.
Allumé (vert)	La carte de gestion à distance est sous tension.
Clignotant (vert)	- Réception/transmission d'un paquet de données - Réinitialisation terminée

Guide d'installation

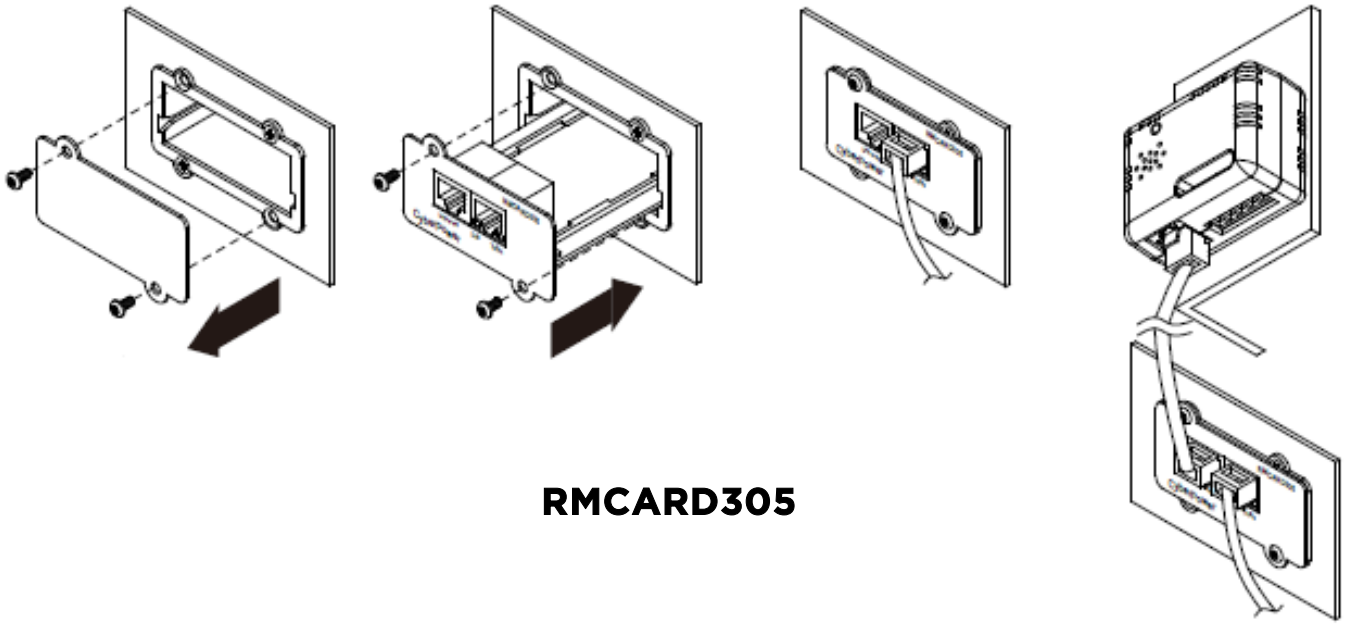
Étape 1. Installation du matériel

Remarque : vous n'avez pas besoin de mettre l'onduleur hors tension pour installer la carte de gestion à distance CyberPower, car elle est échangeable à chaud.

1. Ôtez les deux vis de fixation du connecteur d'extension et ôtez le capot.
2. Installez la carte de gestion à distance CyberPower dans le connecteur d'extension.
3. Insérez et serrez les vis de fixation.
4. Branchez un câble Ethernet sur le port Ethernet de la carte de gestion à distance CyberPower.
5. (*Facultatif)* Pour connecter un capteur d'environnement, utilisez un câble Ethernet RJ45. Branchez une extrémité sur le port universel de RMCARD et l'autre sur le capteur. Pour plus d'informations, reportez-vous au manuel d'utilisation d'ENVIROSENOR.



RMCARD205



RMCARD305

Étape 2. Configuration de l'adresse IP de la carte de gestion à distance CyberPower

Remarque : ces instructions sont valables pour le système d'exploitation Windows. Si vous utilisez un autre système d'exploitation, reportez-vous à l'annexe 4.

Méthode 1 : utilisation de l'utilitaire réseau d'équipement électrique

1. Installez l'utilitaire réseau d'équipement électrique téléchargeable depuis www.cyberpower.com.
2. Une fois l'installation terminée, exécutez l'utilitaire réseau d'équipement électrique.
3. La fenêtre principale du programme Utilitaire réseau d'équipement électrique est présentée dans la figure 1. L'outil de configuration affiche tous les équipements de gestion à distance CyberPower présents sur le sous-réseau local. Le bouton Actualiser sert à chercher à nouveau le sous-réseau local.

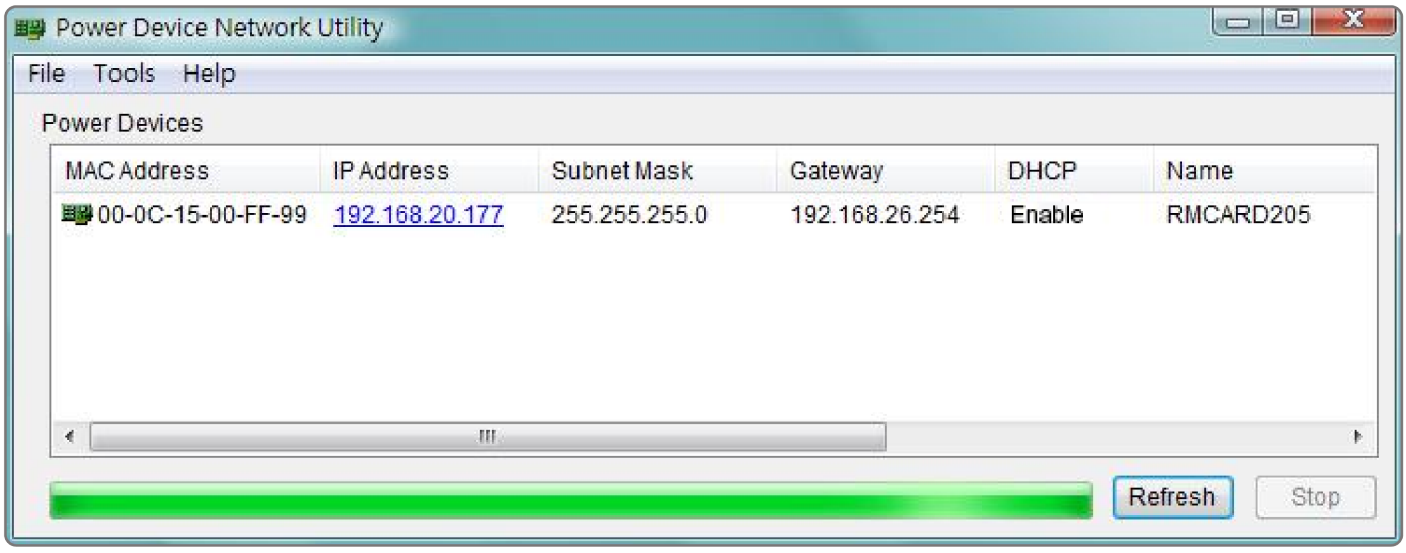


Figure 1. Fenêtre principale du programme Utilitaire réseau d'équipement électrique.

4. Sélectionnez la carte de gestion à distance que vous configurez. Cliquez sur le menu Outils et sélectionnez « Configurer un équipement » ou double-cliquez sur l'équipement que vous voulez configurer.
5. Vous pouvez modifier l'adresse IP, le masque de sous-réseau et l'adresse de passerelle pour l'adresse MAC d'équipement indiquée dans la fenêtre Paramètres réseau d'équipement, comme illustré dans la figure 2. L'adresse IP par défaut est 192.168.20.177 et le masque de sous-réseau par défaut est 255.255.255.0.

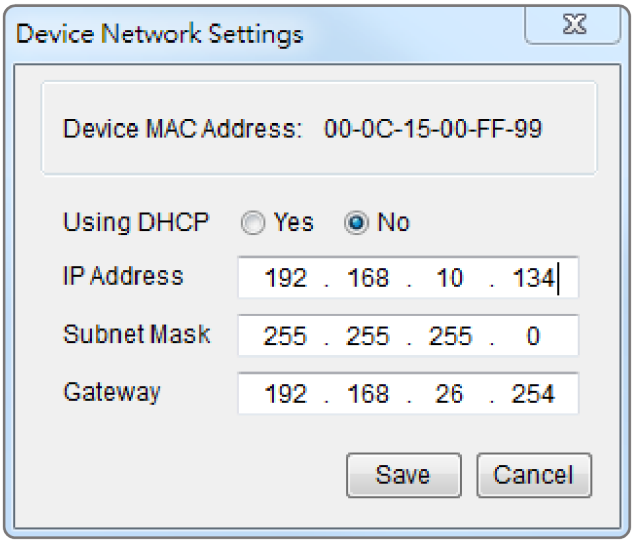


Figure 2. Fenêtre Paramètres réseau d'équipement.

6. Modifiez l'adresse IP, le masque de sous-réseau ou l'adresse de passerelle. Entrez les nouvelles adresses dans les champs correspondants, puis cliquez sur « Enregistrer ».
7. Vous devrez entrer un nom d'utilisateur et un mot de passe pour la carte de gestion à distance dans la fenêtre d'authentification, comme illustré dans la figure 3.
   - Nom d'utilisateur par défaut : **cyber**
   - Mot de passe par défaut : **cyber**

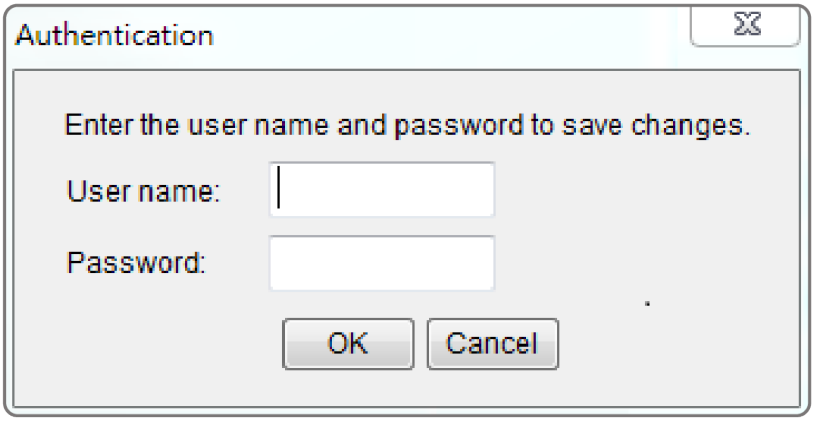


Figure 3. Fenêtre d'authentification.

8. Si l'adresse IP a été modifiée avec succès, un message s'affiche pour confirmer que la configuration IP est correcte, comme illustré dans la figure 4.

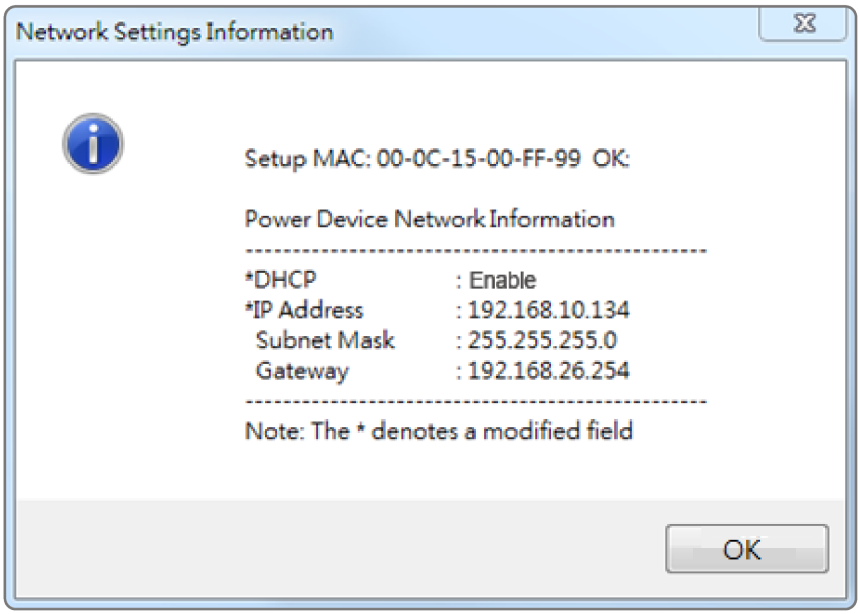


Figure 4. Message de configuration réussie de l'adresse IP.

9. En cas d'échec de la modification de l'adresse IP, un message d'avertissement s'affiche. Réessayez de modifier l'adresse IP. Si le problème persiste, reportez-vous à la section Dépannage pour obtenir de l'aide.

Méthode 2 : utilisation d'une invite de commande

1. Relevez l'adresse MAC indiquée sur l'étiquette apposée sur la carte de gestion à distance. Chaque carte de gestion possède une adresse MAC unique.

   Remarque : l'adresse MAC est indiquée sur l'étiquette apposée sur la carte.
2. Utilisez la commande ARP pour configurer l'adresse IP.

   Exemple :

   Pour attribuer l'adresse IP 192.168.10.134 à la carte de gestion à distance dont l'adresse MAC est 00-0C-15-00-FF-99, saisissez ce qui suit dans l'invite de commande sur un PC connecté au même réseau que la carte de gestion à distance.

   (1) Saisissez « `arp -s 192.168.10.134 00-0C-15-00-FF-99` » pour Windows ou « `arp -s 192.168.10.134 00:0c:15:00:ff:99` » pour Mac OS, puis appuyez sur Entrée.
3. Utilisez la commande Ping pour attribuer une taille de 123 octets à l'IP.

   (1) Saisissez « `ping 192.168.10.134 -l 123` », puis appuyez sur Entrée.

   (2) Si les réponses sont reçues, votre ordinateur peut communiquer avec l'adresse IP.

Pour sélectionner une adresse IP disponible pour la carte de gestion à distance, reportez-vous à l'annexe 1.

Interface Web

Connexion au compte utilisateur

Vous devrez entrer un nom d'utilisateur et un mot de passe pour vous connecter à l'interface, puis vous pourrez choisir votre langue préférée. Il existe deux types de compte utilisateur.

1. Administrateur
   - Nom d'utilisateur par défaut : **cyber**
   - Mot de passe par défaut : **cyber**
2. Affichage uniquement
   - Nom d'utilisateur par défaut : **device**
   - Mot de passe par défaut : **cyber**

Vous serez invité à réinitialiser le nom d'utilisateur et le mot de passe lors de la première connexion. L'administrateur a accès à toutes les fonctions, y compris à l'activation/la désactivation du compte Affichage uniquement. L'observateur a accès aux fonctions en lecture seule, mais ne peut pas modifier les paramètres.

Remarque : 1. Le compte Administrateur est également utilisé pour la connexion FTP, l'utilitaire réseau d'équipement électrique et l'utilitaire de mise à niveau et de configuration.

2. Un seul utilisateur à la fois peut se connecter et accéder à l'équipement.

Contenu Web

Remarque : l'anglais est la langue par défaut, mais vous pouvez choisir une autre langue.

[Résumé] Aperçu du fonctionnement du système et des éléments qui sont automatiquement actualisés ; les onduleurs peuvent toutefois avoir des éléments affichés différents, en fonction du modèle.

Élément	Définition
Condition actuelle	Affiche la condition de fonctionnement actuelle de l'onduleur et du capteur d'environnement.
État de l'onduleur	
Capacité de la batterie	Graphique du pourcentage de la capacité actuelle de la batterie de l'onduleur.
Charge	Graphique de la charge de l'onduleur exprimée en pourcentage du nombre de watts disponibles.
Autonomie restante	Durée pendant laquelle l'onduleur peut maintenir sa charge en étant alimenté par la batterie.
Données système	
Nom	Nom attribué à l'onduleur.
Emplacement	Description de l'emplacement de l'onduleur.
Contact	Personne à contacter concernant cet onduleur.

Disponibilité	Durée pendant laquelle le système a fonctionné en continu.
État de l'environnement	
Température	Graphique du relevé de température actuelle du capteur d'environnement.
Humidité	Graphique du relevé d'humidité actuelle du capteur d'environnement.
Données environnementales	
Nom	Nom du capteur d'environnement.
Emplacement	Emplacement du capteur d'environnement.
Événements récents de l'équipement	Liste des cinq événements les plus récents de l'équipement. Tous les événements sont liés à des changements de configuration.

[Onduleur] Les événements suivants peuvent être affichés/configurés sur la page de l'onduleur ; les onduleurs peuvent toutefois avoir des éléments affichés/configurés différents, en fonction du modèle.

[Onduleur->État] Affiche les informations de base sur l'état actuel de l'onduleur. Les éléments affichés sont automatiquement actualisés.

Élément	Définition
Entrée	
État	État actuel de l'alimentation secteur fournie à l'onduleur.
Tension	État actuel de la tension d'entrée fournie à l'onduleur.
Fréquence	Fréquence actuelle de l'alimentation secteur fournie à l'onduleur.
Bypass	
État	Affiche l'état actuel du circuit bypass.
Tension	Tension du bypass fourni à l'onduleur.
Fréquence	Fréquence du bypass fourni à l'onduleur.
Courant	Courant du bypass fourni à l'onduleur.
Facteur de puissance	Ratio entre la puissance réelle transmise au bypass et la puissance apparente du bypass.
Sortie	
État	État actuel de la puissance de sortie que l'onduleur fournit à l'équipement connecté.
Tension	Tension de sortie que l'onduleur fournit à l'équipement connecté.
Fréquence	Fréquence de sortie que l'onduleur fournit à l'équipement connecté.

Charge	Puissance tirée par l'équipement connecté exprimée en pourcentage de la capacité de charge totale de l'onduleur et affichée en watts.
Courant	Courant de sortie que l'onduleur fournit à l'équipement connecté.
Facteur de puissance	Ratio entre la puissance active transmise à la charge et la puissance apparente dans le circuit.
Puissance active	Capacité du circuit à accomplir une tâche à un moment donné.
Puissance apparente	Produit du courant et de la tension du circuit.
Puissance réactive	Portion du flux de puissance temporairement stocké sous forme de champs magnétiques ou électriques, en raison des éléments inductifs et capacitifs du réseau, puis renvoyée à la source.
Charge non critique (NCL, Non-Critical Load)	État actuel des sorties NCL.
Énergie	Relevé du compteur d'énergie de l'équipement exprimée en kWh.
Batterie	
État	État actuel de la batterie de l'onduleur.
Mode de charge	**Mode SBM :** utilisation du mode de gestion intelligente des batteries (SBM, Smart Battery Management) pour charger les batteries, ce qui contribue à prolonger la durée de vie globale des batteries, et de la technologie de charge rapide. **Mode Normal :** utilisation de la méthode de charge normale pour charger les batteries.
Contrôle de la charge	**En mode SBM :** affiche les 3 étapes de fonctionnement (mode Repos du maintien de la charge) de la gestion intelligente des batteries (SBM). **En mode Normal :** affiche le fonctionnement du chargeur en mode Normal.
Capacité restante	Capacité actuelle des batteries exprimée en pourcentage de la charge complète.
Autonomie restante	Durée estimée pendant laquelle l'onduleur peut alimenter sa charge.
Tension	Tension actuelle de la batterie de l'onduleur.
Système	
État	État de fonctionnement actuel de l'onduleur.
Température	Température de fonctionnement de l'onduleur.

Sectionneur de maintenance	État de fonctionnement actuel du sectionneur de maintenance.

[Onduleur->État de la batterie] Affiche des informations sur la batterie intégrée et les modules de batteries étendu (EBM, Extended Battery Modules), notamment la température du pack de batteries, la tension de chaque batterie du pack et l'état de l'égalisation du pack batteries.

Élément	Définition
Date de la dernière mise à jour	Date à laquelle l'état de la batterie a été mis à jour pour la dernière fois. **Mise à jour :** utilisez cette fonction pour afficher le dernier état de la batterie.
Pack	Nombre actuel de packs de batteries de l'onduleur/du module de batteries étendu.
Température	Température actuelle du pack de batteries de l'onduleur/du module de batteries étendu.
Tension	Tension actuelle de chaque batterie de l'onduleur/du module de batteries étendu.
État d'égalisation	État d'égalisation actuel de la tension des batteries du pack de batteries de l'onduleur/du module de batteries étendu. **Actif :** la fonction d'égalisation du pack de batteries est active. **Inactif :** la fonction d'égalisation du pack de batteries n'est pas active.

[Onduleur->Informations] Affiche les caractéristiques techniques de l'onduleur.

Informations	Description
Modèle	Nom du modèle d'onduleur.
Numéro de série	Numéro de série de l'onduleur.
Tension nominale	Tension de sortie nominale de l'onduleur exprimée en volts.
Fréquence de fonctionnement	Fréquence opérationnelle de la puissance de sortie de l'onduleur.
Puissance nominale	Puissance nominale de l'onduleur exprimée en volts/ampères.
Courant nominal	Courant de sortie nominal de l'onduleur exprimé en ampères.
Puissance de charge	Puissance nominale de l'onduleur exprimée en watts.
Tension nominale de la batterie	Tension nominale de fonctionnement DC de la batterie.
Version du firmware	Numéro de révision du firmware de l'onduleur. **Mise à jour :** utilisez cette fonction pour mettre à niveau le firmware de l'onduleur. Pour plus d'informations, reportez-vous à l'annexe 3.

Version du firmware USB	Numéro de révision du firmware USB de l'onduleur.
Version du firmware LCD	Numéro de révision du firmware LCD de l'onduleur.
Date de remplacement des batteries	Date du dernier remplacement des batteries. Cette date doit être définie manuellement après le remplacement des batteries ou lors de la première installation de l'unité. Si cette date n'a pas été définie, il est recommandé de le faire immédiatement.
Banc NCL	Nombre de bancs de charges non critiques.
Modules de batteries étendus	Nombre de modules de batteries externes connectés à l'onduleur. Ce nombre est configuré manuellement ; les configurations varient d'un modèle à l'autre.
Lieu d'installation	Lorsque vous cliquez sur le bouton « Le trouver », l'alarme retentit ou les voyants clignotent sur l'onduleur pour signaler le lieu spécifique aux utilisateurs. Cela les aide à identifier un onduleur donné dans une installation comportant plusieurs onduleurs.

[Onduleur->Configuration] Configure les paramètres de l'onduleur.

Élément	Définition
Puissance fournie	
Tension	Définissez la tension de sortie de l'onduleur fournie à l'équipement connecté.
Condition de panne d'alimentation secteur	
Sensibilité secteur	Lorsque l'onduleur détecte que la tension du secteur est hors plage, il passe en mode Batterie pour protéger l'équipement branché sur lui. Une faible sensibilité a une plage de tensions plus étendue et la puissance fournie peut être plus variable. La puissance d'un groupe électrogène alimenté par du carburant peut faire basculer l'onduleur en mode Batterie plus fréquemment ; dans ce cas, une faible sensibilité est recommandée. L'onduleur passe alors plus rarement en mode Batterie, ce qui permet d'économiser la puissance de la batterie. Une haute sensibilité permet à l'onduleur de fournir une puissance plus stable à l'équipement, mais il passe plus fréquemment en mode Batterie.
Seuil de tension d'entrée (ou de sortie) haut/bas	Lorsque la tension du secteur ou la tension de sortie (en fonction du modèle d'onduleur) est supérieure/inférieure au seuil, l'onduleur alimente l'équipement connecté par la batterie.

Tolérance en fréquence	Définit la plage acceptable de la fréquence d'entrée. Si elle ne se situe pas dans la plage des valeurs tolérées, l'onduleur alimente l'équipement connecté par la batterie.
Fonctionnement	
Normal	Mode de fonctionnement Normal de l'onduleur.
Mode Générateur	Si l'onduleur utilise un groupe électrogène comme puissance d'entrée, cette option doit lui permettre de fonctionner normalement. Lorsque cette option est sélectionnée, l'onduleur ne peut pas passer en mode Bypass ou ÉCO pour protéger l'équipement connecté.
Mode ÉCO	Mode économique. L'onduleur passe en mode Bypass lorsque la tension/fréquence d'entrée est en-deçà du seuil configuré. Lorsque la tension/fréquence du secteur franchit le seuil, l'onduleur bascule en mode de fonctionnement Normal. Ce mode améliore considérablement l'efficacité de l'onduleur.
Bypass manuel	Détermine s'il faut autoriser l'onduleur à passer en mode Bypass manuel. Lorsque cette option est activée, l'onduleur est forcé à passer en mode Bypass.
Bypass	**Remarque :** l'onduleur peut automatiquement passer en mode Bypass lorsque ces paramètres sont configurés.
Condition du bypass	Pas de bypass : lorsque cette option est sélectionnée, l'onduleur ne passe pas en mode Bypass et cesse de délivrer la puissance de sortie. Contrôle de la tension/fréquence : si la tension du secteur se situe dans la plage des seuils de tension et si la fréquence du secteur se situe dans la plage de la tolérance en fréquence, l'onduleur passe en mode Bypass. Sinon, il cesse de délivrer la puissance de sortie. Contrôle de la tension uniquement : l'onduleur passe en mode Bypass uniquement si la tension du secteur se situe dans la plage des seuils de tension. Sinon, il cesse de délivrer la puissance de sortie.
Bypass quand l'onduleur est hors tension	Quand l'onduleur est hors tension, il passe en mode Bypass.
Rétablissement de l'alimentation	Une fois l'alimentation secteur rétablie, l'onduleur se met automatiquement sous tension et alimente l'équipement connecté. Les paramètres suivants sont utilisés pour configurer le comportement de rétablissement de l'onduleur :

Rétablissement automatique	Si cette option est activée, l'onduleur rétablit la sortie dès que l'alimentation secteur est rétablie. Si cette option est désactivée, l'onduleur ne rétablit la sortie que lorsqu'il est manuellement mis sous tension ultérieurement.
Délai de recharge	Lorsque l'alimentation secteur est rétablie, l'onduleur commence à se recharger jusqu'à l'expiration du délai spécifié avant de rétablir la puissance de sortie.
Capacité rechargée	Lorsque l'alimentation secteur est rétablie, l'onduleur commence à se recharger jusqu'à ce que la capacité des batteries soit atteinte avant de rétablir la puissance de sortie.
Délai de retour	Le délai de retour prend effet à chaque fois que l'onduleur est mis sous tension.
Délai de ligne stable	Lorsque l'onduleur est en mode Batterie et que l'alimentation secteur est rétablie, il attend l'expiration du délai spécifié pour passer du mode Batterie au mode Secteur. Si la capacité de la batterie de l'onduleur est inférieure au seuil de batterie faible lors du rétablissement de l'alimentation secteur, l'onduleur repasse immédiatement en mode Secteur.
Batterie	
Jeu de batteries externes	Nombre de jeux parallèles et capacité des batteries.
Seuil de batterie faible	Lorsque l'onduleur est en mode Batterie, si la capacité restante est inférieure à ce seuil, une alarme sonore retentit.
Modules de batteries externes	Définit le nombre de modules de batteries externes. Cela permet d'établir une estimation précise de l'autonomie en se basant sur le nombre total de batteries connectées à l'onduleur.
Test périodique des batteries	L'onduleur teste périodiquement les batteries afin de vérifier leur bon fonctionnement. **Remarque :** seule la série Online (OL) prend en charge la fonction de gestion intelligente des batteries (SBM, Smart Battery Management). La fonction SBM teste les batteries, même si le paramètre de test périodique des batteries est désactivé.
Mode de charge	**Mode Normal :** utilisation de la méthode de charge normale pour charger les batteries. **Mode SBM :** activation de la gestion intelligente des batteries pour charger les batteries.
Contrôle de la charge	Définit l'état Activé/Désactivé pour constamment surveiller la fonction du chargeur.

Autotest au démarrage de l'onduleur	Lorsque cette option est activée, l'onduleur effectue automatiquement un autotest au démarrage. **Remarque :** l'autotest n'est pas déclenché lorsque l'onduleur effectue un redémarrage automatique.
Système	
Démarrage à froid	Définit l'aptitude de l'onduleur à démarrer en l'absence de puissance d'entrée. Lorsque cette option est activée, l'onduleur peut être mis sous tension à partir des batteries.
Alarme sonore	Si cette option est activée, l'onduleur émet une alarme sonore lorsqu'il fournit une alimentation par batterie, quand la sortie est surchargée ou en présence d'autres conditions (en fonction du modèle d'onduleur).
Fonction de relais sec	Configure l'activation du relais sec de l'onduleur lorsque la condition sélectionnée se produit. Pour plus d'informations sur les fonctions avancées de relais sec de l'onduleur, reportez-vous au manuel de l'onduleur. La fonction de relais sec peut être configurée pour s'activer dans les conditions d'alimentation suivantes : (1) Panne secteur : une panne secteur se produit et l'onduleur fonctionne en mode Batterie. (2) Batterie faible : la capacité de la batterie est trop faible pour prendre en charge l'arrêt des ordinateurs connectés. (3) Alarme : l'onduleur émet une alarme sonore en raison de la survenue d'événements d'avertissement, tels qu'une surcharge. (4) Bypass : l'onduleur est passé en mode Bypass. (5) Dysfonctionnement de l'onduleur : l'onduleur dysfonctionne peut-être à cause d'une panne de matériel.
Délai de l'économiseur d'écran	Si aucun bouton de l'onduleur n'est enfoncé et si une panne secteur ne se produit pas durant ce laps de temps, l'écran LCD passe en mode Veille.
Passage en mode Veille après tout arrêt de Remote	Si cette option est activée, l'onduleur passe en mode Veille après tout arrêt de PowerPanel® Remote + 2 minutes. **Remarque :** pour les clients PowerPanel® Business Edition, si cette option est activée, l'onduleur passe en mode Veille après une panne secteur et le temps MSDT restant + 2 minutes. Pour plus d'informations sur le temps MSDT, reportez-vous à la page d'aide dans Onduleur -> Liste PowerPanel.
Détection d'un problème de câblage	Si cette option est activée, l'onduleur détecte si le câble d'entrée n'est pas relié à la terre ou est inversé. Il est recommandé de s'assurer d'abord que le câblage de l'onduleur est relié à la terre.

Protection contre les surdécharges	Lorsque l'onduleur fonctionne en mode Batterie avec 0 % de temps configuré, RMCARD le fait basculer en mode Veille et la sortie est désactivée.
Banc de sortie non critique	
Seuil d'arrêt	Lorsqu'il fonctionne en mode Batterie, l'onduleur met ce banc de sortie NCL hors tension si la capacité restante de la batterie est inférieure à ce seuil.
Délai d'arrêt	Lorsqu'il fonctionne en mode Batterie, l'onduleur met ce banc de sortie NCL hors tension à l'expiration de ce délai.
Délai de mise sous tension	Lorsque l'alimentation secteur est rétablie, l'onduleur rétablit la sortie de ce banc de sortie NCL à l'expiration de ce délai. Cela permet d'éviter une consommation électrique excessive due au démarrage simultané de tous les équipements connectés.

[Onduleur->Commutateur principal] Active ou désactive la puissance de sortie de l'onduleur.

Élément	Définition
Redémarrer l'onduleur	Met l'onduleur hors tension, puis à nouveau sous tension.
Mettre l'onduleur hors tension	Met l'onduleur hors tension.
Veille de l'onduleur	Cette commande est disponible en mode Panne secteur. Elle fait passer l'onduleur en mode Veille jusqu'à ce que l'alimentation soit rétablie. **Remarque :** certains modèles d'onduleur ne prennent pas en charge cette commande.
Réinitialiser	Réinitialise l'action en attente pour mettre l'onduleur hors tension.
Mettre l'onduleur sous tension	Met l'onduleur sous tension.
Délai d'arrêt/de veille	Délai de mise hors tension de l'onduleur en réponse à une commande « Redémarrer l'onduleur », « Mettre l'onduleur hors tension » ou « Veille de l'onduleur ».
Durée du redémarrage	Après la mise hors tension de l'onduleur, la durée du redémarrage définit combien de temps l'onduleur attend avant de se remettre sous tension en réponse à la commande « Redémarrer l'onduleur ».

Signaler l'arrêt à PowerPanel® Remote	Sélectionnez cette option pour prévenir PowerPanel® Business Remote avant de mettre l'onduleur hors tension. Le délai d'arrêt (MST, temps max. d'arrêt des clients) de l'onduleur peut être modifié pour assurer un arrêt correct.

[Onduleur->Contrôle des bancs] Affiche l'état actuel de chaque banc de sortie et fournit une commande Marche/Arrêt pour le banc de sortie critique/non critique. Le numéro de sortie et le nom de l'équipement permettent d'identifier l'équipement associé à une sortie particulière.

Élément	Définition
Options de contrôle de banc	
MARCHE	Met immédiatement sous tension le banc critique/non critique.
ARRÊT	Met immédiatement hors tension le banc critique/non critique.
Identification du nom d'équipement	
N° de sortie	Numéro de sortie d'onduleur, tel que désigné par la configuration des sorties (en fonction du modèle d'onduleur).
Nom d'équipement	Nom d'équipement attribué à cette sortie.

Remarque : seul l'onduleur commutable à banc de sortie critique prend en charge la commande Marche/Arrêt pour le banc de sortie critique.

[Onduleur->Diagnostics] La page **Onduleur/Diagnostics** permet de vérifier que les conditions de fonctionnement des batteries de l'onduleur sont adéquates. Vous pouvez également procéder à un étalonnage de l'autonomie pour permettre une estimation précise de la charge connectée.

Élément	Définition
Test des batteries	Le **test des batteries** force l'onduleur à passer en mode Batterie pendant 10 secondes. Cela permet à l'utilisateur de vérifier l'état de la batterie et d'obtenir des informations sur la batterie, notamment les résultats et la date du dernier test des batteries. Cliquez sur le bouton « **Démarrer** » pour démarrer le test des batteries. Les informations s'affichent à la fin du test des batteries. **Remarque :** « N/A » signifie que le modèle d'onduleur n'offre pas cette fonction.

Résultats du dernier test	Résultats du test des batteries le plus récent. **Succès :** la batterie a fonctionné normalement durant le test. **Échec :** la batterie a échoué au test. En cas d'échec du test des batteries, procédez comme suit : Recommencez le test des batteries et remplacez les batteries si le test échoue à nouveau. Contactez **CyberPower** pour obtenir de l'aide si le test des batteries échoue après le remplacement des batteries.
Date du dernier test	Date du test des batteries le plus récent.
Estimation de l'autonomie	**La** fonction d'estimation de l'autonomie décharge les batteries de l'onduleur de la capacité des batteries, au moment où l'estimation est demandée, à une capacité proche de zéro avec la charge actuelle. Les résultats de l'estimation de l'autonomie indiquent l'autonomie, l'état de l'estimation et la date de la dernière estimation. Lorsque l'estimation de l'autonomie est initiée, l'équipement connecté est alimenté par les batteries jusqu'à ce qu'elles soient déchargées (capacité proche de zéro). Une fois les batteries déchargées jusqu'à cette capacité, l'équipement connecté est alimenté par le secteur. Les
Estimation de l'autonomie	batteries sont automatiquement rechargées une fois l'estimation réalisée. **Remarque :** cette autonomie estimée peut varier en fonction de la charge et du niveau de charge des batteries au moment de l'estimation de l'autonomie. Les batteries sont automatiquement rechargées une fois l'estimation réalisée. Les utilisateurs peuvent cliquer sur le bouton « Démarrer » pour initier l'estimation de l'autonomie. Cliquez sur le bouton « Abandonner » pour interrompre l'estimation de l'autonomie. Les résultats s'affichent à la fin de l'estimation ou après son abandon.
Autonomie estimée	Autonomie estimée des batteries avec la charge actuelle.
Résultats de la dernière estimation	Résultats de la dernière estimation de l'autonomie. **Succès :** l'estimation de l'autonomie a été réalisée et les batteries sont fonctionnelles. **Annulation :** l'estimation de l'autonomie a été interrompue.
Date de la dernière estimation	Date à laquelle la dernière estimation a été réalisée.

[Onduleur->Planification] Configure l'onduleur pour qu'il s'arrête et redémarre automatiquement à des heures programmées (Une fois/Quotidiennement/Hebdomadairement). La page **Planification** gère les arrêts planifiés et répertorie toutes les planifications configurées. Chaque ligne de planification indique quand elle prendra effet.

[Une fois] : l'utilisateur peut définir un événement ponctuel pour l'arrêt et le redémarrage de l'onduleur.
[Quotidiennement] : définit une reproduction quotidienne de l'arrêt et du redémarrage de l'onduleur.
[Hebdomadairement] : définit une reproduction hebdomadaire de l'arrêt et du redémarrage de l'onduleur.

1. Cliquez sur l'option [Une fois], [Quotidiennement] ou [Hebdomadairement], puis sur « Suivant>> » et entrez la date et l'heure d'arrêt de l'onduleur. Sélectionnez [Jamais], [Instantanément] ou la date et l'heure de redémarrage de l'onduleur. Sélectionnez le banc à contrôler et cliquez sur « Arrêt des clients » pour configurer un arrêt correct de tous les clients. Vous pouvez entrer un « Nom » pour cette planification.
2. Cliquez sur « Appliquer » pour ajouter l'élément à la planification. Cliquez sur « Réinitialiser » pour rétablir les paramètres par défaut.
3. Les paramètres enregistrés sont répertoriés dans le menu [Planification].
4. Pour supprimer l'action planifiée, il suffit de cliquer sur le nom de l'élément répertorié dans le menu [Planification] et de cliquer sur « Supprimer ».

Remarque : le système de gestion permet d'entrer jusqu'à 10 planifications.

[Onduleur->Wake on Lan] Cette fonction permet d'éveiller un ordinateur via le réseau. Entrez l'adresse IP de cet ordinateur lorsqu'il est sous tension ; le système recherche alors son adresse MAC. Il est possible de définir jusqu'à 50 adresses IP.

Élément	Définition
PowerPanel® Remote	
Charger/synchroniser avec la liste PowerPanel® Remote	Activez cette option pour charger et synchroniser la liste des clients WoL avec la liste PowerPanel® Remote.
Conditions d'éveil	
Mise sous tension de l'onduleur	La sélection de cette option permet à RMCARD d'envoyer le signal WoL aux ordinateurs PowerPanel® Remote connectés lorsque l'onduleur est mis sous tension.
Rétablissement de l'alimentation secteur et fourniture de la sortie	La sélection de cette option permet à RMCARD d'envoyer le signal WoL aux ordinateurs PowerPanel® Remote connectés lorsque l'alimentation secteur est rétablie et que l'onduleur est mis sous tension.
Listes WoL	

Liste WoL Remote	Lorsque l'option « Charger/synchroniser avec la liste PowerPanel® Remote » est activée, elle répertorie les adresses IP/MAC des PC PPB Remote ici.
Liste manuelle WoL	Liste manuelle Wake on Lan.

Remarque : les paramètres BIOS de l'ordinateur PowerPanel® Remote doivent prendre en charge WoL et être configurés en conséquence.

[Onduleur->EnergyWise] L'initiative EnergyWise vise à réduire la consommation énergétique des équipements connectés à un réseau Cisco. Grâce à cette compatibilité, la carte de gestion à distance CyberPower peut prendre en charge les autres entités EnergyWise : ils sont plus faciles à surveiller et à contrôler et permettent d'optimiser la consommation d'énergie dans le cadre du programme EnergyWise.

Élément	Définition
Configuration	
Version	Version d'EnergyWise prise en charge.
EnergyWise	Permet la prise en charge Cisco EnergyWise.
Port de service	Numéro de port utilisé pour communiquer avec les équipements EnergyWise (doit être le même que celui configuré dans le commutateur de réseau).
Nom de domaine	Nom de domaine de la solution EnergyWise (doit être le même que celui configuré dans le commutateur de réseau).
Cache hors état	Active/désactive les entrées d'extrémité à stocker dans le cache de la liste EnergyWise du commutateur après un redémarrage.
Mode sécurisé	Permet l'utilisation d'un secret partagé par EnergyWise.
Secret partagé	Secret du domaine EnergyWise.
Liste de nœuds	La liste parent/enfant d'EnergyWise montre toutes les entités EnergyWise et permet aux utilisateurs de configurer des attributs d'entité EnergyWise.
Nom	Nom utilisé pour identifier chaque sortie.
Rôle	Ce paramètre est une chaîne utilisée pour décrire la fonction de l'entité (longueur max. : 31 caractères).
Mots clés	Ce paramètre est une chaîne utilisée pour décrire l'entité (longueur max. : 31 caractères).
Importance	Ce paramètre est une valeur comprise entre 1 et 100 qui indique l'importance de l'entité (de haute à basse).

[Onduleur->Liste PowerPanel®] Affiche des informations sur les ordinateurs PowerPanel® Business connectés. La connexion est établie par PowerPanel® Business. Les systèmes répertoriés sont supprimés s'ils restent déconnectés pendant 1 heure.

Élément	Définition
Configuration	
Durée d'arrêt Remote max. (MST)	Durée maximale pendant laquelle tous les ordinateurs Remote connectés doivent s'arrêter.
Délai d'arrêt Remote max. (MSDT)	Valeur maximale requise entre la panne secteur et l'arrêt correct de tous les clients.
Liste	
Type	Type de PowerPanel® Business • Remote • Management
Condition d'arrêt	Condition d'arrêt de PowerPanel® Business • Aucune • Panne secteur • Batteries faibles • Autonomie insuffisante
État	État de PowerPanel® Business • Connexion • Normal • Arrêt en cours • Arrêt terminé

Remarque : il n'est pas recommandé d'établir la connexion de PowerPanel® Business Edition ou PowerPanel® Business à RMCARD en même temps.

[Envir] Les éléments suivants peuvent être affichés/configurés via la page Envir. Notez que l'onglet Envir apparaît uniquement lorsque ENVIROSENSOR est connecté à RMCARD.

[Envir->État] Affiche les informations de base du capteur d'environnement et des entrées de fermeture de contact.

Élément	Définition
Informations	
Nom	Nom du capteur d'environnement.
Emplacement	Emplacement du capteur d'environnement.
Température	
Valeur actuelle	Température actuelle de l'environnement.
Maximum	Température la plus élevée et heure de détection par le capteur d'environnement.

Minimum	Température la moins élevée et heure de détection par le capteur d'environnement.
Humidité	
Valeur actuelle	Humidité actuelle de l'environnement.
Maximum	Humidité la plus élevée et heure de détection par le capteur d'environnement.
Minimum	Humidité la moins élevée et heure de détection par le capteur d'environnement.
Contact	Nom et état (Normal/Anormal) de chaque contact de relais sec d'entrée.

[Envir->Configuration] Configure les paramètres du capteur d'environnement.

Élément	Définition
Informations	
Nom	Nom utilisé pour identifier le capteur d'environnement.
Emplacement	Endroit où se trouve le capteur d'environnement.
Température	
Seuil haut	Limite supérieure de la température normale.
Seuil bas	Limite inférieure de la température normale.
Hystérésis	Point auquel la différence entre les seuils de température haut et bas passe d'anormale à normale.
Taux de changement	Taux utilisé pour définir un changement de température anormal.
Unité	Unité de mesure de la température.
Humidité	
Seuil haut	Limite supérieure de l'humidité normale.
Seuil bas	Limite inférieure de l'humidité normale.
Hystérésis	Point auquel la différence entre les seuils d'humidité haut et bas passe d'anormale à normale.
Taux de changement	Taux utilisé pour définir un changement d'humidité anormal.
Contact	Entrez le nom de chaque relais à contacts secs d'entrée et utilisez le menu déroulant pour définir l'état normal de chacun d'eux.

[Journaux->Journaux d'événements] Affiche la liste des événements et une brève description de chaque événement avec la marque d'horodatage.

Remarque : 1. Les événements enregistrables sont répertoriés sous « Système->Notifications->Action d'événement ».

2. L'heure enregistrée utilise le format d'horloge 24 heures.

[Journaux->Enregistrements d'état] Cette page permet de visualiser les journaux d'état de l'onduleur et de l'environnement ; différents éléments peuvent toutefois s'afficher, en fonction du produit.

Tous les éléments ont la même définition, car ils sont dans l'état de l'onduleur ou de l'environnement.

- Entrée min. (V) : tension d'entrée minimale du secteur de l'enregistrement précédent.
- Entrée max. (V) : tension d'entrée maximale du secteur de l'enregistrement précédent.
- Entrée (Hz) : Fréquence actuelle de l'alimentation secteur fournie à l'onduleur.
- Sortie (V) : tension de sortie que l'onduleur fournit à l'équipement connecté.
- Sortie (Hz) : fréquence de sortie que l'onduleur fournit à l'équipement connecté.
- Charge (%) : pourcentage de la puissance totale que l'onduleur fournit à l'équipement connecté.
- Capacité (%) : pourcentage de la capacité actuelle de la batterie de l'onduleur.
- Autonomie restante : durée estimée pendant laquelle l'onduleur peut alimenter la charge connectée en mode Batterie.
- Température (°C ou °F) : température actuelle du capteur d'environnement.
- Humidité (% HR) : humidité actuelle du capteur d'environnement.

[Journaux->Enregistrements d'énergie] La page Enregistrements d'énergie affiche une liste d'enregistrements d'énergie avec une marque d'horodatage.

Élément	Définition
Énergie	Énergie consommée par l'équipement durant un intervalle donné, mesurée en kWh.
Coût	Coût de l'énergie consommée par l'équipement durant un intervalle donné.
CO2	Émissions de CO2 de l'équipement durant un intervalle donné.
Énergie cumulée	Énergie cumulée consommée par l'équipement depuis la dernière réinitialisation, mesurée en kWh.
Coût cumulé	Coût cumulé de l'énergie consommée par l'équipement depuis la dernière réinitialisation.
CO2 cumulé	Émissions de CO2 cumulées de l'équipement depuis la dernière réinitialisation.

[Journaux->Graphique] Cette page affiche les données de l'enregistrement d'état. La fonction graphique facilite la visualisation des enregistrements d'état.

Élément	Définition
Période du graphique	Période utilisée pour tracer le graphique. L'affichage des périodes longues prend plus de temps.
Données du graphique	Données utilisées pour tracer le graphique. Plus il y a de données sélectionnées, plus le traçage du graphique est long.
Nœud de graphique	Lorsqu'elle est sélectionnée, l'option « Afficher tous les nœuds en détail » affiche tous les points sur la ligne ; placez le curseur sur le point de données pour afficher des informations sur ce point.
Lancer le graphique dans une nouvelle fenêtre	Lorsque cette case est cochée, le graphique détaillé s'ouvre dans une nouvelle page.

[Journaux->Maintenance] Cette page permet de sélectionner les paramètres « Journaux d'événements » et « Enregistrements d'état ». L'application fournit des informations sur le nombre d'événements enregistrés avant que le journal soit complet.

Élément	Définition
Journaux d'événements	
Effacer tous les journaux	Efface les journaux d'événements existants.
Nombre d'événements	Nombre d'événements existants et nombre maximal d'événements pouvant être enregistrés. Une fois le nombre maximal atteint, les nouveaux événements écrasent les événements plus anciens dans la mémoire.
Enregistrer les journaux d'événements	Enregistre les journaux d'événements existants comme un fichier texte.
Enregistrements d'état	
Intervalle d'enregistrement	Définit la fréquence de l'enregistrement des données d'état. Un court intervalle génère des enregistrements plus fréquents, mais épuise plus rapidement la mémoire disponible. Un long intervalle génère des enregistrements moins fréquents, mais enregistre les donnés pour une période plus longue.
Effacer tous les enregistrements	Efface les enregistrements d'état existants.

Temps restant	Temps durant lequel les enregistrements ont été conservés. Un court intervalle d'enregistrement diminue le temps restant, tandis qu'un long intervalle d'enregistrement l'augmente. Une fois le nombre maximal atteint, les nouveaux enregistrements d'état écrasent les enregistrements d'état plus anciens dans la mémoire.
Enregistrer les enregistrements d'état	Enregistre les enregistrements d'état comme un fichier texte.
Enregistrements d'énergie	
Intervalle d'enregistrement	Fréquence d'enregistrement des données sur l'énergie.
Effacer les enregistrements entiers	Efface les enregistrements d'énergie existants.
Taux d'électricité	Ratio entre le coût de l'énergie et l'énergie.
Émissions de CO2	Ratio entre les émissions de CO2 et l'énergie.
Enregistrer les enregistrements d'énergie	Enregistre les journaux d'événements existants comme un fichier texte.

Remarque : les journaux d'événements et les enregistrements d'état utilisent une mémoire de type premier entré, premier sorti. Lorsque la mémoire est pleine, les données les plus anciennes sont écrasées.

[Journaux->Syslog] Permet aux utilisateurs de définir le serveur Syslog et d'envoyer un message de test.

Élément	Définition
Syslog	Active ou désactive la fonction Syslog.
Code de dispositif	Sélectionnez le dispositif Syslog.
Adresse IP du serveur	Adresse IP du serveur Syslog.
Port serveur	Port UDP utilisé par le serveur Syslog.
Envoyer un test	Envoie un message de test au serveur Syslog.

[Système->Général->Heure] Affiche la date et l'heure système, et permet aux utilisateurs de les définir manuellement ou via le serveur NTP (Network Time Protocol).

Élément	Définition
Paramètres actuels	Affiche la date et l'heure actuelles sur l'état de la carte, et le temps restant jusqu'à la prochaine mise à jour du protocole NTP.
Configuration de l'heure système	
Fuseau horaire	Choisissez le fuseau horaire (GMT, Greenwich Mean Time) de RMCARD.

Via le serveur NTP	Entrez l'adresse IP/le nom de domaine des serveurs NTP et définissez la fréquence de mise à jour de la date et de l'heure par le serveur NTP. Cliquez sur « Mettre à jour maintenant » pour effectuer une mise à jour immédiate.
Configuration manuelle	Entrez la date et l'heure dans le format désigné.

[Système->Général->Identification] Attribue le nom du système, le contact et l'emplacement.

Élément	Définition
Nom	Nom de l'équipement.
Emplacement	Emplacement de l'équipement d'alimentation.
Contact	Personne à contacter concernant cet équipement.

[Système->Général->Heure d'été] Règle l'heure d'été.

Élément	Définition
Configuration de l'heure d'été	
Désactiver	Désactive l'heure d'été.
Heure d'été standard des États-Unis	Définit l'heure d'été standard des États-Unis Début : 2h00, deuxième dimanche de mars. Fin : 2h00, premier dimanche de novembre.
Heure d'été manuelle	Réglage manuel de l'heure d'été.

[Système->Sécurité->Gestion] Définit l'authentification de la connexion et l'authentification logicielle.

Élément	Définition
Authentification de la connexion	
Compte local	Utilisez les paramètres Administrateur ou Observateur du compte local pour vous connecter.
RADIUS, compte local	Utilisez les paramètres de configuration RADIUS pour vous connecter. En cas d'échec de l'authentification RADIUS, les paramètres du compte local sont utilisés pour la connexion.
RADIUS uniquement	Utilisez les paramètres de configuration RADIUS pour vous connecter.
LDAP, compte local	Utilisez les paramètres de configuration LDAP pour vous connecter. En cas d'échec de l'authentification LDAP, les paramètres du compte local sont utilisés pour la connexion.
LDAP uniquement	Utilisez les paramètres de configuration LDAP pour vous connecter.

Authentification logicielle	
Phrase secrète	Phrase d'authentification utilisée pour communiquer avec **PowerPanel®** Business Remote. **Remarque :** pour plus d'informations, reportez-vous à l'annexe 4.
Adresse IP du gestionnaire Administrateur/Observateur	Détermine quelle adresse IP est autorisée à accéder à l'équipement via le compte Administrateur ou Observateur. Pour accéder à la carte de gestion à distance à partir d'une adresse IP, définissez-en une sur 0.0.0.0 ou 255.255.255.255. **Remarque :** il est possible d'autoriser une série d'adresses IP en entrant le masque de sous-réseau. Par exemple, 192.168.20.0/16 signifie que l'adresse IP ayant pour sous-réseau 192.168.0.0 a une autorisation d'accès.

[Système->Sécurité->Compte local] Cette page permet de configurer le compte de connexion.

Informations	Description
Administrateur	L'administrateur a le plein accès aux paramètres de configuration en lecture/écriture.
Observateur	L'observateur a un accès limité en lecture seule.

Modifier le compte Administrateur :

1. Entrez le nom d'utilisateur.
2. Entrez le mot de passe actuel.
3. Définissez l'adresse IP du gestionnaire *(facultatif).*
4. Entrez le nouveau mot de passe.
5. Confirmez le mot de passe.
6. Cliquez sur « Appliquer ».

Remarque : la longueur maximale du nom d'utilisateur et du mot de passe est de 63 caractères.

Modifier le compte Observateur :

1. Sélectionnez « Autoriser l'accès » pour activer le compte Observateur.
2. Entrez le nom d'utilisateur.
3. Définissez l'adresse IP du gestionnaire *(facultatif).*
4. Entrez le nouveau mot de passe.
5. Confirmez le mot de passe.
6. Cliquez sur « Appliquer ».

Remarque : la longueur maximale du nom d'utilisateur et du mot de passe est de 15 caractères.

[Système->Sécurité->Configuration RADIUS] Une fois le serveur RADIUS approprié configuré, la carte de gestion à distance peut utiliser le nom d'utilisateur et le mot de passe définis sur le serveur RADIUS pour se connecter.

Élément	Définition
Adresse IP du serveur	Adresse IP/nom de domaine du serveur RADIUS.
Secret partagé	Secret partagé du serveur RADIUS.
Port serveur	Port UDP utilisé par le serveur RADIUS.
Type d'authentification	Type de protocole d'authentification du serveur RADIUS. • Protocole d'authentification du mot de passe (PAP, Password Authentication Protocol) • Protocole d'authentification de la connexion basée sur un défi (CHAP, Challenge-Handshake Authentication Protocol)
Tester les paramètres	Teste le serveur RADIUS en utilisant les paramètres du nom d'utilisateur et du mot de passe. Si l'authentification réussit, les paramètres sont enregistrés.
Ignorer le test	Enregistre les paramètres du serveur RADIUS sans les tester.

Remarque : pour plus d'informations sur la configuration des comptes sur les serveurs RADIUS, reportez-vous à l'annexe 2.

[Système->Sécurité->Configuration LDAP] Une fois le serveur LDAP approprié configuré, la carte de gestion à distance peut utiliser le nom d'utilisateur et le mot de passe définis sur le serveur LDAP pour se connecter.

Élément	Définition
Serveur LDAP	
Serveur LDAP	Adresse IP/nom de domaine du serveur LDAP.
SSL LDAP	Permet de communiquer avec le serveur LDAP par LDAPS.
Port	Port TCP utilisé par le serveur LDAP(S).
Base DN utilisateur	Base DN du serveur LDAP.
Attribut de connexion	Attribut de connexion de l'entrée utilisateur LDAP (par exemple : cn ou uid).
Authentification LDAP	

Mode d'authentification	Identifie la méthode à utiliser pour l'authentification. • Anonyme : requête de liaison en utilisant l'authentification simple avec un DN de liaison de longueur nulle et un mot de passe de longueur nulle. • Utilisateur accrédité : requête de liaison en utilisant l'authentification simple avec un DN de liaison et un mot de passe de liaison. • Par connexion utilisateur : requête de liaison en utilisant l'authentification simple avec un Base DN utilisateur et un mot de passe de connexion.
Autorisation LDAP	
Mode d'autorisation	Identifie la méthode à utiliser pour l'autorisation. • Par attribut d'utilisateur : détermine le niveau d'accès par attribut d'utilisateur et valeur d'attribut d'utilisateur. • Par groupe : détermine le niveau d'accès par groupe avec recherche d'informations DN, telles que le Base DN de groupe suivant, l'attribut de groupe et la valeur d'attribut de groupe.
Type de serveur LDAP	
Serveur LDAP générique	Sélectionne le type de serveur LDAP OPENLDAP.
Active Directory	Sélectionne le type de serveur LDAP Windows AD.
Domaine AD	Domaine AD du serveur Active Directory.
Test LDAP	
Tester les paramètres	Teste le serveur LDAP(S) en utilisant les paramètres du nom d'utilisateur et du mot de passe. Si l'authentification réussit, les paramètres sont enregistrés.
Ignorer le test	Enregistre les paramètres du serveur LDAP(S) sans les tester.

Remarque : pour plus d'informations sur la configuration des comptes sur les serveurs LDAP et Windows AD, reportez-vous à l'annexe 2.

[Système->Sécurité->Contrôle de session] Définit les paramètres d'expiration pour déconnecter automatiquement les sessions ouvertes.

Élément	Définition
Expiration	Période (en minutes) pendant laquelle le système attend avant de se déconnecter automatiquement.

[Système->Service réseau->TCP/IPv4] Affiche les paramètres TCP/IPv4 actuels. Définit les paramètres serveur DHCP et DNS.

Élément	Définition
Configuration actuelle	Affiche les paramètres TCP/IP actuels : adresse IP, masque de sous-réseau, passerelle et serveur DNS.

DHCP	Sélectionnez l'option « Activer DHCP » et cliquez sur « Appliquer » pour obtenir l'adresse IP, le masque de sous-réseau et la passerelle du serveur DHCP. Sélectionnez l'option « Obtenir l'adresse DNS de DHCP » et cliquez sur « Appliquer » pour obtenir l'IP du DNS du serveur DHCP.
Manuel	Entrez directement les paramètres TCP/IP et cliquez sur « Appliquer ».

[Système->Service réseau->TCP/IPv6] Affiche et configure les paramètres IPv6 actuels.

Élément	Définition
Interface IPv6	Affiche l'adresse IPv6 actuelle.
Passerelle IPv6	Affiche la passerelle IPv6 actuelle.
Configuration IPv6	
Accès	Définissez le service IPv6 sur Activer ou Désactiver.
Mode d'adressage	
Contrôle du routeur	L'adresse IPv6 est attribuée via l'une des méthodes suivantes telle que configurée dans les paramètres du routeur : configuration automatique d'adresse sans état, DHCPv6 sans état ou DHCPv6 avec état.
Manuel	L'adresse IPv6 est attribuée manuellement.
Adresse IPv6 manuelle	Si le paramètre Manuel est sélectionné, entrez directement l'adresse IPv6.

[Système->Service réseau->Service SNMPv1] Permet aux utilisateurs d'utiliser un NMS et de configurer les paramètres SNMPv1 appropriés.

Élément	Définition
Service SNMPv1	
Autoriser l'accès	Définissez le service SNMP sur Activer ou Désactiver.
Contrôle d'accès SNMPv1	
Communauté	Nom utilisé pour accéder à cette communauté depuis un système de gestion de réseau (NMS, Network Management System). La longueur du champ doit être de 1 à 15 caractères.

Adresse IP	L'accès NMS peut être restreint par la saisie d'une adresse IP ou d'un masque de sous-réseau IP spécifique. Les règles suivantes s'appliquent aux masques de sous-réseau : • 192.168.20.255 : accès uniquement par un NMS sur le segment 192.168.20. • 192.255.255.255 : accès uniquement par un NMS sur le segment 192. • 0.0.0.0 (paramètre par défaut) ou 255.255.255.255 : accès par n'importe quel NMS sur n'importe quel segment.
Type d'accès	Action autorisée pour le NMS via la communauté et l'adresse IP. • Lecture seule : commande GET autorisée à tout moment ; commande SET restreinte. • Écriture/lecture : commande GET autorisée à tout moment ; commande SET autorisée à tout moment, à moins qu'une session utilisateur soit active. • Interdit : commandes GET et SET restreintes.

[Système->Service réseau->Service SNMPv3] Permet aux utilisateurs d'utiliser un NMS et de configurer les paramètres SNMPv3 appropriés.

Élément	Définition
Service SNMPv3	
Autoriser l'accès	Définissez le service SNMPv3 sur Activer ou Désactiver.
Contrôle d'accès SNMPv3	
Nom d'utilisateur	Nom utilisé pour identifier l'utilisateur SNMPv3. La longueur du champ doit être de 1 à 31 caractères.
Mot de passe d'authentification	Mot de passe utilisé pour générer la clé d'authentification. La longueur du champ doit être de 16 à 31 caractères.
Mot de passe de confidentialité	Mot de passe utilisé pour générer la clé de chiffrement. La longueur du champ doit être de 16 à 31 caractères.
Adresse IP	L'accès NMS peut être restreint par la saisie d'une adresse IP ou d'un masque de sous-réseau IP spécifique. Les règles suivantes s'appliquent aux masques de sous-réseau : • 192.168.20.255 : accès uniquement par un NMS sur le segment 192.168.20. • 192.255.255.255 : accès uniquement par un NMS sur le segment 192. • 0.0.0.0 (paramètre par défaut) ou 255.255.255.255 : accès par n'importe quel NMS sur n'importe quel segment.
Type d'authentification	Type de hachage utilisé pour l'authentification.

Type de confidentialité	Type de chiffrement/déchiffrement des données.

Remarque : le protocole de confidentialité ne peut pas être sélectionné si aucun protocole d'authentification n'est sélectionné.

[Système->Service réseau->Service Web] Sélectionnez Activer pour autoriser l'accès au service HTTP ou HTTPS ; configure automatiquement le port TCP/IP.

Élément	Définition
Accès	
Autoriser l'accès	Permet l'accès au service HTTP ou HTTPS. Le service HTTPS prend en charge la liste d'algorithmes de chiffrement suivante : • AES (256/128 bits) • Camellia (256/128 bits) • DES (168 bits)
Paramètres HTTP	
Port HTTP	Port TCP/IP du protocole HTTP (Hypertext Transfer Protocol) (80 par défaut)
Paramètres HTTPS	
Port HTTPS	Port TCP/IP du protocole HTTPS (Hypertext Transfer Protocol Secure) (443 par défaut)
État du certificat	• Certificat valide (ou certificat non valide) : cliquez pour afficher des informations détaillées sur le certificat. • Charger le certificat : cliquez pour charger un certificat et remplacer le certificat actuel. **Remarque :** le certificat doit être chargé dans un format PEM (Privacy Enhanced Mail) standard.

[Système->Service réseau->Service de console] Sélectionnez Activer pour autoriser l'accès au service Telnet ou SSH ; configure le port TCP/IP utilisé par Telnet ou SSH pour communiquer.

Élément	Définition
Accès	
Autoriser l'accès	Autorise l'accès à Telnet ou SSH version 2, qui chiffre la transmission des noms d'utilisateur, mots de passe et données.
Paramètres Telnet	
Paramètres SSH	
Port SSH	Port TCP/IP (22 par défaut) utilisé par SSH pour communiquer.

État de la clé d'hôte	• Affiche l'état de l'empreinte de clé d'hôte pour indiquer si elle est valide ou non. • Charger la clé d'hôte : cliquez pour charger une clé d'hôte et remplacer la clé d'hôte actuelle. • Exporter la clé d'hôte : cliquez pour exporter une clé d'hôte actuelle.

Remarque : pour renforcer la sécurité, les utilisateurs peuvent remplacer le port par tout port inutilisé de 5000 à 65535. Les utilisateurs doivent ensuite spécifier un port différent de celui par défaut pour obtenir l'accès. Les clients Telnet nécessitent que les utilisateurs ajoutent un espace et le numéro de port ou deux points et le numéro de port à la ligne de commande pour accéder à la console de contrôle.

[Système->Service réseau->Service FTP] Permet aux utilisateurs d'activer/désactiver le service serveur FTP et de configurer le port TCP/IP du serveur FTP (21 par défaut).

Élément	Définition
Autoriser l'accès	Permet l'accès au serveur FTP.
Port de service	Port TCP/IP du serveur FTP (21 par défaut) Les utilisateurs peuvent remplacer le port par tout port inutilisé de 5000 à 65535 pour renforcer la sécurité.

Remarque : le serveur FTP est utilisé pour mettre à niveau le firmware. Pour plus d'informations sur le processus de mise à niveau, reportez-vous à la section « Mise à niveau du firmware ».

[Système->Notifications->Action d'événement] Configure les paramètres de notification pour chaque événement d'équipement. Les événements sont catégorisés pour faciliter la gestion.

- Journal : enregistre l'événement dans les journaux d'événements.
- E-mail : envoie un e-mail à un utilisateur donné (nécessite un serveur SMTP disponible).
- Trap : trap SNMP envoyé à une adresse IP donnée.
- Syslog : envoie un message Syslog à un serveur Syslog donné (nécessite un serveur Syslog disponible).
- SMS : envoie un message succinct à un numéro de téléphone mobile donné (nécessite un fournisseur de services SMS).

[Système->Notifications->Serveur SMTP] Après la configuration du serveur SMTP approprié, un e-mail de notification d'événement peut être envoyé aux destinataires lorsque certains événements se produisent.

Élément	Définition
Fournisseur de services	Fournisseur de services du compte e-mail. Deux options existent : Général et Gmail.
Général	Sélectionnez le fournisseur de services Général. Complétez tous les champs de paramètres et cliquez sur Appliquer pour enregistrer.

Gmail	Sélectionnez le fournisseur de services Gmail. Cliquez sur Autoriser pour autoriser l'envoi d'une notification par e-mail. Entrez ensuite le nom de l'expéditeur et cliquez sur Appliquer pour enregistrer les paramètres.
Adresse du serveur SMTP	Adresse IP ou nom d'hôte du serveur SMTP utilisé pour envoyer des notifications par e-mail.
Adresse e-mail de l'expéditeur	Adresse e-mail utilisée pour envoyer la notification par e-mail.
Authentification	Sélectionnez cette option si le serveur SMTP doit authentifier l'utilisateur.
Compte	Compte utilisé pour l'authentification avec une longueur maximale de 63 caractères.
Mot de passe	Mot de passe utilisé pour l'authentification avec une longueur maximale de 63 caractères.
Connexion sécurisée	Active la sécurité TLS ou SSL.
Port de service	Numéro du port utilisé pour communiquer avec le serveur SMTP.

[Système->Notifications->Destinataires d'e-mails] Configurez jusqu'à cinq destinataires qui recevront des notifications par e-mail lorsque les événements configurés se produiront.

Pour ajouter un nouveau destinataire, cliquez sur « Nouveau destinataire ». Pour modifier ou supprimer un destinataire existant, cliquez sur son adresse e-mail. Pour vérifier que les paramètres SMTP et les destinataires d'e-mails sont correctement définis, cliquez sur le bouton « TEST » pour envoyer un message de test.

[Système->Notifications->Récepteurs de trap] Configurez jusqu'à 10 récepteurs de TRAP SNMP par adresse IP (IPv6 pris en charge). SNMPv1 et v3 sont pris en charge. Les récepteurs de TRAP répertoriés recevront une notification lorsque les événements d'équipement se produiront.

Pour ajouter un nouveau récepteur, cliquez sur « Nouveau récepteur ». Pour modifier ou supprimer un récepteur existant, cliquez sur son adresse IP ou sur son nom. Pour vérifier que les traps peuvent être correctement reçus, cliquez sur le bouton « TEST ».

[Système->Notifications->Service SMS] Le service de message succinct (SMS, Short Message Service) est un service de communication utilisé par les systèmes de communication mobile. L'utilisation de protocoles de communication standardisés permet l'échange de messages textuels succincts entre les équipements mobiles. Le système offre 4 méthodes aux utilisateurs pour choisir comment ils veulent envoyer des messages.

Élément	Description
Le fournisseur de services est Clickatell	Sélectionnez l'option **Clickatell** dans le champ Méthode SMS. Renseignez tous les détails du compte, notamment les champs Nom d'utilisateur, Mot de passe et ID HTTP API. Par exemple : Clickatell (compte avant 2016/11) Nom d'utilisateur Nom Mot de passe Passwd ID HTTP API 3234599 Clickatell (compte après 2016/11) ID HTTP API 3234599
Le fournisseur de services accepte HTTP GET	Cette spécification du fournisseur de services SMS est requise avant d'utiliser la méthode **HTTP GET**. Sélectionnez l'option Utilisation de **HTTP GET** dans le champ Méthode SMS. Insérez le numéro de téléphone mobile du destinataire E_PHONE_NUMBER et le message d'événement E_PHONE_MESSAGE décrits par la spécification du fournisseur de services SMS, puis complétez le champ URL. Les expressions seront remplacées par le contenu adéquat avant l'envoi du message par le fournisseur de services SMS. Par exemple : URL http://ServiceProviderURL?user=Nom&password=Passwd&api_id=3234599&to=E_PHONE_NUMBER&text=E_MESSAGE
Le fournisseur de services accepte HTTP POST	Cette spécification du fournisseur de services SMS est requise avant d'utiliser la méthode HTTP POST pour distribuer des messages via le fournisseur de services SMS. Sélectionnez l'option Utilisation de **HTTP POST** dans le champ Méthode SMS. Insérez le numéro de téléphone mobile du destinataire E_PHONE_NUMBER et le message d'événement E_PHONE_MESSAGE décrits par la spécification du fournisseur de services SMS, puis complétez les champs POST URL et POST BODY. Les expressions seront remplacées par le contenu adéquat avant l'envoi du message par le fournisseur de services SMS. Par exemple : URL http://ServiceProviderURL Contenu user=Nom&password=Passwd&api_id=3234599&to=E_PHONE_NUMBER&text=E_MESSAGE

Le fournisseur de services accepte l'e-mail (SMTP)	Cette spécification du fournisseur de services SMS est requise avant d'utiliser l'e-mail pour distribuer des messages via le fournisseur de services SMS. Sélectionnez l'option Utilisation de l'e-mail dans le champ Fournisseur de services. Insérez le numéro de téléphone mobile du destinataire E_PHONE_NUMBER et le message d'événement E_PHONE_MESSAGE décrits par la spécification du fournisseur de services SMS. Entrez l'adresse du destinataire, l'objet et le contenu. Les expressions seront remplacées par le contenu adéquat avant l'envoi du message par le fournisseur de services SMS. Par exemple : Adresse sample@cyberpower.com Objet TestSubject Contenu E_PHONE_NUMBER&text=E_MESSAGE

[Système->Notifications->Destinataires des SMS] Les utilisateurs peuvent configurer jusqu'à 10 numéros de téléphone mobile comme destinataires des SMS. Les destinataires recevront une notification de message succincte lorsque les événements configurés se produiront.

Pour ajouter un nouveau destinataire, cliquez sur « Nouveau destinataire ». Pour modifier ou supprimer un destinataire existant, cliquez sur son numéro de téléphone mobile ou son nom. Pour tester les paramètres de SMS, cliquez sur le bouton « TEST » et regardez si vous recevez correctement le message de test.

[Système->Réinitialiser/Redémarrer] Réinitialise ou redémarre le système RMCARD.

Élément	Définition
Redémarrer le système	Redémarre le système sans l'arrêter et redémarrer l'onduleur.
Réinitialiser le système	Réinitialise le système à ses paramètres par défaut d'usine. Le système redémarre. Cette action n'arrête pas ou ne redémarre pas l'onduleur.
Réinitialiser le système (paramètres TCP/IP réservés)	Réinitialise le système à ses paramètres par défaut d'usine, mais en réservant TCP/IP. Le système redémarre. Cette action n'arrête pas ou ne redémarre pas l'onduleur.

[Système->À propos] Affiche les informations système de la carte de gestion à distance.

Élément	Définition
Nom du modèle	Nom de modèle de la carte de gestion à distance.
Version matérielle	Version matérielle de la carte de gestion à distance.
Version du firmware	Version du firmware actuellement installée sur la carte de gestion à distance.
Date de mise à jour du firmware	Date de la dernière mise à jour du firmware.
Numéro de série	Numéro de série de la carte de gestion à distance.
Adresse MAC	Adresse MAC de la carte de gestion à distance.
Enregistrer la configuration	Cliquez sur « Enregistrer » pour enregistrer le fichier de configuration RMCARD. Le format par défaut du nom du fichier texte sera AAAA_MM_JJ_HHMM.txt.
Restaurer la configuration	Utilisez cette fonction pour restaurer une configuration précédemment enregistrée. Cliquez sur « Choisir un fichier » pour sélectionner l'emplacement du fichier de configuration enregistré et cliquez sur « Soumettre ». Remarque : le fichier de configuration enregistré contient les informations de sécurité, telles que le nom d'utilisateur et le mot de passe. Une fois la configuration restaurée, il est recommandé de supprimer le fichier pour préserver la sécurité des informations sensibles.
Informations de diagnostic	Cliquez sur le bouton « Enregistrer » pour enregistrer toutes les informations de diagnostic dans un fichier. Les informations enregistrées comprennent les journaux d'événements, les enregistrements d'état et d'autres informations sur RMCARD/onduleur/commutateur de transfert automatique. Il est recommandé d'enregistrer ces informations avant de contacter le support technique CyberPower pour obtenir une assistance.

Interface de ligne de commande

Comment se connecter

Les utilisateurs peuvent se connecter à l'interface de ligne de commande via l'accès réseau de la console (Telnet ou SSH) ou l'accès local (port Série).

1. Accès réseau à l'interface de ligne de commande

Lorsque l'utilisateur se connecte avec le nom d'utilisateur et le mot de passe de l'administrateur via Telnet ou SSH, deux types d'interfaces dont disponibles. La première est l'interface de ligne de commande (CLI, Command Line Interface) et la seconde est une interface de menu. L'interface par défaut est CLI. Pour basculer vers l'interface de menu, il suffit à l'utilisateur de saisir la commande [menumode]. Pour revenir à l'interface CLI, il doit se déconnecter et se connecter à RMCARD.

Comment utiliser Telnet pour accéder à l'interface de ligne de commande

Étape 1 : assurez-vous que l'ordinateur a accès au réseau installé RMCARD. À l'invite de commande, saisissez telnet et l'adresse IP de RMCARD (par exemple, telnet 139.225.6.133, si RMCARD utilise le port Telnet par défaut 23), puis appuyez sur Entrée.

Étape 2 : entrez le nom d'utilisateur et le mot de passe (par défaut, nom d'utilisateur : cyber, mot de passe : cyber).

Comment utiliser SSH pour accéder à l'interface de ligne de commande

L'utilisation de SSH est fortement recommandée pour accéder à l'interface de ligne de commande. SSH chiffre les noms d'utilisateur, mots de passe et données transmises. Pour utiliser SSH, vous devez d'abord le configurer et installer un programme client SSH (ex., PuTTY, HyperTerminal ou Tera Term) sur votre ordinateur.

Remarque : si vous utilisez PuTTY pour configurer l'accès SSH, configurez la discipline Ligne de Terminal sur « Forcer la déconnexion », comme illustré dans la figure 5.

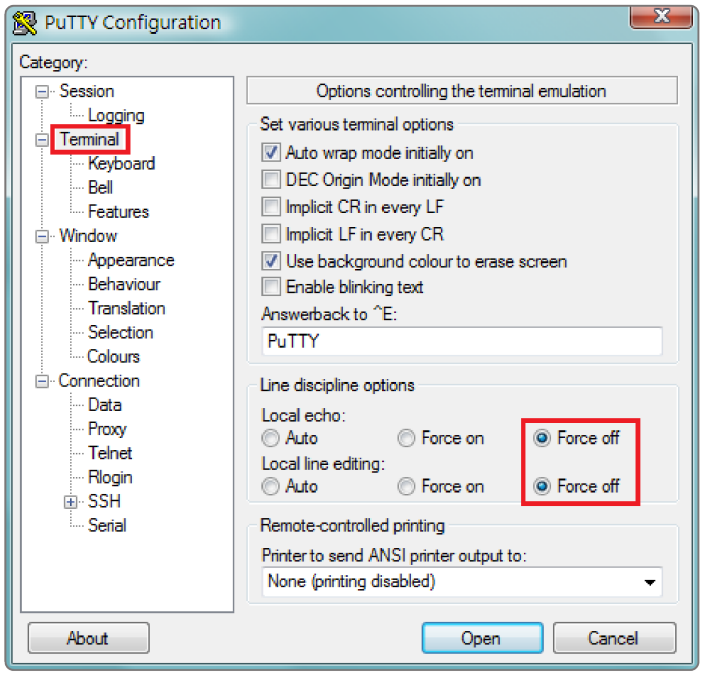


Figure 5. Fenêtre Configuration PuTTY.

2. Accès local à l'interface de ligne de commande

Pour vous connecter via une connexion série, assurez-vous que le PC/serveur est directement connecté au port Universel de RMCARD via le câble de connexion au port Série RJ45/DB9 inclus, puis procédez comme suit .

Étape 1. Ouvrez le logiciel Hyper Terminal (ex., PuTTY, HyperTerminal ou Tera Term) sur votre PC et sélectionnez un nom et une icône pour la connexion.

Étape 2. Définissez les paramètres du port COM avec les valeurs suivantes :

*Bits par seconde : 9 600
*Bits de données : 8
*Parité : Aucune
*Bits d'arrêt : 1
*Contrôle de flux : Aucun

Étape 3. Appuyez sur Entrée pour accéder au menu Authentification.

Étape 4. Entrez le nom d'utilisateur et le mot de passe de RMCARD dans le menu Authentification.

Remarque : la connexion série peut uniquement accéder au mode Ligne de commande et ne prend pas en charge le mode Menu.

Comment utiliser l'interface de ligne de commande

Tandis que vous utilisez l'interface de ligne de commande, vous pouvez exécuter les actions suivantes :

1. Mettre fin à la connexion à l'interface de ligne de commande ➔ Saisissez « **exit** » et appuyez sur Entrée.
2. Passer en mode Menu ➔ Saisissez « **menumode** » et appuyez sur Entrée.
3. Afficher la liste des commandes ou arguments disponibles ➔ Saisissez « **?** » (ex., `date ?`).
4. Afficher la dernière commande saisie dans la session ➔ Appuyez sur la touche fléchée HAUT/BAS. (La session peut mémoriser les 10 dernières commandes.)
5. Une commande peut prendre en charge plusieurs options ➔ Pour définir la date du 21 mars 2015 (ex., `date aaaa 2015 mm 3 jj 21`).

Codes de réponse de commande

Si la commande ou l'argument n'est pas reconnu ou est incorrect, l'interface de la console affiche [^] sous la commande ou l'argument erroné. Le message d'erreur suivant s'affiche :

Commande introuvable	RMCARD ne connaît pas cette commande. L'interface de la console affiche la liste des commandes disponibles.
Erreur de paramètre	Le type ou le format du paramètre n'est pas autorisé. L'interface de la console affiche la liste des valeurs ou formats disponibles.

Description des commandes

ups

Description : affiche des informations sur l'onduleur, l'entrée, la sortie. Et utilise le commutateur principal pour contrôler l'onduleur.

Option	Argument	Description
info	show	Affiche des informations sur l'onduleur.
input	show	Affiche des informations sur l'entrée de l'onduleur.
output	show	Affiche des informations sur la sortie de l'onduleur.

Exemple 1 :

Pour afficher des informations sur l'onduleur

```
CyberPower > ups info show
Informations sur l'onduleur
    Modèle : OL1000XL
    Tension nominale : 100 V
    Fréquence de fonctionnement : 40~70 Hz
    Puissance nominale : 1 000 VA
    Courant nominal : 10 Amp
    Puissance de charge : 900 Watts
    Tension nominale de la batterie : 36 V
    Version USB : 0.1B
    Date du prochain remplacement des batteries : 10/08/2018
    Banc NCL : 1
    Pack de batteries étendu : 4
```

upsctrl

Description : permet d'utiliser le commutateur principal de l'onduleur.

Option	Argument	Description
reboot	délai d'arrêt / durée de redémarrage (ex., 10/10) délai d'arrêt : 0 | 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600 durée de redémarrage : 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600	Met l'onduleur hors tension, puis à nouveau sous tension. Une chaîne inclut le délai d'arrêt (en secondes) et la durée de redémarrage (en secondes). Ex. : 10/10 signifie un délai d'arrêt de 10 secondes et une durée de redémarrage de 10 secondes.
on		Met l'onduleur sous tension.
off	0 | 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600	Met l'onduleur hors tension. L'argument est le délai d'arrêt en secondes.

Option	Argument	Description
sleep	0 | 10 | 20 | 30 | 60 | 120 | 180 | 300 | 600	Cette commande est disponible en mode Panne secteur. Elle peut faire passer l'onduleur en mode Veille jusqu'à ce que l'alimentation soit rétablie. L'argument est le délai de mise en veille en secondes.

Exemple 1 :

pour redémarrer l'onduleur avec un délai d'arrêt de 10 secondes et une durée de redémarrage de 20 secondes.

```
CyberPower > upsctrl reboot 10/20
```

upscfg

Description : affiche et configure l'alimentation électrique de l'onduleur, la sensibilité de l'onduleur, le seuil de haute tension de l'onduleur, le seuil de basse tension de l'onduleur, la condition de bypass de l'onduleur, le seuil haut de bypass de l'onduleur, le seuil bas de bypass de l'onduleur, le délai de recharge de l'onduleur, la capacité de recharge de l'onduleur, le mode de fonctionnement de l'onduleur et le délai de retour de l'onduleur.

Option	Argument	Description
show		
outpwr	<puissance de sortie en VAC>	Définit la tension de sortie fournie à l'équipement connecté.
sen	high | medium | low	Une faible sensibilité a une plage de tensions plus étendue et la puissance fournie peut être plus variable. La puissance d'un groupe électrogène alimenté par du carburant peut faire basculer l'onduleur en mode Batterie plus fréquemment ; dans ce cas, une faible sensibilité est recommandée. L'onduleur passe alors plus rarement en mode Batterie, ce qui permet d'économiser la puissance de la batterie. Une haute sensibilité permet à l'onduleur de fournir une puissance plus stable à l'équipement, mais il passe plus fréquemment en mode Batterie.
hvlimit	<seuil haut en VAC>	Lorsque la tension du secteur (ou la tension de sortie) est supérieure au seuil, l'onduleur alimente l'équipement connecté par la batterie.

lvlimit	<seuil bas en VAC>	Lorsque la tension du secteur (ou la tension de sortie) est supérieure au seuil, l'onduleur alimente l'équipement connecté par la batterie.
bypasscond	nobypass | freqvolt | voltonly	**Pas de bypass**—Lorsque cette option est sélectionnée, l'onduleur ne passe pas en mode Bypass et cesse de délivrer la puissance de sortie. **Contrôle de la tension/fréquence**—Si la tension du secteur se situe dans la plage de *tension de bypass haute/basse* et si la fréquence du secteur se situe dans la plage de la *tolérance en fréquence*, l'onduleur passe en mode Bypass. Sinon, il cesse de délivrer la puissance de sortie. **Contrôle de la tension uniquement**—L'onduleur passe en mode Bypass uniquement si la tension du secteur se situe dans la plage de *tension de bypass haute/basse*. Sinon, il cesse de délivrer la puissance de sortie.
bypasshvlimit	10 | 15	Définit la tension de bypass haute en pourcentage. Si la tension du secteur dépasse les seuils, l'onduleur ne peut plus passer en mode Bypass.
bypasslvlimit	10 | 15 | 20	Définit la tension de bypass basse en pourcentage. Si la tension du secteur dépasse les seuils, l'onduleur ne peut plus passer en mode Bypass.
rechargedelay	0 | 60 | 120 | 180 | 300 | 600 | 1200 | 1800 | 3600	Définit le délai de recharge en secondes. Lorsque l'alimentation secteur est rétablie, l'onduleur commence à se recharger jusqu'à l'expiration du délai spécifié avant de rétablir la puissance de sortie.
rechargecap	0 | 15 | 30 | 45 | 60 | 75 | 90	Définit la capacité de recharge en pourcentage. Lorsque l'alimentation secteur est rétablie, l'onduleur commence à se recharger jusqu'à ce que la capacité des batteries soit atteinte avant de rétablir la puissance de sortie.

Option	Argument	Description
workmode	normal | eco10% | eco15% | generator | bypass	**normal**—Mode de fonctionnement Normal de l'onduleur. **eco10%**—L'onduleur en ligne passe en mode Économie 10 %. **eco15%**—L'onduleur en ligne passe en mode Économie 15 %. **generator**—Si l'onduleur utilise un groupe électrogène comme puissance d'entrée, cette option doit lui permettre de fonctionner normalement. Lorsque cette option est sélectionnée, l'onduleur ne peut pas passer en mode Bypass pour protéger l'équipement alimenté. **bypass**—Détermine s'il faut autoriser l'onduleur à passer en mode Bypass manuel. Lorsque cette option est activée, l'onduleur est forcé à passer en mode Bypass.
returndelay	0 ~ 600	Lorsque l'alimentation secteur est rétablie, l'onduleur commence à se recharger jusqu'à l'expiration du délai spécifié avant de rétablir la puissance de sortie. Les numéros compris dans la plage de 1 à 600 secondes sont divisibles par 5.

Exemple 1 :

Pour afficher la valeur de tension disponible pouvant être définie pour la puissance de sortie de cet onduleur.

```
CyberPower > upscfg supply?
    100
    110
    115
```

Exemple 2 :

Pour définir la condition de bypass comme vérifier la tension du secteur uniquement.

```
CyberPower > upscfg bypasscond voltonly
```

Exemple 3 :

Pour définir un délai de recharge de l'onduleur de 2 minutes.

```
CyberPower > upscfg rechargedelay 120
```

Exemple 4 :

Pour faire passer l'onduleur en ligne en mode Générateur

```
CyberPower > upscfg mode generator
```

upsbatt

Description : affiche des informations sur la batterie et exécute le test de la batterie et l'étalonnage de l'autonomie de la batterie.

Option	Argument	Description
show		Affiche toutes les informations sur la batterie de cet onduleur.
test		Exécute immédiatement le test de la batterie.
cal	start | stop	Démarre ou arrête l'étalonnage de l'autonomie.
rdyyyy	<numéro de l'année>	Définit l'année de la date de remplacement de la batterie par AD.
rdmm	<numéro du mois>	Définit le mois de la date de remplacement de la batterie.
rddd	<numéro de la date>	Définit le jour du mois.

Exemple 1 :

Pour exécuter un autotest de la batterie.

```
CyberPower > upsbatt test
```

Exemple 2 :

Pour démarrer l'étalonnage de l'autonomie de la batterie.

```
CyberPower > upsbatt cal start
```

Exemple 3 :

Pour définir la date de remplacement de la batterie au 29 mai 2018.

```
CyberPower > upsbatt rdyyyy 2018 rdmm 5 rddd 29
```

atsoltsta

Description : affiche des informations sur l'état de la sortie du commutateur de transfert automatique.

Option	Argument	Description
show		Affiche des informations sur l'état de la sortie du commutateur de transfert automatique.
index	<1 | 2 |...| numéro de sortie |all>	Sélectionne l'indice de la sortie du commutateur de transfert automatique.

Exemple 1 :

Pour afficher l'état de toutes les sorties.

```
CyberPower > atsoltsta index all show
```

atsoltcfg

Description : affiche et configure les informations sur la sortie du commutateur de transfert automatique.

Option	Argument	Description
show		Affiche des informations sur la configuration de la sortie du commutateur de transfert automatique.
index	<1 | 2 |...| numéro de sortie |all>	Sélectionne l'indice de la sortie du commutateur de transfert automatique.
name	<nom de la sortie>	Définit le nom de la sortie du commutateur de transfert automatique.
td_on	<-1 | 0 | 1 | 2 |...|7200 >	Active le délai de la sortie du commutateur de transfert automatique.
td_off	<-1 | 0 | 1 | 2 |...|7200 >	Désactive le délai de la sortie du commutateur de transfert automatique.
td_reboot	<5 | 6 |...|60>	Définit la durée de redémarrage de la sortie du commutateur de transfert automatique.
set	<1 | 2 |...| numéro de sortie |all> <nom de la sortie> <-1 | 0 | 1 | 2 |...|7200 > <-1 | 0 | 1 | 2 |...|7200 > <5 | 6 |...|60>	Modifie la configuration de la sortie du commutateur de transfert automatique.

Exemple 1 :

Pour afficher la configuration de toutes les sorties.

```
CyberPower > atsoltcfg index all show
```

Exemple 2 :

Pour nommer la sortie 1 test_1.

```
CyberPower > atsoltcfg index 1 name test_1
```

Exemple 3 :

Pour définir le délai de mise sous tension de la sortie 2 sur 3 secondes.

```
CyberPower > atsoltcfg index 2 td_on 3
```

Exemple 4 :

Pour définir le délai de mise hors tension de la sortie 3 sur 3 secondes.

```
CyberPower > atsoltcfg index 3 td_off 3
```

Exemple 5 :

Pour définir le délai de mise hors tension de la sortie 4 sur « ne jamais mettre hors tension ».

```
CyberPower > atsoltcfg index 4 td_off -1
```

Exemple 6 :

Pour définir la durée de redémarrage de la sortie 5 sur 5 secondes.

```
CyberPower > atsoltcfg index 5 td_reboot 5
```

Exemple 7 :

Pour nommer la sortie 1 test_1, définir le délai de mise sous tension sur 3 secondes, définir le délai de mise hors tension sur 4 secondes et définir la durée de redémarrage sur 5 secondes avec une seule commande.

```
CyberPower > atsoltcfg set 1 test_1 3 4 5
```

atsoltctrl

Description : configure l'état de la sortie du commutateur de transfert automatique.

Option	Argument	Description
index	<1 | 2 |...| numéro de sortie |all>	Sélectionne l'indice de la sortie du commutateur de transfert automatique.
act	<on | off | reboot | td_on | td_off | td_reboot>	Contrôle la sortie du commutateur de transfert automatique.

Exemple 1 :

Pour mettre immédiatement sous tension la sortie 1.

```
CyberPower > atsoltctrl index 1 act on
```

Exemple 2 :

Pour mettre sous tension la sortie 2 avec un délai.

```
CyberPower > atsoltctrl index 2 act td_on
```

atssrccfg

Description : affiche et configure la source préférée du commutateur de transfert automatique.

Option	Argument	Description
show		Affiche des informations sur la source préférée du commutateur de transfert automatique.
prefer	<a | b | none >	Définit la source préférée du commutateur de transfert automatique.

Exemple 1 :

Pour afficher des informations sur la source préférée du commutateur de transfert automatique.

```
CyberPower > atssrccfg show
```

Exemple 2 :

Pour définir la source A comme la source préférée du commutateur de transfert automatique.

```
CyberPower > atssrccfg prefer a
```

date

Description : affiche et configure le fuseau horaire, le format de date, la date, l'heure.

Option	Argument	Description
show		Affiche des informations sur la date système de RMCARD.
timezone	<décalage horaire>	Choisissez le fuseau horaire (GMT, Greenwich Mean Time) de RMCARD.
format	mm/dd/yyyy | yyyy/mm/dd | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Définit le format de la date système
yyyy	<numéro de l'année>	Définit l'année de la date système par AD.
mm	<numéro du mois>	Définit le mois de la date système.
dd	<numéro de la date>	Définit le jour du mois.
time	<00:00:00>	Définit l'heure système.

Exemple 1 :

Pour définir le décalage horaire sur +08:00.

```
CyberPower > date timezone +0800
```

Exemple 2 :

Pour définir la date du 21 mars 2015.

```
CyberPower > date yyyy 2015 mm 3 dd 21
```

Exemple 3 :

Pour définir l'heure sur 13:45:12.

```
CyberPower > date time 13:45:12
```

ntp

Description : affiche et configure l'adresse IP du serveur NTP et l'intervalle de temps entre les mises à jour du serveur NTP.

Option	Argument	Description
show		Affiche toutes les informations sur NTP pour RMCARD.

access	enable | disable	Si enable a été défini, le système définit la date et l'heure à partir du serveur NTP.
priip	<ip serveur ntp principal>	Définit l'adresse IP/le nom de domaine des serveurs NTP principaux.
secip	<ip serveur ntp secondaire>	Définit l'adresse IP/le nom de domaine des serveurs NTP secondaires.
update	now | 1-8760	**now**—Choisissez *Mettre à jour maintenant* pour effectuer une mise à jour immédiate. **1-8760**—Définissez la fréquence des mises à jour de la date et de l'heure à partir du serveur NTP.

Exemple 1 :

Pour permettre au serveur NTP de définir la date et l'heure de RMCARD.

```
CyberPower > ntp access enable
```

Exemple 2 :

Pour configurer 192.168.26.22 comme adresse IP du serveur NTP principal.

```
CyberPower > ntp priip 192.168.26.22
```

Exemple 3 :

Pour lancer une mise à jour immédiate de l'heure par le serveur NTP.

```
CyberPower > ntp update now
```

sys

Description : affiche et configure l'identification de RMCARD, réinitialise RMCARD.

Option	Argument	Description
show		Affiche toutes les informations sur RMCARD.
name	<nom du système>	Définit le nom de l'équipement.
location	<emplacement du système>	Définit l'emplacement de l'équipement d'alimentation.
contact	<contact du système>	Définit la personne à contacter concernant cet équipement.
reset	reboot | notcpip | all	**reboot**—Redémarre RMCARD. **notcpip**—Réinitialise les paramètres par défaut du système, mais réserve les paramètres TCP/IP et le redémarre. **all**—Définissez all pour réinitialiser les paramètres par défaut du système et le redémarrer.

Exemple 1 :

Pour afficher toutes les informations sur le système.

```
CyberPower > sys show
```

```
Nom : RMCARD205 (305)
Emplacement : Salle de serveurs
Contact : Administrateur
Modèle : RMCARD205 (305)
Version matérielle : 1.1
Version du firmware : 1.0.3
Date de mise à jour du firmware : 03/08/2015
Numéro de série : TALGY2001975
Adresse MAC : 00-0C-15-00-B9-42
```

Exemple 2 :

Pour réinitialiser RMCARD sur les paramètres par défaut.

```
CyberPower > sys reset all
```

dst

Description : affiche et configure le type d'heure d'été.

Option	Argument	Description
show		Affiche toutes les informations sur l'heure d'été pour RMCARD.
mode	disable | us | manual	**disable**—Désactive l'heure d'été. **us**—Heure d'été standard des États-Unis. **manual**—Réglage manuel de l'heure d'été. Une fois cette commande entrée, entrez l'heure de début et de fin étape par étape. Paramètres de la **semaine du mois** : first | second | third | forth | last Paramètres du **jour de la semaine** : Mon | Tue | Wed | Thu | Fri | Sat | Sun Paramètres du **mois** : Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec

Exemple 1 :

Pour définir manuellement l'heure d'été.

```
CyberPower > dst type manual
Heure de début (0~23) : 2
Semaine du mois de début : second
Jour de la semaine de début : Sun
Mois de début : Mar
Heure de fin (0~23) : 2
Semaine du mois de fin : first
Jour de la semaine de fin : Sun
```

```
    Mois de fin : Nov
```

Exemple 2 :

Pour afficher les paramètres d'heure d'été.

```
CyberPower > dst show
    DST : Réglage manuel de l'heure d'été
    Début : 02:00, le deuxième dimanche de mars
    Fin : 02:00, le premier dimanche de novembre
```

login

Description : affiche et configure l'authentification de la connexion.

Option	Argument	Description
show		Affiche toutes les informations de connexion pour RMCARD.
type	local | radiuslocal | radiusonly | ldaplocal | ldaponly	**local**—L'utilisateur se connecte à la carte de gestion à distance avec le nom d'utilisateur et le mot de passe configurés dans le compte local. **radiuslocal**—L'utilisateur se connecte à la carte de gestion à distance avec le nom d'utilisateur et le mot de passe pour s'authentifier d'abord avec le serveur RADIUS. Si le serveur RADIUS ne répond pas, le nom d'utilisateur et le mot de passe configurés dans le compte local sont utilisés. **radiusonly**—L'utilisateur se connecte à la carte de gestion à distance avec le nom d'utilisateur et le mot de passe pour s'authentifier uniquement avec le serveur RADIUS. **ldaplocal**—L'utilisateur se connecte à la carte de gestion à distance avec le nom d'utilisateur et le mot de passe pour s'authentifier d'abord avec le serveur LDAP. Si le serveur LDAP ne répond pas, le nom d'utilisateur et le mot de passe configurés dans le compte local sont utilisés. **ldaponly**—L'utilisateur se connecte à la carte de gestion à distance avec le nom d'utilisateur et le mot de passe pour s'authentifier uniquement avec le serveur LDAP.
secretphrase	<phrase d'authentification>	Phrase d'authentification utilisée pour communiquer avec **PowerPanel®** Business Remote.
timeout	1~10	Période (en minutes) pendant laquelle le système

		attend avant de se déconnecter automatiquement. La plage de l'argument va de 1 à 10 (en minutes).

Exemple 1 :

Pour faire passer le type d'authentification à Radius, compte local.

```
CyberPower > login type radiuslocal
```

admin / device

Description : affiche et configure l'adresse IP de gestionnaire principal/secondaire, le nom d'utilisateur, le mot de passe de l'administrateur/utilisateur de l'équipement.

Option	Argument	Description
show		Affiche toutes les informations sur l'administrateur ou l'équipement pour cette RMCARD.
access	enable | disable	Active ou désactive l'équipement.
primip	<IP gestionnaire principal>	Définit l'adresse IP de gestionnaire principal de l'administrateur/équipement.
secmipac	enable | disable	Active ou désactive l'adresse IP de gestionnaire secondaire de l'administrateur/équipement.
secmip	<IP gestionnaire secondaire>	Définit l'adresse IP de gestionnaire secondaire de l'administrateur/équipement.
name	<nom d'utilisateur>	Définit le nom d'utilisateur de l'administrateur/équipement.
passwd	<mot de passe utilisateur>	Définit le mot de passe utilisateur de l'administrateur/équipement.

Exemple 1 :

Pour définir 192.168.26.0/24 comme adresse IP de gestionnaire administrateur principal.

```
CyberPower > admin primip 192.168.26.0/24
Entrer le mot de passe administrateur : cyber
Succès
```

radius

Description : affiche et configure les informations sur le serveur RADIUS.

Option	Argument	Description
show		Affiche toutes les informations sur le serveur RADIUS pour RMCARD.
pri sec	show	Affiche les informations sur le serveur Radius principal/secondaire.

add		Ajoute le serveur radius, puis l'adresse IP du serveur radius/le secret/le port entrés s'affichent.
add	<IP serveur> <secret serveur> <port serveur>	Ajoute les informations sur le serveur radius, y compris IP/secret/port serveur simultanément.
priip secip	<IP serveur radius>	Définit l'adresse IP du serveur RADIUS principal/secondaire.
priport secport	<port serveur radius>	Définit le port UDP utilisé par le serveur RADIUS principal/secondaire.
prisecret secsecret	<secret serveur radius>	Définit le secret partagé du serveur Radius principal/secondaire.
pridel secdel		Supprime le serveur Radius principal/secondaire.

Exemple 1 :

Pour afficher les informations sur le serveur radius principal.

```
CyberPower > radius pri show
    IP serveur : 192.168.26.33
    Secret serveur : testsecret
    Port serveur : 1826
```

Exemple 2 :

Pour afficher les informations sur le serveur radius secondaire.

```
CyberPower > radius sec show
    IP serveur : 192.168.30.58
    Secret serveur : testsecret2
    Port serveur : 1508
```

Entrez la commande suivante pour ajouter la configuration des informations sur le serveur Radius avec une seule commande :

```
radius add <IP serveur> <Secret partagé> <Port serveur>
```

Par exemple :

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

Remarque : cette commande unique pourrait ne pas s'exécuter avec succès si deux serveurs Radius sont déjà configurés.

ldap

Description : affiche et configure les informations sur le serveur LDAP.

Option	Argument	Description
show		Affiche toutes les informations sur le serveur LDAP pour RMCARD.
add		Ajoute le serveur LDAP, puis les informations

		d'entrée pour les exigences apparaissent.
pritype sectype	openldap | ad	Définit le type de serveur LDAP.
priip secip	<IP serveur LDAP>	Définit l'adresse IP du serveur LDAP principal/secondaire.
prissl secssl	enable | disable	Active ou désactive l'utilisation des serveurs LDAP.
priport secport	< port serveur LDAP>	Définit le port TCP utilisé par le serveur LDAP principal/secondaire.
pridn secdn	<Base DN serveur LDAP>	Définit le Base DN du serveur LDAP principal/secondaire.
priaddomain secaddomain	<domaine AD serveur LDAP>	Définit le domaine AD du serveur Active Directory principal/secondaire.
priattr secattr	<attribut connexion serveur LDAP>	Définit l'attribut de connexion de l'entrée utilisateur LDAP principal/secondaire.
pridel secdel		Supprime le serveur LDAP principal/secondaire.

Exemple 1 :

Pour ajouter un serveur LDAP.

```
CyberPower > ldap add
Entrer le type de serveur LDAP [openldap | ad] : ad
Entrer l'adresse IP : 192.168.26.33
Utiliser SSL [enable | disable] : disable
Entrer le port LDAP : 389
Entrer base DN : dc=cyber,dc=com
Entrer l'attribut de connexion : cn
Entrer le domaine AD : cyber.com
```

Exemple 2 :

Pour afficher des informations sur le serveur LDAP.

```
CyberPower > ldap show
Serveur LDAP principal
    Type : Windows AD
    Serveur LDAP : 192.168.26.33
    SSL LDAP : Disable
    Port : 389
    Base DN : dc=cyber,dc=com
    Attribut de connexion : cn
    Domaine AD : cyber.com
```

tcpip

Description : affiche et configure l'IP IPv4, le masque de réseau, la passerelle, DNS.

Option	Argument	Description
show		Affiche toutes les informations IPv4 pour RMCARD.
dhcp	enable | disable	Active ou désactive DHCP.
dns	manual | auto	**Auto** — Obtient l'adresse DNS de DHCP lorsque DHCP est activé. **Manual** — Obtient manuellement l'adresse DNS lorsque DHCP est activé.
ip	<IP système>	Définit l'adresse IP du système.
netmask	<masque réseau système>	Définit le masque réseau du système.
gateway	<passerelle système>	Définit la passerelle du système.
dnsip	<dns système>	Définit l'adresse DNS du système.

Exemple 1 :

Pour désactiver DHCP et définir 192.168.26.33 comme adresse IP.

```
CyberPower > tcpip dhcp disable ip 192.168.26.33
```

tcpip6

Description : affiche et configure l'état du contrôle de routeur IPv6, l'IP manuelle IPv6.

Option	Argument	Description
show		Affiche toutes les informations IPv6 pour RMCARD.
access	enable | disable	Active ou désactive le service IPv6.
routerctrl	enable | disable	L'adresse IPv6 est attribuée par la méthode (autoconfiguration d'adresse sans état, DHCPv6 sans état ou DHCPv6 avec état) décidée par les paramètres du routeur.
manual	enable | disable	Active ou désactive l'IP manuelle IPv6.
ip	<IP IPv6 manuelle>	Définit l'IP IPv6 manuelle.

Exemple 1 :

Pour définir l'adresse IP manuelle Ipv6, puis afficher les informations sur IPv6.

```
CyberPower > tcpip6 manual enable ip 2001:cdba:0:0:0:0:3257:9652 show
    Accès : Activer
    Contrôle du routeur : Activer
    Manuel : Activer
    Adresse IPv6 manuelle : [2001:cdba::3257:9652]
```

snmpv1

Description : affiche et configure l'état de SNMPv1.

Option	Argument	Description
show		Affiche l'état de SNMPv1 pour RMCARD
index	<1 | 2 | 3 | 4>	Sélectionne l'indice de la communauté SNMPv1.
set	<1 | 2 | 3 | 4>	Modifie les informations sur la communauté SNMPv1.
access	enable | disable	Active ou désactive SNMPv1.
community	<communauté>	Modifie le nom de la communauté SNMPv1.
ip	<adresse IP>	Modifie l'adresse IP de la communauté SNMPv1.
type	<lecture seule | lecture/écriture | interdit>	Modifie le type de communauté SNMPv1.

Exemple 1 :

Pour afficher les informations sur la seconde communauté SNMPv1.

```
CyberPower > snmpv1 index 2 show
    Communauté : privée
    Adresse IP : 192.169.203.20
    Type : Lecture/Écriture
```

Exemple 2 :

Pour remplacer le nom de la première communauté SNMPv1 par Public1.

```
CyberPower > snmpv1 index 1 community Public1
```

Exemple 3 :

Pour remplacer l'adresse IP de la troisième communauté SNMPv1 par 192.168.203.88.

```
CyberPower > snmpv1 index 3 ip 192.168.203.88
```

Exemple 4 :

Pour remplacer le type de la quatrième communauté SNMPv1 par lecture/écriture.

```
CyberPower > snmpv1 index 4 type readwrite
```

Entrez la commande suivante pour configurer tous les paramètres avec une seule commande :

```
snmpv1 set <1 | 2 | 3 | 4> <Communauté> <adresse IP> <lecture seule |
lecture/écriture | interdit>
```

Par exemple :

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

snmpv3

Description : affiche et configure l'état de SNMPv3.

Option	Argument	Description
show		Affiche l'état de SNMPv3 pour RMCARD
index	<1 | 2 | 3 | 4>	Sélectionne l'indice de l'utilisateur SNMPv3.
set	<1 | 2 | 3 | 4>	Modifie les informations sur l'utilisateur SNMPv3.
access	enable | disable	Active ou désactive SNMPv3.
name	<nom d'utilisateur>	Modifie le nom d'utilisateur SNMPv3.
status	<enable | disable>	Active ou désactive l'utilisateur SNMPv3.
ip	<adresse IP>	Modifie l'adresse IP de l'utilisateur SNMPv3.
auth	<md5 | sha | aucun>	Modifie le protocole d'authentification de l'utilisateur SNMPv3.
authkey	<clé d'authentification>	Modifie le mot de passe d'authentification de l'utilisateur SNMPv3.
priv	<aes | des | aucun>	Modifie le protocole de confidentialité de l'utilisateur SNMPv3.
privkey	<clé privée>	Modifie le mot de passe de confidentialité de l'utilisateur SNMPv3.

Exemple 1 :

Pour afficher les informations sur le premier utilisateur SNMPv3.

```
CyberPower > snmpv3 index 1 show
    Nom d'utilisateur : CyberPower
    État : Activer
    Adresse IP : 192.169.30.58
    Protocole d'authentification : MD5
    Protocole privé : aes
```

Exemple 2 :

Pour remplacer le nom du deuxième utilisateur SNMPv3 par CyberPower.

```
CyberPower > snmpv3 index 2 name CyberPower
```

Exemple 3 :

Pour activer le troisième utilisateur SNMPv3.

```
CyberPower > snmpv3 index 3 status enable
```

Exemple 4 :

Pour remplacer l'adresse IP du quatrième utilisateur SNMPv3 par 192.168.203.66.

```
CyberPower > snmpv3 index 4 ip 192.168.203.66
```

Exemple 5 :

Pour remplacer le protocole d'authentification du deuxième utilisateur SNMPv3 par md5 et définir son mot de passe d'authentification sur **test_authkey_123456**.

```
CyberPower > snmpv3 index 2 auth md5 authkey test_authkey_123456
```

Exemple 6 :

Pour remplacer le mot de passe d'authentification du premier utilisateur SNMPv3 par

test_authkey_123456.

CyberPower > **snmpv3 index 1 authkey test_authkey_123456**

Exemple 7 :

Pour remplacer le protocole d'authentification du troisième utilisateur SNMPv3 par Aucun.

CyberPower > **snmpv3 index 3 auth none**

Exemple 8 :

Pour remplacer le protocole de confidentialité du deuxième utilisateur SNMPv3 par aes et définir son mot de passe de confidentialité sur **test_privkey_123456**.

CyberPower > **snmpv3 index 2 priv aes privkey test_privkey_123456**

Exemple 9 :

Pour remplacer le mot de passe de confidentialité du premier utilisateur SNMPv3 par **test_privkey_123456**.

CyberPower > **snmpv3 index 1 privkey test_privkey_123456**

Exemple 10 :

Pour remplacer le protocole de confidentialité du troisième utilisateur SNMPv3 par Aucun.

CyberPower > **snmpv3 index 3 priv none**

Entrez la commande suivante pour configurer tous les paramètres avec une seule commande :

snmpv3 set <1 | 2 | 3 | 4> <nom d'utilisateur> <adresse IP> <md5 | sha | aucun> <clé d'authentification> <aes | des | aucun> <clé de confidentialité>

Par exemple :

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

trap

Description : affiche et configure les informations sur le récepteur de trap SNMP.

Option	Argument	Description
show		Affiche toutes les informations sur le récepteur de trap SNMP pour RMCARD.
add		Ajoute le récepteur de trap pour RMCARD.
index	<1 | 2 | ... | 10>	Sélectionne l'indice du récepteur de trap.
name	<nom du récepteur de trap>	Modifie le nom du récepteur de trap.
ip	<IP du récepteur de trap>	Modifie l'adresse IP du récepteur de

		trap.
ver	<v1 | v3>	Modifie la version SNMP du récepteur de trap.
status	<enable | disable>	Active ou désactive le récepteur de trap.
community	<communauté du récepteur de trap>	Modifie le nom de la communauté SNMPv1 du récepteur de trap.
user	<1 | 2 | 3 | 4>	Sélectionne l'utilisateur SNMPv3 du récepteur de trap.
delete		Supprime le récepteur de trap.

Exemple 1 :

Pour afficher les informations sur le sixième récepteur de trap.

```
CyberPower > trap index 6 show
    Nom de trap : CyberPower
    État : Activer
    Adresse IP : 192.168.203.68
    Type : SNMPv1
    Communauté : test_community
```

Exemple 2 :

Pour remplacer le nom du deuxième récepteur de trap par test.

```
CyberPower > trap index 2 name test
```

Exemple 3 :

Pour remplacer l'adresse IP du troisième récepteur de trap par 192.168.30.85.

```
CyberPower > trap index 3 ip 192.168.30.85
```

Exemple 4 :

Pour remplacer la version SNMP du quatrième récepteur de trap par SNMPv3.

```
CyberPower > trap index 4 ver v3
```

Exemple 5 :

Pour remplacer le cinquième récepteur de trap.

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

Exemple 6 :

Pour remplacer le nom de la communauté du deuxième récepteur de trap par CyberPower, à condition que la version SNMP du récepteur de trap soit SNMPv1.

```
CyberPower > trap index 2 community CyberPower
```

Exemple 7 :

Pour remplacer l'utilisateur SNMPv3 du dixième récepteur de trap par SNMPv3 user2, à condition que la version SNMP du récepteur de trap soit SNMPv3.

```
CyberPower > trap index 10 user 2
```

Exemple 8 :

Pour supprimer le cinquième récepteur de trap.

```
CyberPower > trap index 5 delete
```

Entrez la commande suivante pour ajouter la configuration du récepteur de trap avec une seule commande :

Pour SNMPv1 : `trap add <nom du trap> <IP du récepteur de trap> v1 <communauté>`

Par exemple :

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

Pour SNMPv3 : `trap add <nom du trap> <IP du récepteur de trap> v3 <1 | 2 | 3 | 4>`

Par exemple :

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

web

Description : affiche et configure le type d'accès web, le port http et le port https.

Option	Argument	Description
show		Affiche toutes les informations web pour RMCARD.
access	http | https | disable	**http** — Permet l'accès au service http. **https** — Permet l'accès au service https. **disable** — Désactive le service web.
httpport	<port http>	Port TCP/IP du protocole HTTP (Hypertext Transfer Protocol) (80 par défaut)
httpsport	<port https>	Port TCP/IP du protocole HTTPS (Hypertext Transfer Protocol Secure) (443 par défaut)

Exemple 1 :

Pour définir le port serveur HTTP sur 5000.

```
CyberPower > web httpport 5000
```

console

Description : affiche et configure le type d'accès réseau console, le port telnet et le port SSH.

Option	Argument	Description
show		Affiche toutes les informations de console pour RMCARD.
access	telnet | ssh | disable	**telnet** — Active l'accès à Telnet. **ssh** — Active l'accès à SSH. **disable** — Désactive le service de console.

telnet	<enable | disable>	**enable** — Active Telnet. **disable** — Désactive Telnet.
ssh	<enable | disable | reset_hostkey>	**enable** — Active SSH. **disable** — Désactive SSH. **reset_hostkey** — Réinitialise la clé d'hôte SSH par défaut.
telnetport	<port telnet>	Port TCP/IP (23 par défaut) utilisé par Telnet pour communiquer.
sshport	<port ssh>	Port TCP/IP (22 par défaut) utilisé par SSH pour communiquer.

Exemple 1 :

Pour activer Telnet comme type de console.

```
CyberPower > console telnet enable
```

Exemple 2 :

Pour activer SSH comme type de console.

```
CyberPower > console ssh disable
```

Remarque : les modes telnet et ssh sont des options pour basculer entre les deux. Par exemple, telnet est automatiquement désactivé lorsque ssh est activé comme type de console et vice versa.

Exemple 3 :

Pour réinitialiser la clé d'hôte SSH par défaut.

```
CyberPower > console ssh reset_hostkey
```

Remarque : le système redémarre après la réinitialisation de la clé d'hôte SSH de RMCARD aux paramètres par défaut.

ftp

Description : affiche et configure le type d'accès FTP et le port TCP/IP de FTP.

Option	Argument	Description
show		Affiche toutes les informations sur le serveur FTP pour RMCARD.
access	enable | disable	Active ou désactive le serveur FTP.
port	<port ftp>	Port TCP/IP du serveur FTP (21 par défaut)

Exemple 1 :

Pour activer le service FTP.

```
CyberPower > ftp access enable
```

eventlog

Description : affiche et efface le journal d'événements de RMCARD et de l'onduleur.

Option	Argument	Description
show		Affiche la liste des événements et une brève description de chaque événement avec la marque d'horodatage.
clear		Efface les journaux d'événements existants.

Exemple 1 :

CyberPower > **eventlog show**

```
12/11/2015 03:32:08 Admin login from 192.168.26.33.
```

.....

Utilisez ensuite les touches suivantes pour naviguer dans le journal d'événements.

Touche	Description
ESPACE	Affiche la page suivante du journal d'événements.
Q	Ferme le journal d'événements et revient à l'interface de ligne de commande.

Exemple 2 :

Pour effacer tous les journaux d'événements.

```
CyberPower > eventlog clear
Do you want to clear all eventlog [yes / no]: yes
```

syslog

Description : affiche et configure les informations sur le serveur SYSLOG.

Option	Argument	Description
show		Affiche toutes les informations sur le serveur syslog pour RMCARD.
s1 s2 s3 s4	show	Affiche les informations sur les serveurs syslog 1 à 4.
add		Ajoute le serveur syslog, puis l'adresse IP du serveur syslog/le port entrés s'affichent.
add	<IP serveur> <port serveur>	Ajoute les informations sur le serveur syslog, y compris IP/port serveur simultanément.
access	enable | disable	Active ou désactive le serveur syslog.
facility	kernel | user | mail | system | auth1 | syslog | link | news | uucp | clock1 | auth2 | ftp | ntp |	Sélectionne le dispositif Syslog.

	logaudit | logalert | clock2 | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7	
s1test s2test s3test s4test		Envoie un message de test aux serveurs Syslog 1 à 4.
ip1 ip2 ip3 ip4	<IP serveur SYSLOG>	Envoie l'adresse IP des serveurs Syslog 1 à 4.
port1 port2 port3 port4	<port serveur SYSLOG>	Définit le port UDP utilisé par les serveurs Syslog 1 à 4.
s1del s2del s3del s4del		Supprime les serveurs Syslog 1 à 4.

Exemple 1 :

Pour afficher les informations syslog du serveur 1

```
CyberPower > syslog s1 show
    IP : 192.168.26.33
    Port : 514
```

Exemple 2 :

Pour afficher les informations syslog du serveur 2

```
CyberPower > syslog s2 show
    IP : 192.168.203.89
    Port : 268
```

Exemple 3 :

Pour afficher les informations syslog du serveur 3

```
CyberPower > syslog s3 show
    IP : 192.168.30.15
    Port : 101
```

Exemple 4 :

Pour afficher les informations syslog du serveur 4

```
CyberPower > syslog s4 show
    IP : 192.168.26.93
    Port : 358
```

Entrez la commande suivante pour configurer tous les paramètres avec une seule commande :

```
syslog add <addresse IP serveur> <port serveur>
```

Par exemple :

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

Remarque : cette commande unique pourrait ne pas s'exécuter avec succès si quatre serveurs Syslog sont déjà configurés.

menumode

Description : passe en mode Menu.

clear

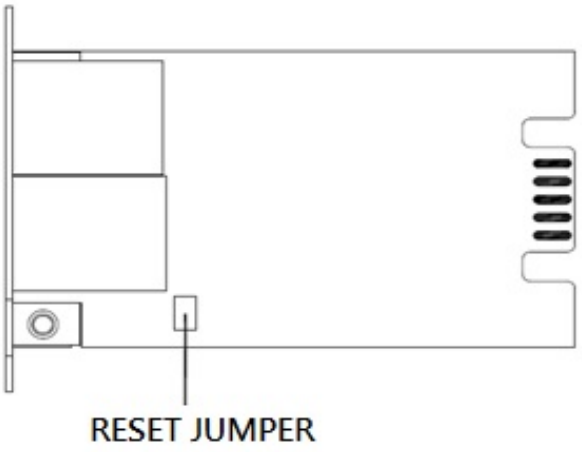
Description : efface l'écran de la console.

exit

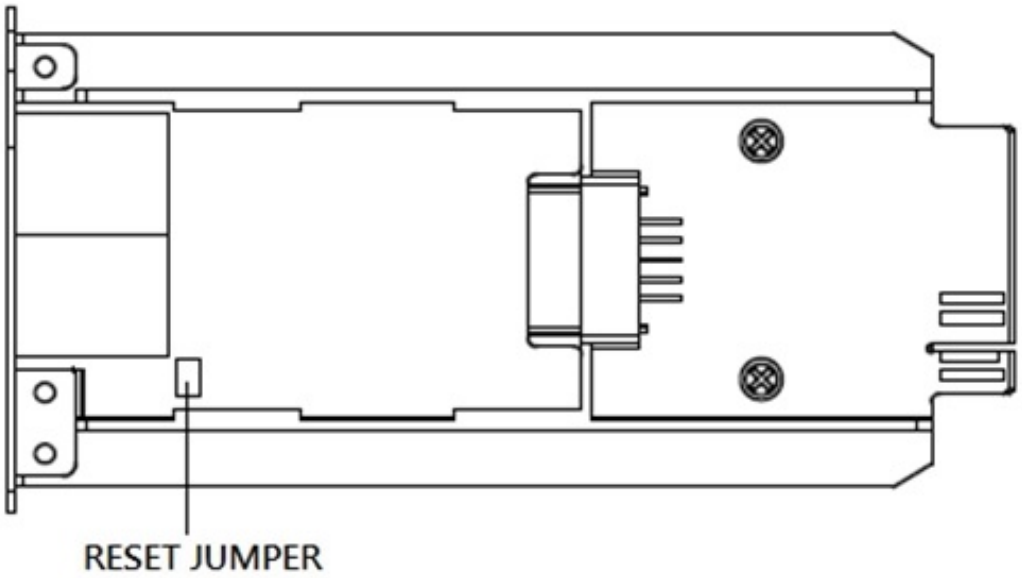
Description : coupe la connexion à l'interface de ligne de commande.

Réinitialisation aux paramètres par défaut d'usine / Récupération à partir d'un mot de passe perdu

Pour réinitialiser la carte de gestion à distance CyberPower à ses paramètres par défaut d'usine (y compris le nom d'utilisateur et le mot de passe de connexion web), procédez comme suit :



RMCARD205



RMCARD305

1. Retirez la carte de l'onduleur sans mettre hors tension l'onduleur/ATS PDU.
2. Retirez le cavalier des broches de réinitialisation, comme illustré. Ne jetez pas le cavalier.
3. Insérez la carte dans le port d'extension de l'onduleur/ATS PDU.
4. Attendez que la LED verte Tx/Rx clignote (la fréquence du clignotement ON/OFF est une fois par seconde).
5. Retirez à nouveau la carte.
6. Remettez en place le cavalier sur les broches de réinitialisation.
7. Réinstallez la carte dans le port d'extension et serrez les vis de maintien.

Mise à niveau du firmware de RMCARD

En mettant à niveau le firmware, vous pouvez accéder aux nouvelles fonctions et mises à jour/améliorations de la fonctionnalité existante. Le service FTP doit être activé avant de tenter d'exécuter une mise à niveau du firmware. Vous pouvez vérifier la version du firmware à la page **[Système->À propos]** de l'interface utilisateur web de RMCARD. Il y a deux fichiers à mettre à jour pour mettre à niveau la version du firmware.

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

Remarque : pour être sûr de maintenir le firmware de RMCARD à jour, visitez le site Web de CyberPower tous les 3 mois afin de vérifier si une nouvelle version du firmware est disponible.

Remarque : ne mettez pas l'onduleur hors tension durant l'exécution d'une mise à niveau du firmware.

Remarque : pour mettre à jour le firmware de RMCARD avec succès, assurez-vous que les connexions des ports 20 et 21 du firewall ne sont pas bloquées.

Méthode 1 : utilisation de la commande FTP

Pour mettre à niveau le firmware, procédez comme suit :

1. Téléchargez la dernière version du firmware
2. Extrayez les fichiers téléchargés dans « C:\ ».
3. Ouvrez une fenêtre d'invite de commande.
4. Connectez-vous à la carte de gestion à distance CyberPower en saisissant la commande FTP suivante à l'invite de commande :
   (1) `ftp`
   (2) `ftp> open`
   (3) To [adresse IP actuelle de RMCARD] [port] ; ex. : `To 192.168.22.126 21`
   (4) Entrez le NOM D'UTILISATEUR et le MOT DE PASSE (mêmes que pour le compte Administrateur dans l'interface utilisateur Web ; voir les paramètres d'usine par défaut à la page 6).
5. Chargez le fichier A. Saisissez :
   `ftp > bin`
   `ftp > put cpsrm2scfw_XXX.bin`
6. Le chargement est à présent terminé. Saisissez :
   `ftp > quit`
7. Le système redémarre lorsque vous saisissez « quit ».
8. Connectez-vous à nouveau au serveur FTP en procédant comme à l'étape 4.
9. Chargez le fichier B. Saisissez :
   `ftp > bin`
   `ftp > put cpsrm2scdata_XXX.bin`
10. Le chargement est à présent terminé. Saisissez :
    `ftp > quit`

11. Le système redémarre lorsque vous saisissez « `quit` ».

Méthode 2 : utilisation de l'utilitaire de mise à niveau et de configuration (outil de mise à niveau du firmware en masse)

1. Installez l'utilitaire de mise à niveau et de configuration CyberPower disponible en téléchargement sur www.CyberPower.com.
2. Une fois l'installation terminée, exécutez l'utilitaire de mise à niveau et de configuration.
3. La fenêtre principale de l'utilitaire de mise à niveau et de configuration est présentée dans la figure 6. L'outil de configuration affiche tous les équipements de gestion à distance CyberPower présents sur le sous-réseau local. Le bouton « Découvrir » sert à chercher à nouveau le sous-réseau local.

   Remarque : vous pouvez cliquer sur « Afficher » pour sélectionner les éléments que vous voulez afficher.

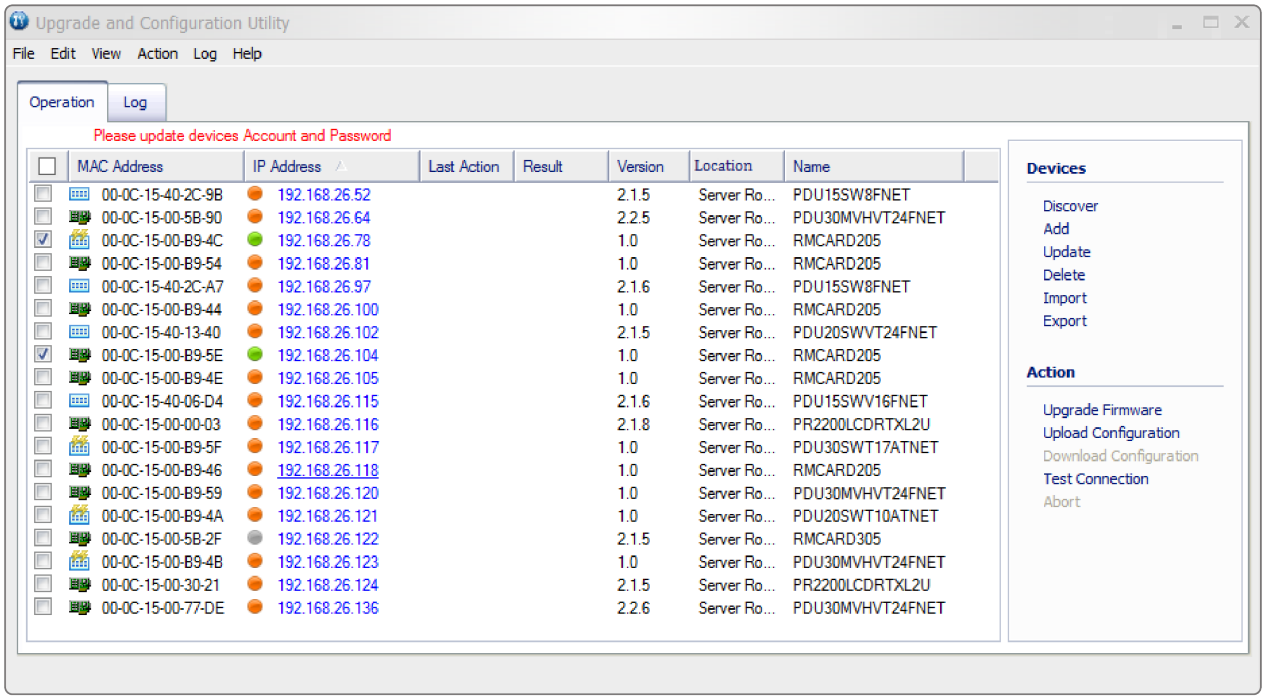


Figure 6. Fenêtre principale de l'utilitaire de mise à niveau et de configuration.

4. Cochez les cases pour sélectionner les équipements que vous souhaitez mettre à niveau, puis cliquez sur « Mettre à jour » à droite pour mettre à jour le compte et le mot de passe de l'utilisateur de l'équipement. Une fois la mise à jour confirmée, l'icône d'état à côté de l'adresse IP passe de l'orange au vert.

   Remarque : vous devez mettre à jour le compte et le mot de passe de l'utilisateur de l'équipement avant de mettre à niveau le firmware.

5. Sélectionnez les équipements que vous souhaitez mettre à niveau en cochant leurs cases respectives, puis cliquez sur « Mettre à niveau le firmware ».

   Remarque : vous pouvez mettre à niveau le firmware de plusieurs équipements qui

utilisent les mêmes fichiers de firmware (mise à niveau de firmware en masse).

6. Sélectionnez les fichiers Firmware et Données et cliquez sur OK pour exécuter la mise à niveau du firmware, comme illustré dans la figure 7.

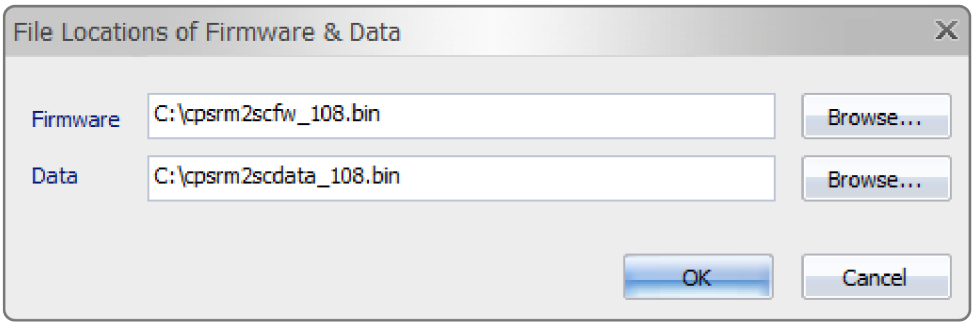


Figure 7. Fenêtre Emplacements des fichiers Firmware et Données.

7. Cliquez sur « Oui » pour démarrer la mise à niveau du firmware sur les équipements sélectionnés, comme illustré dans la figure 8.

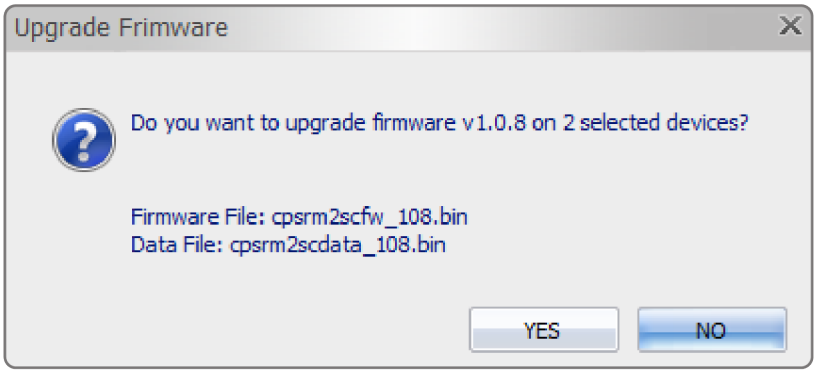


Figure 8. Fenêtre de confirmation du message de mise à niveau du firmware.

8. Si la mise à niveau du firmware est implémentée, le résultat s'affiche dans la fenêtre principale, comme illustré dans la figure 9.

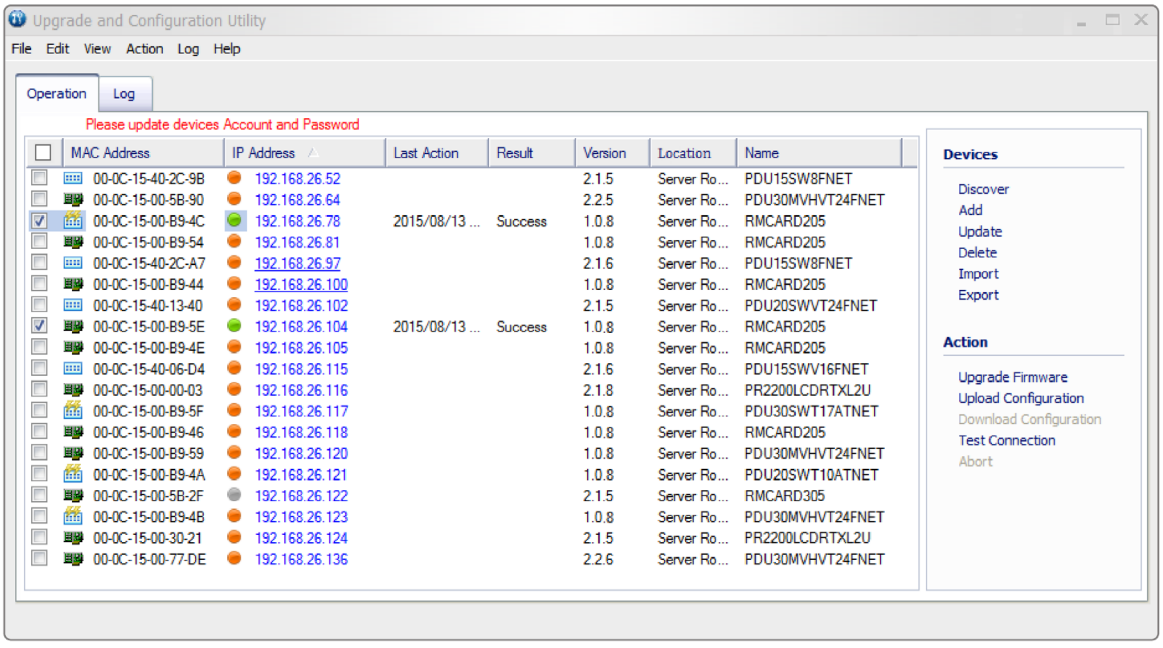


Figure 9. Succès de la mise à niveau du firmware dans la fenêtre principale.

Méthode 3 : utilisation de la commande Secure Copy (SCP)

Suivez les étapes ci-dessous pour mettre à jour le firmware via SCP.

Remarque : seules les versions 1.1.2 et ultérieures du firmware prennent en charge la fonctionnalité de mise à jour du firmware via SCP.

Pour les utilisateurs de Windows :

1. Téléchargez tout utilitaire client PuTTY Secure Copy (PSCP).
2. Enregistrez les fichiers du firmware et l'utilitaire PSCP dans le même dossier.
3. Ouvrez l'interface de ligne de commande et modifiez le chemin de manière à ce qu'il indique l'emplacement où les fichiers du firmware et l'utilitaire PSCP sont enregistrés.
4. Saisissez la commande suivante pour mettre à jour le firmware :

   `pscp -scp <nom de fichier> <utilisateur>@<adresse IP de RMCARD>:`

Remarque :

(1) le paramètre SSH de RMCARD doit être activé.

(2) `<nom de fichier>` est le nom de fichier du firmware. Deux fichiers de firmware doivent être chargés : `cpsrm2scfw_XXX.bin` et `cpsrm2scdata_XXX.bin` . Pour mettre à niveau la version du firmware, les deux fichiers doivent être chargés. Il n'est possible de charger qu'un seul fichier de firmware à la fois. Il est recommandé de commencer par charger le fichier de firmware `cpsrm2scfw_XXX.bin`, puis le fichier de données `cpsrm2scdata_XXX.bin`.

(3) `<utilisateur>` est le nom d'utilisateur du compte SSH sur RMCARD.

(4) Assurez-vous d'ajouter « : » après l'adresse IP.

Par exemple :

`pscp -scp cpsrm2scfw_xxx.bin cyber@192.168.1.100:`

Remarque : `cpsrm2scfw_xxx.bin` est le fichier de la version du firmware mise à jour.

5. Après l'exécution de la commande, un message peut s'afficher pour vous demander si vous faites confiance à l'hôte. Pour continuer, saisissez « **y** » dans les 10 secondes qui suivent.
6. Dans l'écran suivant, saisissez le mot de passe de RMCARD. Le transfert du fichier du firmware peut prendre quelques minutes. Patientez jusqu'à ce que l'indicateur de progression indique 100 %. Le système se déconnecte automatiquement et redémarre une fois le transfert terminé.
7. Répétez les étapes 4 à 6 pour charger le fichier de données`cpsrm2scdata_XXX.bin` et terminer le processus de mise à jour du firmware.
8. En cas d'échec du transfert du fichier du firmware, un message d'erreur apparaît. Essayez de saisir à nouveau la commande et de l'exécuter.

Pour les utilisateurs de Linux, MacOS et Unix :

1. Installez la distribution correspondante d'un client SSH ou SCP. Par exemple, le client Openssh.
2. Ouvrez le terminal et modifiez le chemin de manière à ce qu'il indique l'emplacement où les fichiers du firmware sont enregistrés.
3. Saisissez la commande suivante pour mettre à jour le firmware :

   `scp <nom de fichier> <utilisateur>@<adresse IP de RMCARD>:`

Remarque :

(1) le paramètre SSH de RMCARD doit être activé.

(2) `<nom de fichier>` est le nom de fichier du firmware. Deux fichiers de firmware doivent être chargés : `cpsrm2scfw_XXX.bin` et `cpsrm2scdata_XXX.bin` . Pour mettre à niveau la version du firmware, les deux fichiers doivent être chargés. Il n'est possible de charger qu'un seul fichier de firmware à la fois. Il est recommandé de commencer par charger le fichier de firmware `cpsrm2scfw_XXX.bin`, puis le fichier de données `cpsrm2scdata_XXX.bin`.

(3) `<utilisateur>` est le nom d'utilisateur du compte SSH sur RMCARD.

(4) Assurez-vous d'ajouter « : » après l'adresse IP.

Par exemple :

`scp cpsrm2scfw_xxx.bin cyber@192.168.1.100:`

Remarque : `cpsrm2scfw_xxx.bin` est le fichier de la version du firmware mise à jour.

4. Après l'exécution de la commande, un message peut s'afficher pour vous demander si vous faites confiance à l'hôte. Pour continuer, saisissez « **y** » dans les 10 secondes qui suivent.
5. Dans l'écran suivant, saisissez le mot de passe de RMCARD. Le transfert du fichier du firmware peut prendre quelques minutes. Patientez jusqu'à ce que l'indicateur de progression indique 100 %. Le système se déconnecte automatiquement et redémarre une fois le transfert terminé.
6. Répétez les étapes 3 à 5 pour charger le fichier de données`cpsrm2scdata_XXX.bin` et terminer le processus de mise à jour du firmware.
7. En cas d'échec du transfert du fichier du firmware, un message d'erreur apparaît. Essayez de saisir à nouveau la commande et de l'exécuter.

Enregistrement et restauration des paramètres de configuration

Méthode 1 : utilisation de l'interface Web
Vous pouvez facilement enregistrer et restaurer la configuration de l'équipement sur votre PC local dans **[Système->À propos]**.

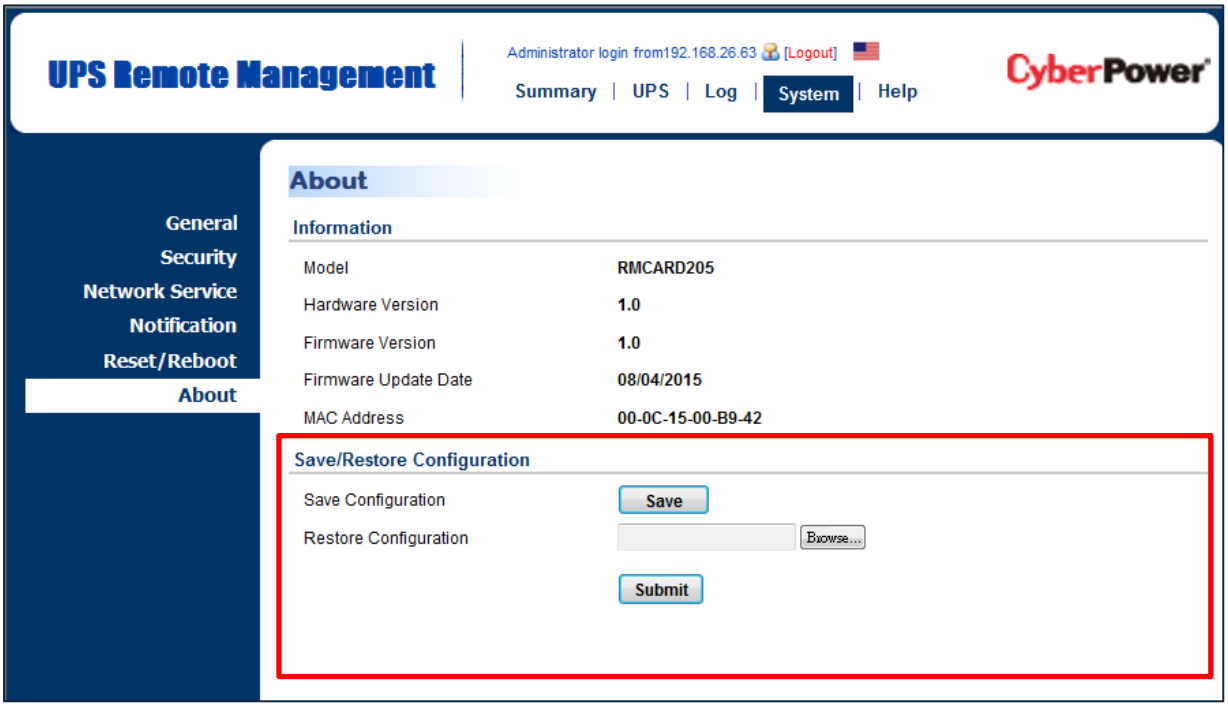


Figure 10. Configuration de l'enregistrement/restauration dans la fenêtre principale.

Vous pouvez facilement enregistrer et restaurer la configuration de l'équipement sur votre PC local dans **[Système->À propos]**, comme illustré dans la figure 10.
Pour enregistrer le fichier de configuration sur votre PC local, cliquez sur « Enregistrer ». Le format par défaut du fichier texte sera AAAA_MM_JJ_HHMM.txt. Pour restaurer une configuration précédemment enregistrée, cliquez sur « Parcourir » pour sélectionner l'emplacement du fichier de configuration enregistré et cliquez sur « Soumettre ».

Remarque : seules les versions 1.1.5 et ultérieures du firmware prennent en charge la fonctionnalité d'enregistrement et de restauration de la configuration avec les paramètres actuels de l'onduleur et du commutateur de transfert automatique.

Méthode 2 : utilisation de la commande Secure Copy (SCP)
Suivez les étapes ci-dessous pour restaurer la configuration via SCP.

Remarque : seules les versions 1.1.2 et ultérieures du firmware prennent en charge la fonctionnalité de restauration de la configuration via SCP.

Pour les utilisateurs de Windows :

1. Téléchargez tout utilitaire client PuTTY Secure Copy (PSCP).
2. Enregistrez le fichier de configuration et l'utilitaire PSCP dans le même dossier.
3. Ouvrez l'interface de ligne de commande et modifiez le chemin de manière à ce qu'il indique l'emplacement où sont enregistrés le fichier de configuration et l'utilitaire PSCP.
4. Saisissez la commande suivante pour restaurer la configuration :
   pscp -scp <nom de fichier> <utilisateur>@<adresse IP de RMCARD>:

Remarque :

(1) le paramètre SSH de RMCARD doit être activé.

(2) `<nom de fichier>` est le nom du fichier de configuration avec le format par défaut suivant : AAAA_MM_JJ_HHMM.txt.

(3) `<utilisateur>` est le nom d'utilisateur du compte SSH sur RMCARD.

(4) Assurez-vous d'ajouter « : » après l'adresse IP.

Par exemple :

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

Remarque : `AAAA_MM_JJ_HHMM.txt` est le fichier de configuration à restaurer.

5. Après l'exécution de la commande, un message peut s'afficher pour vous demander si vous faites confiance à l'hôte. Pour continuer, saisissez « y » dans les 10 secondes qui suivent.
6. Dans l'écran suivant, saisissez le mot de passe de RMCARD. Patientez jusqu'à ce que l'indicateur de progression indique 100 %. Le système se déconnecte automatiquement et redémarre une fois le transfert terminé.

Pour les utilisateurs de Linux, MacOS et Unix :

1. Installez la distribution correspondante d'un client SSH ou SCP. Par exemple, le client OpenSSH.
2. Ouvrez le terminal et modifiez le chemin de manière à ce qu'il indique l'emplacement où les fichiers de configuration sont enregistrés.
3. Saisissez la commande suivante pour restaurer la configuration :
   scp <nom de fichier> <utilisateur>@<adresse IP de RMCARD>:

Remarque :

(1) le paramètre SSH de RMCARD doit être activé.

(2) `<nom de fichier>` est le nom du fichier de configuration avec le format par défaut suivant : AAAA_MM_JJ_HHMM.txt.

(3) `<utilisateur>` est le nom d'utilisateur du compte SSH sur RMCARD.

(4) Assurez-vous d'ajouter « : » après l'adresse IP.

Par exemple :

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

Remarque : `AAAA_MM_JJ_HHMM.txt` est le fichier de configuration à restaurer.

4. Après l'exécution de la commande, un message peut s'afficher pour vous demander si vous faites confiance à l'hôte. Pour continuer, saisissez « y » dans les 10 secondes qui suivent.
5. Dans l'écran suivant, saisissez le mot de passe de RMCARD. Patientez jusqu'à ce que l'indicateur de progression indique 100 %. Le système se déconnecte automatiquement et redémarre une fois le transfert terminé.

Chargement de la clé d'hôte SSH via Secure Copy (SCP)

Vous pouvez charger une clé d'hôte SSH sur RMCARD205 à l'aide des commandes Secure Copy.

Asssurez-vous que le nom du fichier chargé contient la chaîne de début « ssh_hostkey_ ».

Les exemples de noms de fichier suivants sont acceptables :

ssh_hostkey_sample1.pem
ssh_hostkey_1024.pem
ssh_hostkey_type100.***

Exemple de processus de chargement

1. Téléchargez l'utilitaire client PuTTY Secure Copy (PSCP).
2. Placez le fichier de clé d'hôte SSH et l'utilitaire PSCP dans le même dossier.
3. Ouvrez l'invite de commande et modifiez le chemin de manière à ce qu'il indique l'emplacement où le fichier de la clé d'hôte SSH et l'utilitaire PSCP sont enregistrés.
4. Saisissez la commande suivante :

   `pscp -scp <nom de fichier> <compte_admin>@<adresse IP de RMCARD>:`

   Ex. :pscp -scp ssh_hostkey_xxx.xxx cyber@192.168.203.66:
5. Après l'exécution de la commande, un message peut s'afficher pour vous demander si vous faites confiance à l'hôte. Saisissez « **y** » dans les 10 secondes qui suivent.
6. Dans l'écran suivant, saisissez le mot de passe admin. Le transfert du fichier peut prendre quelques minutes. Patientez jusqu'à ce que l'indicateur de progression indique 100 %. Le système se déconnecte automatiquement et redémarre une fois le transfert terminé.

Exigences de la clé d'hôte

Les clés d'hôte SSH sont créées avec les clés RSA 2 048 bits ou 4 096 bits.

Dépannage

Problème	Solution
Impossible de configurer la carte de gestion à distance avec la méthode 1 ou 2	1. Vérifiez l'état des LED ; normal si les LED jaune et verte sont toutes les deux allumées. Si la LED verte est éteinte : ►Vérifiez que la carte de gestion à distance est correctement installée dans l'équipement et que l'équipement est alimenté. Si la LED jaune est éteinte : ►Assurez-vous que la connexion réseau est correcte. 2. Assurez-vous que le PC utilisé se trouve sur le même sous-réseau local que l'équipement CyberPower avec lequel vous essayez de communiquer. 3. Assurez-vous que le cavalier est correctement installé sur la broche de réinitialisation.
Impossible d'envoyer un test Ping à la carte de gestion à distance	1. Utilisez la méthode 1 et/ou 2 pour obtenir/définir une adresse IP correcte pour la carte de gestion à distance. 2. Si le PC utilisé se trouve sur un autre sous-réseau que la carte de gestion à distance, vérifiez la configuration du masque de sous-réseau et l'adresse IP de la passerelle.
Nom d'utilisateur et mot de passe perdus	Reportez-vous à la section « Réinitialisation aux paramètres par défaut d'usine / Récupération à partir d'un mot de passe perdu »
Configuration réseau par défaut	IP : 192.168.20.177 Masque de sous-réseau : 255.255.255.0 DHCP : On
Impossible d'accéder à l'interface Web	1. Assurez-vous que vous pouvez envoyer un test Ping à RMCARD. 2. Assurez-vous que vous spécifiez l'URL correcte. 3. Assurez-vous que l'accès HTTP/HTTPS est activé en vous connectant à la carte via CLI (client Telnet ou SSH).
Impossible d'exécuter une commande SNMP get/set	SNMPv1 : vérifiez le nom de communauté. SNMPv3 : vérifiez la configuration du profil utilisateur.
Impossible de recevoir des traps	1. Assurez-vous que les types de trap (SNMPv1/SNMPv3) et les récepteurs de trap sont correctement configurés. 2. Assurez-vous que l'adresse IP de la passerelle est correctement configurée si RMCARD et NMS se trouvent sur des réseaux différents.

Certificats de conformité

Avertissement de la FCC

Cet équipement a été testé et déclaré conforme aux limites pour un équipement numérique de Classe A, selon la section 15 des règlements de la FCC. Ces limites sont destinées à assurer une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Cet équipement produit, utilise et peut émettre de l'énergie radio électrique et, s'il n'est pas installé et utilisé conformément aux présentes instructions, peut causer des interférences nuisibles aux communications radio. L'utilisation de cet appareil dans une installation résidentielle peut entraîner des interférences nuisibles, lesquelles devront être corrigées aux frais de l'utilisateur.

Les accessoires spéciaux éventuellement requis pour la conformité doivent être spécifiés dans les instructions.

Cet équipement est conforme à la section 15 des règlements de la FCC. Son fonctionnement est soumis aux deux conditions suivantes : (1) Cet équipement ne doit pas provoquer d'interférences nuisibles et (2) il doit accepter toute autre interférence reçue, y compris les interférences pouvant entraîner un fonctionnement non désiré.

The Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.
Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Union européenne

Ce produit appartient à la Classe A. Dans un environnement domestique, il peut provoquer des perturbations radioélectriques. Le cas échéant, l'utilisateur devra prendre les mesures adéquates.

⚠ **AVERTISSEMENT :** ce produit peut vous exposer à des produits chimiques, y compris à du styrène, qui
est reconnu, en Californie, pour causer le cancer, et à du bisphénol A, qui est reconnu, en Californie, pour causer des malformations congénitales ou autres problèmes du système reproducteur.
Pour en savoir plus, consultez le site www.P65Warnings.ca.gov.

Annexe 1 : identification de l'adresse IP pour la carte de gestion à distance CyberPower

Présentation

Tous les équipements connectés à un réseau informatique doivent avoir une adresse IP. L'adresse IP de chaque équipement est unique. Une même adresse ne peut pas être utilisée deux fois. Pour attribuer une adresse IP à la carte de gestion à distance CyberPower, vous devez déterminer la plage d'adresses IP disponibles, puis en choisir une inutilisée pour l'attribuer à la carte de gestion à distance.

Remarque : vous devrez peut-être contacter votre administrateur de réseau pour obtenir une adresse IP disponible.

Pour trouver une adresse IP, procédez comme suit :

1. **Localisez le sous-réseau de la carte de gestion à distance CyberPower.**
   Une façon de déterminer la plage d'adresses IP possibles est d'afficher la configuration réseau sur une station de travail. Cliquez sur [Démarrer] et sélectionnez [Exécuter]. Saisissez « command » dans la fenêtre ouverte et cliquez sur [OK]. À l'invite de commande, saisissez « ipconfig /all » et appuyez sur [Entrée]. L'ordinateur affiche les informations réseau suivantes :

```
Adaptateur Ethernet
Suffixe DNS spécifique à la connexion.....: xxxx.com
 Description.....: Adaptateur LAN D-Link DE220 ISA PnP
 Adresse physique.....: 00-80-C8-DA-7A-C0
 DHCP activé.....: Oui
 Autoconfiguration activée...: Oui
 Adresse IP.....: 192.168.20.102
 Masque de sous-réseau.....: 255.255.255.0
 Passerelle par défaut.....: 192.168.20.1
 Serveur DHCP.....: 192.168.20.1
 Serveurs DNS.....: 211.20.71.202
                                168.95.1.1
```

2. **Sélectionnez une adresse IP pour la carte de gestion à distance CyberPower.**
   Vérifiez que les adresses IP de l'ordinateur et la carte de gestion à distance appartiennent au même sous-réseau. Reportez-vous aux informations réseau ci-dessus. L'adresse IP possible pour la carte de gestion à distance peut être 192.168.20.* (* représente tout nombre compris entre 1 et 255). De même, si le masque de sous-réseau est 255.255.0.0, l'adresse IP de la carte de gestion à distance peut être 192.168.*.* pour atteindre le même sous-réseau que l'ordinateur.
   Pour vérifier qu'aucun autre équipement n'est connecté au réseau avec la même adresse IP, exécutez le test « Ping 192.168.20.240 » à l'invite DOS Mode si vous souhaitez configurer l'adresse IP 192.168.20.240. Si la réponse ci-dessous s'affiche, l'adresse IP n'est probablement pas utilisée et peut être disponible pour la carte de gestion à distance CyberPower.

```
Exécution du test 192.168.20.240 avec 32 octets de données :

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Si la réponse ci-dessous s'affiche, l'adresse IP est utilisée. Essayez une autre adresse IP jusqu'à ce que vous en trouviez une disponible.

```
Exécution du test 192.168.20.240 avec 32 octets de données :

Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
Reply from 192.168.20.240: bytes=32 time<10ms TTL=64
```

Annexe 2 : comment configurer un compte utilisateur RMCARD sur les serveurs d'authentification

RADIUS

1. Ajoutez un nouvel attribut dans le dictionnaire RADIUS en tant que fournisseur Cyber :
   3808 – Fournisseur
2. Ajoutez deux nouveaux attributs spécifiques à l'interface serveur RADIUS sous le fournisseur :

(1)**Cyber-Service-Type** (variable de nombre entier)

Cyber-Service-Type peut accepter trois valeurs de paramètre d'entier :

1 – Administrateur

2 – Observateur

3 – Utilisateur des sorties

(2)**Cyber-Outlets** (variable de chaîne)

Cyber-Outlets peut accepter une chaîne décrivant les numéros de sortie. Cet attribut permettra à l'utilisateur des sorties d'accéder aux sorties désignées et de les contrôler. Par exemple, Cyber-Outlets="1,2,5" permet à l'utilisateur de contrôler les sorties 1, 2 et 5.

Exemple de fichier de dictionnaire :

```
FOURNISSEUR          Cyber        3808
DÉBUT-FOURNISSEUR    Cyber
ATTRIBUT       Cyber-Service-Type     1      entier
ATTRIBUT       Cyber-Outlets           2      chaîne
VALEUR           Cyber-Service-Type     Admin      1
VALEUR           Cyber-Service-Type     Observateur     2
VALEUR           Cyber-Service-Type     Sortie     3
FIN-FOURNISSEUR    Cyber
```

LDAP et Windows AD

Ajoutez l'un des attributs ci-dessous à **description** dans l'interface d'OpenLDAP ou de Windows AD pour indiquer le type de compte utilisateur et l'authentification :

1. **cyber_admin** (Administrateur)
2. **cyber_viewer** (Observateur)
3. **cyber_outlet="string"** (Utilisateur des sorties)

La chaîne entrée dans cyber_outlet désigne les sorties auxquelles l'utilisateur des sorties peut accéder et qu'il peut contrôler. Par exemple, cyber_outlet="1,2,5" permet à l'utilisateur de contrôler les sorties 1, 2 et 5.

Annexe 3 : mise à niveau du firmware de l'onduleur

Vous pouvez vérifier la « version du firmware » à la page **[Onduleur->Informations]** de l'interface utilisateur web de RMCARD.

Méthode 1 : utilisation de l'interface Web

1. Mettez l'onduleur hors tension via [Onduleur->Commutateur principal].
2. Accédez à la page Version du firmware via [Onduleur->Informations->Version du firmware].
3. Chargez le firmware de l'onduleur en cliquant sur Mettre à jour, puis choisissez Fichier pour sélectionner l'emplacement du fichier du firmware de l'onduleur.
4. Cliquez sur Soumettre pour implémenter la mise à jour. Une fenêtre de mise à niveau réussie apparaît après la mise à niveau.
5. Mettez l'onduleur sous tension via [Onduleur->Commutateur principal].

Méthode 2 : utilisation de la commande FTP

Le service FTP doit être activé avant de tenter d'exécuter une mise à niveau du firmware.
Pour mettre à niveau le firmware via FTP, procédez comme suit :

1. Mettez l'onduleur hors tension.
2. Extrayez le fichier de mise à jour dans « C:\ ».
3. Ouvrez une fenêtre d'invite de commande.
4. Connectez-vous à la carte de gestion à distance CyberPower en saisissant la commande FTP suivante à l'invite de commande :
   (1) `ftp`
   (2) `ftp > open`
   (3) To [adresse IP actuelle de RMCARD] [port] ; ex. : `To 192.168.22.126 21`
   (4) Entrez le NOM D'UTILISATEUR et le MOT DE PASSE (mêmes que pour le compte Administrateur dans l'interface utilisateur Web ; voir les paramètres d'usine par défaut à la page 6).
5. Chargez le fichier. Saisissez :
   `ftp > bin`
   `ftp > put XXX.bin`
6. Le chargement est à présent terminé. Saisissez :
   `ftp > quit`
7. Mettez l'onduleur sous tension.

Remarque : 1. La mise à jour peut prendre environ 5 minutes. N'exécutez aucune autre action et ne retirez pas RMCARD durant le processus de mise à jour du firmware de l'onduleur.

Remarque : 2. La progression de la mise à jour s'affiche uniquement dans l'interface Web.

Remarque : 3. Si le message « Chargement d'un firmware d'onduleur non valide » apparaît après le chargement du fichier du firmware de l'onduleur via l'interface Web, vérifiez les points suivants :

(1) Le fichier est un fichier binaire pour le firmware de l'onduleur.

(2) Le fichier du firmware de l'onduleur prend en charge le modèle d'onduleur.

Annexe 4 : support logiciel

PowerPanel® Business Remote permet d'effectuer un arrêt correct du système d'exploitation lorsqu'il est protégé par un onduleur/ATS PDU sur lequel une carte de gestion à distance est installée. Le logiciel PowerPanel® Business est disponible sur le site Web officiel de CyberPower Systems. Consultez le site www.CyberPower.com et accédez à la section des logiciels pour le télécharger gratuitement.

Communication avec PowerPanel® Business Remote

La carte de gestion à distance doit s'authentifier avec PowerPanel® Business Remote via une phrase secrète partagée, comme illustré dans la figure 11.

Remarque : la phrase secrète par défaut est « powerpanel.encryption.key ».

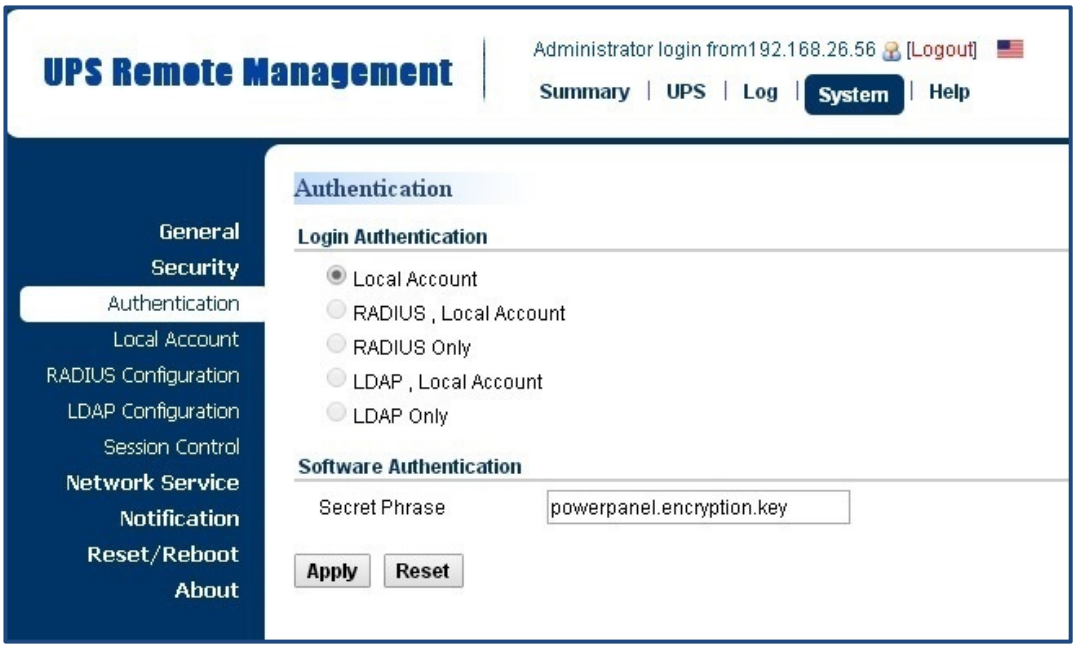


Figure 11. Système RMCARD>Interface Web d'authentification.

Remarque : le logiciel PowerPanel® Business prend en charge l'arrêt correct automatisé des hôtes VMware ESX/ESXi et d'autres plateformes de virtualisation, telles que Microsoft Hyper-V et Citrix.

Obtention d'une adresse IP pour le système d'exploitation Linux

Les instructions fournies à la section « Configuration de l'adresse IP de la carte de gestion à distance CyberPower » sont pour le système d'exploitation Windows. Pour le système d'exploitation Linux, utilisez le logiciel PowerPanel® Business Remote pour effectuer un balayage et obtenir l'adresse IP. Pour ce faire, accédez à **[Puissance->Configuration]** dans l'interface Web de PowerPanel® Business Remote, comme illustré dans la figure 12. Pour en savoir plus, reportez-vous au manuel d'utilisation de PowerPanel® Business.

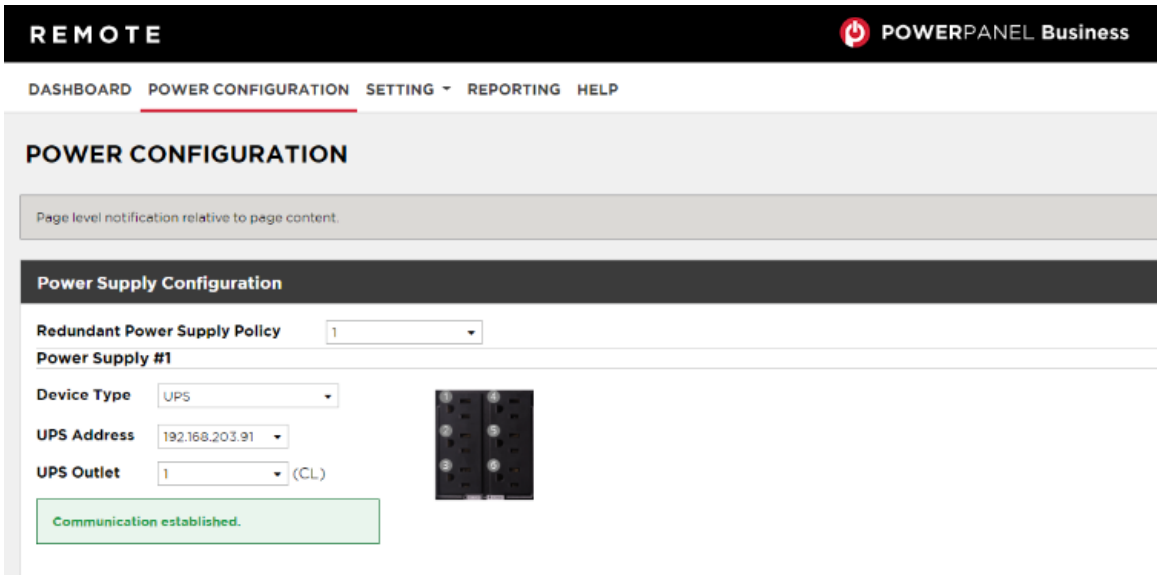
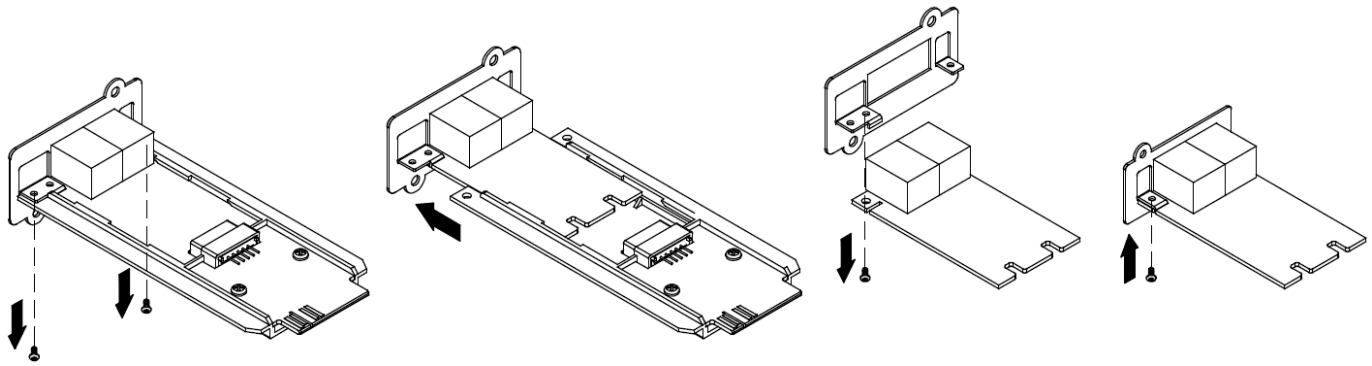


Figure 12. Interface Web de PowerPanel® Business Remote.

Annexe 5 : guide de l'adaptateur RMCARD

Retrait de l'adaptateur pour convertir un système RMCARD305 en système RMCARD205



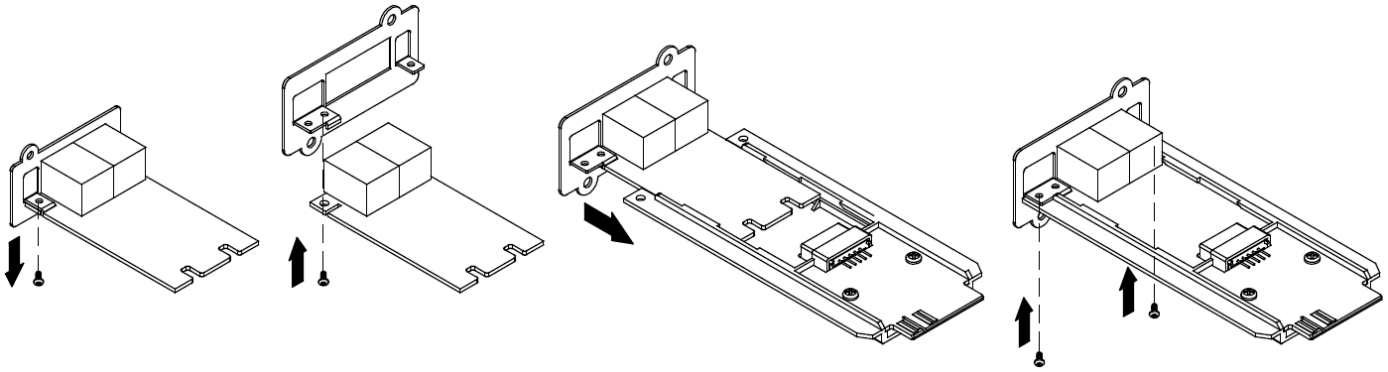
Étape 1. Retirez les deux vis de l'adaptateur qui maintiennent la carte en place.

Étape 2. Retirez la carte de l'adaptateur.

Étape 3. Retirez la vis qui maintient le panneau avant du système RMCARD305 à la carte.

Étape 4. Fixez le panneau avant du système RMCARD205 à la carte.

Ajout de l'adaptateur pour convertir un système RMCARD205 en système RMCARD305



Étape 1. Retirez la vis qui maintient le panneau avant à la carte et retirez le panneau avant du système RMCARD205.

Étape 2. Vissez le panneau avant du système RMCARD305 sur la carte.

Étape 3. Insérez la carte dans l'adaptateur. Assurez-vous que la carte est bien en place.

Étape 4. Utilisez les deux vis de l'adaptateur pour mettre en place la carte.

Remarque : le kit d'adaptateur RMCARD n'est pas inclus avec le système RMCARD205. Contactez CyberPower ou le support technique pour les informations de commande.

Remarque : le système RMCARD205 est conçu pour le port d'extension de la carte SNMP de 43 x 18 mm (1,69 x 0,71 pouces) des onduleurs et ATS PDU CyberPower séries PR, OR et 1-3 kVA OL.

Le système RMCARD305 est conçu pour le port d'extension de la carte SNMP de 57 x 23 mm (2,24 x 0,91 pouces)
de l'onduleur CyberPower série OL6-10 kVA.

NITRAM SASU
www.nitram.fr

NITRAM SASU
Z.I. Saint Séverin
28220 Cloyes S/Loir – France
Tél: +33 (0) 2 37 98 61 50

CE

K01-E000025-00