Schneider Electric

Guide de l'utilisateur

UPS Network Management Card 2

AP9630, AP9631,
AP9335T, AP9335TH, AP9810

本マニュアル＜各国の言語に対応する＞はェブサイト (www.apc.com) からダウンロードできます。

This manual is available in English on the Web site (www.apc.com).

Dieses Handbuch ist in Deutsch auf der Webseite (www.apc.com) verfügbar.

Este manual está disponible en español en la página web (www.apc.com).

Ce manuel est disponible en français sur le site internet (www.apc.com).

Questo manuale è disponibile in italiano sul sito web (www.apc.com).

Este manual está disponível em português no site (www.apc.com).

Данное руководство на русском языке доступно на сайте (www.apc.com)

Deze handleiding is beschikbaar in het Nederlands op Website (www.apc.com).

在公司的网站上（www.apc.com）有本手册的中文版。

웹싸이트 (www.apc.com) 에 한국어 매뉴얼 있습니다 .

This manual is available in English on the enclosed CD.

Dieses Handbuch ist in Deutsch auf der beiliegenden CD-ROM verfügbar.

Este manual está disponible en español en el CD-ROM adjunto.

Ce manuel est disponible en français sur le CD-ROM ci-inclus.

Questo manuale è disponibile in italiano nel CD-ROM allegato.

Este manual está disponível em português no CD fornecido.

Äàííîå ðóêîâîäñòâî íà ðóññêîì ÿçûêå èìåþòñÿ íà ïðèëàãàåìîì êîìïàêò-äèñêå.

Deze handleiding staat in het Nederlands op de bijgevoegde cd.

本マニュアルの日本語版は同梱の CD-ROM からご覧になれます。

동봉된 CD 안에 한국어 매뉴얼이 있습니다 .

您可以从包含的 CD 上获得本手册的中文版本。

Introduction

Description du produit

Fonctionnalités

Les deux cartes de gestion réseau Schneider Electric mentionnées ci-dessous sont des produits basés sur le Web, compatibles IPv6, qui gèrent les périphériques pris en charge selon plusieurs normes ouvertes telles que :

- Protocole HTTP (Hypertext Transfer Protocol)
- Protocole simplifié de gestion de réseau (SNMP) versions 1 et 3 (SNMPv1, SNMPv3)
- Protocole de transfert de fichiers FTP (File Transfer Protocol)
- Telnet
- Secure SHell (SSH)
- Protocole HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)
- SCP (Secure CoPy)

Fonctionnalités de la carte de gestion réseau **AP9630** :

- Contrôle de l'onduleur et programmation des tests automatiques
- Création de journaux de consignation des événements et des données
- Prise en charge de l'utilitaire PowerChute® Network Shutdown.
- Utilisation d'un serveur DHCP (Dynamic Host Configuration Protocol) ou BOOTP (BOOTstrap Protocol) pour fournir les paramètres réseau (TCP/IP) de la carte de gestion réseau.
- Utilisation du service RMS (Remote Monitoring Service).
- Configuration des notifications par consignation des événements (par la carte de gestion réseau et Syslog), par e-mail et par traps SNMP. Vous pouvez configurer les notifications pour un seul événement ou un groupe d'événements, en fonction du niveau de gravité ou de la catégorie des événements.
- Possibilité d'exporter un fichier de configuration utilisateur (.ini) depuis une carte configurée vers une ou plusieurs cartes non configurées sans le convertir en fichier binaire.
- Sélection de protocoles de sécurité pour l'authentification et le codage.
- Communication avec InfraStruXure® Central ou InfraStruXure Manager.

La carte de gestion réseau **AP9631** comprend toutes les fonctions de la carte de gestion réseau AP9630 et présente les caractéristiques supplémentaires suivantes :

- Deux ports USB
- Prise en charge de deux ports universels d'entrée/sortie, auxquels vous pouvez connecter :
  - des capteurs de température ou de température/humidité,
  - des connecteurs d'entrée/sortie de relais acceptant deux contacts d'entrée et un relais de sortie.

Appareils permettant d'installer la carte de gestion réseau. La carte de gestion réseau peut être installée dans les appareils suivants :

- Tous les modèles Smart-UPS® équipés d'un connecteur d'extension interne ou tous les onduleurs Symmetra® sauf les onduleurs Symmetra PX 250 et Symmetra PX 500.
- Châssis d'extension (AP9600)
- Châssis d'extension triple (AP9604)

Configuration initiale IPv4

Vous devez définir deux paramètres TCP/IP pour que votre carte de gestion réseau puisse fonctionner en réseau :

- L'adresse IP de votre carte de gestion réseau
- L'adresse IP de la passerelle par défaut (nécessaire uniquement hors segment du réseau)

Attention : n'utilisez pas l'adresse de retour en boucle (127.0.0.1) comme passerelle par défaut. Ceci désactiverait la carte. Vous devriez alors ouvrir une session à l'aide d'une connexion série et rétablir les paramètres TCP/IP par défaut.

Pour configurer les paramètres TCP/IP, consultez le *Manuel d'installation* de la carte de gestion réseau disponible sur le CD d'*utilitaires* de la carte de gestion réseau et sous forme imprimée.

Pour des informations détaillées sur l'utilisation d'un serveur DHCP pour configurer les paramètres TCP/IP d'une carte de gestion réseau, consultez « Paramètres TCP/IP et de communication » en page 70.

Configuration initiale IPv6

La flexibilité de la configuration réseau IPv6 permet de s'adapter aux exigences de l'utilisateur. Pour configurer les paramètres TCP/IP pour IPv6, consultez le *Manuel d'installation* de la carte de gestion réseau disponible au format PDF sur le CD d'utilitaires de la carte de gestion réseau et sur le site Web à l'adresse **www.apc.com**.

Caractéristiques de la gestion réseau

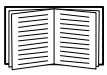
Ces applications et utilitaires fonctionnent avec un onduleur connecté au réseau par l'intermédiaire d'une carte de gestion réseau.

- PowerChute Network Shutdown — Assure l'arrêt progressif à distance sans supervision d'ordinateurs connectés aux onduleurs.
- Base de données de gestion (MIB) PowerNet® avec navigateur MIB standard — Pour exécuter des commandes SNMP SET et GET, et utiliser des traps SNMP.
- InfraStruXure Central — Assure la gestion de l'alimentation au niveau de l'entreprise ainsi que la gestion des agents, des onduleurs et des contrôleurs d'environnement.
- Assistant de configuration IP des périphériques — Pour configurer les paramètres de base d'une ou de plusieurs cartes de gestion sur le réseau.
- Assistant de sécurité — Pour créer les composants nécessaires pour un haut niveau de sécurité de la carte de gestion réseau lorsque vous utilisez le protocole SSL (Secure Sockets Layer) et les protocoles et routines de codage connexes.

Caractéristiques de gestion interne

Présentation

Utilisez l'interface Web ou l'interface par lignes de commande pour consulter l'état de l'onduleur et gérer l'onduleur et la carte de gestion réseau. Vous pouvez aussi utiliser le protocole SNMP pour surveiller l'état de l'onduleur.



Pour de plus amples informations sur les interfaces utilisateur internes, consultez « Interface Web » en page 29 et « Interface en ligne de commande » en page 8. Consultez « SNMP » en page 79 pour des informations sur le contrôle d'accès SNMP à la carte de gestion réseau.

Priorité d'accès pour l'ouverture de session

Un seul utilisateur à la fois peut se connecter à la carte de gestion réseau. Les priorités d’accès suivantes s’appliquent, en ordre décroissant :

- Accès local à l'interface par lignes de commande depuis un ordinateur relié directement en série à la carte de gestion
- Accès Telnet ou SSH à l'interface par lignes de commande depuis un ordinateur distant
- Accès par le Web, directement ou par l'intermédiaire d'InfraStruXure Central

Remarque : le protocole SNMP a le droit d'accès **Écrire +** et **Écrire**. L'accès en « Écriture + » a la priorité maximum et permet de se connecter même lorsqu'un autre utilisateur l'est déjà. L'accès en « Écriture » est équivalent à l'accès par le Web.

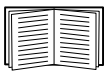
Types de comptes utilisateurs

La carte de gestion réseau a trois niveaux d'accès (Administrateur, Utilisateur du périphérique et Utilisateur en lecture seule) protégés par un mot de passe et un nom d'utilisateur.

- L'administrateur peut utiliser tous les menus de l'interface Web ainsi que toutes les commandes de l'interface par lignes de commande. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux **apc**.
- Le niveau Utilisateur du périphérique permet d'accéder uniquement aux éléments suivants :
  - Dans l'interface Web, accès aux menus de l'onglet **Onduleur** et aux journaux de consignation des événements et des données, accessibles sous les en-têtes **Événements** et **Données** du menu de navigation gauche de l'onglet **Journaux de consignation**. Les journaux de consignation des événements et des données ne comprennent aucun bouton de suppression du journal.
  - Dans l'interface par lignes de commande, accès aux fonctions et options équivalentes.

    Le nom d'utilisateur par défaut est **device** et le mot de passe par défaut est **apc**.
- Un utilisateur en lecture seule dispose de l'accès limité suivant :
  - Accès uniquement par l'intermédiaire de l'interface Web.
  - Accès aux mêmes onglets et menus que le niveau Utilisateur du périphérique, mais sans possibilité de modifier les configurations, de contrôler des périphériques, de supprimer des données, ni d'utiliser des options de transfert de fichiers. Les liens vers les options de configuration sont visibles mais désactivés. Les journaux de consignation des événements et des données ne comprennent aucun bouton de suppression du journal.

    Le nom d'utilisateur par défaut est **readonly** et le mot de passe par défaut est **apc**.



Pour définir les valeurs **Nom d'utilisateur** et **Mot de passe** des trois types de comptes, consultez « Configuration de l'accès utilisateur » en page 66.

Procédure de récupération suite à la perte du mot de passe

Vous pouvez accéder à l'interface par lignes de commande depuis un ordinateur local connecté à la carte de gestion réseau par port série.

1. Sélectionnez un port série de l'ordinateur local et désactivez tout service exploitant ce port.
2. Raccordez le câble série fourni (numéro de pièce 940-0299) au port choisi sur l'ordinateur et au port de configuration de la carte de gestion réseau.
3. Exécutez un programme d'émulation de terminal (tel que HyperTerminal®) et configurez le port sélectionné sur 9600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.
4. Appuyez sur ENTRÉE, plusieurs fois si nécessaire, pour afficher l'invite **Nom d'utilisateur**. Si l'invite **Nom d'utilisateur** ne s'affiche pas, vérifiez les éléments suivants :
   - Le port série n'est pas utilisé par une autre application.
   - Les paramètres de terminal sont conformes à ceux indiqués à l'étape 3.
   - Le câble utilisé est conforme aux instructions de l'étape 2.
5. Appuyez sur le bouton **Réinitialiser**. Le voyant d'état émet alternativement une lumière orange et verte. Appuyez immédiatement une seconde fois sur le bouton **Réinitialiser** pendant que le voyant clignote pour réinitialiser de manière temporaire le nom d'utilisateur et le mot de passe à leurs valeurs par défaut.
6. Appuyez sur ENTRÉE autant de fois que nécessaire pour afficher à nouveau l'invite **Nom d'utilisateur**, puis utilisez la valeur par défaut **apc** pour le nom d'utilisateur et le mot de passe (si vous n'êtes toujours pas connecté dans les 30 secondes après que la fenêtre **Nom d'utilisateur** s'affiche de nouveau, répétez l'étape 5 et recommencez la connexion).
7. Dans l'interface par lignes de commande, tapez les commandes suivantes pour modifier les paramètres **Nom d'utilisateur** et **Mot de passe,** qui sont redevenus **apc** :

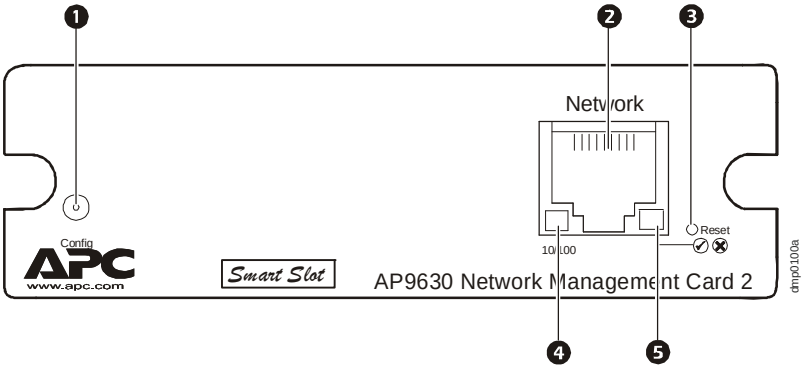
   ```
   user -an votreNomd'administrateur

   user -ap votreMotdepasseAdministrateur
   ```

   Par exemple pour choisir **Admin** comme valeur pour le paramètre de nom d'administrateur, tapez :

   ```
   user -an Admin
   ```

8. Tapez `quit` ou `exit` pour vous déconnecter, rebranchez les câbles série débranchés, puis redémarrez tous les services précédemment désactivés.

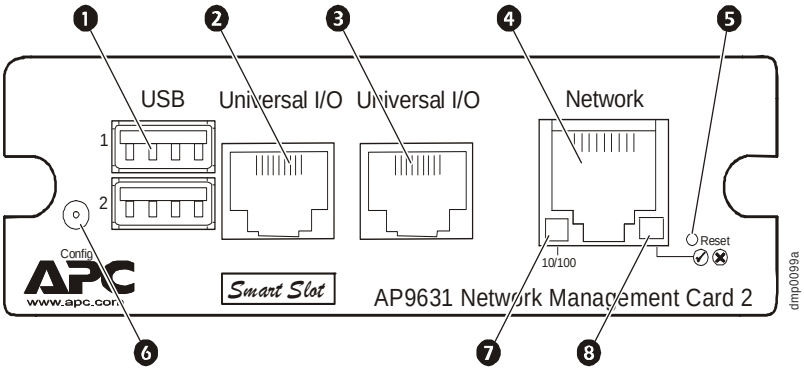
Panneau avant (AP9630)



Fonctionnalités

	Élément	Description
❶	Port série de configuration	Connecte la carte de gestion réseau à un ordinateur local afin de configurer les paramètres réseau initiaux ou d'accéder à l'interface par lignes de commande.
❷	Connecteur 10/100 Base-T	Connecte la carte de gestion réseau au réseau Ethernet.
❸	Bouton Reset (RAZ)	Réinitialise la carte de gestion réseau, qui reste sous tension.
❹	Voyant de liaison RX/TX (10/100)	Voir « Voyant de liaison RX/TX (10/100) » en page 7.
❺	Voyant d'état	Voir « Voyant d'état » en page 6.

Panneau avant (AP9631)



Fonctionnalités

	Élément	Description
❶	Ports USB	Destinés à un emploi ultérieur.
❷ ❸	Ports de capteurs	Permettent de connecter des capteurs de température, des capteurs de température/d'humidité ou des connecteurs d'entrée/sortie de relais acceptant deux contacts d'entrée et un relais de sortie.
❹	Connecteur 10/100 Base-T	Connecte la carte de gestion réseau au réseau Ethernet.

	Élément	Description
❺	Bouton Reset (RAZ)	Réinitialise la carte de gestion réseau, qui reste sous tension.
❻	Port série de configuration	Connecte la carte de gestion réseau à un ordinateur local afin de configurer les paramètres réseau initiaux ou d'accéder à l'interface par lignes de commande.
❼	Voyant de liaison RX/TX (10/100)	Voir « Voyant de liaison RX/TX (10/100) » en page 7.
❽	Voyant d'état	Voir « Voyant d'état » en page 6.

Description des voyants

Voyant d'état

Ce voyant indique l'état de la carte de gestion réseau.

État	Description
Éteint	Vous êtes dans l'un des cas suivants : • La carte de gestion réseau n'est pas alimentée. • La carte de gestion réseau ne fonctionne pas correctement. Elle doit peut-être être réparée ou remplacée. Veuillez contacter l'Assistance clients. Voir « Assistance clients internationale » en page 117.
Vert fixe	Les paramètres TCP/IP de la carte de gestion réseau sont valides.
Orange fixe	Détection d'une panne matérielle de la carte de gestion réseau. Veuillez contacter l'Assistance clients. Voir « Assistance clients internationale » en page 117.
Vert clignotant	Les paramètres TCP/IP de la carte de gestion réseau ne sont pas valides.[1]
Orange clignotant	La carte de gestion réseau émet des requêtes BOOTP.[1]
Vert et orange clignotant alternativement	Si le voyant clignote lentement, la carte de gestion réseau émet des requêtes DHCP[2].[1] S'il clignote rapidement, la carte de gestion réseau est en cours de démarrage.

1. Si vous n'utilisez pas de serveur BOOTP ou DHCP, consultez le *Manuel d'installation* de la carte de gestion réseau fourni en format imprimé et sur le CD-Rom d'*utilitaires* au format PDF pour configurer les paramètres TCP/IP de la carte de gestion réseau.
2. Pour utiliser un serveur DHCP ou BOOTP, consultez « Paramètres TCP/IP et de communication » en page 70.

Voyant de liaison RX/TX (10/100)

Ce voyant indique l'état du réseau de la carte de gestion réseau.

État	Description
Éteint	Vous êtes dans l'un des cas suivants ou plusieurs : • La carte de gestion réseau n'est pas alimentée. • Le câble reliant la carte de gestion au réseau est déconnecté ou défectueux. • Le périphérique connectant la carte de gestion au réseau est hors tension ou ne fonctionne pas correctement. • La carte de gestion réseau elle-même ne fonctionne pas correctement. Elle doit peut-être être réparée ou remplacée. Veuillez contacter l'Assistance clients. Voir « Assistance clients internationale » en page 117.
Vert fixe	La carte de gestion réseau est connectée à un réseau fonctionnant à 10 mégabits par seconde (Mbps).
Orange fixe	La carte de gestion réseau est connectée à un réseau fonctionnant à 100 Mbps.
Vert clignotant	La carte de gestion réseau reçoit ou transmet des paquets de données à 10 Mbps.
Orange clignotant	La carte de gestion réseau reçoit ou transmet des paquets de données à 100 Mbps.

Fonctions de surveillance

Présentation

Pour détecter les problèmes internes et effectuer une restauration en cas d'entrées imprévues, la carte de gestion réseau utilise des mécanismes internes de surveillance du système complet. Lorsque la carte redémarre pour éliminer un problème interne, un événement **Système : Démarrage à chaud** est enregistré dans le journal de consignation des événements.

Mécanisme de surveillance de l'interface réseau

La carte de gestion réseau implémente des mécanismes internes de surveillance afin de protéger sa disponibilité sur le réseau. Par exemple si la carte de gestion réseau ne reçoit aucun trafic réseau pendant 9,5 minutes (que ce soit du trafic direct, comme SNMP, ou du trafic de diffusion, comme une requête de protocole ARP [Address Resolution Protocol]), elle suppose qu'il existe un problème sur son interface réseau et redémarre.

Réinitialisation de la minuterie du réseau

Pour assurer que la carte de gestion réseau ne redémarre pas si le réseau est inactif pendant 9,5 minutes, cette carte tente de contacter la passerelle par défaut toutes les 4,5 minutes. Si la passerelle est présente, elle répond à la carte de gestion réseau, ce qui relance la minuterie pour 9,5 minutes. Si votre application n'a pas besoin de passerelle ou n'en possède pas, spécifiez l'adresse IP d'un ordinateur fonctionnant sur le réseau et présent sur le même sous-réseau. Le trafic réseau de cet ordinateur relance la minuterie de 9,5 minutes suffisamment souvent pour éviter le redémarrage de la carte de gestion réseau.

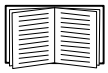
Interface en ligne de commande

Connexion

Présentation

Vous pouvez accéder à l'interface en ligne de commande depuis un ordinateur relié au même réseau que la carte de gestion réseau, par le biais d'une connexion locale (série) ou d'une connexion à distance (Telnet ou SSH).

Pour vous connecter, saisissez votre nom d'utilisateur et votre mot de passe (par défaut : **apc** et **apc** pour un administrateur, ou **device** et **apc** pour un utilisateur de périphérique). Attention, ils sont sensibles à la casse. Un utilisateur en lecture seule ne peut pas accéder à l'interface en ligne de commande.



Si vous avez oublié votre nom d'utilisateur ou votre mot de passe, reportez-vous à la section « Procédure de récupération suite à la perte du mot de passe » à la page 4.

Accès à distance à l'interface en ligne de commande

Vous pouvez accéder à l'interface en ligne de commande via Telnet ou SSH. Telnet est activé par défaut. L'activation de SSH entraîne la désactivation de Telnet.

Utilisez l'interface Web pour activer ou désactiver ces méthodes d'accès. Dans l'onglet **Administration**, sélectionnez **Réseau** dans la barre de menus supérieure, puis l'option d'**accès** sous **Console** dans le menu de navigation de gauche.

Telnet pour un accès de base. Telnet offre une sécurité de base grâce à une authentification par nom d'utilisateur et mot de passe, mais ne présente pas les avantages d'une sécurité renforcée par cryptage.

Pour accéder à l'interface en ligne de commande via Telnet :

1. Depuis un ordinateur ayant accès au réseau sur lequel la carte de gestion réseau est installée, tapez `telnet` à l'invite de commande, suivi de l'adresse IP de la carte de gestion réseau (par exemple `telnet 139.225.6.133` si la carte de gestion réseau utilise le port Telnet par défaut 23), et appuyez sur ENTREE.

   Si la carte de gestion réseau utilise un numéro de port (de 5000 à 32768) autre que celui par défaut, vous devez ajouter deux-points ou un espace (selon votre client Telnet) entre l'adresse IP (ou du nom de domaine) et le numéro de port. (Ces commandes sont celles généralement utilisées ; certains clients ne vous autorisent pas à spécifier le numéro de port en argument et certains systèmes Linux peuvent nécessiter des commandes supplémentaires).

2. Saisissez vos nom d'utilisateur et mot de passe (par défaut, **apc** et **apc** pour un administrateur ou **device** et **apc** pour un utilisateur de périphérique).

SSH pour un accès sécurisé. Si vous utilisez le protocole SSL haute sécurité pour l'interface Web, utilisez SSH pour accéder à l'interface en ligne de commande. SSH crypte les noms d'utilisateurs, les mots de passe et les données transmises. Que vous utilisiez l'interface en ligne de commande via SSH ou Telnet, l'interface, les comptes utilisateurs et les droits d'accès des utilisateurs restent les mêmes. Pour utiliser SSH, vous devez cependant d'abord configurer ce dernier et installer une application client SSH sur votre ordinateur.

Accès local à l’interface en ligne de commande

Vous pouvez accéder localement à l’interface en ligne de commande par l’intermédiaire d’un ordinateur relié à la carte de gestion réseau via un port série :

1. Sélectionnez un port série de l’ordinateur et désactivez tout service utilisant ce port.
2. Connectez le câble série fourni (référence 940-0299) au port choisi de l’ordinateur et au port de configuration de la carte de gestion réseau.
3. Exécutez un programme d’émulation de terminal (tel que HyperTerminal) et configurez le port sélectionné sur 9600 bit/s, 8 bit de données, pas de parité, 1 bit d’arrêt et pas de contrôle de flux.
4. Appuyez sur ENTREE. A l’invite, saisissez votre nom d’utilisateur et votre mot de passe.

Ecran principal

Exemple d’écran principal

Voici un exemple de l’écran qui s’affiche à la connexion à l’interface en ligne de commande sur la carte de gestion réseau.

```
 American Power Conversion            Network Management Card AOS  vx.x.x
(c)Copyright 2010 All Rights Reserved Symmetra APP                 vx.x.x
-------------------------------------------------------------------------------
Name     : Test Lab                                  Date : 10/30/2010
Contact  : Don Adams                                 Time : 5:58:30
Location : Building 3                                User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N+ A+

APC>
```

Champs d’informations et d’état

Champs d’informations de l’écran principal

- Deux champs indiquent les versions du système d’exploitation d’American Power Conversion (AOS) et du microprogramme de l’application (APP). Le nom du microprogramme de l’application identifie le périphérique qui se connecte au réseau par l’intermédiaire de la carte de gestion réseau. Dans l’exemple ci-dessus, la carte de gestion réseau utilise le microprogramme de l’application d’un onduleur Symmetra.

  ```
  Network Management Card AOS    vx.x.x
  Symmetra APP                   vx.x.x
  ```

- Trois champs indiquent le nom du système, la personne à contacter et l’emplacement de la carte de gestion réseau. (Pour définir ces paramètres dans l’interface Web, sélectionnez l’onglet **Administration**, **Général** dans la barre de menus supérieure, puis **Identification** dans le menu de navigation de gauche.)

  ```
  Name   : Test Lab
  Contact: Don Adams
  Location: Building 3
  ```

- Le champ **Up Time** indique la durée de fonctionnement de la carte de gestion réseau depuis son démarrage ou sa dernière réinitialisation.

  ```
  Up Time: 0 Days 21 Hours 21 Minutes
  ```

- Deux champs indiquent la date et l'heure de votre connexion.

  ```
  Date : 10/30/2009
  Time : 5:58:30
  ```

- Le champ **User** indique si vous vous êtes connecté en tant qu'**administrateur** (« Administrator ») ou **Gestionnaire de périphérique** (« Device Manager »). (Un **utilisateur en lecture seule** ne peut pas accéder à l'interface en ligne de commande.) Lorsque vous vous connectez en tant que gestionnaire de périphérique (équivalent de l'utilisateur de périphérique dans l'interface Web), vous pouvez accéder au journal des événements, configurer certains paramètres d'onduleur et afficher le nombre d'alarmes actives.

  ```
  User : Administrator
  ```

Champs d'état de l'écran principal

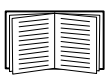
- Le champ **Stat** indique l'état de la carte de gestion réseau. L'état du milieu dépend de l'option choisie, IPv4, IPv6 ou les deux, comme indiqué dans le deuxième tableau ci-dessous.

  ```
  Stat : P+ N+ A+
  ```

P+	Le système d'exploitation (AOS) fonctionne correctement.

IPv4 uniquement	IPv6 uniquement	IPv4 et IPv6*	Description
N+	N6+	N4+ N6+	Le réseau fonctionne correctement.
N?	N6?	N4? N6?	Un cycle de requêtes BOOTP est en cours.
N–	N6–	N4- N6-	La carte de gestion réseau n'a pas réussi à se connecter au réseau.
N!	N6!	N4! N6!	Un autre périphérique utilise l'adresse IP de la carte de gestion réseau.
* Les valeurs N4 et N6 peuvent être différentes : par exemple, il est possible d'avoir N4– N6+.			

A+	L'application fonctionne correctement.
A–	La somme de contrôle de l'application est incorrecte.
A?	L'application est en cours d'initialisation.
A!	L'application n'est pas compatible avec l'AOS.



Si P+ ne s'affiche pas, contactez l'assistance clients. Reportez-vous à la section « Assistance clients internationale » à la page 117.

Remarque : pour afficher l'état de l'onduleur, tapez `ups -st`.

Utilisation de l’interface en ligne de commande

Présentation

L’interface en ligne de commande comporte des options qui permettent de configurer les paramètres réseau et de gérer l’onduleur ainsi que sa carte de gestion réseau.

Saisie des commandes

L’interface en ligne de commande permet de configurer la carte de gestion réseau à l’aide de commandes. Pour ce faire, tapez la commande et appuyez sur ENTREE. Les commandes et leurs arguments peuvent être saisis indifféremment en minuscules, en majuscules ou les deux. Les options sont en revanches sensibles à la casse.

Lorsque vous utilisez l’interface en ligne de commande, vous avez différentes possibilités :

- Tapez `?` et appuyez sur ENTREE pour afficher la liste des commandes disponibles en fonction de votre type de compte.

  Pour obtenir des informations sur le but et la syntaxe d’une commande donnée, tapez cette commande suivie d’un espace, puis du symbole `?` ou du mot `help`. Par exemple, pour afficher les options de configuration RADIUS, tapez :
  `radius ?`
  ou
  `radius help`
- Appuyez sur la flèche HAUT pour afficher la dernière commande saisie au cours de la session. Les flèches HAUT et BAS permettent d’afficher jusqu’aux dix dernières commandes.
- Tapez au moins un caractère d’une commande et appuyez sur la touche de TABULATION pour parcourir la liste des commandes valides qui correspondent au texte saisi dans la ligne de commande.
- Tapez `ups -st` pour afficher l’état de l’onduleur.
- Tapez `exit` ou `quit` pour vous déconnecter de l’interface en ligne de commande.

Syntaxe des commandes

Elément	Description
-	Les options doivent être précédées d’un tiret.
< >	La définition d’une option doit être entre chevrons. Par exemple : `-dp <mot de passe du périphérique>`
[ ]	Si une commande accepte plusieurs options ou qu’une option accepte des arguments mutuellement exclusifs, les valeurs peuvent être saisies entre crochets.
|	Une barre verticale entre des éléments entourés de crochets ou de chevrons indique que ces éléments s’excluent mutuellement. Vous devez utiliser l’un de ces éléments.

Exemples de syntaxe

Commande acceptant plusieurs options :

```
user [-an <nom admin>] [-ap <mot de passe admin>]
```

Dans cet exemple, la commande `user` accepte l'option `-an`, qui définit le nom d'utilisateur avec droits d'administrateur, et l'option `-ap`, qui définit le mot de passe administrateur. Pour modifier le nom d'administrateur et son mot de passe en XYZ :

1. Tapez la commande `user`, une option, puis l'argument XYZ :
   `user -ap XYZ`
2. Lorsque la première commande a été exécutée, tapez la commande `user`, la deuxième option, puis l'argument XYZ :
   `user -an XYZ`

Commande qui accepte comme option des arguments mutuellement exclusifs :

```
alarmcount -p [all | warning | critical]
```

Dans cet exemple, l'option `-p` accepte seulement trois arguments : `all`, `warning` ou `critical`. Par exemple, pour afficher le nombre d'alarmes critiques actives, tapez :
`alarmcount -p critical`

Cette commande échoue si vous tapez un argument autre que ceux spécifiés.

Codes de réponse aux commandes

Les codes de réponse aux commandes permettent de détecter des erreurs avec fiabilité par opérations de script, sans qu'il soit nécessaire que le texte du message d'erreur corresponde.

L'interface en ligne de commande renvoie toutes les opérations de commande au format suivant :

`E [0-9][0-9][0-9]: *Message d'erreur*`

Code	Message d'erreur
E000	Succès
E001	Commande émise avec succès
E002	Redémarrage nécessaire pour que les modifications soient appliquées
E100	Echec de la commande
E101	Commande inconnue
E102	Erreur de paramètre
E103	Erreur dans la ligne de commande
E104	Refusé pour ce niveau d'utilisateur
E105	Préremplissage de commande
E106	Données non disponibles
E107	Communication série perdue avec l'onduleur

Description des commandes

Remarque : les commandes et options disponibles varient d'un onduleur à l'autre.

?

Accès : Administrateur, utilisateur de périphérique

Description : Affiche la liste des commandes disponibles pour votre type de compte dans l'interface en ligne de commande. Pour afficher l'aide concernant une commande spécifique, saisissez cette commande suivie d'un point d'interrogation.

Exemple : Pour afficher la liste des options acceptées par la commande `alarmcount`, tapez :
`alarmcount ?`

about

Accès : Administrateur, utilisateur de périphérique

Description : Affiche les informations relatives au matériel et au microprogramme. Ces informations sont utiles pour le dépannage et permettent de savoir si une mise à jour du microprogramme est disponible sur le site Web.

alarmcount

Accès : Administrateur, utilisateur de périphérique

Description :

Option	Arguments	Description
-p	all	Affiche le nombre d'alarmes actives détectées par la carte de gestion réseau. Les informations concernant ces alarmes figurent dans le journal des événements.
	warning	Affiche le nombre d'alarmes d'avertissement actives.
	critical	Affiche le nombre d'alarmes critiques actives.

Exemple : Pour afficher toutes les alarmes d'avertissement actives, tapez :
`alarmcount -p warning`

boot

Accès : Administrateur uniquement

Description : Définit les paramètres réseau de la carte de gestion réseau, notamment l'adresse IP, le masque de sous-réseau et la passerelle par défaut. Vous pouvez ensuite configurer les paramètres de serveur BOOTP ou DHCP.

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Définit comment les paramètres TCP/IP sont configurés au démarrage, à la réinitialisation ou au redémarrage de la carte de gestion réseau. Reportez-vous à la section « Paramètres TCP/IP et de communication » à la page 70 pour en savoir plus sur les paramètres des différents modes de démarrage.
-c	enable | disable	Uniquement en modes `dhcp`. Active ou désactive l'obligation du serveur DHCP de transmettre le cookie APC.

Option	Argument	Description
Il n'est en général pas nécessaire de modifier la valeur par défaut des trois paramètres suivants : -v <catégorie de fournisseur> : APC -i <ID client> : adresse MAC de la carte de gestion réseau, qui l'identifie de manière unique sur le réseau -u <catégorie d'utilisateur> : nom du module du microprogramme de l'application.		

Exemple : Pour obtenir les paramètres réseau par le biais d'un serveur DHCP :

1. Saisissez `boot -b dhcp`.
2. Activez l'obligation du serveur DHCP de transmettre le cookie APC :
   `boot -c enable`

cd

Accès : Administrateur, utilisateur de périphérique

Description : Ouvre un dossier de l'arborescence de la carte de gestion réseau.

Exemple 1 : Pour passer au dossier `ssh` afin de vérifier si un certificat de sécurité SSH a été téléchargé sur la carte de gestion réseau :

1. Tapez `cd ssh` et appuyez sur ENTREE.
2. Tapez `dir` et appuyez sur ENTREE pour afficher la liste des fichiers contenus dans le dossier SSH.

Exemple 2 : Pour revenir au dossier principal du répertoire, tapez :
`cd ..`

cfgshutdn

Accès : Administrateur, utilisateur de périphérique

Description : Configuration des paramètres de mise hors tension : cette commande vous permet d'afficher et de configurer le délai avant arrêt, le délai avant retour, l'autonomie avec batterie faible, l'heure de veille et l'autonomie de rétablissement minimale de l'onduleur.

Remarque : ces options ne sont pas disponibles sur tous les onduleurs.

Option	Argument	Description
-all		Affiche tous les paramètres de mise hors tension applicables de l'onduleur.
-sd	000 | 090 | 180 | 270 | 360 | 450 | 540 | 630	Définit le délai avant arrêt en secondes.
-lo	02 | 05 | 08 | 11 | 14 | 17 | 20 | 23	Définit l'autonomie avec batterie faible en minutes.
-rd	000 | 060 | 120 | 180 | 240 | 300 | 360 | 420	Définit le délai avant retour de l'onduleur en secondes, c'est-à-dire le délai avant remise sous tension de l'onduleur.
-rrt	0–3600	Définit l'autonomie de rétablissement minimale en secondes, c'est-à-dire que l'autonomie de la batterie nécessaire pour supporter la charge doit atteindre cette valeur pour que l'onduleur se remette sous tension.

Option	Argument	Description
-sl	0,0–359,9	Définit l'heure de veille, en heures. L'argument peut être tout nombre compris entre 0,0 et 359,9.
-rsc	00 | 15 | 30 | 45 | 60 | 75 | 90	Définit le pourcentage de charge minimal de la batterie, par rapport à sa capacité totale.

cfgpower

Accès : Administrateur, utilisateur de périphérique

Description : Configuration des paramètres d'alimentation : vous permet d'afficher et de configurer les points de transfert, la sensibilité et la tension de sortie.

Remarque : ces options ne sont pas disponibles sur tous les onduleurs.

Option	Argument Ces valeurs varient en fonction du périphérique.	Description
-all		Affiche tous les paramètres d'alimentation applicables de l'onduleur.
-l	97–106	Définit le point de transfert bas en V CA.
-h	127–136	Définit le point de transfert haut en V CA.
-ov	100 | 120 | 110 |	Définit la tension de sortie en V CA.
-s	Normal | Reduced | Low	Définit la sensibilité, à l'aide de l'un des trois arguments.
-bu	127 | 130 | 133 | 136 | 139 | 142 | 145 | 148	Définit le seuil maximal de tension de dérivation en V CA. Si la tension dépasse cette valeur, l'onduleur passe en mode de dérivation.
-bl	086 | 088 | 090 | 092 | 094 | 096 | 098 | 100	Définit le seuil minimal de tension de dérivation en V CA. Si la tension tombe sous cette valeur, l'onduleur passe en mode de dérivation.

console

Accès : Administrateur uniquement

Description : Définit le mode d'accès de l'utilisateur à l'interface en ligne de commande, via Telnet (par défaut) ou via Secure SHell (SSH), qui offre une protection supérieure en transmettant les noms d'utilisateur, les mots de passe et les données sous forme cryptée. Vous pouvez changer le paramètre de port Telnet ou SSH pour renforcer la sécurité. Vous pouvez également désactiver l'accès réseau à l'interface en ligne de commande.

Option	Argument	Description
-S	disable | telnet | ssh	Configure l'accès à l'interface en ligne de commande ou en bloque l'accès avec la commande `disable`. L'activation de SSH entraîne l'activation de SCP et la désactivation de Telnet.

Option	Argument	Description
-pt	<numéro du port Telnet>	Définit le port Telnet utilisé pour communiquer avec la carte de gestion réseau (port 23 par défaut).
-ps	<numéro du port SSH>	Définit le port SSH utilisé pour communiquer avec la carte de gestion réseau (port 22 par défaut).
-b	2400 | 9600 | 19200 | 38400	Configure la vitesse de transmission de la connexion par port série (9600 bit/s par défaut).

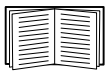
Exemple 1 : Pour activer l'accès SSH à l'interface en ligne de commande, tapez :
```
console -S ssh
```

Exemple 2 : Pour changer de port Telnet et utiliser le port 5000, tapez :
```
console -pt 5000
```

date

Accès : Administrateur uniquement

Définition : Configure la date utilisée par la carte de gestion réseau.



Pour une configuration dans laquelle la date et l'heure de la carte de gestion réseau sont définies par un serveur NTP, reportez-vous à la section « Réglage de la date et de l'heure » à la page 93.

Option	Argument	Description
-d	<"chaîne de date">	Définit la date actuelle. Utilisez le format de date spécifié par la commande `date -f`.
-t	<00:00:00>	Définit l'heure actuelle en heures, minutes et secondes. Utilisez le format 24 heures.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Sélectionne le format numérique auquel toutes les dates s'afficheront dans l'interface utilisateur. Chaque lettre (m pour mois, d pour jour et y pour année) représente un chiffre. Les jours et les mois à un seul chiffre sont précédés d'un zéro.
-z	<décalage horaire>	Définit la différence par rapport au temps moyen de Greenwich afin de spécifier votre fuseau horaire. Cette option vous permet de vous synchroniser avec d'autres utilisateurs situés dans des fuseaux horaires différents.

Exemple 1 : Pour afficher la date au format aaaa-mm-jj, tapez :
```
date -f yyyy-mm-dd
```

Exemple 2 : Pour définir la date au 30 octobre 2009, selon le format configuré dans l'exemple ci-dessus, tapez :
```
date -d "2009-10-30"
```

Exemple 3 : Pour fixer l'heure à 17 h, 21 min et 3 s, tapez :
```
date -t 17:21:03
```

delete

Accès : Administrateur uniquement

Description : Supprime un fichier dans le système de fichiers. (Pour supprimer le journal des événements, reportez-vous à la section « eventlog » commençant à la page 18.)

Argument	Description
<nom du fichier>	Saisissez le nom du fichier à supprimer.

Exemple : Pour supprimer un fichier :

1. Ouvrez le dossier qui contient le fichier à supprimer. Par exemple, pour ouvrir le dossier `logs` (journaux), tapez :
   `cd logs`
2. Pour afficher les fichiers contenus dans le dossier `logs`, tapez :
   `dir`
3. Tapez
   `delete <nom du fichier>`.

detstatus

Accès : Administrateur, utilisateur de périphérique

Description : Affiche l'état détaillé de l'onduleur. Reportez-vous également à l'option -st à la section « ups » à la page 24.

Option	Arguments	Description
-all		Affiche toutes les informations d'état applicables de l'onduleur.
-rt		Autonomie restante en heures et minutes.
-ss		Résumé de l'état de l'onduleur : en ligne, sur batterie, etc.
-soc		Pourcentage de charge de la batterie par rapport à sa capacité totale.
-om		Valeurs de sortie : tension, fréquence, pourcentage en W, pourcentage VA, intensité.
-im		Valeurs d'entrée : tension et fréquence.
-bat		Tension de la batterie
-tmp		Température interne de l'onduleur
-dg		Résultats du test de diagnostic : date et résultat du test automatique, date et résultat du test de calibrage.

dir

Accès : Administrateur, utilisateur de périphérique

Description : Affiche les fichiers et les dossiers enregistrés sur la carte de gestion réseau.

dns

Accès : Administrateur

Description : Configure les paramètres DNS manuels.

Paramètre	Argument	Description
-OM	enable | disable	Ignore les paramètres DNS manuels.
-p	<serveur DNS primaire>	Définit le serveur DNS primaire.
-s	<serveur DNS secondaire>	Définit le serveur DNS secondaire.
-d	<nom de domaine>	Définit le nom de domaine.
-n	<nom de domaine IPv6>	Définit le nom de domaine IPv6.
-h	<nom d'hôte>	Définit le nom d'hôte.

eventlog

Accès : Administrateur, utilisateur de périphérique

Description : Affiche la date et l'heure auxquelles vous avez récupéré le journal des événements, l'état de l'onduleur et l'état des capteurs reliés à la carte de gestion réseau. Affiche les événements les plus récents concernant les périphériques, avec la date et l'heure auxquelles ils sont survenus. Utilisez les touches du clavier suivantes pour naviguer dans le journal des événements :

Touche	Description
ECHAP	Ferme le journal des événements et revient à l'interface en ligne de commande.
ENTREE	Actualise l'affichage du journal. Cette commande permet d'afficher les événements qui ont été enregistrés depuis que vous avez récupéré et affiché le journal.
ESPACE	Affiche la page suivante du journal des événements.
B	Affiche la page précédente du journal des événements. Cette commande n'est pas disponible à partir de la page principale du journal.
D	Supprime le journal des événements. Suivez l'invite pour confirmer ou annuler la suppression. La suppression des événements est définitive.

exit

Accès : Administrateur, utilisateur de périphérique

Description : Ferme la session d'interface en ligne de commande.

format

Accès : Administrateur uniquement

Description : Reformate le système de fichiers de la carte de gestion réseau et efface l'ensemble des certificats de sécurité, des clés de cryptage, des paramètres de configuration et des journaux des événements et de données. Réfléchissez bien avant de lancer cette commande.

Remarque : pour restaurer la configuration par défaut de la carte de gestion réseau, utilisez la commande `resetToDef`.

ftp

Accès : Administrateur uniquement

Description : Active ou désactive l'accès au serveur FTP. En option, remplace le paramètre de port par tout numéro de port inutilisé compris entre 5001 et 32768, afin de renforcer la sécurité.

Option	Argument	Définition
-p	<numéro du port>	Définit le port TCP/IP utilisé par le serveur FTP pour communiquer avec la carte de gestion réseau (port 21 par défaut). Le serveur FTP utilise à la fois le port spécifié et celui dont le numéro est immédiatement inférieur.
-S	enable | disable	Active ou désactive l'accès au serveur FTP.

Exemple : Pour changer de port TCP/IP et utiliser le port 5001, tapez :
`ftp -p 5001`

help

Accès : Administrateur, utilisateur de périphérique

Description : Affiche la liste de toutes les commandes disponibles pour votre type de compte dans l'interface en ligne de commande. Pour afficher l'aide concernant une commande spécifique, saisissez cette commande suivie de `help`.

Exemple 1 : Pour afficher la liste des commandes disponibles pour un utilisateur de périphérique, tapez :
`help`

Exemple 2 : Pour afficher la liste des options acceptées par la commande `alarmcount`, tapez :
`alarmcount help`

netstat

Accès : Administrateur, utilisateur de périphérique

Description : Affiche l'état du réseau et toutes les adresses IPv4 et IPv6 actives.

ntp

Accès : Administrateur, utilisateur de périphérique

Description : Affiche et configure les paramètres de protocole NTP.

Option	Argument	Définition
-OM	enable | disable	Ignore les paramètres manuels.
-p	<serveur NTP primaire>	Spécifie le serveur primaire.
-s	<serveur NTP secondaire>	Spécifie le serveur secondaire.

Exemple 1 : Pour activer l'instruction d'ignorer les paramètres manuels, tapez :
`ntp -OM enable`

Exemple 2 : Pour spécifier le serveur NTP primaire, tapez :
`ntp -p 150.250.6.10`

ping

Accès : Administrateur, utilisateur de périphérique

Description : Détermine si le périphérique dont vous spécifiez l'adresse IP ou le nom de domaine est connecté au réseau. Quatre demandes sont envoyées à cette adresse.

Argument	Description
<adresse IP ou nom de domaine>	Saisissez une adresse IP au format *xxx.xxx.xxx.xxx* ou le nom de domaine configuré par le serveur DNS.

Exemple : Pour déterminer si le périphérique ayant l'adresse IP 150.250.6.10 est connecté au réseau, tapez :
`ping 150.250.6.10`

portspeed

Accès : Administrateur

Description :

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100F	Définit la vitesse de communication du port Ethernet. La commande `auto` permet aux périphériques Ethernet de négocier pour transmettre à la vitesse la plus rapide possible. Reportez-vous à la section « Vitesse du port : » à la page 74 pour en savoir plus sur les paramètres de vitesse du port.

Exemple : Pour configurer le port TCP/IP à une vitesse de communication de 100 Mbit/s en semi-duplex (communication dans un seul sens à la fois), tapez :
`portspeed -s 100H`

prompt

Accès : Administrateur, utilisateur de périphérique

Description : Configure l'invite de l'interface en ligne de commande pour y inclure ou non le type de compte de l'utilisateur connecté. Tous les utilisateurs peuvent modifier ce paramètre. S'il est modifié, tous les comptes utilisateurs utilisent alors la nouvelle configuration.

Option	Argument	Description
-s	long	L'invite inclut le type de compte de l'utilisateur connecté.
	short	Paramètre par défaut. L'invite est constituée des quatre caractères suivants : `APC>`

Exemple : Pour inclure le type de compte de l'utilisateur en cours de session, tapez :
`prompt -s long`

quit

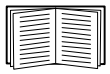
Accès : Administrateur, utilisateur de périphérique

Description : Ferme la session de l'interface en ligne de commande (tout comme la commande « exit »).

radius

Accès : Administrateur uniquement

Description : Affiche les paramètres RADIUS existants, active ou désactive l'authentification RADIUS, et configure les paramètres d'authentification de base pour un ou deux serveurs RADIUS.



Pour en savoir plus sur le résumé de la configuration du serveur RADIUS et la liste des serveurs RADIUS pris en charge, reportez-vous à la section « Configuration du serveur RADIUS » à la page 68.

D'autres paramètres d'authentification pour les serveurs RADIUS sont disponibles dans l'interface Web de la carte de gestion réseau. Reportez-vous à la section « RADIUS » à la page 67 pour en savoir plus.

Pour des informations détaillées sur la configuration de votre serveur RADIUS, reportez-vous au *Manuel de sécurité* disponible sur le CD des *utilitaires* de la carte de gestion réseau et sur le site Web, **www.apc.com**.

Option	Argument	Description
-a	local | radiusLocal | radius	Configure l'authentification RADIUS : `local` : RADIUS est désactivé. L'authentification locale est activée. `radiusLocal` : RADIUS, puis authentification locale. Les authentifications RADIUS et locale sont activées. La première authentification demandée est celle du serveur RADIUS. Si le serveur RADIUS ne répond pas, l'authentification locale est utilisée. `radius` : RADIUS est activé. L'authentification locale est désactivée.
-p1 -p2	<IP du serveur>	Nom ou adresse IP du serveur RADIUS primaire ou secondaire. **REMARQUE :** les serveurs RADIUS utilisent le port 1812 par défaut pour authentifier les utilisateurs. Pour utiliser un autre port, ajoutez deux-points puis le nouveau numéro de port à la suite du nom ou de l'adresse IP du serveur RADIUS.
-s1 -s2	<secret du serveur>	Secret partagé entre le serveur RADIUS primaire ou secondaire et la carte de gestion réseau.
-t1 -t2	<délai d'expiration du serveur>	Durée en secondes pendant laquelle la carte de gestion réseau attend une réponse du serveur RADIUS primaire ou secondaire.

Exemple 1 :

Pour afficher les paramètres RADIUS existants de la carte de gestion réseau, tapez `radius` et appuyez sur ENTREE.

Exemple 2 : Pour activer les authentifications RADIUS et locale, tapez :

```
radius -a radiusLocal
```

Exemple 3 : Pour configurer un délai d'expiration de 10 secondes pour un serveur RADIUS secondaire, tapez :

```
radius -t2 10
```

reboot

Accès : Administrateur

Description : Redémarre l'interface de la carte de gestion réseau.

resetToDef

Accès : Administrateur uniquement

Description : Rétablit tous les paramètres par défaut.

Option	Arguments	Description
-p	all | keepip	Rétablit la configuration par défaut, y compris les actions sur les événements, les paramètres de périphérique et éventuellement les paramètres de configuration TCP/IP.

Exemple : Pour rétablir la configuration par défaut, *sauf* les paramètres TCP/IP de la carte de gestion réseau, tapez :

```
resetToDef -p keepip
```

snmp, snmpv3

Accès : Administrateur uniquement

Description : Active ou désactive le protocole SNMP 1 ou SNMP 3.

Option	Arguments	Description
-S	enable | disable	Active ou affiche la version du protocole SNMP correspondant (1 ou 3).

Exemple : Pour activer SNMP version 1, tapez :

```
snmp -S enable
```

system

Accès : Administrateur uniquement

Description : Affiche et définit le nom du système, la personne à contacter, l'emplacement et la durée de fonctionnement, ainsi que la date et l'heure, le nom de l'utilisateur connecté et l'état du système à haut niveau (P, N et A) (reportez-vous à la section « Champs d'état de l'écran principal »).

Option	Argument	Description
-n	<nom du système>	Définit le nom du périphérique, son emplacement et le nom de la personne responsable de ce périphérique. **REMARQUE :** si vous saisissez une valeur comprenant plus d'un mot, vous devez la mettre entre guillemets. Ces valeurs sont également utilisées par InfraStruXure Central et par l'agent SNMP de la carte de gestion réseau.
-c	<contact système>	
-l	<emplacement système>	

Exemple°1 : Pour définir l'emplacement du périphérique comme `Test Lab`, tapez :

```
system -l "Test Lab"
```

Exemple°2 : Pour définir le nom du système comme `Don Adams`, tapez :

```
system -n "Don Adams"
```

tcpip

Accès : Administrateur uniquement

Description : Affiche et configure manuellement les paramètres réseau suivants de la carte de gestion réseau :

Option	Argument	Description
-S	enable | disable	Active ou désactive TCP/IP.
-i	<adresse IP>	Saisissez l'adresse IP de la carte de gestion réseau au format *xxx.xxx.xxx.xxx*
-s	<masque de sous-réseau>	Saisissez le masque de sous-réseau de la carte de gestion réseau.
-g	<passerelle>	Saisissez l'adresse IP de la passerelle par défaut. **N'utilisez pas** l'adresse de retour en boucle (127.0.0.1) comme passerelle par défaut.
-d	<nom de domaine>	Tapez le nom de domaine configuré par le serveur DNS.
-h	<nom d'hôte>	Tapez le nom d'hôte que la carte de gestion réseau utilisera.

Exemple 1 : Pour afficher les paramètres réseau de la carte de gestion réseau, tapez `tcpip` et appuyez sur ENTREE.

Exemple 2 : Pour configurer manuellement l'adresse IP `150.250.6.10` pour la carte de gestion réseau, tapez :

```
tcpip -i 150.250.6.10
```

tcpip6

Accès : Administrateur uniquement

Description : Active IPv6, affiche et configure manuellement les paramètres réseau suivants de la carte de gestion réseau :

Option	Argument	Description
-S	enable | disable	Active ou désactive IPv6.
-man	enable | disable	Active l'adressage manuel pour l'adresse IPv6 de la carte de gestion réseau.
-auto	enable | disable	Active la configuration automatique de l'adresse IPv6 pour la carte de gestion réseau.
-i	<adresse IPv6>	Définit l'adresse IPv6 de la carte de gestion réseau.
-g	<passerelle IPv6>	Définit l'adresse IPv6 de la passerelle par défaut.
-d6	router | statefull | stateless | never	Définit le mode DHCPv6 avec l'un des paramètres suivants : routeur (contrôlé par le routeur), statefull (état complet, état conservé pour l'adresse et autres informations), stateless (sans état, état non conservé pour les informations autres que l'adresse), never (jamais).

Exemple 1 : Pour afficher les paramètres réseau de la carte de gestion réseau, tapez `tcpip6` et appuyez sur ENTREE.

Exemple 2 : Pour configurer manuellement l'adresse IPv6 2001:0:0:0:0:FFD3:0:57ab pour la carte de gestion réseau, tapez :

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

uio

Accès : Administrateur, utilisateur de périphérique

Description : Cette commande est disponible pour une carte de gestion réseau 2 AP9631, à laquelle est relié un accessoire d'E/S à contact sec (AP9810).

Option	Argument	Description
-rc <n° du port d'E/S universelle>	open | close	Modifie l'état d'une sortie connectée et spécifie le numéro du port d'entrée/sortie universelle.
-st	<n° du port d'E/S universelle> | <n° du port d'E/S universelle>, <n° du port d'E/S universelle> | <n° du port d'E/S universelle>–<n° du port d'E/S universelle>	Affiche l'état des capteurs connectés à l'accessoire d'E/S à contact sec. Pour afficher l'état d'un ou de plusieurs capteurs spécifiques, saisissez leurs numéros de port d'E/S universelle.
-disc	<n° du port d'E/S universelle> | <n° du port d'E/S universelle>, <n° du port d'E/S universelle> | <n° du port d'E/S universelle>–<n° du port d'E/S universelle>	Identifie de nouvelles connexions de contact d'entrée ou de sortie de relais.

Exemple 1 : Pour ouvrir la sortie, tapez :

```
uio -rc 2 open
```

Exemple 2 : Pour afficher l'état des périphériques connectés à un accessoire d'E/S à contact sec installé sur le port 2 d'entrée/sortie universelle, tapez :

```
uio -st 2
```

ups

Remarque : Certaines options de la commande **ups** dépendent du modèle d'onduleur. Il est possible que certaines configurations ne prennent pas en charge toutes les options de la commande **ups**.

Accès : Administrateur, utilisateur de périphérique

Description : Contrôle l'onduleur et affiche les informations concernant son état.

Option	Arguments	Description
-c	off | graceoff | on | reboot | gracereboot | sleep | gracesleep	Configure les actions sur l'onduleur. Reportez-vous à la section « Page Contrôle » à la page 36 pour des informations détaillées.
-r	start | stop	Démarre ou stoppe le calibrage de l'autonomie. Le calibrage recalcule l'autonomie restante et doit respecter les points suivants : • Comme le calibrage épuise temporairement les batteries de l'onduleur, vous ne pouvez l'effectuer que si leur capacité est à 100 %. • Sur certains onduleurs, la charge doit être d'au moins 7 % pour pouvoir procéder au calibrage.
-s	start	Lance un test automatique de l'onduleur.

Option	Arguments	Description
-b	enter | exit	Contrôle l'utilisation du mode de dérivation. Cette commande dépend du modèle d'onduleur et peut ne pas s'appliquer à votre situation. Reportez-vous à la section « Page Contrôle » à la page 36 pour des informations détaillées.
-o#	Off | DelayOff | On | DelayOn | Reboot | DelayReboot| Shutdown | DelayShutdown | Cancel	Contrôle trois groupes de sorties sur un onduleur Smart-UPS XLM. Précisez le numéro du groupe de sorties. Pour des informations sur les groupes de sorties, reportez-vous à la section « Qu'est-ce qu'un groupe de sorties ? » à la page 40. Lorsque l'état du groupe de sorties est **on** (sous tension), trois arguments sont possibles pour cette option : • `Off` : met immédiatement le groupe hors tension. • `DelayOff` : met le groupe hors tension après le nombre de secondes indiqué sous **Délai de mise hors tension**. • `Reboot` : met immédiatement le groupe hors tension, puis le remet sous tension après le nombre de secondes indiqué sous **Durée de redémarrage** et **Délai de mise sous tension**. • `DelayReboot` : met le groupe de sorties hors tension après le nombre de secondes indiqué sous **Délai de mise hors tension**, puis le remet sous tension après le nombre de secondes indiqué sous **Durée de redémarrage** et **Délai de mise sous tension**. • `Shutdown` : redémarre le groupe de sorties si l'onduleur est en ligne. Si l'onduleur fonctionne sur batterie, cette commande met le groupe hors tension et attend le rétablissement de l'alimentation secteur pour le remettre sous tension. • `DelayShutdown` : met le groupe de sorties hors tension après le nombre de secondes indiqué sous **Délai de mise hors tension**. • `Cancel` : annule les commandes précédentes, par exemple la mise hors tension. Lorsque l'état du groupe de sorties est **off** (hors tension), deux arguments sont possibles pour cette option : • `On` : met immédiatement le groupe sous tension. • `DelayOn` : met le groupe sous tension après le nombre de secondes indiqué sous **Délai de mise sous tension**. Les paramètres **Délai de mise sous tension**, **Délai de mise hors tension** et **Durée de redémarrage** doivent être configurés dans l'interface Web. Reportez-vous à la section « Option Groupes de sorties (y compris le délestage automatique) » à la page 40 pour en savoir plus.
-os#		Affiche l'état (sous tension, hors tension, redémarrage en cours) de tous les groupes de sorties. Pour afficher l'état d'un groupe de sorties spécifique, indiquez son numéro. Par exemple, tapez `ups -os1` pour afficher l'état du groupe de sorties 1 (voir la remarque ci-dessous). Remarque : Si vous utilisez cette option sur un onduleur équipé d'un groupe de sortie principal : 1 identifie le groupe de sortie principal, 2 identifie le groupe de sorties commutées 1, 3 identifie le groupe de sorties commutées 2, etc. Sur un onduleur SANS groupe de sorties principal : 1 identifie le groupe de sorties commutées 1, etc.
-st		Affiche l'état de l'onduleur.
-a	start	Teste l'alarme sonore de l'onduleur.

Options de commande des onduleurs MGE Galaxy :

|

Remarque : ces commandes ne sont disponibles que sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000. Certaines options dépendent du modèle d'onduleur spécifique.

Option	Argument	Description
-input	<n° phase> | all	Affiche les valeurs d'entrées pour la phase spécifiée de l'onduleur. L'option « all » permet d'afficher les informations pour toutes les phases de l'onduleur.
	voltage | current | frequency | all	Spécifie la valeur d'entrée pour la commande `ups`. **Exemple :** `ups -input 2 frequency` Affiche la fréquence pour la phase 2 de l'onduleur.
-bypass	<n° phase> | all	Affiche les valeurs d'entrées pour la phase spécifiée de l'entrée secteur de dérivation. L'option « `all` » permet d'afficher toutes les phases de l'entrée secteur de dérivation.
	voltage | current | frequency | all	Spécifie la valeur d'entrée pour la commande `ups`. **Exemple :** `ups -bypass 2 current` Affiche l'intensité pour la phase 2 de l'entrée secteur de dérivation.
-output	<n° phase> | all	Affiche les valeurs de sortie pour la phase spécifiée de l'onduleur. L'option « all » permet d'afficher les informations pour toutes les phases de l'onduleur.
	voltage | current | load | power | percload | pf | frequency | all	Spécifie la valeur de sortie pour la commande ups. **Exemple :** `ups -output 2 percload` Affiche le pourcentage de charge pour la phase 2 de l'onduleur.
-batt		Affiche l'état des batteries de l'onduleur.
-about		Affiche les informations concernant l'onduleur.
-al	<c | w>	Affiche toutes les alarmes existantes. Les options « c » et « w » permettent d'afficher uniquement les alarmes critiques (c) ou d'avertissement (w).

Exemple 1 : Pour lancer le calibrage de l'autonomie, tapez :

```
ups -r start
```

Exemple 2 : Pour mettre immédiatement hors tension le groupe de sorties 2 sur un onduleur Smart-UPS XLM, tapez :

```
ups -o2 off
```

upsfwupdate

Remarque : cette commande est disponible uniquement sur les onduleurs SMX.

Accès : Administrateur, utilisateur de périphérique

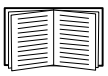
Description : Lance la mise à jour du microprogramme de l'onduleur. Le fichier de mise à jour du microprogramme doit avoir été préalablement récupéré sur le serveur FTP et enregistré dans le répertoire /upsfw/ de la carte de gestion réseau.

Option	Argument	Description
-apply	progress bar	Démarre la mise à jour du microprogramme.
-status	progress bar	Vérifie le statut de la mise à jour du microprogramme en cours.
-lastresult		Affiche le résultat de la dernière mise à jour du microprogramme.
-fileinfo		Affiche les informations concernant le fichier de mise à jour du microprogramme sur la carte de gestion réseau, y compris le nom, la compatibilité avec l'onduleur et la version.

user

Accès : Administrateur uniquement

Description : Configure le nom d'utilisateur et le mot de passe pour chaque type de compte, ainsi que le délai de déconnexion en cas d'inactivité.



Pour en savoir plus sur les autorisations accordées à chaque type de compte (Administrateur, Utilisateur de périphérique, Utilisateur en lecture seule), reportez-vous à la section « Types de comptes utilisateurs » à la page 3.

Option	Argument	Description
-an -dn -rn	<nom administrateur> <nom utilisateur de périphérique> <nom utilisateur en lecture seule>	Définit le nom d'utilisateur (sensible à la casse) pour chaque type de compte. La longueur maximale est de 10 caractères.
-ap -dp -rp	<mot de passe administrateur> <mot de passe utilisateur de périphérique> <mot de passe utilisateur en lecture seule>	Définit le mot de passe (sensible à la casse) pour chaque type de compte. La longueur maximale est de 32 caractères. Le mot de passe ne peut être vide (aucun caractère).
-t	<minutes>	Définit la durée d'attente (par défaut, 3 minutes) avant déconnexion d'un utilisateur inactif.

Exemple 1 : Pour modifier le nom de l'administrateur en XYZ, tapez :

```
user -an XYZ
```

Exemple 2 : Pour faire passer le délai de déconnexion en cas d'inactivité à 10 minutes, tapez :

```
user -t 10
```

web

Accès : Administrateur

Description : Active l'accès à l'interface Web à l'aide du protocole HTTP ou HTTPS.

Pour plus de sécurité, vous pouvez modifier le paramètre de port HTTP ou HTTPS et choisir tout numéro de port inutilisé compris entre 5000 et 32768. Les utilisateurs doivent alors insérer deux-points (:) dans la barre d'adresse de leur navigateur avant de spécifier ce numéro de port. Par exemple, pour se connecter par le port numéro 5000 et l'adresse IP 152.214.12.114 :

```
http://152.214.12.114:5000
```

Option	Argument	Définition
-S	disable | http | https	Configure l'accès à l'interface Web. Lorsque le protocole HTTPS est activé, les données sont cryptées pendant leur transmission et authentifiées par un certificat numérique.
-ph	<n° de port HTTP>	Spécifie le port TCP/IP utilisé par le protocole HTTP pour communiquer avec la carte de gestion réseau (port 80 par défaut).
-ps	<n° de port HTTPS>	Spécifie le port TCP/IP utilisé par le protocole HTTPS pour communiquer avec la carte de gestion réseau (port 443 par défaut).

Exemple : Pour bloquer tout accès à l'interface Web, tapez :

```
web -S disable
```

xferINI

Accès : Administrateur uniquement. Cette commande ne fonctionne qu'en connexion série à l'interface en ligne de commande.

Description : Utilise le protocole XMODEM pour télécharger un fichier .ini pendant que vous êtes connecté à l'interface en ligne de commande via une connexion série. Lorsque le téléchargement est terminé :

- En cas de modification du système ou du réseau, l'interface en ligne de commande redémarre et vous devez vous reconnecter.
- Si vous aviez sélectionné pour le transfert du fichier une vitesse de transfert différente de la vitesse par défaut définie pour la carte de gestion réseau, vous devrez rétablir la vitesse par défaut afin de reprendre la communication avec la carte.

xferStatus

Accès : Administrateur uniquement

Description : Affiche le résultat du dernier transfert de fichier.

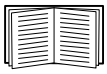
Reportez-vous à la section « Contrôle des mises à niveau et des mises à jour » à la page 107 pour la description des codes de résultat des transferts de fichiers.

Interface Web

Introduction

Présentation

L'interface Web comprend des options permettant de consulter l'état de l'onduleur et de le gérer ainsi que la carte de gestion réseau.



Consultez « Web » en page 76 pour des informations sur la manière de sélectionner, d'activer et de désactiver les protocoles de contrôle d'accès à l'interface Web, et de définir les ports de serveurs Web destinés aux protocoles.

Navigateurs Web pris en charge

Vous pouvez utiliser le navigateur Microsoft® Internet Explorer® (IE) version 7.x ou supérieure (uniquement sur systèmes d'exploitation Windows®) ou Mozilla® Firefox® version 3.0.6 ou supérieures (sur tous les systèmes d'exploitation) pour accéder à la carte de gestion réseau via son interface Web. D'autres navigateurs couramment diffusés peuvent convenir mais n'ont pas fait l'objet de tests complets de la part.

La carte de gestion réseau n'est pas compatible avec un serveur proxy. Avant d'utiliser un navigateur Web pour accéder à son interface Web, vous devez procéder comme suit :

- Configurez votre navigateur Web en désactivant l'utilisation d'un serveur de proxy pour la carte de gestion réseau.
- Configurez le serveur proxy de sorte qu'il n'utilise pas l'adresse IP spécifique de la carte de gestion réseau.

Procédure de connexion

Présentation

Vous pouvez utiliser le nom DNS de la carte de gestion réseau ou son adresse IP système comme adresse URL de l'interface Web. Utilisez votre nom d'utilisateur et votre mot de passe (en respectant les majuscules) pour vous connecter. Le nom d'utilisateur par défaut varie selon le type de compte :

- **apc** pour le niveau Administrateur
- **device** pour le niveau Utilisateur du périphérique
- **readonly** pour le niveau Utilisateur en lecture seule

Le mot de passe par défaut est **apc** pour les trois types de comptes.

Vous pouvez définir la langue d'interface au moment de la connexion en la sélectionnant dans la liste déroulante **Langue**.

Remarque : si vous utilisez le protocole HTTPS (SSL/TLS) comme protocole d'accès, vos informations d'authentification sont comparées à celles que contient un certificat de serveur. Si le certificat a été créé avec l'Assistant de sécurité, et qu'une adresse IP a été spécifiée comme nom générique dans le certificat, vous devez utiliser une adresse IP pour vous connecter à la carte de gestion réseau. Si un nom DNS a été spécifié comme nom générique dans le certificat, vous devez utiliser un nom DNS pour vous connecter.

Pour plus d'informations sur la page Web affichée lors de la connexion, consultez « Page d'accueil » en page 31.

Formats d'adresse URL

Tapez le nom DNS de la carte de gestion réseau ou son adresse IP dans le champ d'adresse URL du navigateur Web et appuyez sur ENTRÉE. Lorsque vous spécifiez dans Internet Explorer un port de serveur Web qui n'est pas le port par défaut, l'URL doit contenir `http://` ou `https://`.

Messages d'erreur courants du navigateur au moment de la connexion.

Message d'erreur	Navigateur	Cause de l'erreur
« Vous n'êtes pas autorisé à afficher cette page » ou « Un utilisateur est actuellement connecté... »	Internet Explorer, Firefox	Un autre utilisateur est connecté.
« Impossible d'afficher cette page ».	Internet Explorer	L'accès par Internet est désactivé, ou l'URL n'est pas correcte.
« Connexion impossible ».	Firefox	

Exemples de formats d'URL.

- Pour un nom DNS « Web1 » :
  - `http://Web1` si votre mode d'accès est HTTP
  - `https://Web1` si votre mode d'accès est HTTPS (HTTP avec SSL)
- Pour une adresse IP système 139.225.6.133 et le port de serveur Web par défaut (80) :
  - `http://139.225.6.133` si votre mode d'accès est HTTP
  - `https://139.225.6.133` si votre mode d'accès est HTTPS (HTTP avec SSL)
- Pour une adresse IP système 139.225.6.133 et un port de serveur Web autre que le port par défaut (5000) :
  - `http://139.225.6.133:5000` si votre mode d'accès est HTTP
  - `https://139.225.6.133:5000` si votre mode d'accès est HTTPS (HTTP avec SSL)
- Pour une adresse IPv6 système de 2001:db8:1::2c0:b7ff:fe00:1100 et un port de serveur Web autre que le port par défaut (5000) :
  - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` si votre mode d'accès est HTTP

Page d'accueil

Présentation

Dans la **page d'accueil** de l'interface, qui s'affiche lorsque vous vous connectez, vous pouvez consulter les alarmes actives et les événements les plus récents enregistrés dans le journal de consignation des événements.

Icônes d'état instantané

Une ou plusieurs icônes avec infobulle indiquent l'état actuel du fonctionnement de l'onduleur :

Symbole	Description
	**Critique** : une alarme critique existe et nécessite une action immédiate.
	**Avertissement** : une alarme nécessite votre attention et pourrait mettre en péril vos données ou votre équipement si le problème n'est pas corrigé.
	**Aucune alarme** : aucune alarme n'est présente ; l'onduleur et la carte de gestion réseau fonctionnent normalement.

Dans le coin supérieur droit de chaque page, l'interface Web affiche les mêmes icônes que celles actuellement affichées dans la **page d'accueil** afin de signaler l'état de l'onduleur :

- L'icône **Aucune alarme** si aucune alarme n'est présente.
- Une des autres icônes (**Critique** et **Avertissement**), voire les deux, en cas d'alarme avec, à la suite de chaque icône, le nombre d'alarmes actives à son niveau de gravité.

Pour revenir à la **page d'accueil** et consulter le récapitulatif de l'état de l'onduleur, y compris les alarmes actives, cliquez sur une icône d'état instantané d'une page de l'interface.

Événements de périphérique récents

Dans la page **Accueil**, la zone **Événements de périphérique récents** affiche en ordre chronologique inverse les événements les plus récents avec la date et l'heure auxquelles il sont survenus. Cliquez sur **Autres événements** pour afficher le journal de consignation des événements complet.

Utilisation des onglets, des menus et des liens

Onglets

En plus de l'onglet de la page **Accueil**, les onglets suivants s'affichent. Cliquez sur un onglet pour afficher l'ensemble d'options de menu correspondantes :

- **Onduleur** : permet d'afficher l'état de l'onduleur, d'émettre des commandes de contrôle de l'onduleur, de configurer les paramètres de l'onduleur, de lancer des tests de diagnostic, de configurer et planifier des arrêts, et de consulter des informations relatives à l'onduleur et à la carte de gestion réseau.
- **Environnement** : permet d'afficher l'état de chaque capteur de température, capteur de température/d'humidité, contact d'entrée ou relais de sortie connecté à la carte de gestion réseau. Permet de consulter les alarmes d'environnement actives et les événements d'environnement récents. Permet aussi de configurer les seuils et autres paramètres relatifs au contrôle d'environnement.

  Remarque : pour l'onduleur, l'onglet **Environnement** s'affiche uniquement lorsqu'un capteur de température, un capteur de température/d'humidité, un contact d'entrée ou un relais de sortie est présent.

- **Journaux de consignation** : permet d'afficher et de configurer les journaux de consignation des événements et des données.
- **Administration** : permet de configurer les paramètres de sécurité, de connexion réseau, de notification, ainsi que les paramètres généraux.

Menus

Menu de navigation de gauche. Chaque onglet (sauf l'onglet de la page Accueil) a un menu de navigation gauche composé d'en-têtes et d'options :

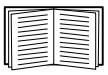
- Si un en-tête comprend des noms d'options en alinéas, l'en-tête lui-même n'est pas un lien de navigation. Cliquez sur une option pour afficher les paramètres ou pour les configurer.
- Si un en-tête ne comprend pas de noms d'options en alinéas, cet en-tête est un lien direct de navigation. Cliquez sur l'en-tête pour afficher les paramètres ou pour les configurer.

Barre de menu supérieure. L'onglet **Administration** comprend différentes options de menu dans la barre de menu supérieure. Sélectionnez l'une de ces options pour afficher son menu de navigation gauche.

Liens rapides

Dans le coin inférieur gauche de chaque page de l'interface se trouvent trois liens configurables. Par défaut, ces liens donnent accès aux URL des pages Web suivantes :

- **Lien 1** : page d'accueil du site Web, www.apc.com
- **Lien 2** : démonstrations de produits activés par le Web
- **Lien 3** : informations sur les services de surveillance à distance



Pour reconfigurer les liens, consultez « Configuration des liens » en page 96.

Surveillance et configuration de l’onduleur

Remarque : pour une carte de gestion réseau d’onduleur AP9631 avec un accessoire d’E/S à contact sec (AP9810) connecté, l’onglet **Onduleur** affiche deux options dans la barre de menu supérieure, **Onduleur** et **Contrôle de la confidentialité**. L’option **Onduleur** permet d’effectuer les tâches décrites dans ce chapitre.

Pour des informations sur l’option **Contrôle de la confidentialité**, consultez « Configuration du contrôle de la confidentialité » à la page 58.

Page Présentation

La page **Présentation** s’affiche par défaut lorsque vous cliquez sur l’onglet **Onduleur** ou que vous sélectionnez l’onglet **Onduleur**, puis **Présentation** dans le menu de navigation gauche de cet onglet.

Etat de fonctionnement

Sous le nom de modèle et le nom configuré de l’onduleur, des icônes et un texte d’accompagnement indiquent l’état de fonctionnement de l’onduleur :

Etat de fonctionnement	Icône	Description
En ligne		**Aucune alarme** : aucune alarme présente ; l’onduleur et la carte de gestion réseau fonctionnent normalement.
Statut d’alarme (le texte d’accompagnement spécifie le statut d’alarme et le décrit brièvement).		**Critique** : une alarme critique nécessite une action immédiate pour éviter la perte de données ou des dommages à l’équipement.
		**Avertissement** : une alarme nécessite votre attention et pourrait mettre en péril vos données ou votre équipement si le problème n’est pas corrigé.

Etat instantané

Les informations suivantes s’affichent (certains champs sont fonction du modèle et ne s’affichent peut-être pas pour le vôtre).

- Sous forme de graphiques :
  - **Charge en Watts** : graphique indiquant la charge de l’équipement relié en pourcentage de watts disponibles.

    Remarque : sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000, le titre du graphique est **Charge.**

  - **Capacité de la batterie** : graphique indiquant le pourcentage de la capacité totale de la batterie de l’onduleur disponible pour l’alimentation des équipements reliés.

- Sous forme de liste :
  - **Tension d'entrée** : tension CA (V CA) reçue par l'onduleur ou, pour les onduleurs triphasés, par chaque phase de l'onduleur.
  - **Tension de sortie** : tension CA (V CA) que l'onduleur ou chacune des phases d'un onduleur triphasé fournit à sa charge.
  - **Température ambiante** : température de l'air à l'intérieur de l'armoire d'entrée/sortie (E/S) de l'onduleur.
  - **Autonomie restante** : durée pendant laquelle l'onduleur peut utiliser la batterie pour continuer d'alimenter la charge.
  - **Dernier transfert de batterie** : cause du dernier basculement vers un fonctionnement sur batteries.
  - **Redondance** : nombre de modules d'alimentation pouvant tomber en panne ou être enlevés sans que l'onduleur bascule en mode de dérivation. Par exemple, avec une redondance n+2, deux modules d'alimentation peuvent tomber en panne ou être enlevés sans provoquer de basculement en mode de dérivation.

Evénements récents de l'onduleur

Les événements les plus récents de l'onduleur sont répertoriés dans l'ordre chronologique inverse. Pour afficher le journal de consignation des événements complet, cliquez sur **Autres événements**.

Page Etat détaillé / Etat

Pour afficher l'état détaillé de l'onduleur, cliquez sur l'option **Etat détaillé** dans le menu de navigation gauche de l'onglet **Onduleur**.

Remarque : la page Etat détaillé n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.

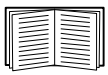
Option Mesures

Pour chaque onduleur, les informations suivantes sont affichées :

Dernier transfert de batterie : cause du dernier basculement en mode d'alimentation sur batteries

Température interne : température à l'intérieur de l'onduleur

Autonomie restante : durée pendant laquelle l'onduleur peut utiliser la batterie pour alimenter la charge



Consultez l'aide en ligne pour afficher les informations détaillées sur des éléments d'état spécifiques au modèle d'onduleur associé à la carte de gestion réseau.

Les types d'informations spécifiques à un modèle qui s'affichent comprennent les valeurs suivantes, dont certaines sont indiquées pour chaque phase dans le cas d'onduleurs triphasés :

- **Informations sur la tension, l'intensité et la fréquence**, telles que la tension d'entrée et de sortie, l'intensité en entrée et en sortie, la fréquence d'entrée, la tension d'entrée en mode de dérivation et les tensions d'entrée minimum et maximum pendant la dernière minute écoulée.
- **Informations sur la charge de l'onduleur**, telles que la charge placée sur l'onduleur en kVA, ou en pourcentage de kVA ou de watts disponibles.
- **Informations sur la tolérance aux défauts**, telles que la puissance redondante disponible.
- **Informations sur les batteries**, telles que la capacité de batterie disponible, le pourcentage de charge des batteries, l'intensité de sortie des batteries, la capacité de tension nominale des batteries, le ratio ampères-heures des armoires de batteries, le nombre de batteries installées et le nombre de batteries défaillantes.

  Rendement de sortie : pourcentage de puissance d'entrée alimentant directement la charge. La charge restante est utilisée par l'onduleur. **Utilisation de l'énergie en sortie** est l'énergie réelle utilisée par la charge à partir de la réinitialisation de l'onduleur à ses valeurs par défaut.
- **Etat des composants internes et externes**, tels que les modules intelligents et d'alimentation, le boîtier de disjoncteurs, le dispositif d'interrupteur externe et le transformateur.

Option Groupes de sorties

Cet écran n'est pas disponible avec tous les modèles d'onduleur.

L'écran Etat des groupes de sorties indique le nom et l'état actuel de tous les groupes de sorties commutées de votre onduleur.

Option Utilisation de l'énergie

Cet écran n'est pas disponible avec tous les modèles d'onduleur.

L'écran d'utilisation de l'énergie vous permet de contrôler la consommation d'énergie de l'équipement relié à votre onduleur. Il indique en outre les données relatives à la consommation d'énergie comme les émissions de dioxyde de carbone et les coûts énergétiques.

Utilisation de l'énergie : estimation de l'électricité consommée à ce jour en kilowatts par heure (kWh). Par exemple, un onduleur alimentant une ampoule de 350 W consomme 350 kWh d'énergie.

Coût total : estimation du coût de l'électricité consommée en devise locale. Par exemple, une ampoule consommant 350 kWh d'énergie sur 1000 heures à un tarif de 0,10 $ par kWh coûte 35 $ pour la totalité de la période.

Emissions de CO_2 : estimation de l'émission totale de dioxyde de carbone (CO_2) à ce jour, en kilogrammes ou livres.

Le coût total et les émissions de CO_2 varient énormément en fonction de la source d'énergie et du réseau de distribution. Vous pouvez obtenir une estimation en choisissant votre pays dans la liste déroulante **Emplacement** et en cliquant sur le bouton **Modifier**. Pour saisir vos propres valeurs, cliquez sur le lien **Modifier les paramètres personnalisés**.

(Vous pouvez également choisir **Personnalisé** dans la liste déroulante et cliquez sur **Modifier** pour saisir vos propres valeurs.)

Page Contrôle

Pour accéder aux actions de commande de l'onduleur, sélectionnez **Onduleur** ou **Groupes de sorties** sous Contrôle.

Remarque : la page Contrôle n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.

Option Onduleur

Cette option s'applique à la fois aux onduleurs individuels et aux groupes de contrôle synchronisé. Pour en savoir plus sur les groupes de contrôle synchronisé, reportez-vous à « Option Contrôle de synchronisation » à la page 47.

Actions (onduleurs individuels et groupes de contrôle synchronisé). Utilisez les actions décrites dans le tableau ci-dessous pour les onduleurs individuels et pour les groupes de contrôle synchronisé, en respectant les principes suivants :

- Les actions **Mettre l'onduleur en mode bypass** et **Retirer l'onduleur du mode bypass** sont prises en charge :
  - uniquement pour les onduleurs individuels, pas pour les groupes de contrôle synchronisé,
  - uniquement pour les onduleurs Symmetra et certains modèles d'onduleurs Smart-UPS.
- Toutes les actions *sauf* **Mettre l'onduleur en mode bypass** et **Retirer l'onduleur du mode bypass** sont prises en charge :
  - pour les onduleurs Smart-UPS, y compris ceux dans les groupes de contrôle synchronisé,
  - pour les onduleurs individuels, y compris les Symmetra.

Remarque : si vous avez sélectionné **Lancer PowerChute Network Shutdown** dans l'interface Web, lancer une action **Mettre l'onduleur hors tension**, **Redémarrer l'onduleur** ou **Mettre l'onduleur en veille** équivaut à lancer la commande `GraceOff` (mise hors tension progressive), `GraceReboot` (redémarrage progressif) ou `GraceSleep` (mise en veille progressive) dans l'interface en ligne de commande.

Pour en savoir plus sur les délais et les paramètres du tableau suivant, reportez-vous à « Pages Configuration » à la page 40 et « Option Contrôle de synchronisation » à la page 47. Pour appliquer un **test de l'alarme de l'onduleur** à un groupe de contrôle synchronisé, reportez-vous à « Page Diagnostics » à la page 51.

Action	Définition
Mettre l'onduleur sous tension (interface Web) `ups -c On` (interface en ligne de commande)	Met l'onduleur sous tension. • Pour les onduleurs avec groupes de sorties, cette action met les groupes de sorties sous tension en fonction de la valeur du **délai de mise sous tension** de chaque groupe. Reportez-vous à la section « Option Groupes de sorties (y compris le délestage automatique) » à la page 40. • Pour les groupes de contrôle synchronisé, après un délai de quelques secondes, l'action met sous tension tous les membres activés du groupe qui sont alimentés en entrée.
Mettre l'onduleur hors tension (interface Web) `ups -c Off` (interface en ligne de commande)	Désactive immédiatement l'alimentation de sortie de l'onduleur et de tous ses groupes de sorties (le cas échéant), sans délai d'arrêt. L'onduleur et tous les groupes de sorties restent éteints jusqu'à ce qu'ils soient de nouveau mis sous tension. Pour les groupes de contrôle synchronisé, cette action met hors tension tous les membres activés du groupe. Aucune valeur de **Délai avant arrêt** n'est utilisée. Les onduleurs s'éteignent après quelques secondes et restent éteints jusqu'à ce qu'ils soient remis sous tension. Reportez-vous à la section « Option Arrêt » à la page 42. **REMARQUE :** pour une action de mise hors tension synchronisée qui utilise la valeur de **Délai avant arrêt** de l'onduleur principal, utilisez le protocole SNMP. Pour l'OID **upsAdvControlUpsOff**, réglez la valeur sur **turnUpsSyncGroupOffAfterDelay (5)**.

Action	Définition
`ups -c GraceOff` (interface en ligne de commande)	Désactive l'alimentation de sortie de l'onduleur et de tous les groupes de sorties (le cas échéant) lorsque le **Délai maximal requis** et le **Délai avant arrêt** configuré sont écoulés. Reportez-vous à la section « Option Clients PowerChute » à la page 47.
Redémarrer l'onduleur (interface Web) `ups -c Reboot` (interface en ligne de commande)	Redémarre l'équipement relié comme suit : • Met l'onduleur hors tension une fois le **Délai avant arrêt** écoulé. • Remet l'onduleur sous tension lorsque la capacité de sa batterie a atteint au moins le pourcentage configuré sous **Capacité minimum de la batterie** ou peut supporter la charge pendant la durée configurée sous **Durée d'autonomie de rétablissement** (ce paramètre dépend du modèle d'onduleur). L'onduleur attend alors pendant la durée spécifiée sous **Délai avant retour**. Reportez-vous à la section « Option Arrêt » à la page 42. • Pour les onduleurs avec groupes de sorties, le **Délai de mise sous tension** commence à la mise sous tension de l'onduleur et se termine à celle d'un groupe de sorties. Dans l'onglet **Onduleur**, configurez le paramètre **Délai de mise sous tension** pour chaque groupe de sorties à l'aide de l'option **paramètres** des **Groupes de sorties**. Reportez-vous à la section « Option Groupes de sorties (y compris le délestage automatique) » à la page 40. Pour une action sur un groupe de contrôle synchronisé : 1. Cette option met hors tension les onduleurs membres du groupe activés après le délai configuré sous **Délai avant arrêt** pour les onduleurs principaux. Reportez-vous à la section « Option Arrêt » à la page 42. 2. L'onduleur principal attend le nombre de secondes spécifié sous **Délai d'alimentation synchronisé** pour laisser aux membres du groupe le temps que leur alimentation d'entrée soit rétablie. Si tous les membres du groupe ont déjà récupéré leur alimentation d'entrée, ce délai est ignoré. Si tous les membres du groupe récupèrent leur alimentation d'entrée pendant ce délai, le temps restant est annulé. Pour configurer le **Délai d'alimentation synchronisé**, reportez-vous à « Configuration d'un membre du groupe de contrôle synchronisé » à la page 49. 3. Le **Délai avant retour** débute lorsque l'onduleur principal atteint la **Capacité minimum de la batterie** configurée (ou la **Durée d'autonomie de rétablissement**). Reportez-vous à la section « Option Arrêt » à la page 42. La **Capacité minimum de la batterie** (ou la **Durée d'autonomie de rétablissement**) de l'onduleur principal est également requise pour les membres du groupe. Vous pouvez toutefois réduire les exigences d'un membre du groupe en configurant son **Décalage de la capacité minimale de la batterie** (ou son **Décalage de la durée d'autonomie de rétablissement**) : par exemple si la **Capacité minimum de la batterie** de l'onduleur principal est de 50 % et que le **Décalage de la capacité minimale de la batterie** est de 5 % pour un membre, ce membre nécessite seulement une capacité de batterie de 45 % pour redémarrer. Reportez-vous à la section « Configuration d'un membre du groupe de contrôle synchronisé » à la page 49.

Action	Définition
`ups -c GraceReboot` (interface en ligne de commande)	• Cette action est similaire à l'action **Redémarrer l'onduleur**, à la différence d'un délai supplémentaire avant l'arrêt. L'équipement relié s'éteint uniquement lorsque l'onduleur (ou l'onduleur principal dans le cas d'une action sur un groupe de contrôle synchronisé) a attendu le **Délai maximal requis** (calculé comme indiqué en section « Option Arrêt » à la page 42). • Pour les onduleurs avec groupes de sorties, le **Délai de mise sous tension** commence à la mise sous tension de l'onduleur et se termine à celle d'un groupe de sorties. Dans l'onglet **Onduleur**, le paramètre **Délai de mise sous tension** peut être configuré pour chaque groupe de sorties par l'option **paramètres** des **Groupes de sorties**. Reportez-vous à la section « Option Groupes de sorties (y compris le délestage automatique) » à la page 40.
Mettre l'onduleur en veille (interface Web) `ups -c Sleep` (interface en ligne de commande)	Bascule l'onduleur en mode veille en désactivant son l'alimentation de sortie pendant une période définie : • L'onduleur désactive son alimentation de sortie une fois le **Délai avant arrêt** configuré écoulé. Reportez-vous à la section « Option Arrêt » à la page 42. • Lorsque l'alimentation d'entrée est rétablie, l'onduleur active son alimentation de sortie après deux périodes configurées : **Heure de veille** et **Délai avant retour**. Reportez-vous à la section « Option Arrêt » à la page 42. • Pour une action sur un groupe de contrôle synchronisé, la carte de gestion réseau de l'onduleur principal attend au maximum le nombre de secondes configuré sous **Délai d'alimentation synchronisé** que les membres du groupe activés récupèrent leur alimentation d'entrée avant d'entamer le **Délai avant retour**. Si tous les membres du groupe ont déjà récupéré leur alimentation d'entrée, le **Délai d'alimentation synchronisé** est ignoré. Si tous les membres du groupe récupèrent leur alimentation d'entrée pendant ce délai, le temps restant est annulé. Reportez-vous à la section « Configuration d'un membre du groupe de contrôle synchronisé » à la page 49.
`ups -c GraceSleep` (interface en ligne de commande)	Bascule l'onduleur en mode veille (désactive l'alimentation pendant une période définie) : • L'onduleur désactive l'alimentation de sortie une fois le **Délai maximal requis** écoulé, afin de permettre au programme PowerChute Network Shutdown de fermer son serveur en toute sécurité, et une fois son propre **Délai avant arrêt** écoulé. Reportez-vous aux sections « Délai maximal requis » à la page 43 et « Option Arrêt » à la page 42. • Lorsque l'alimentation d'entrée est rétablie, l'onduleur active son alimentation de sortie après deux périodes configurées : **Heure de veille** et **Délai avant retour**. Reportez-vous à la section « Option Arrêt » à la page 42. • Pour une action sur un groupe de contrôle synchronisé, la carte de gestion de l'onduleur lançant l'action attend au maximum le nombre de secondes configuré sous **Délai d'alimentation synchronisé** que les membres du groupe activés récupèrent leur alimentation d'entrée avant d'entamer le **Délai avant retour**. Si tous les membres du groupe ont déjà récupéré leur alimentation d'entrée, le **Délai d'alimentation synchronisé** n'intervient pas. Si tous les membres du groupe récupèrent leur alimentation d'entrée pendant ce délai, le temps restant est annulé. Reportez-vous à la section « Configuration d'un membre du groupe de contrôle synchronisé » à la page 49.

Action	Définition

Mettre l'onduleur en mode bypass et **Retirer l'onduleur du mode bypass** (interface Web)
`ups -b Enter`
`ups -b Exit`
(interface en ligne de commande)
	Contrôle l'utilisation du mode de dérivation, qui permet de procéder à des entretiens sur les onduleurs Symmetra et sur certains modèles d'onduleurs Smart-UPS sans qu'il soit nécessaire de mettre l'onduleur hors tension.

Option Groupes de sorties

Pour mettre sous tension, hors tension ou redémarrer un groupe de sorties (lorsque la sortie de l'onduleur est sous tension), sélectionnez l'onglet **Onduleur**, puis **Contrôle - groupes de sorties**.

Sur cette page figure la liste de tous les groupes de sorties, répertoriés par nom et par état (activé ou désactivé), configurés sous l'option **Configuration - groupes de sorties**.

Vous pouvez sélectionner une des actions suivantes (ou aucune) pour le groupe.

- Lorsque l'état du groupe de sorties est **désactivé** :
  - **Immédiatement activé** : le groupe est immédiatement activé.
  - **Activé avec délai** : le groupe est activé après le délai en secondes configuré sous **Délai de mise sous tension**.
- Lorsque l'état du groupe de sorties est **activé** :
  - **Immédiatement désactivé** : le groupe est immédiatement désactivé.
  - **Désactivé avec délai** : le groupe est désactivé après le délai en secondes configuré sous **Délai de mise hors tension**.
  - **Redémarrer immédiatement** : le groupe est immédiatement désactivé, puis activé après le délai en secondes configuré sous **Durée de redémarrage** et sous **Délai de mise sous tension**.
  - **Redémarrer avec délai** : le groupe de sorties est désactivé après le délai en secondes configuré sous **Délai de mise hors tension**, puis activé après le délai en secondes configuré sous **Durée de redémarrage** et sous **Délai de mise sous tension**.
- Sur certains modèles d'onduleurs, lorsque l'état du groupe de sorties est **activé** et que l'onduleur fonctionne sur batterie :
  - **Immédiatement désactivé, Redémarrage secteur** : le groupe est immédiatement désactivé. Une fois le délai en secondes configuré sous **Durée de redémarrage** et sous **Délai de mise sous tension** écoulé, vérifiez que l'alimentation secteur est rétablie et que l'onduleur dispose de l'autonomie de rétablissement nécessaire, puis activez le groupe.
  - **Désactivé avec délai, Redémarrage secteur** : le groupe est désactivé après le délai en secondes configuré sous **Délai de mise hors tension**. Une fois le délai en secondes configuré sous **Durée de redémarrage** et sous **Délai de mise sous tension** écoulé, vérifiez que l'alimentation secteur est rétablie et que l'onduleur dispose de l'autonomie de rétablissement nécessaire, puis activez le groupe.

Après avoir sélectionné une action, cliquez sur **Suivant>>** pour afficher sa description détaillée, y compris la durée des délais. Cliquez sur **Appliquer** pour lancer l'action.

Pages Configuration

Remarque : les pages Configuration ne sont pas disponibles sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.

Qu’est-ce qu’un groupe de sorties ?

Le groupage des sorties est disponible uniquement sur certains modèles d’onduleurs. Pour savoir si votre modèle accepte les groupes de sorties, reportez-vous à sa documentation.

Les paramètres disponibles varient selon le modèle d’onduleur. Consultez l’aide en ligne pour obtenir des informations détaillées sur les champs et valeurs spécifiques à votre modèle d’onduleur.

Groupes de sorties principales. Certains modèles d’onduleurs fournissent une alimentation CA à un groupe de sorties principales.

Remarque : *le groupe de sorties principales contrôle la distribution de l’alimentation vers tous les groupes de sorties commutées de l’onduleur.*

• Si le groupe de sorties principales est désactivé, les groupes de sorties commutées ne peuvent pas être activés.

• Si vous désactivez le groupe de sorties principales, l’onduleur désactive d’abord les groupes de sorties commutées puis le groupe de sorties principales.

• Pour activer un groupe de sorties commutées, l’onduleur doit d’abord activer le groupe de sorties principales puis le groupe de sorties commutées.

Groupes de sorties commutées. Certains modèles d’onduleurs alimentent des groupes de sorties commutées. Chaque groupe peut effectuer des actions indépendamment des autres groupes. En contrôlant à distance chaque groupe de sorties, vous pouvez démarrer ou arrêter les équipements en séquence et redémarrer les équipements verrouillés.

La procédure d’activation et de désactivation des groupes de sorties dépend de leur configuration et de la manière dont vous mettez l’onduleur sous tension ou hors tension :

- Tant que vous n’avez pas configuré les actions décrites en section « Option Groupes de sorties » à la page 39 et les délais correspondants décrits en section « Option Groupes de sorties (y compris le délestage automatique) » à la page 40, tout groupe de sorties désactivé est activé par défaut lorsque vous activez la sortie de l’onduleur et alimente tous les équipements reliés aux sorties de ce groupe.
- Une fois les actions et délais configurés, ils contrôlent l’activation ou la désactivation des groupes de sorties lorsque l’onduleur est mis sous tension ou hors tension depuis l’interface utilisateur de la carte de gestion réseau ou l’interface d’affichage de l’onduleur.

Option Groupes de sorties (y compris le délestage automatique)

Sélectionnez **Configuration** - **groupes de sorties** pour afficher cette option.

Nom et état des groupes de sorties. Le nom et l’état des groupes de sorties s’affiche sur cette page. Cliquez sur le nom d’un groupe de sorties pour afficher ses paramètres ou les configurer sur une autre page (reportez-vous à « Paramètres de mise en séquence » sur cette page).

Paramètre ou champ	Description
Nom	Nom du groupe de sorties qui s’affiche avec le numéro lorsque l’interface affiche ce numéro de groupe de sorties.
Etat	Affiche l’état du groupe de sorties (activé ou désactivé).

Paramètres de mise en séquence. Les paramètres varient selon les modèles d'onduleurs. Utilisez les options de mise en séquence pour définir la manière dont l'onduleur répond aux commandes de l'utilisateur.

Paramètre ou champ	Description
Délai de mise sous tension	Lorsque ce groupe de sorties est désactivé, il laisse écouler ce délai (la durée en secondes dépend du modèle d'onduleur) avant de s'activer lorsque l'action sélectionnée est **Activé avec délai**, **Redémarrer** ou **Redémarrer avec délai**. Case à cocher **Jamais** (disponible uniquement pour certains onduleurs) : pour ignorer le **Délai de mise sous tension**, cochez la case **Jamais**. Seule l'action **Immédiatement activé** active les sorties lorsque la case **Jamais** est cochée.
Délai de mise hors tension	Lorsque ce groupe de sorties est activé, il laisse écouler ce délai (la durée en secondes dépend du modèle d'onduleur) avant de se désactiver lorsque l'action sélectionnée est **Désactivé avec délai**, **Redémarrer** ou **Redémarrer avec délai** (pendant un redémarrage avec délai, le groupe de sorties attend le délai en secondes configuré sous **Durée de redémarrage** et en **Délai de mise sous tension** avant de s'activer). Case à cocher **Jamais** (disponible uniquement pour certains onduleurs) : pour ignorer le **Délai de mise hors tension**, cochez la case **Jamais**. Seule l'action **Immédiatement désactivé** désactive les sorties lorsque la case **Jamais** est cochée.
Durée de redémarrage	Lorsque le groupe de sorties est activé : • Si l'action sélectionnée est **Redémarrer**, le groupe de sorties se désactive immédiatement puis laisse s'écouler ce délai (la durée en secondes dépend du modèle d'onduleur) avant de s'activer. • Si l'action sélectionnée est **Redémarrer avec délai**, le groupe de sorties laisse s'écouler les trois délais suivants : le **Délai de mise hors tension** avant de se désactiver, puis la **Durée de redémarrage**, suivie du **Délai de mise sous tension** avant de se réactiver.
Autonomie de rétablissement minimale	Durée minimale pendant laquelle l'onduleur doit pouvoir alimenter la charge sur batterie avant de pouvoir se remettre sous tension.

Options de délestage. Les paramètres varient selon les modèles d'onduleurs. Utilisez les options de délestage pour définir la manière dont l'onduleur répond aux alarmes. En cas de problème au niveau de la tension d'entrée ou la capacité de la batterie, l'onduleur comprend une fonction de délestage automatique en séquence, puis de démarrage automatique en séquence des groupes de sorties une fois que le problème est résolu.

Paramètre	Description
Paramètres désactivant le groupe de sorties (les paramètres disponibles dépendent du groupe de sorties)	• Lorsqu'une panne d'alimentation est plus longue que la durée en secondes spécifiée. • Lorsque l'autonomie restante de l'onduleur est inférieure à la durée en secondes spécifiée. • L'onduleur est en surcharge (la puissance nécessaire pour alimenter les équipements reliés à l'onduleur dépasse la puissance que l'onduleur peut fournir). • Ignore les délais de mise hors tension des sorties. (Mise hors tension immédiate du groupe de sorties sans attendre le délai en secondes configuré sous **Délai de mise hors tension**. Cette option est désactivée par défaut.) • Laisse le groupe de sorties désactivé après rétablissement de l'alimentation secteur. (Reste hors tension lorsque l'alimentation secteur est rétablie. Cette option est désactivée par défaut et l'onduleur laisse s'écouler la durée en secondes configurée sous **Délai de mise sous tension**, puis active les groupes de sorties.)

Paramètre	Description
Paramètres activant le groupe de sorties	• Le groupe de sorties a attendu la durée en secondes spécifiée. • La batterie se recharge et atteint le pourcentage spécifié de sa pleine capacité.

Evénements et traps des groupes de sorties. Lors d'un changement d'état d'un groupe de sorties, l'événement **Onduleur : groupe de sorties activé** est créé avec le niveau de sévérité Informatif, ou **Onduleur : groupe de sorties désactivé**, avec le niveau de sévérité Avertissement. Le format des messages d'événement est « Onduleur : groupe de sortie *numéro_du_groupe*, *nom_du_groupe*, *action* à cause de *raison* ». Par exemple :

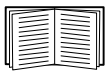
```
Onduleur : groupe de sorties 1, serveur Web, activé.
Onduleur : groupe de sorties 3, imprimante, désactivé.
```

Par défaut, l'événement génère une entrée dans le journal des événements, un e-mail et un message Syslog.

Si vous configurez des récepteurs de traps pour les événements, le trap 298 est généré lorsqu'un groupe de sorties est activé et le trap 299 est généré lorsqu'un groupe de sorties est désactivé. Le message d'événement est l'argument du trap. Le niveau de sévérité par défaut est le même que celui de l'événement.

Option Paramètres d'alimentation

Cette option est disponible sur tous les onduleurs à l'exception des onduleurs MGE Galaxy 300 et MGE Galaxy 7000.



Les paramètres disponibles varient selon le modèle d'onduleur. Consultez l'aide en ligne pour des informations détaillées sur les champs et les valeurs disponibles dans l'option **Alimentation** et spécifiques à votre modèle d'onduleur.

Vous pouvez configurer les types suivants d'éléments spécifiques au modèle :

- Les paramètres de **Tension**, qui déterminent la tension à laquelle l'onduleur commence à utiliser la régulation automatique de tension ou bascule en alimentation sur batterie, ainsi que la sensibilité de l'onduleur aux variations de tension.
- Les paramètres de **Bypass**, qui déterminent dans quelles conditions l'onduleur bascule en mode de dérivation.
- Les **Seuils d'alarme** basés sur l'autonomie et l'alimentation redondante disponibles, ainsi que sur la charge de l'onduleur.

Option Arrêt

Cette option permet d'utiliser l'utilitaire PowerChute Network Shutdown pour désactiver un maximum de 50 serveurs connectés au réseau et utilisant une version client de cet utilitaire.

Paramètre	Définition
Autonomie avec batterie faible	Durée pendant laquelle l'onduleur peut fonctionner sur batterie en cas de batterie faible. Remarque : ce paramètre définit également le temps dont dispose PowerChute pour arrêter les serveurs en toute sécurité en réponse à l'option **Lancer PowerChute Network Shutdown** de la page **Planification**.

Paramètre	Définition
Délai maximal requis	Signale le délai défini par le paramètre **Délai maximal requis**, accessible via l'option **PowerChute** du menu de navigation gauche. Remarque : pour en savoir plus sur les fonctions PowerChute, y compris la manière dont le **Délai maximum avant arrêt** est déterminé, reportez-vous à « Option Arrêt » à la page 42.
Délai avant arrêt	Pour les onduleurs SMX, SMT et SURTD, ce paramètre ne s'applique qu'à un groupe de contrôle synchronisé. Durée d'attente de l'onduleur avant qu'il ne s'arrête complètement en réponse à une commande d'arrêt.
Arrêt de signalisation simple	Lorsqu'il est activé, ce paramètre permet un arrêt du système en toute sécurité et une notification, mais sans les fonctions avancées disponibles uniquement avec la signalisation avancée. Activez l'arrêt de signalisation simple si votre ordinateur est relié à l'onduleur par l'intermédiaire d'un câble de signalisation simple et que le type d'onduleur ne prend pas en charge la signalisation avancée ou qu'il est configuré pour communiquer par signalisation simple.
Autonomie de base avec batterie faible	**Disponible uniquement sur certains modèles d'onduleurs.** Définit le niveau d'autonomie de la batterie auquel l'onduleur envoie un signal d'arrêt pour cause de batterie faible, lorsque le paramètre d'arrêt de signalisation simple est activé.
Heure de veille	Durée pendant laquelle l'onduleur reste en veille (maintient l'alimentation de sortie désactivée) lorsque l'option **Mettre l'onduleur en veille** de la page **Contrôle** est activée.
Durée d'autonomie de rétablissement Capacité minimum de la batterie	La plupart des onduleurs prennent en charge l'un des paramètres suivants pour assurer que leurs batteries aient le temps de se recharger. Si l'alimentation d'entrée est défaillante peu après le redémarrage de l'onduleur, celui-ci peut alors effectuer un arrêt progressif (avant de se mettre sous tension, l'onduleur doit aussi attendre pendant la durée définie sous Délai avant retour). **Durée d'autonomie de rétablissement** : durée pendant laquelle l'onduleur doit pouvoir alimenter la charge sur batterie, nécessaire pour qu'il sorte du mode de veille (ou en cas de redémarrage) et réactive son alimentation de sortie. **Capacité minimum de la batterie** : capacité minimale de la batterie, en pourcentage de la capacité totale, nécessaire à l'onduleur pour sortir du mode de veille (ou en cas de redémarrage) et réactiver son alimentation de sortie.
Délai avant retour	Pour les onduleurs SMX, SMT et SURTD, ce paramètre ne s'applique qu'à un groupe de contrôle synchronisé. Durée avant que l'onduleur se rallume après un arrêt provoqué par une panne de courant ou un arrêt planifié. **REMARQUE :** l'onduleur doit également disposer de la capacité spécifiée sous **Capacité minimum de la batterie** ou de l'autonomie disponible spécifiée sous **Durée d'autonomie de rétablissement** avant de pouvoir se mettre sous tension.

Paramètre	Définition
Délai maximal requis - Négociation forcée	Affiche le délai nécessaire pour garantir que chaque client PowerChute dispose de suffisamment de temps pour être désactivé en toute sécurité lorsque l'onduleur ou le client PowerChute lance un arrêt sécurisé. Lorsque la case **Négociation forcée** est cochée, PowerChute demande à chaque serveur répertorié comme client PowerChute Network Shutdown ses informations sur le temps qui lui est nécessaire pour un arrêt sécurisé. PowerChute recalcule ce délai lorsque l'interface de la carte de gestion réseau de l'onduleur est activée ou réinitialisée. Cette option n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000. Le **Délai maximal requis** est le délai d'arrêt le plus long requis par un des serveurs de la liste, auquel sont ajoutées deux minutes en cas d'événement imprévu. La négociation peut prendre jusqu'à 10 minutes. Si l'option **Négociation forcée** n'est pas sélectionnée, le délai d'arrêt utilisé par défaut pour tous les clients est de deux minutes.
Comportement en cas d'arrêt sur batterie	Lorsque les clients PowerChute Network Shutdown ont mis leurs systèmes informatiques hors tension, ce paramètre détermine si l'onduleur se met automatiquement sous tension ou s'il doit être mis sous tension manuellement une fois l'alimentation d'entrée rétablie. Remarque : cette option n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.
Phrase d'authentification	Phrase (15 à 32 caractères ASCII, sensible à la casse) à utiliser pendant l'authentification MD5 pour la communication PowerChute. Le paramètre Administrateur par défaut est **admin user phrase**.

Arrêt anticipé contrôlé. Ces options ne sont pas disponibles sur tous les onduleurs. Elles permettent d'arrêter un onduleur fonctionnant sur batterie lorsque certaines conditions spécifiées sont satisfaites :

- lorsque le fonctionnement sur batterie dépasse une durée fixée en minutes,
- lorsque l'autonomie restante de l'onduleur est inférieure à une durée fixée en minutes,
- lorsque la charge sur la sortie de l'onduleur est inférieure à un seuil fixé en pourcentage.

Si ces conditions sont activées, l'onduleur s'arrête dans *chacun* de ces cas.

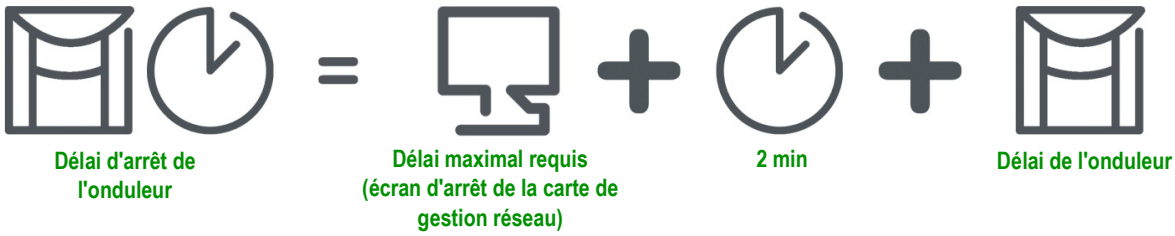
Vous pouvez aussi décider si l'onduleur doit redémarrer ou non après le rétablissement de l'alimentation secteur.

Nous recommandons de ne pas utiliser ces options lorsque l'arrêt du serveur est contrôlé par un logiciel. Par exemple, vous pouvez sélectionner l'option **Ignorer les commandes d'arrêt PCNS** du paramètre **Comportement en cas d'arrêt sur batterie** (vers le bas de cet écran). Alors c'est la carte de gestion réseau qui détermine le comportement de l'onduleur en cas d'arrêt sur batterie, et *non* l'utilitaire PowerChute Network Shutdown (PCNS).

Délais d'arrêt et forçage des négociations. Le délai d'arrêt est calculé différemment pour un onduleur *sans* groupe de sorties ou un onduleur *avec* des groupes de sorties.

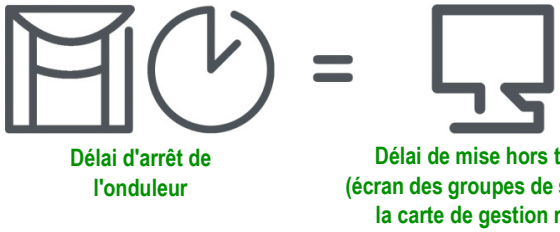
1. Pour un onduleur sans groupe de sorties, le délai d'arrêt est égal au **Délai maximal requis** dans l'écran d'**arrêt** de la carte de gestion réseau *plus* 2 minutes *plus* le délai d'arrêt de l'onduleur.

Onduleur sans groupe de sorties : délai d'arrêt



2. Pour un onduleur avec des groupes de sorties, le délai d'arrêt est égal au **Délai d'arrêt** fixé dans l'écran des **groupes de sorties** de la carte de gestion réseau (cette option n'est pas disponible pour tous les onduleurs).

Onduleur AVEC groupe de sorties : délai d'arrêt



Notez que les appareils SUM se comportent selon le cas 1 ci-dessus et non selon le cas 2.

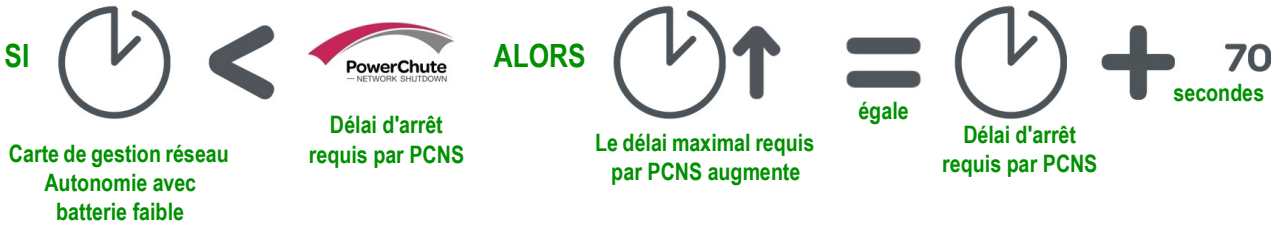
Pour les deux types d'onduleurs, le délai d'arrêt est négocié par interaction entre la carte de gestion réseau et PowerChute Network Shutdown (PCNS).

Lorsque vous modifiez ou ajoutez un client PCNS, utilisez l'option **Négociation forcée** pour redéfinir le délai. Lorsque vous sélectionnez cette option et cliquez sur Appliquer, la procédure est automatique ; les détails sont expliqués ci-dessous.

PCNS commence par vérifier la valeur **Autonomie avec batterie faible** de la carte de gestion réseau, compare cette valeur à son propre délai d'arrêt et, si l'autonomie sur batterie est trop courte, indique à la carte de gestion réseau d'augmenter les délais dans les cas 1 et 2 ci-dessous à la valeur DÉLAI D'ARRÊT REQUIS PCNS* *plus* 70 secondes.

1. Pour un onduleur sans groupe de sorties, le **Délai maximal requis**.

Négociation forcée : onduleur sans groupe de sorties



2. Pour un onduleur avec des groupes de sorties, le **Délai de mise hors tension** du groupe de sorties qui alimente le client PCNS.

*DÉLAI D'ARRÊT REQUIS PCNS = délai d'arrêt + durée de la commande d'arrêt. Lorsque la durée par défaut de 70 secondes est ajoutée, la durée est toujours arrondie à la minute supérieure la plus proche. Par exemple, un total de 3 minutes 50 secondes est arrondi à 4 minutes, et un total de 2 minutes est tout de même arrondi à 3 minutes.

Remarques :
Cette durée de 70 secondes est le délai d'arrêt par défaut du système d'exploitation pour PCNS. PCNS ne modifie jamais la valeur du champ **Autonomie avec batterie faible** de la carte de gestion réseau.
Dans PCNS v3.x, la valeur **Délai maximal requis** n'est jamais utilisée par la carte de gestion réseau pour un onduleur ayant des groupes de sorties.

Option Généralités

Les paramètres varient selon les modèles d'onduleurs. Chaque modèle d'onduleur prend en charge uniquement certains des éléments suivants :

Paramètre	Définition
Nom de l'onduleur	Nom permettant d'identifier l'onduleur.
Position de l'onduleur	Orientation physique de l'onduleur (en rack ou en tour).
Alarme sonore	Active ou désactive l'alarme sonore de l'onduleur et, pour certains modèles d'onduleurs, définit la condition qui provoque le déclenchement de l'alarme.
Dernier remplacement de batterie	Mois et année du dernier remplacement de la batterie.
Nombre de batteries ou Batteries externes	Nombre de batteries dont dispose l'onduleur (à l'exclusion des batteries intégrées). Sur certains modèles comprenant plus de 16 batteries, les batteries doivent être ajoutées par multiple de 16 (par ex. 16, 32, 48, etc.). Ce nombre peut ensuite être ramené à la valeur correcte.
Armoire de batteries externe	Capacité en ampèreheures de l'armoire de batteries d'une source de batterie externe.

Option Programme de test automatique

Cette option permet de définir le moment où l'onduleur lance un test automatique.

Option Mise à jour du microprogramme

Cette option lance la mise à jour du microprogramme de l'onduleur. Le fichier de mise à jour du microprogramme doit avoir été préalablement récupéré sur le serveur FTP et enregistré dans le répertoire /upsfw/ de la carte de gestion réseau.

Option Clients PowerChute

Cliquez sur **Ajouter IP client** pour entrer l'adresse IP d'un nouveau client PowerChute Network Shutdown. Pour supprimer un client, cliquez sur son adresse IP dans la liste puis sur **Supprimer client**.

La liste peut contenir jusqu'à 50 adresses IP de clients.

Remarque : lorsque vous installez un client PowerChute Network Shutdown sur votre réseau, il est automatiquement ajouté à la liste ; lorsque vous désinstallez un client PowerChute Network Shutdown, il est automatiquement supprimé de la liste.

Option Contrôle de synchronisation

Remarque : la page Contrôle de synchronisation n'est pas disponible sur les onduleurs MGE Galaxy 300, MGE Galaxy 7000 et Symmetra.

En quoi consiste le processus de synchronisation ? Si vous appliquez une action à un groupe de contrôle synchronisé, les membres activés de ce groupe ont le comportement suivant :

- Chaque onduleur reçoit la commande quel que soit l'état de sa sortie (par ex. batterie faible).
- L'action applique les délais (tels que le **Délai avant arrêt**, l'**Heure de veille** et le **Délai avant retour**) configurés pour l'onduleur principal.
- Lorsque l'action est lancée, tout onduleur dans l'impossibilité de participer conserve l'état actuel de sa sortie tandis que les autres exécutent l'action. Si un onduleur a déjà sa sortie dans l'état requis par l'action (par ex. un onduleur déjà éteint lorsque l'action de redémarrage de l'onduleur débute), cet onduleur consigne un événement mais exécute le reste de l'action, le cas échéant.
- Tous les onduleurs participants synchronisent l'exécution de leur action (dans un intervalle d'une seconde en conditions idéales pour les onduleurs Smart-UPS, mais quelquefois plus long).
- Pour les actions de redémarrage et de mise en veille :
  - Immédiatement avant de commencer à attendre pendant la durée spécifiée sous **Délai avant retour**, l'onduleur principal attend par défaut jusqu'à 120 secondes (son **Délai d'alimentation synchronisé** configurable) que tous les onduleurs dont l'alimentation d'entrée est désactivée la récupèrent. Tout onduleur dont l'alimentation d'entrée n'est pas rétablie pendant ce délai ne participe pas au redémarrage synchronisé et doit attendre que son alimentation soit rétablie pour redémarrer individuellement.
  - La séquence des voyants à l'avant de l'onduleur n'est pas la même que pour une action de redémarrage ou de mise en veille normale (non synchronisée).
- L'état et les événements de l'onduleur sont signalés de la même manière pour les actions synchronisées que pour les actions exécutées sur des onduleurs individuels.

Directives pour les groupes de contrôle synchronisé. Prenez connaissance des directives suivantes avant de configurer l'onduleur comme membre d'un groupe de contrôle synchronisé :

- Dans un groupe de contrôle synchronisé, tous les onduleurs doivent être du même modèle.
- Les groupes de contrôle synchronisé sont pris en charge par tous les onduleurs Smart-UPS équipés d'un emplacement pour carte de gestion réseau.
- Lorsque son appartenance à un groupe de contrôle synchronisé est activée, la carte de gestion réseau bloque les communications vers l'onduleur provenant d'un périphérique de gestion relié au port de communication série. Toutefois la carte de gestion réseau permet toujours l'accès à l'interface en ligne de commande sur ce port de communication série.

Affichage de l'état d'un membre du groupe de contrôle synchronisé. Lorsque l'appartenance d'un membre à un groupe de contrôle synchronisé est activée, les informations suivantes s'affichent sur cette appartenance.

Elément d'état	Description
Adresse IP	Adresse IP de la carte de gestion réseau de ce membre du groupe (onduleur).
Etat de l'entrée	Etat de l'alimentation d'entrée de ce membre du groupe : **bon** (acceptable) ou **mauvais** (pas acceptable).
Etat de la sortie	Etat de l'alimentation de sortie de ce membre du groupe : **Activé** ou **Désactivé**.

Configuration d’un membre du groupe de contrôle synchronisé

Paramètre	Description
Appartenance aux groupes	Détermine si ce membre du groupe de contrôle synchronisé est un membre actif de son groupe. Si vous désactivez l’appartenance aux groupes, cet onduleur fonctionne comme s’il n’était membre d’aucun groupe de contrôle synchronisé. L’activation ou la désactivation de l’option d’appartenance aux groupes provoque le redémarrage de l’interface de gestion à la connexion suivante. La modification prend effet à ce moment.
Numéro du groupe de contrôle	Identifiant unique du groupe de contrôle synchronisé dont l’onduleur de la carte de gestion réseau est membre. Cette valeur doit être un nombre compris entre 1 et 65534. Un onduleur peut être membre d’un seul groupe de contrôle synchronisé. Tous les membres d’un groupe de contrôle synchronisé doivent avoir le même numéro de groupe de contrôle et la même adresse IP de multidiffusion.
Adresse IP de multidiffusion	Adresse IP utilisée pour communiquer avec les membres d’un groupe de contrôle synchronisé. En protocole IPv6, toute adresse valide de multidiffusion IPv6 peut être utilisée. En protocole IPv4, la plage autorisée va de 224.0.0.3 à 224.0.0.254. Tous les membres d’un groupe de contrôle synchronisé doivent avoir le même numéro de groupe de contrôle et la même adresse IP de multidiffusion.
Délai d’alimentation synchronisé	Durée maximale (120 secondes par défaut) pendant laquelle l’onduleur principal attend, si nécessaire, que l’alimentation des autres membres du groupe soit rétablie une fois qu’il est prêt à être mis sous tension. Une fois ce délai expiré, l’onduleur principal attend d’avoir rechargé sa batterie au niveau d’autonomie spécifié sous Durée d’autonomie de rétablissement ou à la capacité spécifiée sous Capacité minimum de la batterie, si nécessaire, puis attend pendant le délai spécifié sous Délai avant retour avant de se remettre sous tension. **REMARQUE :** pour en savoir plus sur la configuration de la Durée d’autonomie de rétablissement, reportez-vous à la section « Durée d’autonomie de rétablissement » à la page 43. Pour en savoir plus sur la configuration de la Capacité minimum de la batterie, reportez-vous à la section « Capacité minimum de la batterie » à la page 43.
Décalage de la capacité minimale de la batterie ou Décalage de la durée d’autonomie de rétablissement	L’onduleur accepte un seul de ces paramètres, en fonction du modèle. Vous pouvez configurer cette valeur différemment pour chaque membre du groupe de contrôle synchronisé par l’intermédiaire de l’interface de gestion de ce membre. **Décalage de la capacité minimale de la batterie** : pourcentage de la capacité de la batterie soustrait de la Capacité minimum de la batterie de l’onduleur qui lance l’action synchronisée, ce pourcentage servant à déterminer la capacité de batterie nécessaire pour que le membre du groupe concerné soit activé pendant les actions synchronisées. Pour en savoir plus sur la configuration de la Capacité minimum de la batterie, reportez-vous à la section « Capacité minimum de la batterie » à la page 43. **Décalage de la durée d’autonomie de rétablissement** : nombre de secondes soustrait de la Durée d’autonomie de rétablissement de l’onduleur qui lance l’action synchronisée, afin de déterminer l’autonomie disponible nécessaire pour que le membre du groupe concerné soit activé pendant les actions synchronisées. Pour en savoir plus sur la configuration de la Durée d’autonomie de rétablissement, reportez-vous à la section « Durée d’autonomie de rétablissement » à la page 43.
Phrase d’authentification	Phrase (15 à 32 caractères ASCII, sensible à la casse) permettant d’authentifier les membres d’un groupe de contrôle synchronisé. Tous les membres d’un groupe de contrôle synchronisé doivent avoir la même phrase d’authentification. Phrase par défaut : **APC SCG auth phrase**.

Paramètre	Description
Phrase de chiffrement	Clé de chiffrement du protocole qui assure une communication sécurisée entre les membres d'un groupe de contrôle synchronisé. Tous les membres d'un groupe de contrôle synchronisé doivent avoir la même phrase de chiffrement. Phrase par défaut : **APC SCG crypt phrase**.
Port de contrôle synchronisé	Port réseau que les groupes de contrôle synchronisé utilisent pour communiquer. Utilisez n'importe quel port non standard compris entre 5000 et 32768.

Option Unités parallèles (onduleurs Smart-UPS VT)

Paramètre	Description
Configuration de l'unité parallèle	Répertorie toutes les unités parallèles (onduleurs du même type qui partagent une charge et continuent de l'alimenter en cas de défaillance de l'un d'eux). L'onduleur auquel vous êtes connecté est en tête de liste.
Ajouter une unité	Ce bouton permet d'ajouter une unité (9 unités maximum) ou de modifier le nom d'une unité configurée. Spécifiez le nom de l'unité (8 caractères maximum) et son adresse IP.

Page Diagnostics

Vous pouvez lancer un test automatique ou un calibrage d'autonomie pour tous les onduleurs. Le test d'alarme sonore de l'onduleur dépend du modèle et peut ne pas être disponible pour le vôtre.

Remarque : la page Diagnostics n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.

Champ	Description
Test automatique	Résultat (succès, échec ou non disponible) et date du dernier test automatique de l'onduleur.
Calibrage	Résultat du dernier calibrage d'autonomie de la batterie. Le calibrage recalcule l'autonomie restante et doit respecter les points suivants : • Comme le calibrage épuise temporairement les batteries de l'onduleur, vous ne pouvez l'effectuer que si leur capacité est à 100 %. • Sur certains onduleurs, la charge doit être d'au moins 7 % pour pouvoir effectuer le calibrage.
Lancer	Sélectionnez une procédure de diagnostic à effectuer immédiatement : test de l'alarme sonore, test automatique ou calibrage d'autonomie de l'onduleur. Lorsque vous testez l'alarme sonore d'un membre d'un groupe de contrôle synchronisé : • Dans l'interface Web, cette option permet de tester les alarmes de tous les membres activés du groupe. • Dans le protocole SNMP, vous pouvez régler l'OID **upsAdvControlFlashAndBeep** sur **flashAndBeep (2)** pour tester l'alarme d'un onduleur individuel ou sur **flashAndBeepSyncGroup (3)** pour tester les alarmes de tous les membres activés du groupe.

Page Planification (pour les arrêts)

Remarque : la page **Planification - Onduleur** n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.

Pour les options Onduleur et Groupe de sorties

Vous pouvez planifier l'arrêt d'un onduleur sous **Onduleur** ou d'un groupe de sorties spécifique (le cas échéant) sous **Groupes de sorties**.

Les arrêts planifiés configurés s'affichent en haut de la page lorsque vous sélectionnez Onduleur ou Groupes de sorties, avec les détails correspondants, qu'ils soient activés ou désactivés.

Modification, activation, désactivation ou suppression d'un arrêt planifié. Cliquez sur le nom de l'arrêt planifié dans la liste figurant en haut de la page **Onduleur** ou **Groupes de sorties** afin d'accéder à ses paramètres et de les modifier, y compris pour le désactiver temporairement en décochant la case **Activer** ou pour le supprimer définitivement.

Création d'un arrêt planifié d'un onduleur ou d'un groupe de sorties.

1. Sélectionnez **Onduleur** ou **Groupe de sorties** sous **Planification**.
2. Sélectionnez le type d'arrêt à planifier, **Arrêt ponctuel**, **Arrêt quotidien** ou **Arrêt hebdomadaire** (par intervalles de 1, 2, 4 ou 8 semaines) puis cliquez sur le bouton **Suivant**.
3. Pour désactiver temporairement un arrêt planifié, décochez la case **Activer**.
4. Indiquez le nom ainsi que la date et l'heure de l'arrêt.
   Pour les arrêts hebdomadaires, spécifiez la fréquence dans la liste déroulante.
5. Précisez si l'onduleur ou le groupe de sorties doit être remis sous tension après l'arrêt :

   Remise sous tension : spécifiez si l'onduleur doit être remis sous tension à une date et une heure spécifiques, **Jamais** (l'onduleur doit être remis sous tension manuellement) ou **Immédiatement** (l'onduleur sera remis sous tension après un délai de 6 minutes plus le délai spécifié sous Délai avant retour).

   Pour configurer le délai avant retour, reportez-vous à la section « Délai avant retour » à la page 43.

6. Pour un groupe de sorties uniquement, spécifiez le groupe en sélectionnant le bouton approprié.
7. **Signaler l'arrêt du serveur PowerChute** : précisez si les clients indiqués sous « Option Clients PowerChute » doivent être notifiés.

Pour l'onduleur uniquement

Planifier un arrêt synchronisé. Tous les arrêts planifiés sont synchronisés lorsque l'onduleur dont la carte de gestion réseau lance un arrêt est membre d'un groupe de contrôle synchronisé et que son état de membre est activé. Planifiez toujours tous les arrêts à partir du même membre du groupe. Pour qu'un arrêt planifié synchronisé des onduleurs s'effectue, une connexion réseau à chaque onduleur du groupe doit exister au moment où l'action doit intervenir.

Attention : ne planifiez pas d'arrêt par l'intermédiaire de plusieurs membres du groupe. Ce type de planification pourrait produire des résultats imprévisibles.

Page A propos de

Cette option fournit les informations suivantes sur l'onduleur et le microprogramme de sa carte de gestion réseau :

- **Modèle** : nom du modèle d'onduleur.
- **Position** : orientation physique de l'onduleur, en **rack** ou en **tour** (uniquement pour les onduleurs montés en rack ou en tour). (Cette option n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.)
- **Numéro de série** : numéro d'identification unique de l'onduleur, présent également sur l'extérieur de l'onduleur.
- **Version du microprogramme** : numéros de révision des modules du microprogramme actuellement installé sur l'onduleur.
- **Date de fabrication** : date à laquelle la fabrication de l'onduleur a été terminée. (Cette option n'est pas disponible sur les onduleurs MGE Galaxy 300 et MGE Galaxy 7000.)

Les informations suivantes s'affichent également pour les onduleurs MGE Galaxy 300 et MGE Galaxy 7000 :

- **Nom du produit :** marque de l'onduleur.
- **Niveau technique :** niveau technique de l'onduleur.
- **Heure de l'onduleur :** heure locale à l'endroit où se trouve l'onduleur.
- **Pays :** pays où se trouve l'onduleur (onduleur MGE Galaxy 7000 uniquement).
- **Nom du fabricant :** fabricant de l'onduleur.

Surveillance de l’environnement

Remarque : si vous installez un accessoire d'E/S à contact sec (AP9810) sur votre carte de gestion réseau, l'onglet **Environnement** affiche deux options dans la barre de menu supérieure, **E/S universelle** et **Environnement**. Sauf précision supplémentaire, les paramètres décrits dans ce chapitre sont disponibles pour les deux options.

Page Présentation

La page **Présentation** répertorie l'état des appareils de surveillance de l'environnement associés à la carte de gestion réseau AP9631 de l'onduleur.

Intitulé	Informations affichées
Température et humidité	Répertorie tous les capteurs avec pour chacun l'état de l'alarme, la température actuellement enregistrée et l'humidité actuellement enregistrée (si cette dernière est prise en charge). Pour afficher l'état détaillé d'un capteur ou reconfigurer ses paramètres, cliquez sur le nom de ce capteur.
Contacts en Entrée	Répertorie chacun des contacts en entrée activés avec l'état de son alarme et son état actuel (ouvert ou fermé) Pour afficher l'état détaillé d'un contact en entrée activé ou reconfigurer ses paramètres, cliquez sur le nom de ce contact. **Remarque :** pour consulter ou configurer les paramètres d'un contact désactivé, ou bien pour l'activer, vous devez accéder à la page d'interface de ce contact en cliquant sur **Contacts en Entrée** dans le menu de navigation de gauche.
Relais de sortie	Répertorie l'état de l'alarme et l'état actuel (ouvert ou fermé) du relais de sortie du contrôleur d'environnement intégré. Pour consulter l'état détaillé de ce relais de sortie ou reconfigurer ses paramètres, cliquez sur son nom.
Evénements environnementaux récents	La zone **Evénements environnementaux récents** répertorie ces événements en ordre chronologique inverse. Pour afficher le journal de consignation des événements complet, cliquez sur **Autres événements** en bas à droite de la page.

Page Température et humidité

État succinct

Cliquez sur **Température et humidité** dans le menu de navigation de gauche pour afficher le nom de chaque capteur avec l'état de son alarme, sa température et son humidité (si elle est prise en charge).

État détaillé et configuration

Pour afficher l'état détaillé de l'alarme d'un capteur ou configurer ses valeurs, cliquez sur son nom.

Identification et état de l'alarme.

Paramètre	Description
Nom	Nom du capteur. *Au maximum* : 20 caractères.
Emplacement	Emplacement physique du capteur. *Au maximum* : 20 caractères.

Paramètre	Description
État de l'alarme	L'information affichée est l'une des suivantes : • **Normal(e)** si le capteur ne signale aucun état d'alarme. • Si le capteur est en état d'alarme, le texte de l'alarme est affiché en précisant quel seuil est franchi, et la gravité de l'alarme est signalée par une couleur (rouge pour une alarme critique, orange pour un avertissement).
Seuils	Les deux sections qui suivent décrivent les seuils configurables et leurs valeurs d'**Hystérésis**.

Seuils. Pour chaque capteur, les mêmes types de seuils se définissent pour la température et l'humidité (si elle est prise en charge) mesurées au niveau du capteur.

Seuil	Description
Maximum	Une alarme se déclenche si le seuil de température ou d'humidité maximum du capteur est dépassé.
Haute	Une alarme se déclenche si le seuil de température ou d'humidité élevée du capteur est dépassé.
Basse	Une alarme se déclenche si la température ou l'humidité chute sous le seuil inférieur du capteur.
Minimum	Une alarme se déclenche si la température ou l'humidité chute sous le seuil minimum du capteur.

Hystérésis. Cette valeur spécifie à quel niveau la température ou l'humidité doit revenir par rapport à un seuil pour arrêter son alarme de dépassement.

- Pour les seuils Maximum et Haute, le niveau à atteindre pour arrêter l'alarme est égal au seuil moins l'hystérésis.
- Pour les seuils Minimum et Basse, le niveau à atteindre pour arrêter l'alarme est égal au seuil plus l'hystérésis.

Si la température ou l'humidité qui a dépassé un seuil a ensuite tendance à de légères variations, augmentez la valeur d'hystérésis pour éviter de multiples alarmes. Si la valeur d'hystérésis est trop basse, de telles variations peuvent provoquer puis arrêter des dépassements de seuil à répétition.

Exemple de chute de température suivie de variations : le seuil de température Minimum est 55° F et l'hystérésis de la température est 3° F. La température chute en dessous de 55° F, et franchit donc ce seuil. Ensuite la température remonte à 56° puis redescend à 53° F plusieurs fois, mais cela ne provoque aucun événement d'arrêt de l'alarme ni de nouveau dépassement. Pour arrêter l'alarme de dépassement en cours, il faudrait que la température monte au-delà de 58° F (soit 3° F au-dessus du seuil).

Exemple d'augmentation d'humidité suivie de variations : le seuil d'humidité Maximum est 65 % et l'hystérésis d'humidité 10 %. L'humidité augmente au-delà de 65 % et dépasse donc son seuil. Ensuite elle descend à 60 % puis remonte à 70 % plusieurs fois, mais cela ne provoque aucun événement d'arrêt de l'alarme ni de nouveau dépassement. Pour arrêter l'alarme de dépassement en cours, il faudrait que l'humidité chute à moins de 55 % (soit 10 % en dessous du seuil).

Page Contacts en Entrée

État succinct

Cliquez sur **Contacts en Entrée** dans le menu de navigation de gauche pour afficher le nom de chaque contact en entrée avec l'état de son alarme et son état (ouvert ou fermé).

État détaillé et configuration

Pour afficher l'état détaillé d'un contact en entrée ou configurer ses valeurs, cliquez sur son nom.

Paramètre	**Description**
Contact en Entrée	Permet d'activer ou de désactiver le contact en entrée. S'il est désactivé, un contact ne génère aucune alarme même si sa position est anormale.
Nom	Nom du contact en entrée. *Au maximum* : 20 caractères.
Emplacement	Position de ce contact en entrée. *Au maximum* : 20 caractères.
État de l'alarme	**Normal** si le contact en entrée ne signale pas d'alarme, ou bien la gravité de l'alarme s'il signale une alarme.
État	État actuel du contact en entrée : **Fermé** ou **Ouvert**.
État normal	État normal (sans alarme) du contact en entrée : **Fermé** ou **Ouvert**.
Gravité	Gravité de l'alarme générée par l'état anormal du contact en entrée : **Avertissement** ou **Critique**.

Page Relais de sortie

Cette option est uniquement disponible pour les périphériques équipés d'accessoires d'E/S à contact sec. Sélectionnez l'onglet Environnement puis **E/S universelle** dans la barre de menu supérieure. Cliquez sur **Relais de sortie** pour afficher l'état du relais de sortie et configurer ses valeurs.

Paramètre	**Description**
Nom	Nom du relais de sortie. *Au maximum* : 20 caractères.
Emplacement	Emplacement du relais de sortie. *Au maximum* : 20 caractères.
État de l'alarme	**Normal** si le relais de sortie ne signale pas d'alarme, ou bien la gravité de l'alarme s'il signale une alarme.
État	État actuel du relais de sortie : **Fermé** ou **Ouvert**.
État normal	État normal (sans alarme) du relais de sortie : **Fermé** ou **Ouvert**.
Contrôle	Pour modifier l'état actuel du relais de sortie, cochez ce paramètre.
Délai	Nombre de secondes pendant lesquelles un état d'alarme sélectionné doit exister avant que le relais de sortie soit activé. Ce paramètre permet d'éviter qu'une alarme soit activée en raison de brèves conditions transitoires. **REMARQUE :** même si d'autres alarmes paramétrées se produisent après le commencement du délai, celui-ci ne redémarre pas mais continue à s'écouler jusqu'à l'activation du relais de sortie.
Suspendre	Nombre minimum de secondes pendant lesquelles le relais de sortie reste activé après le déclenchement de l'alarme. Même si la condition ayant activé l'alarme est corrigée, le relais de sortie reste activé jusqu'à l'expiration de cette durée de suspension.

Page À propos de

Dans l'option **Environnement** de la barre de menu supérieure, cliquez sur **À propos de** dans le menu de navigation de gauche pour afficher les appareils de contrôle d'environnement fonctionnant avec l'onduleur, ainsi que les versions de leurs microprogrammes.

Configuration du contrôle de la confidentialité

Sur une carte de gestion réseau AP9631 avec jusqu'à deux accessoires d'E/S à contact sec (AP9810) connectés, vous pouvez configurer les sorties en réponse à des événements, et vous pouvez configurer l'onduleur et les sorties en réponse à des alarmes en entrée.

Configuration d'une sortie en réponse à un événement

1. Sélectionnez l'onglet **Onduleur**, **Contrôle de la confidentialité** dans la barre de menu supérieure, puis **par événement** sous **Actions sur les événements** dans le menu de navigation gauche.
2. Cliquez sur le nom d'une catégorie pour consulter tous les événements de cette catégorie, ou sur celui d'une sous-catégorie pour les événements correspondants.
3. Dans la liste d'événements, vérifiez les colonnes marquées pour savoir si l'événement qui vous intéresse est déjà configuré pour modifier l'état du relais de sortie.
4. Pour modifier la configuration existante, cliquez sur le nom de l'événement, sélectionnez le relais de sortie dont l'état devra changer si cet événement est détecté, et cliquez sur **Appliquer**.

Configuration de l'onduleur ou d'une sortie en réponse à une alarme en entrée

1. Sélectionnez l'onglet **Onduleur**, **Contrôle de la confidentialité** dans la barre de menu supérieure, puis **par événement** sous **Actions sur les événements** dans le menu de navigation gauche.
2. Cliquez sur **Contact E/S** puis sur le nom de l'événement à configurer.
3. La carte de gestion réseau accepte jusqu'à quatre entrées. Vous devez spécifier quelle entrée sera associée à cet événement.
    a. Dans la liste déroulante **Port**, sélectionnez le numéro de port de capteurs universel (**1** ou **2**) sur lequel l'E/S à contact sec est installée.
    b. Dans la liste déroulante **Zone**, sélectionnez la lettre de la zone (**A** ou **B**) du contact sur lequel l'entrée est installée.
4. Définissez l'action que l'onduleur doit effectuer lorsque l'entrée change d'état, et sélectionnez la sortie dont l'état doit changer lorsque cet événement est détecté.
5. Cliquez sur **Afficher** pour consulter vos modifications, puis sur **Appliquer**.

Remarque : l'action ainsi configurée est effectuée une fois. Si vous rétablissez l'entrée à son état normal avant que l'alarme s'arrête, la sortie ne changera pas d'état, à moins que l'alarme s'arrête et se déclenche de nouveau.

Journaux de consignation

Utilisation des journaux de consignation des événements et des données

Journal de consignation des événements

Chemin d'accès : Journaux de consignation > Événements > *options*

Vous pouvez consulter, filtrer ou supprimer le journal de consignation des événements. Par défaut, le journal affiche tous les événements enregistrés pendant les deux derniers jours, en ordre chronologique inverse.

Pour consulter les listes de tous les événements configurables ainsi que leur configuration actuelle, sélectionnez l'onglet **Administration**, **Notification** dans la barre de menus supérieure puis **par événement** sous **Actions sur les événements** dans le menu de navigation gauche.

Voir « Configuration par événement » en page 84.

Pour afficher le journal de consignation des événements (Journaux de consignation > Événements > journal de consignation) :

- Par défaut, le journal de consignation des événements s'affiche en page de l'interface Web. L'événement le plus récent est enregistré en page 1. Dans la barre de navigation au-dessous du journal :
  - Cliquez sur un numéro de page pour ouvrir une page spécifique du journal.
  - Cliquez sur **Précédent** ou **Suivant** pour consulter les événements enregistrés immédiatement avant ou après ceux répertoriés dans la page ouverte.
  - Cliquez sur << pour revenir à la première page ou sur >> pour afficher la dernière page du journal.
- Pour consulter les événements répertoriés dans une page, cliquez sur **Ouvrir le journal dans une nouvelle fenêtre** dans la page du journal de consignation des événements pour afficher une vue en plein écran du journal.

Remarque : dans les options de votre navigateur, JavaScript doit être activé pour pouvoir utiliser le bouton **Ouvrir le journal dans une nouvelle fenêtre**.

Vous pouvez également utiliser les protocoles FTP ou Secure CoPy (SCP) pour consulter le journal de consignation des événements. Voir « Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation » en page 64.

Filtrage du journal de consignation (Journaux de consignation > Événements > journal de consignation) :

- **Filtrage du journal par date ou heure :** pour afficher la totalité du journal de consignation des événements ou pour modifier le nombre de jours ou de semaines pour lesquels le journal affiche les événements les plus récents, sélectionnez **Dernier/ère(s)**. Sélectionnez un intervalle de temps dans le menu déroulant, puis cliquez sur **Appliquer**. La configuration du filtre est sauvegardée jusqu'à ce que la carte de gestion réseau redémarre.
  Pour afficher les événements consignés pendant un intervalle de temps spécifique, sélectionnez **Depuis**. Spécifiez les heures (au format 24 heures) et les dates de début et de fin d'affichage des événements, puis cliquez sur **Appliquer**. La configuration du filtre est sauvegardée jusqu'à ce que la carte de gestion réseau redémarre.
- **Filtrage du journal par événement** : pour spécifier les événements à afficher dans le journal, cliquez sur **Filtrer le journal de consignation**. Décochez la case d'option d'une catégorie d'événement ou d'un niveau de gravité d'une alarme pour les supprimer de l'affichage. Le texte dans le coin supérieur droit de la page du journal de consignation des événements indique si un filtre est actif.
  Si vous êtes connecté en tant qu'Administrateur, cliquez sur **Enregistrer en tant que valeur par défaut** pour enregistrer ce filtre comme affichage du journal par défaut pour tous les utilisateurs. Si vous ne cliquez pas sur **Enregistrer en tant que valeur par défaut**, le filtre reste actif jusqu'à ce que la carte de gestion réseau redémarre.
  Pour retirer un filtre actif, cliquez sur **Filtrer le journal de consignation** puis sur **Supprimer le filtre (Afficher tout)**.

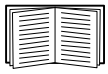
Remarque : les événements sont traités par le filtre en utilisant la logique **OU**.

• Les événements que vous ne sélectionnez pas dans la liste **Filtrer par gravité** ne s'affichent jamais dans le journal de consignation des événements filtré, même si l'événement survient dans une catégorie sélectionnée dans la liste **Filtrer par catégorie**.

• Les événements que vous ne sélectionnez pas dans la liste **Filtrer par catégorie** ne s'affichent jamais dans le journal de consignation des événements filtré, même si les périphériques de la catégorie concernée entrent dans une situation d'alarme sélectionnée dans la liste **Filtrer par gravité**.

Suppression du journal de consignation (Journaux de consignation > Événements > journal de consignation) :

Pour supprimer tous les événements enregistrés dans le journal de consignation, cliquez sur le bouton **Nettoyer le journal de consignation** de la page Web qui contient ce journal. Les événements supprimés ne peuvent plus être récupérés.



Pour désactiver la consignation des événements selon le niveau de gravité qui leur est attribué ou leur catégorie d'événements, consultez « Configuration par groupe » en page 85.

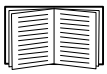
Configuration de la recherche inversée (Journaux de consignation > Événements > recherche inversée) :

La recherche inversée est désactivée par défaut. Activez cette fonction sauf si vous n'avez aucun serveur DNS configuré ou si les performances de votre réseau sont faibles en raison d'un trafic important.

Lorsque la recherche inversée est activée et qu'un événement lié au réseau survient, l'adresse IP et le nom de domaine du périphérique réseau associé à l'événement sont consignés dans le journal de consignation des événements. Si aucun nom de domaine n'existe pour ce périphérique, seule son adresse IP est consignée avec l'événement. Comme les noms de domaines changent généralement moins souvent que les adresses IP, l'activation de la recherche inversée peut améliorer les possibilités d'identifier les adresses des périphériques réseau à l'origine des événements.

Modification de la taille du journal de consignation des événements (Journaux de consignation > Événements > taille) :

Par défaut, le journal de consignation des événements conserve 400 événements. Vous pouvez modifier ce nombre. Lorsque vous modifiez la taille du journal de consignation des événements, toutes les entrées qu'il contient sont supprimées. Pour éviter toute perte de données du journal de consignation, utilisez le protocole FTP ou SCP pour récupérer le journal avant d'entrer une nouvelle valeur dans le champ **Taille du journal de consignation des événements**.



Voir « Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation » en page 64.

Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées.

Journal de consignation des données

Chemin d'accès : Journaux de consignation > Données > *options*

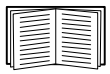
Cette page contient un journal de consignation des mesures concernant l'onduleur,son alimentation d'entrée ainsi que la température ambiante de l'onduleur et des batteries. Chaque entrée est répertoriée selon la date et l'heure auxquelles les données ont été enregistrées.

Affichage du journal de consignation des données (Journaux de consignation > Données > journal de consignation) :

- Par défaut, le journal de consignation des données s'affiche en page de l'interface Web. L'élément de données le plus récent est enregistré en page 1. Dans la barre de navigation au-dessous du journal :
  - Cliquez sur un numéro de page pour ouvrir une page spécifique du journal.
  - Cliquez sur **Précédent** ou **Suivant** pour consulter les données enregistrées immédiatement avant ou après celles répertoriées dans la page ouverte.
  - Cliquez sur << pour revenir à la première page du journal ou sur >> pour afficher la dernière page du journal.

- Pour consulter les données répertoriées dans une page, cliquez sur **Ouvrir le journal dans une nouvelle fenêtre** dans la page du journal de consignation des données pour afficher une vue en plein écran du journal.

Remarque : dans les options de votre navigateur, JavaScript® doit être activé pour pouvoir utiliser le bouton **Ouvrir le journal dans une nouvelle fenêtre**.



Vous pouvez également utiliser les protocoles FTP ou SCP pour consulter le journal de consignation des données. Voir « Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation » en page 64.

Filtrage du journal par date ou heure (Journaux de consignation > Données > journal de consignation) :

pour afficher la totalité du journal de consignation des données ou pour modifier le nombre de jours ou de semaines pour lesquels le journal affiche les événements les plus récents, sélectionnez **Dernier/ère(s)**. Sélectionnez un intervalle de temps dans le menu déroulant, puis cliquez sur **Appliquer**. La configuration du filtre est sauvegardée jusqu'à ce que le périphérique redémarre.

Pour afficher les données consignées pendant un intervalle de temps spécifique, sélectionnez **Depuis**. Spécifiez les heures (au format 24 heures) et les dates de début et de fin d'affichage des données, puis cliquez sur **Appliquer**. La configuration du filtre est sauvegardée jusqu'à ce que le périphérique redémarre.

Suppression du journal de consignation des données :

Pour supprimer toutes les données enregistrées dans le journal de consignation, cliquez sur **Nettoyer le journal de consignation des données** dans la page Web qui contient ce journal. Les données supprimées ne peuvent plus être récupérées.

Définition de la fréquence de collecte des données (Journaux de consignation > Données > intervalle) :

Le paramètre **Fréquence de consignation** permet de définir la fréquence d'échantillonnage et d'enregistrement des données dans le journal de consignation des données, et de consulter le calcul du nombre de jours de données que le journal de consignation peut enregistrer en fonction de l'intervalle choisi. Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées. Pour éviter la suppression automatique des données les plus anciennes, activez et configurez la rotation du journal de consignation des données, décrite dans la section suivante.

Configuration de la rotation du journal de consignation des données (Journaux de consignation > Données > rotation) :

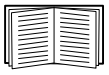
Permet de définir un dépôt du journal de consignation des données protégé par mot de passe sur un serveur FTP spécifié. Lorsque la rotation est activée, le contenu du journal de consignation des données est ajouté au fichier spécifié par nom et par emplacement. Ce fichier est mis à jour selon l'intervalle de téléchargement spécifié.

Paramètre	Description
Rotation des journaux de consignation des données	Activation ou désactivation (par défaut) de la rotation du journal de consignation des données.
Adresse du serveur FTP	Emplacement du serveur FTP où le dépôt de données est enregistré.

Paramètre	Description
Nom d'utilisateur	Nom d'utilisateur requis pour envoyer les données au fichier de dépôt. Cet utilisateur doit aussi être configuré avec autorisation d'accès en lecture et en écriture au fichier de dépôt des données et au répertoire (dossier) dans lequel il est enregistré.
Mot de passe	Mot de passe requis pour envoyer les données au fichier de dépôt.
Chemin du fichier	Chemin d'accès au fichier de dépôt.
Nom de fichier	Nom du fichier de dépôt (fichier texte ASCII).
Délai *X* heures entre les téléchargements.	Nombre d'heures entre les téléchargements de données dans le fichier.
En cas d'échec, retentez le téléchargement toutes les *X* minutes	Nombre de minutes entre chaque tentative de téléchargement de données dans le fichier après un échec du téléchargement.
Jusqu'à *X* fois	Nombre maximum de tentatives de téléchargement après un échec initial.
Jusqu'au succès du téléchargement	Tentatives de téléchargement du fichier jusqu'à ce que le transfert soit terminé.

Pour modifier la taille le journal de consignation des données (Journaux de consignation > Données > taille) :

Par défaut, le journal de consignation des données conserve 400 événements. Vous pouvez modifier le nombre de points de données enregistré dans le journal de consignation. Lorsque vous modifiez la taille du journal de consignation des données, toutes les entrées qu'il contient sont supprimées. Pour éviter toute perte de données du journal de consignation, utilisez le protocole FTP ou SCP pour récupérer le journal avant d'entrer une nouvelle valeur dans le champ **Taille du journal de consignation des données**.



Voir « Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation » en page 64.

Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées.

Utilisation du protocole FTP ou SCP pour récupérer les fichiers de journaux de consignation

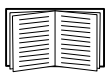
Le niveau Administrateur ou Utilisateur de périphérique permet d'utiliser FTP ou SCP pour récupérer un journal de consignation des événements (*event.txt*) ou des données (*data.txt*) au format texte séparé par des tabulations, qui peut être importé dans un tableur.

- Le fichier contient tous les événements ou toutes les données enregistrés depuis la dernière suppression du contenu du journal de consignation ; dans le cas du journal de consignation des données, celui-ci peut avoir été tronqué s'il avait atteint sa taille maximale.
- Le fichier contient des informations que le journal de consignation des événements ou des données n'affiche pas.
  - Version du format de fichier (premier champ)
  - Date et heure auxquelles le fichier a été récupéré
  - Valeurs **Nom**, **Contact** et **Emplacement**, et adresse IP de la carte de gestion réseau.
  - **Code d'événement** propre à chaque événement consigné (fichier *event.txt* uniquement).

Remarque : la carte de gestion réseau utilise une numérotation à quatre chiffres pour indiquer l'année des entrées du journal de consignation. Vous devrez peut-être sélectionner un format de date à quatre chiffres dans votre tableur pour afficher les quatre chiffres.

Si vous utilisez les protocoles de sécurité codés sur votre système, utilisez SCP pour récupérer le journal de consignation.

Si vous utilisez des méthodes d'authentification non codées pour la sécurité de votre système, utilisez FTP pour récupérer le journal de consignation.



Consultez le *Manuel de Sécurité* disponible sur le CD *Utilitaires* de la carte de gestion réseau et sur le site (**www.apc.com**) pour des informations sur les protocoles et méthodes disponibles pour la configuration du type de sécurité dont vous avez besoin.

Utilisation du protocole SCP pour récupérer les fichiers Pour utiliser SCP afin de récupérer le fichier *event.txt*, utilisez la commande suivante :

`scp` ***`nom_d'utilisateur@nom_d'hôte_ou_adresse_ip`***`:event.txt ./event.txt`

Pour utiliser SCP afin de récupérer le fichier *data.txt*, utilisez la commande suivante :

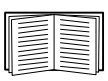
`scp` ***`nom_d'utilisateur@nom_d'hôte_ou_adresse_ip`***`:data.txt ./data.txt`

Utilisation du protocole FTP pour récupérer les fichiers Pour utiliser FTP afin de récupérer le fichier *event.txt* ou *data.txt* :

1. À l'invite de commande, entrez `ftp`, puis l'adresse IP de la carte de gestion réseau et appuyez sur ENTRÉE.

   Si le paramètre **Port** de l'option **Serveur FTP** (configurée dans le menu **Réseau** de l'onglet **Administration**) n'est plus configuré sur la valeur par défaut (**21**), vous devez utiliser la valeur qui lui a été attribuée au niveau de la commande FTP. Pour les clients FTP sous Windows, utilisez la commande suivante (espaces inclus) : (avec certains clients FTP, insérez deux points (:) en remplacement d'un espace entre l'adresse IP et le numéro de port).

   `ftp>open` *`numéro_de_port de_l'adresse_IP`*

   Pour définir un port autre que le port par défaut afin d'améliorer la sécurité du serveur FTP, consultez « Serveur FTP » en page 81. Vous pouvez spécifier n'importe quel port compris entre 5001 et 32768.

2. Utilisez le **nom d'utilisateur** et le **mot de passe** sensibles à la casse pour vous connecter comme Administrateur ou Utilisateur de périphérique. Pour le niveau Administrateur, le **mot de passe** et le **nom d'utilisateur** par défaut sont **apc**. Pour le niveau Utilisateur de périphérique, les valeurs par défaut sont **device** comme **nom d'utilisateur** et **apc** comme **mot de passe**.
3. Utilisez la commande **get** pour transmettre la version texte du journal de consignation sur votre disque local.

   ```
   ftp>get event.txt
   ```

   ou

   ```
   ftp>get data.txt
   ```

4. Vous pouvez utiliser la commande **del** pour supprimer le contenu du journal de consignation des événements ou des données.

   ```
   ftp>del event.txt
   ```

   ou

   ```
   ftp>del data.txt
   ```

   Aucune requête de confirmation de la suppression n'apparaît.

   - Si vous supprimez le journal de consignation des données, le journal de consignation des événements enregistre un événement de suppression de journal.
   - Si vous supprimez le journal de consignation des événements, un nouveau fichier *event.txt* enregistre cet événement.

5. Entrez `quit` à l'invite `ftp>` pour quitter FTP.

Administration : Sécurité

Utilisateurs locaux

Configuration de l'accès utilisateur

Chemin d'accès : Administration > Sécurité > Utilisateurs locaux > *options*

Le compte utilisateur Administrateur a toujours accès à la carte de gestion réseau.

Les comptes Utilisateur de périphérique et Utilisateur en lecture seule sont activés par défaut. Pour désactiver les comptes Utilisateur de périphérique ou Utilisateur en lecture seule, sélectionnez le compte utilisateur dans le menu de navigation gauche, puis décochez la case **Activer**.

Définir le nom d'utilisateur et le mot de passe (sensibles à la casse) pour chaque type de compte se fait de la même manière. La longueur maximum d'un nom d'utilisateur est de 64 caractères, de même que pour le mot de passe. Un mot de passe vierge (aucun caractère) n'est pas autorisé.

Pour des informations sur les autorisations accordées à chaque type de compte (Administrateur, Utilisateur du périphérique, Utilisateur en lecture seule), consultez « Types de comptes utilisateurs » en page 3.

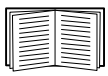
Type de compte	Nom d'utilisateur par défaut	Mot de passe par défaut	Accès autorisé
Administrateur	apc	apc	Interface Web et interface par lignes de commande
Utilisateur de périphérique	device	apc	
Utilisateur en lecture seule	readonly	apc	Interface Web uniquement

Utilisateurs distants

Authentification

Chemin d'accès : Administration > Sécurité > Utilisateurs distants > authentification

Cette option permet de sélectionner le mode de gestion de l'accès à distance à la carte de gestion réseau.



Pour des informations sur l'authentification locale (sans utiliser l'authentification centralisée d'un serveur RADIUS), consultez le *Manuel de sécurité*, disponible sur le CD d'*utilitaires* et sur le site Web à l'adresse **www.apc.com**.

American Power Conversion accepte les fonctions d'authentification et d'autorisation RADIUS (Remote Authentication Dial-In User Service).

- Lorsqu'un utilisateur accède à la carte de gestion réseau ou à tout autre périphérique réseau sur lequel RADIUS est activé, une demande d'authentification est envoyée au serveur RADIUS pour déterminer le niveau d'autorisation de l'utilisateur.
- Les noms d'utilisateurs RADIUS utilisés avec la carte de gestion réseau sont limités à 32 caractères.

Sélectionnez l'une des options suivantes :

- **Authentification locale uniquement** : RADIUS est désactivé. L'authentification locale est activée.
- **Authentification RADIUS, puis locale** : les authentifications RADIUS et locale sont activées. La première authentification demandée est celle du serveur RADIUS. Si le serveur RADIUS ne répond pas, l'authentification locale est utilisée.
- **RADIUS uniquement** : RADIUS est activé. L'authentification locale est désactivée.

Remarque : si **RADIUS uniquement** est sélectionné, et que le serveur RADIUS n'est pas disponible, incorrectement identifié ou incorrectement configuré, l'accès à distance est indisponible pour tous les utilisateurs. Vous devez vous connecter à l'interface par lignes de commande à l'aide d'une connexion série et modifier le paramètre **access** en lui donnant la valeur **local** ou **radiusLocal** pour rétablir l'accès. Par exemple, la commande pour modifier le paramètre d'accès sur **local** serait : `radius -a local`

RADIUS

Chemin d'accès : Administration > Sécurité > Utilisateurs locaux > RADIUS

Cette option permet d'effectuer les actions suivantes :

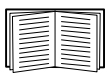
- Répertorier les serveurs RADIUS (deux au maximum) disponibles pour la carte de gestion ainsi que leur délai de temporisation.
- Cliquer sur un lien et configurer les paramètres pour une authentification par un nouveau serveur RADIUS.
- Cliquer sur un serveur RADIUS répertorié pour afficher et modifier ses paramètres.

Paramètre RADIUS	**Définition**
Serveur RADIUS	Nom ou adresse IP du serveur RADIUS (IPv4 ou IPv6). Cliquez sur un lien pour configurer le serveur. **REMARQUE :** les serveurs RADIUS utilisent le port 1812 par défaut pour authentifier les utilisateurs. Pour utiliser un port différent, ajoutez le signe deux points, suivi du nouveau numéro de port, à la suite du nom ou de l'adresse IP du serveur RADIUS.
Secret	Secret partagé entre le serveur RADIUS et la carte de gestion réseau.
Délai de réponse	Durée en secondes pendant laquelle la carte de gestion réseau attend une réponse du serveur RADIUS.
Paramètres de test	Entrez le nom d'utilisateur et le mot de passe Administrateur pour tester le chemin d'accès du serveur RADIUS que vous avez configuré.
Ignorer le test et appliquer	Ne pas tester le chemin d'accès du serveur RADIUS.

Configuration du serveur RADIUS

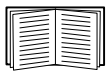
Récapitulatif de la procédure de configuration

Vous devez configurer votre serveur RADIUS afin qu'il fonctionne avec la carte de gestion réseau.



Pour des exemples du fichier des utilisateurs RADIUS disposant d'attributs fournisseur (Vendor Specific Attributes, VSA) et un exemple d'entrée dans le fichier dictionnaire sur le serveur RADIUS, consultez le *Manuel de sécurité*.

1. Ajoutez l'adresse IP de la carte de gestion réseau à la liste des clients du serveur RADIUS (fichier).
2. Les utilisateurs doivent disposer d'attributions Service-Type sauf si des VSA (Vendor Specific Attributes) sont définis. Si aucune attribution Service-Type n'est configurée, les utilisateurs ne disposent que de l'accès en lecture seule (uniquement sur l'interface Web).

   Consultez votre documentation relative au serveur RADIUS pour des informations sur le fichier des utilisateurs RADIUS, et le *Manuel de sécurité* pour voir un exemple.

   3.Les VSA peuvent être utilisés au lieu des attributs Service-Type fournies par le serveur RADIUS. Les VSA nécessitent une entrée de dictionnaire et un fichier d'utilisateurs RADIUS. Dans le fichier de dictionnaire, définissez les noms des mots-clés ATTRIBUTE et VALUE, mais pas des valeurs numériques. Si vous modifiez les valeurs numériques, l'authentification et l'autorisation RADIUS vont échouer. Les VSA ont priorité sur les attributions RADIUS standard.

Configuration d'un serveur RADIUS sous UNIX® avec des mots de passe fantômes

Si des fichiers de mots de passe fantômes UNIX sont utilisés (/etc/passwd) avec les fichiers de dictionnaire RADIUS, vous pouvez utiliser les deux méthodes suivantes pour authentifier les utilisateurs :

- Si tous les utilisateurs UNIX disposent de privilèges administratifs, ajoutez les informations suivantes au fichier « user » RADIUS. Pour autoriser uniquement les comptes Utilisateur de périphérique, modifiez le paramètre Service-Type sur `Device`.

  ```
  DEFAULT  Auth-Type = System
           APC-Service-Type = Admin
  ```

- Ajoutez les noms d'utilisateurs et les attributs au fichier « user » RADIUS et confirmez le mot de passe par rapport à /etc/passwd. L'exemple suivant concerne les utilisateurs `bconners` et `thawk` :

  ```
  bconners Auth-Type = System
           APC-Service-Type = Admin
  thawk    Auth-Type = System
           APC-Service-Type = Device
  ```

Serveurs RADIUS pris en charge

American Power Conversion prend en charge FreeRADIUS et Microsoft IAS 2003. D'autres applications RADIUS courantes peuvent également convenir mais n'ont pas fait l'objet de tests complets de la part.

Délai d'inactivité

Chemin d'accès : Administration > Sécurité > Déconnexion automatique

Utilisez cette option pour configurer la durée d'attente (3 minutes par défaut) du système avant la déconnexion d'un utilisateur inactif. Si vous modifiez cette valeur, vous devez vous déconnecter pour que la modification prenne effet.

Remarque : cette minuterie est conservée si un utilisateur ferme la fenêtre du navigateur sans se déconnecter préalablement en cliquant sur **Déconnexion** dans le coin supérieur droit. Cet utilisateur étant toujours considéré comme connecté, aucun utilisateur ne peut se connecter avant l'expiration du délai spécifié en **Minutes d'inactivité**. Par exemple, lorsque le paramètre **Minutes d'inactivité** a sa valeur par défaut, si un utilisateur ferme la fenêtre du navigateur sans se déconnecter, aucun utilisateur ne peut se connecter avant 3 minutes.

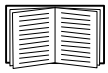
Administration : Fonctions réseau

Paramètres TCP/IP et de communication

Paramètres TCP/IP

Chemin d'accès : administration > Réseau > TCP/IP > paramètres IPv4

L'option **TCP/IP** du menu de navigation gauche, sélectionnée par défaut lorsque vous choisissez **Réseau** dans la barre de menu supérieure, affiche l'adresse IPv4, le masque de sous-réseau, la passerelle par défaut, l'adresse MAC et le mode de démarrage actuels de la carte de gestion réseau.



Pour des informations sur le protocole et les options DHCP, voir **RFC2131** et **RFC2132**.

Paramètre	Description
Activer	Active ou désactive IPv4 avec cette case à cocher.
Manuel	Permet de configurer IPv4 manuellement en entrant l'adresse IP, le masque de sous-réseau et la passerelle par défaut.
BOOTP	Un serveur BOOTP fournit les paramètres TCP/IP. Par intervalles de 32 secondes, la carte de gestion réseau envoie une requête d'attribution réseau à n'importe quel serveur BOOTP : • Si la carte de gestion réseau reçoit une réponse valide, elle démarre les services réseau. • Si la carte de gestion réseau trouve un serveur BOOTP, mais que la requête à ce serveur échoue ou dépasse le délai d'attente, la carte de gestion réseau abandonne ses requêtes de paramètres réseau jusqu'à son redémarrage. • Par défaut, s'il existe des paramètres réseau précédemment configurés et que la carte de gestion réseau ne reçoit aucune réponse valide à cinq requêtes (requête initiale plus quatre tentatives ultérieures), elle utilise les paramètres précédemment configurés afin de rester accessible. Cliquez sur **Suivant>>** pour accéder à la page de configuration BOOTP afin de modifier le nombre de nouvelles tentatives ou l'action à effectuer si toutes les tentatives échouent [1] : • **Nombre maximal de tentatives** : entrez le nombre de tentatives à effectuer lorsqu'aucune réponse valide n'est reçue, ou zéro (0) pour un nombre illimité de tentatives. • **En cas d'échec des nouvelles tentatives** : sélectionnez **Use prior settings** (valeur par défaut) ou **Stop BOOTP request**.

1. En général, il n'est pas nécessaire de modifier les valeurs par défaut de ces trois paramètres des pages de configuration :
   • **Catégorie de fournisseur** : APC
   • **Identifiant client** : adresse MAC de la carte de gestion réseau, qui l'identifie de manière unique sur le réseau local (LAN).
   • **Catégorie d'utilisateur** : nom du module du microprogramme d'application.

Paramètre	Description
DHCP	Paramètre par défaut. Par intervalles de 32 secondes, la carte de gestion réseau envoie une requête d'attribution réseau à n'importe quel serveur DHCP. • Si la carte de gestion réseau reçoit une réponse valide, elle ne demande pas le cookie APC au serveur DHCP pour accepter le bail et démarrer les services réseau. • Si la carte de gestion réseau trouve un serveur DHCP, mais que la requête à ce serveur échoue ou expire, la carte abandonne ses requêtes de paramètres réseau jusqu'à son redémarrage[1]. • **Cookie du fournisseur nécessaire pour accepter l'adresse DHCP** : active ou désactive l'obligation que le serveur DHCP transmette le cookie APC en cochant ou en décochant la case.

1. En général, il n'est pas nécessaire de modifier les valeurs par défaut de ces trois paramètres des pages de configuration :
   • **Catégorie de fournisseur** : APC
   • **Identifiant client** : adresse MAC de la carte de gestion réseau, qui l'identifie de manière unique sur le réseau local (LAN).
   • **Catégorie d'utilisateur** : nom du module du microprogramme d'application.

Options de réponse DHCP

Chaque réponse DHCP valide contient des options fournissant les paramètres TCP/IP que requiert la carte de gestion pour fonctionner en réseau, ainsi que des informations supplémentaires ayant une incidence sur le fonctionnement de la carte de gestion réseau.

Informations spécifiques au fournisseur (option 43). La carte de gestion réseau utilise cette option dans une réponse DHCP pour en définir la validité. Cette option contient une option spécifique au format TAG/LEN/DATA, appelée cookie APC. Ce paramètre est désactivé par défaut.

- **Cookie APC. Tag 1, Len 4, Data « 1APC »**

  L'option 43 prévient la carte de gestion réseau qu'un serveur DHCP est configuré pour prendre en charge les périphériques American Power Conversion.

  Voici un exemple, au format hexadécimal, d'une option d'informations spécifiques au fournisseur contenant le cookie APC :

  ```
  Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
  ```

Options TCP/IP. La carte de gestion réseau utilise les options suivantes dans une réponse DHCP valide pour définir ses paramètres TCP/IP : toutes ces options, sauf la première, sont décrites dans **RFC2132**.

- **Adresse IP** (à partir du champ **yiaddr** de la réponse DHCP, décrit en **RFC2131)** : adresse IP attribuée à la carte de gestion réseau par le serveur DHCP.
- **Masque de sous-réseau** (option 1) : valeur du masque de sous-réseau requise par la carte de gestion réseau pour fonctionner en réseau.
- **Routeur,** c'est-à-dire la passerelle par défaut (option 3) : adresse de la passerelle par défaut requise par la carte de gestion réseau pour fonctionner en réseau.
- **Durée de bail d'adresse IP** (option 51) : durée du bail de l'adresse IP de la carte de gestion réseau.
- **Durée de renouvellement, T1** (option 58) : durée d'attente requise par la carte de gestion réseau après l'attribution d'un bail d'adresse IP avant de demander que cette attribution soit renouvelée.
- **Durée de reliaison, T2** (option 59) : durée d'attente requise par la carte de gestion réseau après l'attribution d'un bail d'adresse IP avant de pouvoir tenter de réassocier cette attribution.

Autres options. La carte de gestion réseau utilise également ces options dans une réponse DHCP valide. Toutes ces options, sauf la dernière, sont décrites dans **RFC2132**.

- **Serveurs du protocole de temps du réseau** (option 42) : jusqu'à deux serveurs NTP (primaire et secondaire) que peut utiliser la carte de gestion réseau.
- **Décalage de temps** (option 2) : décalage du sous-réseau de la carte de gestion réseau en secondes à partir de l'UTC (temps universel coordonné).
- **Serveur de nom de domaine** (option 6) : jusqu'à deux serveurs DNS (primaire et secondaire) que peut utiliser la carte de gestion réseau.
- **Nom d'hôte** (option 12) : nom d'hôte que la carte de gestion réseau utilisera (32 caractères maximum).
- **Nom de domaine** (option 15) : nom de domaine que la carte de gestion réseau utilisera (64 caractères maximum).
- **Nom du fichier d'initialisation** (à partir du champ **file** (fichier) de la réponse DHCP, décrit en **RFC2131)** : chemin d'accès complet à un fichier de configuration utilisateur (fichier .ini) afin de le télécharger. Le champ **siaddr** de la réponse DHCP spécifie l'adresse IP du serveur depuis lequel la carte de gestion réseau va télécharger le fichier .ini. Après le téléchargement, la carte de gestion réseau utilise le fichier .ini comme fichier d'amorçage pour reconfigurer ses paramètres.

Chemin d'accès : Administration > Réseau > TCP/IP > paramètres IPv6

Paramètre	Description
Activer	Active ou désactive IPv6 avec cette case à cocher.
Manuel	Permet de configurer IPv6 manuellement en entrant l'adresse IP et la passerelle par défaut.
Configuration automatique	Lorsque la case Configuration automatique est cochée, le système obtient les préfixes d'adressage du routeur (si possible). Il utilise ces préfixes pour configurer automatiquement les adresses IPv6.
Mode DHCPv6	**Routeur contrôlé** : lorsque cette option est cochée, DHCPv6 est contrôlé par les indicateurs Managed (M) (Géré) et Other (O) (Autre) reçus dans les annonces de routage IPv6. Lorsqu'une annonce de routage est reçue, la carte de gestion réseau vérifie si l'indicateur M ou O est défini. La carte de gestion réseau interprète l'état des « bits » M (indicateur de configuration de l'adresse gérée) et O (indicateur d'autre configuration avec état) dans les cas suivants : • *Aucun n'est défini* : le réseau local n'a aucune infrastructure DHCPv6. La carte de gestion réseau utilise les annonces de routage et la configuration manuelle pour obtenir des adresses sans liaison locale et d'autres paramètres. • *M ou bien M et O sont définis* : dans cette situation, une configuration d'adresse DHCPv6 complète survient. DHCPv6 est utilisé pour obtenir des adresses ET d'autres paramètres de configuration. Ceci est appelé `DHCPv6 avec état`. Lorsque l'indicateur M a été reçu, la configuration d'adresse DHCPv6 reste en effet jusqu'à ce que l'interface concernée soit fermée. Ceci est vrai même si des paquets d'annonces de routage ultérieurs sont reçus dans lesquels l'indicateur M n'est pas défini. Si un indicateur O est reçu en premier, suivi par la réception ultérieure d'un indicateur M, la carte de gestion réseau effectue une configuration d'adresse complète dès la réception de l'indicateur M. • *Seul O est défini* : dans cette situation, la carte de gestion réseau envoie un paquet de requête d'informations DHCPv6. DHCPv6 sera utilisé pour configurer les « autres » paramètres (tels que l'emplacement des serveurs DNS), mais PAS pour fournir des adresses. Ceci est appelé `DHCPv6 sans état`. **Adresse et autres informations :** lorsque cette case d'option est cochée, DHCPv6 est utilisé pour obtenir des adresses ET d'autres paramètres de configuration. Ceci est appelé `DHCPv6 avec état`. **Informations hors adresse uniquement** : lorsque cette option est sélectionnée, DHCPv6 sera utilisé pour configurer les « autres » paramètres (tels que l'emplacement des serveurs DNS), mais PAS pour fournir des adresses. Ceci est appelé `DHCPv6 sans état`. **Jamais** : cette option désactive DHCPv6.

Temps de réponse du ping

Chemin d'accès : Administration > Réseau > Temps de réponse du ping

Cochez la case Activer de l'option **Réponse du ping IPv4 :** pour permettre à la carte de gestion réseau de répondre aux tests Ping du réseau. Décochez-la pour désactiver la réponse d'une carte de gestion réseau. Ceci ne s'applique pas à IPv6.

Vitesse du port :

Chemin d'accès : Administration > Réseau > Vitesse du port

Le paramètre **Vitesse du port** définit la vitesse de communication du port TCP/IP.

- En **Négociation automatique** (valeur par défaut), les périphériques Ethernet négocient les transmissions à la vitesse la plus élevée possible, mais si les vitesses prises en charge de deux périphériques ne correspondent pas, c'est la vitesse la plus lente qui est utilisée.
- Vous pouvez aussi choisir une vitesse de 10 Mbits/s ou 100 Mbits/s, chacune avec l'option semi-duplex (transmissions dans un sens à la fois) ou duplex (transmissions simultanées dans les deux sens sur le même canal).

DNS

Chemin d'accès : Administration > Réseau > DNS > *configuration*

Utilisez les options du menu **DNS** dans le menu de navigation gauche pour configurer le système de noms de domaine (DNS) et le tester :

- Sélectionnez **Serveur DNS primaire** ou **Serveur DNS secondaire** pour spécifier les adresses IPv4 ou IPv6 du serveur DNS primaire ou du serveur secondaire en option. Pour que la carte de gestion réseau puisse envoyer des e-mails, vous devez au moins définir l'adresse IP du serveur DNS primaire.
  - La carte de gestion réseau attend jusqu'à 15 secondes une réponse du serveur DNS primaire ou du serveur DNS secondaire (dans la mesure où un serveur DNS secondaire a été spécifié). Si la carte de gestion réseau ne reçoit pas de réponse pendant ce délai, aucun e-mail ne peut être envoyé. Par conséquent, utilisez des serveurs DNS reliés au même segment du réseau que la carte de gestion réseau ou à un segment adjacent (sans passer par un réseau étendu [WAN]).
  - Après avoir défini les adresses IP des serveurs DNS, vérifiez que le protocole DNS fonctionne correctement en entrant le nom DNS d'un ordinateur de votre réseau pour rechercher son adresse IP.
- **Nom d'hôte** : lorsque vous avez configuré un nom d'hôte dans cette zone et un nom de domaine dans le champ **Nom du domaine**, les utilisateurs peuvent entrer un nom d'hôte dans n'importe quel champ de l'interface de la carte de gestion réseau (à l'exception des adresses électroniques) qui accepte un nom de domaine.
- **Nom du domaine (IPv4)** : vous devez configurer le nom de domaine uniquement ici. Dans tous les autres champs de l'interface de la carte de gestion réseau (à l'exception des adresses électroniques) qui acceptent les noms de domaines, la carte de gestion réseau ajoute ce nom de domaine lorsque seul un nom d'hôte est entré.
  - Pour ignorer tous les cas d'extension d'un nom d'hôte spécifié par l'ajout d'un nom de domaine, définissez le champ du nom de domaine sur sa valeur par défaut (`somedomain.com`) ou sur `0.0.0.0`.
  - Pour ignorer l'extension d'une entrée de nom d'hôte spécifique (par exemple à la définition d'un récepteur de traps), ajoutez un point final. La carte de gestion réseau reconnaît un nom d'hôte comprenant un point final (tel que *`monServeurSnmp.`*) comme étant un nom de domaine complet et n'ajoute alors pas le nom de domaine.
- **Nom du domaine (IPv6)** : spécifiez ici le nom de domaine IPv6.

- Sélectionnez **test** pour envoyer une requête DNS permettant de tester la configuration de vos serveurs DNS :
  - En paramètre **Type de requête**, sélectionnez la méthode à employer pour la requête DNS :
    - **par hôte** : nom URL du serveur
    - **par FQDN** : nom de domaine complet
    - **par IP** : adresse IP du serveur
    - **par MX** : messagerie utilisée par le serveur
  - En **Question de la requête**, identifiez la valeur à attribuer au type de requête sélectionné :

Type de requête sélectionné	**Question de la requête à utiliser**
par hôte	URL
par FQDN	nom de domaine complet : *mon_serveur.mon_domaine.*
par IP	adresse IP
par MX	adresse de messagerie

  - Le résultat de la requête de test DNS s'affiche dans le champ **Réponse à la dernière requête**.

Web

Chemin d'accès : Administration > Réseau > Web > *options*

Option	Description

accès	Pour activer les modifications apportées aux choix ci-dessous, déconnectez-vous de la carte de gestion réseau :
	• **Désactiver** : désactive l'accès à l'interface Web (pour le réactiver, connectez-vous à l'interface par lignes de commande, puis tapez la commande `http -S enable`. Pour l'accès HTTPS, tapez `https -S enable`).
	• **Activer HTTP** (option par défaut) : active le protocole HTTP (Hypertext Transfer Protocol), qui fournit l'accès Web par nom d'utilisateur et mot de passe, mais sans coder les noms d'utilisateurs, les mots de passe ni les données pendant la transmission.
	• **Activer HTTPS** : active le protocole HTTPS (Hypertext Transfer Protocol avec Secure Sockets Layer [SSL]) Le protocole SSL code les noms d'utilisateurs, les mots de passe et les données pendant la transmission, et authentifie la carte de gestion réseau par certificat numérique. Lorsque le protocole HTTPS est activé, votre navigateur affiche une petite icône représentant un cadenas.
	
	Pour choisir une méthode d'utilisation des certificats numériques, consultez « Creating and Installing Digital Certificates » (Création et installation de certificats numériques) dans le *Manuel de sécurité* du CD d'*utilitaires* de la carte de gestion réseau.
	
	Port HTTP : port TCP/IP (port 80 par défaut) utilisé pour communiquer par protocole HTTP avec la carte de gestion réseau.
	
	Port HTTPS : port TCP/IP (port 443 par défaut) utilisé pour communiquer par protocole HTTPS avec la carte de gestion réseau.
	
	Pour plus de sécurité, vous pouvez modifier le paramètre de ces ports sur un port inutilisé compris entre 5000 et 32768. Les utilisateurs doivent alors taper le signe deux points (:) dans le champ d'adresse du navigateur pour spécifier le numéro du port. Par exemple, pour se connecter par le port numéro 5000 et l'adresse IP 152.214.12.114 :
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

Option	Description
certificat SSL	Ajout, remplacement ou suppression d'un certificat de sécurité. **État** : • **Non installé** : un certificat n'est pas installé, ou a été installé par FTP ou SCP à un emplacement incorrect. L'option **Ajouter ou remplacer Fichier du certificat** installe le certificat à l'emplacement correct, **/ssl** sur la carte de gestion réseau. • **Generating** : la carte de gestion réseau génère un certificat car aucun certificat valide n'a été trouvé. • **Loading** : un certificat est en cours d'activation sur la carte de gestion réseau. • **Certificat valide** : un certificat valide a été installé ou a été généré par la carte de gestion réseau. Cliquez sur ce lien pour afficher le contenu du certificat. **Si vous installez un certificat non valide, ou si aucun certificat n'est chargé lorsque vous activez le protocole SSL, la carte de gestion réseau génère un certificat par défaut, processus qui peut retarder l'accès à l'interface jusqu'à une minute.** Vous pouvez utiliser le certificat par défaut pour les protocoles de sécurité codés de base, mais dans ce cas un message d'alerte de sécurité s'affiche chaque fois que vous vous connectez. **Ajouter ou remplacer Fichier du certificat** : entrez le fichier de certificat créé avec l'Assistant de sécurité ou naviguez jusqu'à ce fichier. Pour choisir une méthode d'utilisation des certificats numériques créés par l'Assistant de sécurité ou générés par la carte de gestion réseau, consultez « Creating and Installing Digital Certificates » (Création et installation de certificats numériques) dans le *Manuel de sécurité* du CD d'*utilitaires* de la carte de gestion réseau. **Supprimer** : supprimer le certificat actif.

Console

Chemin d'accès : Administration > Réseau > Console > *options*

Option	Description

accès	Les options suivantes sont proposées pour l'accès par Telnet ou Secure SHell (SSH) :
	• **Désactiver** : désactive tout accès à l'interface par lignes de commande.
	• **Activer Telnet** (option par défaut) : le protocole Telnet transmet les noms d'utilisateurs, les mots de passe et les données sans codage.
	• **Activer SSH** : le protocole SSH transmet les noms d'utilisateurs, les mots de passe et les données sous forme codée, offrant une protection contre les tentatives d'interception, de contrefaçon ou d'altération des données au cours de leur transmission.
	
	Configurez les ports que ces protocoles devront utiliser :
	• **Port Telnet** : port Telnet utilisé pour communiquer avec la carte de gestion réseau (port 23 par défaut). Pour plus de sécurité, vous pouvez modifier le paramètre du port sur un port inutilisé compris entre 5000 et 32768. Les utilisateurs doivent alors taper le signe deux points (:) ou un espace, selon les exigences de votre programme client Telnet, pour spécifier la valeur du port autre que la valeur par défaut. Par exemple pour le port 5000 et l'adresse IP 152.214.12.114, votre client Telnet exige l'une des commandes suivantes :
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **Port SSH** : port SSH utilisé pour communiquer avec la carte de gestion réseau (port 22 par défaut). Pour plus de sécurité, vous pouvez modifier le paramètre du port sur un port inutilisé compris entre 5000 et 32768. Consultez la documentation de votre client SSH pour connaître le format de ligne de commande requis pour spécifier un port autre que le port par défaut.

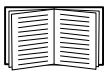
clé de l'hôte SSH	**État** indique l'état de la clé d'hôte (clé privée) : • **SSH désactivé : aucune clé d'hôte utilisée :** lorsqu'il est désactivé, le protocole SSH ne peut pas utiliser de clé d'hôte. • **Generating** : la carte de gestion réseau crée une clé d'hôte car aucune clé d'hôte valide n'a été trouvée. • **Loading** : une clé d'hôte est en cours d'activation sur la carte de gestion réseau. • **Valide** : une des clés d'hôtes suivantes se trouve dans le répertoire **/ssh** (emplacement requis sur la carte de gestion réseau) : •Clé d'hôte de 1024 ou 2048 bits créée par l'Assistant de sécurité. •Clé d'hôte RSA de 2048 bits générée par la carte de gestion réseau. **Ajouter ou Remplacer** : permet de naviguer jusqu'à un fichier de clé d'hôte créé par l'Assistant de sécurité et de le télécharger. Pour utiliser l'Assistant de sécurité, consultez le *Manuel de sécurité* sur le CD d'*utilitaires* de la carte de gestion réseau. **REMARQUE :** pour réduire le temps nécessaire pour activer le protocole SSH, créez une clé d'hôte à l'avance et téléchargez-la. **Si vous activez le protocole SSH sans qu'aucune clé d'hôte ne soit chargée, la carte de gestion réseau prend jusqu'à une minute pour en créer une, délai au cours duquel le serveur SSH est inaccessible.** **Supprimer** : supprime la clé d'hôte active.

Remarque : pour utiliser le protocole SSH, un client SSH doit être installé. La plupart des plateformes Linux et UNIX comprennent un client SSH, mais pas les systèmes d'exploitation Microsoft Windows. Les clients sont disponibles auprès de plusieurs fournisseurs.

SNMP

Tous les noms d'utilisateur, les mots de passe et les noms de communauté pour SNMP sont transmis sur le réseau sous forme de simple texte. Si votre réseau nécessite un codage de haute sécurité, désactivez l'accès SNMP ou paramétrez-le en lecture seule pour chaque communauté (une communauté disposant de l'accès en lecture peut recevoir des informations d'état et utiliser les traps SNMP).

Lorsque vous utilisez InfraStruXure Central pour la gestion d'un onduleur sur le réseau public d'un système InfraStruXure, le protocole SNMP doit être activé dans l'interface de la carte de gestion réseau. L'accès en lecture permet au périphérique InfraStruXure de recevoir les traps de la carte de gestion réseau. Un accès en écriture est nécessaire lorsque vous utilisez l'interface de la carte de gestion réseau pour définir le périphérique InfraStruXure comme destinataire des traps.



Pour des informations détaillées sur l'amélioration et la gestion de la sécurité de votre système, consultez le *Manuel de sécurité* disponible sur le CD d'*utilitaires* de la carte de gestion réseau et sur le site Web, **www.apc.com**.

SNMPv1

Chemin d'accès : Administration > Réseau > SNMPv1 > *options*

Option	Description
accès	**Activer l'accès SNMPv1 :** active SNMP version 1 comme méthode de communication avec ce périphérique.
contrôle d'accès	Vous pouvez configurer jusqu'à quatre entrées de contrôle d'accès pour spécifier les systèmes de gestion réseau (NMS) ayant accès à ce périphérique. Par défaut, la page d'ouverture du contrôle d'accès attribue une entrée à chacune des quatre communautés SNMPv1 disponibles. Vous pouvez toutefois modifier ces paramètres pour attribuer plus d'une entrée à une communauté afin de permettre l'accès par plusieurs adresses, noms d'hôtes ou masques d'adresse IP IPv4 et IPv6 spécifiques. Pour modifier les paramètres de contrôle d'accès pour une communauté, cliquez sur le nom de la communauté. • Si l'entrée du contrôle d'accès par défaut d'une communauté est inchangée, cette communauté a accès à ce périphérique depuis n'importe quel emplacement sur le réseau. • Si vous configurez plusieurs entrées de contrôle d'accès pour un seul nom de communauté, la limite de quatre entrées impose qu'une des autres communautés ou plusieurs n'aient aucune entrée de contrôle d'accès. Si aucune entrée de contrôle d'accès n'est répertoriée pour une communauté, celle-ci n'a pas accès à ce périphérique. **Nom de communauté :** nom que doit utiliser un système NMS pour accéder à la communauté. La longueur maximum est de 15 caractères ASCII et les noms par défaut des communautés sont `public`, `private`, `public2` et `private2`. **IP NMS/Nom d'hôte :** adresse IPv4 ou IPv6, masque de l'adresse IP ou nom d'hôte qui contrôle l'accès par les NMS. Un nom d'hôte ou une adresse IP spécifique (telle que 149.225.12.1) permet uniquement l'accès du NMS à cet emplacement précis. Les adresses IP contenant 255 limitent l'accès de la manière suivante : • 149.225.12.**255** : accès uniquement par un NMS sur le segment 149.225.12. • 149.225.**255.255** : accès uniquement par un NMS sur le segment 149.225. • 149.**255.255.255** : accès uniquement par un NMS sur le segment 149. • 0.0.0.0 (paramètre par défaut) que l'on peut aussi exprimer sous la forme 255.255.255.255 : accès par tous les NMS sur tous les segments. **Type d'accès** : actions qu'un NMS peut effectuer par l'intermédiaire de la communauté. • **Lire** : commandes GET uniquement, à tout moment. • **Écrire** : commandes GET à tout moment, commandes SET lorsqu'aucun utilisateur n'est connecté à l'interface Web ni à l'interface par lignes de commande. • **Écrire+** : commandes GET et SET à tout moment. • **Désactiver** : Aucune commande GET ni SET, à aucun moment.

SNMPv3

Chemin d'accès : Administration > Réseau > SNMPv3 > *options*

Pour les destinataires de commandes GET, SET et de traps SNMP, SNMPv3 utilise un système de profils pour identifier les utilisateurs. Un utilisateur SNMPv3 doit avoir un profil utilisateur assigné dans le logiciel MIB pour effectuer des GET et des SET, naviguer dans la MIB et recevoir des traps.

Remarque : pour utiliser SNMPv3, vous devez avoir un programme MIB compatible SNMPv3.

La carte de gestion réseau prend en charge l'authentification SHA ou MD5 et le codage AES ou DES.

Option	Description
accès	**Accès SNMPv3 :** permet d'activer SNMPv3 comme méthode de communication avec ce périphérique.
profils utilisateur	Répertorie par défaut les paramètres de quatre profils utilisateurs, configurés avec les noms d'utilisateurs **apc snmp profile1** à **apc snmp profile4** et sans authentification ni confidentialité (pas de codage). Pour modifier les paramètres suivants d'un profil utilisateur, cliquez sur un nom d'utilisateur dans la liste. **Nom d'utilisateur :** identifiant du profil utilisateur. SNMP version 3 mappe les commandes GET, SET et les traps vers un profil utilisateur en vérifiant la correspondance entre le nom d'utilisateur du profil et celui présent dans le paquet de données transmis. Un nom d'utilisateur peut contenir jusqu'à 32 caractères ASCII. **Phrase secrète d'authentification :** phrase de 15 à 32 caractères ASCII (par défaut `apc auth passphrase`) qui permet de vérifier que le NMS en communication avec le périphérique par protocole SNMPv3 est bien le NMS qu'il dit être, que le message n'a pas été modifié au cours de la transmission, et que le message a été communiqué en temps utile, indiquant qu'il n'a subi aucun retard et qu'il n'a pas été copié puis renvoyé ultérieurement à une heure inappropriée. **Phrase secrète de confidentialité :** phrase de 15 à 32 caractères ASCII (par défaut `apc crypt passphrase`) qui garantit la confidentialité des données (par l'intermédiaire d'un codage) envoyées par un NMS à ce périphérique ou reçues depuis ce périphérique par protocole SNMPv3. **Protocole d'authentification :** l'implémentation du protocole SNMPv3 prend en charge les authentifications SHA et MD5. L'authentification n'interviendra que si un protocole d'authentification est sélectionné. **Protocole de confidentialité :** l'implémentation du protocole SNMPv3 prend en charge les protocoles AES et DES comme protocoles de codage et de décodage des données. La confidentialité des données transmises nécessite qu'un protocole de confidentialité soit sélectionné et qu'une phrase secrète de confidentialité soit fournie dans la requête provenant du NMS. Lorsqu'un protocole de confidentialité est activé mais que le NMS ne fournit pas de phrase secrète de confidentialité, la requête SNMP n'est pas codée. **REMARQUE :** vous ne pouvez pas sélectionner le protocole de confidentialité si aucun protocole d'authentification n'est sélectionné.

Option	Description
contrôle d'accès	Vous pouvez configurer jusqu'à quatre entrées de contrôle d'accès pour spécifier les NMS ayant accès à ce périphérique. Par défaut, la page d'ouverture du contrôle d'accès attribue une entrée à chacun des quatre profils utilisateurs. Vous pouvez toutefois modifier ces paramètres pour attribuer plus d'une entrée à un profil utilisateur afin de permettre l'accès par plusieurs adresses IP, noms d'hôtes ou masques d'adresse IP spécifiques. • Si l'entrée de contrôle d'accès par défaut d'un profil utilisateur est inchangée, tous les NMS utilisant ce profil ont accès à ce périphérique. • Si vous configurez plusieurs entrées de contrôle d'accès pour un seul profil utilisateur, la limite de quatre entrées impose qu'un des autres profils utilisateurs ou plusieurs n'aient aucune entrée de contrôle d'accès. Si aucune entrée de contrôle d'accès n'est répertoriée pour un profil utilisateur, aucun NMS utilisant ce profil n'a accès à ce périphérique. Pour modifier les paramètres de contrôle d'accès pour un profil utilisateur, cliquez sur son nom d'utilisateur. **Accès :** cochez la case **Activer** pour activer la contrôle d'accès spécifié par les paramètres de cette entrée de contrôle d'accès. **Nom d'utilisateur :** sélectionnez dans la liste déroulante le profil utilisateur auquel ce contrôle d'accès va s'appliquer. Les choix possibles sont les quatre noms d'utilisateurs que vous configurez par l'intermédiaire de l'option **profils utilisateurs** du menu de navigation gauche. **IP NMS/Nom d'hôte :** adresse IP, masque de l'adresse IP ou nom d'hôte qui contrôle l'accès par les NMS. Un nom d'hôte ou une adresse IP spécifique (telle que 149.225.12.1) permet uniquement l'accès du NMS à cet emplacement précis. Un masque d'adresse IP contenant la valeur 255 limite l'accès de la manière suivante : • 149.225.12.**255** : accès uniquement par un NMS sur le segment 149.225.12. • 149.225.**255.255** : accès uniquement par un NMS sur le segment 149.225. • 149.**255.255.255** : accès uniquement par un NMS sur le segment 149. • 0.0.0.0 (paramètre par défaut) que l'on peut aussi exprimer sous la forme 255.255.255.255 : accès par tous les NMS sur tous les segments.

Modbus

Chemin d'accès : Administration > Réseau > Modbus > tcp

Permet d'activer ou de désactiver l'accès au Modbus TCP en cochant ou en décochant la case **Activer**.

La zone **Port** permet de spécifier le port sur lequel Modbus TCP fournit le service.

Serveur FTP

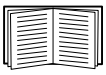
Chemin d'accès : Administration > Réseau > Serveur FTP

Les paramètres de **Serveur FTP** permettent d'activer (par défaut) ou de désactiver l'accès au serveur FTP et de spécifier le port TCP/IP (port 21 par défaut) que le serveur FTP utilise pour communiquer avec la carte de gestion réseau. Le serveur FTP utilise à la fois le port du numéro spécifié et celui du numéro immédiatement inférieur.

Vous pouvez remplacer le paramètre **Port** par le numéro d'un port inutilisé quelconque entre 5001 et 32768, afin de fournir une sécurité supplémentaire. Les utilisateurs doivent alors utiliser le signe deux points (:) pour spécifier le numéro de port autre que par défaut. Par exemple, pour le port 5001 et l'adresse IP 152.214.12.114, la commande serait `ftp 152.214.12.114:5001`.

Remarque : FTP permet de transférer les fichiers sans codage. Pour une plus haute sécurité, désactivez le serveur FTP et transférez les fichiers avec le protocole SCP. Sélectionner et configurer Secure SHell (SSH) active automatiquement le protocole SCP.

Dès lors que vous souhaitez qu'un onduleur soit accessible pour être géré par InfraStruXure Central, le paramètre Serveur FTP doit être activé dans l'interface de la carte de gestion réseau de cet onduleur.



Pour des informations détaillées sur l'amélioration et la gestion de la sécurité de votre système, consultez le *Manuel de sécurité* disponible sur le CD d'*utilitaires* de la carte de gestion réseau et sur le site Web.

Administration : Notification

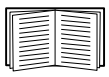
Actions sur les événements

Chemin d'accès : Administration > Notification > Actions sur les événements > *options*

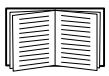
Types de notification

Vous pouvez configurer des actions sur les événements en réaction à un événement ou un groupe d'événements. Ces actions envoient une notification aux utilisateurs de différentes manières :

- Notification active et automatique. Les utilisateurs ou les services de surveillance spécifiés sont contactés directement.
  - Notification par e-mail
  - Traps SNMP
  - Service de surveillance à distance
  - Notification Syslog
- Notification indirecte
  - Journal de consignation des événements. Si aucune notification directe n'est configurée, les utilisateurs doivent consulter le journal de consignation des événements pour savoir lesquels se sont produits.

    Vous pouvez aussi consigner au journal les données de performances à utiliser pour la surveillance du périphérique. Voir « Journal de consignation des données » en page 61 pour obtenir des informations sur la configuration et l'utilisation de cette option de consignation des données.
  - Requêtes (SNTP et GET)

    Pour de plus amples informations, reportez-vous à la section « SNMP » en page 79. Le protocole SNMP permet à un NMS d'exécuter des requêtes d'information. En SNMPv1, qui ne crypte pas les données avant la transmission, configurer le type d'accès SNMP le plus restreint (en lecture) permet d'utiliser des requêtes d'information sans risque d'autoriser des modifications de configuration à distance.

La carte de gestion réseau accepte l'utilisation du **MIB RFC1628** (Management Information Base). Voir “Traps SNMP” pour des informations sur la configuration d'un récepteur de traps. Le groupe de trois événements **1628 MIB** fonctionne uniquement avec ce MIB mais pas avec le MIB Powernet alternatif. Ils peuvent être configurés comme n'importe quel événement (voir “Configuration des actions sur les événements” ci-dessous).

Configuration des actions sur les événements

Paramètres de notification. Pour les événements auxquels un événement d'arrêt est associé, vous pouvez aussi définir les paramètres suivants en configurant les événements individuellement ou par groupe, selon les explications indiquées dans les deux sections qui suivent. Pour accéder à ces paramètres, cliquez sur le nom du récepteur ou du destinataire.

Paramètre	Description
Délai de *X* avant envoi	Si l'événement persiste pendant le temps spécifié, une notification est envoyée. Si la condition disparaît avant l'expiration du délai, aucune notification n'est envoyée.

Paramètre	Description
Répéter tou(te)s les *X*	La notification est envoyée selon la période indiquée (ex. : toutes les 2 minutes).
Jusqu'à *X* fois	Tant que l'événement est actif, la notification est répétée autant de fois qu'indiqué.
Jusqu'à ce que la condition disparaisse	La notification est envoyée en répétition jusqu'à ce que la condition disparaisse ou soit corrigée.

Configuration par événement. Pour définir les actions sur les événements pour un événement individuel :

1. Sélectionnez l'onglet **Administration**, **Notification** dans la barre de menu supérieure, puis **par événement** sous **Actions sur les événements** dans le menu de navigation gauche.
2. Dans la liste d'événements, vérifiez les colonnes marquées pour savoir si l'action qui vous intéresse est déjà configurée (par défaut, la consignation au journal est configurée pour tous les événements).
3. Pour consulter ou modifier la configuration actuelle (par exemple la notification des destinataires par e-mail ou appel téléphonique, ou la notification des systèmes de gestion réseau (NMS) par traps SNMP, cliquez sur le nom de l'événement.

Remarque : si aucun serveur Syslog n'est configuré, les éléments qui concernent la configuration Syslog ne s'affichent pas.

Lorsque les détails de configuration d'un événement sont affichés, vous pouvez modifier cette configuration, activer ou désactiver la consignation des événements ou la notification Syslog, ou encore désactiver la notification pour des destinataires par e-mail ou des récepteurs de traps spécifiques, mais vous ne pouvez pas ajouter ou supprimer de destinataires ou de récepteurs. Pour ajouter ou supprimer des destinataires ou des récepteurs, consultez les sections suivantes :

• « Identification de serveurs Syslog » en page 90

• « destinataires des e-mails » en page 87

• « Récepteurs de traps » en page 88

Configuration par groupe. Pour configurer simultanément un groupe d'événements :

1. Sélectionnez l'onglet **Administration**, **Notification** dans la barre de menu supérieure, puis **par groupe** sous **Actions sur les événements** dans le menu de navigation gauche.
2. Choisissez comment grouper les événements à configurer :
   – Sélectionnez **Événements par gravité**, puis sélectionnez tous les événements pour un ou plusieurs niveaux de gravité. Vous ne pouvez pas modifier la gravité d'un événement.
   – Sélectionnez **Événements par catégorie**, puis sélectionnez tous les événements pour une ou plusieurs catégories définies.
3. Cliquez sur **Suivant>>** pour changer de page afin d'effectuer les actions suivantes :
   a. Sélectionner les actions sur les événements pour le groupe d'événements.
      • Pour sélectionner une action autre que **Consignation** (action par défaut), il faut d'abord qu'au moins un destinataire ou un récepteur concerné soit configuré.
      • Si vous sélectionnez **Consignation** en ayant configuré un serveur Syslog, sélectionnez **Journal de consignation des événements** ou **Syslog** (voire les deux) dans la page suivante.
   b. Sélectionnez l'option de laisser activée la nouvelle action sur les événements configurée pour ce groupe d'événements, ou bien de la désactiver.

Notification directe active et automatique

Notification par e-mail

Présentation de la configuration. Utilisez le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des e-mails à quatre destinataires maximum lorsqu'un événement se produit.

Pour utiliser la fonction E-mail vous devez configurer les paramètres suivants :

- L'adresse IP du serveur de noms de domaines (DNS) principal et, en option, du serveur secondaire. (Voir « DNS » en page 74.)
- L'adresse IP ou le nom DNS du **Serveur SMTP** et l'**Adresse de l'expéditeur**. (Voir « SMTP » en page 87.)
- L'adresse de messagerie de quatre destinataires maximum. (Voir « destinataires des e-mails » en page 87.)

Vous pouvez utiliser le paramètre **Adresse du destinataire** de l'option **destinataires** pour envoyer l'e-mail à un pager en mode texte.

SMTP.

Chemin d’accès : Administration > Notification > E-mail > serveur

Paramètre	Description
Serveur SMTP local	Adresse IPv4/ IPv6 ou nom DNS du serveur SMTP local. **REMARQUE :** cette définition est uniquement requise lorsqu'un **serveur SMTP** et défini comme **Local**. Voir « destinataires des e-mails » en page 87.
Adresse de l''expéditeur	Contenu du champ **De** des e-mails envoyés par la carte de gestion réseau : • au format *utilisateur@* [*adresse_IP*] (si une adresse IP est spécifiée en **Serveur SMTP local**) • au format *utilisateur@* [*domaine*] (si un DNS est configuré et que son nom DNS est spécifié en **Serveur SMTP local**) dans les e-mails. **REMARQUE :** le serveur SMTP local peut nécessiter l’utilisation d’un compte utilisateur valide sur le serveur pour ce paramètre. Voir la documentation du serveur.

destinataires des e-mails.

Chemin d’accès : Administration > Notification > E-mail > destinataires

Identifiez un maximum de quatre destinataires d'e-mails.

Paramètre	Description
Adresse du destinataire	Nom d’utilisateur et de domaine du destinataire. Pour envoyer un e-mail à un pager, utilisez l’adresse de messagerie du compte de passerelle du pager du destinataire concerné (par exemple : `myacct100@skytel.com`). La passerelle du pager génèrera la page. Pour contourner la recherche du serveur DNS de l'adresse IP du serveur de messagerie, indiquez l'adresse IP entre crochets au lieu du nom de domaine (ex. : utilisez jdupont@[xxx.xxx.x.xxx] au lieu de jdupont@societe.com. Cette indication est utile lorsque la recherche de serveur DNS ne fonctionne pas correctement. **Remarque :** le pager du destinataire doit être compatible avec une messagerie textuelle.
Génération d'e-mails	Active (par défaut) ou désactive l’envoi d'e-mail au destinataire.

Paramètre	Description
Serveur SMTP	Sélectionnez l'une des options suivantes de routage des e-mails : • **Local** : par le serveur SMTP de la carte de gestion réseau. Ce paramètre (recommandé) assure l'envoi de l'e-mail avant les 20 secondes de délai de temporisation de la carte de gestion réseau, avec plusieurs nouvelles tentatives si nécessaire. Configurez aussi les éléments suivants : • Activez le transfert au serveur SMTP de la carte de gestion réseau pour qu'il puisse exécuter le routage des e-mails vers des serveurs SMTP externes. En général, les serveurs SMTP ne sont pas configurés pour transférer les e-mails. Consultez votre administrateur réseau (gestion du serveur SMTP) avant de modifier la configuration de votre serveur SMTP pour autoriser les transferts. • Configurez un compte de messagerie spécial pour que la carte de gestion réseau transfère les e-mails vers un compte de messagerie externe. • **Destinataire** : directement par le serveur SMTP du destinataire. Avec ce paramètre, la carte de gestion réseau tente d'envoyer l'e-mail une seule fois. Si le serveur SMTP distant est très actif, le délai de temporisation risque d'empêcher l'envoi de certains e-mails. Lorsque le destinataire utilise le même serveur SMTP que la carte de gestion réseau, ce paramètre n'a aucun effet.
Format	Le format long contient le nom, l'emplacement, le contact, l'adresse IP, le numéro de série du périphérique, la date et l'heure, le code d'événement et la description de l'événement. Le format court ne fournit que la description de l'événement.
Langue	Permet de sélectionner une langue dans la liste déroulante pour l'envoi des e-mails. Il est possible d'utiliser différentes langues selon les utilisateurs.
Nom d'utilisateur Mot de passe Confirmez votre mot de passe	Si votre serveur de messagerie requiert une authentification, entrez votre nom d'utilisateur et votre mot de passe ici. Cette authentification est simple et non SSI.

Test d'E-mail.

Chemin d'accès : Administration > Notification > E-mail > test

Permet d'envoyer un message de test à un destinataire configuré.

Traps SNMP

Récepteurs de traps.

Chemin d'accès : Administration > Notification > Traps SNMP > récepteurs de trap

Affiche les récepteurs de traps par IP NMS/Nom d'hôte. Vous pouvez configurer jusqu'à six récepteurs de traps.

- Pour configurer un nouveau récepteur de traps, cliquez sur **Ajouter récepteur de trap**.
- Pour modifier ou supprimer un récepteur de traps, cliquez d'abord sur son adresse IP ou son nom d'hôte pour accéder à ses paramètres (si vous supprimez un récepteur de traps, tous les paramètres de notification configurés en Actions sur les événements pour ce récepteur de traps reprennent leur valeur par défaut).

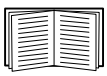
- Pour spécifier le type de trap pour un récepteur de traps, sélectionnez le bouton d'option SNMPv1 ou SNMPv3. Pour qu'un NMS reçoive les deux types de traps, vous devez configurer deux récepteurs de traps pour lui (un pour chaque type).

Élément	Définition
Génération de trap	Active (par défaut) ou désactive la génération de traps pour ce récepteur de traps.
Génération de traps Powernet MIB/ Génération de traps RFC1628	Sélectionnez l'un de ces deux types de génération de traps MIB pour chaque trap créé. Le type RFC 1628 correspond au MIB générique standard pour les onduleurs. L'option Powernet, personnalisée pour Schneider Electric, comporte de nombreuses variables supplémentaires adaptées aux produits de cette entreprise. Si vous utilisez le MIB RFC1628, vous pouvez aussi utiliser les trois notifications d'événements RFC1628 (voir “Actions sur les événements”). Ces notifications permettent d'éviter de configurer les événements à notifier hors de l'environnement de la carte de gestion réseau (voir le MIB RFC1628).
IP NMS/Nom d'hôte	Adresse IPv4/ IPv6 ou nom d'hôte du récepteur de traps. La valeur par défaut 0.0.0.0 laisse le récepteur de traps non défini.
Langue	Sélectionnez une langue dans la liste déroulante. Cette langue peut être différente de celle de l'interface utilisateur et de celle d'autres récepteurs de traps.

Option SNMPv1.

Élément	Définition
Nom de communauté	Nom (`public` par défaut) utilisé comme identifiant lorsque des traps SNMPv1 sont envoyés à ce récepteur de traps.
Authentifier les traps	Lorsque cette option est activée (par défaut), le NMS identifié par le paramètre IP NMS/Nom d'hôte reçoit des traps d'authentification (traps générés en cas de tentatives non valides de connexion au périphérique). Pour désactiver cette possibilité, décochez cette case.

Option SNMPv3. Sélectionnez l'identifiant du profil utilisateur pour ce récepteur de traps (pour afficher les paramètres des profils utilisateurs identifiés par les noms d'utilisateurs que vous pouvez sélectionner ici, cliquez sur **Réseau** dans la barre de menu supérieure et sur **profils utilisateurs** sous **SNMPv3** dans le menu de navigation gauche).



Voir « SNMPv3 » en page 80 pour plus d'informations sur la création de profils utilisateurs et la sélection de méthodes d'authentification et de cryptage.

Test de traps SNMP

Chemin d’accès : Administration > Notification > Traps SNMP > test

Résultat du dernier test. Résultat du plus récent test de trap SNMP. Un test de trap réussi confirme uniquement qu'un trap a été envoyé ; il ne confirme pas que ce trap a bien été reçu par le récepteur de trap sélectionné. Un test de trap est réussi si l'un des cas suivants est vrai :

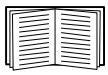
- La version SNMP (SNMPv1 ou SNMPv3) configurée pour le récepteur de trap sélectionné est activée sur le périphérique.
- Le récepteur de trap est activé.
- Si un nom d'hôte est sélectionné en adresse **À**, ce nom d'hôte peut être mis en correspondance avec une adresse IP valide.

À Sélectionnez l'adresse IP ou le nom d'hôte auquel un test de trap SNMP sera envoyé. Si aucun récepteur de trap n'est configuré, un lien vers la page de configuration de **Récepteur de trap** s'affiche.

Service de surveillance à distance

Chemin d’accès : Administration > Notification > Surveillance à distance

Le service de surveillance à distance (service RMS) est un service en option qui permet de surveiller votre système depuis un centre de traitement distant 24 heures sur 24, 7 jours sur 7, et de vous envoyer des notifications pour les événements qui surviennent sur vos périphériques et votre système.



Pour souscrire au service RMS, veuillez contacter votre distributeur ou cliquer sur le lien dans la partie supérieure de cet écran : **Site Web du service de surveillance à distance**.

Inscription. Pour activer le service RMS pour la carte de gestion réseau, sélectionnez **Activer le service de surveillance à distance**, activez au choix le bouton d'option **Enregistrer la société et le périphérique** ou **Enregistrer le périphérique uniquement**, remplissez le formulaire et cliquez sur **Send RMS Registration**.

La case à cocher **Réinitialiser l'enregistrement auprès du service de surveillance à distance**permet d'interrompre ce service à titre temporaire ou définitif (par exemple si vous déplacez une carte de gestion réseau).

Syslog

Chemin d’accès : Journaux de consignation > Syslog > *options*

La carte de gestion réseau peut envoyer des messages à quatre serveurs Syslog au maximum lorsqu'un événement se produit. Les serveurs Syslog enregistrent les événements qui se produisent sur les périphériques du réseau dans un journal de consignation qui fournit un enregistrement centralisé de ces événements.

Le présent guide d’utilisation ne décrit pas Syslog ni les valeurs de configuration de Syslog en détail. Pour de plus amples informations concernant Syslog, consultez **RFC3164**.

Identification de serveurs Syslog.

Chemin d’accès : Journaux de consignation > Syslog > serveurs

Paramètre	Définition
Serveur Syslog	Utilise des adresses IPv4/ IPv6 ou des noms d'hôtes pour identifier jusqu'à quatre serveurs devant recevoir les messages Syslog envoyés par la carte de gestion réseau.
Port	Port UDP (user datagram protocol) que la carte de gestion réseau utilisera pour envoyer des messages Syslog. La valeur par défaut est **514** (numéro du port UDP attribué à Syslog).
Protocole	Choisissez le protocole UDP ou TCP.
Langue	Choisissez la langue à utiliser pour les messages Syslog.

Paramètres Syslog.

Chemin d’accès : Journaux de consignation > Syslog > paramètres

Paramètre	Définition
Génération de messages	Active (par défaut) ou désactive la fonction Syslog.
Code site	Sélectionne le code site attribué aux messages Syslog de la carte de gestion réseau (**Utilisateur**, par défaut). **REMARQUE : Utilisateur** définit le mieux les messages Syslog envoyés par la carte de gestion réseau. **Ne modifiez pas** cette sélection, sauf en cas de conseil en ce sens de la part de l'administrateur du réseau Syslog ou de votre administrateur réseau.
Mise en correspondance de gravité	Fait correspondre chaque niveau de gravité des événements de la carte de gestion réseau ou de l'environnement avec les priorités Syslog disponibles. Il ne devrait pas être nécessaire de modifier ces paramètres. Les définitions suivantes sont celles de RFC3164 : • **Urgence** : le système est inutilisable. • **Alerte** : une action doit intervenir immédiatement. • **Critique** : conditions critiques. • **Erreur** : conditions d’erreur. • **Avertissement** : conditions d’avertissement. • **Remarque** : conditions normales mais à surveiller. • **Info** : messages d’information. • **Débogage** : messages de débogage. Voici les paramètres par défaut correspondant aux paramètres **Local Priority** : • **Grave** correspond à **Critique**. • **Avertissement** correspond à **Avertissement**. • **Informatif** correspond à **Info**. **REMARQUE :** Pour désactiver les messages Syslog, consultez la section « Configuration des actions sur les événements » en page 83.

Test Syslog et exemple de format.

Chemin d’accès : Journaux de consignation > Syslog > test

Envoie un message de test aux serveurs Syslog configurés dans l'option **serveurs**.

1. Sélectionnez la gravité à attribuer au message de test.
2. Définissez le message de test selon les champs de message requis :
   – Priorité (PRI) : priorité Syslog attribuée à l’événement objet du message, et code site des messages envoyés par la carte de gestion réseau.
   – En-tête : horodatage et adresse IP de la carte de gestion réseau.
   – Partie message (MSG) :
      • Le champ TAG suivi du signe deux points et d'un espace identifie le type d'événement.
      • Le champ CONTENT porte le texte de l’événement, suivi (en option) par un espace et le code de l’événement.

      Par exemple, `APC: Test Syslog` valide.

Administration : Options Généralités

Identification

Chemin d'accès : Administration > Généralités > Identification

Permet de définir le **Nom** (nom du périphérique), l'**Emplacement** (emplacement physique) et le **Contact** (personne responsable du périphérique) utilisés par InfraStruXure Central, InfraStruXure Manager et l'agent SNMP de la carte de gestion réseau. Ces paramètres sont les valeurs de **sysName**, **sysContact** et **sysLocation** utilisées pour les OID (identifications d'objets) MIB-II.

Pour plus d'informations sur les OID MIB-II, consultez le *Guide de référence de la base de données MIB PowerNet*®, disponible sur le CD d'*utilitaires* de la carte de gestion réseau et sur le site, **www.apc.com**.

Les zones **Nom** et **Emplacement** identifient également le périphérique lorsque vous vous enregistrez au service de surveillance à distance. Consultez « Service de surveillance à distance » en page 90 pour plus d'informations.

Réglage de la date et de l'heure

Mode

Chemin d'accès : Administration > Généralités > Date/heure > mode

Permet de configurer la date et l'heure utilisées par la carte de gestion réseau. Vous pouvez modifier les paramètres actuels manuellement ou par l'intermédiaire d'un serveur NTP (Network Time Protocol) :

- **Mode manuel** : utilisez l'une de ces méthodes :
  - Entrez la date et l'heure de la carte de gestion réseau.
  - Cochez la case **Appliquer l'heure système local** pour que les paramètres de date et d'heure correspondent à ceux de l'ordinateur que vous utilisez.
- **Synchroniser avec le serveur NTP** : un serveur NTP définit la date et l'heure pour la carte de gestion réseau.

Remarque : par défaut, toute carte de gestion réseau du côté privé d'un système InfraStruXure Central obtient ses paramètres d'heure en utilisant InfraStruXure Central comme serveur NTP.

Paramètre	Définition
Serveur NTP primaire	Entrez l'adresse IP ou le nom de domaine du serveur NTP primaire.
Serveur NTP secondaire	Entrez l'adresse IP ou le nom de domaine du serveur NTP secondaire, le cas échéant.
Fuseau horaire	Permet de sélectionner un fuseau horaire. Le nombre d'heures qui précède chaque fuseau horaire dans la liste correspond au décalage par rapport au temps universel coordonné (UTC), anciennement intitulé Heure du méridien de Greenwich (GMT).
Fréquence de mise à jour	Définit à quelle fréquence (en heures) la carte de gestion réseau accède au serveur NTP pour effectuer une mise à jour. *Au minimum* : 1; *au maximum* : 8760 (1 an).

Paramètre	Définition
Mettre à jour avec NTP	Permet de lancer une mise à jour immédiate de la date et de l'heure par l'intermédiaire du serveur NTP.

Heure d'été

Chemin d'accès : Administration > Généralités > Date/heure > heure d'été

Permet d'activer l'heure d'été traditionnelle des États-Unis (DST), ou d'activer et de configurer une heure d'été personnalisée correspondant à celle de votre zone géographique. L'heure DST est désactivée par défaut.

Personnalisation de l'heure d'été traditionnelle des États-Unis (DST) :

- Si l'heure DST locale débute ou finit toujours à la quatrième occurrence d'un jour de semaine spécifique d'un mois (par exemple le quatrième dimanche), sélectionnez **Quatrième/Dernier**. Dans les années qui suivent, si ce mois comprend éventuellement un cinquième dimanche, le paramètre d'heure change tout de même le quatrième dimanche.
- Si l'heure DST locale débute ou finit toujours à la dernière occurrence d'un jour de semaine spécifique d'un mois, que cette occurence soit la quatrième ou la cinquième, sélectionnez **Cinquième/Dernier**.

Format

Chemin d'accès : Administration > Généralités > Date et heure > format de la date

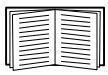
Sélectionne le format numérique auquel toutes les dates seront affichées dans l'interface utilisateur. Chaque lettre de ces formats (m pour mois, d pour jour et y pour année) représente un chiffre. Les jours et les mois calendaires à un seul chiffre sont affichés en deux chiffres commençant par un zéro.

Utilisation d'un fichier .ini

Chemin d'accès : Administration > Généralités > Fichier de configuration utilisateur

Permet d'utiliser les paramètres d'une carte de gestion réseau pour en configurer une autre. Récupérez le fichier config.ini de la carte de gestion réseau configurée, personnalisez ce fichier (par exemple en modifiant l'adresse IP) et téléchargez-le sur la nouvelle carte de gestion réseau. Le nom du fichier peut contenir jusqu'à 64 caractères et doit avoir l'extension .ini.

État	Progression du téléchargement. Le téléchargement réussit même si le fichier contient des erreurs ; dans ce cas, un événement système signale les erreurs dans le journal de consignation des événements.
Télécharger	Naviguez jusqu'au fichier personnalisé et téléchargez-le afin que la carte de gestion réseau l'utilise pour effectuer sa propre configuration.



Pour récupérer le fichier d'une carte de gestion réseau configurée et le personnaliser, consultez « Exportation des paramètres de configuration » en page 99.

Au lieu de télécharger le fichier sur une seule carte de gestion réseau, vous pouvez l'exporter vers plusiers cartes de gestion réseau en utilisant un script FTP ou SCP ou un fichier de commandes, et l'utilitaire de fichier .ini, disponible à l'adresse **www.apc.com/tools/download**.

Journal de consignation des événements, unités de température, langue et page de connexion

Chemin d'accès : Administration > Généralités > Préférences

Code couleur du journal de consignation des événements

Cette option est désactivée par défaut. Cochez la case Activer de l'option **Code couleur du journal de consignation des événements** pour activer le codage couleur du texte d'alarme enregistré dans le journal de consignation des événements. Les entrées d'événements système et de modifications de la configuration ne changent pas de couleur.

Couleur du texte	Gravité de l'alarme
Rouge	**Critique** : une alarme critique existe et nécessite une action immédiate.
Orange	**Avertissement** : une alarme nécessite votre attention et pourrait mettre en péril vos données ou votre équipement si le problème n'est pas corrigé.
Vert	**Alarm Cleared** : les conditions ayant déclenché l'alarme se sont améliorées.
Noir	**Normal :** aucune alarme. La carte de gestion réseau et tous les périphériques connectés fonctionnent normalement.

Modification de l'échelle de température par défaut

Sélectionnez l'échelle de température (Fahrenheit ou Celsius) dans laquelle s'afficheront les mesures de température dans cette interface utilisateur.

Spécification de la langue de l'interface utilisateur

Vous pouvez spécifier la langue par défaut de l'interface utilisateur dans le champ **Langue**. Vous pouvez aussi effectuer cette opération lors de votre connexion. Sélectionnez l'une des langues affichées dans la liste déroulante.

Remarque : vous pouvez également spécifier différentes langues pour les destinataires d'e-mails et les récepteurs de traps SNMP. Consultez « destinataires des e-mails » en page 87 et « Récepteurs de traps » en page 88.

Spécification d'une page de connexion par défaut

Permet de configurer la page Web qui s'affiche par défaut lorsque vous vous connectez.

Réinitialisation de la carte de gestion réseau

Chemin d'accès : Administration > Généralités > Réinitialiser/Redémarrer

Action	Définition
Redémarrer l'interface de gestion	Redémarre l'interface de la carte de gestion réseau.
Réinitialiser tout[1]	Décochez la case **Exclure TCP/IP** pour réinitialiser tous les paramètres de configuration ; cochez la case **Exclure TCP/IP** pour réinitialiser tous les paramètres sauf le paramètre TCP/IP.
Réinitialiser uniquement[1]	**TCP/IP** : cette option permet de définir la configuration TCP/IP sur **DHCP & BOOTP** (paramètre par défaut), qui requiert que la carte de gestion réseau reçoive ses paramètres TCP/IP d'un serveur DHCP ou BOOTP. Voir « Paramètres TCP/IP et de communication » en page 70.
	Configuration de l'événement : toutes les modifications de configuration des événements, par événement et par groupe, sont rétablies à leurs paramètres par défaut.
	Restauration des valeurs par défaut de l'onduleur : rétablit les valeurs par défaut uniquement pour les paramètres de l'onduleur, pas pour les paramètres réseau.
	Alarmes de perte de communication environnementale : cette option efface toutes les alarmes environnementales déclenchées par une perte de communication avec un capteur externe. Par exemple si un capteur de température se déconnecte et déclenche ainsi une alarme, la réinitialisation des alarmes de perte de communication environnementale ramène l'état de cette alarme à l'état normal. **REMARQUE :** pour effacer les alarmes déclenchées par un capteur connecté au port de capteur universel d'une carte de gestion réseau AP9631, reconnectez le capteur ou redémarrez la carte de gestion réseau.
	Contrôle de la confidentialité : réinitialise les paramètres qui définissent la manière dont la carte de gestion réseau répond aux alarmes détectées au niveau de l'accessoire d'E/S à contact sec.
1. La réinitialisation peut prendre jusqu'à 1 minute. Le nom de l'onduleur n'est pas réinitialisé.	

Configuration des liens

Chemin d'accès : Administration > Généralités > Liens rapides

Sélectionnez l'onglet **Administration** puis **Généralités** dans la barre de menu supérieure, et **Liens rapides** dans le menu de navigation gauche afin de consulter et de modifier les liens URL affichés en bas à gauche de chaque page de l'interface.

Par défaut, ces liens donnent accès aux pages Web suivantes :

- **Link 1** : page d'accueil du site Web www.apc.com.
- **Link 2** : page qui permet d'utiliser des échantillons de produits en ligne.
- **Link 3** : page d'accueil du service de surveillance à distance.

Pour reconfigurer les liens ci-dessous, cliquez sur le nom du lien dans la colonne **Affichage** :

- **Affichage** : nom abrégé du lien affiché sur chaque page de l'interface.
- **Nom** : nom qui identifie entièrement la cible ou l'objet du lien
- **Adresse** : sous forme d'URL, par exemple l'URL d'un autre périphérique ou serveur.

À propos de la carte de gestion réseau

Chemin d'accès : Administration > Généralités > À propos de

Les informations relatives au matériel sont utiles au Service d'assistance pour résoudre les problèmes sur la carte de gestion réseau. Le numéro de série et l'adresse MAC figurent également sur la carte de gestion réseau elle-même.

Les informations relatives au microprogramme du module d'application, APC OS (AOS), et le contrôleur de démarrage de la carte de gestion réseau indiquent le nom, la version du microprogramme et la date et l'heure de création de chaque module du microprogramme. Ces informations sont également utiles pour le dépannage et permettent de savoir si une mise à jour de microprogramme est disponible sur le site Web.

Autonomie de gestion indique depuis combien de temps l'interface fonctionne de manière continue.

Assistant de configuration IP des équipements

Fonctionnalités, configuration requise et installation

Utilisation de l'assistant pour configurer les paramètres TCP/IP

L'assistant de configuration IP des équipements configure l'adresse IP, le masque de sous-réseau et la passerelle par défaut d'une ou plusieurs cartes de gestion réseau ou périphériques en réseau (périphériques équipés d'une carte de gestion réseau intégrée).

- À distance par l'intermédiaire du réseau TCP/IP afin de détecter et de configurer des cartes de gestion réseau ou des périphériques non configurés sur le même segment de réseau que celui de l'ordinateur où se trouve l'assistant.
- Par connexion directe entre un port série de votre ordinateur et une carte de gestion réseau ou un périphérique afin de les configurer ou reconfigurer.

Configuration minimale requise

L'assistant fonctionne sous les systèmes d'exploitation Microsoft Windows 2000, Windows Server® 2003 et Windows XP.

Installation

Installation de l'assistant à partir du CD d'*utilitaires* :

1. Si la fonction d'exécution automatique est activée, l'interface utilisateur s'affiche lorsque vous insérez le CD. Sinon, ouvrez le fichier **contents.htm** à partir du CD.
2. Cliquez sur **Device IP Configuration Wizard** (assistant de configuration IP des équipements) et suivez les instructions.

Installation de l'assistant à partir d'un fichier exécutable téléchargé :

1. Allez sur **www.apc/tools/download**.
2. Téléchargez l'assistant de configuration IP des équipements.
3. Lancez le fichier exécutable depuis le dossier dans lequel vous l'avez téléchargé.

Exportation des paramètres de configuration

Récupération et exportation du fichier .ini

Récapitulatif de la procédure

Un Administrateur peut récupérer le fichier .ini d'une carte de gestion réseau et l'exporter vers une autre carte de gestion réseau ou plusieurs.

1. Configurez une carte de gestion réseau avec les paramètres que vous souhaitez exporter.
2. Récupérez le fichier .ini de cette carte de gestion réseau.
3. Personnalisez le fichier en modifiant au moins les paramètres TCP/IP.
4. Utilisez un protocole de transfert de fichiers pris en charge par la carte de gestion réseau pour transférer une copie du fichier vers une carte de gestion réseau ou plusieurs. Pour un transfert vers plusieurs cartes de gestion réseau, utilisez un script FTP ou SCP, ou bien l'utilitaire de fichiers .ini.

Chaque carte de gestion réseau destinataire utilise le fichier pour reconfigurer ses propres paramètres, puis le supprime.

Contenu du fichier .ini

Le fichier config.ini que vous récupérez d'une carte de gestion réseau contient les informations suivantes :

- des *en-têtes de section* et des *mots-clés* (uniquement ceux pris en charge par le périphérique duquel provient le fichier récupéré) *:* les en-têtes de section sont des noms de catégories entre crochets ([ ]). Les mots-clés, sous chaque en-tête de section, sont des étiquettes qui décrivent les paramètres spécifiques de la carte de gestion réseau. Chaque mot-clé est suivi du signe « égal » et d'une valeur (valeur par défaut ou valeur configurée).
- le mot-clé pour `Override` : avec sa valeur par défaut, ce mot-clé interdit l'exportation d'un ou de plusieurs mots-clés et de leurs valeurs spécifiques vers le périphérique concerné. Par exemple dans la section `[NetworkTCP/IP]`, la valeur par défaut en `Override` (l'adresse MAC de la carte de gestion réseau) bloque l'exportation des valeurs `SystemIP`, `SubnetMask`, `DefaultGateway` et `BootMode`.

Procédures détaillées

Récupération. Pour configurer et récupérer un fichier .ini à exporter :

1. Si possible, utilisez l'interface d'une carte de gestion réseau pour configurer cette carte avec les paramètres à exporter. Modifier directement le fichier .ini risque d'introduire des erreurs.
2. Pour utiliser le protocole FTP afin de récupérer le fichier config.ini de la carte de gestion réseau configurée :
   a. Ouvrez une connexion avec la carte de gestion réseau en utilisant son adresse IP :

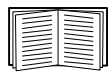
      ```
      ftp> open adresse_ip
      ```

b. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.

c. Récupérez le fichier config.ini contenant les paramètres de la carte de gestion réseau :

```
ftp> get config.ini
```

Le fichier est alors copié dans le dossier depuis lequel vous avez lancé le protocole FTP.



Pour récupérer les paramètres de configuration de plusieurs cartes de gestion réseau et les exporter vers d'autres cartes de gestion réseau, consultez *Release Notes: ini File Utility, version 1.0* (Notes de mise à jour : utilitaire pour fichier .ini, version 1.0) disponible sur le CD d'*utilitaires* de la carte de gestion réseau et à l'adresse **www.apc.com**.

Personnalisation. Avant d'exporter le fichier, vous devez le personnaliser.

1. Pour cela, utilisez un éditeur de texte.
   – Les en-têtes de section, les mots-clés et les valeurs prédéfinies ne sont pas sensibles à la casse, mais les valeurs de chaîne que vous définissez le sont.
   – Utilisez des guillemets accolés pour indiquer une absence de valeur. Par exemple, `LinkURL1=""` indique que l'URL est volontairement non définie.
   – Mettez entre guillemets toute valeur qui contient un espace à sa gauche ou à sa droite, ou qui est déjà entre guillemets.
   – Pour exporter des événements planifiés, configurez les valeurs directement dans le fichier .ini.
   – Pour exporter une heure système avec la plus grande précision possible, si les cartes de gestion réseau destinataires peuvent accéder à un serveur NTP, configurez le paramètre `NTPEnable` sur `enabled` (activé) :

     ```
     NTPEnable=enabled
     ```

     Vous pouvez aussi réduire le temps de transmission en exportant la section `[SystemDate/Time]` dans un fichier .ini séparé.
   – Pour ajouter des commentaires, commencez chaque ligne de commentaire par un point-virgule (`;`).
2. Copiez le fichier personnalisé dans le même dossier sous un nom différent :
   – Le nom du fichier peut contenir jusqu'à 64 caractères et doit avoir l'extension .ini.
   – Conservez le fichier personnalisé initial pour utilisation future. **Le fichier que vous conservez constitue le seul enregistrement de vos commentaires.**

Transfert du fichier vers une carte de gestion réseau unique. Pour transférer le fichier .ini vers une autre carte de gestion réseau, procédez selon l'une des méthodes suivantes :

- À partir de l'interface Web de la carte de gestion réseau destinataire, sélectionnez l'onglet **Administration** puis **Généralités** dans la barre de menu supérieure, enfin **Fichier de configuration utilisateur** dans le menu de navigation gauche. Entrez le chemin complet, ou utilisez la commande **Parcourir...**.
- Utilisez un protocole de transfert de fichiers pris en charge par les cartes de gestion réseau (FTP, Client FTP, SCP ou TFTP). Les exemples suivants utilisent le protocole FTP :
  a. Depuis le dossier contenant la copie du fichier .ini personnalisé, utilisez FTP pour vous connecter à la carte de gestion réseau vers laquelle vous exportez ce fichier :

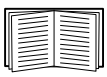
     ```
     ftp> open adresse_ip
     ```

b. Exportez le fichier .ini personnalisé vers le répertoire racine de la carte de gestion réseau de destination :

```
ftp> put nom_du_fichier.ini
```

Exportation du fichier vers plusieurs cartes de gestion réseau. Pour exporter le fichier .ini vers plusieurs cartes de gestion réseau :

- Utilisez FTP ou SCP, mais écrivez un script qui incorpore et répète les étapes utilisées pour exporter le fichier vers une carte de gestion réseau unique.
- Utilisez un fichier de traitement par lots et l'utilitaire de fichiers .ini.



Pour créer le fichier de lot et utiliser l'utilitaire, consultez *Release Notes: ini File Utility, version 1.0* (Notes de mise à jour : utilitaire pour fichier .ini, version 1.0) disponible sur le CD d'*utilitaires* de la carte de gestion réseau.

Événements de téléchargement et messages d'erreur

L'événement et ses messages d'erreurs

L'événement suivant survient quand la carte de gestion réseau destinataire achève l'utilisation du fichier .ini pour mettre à jour ses paramètres.

```
Téléchargement du fichier de configuration terminé avec nombre valeurs
valides.
```

Si un mot-clé, un nom de section ou une valeur est non valide, le téléchargement par la carte de gestion réseau destinataire réussit et un texte supplémentaire sur l'événement signale l'erreur.

Texte sur l'événement	Description
Avertissement au niveau du fichier de configuration : mot clé non valide à la ligne *numéro*. Avertissement au niveau du fichier de configuration : valeur non valide à la ligne *numéro*.	Toute ligne contenant un mot-clé ou une valeur non valide est ignorée.
Avertissement au niveau du fichier de configuration : section non valide à la ligne *numéro*.	Si un nom de section est non valide, toutes les paires de mots-clés/ valeurs de cette section sont ignorées.
Avertissement au niveau du fichier de configuration : un mot clé se trouve hors de la section à la ligne *numéro*.	Un mot-clé entré au début du fichier (c'est-à-dire avant tout en-tête de section) est ignoré.
Avertissement au niveau du fichier de configuration : le fichier de configuration dépasse la taille maximale.	Un fichier trop volumineux provoque un téléchargement incomplet. Réduisez la taille du fichier, ou divisez-le en deux fichiers et tentez de nouveau le téléchargement.

Messages dans le fichier config.ini

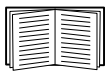
Un périphérique associé à la carte de gestion réseau depuis laquelle vous téléchargez le fichier config.ini file doit être détecté avec succès pour que sa configuration soit prise en compte. Si le périphérique (tel qu'un onduleur) est absent ou n'est pas détecté, le fichier config.ini contient un message sous le nom de section approprié, au lieu des mots-clés et des valeurs. Par exemple :

```
UPS not discovered

IEM not discovered
```

Si vous n'aviez pas l'intention d'exporter la configuration du périphérique comme partie de l'importation du fichier .ini file, ignorez ces messages.

Erreurs générées par les valeurs ignorées

Le mot-clé `Override` et sa valeur vont générer des messages d'erreur dans le journal de consignation des événements lorsqu'il bloque l'exportation des valeurs.

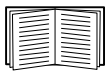


Consultez « Contenu du fichier .ini » en page 99 pour des informations sur les valeurs qui sont ignorées.

Les valeurs ignorées étant spécifiques à chaque périphérique et inappropriées pour l'exportation vers d'autres cartes de gestion réseau, ignorez ces messages d'erreur. Pour éviter ces messages d'erreur, supprimez les lignes contenant le mot-clé `Override` et celles contenant les valeurs qu'elles ignorent. Ne supprimez pas et ne modifiez pas la ligne contenant l'en-tête de section.

Sujets connexes

Sous les systèmes d'exploitation Windows, au lieu de transférer les fichiers .ini, vous pouvez utiliser l'assistant de configuration IP pour mettre à jour les paramètres TCP/IP de base de la carte de gestion réseau et configurer d'autres paramètres par l'intermédiaire de son interface utilisateur.



Voir « Assistant de configuration IP des équipements » en page 98.

Transferts de fichiers

Mise à niveau du microprogramme

Avantages de la mise à niveau du microprogramme

Lorsque vous mettez à niveau le microprogramme de la carte de gestion réseau 2 de l'onduleur :

- Vous obtenez les dernières corrections et améliorations.
- De nouvelles fonctions sont immédiatement disponibles.

Si les versions du microprogramme sont maintenues à jour sur l'ensemble de votre réseau, toutes les cartes de gestion réseau prennent en charge les mêmes fonctions de la même manière.

Fichiers de microprogramme (carte de gestion réseau 2)

Une version de microprogramme comprend trois modules : un module de système d'exploitation American Power Conversion (AOS), un module d'application et un module de contrôleur de démarrage (bootmon). Chaque module contient un ou plusieurs contrôles par redondance cyclique (CRC) pour éviter que ses données soient corrompues pendant le transfert.

Les fichiers des modules de système d'exploitation American Power Conversion (AOS), d'application et de contrôleur de démarrage utilisés avec la carte de gestion réseau possèdent le même format de base :

`apc_`*`version-matériel_type_version-microprogramme`*`.bin`

- `apc` : indique le contexte.
- *`version-matériel`* : `hw0`*`x`* identifie la version du matériel sur lequel ce fichier binaire est utilisable.
- *`type`* : identifie si le fichier est le module de système d'exploitation American Power Conversion (AOS), le module d'application ou le module de contrôleur de démarrage de la carte de gestion réseau.
- *`version`* : numéro de version du fichier.
- `bin` : indique qu'il s'agit d'un fichier binaire.

Pour obtenir la dernière version du microprogramme

Remarque : lors d'une mise à niveau manuelle, vous pouvez sauter l'installation du fichier bootmon si aucune mise à jour n'est disponible. Avec l'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 (NMC2 Firmware Upgrade Utility), les mises à jours du fichier bootmon sont automatiques.

Utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 pour systèmes Microsoft Windows. L'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 automatise le transfert des modules de microprogramme sur tous les systèmes d'exploitation pris en charge par Windows. Vous pouvez obtenir gratuitement la dernière version de cet utilitaire sur **www.apcc.com/tools/download**. Recherchez sur cette page Web la dernière version du microprogramme pour votre produit, ainsi que l'outil automatisé qui y est inclus. N'utilisez **jamais** un utilitaire prévu pour un produit spécifique pour mettre à niveau le microprogramme d'un autre produit.

Mises à niveau manuelles, principalement pour les systèmes Linux. Si aucun des ordinateurs de votre réseau ne fonctionne sous un système d'exploitation Microsoft Windows, vous devez mettre à niveau le microprogramme de vos cartes de gestion réseau à l'aide des modules de microprogramme AOS et d'application séparés.

Remarque : lors des mises à niveau manuelles, chargez d'abord le module de contrôleur de démarrage, puis le module de système d'exploitation et enfin le module d'application.

Pour extraire les fichiers de microprogramme :

1. Lancez l'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2.
2. A l'invite, cliquez sur **Next>** (Suivant) puis spécifiez l'emplacement du répertoire de destination des fichiers.
3. Lorsque le message **Extraction Complete** (Extraction terminée) s'affiche, fermez la boîte de dialogue.

Méthodes de transfert des fichiers de microprogramme

Utilisez l'une des méthodes suivantes pour mettre à niveau le microprogramme d'une carte de gestion réseau :

- A partir d'un ordinateur relié au réseau et fonctionnant sous un système d'exploitation Microsoft Windows, vous pouvez utiliser l'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 téléchargé à partir du site Web.

  Remarque : l'utilitaire fonctionne uniquement avec une carte de gestion réseau possédant une adresse IPv4.

- A partir d'un ordinateur relié au réseau et fonctionnant sous un système d'exploitation pris en charge, utilisez le protocole FTP ou SCP pour transférer les modules AOS et d'application individuels.
- Pour une carte de gestion réseau se trouvant hors réseau, utilisez XMODEM par l'intermédiaire d'une connexion série pour transférer les modules individuels depuis votre ordinateur vers la carte de gestion réseau.

  Avertissement : lorsque vous transférez des modules de microprogramme individuels, **vous devez** transférer le module AOS vers la carte de gestion réseau avant de transférer le module d'application.

- Utilisez une clé USB pour transférer les modules de microprogramme individuels de votre ordinateur à la carte de gestion réseau (AP9631 uniquement).

Utilisation du protocole FTP ou SCP pour mettre à niveau une carte de gestion réseau 2 individuelle

FTP. Pour utiliser FTP afin de mettre à niveau une carte de gestion réseau via le réseau :

- La carte de gestion réseau doit être connectée au réseau et son adresse IP système, son masque de sous-réseau et sa passerelle par défaut doivent être configurés.
- Le serveur FTP doit être activé au niveau de la carte de gestion réseau.
- Les fichiers de microprogramme doivent être extraits depuis l'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 (reportez-vous à la section « Pour extraire les fichiers de microprogramme : »).

Pour transférer les fichiers :

1. Sur un ordinateur relié au réseau, ouvrez une fenêtre d'invite de commande. Accédez au répertoire qui contient les fichiers du microprogramme, ainsi que la liste des fichiers :

   ```
   C:\>cd apc
   C:\apc>dir
   ```

   Pour les fichiers répertoriés, *xxx* représente le numéro de version du microprogramme :

   - `apc_hw05_aos_`*xxx*`.bin`
   - `apc_hw05_`*application_xxx*`.bin`

2. Ouvrez une session client FTP :

   ```
   C:\apc>ftp
   ```

3. Saisissez `open` et l'adresse IP de la carte de gestion réseau, puis appuyez sur ENTREE. Si le paramètre **port** du serveur FTP n'est plus configuré sur la valeur par défaut (**21**), vous devez utiliser la valeur qui lui a été attribuée au niveau de la commande FTP.

   - Pour les clients Windows FTP, séparez le numéro d'un port autre que le port par défaut et l'adresse IP par un espace. Par exemple :
     `ftp> open 150.250.6.10 21000`
   - Certains clients FTP requièrent l'insertion de deux-points au lieu d'un espace avant le numéro de port.

4. Connectez-vous en tant qu'Administrateur : le nom d'utilisateur et le mot de passe par défaut sont **apc**.

5. Mettez à niveau le module AOS (dans cet exemple, *xxx* représente le numéro de version du microprogramme) :

   ```
   ftp> bin
   ftp> put apc_hw05_aos_xxx.bin
   ```

6. Lorsque le protocole FTP confirme le transfert, saisissez `quit` pour fermer la session.

7. Après 20 secondes, répétez la procédure de l'étape 2 à l'étape 6. A l'étape 5, utilisez le nom de fichier du module d'application.

SCP. Pour mettre à niveau le microprogramme de la carte de gestion réseau à l'aide du protocole SCP (Secure CoPy) :

1. identifiez et trouvez les modules de microprogramme décrits dans les précédentes instructions relatives au protocole FTP.

2. Utilisez une ligne de commande SCP pour transférer le module AOS vers la carte de gestion réseau. Dans l'exemple suivant, *xxx* représente le numéro de version du module AOS :

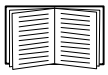
   ```
   scp apc_hw05_aos_xxx.bin apc@158.205.6.185:apc_hw05_aos_xxx.bin
   ```

3. Utilisez une ligne de commande SCP similaire, contenant le nom du module d'application, pour transférer le module d'application vers la carte de gestion réseau.

Mise à niveau de plusieurs cartes de gestion réseau

Utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2. Utilisez cet outil si vous devez effectuer plusieurs mises à niveau de microprogramme en IPv4 sous Windows. L'utilitaire enregistre toutes les étapes de la mise à niveau dans un journal à des fins de référence pour sa validation.

Exportation des paramètres de configuration. Vous pouvez créer des fichiers de commandes et utiliser un utilitaire pour récupérer les paramètres de configuration de plusieurs cartes de gestion réseau et les exporter vers d'autres cartes.



Consultez *Release Notes : ini File Utility, version 1.0*, disponible sur le CD des *utilitaires* de la carte de gestion réseau.

Utilisation du protocole FTP ou SCP pour mettre à niveau plusieurs cartes de gestion réseau. Pour mettre à niveau plusieurs cartes de gestion réseau à l'aide d'un client FTP ou du protocole SCP, écrivez un script qui permet d'effectuer automatiquement la procédure.

Utilisation de l'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 pour des mises à niveau multiples

Après l'avoir téléchargé à partir du site Web, double-cliquez sur le fichier .exe pour lancer l'utilitaire (qui fonctionne UNIQUEMENT avec IPv4) et suivez les étapes ci-dessous pour mettre à niveau le microprogramme de votre carte de gestion réseau :

1. Saisissez une adresse IP, un nom d'utilisateur et un mot de passe, et appuyez sur le bouton **Ping** si vous devez vérifier une adresse IP.
2. Appuyez sur le bouton **Device List** [Liste des périphériques] pour ouvrir le fichier `iplist.txt`. Les adresses IP, les noms d'utilisateur et les mots de passe de tous les périphériques s'affichent, par exemple :
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc

   Le nouvel utilitaire fonctionne parfaitement avec n'importe quel fichier `iplist.txt` existant que vous utilisiez avec l'ancienne version.
3. Cochez la case **Upgrade From Device List** [Mettre à niveau à partir de la liste des périphériques] pour utiliser le fichier `iplist.txt`. Décochez cette case pour mettre à niveau le microprogramme à l'aide de l'adresse IP, du nom d'utilisateur et du mot de passe que vous avez saisis dans la boîte de dialogue.
4. Appuyez sur le bouton **Upgrade Now** [Mettre à niveau maintenant] pour lancer la ou les mises à niveau de la version du microprogramme.
5. Choisissez **View Log** [Consulter le journal] pour vérifier les mises à niveau.

Utilisation du protocole XMODEM pour mettre à niveau une carte de gestion réseau

Pour utiliser XMODEM pour la mise à niveau d'une carte de gestion réseau qui n'est pas sur le réseau, vous devez extraire les fichiers de microprogramme de l'utilitaire de mise à niveau de microprogramme de carte de gestion réseau 2 (reportez-vous à la section « Pour extraire les fichiers de microprogramme : »).

Pour transférer les fichiers :

1. Sélectionnez un port série au niveau de l'ordinateur local et désactivez tout service utilisant ce port.
2. Connectez le câble de configuration série fourni (réf. 940-0299) au port choisi et au port série de la carte de gestion réseau.
3. Exécutez un programme d'émulation de terminal (tel que HyperTerminal) et configurez le port sélectionné sur 57600 bit/s, 8 bits de données, pas de parité, 1 bit d'arrêt et pas de contrôle de flux.
4. Appuyez sur le bouton **Reset** [Réinitialisation] de la carte de gestion réseau, puis immédiatement sur **Entrée**, deux fois ou jusqu'à ce que l'invite du contrôleur de démarrage affiche : `BM>`

5. Saisissez `XMODEM` et appuyez sur ENTREE.
6. Dans le menu du programme d'émulation de terminal, sélectionnez XMODEM puis le fichier de microprogramme AOS binaire à transférer via XMODEM. Une fois le transfert XMODEM terminé, l'invite du contrôleur de démarrage s'affiche à nouveau.
7. Pour installer le module d'application, répétez les étapes 5 et 6. A l'étape 6, utilisez le nom de fichier du module d'application.
8. Tapez `reset` ou appuyez sur le bouton Reset pour redémarrer la carte de gestion réseau.

Pour en savoir plus sur le format utilisé pour les modules de microprogramme, reportez-vous à « Fichiers de microprogramme (carte de gestion réseau 2) » à la page 103.

Utilisez une clé USB pour transférer les fichiers (AP9631 uniquement).

Remarque : avant de démarrer le transfert, veillez à ce que la clé USB soit au format FAT32.

1. Téléchargez les fichiers de mise à niveau et dézippez-les.
2. Créez un fichier `apcfirm` sur la clé USB.
3. Placez les fichiers extraits dans le répertoire `apcfirm`.
4. Insérez la clé USB dans l'un des ports USB de la carte de gestion réseau.
5. Réinitialisez la carte de gestion réseau et attendez que la carte redémarre complètement.
6. Vérifiez que la mise à nouveau a réussi en suivant les procédures décrites à la section « Contrôle des mises à niveau et des mises à jour » à la page 107.

Contrôle des mises à niveau et des mises à jour

Vérification du succès ou de l'échec du transfert

Pour vérifier si une mise à niveau de microprogramme a réussi, utilisez la commande `xferStatus` dans l'interface en ligne de commande afin de consulter le résultat du dernier transfert, ou une commande SNMP GET pour l'OID **mfiletransferStatusLastTransferResult**.

Codes de résultat du dernier transfert

Code	Description
Successful	Le transfert de fichier a réussi.
Result not available	Aucun transfert de fichier n'a été enregistré.
Failure unknown	Le dernier transfert de fichier a échoué pour un motif inconnu.
Server inaccessible	Le serveur TFTP ou FTP est introuvable sur le réseau.
Server access denied	L'accès au serveur TFTP ou FTP a été refusé.
File not found	Le serveur TFTP ou FTP n'a pas pu localiser le fichier spécifié.
File type unknown	Le fichier a été téléchargé mais son contenu n'a pu être identifié.
File corrupt	Le fichier a été téléchargé mais au moins un contrôle par redondance cyclique (CRC) a échoué.

Vérification des numéros de version des microprogrammes installés

Utilisez l'interface Web pour vérifier les versions des modules de microprogramme mis à niveau en sélectionnant l'onglet **Administration** puis **Généralités** dans la barre de menu supérieure, et **A propos de** dans le menu de navigation gauche, ou utilisez une commande SNMP GET pour l'OID **sysDescr** MIB II. Dans l'interface en ligne de commande, utilisez la commande `about`.

Ajout et modification de modules de prise en charge linguistique

Les fichiers de modules de prise en charge linguistique de la carte de gestion réseau 2 contiennent les informations requises pour afficher l'interface utilisateur dans d'autres langues que l'anglais. Chaque module de prise en charge linguistique peut contenir jusqu'à cinq langues (c'est pourquoi la liste déroulante **Language** vous propose jusqu'à cinq langues lorsque vous vous connectez).

L'interface utilisateur propose neuf langues : français, italien, allemand, espagnol, portugais brésilien, russe, coréen, japonais et chinois simplifié.

Les fichiers de modules de prise en charge linguistique sont disponibles sur la page de téléchargements de la carte de gestion réseau 2 pour onduleur sur le site Web, **www.apc.com**. Ils ont tous une extension .lpk et sont nommés sur le modèle suivant :

```
<nom application>_<version application>_<codes langue>.lpk
```

Par exemple, pour une application en 3 phases pour un onduleur Symmetra, le nom de fichier est :

```
sy3p_510_esESzhCnjaJAptBrkoKo.lpk
```

où `esESzhCnjaJAptBrkoKo` signifie espagnol, chinois, japonais, portugais brésilien et coréen.

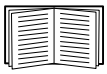
Il se peut que vous ayez besoin d'utiliser l'interface utilisateur dans une langue actuellement non disponible. Pour ce faire, vous devez télécharger le pack de prise en charge linguistique sur le site Web et suivre les étapes ci-dessous :

1. Connectez-vous à la carte de gestion réseau via FTP.
2. Transférez le module de prise en charge linguistique requis sur la carte de gestion réseau. Saisissez par exemple :
   ```
   put <chemin complet/nom du module de prise en charge linguistique>.lpk
   ```
3. Lorsque le transfert du fichier est terminé, déconnectez-vous du serveur FTP et la carte de gestion réseau redémarre.
4. Lorsque le redémarrage est terminé, le nouveau module de prise en charge linguistique est prêt.

Remarque : tout module de prise en charge linguistique actuellement sur la carte est supprimé avant le transfert du nouveau module. En cas de problème pendant le transfert du module, aucun module de prise en charge linguistique n'est présent sur la carte de gestion réseau. Dans ce cas, seul l'anglais est disponible. Si ce problème se produit, procédez de nouveau au chargement du module de prise en charge linguistique adéquat.

Dépannage

Problèmes d'accès à la carte de gestion réseau



Pour des problèmes qui ne sont pas décrits dans cette documentation, consultez les organigrammes de dépannage sur le CD d'*utilitaires* de la carte de gestion réseau. Cliquez sur le lien **Dépannage** dans l'interface du CD.

Si le problème persiste, consultez Voir « Assistance clients internationale » en page 117..

Problème	**Solution**
Impossible d'effectuer le test Ping sur la carte de gestion réseau	Si le témoin d'état de la carte de gestion réseau est vert, essayez un test Ping sur un nœud différent du même segment de réseau que celui de la carte de gestion réseau. En cas d'échec, le problème ne vient pas de la carte de gestion réseau. Si le témoin d'état n'est pas vert ou si le test ping réussit, procédez aux vérifications suivantes : • Vérifiez que la carte de gestion réseau est correctement installée dans l'onduleur. • Vérifiez toutes les connexions réseau. • Vérifiez les adresses IP de la carte de gestion réseau et du NMS. • Si le NMS se trouve sur un réseau (ou un sous-réseau) physique différent de celui de la carte de gestion réseau, vérifiez l'adresse IP de la passerelle par défaut (ou du routeur). • Vérifiez le nombre de bits du sous-réseau indiqués pour le masque de sous-réseau de la carte de gestion réseau.
Impossible d'allouer le port de communication par l'intermédiaire d'un programme de terminal	Avant de pouvoir utiliser un programme de terminal pour configurer la carte de gestion réseau, vous devez fermer tous les services, programmes ou applications qui utilisent le port de communication.
Impossible d'accéder à l'interface par lignes de commande par l'intermédiaire d'une connexion série	Assurez-vous que vous n'avez pas modifié la vitesse de transmission. Essayez 2400, 9600, 19200 ou 38400.
Impossible d'accéder à distance à l'interface par lignes de commande	• Assurez-vous que vous utilisez la méthode d'accès correcte, Telnet ou Secure SHell (SSH). Un Administrateur peut activer ces méthode d'accès. Par défaut, le protocole Telnet est activé. L'activation de SSH provoque la désactivation automatique de Telnet. • Pour SSH, la carte de gestion réseau peut créer une clé d'hôte. La carte de gestion réseau peut prendre jusqu'à une minute pour créer la clé d'hôte ; pendant ce temps, SSH est inaccessible.
Impossible d'accéder à l'interface Web	• Vérifiez que l'accès HTTP ou HTTPS est activé. • Assurez-vous que vous spécifiez l'URL correcte (cohérente avec le système de sécurité utilisé par la carte de gestion réseau). Le protocole SSL requiert de taper **https**, et non pas **http**, au début de l'URL. • Vérifiez que vous pouvez effectuer un test Ping sur la carte de gestion réseau. • Vérifiez que vous utilisez un navigateur Web pris en charge par la carte de gestion réseau. Voir « Navigateurs Web pris en charge » en page 29. • Si la carte de gestion réseau vient juste de redémarrer et que la sécurité SSL est en cours de configuration, il se peut que la carte de gestion réseau soit en train de créer un certificat de serveur. La carte de gestion réseau peut prendre jusqu'à une minute pour créer ce certificat ; pendant ce temps, le serveur SSH est inaccessible.

Problèmes SNMP

Problème	Solution
Impossible d'exécuter une commande GET	• Vérifiez le nom de communauté (SNMPv1) en lecture (GET) ou la configuration du profil utilisateur (SNMPv3). • Utilisez l'interface par lignes de commande ou l'interface Web pour vous assurer de l'accessibilité par NMS. Voir « SNMP » en page 79.
Impossible d'exécuter une commande SET	• Vérifiez le nom de communauté (SNMPv1) en lecture/écriture (SET) ou la configuration du profil utilisateur (SNMPv3). • Utilisez l'interface par lignes de commande ou l'interface Web pour vous assurer que le NMS dispose de l'accès (SNMPv1) en écriture (SET) ou de l'accès à l'adresse IP cible par l'intermédiaire de la liste de contrôle d'accès (SNMPv3). Voir « SNMP » en page 79.
Impossible de recevoir les traps au niveau du NMS	• Assurez-vous que le type de trap (SNMPv1 ou SNMPv3) est correctement configuré pour le NMS comme destinataire des traps. • Pour SNMPv1, demandez à l'OID **mconfigTrapReceiverTable** MIB de vérifier que l'adresse IP du NMS est correctement répertoriée et que le nom de communauté défini pour le NMS correspond au nom de communauté figurant dans le tableau. Si ne n'est pas le cas, exécutez les commandes SET sur les OID **mconfigTrapReceiverTable** ou utilisez l'interface par lignes de commande ou l'interface Web pour remédier au problème de définition des destinataires des traps. • Pour SNMPv3, vérifiez la configuration du profil utilisateur du NMS et lancez un test de trap. Consultez « SNMP » en page 79, « Récepteurs de traps » en page 88 et « Test de traps SNMP » en page 90.
Les traps reçus au niveau du NMS ne sont pas identifiés	Reportez-vous à la documentation de votre NMS pour vérifier que les traps sont correctement intégrées à la base de données des alarmes/traps.

Problèmes de synchronisation

Problème	Solution
Un membre de groupe de contrôle synchronisé ne participe pas à une action synchronisée.	Assurez-vous que que l'état du membre de groupe est défini sur **Activé**. Vérifiez aussi la capacité de la batterie du membre de groupe, dans le cas où l'action synchronisée à provoqué la mise sous tension des onduleurs.
Une tentative d'ajouter un membre à un groupe de contrôle synchronisé échoue.	Les valeurs **Adresse IP de multidiffusion**, **Numéro de groupe de contrôle synchronisé** et la version du microprogramme doivent correspondre à celles des autres membres du groupe.

Annexe A: Interface par lignes de commande

?

about

alarmcount
[-p [all | warning | critical]]

boot
[-b <dhcp | bootp | manual>]
[-c <dhcp cookie> [enable | disable]]
[-v <vendor class>]
[-i <client id>]
[-u <user class>]

cd

console
[-S <disable | telnet | ssh>]
[-pt <telnet port #>]
[-ps <ssh port #>]
[-b <baud rate> [2400 | 9600 | 19200 | 38400]]

date
[-d <“datestring”>]
[-t <00:00:00>]
[-f [mm/dd/yy | dd.mm.yyyy | mmm-dd-yy |
dd-mmm-yy | yyyy-mm-dd]]
[-z <time zone offset>]

delete

dir

dns
[-OM [enable | disable]]
[-p <primary DNS server>]
[-s <secondary DNS server>]
[-d <domain name>]
[-n <domain name IPv6>]
[-h <host name>]

eventlog

exit

format

ftp
[-p <port number>]
[-S <enable | disable>]

help

netstat

ntp
[-OM [enable | disable]]
[-p <primary NTP server>]
[-s <secondary NTP server>]

ping
[<IP address or DNS name>]

portspeed
[-s [auto | 10H | 10F | 100H | 100F]]

prompt
[-s [long | short]]

quit

radius
[-a <access> [local | radiusLocal | radius]]
[-p# <server IP>]
[-s# <server secret>]
[-t# <server timeout>]

reboot

resetToDef
[-p [all | keepip]]

snmp, snmp3
[-S [enable | disable]]

system
[-n <system name>]
[-c <system contact>]
[-l <system location>]

tcpip
[-i <IP address>]
[-s <subnet mask>]
[-g <gateway>]
[-d <domain name>]
[-h <host name>]

tcpip6
[-S [enable | disable]]
[-man [enable | disable]]
[-auto [enable | disable]]
[-i <IPv6 address>]
[-g <IPv6 gateway>]
[-d6 [router | stateful | stateless | never]]

uio
[-rc <dI> [open | close]
[-st <port # | port #]]
[-disc <port # | port #]]

ups
[-c <off | graceoff | on | reboot | gracereboot | sleep | gracesleep>]
[-r <start | stop>]
[-s <start>]
[-b <enter | exit>]
[-o# <off | delayoff | on | delayon | reboot>]
[-os#]
[-st]

user
[-an <Administrator name>]
[-dn <Device User name>]
[-rn <Read-Only User name>]
[-ap <Administrator password>]
[-dp <Device User password>]
[-rp <Read-Only User password>]
[-t <inactivity timeout in minutes>]

web
[-S <disable | http | https>]
[-ph <http port #>]
[-ps <https port #>]

xferINI

xferStatus

Garantie usine de deux ans

Cette garantie s’applique uniquement aux produits que vous achetez pour une utilisation personnelle conforme aux instructions du présent manuel.

Conditions de la garantie

APC garantit que ses produits seront exempts de tous défauts dus au matériel ou à la fabrication pendant une période de deux ans à compter de la date d’achat. APC répare ou remplace les produits défectueux couverts par la présente garantie. Cette garantie ne couvre pas les dommages résultant d’un accident, d’une négligence ou d’une mauvaise utilisation, ni d’une modification ou adaptation quelconque du produit. La réparation ou le remplacement d’un produit défectueux ou d’une pièce de celui-ci n’étend pas la période de garantie d’origine. Toute pièce fournie dans le cadre de cette garantie peut être neuve ou avoir été réusinée.

Garantie non transférable

Cette garantie ne s’applique qu’à l’acheteur d’origine qui doit avoir enregistré correctement le produit. Pour enregistrer le produit, visitez le site Web d’APC **www.apc.com**.

Exclusions

Dans le cadre de cette garantie, APC ne peut être tenu responsable si, après contrôle et examen effectué par APC, il s’avère que le produit n’est pas défectueux ou que le défaut présumé est la conséquence d’une mauvaise utilisation, d’une négligence, d’une mauvaise installation ou d’un mauvais contrôle de la part de l’acheteur ou d’un tiers. De plus, APC ne peut être tenu responsable dans le cadre de cette garantie en cas de tentative non autorisée de réparation ou de modification d’une connexion ou d’un voltage électrique incorrect ou inadapté, de conditions de fonctionnement sur site inappropriées, d’une atmosphère corrosive, de réparations, d’installations, d’exposition aux éléments naturels, de catastrophes naturelles, d’incendie, de vol ou d’installation contraire aux recommandations ou spécifications d’APC ou de tout autre événement si le numéro de série APC a été modifié, dégradé ou effacé ou de toute autre cause non survenue dans le cadre d’une utilisation autorisée.

CE CONTRAT NE PRESENTE AUCUNE GARANTIE, EXPLICITE OU IMPLICITE, PAR EFFET DE LA LOI OU DE TOUTE AUTRE MANIERE, CONCERNANT LES PRODUITS VENDUS, REPARES OU FOURNIS. APC REJETTE TOUTE GARANTIE IMPLICITE DE COMMERCIABILITE, SATISFACTION OU ADEQUATION A UN USAGE PARTICULIER. LES GARANTIES EXPLICITES D’APC NE PEUVENT ETRE ETENDUES, DIMINUEES OU AFFECTEES PAR LES CONSEILS OU SERVICES TECHNIQUES OU AUTRES OFFERTS PAR APC CONCERNANT LES PRODUITS, ET AUCUNE OBLIGATION OU RESPONSABILITE NE PEUT S’EN DEGAGER. LES GARANTIES ET COMPENSATIONS CI-DESSUS SONT EXCLUSIVES ET REMPLACENT TOUTES LES AUTRES GARANTIES ET COMPENSATIONS. EN CAS DE NON-RESPECT DE CES GARANTIES, LA RESPONSABILITE D’APC ET LE RECOURS DE L’ACHETEUR SE LIMITENT AUX GARANTIES INDIQUEES CI-DESSUS. LES GARANTIES OCTROYEES PAR APC S’APPLIQUENT UNIQUEMENT A L’ACHETEUR ET NE SONT PAS TRANSFERABLES A UN TIERS.

EN AUCUN CAS, APC, SES AGENTS, SES DIRECTEURS, SES FILIALES OU SES EMPLOYES NE POURRONT ETRE TENUS RESPONSABLES POUR TOUTE FORME DE DOMMAGES INDIRECTS, PARTICULIERS, IMMATERIELS OU EXEMPLAIRES, SUITE A L'UTILISATION, L'ENTRETIEN OU L'INSTALLATION DES PRODUITS, QUE CES DOMMAGES REVETENT UN CARACTERE CONTRACTUEL OU DELICTUEL, SANS TENIR COMPTE DES DEFAUTS, DE LA NEGLIGENCE OU DE LA RESPONSABILITE ABSOLUE, OU MEME SI APC A ETE PREVENU DE L'EVENTUALITE DE TELS DOMMAGES. SPECIFIQUEMENT, APC N'EST RESPONSABLE D'AUCUN COUT, TEL QUE LA PERTE DE PROFITS OU DE REVENUS, LA PERTE DE L'UTILISATION DE MATERIEL, DE LOGICIELS, DE DONNEES, LE COUT DE SUBSTITUTS, LES RECLAMATIONS PAR DES TIERS OU AUTRES.

AUCUN REPRESENTANT, EMPLOYE OU AGENT D'APC N'EST AUTORISE A APPORTER DES ANNEXES OU DES MODIFICATIONS AUX CONDITIONS DE LA PRESENTE GARANTIE. LES CONDITIONS DE LA GARANTIE NE PEUVENT ETRE MODIFIEES, LE CAS ECHEANT, QUE PAR ECRIT ET AVEC LA SIGNATURE D'UN AGENT APC ET DU SERVICE JURIDIQUE.

Réclamations

Les Clients désirant effectuer une réclamation peuvent accéder au service d'assistance Clients d'APC en visitant la page Support du site Web d'APC à l'adresse **www.apc.com/support**. Sélectionnez votre pays dans le menu déroulant se trouvant en haut de la page Web. Sélectionnez l'onglet Support pour obtenir les coordonnées du service d'assistance Clients dans votre région.

Assistance clients internationale

L'assistance clients pour ce produit et tout autre produit est disponible gratuitement de l'une des manières suivantes :

- Visitez le site Web pour consulter les réponses aux questions fréquemment posées (FAQ), pour accéder aux documents de la base de connaissance et soumettre vos demandes d'assistance.
  - **www.apc.com** (Siège social)

    Suivez les liens des pages Web menant au pays de votre choix, chacun fournissant des informations relatives à l'assistance clients.
  - **www.apc.com/support/**

    Assistance globale incluant des FAQ, une base de connaissance et une assistance via Internet.
- Contactez un centre d'assistance clients par téléphone ou en envoyant un courrier électronique.
  - Centres régionaux :

InfraStruXure Ligne directe d'assistance à la clientèle	(1)(877)537-0607 (gratuit aux États-Unis)
(Siège social) Etats-Unis, Canada	(1)(800)800-4272 (gratuit aux Etats-Unis)
France	+800 0272 0272
Europe, Moyen-Orient et Afrique	(353)(91)702000 (Irlande)
Amérique latine	(1)(401)789-5735 (Etats-Unis)
Japon	03-6402-2001

  - Centres locaux, relatifs à un pays : connectez-vous à **www.apc.com/support/contact** pour plus d'informations.

Contactez le représentant ou tout autre revendeur chez qui vous avez acheté le produit pour obtenir des informations relatives à l'assistance clients.

990-3402D-012 **05/2012**