Guide de l’utilisateur

Carte de gestion réseau pour Easy UPS, monophasé et triphasé - Guide de l’utilisateur

AP9544, AP9547

990-91545F-012
05/2025

Schneider Electric

Avertissement légal de Schneider Electric

Schneider Electric ne garantit pas que les informations fournies dans ce manuel fassent autorité, ni qu'elles soient correctes ou complètes. Le présent document ne peut remplacer un plan de développement détaillé opérationnel et spécifique à un site. Par conséquent, Schneider Electric rejette toute responsabilité liée aux dommages, aux violations de réglementations, à une installation incorrecte, aux pannes du système ou à tout autre problème qui pourrait survenir suite à l'utilisation de cette publication.

Les informations contenues dans le présent document sont fournies en tant que telles et ont été préparées uniquement dans le but d'évaluer la conception et la construction d'un datacenter. Schneider Electric a compilé cette publication en toute bonne foi. Toutefois aucune garantie n'est donnée, expresse ou implicite, quant à l'exhaustivité ou à l'exactitude informations contenues dans cette publication.

EN AUCUN CAS SCHNEIDER ELECTRIC, NI AUCUNE SOCIÉTÉ PARENTE, AFFILIÉE OU FILIALE DE SCHNEIDER ELECTRIC OU LEURS AGENTS, DIRECTEURS OU EMPLOYÉS RESPECTIFS NE POURRA ÊTRE TENU RESPONSABLE DE TOUT DOMMAGE DIRECT, INDIRECT, IMMATÉRIEL, EXEMPLAIRE, SPÉCIAL OU ACCIDENTEL (Y COMPRIS, SANS LIMITATION, LES DOMMAGES DUS À LA PERTE DE CLIENTÈLE, DE CONTRATS, DE REVENUS, DE DONNÉES, D'INFORMATIONS, OU À L'INTERRUPTION D'ACTIVITÉ) RÉSULTANT DE, PROVOQUÉ PAR, OU EN RAPPORT AVEC L'UTILISATION OU L'INCAPACITÉ D'UTILISER CETTE PUBLICATION OU SON CONTENU, ET CE MÊME SI SCHNEIDER ELECTRIC A ÉTÉ EXPRESSÉMENT AVISÉ DE L'ÉVENTUALITÉ DE TELS DOMMAGES. SCHNEIDER ELECTRIC SE RÉSERVE LE DROIT DE MODIFIER OU DE METTRE À JOUR LE CONTENU DU PRÉSENT DOCUMENT, OU TOUTES INFORMATIONS ASSOCIÉES, ET SON FORMAT À TOUT MOMENT SANS PRÉAVIS.

Les droits de reproduction, de propriété intellectuelle et tous autres droits de propriété sur le contenu (y compris, mais sans s'y limiter, les logiciels, les fichiers audio, vidéo et texte, et les photographies) sont détenus par Schneider Electric ou ses concédants. Tout droit non expressément garanti dans le présent avis est réservé. Aucun droit d'aucune sorte n'est concédé, cédé ou ne sera transféré de quelque manière que ce soit aux personnes accédant à ces informations.

Le présent document ne peut être revendu, intégralement ou en partie.

Table des matières

Introduction 1

Description du produit 1

Fonctionnalités 1
Appareils compatibles 2
Configuration initiale IPv4 2
Configuration initiale IPv6 2
Gestion de réseau avec d'autres applications 3

Fonctions de gestion interne 4

Présentation 4
Priorité d'accès pour la connexion 4
Types de comptes utilisateur 4

Comment réinitialiser son compte après avoir oublié son mot de passe 5

Panneau avant (AP9544/AP9547) 6

Description des voyants 7

Voyant d'état 7
Voyant de liaison RX/TX (10/100/1000) 7

Fonctions de surveillance 8

Présentation 8
Interface réseau du mécanisme de surveillance 8
Réinitialisation du compteur réseau 8
Déconnexion automatique 8

Interface utilisateur Web 9

Introduction 9

Présentation 9
Navigateurs Web pris en charge 9

Procédure de connexion 9

Présentation 9
Formats d'adresse URL 10
Première connexion 11

Écran d'accueil 11
Présentation 11
Icônes et liens 11

Surveillance de l'onduleur : Menu État 12

Onduleur dans le menu État 12
Aperçu du menu État 13
Mesures dans le menu État 14
E/S universelle dans le menu État 16
Réseau dans le menu État 16
Entretien dans le menu État 16

Contrôle de l'onduleur 18

Onduleur dans le menu Contrôle 18
Sécurité dans le menu Contrôle 19
Réseau dans le menu Contrôle. 19

Configuration de vos paramètres : 1 20

Paramètres d'alimentation dans le menu Configuration 20
Écrans Onduleur - Généralités 21
Écran Programme de test automatique 21
Arrêt dans le menu Configuration 22
Début de l'arrêt 22
Durée de l'arrêt 22
Paramètres d'arrêt de PowerChute 23
Planification de l'arrêt 25
Pour l'onduleur 25
Clients PowerChute Network Shutdown 26
Menu Sécurité 26
Écran Contacts d'entrée 26
Écran Relais de sortie 27
Configuration de la politique de contrôle 27

Menu Sécurité 28
Écran Gestion des sessions 28
Réponse ping 28
Utilisateurs locaux 28
Authentification des utilisateurs distants 30
Écran RADIUS 31
Configuration du serveur RADIUS 31
Écrans Pare-feu 32
Configuration de sécurité 802.1X 35

Configuration de vos paramètres : 2 36

Réseau dans le menu Configuration 36
Paramètres TCP/IP pour l'écran IPv4 36
Paramètres TCP/IP pour l'écran IPv6 37
Options de réponse DHCP 38
Écran Vitesse du port 39
Écran DNS 40
Test de l'écran DNS 40
Écran d'accès Web 41
Écran du certificat SSL Web 41
Écran de la console 42
Écrans SNMP 43
Écrans Modbus 46
Écran BACnet 47
Écran Serveur FTP 49
Écran Wi-Fi 50

Menu Notification 51
Types de notification 51
Configuration des actions sur les événements 52
Écrans de notification par e-mail 53
Écran des récepteurs de traps SNMP 56
Écran de test des traps SNMP 57

Menu Généralités 57
Écran d'identification 57
Écran Date/heure 57
Création et importation de paramètres avec le fichier de configuration 58
Écran de configuration des liens 59

Journaux dans le menu Configuration 59
Identification des serveurs Syslog 59
Paramètres Syslog 59
Test Syslog et exemple de format 60

Menu Tests 61

Test et calibrage 61

Configuration du clignotement des voyants LED de la carte de gestion réseau 61

Menus des journaux 62

Utilisation des journaux de consignation des événements et des données 62

Journal de consignation des événements 62
Journal de consignation des données 64
Utilisation du protocole SCP ou FTP pour récupérer les fichiers de journaux de consignation 65

Journal de l'onduleur 67

Journal de consignation du pare-feu 67

À propos du menu 68

À propos de la carte de gestion réseau 68

À propos de l'onduleur 68
À propos de la carte de gestion réseau et des modules de micrologiciel 68
Écran Assistance 69

Assistant de configuration IP des périphériques 70

Fonctionnalités, configuration requise et installation 70

Configuration requise 70
Installation 70

Exportation des paramètres de configuration 71

Récupération et exportation du fichier .ini 71

Résumé de la procédure 71
Contenu du fichier .ini 71
Procédures détaillées 71

Événement de téléchargement et messages d'erreur 73

L'événement et ses messages d'erreur 73
Messages dans le fichier config.ini 73
Erreurs générées par les valeurs ignorées 74

Sujets connexes 74

Mises à niveau du micrologiciel de la carte de gestion réseau 75

Mise à jour du micrologiciel vers la version 3.0 ou supérieure 75

Méthodes de transfert des fichiers de micrologiciel 75

Mise à jour du micrologiciel vers la version 2.5 ou inférieure 75

Méthodes de transfert des fichiers de micrologiciel 75

Utilisation de l'utilitaire de mise à niveau de micrologiciel. 76

Utilisation du protocole FTP ou SCP pour mettre à niveau une carte de gestion réseau unique 76

Utilisation du protocole XMODEM pour mettre à niveau une carte de gestion réseau 77

Utiliser une clé USB pour transférer les fichiers (AP9631 uniquement) 78

Mise à niveau du micrologiciel sur plusieurs cartes de gestion réseau 78

Vérification des mises à niveau 79

Vérification du succès ou de l'échec du transfert 79

Codes de résultat du dernier transfert 80

Vérification des numéros de version des micrologiciels installés 80

Changement de la langue de l'interface utilisateur. 80

Dépannage 81

Problèmes d'accès à la carte de gestion réseau 81

Problèmes SNMP. 82

Problèmes Modbus. 83

Problèmes liés au périphérique Wi-Fi USB APC (AP9834) 83

Description des voyants 84

Garantie usine de deux ans 85

Conditions de garantie 85

Garantie non transférable 85

Exclusions 85

Réclamations 86

. 87

Introduction

Description du produit

Fonctionnalités

Les cartes de gestion réseau Schneider Electric pour onduleurs Easy UPS, monophasés et triphasés (AP9544 et AP9547) mentionnés ci-dessous sont des produits basés sur Web, compatibles IPv6. Les appareils comportant une carte de gestion réseau (NMC) peuvent être gérés à l'aide de plusieurs normes ouvertes, telles que :

Protocole HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)	Secure SHell (SSH)
Secure Copy (SCP)	Démarrage sécurisé avec racine de confiance pour une sécurité accrue
RADIUS	Protocole d'authentification extensible (EAP) sur réseau local (EAPoL)
Protocole de réseaux d'automatisation et de contrôle des bâtiments (BACnet - AP9547 uniquement)	Protocole de gestion réseau simple, versions 1, 2c et 3
Syslog	Telnet
Modbus TCP/IP	Protocole HTTP (Hypertext Transfer Protocol)
Protocole de transfert de fichiers FTP (File Transfer Protocol)	

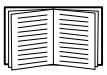
Cartes de gestion réseau **AP9544** et **AP9547** :

- Fournissent un port hôte USB-A, qui prend en charge la mise à niveau le microprogramme de la carte de gestion réseau à partir d'une clé USB, et de l'appareil Wi-Fi USB APC (AP9834) en option. Le port hôte USB-A de la carte de gestion réseau AP9544 prend en charge une entrée à contact sec et deux relais de sortie lorsqu'il est connecté à l'accessoire « USB vers contact sec » en option de la carte de gestion réseau (AP9811).
- Fournissent des données et des journaux des événements.
- Vous permettent de définir des notifications via la consignation des événements, par e-mail et via des traps SNMP.
- Assurent la prise en charge de PowerChute® Network Shutdown. **REMARQUE :** la carte AP9547 des onduleurs triphasés ne prend en charge que l'arrêt des serveurs connectés et des applications exécutées sur ces serveurs. Elle n'est pas prise en charge pour arrêter le ou les onduleurs.
- Offrent une assistance via le protocole DHCP (Dynamic Host Configuration Protocol) ou BOOTstrap
- Le serveur de protocole (BOOTP) fournit les valeurs réseau (TCP/IP) de la carte de gestion réseau.
- Offrent la possibilité d'exporter le fichier de configuration de l'utilisateur (.ini) à partir d'une carte configurée vers une ou plusieurs cartes non configurées, sans convertir le fichier en format binaire.
- Offrent une gamme de protocoles de sécurité pour l'authentification et le chiffrement.
- Communiquent avec Data Center Expert, Data Center Operation ou EcoStruxure™ IT.
- Prennent en charge Modbus TCP/IP.

Appareils compatibles

La carte de gestion réseau de l'onduleur Easy UPS est compatible avec :

- Modèles monophasés : appareils Easy UPS On-Line (AP9544 uniquement).
- Modèles triphasés : Easy UPS 3S, 3S Pro, 3M, 3L, Galaxy 3L et Galaxy PW de 2e génération. (Ap9547 uniquement).



Reportez-vous à l'article **FA237786** de la Base de connaissances pour obtenir une liste des onduleurs avec lesquels les cartes de gestion réseau sont compatibles.

Configuration initiale IPv4

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

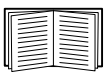
- L'adresse IP de la carte de gestion réseau
- Le masque de sous-réseau de la carte de gestion réseau
- L'adresse IP de la passerelle par défaut (nécessaire uniquement hors segment du réseau)

REMARQUE : en cas d'indisponibilité de la passerelle par défaut, utilisez l'adresse IP d'un ordinateur connecté au même sous-réseau que la carte de gestion réseau et habituellement utilisé. La carte de gestion réseau utilise la passerelle par défaut pour tester le réseau lorsque le trafic est faible.

REMARQUE : le préfixe de l'adresse MAC de la carte de gestion réseau MAC est 00:C0:B7 ou 28:29:86. Pour vérifier l'adresse MAC de votre carte de gestion réseau, allez à **« About (À propos de) > Network (Réseau) »** Vous pouvez utiliser ce préfixe d'adresse MAC pour configurer votre service DHCP.



REMARQUE : n'utilisez pas l'adresse de retour en boucle (127.0.0.1) comme adresse de passerelle par défaut. Ceci entraînerait une désactivation de 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 **Guide d'installation de la carte de gestion réseau pour l'onduleur Easy UPS** disponible sur le site Web de Schneider Electric et sous forme imprimée.

Pour des informations détaillées sur l'utilisation d'un serveur DHCP pour la configuration des paramètres TCP/IP d'une carte de gestion réseau, reportez-vous à la section « Options de réponse DHCP ».

Configuration initiale IPv6

La configuration réseau IPv6 offre la souplesse requise pour s'adapter à vos besoins. IPv6 peut être utilisé partout où une adresse IP est saisie dans cette interface. Vous pouvez la configurer manuellement, automatiquement ou à l'aide de DHCPv6. Voir « Paramètres TCP/IP pour l'écran IPv6 ».

Gestion de réseau avec d’autres applications

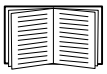
Ces applications, utilitaires et ressources fonctionnent avec un onduleur connecté au réseau par l’intermédiaire d’une carte de gestion réseau.

- PowerChute Network Shutdown — Assure l’arrêt progressif à distance sans supervision d’ordinateurs connectés aux onduleurs.
- APC PowerNet® MIB — Découvrez comment accéder aux onduleurs via SNMP.
- Data Center Expert — Fournit une gestion de l’alimentation de niveau entreprise ainsi qu’une gestion des agents SNMP, tels que les onduleurs en réseau et les capteurs environnementaux.
- EcoStruxure IT — Logiciel basé sur le cloud qui vous permet de surveiller vos onduleurs via SNMP et Modbus.
- Utilitaire de configuration IP des équipements — Permet de configurer les paramètres de base d’une ou plusieurs cartes de gestion réseau sur le réseau. Voir « Assistant de configuration IP des périphériques ».
- Assistant de sécurité — Aide à l’importation des certificats du serveur TLS (Transport Layer Security) et des clés hôtes SSH (Secure SHell), contribuant ainsi à protéger l’intégrité et à la confidentialité de la communication avec la carte de gestion réseau.

Fonctions de gestion interne

Présentation

Utilisez l'interface utilisateur Web ou l'interface par ligne 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, consultez la section « Interface utilisateur Web » et le **Guide de carte de gestion réseau pour onduleur Easy UPS CLI**. Reportez-vous à la section « Écrans SNMP » pour en savoir plus sur le contrôle de l'accès SNMP à la carte de gestion réseau.

Priorité d'accès pour la connexion

Vous pouvez permettre à plusieurs utilisateurs de se connecter simultanément, chacun d'eux disposant d'un même accès. Reportez-vous à la section « Écran Gestion des sessions ».

Types de comptes utilisateur

La carte de gestion réseau dispose de divers niveaux d'accès : Super-utilisateur, Administrateur, Utilisateur d'appareil, Utilisateur en lecture seule et Utilisateur réseau uniquement :

- Un **super-utilisateur** peut utiliser tous les menus de l'interface utilisateur et toutes les commandes de l'interface par ligne de commande. Il peut également définir d'autres comptes utilisateur et configurer des variables pour des utilisateurs supplémentaires. Le nom d'utilisateur et le mot de passe par défaut sont tous les deux `apc` à la première connexion. Il vous sera demandé de saisir un nouveau mot de passe après votre connexion.
  REMARQUE : le super-utilisateur ne peut être renommé ni supprimé, mais il peut être désactivé. Il est recommandé de désactiver le compte du super-utilisateur une fois que les comptes administrateur supplémentaires ont été créés. Assurez-vous qu'il y a au moins un compte administrateur activé avant de désactiver le compte super-utilisateur.

  Un **administrateur** peut utiliser tous les menus de l'interface utilisateur et toutes les commandes de l'interface par ligne de commande. Le nom d'utilisateur par défaut est `apc` et vous devez définir un mot de passe avant de pouvoir activer le compte utilisateur.
- Un **utilisateur du périphérique** a accès en lecture et en écriture aux écrans liés au périphérique. Les fonctions administratives telles que la gestion de session sous le menu Sécurité et Pare-Feu sous Journaux de consignation sont grisées.

  Le nom d'utilisateur par défaut est `device` et vous devez définir un mot de passe avant de pouvoir activer le compte utilisateur.
- Un **utilisateur en lecture seule** a accès aux mêmes menus que le niveau Utilisateur du périphérique ci-dessus, 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 d'événements et de données n'affichent pas de bouton permettant à cet utilisateur d'effacer le journal).

  Le nom d'utilisateur par défaut est `readonly` et vous devez définir un mot de passe avant de pouvoir activer le compte utilisateur.
- Un **utilisateur réseau uniquement** peut seulement se connecter à l'aide de l'interface utilisateur (IU) Web et l'interface par ligne de commande (Telnet/SSH non série). Il n'y a pas de nom et de mot de passe par défaut.



Les comptes Administrateur, Utilisateur de périphérique, Utilisateur en lecture seule et Utilisateur réseau uniquement sont désactivés par défaut et ne peuvent être activés qu'après modification du mot de passe par défaut (`apc`) du super-utilisateur.



Pour définir les valeurs **Nom d'utilisateur** et **Mot de passe** pour les types de compte Administrateur, Utilisateur de périphérique et Lecture seule, consultez la section « Utilisateurs locaux ».

Comment réinitialiser son compte après avoir oublié son mot de passe



REMARQUE : la réinitialisation de votre carte de gestion réseau réinitialisera la carte à sa configuration par défaut.

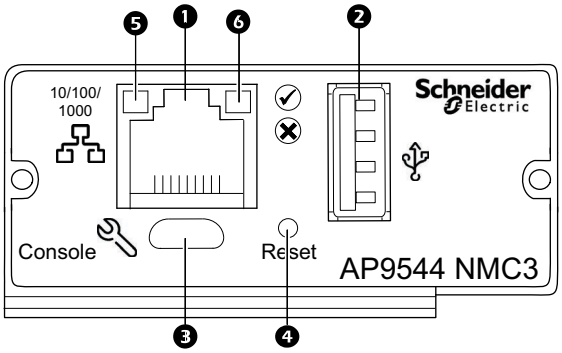
Si vous avez oublié votre mot de passe, vous devez utiliser le bouton **Réinitialiser** situé sur la carte de gestion réseau afin d'effacer toute la configuration, y compris le mot de passe. Maintenez le bouton **Réinitialiser** pendant 20 à 25 secondes, en veillant à ce que le voyant LED d'état clignote en vert cette fois. Lorsque le voyant LED d'état passe de l'ambre à l'orange, relâchez le bouton **Réinitialiser** pour permettre à la carte de gestion réseau de terminer le processus de redémarrage.

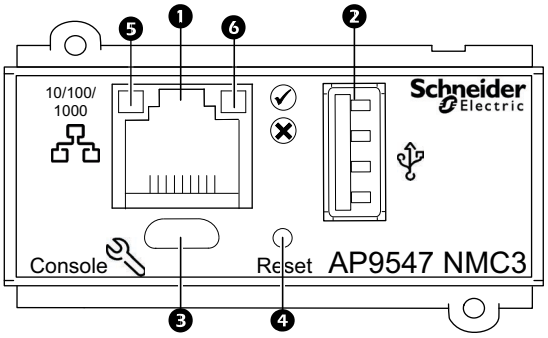
Une fois la carte de gestion réseau redémarrée, vous devez la reconfigurer. Pour de plus amples informations, consultez le **Guide d'installation de la carte de gestion réseau pour onduleur Easy UPS** ou l'article **FA156064** de la Base de connaissances.



Il est recommandé d'exporter le fichier .Ini après avoir configuré votre carte de gestion réseau afin de prévenir toute perte de données en cas de perte du mot de passe. Reportez-vous à la section « Récupération et exportation du fichier .ini ».

Panneau avant (AP9544/AP9547)





	Elément	Description
❶	Connecteur 10/100/1000 Base-T	Permet de connecter la carte de gestion réseau au réseau Ethernet.
❷	Port USB	Prise en charge des mises à jour du microprogramme de la carte de gestion réseau et de l'onduleur et de l'appareil Wi-Fi USB APC (AP9834) en option. Voir "Update the UPS firmware from a USB drive" et « Écran Wi-Fi ». Le port hôte USB-A de la carte de gestion réseau AP9544 prend en charge une entrée à contact sec et deux relais de sortie lorsqu'il est connecté à l'accessoire « USB vers contact sec » en option de la carte de gestion réseau (AP9811).
❸	Port de console USB	Permet de connecter la carte de gestion réseau à un ordinateur local via un câble micro-USB (référence APC 960-0603), afin de configurer les paramètres réseau initiaux ou d'accéder à l'interface de commande par ligne (CLI).
❹	Bouton de réinitialisation	Permet de redémarrer l'interface de gestion réseau. **REMARQUE :** cela n'affecte pas l'alimentation de sortie du périphérique dans lequel la carte de gestion réseau est installée.
❺	Voyant de liaison RX/TX (10/100/1000)	Reportez-vous à la section « Voyant de liaison RX/TX (10/100/1000) ».
❻	Voyant d'état	Un voyant LED (light-emitting diode) est une source de lumière. Reportez-vous à la section « Voyant d'état ».

Description des voyants

Voyant d'état

Ce voyant LED (light-emitting diode) indique l'état de la carte de gestion réseau.

État	Description
Off (Arrêt)	Il peut s'agir d'une des situations suivantes : • La carte de gestion réseau n'est pas alimentée. • La carte de gestion réseau n'est pas installée correctement. Elle doit peut-être être réparée ou remplacée. Veuillez contacter l'assistance clients. Reportez-vous à la section « Assistance clients internationale ».
Vert fixe	Les paramètres TCP/IP de la carte de gestion réseau sont valides.
Orange fixe	Il peut s'agir d'une des situations suivantes : • Une panne de matériel a été détectée dans la carte de gestion réseau. Veuillez contacter l'assistance clients. Reportez-vous à la section « Assistance clients internationale ». • La carte de gestion réseau est en mode Bootmonitor. Reportez-vous à la section « À propos de la carte de gestion réseau et des modules de micrologiciel » pour en savoir plus.
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 en alternance	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 utilisez un serveur BOOTP ou DHCP, consultez le **Guide d'installation de la carte de gestion réseau pour onduleur Easy UPS** afin de configurer les paramètres TCP/IP de la carte.
2. Pour utiliser un serveur DHCP, reportez-vous à la section « Options de réponse DHCP ».

REMARQUE : si le câble micro-USB reste connecté pendant que la carte de gestion réseau est en train de démarrer, celle-ci attendra 90 secondes pour accéder au moniteur de démarrage. Reportez-vous à la section « Utilisation du protocole XMODEM pour mettre à niveau une carte de gestion réseau ». Aucun voyant n'est actif pendant ce délai. Il est recommandé de débrancher le câble micro-USB si l'accès local à la CLI n'est pas nécessaire.

Voyant de liaison RX/TX (10/100/1000)

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

État	Description
Off (Arrêt)	Vous êtes dans au moins l'une des situations suivantes : • La carte de gestion réseau n'est pas alimentée. • Le câble reliant la carte de gestion au réseau est déconnecté ou ne fonctionne pas correctement. • L'équipement 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. Reportez-vous à la section « Assistance clients internationale ».
Jaune fixe	La carte de gestion réseau est connectée à un réseau fonctionnant à 10 à 100 mégabits par seconde (Mbit/s).

État	Description
Vert fixe	La carte de gestion réseau est connectée à un réseau fonctionnant à 1 000 Mbit/s.
Jaune clignotant	La carte de gestion réseau reçoit ou transmet des paquets de données à 10 à 100 Mbit/s.
Vert clignotant	La carte de gestion réseau reçoit ou transmet des paquets de données à 1 000 Mbit/s.

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. Lors du redémarrage pour restauration suite à un problème interne, un événement **System: Network Interface restarted** (Système : interface réseau redémarrée) est enregistré dans le journal d'événements.

Interface réseau du mécanisme de surveillance

La carte de gestion réseau implémente de nombreux mécanismes de surveillance internes 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), elle suppose la présence d'un problème sur l'interface réseau et redémarre.

Réinitialisation du compteur réseau

Pour s'assurer que la carte de gestion réseau ne redémarre pas si le réseau est inactif pendant 9,5 minutes, le mécanisme de surveillance essaye 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 le compte à rebours de 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 redémarrera assez souvent le compteur de 9,5 minutes pour éviter à la carte de gestion réseau de redémarrer.

Déconnexion automatique

Par défaut, les utilisateurs seront automatiquement déconnectés des interfaces Web et CLI de la carte de gestion réseau après 3 minutes d'inactivité. Le délai de déconnexion par défaut de chaque utilisateur peut être ajusté par le biais de l'interface Web :

Configuration > Sécurité > Utilisateurs locaux > Gestion

- Cliquez sur l'hyperlien du nom d'utilisateur du compte que vous voulez modifier.
- Dans la rubrique Délai d'expiration de session, modifiez le nombre de minutes.

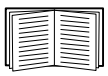
Déconnexion automatique	Durée (min.)
Par défaut	3
Minimum	1
Maximum	60 (1 h)

Interface utilisateur Web

Introduction

Présentation

L'interface utilisateur Web fournit les options pour gérer l'onduleur et la carte de gestion réseau (NCMC) de l'onduleur, ainsi que pour afficher l'état de l'onduleur.



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

Navigateurs Web pris en charge

L'IU Web de la carte de gestion réseau est compatible avec :

- Systèmes d'exploitation Windows® :
  - La dernière version de Microsoft® Edge®

    REMARQUE : l'écran de mise à jour du microprogramme de l'onduleur n'est pas compatible avec le navigateur Edge®. Reportez-vous à la section « Clients PowerChute Network Shutdown ».

- Tous les systèmes d'exploitation :
  - Les dernières versions de Mozilla® Firefox® ou Google® Chrome®

D'autres navigateurs courants peuvent fonctionner mais n'ont pas été entièrement testés.

La carte de gestion réseau ne peut pas fonctionner avec un serveur proxy. Avant de pouvoir utiliser un navigateur pour accéder à l'interface utilisateur de la carte de gestion réseau, vous devez effectuer l'une des opérations suivantes :

- Configurez le navigateur pour désactiver l'utilisation d'un serveur proxy pour la carte de gestion réseau.
- Configurez le serveur proxy de manière à ce qu'il ne mandate 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 utilisateur. Utilisez votre nom d'utilisateur et votre mot de passe (sensibles à la casse) pour vous connecter. Le nom d'utilisateur par défaut est différent selon les types de compte :

- `apc` pour l'administrateur ou le super-utilisateur
- `périphérique` pour un utilisateur de périphérique
- `readonly` pour un utilisateur lecture seule

Voir également « Types de comptes utilisateur ».

Vous pouvez définir la langue de l'interface utilisateur au moment de la connexion en la sélectionnant dans la liste déroulante **Langue**. Reportez-vous à la section « Changement de la langue de l'interface utilisateur ».



Lorsque HTTPS est activé, la carte de gestion réseau génère son propre certificat. Ce certificat permet de négocier les méthodes de chiffrement avec votre navigateur. Reportez-vous au **Manuel de sécurité** pour de plus amples détails.

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 un port de serveur Web différent du port par défaut dans Internet Explorer, vous devez inclure `http://` ou `https://` dans l'URL.

REMARQUE : HTTP est désactivé par défaut et HTTPS est activé par défaut.

Messages d'erreur des navigateurs courants lors de la connexion.

Message d'erreur	Navigateur	Cause de l'erreur
« This page cannot be displayed » [Impossible d'afficher la page].	Internet Explorer	L'accès à Internet est désactivé ou l'URL n'est pas correcte.
« Unable to connect » [Impossible de se connecter]	Firefox, Chrome	

Exemples de formats d'URL. Voir également « Paramètres TCP/IP pour l'écran IPv6 ».

Exemple et mode d'accès	Format d'URL
Nom DNS de `Web1`	
HTTP	`http://Web1`
HTTPS	`https://Web1`
Pour une adresse IP système `139.225.6.133` et un port de serveur Web par défaut (80) :	
HTTP	`http://139.225.6.133`
HTTPS	`https://139.225.6.133`
Pour une adresse IP système `139.225.6.133` et un port de serveur Web par défaut (5000) :	
HTTP	`http://139.225.6.133:5000`
HTTPS	`http://139.225.6.133:5000`
Adresse IPv6 système `2001:db8:1::2c0:b7ff:fe00:1100` et port de serveur Web différent du port par défaut (5000)	
HTTP	`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`

Première connexion

Lors de la première connexion à votre carte de gestion réseau, il vous sera demandé de modifier le mot de passe du super-utilisateur (`apc`). Une fois connecté, vous serez dirigé vers l'écran Présentation du récapitulatif de configuration. Cet écran présente tous les protocoles du système ainsi que leurs valeurs actuelles (p. ex. activé/désactivé). Vous pouvez accéder à cet écran à tout moment par la suite en suivant le chemin d'accès : **Configuration > Réseau > Récapitulatif**.

Écran d'accueil

Présentation

Chemin d'accès : Accueil

Sur l'écran **Accueil** de l'interface, vous pouvez voir les alarmes actives et les événements les plus récents enregistrés dans le journal de consignation des événements.

Une ou plusieurs icônes avec un texte complémentaire indiquent l'état de fonctionnement actuel de l'onduleur :

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

Dans l'angle supérieur droit de chaque écran, les mêmes icônes indiquent l'état de l'onduleur. Si une alarme **Critique** ou un **Avertissement** est présent(e), le nombre d'alarmes actives est également affiché.

Pour afficher le journal de consignation des événements complet, cliquez sur **Autres événements**.

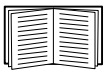
Icônes et liens

Pour faire de n'importe quel écran l'écran « accueil » (c'est-à-dire l'écran qui s'affiche lorsque vous vous connectez pour la première fois), accédez à cet écran et cliquez sur  l'icône dans l'angle supérieur droit.

Cliquez sur  pour revenir à l'affichage de l'écran d'accueil lorsque vous vous connectez.

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

- Lien 1 : la page **Base de connaissances** de www.se.com contenant des informations de dépannage utiles
- Lien 2 : la page **Informations sur le produit** du site Web www.se.com contenant des informations en arrière-plan sur votre matériel
- Lien 3 : la page **Téléchargements** du site Web www.se.com contenant le microprogramme et le logiciel disponibles.

 Pour reconfigurer les liens, consultez la section « Écran de configuration des liens ».

Surveillance de l’onduleur : Menu État

Les options ci-dessous ne sont pas disponibles pour tous les onduleurs.

Les options du menu État indiquent l’état actuel de votre onduleur et de votre réseau.

Vous pouvez configurer votre onduleur et votre réseau en utilisant les options du menu Configuration ; voir Configuration de vos paramètres : 1 et Configuration de vos paramètres : 2

Consultez les sections suivantes :

- Onduleur dans le menu État
- Aperçu du menu État
- Mesures dans le menu État
- E/S universelle dans le menu État
- Entretien dans le menu État

Onduleur dans le menu État

Chemin d’accès : État > Onduleur

Les options ci-dessous ne concernent que les appareils monophasés Easy UPS On-Line dotés d’une carte AP9544.

Affiche la charge de l’onduleur, la charge de la batterie, la tension et d’autres informations utiles.

Champ	Description
Mesures à l’entrée de l’onduleur	
Tension	Tension en courant alternatif (VCA) reçue par l’onduleur.
Fréquence	Fréquence, en Hertz, de la tension d’entrée.
Tension maximum	La tension d’entrée la plus élevée sur l’onduleur pendant la minute de fonctionnement précédente.
Tension minimale	La tension d’entrée la plus faible sur l’onduleur pendant la minute de fonctionnement précédente.
Mesures à la sortie de l’onduleur	
Tension	Tension en courant alternatif (VCA) que l’onduleur fournit à sa charge.
Courant	Courant, en ampères, appliqué à la charge.
Pourcentage de puissance active	Puissance active, en pourcentage.
Fréquence	Valeur réelle de la fréquence de tension de sortie, en Hertz.
Pourcentage de puissance apparente	Puissance apparente, en pourcentage.

Champ	Description
Mesures des batteries de l'onduleur	
Tension de batterie	Tension en CC des batteries.
Capacité restante de la batterie	Pourcentage de capacité de la batterie d'onduleur, disponible pour supporter la charge connectée.
Dernier remplacement de batterie	Dernière date à laquelle une batterie a été remplacée, au format MM/JJ/AA.
Tension nominale de la batterie	Capacité de tension nominale des batteries de l'onduleur; tension CC que les batteries sont censées fournir lorsque l'onduleur les utilise pour l'alimentation en sortie.
Température interne	Température à l'intérieur de l'onduleur.
Autonomie restante	Durée, en heures et minutes, pendant laquelle l'onduleur peut supporter sa charge tout en étant alimenté par la batterie.
Courant de la batterie	Courant en sortie de la batterie.
Capacité de la batterie	Pourcentage de la capacité de la batterie de l'onduleur disponible pour prendre en charge l'équipement connecté.
Plage de fréquence de dérivation	
Limite inférieure	Limite inférieure de la plage de fréquence de dérivation, en Hertz (Hz).
Limite supérieure	Limite supérieure de la plage de fréquence de dérivation, en Hertz (Hz).
Plage de tension du mode Éco	
Limite inférieure	Limite inférieure de la plage de tension du mode Éco.
Limite supérieure	Limite supérieure de la plage de tension du mode Éco.
État du bloc-batteries de l'onduleur	
Bloc-batteries N	État du bloc-batteries de l'onduleur. Par exemple, **Installé**, **Non installé**.
ID de batterie	ID du bloc-batteries.

Aperçu du menu État

Chemin d'accès : État > Aperçu

Les options ci-dessous ne concernent que les onduleurs triphasés pris en charge, dotés d'une carte AP9547.

Cela offre un aperçu sur l'onduleur, notamment les alarmes actives, la capacité de la batterie et d'autres informations utiles.

Champ	Description
État instantané	
Charge	Graphique indiquant la charge de l'équipement relié supporté par l'onduleur, en pourcentage de puissance nominale.
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.

Champ	Description
Tension d'entrée	Tension CA (Vca) reçue entre phases de l'onduleur.
Tension de sortie	Tension CA (Vca) que l'onduleur fournit à la charge.
Autonomie restante	Durée, en heures et minutes, pendant laquelle l'onduleur peut supporter sa charge tout en étant alimenté par la batterie.
Dernier transfert de batterie	Le motif du dernier passage à l'alimentation par batterie de l'onduleur.
Température ambiante	Température à l'intérieur de l'onduleur.
Evénements de périphérique récents	
Une liste des événements récents de l'onduleur dans l'ordre chronologique inverse. Pour afficher le journal de consignation des événements complet, cliquez sur **Autres événements**.	

Mesures dans le menu État

Les options ci-dessous ne concernent que les onduleurs triphasés pris en charge, dotés d'une carte AP9547.

Chemin d'accès : État > Mesures > Entrée

Champ	Description
Fréquence	Fréquence, en Hertz, de la tension d'entrée.
Tension	Tension CA (Vca), en volts, reçue par chaque phase de l'onduleur.
Courant	Intensité, en ampères, du courant fourni par la tension d'entrée pour chaque phase.

Chemin d'accès : État > Mesures > Dérivation

Champ	Description
Fréquence	Fréquence, en Hertz, de la tension d'entrée de dérivation.
Tension	Tension CA (Vca), en volts, mesurée entre phases de l'entrée de dérivation. La tension phase-neutre n'est pas mesurée.

Chemin d'accès : État > Mesures > Sortie

Champ	Description
Puissance active totale	Charge exercée sur la sortie de l'onduleur par l'équipement relié, en kW.
Puissance apparente totale	Charge exercée sur la sortie de l'onduleur par l'équipement relié, en kVA.
Pourcentage de charge totale en sortie	Taux de puissance (charge) de l'équipement relié supporté par l'onduleur, en pourcentage de puissance nominale.
Fréquence	Valeur réelle de la fréquence de tension de sortie, en Hertz.

Champ	Description
Puissance nominale apparente de sortie	Valeur maximale (en kVA) disponible pour l'onduleur. Si la charge est supérieure à cette valeur, une alarme de surcharge est générée.
Tension	Tension CA (Vca), en volts, que chaque phase de l'onduleur fournit à sa charge.
Courant	Courant, en ampères, appliqué à la charge par chaque phase.
Puissance active	Charge exercée sur la chaque phase de l'onduleur par l'équipement relié, en kW.
Puissance apparente	Identifie la charge placée sur chaque phase de l'onduleur par l'équipement connecté, en kVA.

Chemin d'accès : État > Mesures > Batterie

Champ	Description
Autonomie restante	Durée, en heures et minutes, pendant laquelle l'onduleur peut supporter sa charge tout en étant alimenté par la batterie.
Capacité restante de la batterie	Charge de batterie mesurée, en pourcentage de la capacité de charge maximum
Autonomie de la batterie	Durée pendant laquelle l'onduleur fonctionne sur batterie au lieu de l'alimentation secteur CA.
Tension de batterie (+/-)	Valeur réelle de la tension mesurée de la batterie en CC.
Courant de la batterie (+/-)	Valeur réelle du courant de batterie mesuré.
Température de la batterie	Valeur réelle de la température de la batterie.
Résultat du dernier test de la batterie	Résultat du test automatique de la batterie.
Dernier transfert de batterie	Le motif du dernier passage à l'alimentation par batterie de l'onduleur.

Chemin d'accès : État > Mesures > Autres paramètres

Champ	Description
Mode Éco	Indique si le mode Éco est activé ou désactivé. Lorsque l'onduleur est réglé pour fonctionner en mode Économie et que la tension secteur est dans la plage de tolérance, l'onduleur fonctionne en mode « Hors ligne », directement sur le secteur (ou dérivation) et revient en mode « En ligne » (ou inverseur) lorsque la tension secteur n'est plus dans la plage de tolérance.
Type d'onduleur	Indique comment l'onduleur est configuré : Simple, Redondant 1+1, Parallèle ou Parallèle 3:3.
Secteur CA	Indique si la tension secteur CA est utilisée comme source pour le convertisseur de puissance.

Champ	Description
État du commutateur de dérivation statique de l'onduleur	Ce commutateur est interne à l'onduleur et permet à l'appareil de commutation de placer l'onduleur en mode Dérivation Lorsque le commutateur de dérivation statique est fermé, la source fournit l'alimentation à la charge et l'appareil de commutation peut placer l'onduleur en mode Dérivation. Lorsque le commutateur de dérivation statique est ouvert, l'onduleur fournit l'alimentation à la charge.

E/S universelle dans le menu État

Chemin d'accès : Chemin d'accès : État > E/S universelle

Cette option n'est pas disponible pour tous les appareils.

Contacts d'entrée affiche le nom, le statut d'alarme et l'état (ouvert ou fermé) de chaque contact. Ils sont automatiquement localisés et affichés ici lorsque vous installez l'accessoire environnemental. Pour afficher l'état détaillé d'un contact d'entrée ou configurer ses valeurs, cliquez sur son nom. Si les contacts sont configurés et désactivés, ils ne s'affichent pas à cet endroit. Pour de plus amples informations, reportez-vous à la section **Écran Contacts d'entrée**.

Relais de sortie affiche le nom et l'état (ouvert ou fermé) de chaque relais. Ils sont automatiquement localisés et affichés ici lorsque vous installez l'accessoire environnemental. Pour afficher l'état détaillé d'un relais de sortie ou configurer ses valeurs, cliquez sur son nom. Pour de plus amples informations, reportez-vous à la section **Écran Relais de sortie**.

Événements environnementaux récents affiche les événements liés à votre surveillance environnementale, par exemple une violation de seuil de température ou un message d'avertissement concernant un contact de surveillance environnementale. Cliquez sur le lein **Autres événements** pour afficher la liste complète des événements récents.

Réseau dans le menu État

Chemin d'accès : État > Réseau

L'écran Réseau vous indique votre adresse IP, votre nom de domaine et les paramètres de port Ethernet. Voir Réseau dans le menu Configuration pour des informations détaillées sur les champs.

Entretien dans le menu État

Chemin d'accès : État > Entretien

Les options ci-dessous ne concernent que les onduleurs triphasés pris en charge, dotés d'une carte AP9547.

Cela offre un aperçu sur l'onduleur, notamment les alarmes actives, la capacité de la batterie et d'autres informations utiles.

Champ	Description
Cycle d'entretien	
Condensateur CC	Cycle d'entretien du condensateur CC.
Condensateur CA	Cycle d'entretien du condensateur CA.
Alimentation électrique d'appoint	Cycle d'entretien de l'alimentation électrique d'appoint.
Filtre à air	Cycle d'entretien du filtre à air.
Batterie	Cycle d'entretien de la batterie.
Cycle de garantie	
Garantie	Cycle de garantie de l'onduleur.
Durée de fonctionnement	
Condensateur CA	Durée de fonctionnement du condensateur CA depuis son dernier remplacement.
Condensateur CC	Durée de fonctionnement du condensateur CC depuis son dernier remplacement.

Contrôle de l’onduleur

Les options ci-dessous ne sont pas disponibles pour tous les onduleurs.

Les options du menu Contrôle vous permettent de prendre des mesures immédiates affectant votre onduleur et vos sorties, et comprennent également quelques fonctions de sécurité et réseau. Consultez les sections suivantes :

- « Onduleur dans le menu Contrôle »
- « Sécurité dans le menu Contrôle »
- « Réseau dans le menu Contrôle »

Onduleur dans le menu Contrôle

Chemin d’accès : Contrôle > Onduleur

Les options ci-dessous ne concernent que les appareils monophasés Easy UPS On-Line dotés d’une carte AP9544.

Lorsque vous choisissez une case d’option et cliquez sur Suivant, un autre écran résume l’action à effectuer ; cliquez sur Appliquer à ce stade pour poursuivre l’action.

Action	Description
Redémarrer l’onduleur	Redémarre l’équipement relié en mettant l’onduleur hors tension, puis sous tension. Les paramètres suivants contrôlent le redémarrage : • Délai d’arrêt • Capacité minimum de la batterie • Délai de rétablissement
Mise hors tension de l’onduleur	Désactive immédiatement l’alimentation de sortie de l’onduleur, sans délai d’arrêt. L'ondulateur reste hors tension jusqu’à ce que vous le mettiez à nouveau sous tension.
Mettre l’onduleur en veille	Met l’onduleur en mode Veille en désactivant l’alimentation de sortie pour une période définie par les paramètres suivants : Cliquez sur Suivant pour afficher des détails spécifiques sur la temporisation et les délais. • L’onduleur attend les délais configurés comme « Délai d’arrêt » avant de se mettre hors tension. • Lorsque l’alimentation d’entrée est rétablie, l’onduleur active son alimentation de sortie après deux périodes configurées: « Durée de veille » et « Délai de rétablissement ».
Mettre l’onduleur en mode Dérivation/ Sortir l’onduleur du mode Dérivation	Ces options contrôlent l’utilisation du mode de dérivation, qui permet de procéder à des entretiens sur l’onduleur sans qu’il soit nécessaire de le mettre hors tension.

Action	Description
Signaler l'arrêt du serveur PowerChute®	Sélectionnez cette option pour demander à tous les serveurs configurés comme « Clients PowerChute Network Shutdown » qui sont en communication avec cet onduleur de se mettre hors tension conformément aux valeurs configurées pour « Paramètres d'arrêt de PowerChute ». Cette option ne notifiera pas les serveurs lors de l'exécution d'actions de contrôle de dérivation.

Sécurité dans le menu Contrôle

Chemin d'accès : Contrôle > Sécurité > Gestion des sessions

Les écrans donnent des détails sur les utilisateurs qui sont connectés, l'interface qu'ils utilisent (par exemple l'interface utilisateur Web, l'interface par ligne de commande), leur adresse IP et leur durée de connexion.

Si vous disposez de droits suffisants, cliquez sur le nom pour voir quels moyens d'authentification ont été utilisés pour valider l'utilisateur. Vous pouvez alors également utiliser le bouton **Mettre fin à la session** pour déconnecter un utilisateur.

Réseau dans le menu Contrôle

Chemin d'accès : Contrôle > Réseau > Réinitialiser/Redémarrer

Utilisez ces options pour réinitialiser différentes options de la carte de gestion réseau et de l'interface utilisateur.

Action	Description
Redémarrer l'interface de gestion	Redémarre l'interface de gestion (par exemple l'interface utilisateur Web, l'interface par ligne de commande) en vous déconnectant. L'onduleur et la carte de gestion réseau ne sont pas redémarrés.
Réinitialiser tout[1]	Attention : Cette option réinitialise toutes les valeurs configurables aux valeurs par défaut. • Si vous ne sélectionnez pas **Exclure TCP/IP**, toutes les valeurs et tous les paramètres sont réinitialisés à leurs valeurs par défaut, y compris le paramètre qui détermine la façon dont ce périphérique obtient ses valeurs de configuration TCP/IP ainsi que la configuration EAPoL. La valeur par défaut des paramètres de configuration TCP/IP est DHCP et celle de l'accès EAPoL est Désactivé. • Si vous ne sélectionnez pas **Exclure TCP/IP**, toutes les valeurs et tous les paramètres, à l'exception du paramètre qui détermine la façon dont ce périphérique obtient ses valeurs de configuration TCP/IP, sont réinitialisés à leurs valeurs par défaut.
Réinitialisation uniquement[1]	**TCP/IP** : Réinitialise uniquement le paramètre qui détermine la façon dont ce périphérique doit obtenir sas valeurs de configuration TCP/IP, y compris la configuration EAPoL qui est réinitialisée sur Désactivé. La valeur par défaut du paramètre de configuration TCP/IP est DHCP et celle de l'accès EAPoL est Désactivé.
	Configuration des événements : Réinitialise les événements à leur configuration par défaut. Tout événement ou groupe spécifiquement configuré reviendra également à la valeur par défaut. Reportez-vous à la section « Menu Notification »
	Alarmes de perte de communication environnementale : Réinitialise l'alarme de perte de communication environnementale qui est déclenchée lorsqu'un périphérique du port E/S universelle est débranché.

[1]La réinitialisation peut prendre jusqu'à 1 minute. Le nom de l'onduleur que vous avez configuré n'est pas réinitialisé (voir « Écrans Onduleur - Généralités »).

Configuration de vos paramètres : 1

Les options ci-dessous ne sont pas disponibles pour tous les onduleurs.

Les options du menu Configuration vous permettent de définir les valeurs de fonctionnement fondamentales de votre onduleur et de votre carte de gestion réseau.

Consultez les sections ci-dessous, ainsi que « Configuration de vos paramètres : 2 ».

- « Paramètres d'alimentation dans le menu Configuration »
- « Menu Sécurité »
- « Écrans Onduleur - Généralités »
- « Écran Programme de test automatique »
- « Arrêt dans le menu Configuration »
- « Planification de l'arrêt »
- « Clients PowerChute Network Shutdown »
- « Menu Sécurité »

REMARQUE : Vous pouvez consulter quelques-uns de vos paramètres de configuration sur l'écran Synthèse de la configuration (**Configuration > Réseau > Synthèse**).

Paramètres d'alimentation dans le menu Configuration

Chemin d'accès : Configuration > Paramètres d'alimentation

Les options ci-dessous ne concernent que les appareils monophasés Easy UPS On-Line dotés d'une carte AP9544.

La **tension nominale de sortie** est la tension en courant alternatif que l'onduleur fournit à la charge lorsqu'il fonctionne sur batterie. Vous pouvez configurer les types suivants d'éléments spécifiques à l'appareil :

- Tension de transfert **élevée** et **basse** : la tension de transfert élevée et basse, en Vca.
- **Fréquence de sortie** : Fréquence d'entrée et de sortie en hertz (Hz).

Écrans Onduleur - Généralités

Chemin d'accès : Configuration > Onduleur

Champ	Description
Nom de l'onduleur	Nom permettant d'identifier l'onduleur.
Dernier remplacement de batterie	Entrez le mois et l'année du dernier remplacement de la batterie de l'onduleur.
Nombre de 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.

Chemin d'accès : Configuration > Onduleur > Alimentation

Les options ci-dessous ne concernent que les onduleurs triphasés pris en charge, dotés d'une carte AP9547.

Les seuils d'alarme sont basés sur l'autonomie et l'alimentation redondante disponibles, ainsi que sur la charge de l'onduleur. Vous pouvez configurer le seuil **Alarme en cas de surcharge**, qui déclenche une alarme si la charge dépasse la valeur configurée, en kVA.

Écran Programme de test automatique

Chemin d'accès : Onduleur > Configuration > Programme de test automatique

Les options ci-dessous ne concernent que les appareils monophasés Easy UPS On-Line dotés d'une carte AP9544.

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

Arrêt dans le menu Configuration

Chemin d'accès : Configuration > Arrêt

Utilisez cet écran pour configurer les paramètres d'arrêt d'un onduleur. Voir le tableau ci-dessous ainsi que « Arrêt anticipé contrôlé et Fin de l'arrêt ».

Début de l'arrêt

Définissez les délais et les durées pris en considération lorsque l'arrêt d'un onduleur est requis.

Champ	Description
Autonomie avec batterie faible	Pour un onduleur sur batterie, cela définit le seuil d'autonomie restant, en dessous duquel un état de batterie faible est déclenché sur l'onduleur. Par exemple, si l'autonomie avec batterie faible est définie sur dix minutes et que l'autonomie prévue restante de l'onduleur atteint dix minutes ou moins, un état de batterie faible est déclenché. Si l'alimentation d'entrée n'est pas rétablie sur l'onduleur, celui-ci sera mis hors tension une fois la batterie épuisée. Un état de batterie faible déclenche un arrêt sur tous les clients PowerChute Network Shutdown associés à la carte de gestion réseau.
Délai maximal requis	Calcule 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 progressif. • Il s'agit du délai d'arrêt le plus long que requiert un serveur répertorié comme client PowerChute Network Shutdown. • Il est calculé chaque fois que l'interface de gestion de l'onduleur est mise sous tension ou réinitialisée, ou lorsque vous sélectionnez l'option *Négociation forcée* et que vous cliquez sur Appliquer. Reportez-vous à la section « Délais d'arrêt et PowerChute Network Shutdown ».

Durée de l'arrêt

Spécifiez la durée pendant laquelle l'onduleur est mis hors tension.

Champ	Description
Durée de veille	Définit la durée pendant laquelle l'onduleur garde sa sortie hors tension lorsque vous exercez une commande Veille de l'onduleur. Quand l'onduleur est mis hors tension, il se remet en marche après l'expiration de la durée de veille définie ici, augmentée de la durée de retour. Si l'alimentation secteur n'a pas été rétablie à ce stade, l'onduleur attendra qu'elle soit rétablie pour se remettre en marche. La commande Veille peut être exécutée sur l'écran de l'onduleur, le « Onduleur dans le menu Contrôle », via la commande SNMP ou via PowerChute Business Edition.

Paramètres d’arrêt de PowerChute

Chemin d’accès : Configuration > PowerChute > Configuration de PowerChute®



Il s’agit du chemin de navigation pour les onduleurs triphasés dotés d’une carte AP9547.

Ces options ne sont pas disponibles sur tous les onduleurs.

Spécifiez les paramètres d’arrêt utilisés par PowerChute Network Shutdown.

Champ	Description
Délai maximal requis - Négociation forcée	L’activation de la *négociation forcée* réinitialise la valeur de délai maximale requise à la durée de la batterie faible. La carte de gestion réseau envoie un paquet d’états mis à jour à tous les agents PowerChute enregistrés. PowerChute compare ensuite la durée de batterie faible envoyée dans ce paquet à sa durée d’arrêt totale requise et augmente le délai maximal requis en conséquence, ou le délai d’arrêt pour le groupe de sorties avec lequel elle est enregistrée. PowerChute effectue un contrôle de vérification de l’autonomie restante toutes les 30 secondes, ce qui permet de comparer la durée d’arrêt totale requise de PowerChute à la durée de batterie faible de la carte de gestion réseau. Sélectionner l’option Négociation forcée permet de réinitialiser le délai de mise hors tension pour tous les groupes de sorties à la même valeur que la durée de batterie faible. L’option Négociation forcée peut prendre jusqu’à dix minutes pour calculer la valeur requise par tous les clients PowerChute enregistrés sur la carte de gestion réseau. Pour de plus amples informations, reportez-vous à la section Délais d’arrêt et PowerChute Network Shutdown.
Délai négocié maximal	Le délai négocié maximal est le délai d’arrêt le plus long que requiert un serveur répertorié comme client PowerChute Network Shutdown pour s’arrêter en toute sécurité lorsque l’onduleur lance un arrêt progressif. Ce délai est calculé lorsque l’interface de gestion de l’onduleur est activée ou réinitialisée.
Comportement en cas d’arrêt sur batterie	Définissez le comportement d’un onduleur après un arrêt : • Redémarrer une fois l’alimentation rétablie - Lorsque l’alimentation secteur est rétablie, redémarrez l’onduleur. • Arrêt définitif - L’onduleur reste hors tension, même si l’alimentation secteur est rétablie.
Nom d’utilisateur	Saisissez le nom d’utilisateur à utiliser pour PowerChute.
Phrase d’authentification	Cette phrase est utilisée pour l’authentification entre PowerChute et la carte de gestion réseau. La phrase est vide par défaut ; vous devez la définir avant de pouvoir activer PowerChute.
Protocoles de communication PCNS	Sélectionnez le protocole de communication pour communiquer avec PowerChute : HTTPS ou HTTP.

Arrêt anticipé contrôlé et Fin de l’arrêt.



Ces options ne sont pas disponibles sur tous les onduleurs.

Les options Arrêt anticipé contrôlé vous permettent d'arrêter un onduleur sur batterie lorsque l'une QUELCONQUE des conditions que vous spécifiez est remplie :

- 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. (L'autonomie est la durée pendant laquelle l'onduleur peut utiliser la batterie pour continuer d'alimenter la charge actuelle.)
- Lorsque la charge de la batterie est inférieure à un pourcentage défini de sa capacité totale.
- Lorsque la charge sur la sortie de l'onduleur est inférieure à un seuil fixé en pourcentage.

Avec **Maintenir hors tension après rétablissement de de l'alimentation**, vous pouvez également décider si l'onduleur se remet en marche ou pas une fois l'alimentation secteur c.a. rétablie.

Les options **Fin d'arrêt** vous permettent de définir un état et un délai déterminant quand un onduleur peut se remettre en marche après le rétablissement de l'alimentation secteur c.a.. En fonction du modèle d'onduleur, vous pouvez spécifier une **Capacité minimum de la batterie** ou **"Min Return Runtime"** l, avant que l'onduleur ne se remette en marche.

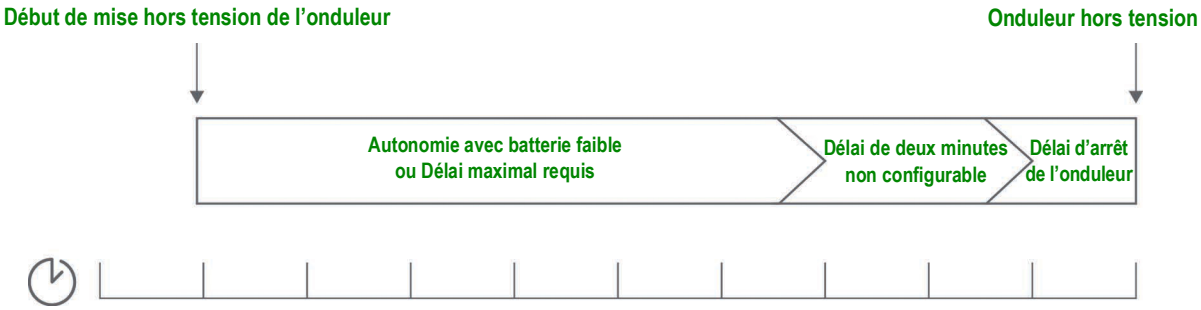
Délais d'arrêt et PowerChute Network Shutdown.

La section suivante décrit comment la durée de batterie faible, le délai maximal requis et les délais de mise hors tension des groupes de sorties impactent la séquence d'arrêt de PowerChute.

Pour de plus amples informations sur la séquence d'arrêt de PowerChute, consultez le **Guide de l'utilisateur**.

Pour les deux types d'onduleurs, avec et sans groupes de sorties, le délai d'arrêt est négocié par interaction entre la carte de gestion réseau et PowerChute Network Shutdown, comme suit :

Groupes de sorties d'alimentation. Pour un onduleur SANS groupes de sorties, le délai d'arrêt correspond à la valeur la plus élevée du **délai maximal requis** ou de l'**autonomie avec batterie faible** sur l'écran **Arrêt** de la carte de gestion réseau, augmentée d'un délai de 2 minutes non configurable et du délai d'arrêt de l'onduleur.



Onduleur sans groupes de sorties -Durée d'arrêt en minutes

Remarque : Si un arrêt a été déclenché par un état Batterie faible, la valeur Autonomie avec batterie faible prévaut sur la valeur Délai maximal requis.

Remarques :

Pour de plus amples informations sur les séquences d'arrêt de PowerChute, consultez la rubrique « *Exemples de scénarios d'arrêt* » dans le **Guide de l'utilisateur** de PowerChute Network Shutdown, disponible sur le site Web de Schneider Electric.

Pendant la comparaison de la durée d'arrêt requise de PowerChute et du délai maximal requis/ délai de mise hors tension des groupes de sorties, la valeur la plus grande est utilisée. Par exemple, si la durée d'arrêt de la ligne de commande du client PowerChute est définie sur 8 minutes, mais que l'autonomie avec batterie faible de l'onduleur est de 10 minutes, la carte de gestion réseau utilise la valeur la plus grande de 10 minutes pour le délai maximal requis.

En mode Négociation forcée, la carte de gestion réseau interroge les clients PowerChute pour obtenir le temps d'arrêt requis de chacun d'eux. Par conséquent, la mise à jour des valeurs de délai maximal requis/délai de mise hors tension des groupes de sorties peut prendre jusqu'à dix minutes.

PowerChute ne modifie jamais la valeur du champ **Autonomie avec batterie faible** de la carte de gestion réseau.

Avec PowerChute Network Shutdown v3.x ou ultérieure, la valeur **Délai maximal requis** n'est jamais utilisée par la carte de gestion réseau pour un onduleur avec groupes de sorties.

Planification de l'arrêt

Chemin d'accès : Configuration > Planification

Les options ci-dessous ne concernent que les appareils monophasés Easy UPS On-Line dotés d'une carte AP9544.

REMARQUE : Ne créez pas de programmes d'arrêt qui se chevauchent. Par exemple, si un arrêt hebdomadaire est défini entre 20 h 00 et 21 h 00, et qu'un arrêt ponctuel est défini entre 20 h 10 et 20 h 30, cela présente un chevauchement des programmes d'arrêt. Le chevauchement des programmes d'arrêt entraîne un comportement inconnu et imprévisible.

Pour l'onduleur

Vous pouvez planifier l'arrêt d'un onduleur sous **Onduleur**.

Les arrêts planifiés configurés s'affichent en haut de la page lorsque vous sélectionnez **Onduleur**, avec les détails correspondants, notamment s'ils sont actuellement activés ou désactivés.

Modification, activation, désactivation ou suppression d'un arrêt planifié. Cliquez sur le nom du calendrier dans la liste de planification en haut de l'écran **Onduleur**. Cet écran affiche les détails complets et vous permet de modifier les paramètres. Vous pouvez notamment le désactiver temporairement en décochant la case **Activer** ou le supprimer définitivement.

Création d'un calendrier d'arrêt de l'onduleur.

1. Dans l'onglet **Planification**, sélectionnez **Onduleur.**
2. Utilisez les cases d'option pour sélectionner le type d'arrêt à planifier, **Arrêt ponctuel**, **Arrêt quotidien** ou **Arrêt hebdomadaire**, puis cliquez sur le bouton **Suivant**.
3. Pour désactiver un calendrier temporairement, décochez la case **Activer**.
4. Indiquez le nom ainsi que la date et l'heure de planification.
   Pour les arrêts hebdomadaires, spécifiez la fréquence dans la liste déroulante.
5. Précisez si l'appareil doit se remettre en marche après l'arrêt :

   Remise en marche : Spécifiez si l'onduleur doit se remettre en marche à une date et une heure spécifiques, **Jamais** (l'onduleur doit être remis en marche manuellement) ou **Immédiatement** (l'onduleur sera remis en marche après un délai de 6 minutes).

Signaler les clients PowerChute Network Shutdown : Indiquez si les clients PowerChute doivent être notifiés ; voir « Clients PowerChute Network Shutdown ».

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

Clients PowerChute Network Shutdown

Chemin d'accès : Onduleur > Configuration > PowerChute

Le chemin de navigation pour les onduleurs triphasés dotés d'une carte AP9547 est **Configuration > PowerChute > PowerChute®.**

PowerChute Network Shutdown peut arrêter vos onduleurs à distance.

Lorsque vous installez un client PowerChute Network Shutdown à votre réseau, il est automatiquement ajouté à cette liste. Lorsque vous désinstallez un client PowerChute Network Shutdown, il est automatiquement retiré.

Cliquez sur **Ajouter 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.

Avec les groupes de sorties, vous devez également spécifier quel groupe de sorties fournit l'alimentation au client PowerChute.

REMARQUE : PowerChute ne peut pas se connecter à la carte de gestion réseau si le protocole HTTP est désactivé sur cette carte. Consultez la rubrique « Écran d'accès Web » pour activer le protocole HTTP ou HTTPS.

Menu Sécurité

Le menu **E/S universelle** est opérationnel lorsque vous avez installé l'USB sur l'accessoire à contact sec de la carte de gestion réseau (AP9811). Leur utilisation est souvent appelée surveillance environnementale.

Écran Contacts d'entrée

Chemin d'accès : E/S universelle > Contacts d'entrée

Contacts d'entrée affiche le nom, le statut d'alarme et l'état (ouvert ou fermé) de chaque contact. Ils sont automatiquement localisés et affichés ici lorsque vous installez l'accessoire environnemental.

Pour afficher l'état détaillé d'un contact d'entrée ou configurer ses valeurs, cliquez sur son nom. S'il est désactivé, le contact ne génère aucune alarme même si sa position est anormale. Les autres champs sont exposés ci-dessous :

Champ	Description
État d'alarme	**Normal** si le contact d'entrée ne signale aucune alarme ou la gravité de l'alarme s'il en signale une. Si un contact n'est pas activé, il affiche **Désactivé**.
États	État actuel de ce contact d'entrée : **Fermé** ou **Ouvert**.
État normal	État normal (sans alarme) du contact d'entrée : **Fermé** ou **Ouvert**.
Gravité	Gravité de l'alarme générée par l'état anormal du contact d'entrée : **Avertissement** ou **Critique**.

Écran Relais de sortie

Chemin d'accès : E/S universelle > Relais de sortie

Relais de sortie affiche le nom et l'état (ouvert ou fermé) de chaque relais. Ils sont automatiquement localisés et affichés ici lorsque vous installez l'accessoire environnemental.

Pour afficher l'état détaillé d'un relais de sortie ou configurer ses valeurs, cliquez sur son nom. Les champs sont exposés ci-dessous :

Champ	Description
États	État actuel du relais de sortie : **Fermé** ou **Ouvert**.
État normal	État normal (sans alarme) du relais de sortie : **Fermé** ou **Ouvert**.
Commande	Pour modifier l'état actuel de ce relais de sortie, sélectionnez cette case à cocher et cliquez sur Appliquer.
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. Si d'autres alarmes paramétrées se produisent après le début du délai, celui-ci ne redémarre pas, mais continue à s'écouler jusqu'à l'activation du relais de sortie.
Suspendre	Nombre minimal 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 expiration de cette période.

Configuration de la politique de contrôle

Chemin d'accès : E/S universelle > Politique de contrôle

Sur la carte de gestion réseau AP9544 avec USB connecté o l'accessoire à contact sec de la carte de gestion réseau (AP9811), vous pouvez :

- configurer les relais de sortie pour qu'ils s'ouvrent ou se ferment en fonction des événements d'onduleur et des contacts d'entrée, voir **Configuration d'une sortie en réponse à un événement**
- configurer l'onduleur pour qu'il effectue des actions en fonction des contacts d'entrée, voir **Configuration de l'onduleur ou d'une sortie en réponse à une alarme en entrée**

Tous les onduleurs ne peuvent pas être configurés pour répondre aux contacts d'entrée.

Configuration d'une sortie en réponse à un événement.

1. Dans le menu **Configuration**, sélectionnez **E/S universelle** et **Politique de contrôle**.
2. Cliquez sur le bouton **Ajouter une politique**.
3. Cliquez sur le nom d'une catégorie ou d'une sous-catégorie pour afficher les événements correspondants.
4. Pour configurer un événement, cliquez sur son nom, sélectionnez la case à cocher du relais de sortie qui changera d'état lorsque cet événement surviendra, puis cliquez sur **Enregistrer la politique**.

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

1. Dans le menu **Configuration**, sélectionnez **E/S universelle** et **Politique de contrôle**.
2. Cliquez sur le bouton **Ajouter une politique**.
3. Cliquez sur la sous-catégorie **Contact d’E/S**.
4. Choisissez l’événement ayant la même gravité que le contact d’entrée. Par exemple, si la gravité du contact d’entrée est critique, choisissez l’événement critique.
5. Dans la rubrique **Commande de contrôle de l’appareil**, sélectionnez l’action que l’onduleur effectuera (le cas échéant) lorsque l’entrée change d’état.
6. Dans la rubrique **Commande du relais de sortie**, sélectionnez la sortie qui va s’ouvrir ou se fermer (le cas échéant).
7. Cliquez sur **Enregistrer la politique**.



L’action ainsi configurée est effectuée une seule fois.

Si vous rétablissez l’entrée à son état normal avant que la condition d’alarme soit désactivée, la sortie ne s’ouvrira pas ou ne se fermera pas à nouveau, sauf si la condition d’alarme est désactivée, puis se reproduit.

Menu Sécurité

Écran Gestion des sessions

Chemin d’accès : Configuration > Sécurité > Gestion des sessions

Si l’option **Autoriser les connexions simultanées** est activé, deux utilisateurs ou plus peuvent se connecter simultanément. Chaque utilisateur dispose d’un accès identique et chaque interface (HTTP, FTP, console telnet, console série (interface par ligne de commande), etc.) est comptabilisée comme un utilisateur connecté. L’option **Autoriser les connexions simultanées** permet de connecter au maximum huit utilisateurs à l’interface Web, cinq utilisateurs à l’interface par ligne de commande et un utilisateur à la console série de manière simultanée.

Effacement de l’authentification distante : La carte de gestion réseau prend en charge le stockage Radius des mots de passe sur un serveur. Toutefois, si vous activez ce remplacement, la carte de gestion réseau permettra à un utilisateur local de se connecter en utilisant le mot de passe de la carte stocké localement sur cette dernière. Voir également « Utilisateurs locaux » et « Authentification des utilisateurs distants ».

Réponse ping

Chemin d’accès : Configuration > Sécurité > Réponse ping

Cochez la case **Réponse ping IPv4** pour permettre à la carte de gestion réseau 3 de répondre aux tests Ping du réseau. Ceci ne s’applique pas au mode IPv6.

Utilisateurs locaux

Utilisez ces options de menu pour afficher et configurer l’accès et les préférences individuelles (comme le format de date affiché) pour les interfaces utilisateur de la carte de gestion réseau. Cela s’applique aux utilisateurs tels que définis par leur nom de connexion.

Chemin d’accès : Configuration > Sécurité > Utilisateurs locaux > Gestion

Configuration de l'accès utilisateur. Avec cette option, un administrateur ou un super-utilisateur peut afficher et configurer les utilisateurs autorisés à accéder à l'interface utilisateur. Cliquez sur le lien de nom pour afficher les détails d'un utilisateur, et pour le modifier ou le supprimer.

Cliquez sur **Ajouter un utilisateur** pour ajouter un utilisateur. Dans l'écran **Configuration utilisateur** résultant, vous pouvez ajouter un utilisateur et lui interdire l'accès en décochant la case **Accès**. La longueur maximale du nom et du mot de passe est de 64 octets, cette valeur étant inférieure pour les caractères multi-octets. Vous devez saisir un mot de passe.



Si le nom et le mot de passe dépassent 64 octets, ils peuvent être tronqués.
Pour modifier le paramétrage d'un administrateur/super-utilisateur, vous devez saisir les trois champs de mot de passe.

Créez un mot de passe en utilisant une combinaison de caractères minuscules et majuscules, de chiffres et de caractères spéciaux. Les mots de passe ne peuvent pas dépasser 64 caractères ASCII.

Utilisez l'option **Délai d'expiration de la session** pour configurer le délai pendant lequel cette interface utilisateur attend avant de déconnecter cet utilisateur (trois minutes par défaut). Si vous modifiez cette valeur, vous devez vous déconnecter pour que la modification prenne effet.

Remplacement de l'authentification distante série : En sélectionnant cette option, vous pouvez contourner RADIUS en utilisant la connexion à la console série (interface par ligne de commande). Cet écran l'active pour l'utilisateur sélectionné, mais elle doit également être activée globalement pour fonctionner, via « Écran Gestion des sessions ».

Voir également la section « Configuration > Sécurité > Utilisateurs locaux > Paramètres par défaut » ci-dessous. Pour des informations de base sur les comptes, reportez-vous à la section « Types de comptes utilisateur ».

Préférences utilisateur. Cochez la case **Code couleur du journal de consignation des événements** pour activer le codage couleur du texte d'alarme enregistré dans le journal 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** : alarme critique qui nécessite une action immédiate.
Orange	**Avertissement** : alarme nécessitant votre attention et susceptible de compromettre vos données ou votre équipement si le problème n'est pas corrigé.
Vert	**Alarme effacée** : amélioration des conditions ayant déclenché l'alarme.
Noir	**Normal** : pas d'alarme. La Carte de gestion réseau et tous les appareils connectés fonctionnent normalement.
Bleu :	**Informatif** : alarme destinée à fournir des informations. La Carte de gestion réseau et tous les appareils connectés fonctionnent normalement.

Format d'exportation des journaux : les fichiers journaux exportés peuvent être formatés en CSV (valeurs séparées par des virgules) ou à l'aide de tabulations. Reportez-vous à la section « Pour afficher le journal de consignation des événements ».

Sélectionnez l'échelle de température pour les mesures dans cette interface utilisateur. **Unités de mesure américaines** correspond aux degrés Fahrenheit et **Système métrique** correspond aux degrés Celsius.

Vous pouvez spécifier la langue par défaut de l'interface utilisateur dans le champ **Langue**. Vous pouvez également le faire lors de la connexion.

Vous pouvez également spécifier différentes langues pour les destinataires d'e-mails et les récepteurs de traps SNMP. Reportez-vous aux sections « Destinataires de l'e-mail » et « Récepteurs de traps ».

Chemin d'accès : Configuration > Sécurité > Utilisateurs locaux > Paramètres par défaut

La configuration de valeurs par défaut permet d'accélérer l'ajout d'utilisateurs. Utilisez cette option pour définir les valeurs par défaut pour de nombreuses options de l'écran Gestion ;
« Configuration > Sécurité > Utilisateurs locaux > Gestion » ci-dessus.

Authentification des utilisateurs distants

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

Authentification. Indiquez le mode d'authentification requis des utilisateurs lors de la connexion.

Pour de plus amples informations sur l'authentification locale (qui n'utilise pas l'authentification centralisée d'un serveur RADIUS), reportez-vous au **Manuel de sécurité** disponible sur le site Web de Schneider Electric.

APC accepte les fonctions d'authentification et d'autorisation RADIUS (Remote Authentication Dial-In User Service) suivantes :

- Lorsqu'un utilisateur accède à la carte de gestion réseau ou à un 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'utilisateur 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. Reportez-vous à la section « Utilisateurs locaux ».
- **Authentification RADIUS, puis locale** : les deux 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** : il n'y a pas d'authentification locale.

  Si l'option **RADIUS uniquement** est sélectionnée et que le serveur RADIUS est indisponible, incorrectement identifié ou incorrectement configuré, l'accès à distance est indisponible pour tous les utilisateurs. Pour rétablir l'accès, vous devez vous connecter à l'interface par ligne de commande à l'aide d'une connexion série et modifier le paramètre **accès** en lui attribuant la valeur **local** ou **radiusLocal**.

  Par exemple, la commande pour modifier le paramètre d'accès à la valeur **local** serait :`radius -a local`

Voir également la section « Écran RADIUS » ci-dessous.« Configuration du serveur RADIUS »

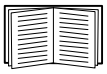
Écran RADIUS

Chemin d'accès : Configuration > Sécurité > Utilisateurs distants > RADIUS

Vous pouvez utiliser un serveur RADIUS pour authentifier les utilisateurs distants. Utilisez cette option pour effectuer ce qui suit :

- Répertorier les serveurs RADIUS (deux au maximum) disponibles pour la carte de gestion réseau ainsi que le délai d'attente de chacun d'eux.
- Configurer les paramètres d'authentification pour un serveur RADIUS nouveau ou existant en cliquant sur un lien **Serveur Radius**.

Paramètre RADIUS	Description
Serveur RADIUS	Nom ou adresse IP du serveur (IPv4 ou IPv6). **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. La carte de gestion réseau prend en charge les ports 1812, 5000 jusqu'à 32768.
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 d'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 au serveur RADIUS.

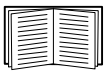


Reportez-vous également à la section « Authentification des utilisateurs distants » ci-dessus et à la section « Configuration du serveur RADIUS » ci-dessous.

Configuration du serveur RADIUS

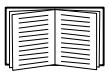
Récapitulatif de la procédure de configuration.

Vous devez configurer votre serveur RADIUS pour qu'il fonctionne avec la carte de gestion réseau ; voir les étapes ci-dessous.



Pour des exemples de 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** disponible sur le site Web de Schneider Electric.

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'attributs Service-Type sauf si des attributs fournisseur (VSA) sont définis. Si aucun attribut Service-Type n'est configuré, les utilisateurs ne disposent que de l'accès en lecture seule (uniquement sur l'interface utilisateur).



Consultez la documentation relative à votre serveur RADIUS pour en savoir plus sur le fichier des utilisateurs RADIUS et le **Manuel de sécurité** pour avoir un exemple.

1. Les VSA peuvent être utilisés au lieu des attributs Service-Type fournis par le serveur RADIUS. Les VSA nécessitent une entrée de dictionnaire et un fichier d'utilisateur RADIUS. Dans le fichier 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 échoueront. Les VSA ont priorité sur les attributs 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 l'une des deux méthodes suivantes pour authentifier les utilisateurs :

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

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

- Ajoutez les noms d'utilisateurs et attributs au fichier « utilisateur » 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.

FreeRADIUS v1.x et v2.x, et Microsoft Server 2008 et 2012 Network policy Server (NPS) sont pris en charge. Les autres applications RADIUS couramment disponibles peuvent fonctionner, mais il se peut qu'elles ne soient pas entièrement testées.

Écrans Pare-feu

Chemin d'accès : Configuration > Sécurité > Pare-feu > Configuration

Active ou désactive la fonctionnalité de pare-feu. La politique configurée est indiquée par défaut. Cochez la case **Activer** pour activer le pare-feu. La case est décochée par défaut.

- Cliquez sur **Appliquer** pour confirmer une politique de pare-feu que vous avez choisi d'activer. La page **Confirmation de pare-feu** s'ouvre.
  - La page Confirmation contient une recommandation pour tester le pare-feu avant de l'activer. Ce n'est pas obligatoire.
  - Le premier hyperlien renvoie vers la page Politique de pare-feu.
  - Le second hyperlien renvoie vers la page Test de pare-feu.
  - Cliquez sur **Appliquer** pour activer le pare-feu et retourner à la page Configuration.
  - Cliquez sur **Annuler** pour retourner à la page Configuration sans activer le pare-feu.
- Cliquez sur **Annuler** : Aucune nouvelle sélection ne sera activée. Vous restez sur la page Configuration.

Chemin d'accès : Configuration > Sécurité > Pare-feu > Politique active

Sélectionnez une politique active dans la liste déroulante Politiques disponibles et vérifiez la validité de cette politique. La politique active actuelle est affichée par défaut ; vous pouvez sélectionner une autre politique dans la liste.

- Cliquez sur **Appliquer** pour activer vos modifications. Si un autre pare-feu a été sélectionné et activé, la modification prend immédiatement effet. Si un une politique de pare-feu nouvellement configurée a été sélectionnée, il est recommandé de tester le nouveau pare-feu avant de l'activer. (Voir la section Configuration ci-dessus.)
- Cliquez sur **Annuler** pour rétablir la politique active originale et rester sur la page Politique active.

Chemin d'accès : Configuration > Sécurité > Pare-feu > Règles actives

Lorsqu'un pare-feu est activé, cette page en lecture seule répertorie les règles individuelles appliquées par une politique active actuelle. Consultez la section **Créer/modifier une politique** pour obtenir des descriptions des champs (Priorité, Destination, Source, Protocole, Action et Journal).

Chemin d'accès : Configuration > Sécurité > Pare-feu > Créer/modifier une politique

Créer une nouvelle politique ou modifier une politique existante :

REMARQUE : Bien que vous ne puissiez pas supprimer une politique de pare-feu active, vous pouvez modifier une politique exécutée, mais cela n'est pas recommandé, car les modifications sont appliquées immédiatement. Désactivez plutôt le pare-feu, modifiez la politique, testez-la, puis réactivez-la.

Créer une nouvelle politique : Cliquez sur **Ajouter une politique** et tapez le nom du nouveau fichier de pare-feu. Le nom de fichier doit comporter une extension de fichier .fwl. Si aucune extension de fichier n'est spécifiée, fwl sera ajouté au nom automatiquement.

- Cliquez sur **Appliquer**. Si le nom du fichier est valide, le fichier vide de police de pare-feu sera créé. Il sera disponible dans le dossier /fwl avec les autres politiques présentes dans le système.
- Cliquez sur **Annuler** pour retourner à la page précédente sans créer de nouveau fichier de pare-feu.

Modifier une politique existante :

Sélectionnez **Modifier une politique** pour aller à la page de modification. Vous pouvez modifier une politique de pare-feu qui n'est pas active.

Page d'avertissement : Si vous tentez de modifier la politique active, une page d'avertissement s'ouvre : **« La modification de la politique de pare-feu active entraînera l'application immédiate des modifications apportées. Il est recommandé de désactiver le pare-feu et de tester la politique avant de l'activer. »**

- Cliquez sur **Appliquer** pour quitter la page Avertissement et retourner à la page Modifier la politique.
- Cliquez sur **Annuler** pour quitter la page Avertissement et retourner à la page Créer/modifier une politique.

1. Sélectionnez la politique que vous souhaitez modifier dans la liste déroulante **Nom de politique**, puis cliquez sur **Modifier la politique**.
2. Cliquez sur **Ajouter une règle** ou sélectionnez la **Priorité** d'une règle existante pour aller à la page **Modifier la règle**. Sur cette page, vous pouvez modifier les paramètres de règle ou supprimer la règle sélectionnée.

Paramètre	Description
Priorité	Si deux règles entrent en conflit, celle ayant le plus haut niveau de priorité prévaudra. Le niveau de priorité le plus haut est 1 ; le plus bas est 250.
Type	**hôte** : dans le champ IP/tout, vous saisirez une seule adresse IP. **sous-réseau** : dans le champ IP/tout, vous saisirez une adresse de sous-réseau. **plage** : dans le champ IP/tout, vous saisirez une plage d'adresses IP.
IP/tout	Spécifiez l'adresse IP ou la plage d'adresses à laquelle cette règle s'applique, ou sélectionnez l'une des options suivantes : • **tout** La règle s'applique indépendamment de l'adresse IP. • **anyipv4** : la règle s'applique pour n'importe quelle adresse IPv4. • **anyipv6** : la règle s'applique pour n'importe quelle adresse IPv6.
Port	Spécifiez un port auquel la règle s'applique. • **Aucun** : la règle s'appliquera à n'importe quel port. • **Ports courants configurés** : sélectionnez un port standard. • **Autre** : spécifiez un numéro de port non standard.
Protocole	Spécifiez à quel protocole la règle s'applique. • **tout** : n'importe quel protocole. • **tcp** : utilisé pour un transfert fiable des informations entre les applications. • **udp**: solution de rechange au TCP utilisée pour un transfert d'informations plus rapide et utilisant moins de bande passante. Bien qu'il présente moins de délais, l'UDP est moins fiable que le TCP. • **icmp** : utilisé pour signaler les erreurs pour le dépannage. • **icmpv6** : utilisé pour signaler les erreurs pour le dépannage sur les applications utilisant IPv6.
Action	**autoriser** : autoriser le paquet qui correspond à cette règle. **rejeter** : rejeter le paquet qui correspond à cette règle.
Journal	Si cette règle est appliquée au paquet, que celui-ci soit bloqué ou autorisé, cela ajoutera une entrée au journal de pare-feu. Reportez-vous à la section « Journal de consignation du pare-feu ».

Il est recommandé d'ajouter l'une des règles suivantes comme règle de priorité la plus basse dans votre politique de pare-feu :

- Pour ajouter le pare-feu comme une liste d'autorisation, ajoutez
  `250 Dest any / Source any / protocol any / discard`
- Pour ajouter le pare-feu comme une liste de blocage, ajoutez
  `250 Dest any / Source any / protocol any / allow`

Supprimer une politique :

Sélectionnez **Supprimer une politique** pour ouvrir la page Confirmer la suppression.

Cliquez sur **Appliquer** pour confirmer ; le fichier de pare-feu sélectionné sera supprimé du système de fichiers.

Chemin d'accès : Configuration > Sécurité > Pare-feu > Charger la politique

Chargez une politique (avec le suffixe .fwl) depuis une source externe à ce périphérique.

Chemin d'accès : Configuration > Sécurité > Pare-feu > Test

Appliquez temporairement les règles d'une politique choisie, pour une période que vous spécifiez.

Configuration de sécurité 802.1X

Chemin d'accès : Configuration > Sécurité > Sécurité 802.1X

La carte de gestion réseau assume le rôle de demandeur dans une architecture EAPoL (Extensible Authentication Protocol over LAN) utilisée pour le contrôle d'accès réseau basé sur le port IEEE 802.1X. La carte de gestion réseau prend en charge EAP-TLS comme méthode d'authentification qui vous demande de téléverser 3 certificats côté client. La clé privée est stockée dans un format chiffré. Vous devez fournir une secrète valide pour pouvoir activer l'accès de sécurité 802.1X.

REMARQUE : La carte de gestion réseau ne prend en charge que la méthode d'authentification EAP-TLS.

L'interface utilisateur basée sur le Web offre les options suivantes pour la configuration EAPoL :

Paramètre	Description
Accès EAPoL	Utilisé pour activer ou désactiver l'accès de sécurité 802.1X. **REMARQUE :** L'accès de sécurité 802.1X est désactivé par défaut. Vous ne pouvez activer l'accès que si des certificats valides et une phrase secrète valide pour la clé privée ont été fournis.
Identifiant du demandeur	Vous permet de définir votre propre identifiant de demandeur (limite de 32 caractères, espaces comprises). **REMARQUE :** Par défaut, l'identifiant du demandeur est défini sur « NMC-Supplicant-xx: xx:xx:xx:xx:xx », où six octets de « xx » représentent l'ID MAC de la carte de gestion réseau.
Certificat CA	Téléversez/remplacez ou supprimez un certificat racine CA. Les formats de fichiers pris en charge sont PEM (Privacy Enhanced Mail) ou DER (Distinguished Encoding Rules) avec extension de fichier autorisée .pem, .PEM, .der ou .DER.
Certificat de clé privée	Téléversez/remplacez ou supprimez une clé privée chiffrée. Les formats de fichiers pris en charge sont PEM (Privacy Enhanced Mail) ou DER (Distinguished Encoding Rules) avec extension de fichier autorisées .key ou .KEY. **REMARQUE :** Les clés privées non chiffrées ne sont pas acceptées.
Phrase secrète de la clé privée	Fournissez la phrase secrète pour déchiffrer ou chiffrer la clé privée. Limite de 64 caractères, espaces comprises.
Certificat utilisateur/public	Téléversez/remplacez ou supprimez un certificat utilisateur/public. Les formats de fichiers pris en charge sont PEM (Privacy Enhanced Mail) ou DER (Distinguished Encoding Rules) avec extension de fichier autorisée .pem, .PEM, .der ou .DER.

Configuration de vos paramètres : 2

Les options du menu Configuration vous permettent de définir les valeurs de fonctionnement fondamentales de votre onduleur et de votre carte de gestion réseau.

Consultez les sections ci-dessous, ainsi que « Configuration de vos paramètres : 1 ».

- « Réseau dans le menu Configuration »
- « Menu Notification »
- « Menu Généralités »
- « Journaux dans le menu Configuration »

REMARQUE : Vous pouvez consulter quelques-uns de vos paramètres de configuration sur l'écran Synthèse de la configuration(**Configuration > Réseau > Synthèse**).

Réseau dans le menu Configuration

Paramètres TCP/IP pour l'écran IPv4

Chemin d'accès : Configuration > Réseau > TCP/IP > Paramètres IPv4

Cette option affiche l'adresse IPv4, le masque de sous-réseau, la passerelle par défaut, l'adresse MAC et le mode de démarrage de la carte de gestion réseau. Utilisez la partie inférieure de l'écran pour configurer ces paramètres, y compris la désactivation d'IPv4.

Pour en savoir plus sur les options DHCP et DHCP, reportez-vous à RFC2131 et RFC2132.

Option	Description
Manuel	Spécifiez ici l'adresse IPv4, le masque de sous-réseau et la passerelle par défaut.
BOOTP*	Toutes les 32 secondes, le périphérique demande une attribution réseau à n'importe quel serveur BOOTP : • S'il reçoit une réponse valide, il démarre les services réseau. • Si des paramètres réseau ont déjà été configurés et qu'il ne reçoit aucune réponse valide à cinq requêtes (requête initiale plus quatre autres tentatives), il utilise les paramètres précédemment configurés. Cela garantit qu'il reste accessible si un serveur BOOTP n'est plus disponible. • S'il trouve un serveur BOOTP, mais que la requête à ce serveur échoue ou dépasse le délai d'attente, le périphérique abandonne ses requêtes de paramètres réseau jusqu'à son redémarrage.
DHCP*	Toutes les 32 secondes, le périphérique demande une attribution réseau à n'importe quel serveur DHCP : • S'il trouve un serveur DHCP, mais que la requête à ce serveur échoue ou dépasse le délai d'attente, il abandonne ses requêtes de paramètres réseau jusqu'à son redémarrage. • Le cas échéant, vous pouvez configurer le périphérique avec l'option **Cookie du fournisseur nécessaire pour accepter l'adresse DHCP** afin d'accepter le bail et de démarrer les services réseau. Reportez-vous à la section « Options de réponse DHCP ».

*Catégorie de fournisseur : APC
ID client : adresse MAC du périphérique. Si vous modifiez cette valeur, la nouvelle valeur doit être unique sur le réseau local.
Catégorie d'utilisateur : nom du module du firmware de l'application. Reportez-vous à la section « Mises à niveau du micrologiciel de la carte de gestion réseau ».

Paramètres TCP/IP pour l'écran IPv6

Chemin d'accès : Configuration > Réseau > TCP/IP > Paramètres IPv6

Cette option affiche les paramètres IPv6 actuels de la carte de gestion réseau. Utilisez la partie inférieure de l'écran pour configurer ces paramètres, y compris la désactivation d'IPv6.

Vous avez le choix entre l'adressage IP manuel et automatisé. Il est possible d'utiliser les deux modes simultanément. Pour **Manuel**, cochez la case et entrez l'adresse **IPv 6** du système et la **passerelle par défaut**.

Cochez la case **Configuration automatique** pour permettre au système d'obtenir les préfixes d'adressage du routeur (le cas échéant). Il utilisera ces préfixes pour configurer automatiquement les adresses IPv6.

Formats IPv6 possibles	Description
fe80:0000:0000:0000:0204:61ff:fe9d:f156	Forme complète d'IPv6
fe80:0:0:0:204:61ff:fe9d:f156	Zéros à gauche supprimés
fe80::204:61ff:fe9d:f156	réduire plusieurs zéros à :: dans l'adresse IPv6
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 avec quatre nombres décimaux séparés par des points à la fin
fe80:0:0:0:0204:61ff:254.157.241.86	Zéros à gauche supprimés, IPv4 avec quatre nombres décimaux séparés par des points à la fin
fe80::204:61ff:254.157.241.86	Quatre nombres décimaux séparés par des points à la fin, réduction de plusieurs zéros
::1	hôte local
fe80::	Préfixe de liaison locale
2001::	Préfixe de monodiffusion global

Pour le **mode DHCPv6**, consultez le tableau ci-dessous.

Mode DHCPv6 pour la configuration IPv6	
Option	**Description**
Routeur contrôlé	Lorsque cette case d'option est sélectionnée, DHCPv6 est contrôlé par les indicateurs **M** (indicateur de configuration d'adresse géré) et **O** (autre indicateur de configuration avec état) reçus dans les annonces de routage IPv6. Lorsqu'une annonce de routage est reçue, la carte de gestion réseau vérifie si les indicateurs M et O sont définis. La carte de gestion réseau les interprète comme suit : • **Aucun n'est défini** : indique que 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 M et O sont définis** : dans ce cas, une configuration d'adresse DHCPv6 complète se produit. DHCPv6 est utilisé pour obtenir des adresses ET d'autres paramètres de configuration. On parle dans ce cas de « DHCPv6 avec état ». Une fois l'indicateur M reçu, la configuration d'adresse DHCPv6 reste en vigueur jusqu'à ce que l'interface en question soit fermée, même si les paquets d'annonces de routage ultérieurs sont reçus sans indicateur M défini. Si un indicateur O est reçu en premier, suivi ensuite d'un indicateur M, la carte de gestion réseau procède à une configuration d'adresse complète à la réception de l'indicateur M. • **Seul O est défini** : dans ce cas, la carte de gestion réseau envoie un paquet de requêtes d'information DHCPv6. DHCPv6 est utilisé pour configurer les « autres » paramètres (tels que l'emplacement des serveurs DNS), mais PAS pour fournir des adresses. On parle dans ce cas de « DHCPv6 sans état ».
Adresse et autres informations	DHCPv6 est utilisé pour obtenir des adresses ET d'autres paramètres de configuration. On parle dans ce cas de « DHCPv6 avec état ».
Informations hors adresse uniquement	DHCPv6 est utilisé pour configurer les « autres » paramètres (tels que l'emplacement des serveurs DNS), mais PAS pour fournir des adresses. On parle dans ce cas de « DHCPv6 sans état ».
Jamais	DHCPv6 n'est PAS utilisé pour les paramètres de configuration.

Options de réponse DHCP

Chaque réponse DHCP valide contient des options qui fournissent les paramètres TCP/IP nécessaires à la carte de gestion réseau pour fonctionner en réseau. Chaque réponse comporte également d'autres informations qui ont une incidence sur le fonctionnement de la carte de gestion réseau. Consultez également l'article **FA156110** de la base de connaissances.

Informations spécifiques au fournisseur (option 43). La carte de gestion réseau utilise cette option dans une réponse DHCP pour en déterminer la validité. Cette option contient une option 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 informe la carte de gestion réseau qu'un serveur DHCP est configuré pour prendre en charge les périphériques.

  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 dans **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 un renouvellement de cette attribution.
- **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 lier à nouveau ce bail.

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, par rapport au temps universel coordonné (TUC).
- **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 va utiliser (32 caractères maximum).
- **Nom de domaine** (option 15) : nom de domaine que la carte de gestion réseau va utiliser (64 caractères maximum).
- **Nom du fichier de démarrage** (à partir du champ **file (fichier)** de la réponse DHCP, décrit dans **RFC2131**) : chemin d'accès complet à un fichier de configuration utilisateur (fichier .ini) à 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.
- **Nom de domaine complet** (FQDN, option 81) : nom de domaine complet de la carte de gestion réseau.

Écran Vitesse du port

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

Le paramètre Vitesse du port définit la vitesse de communication du port du réseau Ethernet. Votre paramètre actuel est affiché dans **Vitesse actuelle**.

Vous pouvez modifier le paramètre en sélectionnant une case d'option sous **Vitesse du port** :

- En **Négociation automatique** (valeur par défaut), les périphériques réseau négocient les transmissions à la vitesse la plus élevée possible. Si les vitesses prises en charge de deux périphériques ne correspondent pas, la vitesse la plus lente est utilisée.
- Vous pouvez également choisir **10** Mbit/s ou **100** Mbit/s, avec dans chaque cas les options suivantes :
  - **semi-duplex** (communication dans un seul sens à la fois) ou
  - **duplex** (communication dans les deux sens sur le même canal simultanément).

REMARQUE : Vous ne pouvez modifier la vitesse du port qu'à 1 000 Mbit/s en sélectionnant le bouton radio **Négociation automatique**.

Écran DNS

Chemin d'accès : Configuration > Réseau > DNS > Configuration

Les valeurs figurant sous **État du système de noms de domaine** répertorient votre état et votre configuration actuels.

Utilisez les options sous **Paramètres manuels du système de noms de domaine** pour configurer le système de noms de domaine :

- Si l'option **Effacer les paramètres DNS manuels** est activée, les données de configuration d'autres sources comme DHCP sont ici prioritaires sur les configurations manuelles.
- Spécifiez le **serveur DNS primaire** et, le cas échéant, le **serveur DNS secondaire** avec les adresses IPv4 ou IPv6. 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 secondaire. Si elle ne reçoit pas de réponse passé 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, testez-les. Reportez-vous à la section « Test de l'écran DNS ».
- **Synchronisation du nom système** : si cette option est activée, le nom d'hôte DNS est synchronisé avec le nom système de la carte de gestion réseau. Cliquez sur le lien Nom système pour le définir.

  Si le nom d'hôte DNS et le nom système de la carte de gestion réseau sont synchronisés, la longueur du nom système est limitée à un certain nombre de caractères, selon les RFC du DNS. S'ils ne sont pas synchronisés, la longueur du nom système est limitée à 255 caractères.

- **Nom d'hôte** : une fois que vous avez configuré un nom d'hôte dans cette zone et un nom de domaine dans le champ **Nom de domaine**, les utilisateurs peuvent saisir 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 de domaine (IPv4/IPv6)** : pour l'interface de la carte de gestion réseau, vous devez configurer le nom de domaine uniquement ici. Dans tous les autres champs de cette interface qui acceptent les noms de domaines (à l'exception des adresses électroniques), la carte de gestion réseau ajoute ce nom de domaine par défaut lorsque seul un nom d'hôte est saisi.
  - 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 le nom d'hôte avec un point final (tel que `mySnmpServer.`) comme si c'était un nom de domaine complet et n'ajoute pas de nom de domaine.
- **Nom de domaine (IPv6)** : spécifiez ici le nom de domaine IPv6.

Test de l'écran DNS

Chemin d'accès : Configuration > Réseau > DNS > Test>

Utilisez cette option pour envoyer une requête DNS qui teste la configuration de vos serveurs DNS en recherchant l'adresse IP. Pour savoir comment configurer vos serveurs, reportez-vous à la section « Écran DNS ».

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

- Pour le **Type de requête**, sélectionnez la méthode à employer pour la requête DNS. Reportez-vous au tableau ci-dessous.
- Dans le champ **Question de la requête**, spécifiez la valeur à attribuer au type de requête sélectionné, comme indiqué dans le tableau.

Type de requête sélectionné	Question de la requête à utiliser
par hôte	Nom d'hôte, URL
par FQDN	Nom de domaine complet, `mon_serveur.mon_domaine.com`
par IP	Adresse du serveur
par MX	Adresse de messagerie

Écran d'accès Web

Chemin d'accès : Configuration > Réseau > Web > Accès

Utilisez cette option pour configurer la méthode d'accès à l'interface Web. (Afin d'activer des modifications ici, vous devez redémarrer la carte de gestion réseau. Reportez-vous à la section « Réseau dans le menu Contrôle »).

Vous pouvez autoriser l'accès à cette interface utilisateur via **HTTP** ou **HTTPS** ou via les deux protocoles au moyen des cases à cocher Activer. HTTP est désactivé par défaut et HTTPS est activé par défaut. HTTPS chiffre les noms d'utilisateurs, les mots de passe et les données durant la transmission, mais ce n'est pas le cas de HTTP.

HTTPS authentifie également la carte de gestion réseau au moyen d'un certificat numérique. Consultez la section « Créer et installer des certificats numériques » dans le **Manuel de sécurité** disponible sur le site Web de Schneider Electric pour voir comment utiliser les certificats numériques.

Pour les **ports**, vous pouvez modifier le paramètre sur n'importe quel port inutilisé afin de renforcer la sécurité ; la page s'étend de 5000 à 32768. Vous devez alors insérer 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(s)://152.214.12.114:5000
```

Écran du certificat SSL Web

Chemin d'accès : Configuration > Réseau > Web > Certificat SSL

Ajout, remplacement ou suppression d'un certificat de sécurité. SSL (Secure Socket Layer) est un protocole servant à chiffrer les données entre votre navigateur et le serveur Web.

L'**état** peut être :

- **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.
- **Certificat non installé** : aucun certificat n'est installé, ou le certificat a été installé par FTP ou SCP à un emplacement incorrect. L'option **Ajouter ou remplacer le fichier du certificat** installe le certificat à l'emplacement correct : **/ssl** sur la carte de gestion réseau.
- **Génération en cours** : la carte de gestion réseau est en train de générer un certificat car aucun certificat valide n'a été trouvé.
- **Chargement en cours** : un certificat est en cours d'activation sur la carte de gestion réseau.

Si vous installez un certificat non valide ou si aucun certificat n'est chargé lorsque le protocole SSL est activé, la carte de gestion réseau génère un certificat par défaut, ce qui peut retarder l'accès à l'interface d'une minute maximum. Vous pouvez utiliser le certificat par défaut pour les protocoles de sécurité chiffrés de base, auquel cas un message d'alerte de sécurité s'affiche chaque fois que vous vous connectez.

Ajouter ou remplacer le fichier du certificat : accédez au fichier de certificat créé avec l'assistant de sécurité. Consultez la section « Créer et installer des certificats numériques » dans le **Manuel de sécurité** disponible sur le site Web de Schneider Electric pour voir comment utiliser les certificats numériques créés par l'assistant de sécurité ou générés par la carte de gestion réseau.

Supprimer : supprime le certificat. Consultez également le texte à l'écran.

Écran de la console

Chemin d'accès : Configuration > Réseau > Console > Accès

Chemin d'accès : Configuration > Réseau > Console > Clé d'hôte SSH

Accès à la console. Vous devez activer l'accès à la console pour mettre à jour le firmware de l'onduleur. Reportez-vous à la section. L'accès à la console permet d'utiliser l'interface par ligne de commande.

Vous pouvez autoriser l'accès à cette interface via **Telnet** ou **SSH**, ou via les deux protocoles au moyen des cases à cocher Activer. Telnet est désactivé par défaut et SSH est activé par défaut. Contrairement à SSH, Telnet ne chiffre par les noms d'utilisateurs, les mots de passe et les données durant la transmission.

REMARQUE : Si vous activez SSH, SCP (SeCure CoPy) est également activé pour un transfert sécurisé des fichiers. Consultez la section « Mises à niveau du micrologiciel de la carte de gestion réseau » pour en savoir plus sur l'utilisation de SCP.

Pour les **ports** à utiliser pour la communication avec la carte de gestion réseau, vous pouvez choisir un port inutilisé compris entre 5000 et 32768 afin d'accroître la sécurité

- **Port Telnet** : la valeur de ce paramètre est 23 par défaut. Vous devez alors insérer le signe deux-points (:) ou un espace pour choisir un port autre que celui par défaut, selon les exigences du programme client Telnet.

  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` ***ou*** `telnet 152.214.12.114 5000`
- **Port SSH** : la valeur par défaut est 22. Consultez la documentation de votre client SSH pour connaître le format de ligne de commande requis pour spécifier un port autre que celui par défaut. Voir également la section « Clé d'hôte SSH » ci-dessous.

Clé d'hôte SSH. Si vous utilisez SSH (Secure Shell Protocol) pour l'accès à l'interface par ligne de commande de la console, vous devez ajouter, remplacer ou supprimer la clé d'hôte dans l'écran Clé de l'hôte SSL.

Le champ **État** indique si la clé d'hôte (clé privée) est valide. L'état peut être :

- **SSH désactivé :** aucune clé d'hôte utilisée.
- **Génération en cours** : la carte de gestion réseau est en train de créer une clé d'hôte car aucune clé d'hôte valide n'a été trouvée.
- **Chargement en cours** : une clé d'hôte est en cours d'activation sur la carte de gestion réseau.
- **Validité** : une des clés d'hôtes suivantes se trouve dans le répertoire **/ssh** (emplacement requis sur la Carte de gestion réseau) :
  - Clé d'hôte de 1 024 ou 2 048 bits créée par l'assistant de sécurité.
  - Clé d'hôte RSA de 2 048 bits générée par la Carte de gestion réseau

Ajouter ou Remplacer la clé d'hôte : permet de télécharger un fichier de clé d'hôte créé par l'assistant de sécurité. Pour utiliser l'assistant de sécurité, consultez le **Manuel de sécurité**. Pour utiliser une clé d'hôte créée en externe, chargez la clé avant d'activer SSH (avec « Accès à la console » ci-dessus).

REMARQUE : Pour réduire le temps nécessaire à l'activation du protocole SSH, créez une clé d'hôte et téléchargez-la à l'avance. *Si vous activez le protocole SSH sans qu'aucune clé d'hôte n'ait été chargée, il faut jusqu'à une minute à la carte de gestion réseau pour en créer une, durée pendant laquelle le serveur SSH est inaccessible.*

Supprimer : supprime la clé d'hôte. Consultez également le texte à l'écran.

Pour utiliser le protocole SSH, un client SSH doit être installé. La plupart des plateformes Linux et UNIX incluent un client SSH, contrairement aux systèmes d'exploitation Microsoft Windows (à l'exception de Windows 10). Les clients pour Windows sont disponibles auprès de plusieurs fournisseurs, tels que PuTTY, disponible sur **www.putty.org**.

Écrans SNMP

Tous les noms d'utilisateur, mots de passe et noms de communauté liés à SNMP sont transférés sur le réseau sous forme de texte brut. Si votre réseau requiert un chiffrement de sécurité élevée, désactivez l'accès SNMP ou paramétrez-le en lecture pour chaque communauté. (Une communauté disposant de l'accès en lecture peut recevoir des informations d'état et utiliser les traps SNMP.)

Lors de l'utilisation de **Data Center Expert** pour gérer un onduleur sur le réseau public d'un système, vous *devez* avoir SNMPv1 ou SNMPv3 activé dans l'interface de la carte de gestion réseau. L'accès en lecture seule permet au périphérique de recevoir les traps de la carte de gestion réseau. Un accès en écriture est cependant nécessaire lorsque vous utilisez l'interface utilisateur de la carte de gestion réseau pour définir le périphérique pour récepteur de traps.

Pour plus d'informations sur l'amélioration et la gestion de la sécurité de votre système, reportez-vous au **Manuel de sécurité**.

SNMPv1.

Chemin d'accès : Configuration > Réseau > SNMPv1 > Accès et contrôle d'accès

Utilisez **Accès** pour activer ou désactiver SNMP version 1 comme méthode de communication avec la carte de gestion réseau.



SNMPv1 est désactivé par défaut. Le **Nom de la communauté** doit être défini avant que les communications SNMPv1 puissent être établies.



L'utilisation de SNMPv2c est prise en charge par les options SNMPv1.

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 la carte de gestion réseau. Pour apporter une modification, cliquez sur un nom de communauté.

Par défaut, une entrée est affectée à chacune des quatre communautés SNMPv1 disponibles. Vous pouvez modifier ces paramètres afin d'appliquer *plusieurs entrées à une communauté* pour accorder l'accès via plusieurs adresses IPv4 et IPv6, noms d'hôte ou masques d'adresses IP spécifiques.

- Par défaut, une communauté a accès à la carte de gestion réseau depuis n'importe quel point du réseau.
- Si vous configurez plusieurs entrées de contrôle d'accès pour un nom de communauté, cela implique qu'une ou plusieurs des autres communautés n'auront pas accès au périphérique.

Nom de la communauté : le nom d'un poste de gestion réseau (NMS, Network Management Station) doit utiliser pour accéder à la communauté. La longueur maximale est de 16 caractères ASCII.

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 (par exemple 149.225.12.1) permet uniquement l'accès du système de gestion réseau 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 également 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.

- **Lecture** : commandes GET uniquement, à tout moment.
- **Écriture** : commandes GET à tout moment, commandes SET quand aucun utilisateur n'est connecté ni à l'interface utilisateur Web ni à l'interface par ligne de commande.
- **Écriture+** : commandes GET et SET à tout moment.
- **Désactiver** : aucune commande GET ou SET, à aucun moment.

SNMPv3.

Chemin d'accès : Configuration > Réseau > SNMPv3 > Accès, profils utilisateur et contrôle d'accès

Pour les destinataires de commandes GET, SET et de traps, SNMPv3 utilise un système de profils utilisateur pour identifier les utilisateurs. Un utilisateur SNMPv3 doit se voir attribuer un profil utilisateur dans le logiciel MIB pour exécuter des commandes GET et SET, naviguer dans la MIB et recevoir des traps.



SNMPv3 est désactivé par défaut. Un profil d'utilisateur valide doit être activé avec des phrases secrètes (**Phrases secrètes d'authentification**, **Phrase secrète de confidentialité**) définies avant que les communications SNMPv3 puissent être établies



Pour utiliser SNMPv3, vous devez avoir un programme MIB compatible avec SNMPv3.

La carte de gestion réseau prend en charge les protocoles d'authentification SHA et MD5 et les chiffrements AES et DES.

Activer l'accès SNMPv3 sous accès active cette méthode de communication avec ce périphérique.

Profils utilisateur. Répertorie par défaut les paramètres de quatre profils utilisateur, configurés avec les noms d'utilisateur **apc snmp profile1** jusqu'à **apc snmp profile4**, sans authentification ni confidentialité (pas de chiffrement). Pour modifier les paramètres suivants d'un profil utilisateur, cliquez sur le nom d'utilisateur dans la liste.

- **Nom d'utilisateur :** identifiant du profil utilisateur. SNMP version 3 mappe les commandes GET, SET et les traps sur 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 être composé de 32 caractères ASCII maximum.
- **Phrase secrète d'authentification :** phrase de 15 à 32 caractères ASCII qui vérifie que le NMS qui communique avec ce périphérique via SNMPv3 est bien celui qu'il prétend être.
  Elle vérifie aussi que le message n'a pas été modifié durant la transmission et qu'il a été communiqué en temps voulu. Cela indique qu'il n'a pas été retardé, copié et renvoyé ultérieurement à un moment inadapté.
- **Phrase secrète de confidentialité :** phrase de 15 à 32 caractères ASCII qui garantit la confidentialité des données envoyées par une station de gestion réseau (NMS) à ce périphérique ou reçues depuis ce périphérique par le protocole SNMPv3, au moyen d'un chiffrement
- **Protocole d'authentification :** l'implémentation du protocole SNMPv3 prend en charge les authentifications SHA et MD5. Il convient de sélectionner l'une d'entre elles.
- **Protocole de confidentialité :** l'implémentation du protocole SNMPv3 prend en charge les protocoles AES et DES comme protocoles de chiffrement et de déchiffrement des données. Vous devez utiliser un protocole et un mot de passe de confidentialité ; sinon, la requête SNMP n'est pas chiffrée.

  Vous ne pouvez pas sélectionner de protocole de confidentialité si aucun protocole d'authentification n'a été sélectionné.

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 la carte de gestion réseau. Pour apporter une modification, cliquez sur un nom d'utilisateur.

Par défaut, une entrée est affectée à chacun des quatre profils utilisateur. Vous pouvez modifier ces paramètres afin d'appliquer *plusieurs entrées à un profil utilisateur* pour accorder l'accès via plusieurs adresses IP, noms d'hôte ou masques d'adresse IP spécifiques.

- Par défaut, tous les systèmes de gestion réseau qui utilisent ce profil ont accès à ce périphérique.
- Si vous configurez plusieurs entrées de contrôle d'accès pour un profil utilisateur, cela implique qu'un ou plusieurs des autres profils utilisateur ne doivent pas avoir accès au périphérique.

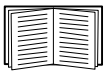
Nom d'utilisateur : sélectionnez dans la liste déroulante le profil utilisateur auquel ce contrôle d'accès va s'appliquer. Les choix disponibles sont les quatre noms d'utilisateur que vous configurez via l'option « Profils utilisateur ».

IP NMS/Nom d'hôte : adresse IP, masque de l'adresse IP ou nom d'hôte qui contrôle l'accès par les systèmes de gestion réseau. Un nom d'hôte ou une adresse IP spécifique (par exemple 149.225.12.1) permet uniquement l'accès du système de gestion réseau 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 également exprimer sous la forme 255.255.255.255 : accès par tous les NMS sur tous les segments.

Écrans Modbus

Utilisez les options Modbus pour configurer votre carte de gestion réseau de sorte qu'elle utilise le protocole Modbus, afin de se connecter au système de gestion de protocole (BMS, Building Management System).



Pour de plus amples informations sur l'implémentation de Modbus sur votre onduleur, consultez l'**Addenda à la documentation Modbus** ou le **Plan de registre Modbus pour AP9547**.



REMARQUE : La carte de gestion réseau prend en charge 5connexions TCP Modbus.

TCP Modbus.

Chemin d'accès : Configuration > Réseau > Modbus > TCP

1. Utilisez **Accès** pour activer ou le TCP Modbus comme méthode de communication avec la carte de gestion réseau.
2. Définissez le numéro de **Port** pour la connexion du TCP. Il peut être défini sur 502 (par défaut) ou sur une valeur comprise entre 5 000 et 32 768.
3. Cliquez sur Appliquer pour sauvegarder vos modifications.

Écran BACnet

BACnet n’est pas pris en charge sur la carte AP9544.

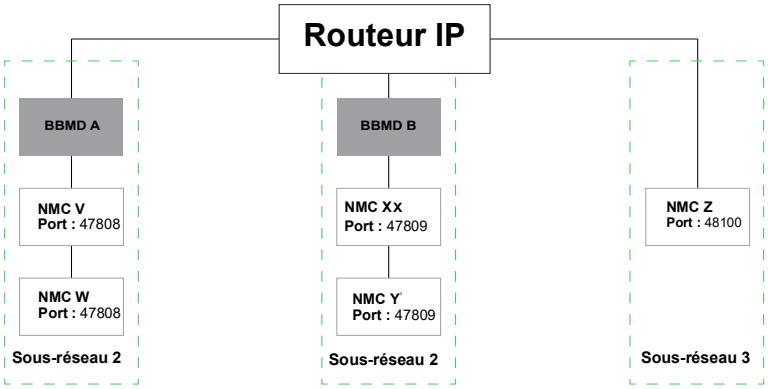
Utilisez les options BACnet pour configurer votre carte de gestion réseau de sorte qu’elle utilise le protocole BACnet et mettre les données de l’onduleur à la disposition aux réseaux d’automatisation et de contrôle des bâtiments.

Pour de plus amples informations sur les points de données de l’onduleur rendus disponibles via BACnet, consultez la **Carte d’application BACnet**.

Configuration BACnet

Option	Description
Accès	Cochez cette case pour activer ou désactiver BACnet Si cette case n’est pas cochée, il n’est pas possible d’accéder à la carte de gestion réseau via BACnet. BACnet est désactivé par défaut. **REMARQUE :** BACnet ne peut pas être activé jusqu’à ce que le **Mot de passe de contrôle de la communication du périphérique** soit défini.
Identifiant du périphérique	Un identifiant unique pour ce périphérique BACnet, utilisé pour son adressage. Plage acceptable : 0–4194303.
Nom du périphérique	Nom de ce périphérique BACnet, qui doit être unique sur le réseau BACnet. Le nom par défaut du périphérique est « BACn »+ les huit derniers chiffres de l’adresse MAC de la carte de gestion réseau. La longueur minimale est 1 caractère, la longueur maximale est 150 caractères et les caractères spéciaux sont autorisés.
Protocole réseau	Sélectionnez le protocole à utiliser : • BACnet/IP
Délai d’attente APDU	Le nombre de millisecondes pendant lequel la carte de gestion réseau attendra une réponse à une requête BACnet. Plage acceptable : 1 000-30 000. La valeur par défaut est 6 000.
Tentatives APDU	Le nombre de tentatives de requêtes BACnet que la carte de gestion réseau effectuera avant d’abandonner la requête. Plage acceptable : 1–10. La valeur par défaut est 3.
Mot de passe du contrôle de communication du périphérique	Le service Contrôle de communication du périphérique est utilisé par un client BACnet afin de demander à un périphérique distant (p. ex. Une carte de gestion réseau avec BACnet activé) d’arrêter de répondre à toutes les APDU (excepté le service Contrôle de communication du périphérique) pour une période définie. Ce service peut être utilisé à des fins de diagnostic. Indiquez le mot de passe de contrôle de communication du périphérique pour garantir qu’un client BACnet ne puisse pas contrôler la communication BACnet d’une carte de gestion réseau sans d’abord fournir le mot de passe défini ici. Le mot de passe doit comporter 8 à 20 caractères et doit contenir : • Un chiffre. • Une lettre majuscule. • Une lettre minuscule. • Un caractère spécial. Il est recommandé de mettre à jour le mot de passe lorsque vous activez BACnet pour la première fois. Vous n’avez pas à connaître le mot de passe actuel pour le mettre à jour.

BACnet/IP

Option	Description
Port local	Port UDP/IP utilisé par la carte de gestion réseau pour envoyer et recevoir des messages BACnet/IP. Plage acceptable : 5 000–65 535. Par défaut : 47 808. **REMARQUE :** L'adresse d'une carte de gestion réseau avec BACnet/IP activé est définie comme l'adresse IP de la carte de gestion réseau et du port local.
Activer l'enregistrement d'un périphérique étranger	Cochez la case pour enregistrer la carte de gestion réseau avec un périphérique de gestion de diffusion BACnet (BBMD). **REMARQUE :** Vous devez enregistrer votre carte de gestion réseau comme périphérique étranger avec un BBMD si aucun BBMD ne se trouve actuellement sur le sous-réseau de la carte de gestion réseau, ou si celle-ci utilise un autre port local sur le BBMD.  Dans l'exemple ci-dessus : • BBMD A gère les messages diffusés aux NMC V et W. • BBMD B gère les messages diffusés aux NMC X et Y. • Seule la NMC Z doit être enregistrée avec le BBMD A ou B comme périphérique étranger, car il n'y a aucun BBMD présent sur son sous-réseau. • Une fois enregistrée, la NMC Z peut recevoir les messages diffusés par le BBMD avec lequel elle est enregistrée et peut envoyer des messages à ce BBMD, qui les diffuse à son tour à tous les périphériques présents sur son sous-réseau, ainsi qu'aux autres BBDM présents sur le réseau via le routeur IP.

Option	Description
État	État d'enregistrement d'un périphérique étranger (FDR) : • **Enregistrement de périphérique étranger inactif** Le FDR sera inactif si : – le FDR est activé et BACnet est désactivé – le FDR est désactivé et BACnet est activé – le FDR est désactivé et BACnet est désactivé • **Enregistrement réussi** Le FDR a été effectué avec succès. • **Enregistrement rejeté** Le FDR a échoué. La carte de gestion réseau réessaiera l'enregistrement automatiquement, mais vous pouvez également cocher la case **Activer l'enregistrement de périphérique étranger** pour demander à la carte de gestion réseau de réessayer l'enregistrement. • **Enregistrement envoyé** La demande de FDR a été envoyée, mais n'a pas encore été finalisée.
Périphérique de gestion de diffusion BACnet/IP	L'adresse IP ou le nom de domaine complet (FQDN) du périphérique de gestion de diffusion BACnet avec lequel cette carte de gestion réseau sera enregistrée.
Port	Le port du BBMD avec lequel cette carte de gestion réseau sera enregistrée.
TTL (durée de vie)	Le nombre de secondes (Time To Live, durée de vie) pendant lequel le BBMD maintiendra la carte de gestion réseau comme périphérique enregistré. Si la carte de gestion réseau n'est pas réenregistrée avant l'expiration de ce délai, le BBMD la supprimera du tableau des périphériques étrangers et la elle ne sera plus disponible pour envoyer et recevoir des messages diffusés par le BBMD. Le TTL contrôle la fréquence à laquelle la carte de gestion réseau est enregistrée avec le BBMD, car la carte de gestion réseau tentera de se réenregistrer avant l'expiration de ce délai.

Écran Serveur FTP

Chemin d'accès : Configuration > Réseau > Serveur FTP

Utilisez cet écran pour accéder à un serveur FTP et pour définir un port.

Option	Description
Accès	Le serveur FTP transmet les fichiers sans les chiffrer. Le serveur FTP est désactivé par défaut. Pour chiffrer les fichiers avant de les transférer, utilisez le protocole Secure CoPy (SCP). SCP (via SSH) est activé par défaut. Cependant, il n'autorisera le transfert de fichiers avant que le mot de passe par défaut du super-utilisateur (`apc`) soit modifié. **REMARQUE** : Chaque fois que vous voulez qu'un périphérique soit accessible pour la gestion par l'option Data Center Expert ou Fonctionnement, le serveur FTP doit être activé dans l'interface de la carte de gestion réseau de l'onduleur concerné. Pour plus d'informations sur l'amélioration et la gestion de la sécurité de votre système, reportez-vous au **Manuel de sécurité**.

Option	Description
Port	Le port TCP/IP du serveur FTP (par défaut, 21). Le serveur FTP utilise à la fois le port spécifié et celui dont le numéro est immédiatement inférieur. Les numéros de port par défaut autorisés sont indiqués à l'écran : 21 et 5001-32768 **REMARQUE** : La configuration du serveur pour utiliser un port non défini par défaut améliore la sécurité en demandant aux utilisateurs d'ajouter le nom du port à l'adresse IP dans une ligne de commande FTP. Le nom du port ajouté doit être précédé par une espace ou par deux points, selon le client FTP utilisé.

Écran Wi-Fi

Chemin d'accès : Configuration > Réseau > Wi-Fi

REMARQUE : Cet écran est pertinent lorsque le périphérique APC USB Wi-Fi (AP9834) en option est inséré dans un port USB d'une carte AP9544/AP9547.

IMPORTANT : Il est recommandé de ne pas télécharger un fichier de configuration.ini à partir d'un appareil câblé et de télécharger l'intégralité du fichier sur un appareil Wi-Fi. Il n'est pas non plus recommandé de télécharger un fichier config.ini à partir d'un appareil Wi-Fi et de pousser l'intégralité du fichier vers un appareil câblé, sauf si toute la section `[NetworkWiFi]` est supprimée ou apparaît sous forme de commentaire en utilisant un point-virgule (par exemple `; WiFi=activé`).
La section `[NetworkWiFi]` contient les paramètres du périphérique spécifiques à l'utilisation du Wi-Fi. Ces paramètres ne doivent pas être téléchargés sur un périphérique câblé.

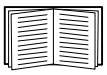
Utilisez cet écran pour consulter l'état actuel du réseau Wi-Fi, activer/désactiver le Wi-Fi et configurer les paramètres du réseau Wi-Fi.

REMARQUE : L'activation/désactivation du Wi-Fi permet de désactiver/activer la connexion filaire du réseau local. La carte de gestion réseau redémarre lorsque les paramètres Wi-Fi sont configurés. Après le redémarrage, le réseau câblé sera désactivé et la carte de gestion réseau tentera de se connecter au **nom de réseau (SSID)** indiqué.

Nom de réseau (SSID) : indiquez le nom de réseau (SSID) du réseau Wi-Fi. La longueur maximale est de 32 caractères.

Type de sécurité : indiquez le type de sécurité du réseau Wi-Fi et fournissez les détails d'authentification :

Option	Description
WPA	**Mot de passe Wi-Fi :** indiquez le mot de passe du réseau Wi-Fi. La longueur maximale est de 64 caractères.
WPA2-AES	
WPA2-Mixed	
WPA2-TKIP	
WPA2-Enterprise	• **Nom d'utilisateur :** nom d'utilisateur pour l'authentification WPA2-Enterprise. La longueur maximale est de 32 caractères. • **Mots de passe :** mot de passe pour l'authentification WPA2-Enterprise. La longueur maximale est de 32 caractères. • **Identité externe :** indiquez l'identité externe WPA-2-Enterprise. il s'agit d'une méthode d'identification chiffrée en option, utilisée par le serveur WPA-2-Enterprise. Par exemple : user@example.com ou anonyme. La longueur maximale est de 32 caractères.



Pour en savoir plus sur la mise à niveau du firmware du périphérique APC USB Wi-Fi (AP9834), consultez la commande `wifi` dans le **Guide de la carte de gestion réseau pour Easy UPS CLI**.

Pour dépanner la connexion au périphérique APC USB Wi-Fi (AP9834), ainsi que pour des descriptions des voyants LED du périphérique, voir « Problèmes liés au périphérique Wi-Fi USB APC (AP9834) ».

Menu Notification

Reportez-vous aux sections suivantes :

- « Types de notification »
- « Configuration des actions sur les événements »
- « Écrans de notification par e-mail »
- « Écran de test des traps SNMP »
- « Écran des récepteurs de traps SNMP »

Types de notification

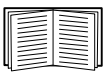
Vous pouvez configurer des actions de notification survenant en réponse à un événement. Vous pouvez notifier les utilisateurs d'un événement de différentes manières :

- notification active et automatique. Les utilisateurs ou les services de surveillance spécifiés sont contactés directement.
  - Notification par e-mail
  - Traps SNMP
  - Notification Syslog
- Notification indirecte
  - Journal 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 également consigner les données de performances du système à utiliser pour la surveillance de l'équipement. Reportez-vous à la section « Journal de consignation des données » pour obtenir des informations sur la configuration et l'utilisation de l'option de consignation des données.

  - Requêtes (commandes SNMP GET)

    Pour de plus amples informations, reportez-vous à la section « Écran des récepteurs de traps SNMP ».« Écran de test des traps SNMP » Le protocole SNMP permet à un NMS d'exécuter des requêtes d'information. Avec SNMPv1, qui ne chiffre pas les données avant la transmission, la configuration du type d'accès SNMP le plus restreint (en lecture) permet d'utiliser les 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 « Écran des récepteurs de traps SNMP » pour des informations sur la configuration d'un récepteur de traps. Le groupe de trois événements **MIB 1628** 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

Configuration par événement.

Chemin d'accès : Configuration > Notification > Actions sur les événements > Par événement

Par défaut, la consignation d'un événement est sélectionnée pour tous les événements. Pour définir les actions sur les événements pour un événement individuel :

1. Sélectionnez le menu **Configuration**, puis **Notification**, **Actions sur les événements** et **Par événement**.
2. Pour rechercher un événement, cliquez sur un en-tête de colonne pour voir les listes sous les catégories **Événements d'alimentation**, **Événements environnementaux** ou **Événements système**.

   Vous pouvez aussi cliquer sur une sous-catégorie sous les en-têtes, par exemple **État de la ligne d'entrée** ou **Température**.
3. Cliquez sur le nom de l'événement pour afficher ou modifier la configuration actuelle, par exemple les destinataires à notifier par e-mail ou les systèmes de gestion réseau (NMS) à notifier par traps SNMP. Reportez-vous à la section « Paramètres de notification ». Cochez la case **Journal des événements** pour activer ou désactiver une entrée du journal des événements pour cet événement.



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 activer ou désactiver la consignation des événements ou Syslog, ou encore désactiver la notification pour des destinataires par email ou des récepteurs de traps spécifiques, mais vous ne pouvez ni ajouter ni supprimer des destinataires ou des récepteurs. Pour ajouter ou supprimer des destinataires ou des récepteurs, reportez-vous aux sections suivantes :

- « Identification des serveurs Syslog »
- « Destinataires de l'e-mail »
- « Récepteurs de traps »

Configuration par groupes d'événements.

Chemin d'accès : Configuration > Notification > Actions sur les événements > Par groupe

Pour configurer simultanément un groupe d'événements :

1. Sélectionnez le menu **Configuration**, puis **Notification**, **Actions sur les événements** et **Par groupe**.
2. Choisissez comment grouper les événements à configurer :
   - Sélectionnez **Événements par gravité**, puis sélectionnez 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 prédéfinies.
3. Cliquez sur Suivant pour changer d'écran 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** (par défaut), vous devez d'abord configurer au moins un destinataire ou un récepteur concerné.
      - Si vous sélectionnez **Journalisation** en ayant configuré un serveur Syslog, sélectionnez **Journal des événements** ou `Syslog` (ou les deux) sur l'écran suivant. (Reportez-vous à la section « Journaux dans le menu Configuration »).

b. Choisissez d'activer ou de désactiver la nouvelle action sur les événements configurée pour ce groupe d'événements.

Reportez-vous directement à la section « Paramètres de notification » ci-dessous.

Paramètres de notification. Ces champs de configuration définissent les paramètres pour envoyer les notifications des événements. Reportez-vous aux sections « Configuration par événement » et « Configuration par groupes d'événements ».

Pour accéder à ces paramètres, cliquez sur le nom du récepteur ou du destinataire.

Champ	Description
Délai de notification	Si l'événement persiste pendant la durée spécifiée, une notification est envoyée. Si la condition disparaît avant l'expiration du délai, aucune notification n'est envoyée.
Intervalle de répétition	La notification est envoyée de manière répétée selon l'intervalle spécifié (la valeur par défaut est 2 minutes jusqu'à ce que la condition disparaisse).
Nombre de notifications après la notification initiale	Tant que l'événement est actif, la notification est répétée le nombre de fois indiqué.
ou	
Notifier jusqu'à ce que la condition disparaisse	La notification est envoyée de manière répétée jusqu'à ce que la condition disparaisse ou soit corrigée.

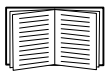
Pour les événements auxquels est associé un événement d'arrêt, vous pouvez également définir ces paramètres. (Comme exemple d'événement auquel est associé un événement d'arrêt, citons `Onduleur : Perte de communication avec les blocs-batteries` et `l'onduleur : Communication rétablie avec les blocs-batteries`).

Écrans de notification par e-mail

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

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

- Les adresses IP du serveur de noms de domaine (DNS) primaire et, le cas échéant, du serveur secondaire. (Reportez-vous à la section « Écran DNS »).
- L'adresse IP ou le nom DNS du **serveur SMTP** et l'**adresse de l'expéditeur**. (Reportez-vous à la section « Serveur SMTP » ci-dessous).
- L'adresse e-mail de quatre destinataires maximum. (Reportez-vous à la section « Destinataires de l'e-mail »).



Vous pouvez utiliser le paramètre **Adresse du destinataire** de l'option **destinataires** pour envoyer l'email à un écran en mode texte.

Serveur SMTP.

Chemin d'accès : Configuration > Notification > E-mail > Serveur

Cet écran répertorie vos serveurs DNS primaire et secondaire (voir « Écran DNS ») ainsi que les champs suivants :

Champ	Description
Configuration des e-mails sortants	
Adresse de l'expéditeur	Contenu du champ **Expéditeur** des e-mails envoyés par la carte de gestion réseau : • au format *utilisateur*@ [*adresse_IP*] (si une adresse IP est spécifiée comme **serveur SMTP local**). • au format *utilisateur@domaine* (si un DNS est configuré et que son nom DNS est spécifié comme **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. Reportez-vous à la documentation fournie avec le serveur.
Serveur SMTP	Adresse IPv4/IPv6 ou nom DNS du serveur SMTP local. **REMARQUE :** cette définition est uniquement requise lorsqu'un **serveur SMTP** est défini comme **Local**. Reportez-vous à la section « Destinataires de l'e-mail »
Authentification	Activez ce paramètre si le serveur SMTP requiert une authentification.
Port	Le serveur SMPT par défaut est 25. Autres ports : 465, 587, 2 525, 5 000 à 32 768.
Nom d'utilisateur/ Mot de passe/ Confirmation du mot de passe	Si votre serveur de messagerie requiert une authentification, saisissez ici le nom d'utilisateur et le mot de passe. Il s'agit d'une authentification simple et non pas SSI.
Avancé	
Utiliser SSL/TLS	• **Jamais** : le serveur SMTP ne requiert pas de chiffrement ni n'en prend en charge. • **Si pris en charge** : le serveur SMTP annonce la prise en charge de STARTTLS mais *ne requiert pas* le chiffrement de la connexion. La commande STARTTLS est envoyée une fois l'annonce effectuée. • **Toujours** : lorsqu'une connexion au serveur SMTP survient, celui-ci requiert l'envoi de la commande STARTTLS. • **Implicitement** : le serveur SMTP accepte uniquement les connexions chiffrées dès le début. Aucun message STARTTLS n'est envoyé au serveur.
Certificat racine CA nécessaire	N'activez ce paramètre que si la politique de sécurité de votre entreprise ne prévoit pas l'approbation implicite des connexions SSL. Si ce paramètre est activé, il convient de charger un certificat racine CA sur la carte de gestion réseau pour permettre l'envoi des e-mails chiffrés.
Nom de fichier	Ce champ est tributaire des certificats racine CA installés sur la carte de gestion réseau et de la nécessité ou non d'un tel certificat.

Destinataires de l'e-mail.

Chemin d'accès : Configuration > Notification > E-mail > Destinataires

Spécifiez un maximum de quatre destinataires des e-mails. Cliquez sur un nom pour configurer les paramètres. Reportez-vous également à la section « Serveur SMTP » ci-dessus.

Champ	Description
Génération d'e-mails	Active (par défaut) ou désactive l'envoi des e-mails au destinataire.
Adresse du destinataire	Noms d'utilisateur et de domaine du destinataire Pour utiliser l'e-mail comme service de radiomessagerie, utilisez l'adresse email du compte de passerelle de radiomessagerie du destinataire concerné (par exemple: `myacct100@skytel.com`). La passerelle de radiomessagerie générera l'alerte. 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. Par exemple, utilisez jsmith@[xxx.xxx.x.xxx] au lieu de jsmith@company.com. Ceci est utile lorsque la recherche de serveur DNS ne fonctionne pas correctement. **REMARQUE :** le pager du destinataire doit être compatible avec la messagerie texte.
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	Choisissez dans la liste déroulante la langue dans laquelle tous les e-mails doivent être envoyés. Il est possible d'utiliser différentes langues selon les utilisateurs. Reportez-vous à la section « Changement de la langue de l'interface utilisateur ».
Serveur	Sélectionnez l'une des options suivantes pour le routage des e-mails : • **Local** : via le serveur SMTP local du site. Ce paramètre recommandé garantit que l'e-mail est envoyé au moyen du serveur SMTP local du site. Si vous choisissez ce paramètre, vous limitez les retards, les pannes réseau et les nouvelles tentatives d'envoi d'e-mails pendant de nombreuses heures. Si vous choisissez le paramètre Local, vous devez également activer la transmission au serveur SMTP de votre périphérique et configurer un compte e-mail externe spécial pour recevoir l'e-mail transmis. Consultez l'administrateur de votre serveur SMTP avant de procéder à ces modifications. • **Destinataire** : via le serveur SMTP du destinataire. La carte de gestion réseau effectue une recherche d'enregistrement MX dans l'adresse e-mail des destinataires et l'utilise comme serveur SMTP. L'e-mail n'est envoyé qu'une fois, si bien qu'il peut être facilement perdu. • **Client** : ce paramètre permet à chaque destinataire de l'e-mail d'avoir ses propres paramètres de serveur. Ces paramètres sont indépendants de ceux indiqués sous « Serveur SMTP » ci-dessus.

Certificats SSL d'e-mails.

Chemin d'accès : Configuration > Notification > E-mail > Certificats SSL

Chargez un certificat SSL d'e-mail sur la carte de gestion réseau pour plus de sécurité. Le fichier doit avoir l'extension `.crt` ou `.cer`. Il est possible de charger jusqu'à cinq fichiers à tout moment.

Une fois le certificat installé, ses détails sont également affichés ici. En cas de certificat incorrect, « n/a » est affiché pour tous les champs, à l'exception de Nom de fichier.

Il est possible de supprimer des certificats dans cet écran. Vous devez modifier manuellement tous les destinataires d'e-mails qui utilisent le certificat afin de supprimer toute référence à celui-ci.

Test d'e-mail.

Chemin d'accès : Configuration > Notification > E-mail > Test

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

Écran des récepteurs de traps SNMP

Récepteurs de traps.

Chemin d'accès : Configuration > Notification > Traps SNMP > Récepteurs de traps

Avec les traps SNMP (Simple Network Management Protocol), vous pouvez être notifié automatiquement des événements importants liés à l'onduleur. Ils constituent un outil utile pour surveiller les périphériques de votre réseau.

Les récepteurs de traps sont affichés par **IP NMS/nom d'hôte**, NMS signifiant système de gestion réseau. Vous pouvez configurer jusqu'à six récepteurs de traps.

Pour configurer un nouveau récepteur de traps, cliquez sur **Ajouter récepteur de trap**. Pour en modifier (ou en supprimer) un, cliquez sur son adresse IP/nom d'hôte.

Si vous supprimez un récepteur de traps, tous les paramètres de notification configurés sous « Configuration des actions sur les événements » pour ce récepteur de traps prennent leur valeur par défaut.

Sélectionnez la case d'option **SNMPv1** ou **SNMPv3** pour spécifier le type de trap. Pour qu'un NMS reçoive les *deux* types de traps, vous devez configurer séparément deux récepteurs de traps (un pour chaque type).

Champ	Description
Génération de traps	Active (par défaut) ou désactive la génération de traps pour ce récepteur de traps.
MIB Powernet - Génération de traps/RFC1628	Sélectionnez l'un de ces deux types de génération de traps MIB pour chaque trap créé. L'option Powernet, personnalisée pour Schneider Electric, comporte de nombreuses variables supplémentaires adaptées aux produits de cette entreprise. Le type RFC1628 correspond au MIB générique standard pour les onduleurs. Si vous utilisez le MIB RFC1628, vous pouvez aussi utiliser les trois notifications d'événements RFC1628 (voir « Configuration des actions sur les événements »). Elles permettent d'éviter de configurer les événements de notification hors de l'environnement de la carte de gestion réseau (voir **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 la langue dans la liste déroulante. Elle peut être différente de celle de l'interface utilisateur et de celle des autres récepteurs de traps.
SNMPv1	Nom de la communauté : nom utilisé comme identifiant lorsque des traps SNMPv1 sont envoyés à ce récepteur de trap. 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).
SNMPv3	Nom d'utilisateur : sélectionnez l'identifiant du profil utilisateur pour ce récepteur de traps. Reportez-vous à « Profils utilisateur » sous « Écrans SNMP ».

Écran de test des traps SNMP

Chemin d'accès : Configuration > Notification > Traps SNMP > Test

Résultat du dernier test : résultat du test de traps SNMP le plus récent. 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 traps sélectionné. Un test de trap est réussi si toutes les conditions suivantes sont remplies :

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

À : Sélectionnez l'adresse IP ou le nom d'hôte auquel un trap SNMP de test sera envoyé. Si aucun récepteur de traps n'est configuré, un lien vers l'écran de configuration du **récepteur de traps** s'affiche. Reportez-vous à la section « Écran des récepteurs de traps SNMP » ci-dessus.

Menu Généralités

Ce menu concerne différents éléments de configuration, notamment l'identification du périphérique, la date et l'heure, l'exportation et l'importation des options de configuration de carte de gestion réseau, les trois liens en bas à gauche de l'écran et la consolidation des données aux fins de dépannage.

Écran d'identification

Chemin d'accès : Configuration > Généralités > Identification

Permet de définir le **Nom** (nom du système de carte de gestion réseau, voir « Écran DNS »), l'**Emplacement** (emplacement physique) et le **Contact** (personne responsable du périphérique) utilisés par :

- l'agent SNMP de la carte de gestion réseau
- Data Center Expert



Le champ de nom est utilisé par les identifiants d'objets (OID) **sysName**, **sysContact** et **sysLocation** dans l'agent SNMP de la carte de gestion réseau. Pour de plus amples informations sur les OID MIB-II, consultez le *Guide de référence de la base d'informations sur la gestion (MIB)* du SNMP *PowerNet*® disponible sur le site Web de Schneider Electric.

Écran Date/heure

Mode.

Chemin d'accès : Configuration > 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) :

Avec les deux, vous sélectionnez le **fuseau horaire**. Il s'agit de la différence d'heure locale avec le temps universel coordonné (TUC), également appelé temps universel (GMT).

- **Mode manuel** : utilisez l'une des méthodes suivantes :
  - Saisissez la date et l'heure de la carte de gestion réseau.
  - Cochez la case **Appliquer l'heure système local** pour lire les paramètres de date et d'heure de l'ordinateur que vous utilisez et les appliquer ici.

- **Synchroniser avec le serveur NTP** : faites définir la date et l'heure de la carte de gestion réseau par un serveur NTP (Network Time Protocol).



Par défaut, toute carte de gestion réseau située sur le côté privé de Data Center Expert obtient ses paramètres d'heure en utilisant Data Center Expert comme serveur NTP.

Champ	Description
Effacer les paramètres NTP manuels	Si vous sélectionnez cette option, les données des autres sources (en général DHCP) sont prioritaires sur les configurations NTP que vous définissez ici.
Serveur NTP primaire	Saisissez l'adresse IP ou le nom de domaine du serveur NTP primaire.
Serveur NTP secondaire	Saisissez l'adresse IP ou le nom de domaine du serveur NTP secondaire, le cas échéant.
Fréquence de mise à jour	Définit à quelle fréquence (en heures) la carte de gestion réseau accède au serveur NTP pour procéder aux mises à jour. *Minimum* : 1 ; *Maximum* : 8760 (1 an).
Mettre à jour avec NTP maintenant	Permet de lancer une mise à jour immédiate de la date et de l'heure par le serveur NTP.

Heure d'été.

Chemin d'accès : Configuration > Généralités > Date/heure > Heure d'été

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

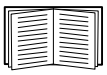
Lorsque vous personnalisez l'heure d'été, le système fait avancer l'horloge d'une heure lorsque l'heure et la date que vous spécifiez sous **Début** sont atteintes, et la fait retarder d'une heure lorsque l'heure et la date que vous spécifiez sous **Fin** sont atteintes.

- Si l'heure d'été locale débute ou finit toujours à la *quatrième* occurrence d'un jour de semaine spécifique d'un mois donné (par exemple le quatrième dimanche), sélectionnez **Quatrième/Dernier**. Si le mois comporte un cinquième dimanche, sélectionnez toujours **Quatrième/Dernier**.
- Si l'heure d'été locale débute ou finit toujours à la *dernière* occurrence d'un jour de semaine spécifique d'un mois, que cette occurrence soit la quatrième ou la cinquième, sélectionnez **Cinquième/Dernier**.

Création et importation de paramètres avec le fichier de configuration

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

Vous pouvez accélérer et simplifier la configuration des nouveaux périphériques en réutilisant les paramètres de configuration existants avec cette option. Sélectionnez **Téléverser** pour transférer les données de configuration vers cette interface et **Téléchargement** pour les transférer à partir de l'interface (utilisez ensuite le fichier pour configurer une autre interface). Le nom par défaut du fichier est **config.ini**.



Pour récupérer le fichier d'une carte de gestion réseau configurée et le personnaliser, reportez-vous à la section « Exportation des paramètres de configuration ».

Écran de configuration des liens

Chemin d'accès : Configuration > Généralités > Liens rapides

Utilisez cette option pour visualiser et modifier les liens d'URL affichés en bas à gauche de chaque écran de l'interface.

Pour reconfigurer un lien, cliquez sur son nom dans la colonne **Nom**. Vous pouvez rétablir la valeur par défaut des liens à tout moment en cliquant sur **Rétablir les valeurs par défaut**.

Journaux dans le menu Configuration

Chemin d'accès : Configuration > Journaux > 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 de manière centralisée dans un journal les événements qui se produisent sur les équipements du réseau.



Le présent Guide de l'utilisateur ne décrit pas Syslog ni les valeurs de configuration de Syslog en détail. Pour de plus amples informations concernant Syslog, consultez **RFC3164**.

Identification des serveurs Syslog

Chemin d'accès : Configuration > Journaux > Syslog > Serveurs

Champ	Description
Serveur Syslog	Utilise des adresses IPv4/IPv6 ou des noms d'hôte pour identifier jusqu'à quatre serveurs devant recevoir les messages Syslog envoyés par la carte de gestion réseau.
Port	Le port UDP (User Datagram Protocol) que la carte de gestion réseau utilise pour envoyer les messages Syslog. La valeur par défaut est `514`.
Langue	Choisissez la langue des messages Syslog.
Protocole	Choisissez le protocole UDP ou TCP.

Paramètres Syslog

Chemin d'accès : Configuration > Journaux > Syslog > Paramètres

Champ	Description
Génération de messages	Activez la génération et la consignation des messages Syslog pour les événements pour lesquels Syslog est défini comme méthode de notification Reportez-vous à la section « Configuration des actions sur les événements ».
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 si l'administrateur du système ou du réseau Syslog vous le demande.

Champ	Description
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. Les options locales sont Critique, Avertissement et Informatif. Vous n'avez a priori pas besoin 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. • **Attention** : conditions normales mais à surveiller • **Informatif** : messages d'information • **Débogage** : messages de débogage Voici les paramètres par défaut correspondant aux paramètres **Priorité locale** : • **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 ».

Test Syslog et exemple de format

Chemin d'accès : Journaux > Syslog > Test

Envoyez un message de test aux serveurs Syslog (configurés sous l'option « Identification des serveurs Syslog » ci-dessus). Le résultat sera envoyé à tous les serveurs Syslog configurés.

Sélectionnez la gravité à attribuer au message de test, puis définissez ce dernier. Le format du message doit inclure le type d'événement (APC, système ou périphérique, par exemple), suivi de deux points, d'un espace et du texte de l'événement. Le message doit être composé de 50 caractères au maximum.

- Priorité Syslog attribuée à l'événement objet du message, et code site des messages envoyés par la carte de gestion réseau.
- L'en-tête : un horodatage et l'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 comporte le texte de l'événement, suivi (le cas échéant) d'une espace et du code de l'événement.

  Exemple : `APC : Le test Syslog est valide.`

Menu Tests

Test et calibrage

Chemin d'accès : Tests > Onduleurs

Les options ci-dessous ne concernent que les appareils monophasés Easy UPS On-Line dotés d'une carte AP9544.

Avec certains onduleurs, vous pouvez exécuter un auto-test, un test d'alarme ou un calibrage d'autonomie de votre onduleur. Les champs **Self-Test (Test automatique)** et **Calibration (Calibrage)** affichent les résultats des tests et des calibrages les plus récents.

Un calibrage en temps réel permet à l'onduleur de recalculer sa capacité de fonctionnement disponible en fonction de sa charge actuelle. Cela permet d'améliorer la précision de l'autonomie indiquée. Comme le calibrage épuise temporairement les batteries de l'onduleur, vous ne pouvez l'effectuer que si leur capacité est à 100 %. La charge de votre onduleur doit être d'au moins 15 % sans fluctuation pour garantir qu'un calibrage soit accepté.

Attention - Les calibrages lors de l'exécution déchargent fortement les batteries de l'onduleur, ce qui peut empêcher temporairement celui-ci de prendre en charge la charge en cas de panne de courant.

Les calibrages fréquents réduisent la durée de vie des batteries.

Effectuez un calibrage chaque fois que vous augmentez de manière significative la charge que l'onduleur supporte.

Le test d'alarme d'un onduleur est propre à un périphérique et peut ne pas être disponible sur votre modèle. Pour activer l'alarme, reportez-vous à « Écrans Onduleur - Généralités ».

- Lorsque vous sélectionnez **UPS Alarm Test (Test de l'alarme de l'onduleur)**, l'onduleur émet un signal sonore pendant quatre secondes et les voyants s'allument.
- Lorsque vous sélectionnez **UPS Alarm Test - Continuous (Test de l'alarme de l'onduleur - Continu)**, l'onduleur émet des signaux sonores et allume ses voyants jusqu'à ce que vous annuliez le test. Une puce séparée s'affiche sur cet écran, **Cancel Continuous Alarm Test (Annuler le test de l'alarme continu)**. Pour annuler le test, sélectionnez-la et cliquez sur Apply (Appliquer). Vous pouvez également appuyer sur une touche quelconque sur l'interface d'affichage LED de l'onduleur. Ce test est utile pour localiser un onduleur.

Configuration du clignotement des voyants LED de la carte de gestion réseau

Chemin d'accès : Tests (Tests) > Network (Réseau) > LED Blink (Voyant clignotant)

Si vous ne parvenez pas à trouver votre onduleur, saisissez un nombre de minutes dans le champ **LED Blink Duration (Durée de clignotement du voyant)**, puis cliquez sur Apply (Appliquer). Les voyants LED de votre carte de gestion réseau commenceront à clignoter. Ceci peut vous aider à localiser le périphérique physique.

Menus des journaux

Utilisation des journaux de consignation des événements et des données

Le journal de consignation des événements enregistre les occurrences d'événements individuelles. Le journal de consignation des données, en revanche, vous fournit un instantané de votre système en enregistrant des valeurs à intervalles réguliers.

Journal de consignation des événements

Chemin d'accès : Journaux > Événements > *Options disponibles*

Avec la fonctionnalité de base, seuls les 25 derniers événements sont enregistrés dans le journal de consignation des événements.

Par défaut, le journal affiche tous les événements enregistrés pendant les deux derniers jours, dans l'ordre chronologique inverse. Reportez-vous à la section « Configuration par événement ».

De plus, le journal enregistre : i) tout événement qui envoie un trap SNMP, à l'exception des tentatives d'authentification infructueuses au serveur SNMP, ii) les événements système internes anormaux.

Vous pouvez activer le codage couleur des événements via « Utilisateurs locaux » dans le menu Configuration.

Pour afficher le journal de consignation des événements.

Chemin d'accès : Journal > Événements > Journal

Par défaut, le journal de consignation des événements affiche d'abord les événements les plus récents. Pour afficher les événements répertoriés ensemble sur une page Web, cliquez sur le bouton **Ouvrir le journal dans une nouvelle fenêtre**. Pour ce faire, JavaScript doit être activé dans votre navigateur.

Pour ouvrir le journal dans un fichier texte ou l'enregistrer sur disque, cliquez sur l'icône de disquette , sur la même ligne que l'en-tête **Journal de consignation des événements**.

Vous pouvez également utiliser les protocoles FTP ou Secure CoPy (SCP) pour consulter le journal de consignation des événements. Reportez-vous à la section « Utilisation du protocole SCP ou FTP pour récupérer les fichiers de journaux de consignation ».

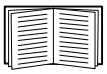
Pour filtrer le journal de consignation des événements. Utilisez le filtrage pour masquer des informations que vous ne souhaitez pas afficher.

Filtrage du journal par date ou heure	Utilisez les cases d'option **Dernier** ou **Depuis**. (La configuration du filtre est sauvegardée jusqu'à ce que la carte de gestion réseau redémarre).
Filtrage du journal par gravité ou catégorie d'événement	Cliquez sur **Filtrer le journal de consignation**. Désactivez une case à cocher pour la retirer de la vue. Une fois que vous avez cliqué sur **Appliquer**, un texte dans l'angle supérieur droit de la page Journal de consignation des événements indique qu'un filtre est actif. Le filtre est actif jusqu'à ce que vous l'effaciez ou 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)**. Si vous êtes connecté en tant qu'administrateur, cliquez sur **Enregistrer en tant que valeur par défaut** pour enregistrer ce filtre comme nouvel affichage du journal par défaut pour tous les utilisateurs.

Points importants concernant le filtrage :

- Les événements sont traités par le filtre selon la logique OU. Si vous appliquez un filtre, il fonctionne indépendamment des autres filtres.
- Les événements que vous avez désactivés dans la liste **Filtrer par gravité ne** ne s'affichent jamais dans le journal de consignation des événements filtré, même s'ils sont sélectionnés dans la liste **Filtrer par catégorie**.
- De même, les événements que vous désactivez dans la liste **Filtrer par catégorie** ne ne s'affichent jamais dans le journal de consignation des événements filtré.

Pour supprimer le journal de consignation des événements. Pour supprimer tous les événements, cliquez sur **Nettoyer le journal**. La suppression des événements est définitive.



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

Pour configurer la recherche inversée :

Chemin d'accès : Journaux de consignation > Événements > Recherche inversée

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.

La recherche inversée est désactivée par défaut. Vous ne devriez pas avoir besoin de l'activer si vous n'avez pas de serveur DNS configuré ou si vos performances réseau sont médiocres car elle génère un fort trafic réseau.

Pour redimensionner le journal de consignation des événements.

Chemin d'accès : Journaux > Événements > Taille

Utilisez la taille du journal de consignation des événements pour spécifier le nombre maximal d'entrées de journal.



Attention : lorsque vous redimensionnez le journal de consignation des événements pour spécifier une taille maximale, *toutes les entrées de journal existantes sont supprimées*. Pour éviter de perdre des données de consignation, utilisez FTP ou SCP pour récupérer d'abord le journal ; voir « Utilisation du protocole SCP ou FTP pour récupérer les fichiers de journaux de consignation ».
Lorsque le journal atteint par la suite la taille maximale, les entrées les plus anciennes sont supprimées.

Journal de consignation des données

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

Utilisez le journal de consignation des données pour afficher des mesures concernant l'onduleur, son alimentation d'entrée ainsi que la température ambiante au niveau de l'onduleur et des batteries.

Les étapes permettant d'afficher et de redimensionner le journal de consignation des données sont les mêmes que celles du journal de consignation des événements, à cette différence près que vous utilisez les options de menu sous **Données** au lieu de **Événements**. Reportez-vous aux sections « Pour afficher le journal de consignation des événements » et « Pour redimensionner le journal de consignation des événements ».

Pour filtrer le journal de consignation des données par date ou heure, utilisez les cases d'option **Dernier** ou **Depuis**. (La configuration du filtre est sauvegardée jusqu'à ce que la carte de gestion réseau redémarre). Pour supprimer toutes les données enregistrées dans le journal de consignation des données, cliquez sur **Effacer le journal de consignation des données**. La suppression est définitive.

Pour définir l'intervalle de collecte des données (Journaux de consignation > Données > Intervalle) : définissez, dans le paramètre **Fréquence de consignation**, la fréquence à laquelle les données sont recherchées et stockées dans le journal de consignation des données. Lorsque vous cliquez sur Appliquer, le nombre de jours de stockage possibles est recalculé et s'affiche en haut de l'écran.

Lorsque le journal de consignation est plein, les entrées les plus anciennes sont supprimées. Pour éviter la suppression automatique des données plus anciennes, voir « Pour configurer la rotation du journal de consignation des données (Journaux de consignation > Données > Rotation) : » ci-dessous.

REMARQUE : comme l'intervalle spécifie à quelle fréquence les données sont enregistrées, *plus il est petit*, plus les données sont souvent enregistrées et plus le fichier de consignation est volumineux.

Pour configurer la rotation du journal de consignation des données (Journaux de consignation > Données > Rotation) : lorsque la rotation est activée, le contenu du journal de consignation des données est ajouté au fichier spécifié par son nom et son emplacement. Cela signifie que vous pouvez stocker les données avant qu'elles ne soient supprimées ; voir « Pour définir l'intervalle de collecte des données (Journaux de consignation > Données > Intervalle) : » ci-dessus.

Utilisez cette option pour configurer la protection par mot de passe et d'autres paramètres.

Champ	Description
Serveur FTP	Adresse IP ou nom d'hôte du serveur où le fichier résidera.
Nom d'utilisateur et mot de passe	Nom d'utilisateur et mot de passe requis pour envoyer les données au référentiel. Cet utilisateur doit également être configuré avec autorisation d'accès en lecture et en écriture au référentiel des données et au répertoire (dossier) dans lequel il est enregistré.
Chemin du fichier	Chemin d'accès au référentiel.
Nom de fichier	Nom du référentiel (fichier texte ASCII), par exemple `datalog.txt`. Toutes les nouvelles données sont ajoutées à ce fichier et ne le remplacent pas.
Nom de fichier unique	Cochez cette case pour enregistrer le journal au format `mmjjaaaa_<filename>.txt`, où le nom de fichier correspond à celui que vous avez spécifié dans le champ **Nom de fichier** ci-dessus. Toute nouvelle donnée est ajoutée au fichier, mais chaque jour possède son propre fichier.

Champ	Description
Délai *n* heures entre les téléchargements.	Nombre d'heures entre les téléchargements des données dans le fichier (maximum 24 heures).
En cas d'échec, retentez le téléchargement toutes les *n* minutes	Nombre de minutes entre chaque tentative de téléchargement des données dans le fichier après un échec du téléchargement.
jusqu'à *n* fois	Nombre maximal de tentatives de téléchargement après un échec initial.
Jusqu'au succès du téléchargement	Tentative de téléchargement du fichier jusqu'à ce que le transfert soit terminé.

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

Le niveau Administrateur ou Utilisateur de périphérique permet d'utiliser SCP OU ftp 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. Tous deux résident sur la carte de gestion réseau.

- Le fichier contient tous les événements ou toutes les données enregistrés depuis la dernière suppression du contenu du journal ou, dans le cas du journal des données, depuis qu'il a été tronqué parce que sa taille maximale a été atteinte.
- Le fichier contient des informations que le journal de consignation des événements ou des données n'affiche pas.
  - Version de l'application
  - Date et heure auxquelles le fichier a été récupéré
  - Valeurs **Nom**, **Contact**, Emplacement **et Adresse** IP de la carte de gestion réseau.
  - Nom du modèle d'onduleur (*fichier data.txt* uniquement)
  - **Code d'événement** propre à chaque événement consigné (*fichier event.txt* uniquement).
  - La carte de gestion réseau utilise une numérotation à quatre chiffres pour indiquer l'année des entrées du journal. Il se peut que vous deviez sélectionner un format de date à quatre chiffres dans la feuille de calcul pour un affichage complet.



Si vous utilisez les protocoles de sécurité basés sur le chiffrement, consultez la section « Utilisation du protocole SCP pour récupérer les fichiers ». Si vous utilisez des méthodes d'authentification non chiffrées pour la sécurité, consultez la section « Utilisation du protocole FTP pour récupérer les fichiers ».



Consultez le **Manuel de sécurité** afin d'en savoir plus sur les protocoles et méthodes disponibles pour configurer le type de sécurité dont vous avez besoin.

Utilisation du protocole SCP pour récupérer les fichiers. Activez SSH sur la carte de gestion réseau ; voir « Accès à la console ». **REMARQUE :** les commandes ci-dessous sont données uniquement à titre d'exemples.

Pour récupérer le fichier *event.txt*, utilisez la commande suivante :

```
scp <username@hostname> ou <ip_address>:event.txt ./event.txt
```

Pour récupérer le fichier *data.txt*, utilisez la commande suivante :

```
scp <username@hostname> ou <ip_address>:data.txt ./data.txt
```

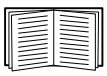
Utilisation du protocole FTP pour récupérer les fichiers. Pour utiliser FTP afin de récupérer le fichier *event.txt* ou *data.txt* :

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** pour l'option **Serveur FTP** (voir « Serveur FTP ») n'est plus configuré sur la valeur par défaut (`21`), vous devez utiliser la valeur différente de celle par défaut dans la commande FTP.

   Pour les clients FTP sous Windows, utilisez la commande suivante (espaces incluses) : (Avec certains clients FTP, insérez le signe deux-points (:) en remplacement d'une espace entre l'adresse IP et le numéro de port.)

   `ftp>open` *`adresse_ip numéro_port`*

   Pour définir une valeur de port autre que celle par défaut afin de renforcer la sécurité du serveur FTP, consultez la section « Serveur FTP ». 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 nom d'utilisateur par défaut est `apc`. Pour l'utilisateur de périphérique, le nom d'utilisateur par défaut est `device`.
3. Pour configurer le mode de transfert de fichiers en binaire, saisissez :

   ```
   ftp>bin
   ```

   Pour afficher une barre de progression pendant le transfert de fichiers, saisissez :

   ```
   ftp>hash
   ```

4. Utilisez la commande `get` pour transmettre la version texte du journal sur votre disque local.

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

   ou

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

5. 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
   ```

   Vous n'avez pas à confirmer la suppression.

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

6. Tapez `quit` à l'invite `ftp>` pour quitter FTP.

Journal de l’onduleur

Chemin d’accès : Journaux > Onduleur



Cette option de menu n’est pas disponible pour tous les onduleurs.

Ces informations sont dérivées de votre onduleur et sont distinctes des journaux de votre carte de gestion réseau. (Elles ne sont pas directement liées à la carte de gestion réseau « Journal de consignation des événements »ou à un sous-ensemble de celle-ci.)

Ces informations peuvent aider l’équipe d’assistance technique à résoudre les problèmes.

Journaux des événements de transfert de l’ondulateur : affiche un tableau des événements de transfert stockés par l’onduleur, y compris les transferts à la batterie et les transferts à la dérivation.

Journaux des défaillances de l’ondulateur : affiche un tableau des défaillances stockées de l’onduleur.

Journal de consignation du pare-feu

Chemin d’accès : Journal de consignation > Pare-feu

Si vous créez une stratégie de pare-feu, les événements du pare-feu seront consignés dans ce journal. Pour plus d’informations sur la mise en œuvre d’une stratégie, consultez la section « Écrans Pare-feu ».

Ces informations peuvent aider l’équipe d’assistance technique à résoudre les problèmes.

Les entrées du journal de consignation contiennent des informations sur le trafic et les actions liées aux règles (autorisé, supprimé). S’ils sont consignés ici, ces événements ne le sont pas dans le journal de consignation des événements principal. Reportez-vous à la section « Journal de consignation des événements ».

Le journal de consignation du pare-feu contient jusqu’à 50 des événements les plus récents. Le journal de consignation du pare-feu est effacé lorsque la carte de gestion réseau redémarre.

À propos du menu

À propos de la carte de gestion réseau

À propos de l'onduleur

Chemin d'accès : About (À propos de) > UPS (Onduleur)

Les informations affichées sous Onduleur varient en fonction du périphérique utilisé.

Champ	Description
Nom du produit	Le nom de la gamme d'onduleurs.
Modèle	Ce champ identifie votre onduleur.
Date de fabrication	Date à laquelle votre onduleur a été fabriqué.
Numéro de série	Le numéro d'identification unique de l'onduleur. Le numéro de série figure également à l'extérieur de l'onduleur.
Date de fabrication	Date à laquelle votre onduleur a été fabriqué.
Version du micrologiciel	Les numéros de version des modules de micrologiciels actuellement installés sur l'onduleur.
Nom du fabriquant	Le fabricant de l'onduleur.
Classé VA	La puissance apparente nominale de l'onduleur en VA.
Tension d'entrée nominale	La tension d'entrée nominale de l'onduleur en Vca.
Tension nominale de sortie	La tension de sortie nominale de l'onduleur en Vca.
Fréquence de sortie nominale	La fréquence nominalede la tension de sortie de l'onduleur en Hz.
Courant de sortie nominal	Le courant de sortie nominal de l'onduleur en A.
Tension nominale de la batterie	La tension nominale de l'onduleur en Vcc.
Phases d'entrée	Le nombre de phases d'entrée de l'onduleur.
Phase de sortie	Le nombre de phases de sortie de l'onduleur.

Le tableau **À propos des blocs-batteries de l'onduleur** affiche la version du micrologiciel, le modèle, le numéro de série et la date de fabrication des blocs-batteries de l'onduleur.

À propos de la carte de gestion réseau et des modules de micrologiciel

Chemin d'accès : About (À propos de) > Network (Réseau)

Site de fabrication du matériel : Ces informations sur le matériel sont utiles pour dépanner les problèmes concernant votre carte de gestion réseau. **Autonomie de gestion** indique la durée pendant laquelle cette interface de gestion a fonctionné en continu; en d'autres termes, il s'agit de la période écoulée depuis que la carte de gestion réseau à été démarrée à chaud ou à froid.

Module d'application, **SE APC (AOS)** et **Gestion de la réinitialisation** : Ces informations sont utiles pour le dépannage et pour déterminer si une mise à jour du micrologiciel est disponible, **www.se.com/ww/en/download/software-firmware**.

Étiquette de champ	Description
Nom	Le nom du module de micrologiciel. Le nom du **module d'application** diffère selon le type d'onduleur. Le **module APC AOS** s'appelle toujours **aos**, et le **module de gestion de la réinitialisation** **boot**.
Version	Le numéro de version du module de micrologiciel. Les numéros de version des modules peuvent être différents, mais les modules compatibles sont publiés ensemble. Reportez-vous à la section « Mises à niveau du micrologiciel de la carte de gestion réseau ».
Date et heure	La date et heure auxquelles le module de micrologiciels a été chargé.

Voir également « Vérification des numéros de version des micrologiciels installés ».

Écran Assistance

Chemin d'accès : About (À propos de) > Support (Assistance)

Avec cette option, vous pouvez consolider différentes données de cette interface dans un seul fichier compressé à des fins de dépannage et d'assistance clients. Les données comprennent les journaux de consignation des événements et des données, le fichier de configuration (voir « Création et importation de paramètres avec le fichier de configuration ») et les informations de débogage complexes.

Cliquez sur **Generate Logs (Générer des journaux de consignation)** pour créer le fichier, puis sur **Download (Téléchargement)**. Vous êtes invité à indiquer si vous voulez afficher ou enregistrer le fichier compressé.

Assistant de configuration IP des périphériques

Fonctionnalités, configuration requise et installation

L'assistant de configuration IP des périphériques peut détecter les cartes de gestion réseau auxquelles aucune adresse IP n'est affectée. Une fois les cartes détectées, vous pouvez configurer leurs paramètres d'adresse IP.

Vous pouvez également rechercher les équipements déjà présents sur le réseau en entrant une plage d'adresses IP pour définir la recherche. L'assistant analyse les adresses IP de la plage définie et détecte les cartes possédant déjà une adresse IP affectée par DHCP.

REMARQUES :

• Vous ne pouvez pas rechercher les périphériques attribués déjà sur le réseau à l'aide d'une plage d'adresses IP à moins d'activer SNMPv1 sur la carte de gestion réseau et de définir le **Community Name (Nom de communauté)** sur « public ». Pour de plus amples informations, reportez-vous à la section « Écrans SNMP ».

• Une fois l'adresse IP de la carte de gestion réseau configurée, pour accéder à l'interface Web de la carte de gestion réseau dans un navigateur, vous devez modifier l'URL de `http` à `https`.

Pour des informations détaillées sur l'assistant, consultez l'article de la base de connaissances **FA156064**.

L'article **FA156064** de la base de connaissances détaille aussi l'utilisation de l'option DHCP 12.

Configuration requise

L'assistant s'exécute sur Windows Server® 2012, Windows Server 2016, Windows Server 2019 et sur les versions 32 et 64 bits des systèmes d'exploitation Windows 8.1 et Windows 10.

L'assistant est compatible uniquement avec IPv4.

Installation

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

1. Accédez à **www.se.com/ww/en/download/software-firmware**.
2. Filtrer par Software (Logiciel) / Firmware (Micrologiciel) > Wizards and Configurators (Assistants et configurateurs).
3. Téléchargez l'assistant de configuration IP des équipements.
4. Lancez le fichier exécutable depuis le dossier dans lequel vous l'avez téléchargé.

Une fois installé, l'assistant est accessible via les options du menu Windows.

Exportation des paramètres de configuration

Récupération et exportation du fichier .ini

Résumé de la procédure

Un administrateur peut récupérer le fichier .ini d'une carte de gestion réseau et l'exporter vers une ou plusieurs autres cartes de gestion réseau. Les étapes sont décrites ci-dessous ; consultez les détails dans les sections suivantes.

1. Configurez une carte de gestion réseau avec les paramètres voulus et exportez-les. Voir « Création et importation de paramètres avec le fichier de configuration ».
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 ou plusieurs cartes de gestion réseau. Pour un transfert vers plusieurs cartes de gestion réseau, utilisez un script FTP ou SCP, ou 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 pour l'onduleur et la carte de gestion réseau duquel vous récupérez le fichier) *:* **Les en-têtes de section** sont des noms de catégories entre crochets ([ ]). **Les mots-clés**, sous chaque en-tête de section, sont des étiquettes décrivant 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 **`Override`** : Avec sa valeur par défaut, ce mot-clé empêche l'exportation d'un ou plusieurs mots-clés et de leurs valeurs spécifiques à l'appareil. Par exemple, dans la section `[NetworkTCP/IP]`, la valeur par défaut pour `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. (La modification directe du fichier .ini risque d'introduire des erreurs.)
2. L'exemple ci-dessous montre comment utiliser FTP pour récupérer le fichier config.ini depuis la carte de gestion réseau configuré à l'aide d'un client de type invite de commandes :
   a. Ouvrez une connexion avec la carte de gestion réseau à l'aide de son adresse IP :
      ```
      ftp> ip_address
      ```
   b. Connectez-vous avec le nom d'utilisateur et le mot de passe d'Administrateur.
   c. Pour configurer le mode de transfert de fichiers en binaire, saisissez :
      ```
      ftp> bin
      ```

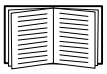
Pour afficher une barre de progression pendant le transfert de fichiers, saisissez :

```
ftp> hash
```

d. 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 client 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 (Notes de mise à jour : utilitaire de fichier.ini),* disponible sur le **site Web de Schneider Electric**. Ou consultez également l'article **FA156117** de la base de connaissances.

Personnalisation. Vous devez personnaliser le fichier avant de le transférer vers une autre carte de gestion réseau.

1. Utilisez pour ce faire 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 (Network Time Protocol), configurez le paramètre `NTPEnable` sur `enabled (activé)` :

   ```
   NTPEnable=enabled (activé)
   ```

   Vous pouvez également 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 être composé de 64 caractères maximum et doit inclure l'extension .ini.
   - Conservez le fichier personnalisé initial pour une éventuelle utilisation ultérieure. *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 un autre Carte de gestion réseau, effectuez l'une des opérations suivantes :

- À partir de l'interface utilisateur de la carte de gestion réseau destinataire, sélectionnez **Configuration (Configuration)** - **General (Généralités)** - **User Config File (Fichier de configuration utilisateur)**. Saisissez le chemin complet du fichier ou cliquez sur **Browse (Parcourir)** sur votre PC local.
- Utilisez un protocole de transfert de fichiers pris en charge par les Carte 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 le protocole FTP pour vous connecter à la carte de gestion réseau vers laquelle vous exportez ce fichier :

  ```
  ftp> open ip_address
  ```

  b. Pour configurer le mode de transfert de fichiers en binaire, saisissez :

  ```
  ftp> bin
  ```

  Pour afficher une barre de progression pendant le transfert de fichiers, saisissez :

  ```
  ftp> hash
  ```

c. Exportez le fichier .ini personnalisé vers le répertoire racine de la carte de gestion réseau destinataire :

   `ftp> put` *nom du fichier*`.ini`

Transfert du fichier vers plusieurs cartes de gestion réseau. Procédez de la manière suivante :

- Utilisez le protocole 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 batch et utiliser l'utilitaire, consultez *Release Notes: ini File Utility (Notes de mise à jour : utilitaire de fichier.ini),* disponible sur le site Web de Schneider Electric. Ou consultez l'article FA156117 de la base de connaissances.

Événement de téléchargement et messages d'erreur

L'événement et ses messages d'erreur

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 *nombre*. Avertissement au niveau du fichier de configuration : Valeur non valide à la ligne *x*.	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 *x.*	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 *x*.	Tout mot-clé saisi 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 entraîne un téléchargement incomplet. Réduisez la taille du fichier, ou divisez-le en deux fichiers et essayez à nouveau de le télécharger.

Messages dans le fichier config.ini

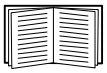
Un périphérique associé à la carte de gestion réseau depuis laquelle vous téléchargez le fichier config.ini doit être détecté avec succès pour que sa configuration soit prise en compte. Si le périphérique (tel qu'un onduleur) est absent ou n'est pas détecté, le fichier config.ini contient un message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

```
Onduleur non détecté
```

Si vous n’aviez pas l’intention d’exporter la configuration de l’appareil dans le cadre de l’importation du fichier .ini, 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.

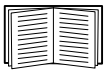


Consultez « Contenu du fichier .ini » pour des informations sur les valeurs qui sont ignorées.

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’utilitaire de configuration IP des équipements pour mettre à jour les paramètres TCP/IP de base de la carte de gestion réseau et configurer d’autres paramètres via l’interface utilisateur.



Reportez-vous à la section « Assistant de configuration IP des périphériques ».

Mises à niveau du micrologiciel de la carte de gestion réseau

Mise à jour du micrologiciel vers la version 3.0 ou supérieure

Les fichiers de micrologiciel pour la carte de gestion de réseau pour Easy UPS, monophasé (AP9544) de la version 3.0 ou supérieure nécessitent un abonnement actif au système Secure NMC System. Le système Secure NMC System protège votre entreprise en garantissant que vos appareils connectés sont protégés contre les menaces inconnues, conformes à l'évolution de la réglementation et résilients pendant toute la durée de vie de votre matériel. Pour en savoir plus, veuillez consultez **www.se.com/secure-nmc**.

Méthodes de transfert des fichiers de micrologiciel

Pour mettre à niveau le micrologiciel d'une ou plusieurs carte de gestion réseau AP9544, téléchargez l'outil Secure NMC System pour votre application depuis le site Web de Schneider Electric. Pour plus d'informations sur l'utilisation de l'outil Secure NMC System, veuillez consulter le **Guide de l'utilisateur** de l'outil SNS.

REMARQUE : Pour mettre à niveau le micro-logiciel d'une ou plusieurs cartes de gestion réseau AP9547, veuillez contacter votre représentant de service Schneider Electric local ou un partenaire de service certifiés Schneider Electric.

Mise à jour du micrologiciel vers la version 2.5 ou inférieure

La mise à niveau revient à placer le fichier `.nmc3` sur la carte de gestion réseau et ne correspond pas à une réelle installation. Vérifiez régulièrement le site **www.se.com/ww/en/download/software-firmware** pour toute nouvelle mise à niveau.

Le nom du fichier `.nmc3` a le format suivant :

```
apc_hardware-version_type_firmware-version.nmc3
```

- `apc` : Indique le contexte.
- `Version du matériel : hw0n` identifie la version du matériel sur lequel ce fichier est utilisable.
- `type` : Identifie le module.
- `version` : Le numéro de version du fichier.

Méthodes de transfert des fichiers de micrologiciel

La mise à niveau vers la version 2.5 ou une version antérieure du micrologiciel de la carte AP9547 doit être effectuée exclusivement par les représentants du service Schneider Electric ou les partenaires de service certifiés Schneider Electric.

Obtenez gratuitement la dernière version du micrologiciel depuis **www.se.com/ww/en/download/software-firmware**. Utilisez l'une des quatre méthodes suivantes pour mettre à niveau le micrologiciel d'une ou plusieurs cartes de gestion réseau :

- Sur un système d'exploitation Windows, utilisez **l'utilitaire de mise à niveau du micrologiciel** téléchargé depuis **le site Web de Schneider Electric**. Reportez-vous à la section « Utilisation de l'utilitaire de mise à niveau de micrologiciel ».
- Sur tout système d'exploitation compatible, utilisez **FTP ou SCP** pour transférer le fichier `.nmc3`. Reportez-vous à la section « Utilisation du protocole FTP ou SCP pour mettre à niveau une carte de gestion réseau unique ».
- Pour une Carte de gestion réseau qui n'est PAS sur votre réseau, utilisez **XMODEM** via un port de communication virtuel USB via le chargeur de démarrage pour transférer le fichier `.nmc3` de votre ordinateur vers la carte de gestion réseau. Reportez-vous à la section « Utilisation du protocole XMODEM pour mettre à niveau une carte de gestion réseau ».
- Utilisez un **périphérique USB** pour transférer le fichier de micrologiciel depuis votre ordinateur. Reportez-vous à la section « Utiliser une clé USB pour transférer les fichiers (AP9631 uniquement) ».
- Pour mettre à niveau plusieurs **cartes de gestion réseau**, reportez-vous aux sections « Utilisation de l'utilitaire de mise à niveau de micrologiciel de la carte de gestion réseau pour des mises à niveau multiples sous Windows » et « Mise à niveau du micrologiciel sur plusieurs cartes de gestion réseau ».

Utilisation de l'utilitaire de mise à niveau de micrologiciel

Cet utilitaire de mise à niveau du micrologiciel fait partie du package de mise à niveau du micrologiciel disponible sur **le site Web de Schneider Electric**. (N'utilisez *jamais* un utilitaire prévu pour un produit spécifique pour mettre à niveau le micrologiciel d'un autre produit.)

Utilisation de l'utilitaire pour des mises à niveau sous Windows. Sur tout système d'exploitation Windows pris en charge, l'utilitaire de mise à niveau du micrologiciel de la carte de gestion réseau automatise le transfert du fichier `.nmc3`.

Décompressez le fichier de mise à niveau de micrologiciel téléchargé et double-cliquez sur le fichier .exe. Saisissez l'adresse IP de l'hôte, le nom d'utilisateur et le mot de passe dans les champs de dialogue. Vous devez également sélectionner soit FTP, soit SCP, ainsi que le port associé. **REMARQUE :** Le protocole choisi doit être activé sur la carte de gestion réseau pour que la mise à niveau du miccrologiciel puisse être effectuée. Voir également « Utilisation de l'utilitaire de mise à niveau de micrologiciel de la carte de gestion réseau pour des mises à niveau multiples sous Windows ».

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

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 (reportez-vous à la section « Serveur FTP »).

Pour transférez le fichier, suivez ces étapes :

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

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

Pour en savoir plus sur les fichiers, reportez-vous à la section « À propos de la carte de gestion réseau et des modules de micrologiciel ».

2. Ouvrez une session client FTP :

   `C:\apc>ftp`

3. Saisissez `open (ouvrir)` et **l'adresse IP** de la carte de gestion réseau, puis appuyez sur ENTRÉE. 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 (avec un espace avant 21000) :
     `ftp> open (ouvrir) 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.
5. Mise à niveau du micrologiciel.

   `ftp> bin`
   `ftp> put apc_hw21_AA_v-v-v-v.nmc3` (où AA est l'application, par exemple eu3p, et v-v-v-v est le numéro de version du micrologiciel)
6. Lorsque le protocole FTP confirme le transfert, saisissez `Quit (Quitter)` pour fermer la session.

SCP. Pour utiliser Secure Copy (SCP) afin de mettre à jour le micrologiciel de la carte de gestion réseau, suivez ces étapes :

1. Utilisez une ligne de commande SCP pour transférer le fichier `.nmc3` vers la carte de gestion réseau. L'exemple suivant utilise *`v-v-v-v`* pour représenter le numéro de version du module d'application :

   `scp apc_hw21_eu3p_v-v-v-v.nmc3 apc@158.205.6.185:apc_hw21_eu3p_v-v-v-v.nmc3`

REMARQUE : Pour utiliser SCP, SSH doit être activé. Reportez-vous à « Écran de la console » pour activer SSH.

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

Pour utiliser XMODEM afin de mettre à niveau une carte de gestion réseau qui n'est pas sur le réseau :

1. Connectez le câble micro-USB fourni (référence 960-0603) à la carte de gestion réseau et au port USB d'un ordinateur local.
2. Appuyez sur le bouton **Reset (Réinitialiser)** de la carte de gestion réseau.
3. Lorsque la carte de gestion réseau détecte une connexion USB pendant son démarrage, elle attend 90 secondes pour laisser suffisamment de temps au système d'exploitation pour reconnaître et configurer un port de communication virtuel. Lorsque le port de communication virtuel est prêt, exécutez un programme de terminal, tel que HyperTerminal ou Tera Term, pour sélectionner le port de communication virtuel.
4. Appuyez sur **Entrée** deux fois, ou jusqu'à ce que l'invite du module de gestion de la réinitialisation s'affiche : `BM>`

   REMARQUE : Si aucune connexion au module de gestion de la réinitialisation n'est établie dans les 90 secondes suivant le redémarrage de la carte de gestion réseau, ce dernier poursuivra son processus de démarrage normal.
5. Tapez `XMODEM` et appuyez sur **Entrée**.
6. Depuis le menu du programme terminal, sélectionnez XMODEM, puis sélectionnez le fichier `.nmc3` pour le transfert à l'aide de XMODEM. Une fois le transfert XMODEM terminé, l'invite du module de gestion de la réinitialisation s'affiche à nouveau.

   Tapez `reset (réinitialiser)` ou appuyez sur le bouton **Reset (Réinitialiser)** pour redémarrer la carte de gestion réseau.

REMARQUE : Un pilote est nécessaire pour se connecter à la console de la carte de gestion réseau via Windows 7. Le pilote peut être téléchargé depuis la page produit AP9544/AP9547 sur le **site Web de Schneider Electric**, situé dans la section **Logiciels/Micrologiciels**. Aucun pilote n'est requis pour Windows 10.

1. Lorsque vous connectez la carte de gestion réseau via le câble micro-USB, un périphérique appelé « NMC3-CDC » est détecté dans « Other Devices » (Autres périphériques).
2. Faites un clic droit sur ce périphérique et sélectionnez « Update Driver Software... » (Mettre à jour le pilote…)
3. Sélectionnez l'option « Browse my computer for driver software » (Parcourir mon ordinateur à la recherche d'un pilote) et accédez à l'emplacement de téléchargement du pilote (usb_cdc_ser.inf).
4. Acceptez le message de sécurité du pilote non signé.

Windows va désormais reconnaître la carte de gestion réseau et lui attribuer un port COM.

Utiliser une clé USB pour transférer les fichiers (AP9631 uniquement)

Cette fonctionnalité est disponible dans la version v1.3.3.1 du chargeur de démarrage et les versions supérieures. Avant de commencer le transfert, assurez-vous que la clé USB est formatée en FAT, FAT16 ou FAT32.

1. Téléchargez le fichier de mise à niveau du micrologiciel.
2. Créez un dossier nommé **apcfirm** sur la clé USB.
3. Placez le fichier `.nmc3` dans le répertoire du fichier **apcfirm**.
4. Utilisez un éditeur de texte pour créer un fichier nommé **nmc3.rcf.** (L'extension doit être .rcf, pas .txt par exemple.)
5. Dans le fichier **nmc3.rcf**, ajoutez une ligne pour le package du micrologiciel à mettre à niveau. Par exemple, pour mettre à niveau **l'application** de l'onduleur triphasé vers la version v1.5.0.6, tapez :

   NMC3=apc_hw21_eu3p_1-0-0-1.nmc3
6. Placez le fichier nmc3.rcf dans le dossier **apcfirm** sur la clé USB.
7. Insérez la clé USB dans un port USB de votre carte de gestion réseau, voir« Panneau avant (AP9544/AP9547) »
8. Redémarrez la carte de gestion réseau et attendez qu'elle redémarre complètement.
9. Vérifiez que la mise à niveau a été effectuée avec succès à l'aide des procédures décrites dans « Vérification des mises à niveau ».

Mise à niveau du micrologiciel sur plusieurs cartes de gestion réseau

Utilisez l'une des trois méthodes suivantes :

- **Utilitaire de mise à niveau de micrologiciel de carte de gestion réseau sous Windows**. Reportez-vous à la section « Utilisation de l'utilitaire de mise à niveau de micrologiciel de la carte de gestion réseau pour des mises à niveau multiples sous Windows ».
- **Utilisation de FTP ou SCP**. 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.
- **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 (Notes de mise à jour : utilitaire de fichier.ini),* disponible dans la base de connaissances, **http://www.se.com/site/support/**.

Utilisation de l'utilitaire de mise à niveau de micrologiciel de la carte de gestion réseau pour des mises à niveau multiples sous Windows. Après avoir téléchargé l'utilitaire de mise à niveau depuis la page de téléchargement de la carte de gestion réseau sur le site Web de Schneider Electric, double-cliquez sur le fichier .exe et décompressez le contenu.

1. Localisez le fichier `devices.txt` dans le répertoire avec l'utilitaire. Ouvrez et modifiez ce fichier avec un éditeur de texte pour y saisir les informations nécessaires pour chaque périphérique de la carte de gestion réseau à mettre à niveau :
   - [Appareil] : Cet en-tête de section doit être inclus pour chaque carte de gestion réseau à mettre à niveau.
   - Hôte : L'adresse Ipv4 de l'appareil.
   - Protocole : FTP ou SCP.
   - Port : Le port associé de SCP ou FTP.
   - Nom d'utilisateur : Le nom d'utilisateur d'un Administrateur, activé sur la carte de gestion réseau.
   - Mots de passe : Le mot de passe d'un Administrateur, activé sur la carte de gestion réseau

   Supprimez tous les commentaires et points-virgules de `devices.txt`, et enregistrez vos modifications.

   Par exemple :

   ```
   [Équipement]
   Hôte=192.168.0.1
   Protocole=SCP
   Port=22
   Nom d'utilisateur=apc
   Mot de passe=apc


   [Équipement]
   Hôte=192.168.0.2
   Protocole=SCP
   Port=22
   Nom d'utilisateur=apc
   Mot de passe=apc
   ```

   Vous pouvez le cas échéant utiliser un fichier `devices.txt` existant.
2. Utilisation de l'utilitaire de mise à niveau de micrologiciel. Si les informations correctes ont été fournies dans le fichier `devices.txt`, le message suivant apparaîtra dans l'utilitaire :

   ```
   Une liste de périphériques a été détectée et importée ; par conséquent,
   les hôtes listés dans la fenêtre d'événements ci-dessous seront utilisés
   comme actifs.
   ```
3. Cliquez sur **Start Update (Démarrer la mise à niveau)** dans l'utilitaire pour démarrer la ou les mises à niveau du micrologiciel.

Vérification des mises à niveau

Vérification du succès ou de l'échec du transfert

Pour vérifier si une mise à niveau de micrologiciels a réussi, utilisez la commande `xferStatus` dans l'interface par ligne de commande afin de consulter le résultat du dernier transfert.

Codes de résultat du dernier transfert

Les erreurs de transfert possibles incluent l'impossibilité de trouver le serveur TFTP ou FTP, le refus de l'accès au serveur, l'impossibilité pour le serveur de trouver ou de reconnaître le fichier de transfert ou l'altération du fichier de transfert.

Vérification des numéros de version des micrologiciels installés

Chemin d'accès : À propos de - Réseau

Utilisez l'interface utilisateur Web pour vérifier les versions des modules de micrologiciels mis à niveau. Vous pouvez également utiliser une commande SNMP GET pour l'OID MIB II **sysDescr**. Dans l'interface par ligne de commande, utilisez la commande **about (à propos de)**.

Changement de la langue de l'interface utilisateur

Vous pouvez afficher l'interface utilisateur (UI) de la carte de gestion réseau dans différentes langues en sélectionnant une langue dans la liste déroulante **Language (Langue)** sur l'écran **Login (Connexion)**.

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

Dépannage

Problèmes d’accès à la carte de gestion réseau

Consultez la base de connaissances sur www.se.com/support pour un dépannage étape par étape et des solutions utiles aux problèmes courants. Pour contacter l’assistance clients, reportez-vous à « Assistance clients internationale ».

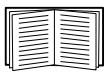
Problème	Solution
Impossible de contacter la carte de gestion réseau par ping	Si le témoin d’état de la carte de gestion réseau est vert, tentez un test ping sur un nœud différent du même segment de réseau que celui de la carte de gestion réseau. Si cela ne fonctionne pas, le problème ne vient pas de la carte de gestion réseau. Si le voyant d’état n’est pas vert ou que le test ping réussit, procédez aux vérifications suivantes : • Vérifiez que la carte de gestion réseau est correctement installée dans l’Onduleurs. • 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 numéro des octets du sous-réseau du 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 ligne 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 ligne 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, Telnet est désactivé et SSH est activé. Les protocoles SSH et Telnet peuvent être activés/ désactivés indépendamment. • 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.

Problème	Solution
Impossible d'accéder à l'interface utilisateur	• Vérifiez que l'accès HTTP ou HTTPS est activé. • Assurez-vous l'URL spécifiée est 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 envoyer un test ping à la carte de gestion réseau. • Vérifiez que vous utilisez un navigateur Web pris en charge par la carte de gestion réseau. Reportez-vous à la section « Assistance clients internationale ». • 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 générer 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 ligne de commande ou l'interface utilisateur pour vérifier que le NMS dispose d'un accès. Reportez-vous à la section « Écrans SNMP ».
Impossible d'exécuter une commande SET	• Vérifiez que le protocole SNMP est activé. Les protocoles SNMPv1 et SNMPv3 sont désactivés par défaut. • Vérifiez le nom de communauté (SNMPv1) en lecture/écriture (SET) ou la configuration du profil utilisateur (SNMPv3). • Utilisez l'interface par ligne de commande ou l'interface utilisateur pour vous assurer que le NMS dispose de l'accès (SNMPv1) en écriture (SET) ou de l'accès à l'adresseIP cible par l'intermédiaire de la liste de contrôle d'accès (SNMPv3). Reportez-vous à la section « Écrans SNMP ».
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, interrogez l'OID **mconfigTrapReceiverTable** de la MIB pour 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 ligne de commande ou l'interface utilisateur 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. Reportez-vous aux sections « Écrans SNMP », « Récepteurs de traps », et « Écran de test des traps SNMP ».
Les traps reçus au niveau du NMS ne sont pas identifiés	Reportez-vous à la documentation fournie avec votre NMS pour vérifier que les traps sont correctement intégrés à la base de données des alarmes/traps.

Problèmes Modbus



Pour de plus amples informations sur l'implémentation de Modbus sur votre onduleur, consultez l'**Addenda à la documentation Modbus** ou le **Plan de registre Modbus pour AP9547**.

Problèmes liés au périphérique Wi-Fi USB APC (AP9834)

Problème	Solution
Impossible de se connecter au réseau Wi-Fi	• Vérifiez que le périphérique Wi-Fi USB APC est correctement inséré dans un port USB d'une carte AP9544/AP9547. • Vérifiez que les paramètres Wi-Fi corrects sont indiqués dans l'interface utilisateur Web ou l'interface de ligne de commande de la carte de gestion réseau. • Vérifiez que les paramètres Wi-Fi corrects sont indiqués dans l'interface utilisateur Web ou l'interface de ligne de commande de la carte de gestion réseau. Si les paramètres Wi-Fi sont saisis incorrectement ou laissés vides, la carte de gestion réseau enregistrera une erreur dans le journal des événements. Par exemple : « USB Wi-Fi Device error. Wi-Fi Settings » (Erreur du périphérique Wi-Fi USB. Paramètres Wi-Fi). Si le problème persiste, contactez un administrateur réseau pour qu'il diagnostique les problèmes de connexion.
Impossible de résoudre l'état du voyant rouge fixe de l'appareil	• Vérifiez que les paramètres Wi-Fi corrects sont indiqués dans l'interface utilisateur Web ou l'interface de ligne de commande de la carte de gestion réseau. • Résolvez tous les événements liés au Wi-Fi dans le journal des événements de la carte de gestion réseau. Par exemple : « USB Wi-Fi Device error. Wi-Fi Settings » (Erreur du périphérique Wi-Fi USB. Paramètres Wi-Fi). • Réactivez la connexion filaire et configurez les paramètres Wi-Fi via une autre méthode : – Interface utilisateur sur le Web (**Configuration (Configuration) > Network (Réseau) > Wi-Fi (Wi-Fi)**) – Interface en ligne de commande (commande `wifi`) – fichier config.ini (section `NetworkWiFi`) Si la connexion filaire n'est plus disponible, connectez le câble micro-USB (960-0603) au port console de la carte de gestion réseau pour accéder à l'interface de ligne de commande (CLI) et transférez le fichier config.ini à l'aide de la commande xferINI. Pour de plus amples informations, consultez le **Guide de carte de gestion réseau pour onduleur Easy UPS CLI**. Si le problème persiste, contactez l'assistance clients. Reportez-vous à la section « Assistance clients internationale ».

Description des voyants

État	Description
Off	Il peut s'agir d'une des situations suivantes : • L'appareil n'est pas inséré dans un port USB d'une carte de gestion réseau AP9544/AP9547. • Le micrologiciel de la carte de gestion réseau ne prend pas en charge le Wi-Fi. La prise en charge du Wi-Fi est disponible à partir de la version 1.4 du micrologiciel. Reportez-vous à la section « Mises à niveau du micrologiciel de la carte de gestion réseau ». • L'appareil ne fonctionne pas correctement. Il doit peut-être être réparé ou remplacé. Veuillez contacter l'assistance clients. Reportez-vous à la section « Assistance clients internationale ».
Vert fixe	L'appareil est connecté à un point d'accès, mais aucune activité réseau n'est détectée.
Vert clignotant	L'appareil est connecté à un point d'accès et le réseau Wi-Fi est actif.
Rouge fixe	Il peut s'agir d'une des situations suivantes : • L'appareil présente une erreur permanente. • Il y a une erreur permanente avec les paramètres Wi-Fi de la carte de gestion réseau. • Des problèmes insolubles de connexion à un point d'accès ont été rencontrés.
Rouge clignotant	L'appareil est en train d'établir une connexion Wi-Fi avec un point d'accès.

Garantie usine de deux ans

Cette garantie s'applique uniquement aux produits que vous avez achetés pour les utiliser conformément aux instructions données dans ce manuel.

Conditions de garantie

APC garantit que ses produits seront exempts de tout défaut matériel ou de fabrication pendant une période de deux ans à compter de la date d'achat. APC procédera à la réparation ou au remplacement de tout produit défectueux couvert par cette garantie. Cette garantie ne s'applique pas au matériel qui a été endommagé par accident, négligence ou mauvaise utilisation, ou qui a été modifié de quelque manière que ce soit. La réparation ou le remplacement d'un produit défectueux ou d'un de ses composants ne prolonge 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, consultez le site Web de Schneider Electric www.se.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. APC ne peut en outre 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'une tension électrique incorrecte ou inadaptée, 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, d'installation contraire aux recommandations ou spécifications d'APC, de tout autre événement si le numéro de série APC a été modifié, dégradé ou effacé, ou de toute autre cause survenue en dehors du cadre d'une utilisation autorisée.

IL N'EXISTE AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, PAR APPLICATION DE LA LOI OU AUTRE, DE PRODUITS VENDUS, RÉPARÉS OU FOURNIS DANS LE CADRE DE CET ACCORD OU EN RAPPORT AVEC CELUI-CI. APC REJETTE TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE, DE SATISFACTION ET D'ADÉQUATION À UN USAGE PARTICULIER. LES GARANTIES EXPLICITES D'APC NE PEUVENT ÊTRE ÉTENDUES, DIMINUÉES OU AFFECTÉES PAR LES CONSEILS OU SERVICES TECHNIQUES OU AUTRES OFFERTS PAR APC CONCERNANT LES PRODUITS, ET AUCUNE OBLIGATION OU RESPONSABILITÉ NE PEUT S'EN DÉGAGER. LES PRÉSENTS RECOURS ET GARANTIES SONT EXCLUSIFS ET PRIMENT SUR TOUS LES AUTRES RECOURS ET GARANTIES. EN CAS DE NON-RESPECT DE CES GARANTIES, LA RESPONSABILITÉ D'APC ET LE RECOURS DE L'ACHETEUR SE LIMITENT AUX GARANTIES INDIQUÉES CI-DESSUS. LES GARANTIES OCTROYÉES PAR APC S'APPLIQUENT UNIQUEMENT À L'ACHETEUR ET NE SONT PAS TRANSFÉRABLES À UN TIERS.

EN AUCUN CAS, APC, SES AGENTS, SES DIRECTEURS, SES FILIALES OU SES EMPLOYÉS NE POURRONT ÊTRE TENUS RESPONSABLES POUR TOUTE FORME DE DOMMAGES INDIRECTS, PARTICULIERS, IMMATÉRIELS OU EXEMPLAIRES, SUITE À L'UTILISATION, L'ENTRETIEN OU L'INSTALLATION DES PRODUITS, QUE CES DOMMAGES REVÊTENT UN CARACTÈRE CONTRACTUEL OU DÉLICTUEL, SANS TENIR COMPTE DES DÉFAUTS, DE LA NÉGLIGENCE OU DE LA RESPONSABILITÉ ABSOLUE, OU MÊME SI APC A ÉTÉ PRÉVENU DE L'ÉVENTUALITÉ DE TELS DOMMAGES. SPÉCIFIQUEMENT, APC N'EST RESPONSABLE D'AUCUN COUT, TEL QUE LA PERTE DE PROFITS OU DE REVENUS, LA PERTE DE MATÉRIEL, LA PERTE DE L'UTILISATION DE MATÉRIEL, LA PERTE DE LOGICIELS OU DE DONNÉES, LE COUT DE SUBSTITUTS, LES RÉCLAMATIONS PAR DES TIERS OU AUTRES.

AUCUN REPRÉSENTANT, EMPLOYÉ OU AGENT D'APC N'EST AUTORISÉ À APPORTER DES ANNEXES OU DES MODIFICATIONS AUX CONDITIONS DE LA PRÉSENTE GARANTIE. LES CONDITIONS DE LA GARANTIE NE PEUVENT ÊTRE MODIFIÉES, LE CAS ÉCHÉANT, QUE PAR ÉCRIT 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 Assistance du site Web de Schneider Electric à l'adresse suivante **www.se.com/support**. Sélectionnez votre pays dans le menu déroulant situé en haut de la page. Sélectionnez l'onglet Support (Assistance) pour obtenir les coordonnées du service d'assistance clients dans votre région.

Avis sur le Copyright

Bibliothèque de cryptologie Cryptlib

Cryptlib copyright © Digital Data Security New Zealand Ltd 1998.

Berkeley Database

Copyright © 1991, 1993 The Regents of the University of California. Tous droits réservés.

La redistribution et l'utilisation sous forme de code source ou binaire, avec ou sans modification, sont autorisées à condition que les conditions suivantes soient respectées :

1. Toute redistribution du code source doit conserver l'avis de droit d'auteur ci-dessus, cette liste de conditions et l'avertissement suivant.
2. Les redistributions sous forme binaire doivent reproduire l'avis de droit d'auteur ci-dessus, cette liste de conditions et l'avertissement suivant dans la documentation et/ou les autres éléments fournis avec la distribution.
3. Tous les supports publicitaires mentionnant les fonctionnalités ou l'utilisation de ce logiciel doivent afficher la mention suivante : Ce produit comprend un logiciel développé par l'Université de Californie, Berkeley et ses contributeurs.
4. Ni le nom de l'Université ni les noms de ses contributeurs ne peuvent être utilisés pour cautionner ou promouvoir des produits dérivés de ce logiciel sans autorisation écrite préalable spécifique.

CE LOGICIEL EST FOURNI PAR LES RÉGENTS ET LES CONTRIBUTEURS « TEL QUEL » ET TOUTE GARANTIE EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, EST EXCLUE. EN AUCUN CAS LES RÉGENTS OU LES CONTRIBUTEURS NE SERONT RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX, EXEMPLAIRES OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS S'Y LIMITER, L'ACQUISITION DE BIENS OU DE SERVICES DE REMPLACEMENT ; LA PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS ; OU L'INTERRUPTION D'ACTIVITÉ), QUELLE QU'EN SOIT LA CAUSE ET SUR TOUTE THÉORIE DE RESPONSABILITÉ, QU'ELLE SOIT CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE), DÉCOULANT DE QUELQUE MANIÈRE QUE CE SOIT DE L'UTILISATION DE CE LOGICIEL, MÊME SI L'ON A ÉTÉ AVERTIS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Lua

Copyright © 1994–2021 Lua.org, PUC-Rio.

La permission est accordée, à titre gratuit, à toute personne obtenant une copie de ce logiciel et de sa documentation associée (le « Logiciel »), de traiter le Logiciel sans restriction, y compris, sans limitation, les droits d'utiliser, de copier, de modifier, de fusionner, de publier, de distribuer, de concéder en sous-licence et/ou de vendre des copies.

Le présent avis de droit d'auteur et la présente mention d'autorisation doivent être incluses dans toutes les copies ou parties substantielles du Logiciel.

LE LOGICIEL EST FOURNI « TEL QUEL », SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET D'ABSENCE DE CONTREFAÇON. EN AUCUN CAS LES AUTEURS OU LES DÉTENTEURS DES DROITS D'AUTEUR NE SERONT TENUS RESPONSABLES DE TOUTE RÉCLAMATION, DE TOUT DOMMAGE OU DE TOUTE AUTRE RESPONSABILITÉ, QUE CE SOIT DANS LE CADRE D'UNE ACTION CONTRACTUELLE, DÉLICTUELLE OU AUTRE, DÉCOULANT DU LOGICIEL, DE SON UTILISATION OU DE TOUTE AUTRE TRANSACTION RELATIVE À CE LOGICIEL.

Assistance clients internationale

Les conditions d'accès au service client peuvent varier selon le produit. L'assistance clients pour ce produit ou tout autre produit est disponible gratuitement des manières suivantes :

- rendez-vous sur le site Web de Schneider Electric pour accéder aux documents de la Base de connaissances Schneider Electric et soumettre des demandes d'assistance client.
  - **www.schneider-electric.com** (Siège social)
    Connectez-vous au site Web Schneider Electric spécifique à votre pays, qui contient des informations relatives à l'assistance clients.
  - **www.schneider-electric.com/support/**
    Recherche d'assistance mondiale dans la Base de connaissances Schneider Electric et utilisation de l'assistance électronique.
- Contactez le centre d'assistance client de Schneider Electric par téléphone ou par e-mail.
  - Centres locaux spécifiques aux pays : rendez-vous sur **www.schneider-electric.com > Assistance > Opérations dans le monde** pour obtenir les coordonnées.

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

© 2025 Schneider Electric. Tous droits réservés. Schneider Electric, APC et Network Management Card sont des marques commerciales et la propriété de Schneider Electric SE, de ses filiales ou de ses sociétés affiliées. Toutes les autres marques sont la propriété de leurs détenteurs respectifs.

990–91545F-012 **05/2025**