

La puissance derrière la compétitivité

# Delta InsightPower SNMP IPv6 pour PDU

Manuel d'utilisation

[www.deltapowersolutions.com](http://www.deltapowersolutions.com)



**DELTA**  
Smarter. Greener. Together.

## Conservez ce manuel

Le présent manuel renferme des instructions et des avertissements importants qui doivent être observés durant l'installation, le fonctionnement, l'entreposage et la maintenance de ce produit. Le non-respect de ces instructions et avertissements annule la garantie.

Copyright©2013 par Delta Electronics Inc. Tous droits réservés. Tous les droits relatifs au présent manuel d'utilisateur (« Manuel »), y compris, mais sans s'y restreindre, le contenu, les informations et les figures, sont entièrement détenus par et réservés à Delta Electronics Inc. (« Delta »). Le présent manuel est destiné uniquement au fonctionnement et à l'utilisation de ce produit. Toute cession, duplication, diffusion, reproduction, modification, traduction, extraction ou utilisation du présent manuel, en tout ou en partie, est interdite sans l'autorisation écrite préalable de Delta. Attendu que Delta ne cesse d'améliorer et de développer le produit, la société peut être amenée à modifier à tout moment les informations contenues dans ce manuel sans pour autant être tenue d'informer quiconque de ces révisions ou modifications. Delta veille autant que possible à garantir l'exactitude et l'intégrité du présent manuel. Delta décline toute forme de garantie ou d'engagement, explicite ou implicite, y compris sans toutefois s'y limiter, l'exhaustivité, l'absence de vice, l'exactitude, l'absence de violation, la qualité marchande ou l'adéquation à un usage particulier du présent manuel.

# Table des matières

<b>Chapitre 1 : Instructions de sécurité importantes</b>	<b>1</b>
1-1 Avertissements	1
1-2 Conformité aux normes	1
<b>Chapitre 2 : Introduction</b>	<b>2</b>
2-1 Description du produit	2
2-2 Fonctionnalités	2
2-3 Contenu de l'emballage	3
2-4 Interface	4
<b>Chapitre 3 : Installation</b>	<b>7</b>
3-1 Installation du SNMP IPv6 sur votre PDU	7
3-2 Raccordement de plusieurs dispositifs PDU	8
<b>Chapitre 4 : Configurations système</b>	<b>10</b>
4-1 Configuration via InsightPower SNMP IPv6 pour PDU Web	10
4-2 Configuration avec EzSetting	12
4-3 Configuration via Telnet	14
4-4 Configuration via le port COM	14
4-5 Configuration par mode Texte	16
<b>Chapitre 5 : InsightPower SNMP IPv6 pour PDU Web.</b>	<b>23</b>
5-1 Monitor (Moniteur)	24
5-1-1 Information (Informations)	24
Status (Etat)	24
Detail (Informations détaillées)	25
5-1-2 History (Historique)	25
Event Log (Journal des événements)	25
Energy Log (Journal énergie)	26
Energy Compare (Comparaison énergétique)	27

	Data Log (Journal des données)-----	28
	Configuration-----	28
<b>5-1-3</b>	<b>Environment (Environnement) -----</b>	<b>29</b>
	Information (Informations) -----	29
	Configuration-----	30
<b>5-1-4</b>	<b>About (A propos) -----</b>	<b>30</b>
	Information (Informations) -----	30
<b>5-2</b>	<b>Device (Dispositif) -----</b>	<b>31</b>
<b>5-2-1</b>	<b>Configuration -----</b>	<b>31</b>
	PDU -----	31
	<b>System (Système) -----</b>	<b>32</b>
<b>5-3-1</b>	<b>Administration -----</b>	<b>32</b>
	User Manager (Gestionnaire des utilisateurs)-----	32
	TCP/IP-----	33
	Web -----	34
	Console-----	35
	FTP-----	36
	Time Server (Serveur de temps)-----	37
	Syslog-----	38
	Batch Configuration (Configuration de lot)-----	38
	Upgrade (Mise à niveau)-----	40
<b>5-3-2</b>	<b>Notification -----</b>	<b>41</b>
	SNMP Access (Accès SNMP)-----	41
	SNMPv3 USM (Gestion des sessions utilisateur SNMPv3)-----	42
	SNMP Trap (Alerte SNMP) -----	43
	Mail Server (Serveur de messagerie) -----	44
<b>Chapitre 6 : Mise à niveau du microprogramme du dispositif</b>		
	<b>SNMP-----</b>	<b>46</b>
<b>Chapitre 7 : Dépannage -----</b>		<b>49</b>
<b>Annexe A : Spécifications -----</b>		<b>56</b>
<b>Annexe B : Garantie-----</b>		<b>57</b>

# Chapitre 1 : Instructions de sécurité importantes

## 1-1 Avertissements

- L'InsightPower SNMP IPv6 pour PDU (ci-après dénommé « SNMP IPv6 ») est compatible avec les modèles suivants : PDU1113, PDU1213, PDU1311, PDU1315, PDU1425, PDU2421, et PDU2525.
- Le SNMP IPv6 doit être monté sur un PDU (Power Distribution Unit, Unité de distribution de puissance). Avant l'installation, assurez-vous que toutes les sources d'énergie et charges critiques raccordées au PDU sont débranchées.
- Le SNMP IPv6 peut fonctionner avec jusqu'à 16 PDU en cascade.
- Cette unité ne doit pas être positionnée ou utilisée en présence de substances inflammables.
- Ne tentez pas de démonter l'unité.
- Ne tentez pas d'effectuer des modifications internes sur l'unité.
- Ne tentez pas de réparer/remplacer des composants internes. Si une réparation est requise, signaler tout entretien au centre d'entretien ou distributeur agréé Delta le plus proche.
- Ne laissez aucun objet ou liquide de quelque type que ce soit pénétrer l'unité.
- Suivez toujours le présent Manuel d'utilisation pour installer et exploiter cette unité.
- Ne lisez pas le CD inclus avec un lecteur CD conventionnel. Cela pourrait générer un bruit important, à un niveau sonore susceptible d'entraîner une perte d'audition irréversible.

## 1-2 Conformité aux normes

- **EN 55022:2006 + A1:2007, Classe B**
- **EN 55024:1998 + A1:2001 + A2:2003**  
CEI 61000-4-2:1995+A1:1998+A2:2000  
CEI 61000-4-3:2006  
CEI 61000-4-4:2004  
CEI 61000-4-5:2005  
CEI 61000-4-6:2007  
CEI 61000-4-8:1993+A1:2000  
CEI 61000-4-11:2004

# Chapitre 2 : Introduction

## **2-1 Description du produit**

L'InsightPower SNMP IPv6 pour PDU (dénommé ci-après « SNMP IPv6 ») est un dispositif offrant une interface entre un PDU (Power Distribution Unit, Unité de distribution de puissance) et un réseau. Ce dispositif communique avec le PDU, obtient des informations et gère à distance le PDU via un système réseau. Le SNMP IPv6 prend en charge des protocoles publics, y compris les protocoles SNMP et HTTP. Vous pouvez configurer ce dispositif en toute simplicité via un système réseau, facilement obtenir l'état du PDU et gérer votre PDU via le SNMP IPv6.

## **2-2 Fonctionnalités**

- **Gestion de PDU en réseau**

Permet la gestion à distance du PDU depuis n'importe quel poste de travail, par Internet ou Intranet.

- **Contrôle du PDU à distance via SNMP et HTTP**

Permet le contrôle à distance du PDU en utilisant le NMS SNMP, la MIB (Management Information Base, Base d'information de gestion) Delta ou un navigateur Web.

- **Configurations des fonctions PDU et système depuis n'importe quel client (protégé par mot de passe)**

Définissez les paramètres du PDU et du système via un navigateur Web.

- **Tenue à jour du journal des événements et des données**

Permet d'obtenir un historique de données relatives à la qualité de puissance du PDU, au journal des événements et à l'état.

**Autres fonctionnalités et protocoles pris en charge :**

- Notifications à l'utilisateur par alertes SNMP et e-mails.
- Protocole NTP.
- Configuration Telnet.
- BOOTP/DHCP

- Protocoles de sécurité HTTPS, SSH, SFTP et SNMPv3.
- Connexion RADIUS et authentification locale.
- Gestion à distance du journal des événements via Syslog.
- Protocole IPv4
- Protocole IPv6 (IPv6 Ready Logo Phase 2 [Core for Host, Logo ID 02-C-000459])
- Contrôle de 16 dispositifs PDU en cascade max.

## 2-3 Contenu de l'emballage

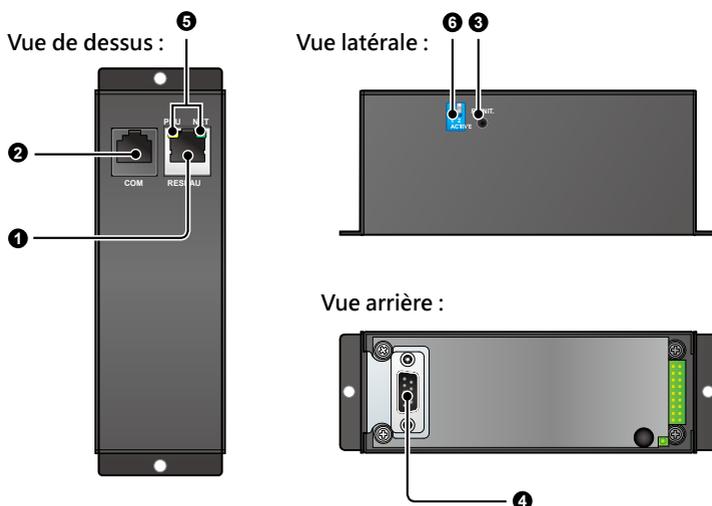
Veillez vérifier attentivement le SNMP IPv6 et les accessoires inclus. Contactez votre revendeur si l'un des éléments est manquant ou endommagé. Si vous devez retourner les articles pour quelque motif que ce soit, assurez-vous de les remballer soigneusement dans les éléments d'emballage d'origine fournis avec l'unité.



N°	Élément	Quantité
1	InsightPower SNMP IPv6 pour PDU	1 pièce
2	Câble RJ45 vers DB9	1 pièce
3	Logiciel et CD du manuel de l'utilisateur	1 pièce

## 2-4 Interface

L'interface contient un port RESEAU, un port COM, des voyants LED, un bouton de réinitialisation, des commutateurs DIP et un port RS232 (femelle) illustrés ci-dessous. Pour connaître leurs fonctions et indications, veuillez vous reporter au tableau suivant.



N°	Élément	Description
1	Port réseau	Se connecte au réseau.
2	Port de la console (COM)	1. Se connecte à un poste de travail avec le câble RJ45 vers DB9 fourni. 2. Se connecte à un EnviroProbe.
3	Bouton de réinitialisation	Permet de réinitialiser uniquement le SNMP IPv6. Cela n'affecte pas le fonctionnement du PDU.

N°	Élément	Description
4	Port RS232 (femelle)	Se connecte au port RS232 (mâle) de votre PDU et obtient les informations du PDU.

- |   |             |  |
|---|-------------|--|
| 5 | Voyants LED | <p>Lorsque le SNMP IPv6 est en cours d'initialisation ou de mise à jour du microprogramme, les deux voyants LED clignotent simultanément pour indiquer son état. Veuillez vous reporter aux indications suivantes :</p> <ul style="list-style-type: none"> <li>• <b>Clignotement simultané rapide</b> (toutes les 50 ms) : Initialisation ou mise à niveau du microprogramme en cours.</li> <li>• <b>Clignotement simultané lent</b> (toutes les 500 ms) : Echec de l'initialisation.</li> </ul> |
|---|-------------|--|



**AVERTISSEMENT :** Ne retirez **PAS** le SNMP IPv6 et ne débranchez pas l'alimentation d'entrée du PDU lors de l'initialisation ou la mise à niveau du microprogramme ! Cela pourrait provoquer une perte de données ou endommager le SNMP IPv6.

Le voyant LED vert indique l'état de connexion réseau :

- **ACTIVE** : La connexion réseau est établie et l'adresse IPv4 peut être utilisée.
- **DESACTIVE** : Pas de connexion réseau.
- **Clignote lentement** (toutes les 500 ms) : Adresse IP incorrecte.

Le voyant LED jaune indique l'état de liaison entre le SNMP IPv6 et le PDU :

- **Clignote rapidement** (toutes les 50 ms) : PDU lié.
- **Clignote lentement** (toutes les 500 ms) : PDU non lié.

**N° Élément Description**

- 6** Commutateurs DIP Déterminent les modes de fonctionnement.

Commutateurs DIP	Mode de fonctionnement	Description
	Mode normal	Le SNMP IPv6 fonctionne avec le PDU. Il fournit les informations d'état et paramètres du PDU via un système réseau.
	Mode d'écriture directe	Le SNMP IPv6 cesse de sonder le PDU, mais transfère les données de communication entre le port de la console et le PDU.
	Mode capteur (avec EnviroProbe)	Le SNMP IPv6 fonctionne avec le PDU et un EnviroProbe en option. Il fournit non seulement les informations d'état et les valeurs de paramètres du PDU, mais également les informations d'état de l'EnviroProbe et ses paramètres environnementaux, tels que la température et l'humidité ambiantes.
	Mode configuration	Dans ce mode, l'utilisateur peut se connecter via le port de la console et configurer les réglages du SNMP IPv6. Veuillez vous reporter à la section <b>4-4 Configuration via le port COM.</b>

**NOTE** 

Pour obtenir des informations sur l'EnviroProbe, veuillez vous reporter au Guide d'installation inclus dans l'emballage de l'EnviroProbe.

## Chapitre 3 : Installation

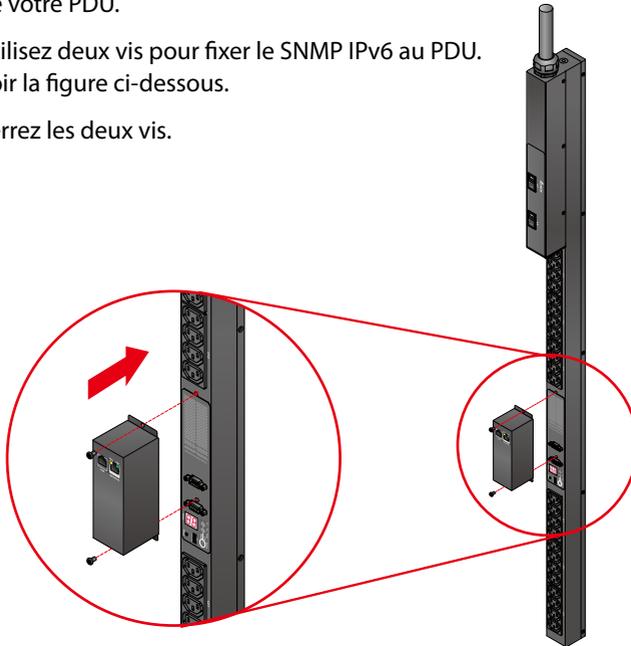


Avant l'installation, assurez-vous de débrancher toutes les sources d'énergie et charges critiques raccordées au PDU. Dans le cas contraire, le SNMP IPv6 pourrait rencontrer des problèmes de court-circuit, entraînant l'arrêt ou l'endommagement du PDU.

### 3-1 Installation du SNMP IPv6 sur votre PDU

Veillez suivre les procédures ci-dessous pour installer le SNMP IPv6 sur votre PDU (*voir Figure 3-a*).

- Etape 1** Mettez le PDU hors tension (assurez-vous que les disjoncteurs d'entrée du PDU sont en position d'**arrêt**).
- Etape 2** Connectez le port RS232 (femelle) du SNMP IPv6 au port RS232 (mâle) de votre PDU.
- Etape 3** Utilisez deux vis pour fixer le SNMP IPv6 au PDU. Voir la figure ci-dessous.
- Etape 4** Serrez les deux vis.



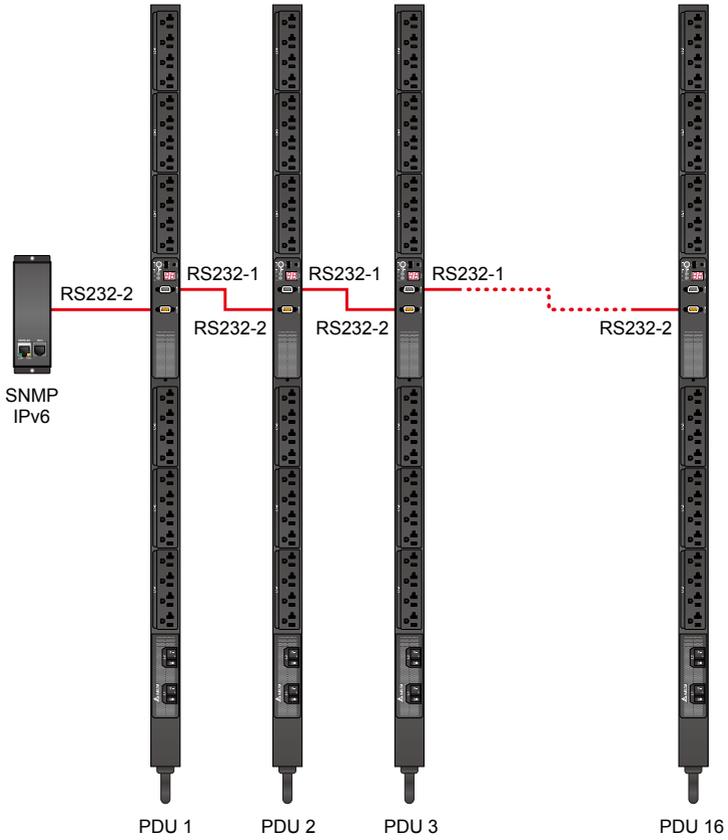
(Figure 3-a : Installation du SNMP IPv6 sur votre PDU)

## 3-2 Raccordement de plusieurs dispositifs PDU

Le SNMP IPv6 peut être connecté à 16 dispositifs PDU max. (différents modèles sont autorisés). Si vous souhaitez disposer des dispositifs PDU en cascade, définissez un numéro d'identification unique (0~15) pour chaque PDU avec ses quatre commutateurs DIP (*voir Tableau 3-1*) et utilisez des câbles RS232 pour raccorder des dispositifs PDU (*voir Figure 3-b*).

Tableau 3-1 : Réglages des commutateurs DIP du PDU

Commutateurs DIP du PDU	Numéro d'identification	Commutateurs DIP du PDU	Numéro d'identification	Commutateurs DIP du PDU	Numéro d'identification
ACTIVE  1 2 3 4	0	ACTIVE  1 2 3 4	6	ACTIVE  1 2 3 4	12
ACTIVE  1 2 3 4	1	ACTIVE  1 2 3 4	7	ACTIVE  1 2 3 4	13
ACTIVE  1 2 3 4	2	ACTIVE  1 2 3 4	8	ACTIVE  1 2 3 4	14
ACTIVE  1 2 3 4	3	ACTIVE  1 2 3 4	9	ACTIVE  1 2 3 4	15
ACTIVE  1 2 3 4	4	ACTIVE  1 2 3 4	10		
ACTIVE  1 2 3 4	5	ACTIVE  1 2 3 4	11		



**(Figure 3-b : Raccordement de plusieurs dispositifs PDU)**

## Chapitre 4 : Configurations système

Il existe différentes manières de configurer votre SNMP IPv6. Si une connexion réseau est disponible, les méthodes suivantes peuvent être appliquées :

- **Interface basée sur le Web** : L'InsightPower SNMP IPv6 pour PDU Web permet une gestion et un contrôle complets du système. Veuillez vous reporter au **chapitre 5 : InsightPower SNMP IPv6 pour PDU Web**.
- **EzSetting** : Utilisez le programme EzSetting prévu pour configurer rapidement votre SNMP IPv6. Veuillez vous reporter à la section **4-2 Configuration avec EzSetting**.
- **Mode Telnet** : Permet de configurer votre SNMP IPv6 en mode texte. Veuillez vous reporter à la section **4-3 Configuration via Telnet**.

Les méthodes mentionnées précédemment nécessitent une connexion réseau. En l'absence d'une telle connexion, vous pouvez utiliser directement une connexion via le port COM pour configurer votre SNMP IPv6. Veuillez vous reporter à la section **4-4 Configuration via le port COM**.

### NOTE



1. Afin d'assurer la sécurité du système, il est fortement recommandé de modifier votre compte et votre mot de passe après la première connexion.
2. Si plusieurs unités SNMP IPv6 sont installées au sein de votre réseau, nous vous conseillons vivement de modifier le nom d'hôte par défaut du SNMP IPv6 afin d'éviter les conflits. Egalement, il est recommandé de désactiver BOOTP/DHCP et d'attribuer manuellement une adresse IP statique valide au SNMP IPv6.

### **4-1** Configuration via InsightPower SNMP IPv6 pour PDU Web

Pour configurer le SNMP IPv6 via votre navigateur Web, veuillez suivre les instructions ci-dessous :

**Etape 1** Utilisez un câble réseau CAT5 pour connecter le port réseau du SNMP IPv6 au réseau. Lancez votre navigateur Web. Dans la barre d'adresse, entrez le nom d'hôte par défaut du SNMP IPv6 « **InsightPower** » ou l'adresse IP par défaut **192.168.1.100**. Si vous ne pouvez pas vous connecter, reportez-vous au **chapitre 7 : Dépannage Q6**.

**NOTE**

Si vous avez précédemment modifié le nom d'hôte ou l'adresse IP du SNMP IPv6, connectez-vous avec les nouveaux réglages.

- Etape 2** Connectez-vous en tant qu'administrateur (compte/mot de passe par défaut : admin/password, sensibles à la casse).
- Etape 3** Indiquez votre langue d'affichage préférée (par défaut : Anglais) dans le menu déroulant en haut à droite de la page. Le SNMP IPv6 se souvient de votre langue préférée. Dans les instructions suivantes, l'anglais est sélectionné comme langue d'affichage.
- Etape 4** Cliquez sur **System (Système)** → **Administration** → **User Manager (Gestionnaire des utilisateurs)**. Gérez vos comptes et mots de passe de connexion dans la sous-rubrique « Local authentication » (Authentification locale). L'autorisation d'accès pour les types de comptes est indiquée comme suit :
- 1) **Administrator (Administrateur)** : Autorisé à modifier tous les réglages.
  - 2) **Device Manager (Gestionnaire de périphériques)** : Autorisé à modifier les réglages relatifs aux périphériques.
  - 3) **Read Only User (Utilisateur en lecture seule)** : Autorisé uniquement à visualiser les réglages, et non pas à effectuer des modifications.

Vous pouvez indiquer manuellement si les utilisateurs sont autorisés à se connecter depuis d'autres réseaux locaux. Si vous souhaitez bloquer les tentatives de connexion depuis les connexion extérieures, sélectionner **Only in This LAN (Sur ce réseau local uniquement)**. Dans le cas contraire, sélectionner **Allow Any (Autoriser tous)**.

- Etape 5** Cliquez sur **System (Système)** → **Administration** → **TCP/IP** pour définir les éléments Host Name (Nom d'hôte), IP address(Adresse IP), Subnet Mask (Masque de sous-réseau) et Gateway IP (IP de la passerelle) pour le SNMP IPv6.
- Etape 6** Cliquez sur **Time Server (Serveur de temps)** pour définir manuellement l'heure et à la date pour le système ou autoriser la synchronisation automatique de l'heure entre le SNMP IPv6 et les serveurs de temps.

**NOTE**

Pour configurer intégralement votre SNMP IPv6, veuillez vous reporter au **chapitre 5 : InsightPower SNMP IPv6 pour PDU Web**.

## 4-2 Configuration avec EzSetting

Inclus dans le CD fourni, le programme EzSetting (compatible avec Windows 2000/2003/2008/XP/Vista/7) vous permet de configurer facilement votre SNMP IPv6 et de mettre à niveau le microprogramme sur vos périphériques SNMP. Suivez les instructions ci-dessous :

- Etape 1** Utilisez un câble CAT5 pour connecter le port réseau du SNMP IPv6 au réseau.
- Etape 2** Assurez-vous que les deux commutateurs DIP du SNMP IPv6 sont placés en position d'**arrêt** (Mode Normal) afin de permettre la communication réseau. Assurez-vous que le poste de travail et le SNMP IPv6 sont sur le même réseau local.
- Etape 3** Insérer le CD fourni dans le lecteur de CD-ROM. Depuis le répertoire racine, lancez EzSetting.
- Etape 4** Cliquez sur **Discover (Détection)** pour rechercher tous les périphériques SNMP disponibles sur le réseau local. Une liste des périphériques apparaîtra.



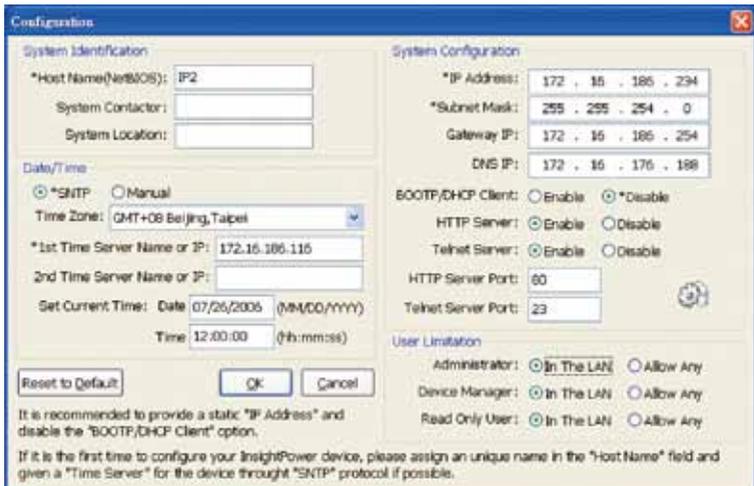
### NOTE

1. Pour rechercher des périphériques SNMP dans un autre domaine, modifiez les éléments **Subnet (Sous-réseau)** et **IPv4/ IPv6 Prefix Length (Longueur de préfixe IPv4/IPv6)** puis cliquez sur **Discover (Détection)**.
2. Si le SNMP IPv6 n'a pas été trouvé, vérifiez le port UDP 3456 sur le poste de travail que vous utilisez. Assurez-vous que celui-ci est ouvert.

**Etape 5** Sélectionnez le SNMP IPv6 que vous souhaitez modifier dans la liste des périphériques. Cliquez sur **Modify (Modifier)** et entrez le compte et le mot de passe administrateur (par défaut : admin/password, sensibles à la casse).



**Etape 6** Cliquez sur **Configuration** pour configurer les réglages réseau.



**NOTE**

Veillez vous reporter au **chapitre 5 : InsightPower SNMP IPv6 pour PDU Web** pour les configurations complètes.

## 4-3 Configuration via Telnet

- Etape 1** Utilisez un câble réseau CAT5 pour connecter le port réseau du SNMP IPv6 au réseau.
- Etape 2** Connectez le poste de travail (Windows ou Linux) au réseau local auquel le SNMP IPv6 est connecté.
- Etape 3** Pour Windows, lancez l'invite de commande DOS (**Start [Démarrer] → Run [Exécuter]** → n'importe quelle touche en **mode invite de commandes** et appuyez sur **Entrée**). Pour Linux, lancez Shell.
- Etape 4** Entrez la commande suivante : **telnet InsightPower** ou **telnet IP address** pour démarrer la connexion telnet avec le SNMP IPv6.
- Etape 5** Une fois la connexion établie, entrez le compte et le mot de passe administrateur (par défaut : admin/password, sensibles à la casse). Le menu principal apparaîtra à l'écran. Veuillez vous reporter à la section **4-5 Configuration par Mode Texte** pour plus d'informations.

### NOTE



1. Le SNMP IPv6 met fin aux connexions inactives au bout de 60 secondes.
2. Veuillez vous reporter au **chapitre 5 : InsightPower SNMP IPv6 pour PDU Web** pour les configurations complètes.

## 4-4 Configuration via le port COM

En cas d'absence de connexion réseau là où vous vous situez, vous pouvez configurer le SNMP IPv6 via la connexion du port COM. Veuillez suivre les instructions ci-dessous :

### NOTE



Si vous exécutez un système différent de Windows, reportez-vous au manuel d'utilisation de votre système pour les clients Telnet.

- Etape 1** Utilisez le câble RJ45 vers DB9 fourni pour connecter le port COM du SNMP IPv6 au port COM des postes de travail.
- Etape 2** Assurez-vous que les deux commutateurs DIP du SNMP IPv6 sont placés en position d'**arrêt** (Mode Normal).

**Etape 3** Pour Windows 2000, 2003, 2008 et XP, appuyez sur **Start (Démarrer)** → **Programs (Programmes)** → **Accessories (Accessoires)** → **Communications** et sélectionnez **HyperTerminal**.



Microsoft a retiré HyperTerminal de Windows Vista et versions ultérieures. Si le programme n'est pas présent sur votre système d'exploitation, vous pouvez télécharger une alternative gratuite de client Telnet/SSH PuTTY à l'adresse <http://www.putty.org>.

**Etape 4** Entrez un nom, choisissez une icône pour la connexion et cliquez sur **OK**. Dans le menu déroulant **Connect using (Connexion en utilisant)**, sélectionnez le port COM connecté au SNMP IPv6.



**Etape 5** Cliquez sur **Configure (Configurer)** et définissez les paramètres du port COM comme suit :



**Etape 6** Cliquez sur **OK** pour continuer. Définissez les deux commutateurs DIP du SNMP IPv6 en position de **marche** (Mode Configuration), et HyperTerminal se connectera automatiquement au SNMP IPv6. Dans le cas contraire, cliquez sur l'icône du téléphone dans la barre d'outils. Une fois la connexion établie, connectez-vous avec le compte et le mot de passe administrateur (par défaut : admin/password, sensibles à la casse). Une fois connecté, le menu principal apparaît à l'écran. Veuillez vous reporter à la section **4-5 Configuration par Mode Texte** pour plus d'informations.

## 4-5 Configuration par mode Texte

Vous pouvez configurer le SNMP IPv6 par mode texte en utilisant des clients Telnet/SSH tels que HyperTerminal et PuTTY. Dans cette section, vous pouvez trouver des descriptions et des réglages par défaut.

### ● Main Menu (Menu principal)

```
+=====+
|Main Menu (Menu principal)|
+=====+
Carte Web version 01.00.00
Adresse MAC 00-30-ab-25-e9-1e
[1]. User Manager (Gestionnaire des utilisateurs)
[2]. TCP/IP Setting (Réglage TCP/IP)
[3]. Network Parameter (Paramètre réseau)
[4]. Time Server (Serveur de temps)
[5]. Soft Restart (Redémarrage en douceur)
[6]. Reset All To Default (Réinitialiser tous
    les paramètres d'usine)
[z]. Exit Without Save (Quitter sans enregistrer)
[0]. Save And Exit (Quitter et enregistrer)
-----
Veuillez indiquer votre choix =>
```

● **User Manager (Gestionnaire des utilisateurs)**

```

+=====+
|User Manager (Gestionnaire|
|  des utilisateurs)|
+=====+
RADIUS
[1]. RADIUS Auth (Auth. RADIUS) : Disable (Désactivation)
[2]. Server (Serveur) :
[3]. Secret :
[4]. Port :      1812
-----
Local Auth (Auth. locale)
  Administrator (Administrateur)
[5]. Account (Compte) :      admin
[6]. Password (Mot de passe) : *****
[7]. Limitation (Limite) :    Only in This LAN (Uniquement
                               sur ce réseau local)
  Device Manager (Gestionnaire de périphériques)
[8]. Account (Compte) :      device (dispositif)
[9]. Password (Mot de passe) : *****
[a]. Limitation (Limite) :    Only in This LAN (Uniquement
                               sur ce réseau local)
  Read Only User (Utilisateur en lecture seule)
[b]. Account (Compte) :      user (utilisateur)
[c]. Password (Mot de passe) : *****
[d]. Limitation (Limite) :    Allow Any (Autoriser tous)
[0]. Back To Previous Menu (Retour au menu précédent)

-----
Veillez indiquer votre choix =>
    
```

N°	Élément	Description	Par défaut
[1]	RADIUS Auth (Auth. RADIUS)	Indique si la connexion RADIUS est autorisée.	Disable (Désactivation)
[2]	Server (Serveur)	Nom du serveur RADIUS.	
[3]	Secret	Secret RADIUS.	
[4]	Port	Numéro du port RADIUS.	1812
[5]	Administrator Account (Compte Administrateur)	Compte/mot de passe par défaut pour l'Administrateur (sensibles à la casse).	admin
[6]	Administrator Password (Mot de passe Administrateur)		password (mot de passe)
[7]	Administrator Limitation (Limite Administrateur)	Restriction de la zone de connexion Administrateur.	Only in This LAN (Uniquement sur ce réseau local)

N°	Élément	Description	Par défaut
[8]	Device Manager Account (Compte Gestionnaire de périphériques)	Compte/mot de passe par défaut (sensibles à la casse) pour le gestionnaire de périphériques. Ce compte est autorisé uniquement pour modifier les réglages relatifs aux périphériques.	device (dispositif)
[9]	Device Manager Password (Mot de passe Gestionnaire de périphériques)		password (mot de passe)
[a]	Device Manager Limitation (Limite Gestionnaire de périphériques)	Restriction de la zone de connexion Gestionnaire de périphériques.	Only in This LAN (Uniquement sur ce réseau local)
[b]	Read Only User Account (Compte Utilisateur en lecture seule)	Compte/mot de passe par défaut (sensibles à la casse) pour le gestionnaire de périphériques. Ce compte est autorisé uniquement à visualiser les réglages, et non pas à effectuer des modifications.	user (utilisateur)
[c]	Read Only User Password (Mot de passe Utilisateur en lecture seule)		password (mot de passe)
[d]	Read Only User Limitation (Limite Utilisateur en lecture seule)	Restriction de la zone de connexion Utilisateur en lecture seule.	Allow Any (Autoriser tous)

## ● Réglage TCP/IP

```

+=====+
|      TCP/IP Setting      |
| (Réglage TCP/IP)       |
+=====+
[1]. IPv4 Address (Adresse IPv4) :      192.168.001.100
[2]. IPv4 Subnet Mask
     (Masque de sous-réseau IPv4) :    255.255.255.000
[3]. IPv4 Gateway IP
     (IP de passerelle IPv4) :         192.168.001.254
[4]. IPv4 DNS or WINS IP
     (IP DNS ou WINS IPv4) :           192.168.001.001
[5]. DHCPv4 Client (Client DHCPv4) :    Activation
[6]. IPv6 Address (Adresse IPv6) :      fe80::230:abff:fe25:900
[7]. IPv6 Prefix Length
     (Longueur de préfixe IPv6) :      64
[8]. IPv6 Gateway IP
     (IP de passerelle IPv6) :         ::
[9]. IPv6 DNS IP (IP DNS IPv6) :        ::
[a]. DHCPv6 :                          Activation
[b]. Host Name (Nom d'hôte) (NetBIOS) :  INSIGHTPOWER
[c]. System Contact (Contact système) :
[d]. System Location (Emplacement système) :
[e]. Auto-Negotiation (Auto-Négociation) : Activation
[f]. Speed (Vitesse) :                  100 M
[g]. Duplex :                           Entier
[h]. Status Stable (Etat stable) :      3
[i]. Telnet Idle Time
     (Durée d'inactivité Telnet) :     60 secondes
[0]. Back To Previous Menu (Retour au menu précédent)

Veuillez indiquer votre choix =>

```

N°	Élément	Description	Par défaut
[1]	IPv4 Address (Adresse IPv4)	Adresse IPv4.	192.168.001.100
[2]	IPv4 Subnet Mask (Masque de sous-réseau IPv4)	Réglage du masque de sous-réseau IPv4.	255.255.255.000
[3]	IPv4 Gateway IP (IP de passerelle IPv4)	Adresse IP de la passerelle IPv4.	192.168.001.254
[4]	IPv4 DNS or WINS IP (IP DNS ou WINS IPv4)	IP Serveur de nom de domaine ou WINS IPv4.	192.168.001.001
[5]	DHCPv4 Client (Client DHCPv4)	Activation/désactivation du protocole DHCPv4.	Activation
[6]	IPv6 Address (Adresse IPv6)	Adresse IPv6.	
[7]	IPv6 Prefix Length (Longueur de préfixe IPv6)	Longueur de préfixe IPv6.	
[8]	IPv6 Gateway IP (IP de passerelle IPv6)	Adresse IP de la passerelle IPv6.	
[9]	IPv6 DNS IP (IP DNS IPv6)	Adresse IP du serveur de nom de domaine IPv6.	
[a]	DHCPv6	Activation/désactivation du protocole DHCPv6.	Activation
[b]	Host Name (Nom d'hôte) (NetBIOS)	Nom d'hôte pour le SNMP IPv6.	INSIGHTPOWER
[c]	System Contact (Contact système)	Informations de contact du système.	
[d]	System Location (Emplacement système)	Informations d'emplacement du système.	
[e]	Auto-Negotiation (Auto-Négociation)	Activation/désactivation de la négociation automatique du taux de transfert (10/100 Mbps).	Activation
[f]	Speed (Vitesse)	Si l'Auto-Négociation est désactivée, vous pouvez indiquer le taux de transfert.	100 M

N°	Élément	Description	Par défaut
[g]	Duplex	Si l'Auto-Négociation est désactivée, vous pouvez indiquer le mode duplex.	Entier
[h]	Status Stable (Etat stable) :	Heure de contrôle de la confirmation de changement d'état.	3
[i]	Telnet Idle Time (Durée d'inactivité Telnet)	Réglage du délai d'attente de connexion Telnet	60 secondes

## ● Network Parameter (Paramètre réseau)

```

+-----+
| Network Parameter |
| (Paramètre réseau) |
+-----+
[1]. HTTP Server (Serveur HTTP) :      Activation
[2]. HTTPS Server (Serveur HTTPS) :    Activation
[3]. Telnet Server (Serveur Telnet) :   Activation
[4]. SSH/SFTP Server
    (Serveur SSH/SFTP) :                Activation
[5]. FTP Server (Serveur FTP) :         Disable (Désactivation)
[6]. Syslog :                           Disable (Désactivation)
[7]. HTTP Port Server
    (Port serveur HTTP) :               80
[8]. HTTPS Server Port
    (Port serveur HTTPS) :              443
[9]. Telnet Server Port
    (Port serveur Telnet) :             23
[a]. SSH Server Port (Port serveur SSH) : 22
[b]. FTP Server Port (Port serveur FTP) : 21
[c]. Syslog Server1 (Serveur Syslog 1) :
[d]. Syslog Server2 (Serveur Syslog 2) :
[e]. Syslog Server3 (Serveur Syslog 3) :
[f]. Syslog Server4 (Serveur Syslog 4) :
[g]. SNMP Get (Obtenir SNMP),
    Set Port (Définir Port) :          161
[0]. Back To Previous Menu (Retour au menu précédent)

Veuillez indiquer votre choix =>

```

N°	Élément	Description	Par défaut
[1]	HTTP Server (Serveur HTTP)	Activation/désactivation du protocole HTTP.	Activation
[2]	HTTPS Server (Serveur HTTPS)	Activation/désactivation du protocole HTTPS.	Activation
[3]	Telnet Server (Serveur Telnet)	Activation/désactivation du protocole Telnet.	Activation
[4]	SSH/SFTP Server (Serveur SSH/SFTP)	Activation/désactivation du protocole SSH/SFTP.	Activation
[5]	FTP Server (Serveur FTP)	Activation/désactivation du protocole FTP.	Disable (Désactivation)
[6]	Syslog	Activation/désactivation du serveur Syslog distant.	Disable (Désactivation)

N°	Élément	Description	Par défaut
[7]	HTTP Server Port (Port serveur HTTP)	Port HTTP.	80
[8]	HTTPS Server Port (Port serveur HTTPS)	Port HTTPS.	443
[9]	Telnet Server Port (Port serveur Telnet)	Port Telnet.	23
[a]	SSH Server Port (Port serveur SSH)	Port SSH.	22
[b]	FTP Server Port (Port serveur FTP)	Port FTP.	21
[c]	Syslog Server 1 (Serveur Syslog 1)	Nom d'hôte du serveur Syslog distant Serveur 1	
[d]	Syslog Server 2 (Serveur Syslog 2)	Nom d'hôte du serveur Syslog distant Serveur 2	
[e]	Syslog Server 3 (Serveur Syslog 3)	Nom d'hôte du serveur Syslog distant Serveur 3	
[f]	Syslog Server 4 (Serveur Syslog 4)	Nom d'hôte du serveur Syslog distant Serveur 4	
[g]	SNMP Get, Set Port (Obtenir SNMP, Définir Port)	Port SNMP.	161

### Time Server (Serveur de temps)

Vous pouvez régler manuellement l'heure et la date pour le SNMP IPv6 ou configurer la synchronisation automatique du serveur de temps. Le SNMP IPv6, Windows XP et versions ultérieures prennent en charge le SNTP (Simple Network Time Protocol). Si vous devez démarrer un entretien du serveur de temps sur votre poste de travail, veuillez vous reporter au **chapitre 7 : Dépannage Q1**.

```

+-----+
|           |
|   Time Server   |
| (Serveur de temps) |
+-----+
[1]. Time Selection
   (Sélection de l'heure) :      SNTP
[2]. Time Zone (Fuseau horaire) : +0h
[3]. 1st Time Server
   (1er serveur de temps) :     POOL.NTP.ORG
[4]. 2nd Time Server
   (2e serveur de temps) :
[5]. Manual Date (Date manuelle) : 01/01/2000 (MM/JJ/AAAA)
[6]. Manual Time (Heure manuelle) : 00:00:00 (hh:mm:ss)
[0]. Back To Previous Menu (Retour au menu précédent)
+-----+
Veuillez indiquer votre choix =>

```

N°	Élément	Description	Par défaut
[1]	Time Selection (Sélection de l'heure)	SNTP ou manuelle.	SNTP
[2]	Time Zone (Fuseau horaire)	Permet de définir votre fuseau horaire.	+0 h
[3]	1 <sup>st</sup> Time Server (1 <sup>er</sup> serveur de temps)	Premier serveur de temps pour SNTP.	POOL.NTP.ORG
[4]	2 <sup>nd</sup> Time Servr (2 <sup>e</sup> serveur de temps)	Deuxième serveur de temps pour SNTP.	
[5]	Manual Date (Date manuelle)	Permet de régler la date manuellement.	01/01/2000
[6]	Manual Time (Heure manuelle)	Permet de régler l'heure manuellement.	00:00:00

● **Soft Restart (Redémarrage en douceur)**

Permet de réinitialiser le SNMP IPv6. Cela n'affectera pas le fonctionnement du PDU.

● **Default Reset (Réinitialisation par défaut)**

Permet de réinitialiser aux paramètres d'usine par défaut.

● **Exit Without Saving (Quitter sans enregistrer)**

Permet de quitter en ignorant les modifications.

● **Save and Exit (Enregistrer et quitter)**

Permet de conserver vos modifications et quitter.

## Chapitre 5 : InsightPower SNMP IPv6 pour PDU Web.

Pour configurer le SNMP IPv6 via l'InsightPower SNMP IPv6 pour PDU Web, veuillez suivre les étapes ci-dessous :

- Etape 1** Assurez-vous que votre SNMP IPv6 est connecté au réseau local. Utilisez un câble réseau CAT5 pour connecter le port réseau du SNMP IPv6 au réseau.
- Etape 2** Lancez votre navigateur Web. Dans la barre d'adresse, entrez le nom d'hôte du SNMP IPv6 **http://InsightPower/** ou **l'adresse IP**. Pour une connexion cryptée, entrez **https://InsightPower/** ou **https://192.168.1.100/**.
- Etape 3** Une fois la connexion établie, la page de connexion apparaît. Entrez votre compte et votre mot de passé (par défaut : admin/password).



### NOTE

1. Si vous avez précédemment modifié le nom d'hôte ou l'adresse IP du SNMP IPv6, connectez-vous avec les nouveaux réglages.
2. Si la page de connexion est accessible, mais si vous ne pouvez pas vous connecter avec le compte et le mot de passe corrects, il se peut qu'une configuration réseau supplémentaire soit nécessaire. Cela peut être dû au fait que le sous-réseau IP de l'ordinateur sur lequel vous vous connectez est différent de celui du SNMP IPv6. Pour résoudre ce problème, veuillez vous reporter au **chapitre 7 : Dépannage Q3**.
3. Le SNMP IPv6 met fin automatiquement aux connexions inactives au bout de 30 minutes.

L'InsightPower SNMP IPv6 pour PDU Web inclut les fonctions Monitor (Moniteur), Device (Dispositif) et System (Système). Ces trois éléments vous permettent de contrôler et de configurer vos PDU. Pour plus d'informations, veuillez vous reporter aux sections **5-1 à 5-3** suivantes.

## **5-1 Monitor (Moniteur)**

Dans la catégorie Monitor (Moniteur), se trouvent quatre éléments : Information (Informations), History (Historique), Environment (Environnement) et About (A propos). Vous pouvez contrôler vos PDU via cette page Monitor (Moniteur).

### **5-1-1 Information (Informations)**

La page Information (Informations) inclut les éléments Status (Etat) et Detail (Informations détaillées). Veuillez noter que les informations diffèrent selon le modèle de PDU ; par conséquent, le contenu figurant sur votre page Web peut varier de celui illustré dans le présent manuel d'utilisation.

#### **● Status (Etat)**

Accédez à **Monitor (Moniteur) → Information (Informations) → Status (Etat)** pour visualiser l'état de votre PDU. La page présente chaque PDU et les informations relatives au branchement, à la charge, à la tension et à la fréquence. Les valeurs seront mises à jour automatiquement. Vous pouvez cliquer sur le bouton en haut à droite, intitulé **Event Log (Journal des événements)** pour suivre les événements rencontrés par votre PDU. Pour plus d'informations sur le journal des événements, veuillez vous reporter à la section **5-1-2 Historique - Journal des événements**.



● **Detail (Informations détaillées)**

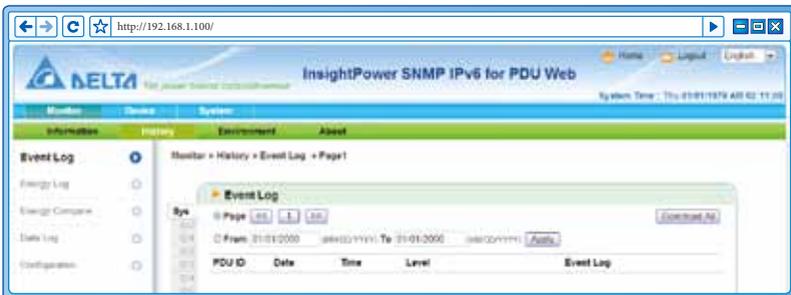
Accédez à **Monitor (Moniteur)** → **Information (Informations)** → **Detail (Informations détaillées)** pour visualiser un numéro d'identification de PDU spécifique, un numéro de modèle, un numéro de série, la version du matériel, la version logicielle, ainsi que des valeurs pertinentes, telles que la charge, la fréquence, les watts et kWh, etc. Vous pouvez également cliquer sur les boutons **Data Log (Journal des données)** et **Energy Log (Journal énergie)** (si votre page Web indique les deux boutons) pour visualiser plus de valeurs pertinentes. Pour plus d'informations sur le journal des données et le journal énergie, veuillez vous reporter aux sections **5-1-2 Historique - Journal des événements** et **5-1-2 Historique - Journal énergie**.



**5-1-2 History (Historique)**

La page History (Historique) contient les cinq éléments suivants : Event Log (Journal des événements), Energy Log (Journal énergie), Energy Compare (Comparaison énergétique), Data Log (Journal des données) et Configuration. Voir ci-dessous pour plus de descriptions.

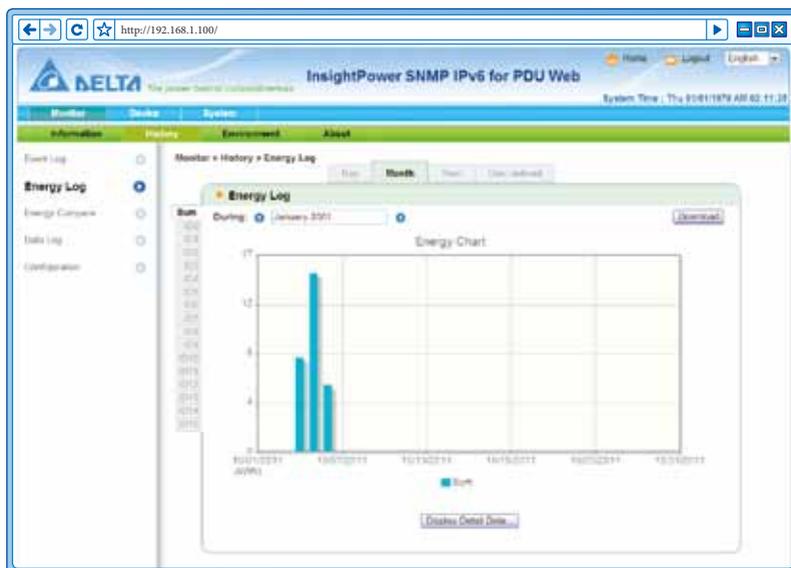
● **Event Log (Journal des événements)**



Accédez à **Monitor (Moniteur)** → **History (Historique)** → **Event Log (Journal des événements)** pour visualiser les événements sélectionnés du PDU. Les événements existants sont écrasés lorsque le nombre maximal d'entrées (1 000) est atteint. Vous pouvez télécharger l'archive complète du journal des événements au cours d'une période définie sur votre ordinateur.

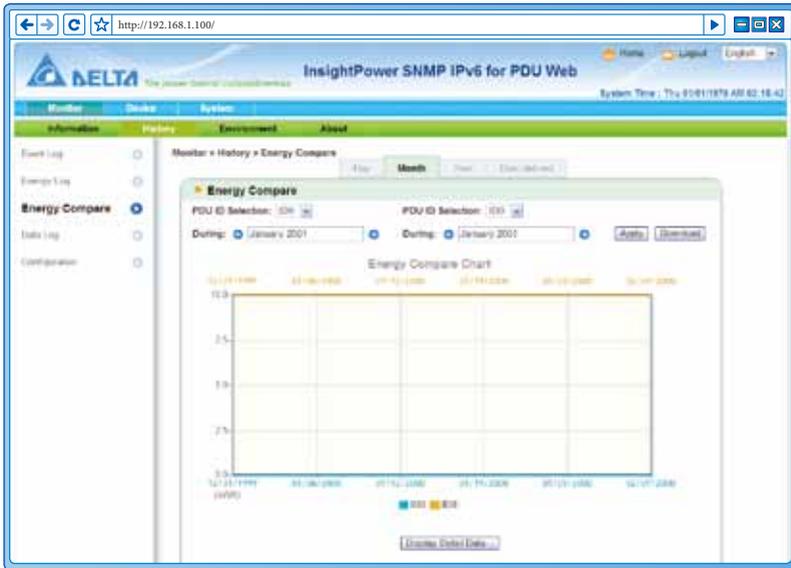
- **PDU ID (Identifiant PDU)** : Numéro d'identification du PDU.
- **Date** : Date à laquelle l'événement s'est produit.
- **Time (Heure)** : Heure à laquelle l'événement s'est produit.
- **Level (Niveau)** : Niveau de l'événement qui s'est produit.
- **Event Log (Journal des événements)** : Description de l'événement qui s'est produit.
- **Download All (Télécharger tous)** : Le SNMP IPv6 envoie une demande à toutes les PDU, collecte les journaux des événements enregistrés dans les PDU et répond à l'utilisateur via le réseau. Veuillez noter que cette option apparaît uniquement lorsque les PDU prennent en charge cette fonction. D'autre part, les journaux des événements enregistrés dans les PDU peuvent différer des journaux des événements enregistrés dans le SNMP IPv6.

## ● Energy Log (Journal énergie)



Accédez à **Monitor (Moniteur)** → **History (Historique)** → **Energy Log (Journal énergie)** pour visualiser le journal énergie du PDU. Vous pouvez définir un créneau horaire spécifique, cliquer sur le bouton **Display Detail Data (Afficher les données détaillées)** pour visualiser les enregistrements détaillés et cliquer sur le bouton **Download (Télécharger)** pour télécharger le journal énergie. Les enregistrements existants sont écrasés lorsque le nombre maximal d'entrées (8 000) est atteint.

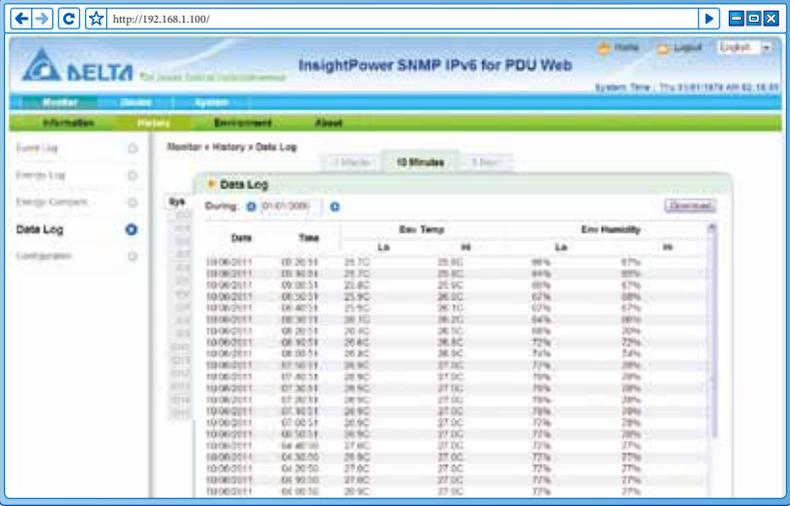
### ● **Energy Compare (Comparaison énergétique)**



Accédez à **Monitor (Moniteur)** → **History (Historique)** → **Energy Compare (Comparaison énergétique)** pour visualiser le tableau de comparaison énergétique de deux PDU sélectionnées. Sélectionnez deux numéros d'identification de PDU, sélectionnez un créneau horaire spécifique, cliquez sur le bouton **Apply (Appliquer)**, un tableau de comparaison énergétique apparaît alors. Vous pouvez cliquer sur le bouton **Display Detail Data (Afficher les données détaillées)** pour visualiser les enregistrements de comparaison détaillés et cliquer sur le bouton **Download (Télécharger)** pour télécharger les journaux de comparaison. Les enregistrements existants sont écrasés lorsque le nombre maximal d'entrées (8 000) est atteint.

## ● Data Log (Journal des données)

Accédez à **Monitor (Moniteur)** → **History (Historique)** → **Data Log (Journal des données)** pour visualiser un journal de données de PDU enregistré dans un créneau horaire spécifique. Le journal des données comprend des informations sur la fréquence de sortie totale, la puissance de sortie totale, la tension de sortie, l'intensité de sortie et la puissance de sortie de chaque branchement du PDU sélectionné. Sélectionnez un numéro d'identification de PDU, puis un créneau horaire spécifique, le journal des données apparaît alors. Vous pouvez cliquer sur le bouton **Download (Télécharger)** pour télécharger le journal des données. Les enregistrements existants sont écrasés lorsque le nombre maximal d'entrées (8 000) est atteint.



Date	Time	Out Temp		Out Humidity	
		La	Rs	La	Rs
10/06/2011	00:20:51	25.1C	25.5C	66%	67%
10/06/2011	00:46:51	25.1C	25.5C	64%	65%
10/06/2011	00:00:51	25.6C	25.6C	66%	67%
10/06/2011	00:30:51	25.5C	26.0C	67%	68%
10/06/2011	00:40:51	25.5C	26.1C	67%	67%
10/06/2011	00:38:51	26.1C	26.2C	64%	65%
10/06/2011	00:20:51	26.1C	26.1C	66%	66%
10/06/2011	00:16:51	26.1C	26.1C	70%	72%
10/06/2011	00:00:51	26.1C	26.1C	74%	74%
10/06/2011	07:16:51	26.1C	27.0C	77%	78%
10/06/2011	07:46:51	26.1C	27.0C	76%	76%
10/06/2011	07:36:51	26.1C	27.0C	76%	76%
10/06/2011	07:26:51	26.1C	27.0C	76%	76%
10/06/2011	07:30:51	26.1C	27.0C	76%	76%
10/06/2011	07:00:51	26.1C	27.0C	73%	73%
10/06/2011	06:50:51	26.1C	27.0C	73%	73%
10/06/2011	04:46:50	27.6C	27.0C	77%	77%
10/06/2011	04:36:50	28.1C	27.0C	77%	77%
10/06/2011	04:30:50	27.6C	27.0C	77%	77%
10/06/2011	04:30:50	27.6C	27.0C	77%	77%
10/06/2011	04:00:50	26.1C	27.0C	77%	77%

## ● Configuration

Accédez à **Monitor (Moniteur)** → **History (Historique)** → **Configuration** pour effacer le journal des événements, le journal énergie, le journal de comparaison énergétique et le journal des données. Vous pouvez également définir les éléments Save Data Interval (Intervalle de sauveg. de données) et Save Energy Interval (Intervalle de sauveg. énergie).

- **Clear History Data (Effacer données de l'historique)** : Vide le journal des données uniquement.
- **Clear Event Log (Effacer journal des événements)** : Vide le journal des événements uniquement.
- **Clear Energy Data (Effacer données énergie)** : Vide le journal énergie et le journal de comparaison énergétique.
- **Save Data Interval (Intervalle de sauveg. de données)** : L'intervalle après lequel une entrée de donnée est enregistrée.

- **Save Energy Interval (Intervalle de sauveg. énergie) :** L'intervalle après lequel une entrée énergie/comparaison énergétique est enregistrée.



### 5-1-3 Environment (Environnement)

La page Environment (Environnement) apparaît uniquement si un EnviroProbe est utilisé. Veuillez noter que le commutateur DIP 1 du SNMP IPv6 devrait être en position de **marche** et le commutateur DIP 2 devrait être en position d'**arrêt** lorsque vous utilisez un EnviroProbe.

La page Environment (Environnement) inclut les éléments Information (Informations) et Configuration. Vous pouvez contrôler et configurer votre EnviroProbe via cette page Environment (Environnement). Pour obtenir des informations sur l'EnviroProbe, veuillez vous reporter au Guide d'installation inclus dans l'emballage de l'EnviroProbe.

#### Information (Informations)

Accédez à **Monitor (Moniteur) → Environment (Environnement) → Information (Informations)** pour visualiser les informations relatives à votre capteur EnviroProbe, les contacts d'entrée et le paramétrage des contacts.



## ● Configuration

Accédez à **Monitor (Moniteur)** → **Environment (Environnement)** → **Configuration** pour configurer le seuil d'avertissement, le seuil d'alarme, le titre et le type de votre EnviroProbe. Reportez-vous au tableau ci-après pour plus d'informations.

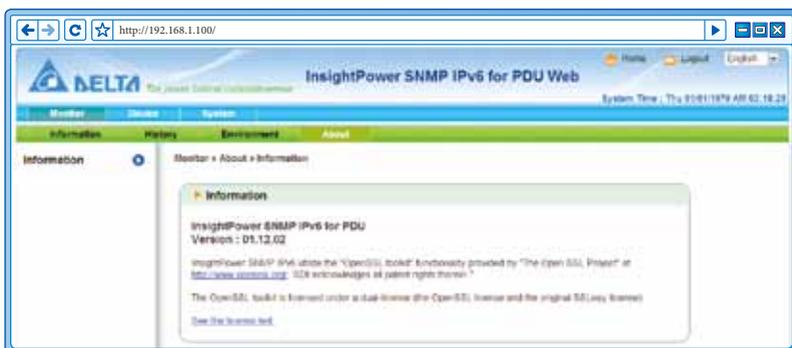


## 5-1-4 About (A propos)

Un seul élément, intitulé Information (Informations) figure dans la catégorie About (A propos). Par ce moyen, vous pouvez obtenir d'autres informations sur le SNMP IPv6.

## ● Information (Informations)

Accédez à **Monitor (Moniteur)** → **About (A propos)** → **Information (Informations)** pour visualiser la version de votre InsightPower SNMP IPv6 pour PDU et d'autres informations sur l'OpenSSL toolkit et les licences.



## 5-2 Device (Dispositif)

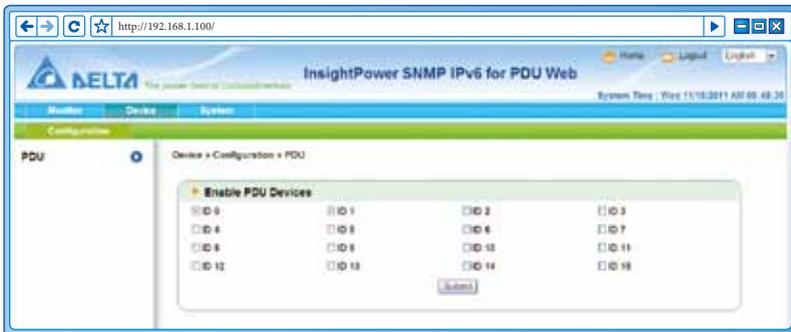
Un seul élément, intitulé Configuration figure dans la catégorie Device (Dispositif). Vous pouvez configurer la ou les PDU à soumettre au contrôle du SNMP IPv6. Voir ci-dessous pour plus de descriptions.

### 5-2-1 Configuration

La page Configuration comprend une seule sélection, **PDU**. Le réglage par défaut du NMP IPv6 permet uniquement de contrôler le PDU dont l'identifiant est défini sur 0. Pour contrôler un autre PDU ou plusieurs dispositifs de PDU, vous pouvez utiliser cette sélection pour réinitialiser le réglage par défaut.

#### ● PDU

Accédez à **Device (Dispositif)** → **Configuration** → **PDU** pour sélectionner le numéro d'identification du PDU. Après avoir cliqué sur le bouton **Submit (Envoyer)**, le SNMP IPv6 s'activera pour contrôler les dispositifs PDU sélectionnés.



## 5-3 System (Système)

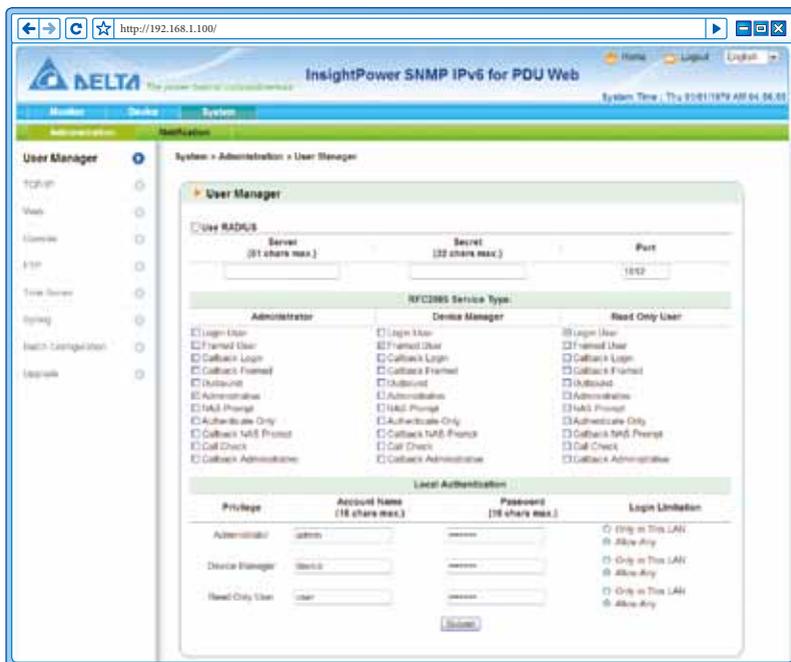
Seul l'administrateur peut visualiser la page System (Système). Dans la catégorie System (Système), se trouvent deux éléments : Administration et Notification. Vous pouvez utiliser ces éléments pour modifier ou visualiser les réglages ou enregistrements pertinents du système. Voir ci-dessous pour plus de descriptions.

### 5-3-1 Administration

La page Administration comprend les neuf sélections suivantes : User Manager (Gestionnaire des utilisateurs, TCP/IP, Web, Console, FTP, Time Server (Serveur de temps), Syslog, Batch Configuration (Configuration de lot) et Upgrade (Mise à niveau).

#### ● User Manager (Gestionnaire des utilisateurs)

Le SNMP IPv6 prend en charge RADIUS. Cochez la case **Use RADIUS (Utiliser RADIUS)**, saisissez les informations requises, notamment Server (Serveur), Secret et Port (par défaut : 1812) et cliquez sur **Submit (Envoyer)** pour activer RADIUS. Vous pouvez définir les types de service pour Administrator (Administrateur), Device Manager (Gestionnaire des périphériques) et Read Only User (Utilisateur en lecture seule). Si RADIUS est désactivé, vous pouvez toujours gérer les éléments Account Name (Nom de compte), Password (Mot de passe) et Login Limitation (Limite de connexion) pour l'authentification locale.



● **TCP/IP**

Cette section permet à l'administrateur de configurer les paramètres du réseau local pour le SNMP IPv6.



● **Réglages TCP/IP pour IPv4**

- 1) **DHCP Client (Client DHCP)** : Activation/désactivation du DHCP. Si activé, le serveur DHCP attribue automatiquement une adresse IP au SNMP IPv6.
- 2) **IP Address (Adresse IP)** : L'adresse IP est au format pointé.
- 3) **Subnet Mask (Masque de sous-réseau)** : Masque de sous-réseau pour votre réseau.
- 4) **Gateway IP (IP de passerelle)** : Adresse IP au format pointé pour la passerelle du réseau.
- 5) **DNS IP (IP du DNS)** : Adresse IP au format pointé du serveur de nom de domaine.
- 6) **Search Domain (Domaine de recherche)** : Si le nom d'hôte indiqué est introuvable, le système ajoute le domaine de recherche à votre nom d'hôte.

● **Réglages TCP/IP pour IPv6**

- 1) **DHCP Client (Client DHCP)** : Activation/désactivation du DHCP. Si activé, le serveur DHCP attribue automatiquement une adresse IP au SNMP IPv6.
- 2) **IP Address (Adresse IP)** : Adresse IPv6.

- 3) **Prefix Length (Longueur de préfixe)** : Longueur de préfixe pour l'adresse IPv6.
  - 4) **Gateway V6IP (IPv6 de passerelle)** : Adresse IP pour la passerelle de réseau IPv6.
  - 5) **DNS V6IP (IPv6 de DNS)** : Adresse IP pour le serveur de nom de domaine IPv6.
- **System (Système)**
    - 1) **Host Name (Nom d'hôte)** : Nom d'hôte du SNMP IPv6 sur le réseau.
    - 2) **System Contact (Contact système)** : Informations de contact du système.
    - 3) **System Location (Emplacement système)** : Informations d'emplacement du système.
  - **Link (Liaison)**
    - 1) **Auto-Negotiation (Auto-négociation)** : Activation/désactivation de la négociation automatique du taux de transfert (10/100 Mbps).
    - 2) **Speed (Vitesse)** : Si l'Auto-Négociation est désactivée, vous pouvez indiquer le taux de transfert.
    - 3) **Duplex** : Si l'Auto-Négociation est désactivée, vous pouvez indiquer le mode duplex.

## ● Web

Cet élément permet à l'administrateur d'activer ou de désactiver les protocoles de communication HTTP/HTTPS.



- **Web**
  - 1) **HTTP** : Activation/désactivation de la connexion HTTP.
  - 2) **HTTPS** : Activation/désactivation de la connexion HTTPS.

- 3) **HTTP Port (Port HTTP)** : Attribution d'un numéro de port HTTP (par défaut : 80).
  - 4) **HTTPS Port (Port HTTPS)** : Attribution d'un numéro de port HTTPS (par défaut : 443).
  - 5) **Web Refresh Period (Délai d'actualisation du Web)** : Intervalle d'actualisation du Web.
- **SSL Certificate (Certificat SSL)**
    - 1) Afin d'assurer une sécurité de connexion entre le SNMP IPv6 si le poste de travail connecté, le certificat SSL peut être utilisé pour crypter et sécuriser l'intégrité des données de transmission.
    - 2) **Certificate File (Fichier de certificat)** : Cet élément vous permet de remplacer votre propre fichier de certificat SSL. Le SNMP IPv6 prend en charge le format PEM généré par OpenSSL. Cliquez sur **Browse (Parcourir)** pour télécharger un fichier de certificat.



Pour plus d'informations sur la génération d'un fichier de certificat SSL privé, veuillez vous reporter au **chapitre 7 : Dépannage Q12** ou visitez le site <http://www.openssl.org/>.

### ● Console

Cet élément permet à l'administrateur d'activer ou de désactiver les protocoles de communication Telnet/SSH.

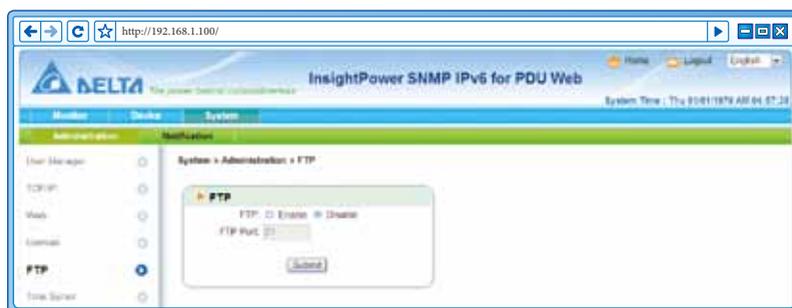


- **Telnet** : Activation/désactivation de la connexion Telnet.
- **SSH/SFTP** : Activation/désactivation de la connexion SSH/SFTP.
- **Telnet Port (Port Telnet)** : Attribution d'un numéro de port Telnet (par défaut : 23).
- **SSH Port (Port SSH)** : Attribution d'un numéro de port du protocole SSH (par défaut : 22).
- **Host Key/Authentication Public Key (Clé d'hôte/Clé publique d'authentification)** :

Cet élément vous permet de remplacer vos propres clés SSH. Le SNMP IPv6 prend en charge des fichiers de clé générés par OpenSSH, notamment les clés DSA, RSA et clés publiques d'authentification. Pour savoir comment générer les clés DSA, RSA et les clés publiques d'authentification pour SSH, veuillez vous reporter au **chapitre 7 : Dépannage Q13**. Vous pouvez utiliser cette page ou le protocole SFTP pour télécharger les fichiers de clé. Pour des informations détaillées, veuillez vous reporter au **chapitre 7 : Dépannage Q14**.

## ● FTP

Cet élément permet à l'administrateur d'activer ou de désactiver les protocoles de communication FTP.



- **FTP** : Activation/désactivation de la connexion FTP.
- **FTP Port (Port FTP)** : Attribution d'un numéro de port FTP (par défaut : 21).

## ● Time Server (Serveur de temps)

Vous pouvez régler manuellement l'heure et la date ou activer la synchronisation automatique de l'heure avec les serveurs SNTP. Veuillez noter que si le serveur SNTP ne répond pas, le journal des événements, le journal énergie, le journal de comparaison énergétique et le journal des données ne seront pas enregistrés, et ce même si le SNTP est activé.



### ● Simple Network Time Server

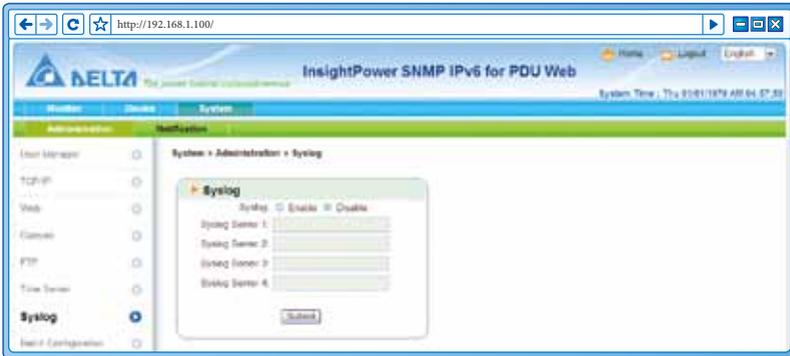
- 1) **Time Zone (Fuseau horaire)** : Dans le menu déroulant, sélectionnez le fuseau horaire de la zone où se trouve le SNMP IPv6.
- 2) **Primary/ Secondary Time Server (Serveur de temps principal/secondaire)** : Il est possible d'ajouter deux serveur de temps. Toutes les 60 minutes, le SNMP IPv6 se synchronise avec le premier serveur qui répond.
- 3) **Enable Daylight Saving (Activer l'heure d'été)** : Cochez la case pour activer l'heure d'été. Pendant cette période, le SNMP IPv6 avance d'une heure.

### ● Manual (Manuel)

Si un serveur de temps n'est pas accessible, vous pouvez toujours régler l'heure et la date manuellement. Veuillez noter qu'à chaque fois que vous redémarrez le module de réseau du SNMP IPv6, l'heure et la date sont rétablies selon les réglages précédemment définis.

## ● Syslog

Syslog est utilisé pour enregistrer le journal des événements sur des serveurs Syslog distants. Cela n'affectera pas le journal des événements local. Après avoir activé Syslog, veuillez configurer une adresse IP de serveur. Vous pouvez configurer simultanément jusqu'à quatre serveur Syslog.



## ● Batch Configuration (Configuration de lot)

Le SNMP IPv6 prévoit une fonction de configuration de lot afin de permettre un paramétrage rapide et simple sur plusieurs dispositifs SNMP IPv6. Vous pouvez dupliquer les réglages en exportant les fichiers de configuration à partir du SNMP IPv6 précédemment configuré avec succès, et en important les fichiers de configuration sur d'autres dispositifs.



- **System Configuration (Configuration système)**

L'élément **System Configuration (Configuration système)** comprend des réglages enregistrés dans les onglets **Device (Dispositif)** et **System (Système)**. Pour télécharger un fichier de configuration, il suffit de cliquer sur **Download (Télécharger)**. Pour télécharger un fichier de configuration, cliquez sur **Browse (Parcourir)**, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur **Upload (Télécharger)**.

**NOTE** 

Si l'adresse IP est statique et si vous souhaitez copier les réglages vers d'autres dispositifs sur le même réseau local, vous devez supprimer manuellement la ligne suivante **IP=xxx.xxx.xxx.xxx** à la section [System] du fichier de configuration exporté. Vous pouvez ouvrir le fichier de configuration avec un éditeur de texte tel que Notepad ou WordPad. Pour modifier/attribuer une adresse IP au SNMP IPv6, consultez le **chapitre 4 : Configurations système**.

- **SNMP Configuration (Configuration SNMP)**

L'élément **SNMP Configuration (Configuration SNMP)** comprend des réglages enregistrés dans l'onglet **Notification**. Pour télécharger un fichier de configuration, il suffit de cliquer sur **Download (Télécharger)**. Pour télécharger un fichier de configuration, cliquez sur **Browse (Parcourir)**, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur **Upload (Télécharger)**.

**NOTE** 

Si vous avez besoin de modifier les lignes de commande, veillez à ne pas supprimer les lignes inchangées. Elles doivent rester telles quelles afin de garantir l'intégrité du fichier de configuration.

## ● Upgrade (Mise à niveau)

La page Upgrade (Mise à niveau) présente la version actuelle du microprogramme du SNMP IPv6. L'administrateur peut utiliser cette page pour mettre à niveau le microprogramme du SNMP IPv6. Cliquez sur **Browse (Parcourir)**, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur **Upload (Télécharger)**. Le processus de mise à niveau prend environ une minute.



### 5-3-2 Notification

La page Notification comprend les quatre éléments suivants : SNMP Access (Accès SNMP), SNMPv3 USM (Gestion des sessions utilisateur SNMPv3), SNMP Trap (Alerte SNMP) et Mail Server (Serveur de messagerie).

#### ● SNMP Access (Accès SNMP)



Le SNMP IPv6 prend en charge le protocole SNMP IPv6 et le SNMP NMS (Network Management System), communément utilisés pour contrôler les périphériques de réseau lors de situations nécessitant une attention administrative. Afin d'empêcher tout accès non autorisé, vous pouvez indiquer les adresses IP du NMS autorisés, leurs chaînes de communauté respectives et les niveaux d'accès. Vous pouvez saisir jusqu'à 256 adresses IP.



Si l'adresse IP **0.0.0.0** figure dans la liste, la restriction d'accès IP NMS est ignorée. Le SNMP IPv6 contrôle la chaîne de communauté afin d'identifier le niveau d'accès et l'autorisation selon vos réglages.

## ● SNMPv3 USM (Gestion des sessions utilisateur SNMPv3)

Le SNMPv3 présente des fonctions telles que le cryptage de paquets et l'authentification afin d'accroître la sécurité. Le SNMPv3 USM (User Session Management, Gestion des sessions utilisateur) vous permet d'attribuer huit noms d'utilisateur dont les droits d'accès sont accordés via le protocole SNMPv3. Vous pouvez également définir les éléments suivants : Security Levels (Niveaux de sécurité), Auth Passwords (Mots de passe d'authentification, Priv Passwords (Mots de passe privés) et Access Levels (Niveaux d'accès).

The screenshot shows the 'SNMPv3 USM' configuration page in the InsightPower SNMP IPv6 for PDU Web interface. The page is titled 'System > Notification > SNMPv3 USM'. It features a table with 8 rows for configuring users. The columns are: User Name (30 bytes max), Security Level, Auth Password (20 8 bytes), Priv Password (20 8 bytes), and Access Level. The first row is pre-filled with 'admin', 'Auth Priv', '11111111', '00000000', and 'Read/Write'. A 'Submit' button is located at the bottom of the table.

User Name (30 bytes max)	Security Level	Auth Password (20 8 bytes)	Priv Password (20 8 bytes)	Access Level
admin	Auth Priv	11111111	00000000	Read/Write
	Auth NoPriv			Disable
	Auth NoPriv			Disable
	Auth NoPriv			Disable
	Auth NoPriv			Disable
	Auth NoPriv			Disable
	Auth NoPriv			Disable
	Auth NoPriv			Disable

## ● SNMP Trap (Alerte SNMP)

L'alerte SNMP prévient les utilisateurs de l'apparition d'événements dans l'environnement contrôlé. Pour activer les alertes SNMP, vous devez ajouter les adresses IP cibles à la liste des IP cibles. Renseignez les éléments suivants : Community String (Chaîne de communauté), Trap Type (Type d'alerte), MIB (Base d'information de gestion), SNMPv3 User Name (Nom d'utilisateur du SNMPv3), UDP port (Port UDP) et Event Level (Niveau d'événement), puis cliquez sur **Add (Ajouter)**. Si vous souhaitez mettre à jour ou supprimer une adresse IP cible, indiquez l'adresse IP dans la liste des IP cibles, puis cliquez sur **Update (Mettre à jour)** ou **Delete (Supprimer)**.



### NOTE

Le SNMP IPv6 prend en charge les alertes SNMPv1, SNMPv2c et SNMPv3 afin de satisfaire la plupart des environnements des clients. Si vous sélectionnez l'alerte SNMPv3, veuillez indiquer un nom d'utilisateur du SNMPv3 USM.

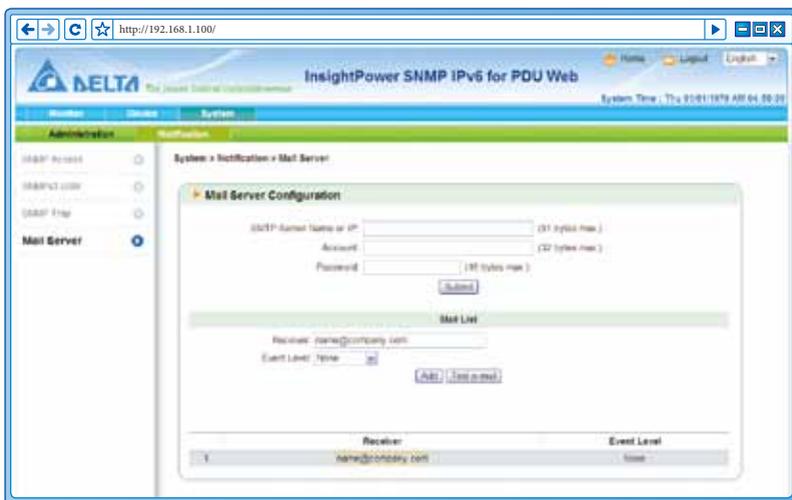
Vous pouvez utiliser Event Level (Niveau d'événement) pour définir les notifications d'événements à envoyer aux adresses IP cibles. Trois niveaux d'événements sont indiqués comme suit :

- **Information** : Toutes les notifications d'événement sont envoyées à l'adresse cible.
- **Warning (Avertissement)** : Les notifications d'avertissement et d'alarme sont envoyées à l'adresse cible.
- **Alarm (Alarme)** : Seules les notifications d'alarme sont envoyées à l'adresse cible.

Vous pouvez accéder à **System (Système)** → **Notification** → **SNMP Trap (Alerte SNMP)** → **Event Level (Niveau d'événement)** pour modifier le niveau d'événement.

## ● Mail Server (Serveur de messagerie)

Vous pouvez configurer un serveur SMTP et indiquer une liste de destinataires de messagerie qui recevront des notifications à l'apparition d'événements. Vous pouvez saisir jusqu'à 256 destinataires.



### NOTE

Si un serveur DNS est indisponible dans le réseau, vous devez attribuer manuellement une adresse de serveur SMTP pour activer le système de notification par messagerie.

#### ● SMTP Server Name or IP (Nom de serveur ou IP du SMTP)

Si un nom d'hôte est renseigné, l'élément **DNS IP (IP de DNS)** doit être complété dans **TCP/IP**. Veuillez vous reporter à la section **5-3-1 Administration - TCP/IP**.

#### ● Account (Compte)

Compte de connexion du serveur de messagerie.

#### ● Password (Mot de passe)

Mot de passe de connexion du serveur de messagerie.

- **Receiver (Destinataire)**

Adresses e-mail des destinataires.

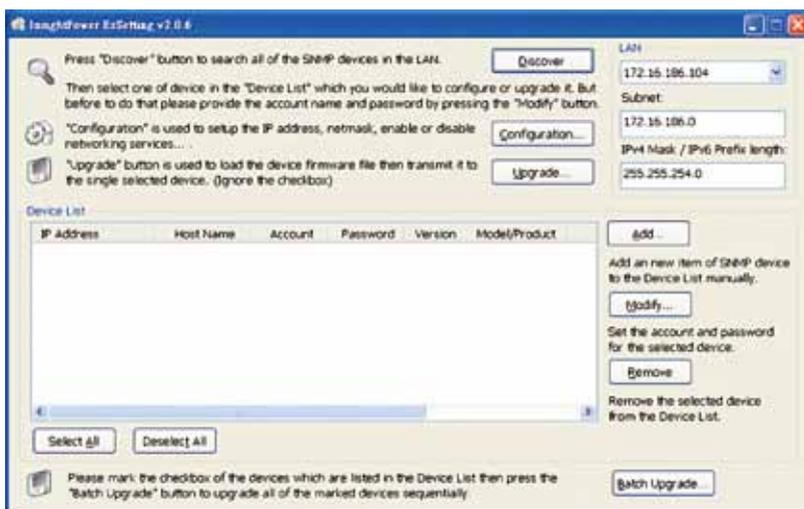
- **Event Level (Niveau d'événement)**

Sélectionnez le niveau d'événement pour lequel, lorsqu'il apparaît, une notification par e-mail est envoyée au destinataire correspondant.

- 1) **Information** : Toutes les notifications d'événement sont envoyées à l'adresse cible.
- 2) **Warning (Avertissement)** : Les notifications d'avertissement et d'alarme sont envoyées à l'adresse cible.
- 3) **Alarm (Alarme)** : Seules les notifications d'alarme sont envoyées à l'adresse cible.

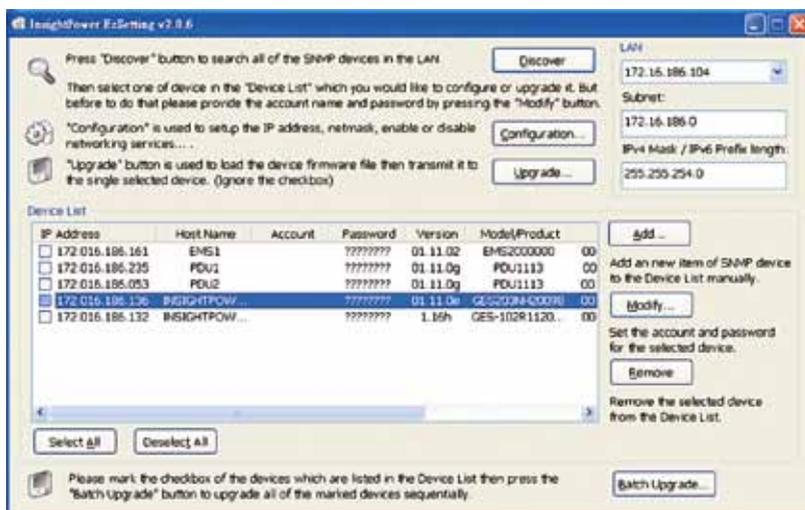
## Chapitre 6 : Mise à niveau du microprogramme du dispositif SNMP

Avec le programme EzSetting fourni, vous pouvez réaliser en toute simplicité une mise à niveau du microprogramme sur vos périphériques SNMP par réseau local. Veuillez vous reporter aux instructions suivantes.



**Etape 1** Le masque de sous-réseau vous permet de définir la plage de détection du dispositif dans les sous-réseaux spécifiés. Assurez-vous que le dispositif SNMP que vous souhaitez mettre à niveau figure dans le sous-réseau indiqué. Dans le cas contraire, modifiez le sous-réseau et le masque de sous-réseau.

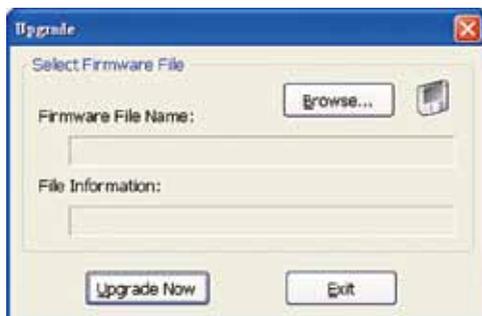
**Etape 2** Cliquez sur **Discover (Détection)**. Une liste des dispositifs SNMP apparaîtra.



**Etape 3** Sélectionnez un dispositif dans la liste des périphériques, cliquez sur **Modify (modifier)** et renseignez le compte et le mot de passe administrateur.



**Etape 4** Cliquez sur **Upgrade (Mise à niveau)**. La boîte de dialogue de mise à niveau apparaît. Cliquez sur **Browse (Parcourir)** pour sélectionner un fichier binaire de microprogramme valable. Vérifiez la version du microprogramme indiquée dans File Information (Informations fichier), puis cliquez sur **Upgrade Now (Mettre à niveau maintenant)** pour continuer.



**Etape 5** Le processus de mise à niveau prend environ 20 secondes.



**Etape 6** Une fois la mise à niveau effectuée, la boîte de dialogue suivante apparaît. Le dispositif prend environ 1 minute pour redémarrer.



## Chapitre 7 : Dépannage

### Q1. Comment configurer un serveur SNTP sur mon poste de travail pour synchroniser le SNMP IPv6 ?

Pour activer les services SNTP dans Windows XP, allez sur **Start (Démarrer) → Control Panel (Panneau de configuration) → Add/Remove Programs (Ajout/Suppression de programmes) → Add/ Remove Windows Components (Ajouter ou supprimer des composants Windows) → Networking Services (Services de mise en réseau) → contrôlez Simple TCP/ IP Services (Services TCP/IP simplifiés) → OK**. Pour activer la synchronisation de l'heure, vous devez paramétrer les adresses du serveur de temps SNTP dans **Time Server (Serveur de temps)**. Veuillez vous reporter au *chapitre 4 : Configurations système*.

### Q2. Comment s'assurer que la liaison entre le SNMP IPv6 et le PDU est établie ?

Si la liaison entre le SNMP IPv6 et le PDU est correctement établie, le voyant LED jaune clignote rapidement. Dans le cas contraire, contrôlez que le réglage de l'identifiant du dispositif sur le SNMP IPv6 et le PDU est cohérent.

```
C:\>ping 172.16.186.230

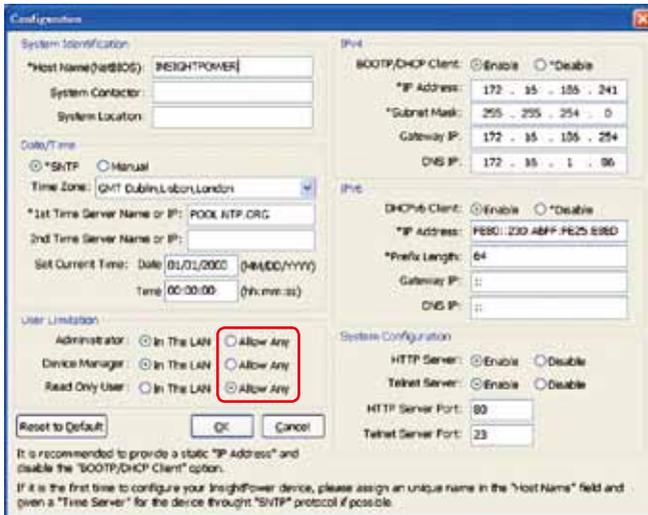
Test de ping 172.16.186.230 avec 32 octets de données :
Réponse de 172.16.186.230 : octets=32 temps=2 ms TTL=64
Réponse de 172.16.186.230 : octets=32 temps=2 ms TTL=64
Réponse de 172.16.186.230 : octets=32 temps=2 ms TTL=64
Réponse de 172.16.186.230 : octets=32 temps=4 ms TTL=64

Statistiques du test ping pour 172.16.186.230 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (0 % de perte),
    Durée approximative des boucles en millisecondes :
        Minimum = 2 ms, Maximum = 4 ms, Moyenne = 2 ms

C:\>
```

### Q3. Je peux accéder à l'InsightPower SNMP IPv6 pour PDU Web, mais je ne peux pas me connecter.

Contrôlez les adresses IP du SNMP IPv6 et du poste de travail sur lequel vous tentez de connecter. Par défaut, ils doivent être dans le même réseau local, de sorte que vous puissiez vous connecter via l'interface Web. Vous pouvez activer les connexions externes pour résoudre ce problème. Pour ce faire, lancez Ez-Setting et définissez l'élément User Limitation (Limite utilisateur) sur Allow Any (Autoriser tous), comme illustré ci-dessous.



**Q4. Je ne parviens pas à me connecter au SNMP IPv6 via son nom d'hôte, comment procéder ?**

Si vous attribuez simplement une nouvelle adresse IP statique au SNMP IPv6, vous pouvez avoir besoin de rafraîchir la table NetBIOS, de sorte qu'elle corresponde au nouveau réglage. Bien que Windows mette à jour régulièrement sa table NetBIOS, vous pouvez la forcer manuellement à se rafraîchir en saisissant la commande suivante **nbstat -R** dans l'invite de commande DOS. Vous pouvez ensuite vous connecter au SNMP IPv6 par son nom d'hôte. Assurez-vous également que le nom d'hôte attribué au SNMP IPv6 ne dépasse pas 16 octets.

**Q5. Comment vérifier l'adresse IP de mon poste de travail ?**

Pour Windows, veuillez entrer **ipconfig /all** dans l'invite de commande DOS. Pour UNIX, veuillez entrer **ifconfig** dans Shell. Vous devriez maintenant être en mesure de vérifier IP et MAC (adresse physique).

```

Adresse physique. . . . . : 00-23-4D-A2-3A-2C
DHCP activé . . . . . : Oui
Autoconfiguration activée . . . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::ad55:5b9b:74c6:e5fc%12 (Préférée)
Adresse IPv4. . . . . : 172.16.186.97 (Préférée)
Masque de sous-réseau . . . . . : 255.255.254.0

C:\>

```

**Q6. Je ne parviens pas à effectuer un test ping sur le SNMP IPv6 depuis mon poste de travail, comment procéder ?**

Si le SNMP IPv6 ne répond pas, vérifiez les éléments suivants :

- 1) Si le voyant LED vert du SNMP IPv6 est éteint, vérifiez que le câble réseau est correctement raccordé du SNMP IPv6 au routeur ou concentrateur.
- 2) Si le voyant LED vert est allumé, il se peut que l'adresse IP actuelle soit inaccessible. Attribuez manuellement une adresse IP valable au SNMP IPv6.
- 3) Si le voyant LED vert clignote et que (1) votre configuration réseau comprend un serveur DHCP, assurez-vous que le service DHCP fonctionne correctement ; (2) dans le cas contraire, assurez-vous que l'IP attribué n'est pas déjà pris sur le réseau. Veuillez noter que si la configuration actuelle n'est pas utilisable, le SNMP IPv6 réinitialisera les réglages IP par défaut (adresse IPv4 : 192.168.1.100/masque de réseau : 255.255.255.0/passerelle : 192.168.1.254).
- 4) Si le problème persiste, utilisez un câble réseau pour relier votre SNMP IPv6 au poste de travail. Effectuez un test ping de l'adresse IP statique ou par défaut du SNMP IPv6, selon vos configurations. Si une réponse de test ping est reçue avec succès, indiquant que le SNMP IPv6 fonctionne correctement, vérifiez votre équipement réseau. Si ce n'est pas le cas, contactez votre revendeur local ou un technicien pour demander de l'aide.

**Q7. Je ne parviens pas à effectuer une commande d'obtention de SNMP, comment procéder ?**

Veuillez vous reporter à la section **5-3-2 Notification** pour vérifier les réglages du SNMP. Assurez-vous que l'adresse IP du poste de travail est ajoutée à la liste IP NMS avec un accès en lecture ou en lecture/écriture. La chaîne de communauté sur le poste de travail et le SNMP IPv6 doivent correspondre.

**Q8. Je ne parviens pas à effectuer une commande de configuration du SNMP, comment procéder ?**

Veuillez vous reporter à la section **5-3-2 Notification** pour vérifier les réglages du SNMP. Assurez-vous que l'adresse IP du poste de travail est ajoutée à la liste IP NMS avec un accès en lecture/écriture. La chaîne de communauté sur l'ordinateur et le SNMP IPv6 doivent correspondre.

**Q9. Je ne parviens pas à recevoir une alerte SNMP, comment procéder ?**

Veuillez vous reporter à la section **5-3-2 Notification** pour vérifier les réglages d'alerte SNMP. Assurez-vous que l'adresse IP du poste de travail est ajoutée à la liste IP cible.

### Q10. J'ai oublié le compte et le mot de passe administrateur, comment procéder ?

Vous pouvez réinitialiser le compte et le mot de passe administrateur via le mode texte. Veuillez vous reporter à la section **4-4 Configuration via port COM** pour établir une connexion par port COM avec le SNMP IPv6. Lorsque les informations de connexion sont demandées, renseignez **rstadmin** dans un délai de 30 secondes, puis appuyez sur **Entrée**. Le compte et le mot de passe administrateur sont maintenant réinitialisés aux valeurs par défaut (admin/password).

### Q11. Comment activer IPv6 dans Windows XP ?

Si vous utilisez Windows XP, veuillez activer IPv6 dans un premier temps (cliquez sur **START [Démarrer] → RUN [Exécuter]**, puis entrez **ipv6 install**). Le SNMP IPv6 prend en charge IPv6 sans aucune configuration supplémentaire requise. Cependant, veuillez noter qu'IPv6 est automatiquement désactivé si une LLA (Local-link Address, Adresse de liaison locale) existe déjà sur le réseau local. Si le SNMP IPv6 obtient des enregistrements IPv4 et IPv6 depuis la résolution DNS, l'IPv4 est utilisé en tant qu'adresse principale pour le nom d'hôte en question.

Pour en savoir plus sur la compatibilité de l'IPv6, visitez IETF (<http://tools.ietf.org/html>) ou le programme IPv6 Ready Logo (<http://www.ipv6ready.org>).

### Q12. Comment générer un fichier de certificat SSL privé (au format PEM) pour une connexion HTTPs ?

Afin d'assurer une sécurité de connexion entre le SNMP IPv6 et votre poste de travail, vous pouvez créer votre propre fichier de certificat SSL. Veuillez télécharger et installer l'OpenSSL Toolkit à l'adresse <http://www.openssl.org>. Lancez l'invite de command Shell ou DOS et entrez la commande suivante pour créer votre propre fichier de certificat :

```
openssl req -x509 -nodes -days 3650 -newkey  
rsa:1024 -keyout cert.pem -out cert.pem
```

- 1) Répondez aux questions. Continuez selon les indications fournies. Une fois terminé, un fichier intitulé cert.pem est créé dans le répertoire de travail actuel.
- 2) Téléchargez cert.pem sur l'InsightPower SNMP IPv6 pour PDU Web. Veuillez vous reporter à la section **5-3-1 Administration - Web**.

### Q13. Comment générer les clés DSA, RSA et les clés publiques pour SSH ?

**Pour Linux :**

- 1) Veuillez télécharger et installer OpenSSH à l'adresse <http://www.openssl.org>.

- 2) Lancez Shell et entrez les commandes suivantes pour créer vos propres clés (veuillez ignorer lorsqu'il vous est demandé de saisir la phrase secrète) :

```
DSA Key:ssh-keygen -t dsa
```

```
RSA Key:ssh-keygen -t rsa
```

- 3) Téléchargez les clés DSA et RSA sur l'InSightPower SNMP IP0 pour PDU Web. Veuillez vous reporter à la section **5-3-1 Administration – Console** pour plus d'informations

**Pour Windows :**

- 1) Veuillez télécharger et installer PuTTY à l'adresse <http://www.putty.org>.
- 2) Exécutez putty en.exe à partir du répertoire installé.
- 3) Sélectionnez **SSH-2 RSA** dans la zone des paramètres et cliquez sur **Key (Clé) → Generate key pair (Générer paire de clés)** pour générer une clé RSA.
- 4) Cliquez sur **Conversions → Export OpenSSH Key (Exporter clé OpenSSH)** et attribuez un nom de fichier à la clé RSA. Veuillez ignorer lorsqu'il vous est demandé de saisir la phrase secrète de la clé.
- 5) Sélectionnez **SSH-2 DSA** dans les paramètres et cliquez sur **Key (Clé) → Generate key pair (Générer paire de clés)** pour générer une clé DSA.
- 6) Cliquez sur **Conversions → Export OpenSSH Key (Exporter clé OpenSSH)** et attribuez un nom de fichier à la clé DSA. Veuillez ignorer lorsqu'il vous est demandé de saisir la phrase secrète de la clé.
- 7) Copiez la clé générée à partir de la zone de texte, collez la dans un éditeur de texte et enregistrez en tant que fichier texte.



- 8) Téléchargez les clés DSA/RSA et clés publiques sur l'InsightPower SNMP IPv6 pour PDU Web. Veuillez vous reporter à la section **5-3-1 Système – Console** pour plus d'informations.

**Q14. Comment télécharger les fichiers de configuration/microprogramme/ clé via SSH/SFTP ?**

Pour configurer rapidement votre SNMP IPv6, vous pouvez télécharger les fichiers via SSH/SFTP. Le SNMP IPv6 importe automatiquement vos réglages après avoir téléchargé les fichiers dans les répertoires en question. Veuillez vous reporter au tableau suivant :

Répertoire	Fichiers
\config_snmp	snmp.ini
\config_system	configure.ini
\ssh_dsa	Clé DSA
\ssh_rsa	Clé RSA
\ssh_pubkey	Clé publique
\upgrade_snmp	Package de mise à niveau du microprogramme SNMP IPv6 (binaire)
\upgrade_device*	Package de mise à niveau du microprogramme du dispositif (binaire)

\*Apparaît sur les dispositifs spécifiques uniquement.

Téléchargez les fichiers dans les répertoires correspondants. Assurez-vous que les noms de fichier ne contiennent pas de caractères non anglais, afin d'éviter toute erreur de lecture. Ecrasez les fichiers existants si votre client SFTP vous le demande.

### Q15. Comment tester le SNMPv3 dans Linux ?

Avant de pouvoir accéder à SNMP OID (identificateur d'objet) via le protocole SNMPv3, le tableau SNMPv3 USM doit être organisé. Veuillez vous reporter à la section **5-3-2 Notification – SNMPv3 USM** pour plus d'informations.

Pour tester le SNMPv3 dans Linux, lancez Shell et entrez la commande suivante :

```
snmpwalk -v 3 -u <user> -l authPriv -A <password>
-X <password> -n <context name> -t 3 <ip>
1.3.6.1.2.1.1.1.0
```

-v : 1 pour le SNMPv1, 3 pour le SNMPv3.

-l : Suivent les niveaux de sécurité. Ces derniers sont : noAuthNoPriv, authNoPriv et authPriv.

-u : Nom d'utilisateur attribué selon le tableau SNMPv3 USM.

-A : Mot de passe Auth attribué selon le tableau SNMPv3 USM.

-X : Mot de passe Priv attribué selon le tableau SNMPv3 USM.

-n : Nom de contexte attribué selon le tableau SNMPv3 USM.

-t : Délai d'expiration en secondes.

<ip> : Adresse IP du SNMP IPv6.

<oid> : Prochain SNMP OID disponible (par exemple 1.3.6.1.2.1.1.1.0). Veuillez vous reporter à la MIB RFC1213.

### Q16. Pourquoi le SNMP IPv6 ne contrôle-t-il qu'un dispositif de PDU ?

Le réglage par défaut du NMP IPv6 permet uniquement de contrôler le PDU dont l'identifiant est défini sur 0. Pour contrôler un autre PDU ou plusieurs dispositifs de PDU, l'utilisateur peut utiliser l'InsightPower SNMP IPv6 pour PDU Web (**Device [Dispositif] → Configuration → PDU**) ou le protoo le SNMP pour reß aurer le réglage par défaut.

## Annexe A : Spécifications

Modèle	InsightPower SNMP IPv6 pour PDU
Entrée de puissance	5 Vdc
Consommation électrique	2 watt (maximum)
Connexion réseau	Connecteur enfichable RJ-45 (10/100 M)
<b>Physique</b>	
Dimensions (l x P x H)	45 mm x 128 mm x 55 mm
Poids	280 g
<b>Environnemental</b>	
Température de fonctionnement	0 ~ 40 °C
Température de stockage	-40 ~ 125 °C
Humidité de fonctionnement	10 ~ 80 % (sans condensation)



- \* Reportez-vous à la plaque signalétique pour connaître la classe de sécurité.
- \* Toutes les spécifications sont modifiables sans préavis.

## Annexe B : Garantie

Le Vendeur garantit que le présent produit, si celui-ci est utilisé conformément à toutes les instructions applicables, est exempt de défaut de pièce et main d'œuvre durant la période de garantie. Durant cette période, le Vendeur s'engage à réparer ou à remplacer, à sa seule discrétion, tout produit qui s'avérerait défectueux.

La garantie ne couvre pas l'usure normale ni les dommages résultant d'une installation, d'un fonctionnement, d'une utilisation, d'une maintenance impropres ou d'un cas de force majeure (p. ex. guerre, incendie, catastrophe naturelle, etc.). Cette garantie exclut en outre expressément tous les dommages consécutifs et indirects.

Un service de maintenance moyennant des frais est proposé pour les dommages survenus à l'issue de la période de garantie. Pour toute demande de maintenance, veuillez vous adresser directement au fournisseur ou au Vendeur.



**AVERTISSEMENT :** Chaque utilisateur doit s'assurer, avant toute utilisation, que l'environnement et les caractéristiques de charge sont sûrs et conviennent à l'installation et à l'utilisation du produit. Le manuel d'utilisateur doit être suivi attentivement. Le Vendeur ne formule aucune allégation ni n'offre aucune garantie quant à l'adéquation ou au caractère approprié du produit pour une application spécifique.





