Dominion® PX

Manuel d'utilisation

Version 1.1.0

DPX-0G-F
Mars 2008
255-80-6080-00

Informations FCC (Etats-Unis seulement)

Cet équipement a été testé et certifié conforme aux limites d'un dispositif numérique de catégorie A selon l'article 15 du code de la Commission fédérale des communications des Etats-Unis (FCC). Ces limites visent à fournir une protection raisonnable contre les interférences nuisibles dans une installation commerciale. Cet équipement génère, utilise et peut émettre des émissions radioélectriques. S'il n'est pas installé et utilisé conformément aux instructions, il risque d'entraîner des interférences perturbant les communications radio. L'utilisation de l'équipement dans un environnement résidentiel peut générer des interférences nuisibles.

Informations VCCI (Japon seulement)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan n'est pas responsable des dégâts subis par ce produit suite à un accident, une catastrophe, une mauvaise utilisation, une modification du produit non effectuée par Raritan ou tout autre événement hors du contrôle raisonnable de Raritan ou ne découlant pas de conditions normales d'utilisation.

Consignes de sécurité

Pour éviter tout risque d'électrocution fatale et de dommages éventuels à l'équipement Raritan :

LES SYSTEMES NE DOIVENT ETRE CONFIGURES QUE PAR UNE PERSONNE COMPETENTE.

CET APPAREIL DOIT ABSOLUMENT ETRE CONNECTE A UNE ALIMENTATION ELECTRIQUE DOTEE D'UN CONDUCTEUR DE TERRE DE PROTECTION.

AVERTISSEMENT : TO ISOLATE THIS EQUIPMENT DISCONNECT POWER SUPPLY PLUG.

ATTENTION ! AFIN D'ISOLER TOTALEMENT CET APPAREIL, DEBRANCHER LA FICHE D'ALIMENTATION.

CAUTION: USE ONLY IN DRY LOCATIONS.

ATTENTION ! UTILISER UNIQUEMENT DANS DES EMPLACEMENTS SECS.

N'utilisez de câble d'alimentation à 2 fils dans aucune configuration du produit.

Testez les prises CA de l'ordinateur et de l'écran pour vérifier qu'elles sont correctement connectées et mises à la terre.

Utilisez uniquement des prises mises à la terre pour l'ordinateur comme pour l'écran. Si vous utilisez un onduleur de secours, débranchez l'ordinateur, l'écran et l'appareil de l'alimentation.

La prise de courant d'installation utilisée pour l'alimentation de cet appareil doit être installée près de celui-ci et doit être aisément accessible.

A l'installation de ce produit, le circuit de distribution l'alimentant doit obligatoirement être protégé par un dispositif de protection du circuit terminal d'une puissance nominale maximum adaptée à celle du produit.

Cette unité de distribution d'alimentation est conçue uniquement pour fournir une alimentation électrique à l'appareil. Aucune barrette d'alimentation secondaire (satellite) ne doit être connectée aux prises.

Ce produit a été conçu pour répondre aux dernières exigences en matière de sécurité. Outre la conformité aux normes d'utilisation générale, il a été configuré en usine pour un usage dans des environnements de montage en rack, aidant ainsi l'installateur à fournir des systèmes conformes aux normes pertinentes.

Etablissez une connexion de mise à la terre afin de brancher la fiche sur le réseau électrique. Lorsque vous déconnectez la mise à la terre, veillez à débrancher préalablement la fiche du réseau électrique.

Table des matières

Chapitre 1 Introduction

L'unité Dominion PX est une unité de distribution d'alimentation intelligente qui permet de redémarrer les serveurs à distance et autres dispositifs réseau, et de contrôler l'alimentation du centre de données, via des commutateurs KVM et des serveurs de console sécurisée Raritan. Depuis le bureau ou de n'importe où, l'unité Dominion PX met sous tension, hors tension ou redémarre des équipements à distance, et contrôle le courant, la tension, l'alimentation et la température.

La Dominion PX offre la possibilité de récupérer des systèmes à distance en cas de panne et/ou de blocage du système. Elle évite les interventions manuelles ou l'envoi de personnel sur le terrain, réduit les temps d'arrêt et les délais de réparation, et augmente la productivité.

Dans ce chapitre

Modèles du produit

Il existe plusieurs modèles de l'unité Dominion PX fabriqués pour les stocks et disponibles presque immédiatement. Raritan propose également des modèles personnalisés fabriqués à la commande et disponibles uniquement à la demande.

Reportez-vous à l'***annexe A*** (voir "Modèles Dominion PX" à la page 134) pour obtenir la liste des modèles de Dominion PX.

Photos du produit

L'unité Dominion PX existe dans les tailles 0U (zéro U), 1U et 2U.

Photos du produit

Taille 0U

Taille 1U

Taille 2U

Caractéristiques du produit

Tous les modèles et les tailles de l'unité Dominion PX présentent les caractéristiques suivantes :

- Contrôle collectif et individuel des prises
- Mise sous tension, hors tension et redémarrage des dispositifs branchés sur chaque prise
- Possibilité de grouper les prises de plusieurs unités Dominion PX en tant que prises virtuelles accessibles depuis une même session
- Contrôle des éléments suivants au niveau de la prise :

  Courant efficace

  Facteur de puissance

  Courant efficace maximum

  Tension efficace

  Puissance active

Puissance apparente

- Possibilité de surveiller la température interne de la Dominion PX et du processeur
- Possibilité de surveiller les facteurs d'environnement, tels que la température externe et l'humidité
- Une alarme sonore et une alarme visuelle (voyant clignotant) pour indiquer une surcharge de courant
- Des seuils d'alarme configurables
- Prise en charge de SNMP v1, v2 et v3.
- Capacité d'envoyer des traps à l'aide du protocole SNMP
- Possibilité de récupérer les données spécifiques à une prise à l'aide du protocole SNMP, notamment l'état, le courant, la tension et la puissance de la prise
- Possibilité de configurer et de définir des valeurs via SNMP, notamment les niveaux de seuil de l'unité et des prises
- Disjoncteurs divisionnaires locaux blindés sur les produits d'une puissance nominale supérieure à 20 A pour protéger l'équipement connecté des surcharges et des courts-circuits
- Intégration aux solutions Paragon, CommandCenter Secure Gateway (CC-SG) et Dominion de Raritan

Contenu de l'emballage

L'emballage de chaque produit contient l'équipement et le matériel suivants.

Produits 0U

- Unité Dominion PX comportant un câble d'alimentation d'1,80 mètre
- Patte de fixation pour 0U et vis
- Support de fixation de montage sans outil pour unités 0U
- Câble null-modem avec connecteurs RJ-45 et DB9F à une extrémité et à l'autre

Produits 1U

- Unité Dominion PX comportant un câble d'alimentation d'1,80 mètre
- Ensemble de fixation 1U et vis
- Câble null-modem avec connecteurs RJ-45 et DB9F à une extrémité et à l'autre

Produits 2U

- Unité Dominion PX comportant un câble d'alimentation d'1,80 mètre
- Ensemble de fixation 2U et vis
- Câble null-modem avec connecteurs RJ-45 et DB9F à une extrémité et à l'autre

Chapitre 2 Montage sur rack de l'unité Dominion PX

Dans ce chapitre

Consignes de sécurité pour montage en rack

Pour les produits Raritan qui doivent être montés en rack, prenez les précautions suivantes :

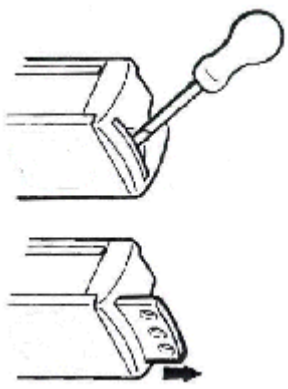
La température de fonctionnement dans un environnement de rack fermé peut être supérieure à la température ambiante. Ne dépassez pas la température ambiante maximum recommandée des appareils (reportez-vous à l'annexe A : Caractéristiques).

Assurez-vous que la circulation d'air dans l'environnement de rack est suffisante.

Montez l'équipement dans le rack avec précaution de façon à éviter tout chargement bancal des composants mécaniques.

Branchez l'équipement au circuit d'alimentation avec précaution afin d'éviter une surcharge des circuits.

Mettez tout l'équipement correctement à la terre sur le circuit terminal, spécialement les raccords d'alimentation.

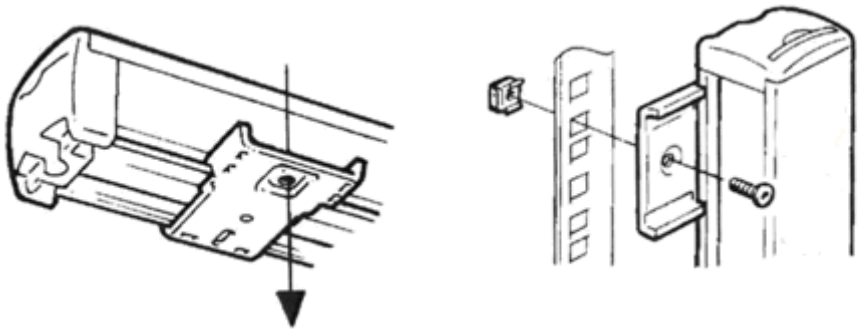


Les unités 0U sont fournies avec du matériel d'isolation de haute qualité en polycarbonate permettant la fixation dans des positions différentes au sein du rack.

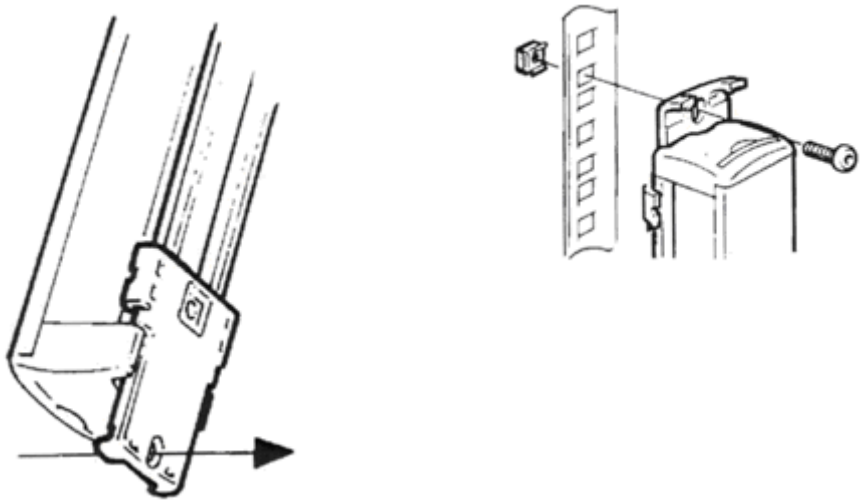
Pour un montage sur panneau/encastré, des pattes de fixation escamotables figurent sur embouts pour permettre le montage sur des rails adaptés.

Consultez les autres options présentées ci-dessous.

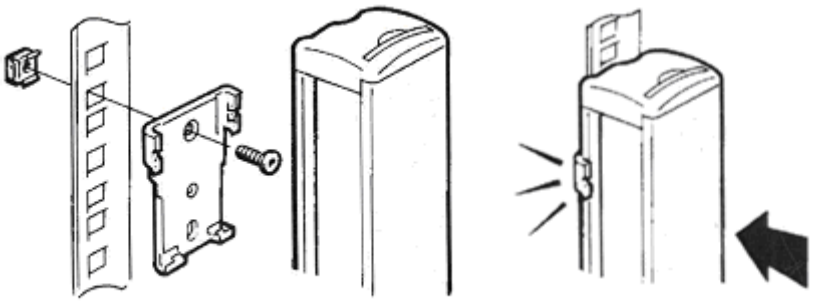
Fixation latérale



Fixation en extrémité



Fixation dissimulée



Instructions de montage sans outil

Les unités 0U sont également livrées avec un kit de montage sans outil composé d'une fixation à griffes dotée d'un bouton argenté sur un côté. Elle se fixe à l'arrière de l'unité Dominion PX 0U (côté opposé aux prises) en alignant le bouton sur les orifices de montage de l'armoire. Notez que cette option de fixation de l'unité Dominion PX n'est pas disponible sur tous les racks.

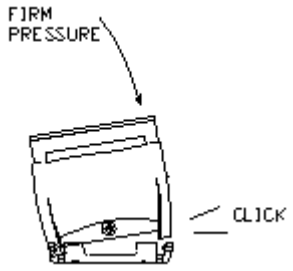
Avant de commencer :

- Assurez-vous que l'armoire dispose d'un espace suffisant pour monter l'unité Dominion PX. Prévoyez environ 3 cm à chaque extrémité (en haut et en bas) de l'unité.
- Il peut être utile de marquer l'arrière de l'unité Dominion PX à travers les trous de montage que vous comptez utiliser. Utilisez ensuite cette marque pour vous aider à aligner correctement les boutons argentés lors de la fixation des griffes.

Pour réaliser le montage :

- Enfichez les fixations à griffes à l'arrière de l'unité Dominion PX. Laissez au moins 60 cm entre les boutons pour assurer la stabilité. Une fois les griffes montées sur le rail de la Dominion PX, elles ne sont plus aisément amovibles ; utilisez un tournevis à tête plate pour les retirer si elles doivent être repositionner.
- Alignez les boutons argentés avec les trous de montage de l'armoire et assurez-vous qu'ils peuvent s'engager simultanément.
- Enfoncez l'unité Dominion PX, en poussant les boutons à travers les trous, puis laissez-la descendre d'environ 1,5 cm. L'unité Dominion PX est maintenant bien en place et l'installation est terminée.

L'image illustre la fermeté de la pression à appliquer pour enficher les griffes sur l'unité Dominion PX 0U. Accrochez d'abord un côté du corps du produit à l'une des extrémités de la fixation en griffes et exercez une pression pour enficher la seconde.



Chapitre 3 Installation et configuration

Ce chapitre explique comment installer une unité Dominion PX et la configurer pour la connectivité réseau.

Dans ce chapitre

Avant de commencer

Avant de commencer l'installation, effectuez les opérations suivantes :

Déballer l'unité Dominion PX et ses composants

1. Retirez l'unité Dominion PX et autres équipements du carton d'expédition. Reportez-vous à la section Contenu de l'emballage pour obtenir la liste complète du contenu du carton.
2. Comparez les numéros d'unité et de série de l'équipement à ceux du bordereau d'emballage situé à l'extérieur du carton et assurez-vous qu'ils correspondent.
3. Inspectez soigneusement l'équipement. Si une partie de l'équipement est endommagée ou manque, contactez le service de support technique Raritan.

Préparer le site d'installation

1. Assurez-vous que la zone d'installation est propre et non exposée à des températures extrêmes ou à l'humidité.
2. Veillez à laisser un espace suffisant autour de l'unité Dominion PX pour le câblage et le branchement sur les prises.
3. Consultez les instructions de sécurité figurant au début de ce manuel d'utilisation.

Remplir la fiche de configuration du matériel

Une fiche de configuration du matériel est fournie à l'***annexe B*** (voir "Fiche de configuration du matériel" à la page 137). Utilisez-la pour noter le modèle, le numéro de série et l'utilisation de chaque dispositif connecté à la Dominion PX.

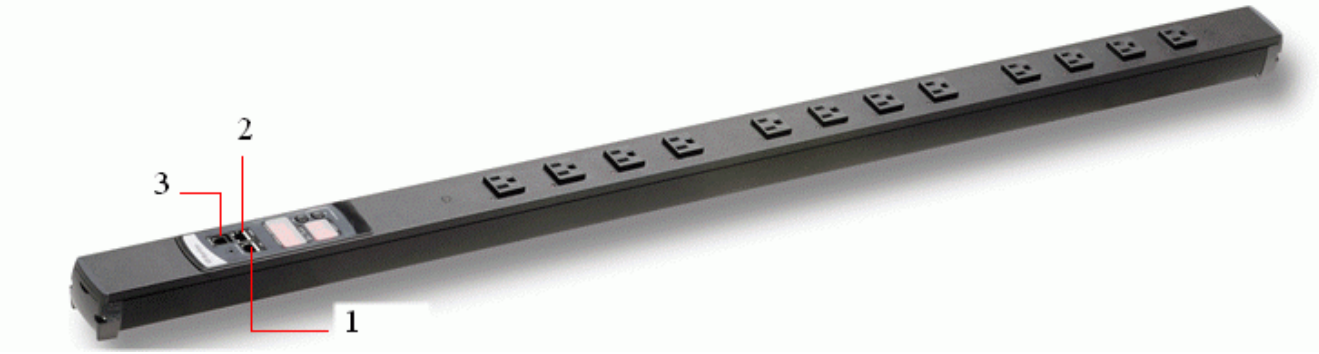
Gardez cette fiche à jour au fur et à mesure de l'ajout et du retrait des dispositifs.

Connecter l'unité Dominion PX à un ordinateur

Vous devez connecter l'unité Dominion PX à un ordinateur pour la configurer ; par l'intermédiaire d'une connexion série entre l'unité et l'ordinateur. Si vous envisagez d'utiliser cette connexion pour vous connecter à l'interface de ligne de commande CLP, laissez le câble connecté une fois la configuration terminée.

L'ordinateur doit disposer d'un programme de communication, tels qu'HyperTerminal ou PuTTY. Vous aurez également besoin du câble null-modem et des connecteurs fournis avec la Dominion PX.

1. Branchez l'extrémité du câble null-modem dotée du connecteur RJ-45 au port libellé **Serial** (Série) à l'avant de la Dominion PX. (Repérez l'emplacement de ce port sur votre Dominion PX à l'aide des images suivantes.)



Numéro	Description
1	Port LAN
2	Port série
3	Port réseau

2. Connectez l'autre extrémité du câble null-modem (contenant le connecteur DB9) au port série (COM) de l'ordinateur.

Connecter l'unité Dominion PX au réseau

Pour utiliser l'interface Web afin d'administrer la Dominion PX, vous devez connecter celle-ci à votre réseau local (LAN).

1. Connectez une des fiches d'un câble UTP Cat 5e standard au port LAN à l'avant de la Dominion PX. (Repérez l'emplacement de ce port sur votre modèle de Dominion PX à l'aide des images de la section ***Connecter l'unité Dominion PX à un ordinateur*** (à la page 12).)
2. Branchez l'autre fiche du câble à votre réseau local.

Configurer l'unité Dominion PX pour la connectivité réseau

Une fois la Dominion PX connectée à votre réseau, vous devez lui fournir une adresse IP et des données de réseau supplémentaires.

1. Sur l'ordinateur connecté à la Dominion PX, ouvrez un programme de communication, tel qu'HyperTerminal ou PuTTY. Assurez-vous que ses paramètres de port sont configurés comme suit :
   - Bits per second (Bits par seconde) = 9600

- Data bits (Bits de données) = 8
- Stop bits (Bits d'arrêt) = 1
- Parity (Parité) = None (Néant)
- Flow control (Contrôle du flux) = None

Remarque : le paramètre Flow control doit être défini sur None pour que le programme de communication fonctionne correctement avec la Dominion PX.

2. Pointez le programme de communication sur le port série de connexion à l'unité Dominion PX et ouvrez une fenêtre de terminal.
3. Appuyez sur **Entrée** pour afficher l'invite d'ouverture de configuration.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command:
```

4. Tapez **config** et appuyez sur **Entrée** pour démarrer le processus de configuration. Vous êtes invité à sélectionner une méthode de configuration IP.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]:
```

5. Vous devez attribuer une adresse IP à la Dominion PX. Il existe deux méthodes pour cela :
   - **Auto configuration** (Configuration automatique)Sélectionnez une méthode de configuration automatique, telle que **dhcp** ou **bootp**, et laissez le serveur DHCP ou BOOTP fournir l'adresse IP.

- **Static IP address** (Adresse IP statique) Sélectionnez **None** (Néant) et attribuez une adresse IP statique à la Dominion PX. Vous serez invité à indiquer l'adresse, le masque réseau et la passerelle.

Remarque : l'adresse IP de l'unité Dominion PX est automatiquement affichée à l'invite système. L'adresse IP par défaut est 192.168.0.192. La méthode de configuration IP par défaut est DHCP, et l'adresse IP par défaut est remplacée par celle affectée par DHCP ou BOOTP, ou par l'adresse IP statique saisie, dès que le processus de configuration est terminé. Pour utiliser l'adresse IP par défaut usine, tapez **none** (néant) comme commande de configuration automatique IP et acceptez la valeur par défaut. L'adresse IP par défaut pour la configuration statique (néant) est 192.168.0.192.

Tapez votre sélection et appuyez sur Entrée. Vous êtes invité à activer le contrôle d'accès IP.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: _
```

6. Par défaut, le contrôle d'accès IP N'EST PAS activé. Ceci désactive le pare-feu de Dominion PX. Laissez cette option désactivée pour le moment. Vous pourrez activer le pare-feu ultérieurement depuis l'interface Web et créer des règles de pare-feu (reportez-vous à la section ***Configuration du pare-feu*** (à la page 55) pour en savoir plus).

Remarque : si vous créez par inadvertance une règle qui vous expulse de la Dominion PX, vous pouvez exécuter à nouveau le programme de configuration et réinitialiser ce paramètre sur **disabled** (désactivé) pour vous autoriser l'accès à l'unité.

7. Dans l'immédiat, appuyez sur Entrée. Vous êtes invité à définir la vitesse de l'interface LAN.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]:
```

8. Par défaut, la vitesse de l'interface LAN est définie sur Auto, ce qui permet au système de sélectionner la vitesse optimale. Pour conserver la valeur par défaut, appuyez sur Entrée. Pour définir la vitesse sur 10 ou 100 Mbps, tapez la vitesse souhaitée et appuyez sur Entrée. Vous êtes invité à sélectionner le mode bidirectionnel de l'interface LAN.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]: 100
LAN interface duplex mode (auto/half/full) [auto]:
```

9. Par défaut, le mode bidirectionnel de l'interface LAN est définie sur **Auto**, ce qui permet au système de sélectionner le mode optimal. Le mode bidirectionnel Half (Semi) permet la transmission des données depuis et vers la Dominion PX, mais non simultanément. Le mode bidirectionnel Full (Simultané) permet la transmission dans les deux sens simultanément.

Pour conserver la valeur par défaut, appuyez sur **Entrée**. Pour indiquer le mode bidirectionnel semi ou simultané, tapez **half** ou **full** et appuyez sur **Entrée**. Vous êtes invité à confirmer les données que vous venez de saisir.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]: 100
LAN interface duplex mode (auto/half/full) [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel _
```

10. Tous les paramètres de configuration ont maintenant été saisis. Toutes les invites sont toujours affichées ; vous pouvez donc vérifier les données entrées. Effectuez une des opérations suivantes :

    - Si les données sont correctes, tapez **y** et appuyez sur **Entrée**. Le système achève la configuration et affiche un message l'indiquant.
    - Si un ou plusieurs paramètres sont incorrects, tapez **n** et appuyez sur **Entrée**. Vous retournez à l'invite de configuration IP illustrée dans la capture d'écran de l'étape 4 et vous pouvez corriger chaque entrée. Lorsque les données sont correctes, tapez **y** et appuyez sur **Entrée** pour terminer la configuration et retourner à l'invite d'ouverture illustrée dans la capture d'écran de l'étape 3.
    - Pour interrompre le processus de configuration, tapez **c** et appuyez sur **Entrée**. La configuration est annulée et vous retournez à l'invite d'ouverture comme illustré dans la capture d'écran de l'étape 3.

11. Si vous avez entré y pour confirmer la configuration, un message s'affiche pour vous indiquer que la configuration est terminée. Vous retournez alors à l'invite d'ouverture comme illustré dans la capture d'écran de l'étape 3. Vous pouvez maintenant utiliser votre unité Dominion PX.

```
Welcome!
At the prompt type one of the following commands:
- "clp"     : Enter Command Line Protocol
- "config"  : Perform initial IP configuration
- "unblock" : Unblock currently blocked users
192.168.0.192 command: config
IP autoconfiguration (none/dhcp/bootp) [none]: dhcp
Enable IP Access Control (yes/no) [no]: no
LAN interface speed (auto/10/100) [auto]: 100
LAN interface duplex mode (auto/half/full) [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel y

Configuring device ...
Done.
```

Remarque : la prise d'effet de l'adresse IP configurée prend environ 15 secondes pour le dispositif connecté via la ligne série, ou plus longtemps si elle est configurée via DHCP.

Réinitialiser les valeurs par défaut usine

Important : la réinitialisation des valeurs par défaut usine d'une DPX doit être effectuée avec précaution. Elle élimine toutes les données saisies, notamment les profils utilisateur, les groupes d'utilisateurs, les seuils, les stratégies d'alerte, etc.

Pour des raisons de sécurité, la Dominion PX ne peut être réinitialisée aux valeurs par défaut usine que depuis la console série locale Pour ce faire :

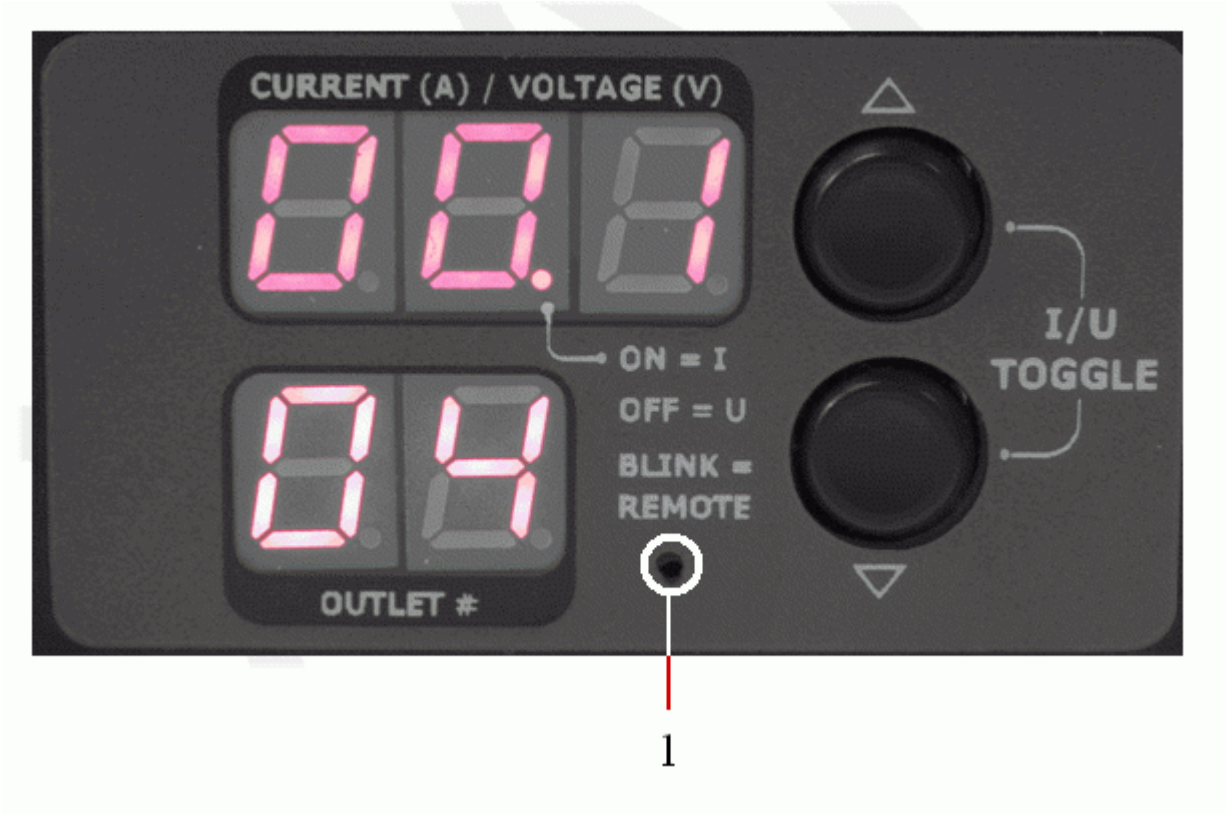
1. Connectez un ordinateur au port série de la Dominion PX.
2. A l'aide d'un programme d'émulation de terminal, tel qu'HyperTerminal, Kermit ou PuTTY (à la vitesse de 9600 bps), ouvrez une fenêtre sur la DPX. Assurez-vous que les paramètres de port série sont configurés comme suit :

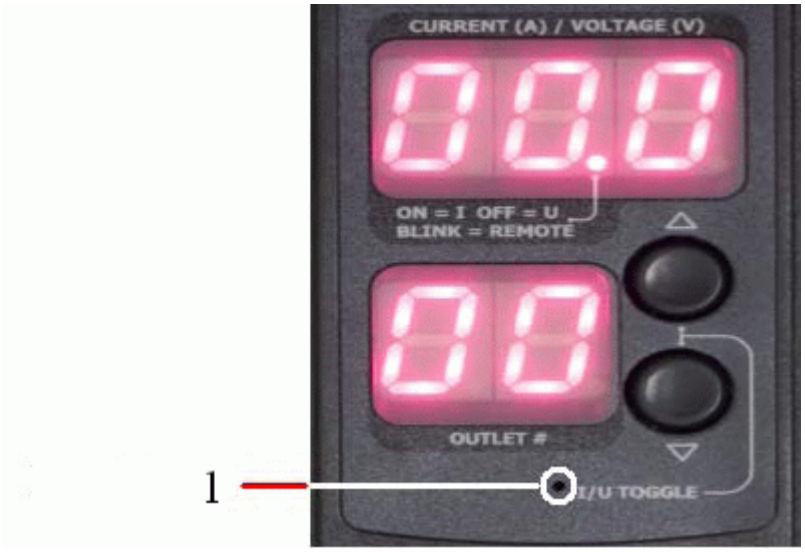
- Baud rate (bits per second) (Débit en bauds (bits par seconde)) = 9600
- Data bits (Bits de données) = 8
- Stop bits (Bits d'arrêt) = 1
- Parity (Parité) = None (Néant)
- Flow control (Contrôle du flux) = None

1. Enfoncez (et relâchez) le bouton Reset (Réinitialiser) de la DPX tout en appuyant plusieurs fois rapidement sur la touche Echap. Une invite (=>) doit apparaît après environ une seconde.
2. Exécutez la commande defaults pour réinitialiser la DPX à ses valeurs par défaut usine.

Remarque : entrez help (aide) pour afficher la liste des commandes disponibles et une brève description de chacune.
HyperTerminal est disponible sous de nombreux systèmes d'exploitation Windows. Il n'est toutefois pas disponible sous Windows Vista. PuTTY est un programme libre téléchargeable depuis Internet. Reportez-vous à la documentation de PuTTY pour en savoir plus sur la configuration.

L'image ci-dessous indique l'emplacement de l'orifice de réinitialisation.





Numéro	Description
1	Orifice de réinitialisation

Chapitre 4 Utilisation de l'unité Dominion PX

Ce chapitre explique comment utiliser l'unité Dominion PX. Il décrit les voyants et les ports sur les panneaux avant et arrière de l'unité Dominion PX, et explique comment utiliser le panneau d'affichage. Il explique également comment le disjoncteur fonctionne et quand l'alarme est émise.

Dans ce chapitre

Panneau avant

Le panneau avant des unités Dominion PX 1U et 2U se compose d'un voyant bleu sur la droite et de trois ports de connexion sur la gauche, tandis que le modèle 0U se compose de prises de courant pour brancher des dispositifs sur la Dominion PX, d'un panneau d'affichage et de trois ports de connexion.

Ports de connexion

Les trois ports, de gauche à droite, sont libellés **Serial** (Série) (RJ-45), **Feature** (Fonction) (RJ-12) et **LAN** (Réseau local) (Ethernet, RJ-45). Le tableau ci-dessous explique l'utilisation de chaque port.

Port	Utilisation
Serial	Etablir une connexion série entre un ordinateur et la Dominion PX. Prenez le câble null-modem fourni avec l'unité Dominion PX, branchez la fiche du connecteur RJ-45 au port libellé Serial à l'avant de la Dominion PX et la fiche du connecteur DB9F au port série (COM) de l'ordinateur. Le port série assure également l'interface avec certains produits d'accès Raritan (tels que la Dominion KX) par l'utilisation d'un CIM d'alimentation.
Feature	Avec des capteurs d'environnement fournis par Raritan.

LAN	Connexion de la Dominion PX au réseau de votre société Raccordez un câble UTP Catégorie 5e standard à ce port et connectez l'autre fiche à votre réseau. Cette connexion est nécessaire à l'administration à distance de la Dominion PX via l'interface Web. Il existe deux petits voyants sous le port LAN. Le vert indique un lien physique et l'activité, et le jaune, la communication à des vitesses de 10/100 BaseT.

Remarque : la connexion d'un CIM d'alimentation, hormis le D2CIM-PWR (P2CIM-PWR par exemple), au port série de la Dominion PX fait passer toutes les prises à l'état ON (sous tension), même si elles étaient précédemment à l'état OFF.

Voyant bleu

Seuls les modèles 1U et 2U comportent un voyant bleu sur le panneau avant. Ce voyant bleu sur le côté droit du panneau avant s'allume dès que l'unité Dominion PX est branchée.

Panneau arrière

Le panneau arrière des unités Dominion PX 1U et 2U se compose, de gauche à droite, d'un câble d'alimentation, de prises pour brancher les dispositifs à la Dominion PX, et d'un panneau d'affichage, tandis que les modèles 0U ne comporte pas de panneau arrière.

Câble d'alimentation

Le câble d'alimentation qui relie la Dominion PX à une source d'alimentation est situé à l'extrême gauche du panneau arrière ou à l'extrémité de l'unité s'il s'agit du type 0U. Tous les dispositifs ne peuvent pas être recâblés par l'utilisateur.

Remarque : chaque modèle de Dominion PX doit être branché sur la prise adaptée à son type.

La Dominion PX ne comporte pas d'interrupteur d'alimentation. Les produits d'une puissance nominale supérieure à 20 A sont dotés de disjoncteurs divisionnaires totalement blindés pour éviter un fonctionnement accidentel. Pour effectuer une alimentation cyclique de l'unité, retirez le câble d'alimentation de la source, puis rebranchez-le.

Prises

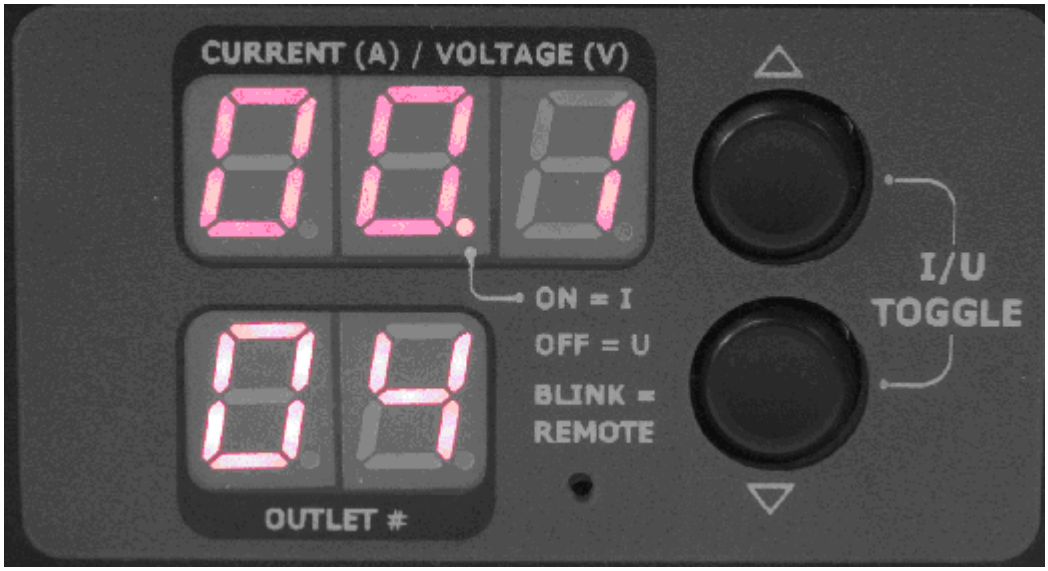
Le nombre de prises sur le panneau arrière dépend du modèle de Dominion PX. Dans le coin supérieur gauche de chaque prise figure un petit voyant. Les unités sont expédiées de l'usine avec toutes les prises sous tension (ON). Le tableau ci-dessous donne la signification des différents états de voyant.

Etat du voyant	Statut de la prise	Signification
Non allumé (gris clair)	Unité inactive	La prise n'est pas alimentée ou l'alimentation du circuit de contrôle est interrompue.
Rouge	Active et sous tension	La prise est active (relais fermé) et sous tension (tension présente).
Rouge clignotant	Active et sous tension	La prise est active et sous tension, mais il y a surcharge et le courant a franchi le seuil non critique.
Vert	Inactive et sous tension	La prise est inactive (relais ouvert) et sous tension.
Vert clignotant	Inactive et hors tension	La prise est inactive et le disjoncteur est inactif
Jaune clignotant	Active et hors tension	La prise est active mais hors tension (disjoncteur ouvert ou autre erreur de rail à haute tension).
Rouge, vert et jaune en alternance	s/o	La Dominion PX vient d'être branchée et son logiciel de gestion est en cours de chargement. OU Une mise à niveau du firmware est en cours sur l'unité.

Remarque : lorsqu'une unité Dominion PX est allumée, le chargement de l'auto-test à la mise sous tension et du logiciel prend quelques instants. Lorsque l'unité démarre, les voyants de la prise passent du rouge au vert et au jaune. Lorsque le logiciel est chargé, les voyants de la prise affichent une couleur fixe et le compteur s'allume.

Affichage à DEL

L'affichage à DEL se situe à côté des prises sur le modèle 0U, et à l'arrière à droite sur les modèles 1U et 2U. L'illustration suivante présente l'affichage à DEL.



L'affichage à DEL est constitué des composants suivants :

- Une rangée inférieure affichant deux chiffres
- Une rangée supérieure affichant trois chiffres
- Boutons **Haut** et **Bas**

Remarque : le petit orifice entre la rangée inférieure et le bouton Bas permet la réinitialisation. Si elle connectée au port série, l'unité Dominion PX peut être réinitialisée à ses valeurs par défaut usine par cet orifice. Reportez-vous à la section **Réinitialiser les valeurs par défaut usine** *(à la page 18) pour en savoir plus. Une simple pression sur cet orifice de réinitialisation redémarre UNIQUEMENT l'unité.*

Rangée inférieure

La rangée inférieure affiche le numéro de la prise.

Rangée supérieure

La rangée supérieure affiche les relevés de courant, de tension et d'alimentation de la prise indiquée dans la rangée inférieure. Lors de la mise à niveau du firmware, la rangée supérieure affiche FuP pour indiquer que le processus est en cours sur l'unité.

➢ *Pour faire fonctionner l'affichage à DEL :*

1. Utilisez les boutons **Haut** et **Bas** pour sélectionner une prise. Appuyez une fois sur le bouton **Haut** pour avancer d'un numéro de prise. Appuyez une fois sur le bouton **Bas** pour reculer d'un numéro de prise.
2. Lorsqu'une prise est sélectionnée, son numéro apparaît dans la rangée inférieure et le courant dans la rangée supérieure. Il s'affiche dans le format suivant : **XX.X (A)**
3. Pour afficher la tension de la prise sélectionnée, appuyez simultanément sur les boutons Haut et Bas. Le relevé de tension remplace le courant pendant environ 5 secondes, puis celui-ci réapparaît.
4. Pour afficher l'alimentation active de la prise sélectionnée, appuyez simultanément sur les boutons Haut et Bas pour afficher la tension, appuyez une seconde fois pour afficher l'alimentation active. Elle s'affiche dans le format suivant : **X.XX** en voltampères **(VA).**

Astuce : la position du point décimal permet de distinguer rapidement la tension, le courant et l'alimentation à l'affichage. La tension ne comporte aucun point décimal, pour le courant, ce point figure entre les premier et second chiffres, et pour l'alimentation, entre les second et troisième chiffres.

Vous pouvez visualiser le courant et la tension de l'unité Dominion PX entière en utilisant les boutons **Haut** et **Bas** pour sélectionner le numéro de prise **00**. Les voyants ne présentent pas l'alimentation active pour l'unité et affichent **---** à la place.

Disjoncteur

La Dominion PX comprend des disjoncteurs divisionnaires qui se déclenchent automatiquement si une surcharge d'alimentation est détectée. La Dominion PX utilise des disjoncteurs à courbe de déclenchement de type C. Si le disjoncteur éteint le rail de tension, la rangée inférieure du panneau d'affichage passe au numéro de prise le plus bas affecté par l'erreur du disjoncteur, et la rangée inférieure affiche les trois lettres suivantes indiquant une erreur de disjoncteur :

CbE

Remarque : les modèles de Dominion PX intégrant des disjoncteurs sont les unités dont la puissance nominale dépasse 20 ampères, notamment DPCS12-30L, DPCS20-30L, DPCS20A-32, DPCS20A-30L6, DPCR20-30L et DPCR20A-32.

Vous pourrez toujours passer d'une prise à l'autre sur le panneau d'affichage de la Dominion PX. Les prises affectées par l'erreur affichent **CbE**. Les prises non affectées présentent les relevés de courant et de tension décrits précédemment.

Pour réarmer les disjoncteurs en cas de surcharge :

- Sur les produits 1U et 2U, détachez le châssis avant pour accéder aux disjoncteurs.
- Sur le produit 0U, accédez aux disjoncteurs en levant le capot à charnière recouvrant leur élément.

Alarme sonore

La Dominion PX comporte une alarme sonore. Elle retentit si un des disjoncteurs est déclenché ou si le capteur de température du tableau de contrôle dépasse 80° C.

L'alarme s'arrête si les conditions d'interruption du disjoncteur disparaissent ou si le capteur de température du tableau de contrôle descend sous 70° C.

Les seuils de température sont définis en usine et peuvent être modifiés par l'utilisateur.

Il faut au maximum trois secondes à l'alarme pour se déclencher après l'interruption du disjoncteur.

Exactitude des mesures

- **Tension (par prise)** : Plage 0-255V, +/-5 %, 3 chiffres, résolution de 1V
- **Courant (par prise)** : Plage 0-25A, +/-5 %, 3 chiffres, résolution de 0,1A

Chapitre 5 Utilisation de l'interface Web

Ce chapitre explique comment utiliser l'interface Web pour administrer une unité Dominion PX.

Dans ce chapitre

Connexion à l'interface Web

Pour vous connecter à l'interface Web, vous devez entrer un nom d'utilisateur et un mot de passe. Pour la première connexion, utilisez le nom d'utilisateur (**admin**) et le mode de passe **(raritan**) par défaut. Vous serez ensuite invité à modifier le mot de passe pour des raisons de sécurité.

Une fois connecté, vous pouvez créer des profils pour vos autres utilisateurs. Ces profils définissent les noms et les mots de passe de connexion des utilisateurs. (Reportez-vous à la section ***Création d'un profil utilisateur*** (à la page 42) pour obtenir les instructions correspondantes.)

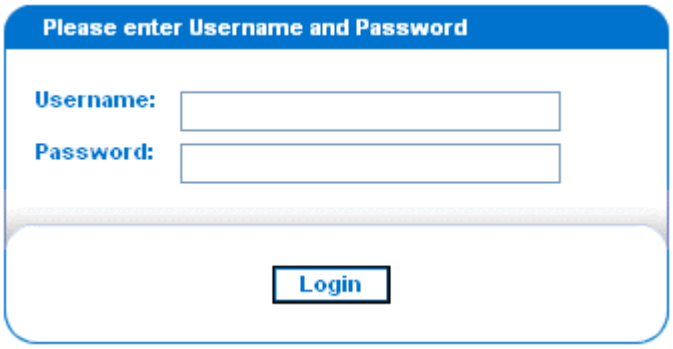
Connexion

➢ *Pour vous connecter à l'interface Web :*

1. Ouvrez un navigateur, tel que Microsoft Internet Explorer ou Mozilla Firefox, et faites-le pointer vers cette URL :

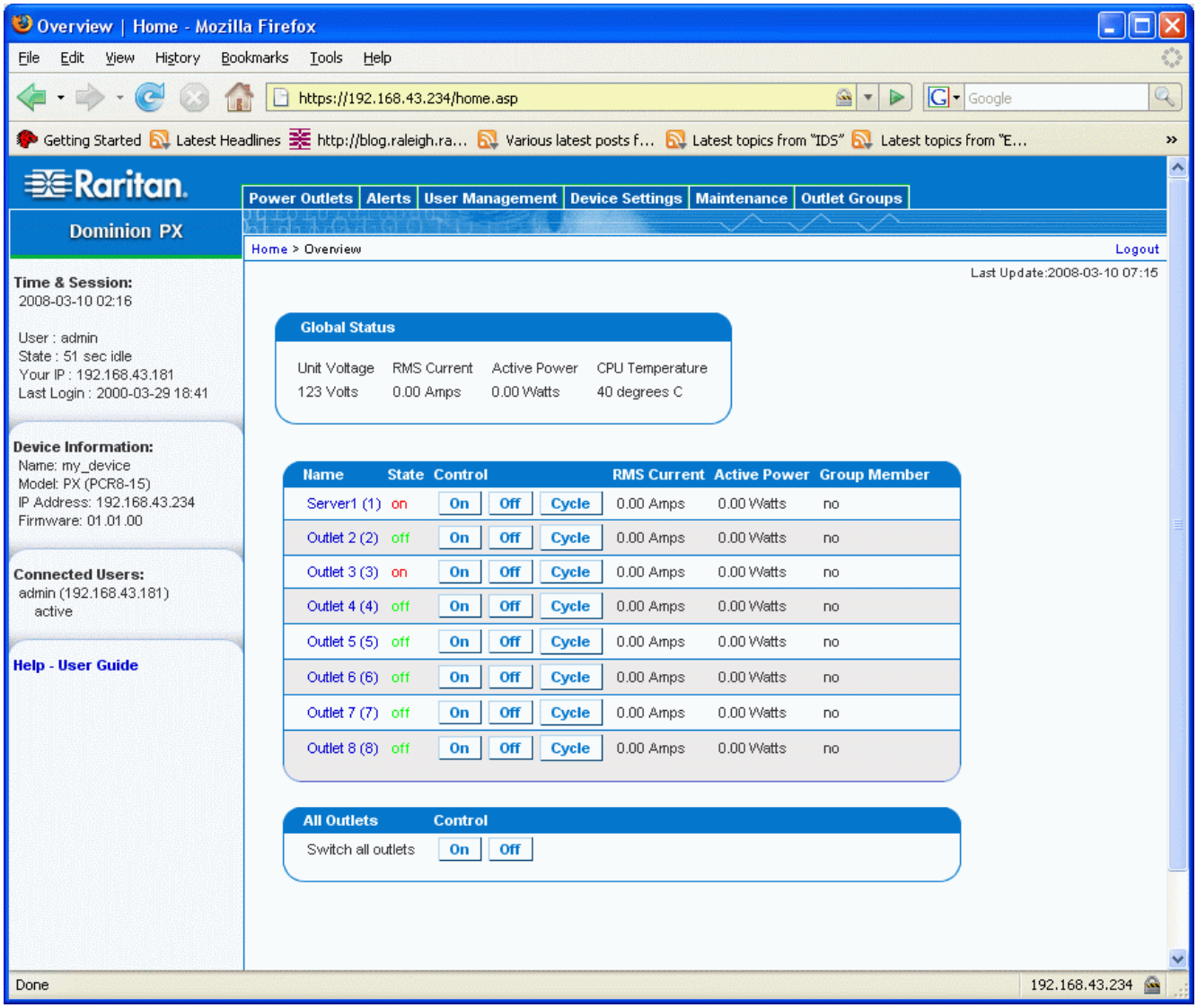
   https://<adresse ip>

où <adresse ip> représente l'adresse IP de la Dominion PX. Une boîte de dialogue de connexion apparaît.



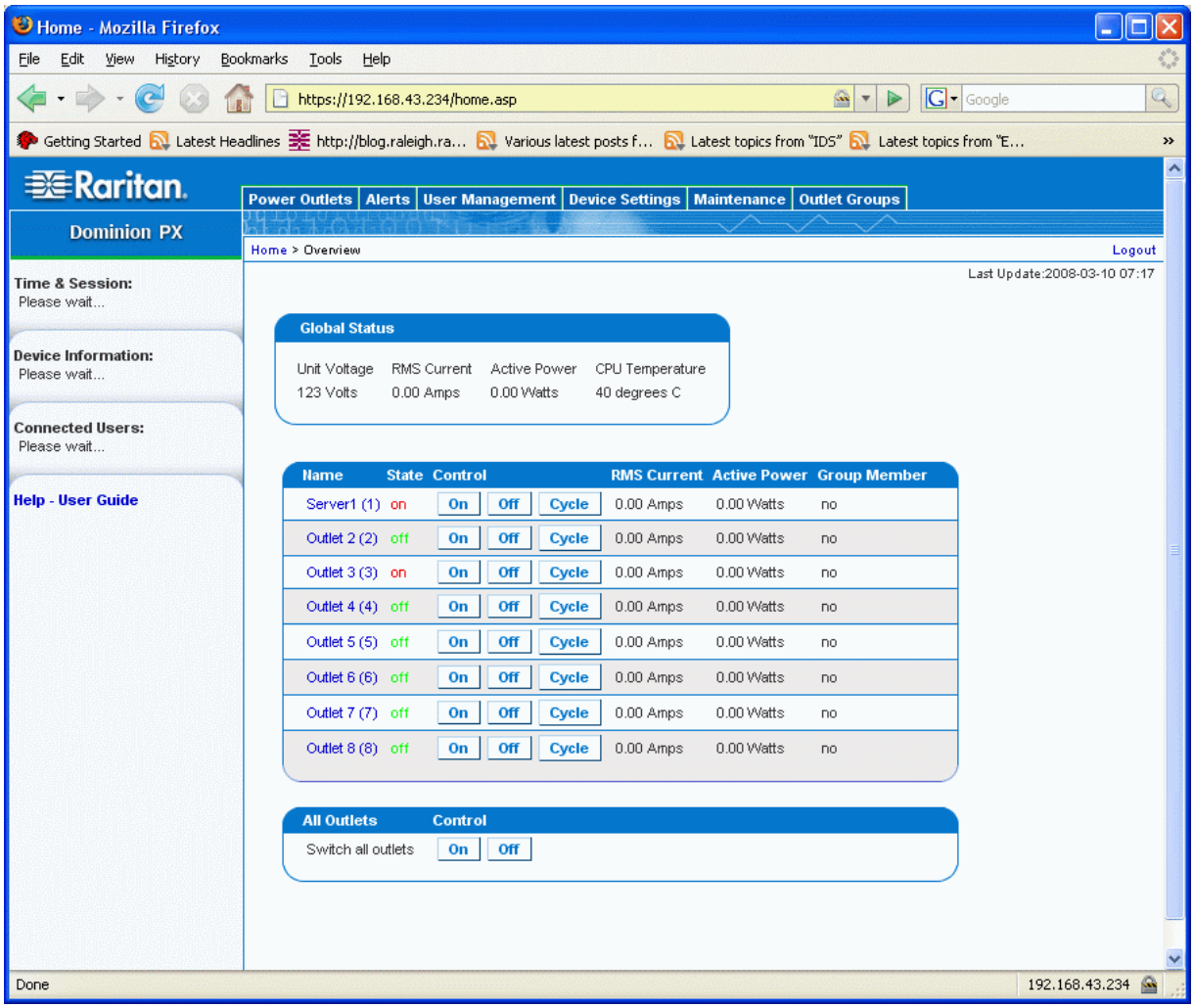
2. Renseignez les champs **Username** (Nom d'utilisateur) et **Password** (Mot de passe). Le nom d'utilisateur et le mot de passe sont sensibles à la casse ; veillez à mettre les bonnes lettres en majuscules.

3. Cliquez sur **Login** (Connexion). La fenêtre d'accueil (Home) s'affiche.



Remarque : la fenêtre d'accueil ci-dessous présente 8 prises. Si votre Dominion PX en compte 20, elles apparaissent toutes les 20 sur la fenêtre d'accueil.

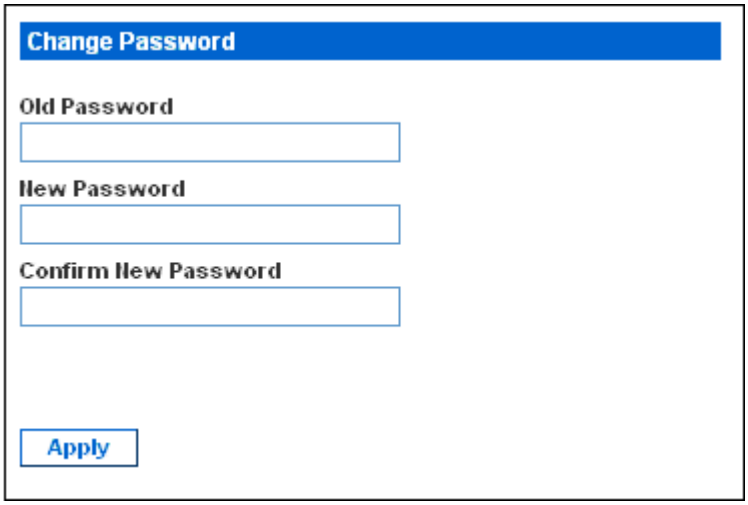
Java Script doit être activé dans le navigateur Web pour un fonctionnement correct. Si Java Script n'est pas activé, les fonctionnalités telles que Status Panel (panneau de statut) sur le côté gauche de l'interface ne s'affiche pas correctement.



Modification de votre mot de passe

➢ *Pour modifier votre mot de passe :*

1. Choisissez **User Management --> Change Password** (Gestion des utilisateurs --> Modifier le mot de passe). La fenêtre Change Password (Modifier le mot de passe) s'affiche.



2. Tapez votre mot de passe actuel dans le champ **Old Password** (Ancien mot de passe).
3. Entrez votre nouveau mot de passe dans les champs **New Password** (Nouveau mot de passe) et **Confirm New Password** (Confirmer le nouveau mot de passe). Les mots de passe sont sensibles à la casse ; veillez à mettre les mêmes lettres en majuscules à chaque fois.
4. Cliquez sur **Apply** (Appliquer). Votre mot de passe a été modifié.

Utilisation de l'interface Web

Chaque fenêtre de l'interface Web présente des menus et un chemin de navigation en haut, et un panneau de statut sur la gauche.

Menus

L'interface Web comporte plusieurs menus, comportant chacun une série d'options propres :

Power Outlets (Prises d'alimentation)

Outlet Details (Détails des prises)

Outlet Setup (Configuration des prises)

Alerts (Alertes)

Alert Configuration (Configuration des alertes)

Alert Policies (Stratégies d'alerte)

Alert Policy Editor (Editeur des stratégies d'alerte)

Alert Destinations (Destinations des alertes)

User Management (Gestion des utilisateurs)

Change Password (Modifier le mot de passe)

Users & Groups (Utilisateurs & groupes)

User / Group System Permissions (Autorisations système pour utilisateur/groupe)

User / Group Outlet Permissions (Autorisations sur les prises pour utilisateur/groupe)

Device Settings (Paramètres du dispositif)

Unit Setup (Configuration de l'unité)

Environmental Sensors (Capteurs d'environnement)

Network (Réseau)

Security (Sécurité)

Certificate (Certificat)

Date / Time (Date/Heure)

Authentication (Authentification)

SMTP Settings (Paramètres SMTP)

SNMP Settings (Paramètres SNMP)

Event Log (Journal des événements)

Maintenance

Device Information (Informations sur le dispositif)

View Event Log (Affichage du journal des événements)

Update Firmware (Mise à niveau du firmware)

Unit Reset (Réinitialisation de l'unité)

Outlet Groups (Groupes de prises)

Outlet Group Details (Détails sur le groupe de prises)

Outlet Group Devices (Dispositifs du groupe de prises)

Outlet Group Editor (Editeur des groupes de prises)

➢ *Pour sélectionner une option :*

Vous pouvez sélectionner une option dans un menu de deux façons :

- Cliquez sur le nom du menu pour afficher une fenêtre répertoriant chaque option, puis cliquez sur l'option souhaitée pour la sélectionner.
- Positionnez le curseur sur le nom du menu. La liste des options se déroule depuis le menu. Faites glisser le curseur jusqu'à l'option souhaitée, puis cliquez dessus pour la sélectionner.

Chemin de navigation

Lorsque vous sélectionnez une option dans un menu et naviguez jusqu'à une fenêtre spécifique, le système affiche en haut de l'affichage un chemin de navigation indiquant le menu et l'option sélectionnés pour arriver à ce point.

Par exemple, si vous choisissez **User Management --> User/Group System Permissions** (Gestion des utilisateurs --> Autorisation système pour utilisateur/groupe), le chemin de navigation ressemble à l'exemple suivant .

Numéro	Description
1	Cliquez ici pour retourner aux fenêtres précédentes.

Pour retourner à une fenêtre précédente, cliquez sur son nom dans le chemin de navigation. Les chemins de navigation débutent systématiquement à la fenêtre **Home** (Accueil), un simple clic suffit donc pour retourner à celle-ci depuis n'importe quel point de l'interface.

Panneau de statut

Le panneau de statut apparaît sur la gauche de chaque fenêtre de l'interface. Il affiche :

- la date et l'heure actuelles
- des informations sur l'utilisateur, notamment :

  le nom d'utilisateur

  l'état actuel de l'utilisateur (actif, inactif, etc.)

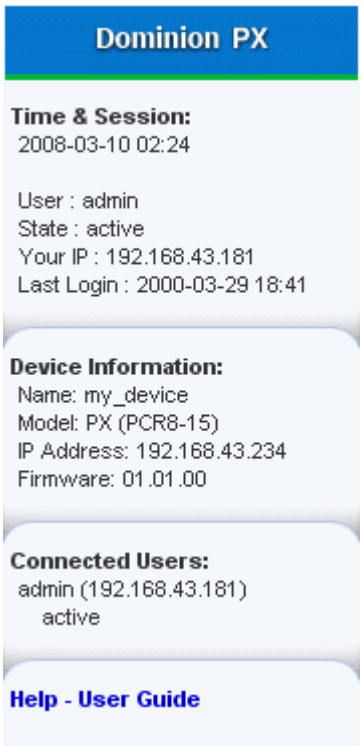
  l'adresse IP de son ordinateur

  la date et l'heure de sa dernière connexion
- des informations sur la Dominion PX, notamment :

  le nom et le numéro de modèle

  l'adresse IP

  la version de firmware
- des informations sur tous les utilisateurs connectés, notamment leur nom d'utilisateur, l'adresse IP et l'état actuel. Votre session en cours est incluse à cette liste.
- un lien vers le manuel d'utilisateur sur le site Web de Raritan.



Le champ **State** (Etat) dans la section des informations utilisateur considère qu'un utilisateur est inactif 30 secondes après la dernière action sur le clavier ou la souris. Il met ensuite à jour la durée d'inactivité toutes les 10 secondes jusqu'à ce qu'une autre action clavier ou souris soit détectée.

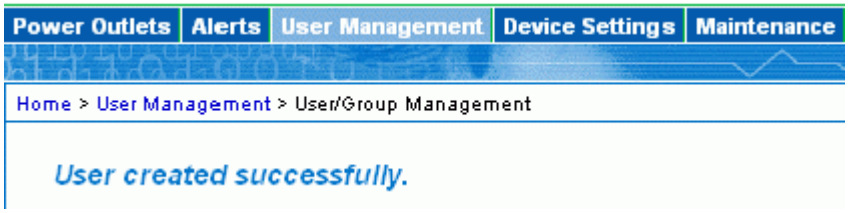
Si vous dépassez le délai d'inactivité, vous serez déconnecté et redirigé automatiquement sur la fenêtre de connexion principale.

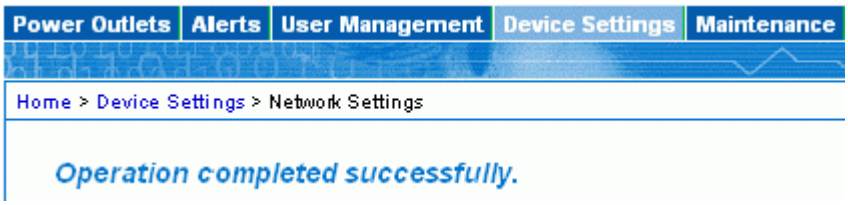
Messages de statut

Lorsque vous effectuez une opération depuis l'interface Web, telle que la création d'un profil utilisateur ou la modification d'un paramètre réseau, un message apparaît en haut de la fenêtre indiquant si l'opération a abouti ou non. Veillez à vérifier ce message pour confirmer la réussite d'une opération.

Messages de réussite

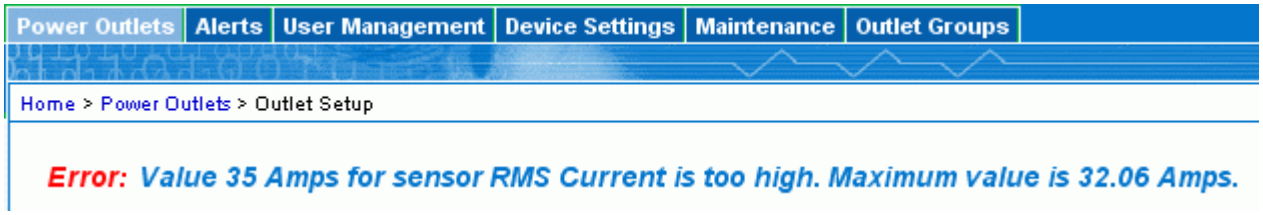
Les exemples suivants présentent des messages de statut après la réussite d'une opération :





Messages d'échec

Les exemples suivants présentent des messages de statut après l'échec d'une opération :



Options non disponibles

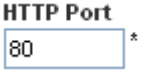
Certaines actions sont parfois indisponibles. Les boutons appropriés sont alors inactifs, même si différents navigateurs peuvent indiquer ceci différemment. Par exemple : si vous sélectionnez le groupe d'utilisateurs Admin dans Internet Explorer, les boutons Copy (Copier), Modify (Modifier) et Delete (Supprimer) sont grisés car ces opérations sont interdites sur le groupe d'utilisateurs Admin. Dans Firefox, en revanche, les boutons apparaissent normalement, mais ne sont pas cliquables.

Reset to Defaults (Réinitialiser aux valeurs par défaut)

De nombreuses fenêtres proposent un bouton **Reset to Defaults** qui rétablit les valeurs par défaut de tous les champs. Si vous utilisez ce bouton, vous devez ensuite cliquer sur **Apply** (Appliquer). Les valeurs par défaut sont ainsi enregistrées. Si vous omettez cette opération, les valeurs modifiées sont toujours présentes lorsque vous retournez à la fenêtre la fois suivante.

Astérisque par défaut

Si un astérisque apparaît après un champ, comme illustré ci-dessous,



ce champ affiche sa valeur par défaut. Si vous modifiez la valeur, l'astérisque disparaît. Si vous rétablissez la valeur par défaut, l'astérisque revient.

Refresh (Actualiser)

De nombreuses fenêtres proposent un bouton **Refresh**. Si une fenêtre est ouverte pendant un certain temps, les informations affichées peuvent devenir « périmées ». Cliquez régulièrement sur ce bouton pour recharger la fenêtre et mettre à jour les informations affichées.

Utilisation de la fenêtre d'accueil

La fenêtre **Home** (Accueil) est la première qui apparaît après la connexion. Elle est constituée d'une zone **Global Status** (Statut global), d'une liste **Outlets** (Prises) et d'un panneau **All Outlets Control** (Contrôle de toutes les prises). La fenêtre d'accueil contient également un panneau des capteurs d'environnement, et d'un horodateur dans l'angle supérieur droit, indiquant la dernière fois où les données à l'écran ont été actualisées.

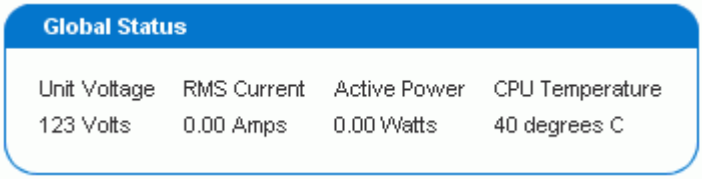
Pour retourner à la fenêtre d'accueil à partir d'une autre dans l'interface Web, cliquez sur :

- le lien **Home** dans le chemin de navigation
- le **logo Raritan** dans l'angle supérieur gauche de la fenêtre
- le nom du modèle de dispositif sous le logo.

Panneau Global Status

Le panneau **Global Status** (Statut global) offre un aperçu de la consommation d'énergie et de la température de la Dominion PX. Il affiche :

- Unit Voltage (Tension de l'unité)
- RMS Current (Courant efficace) (en ampères)
- Active Power (Puissance active) (en watts)
- CPU Temperature (Température du processus) (en degrés Celsius)



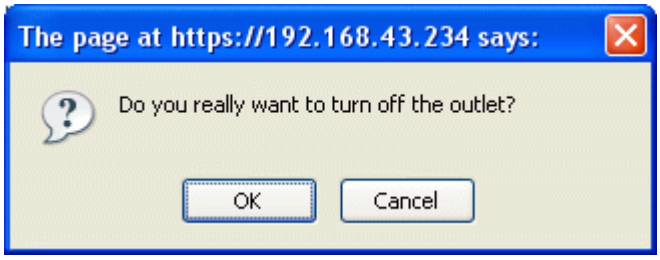
Liste Outlets

La liste **Outlets** (Prises) affiche chaque prise de la Dominion PX sur une rangée de tableau et présente son statut d'alimentation, le courant RMS et la puissance RMS traversant la prise individuelle.

Name	State	Control			RMS Current	Active Power	Group Member
Server1 (1)	on	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 2 (2)	on	On	Off	Cycle	0.00 Amps	0.00 Watts	yes
Outlet 3 (3)	on	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 4 (4)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 5 (5)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 6 (6)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 7 (7)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no
Outlet 8 (8)	off	On	Off	Cycle	0.00 Amps	0.00 Watts	no

Activation, désactivation et alimentation cyclique d'une prise

Pour activer (ON) ou désactiver (OFF) une prise ou effectuer son alimentation cyclique, cliquez sur **On**, **Off** ou **Cycle** dans la rangée de la prise. Pour confirmer votre action, cliquez sur **OK** et la prise sera activée, désactivée ou alimentée cycliquement. Vous pouvez également activer ou désactiver une prise depuis la fenêtre Outlet Details (Détails des prises) (reportez-vous à la figure 49 pour obtenir une représentation de la fenêtre).



Affichage de détails supplémentaires

Pour afficher des détails supplémentaires sur une prise, cliquez sur son nom. La fenêtre Outlet Details (Détails des prises) apparaît (reportez-vous à la figure 49 pour obtenir une représentation de la fenêtre). Cette fenêtre donne le nom et le statut de la prise, ainsi que les éléments suivants :

- RMS Current (Courant efficace)
- Power Factor (Facteur de puissance)
- Maximum RMS Current (Courant efficace maximum)
- RMS Voltage (Tension efficace)
- Active Power (Puissance active)
- Apparent Power (Puissance apparente)

Remarque : RMS fait référence à Root Mean Square (moyenne quadratique), méthode statistique permettant de mesurer certains types de variables. Dans ce contexte, elle donne une valeur de courant ou de tension équivalente à une valeur CC comparable.

All Outlets Control

Le panneau **All Outlets Control** (Contrôle de toutes les prises) au bas de la fenêtre d'accueil vous permet d'activer ou de désactiver toutes les prises. Cliquez sur **On** pour activer toutes les prises, sur **Off** pour les désactiver. Comme pour les prises individuelles, vous devez confirmer la sélection pour qu'elle prenne effet.

Remarque : les utilisateurs doivent être autorisés à accéder à toutes les prises pour se servir du panneau All Outlets Control.

Paramétrage des profils utilisateur

A l'expédition, la Dominion PX intègre un profil utilisateur. Il s'agit du profil Admin utilisé pour la première connexion. Ce profil dispose d'autorisations complètes sur le système et les prises, et doit être réservé à l'administrateur système. Il ne peut être ni modifié ni supprimé.

Tous les utilisateurs doivent avoir un profil. Le profil indique un nom et un mot de passe de connexion, et contient des informations supplémentaires (facultatives) sur l'utilisateur. Il affecte également l'utilisateur à un groupe qui détermine les autorisations au niveau du système et des prises dont dispose l'utilisateur.

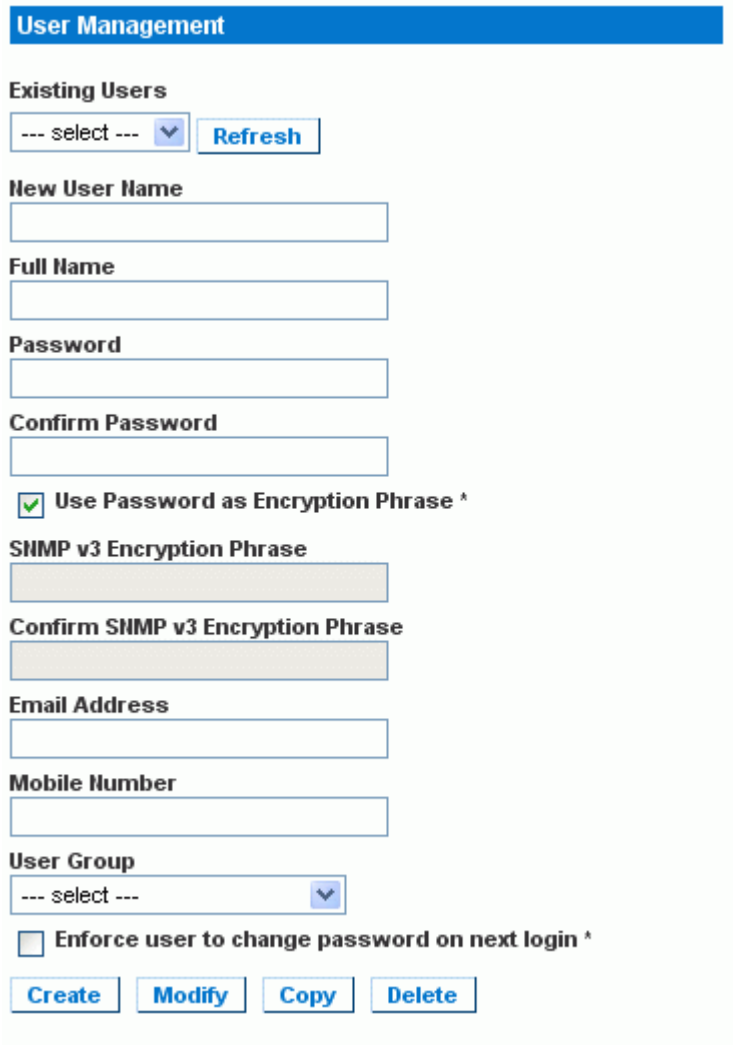
Vous avez la possibilité d'affecter des autorisations individuelles au niveau du système et des prises au lieu d'affecter certains utilisateurs ou tous à un groupe d'utilisateurs.

Remarque : par défaut, plusieurs utilisateurs peuvent se connecter simultanément à l'aide du nom de connexion du même profil. Vous pouvez modifier cette option si un nom de connexion spécifique doit être employé par un seul utilisateur à la fois. Pour ce faire, choisissez ***Device Settings --> Security*** *(Paramètres du dispositif --> Sécurité) et cochez la case* ***Enable Single Login Limitation*** *(Activer la limite de connexion unique).*

Création d'un profil utilisateur

➢ *Pour créer un profil utilisateur :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît. Elle se divise en deux panneaux : **User Management** (Gestion des utilisateurs) et **Group Management** (Gestion des groupes).



Remarque : avant de saisir les données du profil utilisateur, assurez-vous que le groupe d'utilisateurs a été créé et qu'il est disponible à la sélection.

2. Dans le panneau **User Management**, entrez les données suivantes sur l'utilisateur dans les champs correspondants :

Champ	Entrez...
New user name (Nom du nouvel utilisateur)	Le nom que l'utilisateur doit entrer pour se connecter à l'interface Web.
Full Name (Nom complet)	Le prénom et le nom de l'utilisateur

Password (Mot de passe) **Confirm Password (Confirmer le mot de passe)**	Le mot de passe que l'utilisateur doit entrer pour se connecter. Entrez-le d'abord dans le champ **Password** et à nouveau dans le champ **Confirm Password**. Le mot de passe doit comporter au moins quatre caractères et les espaces ne sont pas autorisés. Le mot de passe est sensible à la casse ; veillez à mettre les mêmes lettres en majuscules à chaque fois.
Email address (Adresse électronique)	Une adresse électronique à laquelle l'utilisateur peut être joint.
Mobile number (N° de portable)	Un numéro de téléphone portable auquel l'utilisateur peut être joint.

Remarque : seuls les champs *New user name*, *Password* et *Confirm Password* sont obligatoires.

3. Dans la liste déroulante du champ **User Group** (Groupe d'utilisateurs), effectuez une sélection. Le groupe d'utilisateurs détermine les fonctions système et les prises accessibles à cet utilisateur.
4. Si vous sélectionnez **None** (Néant), l'utilisateur n'est affecté à aucun groupe. Vous devez définir les autorisations de l'utilisateur individuellement. Entretemps, l'accès de l'utilisateur aux fonctions système et aux prises est bloqué. (Pour obtenir des instructions sur la définition des autorisations individuelles, reportez-vous à la section ***Définition des autorisations utilisateur individuelles*** (voir "Paramétrage des autorisations utilisateur individuelles" à la page 46).)
5. Si vous souhaitez que cet utilisateur définisse son propre mot de passe, cochez la case **Enforce user to change password on next login** (Obliger l'utilisateur à changer le mot de passe à la prochaine connexion). L'utilisateur se connecte la première fois à l'aide du mot de passe entré précédemment, puis est obligé de le remplacer par un de son choix.
6. Cliquez sur **Create** (Créer). Le profil utilisateur est créé.

*Remarque : les options **Use Password as Encryption Phrase** (Utiliser le mot de passe comme phrase de chiffrement), **SNMP v3 Encryption Phrase** (Phrase de chiffrement SNMP v3) et **Confirm SNMP Encryption Phrase** (Confirmer la phrase de chiffrement SNMP) ne s'appliquent que si vous utilisez une communication sécurisée SNMP v3. Reportez-vous à l'annexe **Utilisation de SNMP** pour en savoir plus.*

Copie d'un profil utilisateur

Vous pouvez créer un nouveau profil utilisateur doté des mêmes paramètres exactement qu'un profil existant à l'aide de la fonction de copie. Vous pouvez ensuite modifier le profil selon les besoins pour qu'il diffère de l'original. Il s'agit d'une méthode rapide et facile de créer des profils utilisateur.

➢ *Pour copier un profil utilisateur :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.
2. Dans la liste déroulante du champ **Existing Users** (Utilisateurs existants), sélectionnez le profil souhaité.
3. Entrez le nom du nouveau profil utilisateur dans le champ **New User Name** (Nom du nouvel utilisateur).
4. Cliquez sur **Copy** (Copier). Un nouveau profil utilisateur est créé avec les paramètres du profil existant. Pour visualiser le nouveau profil, cliquez sur la liste déroulante du champ **Existing Users**.

Modification d'un profil utilisateur

Chaque utilisateur doté des autorisations de gestion des utilisateurs peut modifier un profil utilisateur. (Reportez-vous à la section ***Définition des autorisations système*** (à la page 48) pour en savoir plus sur la définition des autorisations utilisateur.)

➢ *Pour modifier un profil utilisateur :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.
2. Dans la liste déroulante du champ **Existing Users** (Utilisateurs existants), sélectionnez le profil à modifier. Toutes les informations du profil utilisateur s'affichent hormis le mot de passe.

3. Apportez toutes les modifications nécessaires aux informations affichées. Pour modifier le mot de passe, entrez-en un nouveau dans les champs **Password** (Mot de passe) et **Confirm Password** (Confirmer le mot de passe). Si le champ du mot de passe reste vide, le mot de passe n'est pas modifié.
4. Cliquez sur **Modify** (Modifier). Le profil utilisateur est modifié.

Suppression d'un profil utilisateur

➢ *Pour supprimer un profil utilisateur :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.
2. Dans la liste déroulante du champ **Existing Users** (Utilisateurs existants), sélectionnez le profil à supprimer.
3. Cliquez sur **Delete** (Supprimer). Le profil utilisateur est supprimé.

Paramétrage des autorisations utilisateur individuelles

Si vous avez sélectionné le groupe d'utilisateurs None (Néant) lors de la création du profil utilisateur, vous devez définir des autorisations individuelles. Entretemps, l'accès de l'utilisateur à toutes les fonctions système et prises est bloqué.

Autorisations système

➢ *Pour définir les autorisations système :*

1. Choisissez **User Management --> User/Group System Permissions** (Gestion des utilisateurs --> Autorisations système pour utilisateur/groupe). La fenêtre User/Group System Permissions apparaît (reportez-vous à la figure de la section ***Définition des autorisations système*** (à la page 48)).
2. Dans la liste déroulante du champ **User (not in group)** (Utilisateur (hors groupe)), sélectionnez l'utilisateur. La liste déroulante répertorie tous les profils utilisateur NON affectés à un groupe d'utilisateurs.
3. Définissez les autorisations nécessaires. Cliquez sur l'icône  dans un champ et choisissez **Yes** (Oui) ou **No** (Non).
4. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les autorisations sont appliquées à l'utilisateur.

Autorisations sur les prises

➢ *Pour définir les autorisations sur les prises :*

1. Choisissez **User Management --> User/Group Outlet Permissions** (Gestion des utilisateurs --> Autorisations sur les prises pour utilisateur/groupe). La fenêtre User/Group Outlet Permissions apparaît (reportez-vous à la figure de la section ***Définition des autorisations sur les prises*** (à la page 51)).
2. Dans la liste déroulante du champ **User** (Utilisateur), sélectionnez l'utilisateur.
3. Définissez les autorisations nécessaires. Cliquez sur l'icône dans un champ et choisissez **Yes** (Oui) ou **No** (Non).
4. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les autorisations sont appliquées à l'utilisateur.

Remarque : un « utilisateur » doté d'un niveau de privilèges IPMI au moins est requis pour permuter les prises via IPMI, ce qui n'a aucun effet sur l'utilisation de l'interface Web frontale. Toutefois, le niveau de privilèges n'a aucun rapport avec les autorisations sur les prises.

Paramétrage des groupes d'utilisateurs

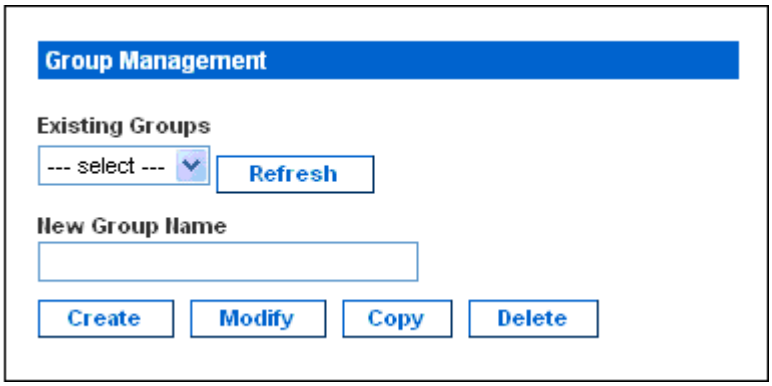
A l'expédition, la Dominion PX intègre un groupe d'utilisateurs. Il s'agit du groupe d'utilisateurs **Admin**. Ce groupe d'utilisateurs accorde des autorisations complètes sur le système et les prises. Il ne peut être ni modifié ni supprimé.

Lors de la création des profils utilisateur, le champ **User Group** (Groupe d'utilisateurs) indique par défaut **Admin**. Si vous ne modifiez pas la valeur de ce champ, l'utilisateur disposera d'un accès total au système et aux prises. Pour restreindre les autorisations de l'utilisateur, créez un groupe disposant d'un accès limité au système et/ou aux prises et affectez l'utilisateur à ce groupe.

Création d'un groupe d'utilisateurs

➢ *Pour créer un groupe d'utilisateurs :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît. Elle se divise en deux panneaux : **User Management** (Gestion des utilisateurs) et **Group Management** (Gestion des groupes).



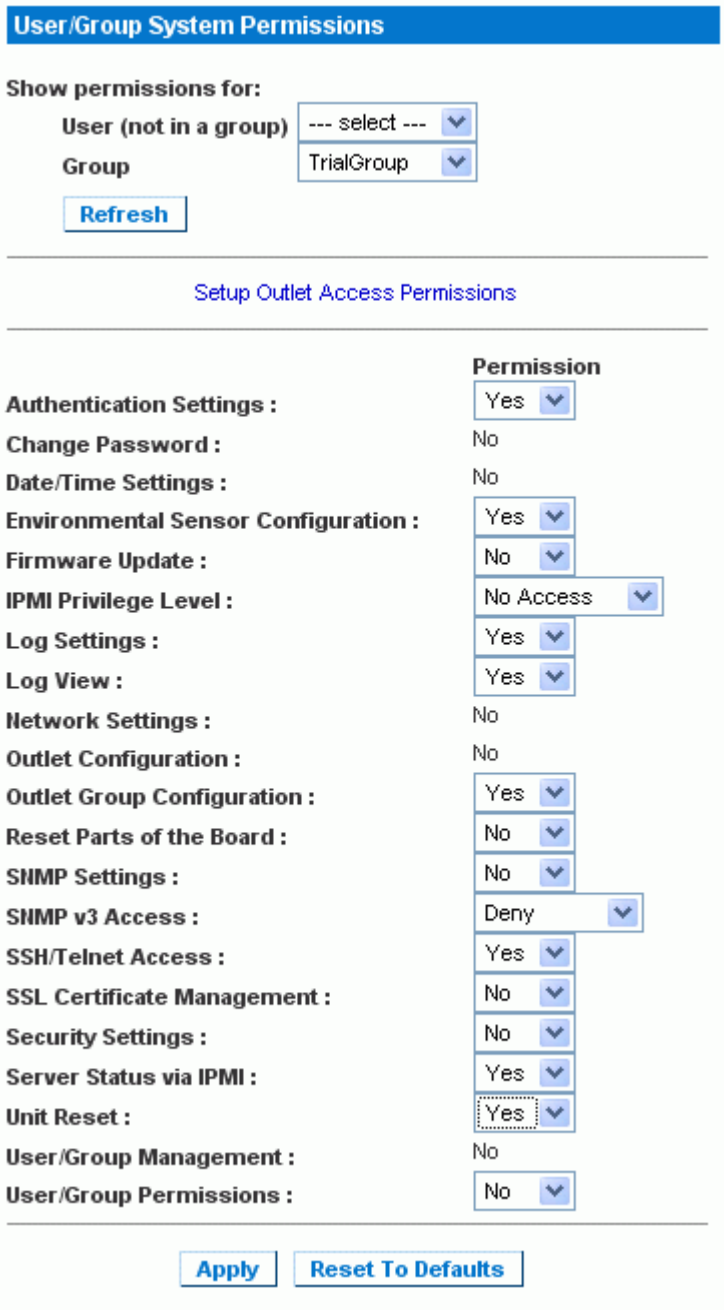
2. Dans le panneau **Group Management**, entrez le nom du groupe dans le champ **New Group Name** (Nom du nouveau groupe).
3. Cliquez sur **Create** (Créer). Le groupe d'utilisateurs est créé.

Définition des autorisations système

Les autorisations système incluent toutes les zones fonctionnelles principales de l'interface Web. Lorsque vous créez un groupe d'utilisateurs, toutes les autorisations système sont définies sur NO (Non).

➢ *Pour définir les autorisations système d'un groupe d'utilisateurs :*

1. Choisissez **User Management --> User/Group System Permissions** (Gestion des utilisateurs --> Autorisations système pour utilisateur/groupe). La fenêtre User/Group System Permissions apparaît.



2. Dans la liste déroulante du champ **Group** (Groupe), sélectionnez le groupe d'utilisateurs. Les autorisations applicables à ce groupe s'affichent. Si vous n'avez pas encore défini les autorisations de ce groupe, toutes les autorisations indiquent **No**.
3. Définissez les autorisations nécessaires. Cliquez sur l'icône dans un champ et sélectionnez **Yes** (Oui) ou **No** (Non).

4. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les autorisations sont appliquées au groupe d'utilisateurs.

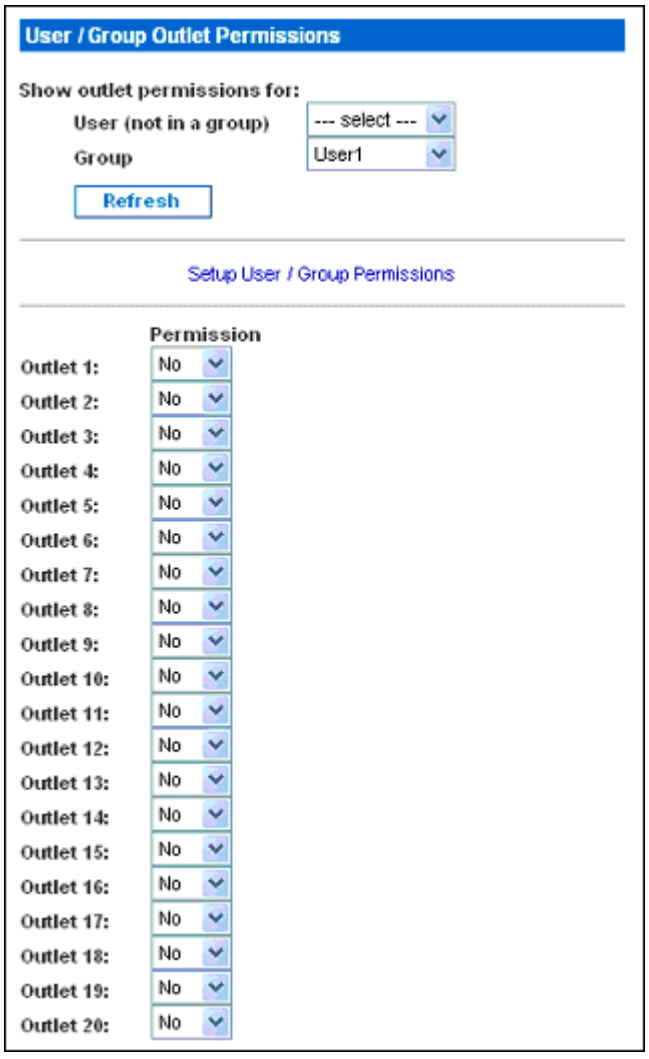
Remarque : le champ User (not in group) (Utilisateur (hors groupe)) de cette fenêtre permet de définir des autorisations utilisateur individuelles. Si vous définissez des autorisations de groupe, vous pouvez omettre ce champ.

Définition des autorisations sur les prises

La définition des autorisations sur les prises vous permet d'indiquer les prises accessibles aux membres d'un groupe d'utilisateurs. Lorsque vous créez un groupe d'utilisateurs, toutes les autorisations sur les prises sont définies sur NO (Non).

➢ *Pour définir les autorisations sur les prises d'un groupe d'utilisateurs :*

1. Choisissez **User Management --> User/Group Outlet Permissions** (Gestion des utilisateurs --> Autorisations sur les prises pour utilisateur/groupe). La fenêtre User/Group Outlet Permissions apparaît.



2. Dans la liste déroulante du champ **Group** (Groupe), sélectionnez le groupe d'utilisateurs. Les autorisations applicables à ce groupe s'affichent. Si vous n'avez pas encore défini les autorisations de ce groupe, toutes les autorisations indiquent **No**.
3. Définissez les autorisations nécessaires. Cliquez sur l'icône  dans un champ et sélectionnez **Yes** (Oui) ou **No** (Non).
4. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les autorisations sont appliquées au groupe d'utilisateurs.

Remarque : le champ User (Utilisateur) de cette fenêtre permet de définir des autorisations utilisateur individuelles. Si vous définissez des autorisations de groupe, vous pouvez omettre ce champ.

Copie d'un groupe d'utilisateurs

Vous pouvez créer un nouveau groupe d'utilisateurs doté des mêmes paramètres exactement qu'un groupe existant à l'aide de la fonction de copie. Vous pouvez ensuite modifier le groupe pour que ses autorisations diffèrent de l'original selon les besoins. Il s'agit d'une méthode rapide et facile de créer des groupes d'utilisateurs.

➢ *Pour copier un groupe d'utilisateurs :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.
2. Dans la liste déroulante du champ **Existing Groups** (Groupes existants), sélectionnez le **groupe d'utilisateurs**.
3. Entrez le nom du nouveau groupe d'utilisateurs dans le champ **New Group Name** (Nom du nouveau groupe).
4. Cliquez sur **Copy** (Copier). Un nouveau groupe d'utilisateurs est créé avec les autorisations du groupe existant. Pour visualiser le nouveau groupe, cliquez sur la liste déroulante du champ **Existing Groups**.

Modification d'un groupe d'utilisateurs

Le seul attribut modifiable d'un groupe d'utilisateurs est son nom.

➢ *Pour modifier le nom d'un groupe d'utilisateurs :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.

2. Dans la liste déroulante du champ **Existing groups** (Groupes existants), sélectionnez le groupe d'utilisateurs à modifier. Le nom apparaît dans le champ **New group name** (Nom du nouveau groupe).
3. Apportez les modifications nécessaires au nom.
4. Cliquez sur **Modify** (Modifier). Le groupe d'utilisateurs est modifié.

Remarque : pour modifier les autorisations sur le système et les prises d'un groupe d'utilisateurs, répétez la procédure de définition des autorisations décrite précédemment et apportez les modifications nécessaires.

Suppression d'un groupe d'utilisateurs

➢ *Pour supprimer un groupe d'utilisateurs :*

1. Choisissez **User Management --> Users & Groups** (Gestion des utilisateurs --> Utilisateurs & groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.
2. Dans la liste déroulante du champ **Existing groups** (Groupes existants), sélectionnez le groupe d'utilisateurs à supprimer.
3. Cliquez sur **Delete** (Supprimer). Le groupe d'utilisateurs est supprimé.

Paramétrage des contrôles d'accès

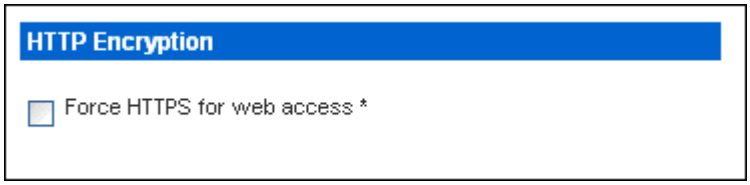
La Dominion PX propose plusieurs d'outils pour contrôler l'accès à l'unité. Vous pouvez exiger le chiffrement HTTPS, activer le pare-feu interne et créer des règles le concernant, et limiter le nombre de connexions.

Chiffrement HTTPS imposé

HTTPS constitue un protocole plus sûr que HTTP car il utilise la technologie SSL (Secure Sockets Layer) pour chiffrer tout le trafic vers et depuis la Dominion PX.

➢ *Pour obliger les utilisateurs à employer HTTPS au lieu d'HTTP lors de l'accès à la Dominion PX via l'interface Web :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau en haut à gauche est libellé **HTTP Encryption** (Chiffrement HTTP).



2. Cochez la case libellée **Force HTTPS for web access** (Forcer HTTPS pour l'accès Web).
3. Cliquez sur **Apply** (Appliquer). HTTPS est maintenant obligatoire pour l'accès par navigateur.

Remarque : les tentatives d'utilisation d'HTTP ne seront automatiquement redirigées vers HTTPS que si l'option Force HTTPS for web access est cochée.

Configuration du pare-feu

L'unité Dominion PX est dotée d'un pare-feu configurable pour interdire son accès à des adresses IP et à des plages d'adresses IP spécifiques. Lors de la configuration initiale de la Dominion PX, vous avez été invité à activer ou désactiver le contrôle d'accès par IP. Si vous avez sélectionné Disable (Désactiver) (valeur par défaut), le pare-feu de la Dominion PX n'a pas été activé.

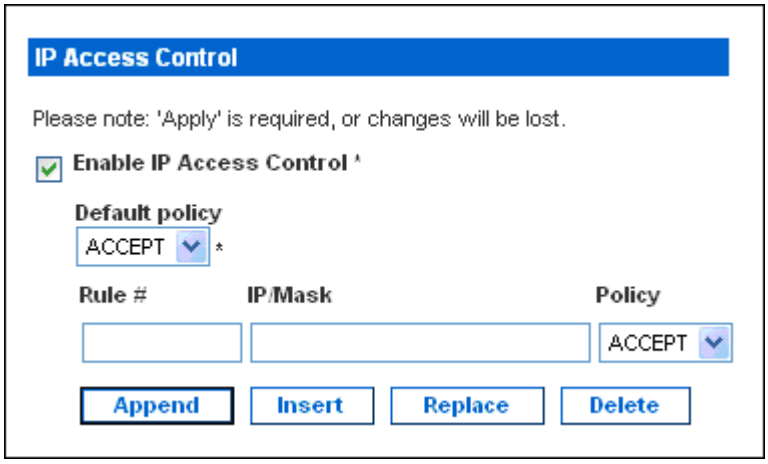
Pour configurer le pare-feu, vous devez l'activer, définir ensuite la stratégie par défaut et créer des règles indiquant les adresses à accepter et à refuser. Les modifications apportées aux règles du pare-feu prennent immédiatement effet. Les activités IP non autorisées cessent instantanément.

Remarque : la désactivation du pare-feu par défaut a pour but d'empêcher les utilisateurs de bloquer accidentellement leur accès à l'unité. Reportez-vous au chapitre **Installation et configuration** *(à la page 10) pour en savoir plus.*

Activation du pare-feu

➢ *Pour activer le pare-feu de la Dominion PX :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau en haut à droite est libellé IP Access Control (Contrôle d'accès par IP). Le pare-feu est contrôlé par ce biais.



2. Cochez la case libellée **Enable IP Access Control** (Activer le contrôle d'accès par IP). Cette option active le pare-feu.
3. Cliquez sur **Apply** (Appliquer). Le pare-feu est activé.

Modification de la stratégie par défaut

Une fois activé, le pare-feu dispose d'une stratégie par défaut intégrée qui accepte le trafic de toutes les adresses IP. Ceci signifie que toute adresse IP non refusée par une règle spécifique est autorisée à accéder à la Dominion PX. Vous pouvez remplacer la stratégie par défaut par DROP ; le trafic de toutes les adresses IP sera refusé, hormis celui autorisé par une règle ACCEPT spécifique.

➢ *Pour modifier la stratégie par défaut :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau en haut à droite est libellé **IP Access Control** (Contrôle d'accès par IP). Le pare-feu est contrôlé par ce biais.
2. Assurez-vous que la case libellée **Enable IP Access Control** (Activer le contrôle d'accès par IP) est cochée.
3. La stratégie par défaut apparaît dans le champ **Default Policy** (Stratégie par défaut) (voir la figure précédente). Pour modifier cette valeur, sélectionnez la stratégie souhaitée dans la liste déroulante du champ.
4. Cliquez sur **Apply** (Appliquer). La nouvelle stratégie par défaut est appliquée.

Création des règles du pare-feu

Les règles du pare-feu acceptent ou refusent le trafic destiné à la Dominion PX en fonction de l'adresse IP de l'hôte émetteur. Lors de la création des règles du pare-feu, gardez les points suivants à l'esprit :

- **Ordre des règles** L'ordre des règles est important. Lorsque le trafic parvient à l'unité Dominion PX, les règles sont exécutées dans l'ordre numérique. La première règle correspondant à l'adresse IP détermine si le trafic est accepté ou refusé. Les règles suivantes correspondant à l'adresse IP n'ont aucun effet sur le trafic.
- **Masque de sous-réseau** Lors de la saisie de l'adresse IP, vous DEVEZ indiquer l'adresse et le masque de sous-réseau. Par exemple, pour indiquer une adresse unique dans un réseau de classe C, utilisez le format suivant :

  x.x.x.x/24

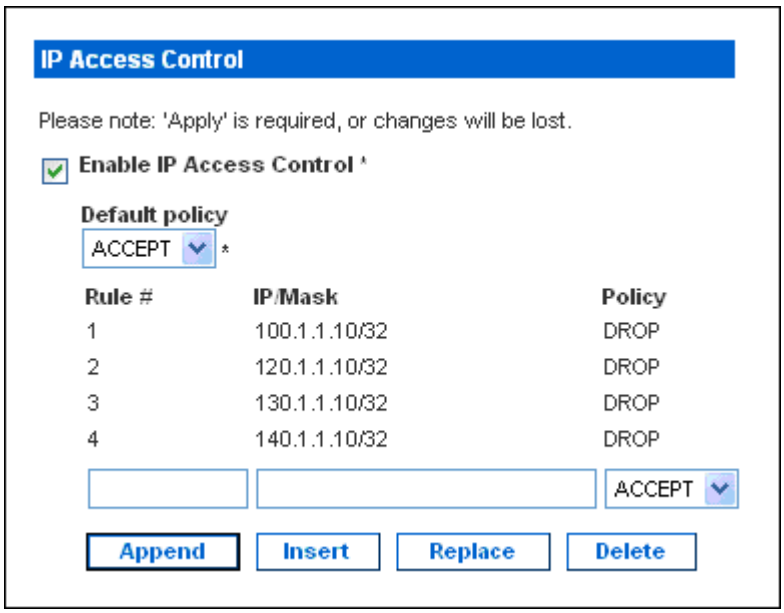
  où /24 = un masque de sous-réseau de 255.255.255.0. Pour indiquer un sous-réseau entier ou une plage d'adresses, modifiez le masque de sous-réseau en conséquence.

➢ *Pour créer des règles de pare-feu :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau en haut à droite est libellé **IP Access Control** (Contrôle d'accès par IP). Le pare-feu est contrôlé par ce biais.
2. Assurez-vous que la case libellée **Enable IP Access Control** (Activer le contrôle d'accès par IP) est cochée.

Action	Procédure
Ajouter une règle à la fin de la liste des règles	• Entrez une adresse IP et un masque de sous-réseau dans le champ **IP/Mask** (IP/Masque). • Sélectionnez **ACCEPT** (Accepter) ou **DROP** (Refuser) dans le champ **Policy** (Stratégie). • Cliquez sur **Append** (Ajouter). N'ENTREZ PAS de numéro de règle. Le système numérote automatiquement la règle.
Insérer une règle entre deux autres	• Entrez le numéro de la règle au-dessus de laquelle vous souhaitez insérer la nouvelle dans le champ **Rule #** (Numéro de règle). Par exemple, pour insérer une règle entre les règles 5 et 6, entrez **6**. • Entrez une adresse IP et un masque de sous-réseau dans le champ **IP/Mask** (IP/Masque). • Sélectionnez **ACCEPT** (Accepter) ou **DROP** (Refuser) dans la liste déroulante du champ **Policy** (Stratégie). • Cliquez sur **Insert** (Insérer). Le système insère la règle et renumérote automatiquement les règles.
Remplacer une règle existante	• Entrez le numéro de la règle à remplacer dans le champ **Rule #** (Numéro de règle). • Entrez une adresse IP et un masque de sous-réseau dans le champ **IP/Mask** (IP/Masque). • Sélectionnez **ACCEPT** (Accepter) ou **DROP** (Refuser) dans la liste déroulante du champ **Policy** (Stratégie). • Cliquez sur **Replace** (Remplacer). Le système remplace la règle existante par celle que vous venez de créer.

1. Lorsque vous avez terminé, les règles s'affichent dans le panneau IP Access Control (Contrôle d'accès par IP) comme illustré ci-dessous.



2. Cliquez sur **Apply** (Appliquer). Les règles sont appliquées.

Suppression des règles du pare-feu

➢ *Pour supprimer une règle de pare-feu :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche.
2. Assurez-vous que la case libellée **Enable IP Access Control** (Activer le contrôle d'accès par IP) est cochée.
3. Entrez le numéro de la règle à supprimer dans le champ **Rule #** (Numéro de règle).
4. Cliquez sur **Delete** (Supprimer). La règle est retirée du panneau **IP Access Control** (Contrôle d'accès par IP).
5. Cliquez sur **Apply** (Appliquer). La règle est supprimée.

Création de règles de contrôle d'accès basé groupe

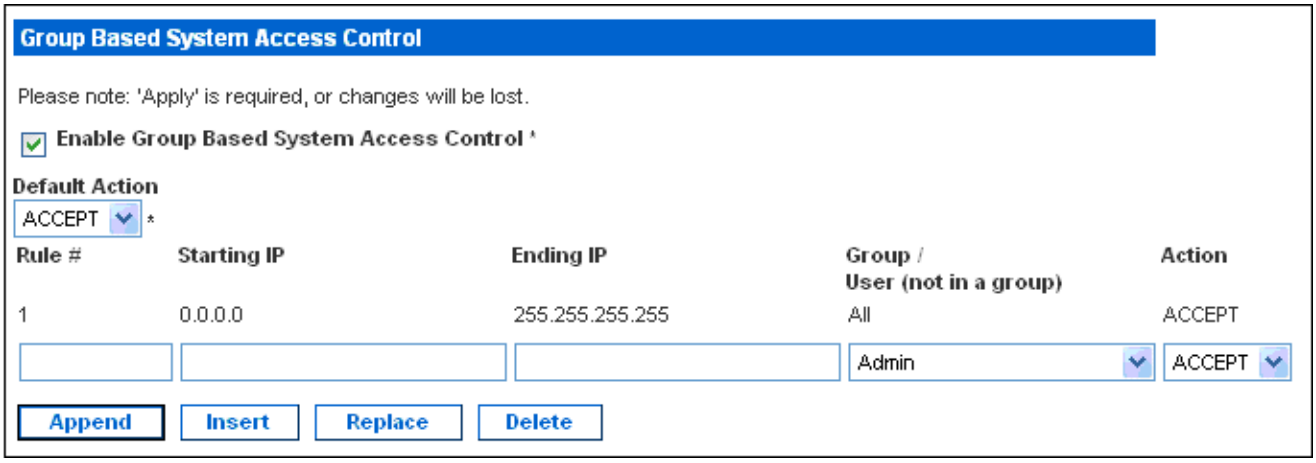
Les règles de contrôle d'accès basé groupe sont similaires aux règles de pare-feu, hormis le fait qu'elles sont applicables aux membres de groupes d'utilisateurs spécifiques. En fait, cette fonction vous permet d'accorder à des groupes d'utilisateurs entiers des autorisations sur le système et les prises en fonction de leurs adresses IP ou de leurs sous-réseaux.

Pour créer des règles de contrôle d'accès basé groupe, vous devez d'abord activer la fonction. Vous devez ensuite définir l'action par défaut, indiquer une fourchette d'adresses IP et associer la règle à un groupe d'utilisateurs spécifique. Enfin, vous devez indiquer si la règle accepte ou refuse le trafic. Toutefois, les modifications apportées n'affecteront les utilisateurs actuellement connectés qu'à l'ouverture de session suivante.

Activation de la fonction

➢ *Pour activer les règles de contrôle d'accès basé groupe :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau **Group Based System Access Control** (Contrôle d'accès système basé groupe) contrôle cette fonction.



2. Cochez la case libellée **Enable Group Based System Access Control** (Activer le contrôle d'accès système basé groupe). Cette option active la fonction.
3. Cliquez sur **Apply** (Appliquer). Les règles de contrôle d'accès basé groupe sont activées.

Modification de l'action par défaut

L'action par défaut apparaît dans le panneau Group Based System Access Control (Contrôle d'accès système basé groupe) de la fenêtre Security Settings (Paramètres de sécurité).

➢ *Pour modifier l'action par défaut :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau **Group Based System Access Control** (Contrôle d'accès système basé groupe) contrôle cette fonction.
2. Assurez-vous que la case libellée **Enable Group Based System Access Control** (Activer le contrôle d'accès système basé groupe) est cochée.
3. Sélectionnez l'action souhaitée dans la liste déroulante du champ **Default Action** (Action par défaut) (reportez-vous à la figure précédente).
4. Cliquez sur **Apply** (Appliquer). L'action par défaut est appliquée.

Création de règles de contrôle d'accès basé groupe

Les règles de contrôle d'accès basé groupe acceptent ou refusent le trafic destiné à la Dominion PX en fonction de l'appartenance de l'utilisateur à un groupe. Comme pour les règles de pare-feu, la position de la règle est importante car les règles sont exécutées dans l'ordre numérique.

➢ *Pour créer des règles de contrôle d'accès basé groupe :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau **Group Based System Access Control** (Contrôle d'accès système basé groupe) contrôle cette fonction.
2. Assurez-vous que la case libellée **Enable Group Based System Access Control** (Activer le contrôle d'accès système basé groupe) est cochée.
3. Créez ou supprimez des règles spécifiques. Le tableau suivant explique comment :

Action	Procédure
Ajouter une règle à la fin de la liste des règles	• Entrez une adresse IP de début dans le champ **Starting IP** (IP de début). • Entrez une adresse IP de fin dans le champ **Ending IP** (IP de fin). • Dans la liste déroulante du champ **Group** (Groupe), sélectionnez un groupe d'utilisateurs. Cette règle ne s'applique qu'aux membres de ce groupe. • Sélectionnez **ACCEPT** (Accepter) ou **DROP** (Refuser) dans la liste déroulante du champ **Policy** (Stratégie). • Cliquez sur **Append** (Ajouter). N'ENTREZ PAS de numéro de règle. Le système numérote automatiquement la règle.
Insérer une règle entre deux autres	• Entrez le plus élevé des numéros des deux règles dans le champ **Rule #** (Numéro de règle). Par exemple, pour insérer une règle entre les règles 5 et 6, entrez **6**. • Entrez une adresse IP de début dans le champ **Starting IP** (IP de début). • Entrez une adresse IP de fin dans le champ **Ending IP** (IP de fin). • Sélectionnez **ACCEPT** (Accepter) ou **DROP** (Refuser) dans la liste déroulante du champ **Action**. • Cliquez sur **Insert** (Insérer). Le système insère la règle et renumérote automatiquement les règles.
Remplacer une règle existante	• Entrez le numéro de la règle à remplacer dans le champ **Rule #** (Numéro de règle). • Entrez une adresse IP et un masque de sous-réseau dans le champ **IP/Mask** (IP/Masque). • Sélectionnez **ACCEPT** (Accepter) ou **DROP** (Refuser) dans la liste déroulante du champ **Action**. • Cliquez sur **Replace** (Remplacer). Le système remplace la règle existante par celle que vous venez de créer.

1. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les règles sont appliquées.

Suppression des règles de contrôle d'accès basé groupe

➢ *Pour supprimer une règle de contrôle d'accès basé groupe :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche.
2. Assurez-vous que la case libellée **Enable Group Based System Access Control** (Activer le contrôle d'accès système basé groupe) est cochée.
3. Entrez le numéro de la règle à supprimer dans le champ **Rule #** (Numéro de règle).
4. Cliquez sur **Delete** (Supprimer). La règle est retirée du panneau **Group Based System Access Control** (Contrôle d'accès système basé groupe).
5. Cliquez sur **Apply** (Appliquer). La règle est supprimée.

Paramétrage des contrôles de connexion des utilisateurs

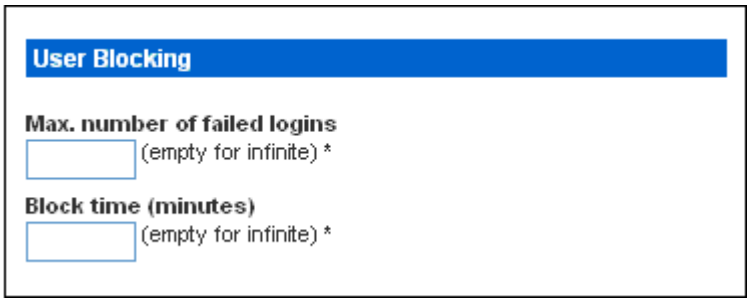
Vous pouvez paramétrer des contrôles de connexion pour empêcher les pirates d'accéder à la Dominion PX et aux dispositifs branchés dessus. Vous pouvez choisir de bloquer des individus après un nombre spécifique d'échecs de connexion, limiter le nombre d'utilisateurs connectés simultanément à l'aide des mêmes données de connexion et obliger les utilisateurs à créer des mots de passe forts.

Activer le blocage des utilisateurs

Le blocage des utilisateurs vous permet de déterminer le nombre de fois où un utilisateur peut tenter de se connecter à la Dominion PX et où l'authentification peut échouer avant que l'utilisateur ne soit bloqué.

➢ *Pour activer le blocage des utilisateurs :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau User Blocking (Blocage des utilisateurs) contrôle cette fonction.



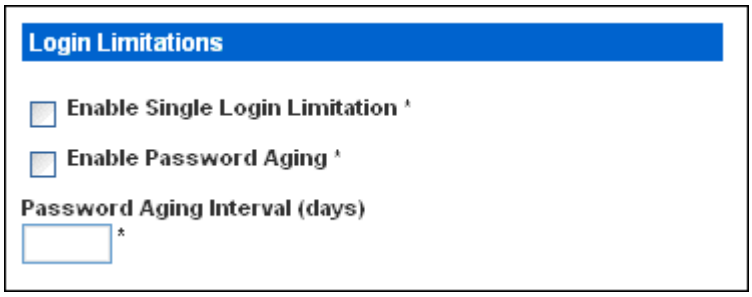
2. Entrez un nombre dans le champ **Max. number of failed logins** (Nombre max. d'échecs de connexion). Il s'agit du nombre maximum d'échecs de connexion autorisé à l'utilisateur avant que l'accès à la Dominion PX ne soit bloqué à ses données de connexion. Si le champ est laissé vide, le nombre d'échecs de connexion n'est pas limité.
3. Entrez un nombre dans le champ **Block time** (Durée de blocage). Il s'agit de la durée en minutes pendant laquelle les données de connexion sont bloquées.
4. Cliquez sur **Apply** (Appliquer). Les limites de blocage des utilisateurs sont appliquées.

Activation des limites de connexion

Les limites de connexion vous permettent de déterminer si plusieurs individus peuvent utiliser les mêmes données de connexion simultanément, et si les utilisateurs doivent modifier leur mot de passe à intervalles réguliers programmés.

➢ *Pour activer les limites de connexion :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau Login Limitations (Limites de connexion) contrôle cette fonction.



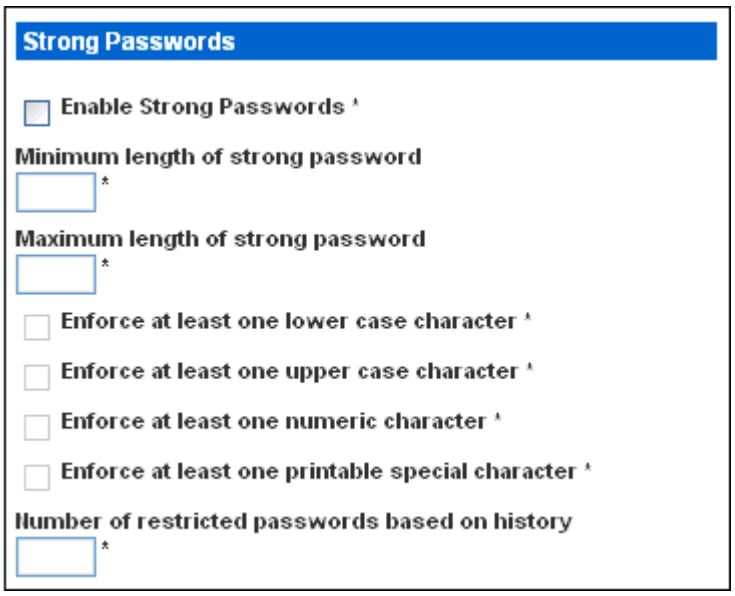
2. Pour empêcher à plusieurs personnes d'utiliser les mêmes données de connexion simultanément, cochez la case libellée **Enable Single Login Limitation** (Activer la limite de connexion unique).
3. Pour obliger les utilisateurs à modifier leur mot de passe régulièrement, cochez la case libellée **Enable Password Aging** (Activer le vieillissement des mots de passe), puis entrez un nombre de jours dans le champ **Password Aging Interval** (Intervalle de vieillissement des mots de passe). Les utilisateurs devront modifier leur mot de passe chaque fois que le nombre de jours est écoulé.
4. Cliquez sur **Apply** (Appliquer). Les contrôles sont appliqués.

Activation des mots de passe forts

La création imposée de mots de passe forts empêche aux intrus de découvrir les mots de passe des utilisateurs et d'accéder à l'unité Dominion PX. Les mots de passe forts doivent comporter au moins huit caractères, contenir des lettres majuscules et minuscules, des chiffres et des caractères spéciaux (tels que @ ou &).

➢ *Pour obliger les utilisateurs à créer des mots de passe forts :*

1. Choisissez **Device Settings --> Security** (Paramètres du dispositif --> Sécurité). La fenêtre Security Settings (Paramètres de sécurité) s'affiche. Le panneau Strong Passwords (Mots de passe forts) apparaît au bas de la fenêtre.



2. Cochez la case libellée **Enable Strong Passwords** (Activer les mots de passe forts) pour activer la fonction de mots de passe forts. Les paramètres par défaut sont les suivants :

Longueur minimum	= 8 caractères
Longueur maximum	= 16 caractères
Au moins un caractère en minuscule	= Obligatoire
Au moins un caractère en majuscules	= Obligatoire
Au moins un caractère numérique	= Obligatoire

Au moins un caractère spécial imprimable	= Obligatoire
Nombre de mots de passe interdits	= 5

3. Apportez les modifications nécessaires aux paramètres par défaut.
4. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les modifications sont appliquées.

Paramétrage d'un certificat numérique

L'objet d'un certificat numérique X.509 est d'assurer que les deux parties d'une connexion SSL sont authentiques. Pour obtenir un certificat pour la Dominion PX, vous devez créer une demande de signature de certificat et la soumettre à une autorité de certification.

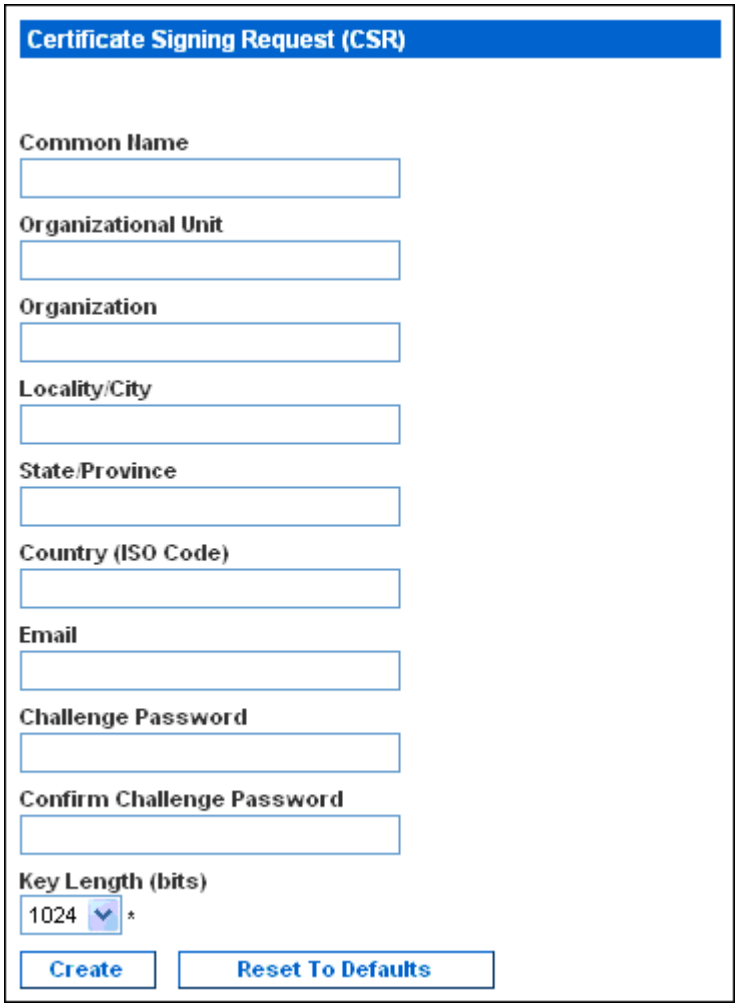
Une fois les données de la demande traitée par l'autorité, un certificat vous est fourni et vous devez l'installer sur la Dominion PX.

Remarque : reportez-vous à **Chiffrement HTTPS imposé** *(à la page 54) pour savoir comment imposer aux utilisateurs l'emploi de SSL lors de la connexion à la Dominion PX.*

Création d'une demande de signature de certificat

➢ *Pour créer une demande de signature de certificat :*

1. Choisissez **Device Settings --> Certificate** (Paramètres du dispositif --> Certificat). La première page de la fenêtre SSL Server Certificate Management (Gestion des certificats du serveur SSL) apparaît.



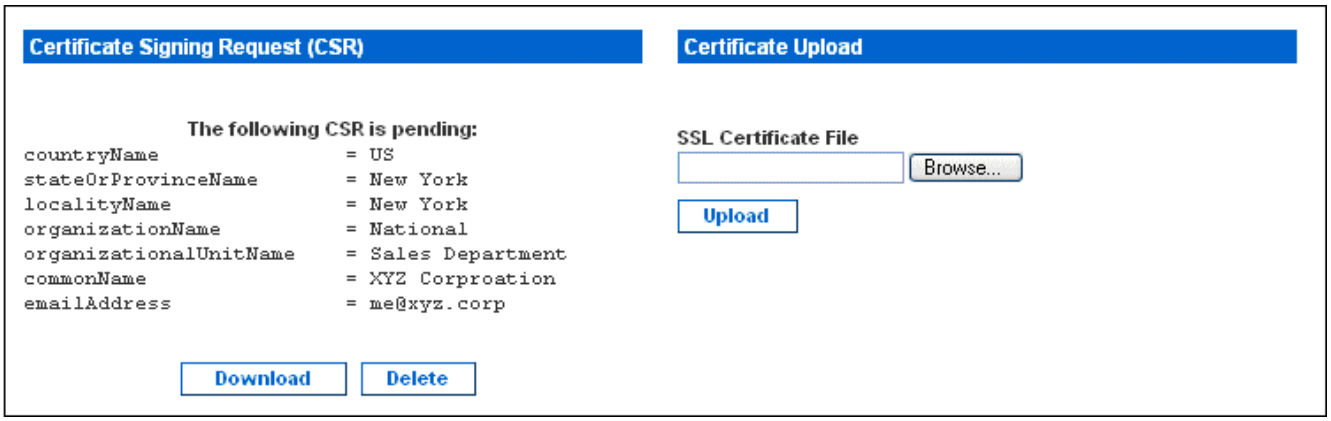
2. Donnez les informations demandées. Entrez les valeurs suivantes dans les champs appropriés :

Champ	Entrez...
Common name (Nom courant)	Le nom de votre société

Organization unit (Service)	Le nom de votre service
Organization (Organisation)	Le nom de votre organisation au sein du service
Locality/City (Localité/Ville)	La ville où se situe votre société
State/Province (Etat/Province)	L'Etat ou la province où se situe votre société
Country (ISO code) (Pays (code ISO))	Le pays où se situe votre société. Utilisez le code ISO standard. Pour obtenir la liste des codes ISO, accédez au site Web suivant : http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.ht
Email	Une adresse électronique à laquelle vous ou un autre utilisateur administratif peut être joint.
Challenge Password (Mot de passe de demande d'accès) **Confirm Challenge Password** (Confirmer le mot de passe de demande d'accès)	Le mot de passe requis pour accéder à la Dominion PX. Entrez-le d'abord dans le champ **Challenge Password**, puis de nouveau dans le champ **Confirm Challenge password**. Le mot de passe est sensible à la casse ; veillez à mettre les mêmes lettres en majuscules à chaque fois.

3. Dans la liste déroulante du champ **Key Length** (Longueur de clé) (bits), sélectionnez la longueur de clé. Par défaut, la valeur est de 1024, mais vous pouvez également sélectionner 2048.

4. Cliquez sur **Create** (Créer). La demande de signature de certificat est créée et la seconde page de la fenêtre SSL Server Certificate Management (Gestion des certificats du serveur SSL) apparaît. Cette fenêtre présente les informations saisies lors de la création de la demande de signature de certificat.



5. Pour télécharger la nouvelle demande sur votre ordinateur, cliquez sur **Download** (Télécharger). Vous êtes invité à ouvrir ou enregistrer le fichier. Le fichier s'appelle **csr**.txt.
6. Une fois le fichier stocké sur votre ordinateur, soumettez-le à une autorité de certification pour obtenir le certificat numérique.

Installation d'un certificat

Une fois le certificat numérique fourni par l'autorité de certification, vous devez l'installer sur la Dominion PX.

➢ *Pour installer un certificat :*

1. Assurez-vous qu'un certificat a été créé avant toute configuration supplémentaire. Ensuite, choisissez **Device Settings --> Certificate** (Paramètres du dispositif --> Certificat). La seconde page de la fenêtre de gestion des certificats du serveur apparaît.
2. Entrez le chemin et le nom du fichier de certificat dans le champ **SSL Certificate File** (Fichier de certificat SSL), ou cliquez sur **Browse** (Parcourir) et sélectionnez le fichier.
3. Cliquez sur **Upload** (Télécharger vers le serveur). Le certificat est installé sur la Dominion PX.

Paramétrage de l'authentification des utilisateurs externes

Pour des raisons de sécurité, les utilisateurs tentant de se connecter à la Dominion PX doivent être authentifiés. Vous pouvez utiliser la base de données locale des profils utilisateur de l'unité Dominion PX, ou utiliser les protocoles LDAP (Lightweight Directory Access Protocol) ou RADIUS (Remote Access Dial-In User Service).

Par défaut, l'unité Dominion PX est configurée pour une authentification locale. Si vous conservez cette méthode, il vous suffit de créer des profils pour chaque utilisateur autorisé. Si vous préférez utiliser un serveur LDAP ou RADIUS externe, vous devez fournir des informations à son sujet au système.

Gardez à l'esprit que vous devez tout de même créer des profils pour les utilisateurs authentifiés en externe. En effet, le profil utilisateur détermine le groupe auquel l'utilisateur appartient, et le groupe détermine les autorisations sur le système et les prises de l'utilisateur.

Paramétrage de l'authentification LDAP

➢ *Pour paramétrer l'authentification LDAP :*

1. Choisissez **Device Settings --> Authentication** (Paramètres du dispositif --> Authentification). La fenêtre Authentication Settings (Paramètres d'authentification) s'affiche. Les paramètres LDAP apparaissent sur le côté gauche de la fenêtre.

2. Cliquez sur la case d'option libellée **LDAP**.
3. Entrez l'adresse IP du serveur LDAP dans le champ **User LDAP Server** (Serveur LDAP utilisateur).
4. Pour chiffrer le trafic depuis et vers le serveur LDAP, cochez la case **SSL Enabled** (SSL activé).
5. Par défaut, la Dominion PX utilise les ports standard 389 pour LDAP et 636 pour LDAP sécurisé (SSL). Si vous préférez utiliser des ports non standard, changez de ports.

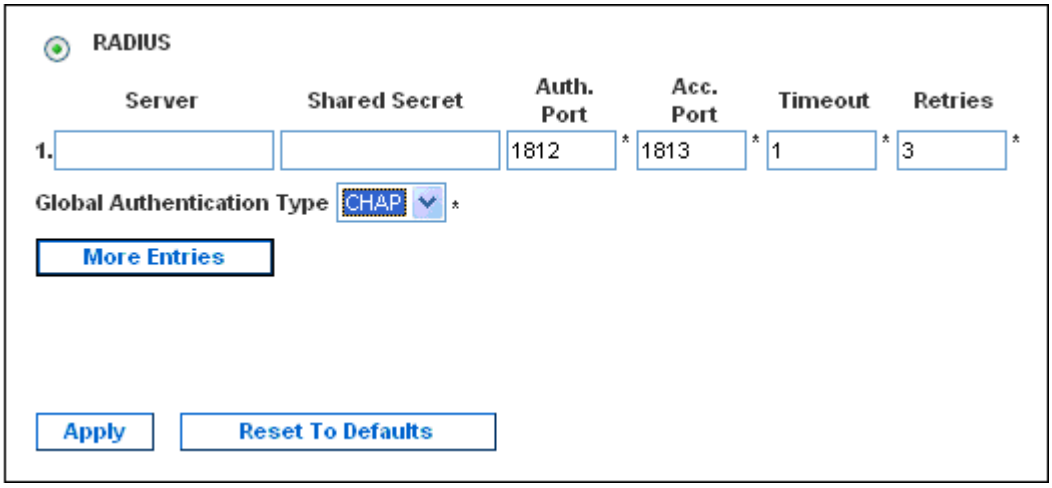
Remarque : le port SSL n'est activé que si vous cochez la case à l'étape 3.

6. Entrez le nom distinct (ND) de base dans le champ **Base DN of user LDAP server** (ND de base du serveur LDAP utilisateur). Le nom distinct de base représente le niveau supérieur de l'arborescence du répertoire LDAP. Il indique à quel endroit du répertoire LDAP vous souhaitez débuter la recherche des informations d'identification de l'utilisateur.
7. Sélectionnez le type de serveur LDAP dans la liste déroulante du champ Type of external LDAP server (Type de serveur LDAP externe). Les options sont les suivantes :
   - Generic LDAP Server (Serveur LDAP générique)
   - Novell Directory Service (Service de répertoires Novell)
   - Microsoft Active Directory
8. Entrez les valeurs suivantes dans les champs correspondants : LDAP a besoin de ces informations pour vérifier les noms d'utilisateur et les mots de passe.
   - Attribut de nom de connexion (également appelé AuthorizationString)
   - Classe d'objets d'entrée d'utilisateur
   - Sous-filtre de recherche des utilisateurs (également appelé BaseSearch)
9. Si vous avez sélectionné **Microsoft Active Directory** à l'étape 6, entrez le nom de domaine dans le champ **Active Directory Domain** (Domaine Active Directory).
10. Cliquez sur **Apply** (Appliquer). L'authentification LDAP est maintenant en place.

Paramétrage de l'authentification RADIUS

➢ *Pour paramétrer l'authentification RADIUS :*

1. Choisissez Device Settings --> Authentication (Paramètres du dispositif --> Authentification). La fenêtre Authentication Settings (Paramètres d'authentification) s'affiche. Les paramètres RADIUS apparaissent sur le côté droit de la fenêtre.



2. Cliquez sur la case d'option libellée **RADIUS**.
3. Entrez l'adresse IP du serveur RADIUS dans le champ **Server** (Serveur).
4. Renseignez le champ **Shared Secret** (Secret partagé). Le secret partagé est nécessaire pour protéger la communication avec le serveur RADIUS.
5. Par défaut, la Dominion PX utilise les ports RADIUS standard 1812 (authentification) et 1813 (statistiques). Si vous préférez utiliser des ports non standard, changez de ports.
6. Entrez le délai (en secondes) dans le champ **Timeout** (Délai d'attente). Ceci définit le délai maximum pour établir le contact avec le serveur RADIUS avant expiration. La valeur par défaut est 1 seconde.
7. Entrez le nombre de tentatives autorisées dans le champ **Retries** (Nouvelles tentatives). La valeur par défaut est 3.
8. Si vous disposez de plusieurs serveurs RADIUS, cliquez sur le bouton **More Entries** (Plus d'entrées). Des champs apparaissent pour quatre serveurs supplémentaires. Entrez les mêmes informations aux étapes 2 à 7 pour chaque serveur supplémentaire.
9. Sélectionnez un protocole d'authentification dans la liste déroulante du champ **Global Authentication Type** (Type d'authentification globale). Les options sont les suivantes :
   - PAP (Password Authentication Protocol)
   - CHAP (Challenge Handshake Authentication Protocol)

En règle générale, le protocole CHAP est considéré plus sûr car le nom d'utilisateur et le mot de passe sont chiffrés, alors qu'ils sont transmis en clair avec le protocole PAP.

10. Cliquez sur **Apply** (Appliquer). L'authentification RADIUS est maintenant en place.

Paramétrage des prises et des seuils d'alimentation

L'unité Dominion PX est livrée avec des seuils de la Dominion PX et d'alimentation de prise déjà définis. Vous pouvez modifier les seuils de la Dominion PX par défaut, et vous pouvez nommer chaque prise et remplacer ses seuils par défaut.

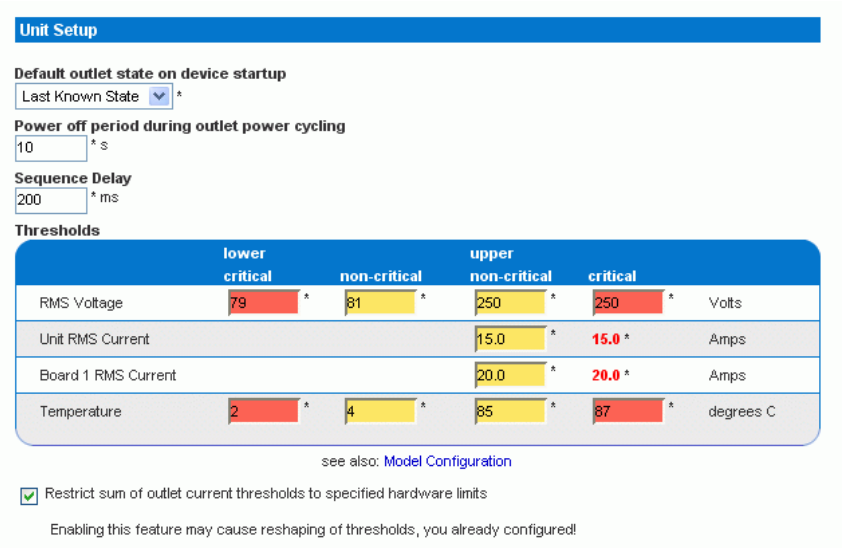
Lors de la définition des seuils, gardez à l'esprit que vous pouvez paramétrer des alertes qui sont déclenchées lorsque ces seuils sont franchis. Reportez-vous à la section ***Paramétrage des alertes*** (à la page 86) pour en savoir plus.

Définition de l'état des prises par défaut

Cette opération consiste à définir une valeur par défaut globale pour l'état d'alimentation des prises à la mise sous tension de l'unité Dominion PX. La définition d'un état de démarrage pour une prise individuelle sur une valeur différente de **Device Default** (Valeur par défaut du dispositif) (reportez-vous à **Nommage des prises**) supplante l'état par défaut de cette prise.

➢ *Pour définir l'état des prises par défaut :*

1. Sélectionnez **Device Settings** (Paramètres du dispositif), puis **Unit Setup** (Configuration de l'unité). La fenêtre Unit Setup apparaît.



2. Sélectionnez l'état par défaut dans la liste déroulante du champ **Default outlet state on device startup** (Etat des prises par défaut au démarrage du dispositif).
3. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Le paramètre d'état par défaut est appliqué.

Définition des seuils de la Dominion PX

➢ *Pour définir les seuils de la Dominion PX :*

1. Choisissez **Device Settings** (Paramètres du dispositif), puis **Unit Setup** (Configuration de l'unité). La fenêtre Unit Setup apparaît.

2. Entrez un nombre dans le champ **Power off period during outlet power cycling** (Période de mise hors tension pendant l'alimentation cyclique des prises). Lors d'une alimentation cyclique, les prises de la Dominion PX sont mises hors tension, puis sous tension. Le nombre entré ici détermine le délai (en secondes) devant s'écouler entre l'arrêt des prises et leur remise sous tension lors de l'alimentation cyclique. La valeur par défaut est de 10 secondes. Le délai d'alimentation cyclique peut être défini sur 0 à 3600 secondes (une heure).

   Remarque : le nombre entré ici s'applique à toutes les prises de la Dominion PX. Vous pouvez toutefois supplanter cette valeur pour des prises spécifiques si vous le souhaitez. Reportez-vous à la section ***Définition des seuils des prises*** (à la page 79) pour en savoir plus. Vous pouvez procéder à l'alimentation cyclique d'une prise depuis la fenêtre Outlet Details (Détails des prises). Reportez-vous à la section ***Alimentation cyclique d'une prise*** (à la page 81) pour obtenir des instructions.

3. Entrez un nombre dans le champ **Sequence Delay** (Délai de séquence) en ms. La valeur par défaut est de 200 millisecondes.
4. Définissez les seuils de tension efficace, de courant et de température pour l'unité dans le panneau **Thresholds** (Seuils). Entrez des seuils critiques et non critiques pour chaque paramètre.
5. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les délais et seuils sont appliqués.

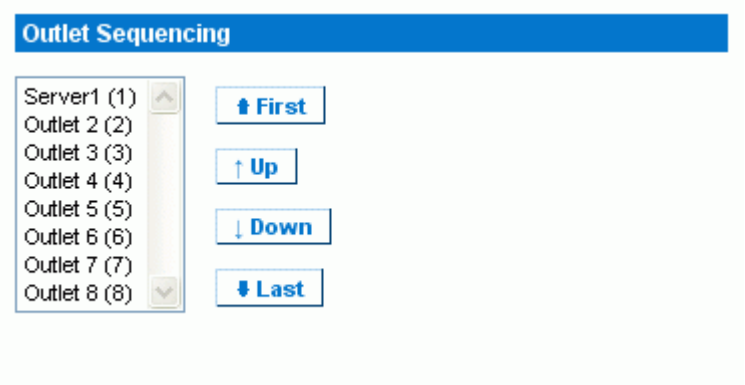
Remarque : en présence de nombreuses prises, en particulier lorsqu'il s'agit de prises groupées d'autres unités Dominion PX, il est conseillé de définir la période de mise hors tension et les délais de séquence sur des valeurs inférieures pour éviter d'avoir à attendre longtemps que toutes les prises soient à nouveau disponibles.

Définition de la séquence de mise sous tension des prises

Vous pouvez définir l'ordre dans lequel les prises de l'unité sont mises sous tension. Ceci est utile lorsque des dispositifs sont dotés de plusieurs alimentations qui doivent être mises sous tension ensemble.

➢ *Pour définir la séquence de mise sous tension des prises :*

1. Sélectionnez **Device Settings** (Paramètres du dispositif), puis **Unit Setup** (Configuration de l'unité). La fenêtre Unit Setup apparaît.



2. La séquence actuelle de mise sous tension des prises apparaît dans la liste sous **Outlet Sequencing** (Mise en séquence des prises). Pour modifier la priorité d'une prise, sélectionnez celle-ci dans la liste et cliquez sur une des quatre options :

- **First** (Première) place la prise au sommet de la liste et elle est la première alimentée.
- **Up** (Haut) fait monter la prise d'une position dans la liste.
- **Down** (Bas) fait descendre la prise d'une position dans la liste.
- **Last** (Dernière) place la prise en bas de la liste et elle est la dernière alimentée.

1. Cliquez sur **Apply** (Appliquer). La nouvelle séquence est enregistrée.

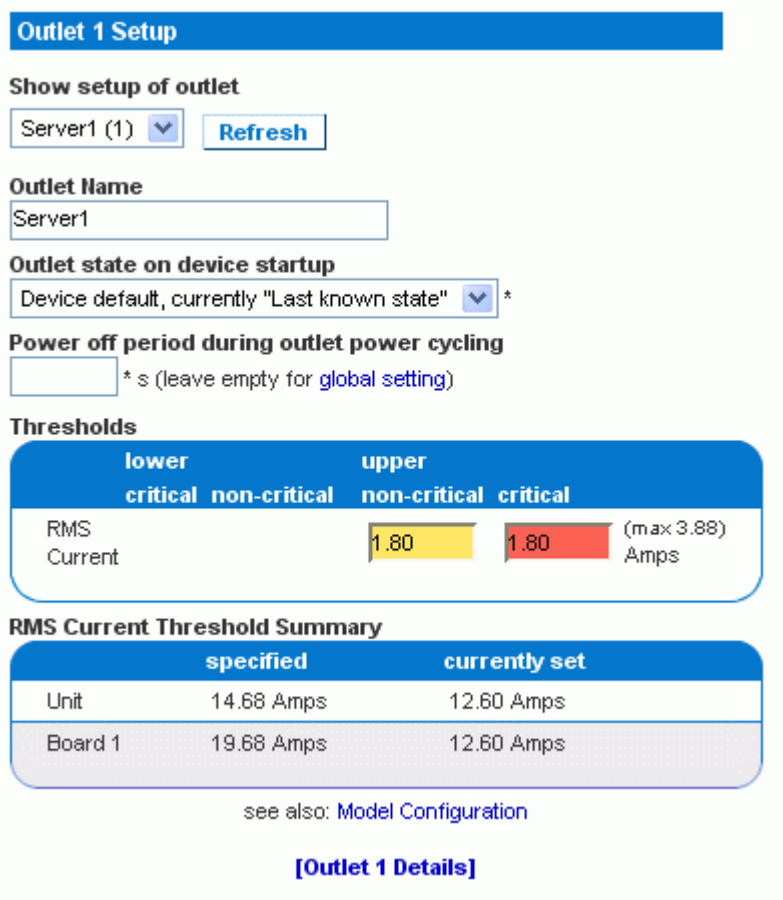
Remarque : si vous utilisez la fonction Outlet Grouping pour grouper des prises, il vous faut ajuster la mise en séquence des prises pour assurer que toutes les prises de l'unité Dominion PX concernée, appartenant au même groupe, sont mises sous tension consécutivement.

Nommage des prises

Vous pouvez donner un nom à chaque prise pour vous aider à identifier le dispositif qui lui est connecté.

➢ *Pour nommer des prises :*

1. Choisissez **Power Outlets --> Outlet Setup** (Prises d'alimentation --> Configuration des prises). La fenêtre Outlet Setup s'affiche.



2. Dans la liste déroulante du champ **Show setup of outlet** (Afficher la configuration de la prise), sélectionnez la prise.
3. Entrez le nom de la prise dans le champ **Outlet Name** (Nom de la prise). Il est recommandé de donner à la prise un nom aisément reconnaissable vous permettant d'identifier le dispositif qui lui est connecté. Vous pouvez toujours modifier le nom si le dispositif est remplacé.

4. Sélectionnez un état dans la liste déroulante du champ Default outlet state on device startup (Etat des prises par défaut au démarrage du dispositif). Ceci détermine si la prise est active ou inactive au démarrage de l'unité Dominion PX. Si cette option est définie sur **Device Default** (Valeur par défaut du dispositif), l'état de cette prise est déterminée par le champ **Default Outlet State** (Etat des prises par défaut) de la page **Unit Setup** (Configuration de l'unité).
5. Cliquez sur **Apply** (Appliquer). Le nouveau nom est appliqué.

Définition des seuils des prises

➢ *Pour définir les seuils de courant d'une prise :*

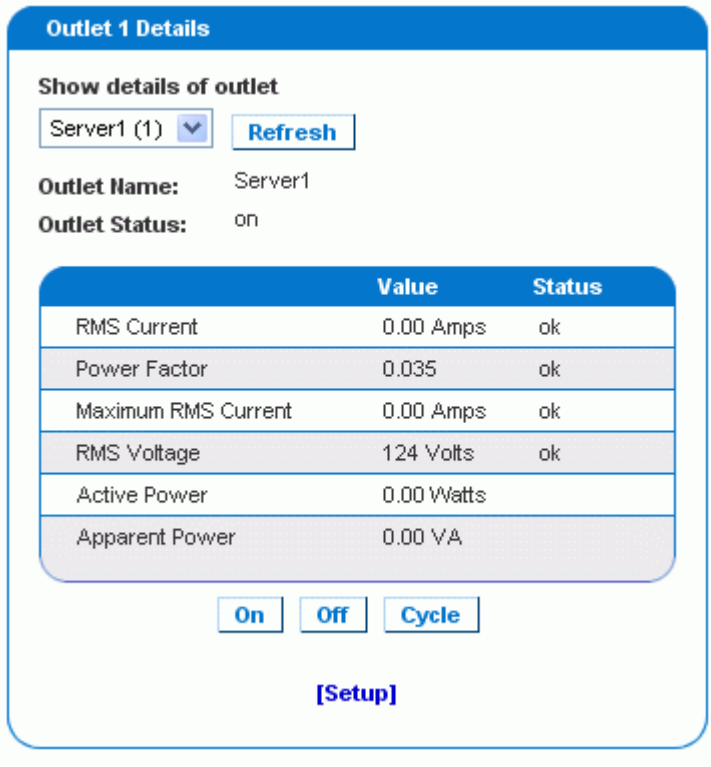
1. Choisissez **Power Outlets --> Outlet Setup** (Prises d'alimentation --> Configuration des prises). La fenêtre Outlet Setup s'affiche.
2. Dans la liste déroulante du champ **Show setup of outlet** (Afficher la configuration de la prise), sélectionnez une prise.
3. Entrez un nombre dans le champ **Power off period during outlet power cycling** (Période de mise hors tension pendant l'alimentation cyclique des prises). Lors d'une alimentation cyclique, la prise est mise hors tension, puis sous tension. Le nombre entré ici détermine le délai (en secondes) devant s'écouler entre l'arrêt de la prise et sa remise sous tension lors de l'alimentation cyclique. Si vous laissez le champ vide, cette prise utilisera la valeur définie par défaut sur la page **Unit Setup** (Configuration de l'unité).

   Remarque : vous pouvez procéder à l'alimentation cyclique d'une prise depuis la fenêtre Outlet Details (Détails des prises). Reportez-vous à la section ***Alimentation cyclique d'une prise*** (à la page 81) pour obtenir des instructions.
4. Définissez les seuils de courant effectif pour la prise dans le panneau **Thresholds** (Seuils).
5. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les détails de configuration sont appliqués.

Affichage des détails des prises

➢ *Pour afficher les détails d'une prise particulière :*

1. Choisissez **Power Outlets --> Outlet Details** (Prises d'alimentation --> Détails des prises). La fenêtre Outlet Details s'affiche.



2. Dans la liste déroulante du champ **Show details of outlet** (Afficher les détails de la prise), sélectionnez une prise. La fenêtre affiche les détails suivants sur la prise :
   - Nom de la prise
   - Statut de la prise
   - Relevés de courant effectif, tension et alimentation, notamment :

     RMS Current (Courant efficace)

     Power Factor (Facteur de puissance)

     Maximum RMS Current (Courant efficace maximum)

     RMS Voltage (Tension efficace)

     Active Power (Puissance active)

     Apparent Power (Puissance apparente)

Remarque : pour afficher la fenêtre Outlet Setup (Configuration des prises), cliquez sur le lien *[Setup]*. Reportez-vous à la section ***Nommage des prises*** (à la page 78) pour obtenir une capture de la fenêtre Outlet Setup.

Alimentation cyclique d'une prise

➢ *Pour effectuer l'alimentation cyclique d'une prise :*

1. Choisissez **Power Outlets --> Outlet Details** (Prises d'alimentation --> Détails des prises). La fenêtre Outlet Details s'affiche.
2. Dans la liste déroulante du champ Show details of outlet (Afficher les détails de la prise), sélectionnez une prise. Le statut de la prise doit être **ON** (Active).
3. Cliquez sur **Cycle**. La prise est désactivée, puis réactivée.

Remarque : vous pouvez également procéder à l'alimentation cyclique d'une prise depuis la fenêtre Home (Accueil).

Le délai entre l'état inactif et actif dans une alimentation cyclique peut être défini sur la Dominion PX dans sa totalité et pour des prises individuelles. Reportez-vous aux sections ***Définition des seuils de la Dominion PX*** (à la page 75) et ***Définition des seuils des prises*** (à la page 79) pour en savoir plus.

Activation ou désactivation d'une prise

➢ *Pour activer ou désactiver une prise :*

1. Choisissez **Power Outlets --> Outlet Details** (Prises d'alimentation --> Détails des prises). La fenêtre Outlet Details s'affiche.
2. Dans la liste déroulante du champ **Show details of outlet** (Afficher les détails de la prise), sélectionnez une prise.
3. Cliquez sur **On** pour activer la prise. Cliquez sur **Off** pour désactiver.

Remarque : vous pouvez également activer ou désactiver une prise depuis la fenêtre Home (Accueil).

Capteurs d'environnement

Outre la surveillance de sa température interne, Dominion PX peut contrôler l'environnement à l'emplacement de ses capteurs.

Connexion des capteurs d'environnement

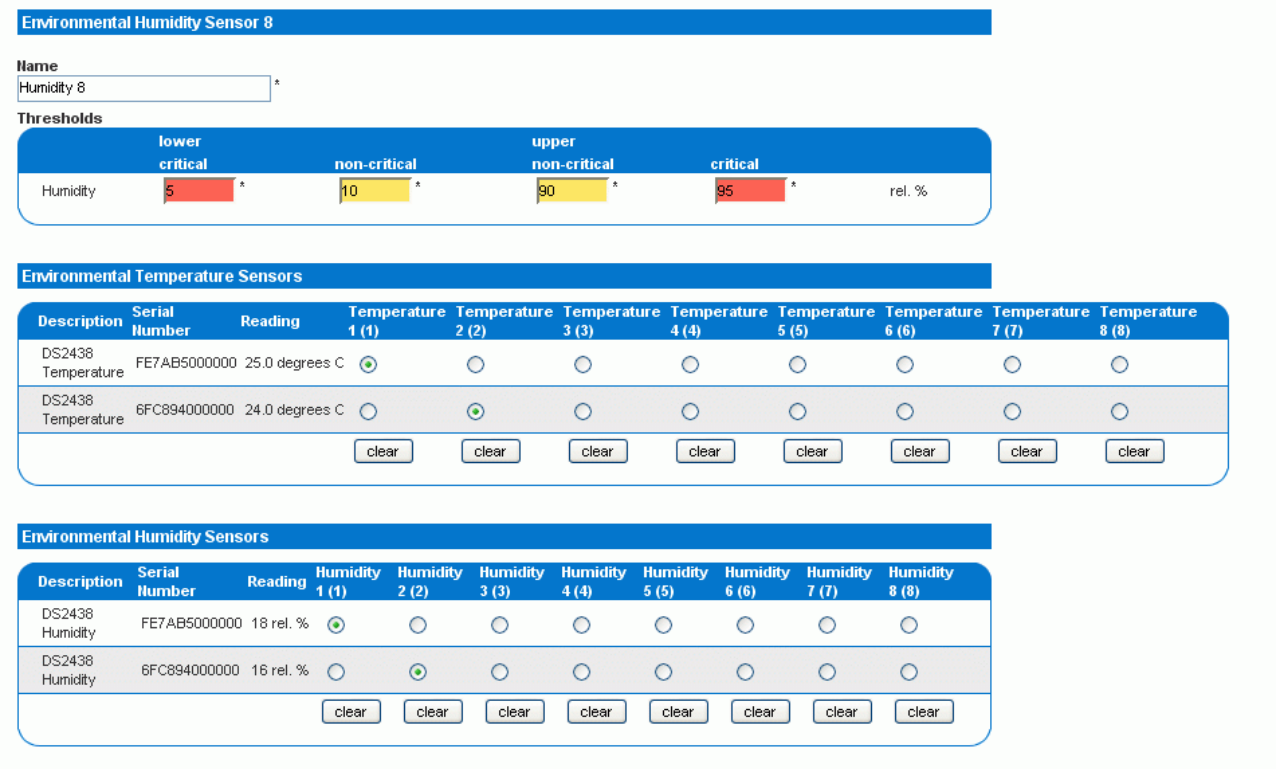
Pour permettre à Dominion PX de mesurer les facteurs d'environnement, connectez le câble des capteurs au port **Feature** (Fonction) de l'unité.

Mappage des capteurs d'environnement

Une fois les capteurs physiquement connectés à la Dominion PX, ils doivent être mappés sur les capteurs logiques de l'unité pour permettre à celle-ci de reconnaître (et d'afficher) leurs relevés.

➢ *Pour mapper les capteurs d'environnement :*

1. Sélectionnez **Device Settings** (Paramètres du dispositif), puis **Environmental Sensors** (Capteurs d'environnement). La fenêtre Environmental Sensors s'affiche. La page indique d'abord les capteurs Température et Humidité logiques.



2. Lorsque des capteurs physiques sont branchés sur la Dominion PX, ils sont répertoriés sous les capteurs logiques. Les capteurs de température figurent dans le tableau **Environmental Temperature Sensors** (Capteurs de température d'environnement), les capteurs d'humidité dans le tableau **Environmental Humidity Sensors** (Capteurs d'humidité d'environnement). Si les capteurs ne sont pas correctement branchés, la page indique « No sensors were detected » (Aucun capteur détecté).
3. Pour chaque capteur physique (affiché dans une rangée) du tableau, cliquez sur la case d'option se trouvant sous le capteur logique (affiché dans une colonne) auquel vous souhaitez le mapper. Dominion PX assure maintenant le suivi des relevés de ce capteur et les affiche sur la page d'accueil lorsque la configuration est terminée.

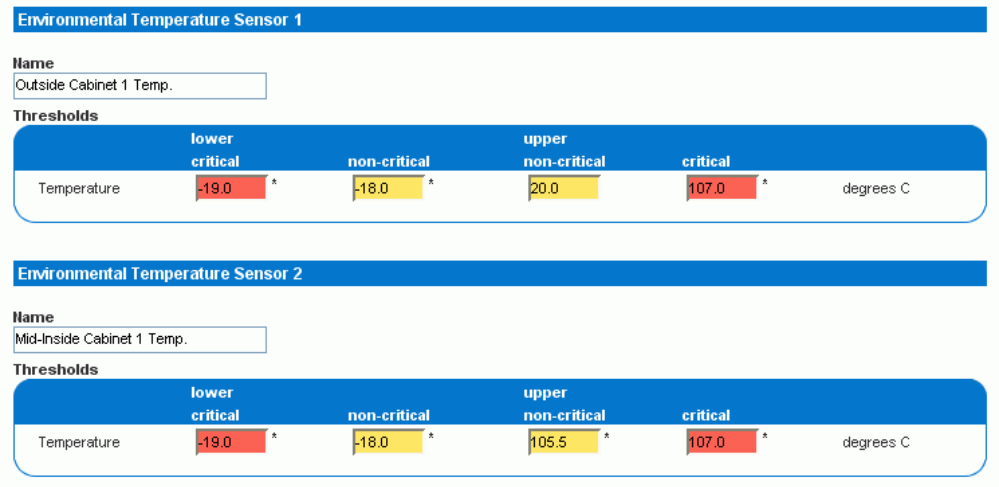
   Si vous ne souhaitez pas effectuer le suivi des relevés d'un capteur particulier, laissez cette rangée vide.
4. Pour dissocier un capteur logique d'un capteur physique, cliquez sur **clear** (effacer) au bas de la colonne. Le capteur logique n'est associé à aucun capteur physique.

Remarque : il est possible (mais pas recommandé) de mapper plusieurs capteurs logiques à un seul capteur physique. Vous ne pouvez pas mapper plusieurs capteurs physiques à un seul capteur logique.

Configuration des capteurs d'environnement et des seuils

Pour rendre les capteurs plus utiles, renommez les capteurs logiques utilisés et configurez leurs paramètres de seuil. La configuration de seuils pour ces capteurs permet à Dominion PX de générer une alerte si les facteurs d'environnement au niveau de ces capteurs sont en dehors de ces valeurs.

1. Depuis la page **Environmental Sensors** (Capteurs d'environnement), repérez les capteurs logiques mappés à des capteurs physiques comme décrit ci-dessus.

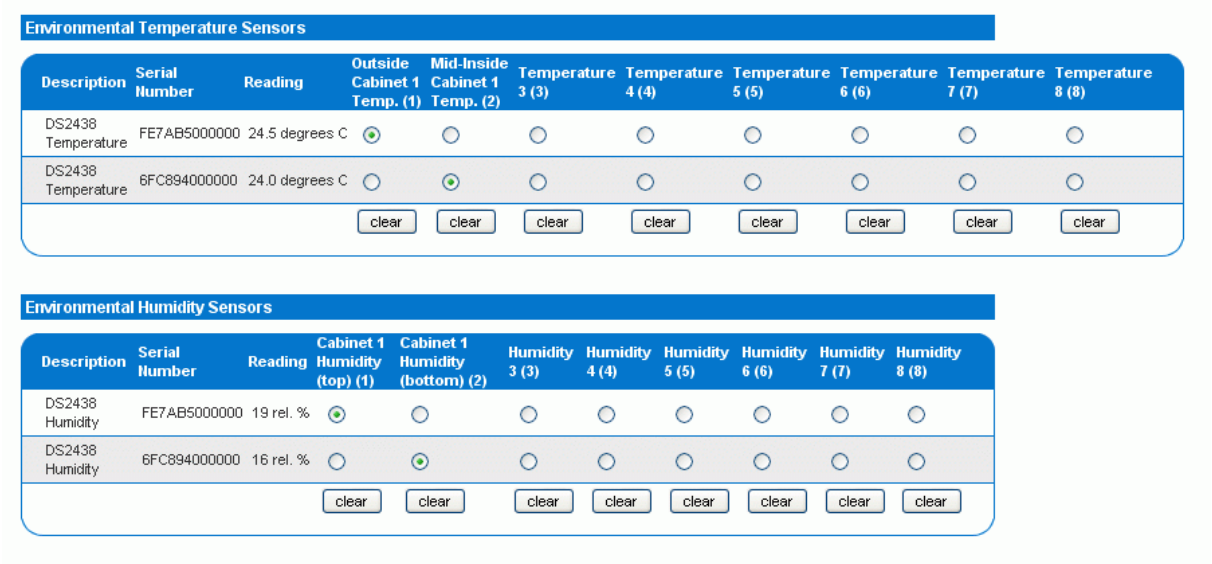


2. Dans le champ **Name** (Nom), entrez un nouveau nom pour chaque capteur mappé afin de vous aider à identifier le capteur et sa fonction.
3. Configurez les seuils supérieurs et inférieurs de chaque capteur utilisé.

- Les valeurs **upper critical** (critique supérieur) et **lower critical** (critique inférieur) sont des points auxquels la Dominion PX considère que l'environnement d'exploitation est critique et en dehors de la plage du seuil acceptable.
- Arrivée à ce point critique, la température ou l'humidité doit descendre sous la valeur **upper non-critical** (non critique supérieur) (ou monter au-dessus de la valeur **Lower Non-Critical** (non critique inférieur)) pour que la Dominion PX considère que l'environnement est à nouveau acceptable.

1. Cliquez sur **Apply** (Appliquer). Le nom du capteur et les paramètres de seuil sont enregistrés.

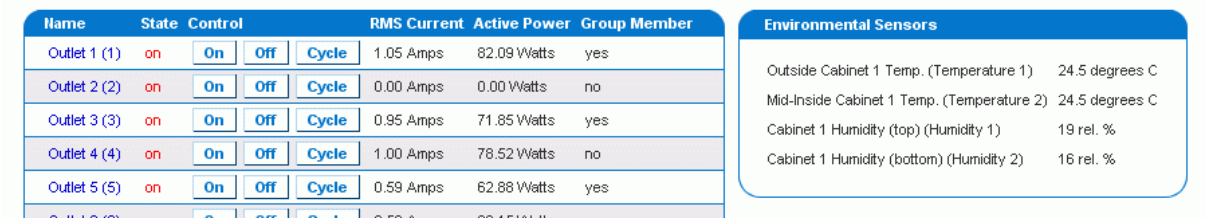
Lorsque les modifications de configuration ont été appliquées, les relevés de capteur s'affichent sur la page d'accueil en regard de la liste des prises et le nom des capteurs est mis à jour. Ce nom à jour apparaît également dans la table des capteurs physiques au bas de la page Environmental Sensors (Capteurs d'environnement). Ceci peut se révéler utile pour garantir que les capteurs physiques et logiques sont correctement mappés.



Remarque : la température ambiante d'exploitation maximum recommandée pour l'unité Dominion PX est de 40 C.

Affichage des relevés de capteur

Les relevés des capteurs mappés apparaissent à côté de la liste des prises lorsque la page d'accueil est affichée. Pour visualiser les relevés depuis une autre page, cliquez sur Home (Accueil) dans le chemin de navigation en haut de la fenêtre.



Paramétrage des alertes

La Dominion PX peut être configurée pour émettre une alerte chaque fois qu'un seuil est franchi, pour l'unité Dominion PX dans son intégralité ou pour une prise spécifique. L'alerte peut être programmée pour envoyer un message électronique à un administrateur, ou un trap SNMP (Simple Network Management Protocol) à une adresse IP spécifique.

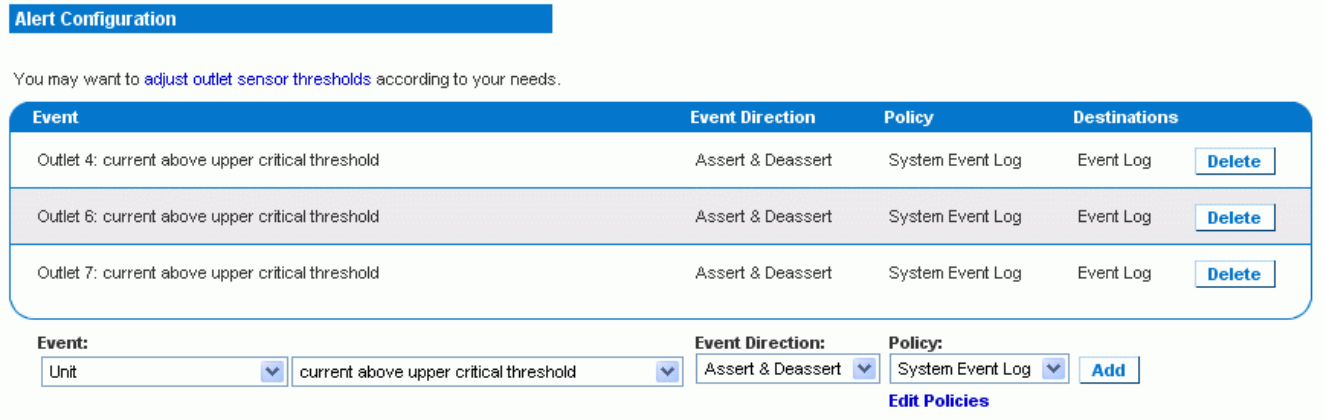
Remarque : reportez-vous à la section **Paramétrage des prises et des seuils d'alimentation** *(à la page 74) pour obtenir des instructions sur la définition des seuils d'alimentation.*

Configuration des événements d'alerte

Les événements d'alerte sont constitués d'une prise, et d'un seuil et d'une stratégie associés.

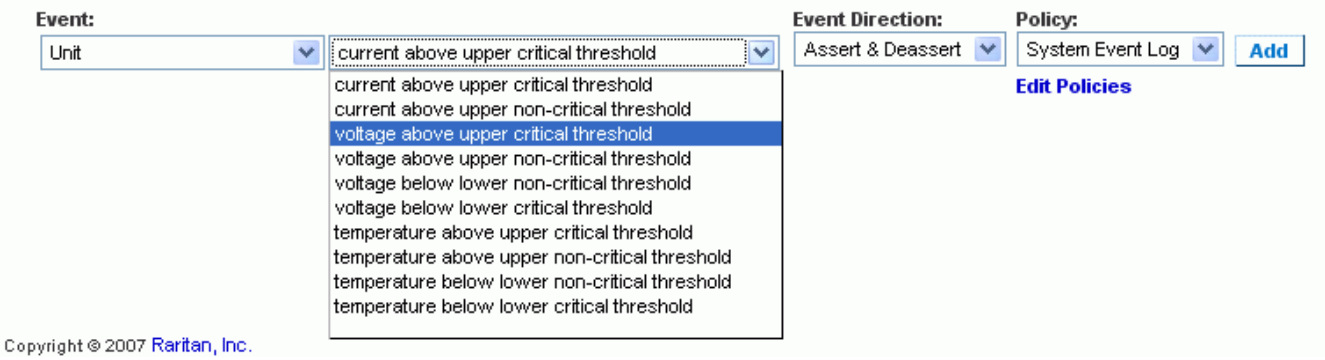
➢ *Pour configurer un événement d'alerte :*

1. Choisissez **Alerts --> Alert Configuration** (Alertes --> Configuration des alertes). La fenêtre Alert Configuration s'affiche. Elle présente toutes les stratégies existantes.



2. Allez au champ **Event** (Evénement) et sélectionnez la prise dans la première liste déroulante (à gauche). Vous pouvez sélectionner l'unité Dominion PX entière ou une prise spécifique. Vous pouvez également sélectionner une carte de relais individuelle, les capteurs de température d'environnement ou les capteurs d'humidité d'environnement.

3. Sélectionnez le seuil dans la seconde liste déroulante du champ **Event** (Evénement) comme illustré ci-dessous. La liste de seuils varie en fonction de la sélection dans la première liste déroulante.



4. Dans la troisième liste déroulante **Event Direction** (Direction de l'événement), effectuez une sélection.

- Si l'alerte est définie sur **Assert** (Affirmer), elle ne se déclenche que si une valeur mesurée franchit un seuil critique (au-dessus d'un seuil critique supérieur ou au-dessous d'un seuil critique inférieur).
- Si l'alerte est définie sur **Deassert** (Infirmer), elle ne se déclenche que si une valeur revient à un état normal (au-dessous d'un seuil non critique supérieur ou au-dessus d'un seuil non critique inférieur).
- Si l'alerte est définie sur **Assert & Deassert**, elle se déclenche si une valeur mesurée franchit un état seuil quelconque.

1. Dans la liste déroulante du champ **Policy** (Stratégie), sélectionnez une stratégie.
2. Cliquez sur **Add** (Ajouter). L'alerte est ajoutée au système.

Remarque : aucune stratégie n'apparaît dans cette liste déroulante tant que vous n'en avez pas créé. Reportez-vous à la section ***Création des stratégies d'alerte*** (à la page 88) pour obtenir des instructions.

Si un capteur Température ou Humidité d'environnement est sélectionné, un événement est créé pour chaque capteur. Ces alertes d'événement peuvent être supprimées ; vous pouvez ainsi ne conserver que celles que vous souhaitez.

Création des stratégies d'alerte

Les stratégies d'alerte vous permettent d'associer des événements à des destinations. Les stratégies déterminent si des événements spécifiques déclenchent une entrée dans le journal des événements, un message électronique à un administrateur, un trap SNMP, la mise sous/hors tension ou l'alimentation cyclique d'une prise sélectionnée ou une combinaison des quatre.

A propos des stratégies

Le tableau ci-dessous illustre la façon dont les stratégies associent des événements à des destinations. Dans cet exemple, cinq événements et deux stratégies sont définis.

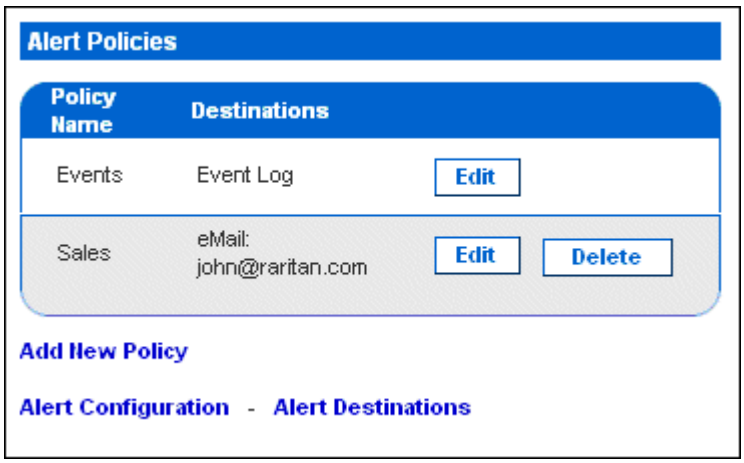
- Les événements **1** et **2** sont associés à la stratégie **Rouge**. Ceci signifie qu'ils déclenchent un message électronique à un administrateur et un trap SNMP.
- Les événements **3**, **4** et **5** sont associés à la stratégie **Syslog**. Ils déclenchent des entrées dans le journal des événements et la commutation de prises sélectionnées, mais n'envoient ni message électronique ni trap.

Evénement nº	Stratégie	Destinations	
1	Rouge	Journal des événements	
		courriel	☑
		Trap SNMP	☑
		Commutation de prises	
2	Rouge	Journal des événements	
		courriel	☑
		Trap SNMP	☑
		Commutation de prises	
3	Syslog	Journal des événements	☑
		courriel	
		Trap SNMP	
		Commutation de prises	☑
4	Syslog	Journal des événements	☑

		courriel	
		Trap SNMP	
		Commutation de prises	☑
5	Syslog	Journal des événements	☑
		courriel	
		Trap SNMP	
		Commutation de prises	☑

➢ *Pour afficher une liste des stratégies existantes :*

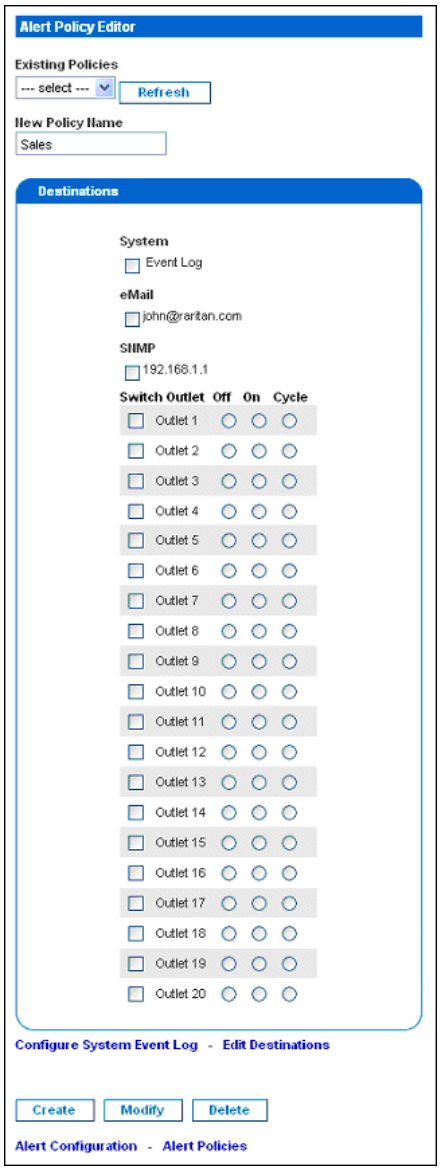
1. Choisissez **Alerts --> Alert Policies** (Alertes --> Stratégies d'alerte). La fenêtre Alert Policies s'affiche. Elle répertorie chaque stratégie et indique leurs destinations.



2. Vous pouvez modifier ou supprimer une stratégie en cliquant sur le bouton correspondant. Vous pouvez ajouter une nouvelle stratégie et configurer des alertes et des destinations en cliquant sur le lien approprié.

➢ *Pour créer une stratégie :*

1. Choisissez **Alerts --> Alert Policy Editor** (Alertes --> Editeur des stratégies d'alerte). La fenêtre Alert Policy Editor s'affiche.



2. Renseignez le champ **New Policy Name** (Nom de la nouvelle stratégie).
3. Sélectionnez les destinations associées à la stratégie dans le panneau Destinations. Les options disponibles sont : **System** (Système) (journal des événements), **Switch Outlet** (Commutation de prises), **eMail** et **SNMP**.
4. Cliquez sur **Create** (Créer). La stratégie est créée.

➢ *Pour modifier une stratégie :*

1. Choisissez **Alerts --> Alert Policy Editor** (Alertes --> Editeur des stratégies d'alerte). La fenêtre Alert Policy Editor s'affiche.
2. Dans la liste déroulante du champ **Existing Policies** (Stratégies existantes), sélectionnez la stratégie à modifier.
3. Apportez les modifications nécessaires au nom ou aux destinations de la stratégie.
4. Cliquez sur **Modify** (Modifier). La stratégie est modifiée.

➢ *Pour supprimer une stratégie :*

1. Choisissez **Alerts --> Alert Policy Editor** (Alertes --> Editeur des stratégies d'alerte). La fenêtre Alert Policy Editor s'affiche.
2. Dans la liste déroulante du champ **Existing Policies** (Stratégies existantes), sélectionnez la stratégie à supprimer.
3. Cliquez sur **Delete** (Supprimer). La stratégie est supprimée.

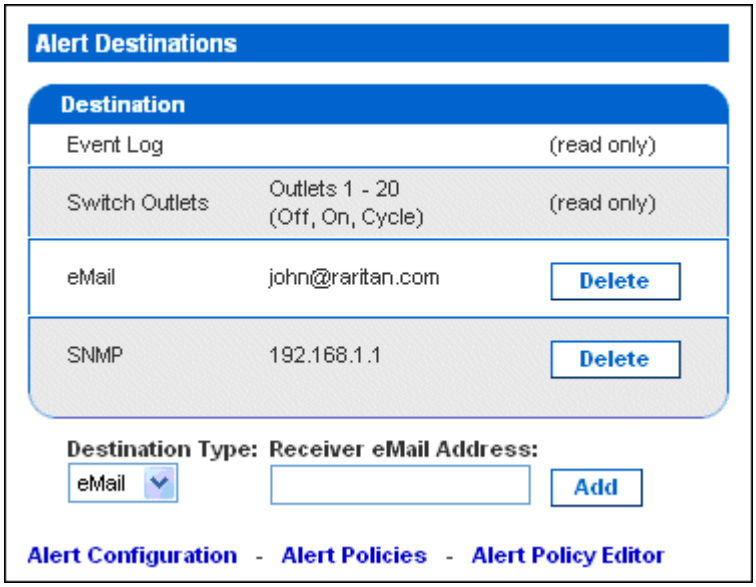
Remarque : la stratégie d'alerte par défaut, System Event Log (Journal des événements système), ne peut pas être supprimée.

Définition de la destination des alertes

La destination d'une alerte peut être une adresse électronique ou un trap SNMP.

➢ *Pour définir la destination :*

1. Choisissez **Alerts --> Alert Destinations** (Alertes --> Destinations des alertes). La fenêtre Alert Destinations s'affiche.



Remarque : si vous n'avez pas configuré le serveur SMTP de la Dominion PX, une note apparaît sur cette page vous invitant à le faire à présent. Vous ne pouvez pas entrer d'adresse électronique tant que le serveur SMTP n'est pas configuré. Cliquez sur le lien here (ici) du serveur SMTP apparaissant sur cette page, ou sélectionnez **Devices Settings --> SMTP Settings** (Paramètres du dispositif --> Paramètres SMTP). Reportez-vous à la section ***Configuration des paramètres SMTP*** (à la page 110) pour en savoir plus.

2. Dans la liste déroulante du champ **Destination Type** (Type de destination), sélectionnez la destination. Les options disponibles sont : **Event Log** (Journal des événements), **Switch Outlet** (Commutation de prises), **eMail** et **SNMP**.
3. Effectuez une des opérations suivantes :

- **Event Log** Il s'agit d'une des options par défaut pour la destination de l'alerte. Si vous avez sélectionné cette option, les entrées d'événement sont consignées dans le journal des événements. Cette destination est intégrée par défaut, et ne peut être ni ajoutée ni supprimée.
- **Switch Outlets** Il s'agit d'une des options par défaut pour la destination de l'alerte. Si vous avez sélectionné cette option, la prise configurée est active, inactive ou alimentée cycliquement. Cette destination est intégrée par défaut, et ne peut être ni ajoutée ni supprimée.
- **Email** Si vous avez sélectionné cette option, entrez l'adresse électronique du destinataire.
- **SNMP** Si vous avez sélectionné cette option, entrez l'adresse IP du trap et la chaîne de communauté.

4. Cliquez sur **Add** (Ajouter). La destination est ajoutée.

Remarque : pour supprimer une destination d'alerte, cliquez sur le bouton *Delete* approprié.

Remarque : la Dominion PX est capable d'envoyer deux types de traps SNMP, à savoir : (1) des traps spécifiques PX, envoyés si le paramètre Event Log est configuré ainsi, les fichiers PDU-MIB doivent être explicites. (2) des traps IPMI PET (Platform Event Traps), générés dans la configuration de l'alerte et envoyés dans des formats IPMI spécifiques, contenant des données brutes. Le détail de ces traps peut être consulté dans : ***http://www.intel.com/design/servers/ipmi/pdf/IPMIv2_0_rev1_0_E3_markup.pdf*** (http://www.intel.com/design/servers/ipmi/pdf/ipmiv2_0_rev1_0_e3_markup.pdf) (chapitre 17.16) et ***http://download.intel.com/design/servers/ipmi/PET100.pdf*** (http://download.intel.com/design/servers/ipmi/pet100.pdf).

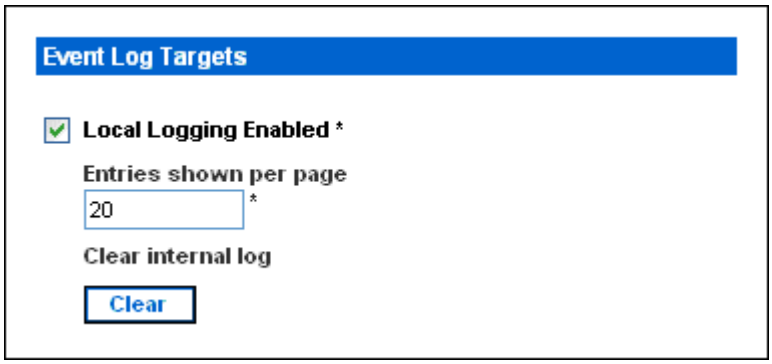
Paramétrage de la journalisation des événements

Par défaut, la Dominion PX capture certains événements système et les enregistre dans un journal local (interne). Vous pouvez élargir la portée de la journalisation pour capturer des événements dans les journaux NFS, SMTP et SNMP également.

Configuration du journal des événements local

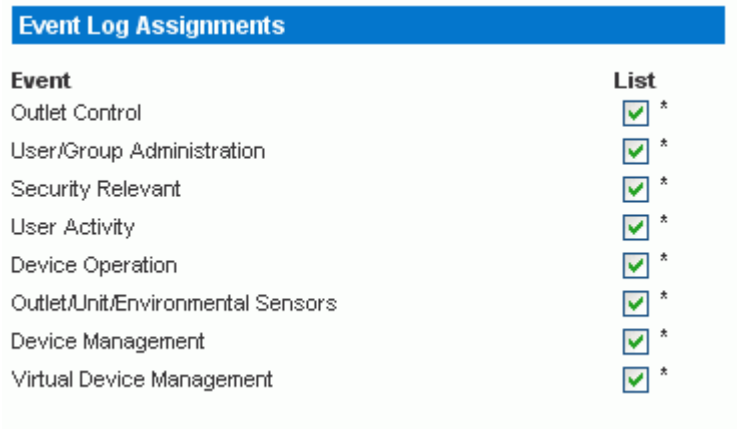
➢ *Pour configurer le journal des événements local :*

1. Choisissez **Device Settings --> Event Log** (Paramètres du dispositif --> Journal des événements). La fenêtre Event Log Settings (Paramètres du journal des événements) s'affiche. Le panneau Local Logging (Journalisation locale) s'affiche d'abord. Il contrôle le journal des événements local.



2. Ce journal est activé par défaut. Pour le désactiver, désélectionnez la case à cocher **Local Logging Enabled** (Journalisation locale activée).
3. Par défaut, 20 entrées apparaissent sur chaque page du journal des événements local lorsqu'il apparaît à l'écran. Pour modifier cette option, remplacez la valeur du champ **Entries shown per page** (Entrées affichées par page).
4. Pour effacer tous les événements du journal local :
   a. Cliquez sur le bouton **Clear** (Effacer). Le bouton devient **Really Clear** (Effacer réellement) et vous êtes invité à ne cliquer dessus que si vous souhaitez effectivement effacer le journal.
   b. Cliquez sur **Really Clear** pour confirmer l'opération ou sur **Cancel** (Annuler) pour l'abandonner.

5. Par défaut, lorsque le journal des événements local est activé, sept types d'événements apparaissent dans le panneau **Event Log Assignments** (Affectations du journal des événements) à droite. Ils sont tous activés par défaut. Pour désactiver des types d'événements, désélectionnez les cases à cocher appropriées.

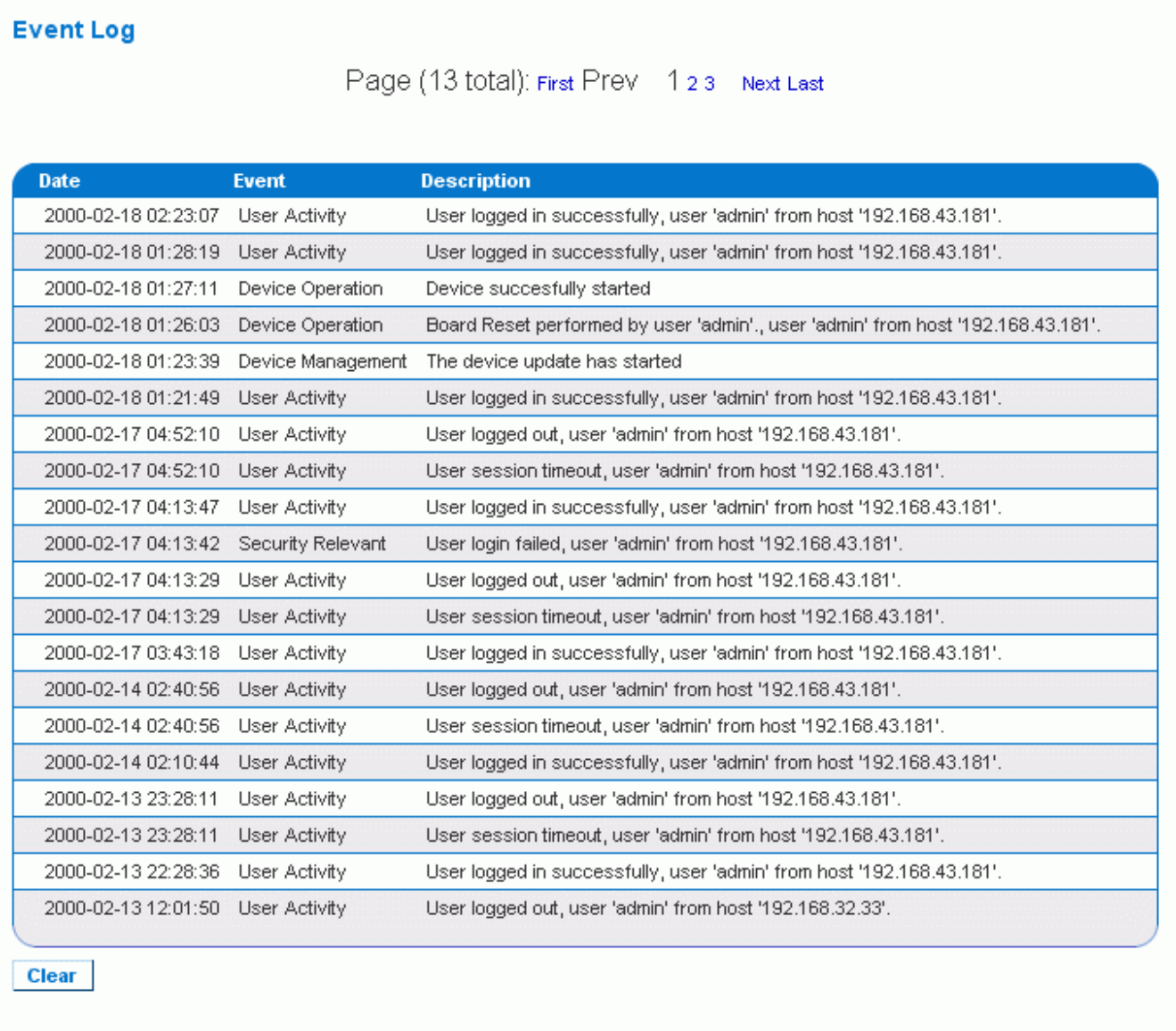


Remarque : reportez-vous à l'annexe **Types d'événements** pour en savoir plus.

6. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). La journalisation locale est configurée.

Affichage du journal des événements interne

Pour afficher le journal des événements interne, sélectionnez Maintenance, puis View Event Log (Affichage du journal des événements).



Event Log

Page (13 total): First Prev 1 2 3 Next Last

Date	Event	Description
2000-02-18 02:23:07	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-18 01:28:19	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-18 01:27:11	Device Operation	Device succesfully started
2000-02-18 01:26:03	Device Operation	Board Reset performed by user 'admin'., user 'admin' from host '192.168.43.181'.
2000-02-18 01:23:39	Device Management	The device update has started
2000-02-18 01:21:49	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-17 04:52:10	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-17 04:52:10	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:47	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:42	Security Relevant	User login failed, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:29	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-17 04:13:29	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-17 03:43:18	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-14 02:40:56	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-14 02:40:56	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-14 02:10:44	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-13 23:28:11	User Activity	User logged out, user 'admin' from host '192.168.43.181'.
2000-02-13 23:28:11	User Activity	User session timeout, user 'admin' from host '192.168.43.181'.
2000-02-13 22:28:36	User Activity	User logged in successfully, user 'admin' from host '192.168.43.181'.
2000-02-13 12:01:50	User Activity	User logged out, user 'admin' from host '192.168.32.33'.

Clear

Entrées

Pour chaque entrée, le journal des événements affiche :

- la date et l'heure de l'événement

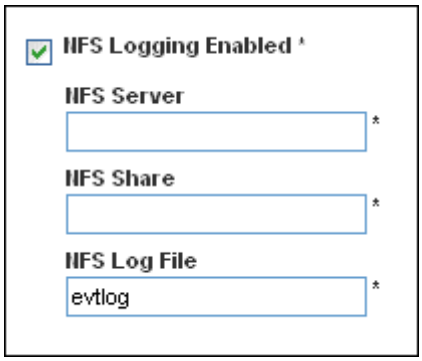
- le type d'événement (message de carte, sécurité, contrôle de l'hôte ou authentification)
- une brève description de l'événement. Par exemple, pour un événement d'authentification, l'entrée du journal indique le nom de connexion de l'utilisateur et l'adresse IP de son ordinateur.

Remarque : par défaut, le journal des événements interne affiche 20 événements par page. Reportez-vous à **Configuration du journal des événements local** *(à la page 94) pour savoir comment modifier ce nombre.*

Configuration de la journalisation NFS

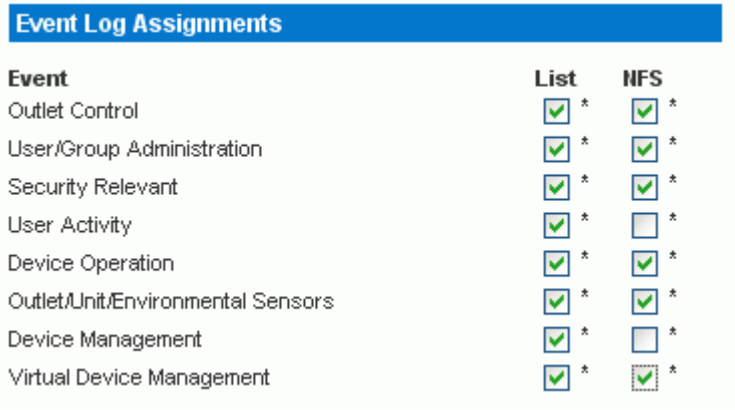
➢ *Pour configurer la journalisation NTS (Network File System) :*

1. Choisissez **Device Settings --> Event Log** (Paramètres du dispositif --> Journal des événements). La fenêtre Event Log Settings (Paramètres du journal des événements) s'affiche. Le panneau NFS Logging contrôle la journalisation NFS.



2. Cochez la case libellée **NFS Logging Enabled** (Journalisation NFS activée).
3. Entrez l'adresse IP du serveur NFS dans le champ **NFS Server** (Serveur NFS).
4. Entrez le nom du répertoire NFS partagé dans le champ **NFS Share** (Partage NFS).
5. Entrez le nom du fichier journal NFS dans le champ **NFS Log File** (Fichier journal NFS). La valeur par défaut est **evtlog**.

6. Par défaut, lorsque la journalisation NFS est activée, sept types d'événements apparaissent dans le panneau **Event Log Assignments** (Affectations du journal des événements) à droite. Ils sont tous désactivés par défaut. Pour les activer, cochez les cases correspondantes.



7. Cliquez sur **Apply** (Appliquer). La journalisation NFS est configurée.

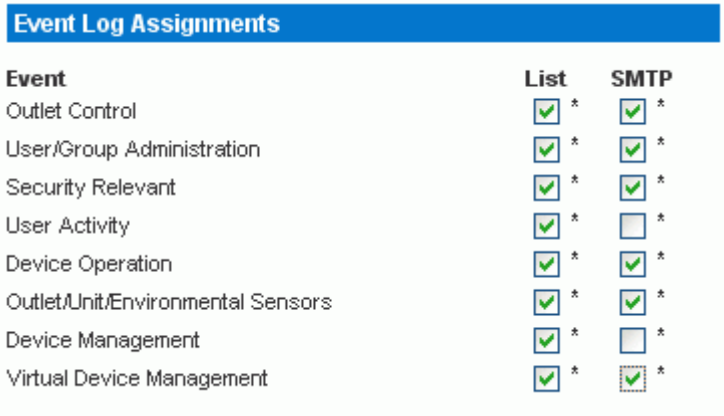
Configuration de la journalisation SMTP

➢ *Pour configurer la journalisation SMTP (Simple Mail Transfer Protocol) :*

1. Choisissez **Device Settings --> Event Log** (Paramètres du dispositif --> Journal des événements). La fenêtre Event Log Settings (Paramètres du journal des événements) s'affiche. Le panneau SMTP Logging contrôle la journalisation SMTP.

2. Cochez la case libellée **SMTP Logging Enabled** (Journalisation SMTP activée).
3. Renseignez le champ **Receiver Email Address** (Adresse électronique du destinataire).

4. Par défaut, lorsque la journalisation SMTP est activée, sept types d'événements apparaissent dans le panneau **Event Log Assignments** (Affectations du journal des événements) à droite. Ils sont tous désactivés par défaut. Pour les activer, cochez les cases souhaitées.



5. Cliquez sur **Apply** (Appliquer). La journalisation SMTP est configurée.

Important : si vous n'avez pas défini les paramètres SMTP de la Dominion PX, vous devez effectuer cette opération pour que la journalisation SMTP fonctionne. Cliquez sur le lien here (ici) au bas du panneau. Reportez-vous à la section *Configuration des paramètres SMTP* **(à la page 110) pour obtenir des instructions.**

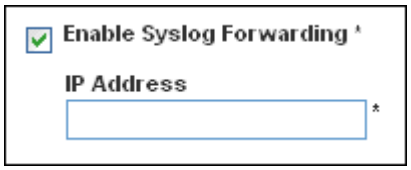
Configuration de la journalisation SNMP

La journalisation des événements peut être effectuée par l'envoi de traps SNMP à un gestionnaire SNMP tiers. Reportez-vous à l'annexe **Utilisation de SNMP** pour savoir comment activer la journalisation des événements SNMP sur Dominion PX.

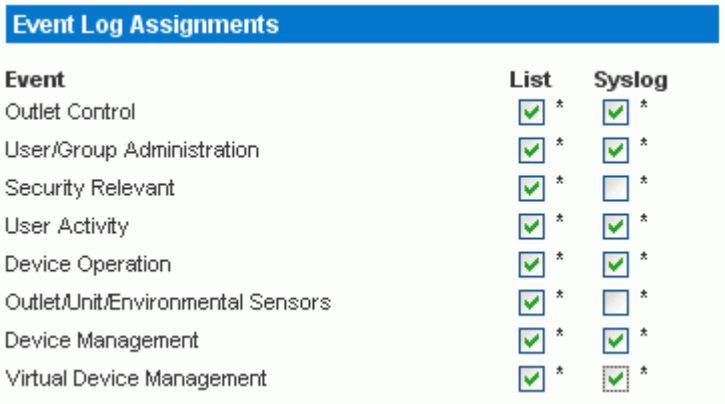
Configuration du transfert Syslog

➢ *Pour configurer le transfert Syslog :*

1. Choisissez **Device Settings --> Event Log** (Paramètres du dispositif --> Journal des événements). La fenêtre Event Log Settings (Paramètres du journal des événements) s'affiche. Le panneau Syslog Forwarding (Transfert Syslog) contrôle le transfert des journaux système.



2. Cochez la case libellée **Enable Syslog Forwarding** (Activer le transfert Syslog).
3. Renseignez le champ **IP Adresse** (Adresse IP). Il s'agit de l'adresse à laquelle le journal système est transféré.
4. Par défaut, lorsque le transfert Syslog est activé, sept types d'événements apparaissent dans le panneau **Event Log Assignments** (Affectations du journal des événements) à droite. Ils sont tous désactivés par défaut. Pour les activer, cochez les cases souhaitées.



5. Cliquez sur **Apply** (Appliquer). Le transfert Syslog est configuré.

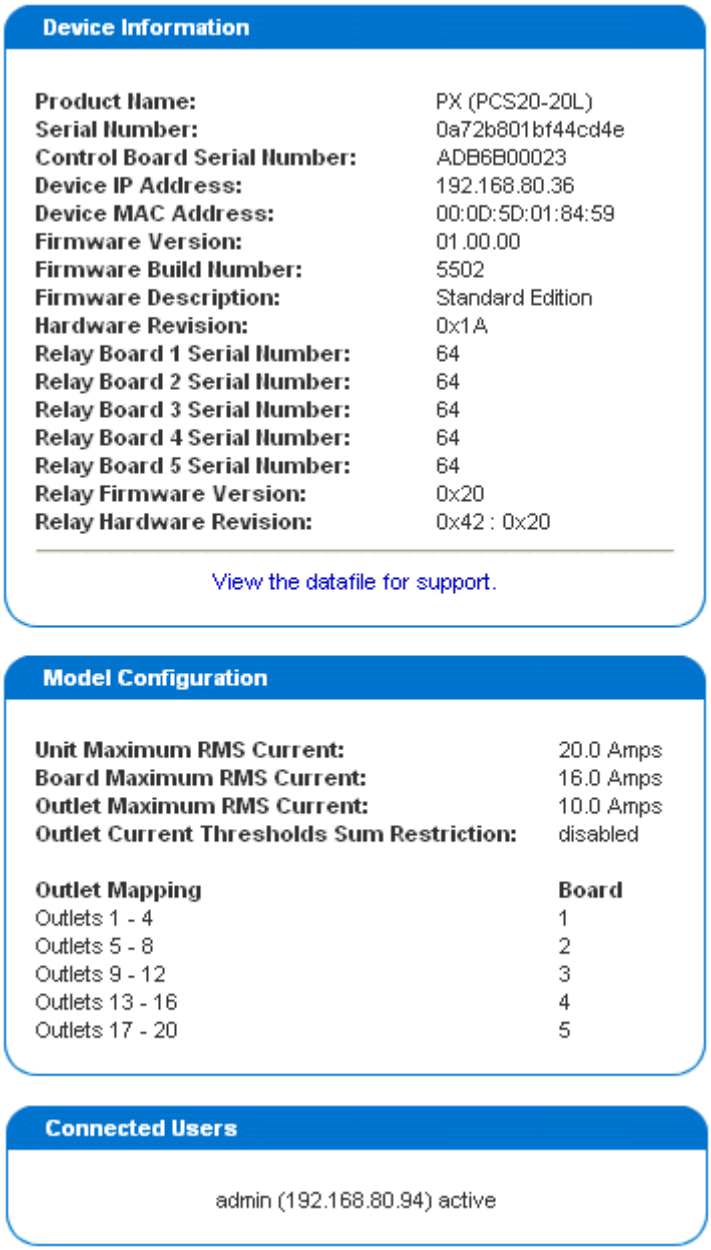
Gestion de l'unité Dominion PX

Vous pouvez afficher des informations de dispositif de base sur la Dominion PX, lui donner un nouveau nom de dispositif et modifier les paramètres réseau saisis au cours du processus de configuration initiale. Vous pouvez également définir la date et l'heure de l'unité, et configurer ses paramètres SMTP pour lui permettre d'envoyer des messages électroniques en cas d'alertes.

Affichage des informations de dispositif de base

➢ *Pour afficher des informations de base sur une unité Dominion PX :*

1. Choisissez **Maintenance --> Device Information** (Maintenance --> Informations sur le dispositif). La fenêtre Device Information s'affiche.



Device Information

Product Name:	PX (PCS20-20L)
Serial Number:	0a72b801bf44cd4e
Control Board Serial Number:	ADB6B00023
Device IP Address:	192.168.80.36
Device MAC Address:	00:0D:5D:01:84:59
Firmware Version:	01.00.00
Firmware Build Number:	5502
Firmware Description:	Standard Edition
Hardware Revision:	0x1A
Relay Board 1 Serial Number:	64
Relay Board 2 Serial Number:	64
Relay Board 3 Serial Number:	64
Relay Board 4 Serial Number:	64
Relay Board 5 Serial Number:	64
Relay Firmware Version:	0x20
Relay Hardware Revision:	0x42 : 0x20

View the datafile for support.

Model Configuration

Unit Maximum RMS Current:	20.0 Amps
Board Maximum RMS Current:	16.0 Amps
Outlet Maximum RMS Current:	10.0 Amps
Outlet Current Thresholds Sum Restriction:	disabled

Outlet Mapping	**Board**
Outlets 1 - 4	1
Outlets 5 - 8	2
Outlets 9 - 12	3
Outlets 13 - 16	4
Outlets 17 - 20	5

Connected Users

admin (192.168.80.94) active

2. Ce panneau Device Information affiche le nom du produit, le numéro de série, et les adresses IP et MAC de la Dominion PX, ainsi que des détails sur le firmware exécuté dans l'unité.
3. Pour ouvrir ou enregistrer un fichier XML fournissant des détails au support technique Raritan, cliquez sur le lien intitulé **View the datafile for support** (Afficher le fichier de données pour le support).

Affichage des informations de configuration du modèle

Pour afficher des informations sur le modèle spécifique de Dominion PX que vous utilisez, choisissez **Maintenance --> Device Information** (Maintenance --> Informations sur le dispositif). La fenêtre Device Information s'affiche. Les informations relatives à votre modèle apparaissent dans le panneau Model Configuration (Configuration du modèle) sous le panneau Device Information. Consultez la figure 64 pour en savoir plus.

Ce panneau affiche :

- le courant efficace maximum de l'unité et de la carte
- le courant efficace maximum de la prise et la restriction totale des seuils de courant
- le nombre de prises mappées à la carte.

Affichage des utilisateurs connectés

Pour afficher la liste des utilisateurs actuellement connectés à la Dominion PX, choisissez **Maintenance --> Device Information** (Maintenance --> Informations sur le dispositif). La fenêtre **Device Information** s'affiche. La liste des utilisateurs connectés apparaît dans le panneau Connected Users. Consultez la figure présentée dans la section ***Affichage des informations de dispositif de base*** (à la page 101) pour en savoir plus.

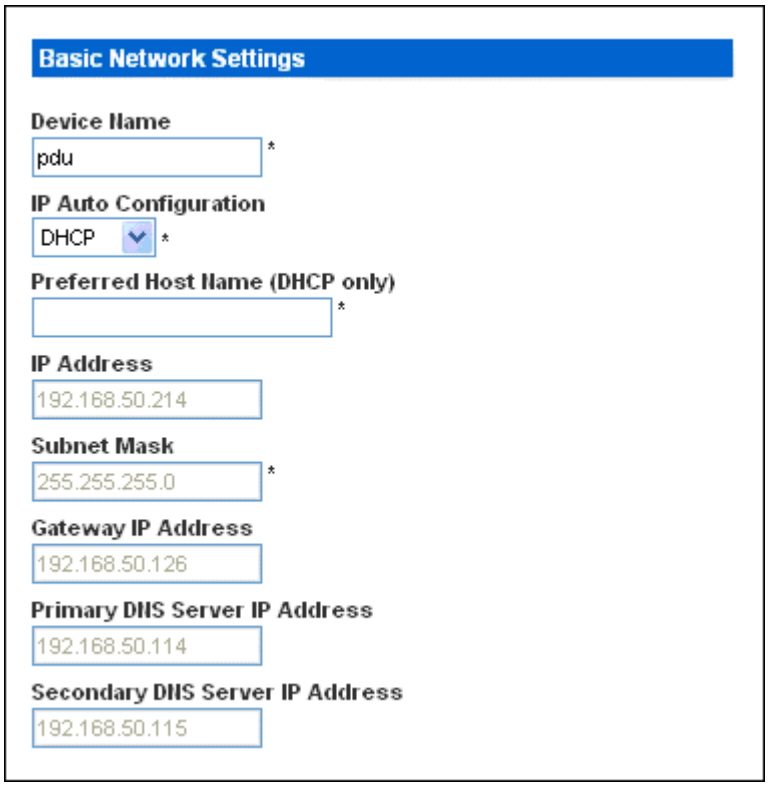
Le panneau affiche le nom d'utilisateur et l'adresse IP de chaque utilisateur, et indique si la connexion est active.

Nommage de la Dominion PX

Par défaut, le nom de dispositif de la Dominion PX est pdu. Il est recommandé de lui donner un nom plus parlant qui permet de l'identifier.

➢ *Pour nommer la Dominion PX :*

1. Choisissez **Device Settings --> Network** (Paramètres du dispositif --> Réseau). La fenêtre Network Settings (Paramètres réseau) s'affiche. Le côté gauche de la fenêtre est formé par le panneau Basic Network Settings (Paramètres réseau de base), qui contient le nom du dispositif.



2. Entrez un nouveau nom dans le champ **Device Name** (Nom du dispositif).
3. Si DHCP est sélectionné pour la configuration IP, le nom entré dans le champ **Preferred Host Name** (Nom de l'hôte privilégié) (DHCP uniquement) est enregistré avec DNS et utilisé sur les adresses IP affectées par DHCP.
4. Cliquez sur **Apply** (Appliquer). L'unité Dominion PX est renommée.

Modification des paramètres réseau

La Dominion PX a été configurée pour la connectivité réseau au cours du processus d'installation et de configuration (reportez-vous au chapitre ***Installation et Configuration*** (à la page 10) pour en savoir plus). Le cas échéant, vous pouvez modifier ces paramètres. Pour ce faire :

1. Choisissez **Device Settings --> Network** (Paramètres du dispositif --> Réseau). La fenêtre Network Settings (Paramètres réseau) s'affiche. Le côté gauche de la fenêtre est formé par le panneau Basic Network Settings (Paramètres réseau de base), qui présente les paramètres réseau actuels. Reportez-vous à la figure présentée dans la section ***Nommage de la Dominion PX*** (à la page 104) pour en savoir plus sur ce panneau.
2. Effectuez une des opérations suivantes :
   - **Auto configuration** (Configuration automatique)Pour configurer la Dominion PX automatiquement, sélectionnez DHCP ou BOOTP dans la liste déroulante du champ IP Auto Configuration (Configuration automatique IP). Si vous sélectionnez DHCP, vous pouvez également entrer un nom d'hôte privilégié (facultatif).
   - **Static IP** (IP statique) Pour entrer une adresse IP statique, sélectionnez none (néant) dans la liste déroulante du champ IP Auto Configuration (Configuration automatique IP), puis entrez :

     l'adresse IP

     le masque de sous-réseau

     l'adresse de passerelle)

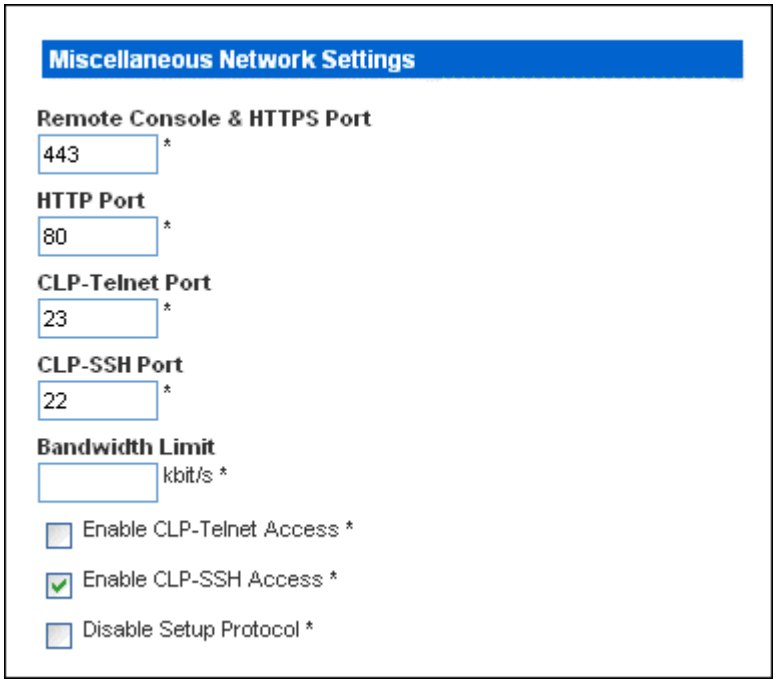
     les adresses de serveurs DNS principal et secondaire (facultatif).
3. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les paramètres réseau sont modifiés.

Modification des paramètres de communication, de port et de bande passante

Vous pouvez utiliser Telnet ou SSH pour vous connecter à l'interface CLP de la Dominion PX. Toutefois, SSH est activé par défaut contrairement à Telnet (car la communication s'effectuant en clair, elle est donc moins sûre). Vous pouvez modifier cette option, et activer ou désactiver une des applications.

Vous pouvez également définir une limite de bande passante et modifier les paramètres de port par défaut. Enfin, vous pouvez activer ou désactiver le protocole d'établissement Raritan (Raritan Setup Protocol).

1. Choisissez **Device Settings --> Network** (Paramètres du dispositif --> Réseau). La fenêtre Network Settings (Paramètres réseau) s'affiche. Le panneau **Miscellaneous Network Settings** (Paramètres réseau divers) en haut à droite contient les paramètres de communication, de port et de bande passante.



2. Par défaut, **CLP-Telnet** est désactivé et **CLP-SSH** activé. Pour modifier cette option, cliquez sur une des cases à cocher.
3. Pour définir une limite supérieure à la quantité de bande passante que Telnet ou SSH est autorisé à utiliser, entrez un nombre de kilobits par seconde dans le champ **Bandwidth Limit** (Limite de bande passante).

4. Par défaut, les ports HTTP, HTTPS, Telnet et SSH sont définis sur les ports standard de ces protocoles de communication. Si vous préférez utiliser des ports différents, vous pouvez modifier les affectations ici.
5. Cliquez sur la case libellée **Disable Setup Protocol** (Désactiver le protocole d'établissement) pour la désactiver.

   Remarque : aucun programme n'est actuellement disponible pour utiliser le protocole d'établissement avec Dominion PX. Cette option peut donc rester désactivée.

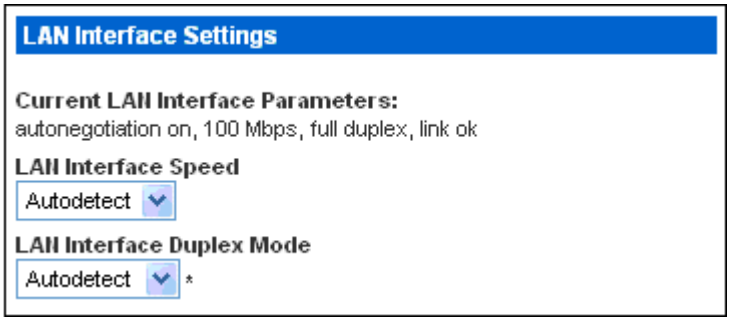
6. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les paramètres sont modifiés.

Modification des paramètres de l'interface LAN

La vitesse et le mode bidirectionnel de l'interface LAN (réseau local) ont été définis au cours du processus d'installation et de configuration (reportez-vous au chapitre ***Installation et configuration*** (à la page 10) pour en savoir plus).

➢ *Pour modifier un des paramètres :*

1. Choisissez **Device Settings --> Network** (Paramètres du dispositif --> Réseau). La fenêtre Network Settings (Paramètres réseau) s'affiche. Le panneau LAN Interface Settings (Paramètres de l'interface LAN) en bas à droite affiche la vitesse et le mode bidirectionnel de l'interface.



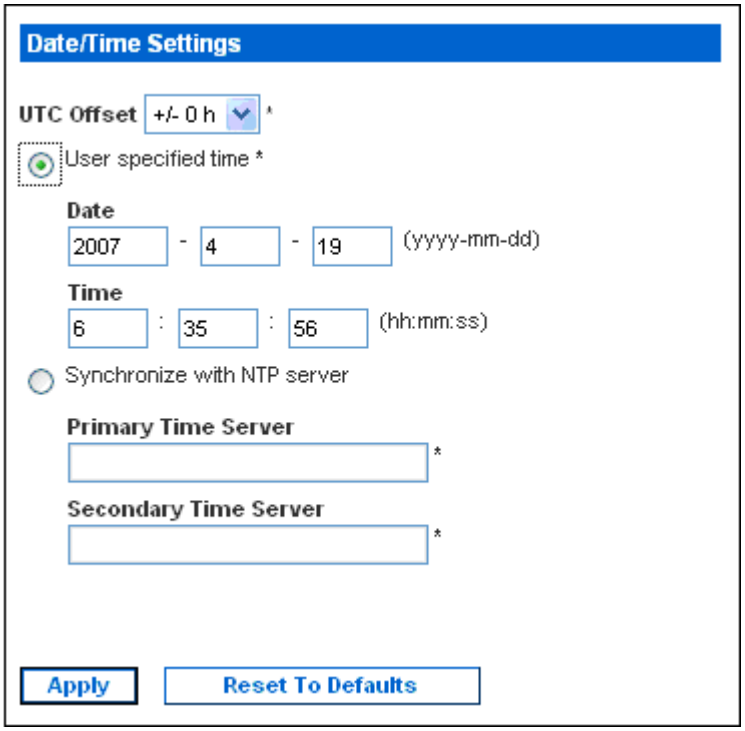
2. Pour modifier la vitesse, sélectionnez la valeur souhaitée dans la liste déroulante du champ **LAN Interface Speed** (Vitesse de l'interface LAN). Les options sont les suivantes :
   - Autodetect (Détection automatique) (le système détecte la vitesse optimum)
   - 10 Mbps
   - 100 Mbps

3. Pour modifier le mode bidirectionnel, sélectionnez la valeur souhaitée dans la liste déroulante du champ **LAN Interface Duplex Mode** (Mode bidirectionnel de l'interface LAN). Les options sont les suivantes :
   - Autodetect (Détection automatique) (le système détecte le mode optimum)
   - Half duplex (Semi-bidirectionnel)
   - Full duplex (Bidirectionnel simultané)
4. Le mode bidirectionnel Half (Semi) permet la transmission des données depuis et vers la Dominion PX, mais non simultanément. Le mode bidirectionnel Full (Simultané) permet la transmission dans les deux sens simultanément.
5. Lorsque vous avez terminé, cliquez sur **Apply** (Appliquer). Les paramètres sont modifiés.

Paramétrage de la date et de l'heure

Vous pouvez paramétrer manuellement l'horloge interne de Dominion PX ou vous pouvez vous relier à un serveur NTP (Network Time Protocol) et le laisser définir la date et l'heure.

1. Choisissez **Device Settings --> Date/Time** (Paramètres du dispositif --> Date/Heure). La fenêtre Date/Time Settings (Paramètres date/heure) s'affiche.



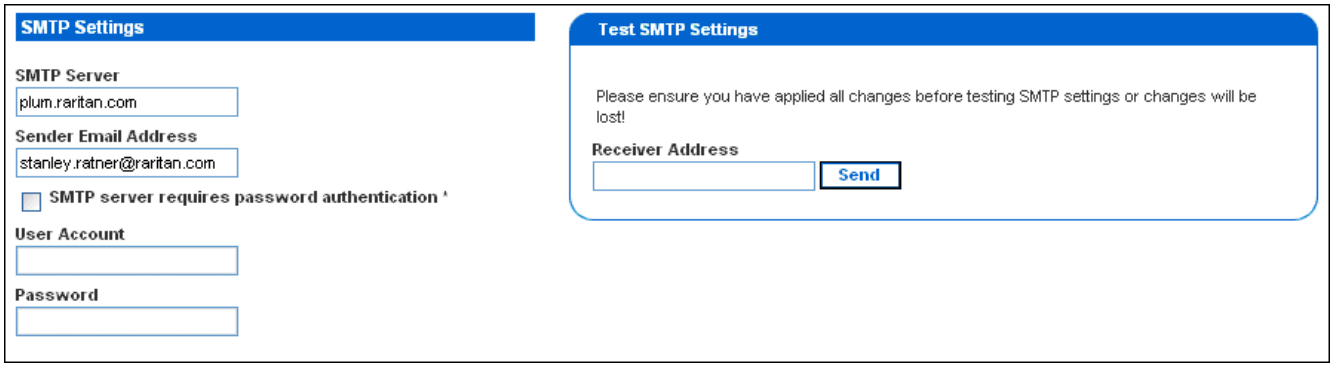
2. Entrez un fuseau horaire en sélectionnant le décalage de temps universel coordonné (UTC) dans la liste déroulante du champ **UTC Offset** (Décalage UTC) (par exemple, Heure de la côte est américaine = UTC-5).
3. Pour paramétrer la date et l'heure manuellement, cliquez sur la case d'option libellée **User specified time** (Heure spécifiée par l'utilisateur), puis renseignez les champs **Date** et **Time** (Heure). Utilisez le format aaaa/mm/jj pour la date et hh:mm:ss pour l'heure.
4. Pour laisser un serveur NTP paramétrer la date et l'heure, cliquez sur la case d'option libellée Synchronize with NTP server (Synchroniser avec le serveur NTP) et entrez les adresses IP des serveurs NTP principal et secondaire dans les champs correspondants. Mais si l'adresse IP de l'unité PX est affectée via DHCP, les adresses des serveurs NTP seront détectées automatiquement et les utilisateurs ne pourront entrer aucune donnée dans les champs des serveurs d'horloge principal et secondaire.
5. Cliquez sur **Apply** (Appliquer). Les paramètres de date et d'heure sont appliqués.

Configuration des paramètres SMTP

Dominion PX vous permet de configurer des alertes afin d'envoyer un message électronique à un administrateur particulier. Pour ce faire, il vous faut configurer les paramètres SMTP de la Dominion PX, et entrer une adresse IP pour votre serveur SMTP et le courriel de l'expéditeur.

Remarque : reportez-vous à la section **Paramétrage des alertes** *(à la page 86) pour obtenir des instructions sur la configuration des alertes pour l'envoi de messages électroniques.*

1. Choisissez **Device Settings --> SMTP Settings** (Paramètres du dispositif --> Paramètres SMTP). La fenêtre SMTP Settings s'affiche.



2. Entrez l'adresse IP du serveur de messagerie dans le champ **SMTP Server** (Serveur SMTP).
3. Entrez l'adresse électronique de l'expéditeur dans le champ **Sender Email Address** (Adresse électronique de l'expéditeur).
4. Si votre serveur SMTP requiert une authentification par mot de passe, renseignez les champs **User Account** (Compte d'utilisateur) et **Password** (Mot de passe).
5. Cliquez sur **Apply** (Appliquer). L'adresse électronique est configurée.
6. Maintenant que vous avez appliqué les paramètres SMTP, vous pouvez les tester pour vous assurer qu'ils fonctionnent correctement. Pour cela, entrez l'adresse électronique du destinataire dans le champ **Receiver Address** (Adresse du destinataire) et cliquez sur **Send** (Envoyer).

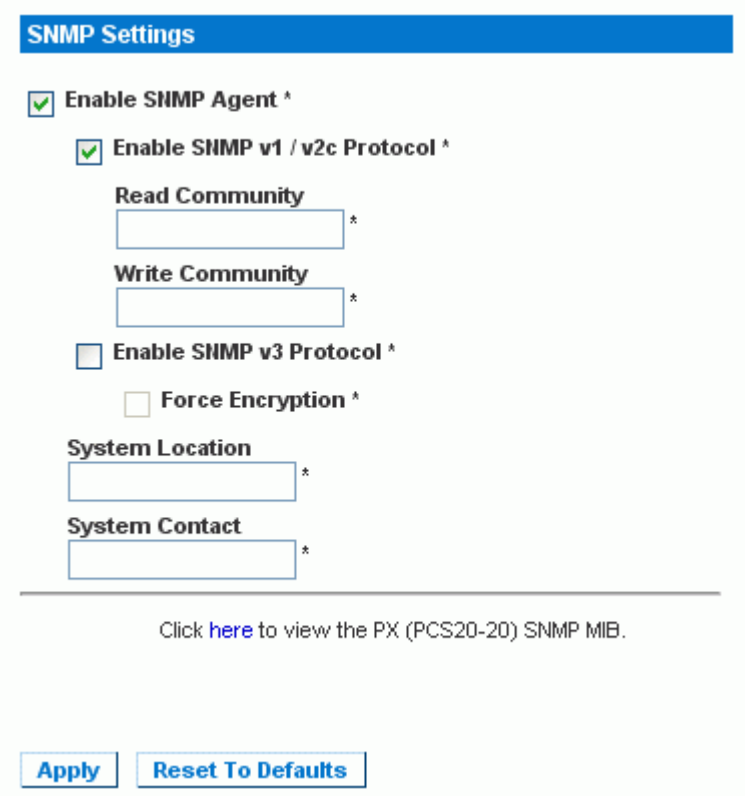
Important : ne testez pas les paramètres SMTP avant de les avoir appliqués. Sinon, ils seront perdus et vous devrez les entrer à nouveau.

Configuration des paramètres SNMP

La fenêtre SNMP Settings (Paramètres SNMP) vous permet d'activer et de désactiver la communication SNMP entre un gestionnaire SNMP et l'unité PX. L'activation de la communication SNMP permet à l'unité PX d'envoyer des traps d'événement SNMP au gestionnaire, et permet à ce dernier de récupérer et de gérer le statut d'alimentation de chaque prise.

➢ *Pour configurer la communication SNMP (nécessaire pour la transmission de traps SNMP et la gestion individuelle des prises) :*

1. Sélectionnez **Device Settings** (Paramètres du dispositif), puis **SNMP Settings** (Paramètres SNMP). La fenêtre SNMP Settings s'affiche.



2. Cochez la case **Enable SNMP Agent** (Activer l'agent SNMP) pour permettre à Dominion PX de communiquer avec des gestionnaires SNMP externes. Différentes options sont maintenant disponibles.

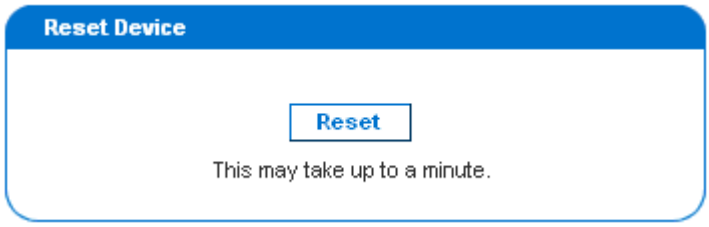
3. Cochez **Enable SNMP v1 / v2c Protocol** (Activer le protocole SNMP v1/v2c) pour permettre la communication avec un gestionnaire SNMP à l'aide du protocole SNMP v2c. Entrez ensuite la chaîne de communauté en lecture seule SNMP dans le champ **Read Community** (Communauté en lecture) et la chaîne de communauté en lecture/écriture dans le champ **Write Community** (Communauté en écriture).
4. Cochez **Enable SNMP v3 Protocol** (Activer le protocole SNMP v3) pour permettre la communication avec un gestionnaire SNMP à l'aide du protocole SNMP v3.
5. Entrez l'emplacement du système dans le champ **System Location**.
6. Entrez le contact système dans le champ **System Contact**.
7. Cliquez sur le lien au bas de la fenêtre pour télécharger un fichier MIB SNMP que Dominion PX utilisera avec votre gestionnaire SNMP.
8. Cliquez sur **Apply** (Appliquer). La configuration SNMP est terminée.

Réinitialisation de la Dominion PX

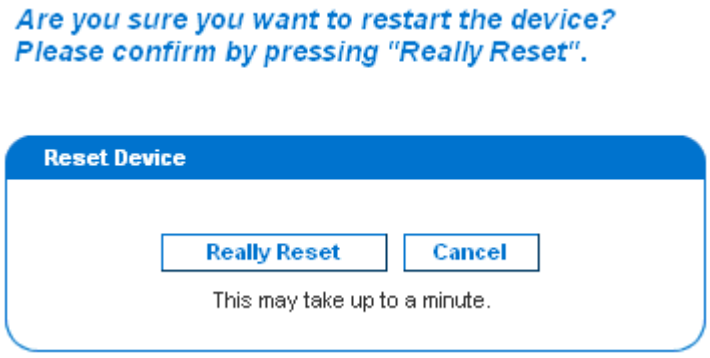
Vous pouvez utiliser la fonction Unit Reset (Réinitialisation de l'unité) pour redémarrer la Dominion PX à partir de l'interface Web.

➢ *Pour réinitialiser la Dominion PX :*

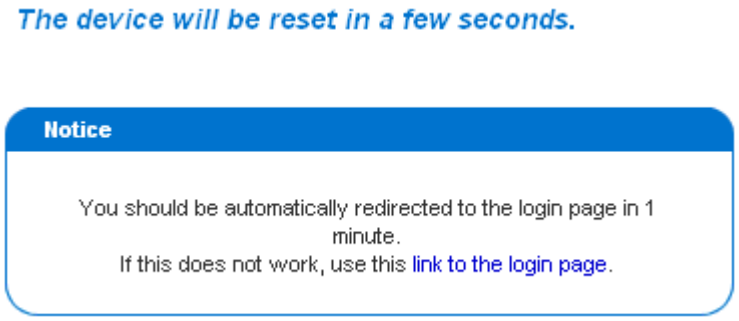
1. Choisissez **Maintenance --> Unit Reset** (Maintenance --> Réinitialisation de l'unité). La fenêtre Reset Operations (Opérations de réinitialisation) apparaît.



2. Cliquez sur Reset (Réinitialiser). Une fenêtre Reset Confirmation (Confirmation de réinitialisation) apparaît.



3. Cliquez sur le bouton **Really Reset** (Oui, réinitialiser), l'unité Dominion PX redémarre. Si vous changez d'avis, cliquez sur Cancel (Annuler) pour abandonner l'opération de réinitialisation. Si vous décidez de poursuivre la réinitialisation, la fenêtre présentée ci-dessous s'affiche et l'opération se produit. Elle dure environ une minute.



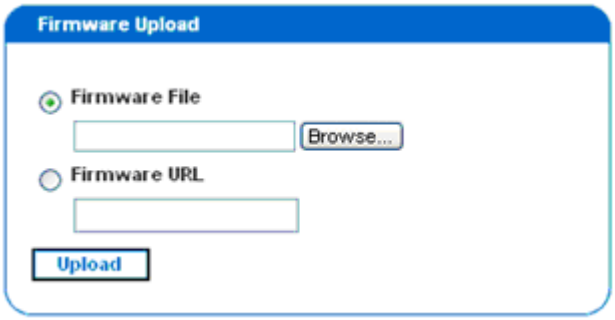
4. Lorsque la réinitialisation est terminée, l'unité Dominion PX redémarre et la fenêtre Login (Connexion) s'affiche. Vous pouvez alors vous reconnecter à l'unité Dominion PX.

Mise à jour du firmware

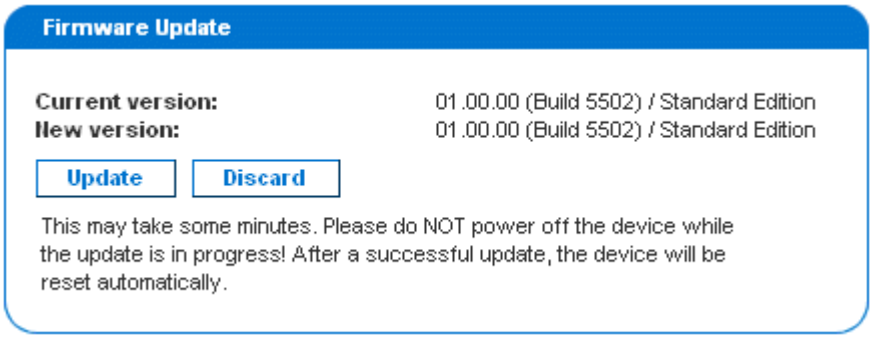
Raritan avertit les clients de la disponibilité d'un nouveau firmware pour mettre à jour la Dominion PX. Ils recevront des instructions quant à l'emplacement de téléchargement du nouveau firmware. Une fois le firmware téléchargé sur un PC, vous pouvez l'installer sur la Dominion PX depuis l'interface Web.

➢ *Pour mettre à jour le firmware :*

1. Choisissez **Maintenance --> Update Firmware** (Maintenance --> Mettre à jour le firmware). La fenêtre Firmware Upload (Téléchargement du firmware) apparaît.



2. Entrez le chemin d'accès complet au fichier de firmware dans le champ Firmware File, ou cliquez sur **Browse** (Parcourir) et sélectionnez le fichier.
3. Ou dans le champ Firmware URL (URL du firmware), entrez un lien d'URL vers l'emplacement réseau où le fichier de firmware peut être récupéré.
4. Cliquez sur **Upload** (Télécharger vers le serveur). La fenêtre Firmware Update (Mise à jour du firmware) apparaît. Elle indique la version actuelle du firmware et la nouvelle, et vous offre une dernière possibilité d'abandonner la mise à jour.

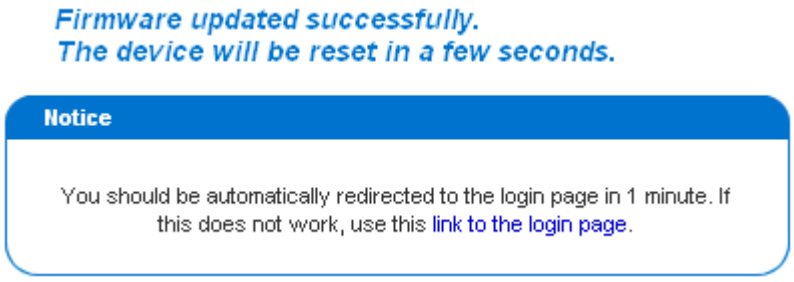


5. Pour continuer la mise à jour, cliquez sur **Update** (Mettre à jour). Pour abandonner la mise à jour, cliquez sur **Discard** (Annuler). La mise à jour peut prendre plusieurs minutes. Le panneau Status (Statut) sur la gauche suit la progression de la mise à niveau.

Remarque : NE METTEZ PAS la Dominion PX hors tension pendant la mise à jour. Pour signaler au niveau du rack qu'une mise à jour est en cours, les voyants des prises clignotent et le panneau d'affichage à trois chiffres de l'unité indique « FuP ».

---

6. A la fin de la mise à jour, un message similaire à celui présenté ci-dessous apparaît pour indiquer que la mise à jour a abouti. La Dominion PX est réinitialisée et la fenêtre Login (Connexion) réapparaît. Vous pouvez à présent vous connecter et reprendre la gestion de la Dominion PX.



Remarque : si vous utilisez Dominion PX avec un gestionnaire SNMP, il est recommandé de télécharger à nouveau le fichier MIB Dominion PX après la mise à jour du firmware de l'unité. Ainsi, votre gestionnaire SNMP dispose du fichier MIB correspondant à la version que vous utilisez. Reportez-vous à l'annexe ***Utilisation de SNMP*** *pour en savoir plus.*

Groupement des prises

A l'aide de la fonction Outlet Grouping (Groupement des prises), les utilisateurs peuvent combiner des prises d'unités Dominion PX distinctes en un groupe unique et logique qui permet de les gérer à partir d'une seule Dominion PX. Les prises groupées se mettent sous tension (et hors tension) ensemble, le groupement est donc idéal pour les serveurs dont les alimentations sont branchées sur plusieurs unités Dominion PX.

Les utilisateurs, ou le groupe auquel ils appartiennent, doivent disposer de l'autorisation **Outlet Group Configuration** (Configuration des groupes de prises) sous User/Group System Permissions (Autorisations système pour utilisateur/groupe) pour gérer ou accéder à un groupe de prises.

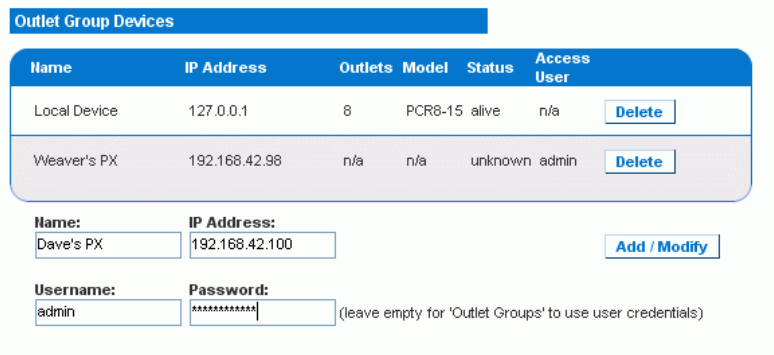
Remarque : la fonction Outlet Grouping prend en charge l'ajout de prises de quatre autres unités Dominion PX au plus. Toutes les unités doivent être accessibles sur IP et exécuter la version 1.1 ou supérieure du firmware.

Identification d'autres unités Dominion PX

Pour ajouter des prises d'autres unités Dominion PX, vous devez en premier lieu identifier les unités Dominion PX qui vont partager leurs prises.

➢ *Pour identifier d'autres unités Dominion PX :*

1. Sélectionnez **Outlet Groups** (Groupes de prises), puis **Outlet Group Devices** (Dispositifs du groupe de prises). La fenêtre Outlet Group Devices s'affiche.



2. Entrez un nom pour identifier l'unité Dominion PX que vous souhaitez ajouter dans le champ **Name**.
3. Entrez l'adresse IP de l'unité Dominion PX que vous souhaitez ajouter dans le champ **IP Address**.
4. Si vous le souhaitez, entrez dans les champs **Username** (Nom d'utilisateur) et **Password** (Mot de passe) les valeurs utilisées pour l'authentification sur l'unité Dominion PX ajoutée. Vous pouvez laisser ces champs vides pour utiliser les mêmes nom d'utilisateur et mot de passe que la Dominion PX à laquelle vous accédez actuellement.
5. Cliquez sur **Add/Modify** (Ajouter/Modifier). La nouvelle Dominion PX est maintenant disponible pour le groupement de prises.

Pour modifier le nom, ou les nom d'utilisateur et mot de passe utilisés pour accéder à une Dominion PX participante, il suffit de retaper les informations pour la même unité Dominion PX et de cliquer à nouveau sur **Add/Modify**.

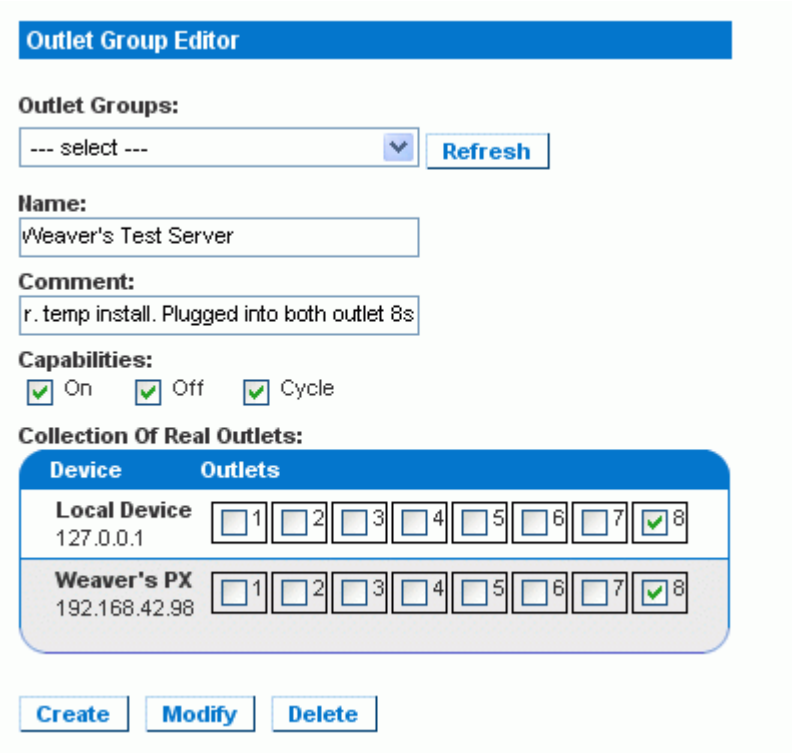
Remarque : vous pouvez ajouter à nouveau l'unité Dominion PX à laquelle vous accédez (si vous l'avez supprimée de la liste) ou modifier ses données en utilisant l'adresse 127.0.0.1.

Regroupement des prises

Lorsque les unités Dominion PX participantes ont été ajoutées à la liste des dispositifs de groupe de prises, leurs prises individuelles peuvent être regroupées. Les prises regroupées se mettent sous et hors tension ensemble grâce à un panneau de configuration de la Dominion PX sur laquelle le groupe de prises a été créé.

➢ *Pour regrouper des prises:*

1. Sélectionnez **Outlet Groups** (Groupes de prises), puis **Outlet Group Editor** (Editeur des groupes de prises). La fenêtre **Outlet Group Editor** s'affiche.



2. Saisissez le nom du groupe de prises dans le champ **Name**. Il est recommandé de donner à ce groupe un nom aisément reconnaissable qui vous permettra d'identifier les dispositifs qui lui sont connectés.
3. Entrez un commentaire sur le groupe de prises dans le champ **Comment** (Commentaire). Ce commentaire permettra d'identifier plus précisément les dispositifs alimentés par ce groupe.
4. Sous le champ **Capabilities** (Capacités), cochez la case des fonctions Power Control (Gestion de l'alimentation) qui doivent être disponibles pour cette prise.

5. Une liste d'unités Dominion PX disponibles et de leurs prises apparaît sous **Collection of Real Outlets** (Ensembles de prises réelles). Cochez la case représentant la prise physique souhaitée pour l'ajouter au groupe. Toutes les prises cochées sont regroupées lorsque vous cliquez sur **Create** (Créer).

   Remarque : il n'est pas recommandé d'ajouter une prise physique à plusieurs groupes de prises.

6. Cliquez sur **Create** (Créer). Le groupe de prises est créé et ajouté à la liste Outlet Groups (Groupes de prises).

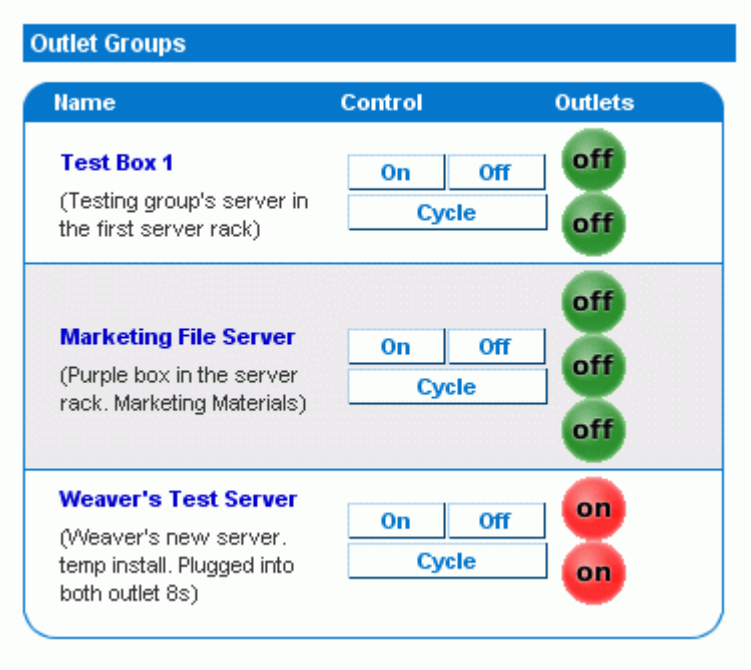
Les prises regroupées sont gérées ensemble. Evitez les actions les affectant individuellement, comme en mettre une SOUS ou HORS tension, ou en débrancher une des unités Dominion PX participantes. Une fois les prises groupées, la gestion de leur alimentation doit être effectuée dans la liste Outlet Groups (Groupes de prises).

Gestion des groupes de prises

Tous les groupes de prises créés à partir de cette Dominion PX apparaissent dans la liste Outlet Groups. A partir de celle-ci, vous pouvez mettre SOUS ou HORS tension, ou effectuer l'alimentation cyclique du groupe de prises (si cette fonction est disponible).

➢ *Pour gérer l'alimentation d'un groupe de prises :*

1. Sélectionnez **Outlet Groups** (Groupes de prises), puis **Outlet Group Details** (Détails sur le groupe de prises). La liste Outlet Groups apparaît.



Remarque : seuls les groupes de prises créés à partir de cette Dominion PX particulière apparaissent dans cette liste Outlet Groups. Les groupes de prises créés sur une autre Dominion PX ne sont pas répertoriés ici, même s'ils contiennent des prises de cette unité.

2. Pour activer, désactiver un groupe de prises ou effectuer son alimentation cyclique, cliquez sur **On**, **Off** ou **Cycle** dans la rangée du groupe.
3. Il vous sera demandé de confirmer votre choix. Cliquez sur **OK** pour poursuivre.

4. La page est actualisée une première fois pour indiquer que la commande souhaitée a été effectuée, puis à nouveau quelques secondes plus tard pour mettre à jour le statut du groupe de prises.

Remarque : la page doit être chargée ou actualisée entièrement avant la sélection d'une action. Si vous sélectionnez une action avant la mise à jour du statut de tous les groupes de prises, la commande est ignorée.

Si vous souhaitez consulter ou modifier la composition d'un groupe de prises, cliquez sur le nom de ce groupe dans la liste pour afficher la fenêtre Outlet Group Editor (Editeur des groupes de prises) lui correspondant.

Modification ou suppression des groupes de prises

1. Sélectionnez **Outlet Groups** (Groupes de prises), puis **Outlet Group Editor** (Editeur des groupes de prises). La fenêtre **Outlet Group Editor** s'affiche.
2. Dans la liste déroulante du champ **Outlet Groups** (Groupes de prises), sélectionnez le groupe de prises souhaité.
3. Les détails le concernant s'affichent. Changez le nom, le commentaire, les capacités ou les prises réelles incluses si vous modifiez le groupe.
4. Cliquez sur **Modify** (Modifier) pour enregistrer vos modifications ou sur **Delete** (Supprimer) pour retirer le groupe de la liste Outlet Groups.

Suppression des dispositifs du groupe de prises

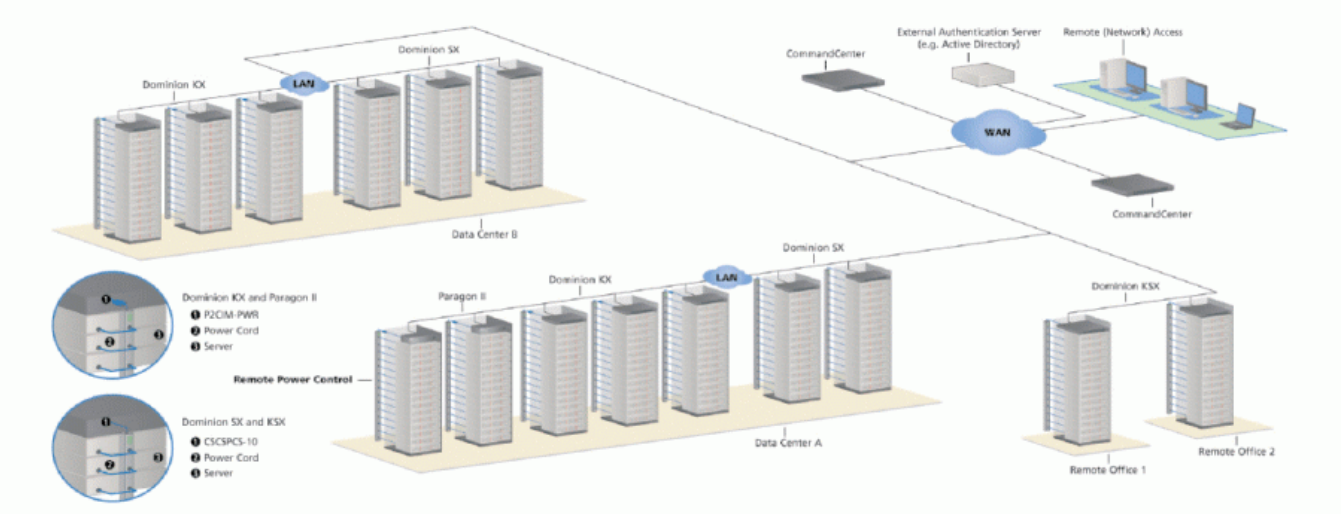
➢ *Pour supprimer une Dominion PX d'un groupement de prises qui n'est plus disponible ou utilisé:*

1. Sélectionnez **Outlet Groups** (Groupes de prises), puis **Outlet Group Devices** (Dispositifs du groupe de prises). La fenêtre Outlet Group Devices apparaît et présente une liste des unités Dominion PX connues.
2. Cliquez sur **Delete** (Supprimer) pour la Dominion PX que vous souhaitez retirer du groupe de prises.

Remarque : si vous supprimez une Dominion PX dont des prises se trouvent dans un groupe, celles-ci seront supprimées du groupe, mais ce dernier continuera d'exister. Retirez le groupe à l'aide de la fenêtre Outlet Group Editor (Editeur des groupes de prises).

Il n'est pas recommandé de supprimer le dispositif hôte (la Dominion PX à laquelle vous avez accès actuellement) de la liste Outlet Group Devices (Dispositifs du groupe de prises). Si vous le supprimez, vous pouvez le rajouter à la liste à l'aide de l'adresse IP 127.0.0.1.

Chapitre 6 Intégration



Dans ce chapitre

Dominion KX

Dominion KX (associé au tout dernier firmware) prend en charge jusqu'à huit unités Dominion PX, et requiert P2CIM-PWR et un câble CAT5 droit. Vous pouvez associer jusqu'à quatre prises à une cible ; ces quatre prises peuvent provenir d'unités Dominion PX distinctes, si nécessaire.

Application KX Manager (Dominion KX-I uniquement)

L'application KX Manager de Raritan permet de configurer des associations.

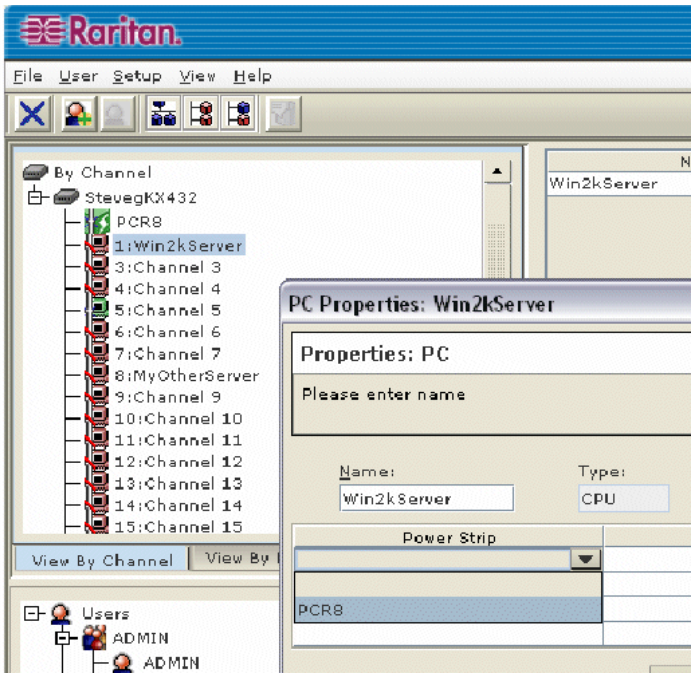
➢ *Pour configurer des associations :*

1. Sélectionnez la cible.
2. Modifiez les options **Properties** (Propriétés) et choisissez les prises à associer. Celles-ci sont automatiquement renommées avec le nom de la cible.

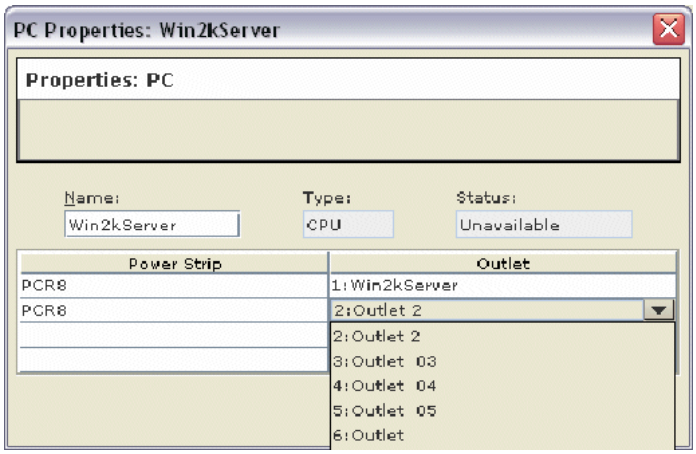
3. Sélectionnez RRC pour le contrôle.
4. Sélectionnez la cible.
5. Sélectionnez On, Off ou Recycle dans le menu contextuel.
6. Reportez-vous au manuel d'utilisation de KX pour en savoir plus.

Associer des prises à une cible

1. Sélectionnez la cible ; sélectionnez Properties (Propriétés) dans le menu contextuel.
2. Sélectionnez jusqu'à huit unités Dominion PX dans la liste déroulante.



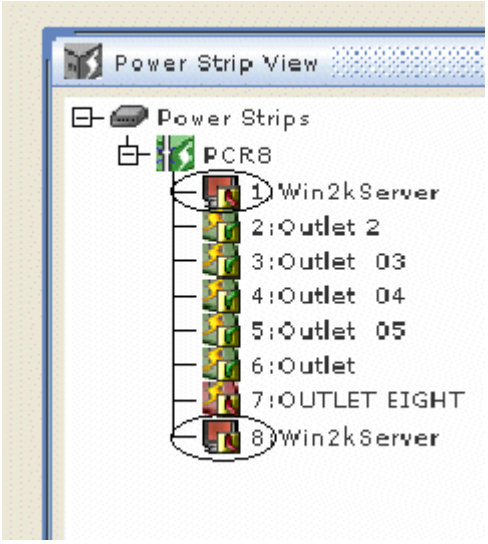
3. Sélectionnez jusqu'à quatre prises au total sur les unités PX.



4. Notez que l'icône de la cible indique maintenant qu'elle est alimentée.

5. Notez que l'icône de la prise indique maintenant une association.

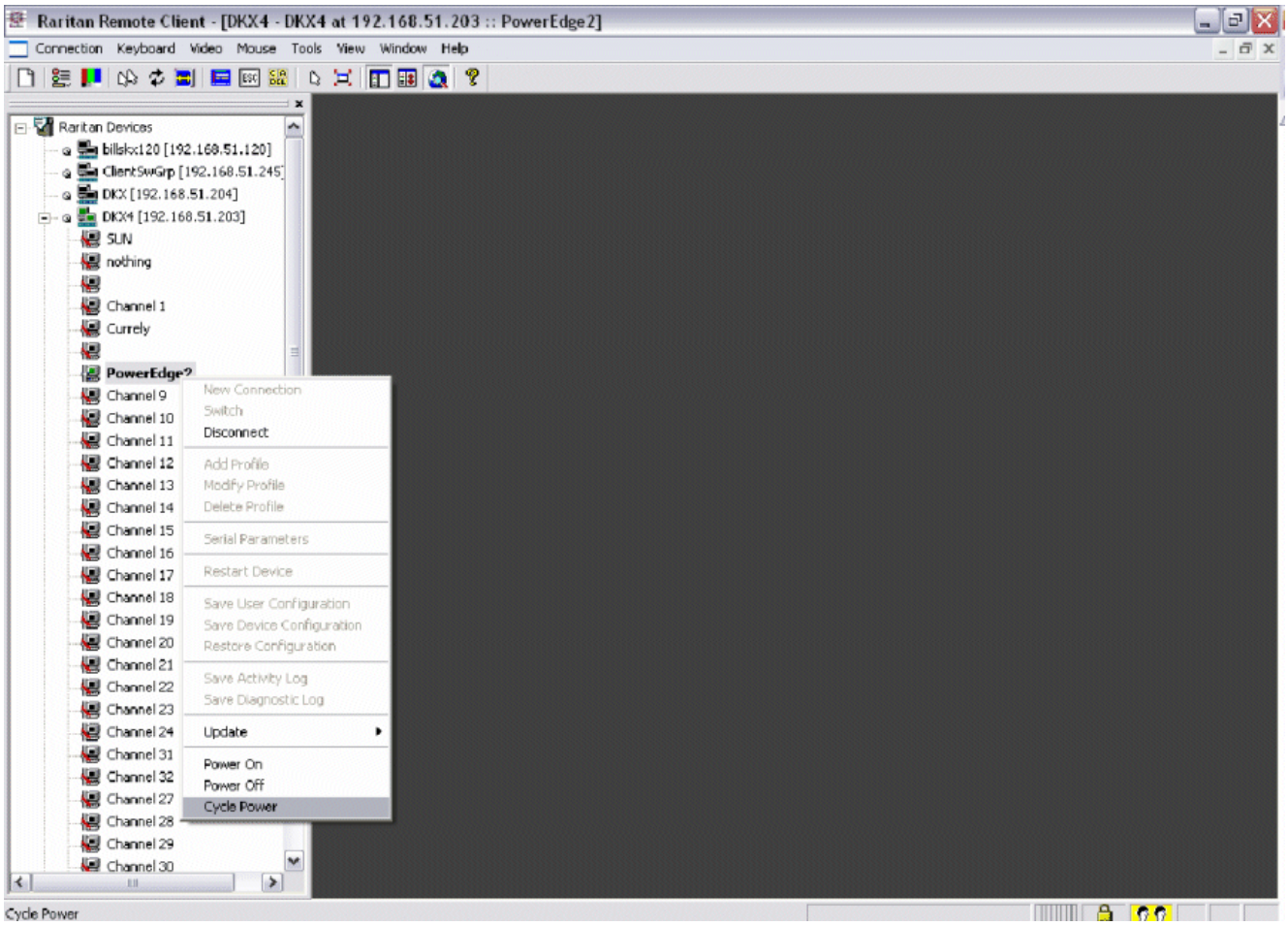
6. Notez que le nom de la prise indique maintenant le nom de la cible.



Gérer l'alimentation d'une cible

1. Sélectionnez la cible associée aux prises.

2. Choisissez une option entre Power On, Power Off ou Cycle Power.



Dominion KX-II

➢ *Pour utiliser la fonction de gestion de l'alimentation de KX II :*

1. Connectez Dominion PX à votre serveur cible.
2. Nommez l'unité Dominion PX.
3. Associez des prises de Dominion PX au serveur cible.
4. Utilisez la gestion de l'alimentation à distance du serveur cible de la page Port Access (Accès aux ports).

Reportez-vous au manuel d'utilisation de Dominion KX-II pour en savoir plus.

Paragon II

Paragon II requiert P2CIM-PWR et un câble Cat5 droit. Vous pouvez associer jusqu'à quatre prises à une cible ; ces quatre prises peuvent provenir d'unités Dominion PX distinctes, si nécessaire.

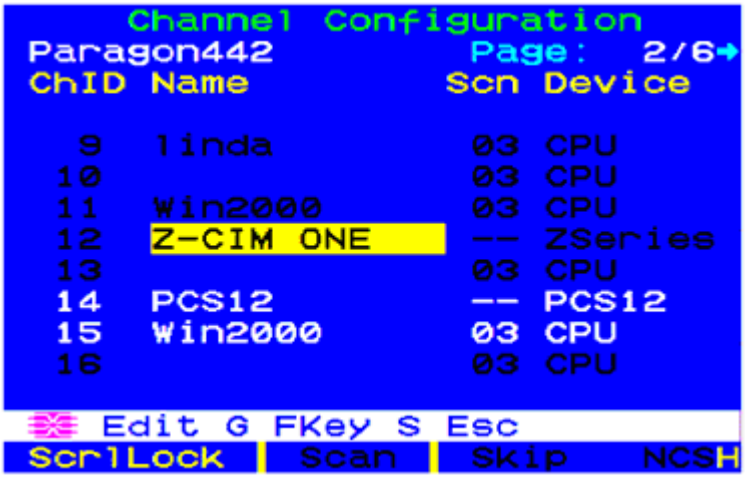
Application Paragon Manager

L'application Paragon Manager de Raritan permet de configurer des associations.

1. Dans Paragon Manager, sélectionnez la cible.
2. Cliquez sur l'icône de la cible et faites-la glisser sur les prises souhaitées.
3. Celles-ci sont automatiquement renommées avec le nom de la cible.
4. Pour activer, désactiver ou réactiver la cible, cliquez dessus et appuyez sur la touche F3 ; sélectionnez On, Off ou Recycle dans le menu déroulant.

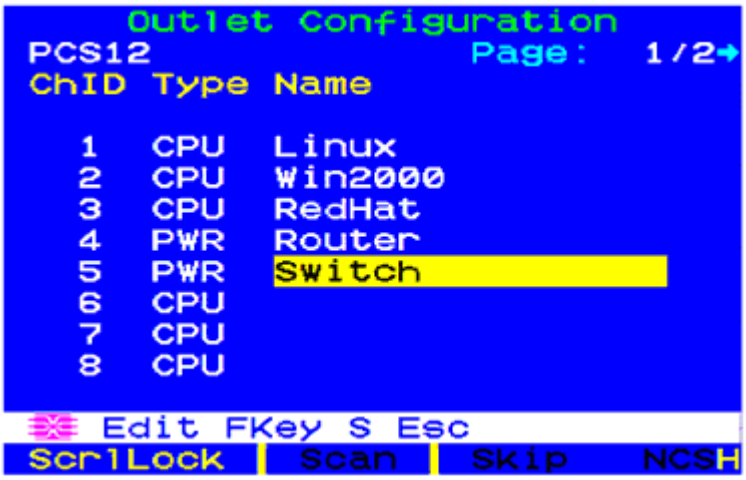
Ajouter une unité Dominion PX dans Paragon II

Vous pouvez ajouter une unité Dominion PX comme n'importe quel dispositif de deuxième niveau. Votre unité Paragon II détecte automatiquement la Dominion PX et remplace le type de dispositif par PCR8, PCS12 ou PCS20. De l'affichage à l'écran, appuyez sur F5 pour ouvrir la page Channel Configuration (Configuration des canaux). Sélectionnez le canal et remplacez son nom par défaut par un nom l'identifiant pour l'unité Dominion PX.



Associer des prises à une cible

De l'affichage à l'écran, appuyez sur **F5** pour ouvrir la page Channel Configuration (Configuration des canaux), puis un canal. Appuyez sur G pour ouvrir l'écran spécial de deuxième niveau (page Outlet Configuration (Configuration des prises)).



Gérer l'alimentation d'une cible

➢ *Pour gérer l'alimentation d'une cible :*

1. A partir du menu Channel Selection by Name (Sélection des canaux par nom) OU Channel Selection (Sélection de canal), appuyez sur **F3** pour contrôler l'alimentation. Le message « X-Power Off; O-Power On; R-Recycle Power » (X-Alimentation désactivée ; O-Alimentation activée ; R-Alimentation réactivée) apparaît sur la ligne d'aide défilante.
2. Lorsqu'aucune prise n'est associée au serveur, « No power outlets » (Aucune prise d'alimentation) s'affiche.
3. Lorsqu'aucune autorisation d'accès aux prises associées au serveur n'existe, « Permission denied » (Autorisation refusée) s'affiche.
4. Sinon, Paragon permute automatiquement sur le canal pour que le serveur soit affiché en arrière-plan. Si la permutation échoue, le message « Switch fail » (Echec de la permutation) s'affiche.
5. Si elle réussit, toutes les prises associées au serveur s'affichent comme présenté à gauche.
6. Sélectionnez une prise et choisissez X, O ou R :
7. Si vous choisissez O, la commande On est exécutée.

8. Si vous choisissez X ou R, le message « Are you sure (yes/no)? » (Etes-vous certain (oui/non) ?) s'affiche. Vous devez entrer « yes » (insensible à la casse) pour exécuter la commande. Le mot doit être saisi en entier.

Gérer l'alimentation d'une prise

Dans le menu Channel Selection (Sélection des canaux) (et NON dans Channel Selection by Name (Sélection des canaux par nom)), vous pouvez accéder aux ports Dominion PX individuels et contrôler l'alimentation.

Sélectionnez une prise et choisissez X, O ou R :

- Lorsqu'aucune autorisation d'accès à la prise n'existe, « Permission denied » (Autorisation refusée) s'affiche.
- Si vous choisissez O, la commande On est exécutée.

Si vous choisissez X ou R, le message « Are you sure (yes/no)? » (Etes-vous certain (oui/non) ?) s'affiche. Vous devez entrer « yes » (insensible à la casse) pour exécuter la commande. Y, y ou ye, etc. n'est pas acceptable. Le mot yes doit être saisi en entier.

Appuyer sur <ENTREE> ne sert à rien.

Le message « X-Power Off; O-Power On; R-Recycle Power » (X-Alimentation désactivée ; O-Alimentation activée ; R-Alimentation réactivée) apparaît sur la ligne d'aide défilante.

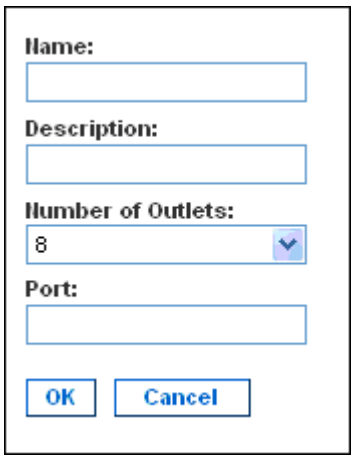
Dominion SX

Lorsque vous vous connectez à une unité Dominion SX, vous êtes autorisé à associer une ou plusieurs de ses prises à des ports DSX spécifiques.

Configurer une unité d'alimentation Dominion PX sur Dominion SX

1. Choisissez **Setup --> Power Strip Configuration** (Paramétrage --> Configuration des barrettes d'alimentation).

2. Cliquez sur **Add** (Ajouter). L'écran Power Strip Configuration (Configuration des barrettes d'alimentation) s'affiche.

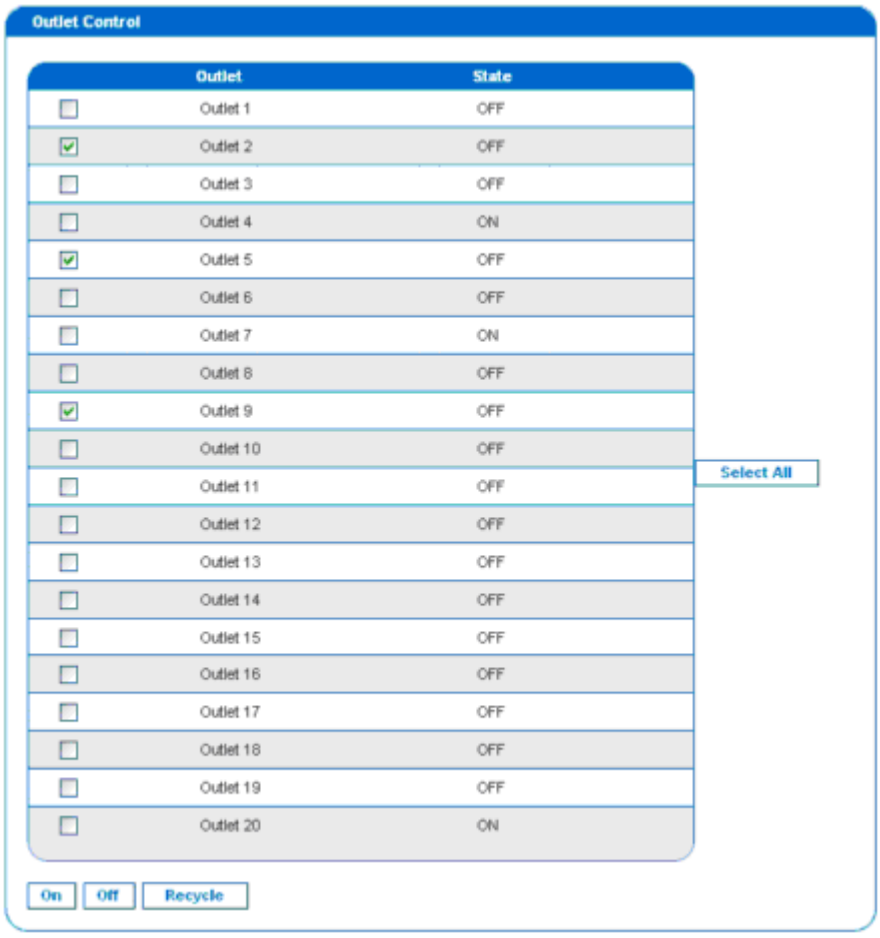


3. Entrez un nom et une description dans les champs Name et Description.
4. Dans la liste déroulante du champ **Number of Outlets** (Nombre de prises), sélectionnez le nombre de prises.
5. Entrez le numéro du port dans le champ Port.
6. Cliquez sur **OK**.

Gérer l'alimentation

1. Choisissez **Power Control --> Power Strip Power Control** (Gestion de l'alimentation --> Gestion de l'alimentation des barrettes d'alimentation).

2. L'écran Outlet Control (Gestion de l'alimentation) apparaît.



3. Cochez la case correspondant au numéro des prises que vous souhaitez gérer, puis cliquez sur les boutons On/Off pour activer ou désactiver les prises sélectionnées.

4. Un message de confirmation apparaît pour indiquer que l'opération a réussi.

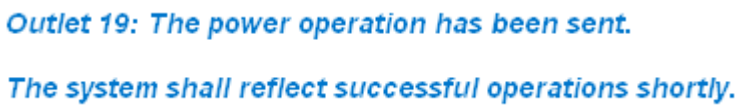
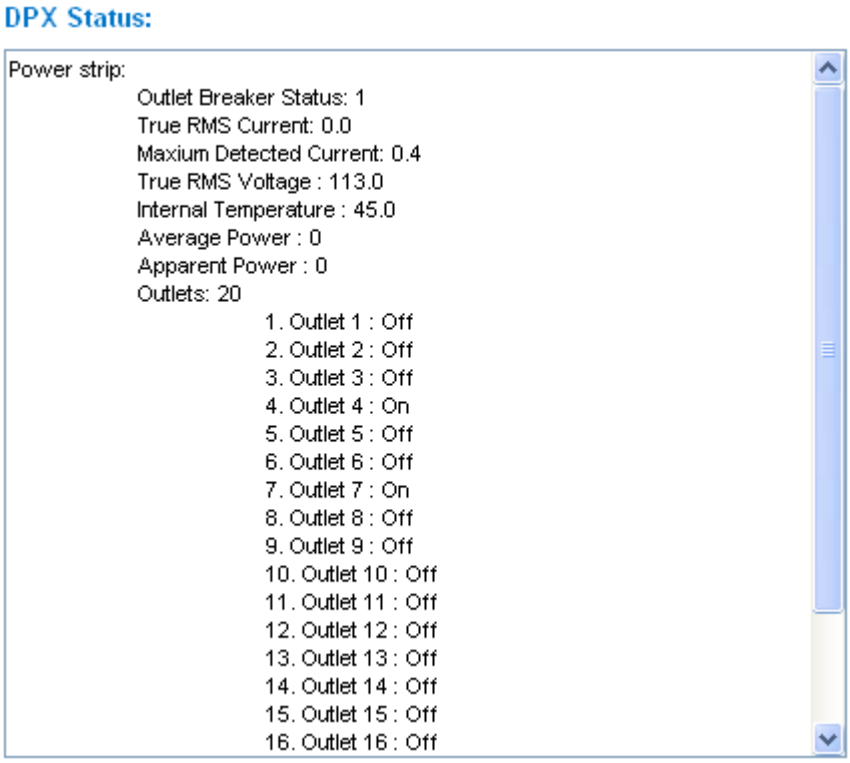


Figure 1: Ecran de confirmation pour une prise

Vérifier le statut des barrettes d'alimentation

1. Choisissez **Power Control --> Power Strip Status** (Gestion de l'alimentation --> Statut des barrettes d'alimentation).



2. Une boîte de statut affiche des détails concernant la Dominion PX gérée, notamment l'état d'alimentation de chacune de ses prises.

Dominion KSX

La prise en charge de KSX pour Dominion PX n'est pas disponible actuellement. Cependant, l'unité Dominion PX peut être gérée comme cible série sur un des ports série de KSX, en interagissant via l'interface CLP.

CommandCenter Secure Gateway

Vous pouvez gérer une Dominion PX à partir de CommandCenter Secure Gateway (CC-SG) si elle est connectée à l'aide d'un des ces produits Raritan :

- Dominion SX
- Dominion KX
- Paragon II
- Reportez-vous au manuel de l'administrateur CC-SG pour en savoir plus.

REMARQUE : si vous devez redémarrer ou mettre HORS tension Dominion PX alors qu'elle est intégrée à un produit Raritan sous la gestion de CC-SG, INTERROMPEZ la gestion du produit intégré tant que Dominion PX n'est pas complètement remise SOUS tension. Sinon, les prises risquent d'être supprimées de la vue CC-SG et vos associations d'alimentation risquent d'être perdues lorsque Dominion PX revient en ligne.

Annexe A Modèles Dominion PX

Modèle	Rack	V	Courant	Type de prise	Nombre de prises	Type de fiche	Nombre de circuits	Nombre de disjoncteurs
DPCR8-15	1U	120	15	Nema 5-15R	8	Nema 5-15P	1	Néant
DPCR8A-16	1U	230	16	IEC320 C13	8	IEC60309 16A	1	Néant
DPCR8A-20L6	1U	208	20	IEC320 C13	8	Nema L6-20P	1	Néant
DPCS12-20	0U	120	20	Nema 5-15R	12	Nema 5-20P	1	Néant
DPCS12A-16	0U	230	16	IEC320 C13	12	IEC60309 16A	1	Néant
DPCS20-20	0U	120	20	Nema 5-15R	20	Nema 5-20P	1	Néant
DPCS20-20L	0U	120	20	Nema 5-15R	20	Nema L5-20P	1	Néant
DPCS20-30L	0U	120	30	Nema 5-15R	20	Nema L5-30P	1	2 (double)
DPCS20A-16	0U	230	16	IEC320 C13	20	IEC60309 16A	1	Néant
DPCS20A-32	0U	230	32	IEC320 C13	20	IEC60309 32A	1	2
DPCS20A-20L6	0U	208	20	IEC320 C13	20	Nema L6-20P	1	Néant
DPCS20A-30L6	0U	208	30	IEC320 C13	20	Nema L6-30P	1	2 (double)
DPCR20-20	2U	120	20	Nema 5-15R	20	Nema 5-20P	1	Néant
DPCR20-30L	2U	120	20	Nema 5-15R	20	Nema L5-30P	1	2 (double)
DPCR20A-32	2U	230	32	IEC320 C13	20	IEC60309 32A	1	2
DPCR20A-30L6	2U	208	30	IEC320 C13	20	Nema L6-30P	1	2

Remarque : selon les réglementations NEC, la valeur nominale des unités nord-américaines doit être réduite de 20 %. Par exemple, une unité Dominion PX dont la puissance nominale est de 30 A peut fournir 24 A de courant en Amérique du Nord.

Quel que soit le modèle Dominion PX, la charge de courant maximum est de 10 A par prise.

Dans ce chapitre

Spécifications matérielles

Modèle	Poids (kg)	Dimensions
DPCR8-15	3,64	440 x 167 x 43 mm
DPCR8A-16	3,64	440 x 167 x 43 mm
DPCR8A-20L6	3,64	440 x 167 x 43 mm
DPCS12-20	3,48	57 x 49,5 x 1 253 mm
DPCS12A-16	3,48	57 x 49,5 x 1 253 mm
DPCS20-20	5,08	57 x 43 x 1 796 mm
DPCS20-20L	5,08	57 x 43 x 1 796 mm
DPCS20-30L	5,36	57 x 43 x 1 796 mm
DPCS20A-16	5,08	57 x 43 x 1 798 mm
PCS20A-32	5,36	57 x 43 x 1 798 mm
DPCS20A-20L6	5,08	57 x 43 x 1 798 mm
DPCS20A-30L6	5,36	57 x 43 x 1 798 mm
DPCR20-20	5,80	440 x 88 x 274 mm
DPCR20-30L	6,08	440 x 88 x 274 mm
DPCR20A-32	6,08	440 x 88 x 274 mm
DPCR20A-30L6	6,08	440 x 88 x 274 mm

Spécifications environnementales

Facteur d'environnement	Seuil
Température ambiante maximum	40 degrés Celsius

Annexe B Fiche de configuration du matériel

Unité de la série Dominion PX _____

Nº de série de l'unité Dominion PX _____

Spécifications environnementales

PRISE 1	PRISE 2	PRISE 3
MODELE	MODELE	**MODELE**
NUMERO DE SERIE	NUMERO DE SERIE	NUMERO DE SERIE
UTILISATION	UTILISATION	UTILISATION
PRISE 4	PRISE 5	PRISE 6
MODELE	MODELE	MODELE
NUMERO DE SERIE	NUMERO DE SERIE	NUMERO DE SERIE
UTILISATION	UTILISATION	UTILISATION
PRISE 7	PRISE 8	PRISE 9
MODELE	MODELE	MODELE
NUMERO DE SERIE	NUMERO DE SERIE	NUMERO DE SERIE
UTILISATION	UTILISATION	UTILISATION
PRISE 10	PRISE 11	PRISE 12

MODELE	MODELE	MODELE
NUMERO DE SERIE	NUMERO DE SERIE	NUMERO DE SERIE
UTILISATION	UTILISATION	UTILISATION
PRISE 13	PRISE 14	PRISE 15
MODELE	MODELE	MODELE
NUMERO DE SERIE	NUMERO DE SERIE	NUMERO DE SERIE
UTILISATION	UTILISATION	UTILISATION
PRISE 16	PRISE 17	PRISE 18
MODELE	MODELE	MODELE
NUMERO DE SERIE	NUMERO DE SERIE	NUMERO DE SERIE
UTILISATION	UTILISATION	UTILISATION
PRISE 19	PRISE 20	
MODELE	MODELE	

NUMERO DE SERIE	NUMERO DE SERIE	
UTILISATION	UTILISATION	

Types d'adaptateurs

_____

Types de câbles

_____

Nom du logiciel

_____

Annexe C Utilisation de l'interface CLP

Ce chapitre explique comment utiliser l'interface CLP (protocole de ligne de commande) pour administrer une unité Dominion PX.

Dans ce chapitre

A propos de l'interface CLP

L'unité Dominion PX offre une interface de ligne de commande qui permet aux administrateurs de centres de données d'effectuer certaines tâches de gestion de base. Cette interface est accessible à l'aide d'une connexion série utilisant un programme d'émulation de terminal, tel qu'HyperTerminal, ou via un client Telnet ou SSH comme PuTTY.

Remarque : l'accès Telnet à l'unité Dominion PX est désactivé par défaut car Telnet transmet en clair et n'est pas sécurisé. Pour activer Telnet, sélectionnez ***Device Settings --> Network*** *(Paramètres du dispositif --> Réseau) et cochez la case libellée* ***Enable CLP-Telnet Access*** *(Activer l'accès CLP-Telnet).*

Remarque : à propos des programmes d'émulation de terminal - HyperTerminal est disponible sur de nombreux systèmes d'exploitation Windows. Il n'est toutefois pas disponible sous Windows Vista. PuTTY est un programme libre téléchargeable depuis Internet. Reportez-vous à la documentation de PuTTY pour en savoir plus sur la configuration.

L'interface de ligne de commande est basée sur la technologie Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP). A l'aide de cette interface, vous pouvez effectuer les opérations suivantes :

- afficher le nom, l'état d'alimentation (activé ou désactivé) et les capteurs associés à chaque prise Dominion PX ;
- mettre chaque prise sous ou hors tension ;
- afficher le statut des capteurs associés à chaque prise.

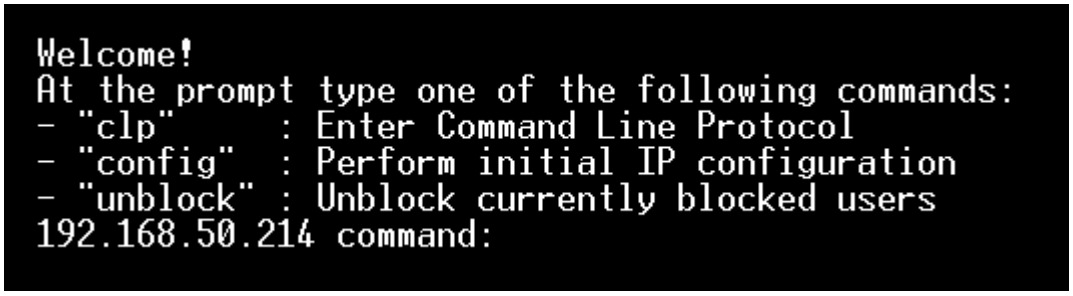
Connexion à l'interface CLP

La connexion via HyperTerminal et une connexion série est un peu différente de la connexion avec Telnet.

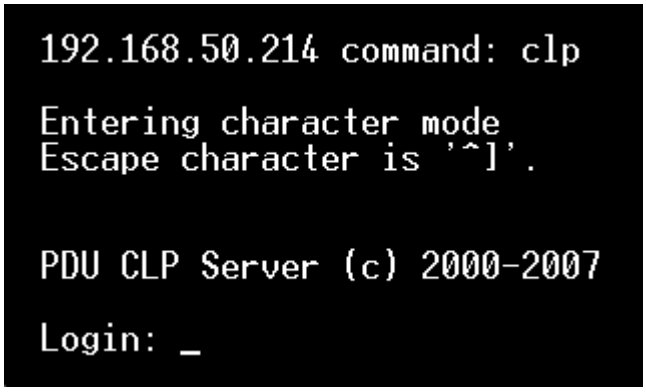
Utilisation d'HyperTerminal

➢ *Pour une connexion à l'aide d'HyperTerminal :*

1. Reliez votre PC au port série de Dominion PX avec un câble série, lancez HyperTerminal et ouvrez une fenêtre de console. Lorsque celle-ci apparaît, elle est vide.
2. Appuyez sur **Entrée** pour afficher une invite de commande.



3. Tapez alors **clp** et appuyez sur **Entrée**. Vous êtes invité à saisir un nom de connexion. Celui-ci est sensible à la casse, veillez à mettre les bonnes lettres en majuscules.



4. Tapez un nom de connexion et appuyez sur **Entrée**. Vous êtes invité à saisir un mot de passe.

5. Tapez un mot de passe et appuyez sur **Entrée**. Le mot de passe est sensible à la casse, veillez à mettre les bonnes lettres en majuscules. Une fois le mot de passe accepté, l'invite système clp:/-> apparaît.

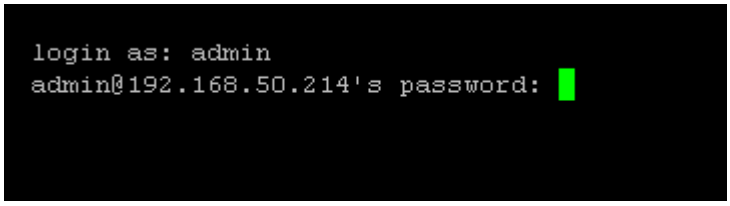
6. Vous êtes maintenant connecté à l'interface CLP et pouvez utiliser celle-ci pour administrer l'unité Dominion PX.

Utilisation de SSH ou de Telnet

➢ *Pour vous connecter à l'aide de SSH ou de Telnet :*

1. Lancez un client SSH ou Telnet, tel que PuTTY, et ouvrez une fenêtre de console. Une invite de connexion apparaît.

2. Tapez un nom de connexion et appuyez sur **Entrée**. Vous êtes invité à saisir un mot de passe.



3. Tapez un mot de passe et appuyez sur **Entrée**. Le mot de passe est sensible à la casse, veillez à mettre les bonnes lettres en majuscules. Une fois le mot de passe accepté, l'invite système clp:/-> apparaît.

```
login as: admin
admin@192.168.50.214's password:
=== SM CLP v1.0.0 SM ME Addressing v1.0.0 Raritan CLP v0.1 ===
clp:/->
```

4. Vous êtes maintenant connecté à l'interface CLP et pouvez utiliser celle-ci pour administrer l'unité Dominion PX.

Affichage des informations sur les prises

La commande show affiche le nom, l'état d'alimentation (activé ou désactivé) et les capteurs associés d'une prise ou de toutes les prises.

Syntaxe

La syntaxe de la commande show est la suivante :

```
clp:/->     show /system1/outlet<numéro de la prise>
```

<numéro de la prise> indique le numéro de la prise. Pour afficher les informations concernant toutes les prises, entrez l'astérisque joker (*) au lieu d'un numéro.

Attributs

Vous pouvez utiliser les attributs name et powerState pour filtrer les résultats de la commande show. L'attribut name affiche le nom de la prise uniquement, l'attribut powerState, l'état d'alimentation (activé ou désactivé).

La syntaxe pour ces deux attributs est la suivante :

```
clp:/->    show -d properties=name /system1/outlet<numéro de la prise>

clp:/->    show -d properties=powerState /system1/outlet<numéro de la
           prise>
```

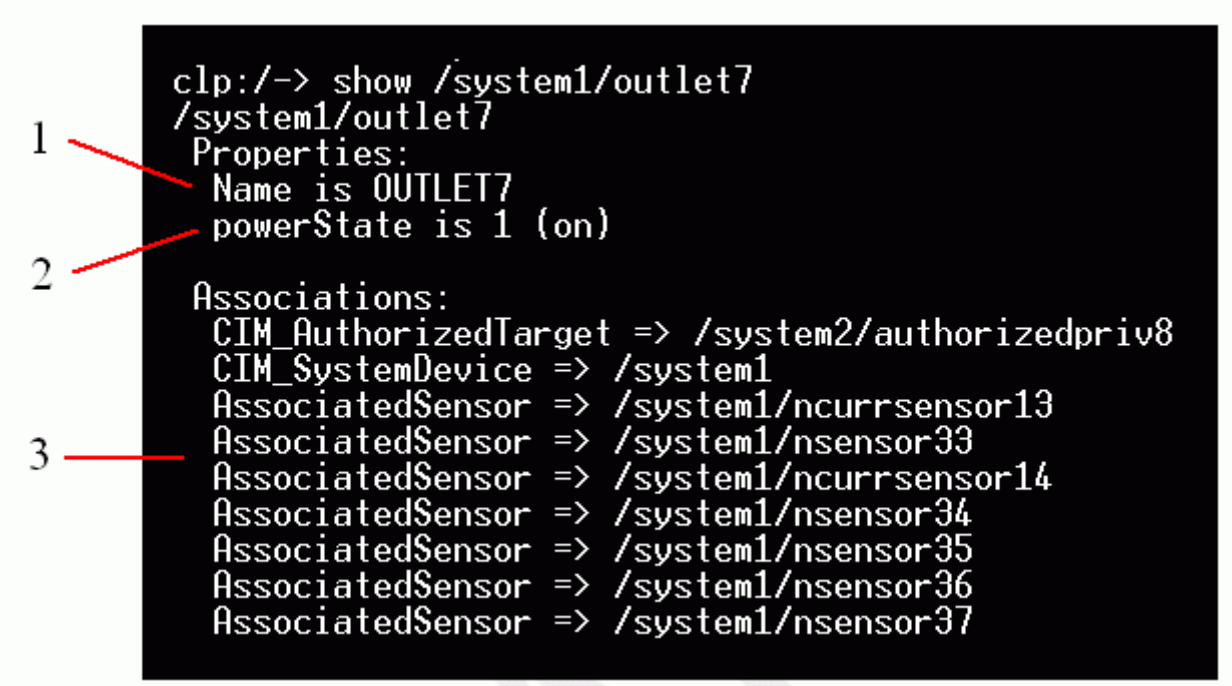
<numéro de la prise> indique le numéro de la prise. Dans les deux cas, le numéro de la prise peut également être un astérisque joker (*).

Exemples

Les exemples suivants illustrent la commande show.

Exemple 1 -- Aucun attribut

L'exemple suivant présente les résultats de la commande show sans attribut.



Numéro	Description
1	Name
2	Power State
3	Associations

Exemple 2 -- Attribut name

L'exemple suivant présente les résultats de la commande show avec l'attribut name.

```
clp:/-> show -d properties=name /system1/outlet7
/system1/outlet7
 Properties:
  Name is OUTLET7
```

Exemple 3 -- Attribut powerState

L'exemple suivant présente les résultats de la commande show avec l'attribut powerState.

```
clp:/-> show -d properties=powerState /system1/outlet7
/system1/outlet7
 Properties:
  powerState is 1 (on)
```

Mise sous ou hors tension d'une prise

La commande set met une prise sous ou hors tension.

Syntaxe

La syntaxe de la commande set est la suivante :

```
clp:/->   set /system1/<numéro de la prise> powerState=on|off
```

où le mot-clé on active la prise et le mot-clé off la désactive.

Interrogation d'un capteur de prise

La commande show utilisée avec le mot-clé Antecedent permet d'interroger les capteurs d'une prise.

```
clp:/->    Show -d properties=Antecedent/system1/outlet<numéro de
           la prise>=>AssociatedSensor
```

<numéro de la prise> indique le numéro de la prise.

Annexe D Utilisation de SNMP

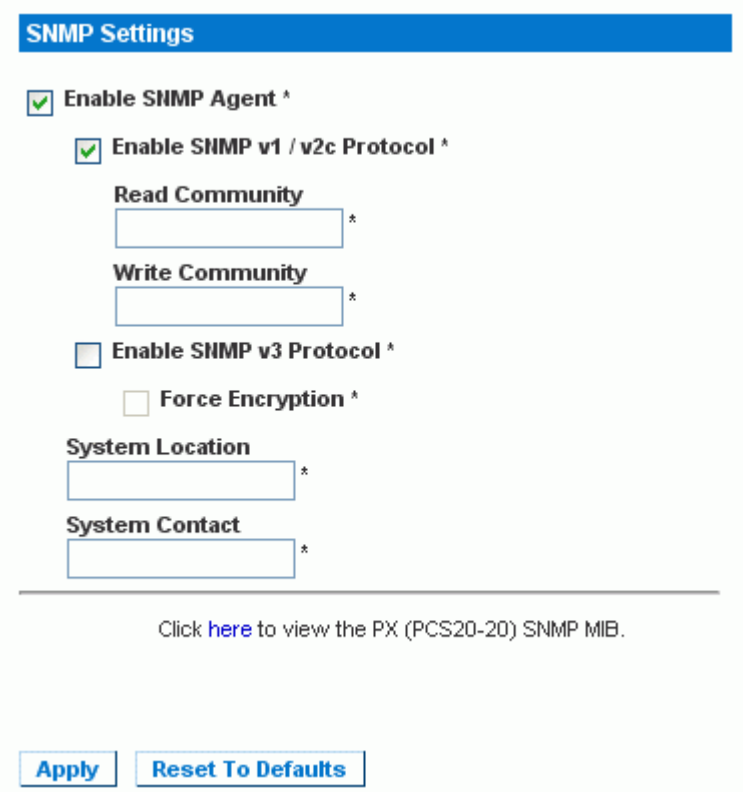
Cette annexe vous indique comment configurer Dominion PX pour l'utiliser avec un gestionnaire SNMP. L'unité Dominion PX peut être configurée pour envoyer des traps à un gestionnaire SNMP, et pour recevoir des commandes GET et SET afin de récupérer un statut et configurer certains paramètres de base.

Dans ce chapitre

Activation de SNMP

Pour communiquer avec un gestionnaire SNMP, vous devez en premier lieu activer l'agent SNMP sur Dominion PX.

1. Sélectionnez **Device Settings** (Paramètres du dispositif), puis **SNMP Settings** (Paramètres SNMP). La fenêtre SNMP Settings s'affiche.



2. Cochez la case **Enable SNMP Agent** (Activer l'agent SNMP) pour permettre à Dominion PX de communiquer avec des gestionnaires SNMP externes. Différentes options sont maintenant disponibles.
3. Cochez **Enable SNMP v1 / v2c Protocol** (Activer le protocole SNMP v1/v2c) pour permettre la communication avec un gestionnaire SNMP à l'aide du protocole SNMP v1 ou v2c. Entrez ensuite la chaîne de communauté en lecture seule SNMP dans le champ **Read Community** (Communauté en lecture) et la chaîne de communauté en lecture/écriture dans le champ **Write Community** (Communauté en écriture).
4. Cochez **Enable SNMP v3 Protocol** (Activer le protocole SNMP v3) pour permettre la communication avec un gestionnaire SNMP à l'aide du protocole SNMP v3.

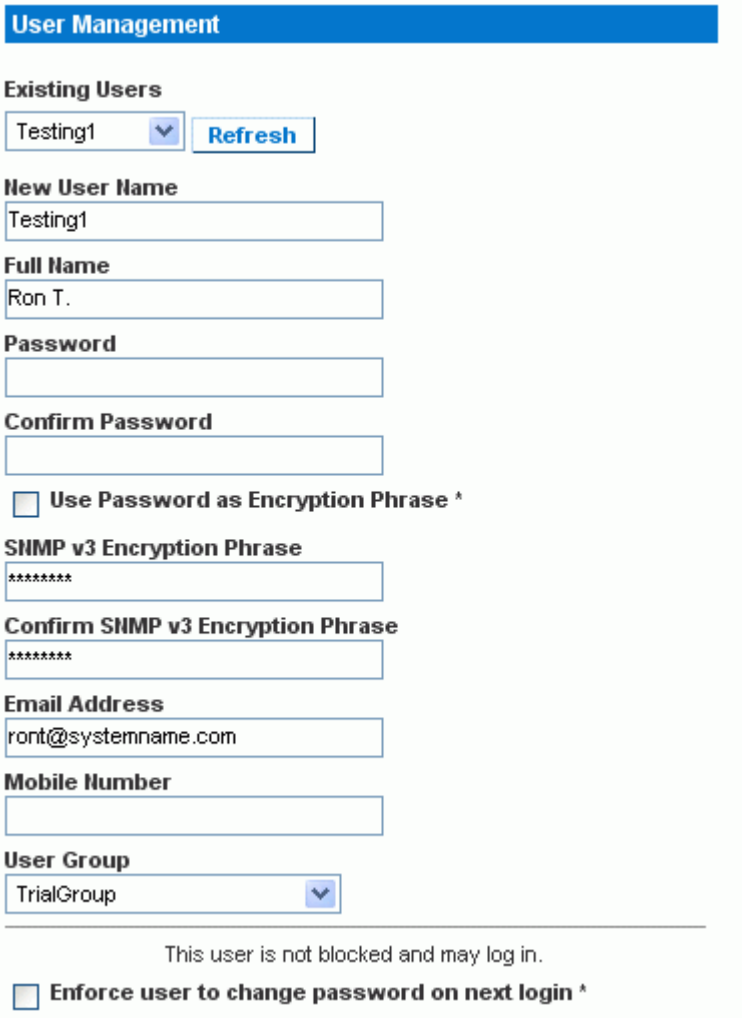
- Cochez également Force Encryption (Forcer le chiffrement) pour forcer l'utilisation de la communication SNMP chiffrée.

1. Entrez la valeur sysLocation MIBII SNMP dans le champ **System Location** (Emplacement système).
2. Entrez la valeur sysContact MIBII SNMP dans le champ **System Contact** (Contact système).
3. Cliquez sur le lien au bas de la fenêtre pour télécharger un fichier MIB SNMP que Dominion PX utilisera avec votre gestionnaire SNMP.
4. Cliquez sur **Apply** (Appliquer). La configuration SNMP est terminée.

Configuration des utilisateurs pour le protocole SNMP v3 chiffré

Le protocole SNMP v3 permet une communication chiffrée. Pour profiter de cette fonction, les utilisateurs doivent disposer d'une phrase de chiffrement, qui sert de secret partagé entre Dominion PX et eux. Cette phrase de chiffrement peut être définie sur la page User Management (Gestion des utilisateurs).

1. Choisissez **User Management**, puis **Users & Groups** (Utilisateurs et groupes). La fenêtre User/Group Management (Gestion des utilisateurs/groupes) apparaît.



2. Dans la liste déroulante du champ **Existing Users** (Utilisateurs existants), sélectionnez le profil à modifier.

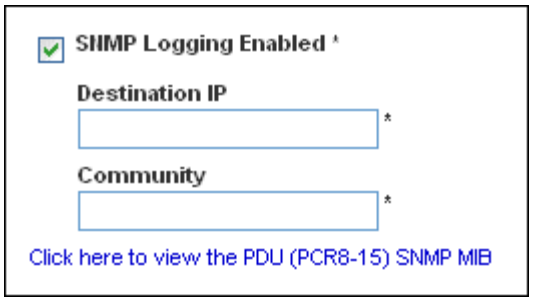
3. Si vous souhaitez utiliser le mot de passe de l'utilisateur comme phrase de chiffrement, laissez la case **Use Password as Encryption Phrase** (Utiliser le mot de passe comme phrase de chiffrement) cochée (ou cochez-la, le cas échéant).
4. Si vous souhaitez définir une phrase différente, désactivez cette case, entrez la nouvelle phrase dans le champ **SNMP v3 Encryption Phrase** (Phrase de chiffrement SNMP v3), puis à nouveau dans le champ **Confirm SNMP v3 Encryption Phrase** (Confirmer la phrase de chiffrement SNMP v3).
5. Cliquez sur Modify (Modifier). L'utilisateur peut maintenant communiquer à l'aide du protocole SNMP v3 chiffré.

Configuration des traps SNMP

Dominion PX tient automatiquement un journal interne des événements qui se produisent (reportez-vous à Paramétrage de la journalisation des événements sous le chapitre Utilisation de l'interface Web). Ces événements peuvent également être utilisés pour envoyer des traps SNMP à un gestionnaire tiers.

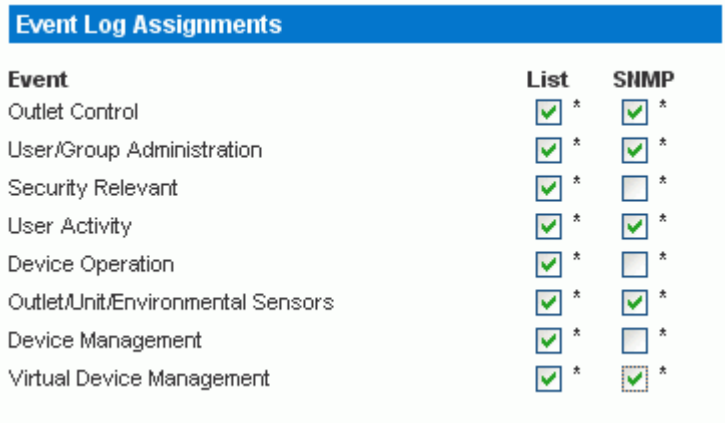
➢ *Pour configurer l'envoi par Dominion PX de traps SNMP :*

1. Choisissez **Device Settings --> Event Log** (Paramètres du dispositif --> Journal des événements). La fenêtre Event Log Settings (Paramètres du journal des événements) s'affiche. Le panneau SNMP Logging (Journalisation SNMP) contrôle l'utilisation des traps SNMP.



2. Cochez la case libellée **SNMP Logging Enabled** (Journalisation SNMP activée).
3. Entrez une adresse IP dans le champ **Destination IP** (Adresse IP de destination). Il s'agit de l'adresse à laquelle les traps sont envoyés par l'agent système SNMP.

4. Entrez le nom de la communauté SNMP dans le champ **Community** (Communauté). La communauté est un groupe représentant Dominion PX et toutes les stations de gestion SNMP.
5. Pour consulter le fichier **Management Information Base** (MIB), cliquez sur le lien libellé **Click here to view the (<device name>) SNMP MIB** (Cliquer ici pour afficher le fichier MIB SNMP de (nom du dispositif). Il est placé sous le champ Community.
6. Lorsque la journalisation SNMP est activée, sept types d'événements apparaissent dans le panneau **Event Log Assignments** (Affectations du journal des événements) à droite. Ils sont tous désactivés par défaut. Pour les activer, cochez les cases souhaitées.



7. Cliquez sur **Apply** (Appliquer). La journalisation SNMP est configurée.

Remarque : vous devriez télécharger à nouveau le fichier MIB de Dominion PX après la mise à jour du firmware de l'unité. Ainsi, votre gestionnaire SNMP dispose du fichier MIB correspondant à la version que vous utilisez.

Requêtes SNMP Get et Set

Outre l'envoi de traps, Dominion PX peut recevoir des requêtes Get et Set SNMP provenant de gestionnaires SNMP tiers. Les requêtes Get permettent de récupérer des informations concernant Dominion PX (telles que l'emplacement système ou le courant d'une prise particulière). Les requêtes Set permettent de configurer un sous-ensemble de ces informations (tel que le nom du système SNMP).

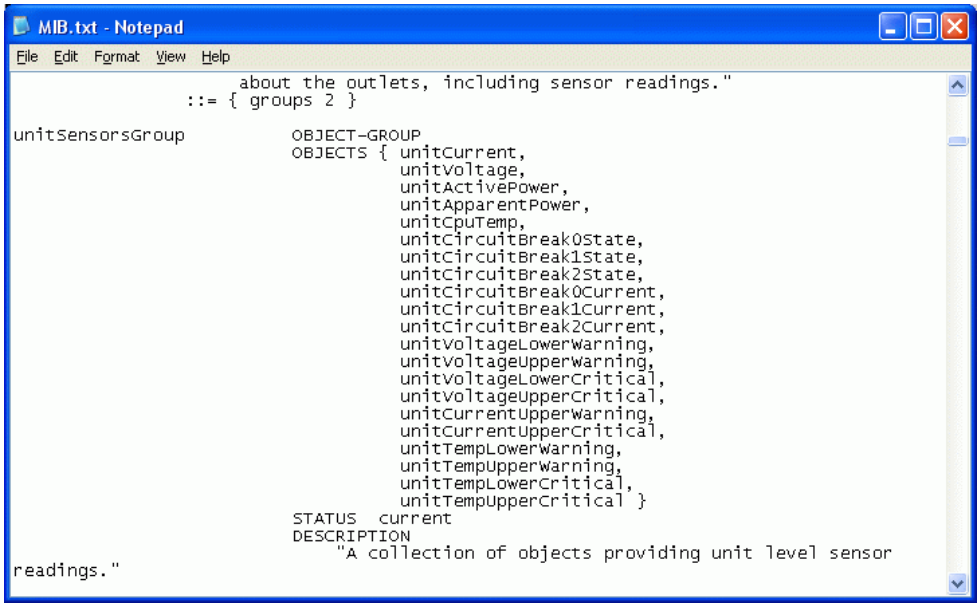
Les objets autorisés pour ces requêtes sont limités à ceux trouvés dans le groupe système SNMP MIBII et le fichier MIB personnalisé de Dominion PX.

Fichier MIB de Dominion PX

Ce fichier MIB est disponible sur la page SNMP Settings (Paramètres SNMP), sur la page Event Logging (Journalisation des événements) ou en pointant votre navigateur vers `http://<adresse-ip>/MIB.txt` ; `<adresse-ip>` désigne l'adresse IP de votre unité Dominion PX.

Présentation

L'ouverture du fichier MIB révèle les objets personnalisés qui décrivent le système Dominion PX au niveau de l'unité et au niveau de la prise individuelle. Généralement, ces objets sont présentés au début du fichier, répertoriés sous leur groupe parent. Ils réapparaissent ensuite individuellement, définis et décrits de manière détaillée.



Par exemple, le groupe **unitSensorsGroup** contient des objets pour les relevés des capteurs de l'unité Dominion PX dans sa totalité. Un objet répertorié sous ce groupe, **unitCurrent**, est décrit plus loin dans le fichier MIB comme « la valeur du capteur de courant de l'unité en milliampères », mesure du courant consommé par Dominion PX. **outletCurrent**, qui fait partie du groupe **outletsGroup**, décrit le courant passant par une prise spécifique.

REMARQUE : lors de l'exécution d'une requête SNMP Get, toutes les valeurs de courant sont exprimées en milliampères (ma). TOUTEFOIS : lors de l'exécution d'une requête SNMP Set, toutes les valeurs sont exprimées en ampères (A).

Commandes Set et seuils SNMP

Plusieurs de ces objets peuvent être configurés à partir du gestionnaire SNMP à l'aide de commandes Set SNMP. Les objets inscriptibles ont un niveau **MAX-ACCESS** en « lecture-écriture » dans le fichier MIB. Ils comprennent des objets de seuil qui provoquent l'envoi d'un avertissement par Dominion PX (et d'un trap SNMP) lorsque certains paramètres sont dépassés. Reportez-vous à la section **Paramétrage des prises et des seuils d'alimentation** du chapitre **Utilisation de l'interface Web** pour obtenir une description du fonctionnement des seuils.

Annexe E Utilisation du jeu d'outils IPMI

Le jeu d'outils IPMI est une ligne de commande qui permet aux utilisateurs d'afficher des informations concernant les canaux, d'imprimer des données sur les capteurs et de définir des paramètres de configuration du réseau local. Les sections suivantes décrivent les commandes IPMI disponibles.

Remarque : l'outil IPMI à code source libre peut être téléchargé de sourceforge et compilé sur un système Linux. Les utilisateurs peuvent ensuite interagir avec Dominion PX via le protocole IPMI grâce à cet outil. Un shell de commande Linux se présenterait comme suit : $ ipmitool -I lan -H 192.168.51.58 -U admin -a channel info

Dans ce chapitre

Commandes de canal

authcap <numéro de canal> <priv max>

Affiche des informations sur les capacités d'authentification du canal sélectionné au niveau de privilège spécifié. Les niveaux de privilèges possibles sont :

1. Niveau rappel
2. Niveau utilisateur
3. Niveau opérateur
4. Niveau administrateur
5. Niveau propriétaire OEM

Exemple

```
$ ipmitool -I lan -H 192.168.51.58 -U admin -a channel
authcap 14 5
```

Reportez-vous à la section **Niveaux de privilèges IPMI** pour en savoir plus sur les privilèges IPMI.

---

info [numéro de canal]

Affiche des informations sur le canal sélectionné. Si aucun canal n'est indiqué, les informations affichées concernent le canal utilisé actuellement :

Exemple

```
$ ipmitool -I lan -H 192.168.51.58 -U admin -a channel info
```

---

getaccess <numéro de canal> [ID utilisateur]

Configure l'ID utilisateur indiqué comme valeur par défaut pour le numéro de canal donné. Lorsque ce canal est utilisé par la suite, l'utilisateur est implicitement identifié par l'ID utilisateur donné.

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1
channel getaccess 14 63
```

---

setaccess <numéro de canal> <ID utilisateur>[callin=on|off] [ipmi=on|off] [link=on|off] [privilege=niveau]

Configure les données d'accès à un canal donné pour l'ID utilisateur indiqué.

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1
channel setaccess 14 63 privilege=5
```

`getciphers <all | supported> <ipmi | sol> [canal]`

Affiche la liste des suites de chiffrement prises en charge pour l'application donnée (ipmi ou sol) sur le canal indiqué.

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1
channel getciphers ipmi 14
```

Commandes d'événement

Les commandes Event vous permettent d'envoyer des événements prédéfinis à un contrôleur de gestion.

`<numéro d'événement prédéfini>`

Envoie un événement prédéfini au journal des événements système. Les valeurs prises en charge actuellement sont :

- Temperature: Upper Critical: Going High (Température: Critique supérieur: En hausse)
- Voltage Threshold: Lower Critical: Going Low (Seuil de tension: Critique inférieur : En baisse)
- Memory: Correctable ECC Error Detected (Mémoire: Erreur ECC rectifiable détectée)

Remarque : ces événements prédéfinis ne produiront vraisemblablement pas d'enregistrements SEL « précis » pour un système particulier car ils ne seront pas correctement liés à un numéro valide de capteur, mais ils suffisent pour vérifier le bon fonctionnement du SEL.

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1
event 1
```

file <nom de fichier>

Les enregistrements de journal des événements spécifiés dans le fichier seront ajoutés au journal des événements système. Chaque ligne de ce fichier est formatée comme suit :

<{Révision évM} {Type de capteur} {Numéro de capteur} {Dir/Type d'événement} {Données d'événement 0} {Données d'événement 1} {Données d'événement 2}>[# COMMENTAIRE]

Remarque : le champ Dir/Type d'événement est codé avec la direction de l'événement indiquée dans le bit de poids fort (bit 7) et le type d'événement contenu dans les 7 bits de poids faible.

Exemple

```
0x4 0x2 0x60 0x1 0x52 0x0 0x0 # Voltage threshold: Lower
Critical: Going Low
```

Commandes LAN

Les commandes LAN vous permettent de configurer les canaux LAN.

print <canal>

Imprime la configuration actuelle du canal indiqué.

set <canal> <paramètre>

Définit le paramètre donné sur le canal indiqué. Les paramètres valides sont :

- *ipaddr <x.x.x.x>* Définit l'adresse IP de ce canal.
- *netmask <x.x.x.x>* Définit le masque de réseau de ce canal.
- *macaddr <xx:xx:xx:xx:xx:xx>* Définit l'adresse MAC de ce canal.
- *defgw ipaddr <x.x.x.x>* Définit l'adresse IP de la passerelle par défaut.
- *defgw macaddr <xx:xx:xx:xx:xx:xx>* Définit l'adresse MAC de la passerelle par défaut.
- *bakgw ipaddr <x.x.x.x>* Définit l'adresse IP de la passerelle de sauvegarde.
- *bakgw macaddr <xx:xx:xx:xx:xx:xx>* Définit l'adresse MAC de la passerelle de sauvegarde.
- *password <pass>* Définit le mot de passe de l'utilisateur null.
- *snmp <chaîne de communauté>* Définit la chaîne de communauté SNMP.
- *user* Active le mode d'accès pour l'id utilisateur 1 (utilisez la commande user pour afficher des informations sur les ID utilisateur pour un canal donné).
- *access <on|off>* Définit le mode d'accès au canal LAN.
- *ipsrc* Définit la source de l'adresse IP :

  none non spécifiée

  static adresse IP statique configurée manuellement

  dhcp adresse obtenue par DHCP

  bios adresse chargée par le BIOS ou un logiciel système
- *arp respond <on|off>* Définit des réponses ARP générées.
- *arp generate <on|off>* Définit des ARP injustifiées générées.
- *arp interval <secondes>* Définit un intervalle ARP injustifié généré.
- *auth <niveau,...> <type,...>* Définit des types d'authentification valides pour un niveau d'authentification donné.

  Niveaux : callback, user, operator, admin (rappel, utilisateur, opérateur, administrateur)

  Types : none, md2, md5, password, oem (néant, md2, md5, mot de passe, oem)

- *cipher_privs <privlist>* Associe les numéros de suites de chiffrement au niveau de privilège maximum autorisé à l'utiliser. Ainsi, les suites de chiffrement peuvent être réservées aux utilisateurs disposant d'un niveau de privilège particulier, afin que, par exemple, les administrateurs soient obligés d'employer une suite de chiffrement plus forte que les utilisateurs de base.

La liste de privilèges (privlist) est formatée comme suit. Chaque caractère représente un niveau de privilège et sa position identifie le numéro de la suite de chiffrement. Par exemple, le premier caractère représente la suite de chiffrement 1 (la suite de chiffrement 0 est réservée), le second représente la suite de chiffrement 2, etc. La liste privlist doit comporter 15 caractères.

Les caractères utilisés dans privlist et leurs niveaux de privilèges associés sont :

- X Suite de chiffrement inutilisée
- c CALLBACK (RAPPEL)
- u USER (UTILISATEUR)
- O OPERATOR (OPERATEUR)
- a ADMIN (ADMINISTRATEUR)
- O OEM

Commandes de capteur

Les commandes de capteur vous permettent d'afficher des informations détaillées sur les capteurs.

list

Répertorie les capteurs et seuils dans un grand tableau.

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -a sensor list
```

get <id> ... [<id>]

Imprime des informations sur des capteurs nommés.

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1 sensor get "R.14 Current"
```

`thresh <id> <seuil> <paramètre>`

Cette commande vous permet de définir une valeur de seuil pour un capteur particulier. Ce dernier est nommé. Les seuils valides sont :

- *unr* Upper Non-Recoverable (Irrécupérable supérieur)
- *ucr* Upper Critical (Critique supérieur)
- *unc* Upper Non-Critical (Non critique supérieur)
- *lnc* Lower Non-Critical (Non critique inférieur)
- *lcr* Lower Critical (Critique inférieur)
- *lnr* Lower Non-Recoverable (Irrécupérable inférieur)

Exemple

```
$ ipmitool -I lan -H allen-dpxpcr20-20 -U admin -P raritan1
sensor thresh "R.14 Current" unr 10.5
```

Commandes OEM

Vous pouvez utiliser les commandes OEM pour gérer et contrôler le fonctionnement de Dominion PX.

La commande OEM Net-Fn est définie comme suit :

```
#define IPMI_NETFN_OEM_PP      0x3C
```

Le tableau répertorie les commandes OEM et donne l'ID de chacune. Les sections qui suivent expliquent chaque commande de manière plus détaillée.

Nom de la commande	ID
Commande Set Power On Delay	0x10
Commande Get Power On Delay	0x11
Commande Set Receptacle State	0x12
Commande Get Receptacle State	0x13
Commande Set Group State	0x14
Commande Set Group Membership	0x15
Commande Get Group Membership	0x16
Commande Set Group Power On Delay	0x17
Commande Get Group Power On Delay	0x18

Nom de la commande	ID
Set Receptacle ACL	0x19
Get Receptacle ACL	0x1A
Set Sensor Calibration	0x1B
Test Actors	0x1C
Test Sensors	0x1D
Commande Set Power Cycle Delay	0x1E
Commande Get Power Cycle Delay	0x1F

Commande Set Power On Delay

Le délai de mise sous tension global définit le temps devant s'écouler entre deux mises sous tension.

Données de requête	1	délai d'1/10 de seconde Le délai est la période minimum qui doit s'écouler entre deux mises sous tension de prise.
Données de réponse	1	Code d'achèvement

Commande Get Power On Delay

Données de requête	-	-
Données de réponse	1	Code d'achèvement
	2	délai d'1/10 de seconde

Commande Set Receptacle State

Cette commande permet la mise sous/hors tension de prises individuelles.

Données de requête	1	Nº de prise [7 - 5] réservé [4 - 0] nº de prise, base 0, nº valide le plus élevé dépend du modèle de dispositif
	2	nouvel état [7 - 1] réservé [0] 1b = mise sous tension, 0b = mise hors tension
Données de réponse	1	Code d'achèvement

Commande Get Receptacle State

Données de requête	1	Nº de prise [7 - 5] réservé [4 - 0] nº de prise, base 0, nº valide le plus élevé dépend du modèle de dispositif
Données de réponse	1	Code d'achèvement
	2	état courant de prise et état visuel [7] réservé [6] 1b = clignotant, 0b = fixe [5] 1b = voyant vert allumé, 0b = éteint [4] 1b = voyant rouge allumé, 0b = éteint [3] 1b = dans la file d'attente pour la mise sous tension, 0b = n'est pas dans la file d'attente [2] 1b = délai de mise hors puis sous tension, 0b = aucun délai [1] 1b = libérée par le disjoncteur logiciel, 0b = norm [0] 1b = mise sous tension, 0b = mise hors tension

Commande Set Group State

Cette commande permet la mise sous/hors tension de toutes les prises d'un groupe. Il n'existe pas de commande Get Group State. L'extraction de l'état d'une prise doit être effectuée à l'aide de la commande Get Receptacle State.

Données de requête	1	Nº du groupe [7 - 5] réservé [4 - 0] nº du groupe, nombres valides : 0 à 23
	2	nouvel état [7 - 1] réservé [0] 1b = mise sous tension, 0b = mise hors tension
Données de réponse	1	Code d'achèvement

Commande Set Group Membership

Données de requête	1	Nº du groupe [7 - 5] réservé [4 - 0] nº du groupe, nombres valides : 0 à 23
	2	[7 - 1] réservé [0] 1b = activer le groupe, 0b = désactiver le groupe
	3	[7] 1b = la prise 7 appartient au groupe ... [0] 1b = la prise 0 appartient au groupe
	4	[7] 1b = la prise 15 appartient au groupe ... [0] 1b = la prise 8 appartient au groupe
	5	[7] 1b = la prise 23 appartient au groupe ... [0] 1b = la prise 16 appartient au groupe
Données de réponse	1	Code d'achèvement

Commande Get Group Membership

Données de requête	1	Nº du groupe [7 - 5] réservé [4 - 0] nº du groupe, nombres valides : 0 à 23
Données de réponse	1	Code d'achèvement
	2	[7 - 1] réservé [0] 1b = le groupe est activé, 0b = le groupe est désactivé
	3	[7] 1b = la prise 7 appartient au groupe ... [0] 1b = la prise 0 appartient au groupe
	4	[7] 1b = la prise 15 appartient au groupe ... [0] 1b = la prise 8 appartient au groupe
	5	[7] 1b = la prise 23 appartient au groupe ... [0] 1b = la prise 16 appartient au groupe

Commande Set Group Power On Delay

Données de requête	1	N° du groupe [7 - 5] réservé [4 - 0] nº du groupe, nombres valides : 0 à 23
	2	délai d'1/10 de seconde Ce délai remplace le délai global pour toutes les prises de ce groupe. Il sera utilisé avec les commandes Set Group State et Set Receptacle State.
Données de réponse	1	Code d'achèvement

Commande Get Group Power On Delay

Données de requête	1	N° du groupe [7 - 5] réservé [4 - 0] nº du groupe, nombres valides : 0 à 23
Données de réponse	1	Code d'achèvement
	2	délai d'1/10 de seconde

Set Receptacle ACL

Les LCA (listes de contrôle d'accès) définissent qui est autorisé à modifier l'état d'une prise. Les LCA seront stockées pour chaque prise de courant individuelle. Une entrée LCA unique définit si un certain ID utilisateur ou niveau de privilège est autorisé ou non à émettre des commandes de contrôle pour la prise de courant. La LCA sera évaluée de haut en bas, l'ordre des entrées est donc important. En cas d'absence d'entrée de LCA, les LCA de prise sont désactivées. Tous les ID utilisateur y ont accès.

Données de requête	1	Nº de prise
	2	nombre d'entrées de LCA à suivre
	3 +N	entrée de LCA [7] 0b = refuser, 1b = autoriser [6] 0b = ID utilisateur, 1b = niveau de privilège [5 - 0] ID utilisateur ou niveau de privilège suivant [6]
Données de réponse	1	Code d'achèvement

Get Receptacle ACL

Données de requête	1	Nº de prise
Données de réponse	1	Code d'achèvement

Données de requête	1	Nº de prise
	2	nombre d'entrées de LCA à suivre
	3 +N	entrée de LCA [7] 0b = refuser, 1b = autoriser [6] 0b = ID utilisateur, 1b = niveau de privilège [5 - 0] ID utilisateur ou niveau de privilège suivant [6]

Set Sensor Calibration

Le calibrage est autorisé uniquement pour les capteurs basés seuil qui retournent un octet de relevé de capteur avec la commande Get Sensor Reading. Les capteurs basés seuil ne disposent pas tous de la fonction de calibrage.

Données de requête	1	Numéro de capteur (ffh = réservé)
	2	Valeur de relevé de capteur réelle Suppose qu'au moment de l'exécution de la commande, une mesure calibrée est appliquée à ce capteur.
Données de réponse	1	Code d'achèvement 00h - Si le calibrage est possible. CDh - Si le capteur ne peut pas être calibré.

Test Actors

Permet de tester le matériel pendant la production

Données de requête	1	[7 - 2] réservé [1] Test à alarme sonore, 0b - désactiver, 1b - activer [0] 7 Test d'affichage de segment, 0b - désactiver, 1b - activer
Données de réponse	1	Code d'achèvement

Test Sensors

Permet de tester le matériel pendant la production

Données de requête	1	-
Données de réponse	1	Code d'achèvement
	2	[7 - 2] réservé [1] bouton bas, 0b - non appuyé, 1b - appuyé [0] bouton haut, 0b - non appuyé, 1b - appuyé

Commande Set Power Cycle Delay

Données de requête	1	Nº de la prise (0xFF pour délai d'unité global)
	2	Délai (secondes), 1 à 255 pour unité et prise, 0 reprise du délai d'unité (prise uniquement)
Données de réponse	1	Code d'achèvement

Commande Get Power Cycle Delay

Données de requête	1	Nº de la prise (0xFF pour délai d'unité global)
Données de réponse	1	Code d'achèvement
	2	Délai (secondes), 1 à 255, 0 si non défini (prise uniquement)

Remarque : les valeurs supérieures à 255 ne peuvent pas être envoyées à Dominion PX via IPMI. Pour cela, vous devez utiliser l'interface Web.

Niveaux de privilèges IPMI

Le niveau de privilège IPMI que vous sélectionnez détermine :

	Niveau de privilège IPMI :					
	Aucun accès	Callback	User	Operator	Administrator	OEM
Authentication Settings (Paramètres d'authentification)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
Change Password (Modifier le mot de passe)	Non	Non	Non	Non	Oui	Oui
Date/Time Settings (Paramètres date/heure)	Non	Non	Non	Oui	Oui	Oui
Firmware Update (Mise à jour du firmware)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
Log Settings (Paramètres du journal)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
Log View (Consultation du journal)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
Network Dyn/DSN Settings (Paramètres réseau dyn/DSN)	Non	Non	Non	Non	Oui	Oui

Power Control Setting (Paramètre de gestion de l'alimentation)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
SNMP Setting (Paramètre SNMP)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
SSH/Telnet Access (Accès SSH/Telnet)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
SSL Certificate Management (Gestion des certificats SSL)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
Security Settings (Paramètres de sécurité)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
Unit Reset (Réinitialisation de l'unité)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non
User/Group Management (Gestion des utilisateurs/groupes)	Non	Non	Non	Non	Oui	Oui
User Group Permissions (Autorisations de groupe d'utilisateurs)	Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non	Oui/Non

Annexe F Types d'événements

Type d'événement	Exemples
Outlet Control (Contrôle des prises)	Prise (nº) mise sous tension par l'utilisateur Prise (nº) mise hors tension par l'utilisateur Prise (nº) mise hors puis sous tension par l'utilisateur
Outlet/Unit/Environmental Sensors (Capteurs de prise/d'unité/d'environnement)	Assertion : Température d'environnement (nombre) au-dessus du seuil non critique supérieur Infirmation : Température d'environnement (nombre) au-dessus du seuil critique supérieur
User/Group Administration (Administration des utilisateurs/groupes)	Utilisateur ajouté Utilisateur modifié Utilisateur supprimé Mot de passe de l'utilisateur modifié Groupe ajouté Groupe modifié Groupe supprimé
Security Relevant (En rapport avec la sécurité)	Echec de la connexion de l'utilisateur
User Activity (Activité des utilisateurs)	Utilisateur connecté Utilisateur déconnecté Session utilisateur a expiré Remarque : les entrées d'activité des utilisateurs dans le journal des événements affichent toujours l'addresse IP de l'ordinateur qui s'est connecté ou déconnecté. Les entrées comportant une adresse IP 127.0.0.1 (adresse IP de bouclage) représentent une connexion série et une session CLP.
Device Operation (Opération sur les dispositifs)	Dispositif démarré
Device Management (Gestion des dispositifs)	Mise à jour du dispositif commencée
Virtual Device Management (Gestion des dispositifs virtuelle)	Connectivité perdue de l'unité PDU principale avec adresse IP esclave :

Annexe G Caractéristiques

Cette annexe décrit :

- Broches série DPX RJ-45

Définition broche RJ-45/de signal			
Broche nº	**Signal**	**Direction**	**Description**
1	DTR	Sortie	Réservé
2	GND	—	Signal de mise à la terre
3	+5V	—	Alimentation de CIM (200 mA, protégé par fusible)
4	TxD	Sortie	Transmission de données (Données en sortie)
5	RxD	Entrée	Réception de données (Données en entrée)
6	N/C	N/C	Aucune connexion
7	GND	—	Signal de mise à la terre
8	DCD	Entrée	Réservé

- Broches fonction DPX RJ-11

Définition broche RJ-11/de signal			
Broche nº	**Signal**	**Direction**	**Description**
1	+12V	—	Alimentation (500 mA, protégé par fusible)
2	GND	—	Signal de mise à la terre
3	RS485 (Data +)	bidirectionnel	Ligne de données +
4	RS485 (Data -)	bidirectionnel	Ligne de données -
5	GND	—	Signal de mise à la terre
6	1-wire		

Index

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

➢ *Etats-Unis/Canada/Amérique latine*

Lundi - Vendredi
8h00 - 20h00, heure de la côte Est des Etats-Unis
Tél. : 800-724-8090 ou 732-764-8886
Pour CommandCenter NOC : appuyez sur 6, puis sur 1.
Pour CommandCenter Secure Gateway : appuyez sur 6, puis sur 2.
Fax : 732-764-8887
E-mail pour CommandCenter NOC : tech-ccnoc@raritan.com
E-mail pour tous les autres produits : tech@raritan.com

➢ *Chine*

Beijing
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-10-88091890

Shanghai
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-21-5425-2499

Guangzhou
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-20-8755-5561

➢ *Inde*

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +91-124-410-7881

➢ *Japon*

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5994
E-mail : support.japan@raritan.com

➢ *Europe*

Europe
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +31-10-2844040
E-mail : tech.europe@raritan.com

Royaume-Uni
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +44-20-7614-77-00
France
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +33-1-47-56-20-39

Allemagne
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0

➢ *Corée*

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +82-2-5578730

➢ *Melbourne, Australie*

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +61-3-9866-6887

➢ *Taiwan*

Lundi - Vendredi
9h00 - 18h00, UTC/GMT - Heure normale 5 - Heure avancée 4
Tél. : +886-2-8919-1333
E-mail : tech.rap@raritan.com