

# Caractéristiques et avantages

## Dominion SX

(ver 3.1)



Caractéristiques	Avantages
<b>Flexibilité</b>	
Gamme étendue de modèles pris en charge	Offre la densité de ports la plus élevée du marché (48 ports) pour un facteur de forme 1U.  Différentes options d'alimentation, incluant des alimentations doubles avec équilibrage de charge et commutation automatique immédiate.  Sélection d'un ou de deux ports Ethernet 10/100 Base-T avec fonction de basculement automatique intelligente. Les modèles sont disponibles avec ou sans modem intégré, et avec un ou deux ports série "au niveau du rack" pour l'accès local.  Modèles disponibles avec 4 à 48 ports. Double alimentation en option sur la plupart des modèles de 8 à 48 ports.
Mémoire étendue sur les modèles à 8, 16, 32 et 48 ports	La mémoire tampon est passée de 65 ko à 256 ko, permettant d'étendre la capacité de journalisation des événements locaux et des alertes de 20 pages à 80 pages. Les utilisateurs seront désormais assurés de disposer de tous les événements qui se produisent lorsqu'ils ne sont pas connectés au dispositif.
Facteur de forme 1U	Un petit facteur de forme permet de gagner de l'espace dans le rack et/ou l'armoire, ce qui en fait un dispositif idéal pour les bureaux distants où l'espace est limité. Supports de fixation inclus sur les modèles DSX à 16 à 48 ports (en option sur les modèles DSX4 et DSX8, sauf sur le modèle DSXA-8 à double alimentation, fourni avec un kit de supports de fixation).
<b>International Language Support</b>	<b>The Raritan Serial Console can support four languages: English, Japanese, Korean and Chinese</b>
<b>Fiabilité</b>	
Fonction de basculement automatique intelligente sur les modèles avec réseau local double	Sur tous les modèles avec réseau local double, l'administrateur peut activer le basculement vers le port du second réseau local. Possibilité d'utiliser une ou deux adresses IP. Tout port de connexion LAN peut être utilisé comme port d'accès à l'unité Dominion SX.
Compatibilité multiplate-forme et indépendance vis-à-vis du matériel	Permet la connexion de plusieurs serveurs distincts, exécutant SUN <sup>®</sup> SolarisTM, HP-UX, AIX, Linux <sup>®</sup> , Windows <sup>®</sup> Server 2003 et UNIX <sup>®</sup> , ainsi que de plusieurs autres dispositifs série à un seul dispositif Dominion SX. Ainsi, cette solution s'avère parfaite dans les situations dans lesquelles un ensemble d'équipements communs est nécessaire à des emplacements distants.
Options d'alimentation AC et CC	Alimentation intégrée garantissant une fourniture appropriée d'électricité et la fiabilité du système. Alimentation AC : à commutation automatique 100/240 V Alimentation AC à commutation automatique : -36-72 V c.c.

Caractéristiques	Avantages
Aucune pièce mobile – fiabilité plus élevée	L'absence de ventilateur ou d'autres pièces mobiles génère moins de pannes, et donc une plus grande fiabilité. Des unités mieux refroidies dissipent moins de chaleur et consomment moins d'énergie.
Modem 56K intégré via une connexion RJ11 (depending on model)	Permet un accès en urgence en cas de défaillance du réseau. Cette caractéristique permet à un administrateur d'accéder à l'équipement du serveur et du réseau pour le dépannage ou la restauration. Le modem intégré permet une installation très propre et évite d'avoir à disposer d'un modem/de câbles et d'une alimentation externes ou d'un serveur d'accès à distance distinct, de cartes modem PCMCIA intercalées ou d'un logiciel d'authentification local, ce qui réduit les niveaux de défaillance possibles.
<b>Sécurité</b>	
Pare-feu complet	User selectable and customizable system security levels catering to wide range of user needs for security. Enhancements to the firewall – added pre- and post-routing and Static NAT (SNAT) support.
Réduction des attaques de type "Man In the Middle"	Sécurité renforcée des canaux de communication par l'utilisation de certificats SSL client et serveur.
Prise en charge du routage statique sélectif	Prend en charge les connexions entre le modem et le port LAN1, le modem et le port LAN 2 ou entre les ports LAN 1 et LAN 2. Les utilisateurs peuvent ainsi utiliser deux réseaux différents (public et privé) et un accès par modem aux dispositifs contrôlés par KVM ou Ethernet. L'utilisation de cette fonction avec celle de pare-feu active l'accès sécurisé.
Adressage de port TCP pour Telnet et SSHv2	L'adressage de port direct peut fonctionner avec l'adressage de port TCP pour Telnet et SSH. Des adresses IP ou des numéros de port TCP indépendants peuvent être affectés à chaque port pour un accès direct par le biais de ce port. La redirection du port COM peut être prise en charge pour les redirecteurs de logiciels tiers.
Groupes d'utilisateurs locaux	Offre la souplesse d'octroyer des autorisations d'utilisateur par unité SX en utilisant les groupes locaux. Le serveur d'authentification peut maintenant renvoyer le groupe une fois qu'il est authentifié et les autorisations peuvent être déterminées localement.
Prise en charge flexible de mots de passe sécurisés	Offre des paramètres de mot de passe sélectionnables par l'utilisateur, de façon à couvrir une plage étendue de niveaux de sécurité de mot de passe.
Bannière d'avis et de consentement personnalisable	Sécurité renforcée avec option d'audit pendant les phases d'identification et d'autorisation.
Rejet des tentatives d'accès via SSHv1	En raison des nombreuses vulnérabilités connues du protocole SSHv1 au niveau de la sécurité, Dominion SX rejettera automatiquement les connexions SSHv1.
Options optimisées de chiffrement	Prise en charge de nouvelles options de chiffrement : sécurité du navigateur Web assurée grâce à un chiffrement SSL sur 128 bits et RC4; pour les connexions SSHv2, AES et 3DES sont pris en charge (en fonction du client).
Prise en charge de l'authentification et des autorisations – Kerberos	Prend en charge les serveurs RADIUS, LDAP, TACACS+, Kerberos V.5 et Active Directory® ; les serveurs primaires et secondaires sont pris en charge.

Caractéristiques	Avantages
Nom d'utilisateur et mot de passe jamais stockés sous forme de texte en clair	Les informations sensibles subissent un hachage MD5 lors du stockage dans l'unité.
Certificats de sécurité définis et installables par l'utilisateur	Dominion SX inclut une sécurité d'authentification des utilisateurs et des certificats de sécurité définis et installables par l'utilisateur. A utiliser avec Active Directory et LDAPS pour des communications sécurisées. Les certificats client et serveur sont pris en charge.
Prise en charge de SecureID	SecureID est pris en charge via RADIUS pour une sécurité renforcée.
Option de déconnexion des serveurs cible	Lorsqu'un utilisateur est déconnecté pour cause d'inactivité, une commande de déconnexion définie par l'utilisateur est envoyée à la cible. La sécurité des sessions utilisateur s'en trouve optimisée, étant donné que le prochain utilisateur à se connecter au port devra ouvrir une session sur le serveur cible avec ses propres informations d'identification. Pour certains utilisateurs, cette fonction est peut-être connue comme une "macro de sortie".
Sécurité par modem à composition automatique	Pour une sécurité renforcée, Dominion SX prend en charge les modems à composition automatique avec les clients Linux <sup>®</sup> et Windows 2000/XP.
Désactivation de l'authentification et des autorisations	Cette option enregistre le temps utilisateur lors de l'accès au dispositif SX dans un centre de données où la sécurité est assurée par d'autres moyens. L'utilisateur n'a pas besoin d'entrer son nom d'utilisateur et son mot de passe.
Option de désactivation de l'authentification locale	Cette option renforce la sécurité là où la stratégie de sécurité l'exige, garantissant qu'un seul service d'annuaire est utilisé pour tous les utilisateurs.
<b>Expérience d'utilisateur final</b>	
Mise en place du langage HTML	Réduit la durée de chargement de l'applet Java dans un navigateur à moins d'une minute.
CLI moderne complète – équivalence avec l'interface utilisateur graphique	Convivialité optimisée avec traitement et historique des commandes. Le module CLI admin dispose des mêmes fonctions que l'interface utilisateur graphique, permettant ainsi la création de scripts pour toute commande.
Gamme étendue de navigateurs pris en charge	Offre une gamme étendue de navigateurs – Netscape <sup>®</sup> 7.0+, Mozilla <sup>®</sup> 1.5+, Mozilla Firefox, Internet Explorer 6.0+ – garantissant la compatibilité avec les systèmes d'exploitation et les dispositifs les plus variés.
Appareil unique – sécurité renforcée, ne nécessite aucun logiciel supplémentaire	Modèle d'appareil offrant une sécurité renforcée sans que l'utilisateur n'accède au système d'exploitation Linux sous-jacent du serveur de console. Propose une vraie fonction "Plug and Play" afin que l'installation et la configuration soient rapides et faciles. Il n'est pas nécessaire d'acquérir d'autres logiciels ou matériel client/hôte ni de prévoir un équipement réseau spécial ou une conception spéciale. Lors de l'utilisation d'un navigateur Web compatible avec Java, aucun logiciel client SSH onéreux n'est nécessaire. L'application supprime également la nécessité de gérer un logiciel client supplémentaire.

Caractéristiques	Avantages
<b>Capacités de gestion</b>	
Facilité d'installation	Installation en moins de trois minutes, à l'aide d'un navigateur Web ou un terminal VT100 (ou équivalent). Dans le cas de certains produits de nos concurrents, l'installation de base exige une modification importante de plusieurs fichiers.
Prise en charge des serveurs IPMI	Gestion et surveillance améliorées des performances des systèmes. Permet la détection et la gestion de serveurs IPMI.
Surveillance et alerte des ports par mot-clé	Aussi parfois appelée "déclencheurs de ports". Les utilisateurs peuvent définir jusqu'à 14 mots-clés par port, comptant chacun 40 caractères maximum. Le dispositif SX analyse les données provenant du port et, s'il rencontre un mot-clé, envoie les alertes via l'agent SNMP ou par courriel aux adresses prédéfinies. Tout problème avec les cibles peut ainsi être détecté et signalé même lorsque l'utilisateur n'est pas connecté, ce qui réduit la durée moyenne de réparation et permet une notification d'un problème plus rapide que par des systèmes de surveillance SNMP classiques.
Accès via un navigateur Web/SSHv2/Telnet	Accès par pointer-cliquer facile via un navigateur Web compatible Java et un client SSHv2/Telnet depuis un ordinateur de bureau, un ordinateur portable ou un appareil mobile de poche.
Prise en charge de VT220/320/ANSI	Choix élargi d'options d'émulation de terminal, permettant la prise en charge d'une plage plus étendue de dispositifs.
Messagerie instantanée SecureChat	Permet de communiquer instantanément par voie chiffrée pour une collaboration en ligne avec d'autres utilisateurs de navigateurs Web autorisés. Contribue à augmenter la participation et l'efficacité d'une main d'œuvre distribuée. Cette caractéristique réduit le temps passé à résoudre des problèmes et permet à plusieurs administrateurs de corriger un problème. Cette caractéristique peut également être utilisée au sein d'une formation.
Traps SNMP complets	Les traps SNMP complets permettent de mettre en place différentes alertes (échecs d'authentification, connexions et déconnexions des ports et autres événements intéressants pour les administrateurs du système).
Syslog	<b>Enhancements in SMTP notifications –persistent attempts (automatic retries) to send SMTP notifications and support for mail server authentication.</b>
Journalisation NFS	Permet de procéder à la journalisation de l'ensemble des frappes et des réponses serveur/dispositif au niveau du ou des serveurs NFS. Essentiellement utilisée pour les journaux d'audit. Pour une sécurité renforcée, les journaux NFS peuvent maintenant être stockés sur le serveur NFS avec les clés de chiffrement définies par l'utilisateur. En cas d'intrusion dans le fichier, les données n'auront ainsi aucune utilité sans la clé utilisée pour leur chiffrement. Les messages Keep-Alive du journal NFS facilitent la surveillance en cas de panne du serveur/dispositif géré.
Modem 56K intégré via une connexion RJ11 pour l'accès hors bande d'urgence	Permet un accès en urgence en cas de défaillance du réseau. Cette caractéristique permet à un administrateur d'accéder à l'équipement du serveur et du réseau en cas de dépannage ou de nécessité de restauration. Le modem intégré permet une installation propre et évite d'avoir à disposer d'un modem/de câbles et d'une alimentation externes. A la différence d'un serveur d'accès à distance distinct, de cartes modem PCMCIA intercalées et de solutions logicielles, le modem intégré, disponible sur certains modèles, réduit les niveaux de défaillance possibles.

Caractéristiques	Avantages
Prise en charge de la gestion de l'alimentation via CLI des barrettes de gestion de l'alimentation à distance de Raritan	<p>Une unité de gestion de l'alimentation Raritan peut être connectée à chaque port série de Dominion SX. Les clients peuvent également commander l'unité de gestion de l'alimentation sans l'aide d'une interface utilisateur graphique, via les scripts et l'interface de ligne de commande.</p> <p><b>Outlet associations for servers and networking devices with multiple power feeds, from one power distribution unit or multiple power distribution units.</b></p>
<b>Intégration à CommandCenter® Secure Gateway</b>	
Extensibilité	Une fois déployés avec CommandCenter Secure Gateway, des milliers de dispositifs Dominion SX peuvent être gérés par le biais d'une authentification et d'une autorisation centralisées.
Mise à niveau des firmware via une connexion réseau ou via CommandCenter Secure Gateway	Simplifie le déploiement des mises à niveau de firmware via CommandCenter Secure Gateway. L'administrateur peut programmer la mise à niveau des firmware pour un seul ou plusieurs dispositifs SX.
Prise en charge de la gestion de l'alimentation de l'interface utilisateur graphique via CommandCenter Secure Gateway ou des barrettes de gestion de l'alimentation à distance de Raritan	Les unités de gestion de l'alimentation de Raritan peuvent être connectées à chaque port série d'un dispositif Dominion SX. Pour les serveurs/équipements à plusieurs alimentations, plusieurs prises d'alimentation peuvent être combinées pour activer ou désactiver les équipements d'un simple clic de souris.
Adresse IP unique pour l'administration et la connexion aux cibles	<p><b>Administrators and users can connect to one IP address with one login via CommandCenter Secure Gateway to manage the SX or the targets. This connection can be via browser or through SSH. Only Raritan allows direct SSH connection to the aggregator.</b></p>

*New feature in Dominion SX Release 3.1 (GA Date via the website: March 2007).*