



Dominion® KX II

KX2-116 KX2-216 KX2-416
KX2-132 KX2-232 KX2-432
KX2-464



Manuel d'utilisation

Version 2.0

Copyright © 2007 Raritan, Inc.

DKX2-0B-E

Mai 2007

255-62-4023-00

Cette page est laissée intentionnellement blanche.

Copyright et marques

Ce document contient des informations propriétaires protégées par droits de copyright. Tous droits réservés. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans l'accord écrit préalable de Raritan, Inc.

© Copyright 2007 Raritan, Inc., CommandCenter®, RaritanConsole, Dominion® et le logo de la société Raritan sont des marques, déposées ou non, de Raritan, Inc. Tous droits réservés. Java® est une marque déposée de Sun Microsystems, Inc. Internet Explorer et Active Directory sont des marques déposées de Microsoft® Corporation. Netscape® et Netscape Navigator sont des marques déposées de Netscape Communication Corporation. Toutes les autres marques, déposées ou non, mentionnées dans ce document appartiennent à leurs propriétaires respectifs.

© Copyright 2007 GoAhead Software, Inc. Tous droits réservés.

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)

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 dommages 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.



Pour toute assistance en Amérique du Nord ou du Sud, veuillez contacter l'équipe de support technique Raritan par téléphone, au (732) 764-8886, par fax, au (732) 764-8887 ou par courrier électronique à l'adresse suivante : tech@raritan.com

*Contactez l'assistance technique – du lundi au vendredi, de 8h00 à 20h00
(heure de la côte Est des Etats-Unis).*

Pour toute assistance dans le reste du monde, consultez la dernière page de ce manuel pour connaître les informations sur le contact des bureaux régionaux Raritan.

Consignes de sécurité

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

- 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.

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](#) pour plus d'informations).
- 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, notamment les raccords d'alimentation tels que les barrettes d'alimentation (autres que celles branchées directement).

Table des matières

Chapitre 1 : Introduction.....	1
Présentation de Dominion KX II	1
Médias virtuels	2
Photos du produit	3
Caractéristiques du produit	4
Matériel	4
Logiciel	4
Terminologie	5
Contenu du coffret.....	6
Manuel d'utilisation.....	7
Présentation	7
Organisation des informations	7
Documentation connexe	7
Chapitre 2 : Mise en route.....	9
Informations de connexion	9
Adresse IP par défaut	9
Systèmes d'exploitation pris en charge (Clients)	9
Navigateurs pris en charge	9
Systèmes d'exploitation et CIM pris en charge (Serveurs cible)	10
Chapitre 3 : Installation et configuration.....	11
Présentation	11
Etape 1 : Configuration des serveurs cible	11
Résolution vidéo	11
Papier peint du Bureau	12
Paramètres de souris.....	12
Paramètres de souris et de vidéo en fonction du système d'exploitation.....	12
Etape 2 : Configuration des paramètres du pare-feu de réseau.....	17
Etape 3 : Connexion de l'équipement.....	18
Etape 4 : Configuration initiale de Dominion KX II	20
Modification du mot de passe par défaut	20
Affectation d'une adresse IP	21
Désignation des serveurs cible	22
Spécification de la détection automatique de l'alimentation.....	22
Note aux utilisateurs de CC-SG.....	23
Authentification à distance	24
Protocoles pris en charge	24
Authentification et autorisation.....	25
Utilisateurs, groupes et autorisations d'accès	26
Présentation	26
Utilisateurs	26
Groupes	26
Relation entre les utilisateurs et les groupes	26
Chapitre 4 : Se connecter à Dominion KX II	27
Interfaces utilisateur	27
Console locale KX II – Dispositifs KX II	27
Console distante KX II – Dispositifs KX II	27
Client MPC (Multi-Platform Client) – Dispositifs KX I et KX II	28
Raritan Remote Client (RRC) – Dispositifs KX I uniquement.....	28
Langues étrangères prises en charge	29
Remarques sur les langues étrangères prises en charge.....	29
Java Runtime Environment (JRE).....	29
Lancement de KX II.....	30
Disposition de la console KX II	31
Navigation dans la console KX II	32
Se déconnecter	32
Arborescence de menu de la console KX II.....	33
Gestion des favoris	34
Menu de gestion des favoris	35
Liste des favoris.....	36
Détection des dispositifs – Sous-réseau local	38

Détection des dispositifs – Sous-réseau KX	39
Ajouter un nouveau favori	40
Chapitre 5 : Accès aux serveurs cible	41
Page d'accès aux ports	41
Menu d'actions relatives aux ports	42
Connexion à un serveur cible	43
Commutation entre les serveurs cible	43
Déconnexion des serveurs cible	43
Alimentation électrique contrôlant un serveur cible	44
Eteindre et rallumer un serveur cible	44
Mettre sous tension un serveur cible	44
Mettre un serveur cible hors tension	44
Chapitre 6 : Virtual KVM Client (Client virtuel KVM)	45
Options	46
Arborescence de menus	46
Barre d'outils	46
Synchronisation des pointeurs de souris	47
Menu de connexion	48
Boîte de dialogue des propriétés	48
Informations sur la connexion	50
Exit (Quitter)	50
Menu de clavier	51
Send Ctrl+Alt+Delete (Envoyer Ctrl+Alt+Suppr)	51
Macros de clavier	51
Menu vidéo	54
Refresh Screen (Actualiser l'écran)	54
Auto-sense Video Settings (Détection automatique des paramètres vidéo)	54
Calibrer les couleurs	54
Video Settings (Paramètres vidéo)	55
Menu de souris	57
Synchronize Mouse (Synchroniser la souris)	57
Curseur de souris simple	57
Standard	58
Intelligent	58
Absolute (Absolu)	58
Médias virtuels	58
Menu Outils	59
Options	59
Menu d'affichage	60
Affichage de la barre d'outils	60
Scaling (Mise à l'échelle)	60
Résolution d'écran de la cible	60
Ecran Help Menu (Menu d'aide)	60
About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan)	60
Chapitre 7 : Médias virtuels	61
Présentation	61
Conditions requises pour l'utilisation des médias virtuels	62
Utilisation des médias virtuels	62
Ouvrir une session KVM	63
Se connecter à un média virtuel	63
Lecteurs locaux	63
Images ISO/CD-ROM/DVD-ROM	64
Déconnexion du média virtuel	65
Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement)	66
Chapitre 8 : User Management	67
User List (Liste des utilisateurs)	68
Ajouter un nouvel utilisateur	69
Modifier un utilisateur existant	70
Liste des groupes d'utilisateurs	71
Ajouter un nouveau groupe d'utilisateurs	72
Configuration des autorisations	73
Configuration des autorisations d'accès aux ports	73

LCA IP de groupes (Liste de contrôle d'accès).....	74
Modifier un groupe d'utilisateurs existant.....	76
Modifier le mot de passe.....	78
Paramètres d'authentification.....	79
Mise en application de l'authentification à distance LDAP.....	81
Mise en application de l'authentification à distance RADIUS.....	83
Chapitre 9 : Gestion Des Dispositifs	85
Menu Network Settings (Paramètres réseau).....	86
Menu Network Basic Settings (Paramètres réseau de base).....	87
Paramètres réseau divers.....	88
Paramètres de l'interface LAN.....	88
Paramètres date/heure.....	90
Gestion des événements.....	91
Gestion des événements - Paramètres.....	91
Gestion des événements - Destinations.....	93
Configuration de l'agent SNMP.....	94
Configuration des traps SNMP.....	95
Page de configuration de l'alimentation.....	96
Page de configuration des ports.....	97
Gestion de l'alimentation.....	98
Branchement de la barrette d'alimentation.....	98
Désigner les barrettes d'alimentation (Page des ports liés aux barrettes d'alimentation).....	99
Associez des serveurs cible aux prises (Page des ports).....	100
Chapitre 10 : Paramètres de sécurité	103
Paramètres de sécurité.....	104
Limitations de connexion.....	105
Mots de passe sécurisés.....	105
Blocage des utilisateurs.....	106
Cryptage & Partage.....	107
Contrôle d'accès IP.....	109
Chapitre 11 : Maintenance	111
Journal d'audit.....	112
Informations relatives au dispositif.....	113
Sauvegarde et restauration.....	114
Mise à niveau du CIM.....	116
Mise à niveau du firmware.....	117
Rapport de mise à niveau.....	119
Redémarrage.....	120
Chapitre 12 : Diagnostics.....	121
Menu Diagnostics.....	121
Page d'interface réseau.....	122
Page de statistiques réseau.....	123
Page d'envoi de commande Ping à l'hôte.....	125
Page de détermination du parcours de réseau jusqu'à l'hôte.....	126
KX Diagnostics (Diagnostics KX).....	127
Chapitre 13 : Console locale KX II.....	129
Console locale KX II.....	129
Connexions physiques.....	129
Bouton de réinitialisation.....	130
Démarrage de la console locale KX II.....	131
Interface de la console locale KX II.....	131
Accès aux serveurs cible.....	132
Administration du port local.....	134
Paramètres du port local (Console locale KX II uniquement).....	134
Restauration des valeurs d'usine (Console locale KX II uniquement).....	136
Chapitre 14 : CC Unmanage	139
Présentation.....	139
Retrait de Dominion KX II de la gestion CC-SG.....	139

Annexe A : Caractéristiques	141
Connexion à distance.....	142
Propriétés KVM.....	142
Ports TCP et UDP utilisés	143
Distance de connexion et résolution vidéo du serveur cible	144
Annexe B : Mise à jour du schéma LDAP	145
Renvoi des informations relatives aux groupes d'utilisateurs.....	145
A partir de LDAP.....	145
A partir de Active Directory (AD) de Microsoft	145
Définition du registre pour autoriser les opérations d'écriture sur le schéma.....	145
Création d'un nouvel attribut	145
Ajout d'attributs à la classe	146
Mise à jour du cache de schéma	147
Modification des attributs du groupe d'utilisateurs pour les membres utilisateurs.....	147
Annexe C : FAQ	149
Questions générales	149
Accès à distance	151
Média virtuel universel	153
Ethernet et mise en réseau IP	154
Serveurs	157
Installation	158
Port local	160
Gestion de l'alimentation.....	162
Evolutivité.....	163
Modules d'interface pour ordinateurs.....	164
Sécurité	165
Capacités de gestion.....	166
Divers	167
Guide de dépannage.....	168

Figures

Figure 1 : Configuration de Dominion KX II.....	1
Figure 2 : Dominion KX2-116.....	3
Figure 3 : Dominion KX2-432.....	3
Figure 4 : CIM Dominion KX II : D2CIM-VUSB (à gauche) ; D2CIM-PWR (à droite)	3
Figure 5 : Terminologie et topologie.....	5
Figure 6 : Configuration de la souris Solaris	15
Figure 7 : Connexions de Dominion KX II	18
Figure 8 : Menu Network Settings (Paramètres réseau)	21
Figure 9 : Configuration des ports.....	22
Figure 10 : Organigramme relatif aux authentifications/autorisations	25
Figure 11 : Page de connexion de la console distante de Dominion KX II.....	30
Figure 12 : Page principale de la console distante KX II.....	31
Figure 13 : Page principale de la console locale KX II	31
Figure 14 : Exemple de hiérarchie de menu (chemins de navigation)	32
Figure 15 : Arborescence de menu des consoles KX II (locale et distante)	33
Figure 16 : Dispositifs favoris (encadré).....	34
Figure 17 : Menu de gestion des favoris	35
Figure 18 : Liste des favoris	36
Figure 19 : Modifier (informations relatives aux favoris).....	37
Figure 20 : Détection des dispositifs - Sous-réseau local	38
Figure 21 : Détection des dispositifs - Sous-réseau KX	39
Figure 22 : Ajouter un nouveau favori	40
Figure 23 : Port Access (Accès aux ports).....	41
Figure 24 : Menu d'actions relatives aux ports.....	43
Figure 25 : Menu d'actions relatives aux ports (options d'alimentation)	44
Figure 26 : Fenêtre de Virtual KVM Client (Client virtuel KVM).....	45
Figure 27 : Arborescence de menus de Virtual KVM Client	46
Figure 28 : Curseurs de souris doubles	47
Figure 29 : Boîte de dialogue des propriétés	48
Figure 30 : Informations sur la connexion	50
Figure 31 : Macros de clavier.....	51
Figure 32 : Ajouter une macro de clavier	52
Figure 33 : Exemple de macro de clavier.....	52
Figure 34 : Nouvelle macro dans le menu Clavier	53
Figure 35 : Video Settings (Paramètres vidéo)	55
Figure 36 : Message du curseur de souris simple.....	57
Figure 37 : Options (Outils).....	59
Figure 38 : Connexion à un média virtuel	61
Figure 39 : Ouvrir une session KVM	63
Figure 40 : Map Virtual Media Drive (Mapper le lecteur de média virtuel)	63
Figure 41 : Map Virtual Media CD/ISO Image (Mapper l'image ISO/CD de média virtuel)	64

Figure 42 : Configuration des serveurs de fichiers.....	66
Figure 43 : Menu User Management (Gestion des utilisateurs).....	67
Figure 44 : User List (Liste des utilisateurs).....	68
Figure 45 : Page User (Utilisateur).....	69
Figure 46 : Liste des groupes d'utilisateurs.....	71
Figure 47 : Page Group (Groupe).....	72
Figure 48 : Liste de contrôle d'accès par adresse IP applicable à des groupes.....	74
Figure 49 : Exemple de LCA IP.....	75
Figure 50 : Modifier un groupe.....	76
Figure 51 : Modifier le mot de passe.....	78
Figure 52 : Paramètres d'authentification.....	79
Figure 53 : Paramètres d'authentification (LDAP).....	81
Figure 54 : Ecran Authentication Settings (Paramètres d'authentification).....	83
Figure 55 : Menu relatif aux paramètres du dispositif.....	85
Figure 56 : Menu Network Settings (Paramètres réseau).....	86
Figure 57 : Paramètres réseau (Paramètres réseau de base).....	87
Figure 58 : Paramètres réseau (paramètres réseau divers).....	88
Figure 59 : Paramètres réseau (Paramètres de l'interface LAN).....	88
Figure 60 : Paramètres date/heure.....	90
Figure 61 : Gestion des événements - Paramètres.....	91
Figure 62 : Configuration de Syslog.....	92
Figure 63 : Gestion des événements - Destinations.....	93
Figure 64 : Configuration de l'alimentation.....	96
Figure 65 : Configuration des ports.....	97
Figure 66 : Branchements des barrettes d'alimentation.....	98
Figure 67 : Page relative aux ports (barrettes d'alimentation).....	99
Figure 68 : Page des ports (ports KVM).....	100
Figure 69 : Page des ports (Paramètres du serveur cible pour D2CIM-VUSB).....	101
Figure 70 : Menu de sécurité.....	103
Figure 71 : Paramètres de sécurité.....	104
Figure 72 : Paramètres de sécurité (Mots de passe sécurisés).....	105
Figure 73 : Paramètres de sécurité (Blocage des utilisateurs).....	106
Figure 74 : Paramètres de sécurité (Cryptage & Partage).....	107
Figure 75 : Paramètres de sécurité (Message d'avertissement relatif au mode de chiffrement).....	107
Figure 76 : Contrôle d'accès IP.....	109
Figure 77 : Menu de maintenance.....	111
Figure 78 : Journal d'audit.....	112
Figure 79 : Informations relatives au dispositif.....	113
Figure 80 : Sauvegarde/Restauration.....	114
Figure 81 : Mise à niveau du CIM à partir de KX Flash.....	116
Figure 82 : Mise à niveau du firmware.....	117
Figure 83 : Vérification de la mise à niveau du firmware.....	118
Figure 84 : Mise à niveau du firmware réussie.....	118

Figure 85 : Rapport de mise à niveau	119
Figure 86 : Redémarrage	120
Figure 87 : Confirmation du redémarrage	120
Figure 88 : Menu Diagnostics	121
Figure 89 : Interface réseau	122
Figure 90 : Statistiques réseau (statistiques)	123
Figure 91 : Statistiques réseau (interfaces).....	123
Figure 92 : Statistiques réseau (route)	124
Figure 93 : Envoyer une commande Ping à l'hôte	125
Figure 94 : Tracer le parcours de réseau jusqu'à l'hôte	126
Figure 95 : KX Diagnostics (Diagnostics KX)	127
Figure 96 : Scripts de diagnostics	128
Figure 97 : Téléchargement de fichier	128
Figure 98 : Console locale Dominion KX II.....	129
Figure 99 : Panneau Local User (Utilisateur local) sur Dominion KX II	129
Figure 100 : Bouton de réinitialisation (partie arrière de l'unité)	130
Figure 101 : Accès au port de la console locale.....	132
Figure 102 : Local Port Settings (Paramètres du port local).....	134
Figure 103 : Restauration des valeurs d'usine (Console locale uniquement).....	136
Figure 104 : Message du dispositif géré par CC-SG.....	139
Figure 105 : Suspendre la gestion par CC-SG.....	139
Figure 106 : Confirmer CC Unmanage	140
Figure 107 : Dispositif retiré de la gestion CC.....	140
Figure 108 : Création d'un nouvel attribut	146
Figure 109 : Ajout d'attributs à la classe	146
Figure 110 : ADSI Edit	147
Figure 111 : Propriétés des utilisateurs.....	148
Figure 112 : Edit Attribute (Modifier l'attribut) - ajout d'un utilisateur au groupe KXII	148

Chapitre 1 : Introduction

Présentation de Dominion KX II

Dominion KX II est un commutateur KVM (écran-clavier-souris) numérique sécurisé conçu pour l'entreprise qui offre un accès au niveau BIOS (et supérieur) et permet de gérer jusqu'à 64 serveurs, où que vous vous trouviez dans le monde, par l'intermédiaire d'un navigateur Web. Sur le rack, Dominion KX II offre une gestion au niveau BIOS de 64 serveurs et autres dispositifs informatiques depuis un ensemble clavier, écran et souris unique. Les fonctions d'accès à distance intégré de Dominion KX II procurent ainsi une gestion totale au niveau de vos serveurs par l'intermédiaire d'un navigateur Web.

L'installation de Dominion KX II est facilitée par l'utilisation d'un câblage UTP (Cat5/5e/6) standard. Ses caractéristiques clés sont les suivantes : média virtuel, chiffrement 128 bits, double alimentation, gestion de l'alimentation à distance, Ethernet double, LDAP, RADIUS, Active Directory, intégration de Syslog et gestion Web. Ces fonctions permettent d'améliorer les temps d'exploitation, la productivité et la sécurité, n'importe où, n'importe quand.

Les produits Dominion KX II peuvent fonctionner de manière autonome et ne dépendent pas d'un dispositif de gestion central. Pour les centres de données et les entreprises de plus grande envergure, plusieurs unités Dominion KX II (associées à des unités Dominion SX pour l'accès à distance à une console série et à des unités Dominion KSX pour la gestion des bureaux distants et des filiales) peuvent être intégrées dans une solution logique *unique* à l'aide de la console de gestion CommandCenter Secure Gateway (CC-SG) de Raritan.

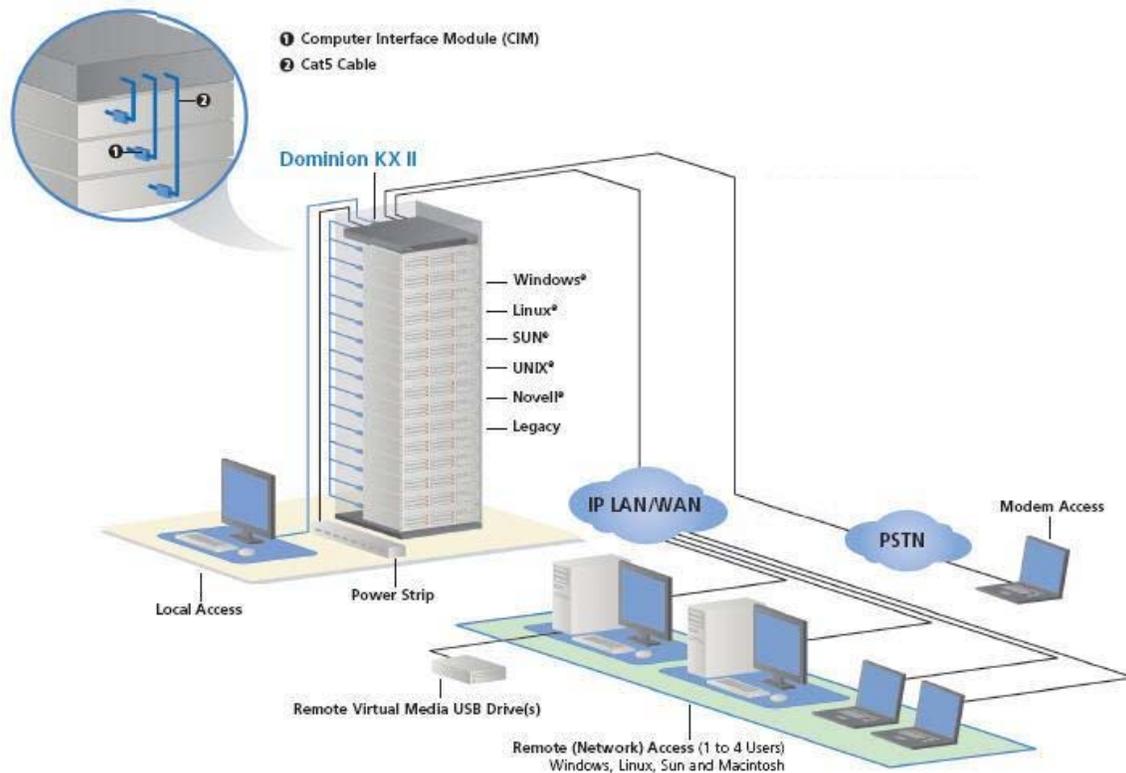


Figure 1 : Configuration de Dominion KX II

Médias virtuels

Tous les modèles Dominion KX II prennent en charge les médias virtuels. Les avantages des médias virtuels (installation de lecteurs/médias à distance sur le serveur cible pour prendre en charge l'installation de logiciel, le démarrage à distance et les diagnostics) sont désormais disponibles dans tous les modèles Dominion KX II.

Chaque produit Dominion KX II est équipé d'un média virtuel pour permettre la gestion à distance des tâches via la gamme la plus vaste de CD, de DVD, d'USB, de périphériques distants et internes ainsi que d'images. Contrairement à d'autres solutions, Dominion KX II prend en charge l'accès de médias virtuels à des disques durs et à des images montées à distance pour plus de flexibilité et de productivité.

Les sessions de médias virtuels sont sécurisées par le biais du chiffrement RC4 ou AES 128 bits.

La nouvelle technologie D2CIM-VUSB CIM (module d'interface pour ordinateur (CIM)) supporte les sessions de médias virtuels sur les serveurs cible qui prennent en charge l'interface USB 2.0. Ce nouveau CIM prend également en charge Absolute Mouse Synchronization™ ainsi que la mise à jour du firmware à distance.

Photos du produit



Figure 2 : Dominion KX2-116



Figure 3 : Dominion KX2-432



Figure 4 : CIM Dominion KX II : D2CIM-VUSB (à gauche) ; D2CIM-PWR (à droite)

Caractéristiques du produit

Matériel

- Accès distant KVM sur IP intégré
- Montage en rack (KX2-464) 1U ou 2U ; supports de fixation fournis
- Double alimentation avec fonction de basculement automatique, alimentation à commutation automatique avec avertissement de panne de courant
- 16, 32 ou 64 (sur KX2-464) ports de serveur
- Fonction pour utilisateurs multiples (1/2/4 utilisateurs distants, 1 utilisateur local)
- Câblage de serveur UTP (Cat5/5e/6)
- Ports Ethernet doubles (10/100/1000 LAN) à protection par basculement
- Possibilité de mises à niveau du champ
- Port utilisateur local pour accès en rack
 - Ports de souris/clavier PS/2
 - Ports USB 2.0 du panneau avant et des trois panneaux arrière pour les dispositifs USB pris en charge
 - Simultanéité complète avec les utilisateurs distants
 - Interface graphique utilisateur (GUI) locale pour l'administration
- Sécurité de l'accès centralisé
- Contrôle d'alimentation intégré
- Voyants indiquant l'état de la double alimentation, l'activité du réseau et l'état des utilisateurs distants
- Touche de réinitialisation matérielle

Logiciel

- Média virtuel avec D2CIM-VUSB CIM
- Synchronisation absolue de la souris avec D2CIM-VUSB CIM
- Plug and Play
- Gestion et accès Web
- Interface utilisateur graphique intuitive
- Chiffrement 128 bits de l'ensemble du signal KVM, signal vidéo et média virtuel inclus
- LDAP, Active Directory, RADIUS ou authentification interne et autorisation
- Adressage DHCP ou IP fixe
- Gestion Syslog et SNMP
- Gestion de l'alimentation associée directement aux serveurs pour éviter les erreurs
- Intégration avec la console de gestion CommandCenter Secure Gateway (CC-SG) de Raritan
- Fonction CC Unmanage pour suspendre la gestion d'un dispositif par CC-SG.

Terminologie

Ce manuel utilise la terminologie suivante pour désigner les composants d'une configuration Dominion KX II type :

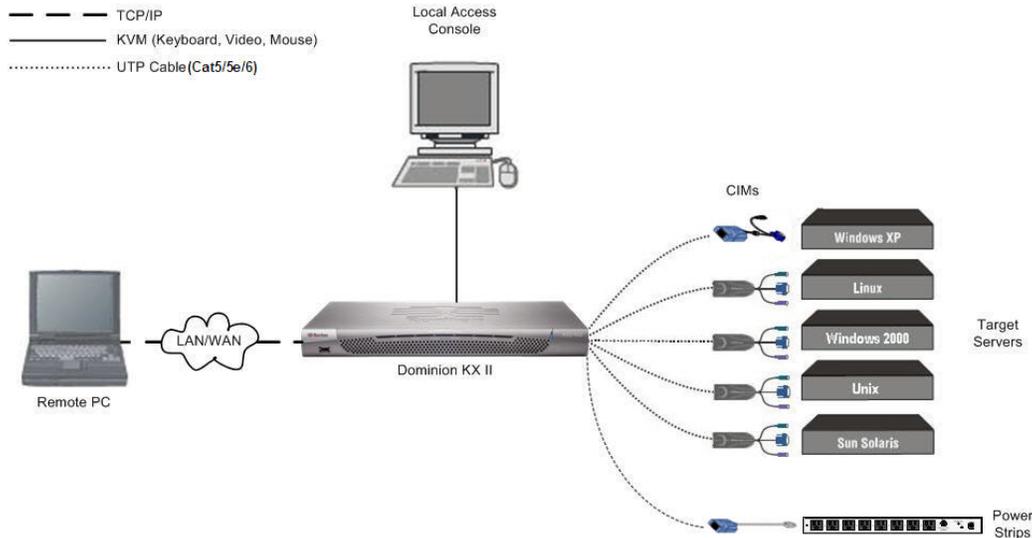


Figure 5 : Terminologie et topologie

**Ordinateur distant
(Remote PC)
(client)**

Ordinateurs mis en réseau utilisés pour accéder aux serveurs cible connectés à Dominion KX II et les gérer. Reportez-vous à [Systèmes d'exploitation pris en charge \(clients\)](#) pour la liste des systèmes d'exploitation pris en charge par Dominion KX II à distance.

**Console d'accès local
(Local Access Console)
(client)**

Console utilisateur facultative (constituée d'un clavier, d'une souris et d'un écran VGA Multisync) directement reliée à Dominion KX II pour gérer localement des serveurs cible (directement au niveau du rack et non par l'intermédiaire du réseau).

**Modules d'interface
pour ordinateurs
(CIM)(Modules
d'interface pour
ordinateurs)**

Clés connectées sur chacun des serveurs cible et chacune des barrettes d'alimentation Raritan. Disponibles pour tous les systèmes d'exploitation pris en charge. Reportez-vous à [CIM pris en charge](#) pour obtenir des informations sur les CIM pris en charge par Dominion KX II.

**Serveurs cible
(Target Servers)**

Serveurs équipés de cartes vidéo et d'interfaces utilisateur (par ex. Windows®, Linux®, Solaris™, etc.) auxquels il est possible d'accéder à distance par l'intermédiaire de Dominion KX II. Reportez-vous à [Systèmes d'exploitation et CIM pris en charge \(Serveurs cible\)](#) pour la liste des systèmes d'exploitation et des CIM pris en charge.

**Barrettes
d'alimentation**

Barrettes d'alimentation Raritan accessibles à distance par l'intermédiaire de Dominion KX II.

Contenu du coffret

Chaque Dominion KX II fourni est un produit autonome totalement configuré, monté dans un châssis de montage en rack 1U (2U pour KX2-464) 19" standard. Les unités Dominion KX II sont livrées avec les éléments suivants :

- (1) Unité Dominion KX
- (1) Guide d'installation et de configuration rapides de Dominion
- (1) CD-ROM du manuel d'utilisation Raritan
- (1) Kit de montage en rack
- (2) Cordons d'alimentation secteur
- (1) Câble réseau Cat5
- (1) Câble réseau croisé Cat5
- (1) Ensemble de 4 pieds en caoutchouc (pour utilisation sur le)
- (1) Note d'application
- (1) Carte de garantie

Manuel d'utilisation

Présentation

Le manuel d'utilisation du Dominion KX II fournit les informations nécessaires pour installer et configurer les serveurs cible ainsi que les barrettes d'alimentation, y accéder, utiliser les médias virtuels, gérer les utilisateurs et la sécurité, ainsi que maintenir et diagnostiquer le Dominion KX II.

Ce manuel d'utilisation est spécifique à Dominion KX II (version 2.0). Pour toute information relative à la version 1.4, veuillez vous reporter au *manuel d'utilisation de Dominion KX 1.4*.

Organisation des informations

Le manuel d'utilisation est organisé comme suit :

- Chapitre 1, *Introduction*. Présentation, fonctions, terminologie et contenu du coffret
- Chapitre 2, *Mise en route*. Informations de connexion, adresse IP par défaut, systèmes d'exploitation, navigateurs et modules d'interface pour ordinateurs (CIM) pris en charge
- Chapitre 3, *Installation et configuration*. Configuration du serveur cible, paramètres du pare-feu, connexions physiques des dispositifs, configuration de l'unité KX II initiale, authentification à distance, utilisateurs, groupes et autorisations d'accès
- Chapitre 4, *Se connecter à Dominion KX II*. Interfaces utilisateur, démarrage de la console KX II à distance, favoris de Dominion KX II
- Chapitre 5, *Accès aux serveurs cible*. Accès, contrôle et commutation entre les serveurs cible
- Chapitre 6, *Client KVM virtuel*. Gestion des serveurs cible, synchronisation des pointeurs de souris, macros de clavier et réglage des paramètres vidéo
- Chapitre 7, *Médias virtuels*. Configuration et accès des médias virtuels
- Chapitre 8, *Gestion des utilisateurs*. Gestion des groupes et des utilisateurs, mots de passe, contrôle d'accès IP des groupes et paramètres d'authentification
- Chapitre 9, *Gestion des dispositifs*. Paramètres réseau, date/heure, gestion des événements, paramètres d'alimentation, configuration des ports et gestion de l'alimentation
- Chapitre 10, *Paramètres de sécurité*. Paramètres de sécurité et contrôle d'accès IP
- Chapitre 11, *Maintenance*. Journal d'audit, informations sur les dispositifs, sauvegarde et restauration, mises à niveau du CIM et du firmware, redémarrage
- Chapitre 12, *Diagnostics*. Interface réseau, statistiques de réseaux, envoi d'une commande Ping à un hôte, détermination d'itinéraire jusqu'à un hôte et diagnostics KX
- Chapitre 13, *Console locale KX II*. Démarrage de la console locale KX II, accès aux serveurs cible et administration du port local
- Chapitre 14, *CC Unmanage*. Suspension de la gestion de KX II par CC-SG
- Annexe A, *Spécifications* Spécifications physiques, ports utilisés, distance de connexion des serveurs cible et résolution vidéo
- Annexe B, *Mise à jour du schéma LDAP*. Mise à jour du schéma LDAP (pour les utilisateurs expérimentés)
- Annexe C, *Foire aux questions (FAQ)*. Questions générales, accès distant, médias virtuels universels, Ethernet et mise en réseau IP, serveurs, installation, port local, gestion de l'alimentation, évolutivité, modules d'interface pour ordinateurs (CIM), sécurité, réparabilité, divers et dépannage

Documentation connexe

Pour de plus amples informations sur le Client MPC (Multi-Platform Client) de Raritan, consultez le manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC).

Pour de plus amples informations sur la gamme entière des produits Raritan, consultez le *CD-ROM Raritan incluant les manuels d'utilisation et les guides de démarrage rapide* ou le site Web de Raritan à l'adresse suivante : <http://www.raritan.com/support/productdocumentation>

Chapitre 2 : Mise en route

Informations de connexion

- Le nom d'utilisateur et le mot de passe par défaut de Dominion KX II sont **admin** et **raritan**. Si vous vous connectez sous ce nom d'utilisateur et ce mot de passe, vous disposez des droits d'administrateur.
- Les mots de passe respectent la casse, ils doivent être saisis exactement de la même manière que lors de leur création. Par exemple, le mot de passe par défaut **raritan** doit être saisi uniquement en lettres minuscules.
- La première fois que vous démarrez Dominion KX II, il vous est demandé de changer le mot de passe par défaut.

Conseil : Pour assurer la sauvegarde et la continuité des opérations, il vous est fortement recommandé de créer un nom d'utilisateur et un mot de passe de secours spécifiques pour l'administrateur et de conserver ces informations dans un emplacement sécurisé.

Adresse IP par défaut

Dominion KX II est livré avec l'adresse IP par défaut 192.168.0.192.

Systemes d'exploitation pris en charge (Clients)

Les systèmes d'exploitation suivants sont pris en charge sur Dominion KX II Remote Console, Virtual KVM Client™ et Multi-Platform Client (MPC) :

SYSTEME D'EXPLOITATION CLIENT	PRISE EN CHARGE DES MEDIAS VIRTUELS SUR ORDINATEUR CLIENT
Windows XP	Oui
Windows 2000 SP4	Oui
Windows Vista	Oui
Red Hat Linux 9.0	Oui, image ISO conservée localement, montage du serveur de fichiers distant directement à partir de KX
Red Hat Enterprise Workstation 3.0 et 4.0	Oui, image ISO conservée localement, montage du serveur de fichiers distant directement à partir de KX
SUSE Linux Professional 9.2 et 10	Oui, image ISO conservée localement, montage du serveur de fichiers distant directement à partir de KX
Fedora™ Core 5 et supérieur	Oui, image ISO conservée localement, montage du serveur de fichiers distant directement à partir de KX
Mac®	Non
Solaris	Non

Navigateurs pris en charge

Dominion KX II prend en charge les navigateurs suivants :

- Internet Explorer 6 et 7
- Firefox® 1.5 et 2.0
- Mozilla® 1.7
- Safari 2.0

Systemes d'exploitation et CIM pris en charge (Serveurs cible)

Outre les nouvelles unités Dominion KX II D2CIM, la plupart des CIM Paragon® et CIM Dominion KX I sont pris en charge. Le tableau suivant indique les systemes d'exploitation des serveurs cible, les CIM, les medias virtuels et les modes souris pris en charge :

SERVEUR CIBLE	CIM PRIS EN CHARGE			VM (MÉDIA VIRTUEL)	MODES SOURIS		
	PARAGON CIMs	DOMINION KX I DCIM	MODELES D2CIM		AM	IM	SM
Windows XP Windows 2000 Windows 2000 Server Windows 2003 Server Windows Vista	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓	✓	✓
Red Hat Linux 9.0 Red Hat Enterprise Workstation 3.0 et 4.0	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (excepté Red Hat Enterprise Workstation 3.0)	✓			✓
SUSE Linux Professional 9.2 et 10	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD P2CIM-USBG2 UKVMC USKVMC P2CIM-PS2DUAL	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora Core 3 et supérieur	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD P2CIM-USBG2 UKVMC USKVMC P2CIM-PS2DUAL	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	P2CIM-AUSB UUSBPD P2CIM-USBG2	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
Tous les systemes d'exploitation Solaris pris en charge dans Dominion KX I	USKVMC P2CIM-SUN P2CIM-SUSB	DCIM-SUN DCIM-SUSB					✓
IBM AIX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Barrettes d'alimentation à distance			D2CIM-PWR				
Dispositifs série	P2CIM-SER P2CIM-SER-EU AUATC						

Légende :

- VM (Virtual Media) : medias virtuels (D2CIM-VUSB uniquement)
- AM (Absolute Mouse) : Absolute Mouse Synchronization (D2CIM-VUSB uniquement)
- IM (Intelligent Mouse) : Intelligent Mouse Mode
- SM (Standard Mouse) : Standard Mouse Mode
- ✓ : pris en charge

Remarque : D2CIM-VUSB n'est pas pris en charge sur les serveurs cible Sun (Solaris).

Chapitre 3 : Installation et configuration

Présentation

Cette section offre un bref aperçu du processus d'installation. Chaque étape est décrite en détails dans les autres sections de ce chapitre.

Pour installer et configurer Dominion KX II :

1. Configurez les serveurs cible.
2. Configurez les paramètres du pare-feu du réseau.
3. Branchez l'équipement.
4. Configurez l'unité Dominion KX II.

Etape 1 : Configuration des serveurs cible

Les serveurs cibles sont les ordinateurs auxquels Dominion KX II permet d'accéder et qu'il permet également de gérer. Avant d'installer Dominion KX II, configurez *tous* les serveurs cible afin d'obtenir des performances optimales. Cette configuration s'applique aux *serveurs cible* uniquement, pas aux postes de travail client (ordinateurs distants) utilisés pour accéder à distance à Dominion KX II. Reportez-vous à [Chapitre 1 : Introduction, Terminologie](#) pour obtenir des informations supplémentaires.

Pour configurer les serveurs cible :

- Vérifiez la résolution vidéo.
- Vérifiez le papier peint du Bureau.
- Réglez les paramètres de la souris.
- Configurez la vidéo et la souris conformément à votre système d'exploitation.

Résolution vidéo

Assurez-vous que Dominion KX II prend en charge la résolution vidéo et le taux de rafraîchissement des différents serveurs cible et que le signal *n'est pas entrelacé*.

Résolutions vidéo prises en charge

Dominion KX II prend en charge les résolutions suivantes :

640 x 350 à 70 Hz	720 x 400 à 85 Hz	1 024 x 768 à 90 Hz
640 x 350 à 85 Hz	800 x 600 à 56 Hz	1 024 x 768 à 100 Hz
640 x 400 à 56 Hz	800 x 600 à 60 Hz	1 152 x 864 à 60 Hz
640 x 400 à 84 Hz	800 x 600 à 70 Hz	1 152 x 864 à 70 Hz
640 x 400 à 85 Hz	800 x 600 à 72 Hz	1 152 x 864 à 75 Hz
640 x 480 à 60 Hz	800 x 600 à 75 Hz	1 152 x 864 à 85 Hz
640 x 480 à 66,6 Hz	800 x 600 à 85 Hz	1 152 x 870 à 75,1 Hz
640 x 480 à 72 Hz	800 x 600 à 90 Hz	1 152 x 900 à 66 Hz
640 x 480 à 75 Hz	800 x 600 à 100 Hz	1 152 x 900 à 76 Hz
640 x 480 à 85 Hz	832 x 624 à 75,1 Hz	1 280 x 960 à 60 Hz
640 x 480 à 90 Hz	1 024 x 768 à 60 Hz	1 280 x 960 à 85 Hz
640 x 480 à 100 Hz	1 024 x 768 à 70 Hz	1280 x 1024 à 60 Hz
640 x 480 à 120 Hz	1 024 x 768 à 72 Hz	1280 x 1024 à 75 Hz
720 x 400 à 70 Hz	1 024 x 768 à 75 Hz	1280 x 1024 à 85 Hz
720 x 400 à 84 Hz	1 024 x 768 à 85 Hz	1 600 x 1 200 à 60 Hz

Remarque : la synchronisation composite et la vidéo Sync-on-Green nécessitent un adaptateur supplémentaire.

Papier peint du Bureau

Pour une utilisation de bande passante et une qualité vidéo optimales, les serveurs cible qui exécutent des interfaces utilisateur graphiques telles que Windows, Linux, X-Windows, Solaris et KDE doivent être configurés. Il n'est pas nécessaire que le papier peint du Bureau soit *complètement* uni. Evitez cependant les papiers peints de Bureau ornés de photos ou de dégradés complexes qui peuvent nuire aux performances.

Paramètres de souris

Le Dominion KX II fonctionne dans plusieurs modes souris :

- [Mode Absolu](#) (D2CIM-VUSB uniquement)
- [Mode Intelligent](#) (n'utilisez pas de souris animée)
- [Mode standard](#)

Quel que soit le mode de souris suivant : Standard ou Intelligent, les paramètres de la souris doivent être configurés sur des valeurs spécifiques décrites plus loin dans ce manuel. En revanche, les paramètres de souris ne doivent pas être modifiés pour la synchronisation absolue de la souris car le module D2CIM-VUSB est requis pour ce mode. La configuration de la souris varie en fonction des systèmes d'exploitation cible. Pour plus de détails, reportez-vous à la documentation de votre système d'exploitation.

Le mode de souris Intelligent fonctionne en général parfaitement sur la plupart des plates-formes Windows. Il se peut que le mode de souris Intelligent produise des résultats instables lorsque Active Desktop est activé sur le serveur cible. Pour davantage d'informations sur le mode de souris Intelligent, consultez le *manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC) (Annexe B : Conditions applicables à la synchronisation intelligente de la souris)* disponible sur le site Web de Raritan à l'adresse suivante :

<http://www.raritan.com/support/productdocumentation> ou les manuels d'utilisation et les guides de configuration rapide du CD-ROM inclus dans le coffret de Dominion KX II.

Paramètres de souris et de vidéo en fonction du système d'exploitation

Cette section fournit des informations sur les modes de vidéo et de souris spécifiques au système d'exploitation utilisé sur le serveur cible.

Paramètres Windows XP/Windows 2003

Pour configurer les serveurs cible exécutant Microsoft Windows XP/2003 :

1. Définissez les paramètres de la souris :
 - a. Sélectionnez **Start (Démarrer) > Control Panel (Panneau de configuration) > Mouse (Souris)**.
 - b. Ouvrez l'onglet **Pointer Options (Options du pointeur)**. Dans la partie **Motion (Vitesse du pointeur)** :
 - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
 - Désélectionnez la case **Enhance pointer precision** (Améliorer la précision du pointeur).
 - Cliquez sur **OK**.
2. Désactivez les effets de transition :
 - a. Sélectionnez l'option **Display (Affichage)** à partir du panneau de configuration.
 - b. Ouvrez l'onglet **Appearance (Apparence)**.
 - c. Cliquez sur le bouton **Effects (Effets)**.

- d. Désélectionnez la case **Use the following transition effect for menus and tooltips (Utiliser l'effet de transition suivant pour les menus et les info-bulles)**.
- e. Cliquez sur **OK**.
- f. Fermez le Panneau de configuration.

***Remarque :** pour les serveurs cible exécutant Windows 2000 ou XP, il est possible que vous souhaitiez créer un nom d'utilisateur qui sera utilisé uniquement pour les connexions à distance par l'intermédiaire de Dominion KX II. Cette opération permet de conserver les paramètres d'accélération/de mouvement lent du pointeur de la souris du serveur cible exclusivement pour la connexion Dominion KX II.*

Les écrans de connexion de Windows XP et 2000 rétablissent les paramètres prédéfinis de la souris qui diffèrent des paramètres suggérés pour une performance optimale de Dominion KX II. En conséquence, il se peut que la synchronisation de la souris ne soit pas optimale pour ces écrans. Si vous savez comment régler le registre des serveurs cible Windows, vous pouvez obtenir une meilleure synchronisation de la souris Dominion KX II dans les écrans de connexion en utilisant l'éditeur de registre Windows pour modifier les paramètres suivants (HKEY_CURRENT_USER\Control Panel\Mouse) : Vitesse de la souris = 0; Seuil de la souris 1 = 0; Seuil de la souris 2 = 0.

Paramètres Windows 2000

Pour configurer les serveurs cible exécutant Microsoft Windows 2000 :

1. Définissez les paramètres de la souris :
 - a. Sélectionnez **Start (Démarrer) > Control Panel (Panneau de configuration) > Mouse (Souris)**.
 - b. Ouvrez l'onglet **Motion (Mouvement)**.
 - Définissez l'accélération du pointeur sur None (Aucune).
 - Réglez la **vitesse de déplacement du pointeur de la souris exactement au milieu**.
 - Cliquez sur **OK**.
2. Désactivez les effets de transition :
 - a. Sélectionnez l'option **Display (Affichage)** à partir du panneau de configuration.
 - b. Ouvrez l'onglet **Effects (Effets)**.
 - c. Désélectionnez la case **Use the following transition effect for menus and tooltips (Utiliser l'effet de transition suivant pour les menus et les info-bulles)**.
 - d. Cliquez sur **OK**.
 - e. Fermez le Panneau de configuration.

Windows Vista

Pour configurer les serveurs cible exécutant Microsoft Windows Vista :

1. Définissez les paramètres de la souris :
 - a. Sélectionnez **Start (Démarrer) > Settings (Paramètres) > Control Panel (Panneau de configuration)**.
 - b. Ouvrez l'onglet **Pointer Options (Options du pointeur)**. Dans la partie **Motion (Vitesse du pointeur)** :
 - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
 - Désélectionnez la case **Enhance pointer precision (Améliorer la précision du pointeur)**.
 - Cliquez sur **OK**.

2. Désactivez les effets de fondu et d'animation :
 - a. Sélectionnez l'option **System (Système)** à partir du **panneau de configuration**.
 - b. Choisissez **Advanced system settings (Paramètres système avancés)**. La boîte de dialogue des propriétés du système s'affiche.
 - c. Ouvrez l'onglet **Advanced (Avancé)**.
 - d. Cliquez sur le bouton **Settings (Paramètres)** dans le champ des performances. La boîte de dialogue des options de performances s'affiche.
 - e. Sous les options **Custom (Personnaliser)**, désélectionnez les cases suivantes :

<i>Options d'animation :</i>	
<input type="checkbox"/>	Animate controls and elements inside windows (Animer les commandes et les éléments à l'intérieur des fenêtres)
<input type="checkbox"/>	Animate windows when minimizing and maximizing (Animer les fenêtres lors de la réduction et de l'agrandissement)
<i>Options de fondu :</i>	
<input type="checkbox"/>	Fade or slide menus into view (Fondre ou faire glisser les menus dans la zone de visualisation)
<input type="checkbox"/>	Fade or slide ToolTips into view (Fondre ou faire glisser les info-bulles dans la zone de visualisation)
<input type="checkbox"/>	Fade out menu items after clicking (Fermer en fondu les commandes de menu après le clic de souris)

- f. Cliquez sur **OK**.
- g. Fermez le Panneau de configuration.

Paramètres Linux

Remarque : les paramètres suivants concernent uniquement le mode souris Standard.

Pour configurer les serveurs cible exécutant Linux (interface utilisateur graphique) :

1. Définissez les paramètres de la souris :
 - a. Sélectionnez **System (Système) > Preferences (Préférences) > Mouse (Souris)**. La boîte de dialogue des préférences de la souris s'affiche.
 - b. Ouvrez l'onglet **Motion (Mouvement)**.
 - c. Définissez la vitesse d'accélération (**Speed Acceleration**) sur 1.
 - d. Réglez l'option **Drag & Drop Threshold (Glisser-déposer le seuil)** sur 1.
2. Configurez la résolution d'écran :
 - a. Sélectionnez **System (Système) > Preferences (Préférences) > Screen Resolution (Résolution d'écran)**. La boîte de dialogue des préférences de résolution d'écran s'affiche.
 - b. Choisissez une **résolution** et un taux de rafraîchissement (**Refresh Rate**) pris en charge par Dominion KX II.

Remarque : dans de nombreux environnements graphiques Linux, la commande <CTRL> <ALT> <+> modifie la résolution vidéo en parcourant toutes les résolutions disponibles qui restent activées dans le fichier XF86Config.

Pour configurer les serveurs cible exécutant Linux (ligne de commande) :

1. Définissez l'accélération du pointeur de la souris et le seuil exactement sur 1. Entrez cette commande : **xset mouse 1 1**. Ce paramètre doit est réglé pour être exécuté lorsque vous vous connectez.
2. Assurez-vous que tous les serveurs cible exécutant Linux utilisent une résolution VESA standard et un taux de rafraîchissement pris en charge par Dominion KX II.
3. Les serveurs cible Linux doivent également être configurés de manière à ce que les temps de passage en blanc correspondent aux valeurs VESA standard +/- 40 % :
 - Localisez le fichier de configuration Xfree86 (XF86Config).
 - Désactivez toutes les résolutions qui ne sont pas prises en charge par Dominion KX II à l'aide d'un éditeur de texte.
 - Désactivez la fonction de bureau virtuel (elle n'est pas prise en charge par Dominion KX II).
 - Vérifiez les temps de passage en blanc (valeurs VESA standard +/- 40 %).
 - Redémarrez l'ordinateur.

Remarque concernant les serveurs cible Red Hat 9

Si vous exécutez Red Hat 9 sur le serveur cible à l'aide de D2CIM-VUSB, et que vous rencontrez des problèmes avec le clavier et/ou la souris, vous pouvez essayer un autre paramètre de configuration.

Conseil : il se peut qu'il faille procéder à ces étapes même après l'installation récente d'un SE.

Pour configurer les serveurs Red Hat 9 à l'aide de D2CIM-VUSB :

1. Localisez le fichier de configuration (généralement `/etc/modules.conf`) sur le système.
2. Avec l'éditeur de votre choix, assurez-vous que la ligne **alias usb-controller** du fichier `modules.conf` est comme suit :

```
alias usb-controller usb-uhci
```

Remarque : si une autre ligne fait apparaître `usb-uhci` dans le fichier `/etc/modules.conf`, elle doit être supprimée ou mise en commentaire.

3. Enregistrez le fichier.
4. Redémarrez le système pour que les modifications prennent effet.

Paramètres Sun Solaris

Pour configurer les serveurs cible exécutant Sun Solaris :

Définissez la valeur d'accélération du pointeur de la souris et le seuil exactement sur 1. Cela peut être effectué :

- à partir de l'interface utilisateur graphique :

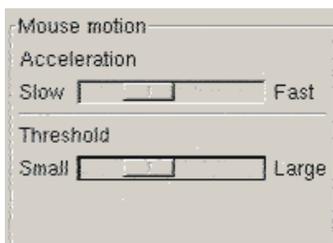


Figure 6 : Configuration de la souris Solaris

- avec la ligne de commande :

```
xset mouse a t
```

(où la lettre « a » représente l'accélération et la lettre « t » le seuil.)

Tous les serveurs cible doivent être configurés sur l'une des [résolutions vidéo](#) prises en charge par Dominion KX II. Les résolutions les plus courantes sur les ordinateurs Sun sont :

1024 x 768 à 60 Hz
1024 x 768 à 70 Hz
1024 x 768 à 75 Hz
1024 x 768 à 85 Hz
1152 x 900 à 66 Hz
1152 x 900 à 76 Hz
1280 x 1024 à 60 Hz

Les serveurs cible exécutant le système d'exploitation Solaris doivent utiliser une sortie vidéo VGA (signaux H-Sync et V-Sync, pas à synchronisation composite).

Pour passer d'une sortie de carte graphique Sun synchronisée de manière composite à une sortie VGA non standard :

1. lancez la commande **Stop+A** pour afficher le mode bootprom.
2. Lancez la commande suivante pour modifier la résolution de sortie :

```
setenv output-device screen :r1024x768x70
```

3. Lancez la commande « **boot** » pour redémarrer le serveur.

Vous pouvez également vous procurer un adaptateur de sortie vidéo auprès de votre représentant Raritan.

SI VOUS AVEZ	UTILISEZ L'ADAPTATEUR DE SORTIE VIDEO SUIVANT :
Sun 13W3 avec une sortie synchronisée de manière composite	Convertisseur APSSUN II Guardian
Sun HD15 avec une sortie synchronisée de manière composite	Convertisseur 1396C pour convertir de HD15 à 13W3 et un convertisseur APSSUN II Guardian pour supporter la synchronisation composite
Sun HD15 avec une sortie synchronisée de manière séparée	Convertisseur APKMSUN Guardian

Remarque : il se peut que certains écrans d'arrière-plan Sun, en particulier ceux ayant un bord sombre, ne se centrent pas de façon précise sur certains serveurs Sun. Utilisez un autre arrière-plan ou une icône de couleur claire dans le coin supérieur gauche.

Paramètres Apple Macintosh

Sur les serveurs cible exécutant des systèmes d'exploitation Apple Macintosh, la meilleure solution est d'utiliser la technologie D2CIM-VUSB et la synchronisation absolue de la souris.

*Remarque : si vous rencontrez des problèmes, cochez l'option **Absolute mouse scaling for MAC server (Mise à l'échelle absolue de la souris pour le serveur MAC)** de la page [Port](#).*

Paramètres IBM AIX

Pour configurer les serveurs cible exécutant IBM AIX :

Accédez au **Style Manager (Gestionnaire de style)**, cliquez sur **Mouse Settings (Paramètres de souris)** et réglez **Mouse acceleration (Accélération de la souris)** sur 1.0 et **Threshold (Seuil)** sur 3.0.

Etape 2 : Configuration des paramètres du pare-feu de réseau

Pour accéder à l'unité Dominion KX II par l'intermédiaire d'un pare-feu de réseau, votre pare-feu doit permettre la communication sur le port TCP 5000 ou tout autre port de votre choix. Reportez-vous à [Paramètres réseau](#) pour de plus amples informations sur la désignation d'un autre port de détection.

Paramètres du pare-feu

POUR BENEFICIER DU DOMINION KX II :	LE PARE-FEU DOIT PERMETTRE LA COMMUNICATION EN AMONT SUR :
Possibilités d'accès Web	Port 443 – port TCP standard pour la communication HTTPS
Redirection automatique des requêtes HTTP vers HTTPS (par ex., de manière à ce que les utilisateurs utilisent « http ://xxx.xxx.xxx.xxx », plus courant, à la place de « https ://xxx.xxx.xxx.xxx »)	Port 80 – port TCP standard pour la communication HTTP

Etape 3 : Connexion de l'équipement

Branchez le Dominion KX II sur l'alimentation, le réseau, le PC local et les serveurs cible. Les numéros des sections décrivant la connexion sont repris dans le schéma ci-dessous.

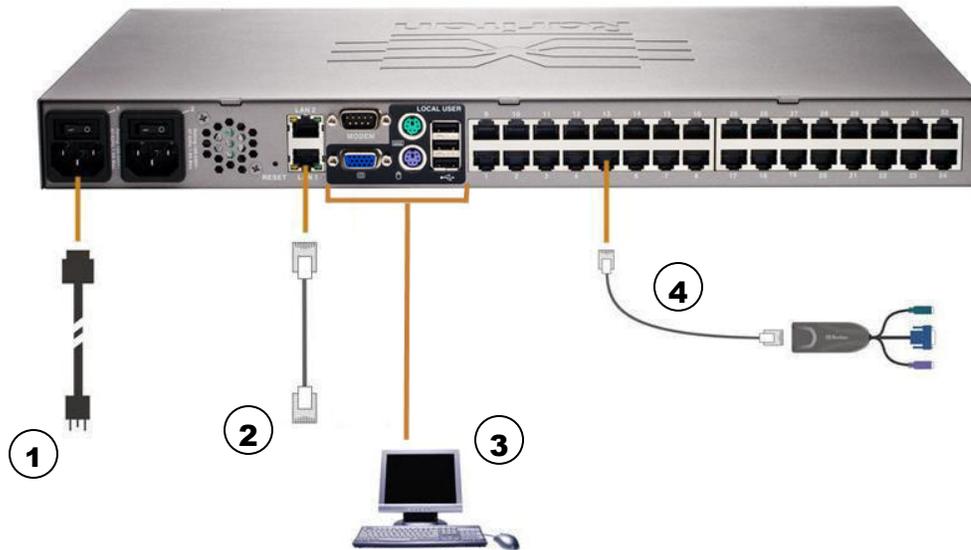


Figure 7 : Connexions de Dominion KX II

1. Alimentation CA

Pour connecter l'alimentation :

1. Raccordez le câble d'alimentation CA fourni à l'unité Dominion KX II et branchez-le à une prise CA.
2. Pour une alimentation à double protection par basculement, raccordez le second câble d'alimentation fourni et branchez-le à une **source d'alimentation différente** de celle auquel le premier câble d'alimentation est raccordé.

***Remarque :** Si vous ne connectez qu'un cordon d'alimentation, le voyant d'alimentation sur le panneau frontal de Dominion KX II est rouge car le système n'est pas configuré pour détecter les deux sources automatiquement. Reportez-vous à [Page de configuration de l'alimentation](#) pour obtenir des informations sur la désactivation de la fonction de détection automatique de la source d'alimentation non utilisée.*

2. Ports réseau

Dominion KX II dispose de deux ports Ethernet pour les basculements (et non pour l'équilibrage des charges). Par défaut, le port actif est le port LAN1 et le basculement automatique est désactivé. Lorsqu'il est activé, si l'interface réseau interne de Dominion KX II ou le commutateur réseau auquel Dominion KX est connecté n'est pas disponible, le port LAN2 est activé à l'aide de la *même* adresse IP.

Pour connecter le réseau :

1. Branchez un câble Ethernet standard (fourni) entre le port réseau LAN1 et un routeur, un concentrateur ou un commutateur Ethernet.
2. Si vous souhaitez utiliser les fonctions de basculement Ethernet de Dominion KX II en option :
 - Branchez un câble Ethernet standard entre le port réseau LAN2 et un routeur, un concentrateur ou un commutateur Ethernet.
 - **Activez le basculement automatique** sur l'écran Network Configuration (Configuration réseau) (reportez-vous à [Paramètres réseau](#), [Paramètres de l'interface LAN](#) pour obtenir davantage d'informations).

Utilisez les deux ports réseau uniquement si vous souhaitez utiliser l'un deux comme port de basculement.

3. Port pour accès local (PC local)

Si vous souhaitez accéder aux serveurs cible de manière pratique au niveau du rack, utilisez le port d'accès local de Dominion KX II. Si le port local est *requis* pour l'installation et la configuration, il est *facultatif* pour l'utilisation ultérieure. Le port local fournit l'interface utilisateur graphique de la console locale KX II pour l'administration et l'accès au serveur cible.

Pour connecter le port local :

Reliez un écran VGA Multisync, une souris et un clavier aux ports Local User (Utilisateur local) respectifs (à l'aide d'un clavier et d'une souris PS/2 ou USB).

4. Ports de serveur cible

Dominion KX II utilise des câbles UTP standard (Cat5/5e/6) pour la connexion aux serveurs cible. Pour plus d'informations, reportez-vous à [Annexe A: Caractéristiques](#).

Pour connecter un serveur cible à Dominion KX II :

1. Utilisez le module d'interface ordinateur (CIM) approprié. Reportez-vous à [CIM pris en charge](#) pour de plus amples informations sur les CIM à utiliser avec chaque système d'exploitation.
2. Reliez le connecteur vidéo HD15 de votre CIM au port vidéo de votre serveur cible. Assurez-vous que la transmission vidéo de votre serveur cible a déjà été définie sur une résolution et un taux de rafraîchissement pris en charge. Avec les serveurs Sun, assurez-vous également que la carte graphique de votre serveur cible a été définie de manière à produire des signaux VGA (H-Sync et V-Sync) standard et non à synchronisation composite.
3. Reliez le connecteur souris/clavier de votre CIM aux ports correspondants de votre serveur cible. Connectez le module d'interface pour ordinateur à un port de serveur disponible à l'arrière de votre unité Dominion KX II, à l'aide d'un câble UTP standard à brochage direct (Cat5/5e/6).

Modification du code de disposition de clavier (cibles Sun)

Exécutez cette procédure si vous utilisez un DCIM-SUSB et souhaitez modifier la disposition du clavier dans une autre langue.

Pour modifier le code de disposition du clavier (DCIM-SUSB uniquement) :

1. Ouvrez une fenêtre de l'éditeur de texte Text Editor sur le poste de travail Sun.
2. Assurez-vous que la touche **VERR NUM** est active, puis appuyez sur la touche **CTRL** située à gauche et sur la touche **DEL** du clavier. La **DEL Caps Lock** commence à clignoter pour indiquer que le CIM est en mode de modification du code de disposition. La fenêtre de texte affiche les informations suivantes : Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX) (Raritan Computer, Inc. Code de disposition de clavier actuel = 22 h (US5 UNIX).
3. Saisissez le code de disposition souhaité (par exemple, **31** pour le clavier japonais).
4. Appuyez sur **Entrée**.
5. Mettez l'unité hors tension, puis à nouveau sous tension. Le DCIM-SUSB procède à une réinitialisation (cycle de mise sous tension).
6. A l'aide de MPC, tapez quelque chose pour vérifier que les caractères sont corrects.

Etape 4 : Configuration initiale de Dominion KX II

La première fois que vous mettez l'unité Dominion KX II sous tension, vous devez effectuer plusieurs opérations de configuration initiales via la console locale KX II.

- Modification du mot de passe par défaut
- Affectation d'une adresse IP
- Désignation des serveurs cible
- Spécification de la détection automatique de l'alimentation

Modification du mot de passe par défaut

Dominion KX II est livré avec un mot de passe par défaut. *La première fois que vous démarrez Dominion KX II, il vous est demandé de changer ce mot de passe.*

Pour changer le mot de passe par défaut :

1. Mettez Dominion KX II sous tension à l'aide de l'interrupteur ou des interrupteurs d'alimentation situés sur la partie arrière de l'unité. Attendez que l'unité Dominion KX II démarre. (Un bip signale la fin du processus de démarrage.)
2. Une fois l'unité démarrée, la console locale de KX II est visible sur l'écran relié au port local de Dominion KX II. Entrez les nom d'utilisateur (**admin**) et mot de passe (**raritan**) par défaut puis cliquez sur **Login (Se connecter)**. L'écran de modification du mot de passe s'affiche.
3. Saisissez votre ancien mot de passe (**raritan**) dans le champ **Old Password (Ancien mot de passe)**.
4. Entrez un nouveau mot de passe dans le champ **New Password (Nouveau mot de passe)**, puis entrez-le à nouveau dans le champ **Confirm New Password (Confirmer le nouveau mot de passe)**. Les mots de passe peuvent contenir jusqu'à 64 caractères et être composés de caractères alphanumériques ainsi que des caractères spéciaux indiqués dans le tableau ci-après.
5. Cliquez sur **Appliquer**.
6. Un message doit s'afficher pour confirmer la réussite de la modification du mot de passe. Cliquez sur **OK**. La page d'accès aux ports apparaît.

*Remarque : le mot de passe par défaut peut également être modifié à partir de Multi-Platform Client (MPC) de Raritan. Pour en savoir plus, consultez le **manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC)**.*

Caractères spéciaux acceptés

CARACTERE	DESCRIPTION	CARACTERE	DESCRIPTION
!	Point d'exclamation	:	Double point
"	Guillemet	;	Point-virgule
#	Carré	=	Signe égal
\$	Symbole du dollar	>	Signe supérieur à
%	Symbole du pourcentage	?	Point d'interrogation
&	« Et » commercial	@	Arobas
'	Apostrophe	[Crochet ouvrant
(Parenthèse ouvrante	\	Trait oblique inversé
)	Parenthèse fermante]	Crochet fermant
*	Astérisque	^	Accent circonflexe
+	Signe plus	_	Trait de soulignement
,	Virgule	`	Accent grave
-	Tiret	{	Accolade gauche
.	Point		Barre
/	Trait oblique	}	Accolade droite
<	Signe inférieur à	~	Tilde

Affectation d'une adresse IP

Ces procédures indiquent comment affecter une adresse IP à l'aide de la page des paramètres réseau. Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à [Paramètres réseau](#).

1. A partir de la console locale KX II, sélectionnez **Device Settings (Paramètres du dispositif) > Network Settings (Paramètres réseau)**. La page des paramètres réseau s'ouvre.

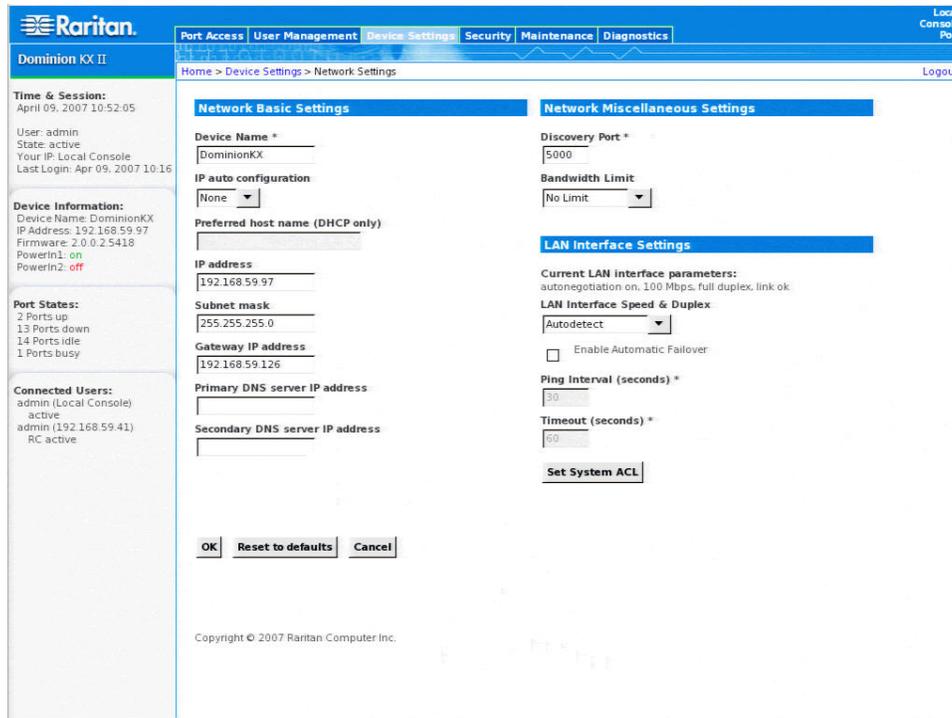


Figure 8 : Menu Network Settings (Paramètres réseau)

2. Spécifiez dans le champ **Device Name** un nom de dispositif évocateur pour votre unité Dominion KX II, pouvant comporter jusqu'à 16 caractères alphanumériques et [caractères spéciaux](#). N'utilisez pas d'espace.
3. Sélectionnez **IP auto configuration (Configuration IP automatique)** à partir de la liste déroulante :
 - **None (Aucune)** (IP statique). Cette option nécessite que vous indiquiez manuellement les paramètres réseau. Cette option est recommandée car Dominion KX II est un dispositif d'infrastructure et son adresse IP ne doit pas être modifiée.
 - **DHCP**. Avec cette option, les paramètres réseau sont attribués par le serveur DHCP.
4. Si vous définissez la configuration IP sur None (Aucune), entrez les paramètres TCP/IP de votre unité Dominion KX II : **IP address (Adresse IP)**, **Subnet mask (Masque de sous-réseau)**, **Gateway IP address (Adresse IP de la passerelle)**, **Primary DNS server IP address (Adresse IP du serveur DNS principal)** et **Secondary DNS server IP address (Adresse IP du serveur DNS secondaire)** (facultatif).
5. Lorsque l'opération est terminée, cliquez sur **OK**.

Il est désormais possible d'accéder à votre unité Dominion KX II depuis le réseau.

Remarque : dans certains environnements, le paramètre par défaut **LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN)** de la fonction **Autodetect (Détection automatique)** (négociation automatique) ne règle pas correctement les paramètres réseau, ce qui entraîne des problèmes réseau. Dans ces cas, le fait de définir le champ **LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN)** de Dominion KX II sur 100 Mbps/Full Duplex (ou toute option appropriée à votre réseau) résout le problème. Reportez-vous à la page [Paramètres réseau](#) pour de plus amples informations.

Désignation des serveurs cible

Pour désigner les serveurs cible :

1. Si vous ne l'avez pas déjà fait, connectez tous les serveurs cible (tel que décrit dans la section [Étape 3 : Connexion de l'équipement, Ports de serveur cible](#)).
2. A l'aide de la console locale KX II, sélectionnez **Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports)**. La page de configuration des ports s'ouvre :

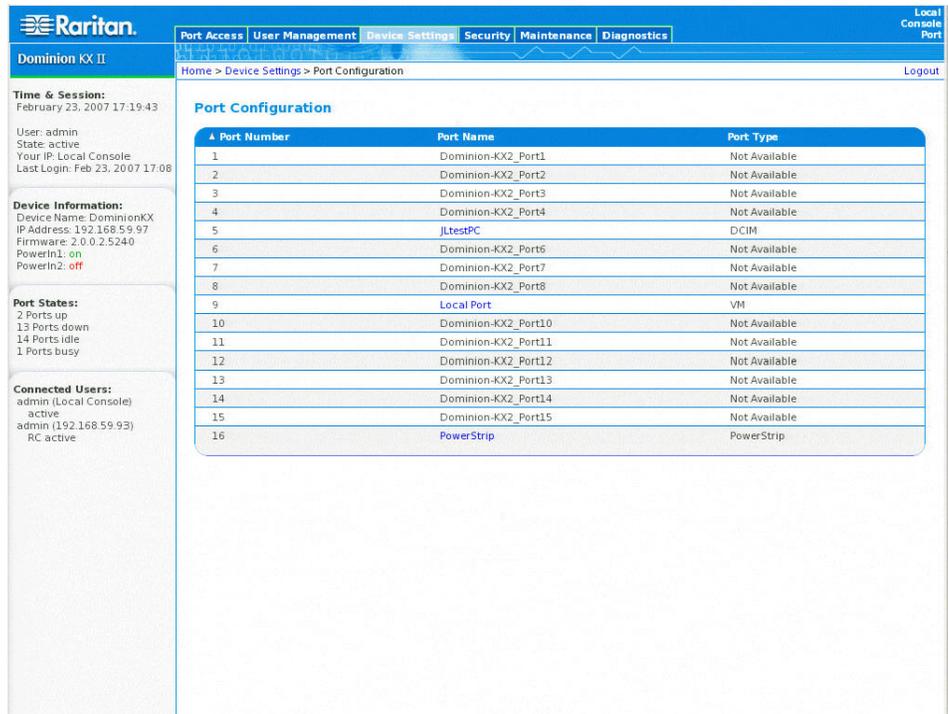


Figure 9 : Configuration des ports

3. Cliquez sur l'option **Port Name (Nom du port)** associée au serveur cible que vous souhaitez renommer. La [Page des ports](#) s'ouvre.
4. Attribuez un nom pour identifier le serveur connecté à ce port. Le nom peut contenir jusqu'à 32 caractères alphanumériques et [caractères spéciaux](#).
5. Cliquez sur **OK**.

Spécification de la détection automatique de l'alimentation

Le Dominion KX II offre une double alimentation. Par ailleurs, il peut détecter et notifier automatiquement l'état de ces alimentations. Une configuration appropriée garantit l'envoi de notifications adéquates par Dominion KX II, en cas de panne de courant. La page de configuration de l'alimentation est définie pour détecter automatiquement les deux alimentations. Utilisez cette page pour désactiver la détection automatique de l'alimentation électrique non utilisée.

Pour désactiver la détection automatique de l'alimentation électrique non utilisée :

1. A l'aide de la console locale KX II, sélectionnez **Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation électrique)**. La page de configuration de l'alimentation électrique s'ouvre.
2. Désélectionnez la case associée à la détection automatique de l'alimentation que vous *n'utilisez pas*.

Pour de plus amples informations, consultez la [Page de configuration de l'alimentation](#).

Note aux utilisateurs de CC-SG

Si vous utilisez Dominion KX II dans une configuration CC-SG, suivez les étapes d'installation décrites ci-dessus, et une fois l'installation terminée, consultez le *manuel d'utilisation CommandCenter Secure Gateway*, le *manuel d'administration* ou le *guide de déploiement* pour continuer (tous ces documents se trouvent sur le site Web de Raritan dans la section Assistance : <http://www.raritan.com/support/productdocumentation>).

Remarque : *La suite de ce manuel d'utilisation s'applique essentiellement au déploiement de/des l'unité/unités Dominion KX II sans utiliser les fonctions d'intégration de CC-SG.*

Authentification à distance

Note aux utilisateurs de CC-SG

Si Dominion KX II est contrôlé par CommandCenter Secure Gateway, CC-SG authentifie les utilisateurs et les groupes, à l'exception des utilisateurs locaux (qui nécessitent l'accès au port local). L'authentification des utilisateurs locaux est telle que configurée pour Dominion KX II.

Pour de plus amples informations sur l'authentification CC-SG, consultez le *manuel d'utilisation CommandCenter Secure Gateway*, le *guide d'administration* ou le *guide de déploiement* sur le site de Raritan : <http://www.raritan.com/support/productdocumentation>.

Protocoles pris en charge

Afin de simplifier la gestion des noms des utilisateurs et des mots de passe, Dominion KX II permet de transférer les requêtes d'authentification vers un serveur d'authentification externe. Deux protocoles d'authentification externes sont pris en charge : LDAP et RADIUS.

Remarque relative à Microsoft Active Directory

Microsoft Active Directory utilise le protocole LDAP de manière native et peut être utilisé comme source d'authentification et serveur LDAP avec Dominion KX II. Si le serveur Microsoft Active Directory dispose d'un composant IAS (serveur d'autorisation Internet), il peut également être utilisé comme source d'authentification RADIUS.

Authentification et autorisation

L'authentification est un processus qui consiste à vérifier qu'un utilisateur est bien celui ou celle qu'il dit être. Une fois l'utilisateur authentifié, le groupe de l'utilisateur est utilisé pour déterminer ses autorisations de port et de système. Les droits accordés à l'utilisateur déterminent le type d'accès autorisé. Cela s'appelle l'autorisation.

Si Dominion KX II est configuré de manière à permettre l'authentification à distance, le serveur d'authentification externe est essentiellement utilisé dans un but d'authentification et non d'autorisation.

L'organigramme illustre ce procédé :

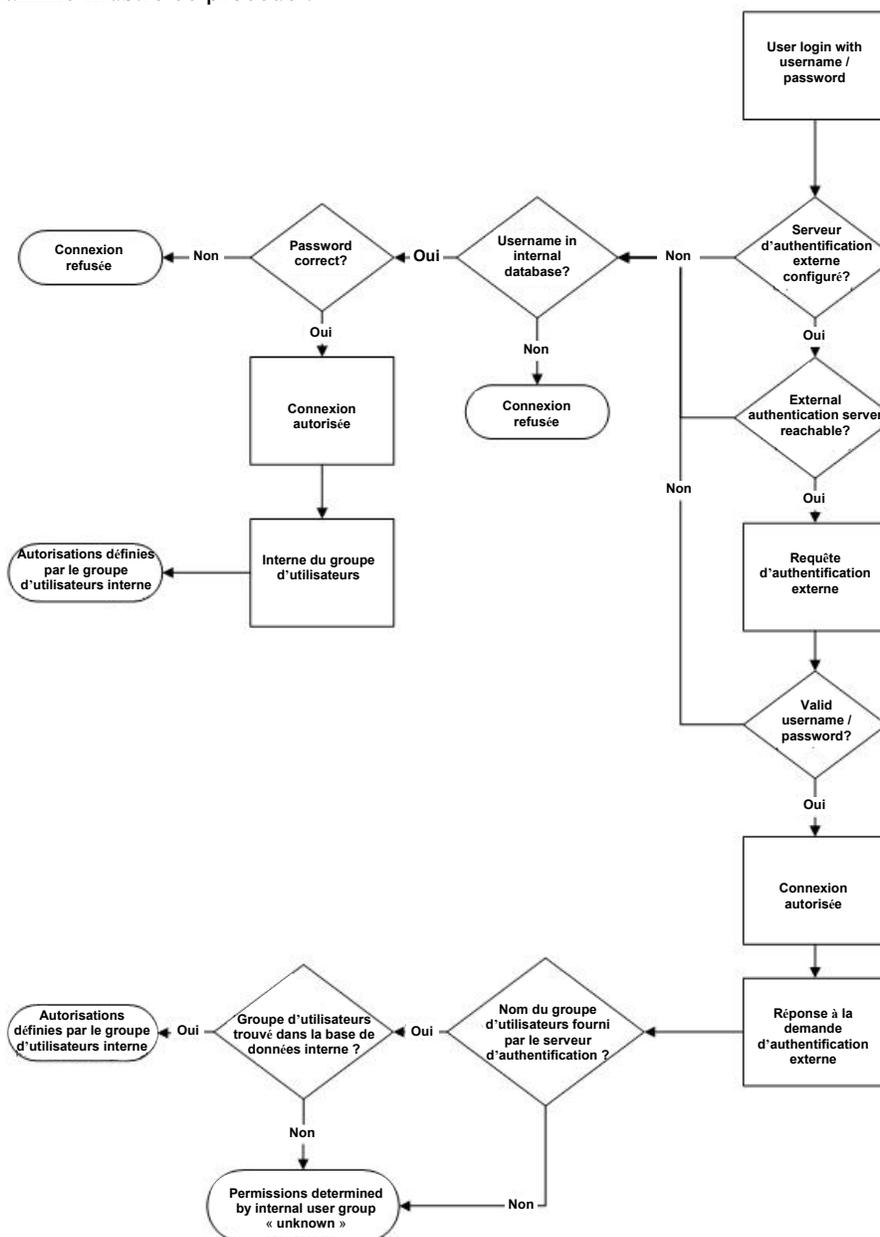


Figure 10 : Organigramme relatif aux authentications/autorisations

Notez l'importance du groupe auquel appartient un utilisateur donné ainsi que la nécessité de configurer le groupe appelé « Unknown » (Inconnu). Si le serveur d'authentification externe renvoie un nom de groupe qui n'est pas reconnu par Dominion KX II, les autorisations de l'utilisateur sont déterminées par le groupe permanent appelé « Unknown » (Inconnu).

Reportez-vous à [Mise en application de l'authentification LDAP](#) et [Mise en application de l'authentification RADIUS](#) pour savoir comment configurer votre serveur d'authentification de manière à ce qu'il renvoie les informations relatives au groupe d'utilisateurs à Dominion KX II dans le cadre de sa réponse à une demande d'authentification.

Utilisateurs, groupes et autorisations d'accès

Présentation

Dominion KX II conserve une liste interne de tous les noms des utilisateurs et des groupes pour déterminer l'autorisation d'accès et les autorisations. Ces informations sont stockées de manière interne à l'aide d'un format crypté. Il existe plusieurs formes d'authentification et celle-ci est connue sous le nom « d'authentification locale ». Tous les utilisateurs doivent être authentifiés, si Dominion KX II est configuré pour LDAP ou RADIUS, cette authentification est traitée en premier puis suivie par l'authentification locale.

Utilisateurs

Un nom d'utilisateur et un mot de passe sont nécessaires pour accéder à l'unité Dominion KX II. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité KX II. Reportez-vous à [Gestion des utilisateurs](#) pour obtenir davantage d'informations sur les processus d'ajout et de modification des utilisateurs.

Groupes

Chaque unité Dominion KX II est livrée avec trois groupes d'utilisateurs par défaut, ces-derniers ne pouvant pas être supprimés :

Admin	Les utilisateurs qui sont membres de ce groupe jouissent de la totalité des droits d'administrateur. L'utilisateur d'origine par défaut est membre de ce groupe et dispose de la totalité des droits de système.
Inconnu	Il s'agit du groupe par défaut des utilisateurs authentifiés de manière externe à l'aide de LDAP ou RADIUS. Si le serveur externe LDAP ou RADIUS ne peut identifier un groupe d'utilisateurs valide, le groupe Inconnu est alors utilisé.
Individuel individuel	Un groupe individuel est essentiellement un « groupe » de un individu. A savoir, l'utilisateur spécifique est dans son propre groupe et non affilié à d'autres groupes <i>réels</i> . Les groupes individuels peuvent être identifiés par le signe « @ » présent dans le Nom de groupe.

Outre les groupes par défaut fournis par le système, vous pouvez aussi créer des groupes et spécifier les autorisations adéquates pour répondre à vos besoins. Reportez-vous à [Gestion des utilisateurs](#) pour obtenir davantage d'informations sur les processus de création et de modification des groupes d'utilisateurs.

Relation entre les utilisateurs et les groupes

Les utilisateurs appartiennent à un groupe et les groupes possèdent des droits. La répartition en groupes des utilisateurs de votre Dominion KX II offre un gain de temps en vous permettant de gérer les autorisations de l'ensemble des utilisateurs d'un groupe donné en une seule fois au lieu de les gérer individuellement.

Vous pouvez également choisir de *ne pas* associer certains utilisateurs à des groupes. Vous avez alors la possibilité de classer l'utilisateur comme « Individuel ».

Si l'authentification se déroule correctement, le dispositif utilise les **Group** information (informations relatives au groupe) pour déterminer les autorisations de l'utilisateur (ports de serveur accessibles, si le redémarrage de l'unité est autorisé, entre autres fonctions).

Chapitre 4 : Se connecter à Dominion KX II

Interfaces utilisateur

Dominion KX II propose plusieurs interfaces utilisateur qui vous garantissent un accès aisé à tout moment, où que vous soyez. Ces interfaces incluent la Console locale KX II, la Console distante KX II et le Client MPC (Multi-Platform Client). Le tableau suivant identifie les interfaces en fonction de leur utilisation locale et à distance liée à l'accès au serveur cible et aux fonctions d'administration :

INTERFACE UTILISATEUR	LOCAL		ACCES	
	ACCES	ADMIN	ACCES	ADMIN
Console locale KX II	✓	✓		
Console distante KX II			✓	✓
Virtual KVM Client (Client virtuel KVM)			✓	
Client MPC (Multi-Platform Client)			✓	✓

Console locale KX II – Dispositifs KX II

Lorsque vous êtes situé au niveau du rack du serveur, Dominion KX II propose une fonctionnalité de commutation et d'administration KVM standard par l'intermédiaire de la console locale KX II. La console locale KX II fournit une connexion (analogique) KVM directe aux serveurs connectés. Les performances sont les mêmes que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Il existe de nombreuses similarités entre l'interface utilisateur graphiques de la console locale KX II et celle de la console distante KX II ; et lorsqu'il y a des différences, elles sont spécifiées dans le manuel d'utilisation. Les interfaces utilisateur des consoles locale et distante KX II sont presque identiques ; les options suivantes sont disponibles dans la console locale KX II, mais *pas* dans la console distante KX II :

- [Local Port Settings \(Paramètres du port local\)](#)
- [Factory Reset \(Restauration des valeurs d'usine\)](#)

Console distante KX II – Dispositifs KX II

La console distante KX II est une interface utilisateur graphique basée sur un navigateur qui vous permet d'accéder aux serveurs cible connectés à Dominion KX II et d'administrer à distance KX II.

Elle offre une connexion numérique à vos serveurs cible connectés. Chaque fois que vous accédez à un serveur cible à l'aide de la console distante KX II, une fenêtre du client virtuel KVM s'ouvre. Un client KVM virtuel s'ouvre pour chacun des serveurs cible, permettant ainsi l'accès simultané lorsque pris en charge par l'unité KX II spécifique (par exemple, KX2-116 prend en charge une session à distance uniquement).

Il existe de nombreuses similarités entre l'interface utilisateur graphiques de la console locale KX II et celle de la console distante KX II ; et lorsqu'il y a des différences, elles sont spécifiées dans le manuel d'utilisation. Les options suivantes sont disponibles dans la console distante KX II mais *pas* dans la console locale KX II :

- [Média virtuels](#)
- [Gestion des favoris](#)
- [Sauvegarde/Restauration](#)
- [Mise à niveau du firmware](#)
- [Rapport de mise à niveau](#)
- [Diagnostics KX](#)

Client MPC (Multi-Platform Client) – Dispositifs KX I et KX II

Le Multi-Platform Client (MPC) de Raritan est une interface graphique qui vous permet d'accéder à distance aux dispositifs cible connectés aux unités Dominion. Vous pouvez configurer le client MPC pour une utilisation autonome ou pour être accessible par l'intermédiaire d'un navigateur Web.

Une fois Dominion KX II installé, vous pouvez soit télécharger une version autonome de MPC de Raritan et établir une connexion réseau initiale, soit lancer l'application directement.

Remarque : le client MPC prend en charge à la fois les dispositifs KX I et KX II ; utilisez le MPC si vous souhaitez accéder à des serveurs connectés aux deux dispositifs avec une interface utilisateur.

Pour lancer le client MPC directement :

1. Pour lancer MPC à partir d'un client exécutant tout type de navigateur, saisissez **http ://ADRESSE-IP/mpc** dans la ligne d'adresse, où **ADRESSE-IP** correspond à l'adresse IP de votre dispositif Raritan. MPC est lancé dans une nouvelle fenêtre qui ne contient **pas** de barre de menus, de barre d'outils, de barre de défilement ou de barre d'adresses. Travaillez dans cette fenêtre et basculez sur d'autres fenêtres ouvertes à l'aide de la commande **ALT + TAB**.
2. Une fois MPC lancé, une arborescence de tous les dispositifs Raritan automatiquement détectés sur votre sous-réseau s'affiche du côté gauche de l'écran. Si vous ne parvenez pas à localiser le nom de votre unité Dominion KX II, créez manuellement une icône en sélectionnant **Connection (Connexion) > New Profile (Nouveau profil)**. La fenêtre Add Connection (Ajouter une connexion) s'affiche alors.
3. Entrez la description d'un dispositif, indiquez un type de connexion, ajoutez l'adresse IP de l'unité Dominion, puis cliquez sur **OK**. Vous pouvez modifier ces spécifications ultérieurement.
4. Dans le panneau du navigateur situé à gauche de l'écran, double-cliquez sur l'icône qui correspond à votre unité Dominion KX II.

Pour obtenir des informations complémentaires sur l'installation et le fonctionnement de MPC, reportez-vous au *manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC)*, disponible sur le site Web de Raritan, [http ://www.raritan.com/support/productdocumentation](http://www.raritan.com/support/productdocumentation) ou sur le CD-ROM des manuels d'utilisation de Raritan et de configuration rapide livré avec votre produit Dominion.

Raritan Remote Client (RRC) – Dispositifs KX I uniquement

Raritan Remote Client (RRC) est une interface utilisateur graphique qui fournit un accès distant aux dispositifs cible.

Remarque : RRC ne peut pas être utilisé avec Dominion KX II ; utilisez MPC à la place.

Langues étrangères prises en charge

Dominion KX II fournit un support clavier pour les langues suivantes : anglais (Etats-Unis), anglais (Royaume-Uni), chinois traditionnel, chinois simplifié, japonais, coréen, français et allemand.

Remarques sur les langues étrangères prises en charge

- Vous pouvez utiliser le clavier pour le chinois, le japonais et le coréen à des fins d'affichage uniquement ; l'entrée de données dans la langue locale n'est pas prise en charge pour le moment en ce qui concerne les fonctions de la console locale KX II.
- En raison d'une limitation de Java® Runtime Environment (JRE), les clients Fedora, Linux et Solaris reçoivent une réponse non-valide lorsque la touche **Alt Gr** est utilisée sur des claviers paramétrés sur la langue Anglais (Royaume-Uni). Fedora, Linux et Solaris ne renvoient pas de réponse lorsqu'une combinaison incluant la touche **Alt Gr** est utilisée avec Java 1.4.2 ou 1.5. Java 1.6 semble apporter des améliorations, cependant les événements associés à *keyPressed* et *keyReleased* renvoient toujours la réponse « code touche inconnu » lorsque la touche **Alt Gr** est utilisée.

Par ailleurs, une touche utilisée en combinaison avec **Alt Gr** (comme par exemple **Alt Gr-4**, qui, sur un clavier du Royaume-Uni, permet de saisir le symbole euro), va seulement générer un événement *keyTyped* suivi d'un événement *keyReleased* pour cette valeur, sans événement *keyPressed*. Java 1.6 apporte une amélioration à ce problème, l'événement *keyPressed* n'est plus vide.

Java Runtime Environment (JRE)

Important : il est recommandé de désactiver la mise en mémoire cache de Java et d'effacer le cache de Java. Pour de plus amples informations, veuillez consulter votre documentation Java ou le *manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC)*.

La console distante Dominion KX II et le client MPC requièrent l'environnement JRE pour fonctionner. La console distante Dominion KX II vérifie la version de Java ; si elle est incorrecte ou périmée, vous êtes alors invité à télécharger une version compatible.

Raritan vous recommande d'utiliser la version 1.5 du programme Java Runtime Environment (JRE) pour garantir des performances optimales. La console distante Dominion KX II et MPC fonctionnent cependant avec la version **1.4.2_05** du programme JRE ou une version supérieure (à l'exception de la version 1.5.0_02). JRE 1.6 est également pris en charge, mais n'a pas été entièrement testé.

Remarque : pour que les claviers multilingues puissent fonctionner dans la console distante KX II (Virtual KVM Client), veuillez installer la version multilingue de Java Runtime Environment (JRE).

Lancement de KX II

Important : quel que soit le navigateur utilisé, vous devez autoriser les fenêtres contextuelles provenant de l'adresse IP du dispositif Dominion pour lancer la console distante KX II.

Remarque : selon le navigateur utilisé et les paramètres de sécurité du navigateur, il est possible que plusieurs avertissements relatifs aux certificats et à la sécurité s'affichent. Il vous faudra accepter ces avertissements pour lancer la console distante KX II.

Vous avez la possibilité de réduire le nombre de messages d'avertissement lors des connexions suivantes en cochant les options suivantes dans les messages d'avertissement relatifs aux certificats et à la sécurité en question :

- In the future, do not show this warning (A l'avenir, ne plus afficher ce message d'avertissement)*
- Always trust content from this publisher (Toujours faire confiance au contenu provenant de cet éditeur)*

Pour lancer la console distante KX II :

1. Connectez-vous à l'un des postes de travail équipés d'une connectivité réseau à votre unité Dominion KX II et de Java Runtime Environment version 1.4.2_2 ou ultérieure (Java Runtime Environment est disponible à l'adresse <http://java.sun.com/>).
2. Lancez un [navigateur Web pris en charge](#) tel que Internet Explorer (IE) ou Firefox.
3. Tapez l'URL suivant : **http ://ADRESSE-IP**, où **ADRESSE-IP** correspond à l'adresse IP que vous avez affectée à l'unité Dominion KX II. Vous pouvez aussi utiliser https, le nom DNS de Dominion KX II attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou simplement taper l'adresse IP dans le navigateur (KX II redirige toujours l'adresse IP de HTTP à HTTPS). La page de connexion s'ouvre :

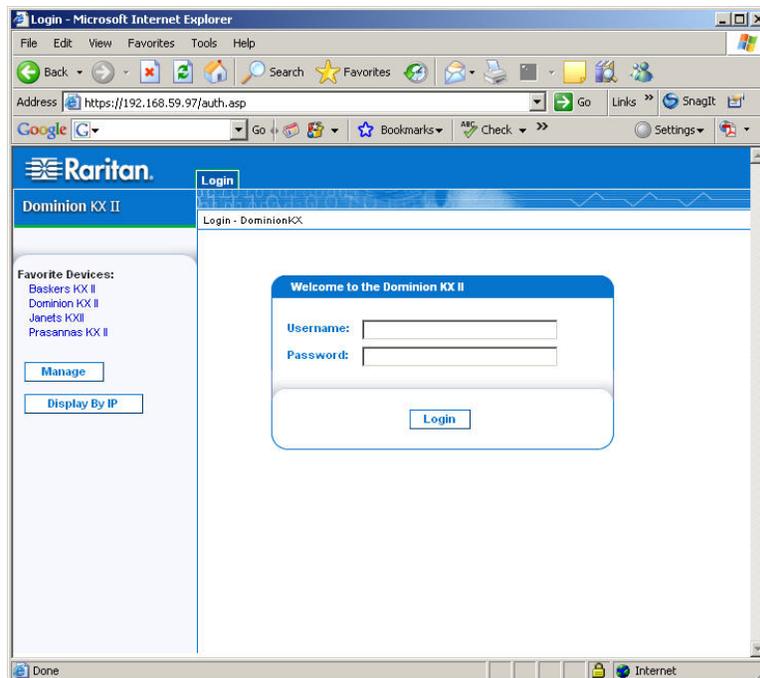


Figure 11 : Page de connexion de la console distante de Dominion KX II

4. Saisissez vos **Username (Nom d'utilisateur)** et **Password (Mot de passe)**. Si c'est la première fois que vous vous connectez, utilisez le nom d'utilisateur et le mot de passe par défaut [**admin** et **Raritan** (tout en minuscules)] ; vous serez ensuite invité à modifier le mot de passe par défaut. Reportez-vous à [Modification du mot de passe par défaut](#) pour obtenir plus d'informations.
5. Cliquez sur Login (Connexion).

Disposition de la console KX II

Les interfaces de la console distante KX II et celle de la console locale KX II fournissent toutes les deux une interface HTML (de type Web) pour la configuration et l'administration, ainsi qu'une liste et des fonctions de sélection relatives aux serveurs cible. Les options sont regroupées sous plusieurs onglets différents.

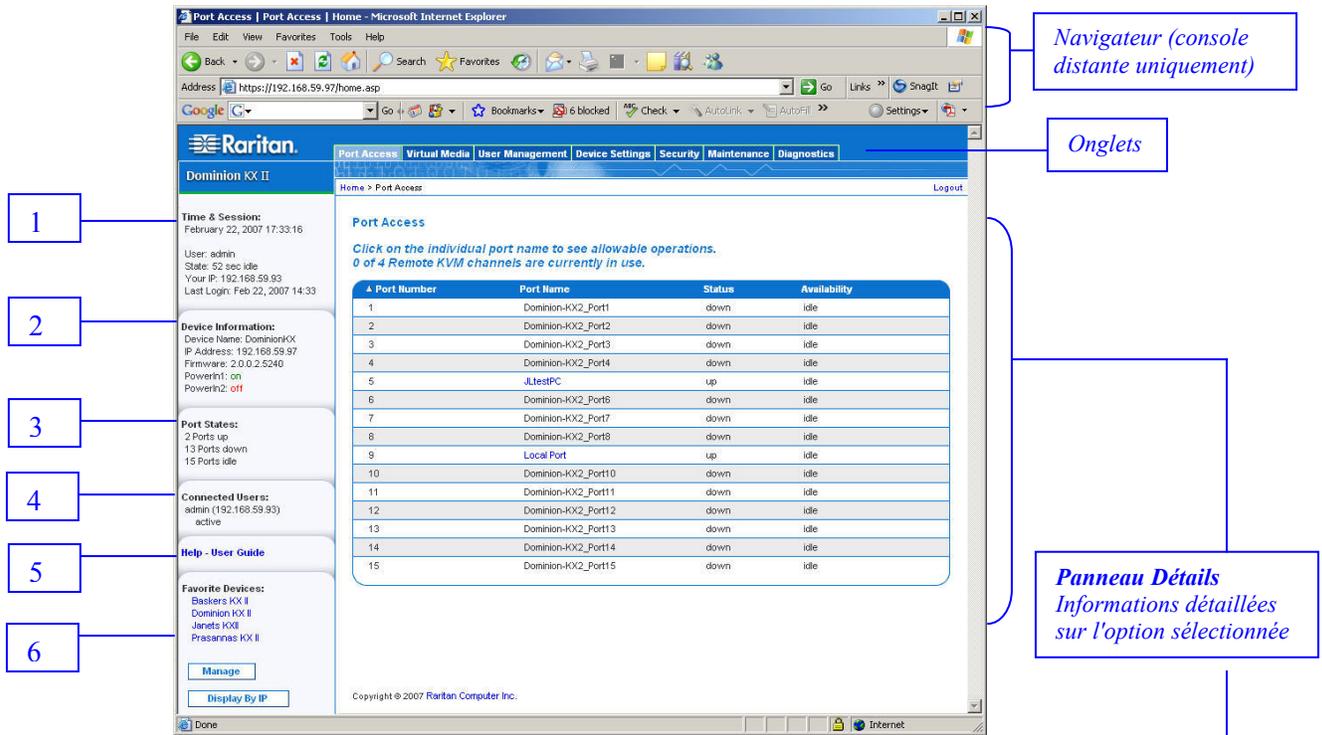


Figure 12 : Page principale de la console distante KX II

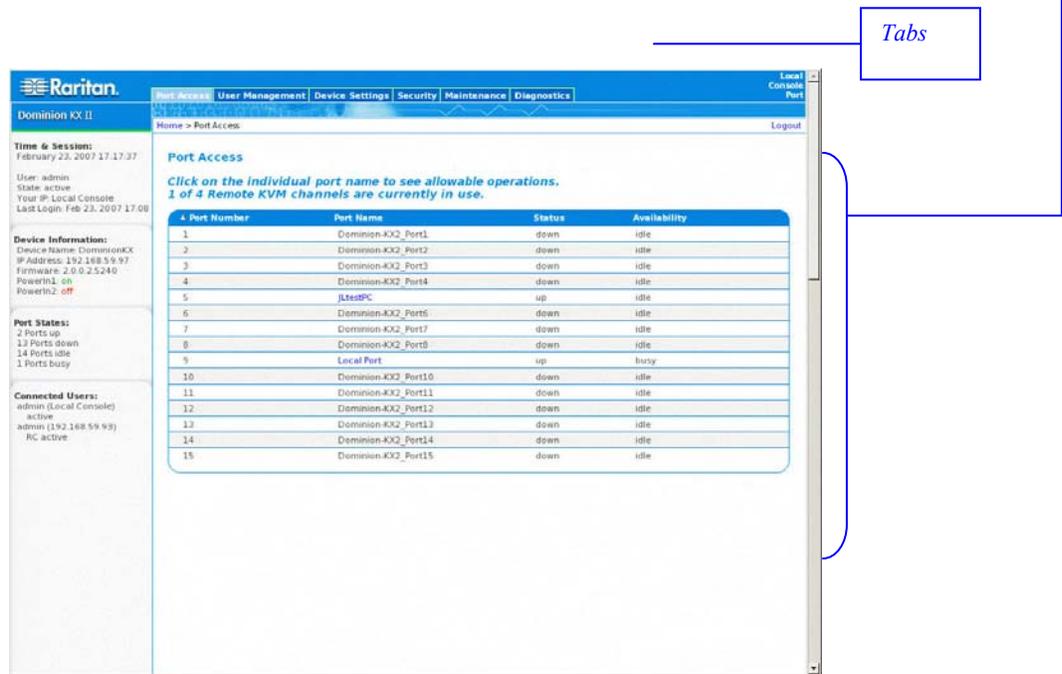


Figure 13 : Page principale de la console locale KX II

Une fois la connexion réussie, la page d'accès aux ports s'affiche avec la liste de tous les ports ainsi que leur état et leur disponibilité. Vous pouvez les trier selon leur numéro de port, leur nom de port, leur état (connecté ou non) et leur disponibilité (ralenti, occupé, indisponible ou en cours de connexion) en cliquant sur l'en-tête de colonne.

Les numéros du tableau suivant correspondent aux numéros indiqués dans la Figure 12.

#	TITRE	DESCRIPTION
1	Temps & session	Date, heure, nom d'utilisateur, état actuel, adresse IP du client et dernière connexion
2	Informations relatives au dispositif	Nom du dispositif, adresse IP, version du firmware et état des deux lignes d'alimentation électrique
3	États des ports	Etat actuel de tous les ports de Dominion KX II
4	Utilisateurs connectés	Liste de tous les utilisateurs actuellement connectés à votre Dominion KX II
5	Aide - Manuel d'utilisation	Accès à ce manuel d'utilisation (Console distante KX II uniquement).
6	Dispositifs favoris	Accès et gestion de la liste de vos favoris (console distante KX II uniquement)

Navigation dans la console KX II

Les interfaces des consoles Dominion KX II (locale et distante) proposent plusieurs méthodes de navigation et de choix de sélection.

Pour sélectionner une option (utilisez n'importe laquelle des méthodes suivantes) :

- Cliquez sur un onglet ; la page des options disponibles s'ouvre.
- Placez le curseur sur un onglet puis sélectionnez l'option appropriée à partir du menu.
- Cliquez sur l'option directement à partir de la hiérarchie de menu affichée (chemins de navigation).

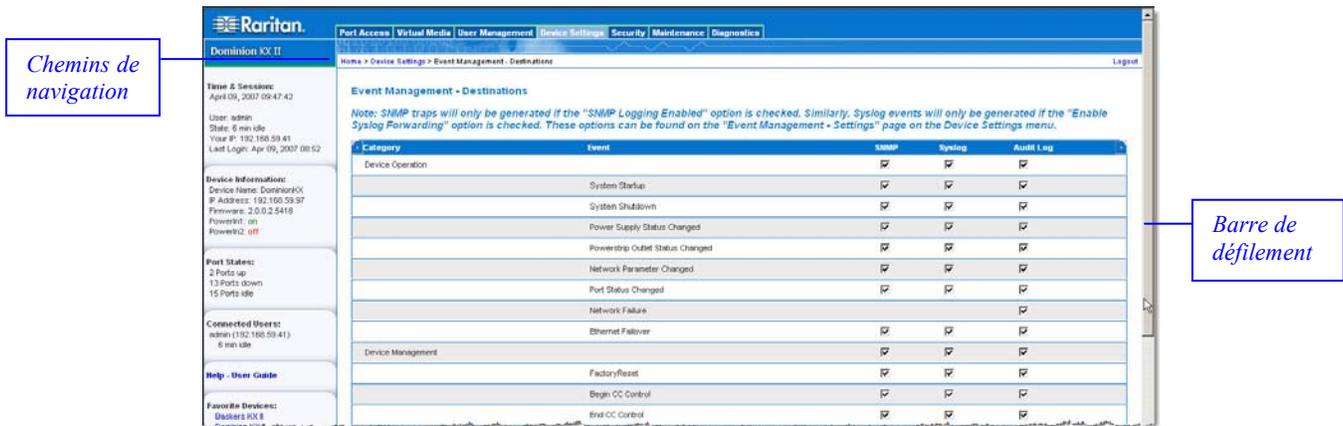


Figure 14 : Exemple de hiérarchie de menu (chemins de navigation)

Pour faire défiler les pages lorsque l'écran ne suffit pas pour les afficher entièrement :

- Utilisez les touches **Page Up (PageSup)** et **Page Down (PageInf)** sur votre clavier ou
- utilisez la barre de défilement située à droite de l'écran.

Pour obtenir de plus amples informations concernant la navigation et la sélection dans le Client MPC (Multi-Platform Client) de Raritan, consultez le *manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC)*.

Se déconnecter

Pour quitter la console Dominion KX II :

Cliquez sur la mention **Logout (Se déconnecter)** située dans le coin supérieur droit de la page.

Remarque : la déconnexion ferme également toute session ouverte du client virtuel KVM.

Arborescence de menu de la console KX II

Le tableau suivant comporte l'ensemble des options de menu disponibles dans les deux interfaces de console KX II (locale et distante). Les différences entre la console locale KX II et la console distante KX II sont identifiées ci-après.

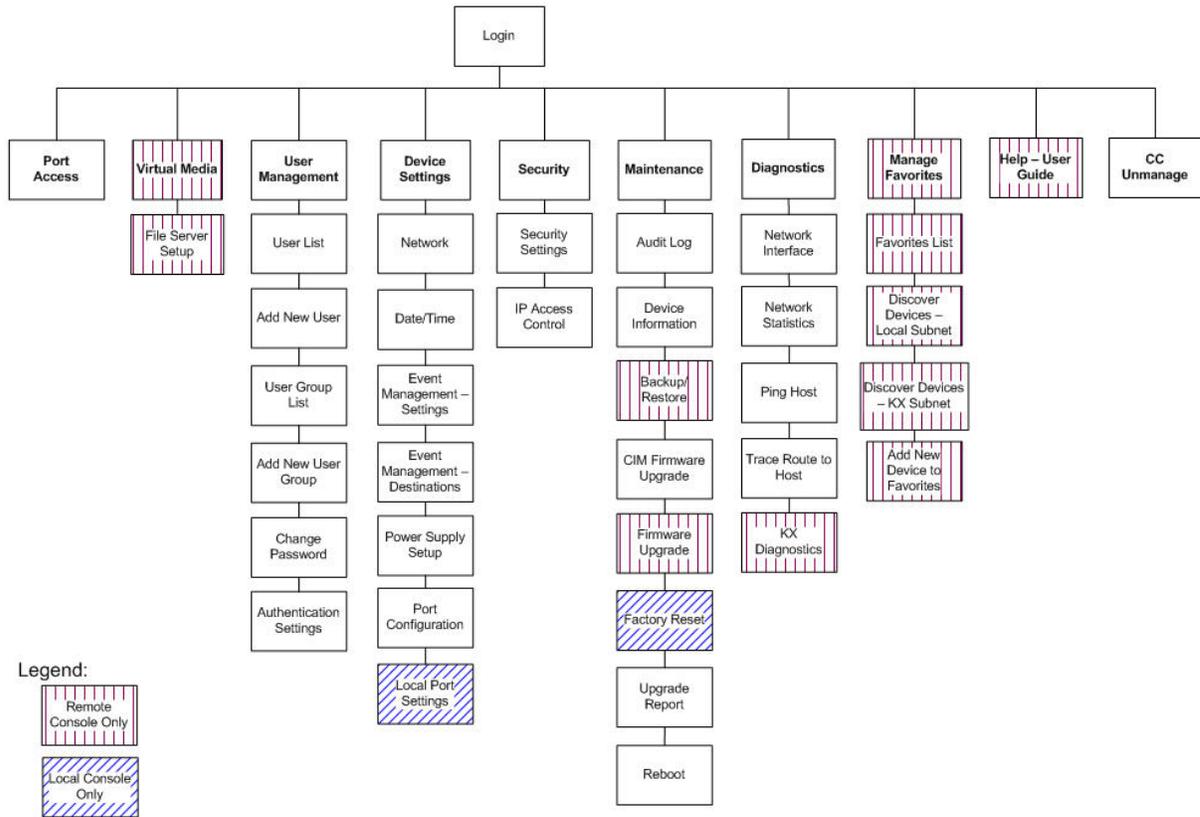


Figure 15 : Arborescence de menu des consoles KX II (locale et distante)

Outre leur identification dans l'arborescence de menu ci-dessus, les différences entre les options de menu de la console locale KX II et celles de la console distante KX II sont identifiées dans le tableau suivant :

OPTION	CONSOLE LOCALE	CONSOLE DISTANTE
Médias virtuels		✓
Configuration des serveurs de fichiers		✓
Sauvegarde/Restauration		✓
Mise à niveau du firmware		✓
KX Diagnostics (Diagnostics KX)		✓
Gestion des favoris		✓
Liste des favoris		✓
Détection des dispositifs – Sous-réseau local		✓
Détection des dispositifs – Sous-réseau KX		✓
Ajouter un nouveau dispositif dans les favoris		✓
Aide - Manuel d'utilisation		✓
Local Port Settings (Paramètres du port local)	✓	
Factory Reset (Restauration des valeurs d'usine)	✓	

Gestion des favoris

Une fonction de gestion des favoris est offerte de façon à ce que vous puissiez organiser et accéder rapidement aux dispositifs que vous utilisez fréquemment. La section des dispositifs favoris se trouve dans la partie inférieure gauche (cadre) de la page d'accès aux ports et permet les opérations suivantes :

- créer et gérer une liste de dispositifs favoris
- accéder rapidement aux dispositifs fréquemment utilisés
- répertorier vos favoris soit par nom, soit par adresse IP
- détecter les dispositifs Dominion KX II en fonction de leur sous-réseau (avant et après la connexion)
- récupérer les dispositifs Dominion KX II détectés à partir du dispositif KX (après la connexion)

Remarque : cette option est disponible uniquement sur la console distante Dominion KX II (et non sur la console locale Dominion KX II).

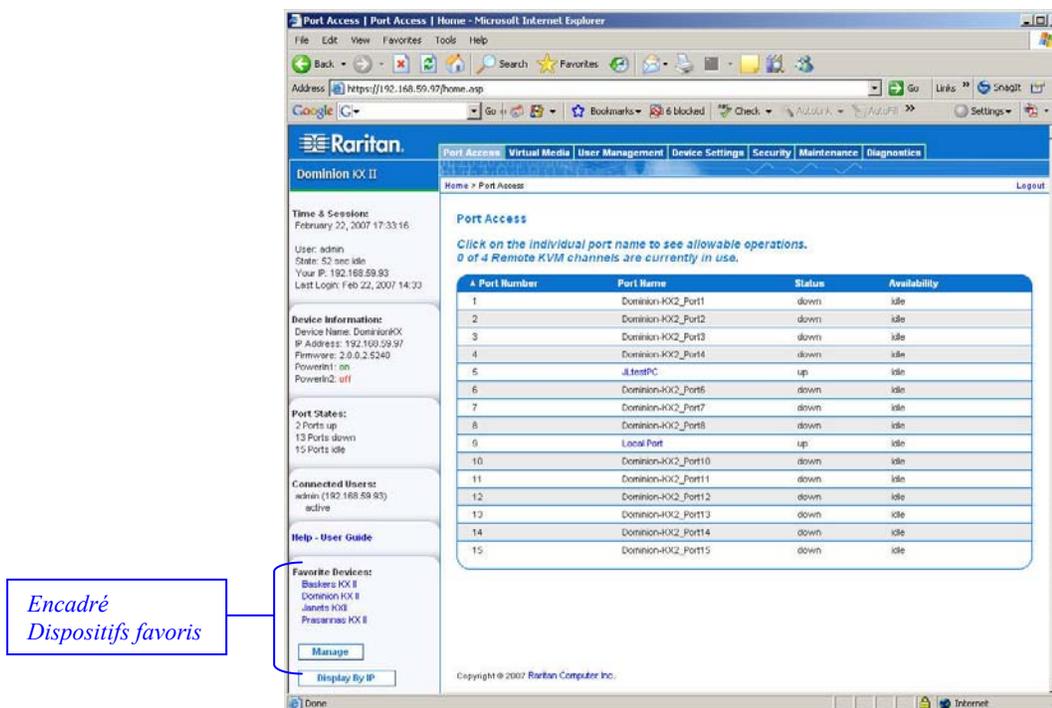


Figure 16 : Dispositifs favoris (encadré)

Pour accéder à un dispositif KX II placé dans les favoris :

Cliquez sur le nom du dispositif (**Dispositifs favoris** répertoriés ci-dessous). Un nouveau navigateur s'ouvre pour le dispositif en question.

Pour basculer entre les différents **Dispositifs favoris** répertoriés en fonction de leur nom ou leur adresse IP :

<p>Pour afficher les favoris en fonction de leur adresse IP</p> <p>Cliquez sur le bouton Display by IP (Afficher par IP)</p>	<p>Pour afficher les favoris en fonction de leur nom</p> <p>Cliquez sur le bouton Display by Name (Afficher par nom)</p>
<p>Favorite Devices: KX 2.0</p> <p>Manage</p> <p>Display By IP</p>	<p>Favorite Devices: 192.168.59.48</p> <p>Manage</p> <p>Display By Name</p>

Dispositifs favoris affichés actuellement par nom

Cliquez sur **Display by IP** pour basculer

Dispositifs favoris affichés actuellement par adresse IP

Cliquez sur **Display by name** pour basculer

Menu de gestion des favoris

Le menu de gestion des favoris propose les options suivantes : Favorites List (Liste des favoris), Discover Devices – Local Subnet (Détecter les dispositifs – sous-réseau local), Discover Devices – KX Subnet (Détecter les dispositifs – sous-réseau KX), et Add New Device to Favorites (Ajouter un nouveau dispositif dans les favoris).

Pour ouvrir le menu de gestion des favoris :

Cliquez sur le bouton **Manage (Gérer)**. La page du menu de gestion des favoris s’ouvre :

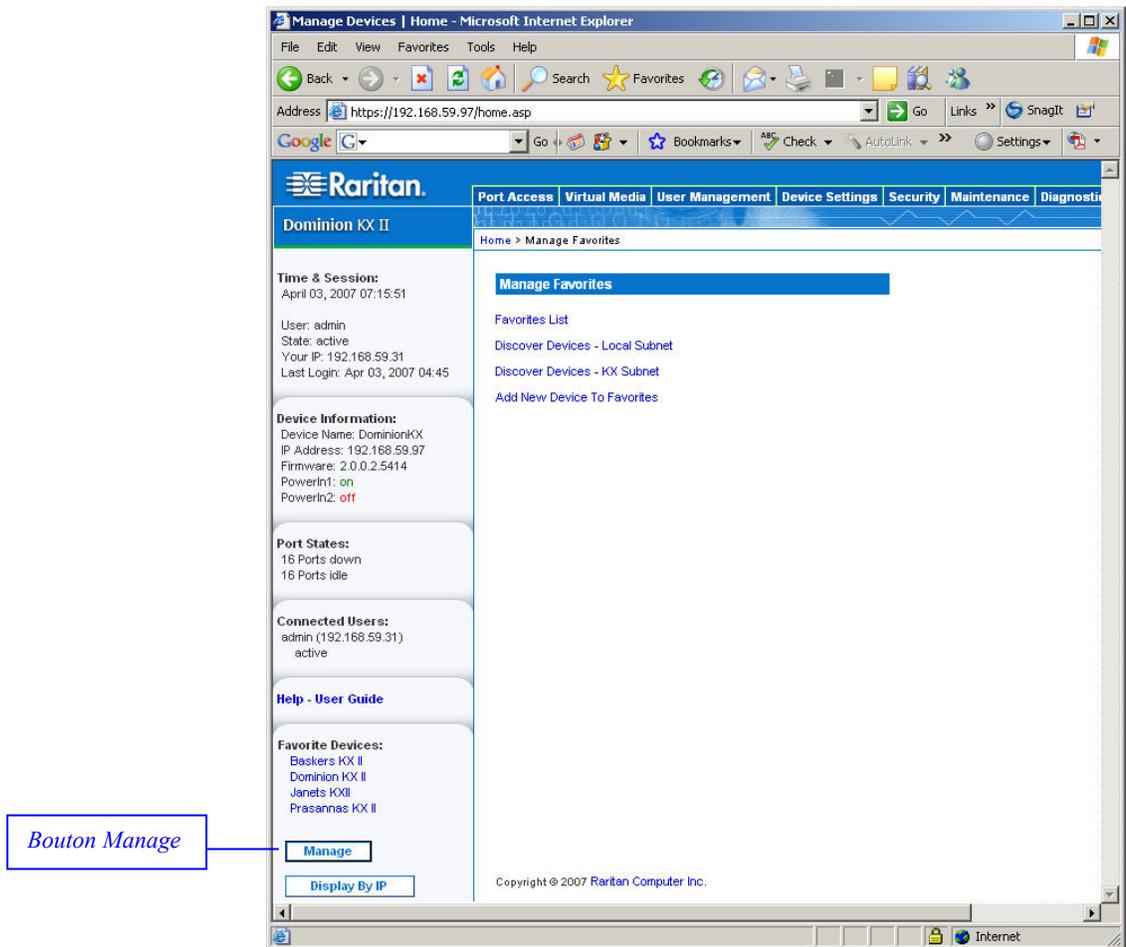


Figure 17 : Menu de gestion des favoris

UTILISEZ :	POUR :
Liste des favoris	Gérer la liste de vos dispositifs favoris
Détection des dispositifs – Sous-réseau local	Détecter les dispositifs sur le sous-réseau local
Détection des dispositifs – Sous-réseau KX	Détecter les dispositifs sur le sous-réseau de dispositifs KX
Ajouter un nouveau dispositif dans les favoris	Ajouter, modifier et supprimer des dispositifs dans votre liste de favoris

Liste des favoris

A partir de la page relative à la liste des favoris, vous pouvez ajouter, modifier et supprimer des dispositifs de votre liste de favoris.

Pour ouvrir la page relative à la liste des favoris :

Sélectionnez **Manage (Gérer) > Favorites List (Liste des favoris)**. La page relative à la liste des favoris s'ouvre :

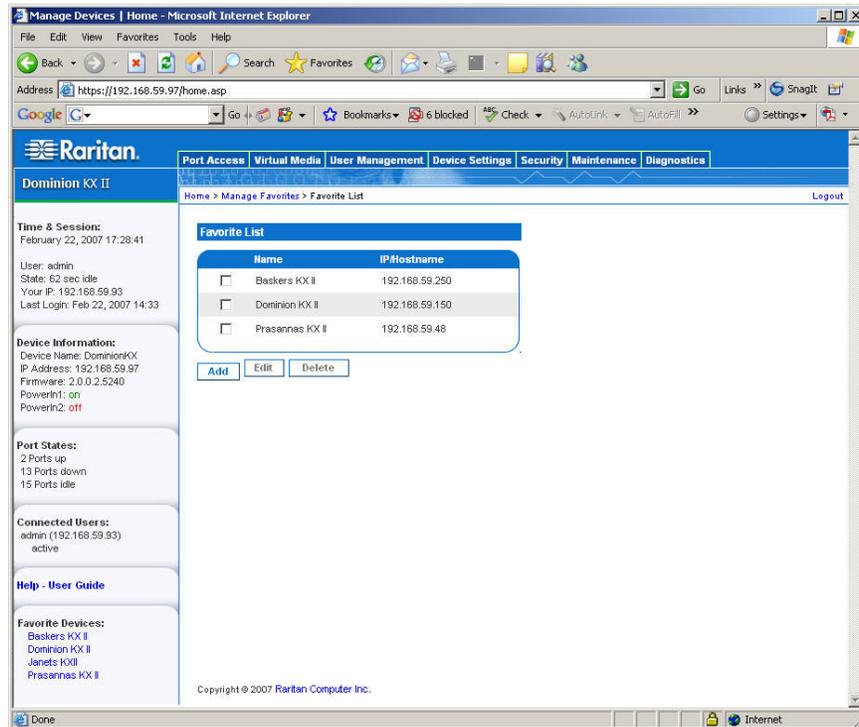


Figure 18 : Liste des favoris

Pour ajouter un favori :

Cliquez sur le bouton **Add (Ajouter)**. La page [Ajouter un nouveau favori](#) s'affiche.

Pour supprimer un favori :

Important : faites attention lorsque vous supprimez des favoris ; il ne vous est pas demandé de confirmer leur suppression.

1. Cochez la case située en regard du dispositif Dominion KX II approprié.
2. Cliquez sur le bouton Delete (Supprimer). Le favori est supprimé de la liste de vos favoris.

Pour modifier un favori :

1. Dans la page de la liste des favoris, cochez la case située en regard du dispositif Dominion KX II approprié.
2. Cliquez sur le bouton **Edit (Modifier)**. La page de modification s'ouvre :

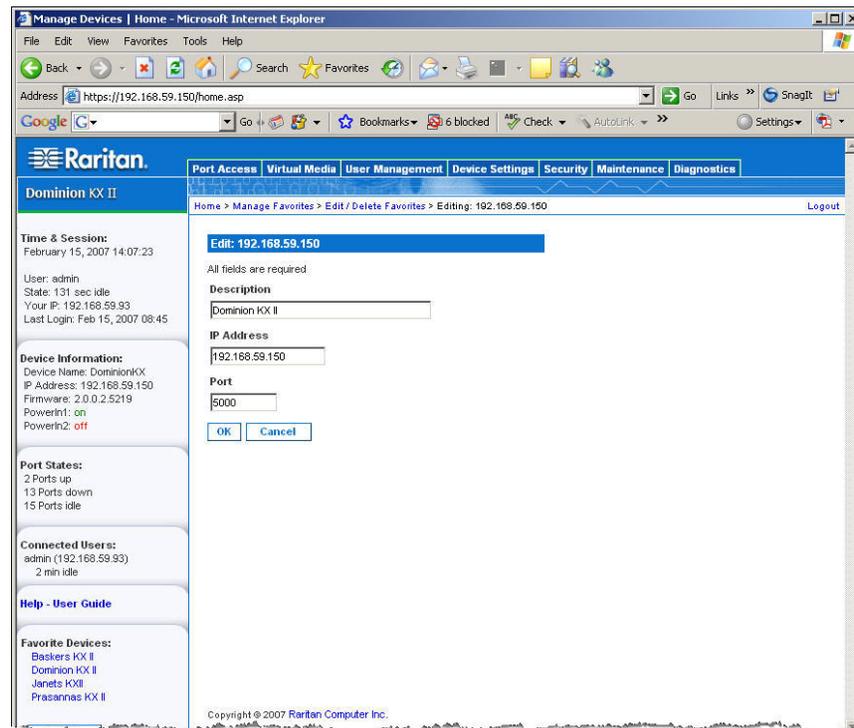


Figure 19 : Modifier (informations relatives aux favoris)

3. Mettez à jour les champs suivants :
 - **Description**. Tapez un nom évocateur.
 - **IP Address (Adresse IP)**. Tapez l'adresse IP de l'unité Dominion KX II.
 - **Port**. Modifiez le port de détection (le cas échéant).
4. Cliquez sur OK.

Détection des dispositifs – Sous-réseau local

Cette option permet de détecter les dispositifs présents sur votre sous-réseau local (c'est-à-dire le sous-réseau sur lequel est exécutée la console distante Dominion KX II), d'accéder à ces dispositifs directement à partir de cette page et de les ajouter à votre liste de favoris.

The screenshot shows the Raritan web interface for Dominion KX II. The main content area is titled 'Discover Devices - Local Subnet'. It includes a checkbox for 'Use Default Port 5000' which is checked, and a 'Discover on Port' field containing '5000'. Below this is a 'Save' button. A table lists discovered devices with columns for 'Name' and 'IP/Hostname'. The table contains 15 entries, including 'Annettes_KX116', 'Annettes_KX432', 'ASTDKXII-416', 'burtykx', 'DeveKX2', and multiple 'Dominion-KX' devices. At the bottom of the table are 'Select All' and 'Deselect All' buttons. Below the table are 'Add' and 'Refresh' buttons. The left sidebar shows session information, device information, port states, and connected users.

Figure 20 : Détection des dispositifs - Sous-réseau local

Pour détecter des dispositifs sur le sous-réseau local :

1. Sélectionnez **Favorites (Favoris) > Discover Devices – Local Subnet (Détecter les dispositifs – sous-réseau local)**. La page de détection des dispositifs sur le sous-réseau local s'ouvre.
2. Sélectionnez le port de détection approprié (refer to [Paramètres réseau divers](#) pour obtenir des **informations relatives au port de détection**) :
 - Pour utiliser le port de détection par défaut, sélectionnez l'option **Use Default Port 5000 (Utiliser le port 5000 par défaut)**.
 - Pour utiliser un port de détection différent :
 - a. Désélectionnez l'option **Use Default Port 5000 (Utiliser le port 5000 par défaut)**.
 - b. Entrez le numéro de port dans le champ **Discover on Port (Détecter le port)**.
 - c. Cliquez sur **Save (Enregistrer)**.
3. Cliquez sur **Refresh (Actualiser)**. La liste des dispositifs du sous-réseau KX est actualisée.

Pour ajouter des dispositifs à votre liste de favoris :

1. Cochez la case située en regard du nom du dispositif/de l'adresse IP.
2. Cliquez sur **Add (Ajouter)**.

*Conseil : utilisez les boutons **Select All (Sélectionner tout)** et **Deselect All (Désélectionner tout)** pour sélectionner (ou désélectionner) rapidement l'ensemble des dispositifs dans le sous-réseau de la console distante.*

Pour accéder à un dispositif détecté :

Cliquez sur le nom du dispositif ou sur son adresse IP. Un nouveau navigateur s'ouvre pour le dispositif en question.

Détection des dispositifs – Sous-réseau KX

Cette option permet de détecter les dispositifs présents sur le sous-réseau de dispositifs KX (c'est-à-dire le sous-réseau de l'adresse IP du dispositif Dominion KX II lui-même), d'accéder à ces dispositifs directement à partir de cette page et de les ajouter à votre liste de favoris.

Cette fonction permet à plusieurs unités Dominion KX II d'interagir et de se mettre à l'échelle automatiquement. La console distante Dominion KX II détecte automatiquement les unités Dominion KX II dans le sous-réseau de Dominion KX II.

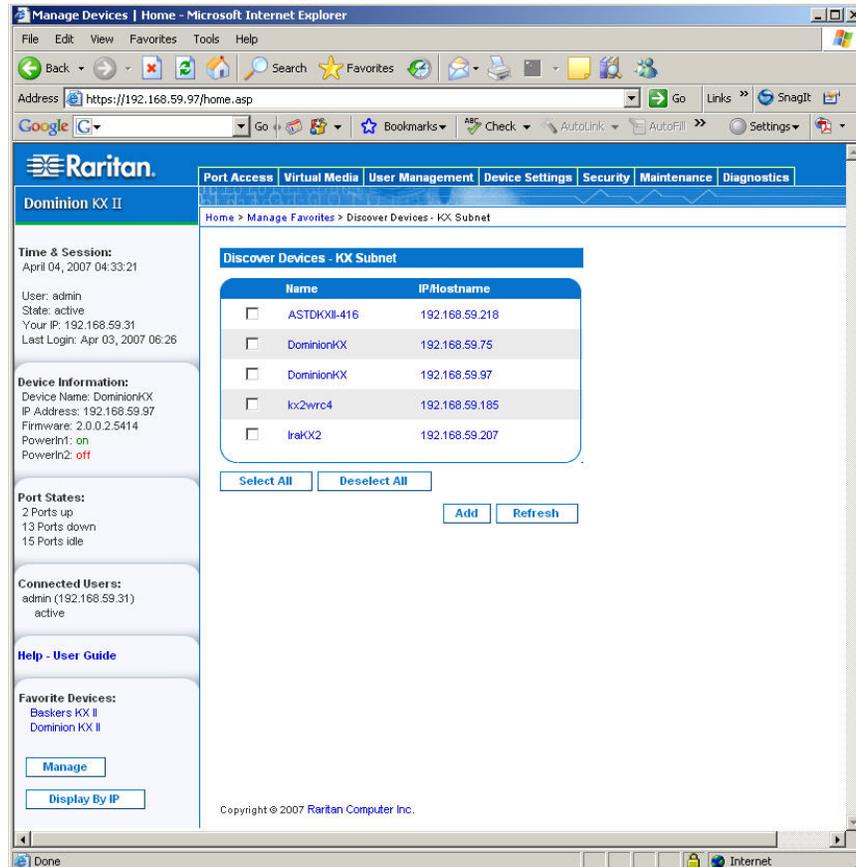


Figure 21 : Détection des dispositifs - Sous-réseau KX

Pour détecter des dispositifs sur le sous-réseau de dispositifs KX :

1. Sélectionnez **Favorites (Favoris) > Discover Devices – KX Subnet (Détecter les dispositifs – sous-réseau KX)**. La page de détection des dispositifs sur le sous-réseau KX s'ouvre.
2. Cliquez sur **Refresh (Actualiser)**. La liste des dispositifs du sous-réseau KX est actualisée.

Pour ajouter des dispositifs à votre liste de favoris :

1. Cochez la case située en regard du nom du dispositif/de l'adresse IP.
2. Cliquez sur **Add (Ajouter)**.

*Conseil : utilisez les boutons **Select All (Sélectionner tout)** et **Deselect All (Désélectionner tout)** pour sélectionner (ou désélectionner) rapidement l'ensemble des dispositifs du sous-réseau de dispositifs Dominion KX II.*

Pour accéder à un dispositif détecté :

Cliquez sur le nom du dispositif ou sur son adresse IP. Un nouveau navigateur s'ouvre pour le dispositif en question.

Ajouter un nouveau favori

Pour ajouter un dispositif dans votre liste de favoris :

1. Sélectionnez **Manage Favorites (Gérer les favoris) > Add New Device to Favorites (Ajouter un nouveau dispositif dans les favoris)**. La page correspondante s'ouvre :

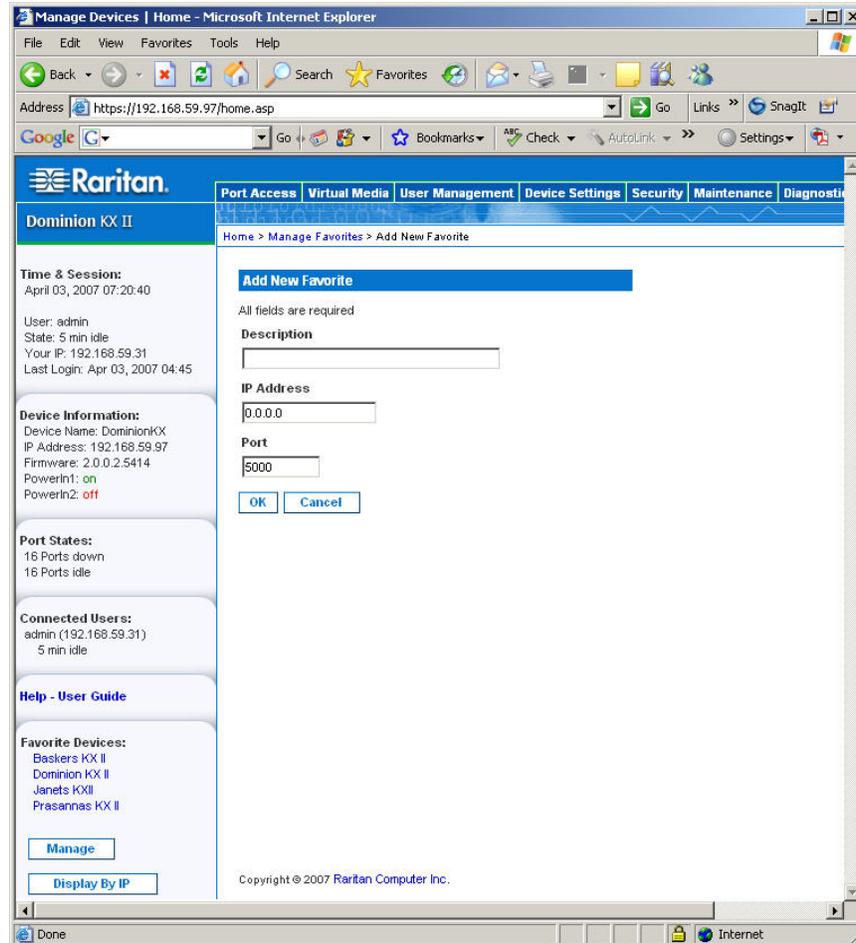


Figure 22 : Ajouter un nouveau favori

2. Tapez une **description** significative.
3. Entrez l'**adresse IP** du dispositif.
4. Modifiez le **port** de détection (le cas échéant).
5. Cliquez sur **OK**. Le dispositif est ajouté à votre liste de favoris.

Chapitre 5 : Accès aux serveurs cible

Page d'accès aux ports

Une fois la connexion à la console locale Dominion KX II réussie, la page d'accès aux ports s'ouvre. Cette page répertorie tous les ports de Dominion KX II, les serveurs cible connectés ainsi que leur état et leur disponibilité. La page d'accès aux ports indique le chemin permettant d'accéder aux serveurs cible connectés à Dominion KX II. Les serveurs cible correspondent aux serveurs que vous souhaitez contrôler par l'intermédiaire de l'unité Dominion KX II ; ils sont connectés aux ports de Dominion KX II, situés sur la partie arrière de l'unité.

Remarque : une nouvelle fenêtre du Client virtuel KVM s'ouvre pour chaque connexion à un serveur cible.

Pour utiliser la page d'accès aux ports :

1. A partir de la console distante KX II, cliquez sur l'onglet **Port Access (Accès aux ports)** pour l'ouvrir. La page d'accès aux ports s'ouvre :

Port Number	Port Name	Status	Availability
1	Dominion-KX2_Port1	down	idle
2	Dominion-KX2_Port2	down	idle
3	Dominion-KX2_Port3	down	idle
4	Dominion-KX2_Port4	down	idle
5	JLTestPC	up	idle
6	Dominion-KX2_Port6	down	idle
7	Dominion-KX2_Port7	down	idle
8	Dominion-KX2_Port8	down	idle
9	Local Port	up	idle
10	Dominion-KX2_Port10	down	idle
11	Dominion-KX2_Port11	down	idle
12	Dominion-KX2_Port12	down	idle
13	Dominion-KX2_Port13	down	idle
14	Dominion-KX2_Port14	down	idle
15	Dominion-KX2_Port15	down	idle

Figure 23 : Port Access (Accès aux ports)

Les serveurs cible sont triés initialement par numéro de port ; vous pouvez modifier l'affichage pour trier en fonction de n'importe laquelle des colonnes.

- **Port Number (Numéro de port).** Les ports sont numérotés de 1 au nombre total de ports disponibles pour l'unité Dominion KX II. Notez que les ports connectés aux barrettes d'alimentation *ne* figurent *pas* dans la liste, ce qui génère des blancs dans la séquence des numéros de port.
- **Port Name (Nom du port).** Le nom du port de Dominion KX II ; il est défini au préalable sur Dominion-KX2-Port#, mais vous pouvez le remplacer par un nom plus évocateur. Lorsque vous cliquez sur le lien Port Name (Nom du port), un menu d'actions relatives au port s'affiche.
- **Status (Etat).** L'état est soit *up*, soit *down*.
- **Availability (Disponibilité).** La **disponibilité** peut correspondre à Idle (Ralenti), Connected (Connecté), Busy (Occupé) ou Unavailable (Indisponible).

2. Cliquez sur l'option **Port Name** (Nom du port) associée au serveur cible auquel vous souhaitez accéder. Le menu d'actions relatif aux ports apparaît. Reportez-vous au [Menu d'actions relatives aux ports](#) pour davantage d'informations sur les options de menu disponibles.
3. Sélectionnez l'option voulue dans le menu d'**actions relatives aux ports**.

Pour modifier l'ordre de tri d'affichage :

Cliquez sur l'en-tête de la colonne que vous souhaitez trier. La liste des serveurs cible est triée par cette colonne.

Menu d'actions relatives aux ports

1. Lorsque vous cliquez sur le lien Port Name (Nom du port) dans la liste d'accès aux ports, un menu d'actions relatives au port s'affiche. Veuillez noter que seules les options disponibles pour le port sélectionné sont répertoriées dans le menu d'actions.

- **Connect (Connecter)**. Permet de créer une nouvelle connexion au serveur cible. Pour la console distante KX II, une nouvelle fenêtre [Virtual KVM Client](#) s'ouvre. En ce qui concerne la console locale KX II, l'affichage bascule de l'interface utilisateur locale sur celle du serveur cible. Sur le port local, l'interface de la console locale KX II doit être visible pour pouvoir procéder à la commutation.

Remarque : cette option ne fonctionne pas pour un port disponible à partir de la console distante KX II si toutes les connexions sont occupées.

- **Switch From (Basculer à partir de)**. Permet de basculer d'une connexion existante au port sélectionné (serveur cible). Cette option de menu est disponible pour chaque connexion ouverte (quatre maximum pour les unités à 4 utilisateurs distants ; deux maximum pour les unités à deux utilisateurs distants ; une maximum pour les unités à 1 utilisateur) ; cette option n'est visible que lorsqu'un ou plusieurs clients virtuels KVM sont ouverts.

Remarque : l'option de menu n'est pas disponible sur la console locale KX II.

- **Disconnect (Déconnecter)**. Permet de déconnecter ce port et ferme la fenêtre du client virtuel KVM correspondant à ce serveur cible. Cette option de menu est disponible uniquement lorsque l'état du port est connecté ou occupé (donc connecté également).

Remarque : cette option de menu n'est pas disponible sur la console locale KX II ; la seule façon de se déconnecter de la cible activée dans la console locale est d'utiliser le [raccourci clavier](#).

- **Power On (Mettre sous tension)**. Permet de mettre le serveur cible sous tension via la prise associée. Cette option est visible uniquement lorsqu'il existe une ou plusieurs associations d'alimentation électrique à cet cible, si la cible est désactivée (état du port déconnecté) et si l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.
- **Power Off (Mettre hors tension)**. Permet de mettre le serveur cible hors tension via les prises associées. Cette option est visible uniquement lorsqu'il existe une ou plusieurs associations d'alimentation électrique à cet cible, si la cible est activée (état du port connecté) et si l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.
- **Power Cycle (Cycle d'alimentation)**. Permet d'éteindre puis de rallumer le serveur cible via les prises associées. Cette option est visible uniquement lorsqu'il existe une ou plusieurs associations d'alimentation électrique à cet cible et lorsque l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.

2. Sélectionnez l'option de menu de votre choix pour ce port afin de l'exécuter.

Connexion à un serveur cible

Pour se connecter à un serveur cible :

1. A partir de la console distante KX II, cliquez sur l'onglet **Port Access (Accès aux ports)** pour l'ouvrir. La page d'accès aux ports s'ouvre.
2. Cliquez sur l'option **Port Name (Nom du port)** associée à la cible à laquelle vous souhaitez accéder. Le **menu d'actions relatives aux ports** apparaît :

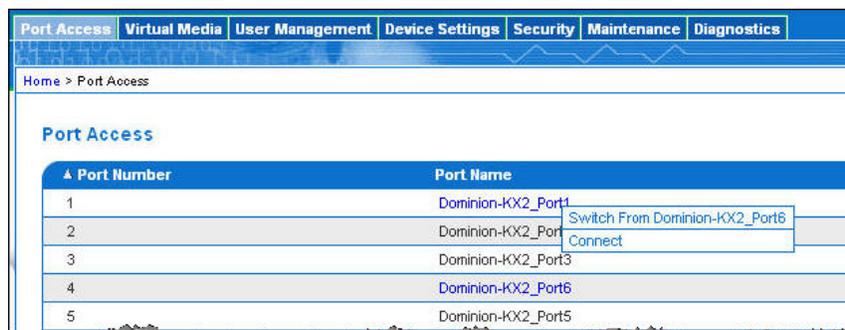


Figure 24 : Menu d'actions relatives aux ports

3. Select **Connect (Connecter)**. Une fenêtre du [Virtual KVM Client](#) s'ouvre pour le serveur cible connecté à ce port.

Commutation entre les serveurs cible

Grâce à Dominion KX II, vous pouvez accéder à plusieurs serveurs cible. Dominion KX II offre la possibilité de basculer d'un serveur cible à l'autre.

Remarque : cette fonction est disponible dans la console distante de Dominion KX II uniquement.

Pour commuter entre les serveurs cible :

1. Si vous utilisez déjà un serveur cible, accédez à la page d'accès aux ports de Dominion KX II.
2. Cliquez sur l'option **Port Name (Nom du port)** associée à la cible à laquelle vous souhaitez accéder maintenant. Le **menu d'actions relatif aux ports** apparaît.
3. Sélectionnez l'option **Switch from (Basculer à partir de)** dans le **menu d'actions relatives aux ports**. La fenêtre du [Virtual KVM Client](#) bascule sur le nouveau serveur cible que vous avez sélectionné.

Déconnexion des serveurs cible

Remarque : cette option de menu n'est pas disponible sur la console locale KX II ; la seule façon de se déconnecter de la cible activée dans la console locale est d'utiliser le [raccourci clavier](#).

Pour déconnecter un serveur cible :

1. Cliquez sur l'option **Port Name (Nom du port)** associée à la cible à partir de laquelle vous souhaitez vous déconnecter. Le **menu d'actions relatif aux ports** apparaît.
2. Sélectionnez l'option **Disconnect (Déconnecter)** dans le **menu d'actions des ports**. La fenêtre du [Virtual KVM Client](#) ferme la fenêtre du serveur cible.

Conseil : vous pouvez également fermer la fenêtre du client virtuel KVM en sélectionnant **Connection > Exit (Quitter)** à partir du menu **Virtual KVM**.

Alimentation électrique contrôlant un serveur cible

Remarque : ces fonctions sont disponibles uniquement si vous avez effectué des associations d'alimentation électrique. Reportez-vous à [Contrôle d'accès IP](#) pour de plus amples informations.

Eteindre et rallumer un serveur cible

Pour éteindre et rallumer un serveur cible :

1. A partir de la console distante KX II, cliquez sur l'onglet **Port Access (Accès aux ports)** pour l'ouvrir. La page d'accès aux ports s'ouvre.
2. Cliquez sur le **nom du port (Port Name)** du serveur cible approprié. Le **menu d'actions relatif aux ports** apparaît.

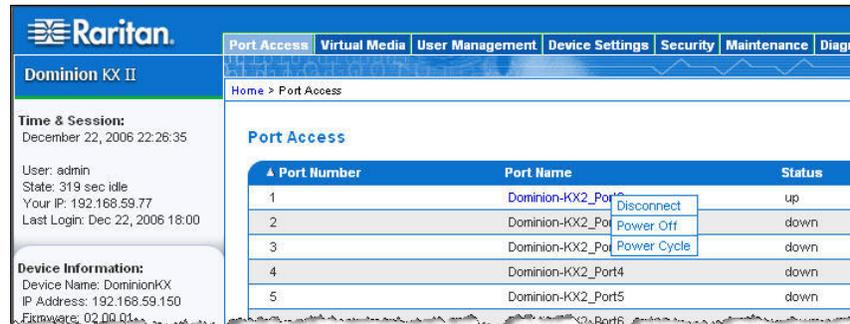


Figure 25 : Menu d'actions relatives aux ports (options d'alimentation)

3. Sélectionnez **Power Cycle (Cycle d'alimentations)**. Un message s'affiche et confirme l'opération effectuée.

Mettre sous tension un serveur cible

Pour mettre sous tension un serveur cible :

1. A partir de la console distante KX II, cliquez sur l'onglet **Port Access (Accès aux ports)** pour l'ouvrir. La page d'accès aux ports s'ouvre.
2. Cliquez sur le **nom du port (Port Name)** du serveur cible approprié. Le **menu d'actions relatif aux ports** apparaît.
3. Sélectionnez **Power On (Mettre sous tension)**.

Mettre un serveur cible hors tension

Pour mettre un serveur cible hors tension :

1. A partir de la console distante KX II, cliquez sur l'onglet **Port Access (Accès aux ports)** pour l'ouvrir. La page d'accès aux ports s'ouvre.
2. Cliquez sur le **nom du port (Port Name)** du serveur cible approprié. Le **menu d'actions relatif aux ports** apparaît.
3. Sélectionnez **Power Off (Mettre hors tension)**.

Chapitre 6 : Virtual KVM Client (Client virtuel KVM)

Chaque fois que vous accédez à un serveur cible à l'aide de la console distante KX II, une fenêtre du client virtuel KVM s'ouvre. Il existe un client virtuel KVM pour *chaque* serveur cible connecté ; ces fenêtres sont accessibles via la barre des tâches de Windows.

Les fenêtres du client Virtual KVM Client peuvent être réduites, agrandies et déplacées sur le bureau de votre ordinateur.

Remarque : le fait d'actualiser votre navigateur HTML entraîne la fermeture de la connexion de Virtual KVM Client ; faites donc attention.

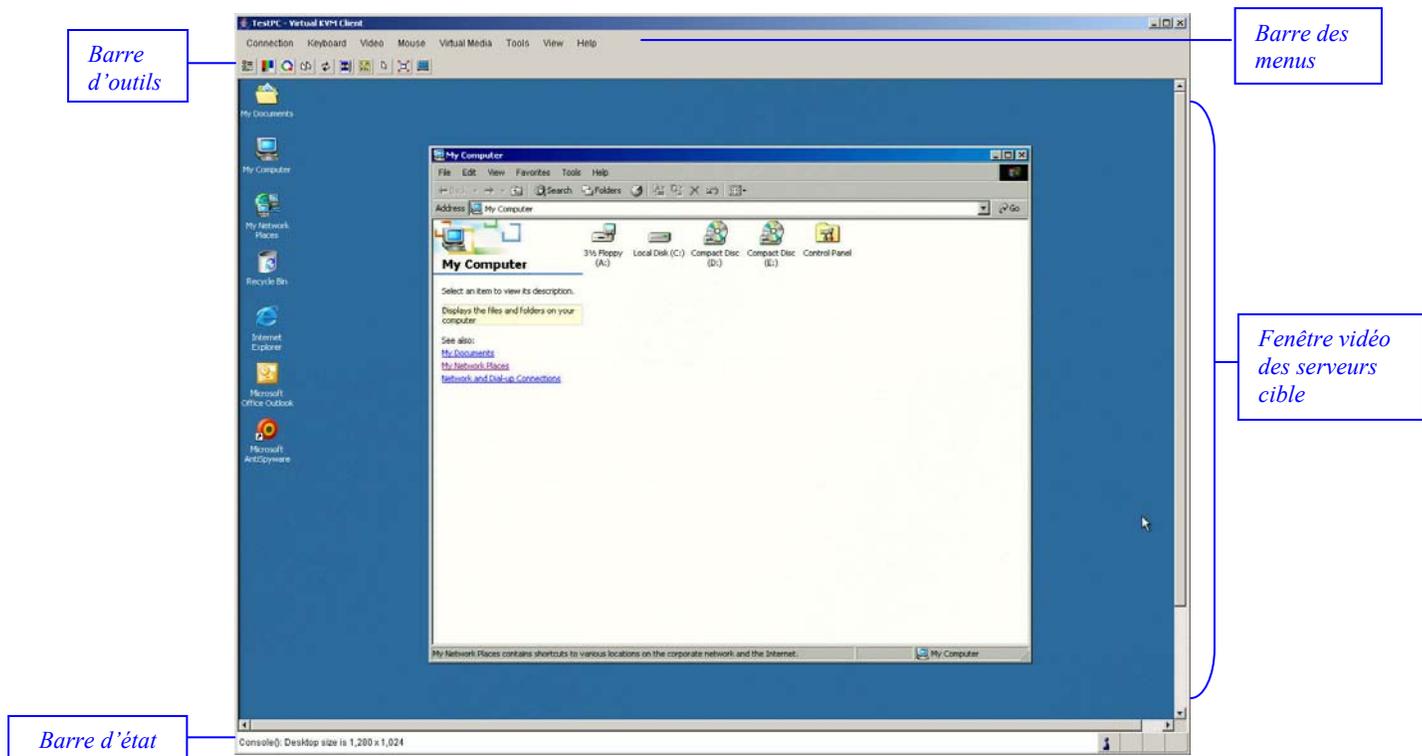


Figure 26 : Fenêtre de Virtual KVM Client (Client virtuel KVM)

Les fonctions suivantes, disponibles dans Virtual KVM Client, sont accessibles par le biais du menu et de la barre d'outils.

FONCTION	DESCRIPTION
Barre des menus	Menus déroulants de commandes et de paramètres.
Barre d'outils	Boutons de raccourci pour lancer les fonctions et les commandes fréquemment utilisées.
Fenêtre vidéo des serveurs cible	Affiche les serveurs cible.
Barre d'état	Informations en temps réel sur les paramètres de connexion, la taille de fenêtre des serveurs cible, le voyant de verrouillage des majuscules et celui du verrouillage numérique.

Options

Arborescence de menus

Le tableau suivant comporte l'ensemble des options de menu disponibles dans Virtual KVM Client.

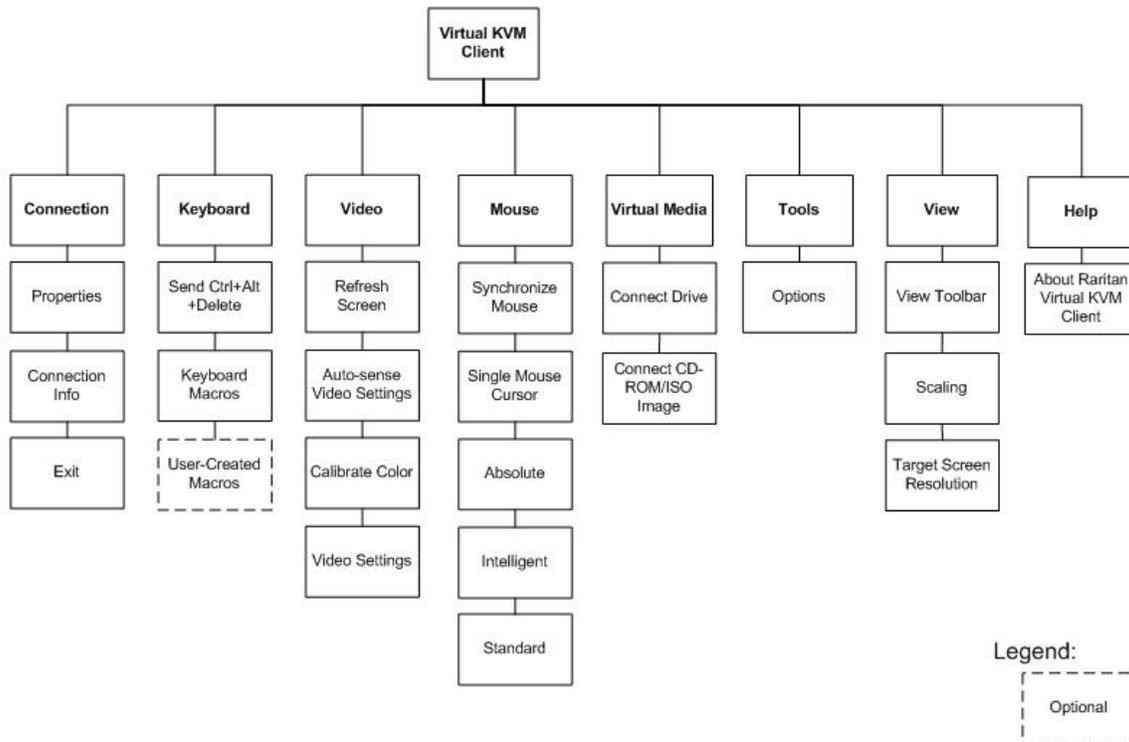


Figure 27 : Arborescence de menus de Virtual KVM Client

Barre d'outils

BOUTON	DESCRIPTION
	Propriétés
	Paramètres vidéo
	Calibrer les couleurs
	Synchroniser les curseurs de souris du client et du serveur cible
	Actualiser l'écran
	Détection automatique de la vidéo)
	Send Ctrl+Alt+Delete (Envoyer Ctrl+Alt+Suppr)
	Basculer entre les modes de souris simple/double
	Plein écran
	Redimensionner la vidéo pour l'ajuster à l'écran

Synchronisation des pointeurs de souris

Lorsque vous affichez à distance un serveur cible utilisant une souris, vous verrez apparaître deux pointeurs de souris : un curseur correspond à votre poste de travail client distant et l'autre au serveur cible. Lorsque le pointeur de votre souris se trouve *dans la zone* de la fenêtre du serveur cible de Virtual KVM Client, les mouvements et les clics de souris sont directement transmis au serveur cible connecté. Lorsqu'il est en mouvement, le pointeur de la souris du client domine légèrement celui de la souris rattachée à la cible en raison des paramètres d'accélération de souris.

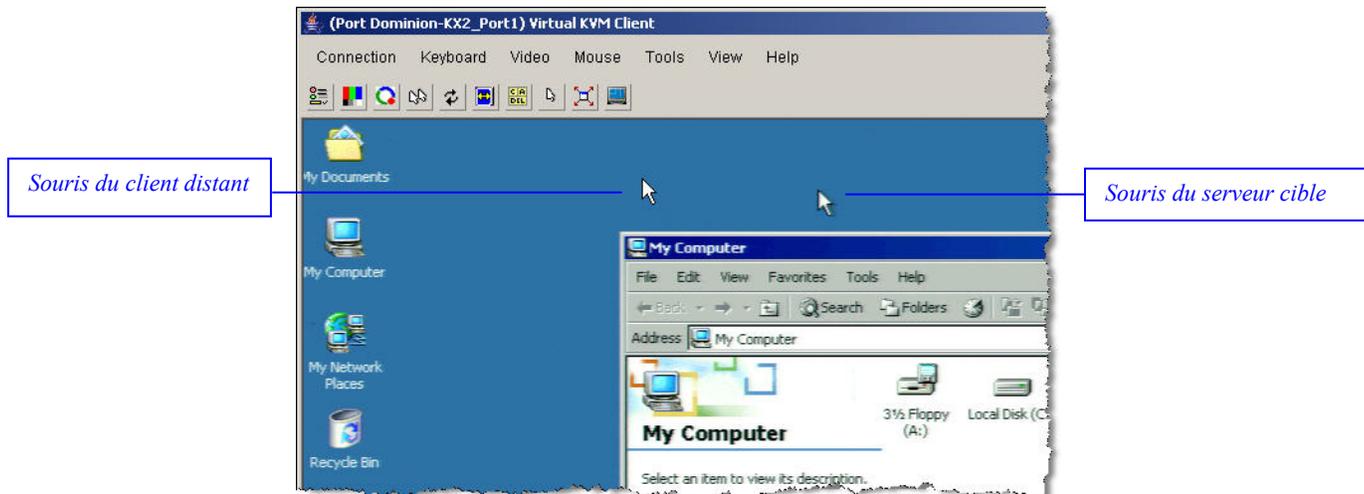


Figure 28 : Curseurs de souris doubles

Avec des connexions de réseau local rapides, vous souhaitez peut-être désactiver le pointeur de la souris de Virtual KVM Client et afficher uniquement le pointeur de la souris du serveur cible. Vous pouvez basculer entre ces deux modes de souris (simple et double). Reportez-vous à [Menu d'actions relatives aux ports](#) pour obtenir des informations supplémentaires sur les modes de souris disponibles.

Menu de connexion

Boîte de dialogue des propriétés

Les algorithmes de compression vidéo dynamique de Dominion KX II maintiennent le caractère convivial des consoles KVM avec différents types de bande passante. Dominion KX II optimise sa sortie KVM pour l'utilisation dans un réseau local mais également pour l'utilisation dans un réseau étendu et à distance. Ces unités peuvent également contrôler le nombre de couleurs et limiter la sortie vidéo afin de proposer un équilibre optimal entre qualité vidéo et réactivité du système pour n'importe quel type de bande passante.

	Connection Properties (Propriétés de la connexion)	Réglez manuellement les options liées à la bande passante (vitesse de connexion, nombre de couleurs transmises, etc.).
---	---	---

Les paramètres de la boîte de dialogue des propriétés peuvent être optimisés pour répondre à vos critères spécifiques selon les différents environnements d'exploitation.

Pour définir les propriétés de la connexion :

1. Sélectionnez **Connection (Connexion) > Properties (Propriétés)**. La fenêtre Properties Dialog (Boîte de dialogue des propriétés) s'affiche.

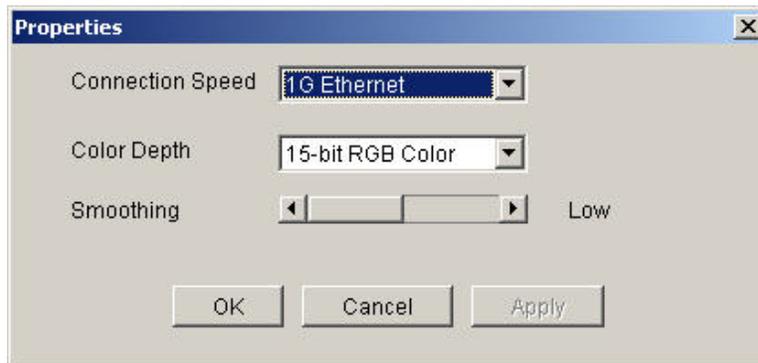


Figure 29 : Boîte de dialogue des propriétés

2. Sélectionnez **Connection Speed (Vitesse de connexion)** à partir de la liste déroulante. Dominion KX II peut détecter automatiquement la bande passante disponible et limiter son utilisation, mais vous pouvez également en régler l'utilisation en fonction des limitations de la bande passante.

Auto
Ethernet 1 G
Ethernet 100 Mo
Ethernet 10 Mo
1,5 Mo (MAX DSL/T1)
1 Mo (DSL/T1 rapide)
512 Ko (DSL/T1 moyen)
384 Ko (DSL/T1 lent)
256 Ko (Câble)
128 Ko (ISDN double)
56 Ko (Modem ISP)
33 Ko (Modem rapide)
24 Ko (Modem lent)

Veuillez noter que ces paramètres représentent des valeurs optimales dans des conditions spécifiques plutôt que le débit exact. Le client et le serveur s'efforcent de transmettre les données vidéo aussi rapidement que possible sur le réseau quels que soient la vitesse réseau et le paramètre d'encodage. Le système sera, cependant, plus réactif si les paramètres coïncident avec l'environnement réel.

3. Sélectionnez **Color Depth (Nombre de couleurs)** à partir de la liste déroulante. Dominion KX II peut adapter de manière dynamique le nombre de couleurs transmis aux utilisateurs distants afin d'optimiser le caractère convivial pour n'importe quel type de bande passante.

Couleurs RVB 15 bits
Couleurs RVB 8 bits
Couleurs 4 bits
Gris 4 bits
Gris 3 bits
Gris 2 bits
Noir et blanc

Important : pour la plupart des tâches d'administration (surveillance de serveur, reconfiguration, etc.), les administrateurs de serveurs n'ont pas besoin de l'ensemble du spectre de couleurs 24 bits ou 32 bits, disponible avec la plupart des cartes graphiques modernes. Si vous tentez de transmettre des images avec un nombre de couleurs aussi élevé, vous risquez de perdre une certaine quantité de la précieuse bande passante de votre réseau.

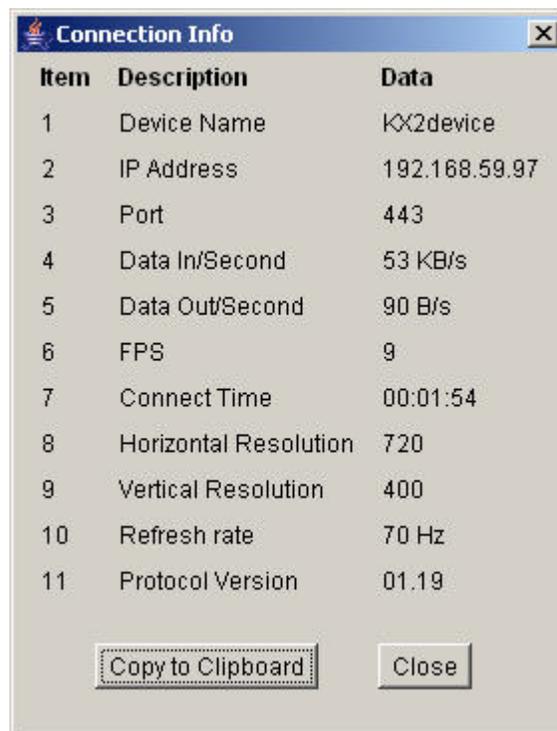
4. Utilisez le curseur de défilement pour sélectionner le niveau de lissage souhaité (mode couleurs 15 bits uniquement). Le niveau de lissage détermine le degré de fusion des zones de l'écran aux variations de couleurs faibles en une couleur unique et uniforme. Le lissage améliore l'apparence des vidéos cible en réduisant les bruits vidéo affichés.
5. Cliquez sur **OK** pour configurer ces propriétés.

Pour quitter sans enregistrer les modifications :
cliquez sur **Cancel (Annuler)**.

Informations sur la connexion

Pour obtenir des informations sur votre connexion à Virtual KVM Client :

Sélectionnez **Connexion (Connexion) > Connexion Info (Informations sur la connexion)**.
La fenêtre d'informations sur la connexion s'affiche alors :



Item	Description	Data
1	Device Name	KX2device
2	IP Address	192.168.59.97
3	Port	443
4	Data In/Second	53 KB/s
5	Data Out/Second	90 B/s
6	FPS	9
7	Connect Time	00:01:54
8	Horizontal Resolution	720
9	Vertical Resolution	400
10	Refresh rate	70 Hz
11	Protocol Version	01.19

Buttons: Copy to Clipboard, Close

Figure 30 : Informations sur la connexion

Les informations suivantes relatives à la connexion en cours s'affichent :

- **Device Name (Nom du dispositif)**. Le nom du dispositif Dominion KX II.
- **IP Address (Adresse IP)**. L'adresse IP du dispositif Dominion KX II.
- **Port**. Le port TCP/IP de communication KVM utilisé pour l'accès au dispositif cible.
- **Data In/Second (Entrée des données/seconde)**. Taux d'entrée des données.
- **Data Out/Second (Sortie des données/seconde)**. Taux de sortie des données.
- **Connect Time (Temps de connexion)**. La durée du temps de connexion.
- **FPS**. Les images par seconde transmises pour la vidéo.
- **Horizontal Resolution (Résolution horizontale)**. La résolution d'écran horizontale.
- **Vertical Resolution (Résolution verticale)**. La résolution d'écran verticale.
- **Refresh Rate (Taux de rafraîchissement)**. La fréquence à laquelle l'écran est actualisé.
- **Protocol Version (Version du protocole)**. La version du protocole RFB.

Pour copier ces informations :

Cliquez sur **Copy to Clipboard (Copier dans Presse-papiers)**. Ces informations peuvent maintenant être copiées dans le programme de votre choix.

Exit (Quitter)

Pour fermer Virtual KVM Client (la cible en cours d'utilisation) :

Sélectionnez **Connexion > Exit (Connexion > Quitter)**.

Menu de clavier

Send Ctrl+Alt+Delete (Envoyer Ctrl+Alt+Suppr)

En raison de son utilisation fréquente, la macro **Ctrl+Alt+Suppr** a été préprogrammée dans Virtual KVM Client.

La séquence de touches est envoyée au serveur cible auquel vous êtes connecté en ce moment. Par opposition, si vous appuyez sur les touches **Ctrl+Alt+Suppr** de votre clavier lors de l'utilisation de Virtual KVM Client, la commande serait d'abord interceptée par votre propre ordinateur en raison de la structure du système d'exploitation, au lieu d'être envoyée au serveur cible comme prévu.

	Send Ctrl+Alt+Delete (Envoyer Ctrl+Alt+Suppr)	Permet d'envoyer la séquence de touches Ctrl+Alt+Suppr au serveur cible.
---	---	---

Pour envoyer la séquence de touches **Ctrl+Alt+Suppr** au serveur cible :

- Sélectionnez **Keyboard (Clavier) > Send Ctrl+Alt+Delete (Envoyer Ctrl+Alt+Suppr)** ou
- Cliquez sur le bouton **Send Ctrl+Alt+Delete (Envoyer Ctrl+Alt+Suppr)** dans la barre d'outils.

Macros de clavier

Les macros de clavier garantissent l'envoi des frappes destinées au serveur cible et leur interprétation par le serveur cible uniquement. Sinon, elles risqueraient d'être interprétées par l'ordinateur sur lequel est exécuté Virtual KVM Client (votre PC client).

Les macros sont stockées sur le PC client et sont spécifiques au PC ; par conséquent si vous utilisez un autre PC, vous ne verrez pas vos macros. Par ailleurs, si une autre personne utilise votre PC et se connecte sous un nom différent, cet utilisateur verra vos macros puisqu'elles font partie intégrante de l'ordinateur. Les macros de clavier créées dans Virtual KVM Client sont disponibles dans MPC et inversement.

Création d'une macro de clavier

Pour créer une macro de clavier (ajouter une macro) :

1. Sélectionnez **Keyboard (Clavier) > Keyboard Macros (Macros de clavier)**. La fenêtre de macros de clavier s'ouvre :

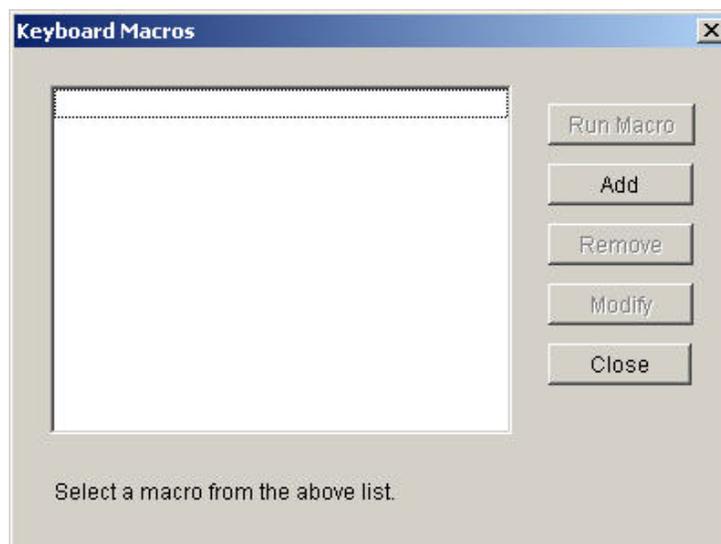


Figure 31 : Macros de clavier

2. Cliquez sur **Add (Ajouter)**. La fenêtre d'ajout de macro de clavier s'ouvre :

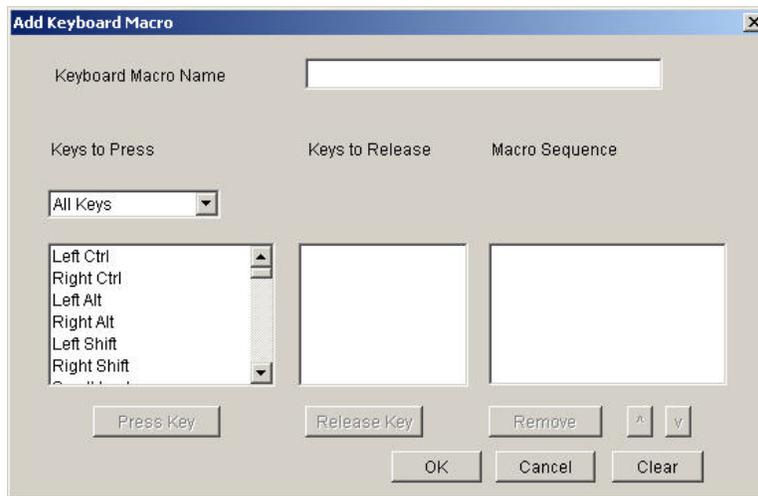


Figure 32 : Ajouter une macro de clavier

3. Saisissez un nom dans le champ **Keyboard Macro Name (Nom de la macro de clavier)**. Il s'agit du nom qui s'affichera dans la barre de menu de Virtual KVM Client, une fois la macro créée. Dans cet exemple, saisissez **Minimize All Windows (Réduire toutes les fenêtres)**.
4. Dans la liste déroulante **Keys to Press (Touches à enfoncer)** :
- Faites défiler la liste et sélectionnez chaque touche pour laquelle vous souhaitez émuler des frappes de touches (dans l'ordre dans lequel les touches seront enfoncées).
 - Cliquez sur le bouton **Press Key (Appuyer sur la touche)** après chaque sélection. Une fois sélectionnées, les touches s'affichent dans le champ **Keys to Release (Touches à relâcher)**.
*Dans cet exemple, sélectionnez deux touches : la touche **Windows** et la touche de la lettre **D**.*
5. Dans le champ **Keys to Release (Touches à relâcher)** :
- Sélectionnez chaque touche pour laquelle vous souhaitez émuler des relâchements de touches (dans l'ordre dans lequel les touches seront relâchées).
 - Cliquez sur **Release Key (Relâcher la touche)** après chaque sélection.
Dans cet exemple, les deux touches enfoncées doivent également être relâchées.
6. Vérifiez le champ **Macro Sequence (Séquence de la macro)** – son contenu est généré automatiquement selon les sélections effectuées dans les champs **Keys to Press (Touches à enfoncer)** et **Keys to Release (Touches à relâcher)**. Vérifiez que la séquence de la **macro (Macro Sequence)** correspond à la séquence de touches exacte de votre choix. [Pour supprimer une étape de la séquence, sélectionnez l'étape et cliquez sur **Remove (Supprimer)**].

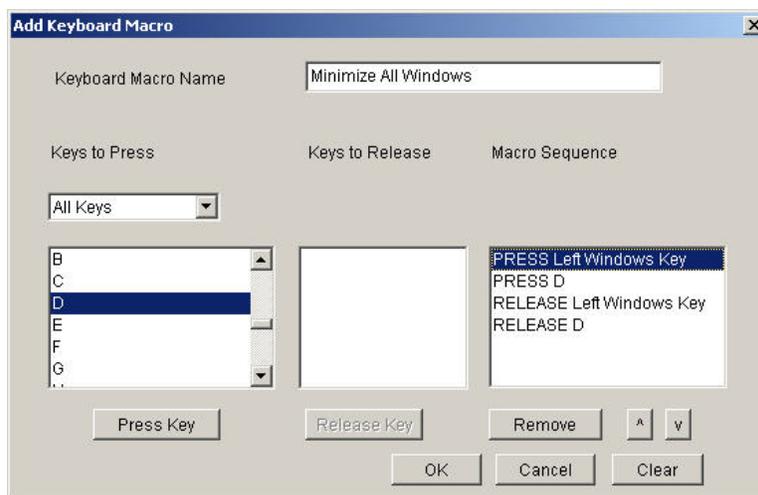


Figure 33 : Exemple de macro de clavier

*Conseil : Utilisez les touches **^** et **v** pour réorganiser la séquence de touches.*

7. Cliquez sur **OK** dans la fenêtre Add Keyboard Macro (Ajouter une macro de clavier) pour enregistrer la macro.
8. Cliquez sur **Close (Fermer)** dans la fenêtre Keyboard Macros (Macros de clavier) (Figure 31). La macro de clavier créée figure maintenant parmi les options de la liste du menu **Keyboard (Clavier)**.



Figure 34 : Nouvelle macro dans le menu Clavier

Pour quitter sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour effacer le contenu des champs et recommencer :

Cliquez sur le bouton **Clear (Effacer)**.

Lancement d'une macro de clavier

Une fois la macro de clavier créée, exécutez-la en cliquant sur son nom dans le menu **Keyboard (Clavier)**.

Pour exécuter une macro (en utilisant cet exemple) :

Sélectionnez **Keyboard (Clavier) > Minimize All Windows (Minimiser toutes les fenêtres)**.

Une autre méthode consiste à sélectionner la macro à partir de la fenêtre Keyboard Macros (Macros de clavier).

Pour exécuter une macro :

1. Sélectionnez **Keyboard (Clavier) > Keyboard Macros (Macros de clavier)**. La fenêtre de macros de clavier s'ouvre.
2. Sélectionnez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur **Run Macro (Exécuter la macro)**.

Modification d'une macro de clavier

Pour modifier une macro :

1. Sélectionnez **Keyboard (Clavier) > Keyboard Macros (Macros de clavier)**. La fenêtre de macros de clavier s'ouvre.
2. Sélectionnez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur **Modify (Modifier)**. La fenêtre d'ajout/de modification de la macro s'ouvre :
4. Faites vos modifications.
5. Cliquez sur **OK**.

Suppression d'une macro de clavier

Faites attention lorsque vous supprimez des macros ; il ne vous est pas demandé de confirmer leur suppression.

Pour supprimer une macro :

1. Sélectionnez **Keyboard (Clavier) > Keyboard Macros (Macros de clavier)**. La fenêtre de macros de clavier s'ouvre.
 2. Sélectionnez la macro parmi celles qui figurent dans la liste.
 3. Cliquez sur **Remove (Supprimer)**. La macro est supprimée.
-

Menu vidéo

Les paramètres vidéo peuvent être actualisés automatiquement de plusieurs manières :

- L'option **Refresh Screen (Actualiser l'écran)** permet d'actualiser l'écran vidéo
- L'option **Auto-sense Video Settings (Détection automatique des paramètres vidéo)** permet de détecter automatiquement les paramètres vidéo du serveur cible
- L'option **Calibrate Color (Calibrer les couleurs)** permet de procéder au calibrage de la vidéo et d'optimiser les couleurs affichées

Vous pouvez également régler les paramètres manuellement via l'option **Video Settings (Paramètres vidéo)**.

Refresh Screen (Actualiser l'écran)

L'option Refresh Screen (Actualiser l'écran) permet d'actualiser l'écran vidéo. L'écran vidéo entier est redessiné.

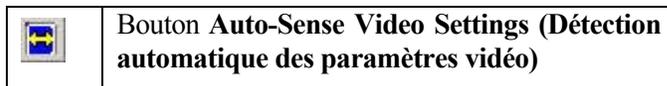


Pour actualiser les paramètres vidéo :

- Sélectionnez **Video (Vidéo) > Refresh Screen (Actualiser l'écran)** ou
- Cliquez sur le bouton **Refresh Screen (Actualiser l'écran)** dans la barre d'outils

Auto-sense Video Settings (Détection automatique des paramètres vidéo)

L'option de détection automatique des paramètres vidéo permet une redétection des paramètres vidéo (résolution, taux de rafraîchissement) et de redessiner l'écran vidéo.



Pour détecter les paramètres vidéo automatiquement :

- Sélectionnez **Video (Vidéo) > Auto-Sense Video Settings (Détection automatique des paramètres vidéo)** ou
- Cliquez sur le bouton de détection **automatique des paramètres vidéo** dans la barre d'outils

Un message s'affiche pour indiquer que le réglage automatique est en cours.

Calibrer les couleurs

Utilisez la commande Calibrate Color (Calibrer les couleurs) pour optimiser les niveaux de couleur (teinte, luminosité, saturation) des images vidéo transmises. Les paramètres couleur de Dominion KX II concernent le serveur cible.



Remarque : l'option de calibrage des couleurs s'applique à la connexion en cours uniquement.

Pour procéder au calibrage des couleurs :

1. Etablissez une connexion KVM distante avec les serveurs cible exécutant une interface utilisateur graphique.
2. Sélectionnez **Video (Vidéo) > Calibrate Color (Calibrer les couleurs)** (ou cliquez sur le bouton de calibrage des couleurs). Le calibrage des couleurs de l'écran du dispositif cible est mis à jour.

Video Settings (Paramètres vidéo)

Utilisez l'option de paramètres vidéo pour ajuster manuellement les paramètres vidéo.

	Video Settings (Paramètres vidéo)	Ouvre la fenêtre Paramètres vidéo pour le réglage manuel des paramètres vidéo.
---	-----------------------------------	--

Pour modifier les paramètres vidéo :

1. Sélectionnez **Video (Vidéo) > Video Settings (Paramètres vidéo)**. La fenêtre des paramètres vidéo s'ouvre et affiche les paramètres actuels :

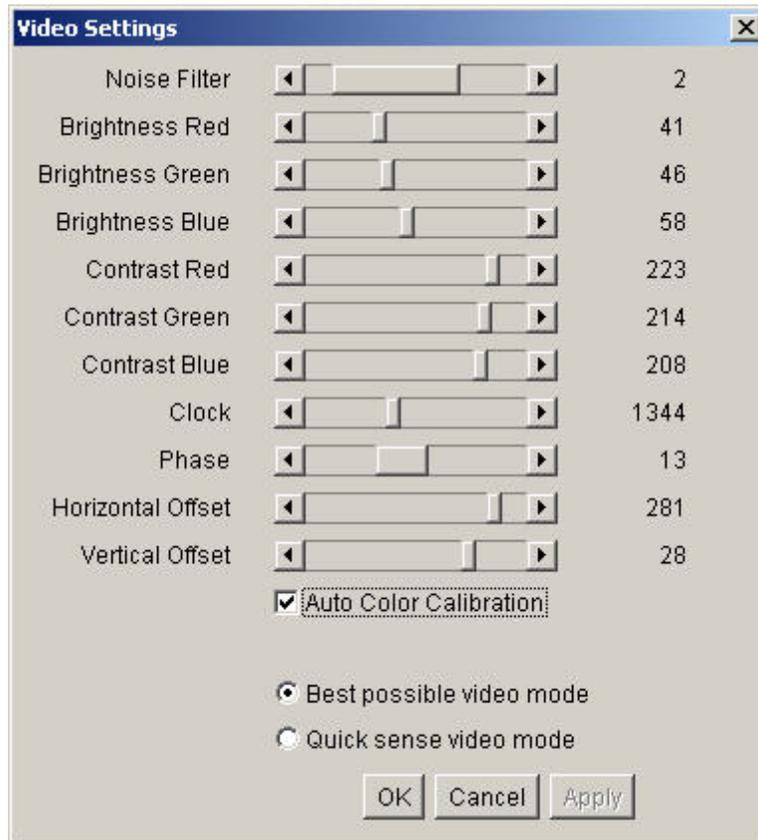


Figure 35 : Video Settings (Paramètres vidéo)

2. Utilisez le curseur de défilement pour régler les paramètres comme vous le souhaitez (à mesure que vous ajustez les paramètres, les résultats sont visibles immédiatement).
 - **Noise Filter (Filtre antiparasite)**. Dominion KX II peut supprimer les interférences électriques de la sortie vidéo des cartes graphiques. Cette fonction permet d'optimiser la qualité des images et de réduire la quantité de bande passante utilisée. Les paramètres plus élevés transmettent des pixels de variante uniquement s'il existe une importante variation de couleurs par rapport aux pixels voisins. Néanmoins, si vous définissez un seuil trop élevé, des modifications souhaitées au niveau de l'écran peuvent être filtrées de manière non intentionnelle.

Les paramètres moins élevés transmettent la plupart des modifications de pixels. Si ce seuil est défini de manière trop faible, l'utilisation de la bande passante risque d'être plus importante.

- **Brightness (Luminosité)** : Utilisez cette option pour ajuster la luminosité de l'écran du serveur cible.
 - **Rouge**. Contrôle la luminosité du signal rouge.
 - **Vert**. Contrôle la luminosité du signal vert.
 - **Bleu**. Contrôle la luminosité du signal bleu.

- Color Contrast Settings (Paramètres de contraste des couleurs) : Contrôlent les paramètres de contraste.
 - **Contrast Red (Contraste du rouge)**. Contrôle le signal rouge.
 - **Contrast Green (Contraste du vert)**. Contrôle le signal vert.
 - **Contrast Blue (Contraste du bleu)**. Contrôle le signal bleu.
- Si l'image vidéo semble très floue ou que sa mise au point ne semble pas correcte, les paramètres de l'horloge et la phase peuvent être ajustés jusqu'à ce qu'une image de meilleure qualité s'affiche sur le serveur cible actif.

Avertissement : veuillez faire attention lorsque vous modifiez les paramètres de l'horloge et de la phase ; en effet ces modifications peuvent entraîner des pertes ou des distorsions vidéo et il se peut que vous ne soyez plus en mesure de revenir à l'état précédent. Contactez le support technique Raritan avant d'effectuer tout changement.

- **Clock (Horloge)**. Contrôle la vitesse d'affichage des pixels vidéo sur l'écran vidéo. Les modifications apportées aux paramètres de l'horloge entraîne l'étirement ou la réduction de l'image vidéo sur le plan horizontal. Nous vous recommandons d'indiquer des nombres impairs. Dans la majorité des cas, ce paramètre ne doit pas être modifié car la détection automatique est en général très précise.
 - **Phase**. les valeurs de phase sont comprises entre 0 et 31 et s'affichent en boucle. Arrêtez le réglage sur la valeur de phase qui produit l'image vidéo de meilleure qualité pour le serveur cible actif.
 - Offset (Décalage) : Permet de contrôler le positionnement à l'écran :
 - **Horizontal Offset (Décalage horizontal)**. Contrôle le positionnement horizontal de l'affichage du serveur cible sur votre écran.
 - **Vertical Offset (Décalage vertical)**. Contrôle le positionnement vertical de l'affichage du serveur cible sur votre écran.
 - **Auto Color Calibration (Calibrage des couleurs automatique)**. Cochez cette option si vous souhaitez un calibrage des couleurs automatique.
 - **Video Sensing (Détection vidéo)** : Sélectionnez le mode de détection vidéo :
 - **Best possible video mode (Mode vidéo optimal)** : Dominion KX II effectue la totalité du processus de détection automatique lorsque vous changez de cibles ou de résolutions cible. La sélection de cette option génère le calibrage de la vidéo pour obtenir une qualité d'image optimale.
 - **Quick sense video mode (Détection rapide du mode vidéo)** : Si vous sélectionnez cette case, Dominion KX II détecte automatiquement et rapidement le mode vidéo utilisé afin d'afficher au plus vite le signal vidéo de la cible. Cette option est particulièrement utile lors de la saisie de la configuration BIOS d'un serveur cible immédiatement après un redémarrage.
3. Cliquez sur **Appliquer**. Les paramètres vidéo sont modifiés.

Remarque : il se peut que certains écrans d'arrière-plan Sun, tels que les écrans à bord très sombres, ne se centrent pas de façon précise sur certains serveurs Sun. Utilisez un arrière-plan différent ou une icône de couleur plus claire dans le coin supérieur gauche de l'écran.

Pour quitter en enregistrant les modifications apportées :
cliquez sur **Cancel (Annuler)**.

Menu de souris

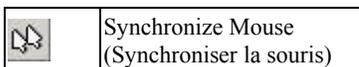
Lors de la gestion d'un serveur cible, la console distante de KX II affiche deux curseurs de souris : un curseur correspond à votre poste de travail client et l'autre au serveur cible. Vous avez la possibilité d'opérer soit en mode souris simple, soit en mode souris double. Si vous choisissez le mode souris double et que les paramètres sont configurés correctement, les deux curseurs de souris s'alignent. Si vous rencontrez des difficultés au niveau de la synchronisation de la souris, consultez [Configuration des serveurs cible](#).

Lorsqu'il y a deux curseurs de souris, Dominion KX II propose plusieurs modes souris :

- Absolu (Synchronisation de la souris)
- Intelligent (Mode souris)
- Standard (Mode souris)

Synchronize Mouse (Synchroniser la souris)

En mode souris double, l'option Synchronize Mouse (Synchroniser la souris) permet de réaligner le pointeur de la souris du serveur cible avec le pointeur de la souris de Virtual KVM Client.

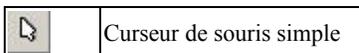


Pour synchroniser la souris :

- Sélectionnez **Mouse (Souris) > Synchronize Mouse (Synchroniser la souris)** ou
- cliquez sur le bouton de synchronisation de la souris dans la barre d'outils.

Curseur de souris simple

Le curseur de souris simple permet d'accéder au mode souris simple dans lequel seul le pointeur de la souris du serveur cible apparaît ; le pointeur de la souris de l'ordinateur local ne s'affiche plus à l'écran. Si vous êtes en mode souris simple, l'option de synchronisation de la souris n'est pas disponible (en effet il n'est pas nécessaire de synchroniser un curseur de souris simple).



Pour entrer dans le mode de souris simple :

- Sélectionnez **Mouse (Souris) > Single Mouse Cursor (Curseur de souris simple)** ou
- cliquez sur le bouton Single/Double Mouse Cursor (Curseur de souris simple/double) dans la barre d'outils.

Pour quitter le mode souris simple :

1. Lorsque vous entrez dans le mode souris simple, le message suivant s'affiche. Cliquez sur **OK**.

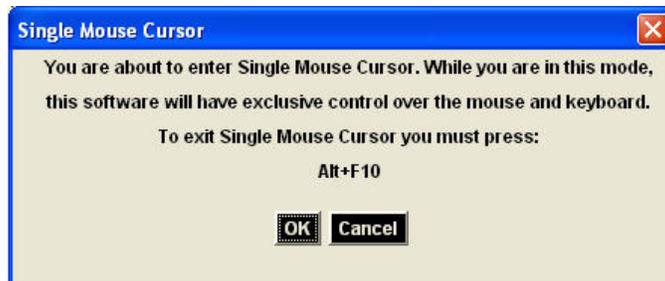


Figure 36 : Message du curseur de souris simple

2. Appuyez sur **Alt+F10** sur le clavier pour quitter le mode de souris simple.

Standard

Il s'agit de l'algorithme de synchronisation standard de la souris utilisant les positions relatives de la souris. Le mode souris Standard requiert que l'option d'accélération soit désactivée et que les autres paramètres de souris soient configurés correctement afin que la souris du client et celle du serveur puissent restées synchronisées. Le mode souris Standard est le mode souris configuré par défaut.

Pour entrer dans le mode de souris Standard :

Sélectionnez **Mouse (Mouse) > Standard**.

Intelligent

En mode souris Intelligent, Dominion KX II peut détecter les paramètres de la souris cible et synchroniser les pointeurs de souris en conséquence, de manière à permettre à l'utilisateur de disposer d'une accélération de la souris au niveau du dispositif cible. Dans ce mode, le curseur de souris effectue une « danse » dans le coin gauche supérieur de l'écran et calcule l'accélération. Pour que ce mode fonctionne correctement, certaines conditions sont nécessaires.

Pour davantage d'informations sur le mode de souris Intelligent, consultez le *manuel d'utilisation Multi-Platform Client (MPC) de Raritan (Annexe B : Conditions applicables à la synchronisation intelligente de la souris)* disponible sur le site Web de Raritan <http://www.raritan.com/support/productdocumentation> ou sur le CD-ROM comportant les *manuels d'utilisation et les guides d'installation rapide de Raritan*, fourni avec le Dominion KX II.

Pour entrer dans le mode de souris Intelligent :

Sélectionnez **Mouse (Souris) > Intelligent**.

Absolute (Absolu)

Remarque : la synchronisation absolue de la souris est disponible uniquement dans le module d'interface pour ordinateurs dont l'option de médias virtuels est activée (D2CIM-VUSB).

Dans ce mode, des coordonnées absolues sont utilisées pour maintenir la synchronisation des pointeurs du client et du dispositif cible, même si l'accélération ou la vitesse du pointeur de la souris cible sont configurées sur des valeurs différentes. Ce mode est pris en charge sur les serveurs de ports USB ; la souris se déplace vers l'emplacement exact sur le serveur cible.

Pour entrer dans le mode de souris Absolu :

Sélectionnez **Mouse (Souris) > Absolute (Absolu)**.

Médias virtuels

Reportez-vous à [Média virtuels](#) pour obtenir des informations complètes sur la configuration et l'utilisation des médias virtuels.

Menu Outils

Options

Le menu Tools (Outils) vous permet de spécifier certaines options relatives à l'utilisation de Virtual KVM Client : la synchronisation de la souris en mode souris double, l'activation de la journalisation, le type de clavier, ainsi que le raccourci-clavier pour quitter le mode de résolution d'écran du dispositif cible.

Pour définir les options d'outils :

1. Sélectionnez **Tools (Outils) > Options**. La fenêtre Options s'affiche :

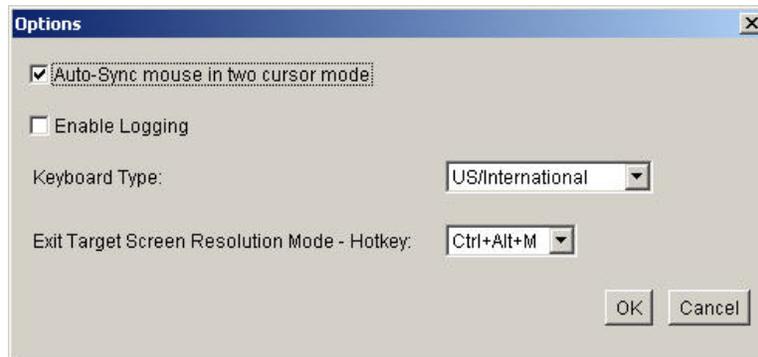


Figure 37 : Options (Outils)

2. Cochez les cases situées en regard des options que vous souhaitez activer :
 - **Auto Sync Mouse in Two Cursor Mode (Synch. auto de la souris en mode double)**. Sélectionnez cette option pour synchroniser automatiquement le curseur de la souris lorsque vous êtes en mode souris double.
 - **Enable Logging (Activer la journalisation)**. Utilisez cette option seulement si le Support technique Raritan vous le demande. Cette option permet de créer un fichier journal dans votre répertoire personnel.
3. **Sélectionnez le type de clavier (Keyboard Type) dans la liste déroulante (le cas échéant). Ces options incluent :**
 - US/International
 - Français (France)
 - Allemand (Allemagne)
 - Japonais
 - United Kingdom
 - Coréen (Corée)
4. **Exit Target Screen Resolution Mode (Quitter le mode de résolution d'écran de la cible) – Raccourci-clavier**. Lorsque vous accédez au mode de résolution d'écran du dispositif cible, l'affichage du serveur cible entre en mode plein écran et acquiert la même résolution que le serveur cible. Il s'agit du raccourci-clavier utilisé pour quitter ce mode ; sélectionnez-le dans la liste déroulante.
5. Cliquez sur **OK**.

Menu d'affichage

Affichage de la barre d'outils

Vous pouvez utiliser le Virtual KVM Client avec ou sans l'affichage de la barre d'outils.

Pour basculer entre l'affichage et le non-affichage de la barre d'outils :

Sélectionnez **View (Affichage) > View Toolbar (Afficher la barre d'outils)**.

Scaling (Mise à l'échelle)

La mise à l'échelle de votre écran cible permet d'afficher la totalité de l'écran du serveur cible. Cette fonction augmente ou réduit la taille de la vidéo cible pour qu'elle s'adapte à la taille de l'écran Virtual KVM Client et conserve le rapport hauteur/largeur de manière à permettre l'affichage de la totalité du bureau du serveur cible sans utiliser la barre de défilement.

Pour activer et désactiver la mise à l'échelle :

Sélectionnez **View (Affichage) > Scaling (Mise à l'échelle)**.

Résolution d'écran de la cible

Lorsque vous accédez au mode de résolution d'écran du dispositif cible, l'affichage du serveur cible entre en mode plein écran et acquiert la même résolution que le serveur cible. Le raccourci-clavier utilisé pour quitter ce mode est spécifié dans la boîte de dialogue Options (par défaut : **Ctrl+Alt+M**).

Pour entrer dans le mode de résolution d'écran de la cible :

Sélectionnez **View (Affichage) > Target Screen Resolution (Résolution d'écran de la cible)**.

Pour quitter le mode de résolution d'écran de la cible :

Appuyez sur le raccourci-clavier configuré dans Figure 37. Le raccourci-clavier par défaut est **Ctrl+Alt+M**.

Ecran Help Menu (Menu d'aide)

About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan)

Cette option de menu fournit les informations relatives à la version de Virtual KVM Client dans le cas où vous avez besoin de l'assistance technique de Raritan.

Pour obtenir les informations sur la version :

Sélectionnez **Help (Aide) > About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan)**.

Chapitre 7 : Médias virtuels

Présentation

Les médias virtuels étendent les fonctionnalités KVM en activant les serveurs cible sur les médias d'accès à distance à partir du PC client et des serveurs de fichiers réseau. Avec cette fonction, les médias montés sur le PC client et sur les serveurs de fichiers réseau sont pour l'essentiel montés virtuellement par le serveur cible. Le serveur cible peut ensuite lire et écrire sur ce média comme si ce dernier était physiquement connecté au serveur cible lui-même. Les médias virtuels peuvent inclure des lecteurs CD/DVD USB et internes, des dispositifs de stockage de masse USB ainsi que des images ISO (images disque).

Ils offrent la possibilité d'effectuer des tâches supplémentaires à distance, telles que :

- transférer des fichiers
- réaliser des diagnostics
- installer ou corriger des applications
- redémarrer des serveurs cible sur le réseau à l'aide d'une image ISO de CD de démarrage, accessible à partir du client
- procéder à l'installation du système d'exploitation

Cette commande KVM évoluée permet de supprimer la majorité des trajets vers le centre de données et d'économiser du temps et de l'argent, augmentant ainsi considérablement la puissance du média virtuel.

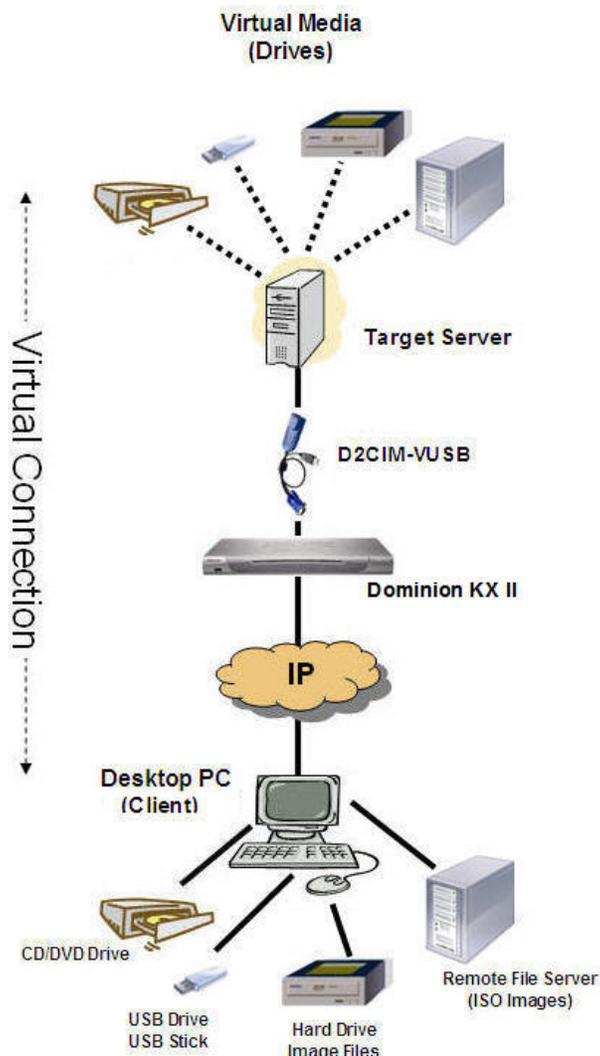


Figure 38 : Connexion à un média virtuel

Conditions requises pour l'utilisation des médias virtuels

Les conditions suivantes doivent être remplies pour pouvoir utiliser un média virtuel :

Modèles

- Pour les utilisateurs qui requièrent l'accès aux médias virtuels, des autorisations KX doivent être configurées pour permettre l'accès aux ports concernés ainsi que l'accès aux médias virtuels de ces ports (Autorisations des ports d'accès aux médias virtuels). Les autorisations d'accès aux ports sont définies au niveau du groupe ; veuillez vous reporter à [Configuration des autorisations d'accès aux ports](#) pour de plus amples informations.
- (Facultatif) Si vous souhaitez utiliser PC-Share, l'option [Mode de partage MV](#) doit également être activée à la page des paramètres de sécurité.

Ordinateur client

- Certaines options de média virtuel nécessitent des droits d'administrateur sur le PC client (par ex., redirection de la totalité des lecteurs).

*Remarque : avec Microsoft Vista, vous devez **désactiver** l'option User Account Control (Gestion des comptes utilisateur) : Control Panel (Panneau de configuration) > User Accounts (Comptes utilisateur) > User Account Control (Gestion des comptes utilisateur) > turn off (désactiver).*

- Les ports USB 2.0 sont rapides et préférables.

Serveur Cible

- Les serveurs cible doivent prendre en charge les lecteurs connectés USB.
- Toutes les interconnexions récentes doivent être installées sur les serveurs cible exécutant Windows 2000.

Utilisation des médias virtuels

Grâce à la fonction de média virtuel de Dominion KX II, vous pouvez monter jusqu'à deux lecteurs (de différents types). Ces lecteurs sont accessibles pendant toute la *durée* de la session KVM.

Par exemple, vous pouvez monter un CD-ROM spécifique, l'utiliser puis le déconnecter lorsque vous avez terminé. Néanmoins, le « canal » du CD-ROM virtuel demeure ouvert afin que vous puissiez monter un autre CD-ROM virtuellement. Ces « canaux » de média virtuel restent ouverts jusqu'à la fermeture de la session KVM.

Pour utiliser un média virtuel :

1. Connectez/reliez le média au serveur de fichiers réseau ou client auquel vous souhaitez accéder à partir du serveur cible. Ceci est la première étape à effectuer et elle doit se dérouler *avant* de tenter d'accéder à ce média.
2. Vérifiez que les [conditions requises](#) sont correctement remplies.
3. **(File server ISO images only) (Images ISO de serveur de fichiers uniquement)** Si vous projetez d'accéder à des images ISO de serveur de fichiers, identifiez ces images et ces serveurs de fichiers par le biais de la console distante de Dominion KX II [Configuration du serveur de fichiers](#).
4. [Ouvrir une session KVM](#) par l'intermédiaire du serveur cible adéquat.
5. Connectez-vous au média virtuel.

POUR :	SELECTIONNEZ CETTE OPTION VM :
Lecteurs locaux	Connecter le lecteur
Lecteurs de CD/DVD locaux	Connecter l'image ISO/CD-ROM
Images ISO	Connecter l'image ISO/CD-ROM
Images ISO de serveur de fichiers	Connecter l'image ISO/CD-ROM

6. Une fois les tâches effectuées, [déconnectez du média virtuel](#).

Ouvrir une session KVM

Pour ouvrir une session KVM :

1. Ouvrez la page d'accès aux ports dans la console distante de Dominion KX II.

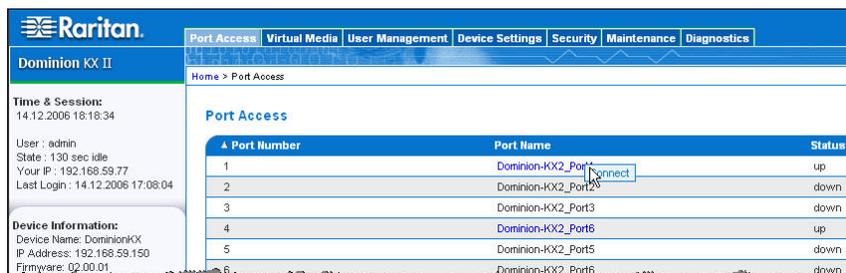


Figure 39 : Ouvrir une session KVM

2. Connectez-vous au serveur cible à partir de la page d'accès aux ports :
 - a. Cliquez sur le nom du port (**Port Name**) du serveur approprié.
 - b. Sélectionnez l'option **Connect (Connecter)** dans le menu d'action des ports.

Le serveur cible s'ouvre dans une fenêtre virtuelle ([Virtual KVM Client](#)).

Se connecter à un média virtuel

Lecteurs locaux

Cette option permet de monter un lecteur *entier* ; le lecteur de disque entier est *monté virtuellement* sur le serveur cible. Utilisez cette option pour les disques durs et externes uniquement car elle n'intègre pas les lecteurs réseau et les lecteurs CD-ROM ou DVD-ROM. C'est la seule option pour laquelle la fonction **Read-Write (Lecture/écriture)** est disponible.

Remarque : il se peut que les serveurs cible exécutant certaines versions du système d'exploitation Windows n'acceptent pas les nouvelles connexions de stockage de masse après qu'une partition de format NTFS (par ex., le disque C local) ait été redirigée vers eux. Si cela se produit, fermez la console distante de KX II puis connectez-la à nouveau avant de rediriger un autre dispositif de média virtuel. Si d'autres utilisateurs sont connectés au même serveur cible, ils doivent également fermer leurs connexions au serveur cible.

Pour accéder à un lecteur de l'ordinateur client :

1. A partir de Virtual KVM Client, sélectionnez **Virtual Media (Médias virtuels) > Connect Drive (Connecter le lecteur)**. La boîte de dialogue Map Virtual Media Drive (Mapper le lecteur de média virtuel) s'ouvre :

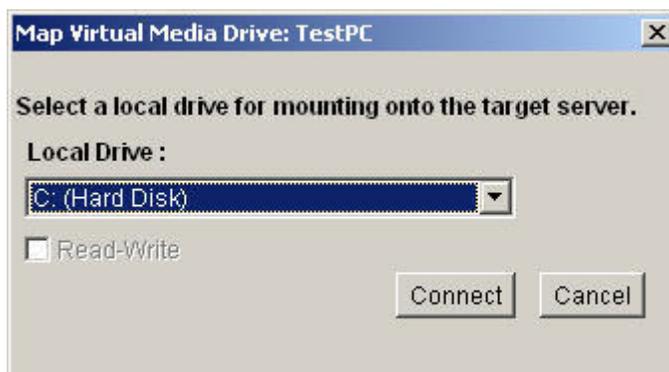


Figure 40 : Map Virtual Media Drive (Mapper le lecteur de média virtuel)

- Sélectionnez le lecteur dans la liste déroulante **Local Drive (Lecteur local)**.
- Si vous souhaitez bénéficier des fonctionnalités de lecture et d'écriture, cochez la case d'option **Read-Write (Lecture/écriture)**. Cette option est désactivée pour les lecteurs non amovibles. Veuillez vous reporter à [conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible](#) pour de plus amples informations. Une fois la case correspondante cochée, vous serez en mesure de lire ou écrire le disque USB connecté.

AVERTISSEMENT : l'activation de la fonction Lecture-écriture peut nuire au système ! L'accès simultané au même lecteur à partir de plusieurs entités peut entraîner une corruption des données. Si vous n'avez pas besoin de l'accès à la fonction d'écriture, ne cochez pas la case de cette option.

- Cliquez sur **Connect (Connecter)**. Le média est alors monté sur le serveur cible virtuellement. Vous pouvez accéder au média de la même manière que pour tout autre lecteur.

Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible

La fonction Lecture-écriture du média virtuel n'est pas disponible dans les situations suivantes :

- pour tous les disques durs
- lorsque le lecteur est protégé en écriture
- lorsque l'utilisateur ne dispose pas de l'autorisation de lecture-écriture :
 - l'accès aux autorisations d'accès aux ports est défini sur *None (Aucun)* ou *View (Afficher)*
 - l'accès des **médias virtuels** aux autorisations d'accès aux ports est défini sur *Read-Only (Lecture seule)* ou *Deny (Refuser)*

Images ISO/CD-ROM/DVD-ROM

Cette option permet de monter des images ISO, CD-ROM et DVD-ROM.

Pour accéder à une image ISO, CD-ROM ou DVD-ROM :

- A partir de Virtual KVM Client, sélectionnez **Virtual Media (Médias virtuels) > Connect CD-ROM/ISO Image (Connecter l'image ISO/CD-ROM)**. La boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image ISO/CD de média virtuel) s'ouvre :

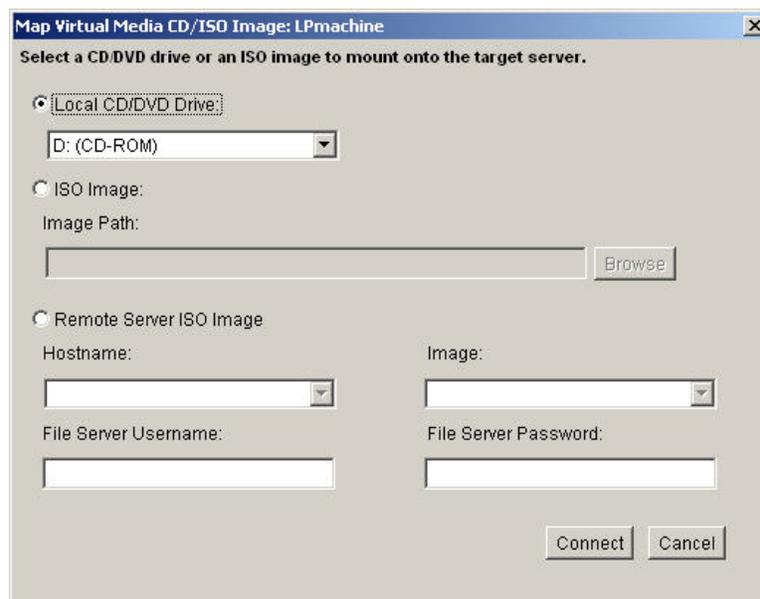


Figure 41 : Map Virtual Media CD/ISO Image (Mapper l'image ISO/CD de média virtuel)

2. Pour les lecteurs de CD-ROM ou DVD-ROM internes et externes :
 - a. sélectionnez l'option **Local CD/DVD Drive (Lecteur CD/DVD local)**.
 - b. Sélectionnez le lecteur dans la liste déroulante **Local CD/DVD Drive (Lecteur CD/DVD local)**. Tous les noms de lecteurs CD/DVD internes et externes sont générés dans la liste déroulante.
 - c. Cliquez sur **Connect (Connecter)**.
3. Pour les images ISO :
 - a. sélectionnez l'option **ISO Image (Image ISO)**. Utilisez cette option lorsque vous souhaitez accéder à une image disque de CD, de DVD ou de disque dur. Le format ISO est le seul format pris en charge.
 - b. Cliquez sur le bouton **Browse (Naviguer)**.
 - c. Localisez l'image disque que vous souhaitez utiliser, puis cliquez sur **Open (Ouvrir)**. Le chemin d'accès est généré dans le champ **Image Path (Chemin d'accès à l'image)**.
 - d. Cliquez sur **Connect (Connecter)**.
4. Pour les images ISO distantes d'un serveur de fichiers :
 - a. sélectionnez l'option **Remote Server ISO Image (Image ISO de serveur à distance)**.
 - b. Sélectionnez les options **Hostname (Nom d'hôte)** et **Image** à partir des listes déroulantes. Les serveurs de fichiers et les chemins d'accès aux images disponibles sont ceux que vous avez configurés via la page [Configuration du serveur de fichiers](#). Seuls les éléments que vous avez configurés à l'aide de la page de configuration des serveurs de fichiers de Dominion KX II figurent dans la liste déroulante.
 - c. **File Server Username** : nom d'utilisateur requis pour l'accès au serveur de fichiers.
 - d. **File Server Password** : mot de passe requis pour l'accès au serveur de fichiers (le champ est dissimulé à mesure que vous saisissez le texte).
 - e. Cliquez sur **Connect (Connecter)**.

Le média est alors monté sur le serveur cible virtuellement. Vous pouvez accéder au média de la même manière que pour tout autre lecteur.

Déconnexion du média virtuel

Pour déconnecter les lecteurs de média virtuel :

- pour les lecteurs locaux, sélectionnez **Virtual Media (Média virtuel) > Disconnect Drive (Déconnecter le lecteur)**
- pour les images ISO, CD et DVD, sélectionnez **Virtual Media (Média virtuel) > Disconnect CD-ROM/ISO Image (Déconnecter l'image ISO/CD-ROM)**

*Remarque : outre l'option **Disconnect (Déconnecter)** de déconnexion de média virtuel, le fait de fermer simplement la connexion KVM déconnecte également le média virtuel.*

Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement)

Remarque : Cette fonction est requise uniquement lors de l'utilisation d'un média virtuel pour l'accès aux images ISO du serveur de fichiers.

Utilisez la page de configuration relative aux serveurs de fichiers de la console distante de Dominion KX II pour spécifier le(s) serveur(s) de fichiers et les chemins d'accès aux images auxquelles vous souhaitez accéder à l'aide du média virtuel de Dominion KX II. Le(s) image(s) ISO de serveur(s) de fichiers spécifiées dans cette page seront alors disponibles à partir des listes déroulantes de **Remote Server ISO Image Hostname (Nom d'hôte d'image ISO de serveur de fichiers)** et **Image** ([Boîte de dialogue Map Virtual Media CD/ISO Image](#)).

Pour désigner les images ISO de serveur de fichiers pour l'accès au média virtuel :

1. sélectionnez **Virtual Media (Média virtuel)** dans Dominion KX II Remote Console (Console distante de Dominion KX II). La page de configuration des serveurs de fichiers s'ouvre :

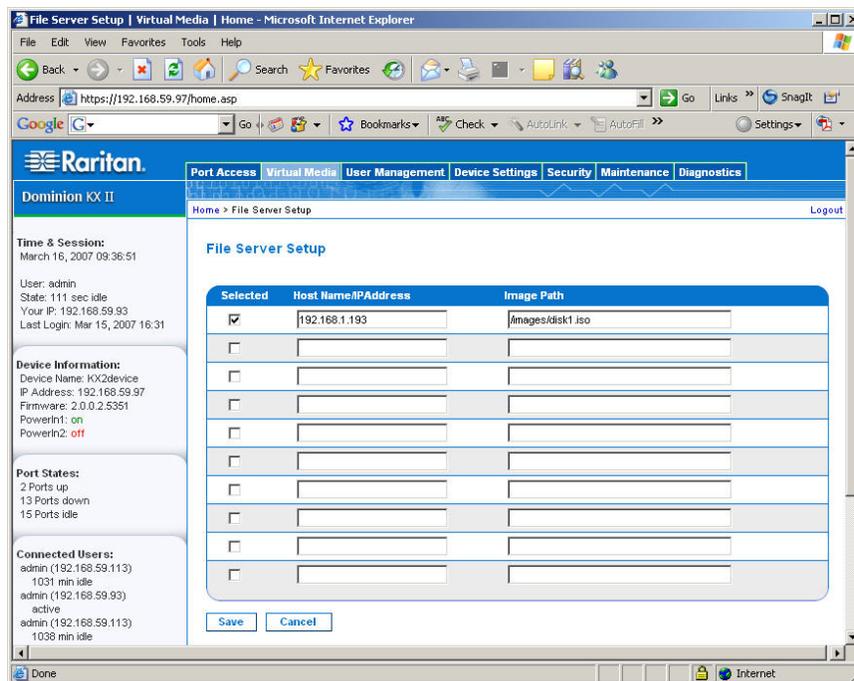


Figure 42 : Configuration des serveurs de fichiers

2. Entrez les informations relatives aux images ISO de serveur de fichiers auxquelles vous souhaitez accéder.
 - **Host Name (Nom d'hôte)/IP Address (Adresse IP)** : nom d'hôte ou adresse IP du serveur de fichiers.
 - **Image Path (Chemin d'accès des images)** : chemin d'accès complet à l'emplacement de l'image ISO.
3. Cochez la case **Selected (Sélectionné)** pour tous les médias auxquels vous souhaitez accéder en tant que médias virtuels.
4. Cliquez sur **Save (Enregistrer)**. Tous les médias que vous avez spécifiés peuvent désormais être sélectionnés dans la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO du média virtuel).

Pour quitter sans enregistrer les modifications :

cliquez sur Cancel (Annuler).

Chapitre 8 : User Management

Le menu User Management (Gestion des utilisateurs) est organisé comme suit : User List (liste des utilisateurs), Add New User (ajouter un nouvel utilisateur), User Group List (liste des groupes d'utilisateurs), Add New User Group (Ajouter un nouveau groupe d'utilisateurs), Change Password (modifier le mot de passe) et Authentication Settings (paramètres d'authentification).

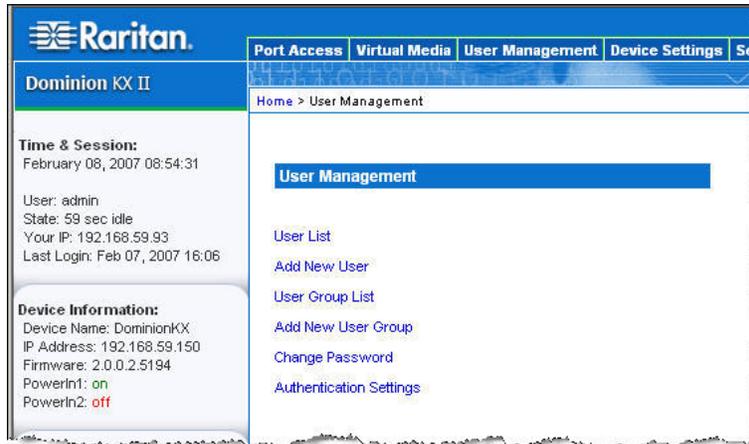


Figure 43 : Menu User Management (Gestion des utilisateurs)

UTILISEZ :	POUR
User List (Liste des utilisateurs)	Affiche une liste alphabétique de tous les utilisateurs ; permet d'ajouter, de modifier ou de supprimer des utilisateurs.
Ajouter un nouvel utilisateur	Permet d'ajouter de nouveaux utilisateurs et de modifier les informations utilisateur.
Liste des groupes d'utilisateurs	Affiche une liste alphabétique de tous les groupes d'utilisateurs ; permet d'ajouter, de modifier ou de supprimer des groupes d'utilisateurs.
Ajouter un nouveau groupe d'utilisateurs	Permet d'ajouter de nouveaux groupes d'utilisateurs et de modifier les informations sur les groupes d'utilisateurs.
Modifier le mot de passe	Permet de modifier le mot de passe d'un utilisateur spécifique.
Paramètres d'authentification	Permet de configurer le type d'authentification utilisé pour l'accès à Dominion KX II.

User List (Liste des utilisateurs)

La page User List (Liste des utilisateurs) affiche une liste de tous les utilisateurs, y compris leur nom d'utilisateur, leur nom complet et leur groupe d'utilisateurs. Cette liste peut être triée en fonction de n'importe quelle colonne, en cliquant sur le nom de la colonne. A partir de la page sur laquelle figure la liste des utilisateurs, vous avez la possibilité d'ajouter, de modifier ou de supprimer des utilisateurs.

Pour afficher la liste des utilisateurs :

Sélectionnez **User Management (Gestion des utilisateurs) > User List (Liste des utilisateurs)**.
La page de la liste des utilisateurs s'ouvre :

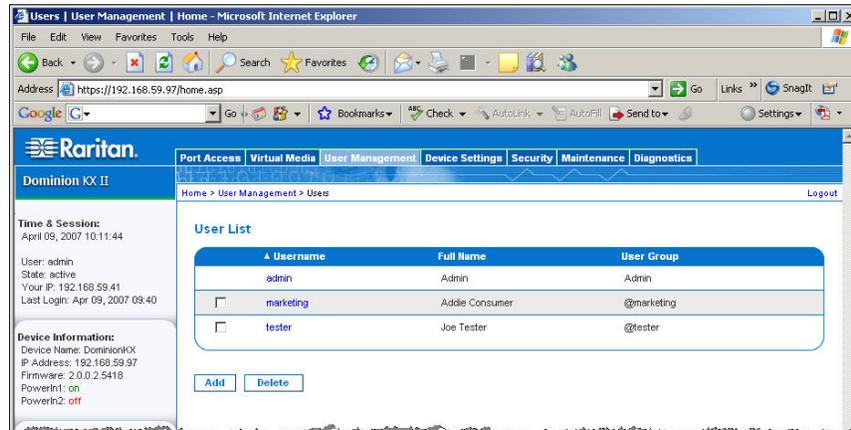


Figure 44 : User List (Liste des utilisateurs)

Pour ajouter un nouvel utilisateur :

Cliquez sur le bouton **Add (Ajouter)**. La page User (Utilisateur) s'ouvre : Pour obtenir des informations complètes sur la page des utilisateurs, reportez-vous à [Ajouter un nouvel utilisateur](#).

Pour modifier un utilisateur existant :

1. Localisez l'utilisateur parmi ceux qui figurent dans la liste.
2. Cliquez sur **Username (Nom d'utilisateur)**. La page User (Utilisateur) s'ouvre : Pour obtenir des informations complètes sur le processus de modification des utilisateurs, reportez-vous à [Modifier un utilisateur existant](#).

Pour supprimer un utilisateur :

1. Sélectionnez l'utilisateur parmi ceux qui figurent dans la liste en cochant la case située à gauche du nom d'utilisateur concerné.
2. Cliquez sur **Supprimer**.
3. Vous êtes invité à confirmer la suppression. Cliquez sur **OK**.

Ajouter un nouvel utilisateur

Il est recommandé de définir les groupes d'utilisateurs *avant* de créer les utilisateurs Dominion KX II, car si vous ajoutez un utilisateur, vous devez attribuer cet utilisateur à un groupe d'utilisateurs existant. Vous pouvez ajouter de nouveaux utilisateurs, modifier leurs informations et réactiver des utilisateurs dans la page des utilisateurs.

Remarque : un nom d'utilisateur peut être désactivé (la case **Active (Actif)** est désélectionnée) lorsque le nombre de tentatives de connexion qui ont échoué a atteint la limite définie dans l'écran des paramètres de sécurité. Reportez-vous à [Définition des autorisations](#) pour de plus amples informations.

Pour ajouter un nouvel utilisateur :

- Ouvrez la page des utilisateurs à l'aide de l'une des méthodes suivantes :
 - Sélectionnez **User Management (Gestion des utilisateurs) > Add New User (Ajouter un nouvel utilisateur)** ou
 - cliquez sur le bouton **Add (Ajouter)** dans la page de la liste des utilisateurs.

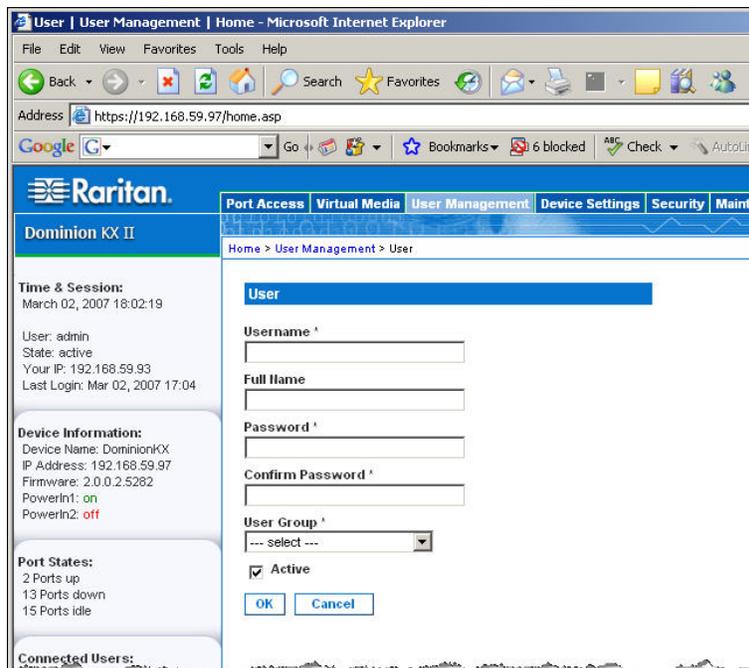


Figure 45 : Page User (Utilisateur)

- Saisissez un nom d'utilisateur unique dans le champ **Username (Nom d'utilisateur)** (16 caractères au maximum).
- Saisissez le nom complet de la personne dans le champ **Full Name (Nom complet)** (64 caractères au maximum).
- Entrez un mot de passe dans le champ **Password (Mot de passe)**, puis entrez-le à nouveau dans le champ **Confirm Password (Confirmer le mot de passe)** (64 caractères au maximum).
- Sélectionnez le groupe dans la liste déroulante des groupes d'utilisateurs (**User Group**). La liste contient tous les groupes que vous avez créés en plus des groupes par défaut fournis par le système [<Unknown (Inconnu)> (paramètre par défaut), Admin, Individual Group (Groupe individuel)]. Si vous ne souhaitez pas assigner cet utilisateur à un groupe d'utilisateurs existant, sélectionnez **Groupe individuel** dans la liste déroulante.

Pour des informations supplémentaires concernant les autorisations d'accès à un groupe individuel, reportez-vous à [Configurer des autorisations pour un groupe individuel](#).

- Pour activer cet utilisateur, cochez la case **Active (Actif)**. L'utilisateur par défaut est activé.
- Cliquez sur **OK**.

Modifier un utilisateur existant

Pour modifier un utilisateur existant :

1. Dans la page des utilisateurs (Figure 45), modifiez les champs appropriés. (Reportez-vous à [Ajouter un nouvel utilisateur](#) pour en savoir plus sur les méthodes d'accès à la page Utilisateur.)
2. Cliquez sur **OK**.

Liste des groupes d'utilisateurs

Les groupes d'utilisateurs sont utilisés avec une authentification distante et locale (par l'intermédiaire de RADIUS ou de LDAP). Il est recommandé de définir les groupes d'utilisateurs *avant* de créer les utilisateurs individuels, car si vous ajoutez un utilisateur, vous devez attribuer cet utilisateur à un groupe d'utilisateurs *existant*.

La page User Group List (Liste des groupes d'utilisateurs) affiche une liste de tous les groupes d'utilisateurs, ces derniers pouvant être triés dans l'ordre croissant ou décroissant en cliquant sur l'en-tête de colonne Group Name. A partir de la page sur laquelle figure la liste des utilisateurs, vous avez la possibilité d'ajouter, de modifier ou de supprimer des groupes d'utilisateurs.

Pour faire une liste des groupes d'utilisateurs :

Sélectionnez **User Management (Gestion des utilisateurs) > User Group List (Liste des groupes d'utilisateurs)**. La page de la liste des groupes d'utilisateurs s'ouvre :

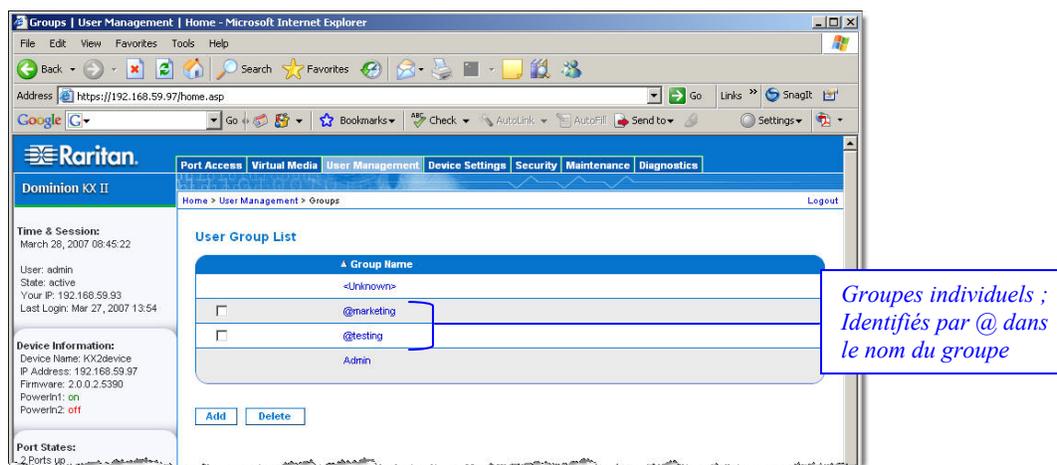


Figure 46 : Liste des groupes d'utilisateurs

Pour ajouter un nouveau groupe d'utilisateurs :

Cliquez sur le bouton **Add (Ajouter)**. La page Group (Groupe) s'ouvre. Pour obtenir des informations complètes sur la page des groupes, reportez-vous à [Ajouter un nouvel utilisateur](#).

Pour modifier un groupe d'utilisateurs existant :

1. Localisez le groupe d'utilisateur parmi ceux qui figurent dans la liste.
2. Cliquez sur Group Name (Nom du groupe). La page Group (Groupe) s'ouvre. Pour obtenir des informations complètes sur le processus de modification des groupes, reportez-vous à [Modifier un utilisateur existant](#).

Pour supprimer un groupe d'utilisateurs :

Important : avant de supprimer un groupe, assurez-vous qu'aucun utilisateur n'est affecté au groupe. Les utilisateurs affectés au groupe seront également supprimés.

Conseil : pour déterminer les utilisateurs d'un groupe particulier, triez la liste des utilisateurs (Figure 44) par groupe d'utilisateurs.

1. Sélectionnez un groupe parmi ceux qui figurent dans la liste en cochant la case située à gauche du nom de groupe.
 2. Cliquez sur **Supprimer**.
 3. Vous êtes invité à confirmer la suppression. Cliquez sur **OK**.
-

Ajouter un nouveau groupe d'utilisateurs

Pour ajouter un nouveau groupe d'utilisateurs :

- Ouvrez la page des groupes en utilisant l'une des méthodes suivantes :
 - Sélectionnez **User Management (Gestion des utilisateurs) > Add New User Group (Ajouter un nouveau groupe d'utilisateurs)** ou
 - cliquez sur le bouton **Add (Ajouter)** dans la page de la liste des groupes d'utilisateurs.

The screenshot shows the 'Group' configuration page in the Raritan Dominion KX II web interface. The page is organized into several sections:

- Group:** A text input field for 'Group Name'.
- Permissions:** A list of checkboxes for 'Device Settings', 'Diagnostics', 'Maintenance', 'PC-Share', 'Security', and 'User Management'.
- Port Permissions:** A table with columns for 'Port', 'Access', 'VM Access', and 'Power Control'. Each port (Dominion-KX2_Port1 to Port16) has dropdown menus for 'Access' (set to 'None') and 'VM Access' (set to 'Deny'), and a 'Power Control' dropdown (set to 'Deny').
- IP ACL:** A section for defining IP Access Control Lists with fields for 'Rule #', 'Starting IP', 'Ending IP', and 'Action' (set to 'ACCEPT'). Buttons for 'Append', 'Insert', 'Replace', and 'Delete' are provided.

At the bottom, there are 'OK' and 'Cancel' buttons, and a copyright notice: 'Copyright © 2007 Raritan Computer Inc.'

Figure 47 : Page Group (Groupe)

La page Groupe est organisée en plusieurs catégories : Group (Groupe), Permissions (Autorisations), Port Permissions (Autorisations d'accès aux ports), et IP ACL (LCA IP).

- Entrez un nom descriptif pour le nouveau groupe d'utilisateurs dans le champ **Group Name (Nom de groupe)**.
- Définissez les **Permissions (Autorisations)** pour le groupe. Cochez les cases situées en regard des autorisations que vous souhaitez assigner à *tous les utilisateurs appartenant à ce groupe*. Reportez-vous à [Définition des autorisations](#) pour de plus amples informations.
- Définissez les **autorisations d'accès aux ports**. Spécifiez les ports de serveur auxquels peuvent accéder les utilisateurs appartenant à ce groupe et le type d'accès. Reportez-vous à [Définition des autorisations](#) pour de plus amples informations.

5. **Définissez le champ LCA IP** (facultatif). Cette fonction limite l'accès au dispositif Dominion KX II en spécifiant les adresses IP ; elle s'applique **uniquement** aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste **Contrôle d'accès IP** qui s'applique à **toutes** les tentatives d'accès au dispositif (et est prioritaire).
6. Cliquez sur **OK**.

Remarque : MPC et le port de la console locale de Dominion KX II proposent plusieurs fonctions d'administration, qui ne sont destinées qu'aux membres du groupe ADMIN par défaut.

Configuration des autorisations

Important : la sélection de la case User Management (Gestion des utilisateurs) permet aux membres du groupe de modifier les autorisations de tous les utilisateurs, y compris les leurs. Accordez ces autorisations avec prudence.

AUTORISATION	DESCRIPTION
Paramètres du dispositif	Paramètres réseau, paramètres date/heure, configuration des ports (nom de canal, association d'alimentation), gestion des événements (SNMP, Syslog), configuration du serveur de fichiers du média virtuel
Diagnostics	Etat d'interface réseau, statistiques de réseaux, envoi d'une commande Ping à un hôte, détermination d'itinéraire jusqu'à un hôte, diagnostics KX
Maintenance	Base des données de sauvegarde et de restauration, mise à niveau du firmware, redémarrage
PC-Share	Accès simultané à la même cible par plusieurs utilisateurs
Sécurité	Certificat SSL, paramètres de sécurité (VM Share, PC-Share), LCA IP
User Management	Gestion des utilisateurs et des groupes d'utilisateurs, authentification à distance (LDAP/RADIUS), paramètres de connexion

Configuration des autorisations d'accès aux ports

Pour chaque port serveur, vous pouvez spécifier le type d'accès, le type d'accès au média virtuel et la gestion de l'alimentation électrique. Veuillez noter que le paramètre par défaut de toutes les autorisations est désactivé.

ACCES		ACCES AU MEDIA VIRTUEL		GESTION DE L'ALIMENTATION	
Option	Description	Option	Description	Option	Description
None* (Aucun)	Accès refusé intégralement	Deny* (Refuser)	L'autorisation d'accès au média virtuel est entièrement refusée pour le port	Deny* (Refuser)	Accès refusé intégralement
View	Afficher (sans pour autant interagir avec) le serveur cible connecté	Read-Only (Lecture seule)	L'accès au média virtuel est limité à l'accès en lecture uniquement	Accès	Accès total
Control (Contrôle)	Contrôle le serveur cible connecté	Read-Write (Lecture-écriture)	Accès total (en lecture, en écriture) au média virtuel		

* Paramètre par défaut

Conseil : utilisez les cases pour configurer chacun des ports avec les mêmes autorisations rapidement.

LCA IP de groupes (Liste de contrôle d'accès)

Important : Soyez prudent lorsque vous utilisez le contrôle d'accès par adresse IP applicable à des groupes. Il est possible que votre accès à Dominion KX II soit bloqué si votre adresse IP se trouve dans la plage des adresses à laquelle l'accès a été refusé.

Cette fonction limite l'accès du dispositif Dominion KX II aux utilisateurs appartenant au groupe sélectionné par le biais de leur adresse IP. Cette fonction s'applique **uniquement** aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste de contrôle d'accès par IP qui s'applique à **toutes** les tentatives d'accès au dispositif sans exception et qui est traitée en premier (donc prioritaire). Reportez-vous à [Contrôle d'accès IP](#) pour de plus amples informations.

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de Dominion KX II. Lorsque vous créez une liste de contrôle d'accès, si 127.0.0.1 se trouve dans la plage des adresses IP bloquées, vous n'aurez plus accès au port local de Dominion KX II.

Utilisez le champ IP ACL (LCA IP) dans la page des groupes pour ajouter, insérer, remplacer et supprimer les règles de contrôle d'accès applicables aux groupes.

Rule #	Starting IP	Ending IP	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▾

Figure 48 : Liste de contrôle d'accès par adresse IP applicable à des groupes

Pour ajouter (modifier) des règles :

1. Saisissez la première adresse IP de la plage définie dans le champ **Starting IP (Adresse IP de départ)**.
2. Entrez la dernière adresse IP de la plage définie dans le champ **Ending IP (Adresse IP de fin)**.
3. Sélectionnez l'**Action** dans la liste des options disponibles.
 - **Accept (Accepter)**. Les adresses IP avec la mention accepter sont autorisées à accéder au dispositif Dominion KX II.
 - **Drop (Refuser)**. Les adresses IP avec la mention refuser se voient refuser l'accès au dispositif Dominion KX II.
4. Cliquez sur **Append (Modifier)**. La règle est ajoutée au bas de la liste des règles.
5. Répétez les étapes 1 à 4 pour chacune des règles que vous souhaitez valider.

Pour insérer une règle :

1. Tapez une **règle (Rule #)**. Un numéro de règle est requis lorsque vous utilisez la commande Insérer.
2. Renseignez les champs des **adresses IP de départ** et de fin.
3. Sélectionnez l'**action** dans la liste déroulante.
4. Cliquez sur **Insert (Insérer)**. Si le numéro de règle que vous venez de taper est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont déplacées d'une rangée vers le bas.

Pour remplacer une règle :

1. Spécifiez le numéro de la **règle** que vous souhaitez remplacer.
2. Renseignez les champs des **adresses IP de départ** et de fin.
3. Sélectionnez l'**action** dans la liste déroulante.
4. Cliquez sur **Replace (Remplacer)**. Votre nouvelle règle remplace la règle d'origine dont le numéro est le même.

Pour supprimer une règle :

1. Spécifiez le numéro de la **règle** que vous souhaitez supprimer.
2. Cliquez sur **Supprimer**.
3. Vous êtes invité à confirmer la suppression. Cliquez sur **OK**.

Important : les règles LCA sont évaluées selon l'ordre dans lequel elles sont répertoriées. Par exemple si, dans l'exemple ci-dessus, les deux règles LCA étaient inversées, Dominion n'accepterait aucune communication.

IP ACL			
Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▾
<input type="button" value="Append"/>	<input type="button" value="Insert"/>	<input type="button" value="Replace"/>	<input type="button" value="Delete"/>

Figure 49 : Exemple de LCA IP

Conseil : les numéros de règles vous permettent de mieux contrôler l'ordre de création des règles.

Modifier un groupe d'utilisateurs existant

Remarque : toutes les autorisations relatives au groupe Admin sont activées (et ne peuvent pas être modifiées).

Pour modifier un groupe d'utilisateurs existant :

1. A partir de la page de groupe, modifiez les champs appropriés puis définissez les autorisations adéquates.

The screenshot shows the Raritan web interface for configuring a group. The main content area is titled 'Group' and shows the following configuration options:

- Group Name:** @marketing
- Permissions:** A list of checkboxes for Device Settings, Diagnostics, Maintenance, PC-Share, Security, and User Management.
- Port Permissions:** A table with columns for Port, Access, VM Access, and Power Control. Each port (Dominion-KX2_Port1 to Port16) has a dropdown menu for Access (set to 'None'), VM Access (set to 'Deny'), and Power Control (set to 'Deny').
- IP ACL:** A section for defining IP Access Control Lists with fields for Rule #, Starting IP, Ending IP, and Action (set to 'ACCEPT').

At the bottom of the page, there is a copyright notice: Copyright © 2007 Raritan Computer Inc.

Figure 50 : Modifier un groupe

2. Définissez les **Permissions (Autorisations)** pour le groupe. Cochez les cases situées en regard des autorisations que vous souhaitez assigner à *tous les utilisateurs appartenant à ce groupe*. Reportez-vous à [Définition des autorisations](#) pour de plus amples informations.
3. Définissez les **autorisations d'accès aux ports**. Spécifiez les ports de serveur auxquels peuvent accéder les utilisateurs appartenant à ce groupe et le type d'accès. Reportez-vous à [Définition des autorisations](#) pour de plus amples informations.
4. Configurez la liste de contrôle d'accès IP (**IP ACL**) (facultatif). Cette fonction limite l'accès au dispositif Dominion KX II par le biais de la spécification des adresses IP. Reportez-vous à [Liste de contrôle d'accès IP applicable à des groupes](#) pour de plus amples informations.
5. Cliquez sur **OK**.

Configurer des autorisations pour un groupe individuel

Pour configurer des autorisations pour un groupe d'utilisateurs individuel :

1. Localisez l'utilisateur parmi les groupes qui figurent dans la liste. Les groupes individuels peuvent être identifiés par le signe @ présent dans le **Nom de groupe**.
2. Cliquez sur **Group Name (Nom du groupe)**. La page Group (Groupe) (Figure 50) s'ouvre.
3. Sélectionnez les autorisations appropriées.
4. Cliquez sur **OK**.

Modifier le mot de passe

Pour modifier votre mot de passe :

1. Sélectionnez **User Management (Gestion des utilisateurs) > Change Password (Modifier le mot de passe)**. La page de modification du mot de passe s'ouvre :

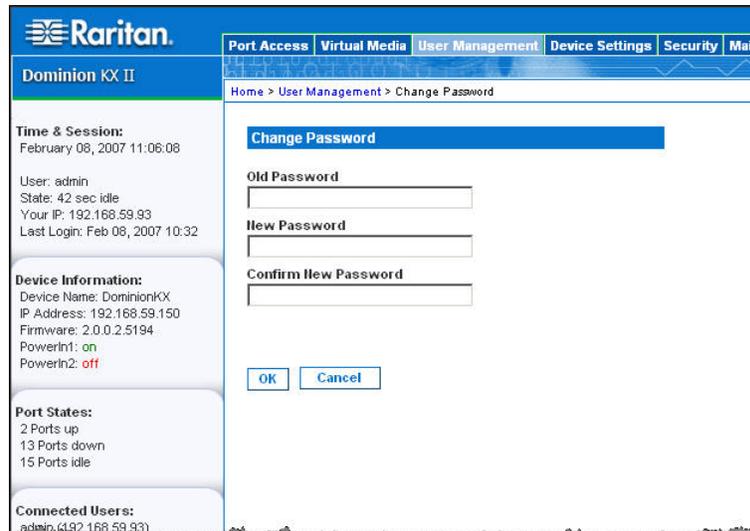


Figure 51 : Modifier le mot de passe

2. Saisissez votre mot de passe actuel dans le champ **Old Password (Ancien mot de passe)**.
3. Entrez un nouveau mot de passe dans le champ **New Password (Nouveau mot de passe)**, puis entrez-le à nouveau dans le champ **Confirm New Password (Confirmer le nouveau mot de passe)**. Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques (présents sur un clavier anglais) et [caractères spéciaux](#).
4. Cliquez sur **OK**.
5. Un message doit s'afficher pour confirmer la réussite de la modification du mot de passe. Cliquez sur **OK**.

Remarque : si des mots de passe sécurisés sont utilisés, cette page affiche des informations sur le format requis pour les mots de passe. Pour de plus amples informations concernant les mots de passe et les mots de passe sécurisés, reportez-vous à [Paramètres de sécurité - Mots de passe sécurisés](#).

Paramètres d'authentification

A partir de la page des paramètres d'authentification, vous pouvez configurer le type d'authentification utilisé pour l'accès à Dominion KX II. Reportez-vous à [Authentification et autorisation](#) pour en savoir plus sur le fonctionnement des processus d'authentification et d'autorisation, ainsi que sur leurs disparités.

Remarque : même si vous sélectionnez l'option d'authentification à distance (LDAP ou RADIUS), l'authentification locale est toujours utilisée.

Pour configurer une authentification :

1. Sélectionnez **User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification)**. La page des paramètres d'authentification s'ouvre :

The screenshot shows the 'Authentication Settings' page for a Raritan Dominion KX II device. The page is organized into several sections:

- Time & Session:** Shows the current date and time (March 01, 2007 16:54:46), user information (admin), and session details (State: 162 sec idle, Your IP: 192.168.59.93, Last Login: Mar 01, 2007 16:06).
- Device Information:** Lists device name (DominionKX), IP address (192.168.59.97), firmware version (2.0.0.2.5274), and power status (PowerIn1: on, PowerIn2: off).
- Port States:** Displays the status of ports (1 up, 14 down, 15 idle).
- Connected Users:** Shows the current user (admin) and idle time (3 min).
- Help - User Guide** and **Favorite Devices** (listing other devices like Baskers KX II, Janets KXII, and Prasannas KX II).
- Authentication Settings:**
 - Local Authentication:** Selected. Includes fields for Primary and Secondary LDAP Servers, Secret Phrase, Confirm Secret Phrase, and an option to Enable Secure LDAP. The Port is set to 389 and Secure LDAP Port to 636. A Certificate File field with a 'Browse...' button is also present.
 - RADIUS:** Unselected. Includes fields for Primary and Secondary RADIUS Servers, Shared Secret, Authentication Port (1812), Accounting Port (1813), Timeout (1 second), and Retries (3).
 - Global Authentication Type:** Set to PAP.
- Buttons:** OK, Reset To Defaults, and Cancel.

Copyright © 2007 Raritan Computer Inc.

Figure 52 : Paramètres d'authentification

2. Sélectionnez l'option de protocole d'authentification que vous souhaitez utiliser (**Authentification locale, LDAP** ou **RADIUS**). La sélection de l'option LDAP a pour effet d'activer les champs LDAP restants ; celle de l'option RADIUS d'activer les champs RADIUS restants.
3. Si vous sélectionnez **Local Authentication (Authentification locale)**, passez à l'étape 6.
4. Si vous sélectionnez **LDAP**, lisez la section intitulée [Mise en application de l'authentification LDAP](#) pour obtenir des informations sur la façon de remplir les champs dans la section LDAP de la page des paramètres d'authentification.
5. Si vous sélectionnez **RADIUS**, lisez la section intitulée [Mise en application de l'authentification RADIUS](#) pour obtenir des informations sur la façon de remplir les champs dans la section RADIUS de la page des paramètres d'authentification.
6. Lorsque l'opération est terminée, cliquez sur **OK** pour enregistrer les opérations.

Pour quitter sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour réinitialiser les paramètres usine :

Cliquez sur le bouton **Reset to Defaults (Restaurer les paramètres par défaut)**.

Mise en application de l'authentification à distance LDAP

LDAP (Lightweight Directory Access Protocol) qui signifie protocole léger d'accès aux annuaires est un protocole de mise en réseau pour la requête et la modification des services d'annuaires fonctionnant sur TCP/IP. Un client démarre une session LDAP en se connectant à un serveur LDAP (le port TCP par défaut est 389). Le client envoie ensuite les demandes de fonctionnement au serveur, et le serveur envoie les réponses en retour.

Rappel : Microsoft Active Directory fonctionne de manière native comme un serveur d'authentification LDAP.

Pour utiliser le protocole d'authentification LDAP, renseignez les informations suivantes :

LDAP

Primary LDAP Server

Secondary LDAP Server

Secret Phrase

Confirm Secret Phrase

Enable Secure LDAP

Port

389

Secure LDAP Port

636

Certificate File

Browse...

DII of Administrative User

User Search DII

Type of External LDAP Server

Generic LDAP server

Active Directory Domain

Figure 53 : Paramètres d'authentification (LDAP)

1. Tapez l'adresse IP ou le nom DNS de votre serveur d'authentification LDAP à distance dans le champ **Primary LDAP Server (Serveur LDAP principal)**. Une fois l'option **Enable Secure LDAP (Activer le LDAP sécurisé)** sélectionnée, le nom DNS doit être utilisé.
2. (Facultatif) Tapez l'adresse IP ou le nom DNS de votre serveur LDAP de sauvegarde dans le champ **Secondary LDAP Server (Serveur LDAP secondaire)**. Une fois l'option **Enable Secure LDAP (Activer le LDAP sécurisé)** sélectionnée, le nom DNS doit être utilisé. Veuillez noter que les champs restants intègrent les mêmes paramètres que le champ du **serveur LDAP principal**.
3. Tapez le mot de passe secret requis pour le serveur afin de le comparer à celui du serveur d'authentification à distance dans le champ **Secret Phrase (Expression secrète)**, puis entrez-le de nouveau dans **Confirm Secret Phrase (Vérifier l'expression secrète)**.
4. Cochez la case **Enable Secure LDAP (Activer le LDAP sécurisé)** si vous souhaitez utiliser le protocole SSL ; le champ **Secure LDAP Port (Sécuriser le port LDAP)** est activé. Le protocole de sécurité SSL est un protocole de cryptage qui permet à Dominion KX II de communiquer en toute sécurité avec le serveur LDAP.
5. Le **port** par défaut est 389. Utilisez le port LDAP TCP standard ou spécifiez un autre port.

6. Le **port LDAP sécurisé** par défaut est le port 636. Utilisez le port par défaut ou spécifiez un autre port. Ce champ est activé lorsque la case Enable Secure LDAP (Activer le LDAP sécurisé) est cochée.
7. **Fichier du certificat.** Consultez l'administrateur de votre serveur d'authentification pour obtenir le fichier de certificat de l'AC au format Base64 codé X-509 pour le serveur LDAP. Utilisez le bouton Browse (Naviguer) pour localiser le fichier du certificat. Ce champ est activé lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée.
8. **ND d'utilisateur administratif.** Correspond à un nom d'utilisateur administratif spécifique ; consultez l'administrateur de votre serveur d'authentification pour connaître les valeurs appropriées à saisir dans ce champ. Exemple de valeur de ND d'utilisateur administratif : « cn=Administrateur,dc=Utilisateurs,dc=testradius,dc=com ».
9. **ND de recherche d'utilisateur.** décrit le nom soumis à l'authentification LDAP et l'emplacement de la base de données où doit débiter la recherche du ND de base spécifié. Exemple de valeur de recherche de base : « cn=Utilisateurs,dc=raritan,dc=com ». Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ces champs.
10. **Type de serveur LDAP externe.** Sélectionnez-le parmi les options disponibles.
 - **Serveur LDAP générique.**
 - **Active Directory de Microsoft.** Active Directory est une mise en application des services d'annuaires LDAP par Microsoft pour être utilisés dans les environnements Windows.
11. **Domaine d'Active Directory.** Saisissez le nom du domaine d'Active Directory.

Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory

Dominion KX II prend en charge l'authentification des utilisateurs auprès d'Active Directory (AD) sans qu'il soit nécessaire de définir les utilisateurs localement au niveau de KX II. Les comptes et mots de passe des utilisateurs Active Directory peuvent ainsi être gérés *exclusivement* au niveau du serveur AD. L'autorisation et les droits des utilisateurs AD sont contrôlés et administrés par le biais de stratégies classiques dans KX II et de droits appliqués localement à des groupes d'utilisateurs AD importés dans KX II.

Remarque : si vous êtes déjà client de Raritan, Inc. et que vous avez configuré le serveur Active Directory en modifiant le schéma AD, Dominion KX II prend toujours en charge cette configuration et il ne vous est pas nécessaire d'effectuer les opérations suivantes. Pour obtenir des informations sur la mise à jour du schéma AD LDAP, reportez-vous à [Annexe B : Mise à jour du schéma LDAP](#).

Pour activer le serveur AD sur Dominion KX II :

1. A l'aide de Dominion KX II, créez des groupes spéciaux et attribuez-leur les droits et privilèges appropriés. Par exemple, créez des groupes tels que : KVM_Admin, KVM_Operator.
2. Sur le serveur Active Directory, créez d'autres groupes portant les *mêmes* noms qu'à l'étape précédente.
3. Sur le serveur AD, affectez les groupes créés aux utilisateurs de Dominion KX II.
4. A partir de Dominion KX II, activez et configurez le serveur AD comme il se doit. Veuillez vous reporter à [Mise en application de l'authentification LDAP](#).

Remarques importantes :

- Le nom de groupe est sensible à la casse.
- Dominion KX II propose les groupes par défaut suivants qui ne peuvent pas être modifiés ni supprimés : Admin et <Unknown>. Vérifiez que le serveur Active Directory n'utilise pas les mêmes noms de groupe.
- Si les informations de groupe retournées par le serveur Active Directory ne correspondent pas à une configuration de groupe KX II, Dominion KX II attribue automatiquement le groupe <Unknown> aux utilisateurs qui ont réussi à s'authentifier.

Mise en application de l'authentification à distance RADIUS

RADIUS est un service utilisateur d'authentification à distance. C'est un protocole d'authentification, d'autorisation et de gestion destiné aux applications d'accès aux réseaux.

Pour utiliser le protocole d'authentification RADIUS :

RADIUS

Primary Radius Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary Radius Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type

PAP ▼

Figure 54 : Ecran Authentication Settings (Paramètres d'authentification)

1. Saisissez l'adresse IP des serveurs d'authentification à distance principal et secondaire (facultatif) que vous utilisez dans les champs respectifs **Primary Radius Server (Serveur Radius principal)** et **Secondary Radius Server (Serveur Radius secondaire)**.
2. Entrez le mot de passe secret du serveur pour l'authentification (dans les champs communs **Shared Secret (Secret partagé)**). Le secret partagé est constitué d'une chaîne de caractères devant être connus à la fois par le serveur Dominion KX II et le serveur RADIUS afin de leur permettre de communiquer en toute sécurité. Il correspond à un mot de passe essentiellement.
3. **Port d'authentification.** Le port d'authentification par défaut est 1812 ; modifiez-le tel que requis.
4. **Port de gestion.** Le port de gestion par défaut est 1813 ; modifiez-le tel que requis.
5. **Délai d'attente (en secondes).** Le délai d'attente par défaut est de 1 seconde ; modifiez-le tel que requis. Le délai d'attente correspond au laps de temps utilisé par Dominion KX II pour obtenir une réponse du serveur RADIUS avant d'envoyer une autre requête d'authentification.
6. **Tentatives d'envoi.** Le nombre de tentatives d'envoi par défaut est de 3 ; modifiez-le tel que requis. Il s'agit du nombre de tentatives accordées à Dominion KX II pour envoyer une requête d'authentification au serveur RADIUS.

7. **Type d'authentification global.** Sélectionnez User List (Liste des utilisateurs) parmi les options de la liste déroulante.
- **PAP.** En mode PAP, les mots de passe sont envoyés en texte brut. Le mode PAP n'est pas interactif ; le nom d'utilisateur et le mot de passe sont envoyés en un ensemble unique de données une fois la connexion établie, et non sous la forme d'une invite de connexion suivie de l'attente d'une réponse.
 - **CHAP.** L'authentification CHAP peut être requise par le serveur à n'importe quel moment. Le protocole CHAP est plus sûr que le mode PAP.

Renvoi des informations relatives aux groupes d'utilisateurs par l'intermédiaire du RADIUS

Lorsque la demande d'authentification RADIUS est acceptée, le dispositif Dominion KX II détermine les autorisations accordées à un utilisateur donné en fonction des autorisations du groupe auquel appartient l'utilisateur.

Votre serveur RADIUS distant peut fournir ces noms de groupes d'utilisateurs en retournant un attribut, mis en application comme un *FILTER-ID (ID FILTRE)* RADIUS. Le format du *FILTER-ID (ID FILTRE)* doit être le suivant :

```
Raritan :G{NOM_GROUPE}
```

NOM_GROUPE est une chaîne de caractères indiquant le nom du groupe auquel l'utilisateur appartient.

Caractéristiques des échanges de communication RADIUS

L'unité Dominion KX II envoie les attributs RADIUS suivants à votre serveur RADIUS :

ATTRIBUT	DONNEES
CONNEXION	
Demande d'accès (1)	
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-IP-Address (Adresse IP NAS) (4)	L'adresse IP de l'unité Dominion KX II.
Nom d'utilisateur (1)	Nom d'utilisateur saisi dans l'écran de connexion
Acct-Session-ID (44)	ID session pour la gestion
Mot de passe d'utilisateur (2)	Mot de passe crypté.
Demande de gestion(4)	
Acct-Status (40)	Start(1) – Démarre la gestion.
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0
NAS-IP-Address (Adresse IP NAS) (4)	L'adresse IP de l'unité Dominion KX II.
Nom d'utilisateur (1)	Nom d'utilisateur saisi dans l'écran de connexion
Acct-Session-ID (44)	ID session pour la gestion
DECONNEXION	
Demande de gestion(4)	
Acct-Status (40)	Stop(2) – Met fin à la gestion
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0
NAS-IP-Address (Adresse IP NAS) (4)	L'adresse IP de l'unité Dominion KX II.
Nom d'utilisateur (1)	Nom d'utilisateur saisi dans l'écran de connexion
Acct-Session-ID (44)	ID session pour la gestion

Chapitre 9 : Gestion Des Dispositifs

Le menu relatif aux paramètres du dispositif est organisé comme suit : Network (Réseau), Date/Time (Date/heure), Event Management (Settings and Destinations) [Gestion des événements (Paramètres et destinations)], Power Supply Setup (Configuration de l'alimentation électrique), Port Configuration (Configuration des ports) et Local Port Settings (Paramètres du port local) (Dominion KX II Local Console uniquement).

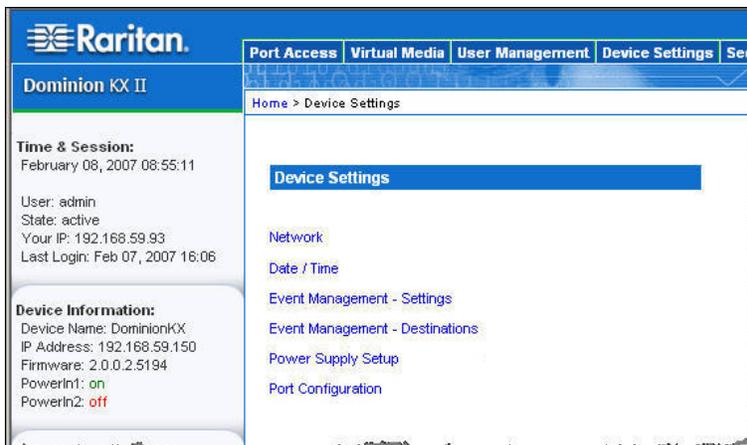


Figure 55 : Menu relatif aux paramètres du dispositif

UTILISEZ :	POUR
Réseau	Personnaliser la configuration réseau de Dominion KX II.
Date/heure	Définir la date, l'heure, le fuseau horaire et le protocole de temps du réseau (NTP).
Gestion des événements – Paramètres	Configurer SNMP et Syslog.
Gestion des événements – Destinations	Sélectionner les événements système devant être suivis et déterminer l'endroit où envoyer ces informations.
Configuration de l'alimentation	Configurer la détection automatique des alimentations de Dominion KX II.
Configuration des ports	Configurer les ports KVM, les CIM d'alimentation et les prises.
Local Port Settings (Paramètres du port local)	Configurer le port local ; <i>Dominion KX II Local Console uniquement.</i>

Menu Network Settings (Paramètres réseau)

Utilisez la page des paramètres réseau pour personnaliser la configuration du réseau (par ex., adresse IP, port de détection et paramètres de l'interface LAN) de votre unité Dominion KX II.

Important : vous devez redémarrer Dominion KX II pour que les nouveaux paramètres réseau soient pris en compte. avant de modifier les valeurs de configuration réseau, assurez-vous qu'il n'existe pas d'autres connexions utilisateur actives sur le dispositif ; toutes les connexions seront interrompues lors du redémarrage de l'unité KX II.

En gros, il existe deux façons de configurer vos paramètres IP :

- **Aucun.** Cette option est recommandée (**IP statique**). Comme Dominion KX II fait partie intégrante de l'infrastructure de votre réseau, vous ne voulez probablement pas que son adresse IP change fréquemment. Cette option vous permet de définir les paramètres de réseau.
- **DHCP.** L'adresse IP est assignée automatiquement par un serveur DHCP.

Pour modifier la configuration de réseau :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Network (Réseau)**. La page des paramètres réseau s'ouvre.

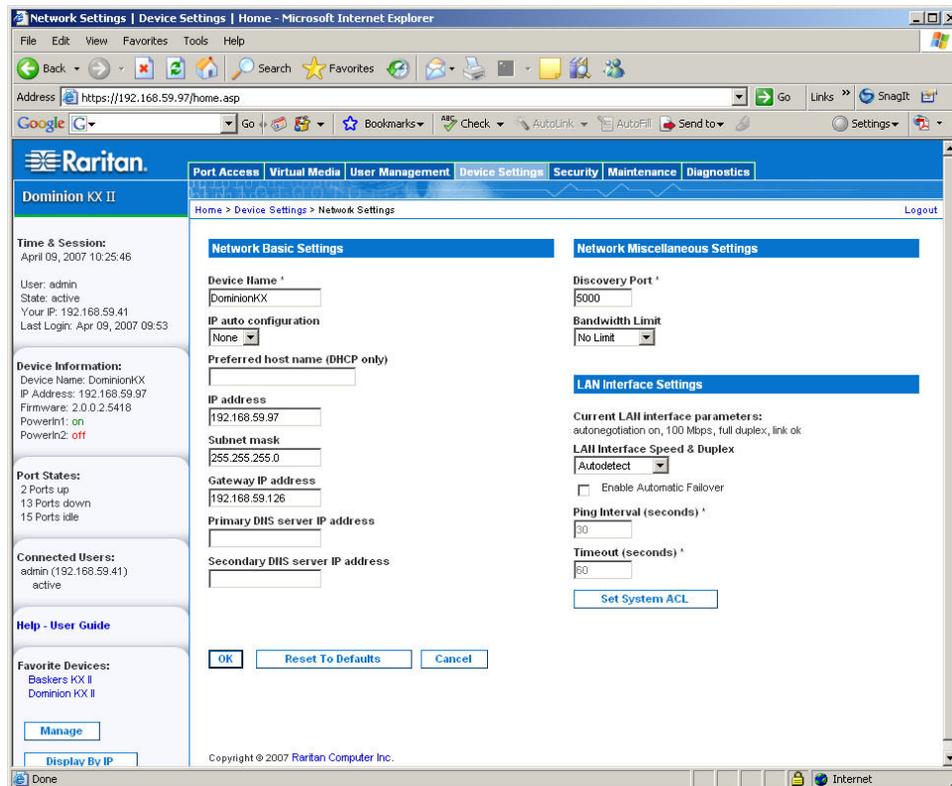


Figure 56 : Menu Network Settings (Paramètres réseau)

2. Mettez à jour les paramètres réseau de base. Reportez-vous à [Paramètres réseau de base](#) pour de plus amples informations sur chacun des champs.
3. Mettez à jour les paramètres réseau divers. Reportez-vous à [Paramètres réseau divers](#) pour de plus amples informations sur chacun des champs.
4. Mettez à jour les paramètres relatifs à l'interface LAN. Reportez-vous à [Paramètres de l'interface LAN](#) pour de plus amples informations sur chacun des champs.
5. Cliquez sur **OK** pour confirmer ces configurations. Si vos modifications nécessitent le redémarrage du dispositif, un message de redémarrage apparaît.

Pour quitter sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour restaurer les paramètres d'usine par défaut :

Cliquez sur **Reset to Defaults (Restaurer les paramètres par défaut)**.

Menu Network Basic Settings (Paramètres réseau de base)

Figure 57 : Paramètres réseau (Paramètres réseau de base)

- **Device Name (Nom du dispositif)**. Tapez un nom unique pour le dispositif (un maximum de 16 caractères ; pas d'espaces). Nommez votre dispositif de façon à ce que vous puissiez l'identifier facilement. Le nom par défaut d'une unité Dominion KX II est : « **DominionKX** ». Les utilisateurs distants verront également ce nom. Toutefois, si un utilisateur MPC a créé un profil de connexion pour ce dispositif, il ne verra pas ce nom mais le champ **Description** du profil.
- **Configuration IP automatique**. Sélectionnez-la parmi les options de la liste déroulante :
 - **Aucun**. Utilisez cette option si vous ne souhaitez pas de configuration IP automatique et préférez définir l'adresse IP vous-même (IP statique). Cette option par défaut est recommandée.

*Lorsque cette option est sélectionnée pour la **configuration IP automatique**, les champs associés aux paramètres réseau de base suivants sont activés, vous permettant ainsi de définir la configuration IP manuellement.*

- ◆ **IP Address (Adresse IP)**. L'adresse IP par défaut est 192.168.0.192.
- ◆ **Masque de sous-réseau**. Le masque de sous-réseau par défaut est 255.255.255.0.
- ◆ **Adresse IP de passerelle**. L'adresse IP associée à la passerelle (le cas échéant).
- ◆ **Adresse IP du serveur DNS primaire**. Le serveur de nom de domaine principal utilisé pour traduire les noms en adresses IP.
- ◆ **Adresse IP du serveur DNS secondaire**. Le serveur de nom de domaine secondaire utilisé pour traduire les noms en adresses IP (le cas échéant).

- **DHCP.** Le protocole de configuration d'hôte dynamique est utilisé par les ordinateurs mis en réseau (clients) pour obtenir des adresses IP uniques et d'autres paramètres à partir du serveur DHCP.
 - ◆ Si DHCP est utilisé, entrez le **nom d'hôte préféré (DHCP uniquement)**. Maximum de 63 caractères.

Paramètres réseau divers

The screenshot shows a configuration window titled "Network Miscellaneous Settings". It contains two main sections: "Discovery Port" with a text input field containing "5000", and "Bandwidth Limit" with a dropdown menu currently set to "No Limit".

Figure 58 : Paramètres réseau (paramètres réseau divers)

- **Port de détection.** La détection de Dominion KX II s'effectue via un port TCP unique et configurable. Le port défini par défaut est le **Port 5000**. Vous pouvez néanmoins configurer ce paramètre de manière à utiliser le port TCP de votre choix (*à l'exception* des ports 80 et 443). Pour accéder à l'unité KX II par-delà un pare-feu, les paramètres du pare-feu doivent permettre la communication bidirectionnelle par l'intermédiaire du port 5000 par défaut ou d'un port personnalisé non défini par défaut, selon la configuration indiquée. Pour de plus amples informations, reportez-vous à [Configuration des paramètres du pare-feu de réseau](#).
- **Limitation de bande passante.** Le paramètre par défaut est *no limit (pas de limitation)*. Sélectionnez le paramètre approprié parmi les options de la liste déroulante pour définir la quantité maximale de bande passante qui peut être utilisée par cette unité Dominion KX II (pour toutes les sessions). Ces options incluent : No Limit, 100 Megabit, 10 Megabit, 5 Megabit, 2 Megabit, 512 Kilobit, 256 Kilobit et 128 Kilobit.

Remarque : une bande passante inférieure peut entraîner le ralentissement des performances.

Paramètres de l'interface LAN

The screenshot shows a configuration window titled "LAN Interface Settings". It displays "Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok". Below this, there is a section for "LAN Interface Speed & Duplex" with a dropdown menu set to "Autodetect" and an unchecked checkbox for "Enable Automatic Failover". Further down, there are two text input fields: "Ping Interval (seconds)" with the value "30" and "Timeout (seconds)" with the value "60". At the bottom, there is a button labeled "Set System ACL".

Figure 59 : Paramètres réseau (Paramètres de l'interface LAN)

- Les paramètres actuels de l'interface LAN sont identifiés dans le champ **Current LAN interface parameters**.

- **Vitesse & Duplex de l'interface LAN.** Sélectionnez les associations de vitesse et de duplex parmi celles disponibles :

Détection automatique	Option par défaut
10 Mbps/Half	
10 Mbps/Full	
100 Mbps/Half	
100 Mbps/Full	
1000 Mbps/Full	Gigabit

- **Half-duplex** permet la communication dans les deux directions, mais seulement une direction à la fois (non simultanément).
- **Full-duplex** permet la communication dans les deux directions simultanément.

Remarque : Des problèmes surviennent parfois lors de l'exécution à 10 Mbits en half duplex ou en full duplex. Si vous rencontrez des problèmes, veuillez sélectionner une autre vitesse et un autre duplex.

- **Activer le basculement automatique.** Activez cette case pour permettre à Dominion KX II de restaurer automatiquement sa connexion réseau par le biais d'un second port réseau en cas de panne du port réseau actif. Lorsque cette option est activée, les deux champs ci-après sont utilisés :
 - **Intervalle Ping (secondes).** L'option Ping interval (Intervalle ping) détermine la fréquence à laquelle Dominion KX II gère l'état de la connexion réseau (une fréquence trop faible risque de surcharger le réseau). L'intervalle Ping par défaut est de 30 secondes.
 - **Temporisation (secondes).** L'option Timeout (Temporisation) détermine la durée pendant laquelle un port réseau doit être inactif avant de passer à un autre port. Les deux ports réseau doivent être connectés au réseau, et l'option de basculement automatique doit être sélectionnée pour être effective. La temporisation par défaut est de 60 secondes.

Remarque : les valeurs par défaut d'intervalle ping et de temporisation génèrent une condition selon laquelle lorsque le dispositif KX essaie de changer, toutes les sessions distantes sont interrompues et doivent être établies de nouveau. La réduction de ces intervalles à des valeurs inférieures permet aux sessions distantes de rester connectées mais entraîne l'augmentation du trafic réseau.

- **Configurer le système LCA.** Cliquez sur ce bouton pour configurer une liste de contrôle d'accès au niveau global pour votre unité Dominion KX II permettant de garantir que votre dispositif ne répondra pas aux paquets envoyés à partir d'adresses IP non autorisées. La page [Contrôle d'accès IP](#) s'ouvre.

Remarque : les valeurs des listes de contrôle d'accès (LCA) sont des valeurs globales qui affectent l'ensemble de l'unité Dominion KX II. Vous pouvez également créer des LCA au niveau du groupe. Vous pouvez, par exemple, créer un groupe d'utilisateurs « Fournisseurs extérieurs », autorisé à accéder à Dominion KX II uniquement à partir d'une plage d'adresses IP donnée (pour plus d'informations sur la procédure à suivre pour créer des listes de contrôle d'accès spécifiques à des groupes, reportez-vous à [LCA IP de groupes](#)).

Paramètres date/heure

Utilisez la page de ces paramètres pour spécifier la date et l'heure de Dominion KX II. Vous pouvez procéder de deux manières :

- Définir la date et l'heure manuellement ou
- synchroniser avec un serveur NTP.

Pour définir la date et l'heure :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Date/Time (Date/heure)**. La page correspondante s'ouvre :

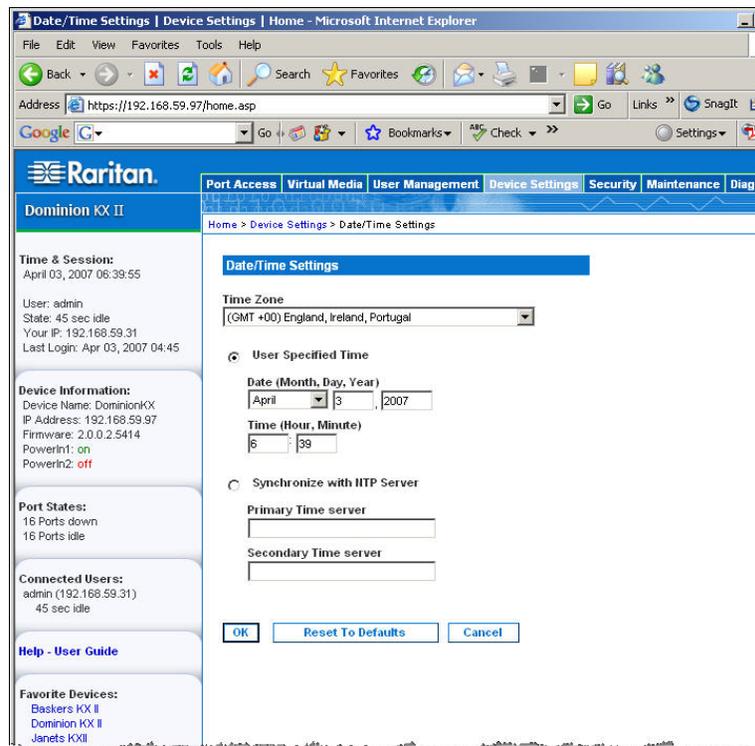


Figure 60 : Paramètres date/heure

2. Sélectionnez votre fuseau horaire à partir de la liste déroulante **Time Zone (Fuseau horaire)**
3. Choisissez la méthode que vous souhaitez utiliser pour définir la date et l'heure.
 - **User specified time (Heure spécifiée par l'utilisateur)**. Sélectionnez cette option pour entrer la date et l'heure manuellement.
 - **Synchronize with NTP Server (Synchroniser avec le serveur NTP)**. Sélectionnez cette option pour synchroniser la date et l'heure avec le serveur de protocole NTP.
4. Pour l'option **Heure spécifiée** par l'utilisateur, saisissez la date et l'heure comme suit :
 - a. Sélectionnez le **mois** dans la liste déroulante.
 - b. Entrez le **jour** du mois.
 - c. Entrez l'**année** dans le format aaaa.
 - d. Entrez l'**heure** dans le format hh :mm (utilisez le système des 24 heures).
5. Pour l'option **Synchroniser avec le serveur NTP** :
 - a. Entrez l'adresse IP du **serveur de temps principal**.
 - b. (Facultatif) Entrez l'adresse IP du **serveur de temps secondaire**.
6. Cliquez sur **OK**.

Gestion des événements

La fonction de gestion des événements de KX II propose un ensemble d'écrans permettant d'activer et de désactiver la distribution des événements système sur SNMP Managers, Syslog et le journal d'audit. Ces événements sont regroupés en différentes catégories, et pour chaque événement vous pouvez déterminer si vous souhaitez que l'événement soit envoyé à une ou plusieurs destinations.

Gestion des événements - Paramètres

Configuration SNMP

Le protocole SNMP est un protocole simplifié de gestion de réseau qui prend en charge la gestion de réseau et la surveillance des dispositifs réseau ainsi que leurs fonctions. Dominion KX II offre la prise en charge de l'agent SNMP via la fonction Event Management (Gestion des événements). Reportez-vous à [Configuration de l'agent SNMP](#) et [Configuration des traps SNMP](#) pour plus d'informations sur les agents et les traps SNMP.

Pour configurer SNMP (permettre la journalisation de SNMP) :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Event Management (Gestion des événements) – Settings (Paramètres)**. La page Gestion des événements – Paramètres s'ouvre :

Figure 61 : Gestion des événements - Paramètres

2. Cochez l'option **Enable SNMP Logging** pour activer les champs SNMP restants.

3. Dans les champs **Name (Nom)**, **Contact (Contact)**, et **Location (Location)**, saisissez le nom de l'agent SNMP (celui de l'unité Dominion) tel qu'il apparaît dans l'interface de la console KX II, un contact pour cette unité et l'emplacement physique de l'unité Dominion.
4. Tapez la **chaîne de communauté de l'agent** (la chaîne de l'unité Dominion). La communauté SNMP est le groupe auquel appartiennent les dispositifs et les postes de gestion exécutant SNMP. Elle permet de définir l'emplacement dans lequel les informations sont envoyées. Le nom de la communauté est utilisé pour identifier le groupe ; un dispositif ou un agent SNMP peuvent appartenir à plus d'une communauté SNMP.
5. Spécifiez si la communauté est en lecture seule ou en lecture-écriture à l'aide de la liste déroulante **Type**.
6. Configurez jusqu'à cinq gestionnaires **SNMP en spécifiant leur IP** de destination, le **Numéro de port** et la Communauté.
7. Cliquez sur le lien **Click here to view the Dominion-KX2 SNMP MIB** pour accéder à la base des informations de gestion SNMP.
8. Cliquez sur **OK**.

Configuration de Syslog



Figure 62 : Configuration de Syslog

Pour configurer Syslog (activer le transfert Syslog) :

1. Cochez la case **Activer le transfert Syslog** pour connecter les messages du dispositif sur un serveur Syslog distant.
2. Entrez l'adresse IP de votre serveur Syslog dans le champ **Adresse IP**.
3. Cliquez sur **OK**.

Pour quitter sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour restaurer les paramètres d'usine par défaut :

Cliquez sur le bouton **Reset to Defaults (Restaurer les paramètres par défaut)**.

Gestion des événements - Destinations

La case Evénements système, si activée, peut générer des événements de notification SNMP (traps) ou être connectée à Syslog ou au journal d'audit. Utilisez cette page pour sélectionner les événements système à suivre et l'emplacement dans lequel envoyer les informations.

Remarque : les traps SNMP sont générés uniquement si l'option SNMP Logging Enabled est cochée ; les événements Syslog ne sont générés que si l'option Enable Syslog Forwarding est cochée. Ces deux options sont expliquées à la page [Gestion des événements - Paramètres](#).

Pour sélectionner des événements et leurs destinations :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Event Management (Gestion des événements) – Destinations**. La page correspondante s'ouvre :

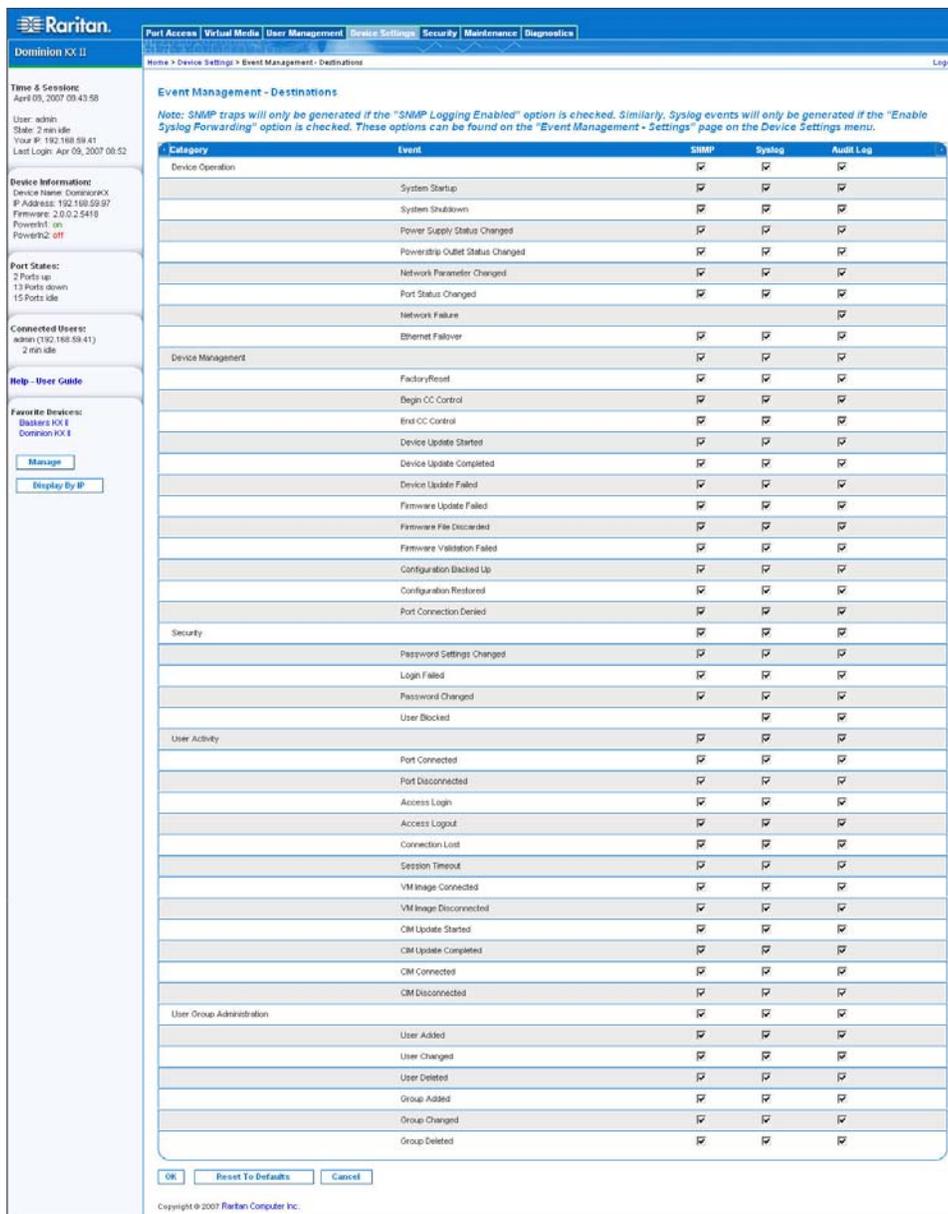


Figure 63 : Gestion des événements - Destinations

Les événements de système sont regroupés en plusieurs catégories : Device Operation, Device Management, Security, User Activity et User Group Administration

2. Cochez les cases en regard des éléments de ligne **Event (Événement)** que vous souhaitez activer ou désactiver, ainsi que l'emplacement dans lequel vous souhaitez envoyer les informations.

Conseil : activez ou désactivez des catégories entières en sélectionnant ou désélectionnant les cases de la ligne Category (Catégorie).

3. Cliquez sur **OK**.

Pour quitter sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour restaurer les paramètres d'usine par défaut :

Cliquez sur le bouton **Reset to Defaults (Restaurer les paramètres par défaut)**.

Configuration de l'agent SNMP

Les dispositifs conformes à SNMP, appelés agents, stockent les données qui leur sont rattachées dans Management Information Bases (MIBs) et renvoient ces données aux gestionnaires SNMP. Utilisez la page de journalisation des événements pour configurer la connexion SNMP entre Dominion KX II (agent SNMP) et un gestionnaire SNMP.

Configuration des traps SNMP

SNMP offre la possibilité d'envoyer des traps ou des notifications pour aider un administrateur à déceler lorsque une ou plusieurs conditions ont été remplies. Le tableau suivant répertorie les traps SNMP de Dominion KX II :

NOM DE TRAP	DESCRIPTION
cimConnected	CIM branché dans le port de Dominion KX II.
cimDisconnected	CIM soit débranché du port de Dominion KX II, soit déconnecté.
cimUpdateCompleted	Processus de mise à jour du firmware CIM terminé.
cimUpdateStarted	Processus de mise à jour du firmware CIM entamé.
configBackup	La configuration du dispositif a été sauvegardée.
configRestore	La configuration du dispositif a été restaurée.
deviceUpdateFailed	La mise à jour du dispositif a échoué.
deviceUpgradeCompleted	Dominion KX II a effectué la mise à jour via un fichier RFP.
deviceUpgradeStarted	Dominion KX II a démarré la mise à jour via un fichier RFP.
ethernetFailover	Un basculement Ethernet a été détecté et restauré sur une nouvelle interface Ethernet.
factoryReset	Les paramètres usine par défaut du dispositif ont été réinitialisés.
firmwareFileDiscarded	Le fichier du firmware a été rejeté.
firmwareUpdateFailed	La mise à jour du firmware a échoué.
firmwareValidationFailed	La validation du firmware a échoué.
groupAdded	Un groupe a été ajouté au système KX II.
groupDeleted	Un groupe a été supprimé du système.
groupModified	Un groupe a été modifié.
ipConflictDetected	Un conflit d'adresse IP a été détecté.
ipConflictResolved	Un conflit d'adresse IP a été résolu.
networkFailure	Une interface Ethernet du produit ne peut plus communiquer via le réseau.
networkParameterChanged	Une modification a été effectuée au niveau des paramètres réseau.
passwordSettingsChanged	Les paramètres des mots de passe sécurisés ont été modifiés.
portConnect	Un utilisateur authentifié au préalable a démarré une session KVM.
portConnectionDenied	Une connexion au port cible a été refusée.
portDisconnect	Un utilisateur engagé dans une session KVM ferme la session correctement.
portStatusChange	Le port est devenu indisponible.
powerNotification	Notification de l'état de la prise d'alimentation : 1=Active, 0=Inactive.
powerOutletNotification	Notification de l'état de la barrette d'alimentation.
rebootCompleted	Le redémarrage du KX est terminé.
rebootStarted	Le KX a commencé à redémarrer, lors de la remise sous tension du système ou lors d'un redémarrage à chaud à partir du système d'exploitation.
securityViolation	Violation de sécurité.
startCCManagement	Le dispositif a été placé sous la gestion CommandCenter.
stopCCManagement	Le dispositif a été retiré de la gestion CommandCenter.
userAdded	Un utilisateur a été ajouté au système.
userAuthenticationFailure	Un utilisateur a essayé de se connecter sans nom d'utilisateur et/ou mot de passe correct.
userConnectionLost	Un utilisateur avec une session active a subi une interruption anormale de session.
userDeleted	Un compte d'utilisateur a été rejeté.
userLogin	Un utilisateur s'est connecté et authentifié avec succès au KX II.
userLogout	Un utilisateur s'est déconnecté correctement du KX II.
userModified	Un compte d'utilisateur a été modifié.
userPasswordChanged	Cet événement est déclenché lorsque le mot de passe de <i>n'importe quel</i> utilisateur du dispositif est modifié.
userSessionTimeout	Un utilisateur avec une session active a subi une interruption de session en raison du délai d'attente.
vmImageConnected	Un utilisateur a tenté de monter un dispositif ou une image sur la cible utilisant les médias virtuels. Pour chaque tentative de mappage (montage) de dispositif/image, le présent événement est généré.
vmImageDisconnected	Un utilisateur a tenté de démonter un dispositif ou une image sur la cible utilisant les médias virtuels.

Page de configuration de l'alimentation

Le Dominion KX II offre une double alimentation. Par ailleurs, il peut détecter et notifier automatiquement l'état de ces alimentations. Utilisez cette page pour indiquer si vous utilisez une ou plusieurs sources d'alimentation électrique. Une configuration appropriée garantit l'envoi de notifications adéquates par Dominion KX II, en cas de panne de courant. Par exemple, si l'alimentation numéro un échoue, le voyant LED situé à l'avant de l'unité devient rouge.

Pour activer la détection automatique des sources d'alimentation utilisées :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation électrique)**. La page de configuration de l'alimentation électrique s'ouvre :

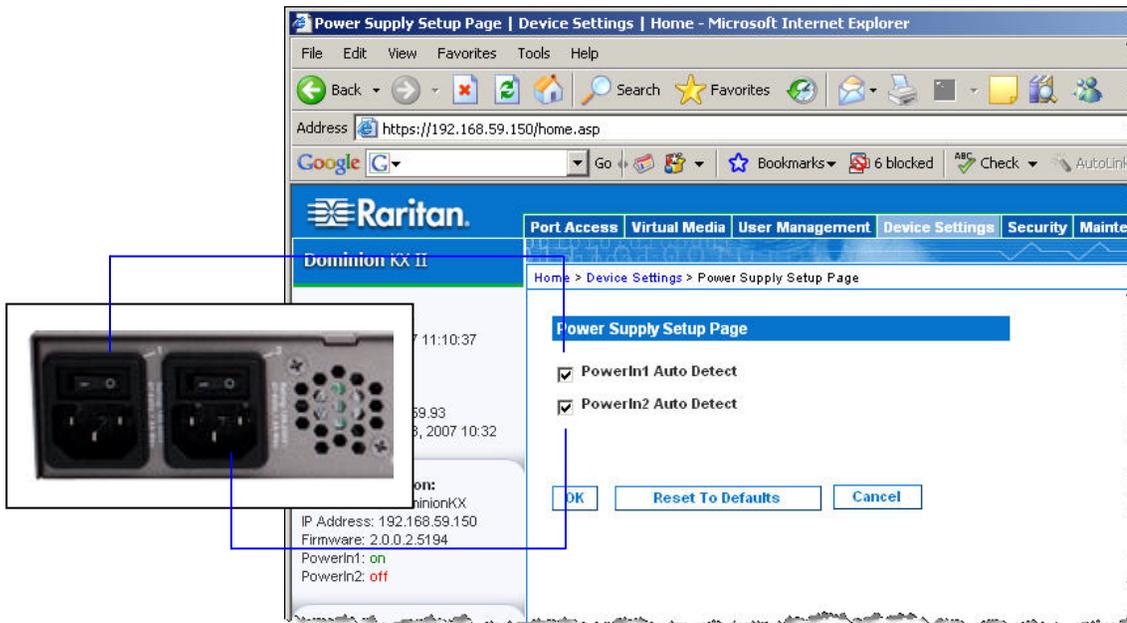


Figure 64 : Configuration de l'alimentation

2. Si vous branchez une arrivée électrique dans l'alimentation numéro un (à gauche – pour la plupart des alimentations électriques sur la partie arrière de l'unité), cochez alors la case **PowerIn1 Auto Detect (Détection automatique PowerIn1)**.
3. Si vous branchez une arrivée électrique dans l'alimentation numéro deux (à droite – pour la plupart des alimentations électriques sur la partie arrière de l'unité), cochez alors la case **PowerIn2 Auto Detect (Détection automatique PowerIn2)**.
4. Cliquez sur **OK**.

Remarque : si l'une de ces cases est cochée et que l'arrivée électrique n'est pas branchée, le voyant d'alimentation sur la partie avant de l'unité s'affiche en rouge.

Pour désactiver la détection automatique :

Désélectionnez la case correspondant à la source d'alimentation appropriée.

Pour restaurer les paramètres d'usine par défaut :

Cliquez sur le bouton **Reset to Defaults (Restaurer les paramètres par défaut)**.

Pour quitter sans enregistrer les modifications :

Cliquez sur le bouton **Cancel (Annuler)**.

Remarque : Dominion KX II n'établit PAS de rapport sur l'état d'alimentation pour CommandCenter. Dominion I (génération I), en revanche, établit des rapports sur l'état d'alimentation pour CommandCenter.

Page de configuration des ports

La page de configuration des ports affiche une liste des ports de Dominion KX II. Les ports connectés aux serveurs cible ou aux barrettes d'alimentation sont affichés en bleu et peuvent être modifiés. Pour les ports qui n'ont pas de CIM connecté ou qui ont un nom de CIM vide, un nom de port par défaut **Dominion-KX2_Port#** est attribué, où **Port#** est le numéro du port physique de Dominion KX II.

Pour modifier la configuration d'un port :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Port Configuration (Configuration du port)**. La page de configuration des ports s'ouvre :

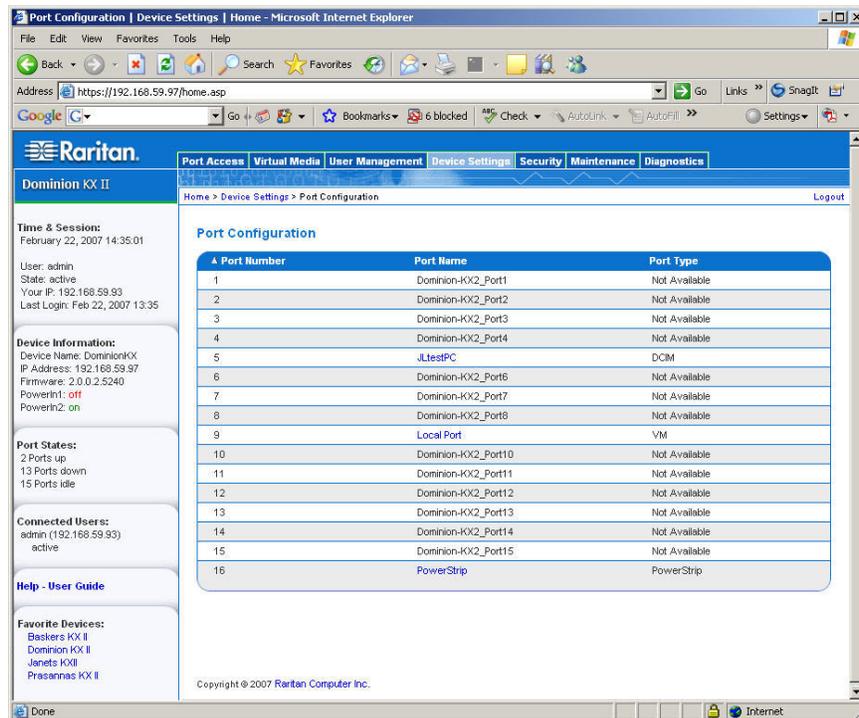


Figure 65 : Configuration des ports

Cette page est affichée initialement par ordre de numéros de port, mais elle peut être triée en fonction de n'importe quel champ en cliquant sur les en-têtes de colonne.

- **Port Number (Numéro de port)**. Les ports sont numérotés de 1 au nombre total de ports disponibles pour l'unité Dominion KX II.
- **Port Name (Nom du port)**. Le nom attribué au port. Un nom de port affiché en noir indique que vous ne pouvez pas modifier le nom et que le port ne peut être modifié ; les noms de port affichés en bleu peuvent être modifiés.
- **Port Type (Type de port)**. Type de CIM connecté au port :

TYPE DE PORT	DESCRIPTION
DCIM	Dominion CIM
Non disponible	Pas de CIM connecté.
PCIM	Paragon CIM
Barrette d'alimentation	CIM d'alimentation
VM (Média virtuel)	CIM des médias virtuels (D2CIM-VUSB)

2. Cliquez sur l'option **Port Name (Nom du port)** associée au port que vous souhaitez modifier.
 - Pour les ports KVM, la [Page des ports](#) s'ouvre. A partir de cette page, vous pouvez nommer les ports et créer des associations d'alimentation.
 - Pour les barrettes d'alimentation, la page des ports relative aux [barrettes d'alimentation](#) s'ouvre. A partir de cette page, vous pouvez nommer les barrettes d'alimentation ainsi que leurs prises.

Gestion de l'alimentation

Dominion KX II permet de contrôler l'alimentation des serveurs cible à distance. Pour utiliser cette fonction, vous devez disposer d'une barrette d'alimentation distante Raritan et du module d'interface pour ordinateurs (CIM) D2CIM-PWR. Une fois les répartitions d'alimentation effectuées, la gestion de l'alimentation à distance de votre serveur cible est possible.

Pour utiliser la fonction de contrôle d'alimentation de Dominion KX II :

1. [Branchez la barrette d'alimentation](#) sur votre serveur cible.
2. [Donnez un nom à la barrette d'alimentation](#)
3. [Associez une ou plusieurs prises](#) à la barrette d'alimentation sur le serveur cible.
4. Utilisez [la gestion de l'alimentation à distance](#) à distance du serveur cible à partir de la [page d'accès aux ports](#).

Branchement de la barrette d'alimentation

Les numéros des étapes décrivant la connexion sont repris dans le schéma ci-dessous.

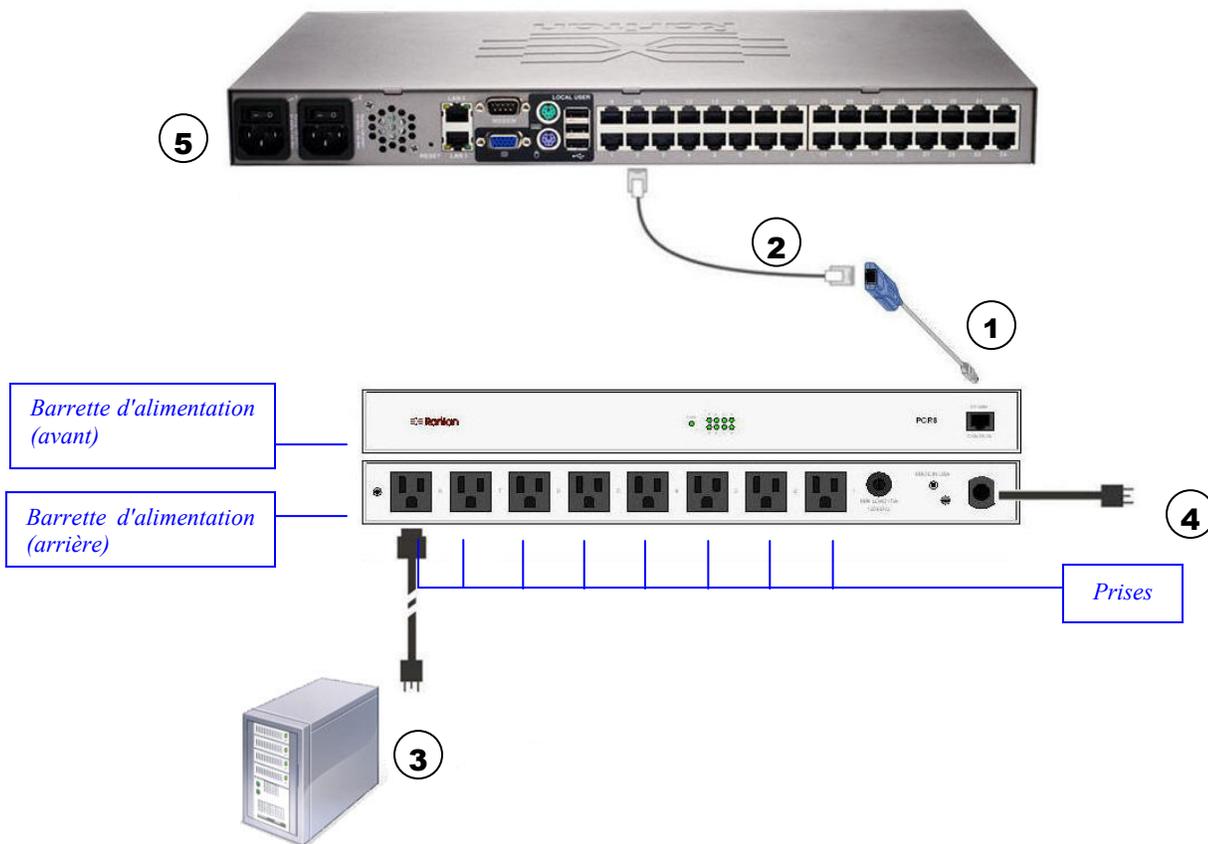


Figure 66 : Branchements des barrettes d'alimentation

Pour brancher la barrette d'alimentation :

1. Branchez la fiche RJ-45 mâle du D2CIM-PWR au connecteur RJ-45 femelle de la barrette d'alimentation.
2. Branchez la fiche RJ-45 femelle du D2CIM-PWR à l'un des connecteurs de port système femelle disponible sur l'unité Dominion KX II à l'aide d'un câble Cat5 à brochage direct.
3. Reliez un cordon d'alimentation CA au serveur cible et une prise de barrette d'alimentation disponible.
4. Branchez la barrette d'alimentation sur une source d'alimentation CA.
5. Mettez l'unité Dominion KX II sous tension.

Désigner les barrettes d'alimentation (Page des ports liés aux barrettes d'alimentation)

Cette page s'ouvre lorsque vous sélectionnez un port à partir de la page [Configuration des ports](#) connectée à une barrette d'alimentation distante Raritan. Les champs **Type** et **Nom** sont pré-générés ; notez que le **Type** (CIM) *ne peut pas* être modifié. Les informations suivantes s'affichent pour chaque prise de barrette d'alimentation : **numéro**, **nom** et **association de ports** de la prise.

Utilisez cette page pour nommer la barrette d'alimentation et ses prises ; tous les noms peuvent contenir jusqu'à 32 caractères alphanumériques y compris les [caractères spéciaux](#).

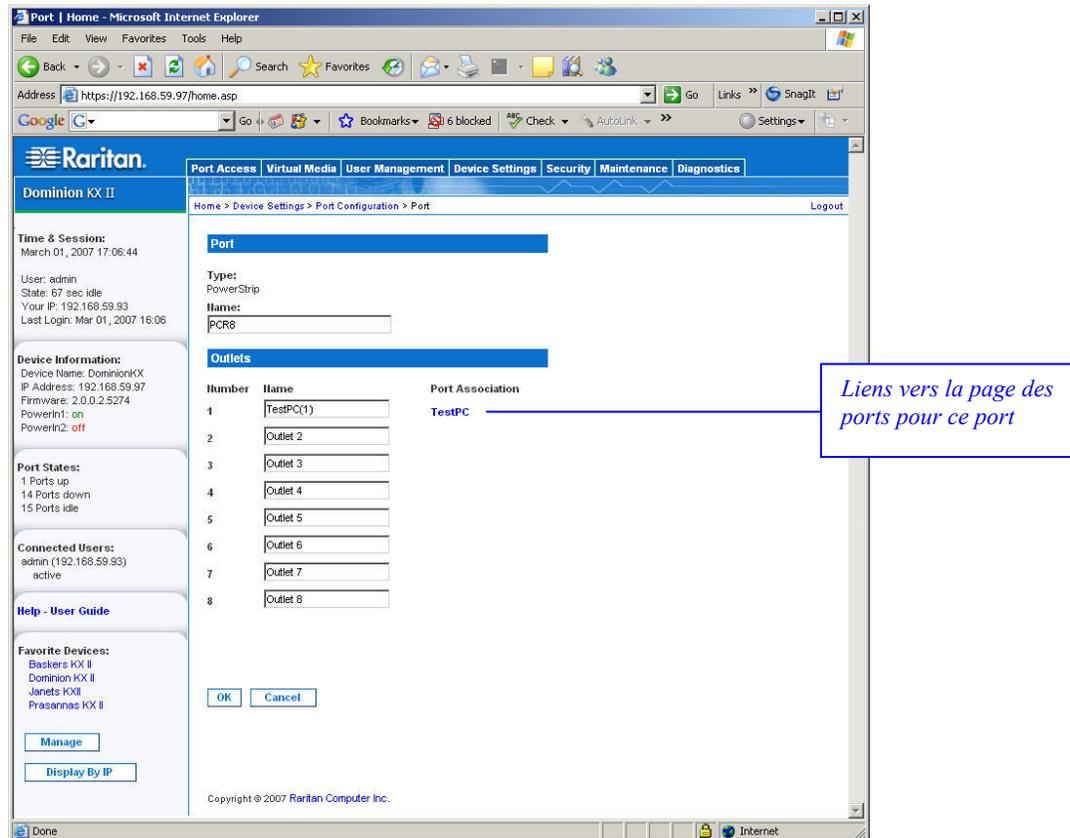


Figure 67 : Page relative aux ports (barrettes d'alimentation)

Remarque : lorsqu'une barrette d'alimentation est associée à un serveur cible (port), le nom de la prise est remplacé par le nom du serveur cible (même si vous attribuez un autre nom à la prise).

Pour nommer la barrette d'alimentation (et les prises) :

Remarque : CommandCenter Service Gateway ne reconnaît pas les noms des barrettes d'alimentation qui contiennent des espaces.

1. Remplacez le **Nom** de la barrette d'alimentation par un texte dont vous vous souviendrez.
2. Modifiez le **nom (prise)** si vous le souhaitez. (Les noms de prise par défaut sont **Prise #**.)
3. Cliquez sur **OK**.

Pour quitter sans enregistrer les modifications :

Cliquez sur le bouton **Cancel (Annuler)**.

Associez des serveurs cible aux prises (Page des ports)

Cette page s'ouvre lorsque vous sélectionnez un port à partir de la page [Configuration des ports](#) connectée à un serveur cible. A partir de cette page, vous pouvez créer des associations d'alimentation, modifier le nom de port pour un nom plus évocateur et mettre à jour les paramètres de serveur cible si vous utilisez [D2CIM-VUSB CIM](#). Les champs **Type** (CIM) et **Nom** (Port) sont pré-générés ; notez que le Type de CIM *ne peut pas* être modifié.

Un serveur peut avoir jusqu'à quatre prises d'alimentation et vous pouvez associer une barrette d'alimentation différente à chacune d'elle. A partir cette page, définissez les associations de façon à pouvoir mettre sous tension, hors tension et réallumer le serveur dans la page d'accès aux ports.

Pour utiliser cette fonction, vous avez besoin :

- de(s) barrette(s) d'alimentation Raritan
- des CIM d'alimentation (D2CIM-PWR)

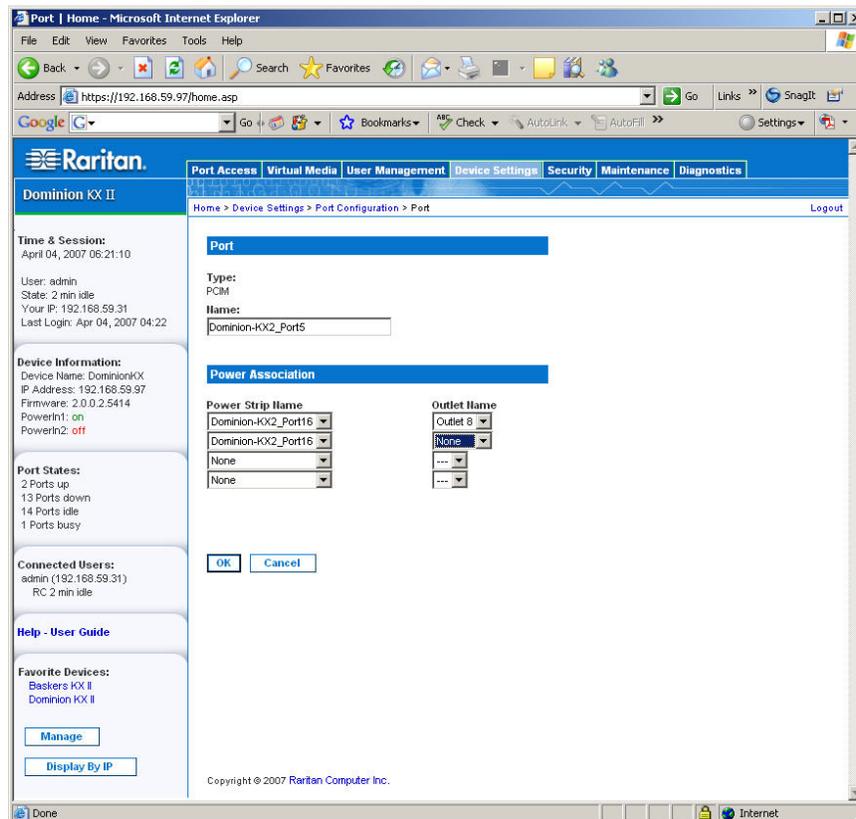


Figure 68 : Page des ports (ports KVM)

Pour créer des associations d'alimentation (associer les prises des barrettes d'alimentation aux serveurs cible) :

Remarque : lorsqu'une barrette d'alimentation est associée à un serveur cible (port), le nom de la prise est remplacé par le nom du serveur cible (même si vous attribuez un autre nom à la prise).

1. Sélectionnez la barrette d'alimentation dans la liste déroulante **Nom de barrette d'alimentation**.
2. Pour cette barrette d'alimentation, sélectionnez la prise à partir de la liste déroulante **Nom de prise**.
3. Répétez les étapes 1 et 2 pour chaque association d'alimentation voulue.
4. Cliquez sur **OK**. Un message de confirmation s'affiche.

Pour modifier le nom du port :

1. Tapez un nom évocateur dans le champ **Nom**. Par exemple, le nom du serveur cible peut correspondre à un candidat susceptible. Le nom peut contenir jusqu'à 32 caractères alphanumériques et [caractères spéciaux](#).
2. Cliquez sur **OK**.

Pour quitter sans enregistrer les modifications :

Cliquez sur le bouton **Cancel (Annuler)**.

Pour supprimer une association de barrettes d'alimentation :

1. Sélectionnez la barrette d'alimentation appropriée dans la liste déroulante **Nom de barrette d'alimentation**.
2. Pour cette barrette d'alimentation, sélectionnez la prise appropriée à partir de la liste déroulante **Nom de prise**.
3. Sélectionnez **Aucun** à partir de la liste déroulante **Nom de prise**.
4. Cliquez sur **OK**. Cette association de barrettes d'alimentation/prises est supprimée. Un message de confirmation s'affiche.

Remarque concernant l'utilisation de D2CIM-VUSB CIM

Si vous utilisez D2CIM-VUSB, il existe des paramètres supplémentaires sur la page des ports pour améliorer les performances.

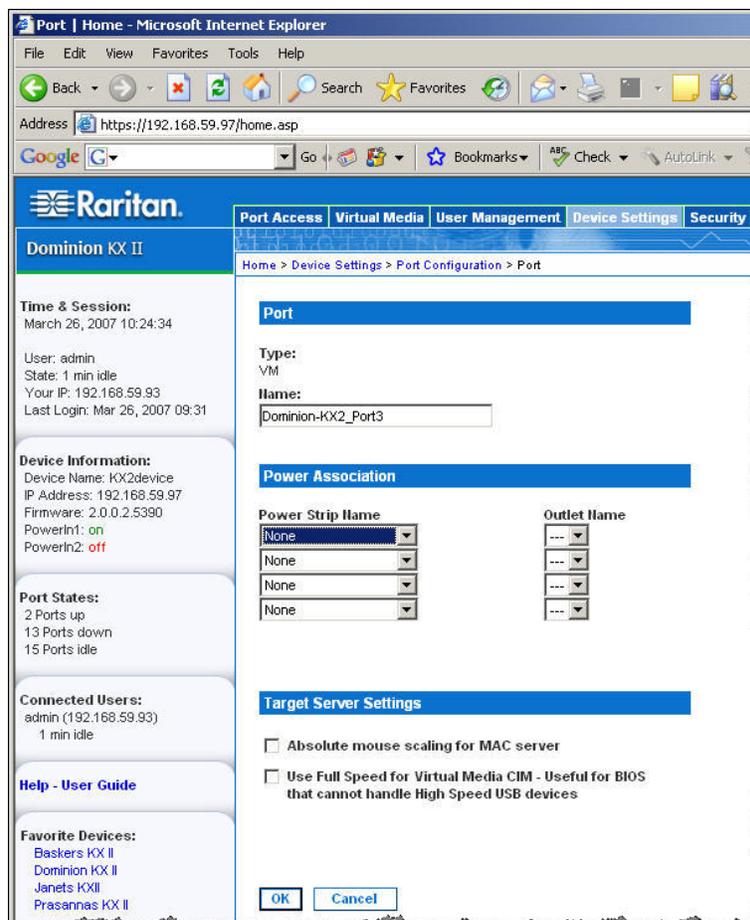


Figure 69 : Page des ports (Paramètres du serveur cible pour D2CIM-VUSB)

Si vous rencontrez des problèmes de synchronisation et utilisez D2CIM-VUSB CIM pour un serveur cible Mac, cochez l'option **Absolute mouse scaling for MAC server (Mise à l'échelle absolue de la souris pour le serveur MAC)**.

Certains niveaux BIOS ne prennent pas en charge les fonctions à haut débit et la tentative de négociation automatique ne fonctionne pas. Si vous rencontrez des problèmes au niveau de BIOS avec le serveur cible, cochez la case **Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du média virtuel)**.

*Remarque : Pour les serveurs cible SUSE 9.2, cochez la case **Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du média virtuel)** pour les ports des serveurs cible. SUSE 9.2 ne fonctionne pas avec le CIM du média virtuel pour le haut-débit.*

Chapitre 10 : Paramètres de sécurité

Le menu de sécurité est organisé comme suit : Paramètres de sécurité et contrôle d'accès IP.

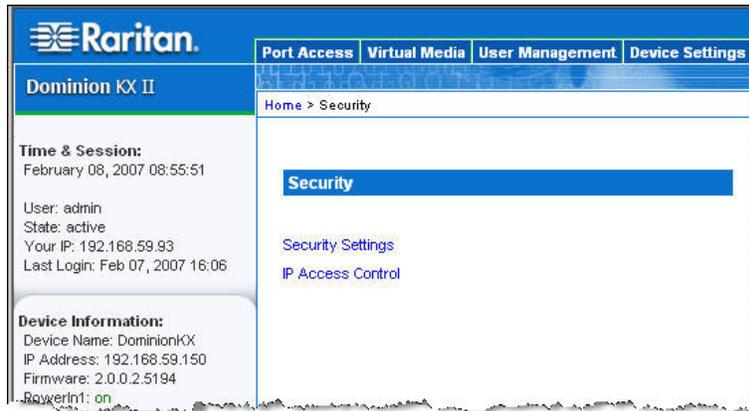


Figure 70 : Menu de sécurité

UTILISEZ :	POUR :
Paramètres de sécurité	Configurer les paramètres de sécurité pour les limitations de connexion, les mots de passe sécurisés, le blocage des utilisateurs et le cryptage & partage.
Contrôle d'accès IP	Contrôler l'accès à votre unité Dominion KX II. Configurer une liste de contrôle d'accès au niveau global pour votre unité KX permettant de garantir que votre dispositif ne répondra pas aux paquets envoyés à partir d'adresses IP non autorisées.

Paramètres de sécurité

A partir de la page des paramètres de sécurité, spécifiez les limitations de connexion, le blocage des utilisateurs, les règles de mot de passe ainsi que le chiffrement et le partage.

Les certificats SSL Raritan sont utilisés pour des échanges clé publiques et privés. Ils fournissent un niveau de sécurité supplémentaire. Les certificats de serveur Web Raritan sont auto-signés ; les certificats d'applet Java sont signés par VeriSign®. Le cryptage garantit la sécurité de vos informations en les protégeant contre l'interception frauduleuse. Ces certificats garantissent la fiabilité de l'entité Raritan, Inc.

Pour configurer les paramètres de sécurité :

1. Sélectionnez **Security > Settings (Paramètres)**. La page des paramètres de sécurité s'ouvre.

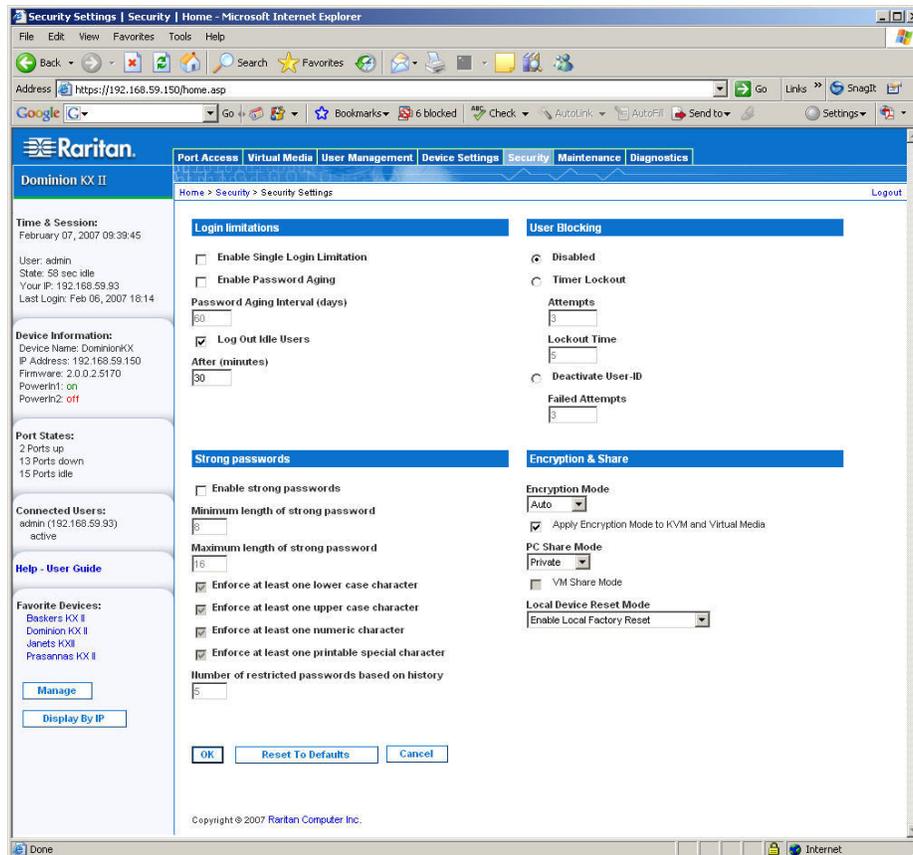


Figure 71 : Paramètres de sécurité

Les champs sont regroupés comme suit : Limitations de connexion, Mots de passe sécurisés, Blocage des utilisateurs et Cryptage & Partage.

2. Mettez à jour les paramètres [Limitations de connexion](#) appropriés.
3. Mettez à jour les paramètres [Mots de passe sécurisés](#) appropriés.
4. Mettez à jour les paramètres [Blocage des utilisateurs](#) appropriés.
5. Mettez à jour les paramètres [Cryptage et partage](#) appropriés.
6. Cliquez sur **OK** lorsque vous avez terminé.

Pour quitter la page sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour réinitialiser les paramètres par défaut :

cliquez sur **Reset to Defaults (Restaurer les paramètres par défaut)**.

Limitations de connexion

Grâce aux limitations de connexion, spécifiez les restrictions en matière de connexion unique, de vieillissement de mot de passe et de déconnexion des utilisateurs inactifs.

- **Activer la limitation de connexion unique.** Si vous sélectionnez cette option, seule une connexion par nom d'utilisateur est autorisée à n'importe quel moment. Si l'option est désélectionnée, une combinaison nom d'utilisateur/mot de passe donnée peut être connectée au dispositif à partir de plusieurs postes de travail client simultanément.
- **Activer le vieillissement du mot de passe.** Si vous sélectionnez cette option, tous les utilisateurs sont obligés de modifier leur mot de passe régulièrement en fonction du nombre de jours spécifiés dans le champ d'intervalle de vieillissement du mot de passe.
 - **Intervalle de vieillissement du mot de passe (jours).** Ce champ est activé et requis lorsque la case **Activer le vieillissement du mot de passe** est cochée. Entrez le nombre de jours après lequel une modification de mot de passe est requise. Le nombre par défaut est 60 jours.
- **Déconnecter les utilisateurs inactifs.** Cochez cette case pour déconnecter automatiquement une session d'utilisateurs après expiration d'un délai défini d'inactivité. Indiquez le délai dans le champ After (Après). S'il y a absence d'activité du clavier ou de la souris, toutes les sessions KVM et toutes les ressources KVM sont déconnectées. En revanche, si une session de média virtuel est en cours, la session n'est pas interrompue.
 - **Après (minutes).** La quantité de temps (en minutes) après laquelle un utilisateur inactif est déconnecté. Ce champ est activé lorsque l'option **Déconnecter les utilisateurs inactifs** est sélectionnée.

Mots de passe sécurisés

Les mots de passe sécurisés fournissent une authentification locale sécurisée du système accrue. Utilisez les mots de passe sécurisés pour spécifier les critères de définition du format au niveau des mots de passe locaux valides de KX II, tels que la longueur minimum et maximum, les caractères requis et la conservation de l'historique des mots de passe.

Strong passwords

Enable strong passwords

Minimum length of strong password
8

Maximum length of strong password
16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history
5

Figure 72 : Paramètres de sécurité (Mots de passe sécurisés)

- **Enable strong passwords (Activer les mots de passe sécurisés).** Les mots de passe des utilisateurs doivent compter un minimum de 8 caractères avec au moins un caractère alphabétique et un caractère non alphabétique (signe de ponctuation, caractère ou chiffre). De plus, les quatre premiers caractères du mot de passe et du nom d'utilisateur ne peuvent être identiques.

Si l'option est sélectionnée, les règles de mot de passe sécurisé sont renforcées. Les utilisateurs dont les mots de passe ne répondent pas aux critères de mot de passe sécurisé sont automatiquement obligés de modifier leur mot de passe lors de leur connexion suivante. Si l'option est désélectionnée, seule la confirmation du format standard est requise. Une fois cochés, les champs suivants sont activés et requis.

- **Longueur minimale du mot de passe sécurisé.** Il doit compter au moins 8 caractères. La valeur par défaut est 8, mais elle peut aller jusqu'à 63.
- **Longueur maximale du mot de passe sécurisé.** La valeur par défaut est 16, mais elle peut aller jusqu'à 64 caractères.
- **Imposer au moins un caractère minuscule.** Lorsqu'elle sélectionnée, cette option impose au moins un caractère minuscule dans le mot de passe.
- **Imposer au moins un caractère majuscule.** Lorsqu'elle sélectionnée, cette option impose au moins un caractère majuscule dans le mot de passe.
- **Imposer au moins un caractère numérique.** Lorsqu'elle sélectionnée, cette option impose au moins un caractère numérique dans le mot de passe.
- **Imposer au moins un caractère spécial imprimable.** Lorsqu'elle sélectionnée, cette option impose au moins un caractère spécial (imprimable) dans le mot de passe.
- **Nombre de mots de passe restreints en fonction de l'historique.** Le champ représente la limite de l'historique des mots de passe ; à savoir le nombre de mots de passe préliminaires qui ne peuvent être répétés. La gamme est de 1 à 12 ; la valeur par défaut étant 5.

Blocage des utilisateurs

Les options de blocage d'utilisateurs spécifient les critères selon lesquels les utilisateurs ont l'accès bloqué au système après un nombre spécifique d'échecs de connexion. Les trois options s'excluent les unes les autres :

- **Désactivé.** L'option par défaut ; les utilisateurs ne sont pas bloqués quel que soit leur nombre d'échecs d'authentification.
- **Verrouillage de l'inactivité.** Les utilisateurs se voient refuser l'accès au système après avoir excédé le nombre d'échecs de connexion autorisé. Une fois sélectionnés, les champs suivants sont activés :
 - **Tentatives.** Le nombre d'échecs de connexion après lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 10 ; la valeur par défaut étant 3 tentatives.
 - **Durée de verrouillage.** Le laps de temps pendant lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 1 440 minutes; la valeur par défaut étant 5 minutes.
- **Désactiver l'ID de l'utilisateur.** Une fois sélectionnée, cette option permet de confirmer que l'utilisateur ne peut plus accéder au système après un nombre spécifique de tentatives de connexion échouées, tel que mentionné dans le champ **Tentatives échouées** :
 - **Tentatives échouées.** Le nombre d'échecs de connexion après lequel l'ID de l'utilisateur est désactivé. Le champ est activé lorsque l'option **Désactiver l'ID de l'utilisateur** est sélectionnée. Les valeurs autorisées sont comprises entre 1 et 10.

Figure 73 : Paramètres de sécurité (Blocage des utilisateurs)

Lorsque l'ID d'un utilisateur est désactivée suite à un nombre spécifique d'échecs de connexion, l'administrateur doit modifier le mot de passe de l'utilisateur et activer le compte de l'utilisateur en cochant la case **Activer** à la page [Utilisateur](#).

Cryptage & Partage

A l'aide des paramètres Cryptage & Partage, spécifiez le type de cryptage utilisé, les modes de partage PC et MV ainsi que le type de réinitialisation effectuée lorsque le bouton de réinitialisation de Dominion KX II est enfoncé.

Figure 74 : Paramètres de sécurité (Cryptage & Partage)

- **Encryption mode (Mode de chiffrement).** Sélectionnez une option parmi celles de la liste déroulante. Si un mode de cryptage est sélectionné, un avertissement s'affiche pour vous informer que votre navigateur ne prend pas en charge le mode sélectionné. Vous ne serez alors pas en mesure de vous connecter à Dominion KX II.

Figure 75 : Paramètres de sécurité (Message d'avertissement relatif au mode de chiffrement)

- **Auto.** Cette option est recommandée. Dominion KX II gère automatiquement le niveau de chiffrement le plus élevé qui soit.
- **RC4.** Permet de sécuriser les noms d'utilisateur, les mots de passe et les données KVM, y compris les transmissions vidéo, à l'aide de la méthode de chiffrement RSA RC4. Le protocole Secure Socket Layer (SSL) à 128 bits permet la création d'un canal de communication privé entre l'unité Dominion KX II et l'ordinateur distant lors de l'authentification de la connexion initiale.
- **AES-128.** La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 128). Si la norme AES-128 est spécifiée, veuillez vous assurer que votre navigateur la prend en charge. Le cas échéant, vous ne pourrez pas vous connecter. Veuillez vous reporter à [Vérifier si votre navigateur prend en charge le chiffrement AES](#) pour de plus amples informations.

- **Appliquer le mode de chiffrement à KVM et au média virtuel.** Une fois sélectionnée, cette option s'applique au mode de chiffrement sélectionné à la fois pour KVM et pour le média virtuel. Après authentification, les données KVM et MV sont également transférées avec un chiffrement de 128 bits.
- **PC share mode (Mode PC-Share).** Permet de déterminer l'accès KVM à distance simultanément *global*, permettant ainsi à huit utilisateurs distants au maximum de se connecter simultanément à une unité Dominion KX II et d'afficher et gérer, simultanément, le même serveur cible par l'intermédiaire du dispositif. Cliquez sur la liste déroulante pour sélectionner l'une des options suivantes :
 - **Private (Privé) :** Pas de partage PC ; il s'agit du mode par défaut. Seul un utilisateur à la fois peut accéder au serveur cible.
 - **PC-Share :** Huit utilisateurs maximum (administrateurs ou non) peuvent accéder simultanément aux serveurs cible. Chaque utilisateur distant dispose du même contrôle au niveau du clavier et de la souris. Notez que des différences de contrôle se produisent si un utilisateur ne s'arrête pas de taper ou de déplacer la souris.
- **Mode de partage de média virtuel.** Cette option est activée uniquement si le mode PC-Share est activé. Lorsqu'elle est sélectionnée, cette option permet le partage des médias virtuels entre plusieurs utilisateurs ; cela signifie que de multiples utilisateurs peuvent accéder à la même session de médias virtuels. Le paramètre par défaut est sur le mode de désactivation.
- **Local device reset mode (Mode Réinitialisation du dispositif local).** Cette option spécifie les actions prises lorsque le bouton de réinitialisation du matériel (situé sur la partie arrière de l'unité) est enfoncé. Reportez-vous à [Bouton de réinitialisation](#) pour de plus amples informations. Sélectionnez l'une des options suivantes :
 - **Enable local factory reset (Activer la réinitialisation locale des paramètres d'usine)** (valeur par défaut). L'unité Dominion KX II retrouve les paramètres d'usine par défaut.
 - **Enable local admin password reset (Activer la réinitialisation locale du mot de passe administrateur).** Permet de réinitialiser le mot de passe d'administrateur local uniquement. Le mot de passe est restauré sur **raritan**.
 - **Disable all local resets (Désactiver toutes les réinitialisations locales).** Aucune action de réinitialisation est prise.

Vérifier si votre navigateur prend en charge le chiffrement AES

Si vous ne savez pas si votre navigateur utilise le chiffrement AES, vérifiez auprès de l'éditeur de votre navigateur ou consultez le site Web suivant en utilisant le navigateur avec la méthode de chiffrement que vous souhaitez vérifier : <https://www.fortify.net/sslcheck.html>. Ce site Web détecte la méthode de chiffrement de votre navigateur et fournit un rapport.

Contrôle d'accès IP

Le contrôle d'accès IP vous permet de contrôler l'accès à votre unité Dominion KX II. Le fait de configurer une Liste de Contrôle d'Accès (LCA) au niveau global pour votre unité KX permet de garantir que votre dispositif ne répondra pas aux paquets envoyés à partir d'adresses IP non autorisées. Le contrôle d'accès IP est global et affecte l'ensemble de l'unité KX. Cependant, vous pouvez également contrôler l'accès à votre unité au niveau du groupe. Reportez-vous à [LCA IP de groupes \(Liste de contrôle d'accès\)](#) pour de plus amples informations sur le contrôle à l'échelle du groupe.

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de Dominion KX II. Lorsque vous créez une liste de contrôle d'accès IP, si 127.0.0.1 se trouve dans la plage des adresses IP bloquées, vous n'aurez plus accès au port local de Dominion KX II.

Pour utiliser le contrôle d'accès IP :

- Ouvrez la page de contrôle d'accès IP via l'une des méthodes suivantes :
 - Sélectionnez **Security (Sécurité) > IP Access Control (Contrôle d'accès IP)** ou
 - cliquez sur le bouton **Set System ACL (Configurer le système LCA)** à la page [Paramètres réseau](#).

La page de contrôle d'accès IP s'ouvre :

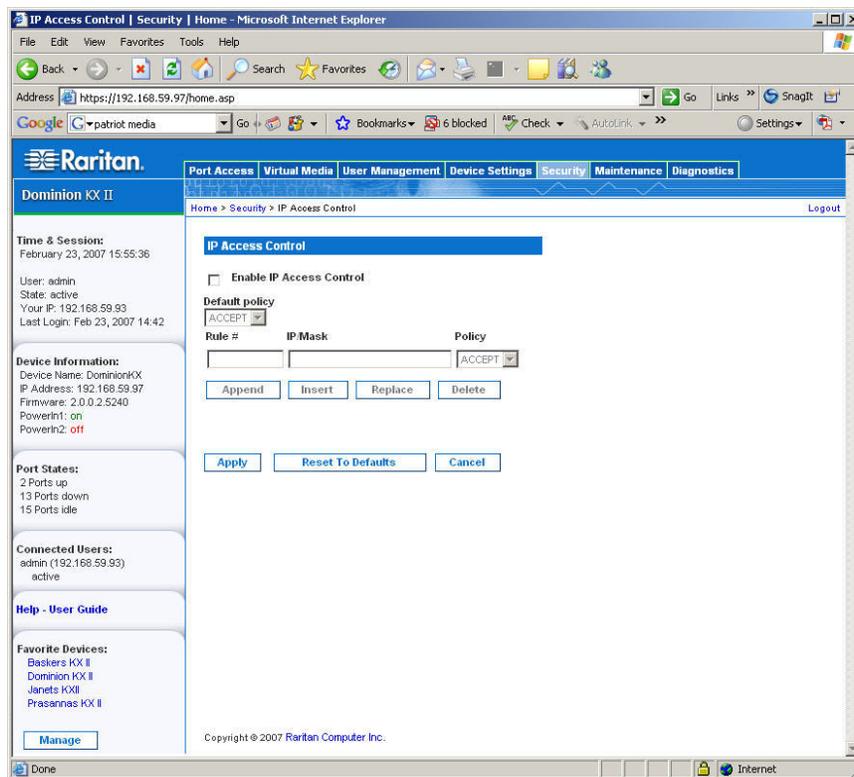


Figure 76 : Contrôle d'accès IP

- Cochez la case en regard de **Enable IP Access Control (Activer le contrôle de l'accès par IP)** pour autoriser le contrôle de l'accès par IP ainsi que les autres champs de la page.
- Sélectionnez la **stratégie par défaut**. Cette action concerne les adresses IP qui ne sont pas dans les plages spécifiées.
 - Accept (Accepter)**. Les adresses IP sont autorisées à accéder au dispositif Dominion KX II.
 - Drop (Refuser)**. Les adresses IP se voient refuser l'accès au dispositif Dominion KX II.

Pour ajouter (modifier) des règles :

1. Entrez l'adresse IP et le masque de sous-réseau dans le champ **IP/Mask (IP/masque)**.
2. Sélectionnez la stratégie à **partir** de la liste déroulante.
3. Cliquez sur **Append (Modifier)**. La règle est ajoutée au bas de la liste des règles.
4. Répétez les étapes 1 à 3 pour chacune des règles que vous souhaitez valider.

Pour insérer une règle :

1. Tapez une **règle (Rule #)**. Un numéro de règle est requis lorsque vous utilisez la commande Insérer.
2. Entrez l'adresse IP et le masque de sous-réseau dans le champ **IP/Mask (IP/masque)**.
3. Sélectionnez la stratégie à **partir** de la liste déroulante.
4. Cliquez sur **Insert (Insérer)**. Si le numéro de règle que vous venez de taper est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont déplacées d'une rangée vers le bas.

Pour remplacer une règle :

1. Spécifiez le numéro de la **règle** que vous souhaitez remplacer.
2. Entrez l'adresse IP et le masque de sous-réseau dans le champ **IP/Mask (IP/masque)**.
3. Sélectionnez la stratégie à **partir** de la liste déroulante.
4. Cliquez sur **Replace (Remplacer)**. Votre nouvelle règle remplace la règle d'origine dont le numéro est le même.

Pour supprimer une règle :

1. Spécifiez le numéro de la **règle** que vous souhaitez supprimer.
2. Cliquez sur **Supprimer**.
3. Vous êtes invité à confirmer la suppression. Cliquez sur **OK**.

Conseil : les numéros de règles vous permettent de mieux contrôler l'ordre de création des règles.

Chapitre 11 : Maintenance

Le menu de maintenance inclut les options suivantes : Audit Log (Journal d'audit), Device Information (Informations relatives au dispositif), Backup/Restore (Sauvegarde/Restauration), CIM Firmware Upgrade (Mise à niveau du firmware CIM), Firmware Upgrade (Mise à niveau du firmware du CIM), Factory Reset (Restauration des valeurs d'usine) (Dominion KX II Local Console uniquement), Upgrade Report (Rapport de mise à niveau) et Reboot (Redémarrage).

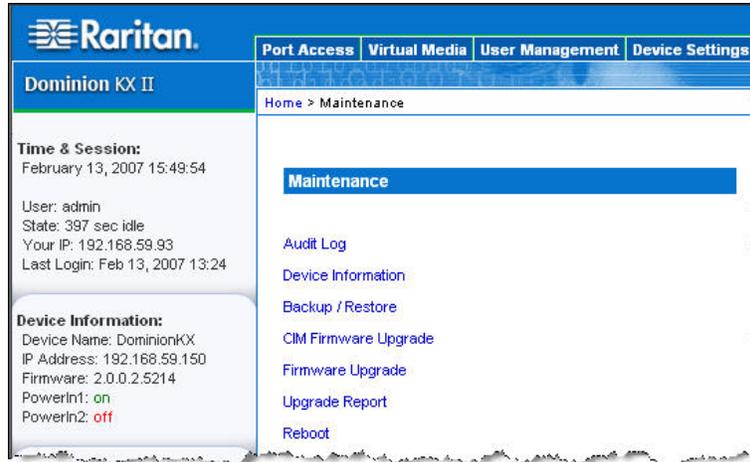


Figure 77 : Menu de maintenance

UTILISEZ :	POUR :	LOCAL	ACCES
Journal d'audit	Afficher les événements de Dominion KX II triés par date et par heure.	✓	✓
Informations relatives au dispositif	Afficher les informations sur Dominion KX II et ses modules d'interface pour ordinateurs (CIM).	✓	✓
Sauvegarde/Restauration	Sauvegarder et restaurer la configuration du dispositif KX II.		✓
Mise à niveau du firmware du CIM	Mettre à niveau vos CIM à l'aide des versions de firmware stockées dans la mémoire de Dominion KX II.	✓	✓
Mise à niveau du firmware	Mettre à niveau le firmware de votre Dominion KX II.		✓
Factory Reset (Restauration des valeurs d'usine)	Procéder à une restauration des valeurs d'usine.	✓	
Rapport de mise à niveau	Afficher les informations relatives aux dernières mises à niveau exécutées.	✓	✓
Redémarrage	Redémarrez l'unité Dominion KX II.	✓	✓

Journal d'audit

Un journal des événements du système Dominion KX II est créé.

Pour afficher le journal d'audit de votre unité Dominion KX II :

Sélectionnez **Maintenance > Audit Log (Journal d'audit)**. La page du journal d'audit s'ouvre :

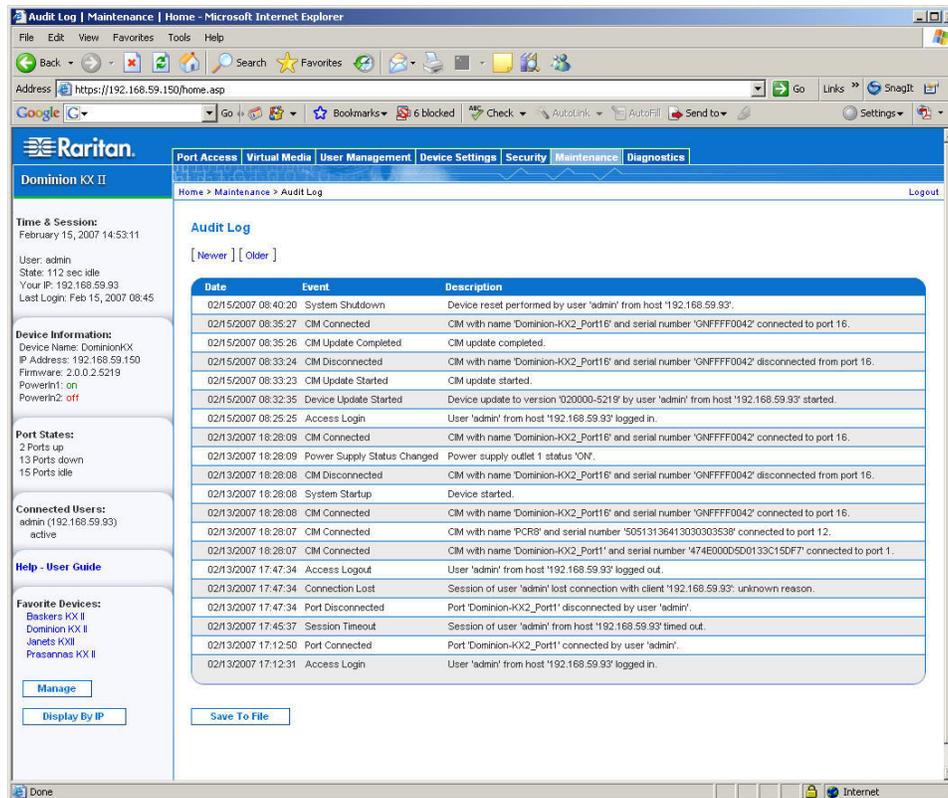


Figure 78 : Journal d'audit

La page du journal d'audit affiche les événements par date et heure (les événements les plus récents étant répertoriés en premier). Le journal d'audit fournit les informations suivantes :

- **Date.** La date et l'heure auxquelles l'événement s'est produit ; système des 24 heures.
- **Événement.** Le nom de l'événement tel que répertorié dans la page de gestion des événements.
- **Description.** Description détaillée de l'événement.

Pour enregistrer le journal d'audit :

Remarque : l'option d'enregistrement du journal d'audit est disponible uniquement sur la console distante Dominion KX II et non sur la console locale.

1. Cliquez sur le bouton **Save to File (Enregistrer sur le fichier)**. Une boîte de dialogue intitulée Fichier d'enregistrement s'ouvre.
2. Sélectionnez le nom et l'emplacement du fichier voulu, puis cliquez sur **Save (Enregistrer)**. Le journal d'audit est enregistré *localement* sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour naviguer dans le journal d'audit :

Utilisez les liens **[Older] [Plus ancien]** et **[Newer] [Plus récent]**.

Informations relatives au dispositif

La page des informations relatives au dispositif fournit des informations détaillées sur votre dispositif Dominion KX II et sur les modules d'interface pour ordinateurs en cours d'utilisation. Ces informations sont utiles si vous avez besoin de contacter le support technique Raritan.

Pour afficher les informations sur votre Dominion KX II et ses modules d'interface pour ordinateurs (CIM) :

Sélectionnez **Maintenance > Device Information (Informations relatives au dispositif)**.
La page des informations relatives au dispositif s'ouvre :

The screenshot shows the Raritan web interface for a Dominion KX II device. The browser window is titled "Device Information | Maintenance | Home - Microsoft Internet Explorer". The address bar shows "https://192.168.59.97/home.asp". The Raritan logo is in the top left. The navigation menu includes "Port Access", "Virtual Media", "User Management", "Device Settings", "Security", "Maintenance", and "Diagnostics". The "Maintenance" menu is selected, and the "Device Information" page is displayed. The page content is as follows:

Time & Session:
Apr 09, 2007 10:44:47
User: admin
State: 1 min idle
Your IP: 192.168.59.41
Last Login: Apr 09, 2007 09:53

Device Information:
Device Name: DominionKX
IP Address: 192.168.59.97
Firmware: 2.0.0.2.5418
PowerIn1: on
PowerIn2: off

Port States:
2 Ports up
13 Ports down
15 Ports idle

Connected Users:
admin (192.168.59.41)
1 min idle

Help - User Guide

Favorite Devices:
Baskers KX II
Dominion KX II
[Manage](#)
[Display By IP](#)

Device Information

Model: DKX2-416
Hardware Revision: 0x44
Firmware Version: 2.0.0.2.5418
Serial Number: HKC6B00016
MAC Address: 00:0d:5d:01:33:c1

CIM Information

Port	Name	Type	Firmware Version	Serial Number
1	Dominion-KX2_Port1	VM	2A36	HJW7250771
3	Dominion-KX2_Port3	PCIM	N/A	GNFFFFFFFFFFFF7565
8	Dominion-KX2_Port8	PowerStrip	00B2	PQ16A00058

Copyright © 2007 Raritan Computer Inc.

Figure 79 : Informations relatives au dispositif

Les informations suivantes relatives au Dominion KX II sont fournies : **Modèle, Numéro de version du matériel et du firmware, Numéro de série et Adresse MAC.**

Les informations suivantes relatives aux CIM en cours d'utilisation sont fournies : **Port (numéro), Nom, Type** (de CIM : DCIM, PCIM, Barrette d'alimentation ou VM), **Versión du Firmware et Numéro de série.**

Sauvegarde et restauration

A partir de la page de sauvegarde/restauration, vous pouvez sauvegarder et restaurer les paramètres et la configuration de votre Dominion KX II. Outre l'utilisation de la sauvegarde et de la restauration pour la continuité des opérations, vous pouvez utiliser cette fonction pour économiser du temps. Par exemple, vous pouvez donner rapidement un accès à votre équipe à partir d'un autre Dominion KX II en sauvegardant les paramètres de configuration utilisateur du KX II en cours d'utilisation et en restaurant ces paramètres sur le nouveau KX II. Vous pouvez également configurer un Dominion KX II et copier sa configuration sur de multiples dispositifs KX II.

Pour accéder à la page de sauvegarde/restauration :

Sélectionnez **Maintenance > Backup/Restore (Sauvegarde/restauration)**. La page de sauvegarde/restauration s'ouvre :

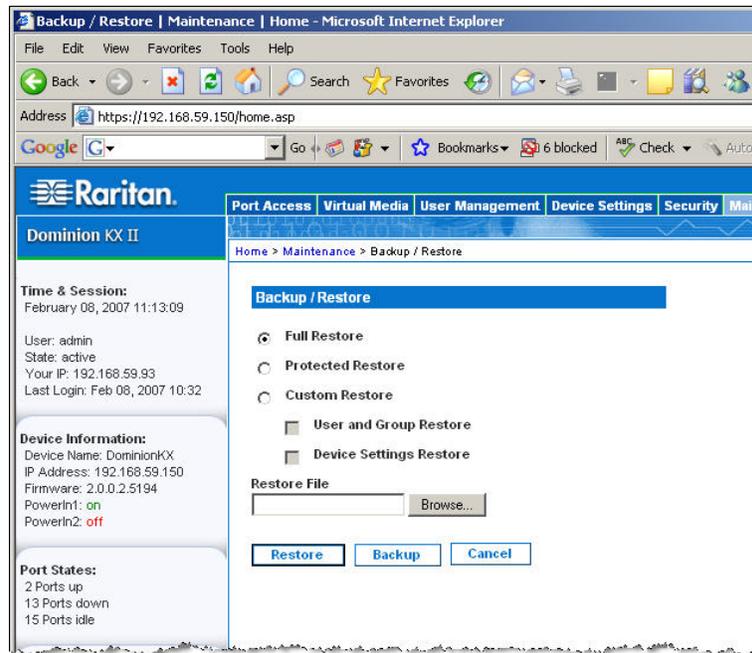


Figure 80 : Sauvegarde/Restauration

Remarque : les sauvegardes sont toujours des sauvegardes système complètes. Les restaurations, en revanche, peuvent être totales ou partielles selon votre critère de sélection.

Pour sauvegarder votre Dominion KX II :

1. Cliquez sur **Backup (Sauvegarder)**. La boîte de dialogue File Download (Téléchargement de fichier) s'ouvre :
2. Cliquez sur **Save (Enregistrer)**. La boîte de dialogue Enregistrement sous s'affiche.
3. Sélectionnez l'emplacement, spécifiez un nom de fichier, puis cliquez sur **Save (Enregistrer)**. La boîte de dialogue Download Complete (Téléchargement terminé) s'ouvre.
4. Cliquez sur **Fermer**. Le journal de sauvegarde est enregistré *localement* sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour réinitialiser votre Dominion KX II :

AVERTISSEMENT : soyez prudent lorsque vous réinitialisez votre Dominion KX II sur une version antérieure. Les noms d'utilisateur et mot de passes spécifiés au moment de la sauvegarde sont restaurés. Si vous ne vous souvenez plus des anciens noms d'utilisateur et mots de passe administratifs, vous n'avez plus accès à KX II.

Par ailleurs, si vous utilisiez une adresse IP différente au moment de la sauvegarde, cette adresse IP est également restaurée. Si la configuration utilise DHCP, il se peut que vous souhaitiez procéder à cette opération uniquement lorsque vous avez accès au port local pour vérifier l'adresse IP après la mise à jour.

1. Sélectionnez le type de restauration que vous souhaitez exécuter :
 - **Full Restore (Restauration totale).** Restauration complète de l'intégralité du système ; utilisée généralement à des fins de sauvegarde et de restauration classiques.
 - **Protected Restore (Restauration protégée).** Tout est restauré à l'exception des informations spécifiques au dispositif telles que le numéro de série, l'adresse MAC, l'adresse IP, le nom, les noms de port, etc. Avec cette option, vous pouvez configurer un Dominion KX II et copier cette configuration sur plusieurs dispositifs KX II.
 - **Custom Restore (Restauration personnalisée).** Via cette option, vous pouvez sélectionner User and Group Restore (Restauration des utilisateurs et des groupes), Device Settings Restore (Restauration des paramètres du dispositif) ou les deux. Cochez les cases appropriées :
 - **User and Group Restore (Restauration des utilisateurs et des groupes).** Cette option inclut uniquement les informations relatives aux utilisateurs et aux groupes. Utilisez cette option pour configurer rapidement des utilisateurs sur un autre Dominion KX II.
 - **Device Settings Restore (Restauration des paramètres du dispositif).** Cette option comprend les paramètres du dispositif uniquement. Utilisez cette option pour copier rapidement les informations relatives au dispositif.
2. Cliquez sur le bouton **Browse (Naviguer)**. Une boîte de dialogue intitulée Choisir le fichier s'ouvre.
3. Localisez et sélectionnez le fichier de sauvegarde approprié puis cliquez sur **Open (Ouvrir)**. Le fichier sélectionné est répertorié dans le champ **Restore File (Restaurer le fichier)**.
4. Cliquez sur **Restore (Restaurer)**. La configuration (en fonction du type de restauration sélectionnée) est restaurée.

Mise à niveau du CIM

Utilisez cette procédure pour mettre à niveau les CIM à l'aide des versions de firmware stockées dans la mémoire de votre unité Dominion KX II. En général, tous les CIM sont mis à niveau lorsque vous mettez à niveau le firmware du dispositif via la page [Mise à niveau de firmware](#). Utilisez la page de mise à niveau des CIM pour mettre à niveau les nouveaux CIM.

Remarque : seuls D2CIM-VUSB et D2CIM-PWR peuvent être mis à niveau à partir de cette page.

Pour mettre à niveau les CIM à l'aide de la mémoire de Dominion KX II :

1. Sélectionnez **Maintenance > CIM Firmware Upgrade (Mise à niveau du firmware du CIM)**. La page de mise à niveau du CIM à partir de KX Flash s'ouvre :

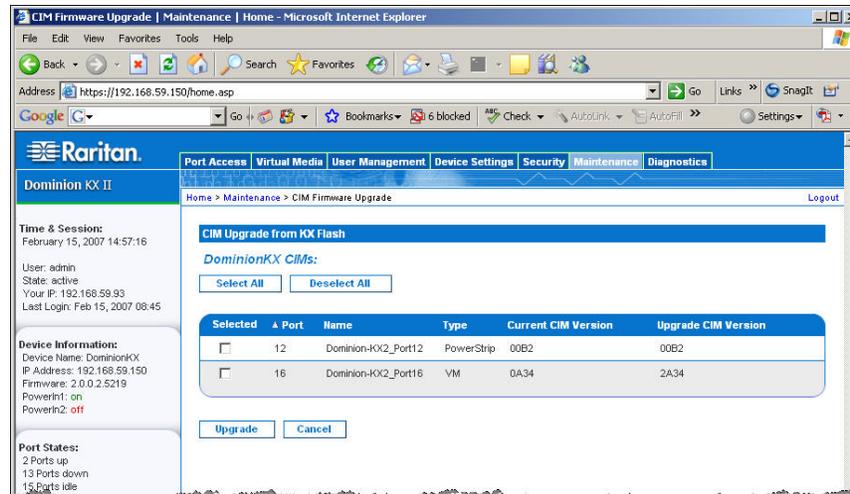


Figure 81 : Mise à niveau du CIM à partir de KX Flash

2. Le **Port** (numéro), le **Nom**, le **Type**, la **Version actuelle du CIM** et la **Mise à niveau de la version du CIM** sont affichés pour faciliter l'identification des CIM.
3. Cochez la case **Selected (Sélectionné)** pour chacun des CIM que vous voulez mettre à niveau.

*Conseil : Utilisez les boutons **Select All (Sélectionner tout)** et **Deselect All (Désélectionner tout)** pour sélectionner (ou désélectionner) rapidement tous les CIM.*

4. Cliquez sur le bouton **Upgrade (Mettre à niveau)**. Vous êtes invité à confirmer la mise à niveau.
5. Cliquez sur **OK** pour continuer la mise à niveau. Les barres de progression s'affichent lors de la mise à niveau. La mise à niveau prend environ 2 minutes (ou moins) par CIM.

Pour quitter sans procéder à la mise à niveau :

Cliquez sur le bouton **Cancel (Annuler)**.

Mise à niveau du firmware

Utilisez la page de mise à niveau du firmware pour mettre à niveau le firmware de votre unité Dominion KX II ainsi que tous les CIM qui lui sont rattachés. Cette page est disponible pour la *console distante KX II* uniquement.

Important : Ne mettez pas votre unité Dominion KX II hors tension et ne déconnectez pas les CIM pendant la mise à niveau ; le cas échéant, cela risque fortement de détériorer l'unité ou les CIM.

Pour mettre à niveau votre unité Dominion KX II :

1. Localisez le fichier de distribution du firmware Raritan (*.RFP) sur la page Web des mises à niveau du firmware Raritan : <http://www.raritan.com/support/firmwareupgrades> et téléchargez le fichier.
2. Décompressez le fichier. Veuillez lire attentivement l'ensemble des instructions incluses dans les fichiers ZIP du firmware avant de procéder à la mise à niveau du dispositif.

Remarque : copiez le fichier de mise à jour du firmware sur un PC local avant de procéder au téléchargement. Ne chargez pas le fichier depuis un lecteur connecté en réseau.

3. Sélectionnez **Maintenance > Firmware Upgrade (Mise à niveau du firmware)**. La page de mise à niveau du firmware s'ouvre :

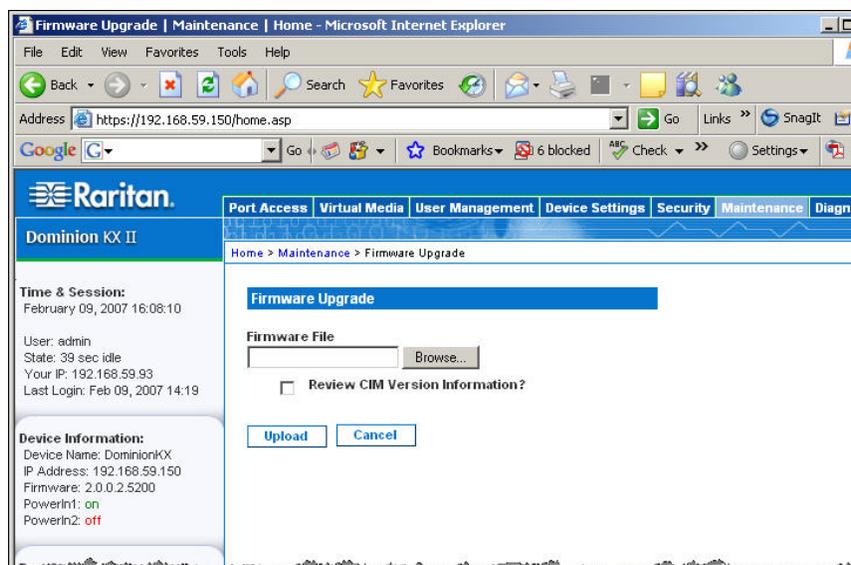


Figure 82 : Mise à niveau du firmware

4. Cliquez sur le bouton **Browse (Naviguer)** pour localiser le répertoire à l'emplacement où vous avez décompressé le fichier de mise à niveau.
5. Sélectionnez la case **Review CIM Version Information? (Vérifier les informations relatives à la version du CIM ?)** si vous souhaitez afficher les informations relatives aux versions des CIM utilisés.
6. Cliquez sur **Upload (Télécharger)** dans la page de mise à niveau du firmware. Les informations concernant les numéros de version et de mise à niveau sont affichées pour votre confirmation (si vous avez opté pour la vérification des informations relatives au CIM, ces informations sont également affichées) :

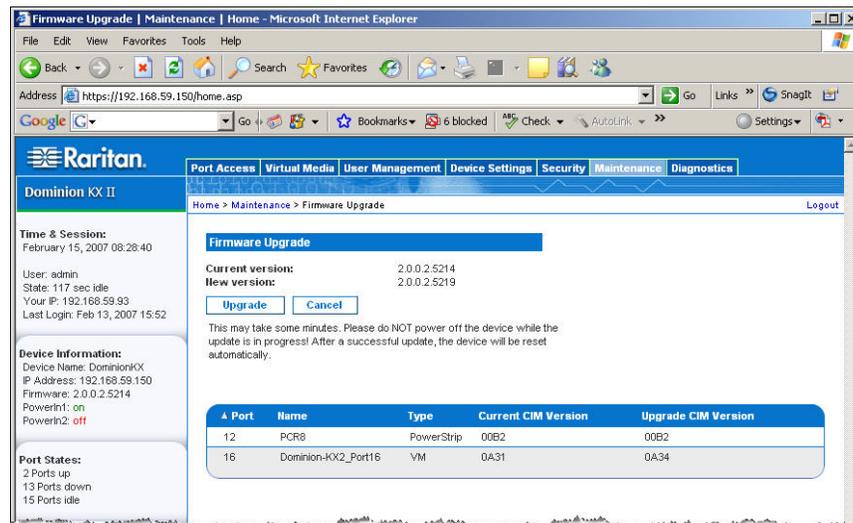


Figure 83 : Vérification de la mise à niveau du firmware

Remarque : A ce stade, les utilisateurs connectés sont déconnectés et toute nouvelle tentative de connexion est bloquée.

7. Cliquez sur **Upgrade (Mettre à niveau)**. Veuillez attendre la fin de la mise à niveau. Les informations sur l'état et les barres de progression s'affichent pendant la mise à niveau. Une fois la mise à niveau terminée, l'unité redémarre (1 bip est émis pour signaler le redémarrage).

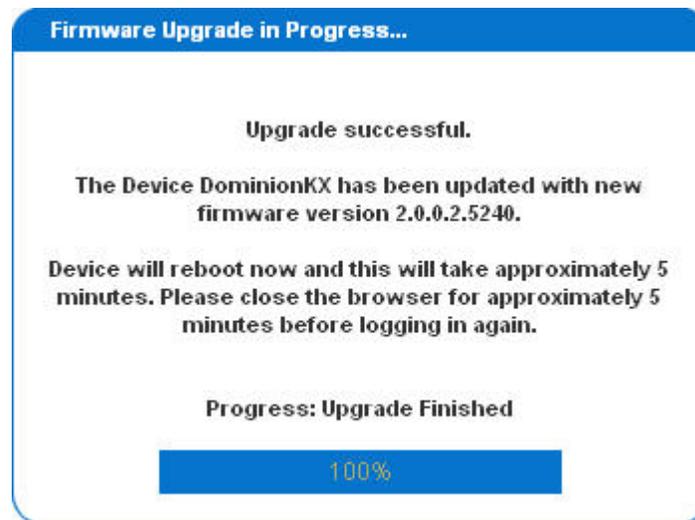


Figure 84 : Mise à niveau du firmware réussie

8. A l'invite, fermez le navigateur et attendez environ 5 minutes avant de vous connecter de nouveau à Dominion KX II.

Pour obtenir des informations sur la mise à niveau du firmware du dispositif via le Client MPC (Multi-Platform Client), consultez le *manuel d'utilisation Multi-Platform Client (MPC) de Raritan et Raritan Remote Client (RRC)*.

Rapport de mise à niveau

Dominion KX II fournit des informations relatives aux mises à niveau effectuées sur l'unité KX II et les CIM qui lui sont rattachés.

Pour afficher le rapport de mise à niveau :

Sélectionnez **Maintenance > Upgrade Report (Rapport de mise à niveau)**. La page du rapport de mise à niveau s'ouvre :

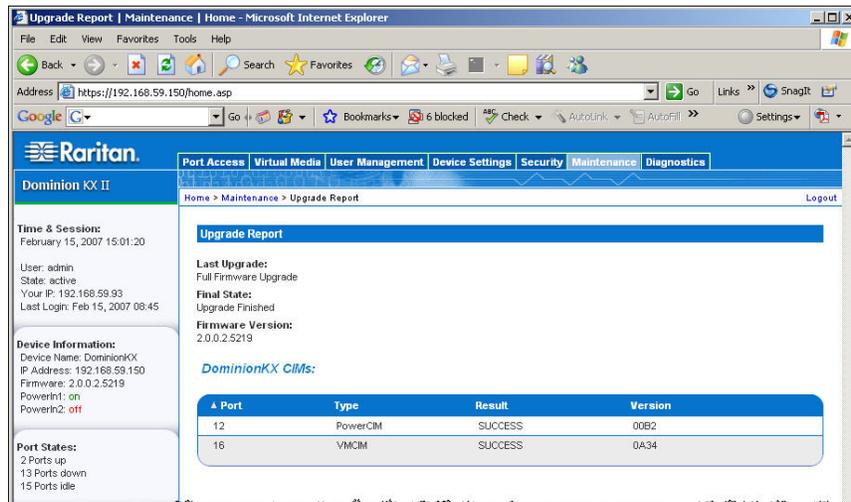


Figure 85 : Rapport de mise à niveau

Des informations sont fournies concernant la dernière mise à niveau exécutée pour Dominion KX II, ainsi que l'état final de cette mise à niveau et la version du firmware. Des informations relatives aux CIM sont également fournies :

- **Port.** Correspond au port sur lequel est connecté le CIM.
- **Type.** Correspond au type de CIM.
- **Result (Résultat).** Correspond au résultat de la mise à niveau (réussite ou échec).
- **Version.** Correspond à la version relative au firmware du CIM.

Redémarrage

La page de redémarrage constitue un moyen contrôlé et sûr de redémarrer votre unité Dominion KX II ; c'est la méthode recommandée pour le redémarrage du système.

Important : toutes les connexions KVM sont fermées et tous les utilisateurs déconnectés.

Pour redémarrer votre Dominion KX II :

1. Sélectionnez **Maintenance > Reboot (Redémarrer)**. La page de redémarrage s'ouvre :

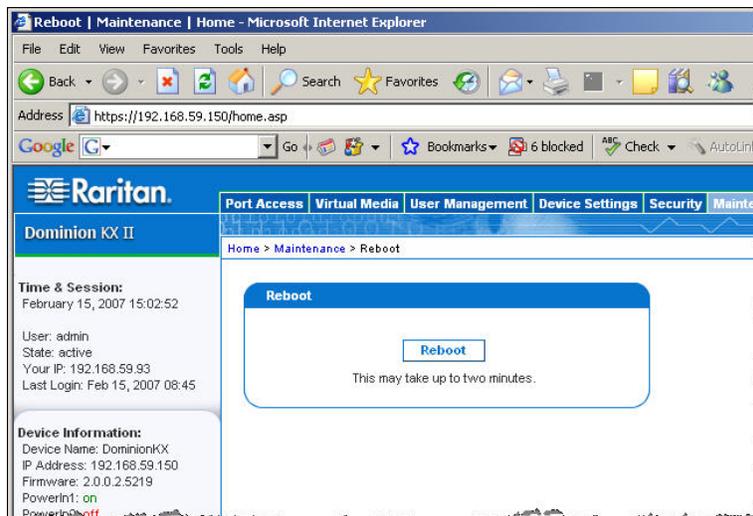


Figure 86 : Redémarrage

2. Cliquez sur le bouton **Reboot (Redémarrer)**. Vous êtes invité à confirmer l'opération :

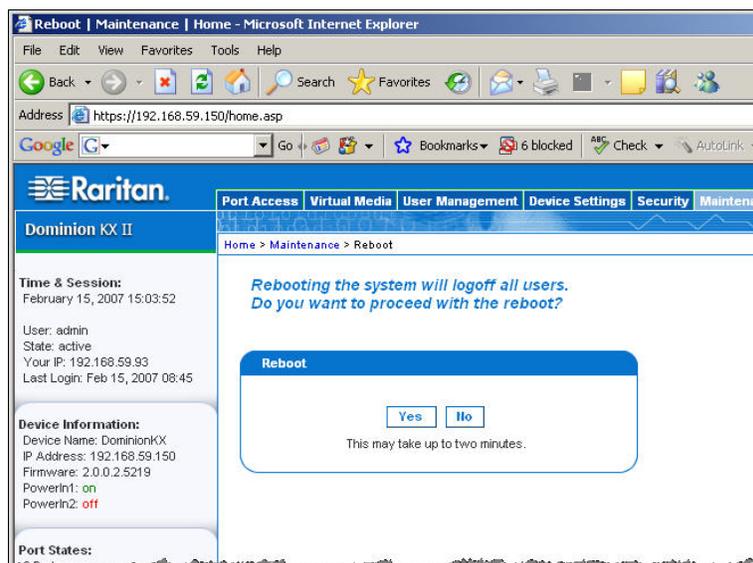


Figure 87 : Confirmation du redémarrage

3. Cliquez sur **Oui** pour procéder au redémarrage.

Pour quitter sans redémarrer :

Cliquez sur **Non**.

Chapitre 12 : Diagnostics

Menu Diagnostics

Les pages de diagnostics sont utilisées pour le dépannage et sont destinées avant tout à l'administrateur du dispositif KX II. Toutes les pages de diagnostics (sauf les diagnostics KX) exécutent les commandes de réseau standard ; les informations affichées sont le résultat de ces commandes.

Les options suivantes du menu Diagnostics vous permettent de déboguer et de configurer les paramètres réseau :

- Interface réseau
- Statistiques réseau
- Envoyer une commande Ping à l'hôte
- Tracer le parcours de réseau jusqu'à l'hôte

L'option Diagnostics KX a été conçue pour être utilisée conjointement au support technique Raritan.

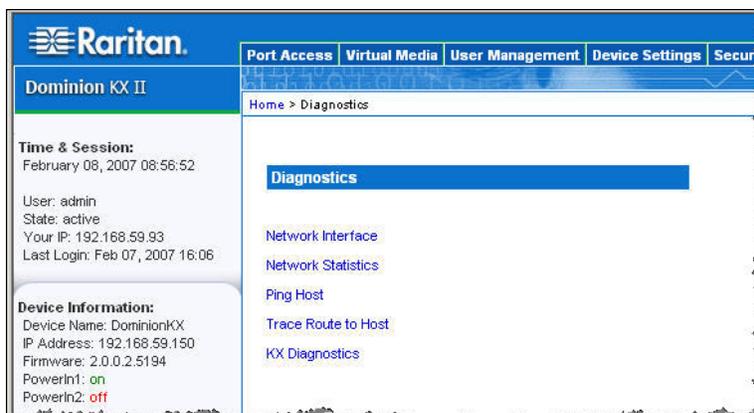


Figure 88 : Menu Diagnostics

UTILISEZ :	POUR :
Interface réseau	Obtenir l'état de l'interface réseau.
Statistiques réseau	Obtenir des statistiques sur le réseau.
Envoyer une commande Ping à l'hôte	Déterminer si un hôte spécifique peut être atteint via un réseau IP.
Tracer le parcours de réseau jusqu'à l'hôte	Déterminer l'ensemble du parcours jusqu'à l'hôte sélectionné.
KX Diagnostics (Diagnostics KX)	Travailler conjointement avec le support technique Raritan (<i>Console distante uniquement</i>) selon leurs instructions.

Page d'interface réseau

Dominion KX II fournit des informations sur l'état de votre interface réseau.

Pour afficher les informations relatives à votre interface réseau :

Sélectionnez **Diagnostics > Network Interface (Interface réseau)**. La page d'interface réseau s'ouvre :

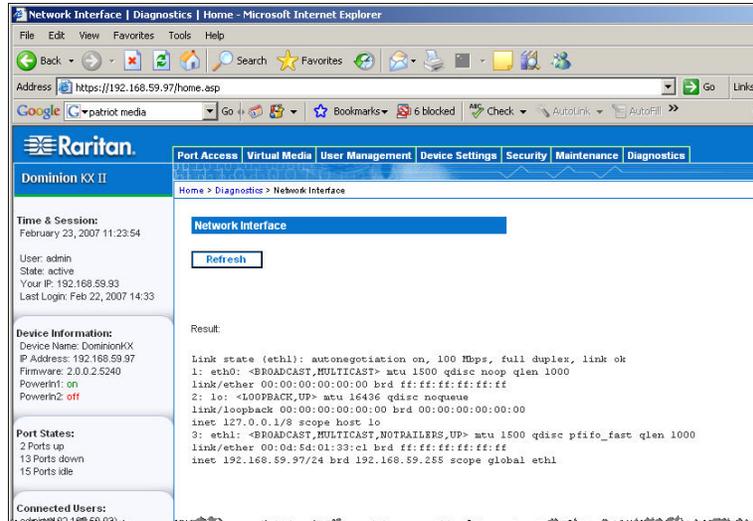


Figure 89 : Interface réseau

Les informations suivantes s'affichent :

- l'état de l'interface Ethernet (connecté ou pas)
- si la commande ping de la passerelle est activée ou non
- le port LAN en cours d'utilisation

Pour actualiser ces informations :

Cliquez sur le bouton **Refresh (Actualiser)**.

Page de statistiques réseau

Dominion KX II fournit des statistiques sur votre interface réseau.

Pour afficher les statistiques relatives à votre interface réseau :

1. Sélectionnez **Diagnostics > Network Statistics (Statistiques réseau)**. La page des statistiques réseau s'ouvre.
2. Sélectionnez l'option appropriée parmi celles de la liste déroulante **Options** :
 - **Statistics (Statistiques)**. Génère une page similaire à celle affichée ci-dessous :

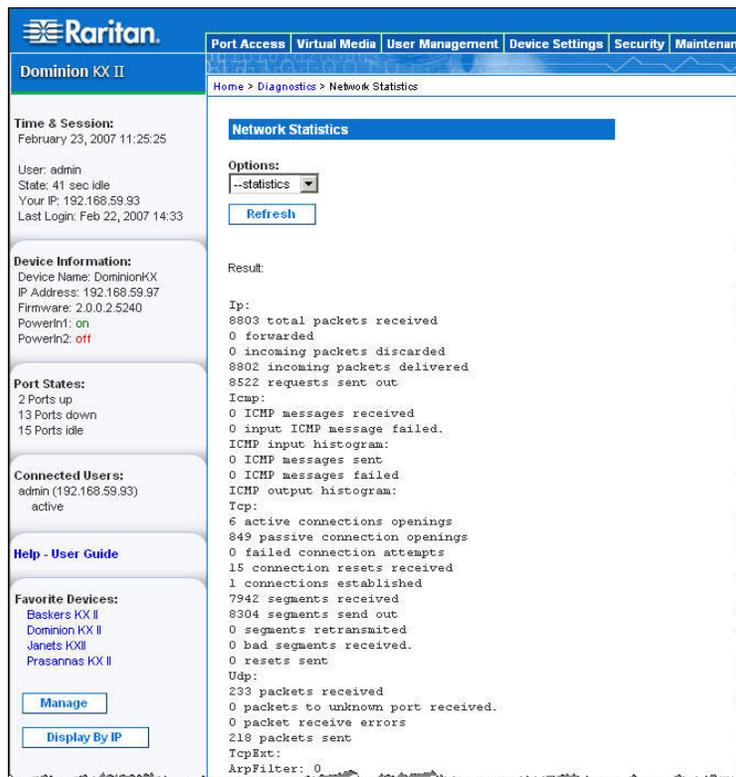


Figure 90 : Statistiques réseau (statistiques)

- **Interfaces**. Génère une page similaire à celle affichée ci-dessous :

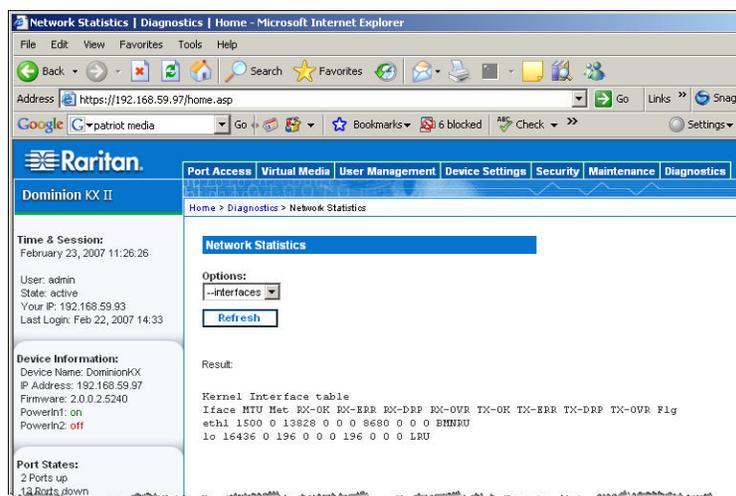


Figure 91 : Statistiques réseau (interfaces)

- **Route.** Génère une page similaire à celle affichée ci-dessous :

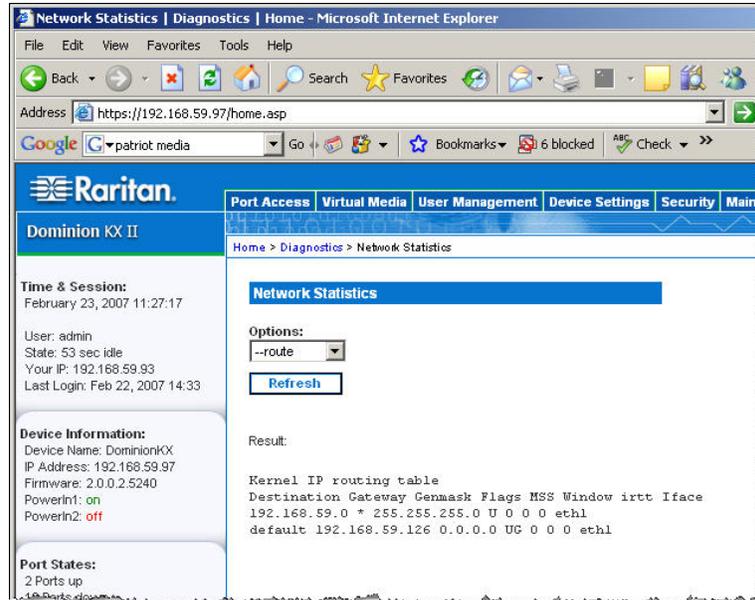


Figure 92 : Statistiques réseau (route)

3. Cliquez sur le bouton **Refresh (Actualiser)**.

Les informations concernées sont affichées dans le champ **Result (Résultat)**.

Page d'envoi de commande Ping à l'hôte

La commande Ping est un outil réseau qui permet de vérifier si un hôte ou une adresse IP spécifique est accessible via un réseau IP. Grâce à cette page Ping Host (Envoi d'une commande Ping à l'hôte), vous pouvez déterminer si un serveur cible ou toute autre unité Dominion KX II est accessible.

Pour envoyer une commande Ping à l'hôte :

1. Sélectionnez **Diagnostics > Ping Host (Envoyer une commande Ping à l'hôte)**. La page Ping Host s'ouvre :

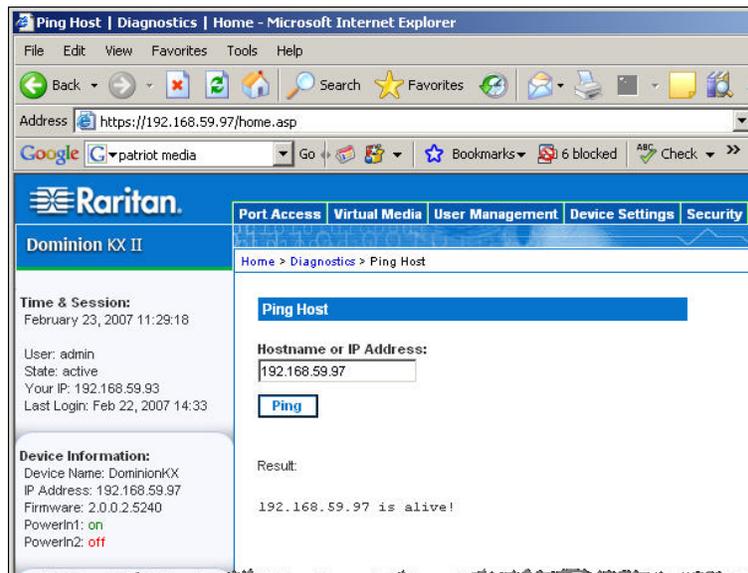


Figure 93 : Envoyer une commande Ping à l'hôte

2. Entrez le nom de l'hôte ou l'adresse IP dans le champ **Hostname or IP Address**.
3. Cliquez sur **Ping**. Les résultats de la commande Ping sont affichés dans le champ **Result (Résultat)**.

Page de détermination du parcours de réseau jusqu'à l'hôte

Cette page est un outil réseau permettant de tracer le parcours de réseau jusqu'au nom d'hôte ou jusqu'à l'adresse IP fournis.

Pour tracer le parcours de réseau jusqu'à l'hôte :

1. Sélectionnez **Diagnostics > Trace Route to Host (Tracer le parcours de réseau jusqu'à l'hôte)**. La page de détermination du parcours de réseau jusqu'à l'hôte s'ouvre :

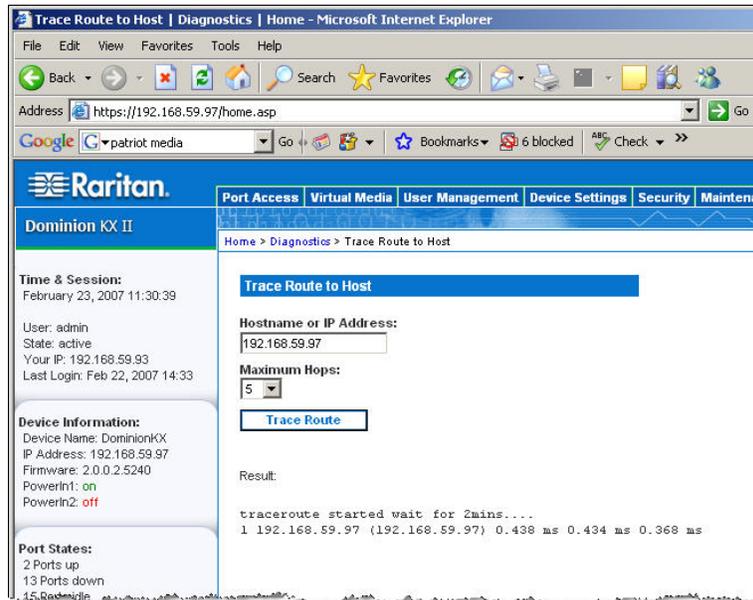


Figure 94 : Tracer le parcours de réseau jusqu'à l'hôte

2. Entrez le nom de l'hôte ou l'adresse IP dans le champ **Hostname or IP Address**.
3. Sélectionnez **Maximum Hops (Sauts maximum)** à partir de la liste déroulante (5 ou 10).
4. Cliquez sur le bouton **Trace Route (Tracer le parcours)**. La commande de détermination d'itinéraire est exécutée pour le nom d'hôte ou l'adresse IP, et le nombre de sauts maximum donnés. Les données de détermination de l'itinéraire sont affichées dans le champ **Result (Résultat)**.

KX Diagnostics (Diagnostics KX)

Remarque : cette page est en principe destinée aux techniciens de l'assistance à la clientèle. Vous pouvez l'utiliser uniquement lorsque le support technique Raritan vous guide dans le processus.

KX Diagnostics télécharge les informations de diagnostics de Dominion KX II vers l'ordinateur client. Trois opérations peuvent être effectuées sur cette page.

- **Interface de ligne de commande.** Activez ou désactivez la fonctionnalité d'interface de ligne de commande. Grâce à cette fonction, un technicien-contrôle Raritan peut ouvrir un client SSH standard, se connecter à l'unité et exécuter les fonctions de diagnostics à distance.
- **Scripts de diagnostics.** Exécutez un script spécial fourni par le support technique Raritan lors d'une session de débogage d'erreurs critiques. Le script est téléchargé vers l'unité et exécuté. Une fois le script exécuté, vous pouvez télécharger les messages de diagnostics via le bouton Save to File (Enregistrer sur fichier).
- **Journal de diagnostics KX.** Téléchargez la capture d'écran des messages de diagnostics à partir de l'unité KX II sur le client. Ce fichier crypté est alors envoyé au support technique Raritan ; seul Raritan est en mesure d'interpréter ce fichier.

Remarque : cette page n'est accessible que par les utilisateurs disposant des droits d'administrateurs.

Pour exécuter les diagnostics du système KX II :

1. Sélectionnez **Diagnostics > KX Diagnostics**. La page des diagnostics KX s'ouvre.

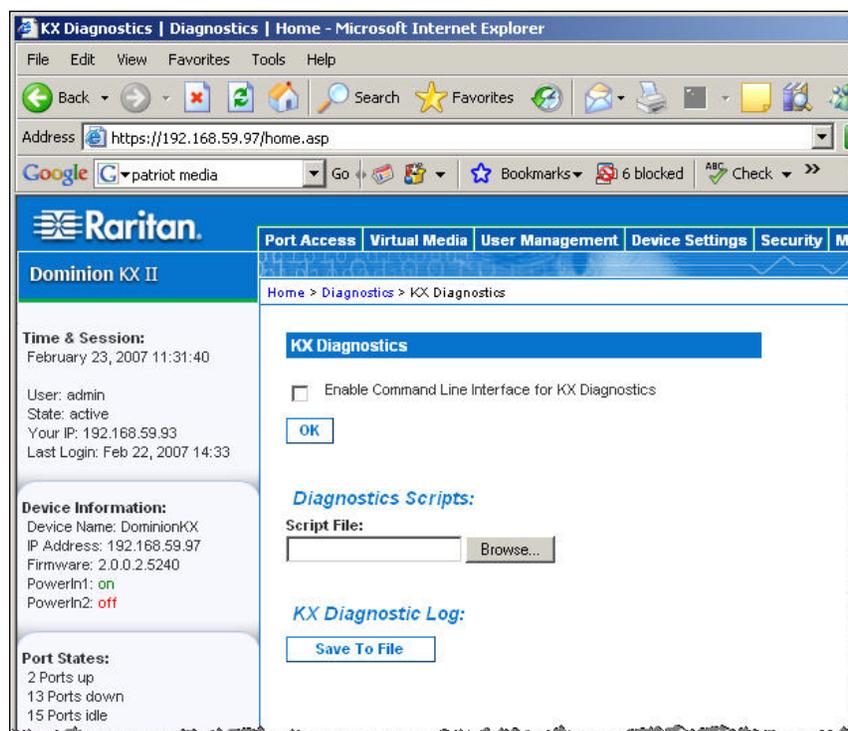


Figure 95 : KX Diagnostics (Diagnostics KX)

2. Pour activer l'interface de ligne de commande de façon à ce qu'elle puisse être utilisée par le support technique Raritan :

Remarque : le port UDP 21 est requis pour cette fonction.

- a. Cochez la case **Enable Command Line Interface for KX Diagnostics (Activer l'interface de ligne de commande des diagnostics KX)**.
 - b. Cliquez sur **OK**.
 - c. Le port UDP 21 doit être ouvert et accessible par le support technique Raritan.
 - d. Le support technique Raritan a également besoin de connaître le mot de passe administratif d'accès au KX II.
 - e. Une fois le test du support technique Raritan achevé, configurez de nouveau le port 21 sur son état initial.
3. **Pour exécuter un fichier de script de diagnostics qui vous a été envoyé par courrier électronique par le support technique Raritan :**
 - a. Récupérez le fichier de diagnostics fourni par Raritan et décompressez-le au format Zip si nécessaire.
 - b. Utilisez le bouton **Browse (Naviguer)**. Une boîte de dialogue intitulée Choisir le fichier s'ouvre.
 - c. Localisez et sélectionnez le fichier de diagnostics.
 - d. Cliquez sur **Ouvrir**. Le fichier s'affiche dans le champ **Script File (Fichier de script)**.



Figure 96 : Scripts de diagnostics

- e. Cliquez sur **Run Script (Exécutez le script)**.
 - f. Envoyez ce fichier au support technique Raritan en suivant les instructions indiquées à l'étape 4.
4. **Pour créer un fichier de diagnostics à envoyer au support technique Raritan.**
 - a. Cliquez sur le bouton **Save to File (Enregistrer sur le fichier)**. La boîte de dialogue File Download (Téléchargement de fichier) s'ouvre.



Figure 97 : Téléchargement de fichier

- b. Cliquez sur **Save (Enregistrer)**. La boîte de dialogue Enregistrement sous s'affiche.
- c. Localisez le répertoire voulu puis cliquez sur **Save (Enregistrer)**.
- d. Envoyez ce fichier par courrier électronique au support technique Raritan.

Chapitre 13 : Console locale KX II

Console locale KX II

Dominion KX II fournit un accès et une administration sur le rack via son port local qui intègre une interface utilisateur graphique par navigateur pour commuter rapidement et aisément entre différents serveurs. La console locale Dominion KX II fournit une connexion analogique directe aux serveurs connectés. Les performances sont les mêmes que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur. La console locale KX II fournit les mêmes fonctionnalités d'administration que la console distante Dominion KX II.

La console locale Dominion KX II prend en charge les claviers de langue suivants : anglais (Etats-Unis), anglais (Royaume-Uni), allemand, français, japonais, coréen, chinois simplifié et chinois traditionnel.

Remarque : vous pouvez utiliser le clavier pour le chinois, le japonais et le coréen à des fins d'affichage uniquement ; l'entrée de données dans la langue locale n'est pas prise en charge pour le moment en ce qui concerne les fonctions de la console locale KX II.

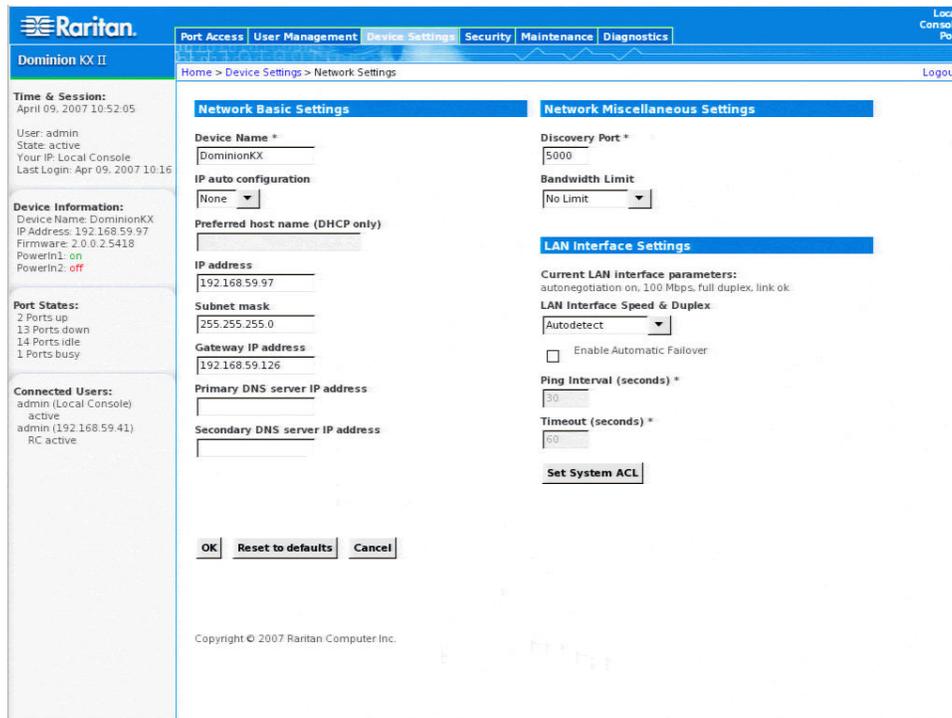


Figure 98 : Console locale Dominion KX II

Connexions physiques

Les connexions physiques des ports locaux peuvent être localisées sur la partie arrière de l'unité Dominion KX II :



Figure 99 : Panneau Local User (Utilisateur local) sur Dominion KX II

Ecran : reliez le port vidéo HD15 (femelle) à un écran VGA Multisync standard.

Clavier : reliez le port clavier Mini-DIN6 (femelle) à un clavier PS/2 standard *ou* l'un des ports USB de type A (femelle) à un clavier USB standard.

Souris : reliez le port souris Mini-DIN6 (femelle) à une souris PS/2 standard *ou* un des ports USB de type A (femelle) à une souris USB standard.

Bouton de réinitialisation

Vous trouverez le bouton de réinitialisation sur la partie arrière de l'unité Dominion KX II. Il est encastré pour éviter les pressions accidentelles (vous aurez besoin d'un objet pointu pour utiliser ce bouton).



Figure 100 : Bouton de réinitialisation (partie arrière de l'unité)

Les opérations effectuées lorsque le bouton de réinitialisation est enfoncé sont définies dans l'interface utilisateur graphique. Reportez-vous à [Paramètres de sécurité, Cryptage et partage](#) pour de plus amples informations.

Remarque : Il est recommandé de sauvegarder le journal d'audit avant de procéder à la restauration des valeurs d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de restauration n'est pas enregistré dans le journal d'audit. Pour plus d'informations sur la sauvegarde du journal d'audit, consultez [Journal d'audit](#).

Pour réinitialiser l'unité :

1. Mettez l'unité Dominion KX II hors tension.
2. Utilisez un objet pointu pour appuyer sur le bouton de réinitialisation et pour le maintenir.
3. **Tout en continuant à maintenir enfoncé le bouton de réinitialisation**, mettez à nouveau sous tension l'unité Dominion KX II.
4. Continuer de le maintenir enfoncé pendant 5 à 10 secondes. Une fois l'unité réinitialisée, deux bips courts signalent la fin du processus.

Démarrage de la console locale KX II

Utilisateurs simultanés

La console locale Dominion KX II dispose d'un chemin permettant d'accéder indépendamment à aux serveurs cible connectés. L'utilisation de la console locale n'empêche pas les autres utilisateurs de se connecter en même temps sur le réseau. Même lorsque des utilisateurs sont connectés à distance au Dominion KX II, vous pouvez toujours accéder à vos serveurs simultanément à partir du rack via la console locale.

Sécurité et authentification

Pour utiliser la console locale Dominion KX II, vous devez d'abord vous authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe valides. Dominion KX II dispose d'un schéma d'authentification et de sécurité entièrement intégré que vous accédez à Dominion KX II par le biais du réseau ou du port local. Dans les deux cas, Dominion KX II permet l'accès uniquement à ces serveurs pour lequel un utilisateur dispose des autorisations d'accès (reportez-vous à [Gestion des utilisateurs](#) pour obtenir des informations supplémentaires sur la spécification des paramètres de sécurité et d'accès au serveur).

Si votre Dominion KX II a été configuré pour des services d'authentification externe (LDAP, RADIUS, Active Directory ou CC-SG de Raritan), les demandes d'authentification au niveau du port de la console locale sont également authentifiées à l'aide du service d'authentification externe.

Remarque : vous pouvez également ne spécifier aucune authentification pour l'accès à la console locale ; cette option est recommandée uniquement dans les environnements sécurisés.

Pour utiliser la console locale KX II :

1. vous avez besoin d'un clavier, d'une souris et d'un affichage vidéo branchés sur les ports locaux situés à l'arrière de l'unité Dominion KX II. Reportez-vous à [Connexions physiques](#) pour de plus amples informations sur les connexions des ports locaux.
2. Démarrez l'unité Dominion KX II ; l'interface de la console locale KX II s'affiche.

Interface de la console locale KX II

L'interface de la console locale KX II est pratiquement identique à celle de la console distante KX II. Lorsqu'il y a des différences, elles sont indiquées dans le présent manuel d'utilisation. Reportez-vous à [Interfaces utilisateur](#), [Console locale KX II](#), and [Arborescence de menus de la console KX II](#) pour de plus amples informations.

Résolutions disponibles

La console locale KX II offre les résolutions suivantes pour prendre en charge divers écrans :

- 800 x 600
- 1 024 x 768
- 1 280 x 1 024

Chacune de ces résolutions prend en charge un taux de rafraîchissement de 60 Hz et 75 Hz.

Accès aux serveurs cible

Affichage du serveur

Une fois connecté à la console locale de KX II, la page d'accès aux ports s'ouvre. Cette page répertorie tous les ports de Dominion KX II, les serveurs cible connectés ainsi que leur état et leur disponibilité.

The screenshot shows the Raritan web interface for a Dominion KX II device. The main content area is titled "Port Access" and contains a table with the following data:

Port Number	Port Name	Status	Availability
1	Dominion-KX2_Port1	down	idle
2	Dominion-KX2_Port2	down	idle
3	LPMachine	up	busy
4	Dominion-KX2_Port4	down	idle
5	Dominion-KX2_Port5	down	idle
6	Dominion-KX2_Port6	down	idle
7	Dominion-KX2_Port7	down	idle
8	Dominion-KX2_Port8	up	idle
9	Dominion-KX2_Port9	down	idle
10	Dominion-KX2_Port10	down	idle
11	Dominion-KX2_Port11	down	idle
12	Dominion-KX2_Port12	down	idle
13	Dominion-KX2_Port13	down	idle
15	Dominion-KX2_Port15	down	idle
16	Dominion-KX2_Port16	down	idle

Additional information visible in the interface includes:

- Time & Session:** March 02, 2007 14:27:49; User: admin; State: active; Your IP: Local Console; Last Login: Mar 02, 2007 14:12.
- Device Information:** Device Name: DominionKX; IP Address: 192.168.59.97; Firmware: 2.0.0.2.5282; PowerIn1: on; PowerIn2: off.
- Port States:** 2 Ports up, 13 Ports down, 14 Ports idle, 1 Ports busy.
- Connected Users:** admin (Local Console) active; admin (192.168.59.93) RC active.

Figure 101 : Accès au port de la console locale

Les serveurs cible sont triés initialement par numéro de port ; vous pouvez modifier l'affichage pour trier en fonction de n'importe laquelle des colonnes.

- **Port Number (Numéro de port).** Les ports sont numérotés de 1 au nombre total de ports disponibles pour l'unité Dominion KX II. Notez que les ports connectés aux barrettes d'alimentation ne figurent pas dans la liste, ce qui génère des blancs dans la séquence des numéros de port.
- **Port Name (Nom du port).** Le nom du port de Dominion KX II ; il est défini au préalable sur Dominion-KX2-Port#, mais vous pouvez le remplacer par un nom plus évocateur. Lorsque vous cliquez sur le lien Port Name (Nom du port), un menu d'actions s'affiche. Reportez-vous à [Menu d'actions relatives aux ports](#) pour davantage d'informations sur les options de menu disponibles.
- **Status (Etat).** L'état est soit up, soit down.
- **Availability (Disponibilité).** Valid Values per (Valeurs valides par) incluent Idle (ralenti), Connected (connecté), Busy (occupé) ou Unavailable (indisponible).

Pour modifier l'ordre de tri :

Cliquez sur l'en-tête de la colonne que vous souhaitez trier. La liste des serveurs cible est triée par cette colonne.

Raccourci-clavier

Comme l'interface de la console locale de Dominion KX II est entièrement remplacée par l'interface du serveur cible auquel vous accédez, un raccourci-clavier est utilisé pour vous permettre de basculer entre les différentes interfaces.

Le raccourci-clavier du port local vous permet d'accéder rapidement à l'interface utilisateur de la console locale de KX II lorsqu'un serveur cible est en cours d'affichage. L'opération définie par défaut est d'appuyer deux fois rapidement sur la touche **Arrêt défil**, mais vous pouvez aussi spécifier toute autre combinaison de touches (reportez-vous à la page de paramétrage des ports locaux) comme raccourci-clavier. Reportez-vous à [Paramètres du port Local](#) pour de plus amples informations.

Accès à un serveur cible

Pour accéder à un serveur cible :

1. Cliquez sur l'option **Port Name (Nom du port)** associée à la cible à laquelle vous souhaitez accéder. Le **menu d'actions relatif aux ports** apparaît.
2. Sélectionnez **Connect (Connecter)** dans le [Menu d'actions relatives aux ports](#). L'affichage vidéo bascule sur l'interface du serveur cible.

Retour à l'interface de la console locale de KX II

Important : le raccourci-clavier par défaut de la console locale de KX II consiste à appuyer deux fois sans interruption sur la touche Arrêt défil. Cette combinaison de touches peut être modifiée dans la page [Paramètres du port local](#).

Pour revenir à la console locale de KX II à partir du serveur cible :

Appuyez rapidement deux fois sur le raccourci-clavier (touche **Arrêt défil** par défaut). L'affichage écran passe de l'interface du serveur cible à celle de la console locale de Dominion KX II.

Administration du port local

Dominion KX II peut être géré soit par la console locale KX II, soit par la console distante KX II. Veuillez noter que la console locale KX II fournit également l'accès aux fonctions d'administration suivantes :

- Local Port Settings (Paramètres du port local)
- Factory Reset (Restauration des valeurs d'usine)

Remarque : seuls les utilisateurs disposant des droits d'administrateur peuvent accéder à ces fonctions.

Paramètres du port local (Console locale KX II uniquement)

A partir de la page de paramétrage des ports locaux, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale KX II, notamment le clavier, le raccourci-clavier du port local, le délai de commutation de l'écran, le mode d'économie d'alimentation, les paramètres de résolution de l'interface utilisateur locale et l'authentification d'utilisateur local.

Remarque : cette fonction est disponible sur la console locale Dominion KX II uniquement.

Pour configurer les paramètres du port local :

1. Sélectionnez **Device Settings (Paramètres du dispositif) > Local Port Settings (Paramètres du port local)**. La page de configuration du port local s'ouvre :

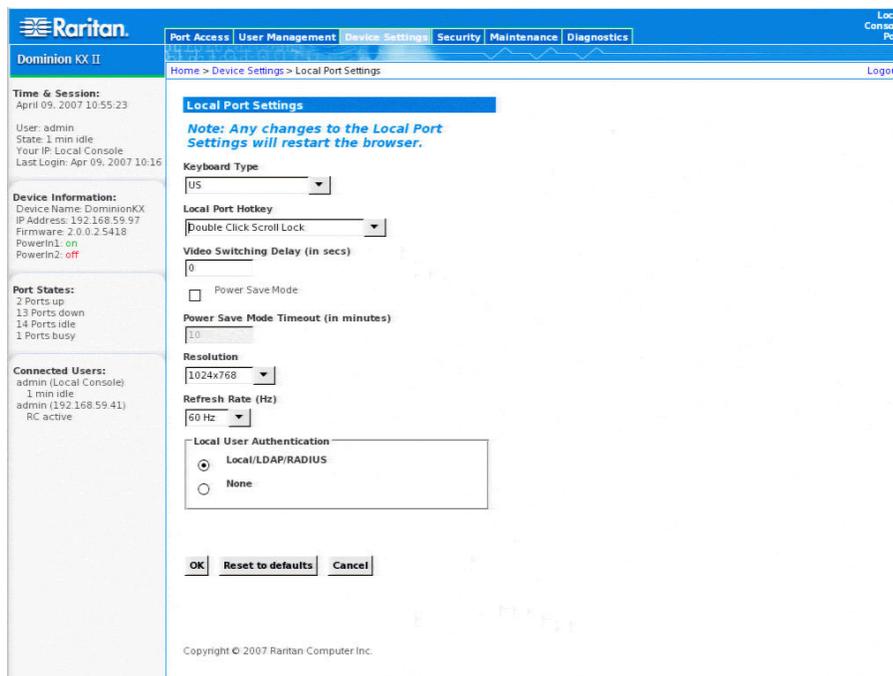


Figure 102 : Local Port Settings (Paramètres du port local)

2. Sélectionnez le type de **clavier approprié (Keyboard Type)** parmi les options de la liste déroulante :
 - US
 - US/International
 - Anglais Royaume-Uni
 - Français
 - Allemand
 - Japonais (JIS)
 - Chinois simplifié
 - Chinois traditionnel
 - Coréen

3. Sélectionnez le raccourci-**clavier du port local**. Le raccourci-clavier du port local vous permet de retourner à l'interface de la console locale KX II lorsque l'interface d'un serveur cible est en cours d'affichage. Le paramètre par défaut est **Double Click Scroll Lock (Double-clic sur la touche Arrêt défil)**, mais vous pouvez également sélectionner à la place n'importe quelle combinaison de touches à partir de la liste déroulante :

HOTKEY (RACCOURCI-CLAVIER) :	APPUYEZ SUR :
Double-clic sur la touche Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur la touche Verr num	La touche Verr num deux fois sans interruption
Double-clic sur la touche Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur la touche Alt gauche	La touche Alt gauche deux fois sans interruption
Double-clic sur la touche Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption

4. Réglez **Video Switching Delay (Délai de commutation écran)** entre 0 et 5 secondes, le cas échéant. En général, la valeur 0 est utilisée à moins que vous n'ayez besoin de plus de temps (certains écrans nécessitent plus de temps pour commuter la vidéo).
5. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique :
- Cochez la case **Power Save Mode** (Mode d'économie d'alimentation).
 - Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.
6. Sélectionnez la **résolution** de la console locale KX II à partir de la liste déroulante :
- 800 x 600
 - 1 024 x 768
 - 1 280 x 1 024
7. Sélectionnez le taux de **rafraîchissement** dans la liste déroulante :
- 60 Hz
 - 75 Hz
8. Sélectionnez le type d'**authentification d'utilisateur local** :
- **Local/LDAP/RADIUS**. C'est l'option recommandée; pour plus d'informations sur le processus d'authentification, consultez les sections [Authentification à distance](#) et [Authentification et autorisation](#).
 - **Aucun**. Il n'y a pas de processus d'authentification pour l'accès à la console locale. Cette option est recommandée pour les *environnements sécurisés uniquement*.
9. Cliquez sur **OK**.

Pour quitter la page sans enregistrer les modifications :

cliquez sur **Cancel (Annuler)**.

Pour réinitialiser les paramètres par défaut :

cliquez sur **Reset to Defaults (Restaurer les paramètres par défaut)**.

Restauration des valeurs d'usine (Console locale KX II uniquement)

Remarque : cette fonction est disponible sur la console locale Dominion KX II uniquement.

Dominion KX II offre plusieurs types de réinitialisation des modes à partir de l'interface utilisateur de la console locale.

Remarque : Il est recommandé de sauvegarder le journal d'audit avant de procéder à la restauration des valeurs d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de restauration n'est pas enregistré dans le journal d'audit. Pour plus d'informations sur la sauvegarde du journal d'audit, consultez [Journal d'audit](#).

Pour procéder à une restauration des valeurs usine :

1. Sélectionnez **Maintenance > Factory Reset (Restauration des valeurs d'usine)**. La page de restauration des valeurs d'usine s'ouvre.

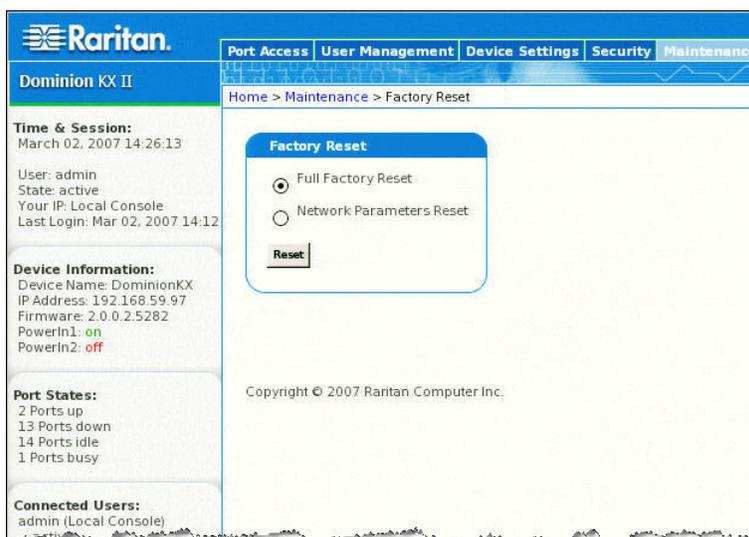


Figure 103 : Restauration des valeurs d'usine (Console locale uniquement)

2. Sélectionnez l'option de restauration appropriée.

- **Full Factory Reset (Restauration intégrale des valeurs d'usine) :** Supprime la totalité de la configuration et restaure les paramètres par défaut d'usine de l'unité dans leur intégralité. Notez que toute association de gestion avec CommandCenter est interrompue. En raison du caractère intégral de cette réinitialisation, vous êtes invité à confirmer la restauration des valeurs d'usine.
- **Network Parameter Reset (Restauration des paramètres réseau) :** Restaure les valeurs d'usine [à partir de Device Settings (Paramètres du dispositif) > Network Settings (Paramètres réseau)] des paramètres réseau de l'unité.

IP auto configuration (Configuration IP automatique)
Adresse IP
Masque de sous-réseau
Adresse IP de passerelle
Adresse IP du serveur DNS primaire
Adresse IP du serveur DNS secondaire
Port de détection
Limitation de bande passante
Vitesse & Duplex de l'interface LAN
Activer le basculement automatique
Intervalle Ping (secondes)
Temporisation (secondes)

Vous êtes invité à confirmer cette opération car tous les paramètres réseau seront effacés définitivement.

3. Cliquez sur **Reset (Réinitialiser)** pour continuer. Vous êtes invité à confirmer la restauration des valeurs d'usine.
4. Cliquez sur **Really Reset (Oui, réinitialiser)** pour continuer. Une fois l'opération effectuée, l'unité Dominion KX II redémarre automatiquement.

Chapitre 14 : CC Unmanage

Présentation

Lorsqu'un dispositif Dominion KX II est sous le contrôle de CommandCenter Secure Gateway et que vous tentez d'accéder au dispositif directement à l'aide de la console distante de Dominion KX II, le message suivant s'affiche (après l'entrée d'un nom d'utilisateur et d'un mot de passe valides) :



Figure 104 : Message du dispositif géré par CC-SG

Retrait de Dominion KX II de la gestion CC-SG

A moins que la gestion de Dominion KX II par CC-SG ne soit suspendue, vous ne pouvez pas accéder au dispositif directement. Toutefois, si KX II ne reçoit pas les messages de détection de collision de CommandCenter (par ex., CommandCenter n'est pas sur le réseau), vous pouvez suspendre la gestion de KX II par CC-SG afin de pouvoir accéder au dispositif. Vous pouvez le faire par l'intermédiaire de la fonction CC Unmanage.

Remarque : les autorisations de maintenance sont requises pour l'utilisation de cette fonction.

Si aucun message de détection de collision n'est reçu, le message suivant s'affiche lorsque vous essayez d'accéder au dispositif directement :

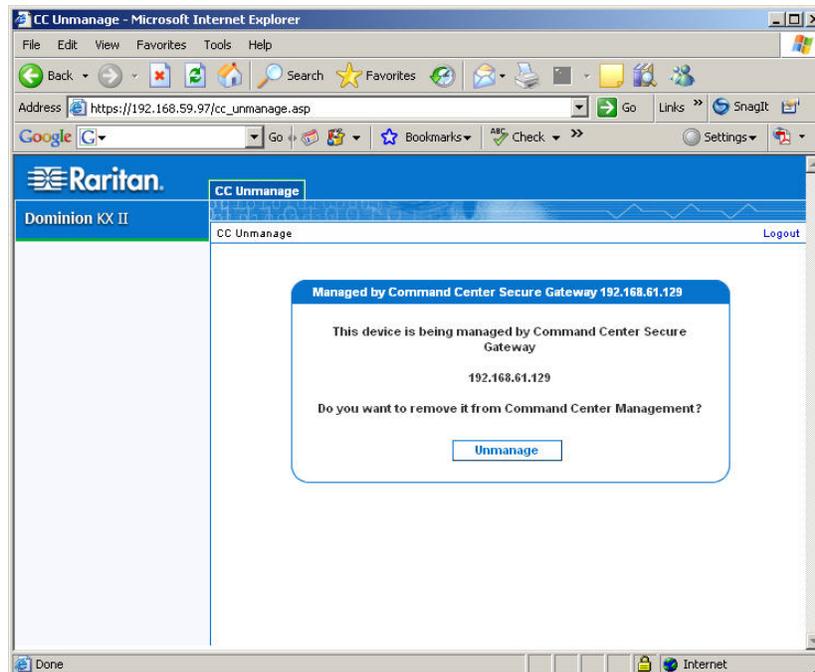


Figure 105 : Suspendre la gestion par CC-SG

Pour suspendre la gestion du dispositif par CC-SG (pour utiliser CC Unmanage) :

1. Cliquez sur le bouton **Unmanage**. Vous êtes invité à confirmer l'opération :



Figure 106 : Confirmer CC Unmanage

2. Cliquez sur le bouton **Really Unmanage**. Un message s'affiche pour confirmer que le dispositif n'est plus placé sous le contrôle de CC.

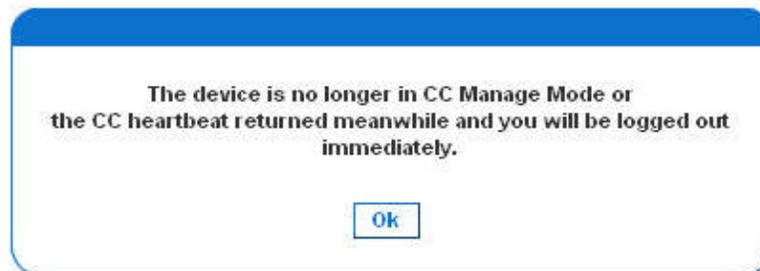


Figure 107 : Dispositif retiré de la gestion CC

3. Cliquez sur **OK**. La page d'accès aux ports s'ouvre.

Annexe A : Caractéristiques

Impératifs d'environnement

EN FONCTIONNEMENT	
Température	0°C - 40°C (32°F - 104°F)
Humidité résiduelle	20 à 85 %
Altitude	S/O
Vibrations	5-55-5 HZ, 0, 38mm, 1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O
A L'ARRET	
Température	0°C - 50°C (32°F - 122°F)
Humidité résiduelle	10 à 90 %
Altitude	S/O
Vibrations	5-55-5 HZ, 0, 38mm, 1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O

Spécifications physiques

N° DE RÉFÉRENCE	DKX2-116	DKX2-132	DKX2-216	DKX2-232	DKX2-416	DKX2-432
Description de l'élément de ligne	Dominion KX II à 16 ports avec accès réseau et port local 1 utilisateur ; média virtuel, double alimentation	Dominion KX II à 32 ports avec accès réseau et port local 1 utilisateur ; média virtuel, double alimentation	Dominion KX II à 16 ports avec accès réseau et port local 2 utilisateurs ; média virtuel, double alimentation	Dominion KX II à 32 ports avec accès réseau et port local 2 utilisateurs ; média virtuel, double alimentation	Dominion KX II à 16 ports avec accès réseau et port local 4 utilisateurs ; média virtuel, double alimentation	Dominion KX II à 32 ports avec accès réseau et port local 4 utilisateurs ; média virtuel, double alimentation
Poids	8,95 lbs ; 3,9 kg	9,0 lbs ; 4,1 kg	8,59 lbs ; 3,9 kg	9,0 lbs ; 4,1 kg	9,04 lbs ; 4,1 kg	9,48 lbs ; 4,3 kg
Dimensions du produit (LxPxH)	1,75" x 17,32" x 11,4" 44 mm x 439 mm x 290 mm	1,75" x 17,32" x 11,4" 44 mm x 439 mm x 290 mm	1,75" x 17,32" x 11,4" 44 mm x 439 mm x 290 mm	1,75" x 17,32" x 11,4" 44 mm x 439 mm x 290 mm	1,75" x 17,32" x 11,4" 44 mm x 439 mm x 290 mm	1,75" x 17,32" x 11,4" 44 mm x 439 mm x 290 mm
Poids à l'expédition	14,85 lbs ; 6,7 kg	14,9 lbs ; 6,8 kg	14,49 lbs ; 6,6 kg	14,9 lbs ; 6,8 kg	14,94 lbs ; 6,8 kg	15,38 lbs ; 7,0 kg
Dimensions à l'expédition (LxPxH)	22" x 16,6" x 6,5" 559 mm x 422 mm x 165 mm	22" x 16,6" x 6,5" 559 mm x 422 mm x 165 mm	22" x 16,6" x 6,5" 559 mm x 422 mm x 165 mm	22" x 16,6" x 6,5" 559 mm x 422 mm x 165 mm	22" x 16,6" x 6,5" 559 mm x 422 mm x 165 mm	22" x 16,6" x 6,5" 559 mm x 422 mm x 165 mm
Code UPC	785813624055	785813624079	785813624086	785813625021	785813625359	785813625380
Alimentation	Alimentation double 100/240 V 50/60 Hz 0,6 A 25,4 watts	Alimentation double 100/240 V 50/60 Hz 0,6 A 26 watts	Alimentation double 100/240 V 50/60 Hz 0,6 A 26,3 watts	Alimentation double 100/240 V 50/60 Hz 0,6 A 27 watts	Alimentation double 100/240 V 50/60 Hz 1 A 62 watts	Alimentation double 100/240 V 50/60 Hz 1 A 64 watts

Spécifications électriques

PARAMETRE	VALEUR
Entrée	
Fréquences nominales	50/60 Hz
Plage de tension nominale	100/240 V c.a.
Courant alternatif efficace maximal	0,6 A max.
Plage de fonctionnement en courant alternatif	100 à 240 V c.a. (+-10 %), 47 à 63 Hz
Sortie	
+5 V c.c., +12 V c.c.	S/O
-5 V c.c., -12 V c.c.	S/O
Puissance de sortie c.c. maximale	S/O
Consommation c.a. maximale	S/O
Dissipation thermique maximale	S/O
Puissance apparente nominale	S/O

Modules d'interface pour ordinateurs

N° DE RÉFÉRENCE	D2CIM-VUSB	DCIM-PS2	DCIM-USB	DCIM-SUSB
Description de l'élément de ligne	Module d'interface pour ordinateurs Dominion KX II [Port USB avec média virtuel]	Module d'interface pour ordinateurs Dominion KX I & II [Port PS/2]	Module d'interface pour ordinateurs Dominion KX I & II [Port USB]	Module d'interface pour ordinateurs Dominion KX I & II [Port USB pour Sun]
Poids du produit	0,2 lb	0,2 lb	0,2 lb	0,2 lb
Dimensions du produit (LxPxH)	33 mm x 76 mm x 15 mm	33 mm x 76 mm x 15 mm	33 mm x 76 mm x 15 mm	33 mm x 76 mm x 15 mm
Poids à l'expédition	0,2 lb	0,2 lb	0,2 lb	0,2 lb
Dimensions à l'expédition (LxPxH)	7,2" x 9" x 0,6"	7,2" x 9" x 0,6"	7,2" x 9" x 0,6"	7,2" x 9" x 0,6"
Code UPC	785813332004	785813338532	785813338518	785813338556

N° DE RÉFÉRENCE	DCIM-SUN	D2CIM-PWR	D2CIM-VUSB-32PAC	D2CIM-VUSB-64PAC
Description de l'élément de ligne	Module d'interface pour ordinateurs Dominion KX I & II [Port Sun, vidéo HD15]	Module d'interface pour ordinateurs Dominion KX II pour barrettes d'alimentation à distance	Dispositif de retour de 32 D2CIM-VUSB	Dispositif de retour de 64 D2CIM-VUSB
Poids du produit	0,2 lb	0,2 lb	6,4 lb	12,8 lb
Dimensions du produit (LxPxH)	33 mm x 76 mm x 15 mm	33 mm x 76 mm x 15 mm	(33 mm x 76 mm x 15 mm)*32	(1.3 mm x 3.0 mm x 0.6 mm)*64
Poids à l'expédition	0,2 lb	0,2 lb	8,01 lb	18,13 lb
Dimensions à l'expédition (LxPxH)	7,2" x 9" x 0,6"	7,2" x 9" x 0,6"	21,65"x12,20"x4,33"	22,64"x9,45"x12,99"
Code UPC	785813338549	785813332011	785813332028	785813332035

Connexion à distance

Réseau : Ethernet 10BASE-T, 100BASE-T et 1000BASE-T (Gigabit)

Protocoles : TCP/IP, UDP, SNMP, HTTP, HTTPS, RADIUS, LDAP

Propriétés KVM

Clavier : PS/2 ou USB

Souris : PS/2 ou USB

Vidéo : VGA

Ports TCP et UDP utilisés

- **HTTP, port 80** – toutes les requêtes reçues par Dominion KX II via le protocole HTTP (port 80) sont automatiquement transmises à HTTPS pour garantir une sécurité complète. Pour plus de facilité, Dominion KX II répond au port 80 (les utilisateurs n'ont ainsi pas à saisir explicitement « https :// » dans le champ URL pour accéder à Dominion KX II) tout en préservant un niveau complet de sécurité.
- **HTTPS, port 443** – ce port est utilisé uniquement dans un seul but : envoyer les clients Web de Dominion KX II (Console KX II, MPC) à l'utilisateur. Aucun autre type de communication n'a lieu sur ce port. Si vous ne souhaitez pas utiliser les fonctions Web de Dominion KX II et préférez plutôt utiliser le logiciel client installé fourni sur le CD-ROM, vous pouvez empêcher l'accès au port 443 par l'intermédiaire de votre pare-feu. Dominion KX II fonctionnera toujours.
- **Protocole Dominion KX II (KVM sur IP Raritan), port 5000 configurable** – à l'exception des ports cités ci-dessus, toutes les communications vers Dominion KX II ont lieu sur un port TCP unique et configurable. Le port défini par défaut est le port 5000. Vous pouvez néanmoins configurer ce paramètre de manière à utiliser le port TCP de votre choix (à l'exception des ports 80 et 443). Pour plus de détails sur la façon de configurer ce paramètre, reportez-vous à [Paramètres réseau](#).
- **SNTP (serveur de temps) sur le port UDP 123 configurable (facultatif)** – Dominion KX II peut, à l'aide d'une fonction facultative, synchroniser son horloge interne sur un serveur de temps central. Cette fonction nécessite l'utilisation du port UDP 123 (le port standard pour SNTP). Elle peut également être configurée sur le port de votre choix.
- **LDAP sur les ports 389 et 636 configurables (facultatif)** – si Dominion KX II est configuré de manière à authentifier à distance les connexions des utilisateurs par l'intermédiaire du protocole LDAP, le port 389 et 636 est utilisé. Le système peut également être configuré pour utiliser le port de votre choix.
- **RADIUS sur le port 1812 configurables (facultatif)** – si Dominion KX II est configuré de manière à authentifier à distance les connexions des utilisateurs par l'intermédiaire du protocole RADIUS, le port 1812 ou 1813 est utilisé. Le système peut également être configuré pour utiliser le port de votre choix.
- **Gestion RADIUS sur le port configurable 1813** – si Dominion KX II est configuré de manière à authentifier à distance les connexions des utilisateurs par l'intermédiaire du protocole RADIUS et qu'il utilise également la gestion RADIUS pour la création du journal des événements, le port 1813 ou un port supplémentaire de votre choix est utilisé pour transmettre les notifications du journal.
- **SYSLOG sur le port UDP 514 configurable** – si Dominion KX II est configuré pour envoyer des messages à un serveur Syslog, les ports indiqués sont utilisés pour la communication (utilise le port UDP 514).
- **Ports SNMP UDP par défaut (facultatif)** – le port 161 est utilisé pour l'accès SNMP entrant/sortant, en lecture/écriture, et le port 162 est utilisé pour le trafic sortant des traps SNMP.
- **Port UDP 21** – Le port 21 est utilisé pour l'interface de ligne de commande de Dominion KX II (lorsque vous travaillez avec le support technique Raritan).

Distance de connexion et résolution vidéo du serveur cible

La distance maximale prise en charge dépend de plusieurs facteurs y compris le type/la qualité du câble Cat5, le type de serveur, le fabricant du serveur, le pilote et l'écran vidéo, les conditions de l'environnement et les attentes de l'utilisateur. Le tableau suivant indique la distance maximale du serveur cible pour différentes résolutions vidéo et taux de rafraîchissement :

RESOLUTION VIDEO	TAUX DE RAFRAICHISSEMENT	DISTANCE MAXIMALE
1 600 x 1 200	60	50 ft (15 m)
1 280 x 1 024	60	100 ft (30 m)
1 024 x 768	60	150 ft (45 m)

L'utilisation des modules Paragon CIM n'augmente pas la distance entre le Dominion KX II et le serveur cible.

En raison de la diversité des types et fabricants de serveurs, des versions de systèmes d'exploitation, des pilotes vidéo, etc. et de la nature subjective de la qualité vidéo, Raritan ne peut pas garantir les performances sur toutes les distances et dans tous les environnements.

Reportez-vous à [Résolutions vidéo prises en charge](#) pour les résolutions vidéo prises en charge par Dominion KX II.

Annexe B : Mise à jour du schéma LDAP

Remarque : les procédures de ce chapitre ne doivent être effectuées que par des utilisateurs confirmés.

Renvoi des informations relatives aux groupes d'utilisateurs

Utilisez les informations de ce chapitre pour renvoyer les informations relatives aux groupes d'utilisateurs (et faciliter le processus d'autorisation), une fois l'authentification réussie.

A partir de LDAP

Lorsque la demande d'authentification LDAP aboutit, Dominion KX II détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel appartient l'utilisateur. Votre serveur LDAP distant peut fournir ces noms de groupes d'utilisateurs en renvoyant un attribut désigné de la manière suivante :

```
rciusergroup          attribute type : chaîne
```

Il est possible que cette opération nécessite une extension de schéma sur votre serveur LDAP. Consultez l'administrateur de votre serveur d'authentification pour activer cet attribut.

In addition, la norme LDAP `memberOf` est utilisée.

A partir de Active Directory (AD) de Microsoft

Remarque : Seul un administrateur Active Directory confirmé doit tenter cette opération.

Le renvoi des informations relatives aux groupes d'utilisateurs à partir de Microsoft Active Directory pour Windows 2000 Server nécessite la mise à jour du schéma LDAP. Pour plus d'informations, consultez votre documentation Microsoft.

1. Installez le plug-in du schéma pour Active Directory – pour plus d'informations, consultez la documentation Microsoft Active Directory.
2. Lancez la console **Active Directory** et sélectionnez **Directory Schema (Schéma Active Directory)**.

Définition du registre pour autoriser les opérations d'écriture sur le schéma

Pour autoriser un contrôleur de domaine à écrire sur le schéma, vous devez définir une entrée de registre permettant les mises à jour du schéma.

1. Cliquez avec le bouton droit de la souris sur le noeud racine **Active Directory Schema (Schéma Active Directory)** dans le volet de gauche de la fenêtre, puis cliquez sur **Operations Master (Maître d'opérations)**.
2. Cochez la case en regard de **The Schema may be modified on this Domain Controller (Le schéma peut être modifié sur ce contrôleur de domaine)**.
3. Cliquez sur **OK**.

Création d'un nouvel attribut

Pour créer de nouveaux attributs pour la classe `rciusergroup` :

1. Cliquez sur le symbole + en regard de **Active Directory Schema (Schéma Active Directory)** dans le volet de gauche de la fenêtre.
2. Cliquez avec le bouton droit de la souris sur **Attributes (Attributs)** dans le volet de gauche.
3. Cliquez sur **New (Nouveau)**, puis sélectionnez **Attribute (Attribut)**. Lorsque le message d'avertissement apparaît, cliquez sur **Continue (Continuer)** et la fenêtre **Create New Attribute (Créer un attribut)** s'affiche.

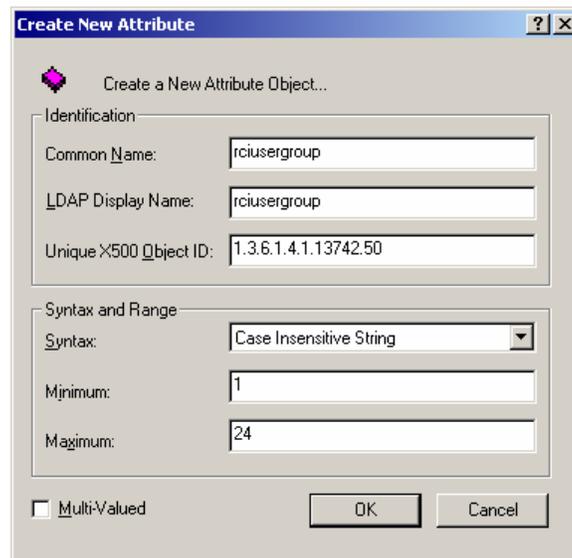


Figure 108 : Création d'un nouvel attribut

4. Saisissez **rcusergroup** dans le champ **Common Name (Nom courant)**.
5. Saisissez **rcusergroup** dans le champ **LDAP Display Name (Nom LDAP affiché)**.
6. Saisissez **1.3.6.1.4.1.13742.50** dans le champ **Unique x5000 Object ID (ID d'objet x5000 unique)**.
7. Cliquez sur la flèche de la liste déroulante **Syntax (Syntaxe)** et sélectionnez **Case Insensitive String (Chaîne ne distinguant pas les majuscules/minuscules)** sur la liste.
8. Saisissez **1** dans le champ **Minimum**.
9. Saisissez **24** dans le champ **Maximum**.
10. Cliquez sur **OK** pour créer l'attribut.

Ajout d'attributs à la classe

1. Cliquez sur **Classes** dans le volet de gauche de la fenêtre.
2. Faites défiler le volet de droite jusqu'à la classe **user (utilisateur)** et cliquez dessus avec le bouton droit de la souris.
3. Sélectionnez **Properties (Propriétés)** dans le menu. La fenêtre **User Properties (Propriétés de l'utilisateur)** s'affiche.
4. Cliquez sur l'onglet **Attributes (Attributs)**.
5. Cliquez sur **Add (Ajouter)**.
6. Sélectionnez **rcusergroup** sur la liste **Select Schema Object (Sélectionner un objet schéma)**.

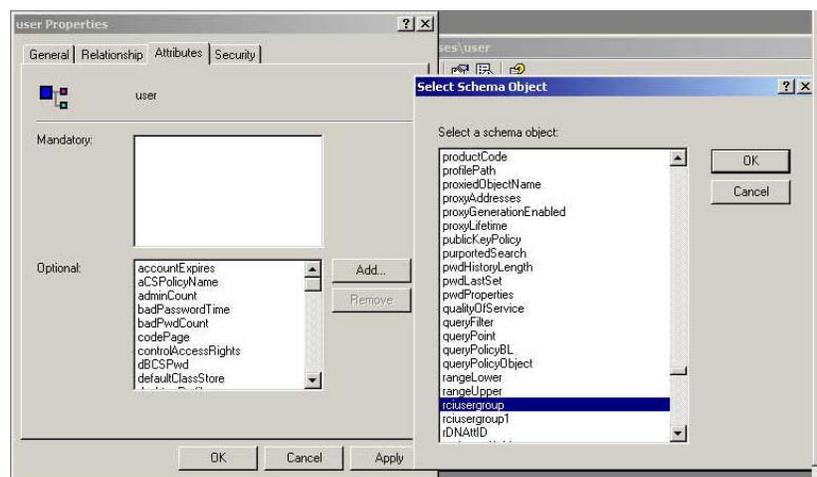


Figure 109 : Ajout d'attributs à la classe

7. Cliquez sur **OK**.
8. Cliquez sur **OK**.

Mise à jour du cache de schéma

1. Cliquez avec le bouton droit de la souris sur **Active Directory Schema (Schéma Active Directory)** dans le volet de gauche de la fenêtre et sélectionnez **Reload the Schema (Recharger le schéma)** dans le menu contextuel.
2. Réduisez la console Active Directory Schema MMC.

Modification des attributs du groupe d'utilisateurs pour les membres utilisateurs

Pour exécuter un script Active Directory sur un serveur Windows 2003, utilisez le script fourni par Microsoft. Ces scripts sont chargés sur votre système lors de l'installation de Microsoft Windows 2003. ADSI (ou Active Directory Service Interface) sert d'éditeur de bas niveau pour Active Directory. Il vous permet d'effectuer des tâches d'administration courantes telles que l'ajout, la suppression et le déplacement d'objets avec un service d'annuaire. Pour plus d'informations, visitez le site Web de Microsoft :

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/ebsca3324-5427-471a-bc19-9aa1decd3d40.msp>.

Pour modifier les attributs d'un utilisateur individuel au sein du groupe **rciusergroup**, procédez comme suit :

1. Dans le menu **Démarrer** de Windows, cliquez sur **Exécuter**.
2. Tapez **regsvr adsiedit.msc**. La fenêtre ADSI Edit s'affiche.

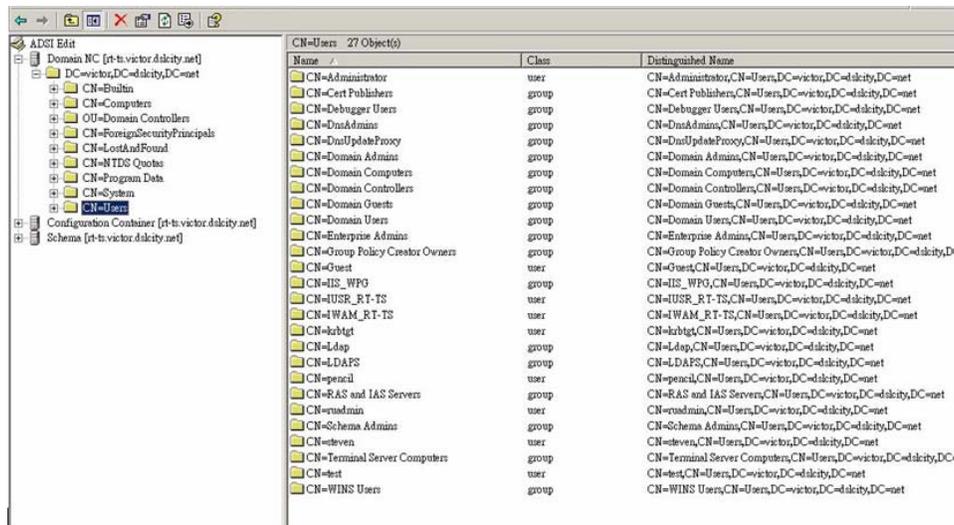


Figure 110 : ADSI Edit

3. Dans le volet de gauche de la fenêtre, sélectionnez le dossier **CN=User**.
4. Recherchez le nom d'utilisateur pour lequel vous souhaitez régler les propriétés dans le volet de droite. Cliquez avec le bouton droit de la souris sur le nom d'utilisateur et sélectionnez **Properties (Propriétés)**.
5. Cliquez sur l'onglet **Attributes (Attributs)**.

6. Cliquez sur la flèche de la liste déroulante **Select a property to view (Sélectionner une propriété à afficher)** et sélectionnez `rciusergroup` dans la liste.

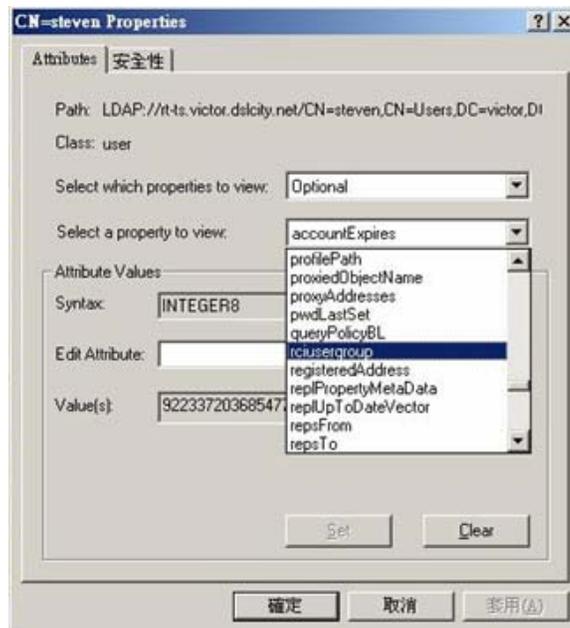


Figure 111 : Propriétés des utilisateurs

7. Dans le panneau **Attribute Values (Valeurs d'attribut)**, saisissez le nom d'utilisateur que vous souhaitez renvoyer à RRC dans le champ **Edit Attribute (Modifier l'attribut)**.

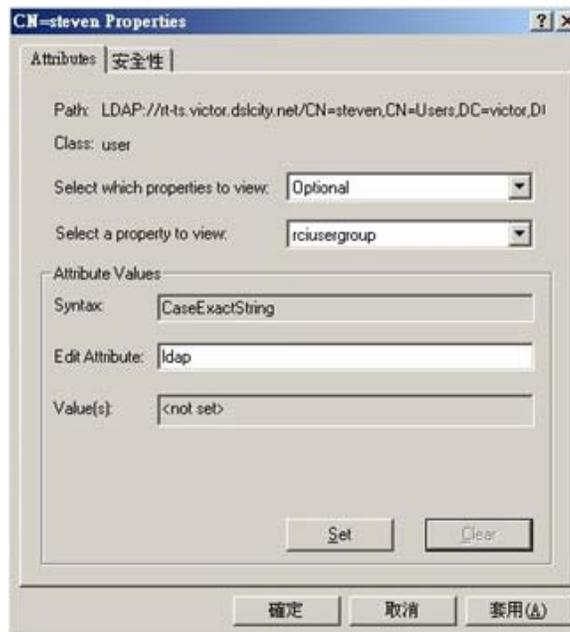


Figure 112 : Edit Attribute (Modifier l'attribut) - ajout d'un utilisateur au groupe KXII

8. Cliquez sur **Set (Définir)**.
9. Cliquez sur **OK**.

Annexe C : FAQ

Questions générales

QUESTION	REPONSE
<p>Qu'est-ce que Dominion KX II ?</p>	<p>Dominion KX II est un commutateur KVM (clavier/vidéo/souris) numérique de la seconde génération qui permet aux administrateurs informatiques d'accéder à et de gérer 16, 32 ou 64* serveurs sur le réseau grâce à la fonction au niveau BIOS. Dominion KX II est entièrement indépendant du matériel et du système d'exploitation. Les utilisateurs peuvent donc dépanner et reconfigurer les serveurs même lorsqu'ils sont éteints.</p> <p>Pour le rack, Dominion KX II offre les mêmes fonctionnalités, facilités, économies d'espace et de coût que les commutateurs KVM analogiques traditionnels. Toutefois, Dominion KX II intègre également la technologie KVM sur réseau IP la plus performante du secteur, permettant ainsi à plusieurs administrateurs d'accéder aux consoles des serveurs KVM de n'importe quel poste de travail mis en réseau.</p>
<p>En quoi Dominion KX II diffère-t-il d'un logiciel de contrôle à distance ?</p>	<p>Lorsque vous utilisez Dominion KX II à distance, l'interface peut, au premier abord, sembler identique à un logiciel de gestion à distance tel que pcAnywhere™, Windows® Terminal Services / Remote Desktop, VNC, etc. Toutefois, Dominion KX II est une solution matérielle, pas logicielle, ce qui le rend beaucoup plus puissant :</p> <ul style="list-style-type: none"> • Ne dépend ni du système d'exploitation ni du matériel - Dominion KX II peut être utilisé pour gérer des serveurs exécutant nombre de systèmes d'exploitation courants, notamment Intel®, Sun®, PowerPC exécutant Windows, Linux®, Solaris™, etc. • Ne dépend pas de l'état ou d'un serveur « agentless » – Dominion KX II n'a pas besoin que le système d'exploitation du serveur géré soit en marche, ni qu'un logiciel spécial soit installé sur le serveur géré. • Hors-bande – Même s'il n'existe pas de connexion disponible sur le réseau même du serveur géré, celui-ci peut quand même être géré par Dominion KX II. • Accès au niveau du BIOS – Même si le serveur est bloqué lors du démarrage, il requiert un redémarrage en mode sans échec ou une modification des paramètres BIOS du système, Dominion KX II fonctionne toujours sans faille pour permettre de procéder à ces configurations.
<p>Quoi de nouveau dans le Dominion KX II par rapport au KX I ?</p>	<p>Dominion KX II offre de nombreuses fonctions inédites et remarquables, notamment les médias virtuels, la double alimentation, Ethernet double d'un Gigaoctet, interfaces utilisateur</p>
<p>Comment dois-je procéder pour migrer de Dominion KX I à Dominion KX II ?</p>	<p>De manière générale, les utilisateurs de KX I peuvent continuer à utiliser leurs commutateurs existants pendant de nombreuses années. À mesure que leurs centres de données se développent, les clients peuvent acheter et utiliser les nouveaux modèles KX II. La console de gestion centralisée de Raritan, CommandCenter® Secure Gateway, ainsi que le client MPC (Multi-Platform Client) prennent tous les deux en charge les commutateurs KX I et KX II de manière transparente.</p>

QUESTION	REPONSE
Mes CIM KX I existants vont-ils fonctionner avec le commutateur Dominion KX II ?	Oui, les CIM KX I existants fonctionnent avec le commutateur Dominion KX II. De plus, les CIM Paragon sélectionnés fonctionnent avec le KX II. Cela permet aux utilisateurs désireux de commuter vers KVM sur IP de migrer en toute facilité vers KX II à partir de Paragon I.
Est-il possible de monter Dominion KX II en rack ?	Oui. Dominion KX II est livré en standard avec des supports de fixation 19". Il peut également être monté en rack par l'arrière de façon à ce que les ports du serveur soient dirigés vers l'avant.
Quelles sont les dimensions de Dominion KX II ?	Dominion KX II mesure uniquement 1U de hauteur (à l'exception de KX2-464* qui mesure 2U de hauteur), s'adapte dans un rack standard de 19" et n'occupe que 11,4" (29 cm) de profondeur.

* KX2-464 disponible en 2007

Accès à distance

QUESTION	REPOSE
Combien d'utilisateurs peuvent accéder à distance aux serveurs sur chaque Dominion KX II ?	Les modèles Dominion KX II permettent la connexion distante d'un maximum de huit utilisateurs par canal pour l'accès et la gestion simultanés d'un serveur cible unique. Pour les dispositifs à un canal tels que DKX2-116, un seul serveur cible peut être utilisé et géré par huit utilisateurs distants maximum. Pour les dispositifs à deux canaux tels que DKX2-216, un maximum de huit utilisateurs distants peuvent utiliser et gérer le serveur sur le canal un et huit autres utilisateurs maximum sur le canal deux. En ce qui concerne les dispositifs à quatre canaux, huit utilisateurs maximum par canal, pour un total de 32 (8 x 4) utilisateurs, peuvent utiliser et gérer quatre serveurs de la même manière que décrite précédemment.
Deux utilisateurs peuvent-ils visualiser le même serveur simultanément ?	Oui, jusqu'à huit personnes peuvent utiliser et gérer n'importe quel serveur unique en même temps.
Deux utilisateurs, l'un à distance et l'autre à partir du port local, peuvent-ils accéder au même serveur ?	Oui, le port local est totalement indépendant des « ports » distants. Le port local permet d'accéder au même serveur via la fonction PC-Share.
Quels sont les matériel, logiciel ou configuration réseau nécessaires pour accéder à Dominion KX II à partir d'un ordinateur client ?	<p>Dominion KX II étant entièrement accessible par le Web, ne requiert aucune installation de logiciel exclusif sur les ordinateurs clients utilisés pour y accéder. (Tout client installé en option est disponible à l'adresse Internet Raritan.com pour pouvoir accéder à Dominion KX II via un modem).</p> <p>Il est possible d'accéder à Dominion KX II par le biais des principaux navigateurs Web : Internet Explorer, Mozilla™ et Firefox, etc. Il est désormais possible d'accéder à Dominion KX II depuis un bureau Windows, Linux, Sun Solaris ou Macintosh® via le client MPC (Multi-Platform Client), basé sur Java, de Raritan et via le nouveau Virtual KVM Client™.</p> <p>Les administrateurs Dominion KX II peuvent également effectuer une gestion à distance (définir des mots de passe et la sécurité, renommer les serveurs, modifier les adresses IP, etc.) grâce à une interface navigateur des plus pratique.</p>

QUESTION	REPOSE															
<p>Quelle est la taille du fichier de l'applet utilisée pour accéder à Dominion KX II ? Combien de temps faut-il pour l'extraire ?</p>	<p>La taille de l'applet Virtual KVM Client utilisé pour accéder à Dominion KX II est d'environ 500 Ko. Le tableau suivant indique le temps nécessaire pour extraire l'applet de Dominion KX II à différentes vitesses réseau :</p> <table border="1" data-bbox="574 296 1192 632"> <tr> <td data-bbox="574 296 776 380">100 Mbps</td> <td data-bbox="776 296 1068 380">Vitesse réseau théorique 100 Mo</td> <td data-bbox="1068 296 1192 380">0,05 seconde</td> </tr> <tr> <td data-bbox="574 380 776 464">60 Mbps</td> <td data-bbox="776 380 1068 464">Vitesse réseau pratique probable 100 Mo</td> <td data-bbox="1068 380 1192 464">0,08 seconde</td> </tr> <tr> <td data-bbox="574 464 776 516">10 Mbps</td> <td data-bbox="776 464 1068 516">Vitesse réseau théorique 10 Mo</td> <td data-bbox="1068 464 1192 516">.4 secondes</td> </tr> <tr> <td data-bbox="574 516 776 569">6 Mbps</td> <td data-bbox="776 516 1068 569">Vitesse réseau pratique probable 10 Mo</td> <td data-bbox="1068 516 1192 569">.8 secondes</td> </tr> <tr> <td data-bbox="574 569 776 632">512 Kbps</td> <td data-bbox="776 569 1068 632">Vitesse de téléchargement d'un modem câblé (type)</td> <td data-bbox="1068 569 1192 632">8 secondes</td> </tr> </table>	100 Mbps	Vitesse réseau théorique 100 Mo	0,05 seconde	60 Mbps	Vitesse réseau pratique probable 100 Mo	0,08 seconde	10 Mbps	Vitesse réseau théorique 10 Mo	.4 secondes	6 Mbps	Vitesse réseau pratique probable 10 Mo	.8 secondes	512 Kbps	Vitesse de téléchargement d'un modem câblé (type)	8 secondes
100 Mbps	Vitesse réseau théorique 100 Mo	0,05 seconde														
60 Mbps	Vitesse réseau pratique probable 100 Mo	0,08 seconde														
10 Mbps	Vitesse réseau théorique 10 Mo	.4 secondes														
6 Mbps	Vitesse réseau pratique probable 10 Mo	.8 secondes														
512 Kbps	Vitesse de téléchargement d'un modem câblé (type)	8 secondes														
<p>Comment puis-je accéder aux serveurs connectés à Dominion KX II en cas d'indisponibilité du réseau ?</p>	<p>Dominion KX II offre un port de modem dédié pour connecter un modem externe. Grâce à un modem connecté de manière externe, il est toujours possible d'accéder à distance à vos serveurs en cas d'urgence. De plus, les ports locaux de Dominion KX II autorisent toujours un accès permanent à vos serveurs depuis le rack, quel que soit l'état du réseau.</p>															
<p>Avez-vous un client qui ne fonctionne pas sous Windows ?</p>	<p>Oui. Les clients Virtual KVM Client et Multi-Platform Client (MPC) permettent tous les deux aux utilisateurs exécutant des systèmes autres que Windows de se connecter aux serveurs cible via les commutateurs Dominion KX I et KX II. Le client MPC peut être exécuté à l'aide d'un navigateur Web ou en mode autonome. Pour en savoir plus, consultez Virtual KVM Client ainsi que le <i>manuel d'utilisation MPC/RRC</i>.</p>															
<p>Ma connexion modem a été coupée et un message d'erreur s'affiche indiquant qu'une erreur de communication inattendue est survenue et que la connexion a été coupée. Que dois-je faire ?</p>	<p>Cette erreur peut se produire en fonction de la fréquence à laquelle vous essayez de vous connecter à l'aide d'un modem. Redémarrez l'unité Dominion KX et le modem. Pour les futures connexions, attendez au moins deux (2) minutes entre chaque tentative.</p>															
<p>Quelquefois, au cours d'une session de Virtual KVM Client, il arrive que la touche Alt se bloque. Que dois-je faire ?</p>	<p>Ce problème survient habituellement lorsque l'on appuie sur la touche Alt sans relâcher la pression. Si, par exemple, vous continuez d'appuyer sur la touche Alt tout en appuyant sur la barre d'espacement, vous risquez de basculer du serveur cible vers le PC client.</p> <p>Le système d'exploitation local interprète ensuite cette combinaison de touches et déclenche l'action correspondante dans la fenêtre active (PC client).</p>															

Média virtuel universel

QUESTION	REPONSE
Quels sont les modèles Dominion KX II qui prennent en charge les médias virtuels ?	Tous les modèles Dominion KX II prennent en charge les médias virtuels. Ils sont disponibles en version autonome et via CommandCenter Secure Gateway (console de gestion centralisée).
Quels types de médias virtuels Dominion KX II prend-il en charge ?	Dominion KX II prend en charge les types de médias suivants : lecteurs CD/DVD internes et connectés USB, dispositifs de stockage de masse USB, lecteurs de disque dur PC et lecteurs distants.
Quelles sont les conditions requises pour l'utilisation des médias virtuels ?	Le nouveau D2CIM-VUSB CIM est requis pour l'utilisation des médias virtuels. Il supporte les sessions de médias virtuels sur les serveurs cible qui prennent en charge l'interface USB 2.0. Disponible en coffrets de 32 et 64 CIM économiques, ce nouveau CIM prend en charge l'application Absolute Mouse Synchronization ainsi que la mise à jour du firmware à distance.
Les médias virtuels sont-ils fiables ?	Oui. Les sessions de médias virtuels sont sécurisées par le biais du chiffrement RC4 ou AES 128 bits.

Ethernet et mise en réseau IP

QUESTION	REPONSE												
<p>Dominion KX II offre-t-il des ports Ethernet doubles d'un Gigaoctet pour fournir une fonction de protection par basculement redondante ou un équilibrage des charges ?</p>	<p>Oui. Dominion KX II comporte des ports Ethernet doubles d'un Gigaoctet pour permettre la protection par basculement redondante. En cas de panne du port Ethernet primaire (ou du commutateur/routeur auquel il est connecté), Dominion KX II bascule sur le port réseau secondaire avec la même adresse IP, empêchant ainsi toute interruption de fonctionnement de votre serveur. Notez que la protection par basculement automatique doit être activée par l'administrateur.</p>												
<p>Quelle est le taux de bande passante requis par Dominion KX II ?</p>	<p>Dominion KX II offre la technologie KVM par IP nouvelle génération : la compression vidéo la plus performante qui soit. Raritan a reçu de nombreuses récompenses techniques confirmant la haute qualité de ses transmissions vidéo et l'utilisation limitée de la bande passante.</p> <p>Raritan a été le premier à développer la fonction KVM sur IP, qui permet aux utilisateurs d'adapter leurs paramètres vidéo pour préserver la bande passante du réseau. Par exemple, lors d'une connexion à Dominion KX II par un modem d'accès à distance, les transmissions vidéo peuvent être converties en échelle de gris, pour une rentabilité optimale tout en garantissant des performances élevées.</p> <p>Sachant cela, les données suivantes concernent Dominion KX II configuré sur les paramètres vidéo par défaut qui, une fois encore, peuvent être adaptés à un environnement spécifique. Ils peuvent être augmentés pour améliorer la qualité vidéo (nombre de couleurs) ou diminués pour optimiser les connexions à faible débit.</p> <p>En règle générale, une estimation raisonnable de l'utilisation de la bande passante (lorsque Dominion KX II est configuré sur ses paramètres par défaut) est d'environ 0,5 Mbps par utilisateur KVM actif (connecté à un serveur qu'il utilise), avec des pointes exceptionnelles pouvant atteindre 2 Mbps. Il s'agit d'une estimation très raisonnable car le niveau de bande passante utilisé est en général plus faible.</p> <p>La bande passante requise par chaque transmission vidéo dépend de la tâche effectuée sur le serveur géré. Plus l'écran change, plus le débit de la bande passante utilisée est important. Le tableau ci-dessous résume certains cas d'utilisation et le débit de bande passante requis lorsque Dominion KX II est configuré sur ses paramètres par défaut avec une vitesse réseau de 10 Mbps :</p> <table border="1" data-bbox="574 1587 1192 1791"> <tbody> <tr> <td>Bureau de Windows inactif</td> <td>0 Mbps</td> </tr> <tr> <td>Déplacement du curseur sur le Bureau</td> <td>0,18 Mbps</td> </tr> <tr> <td>Déplacement d'une fenêtre/boîte de dialogue fixe 400 x 600</td> <td>0,35 Mbps</td> </tr> <tr> <td>Navigation dans le menu Démarrer</td> <td>0,49 Mbps</td> </tr> <tr> <td>Défilement d'une page entière de texte</td> <td>1,23 Mbps</td> </tr> <tr> <td>Exécution de l'écran de veille Maze en 3D</td> <td>1,55 Mbps</td> </tr> </tbody> </table>	Bureau de Windows inactif	0 Mbps	Déplacement du curseur sur le Bureau	0,18 Mbps	Déplacement d'une fenêtre/boîte de dialogue fixe 400 x 600	0,35 Mbps	Navigation dans le menu Démarrer	0,49 Mbps	Défilement d'une page entière de texte	1,23 Mbps	Exécution de l'écran de veille Maze en 3D	1,55 Mbps
Bureau de Windows inactif	0 Mbps												
Déplacement du curseur sur le Bureau	0,18 Mbps												
Déplacement d'une fenêtre/boîte de dialogue fixe 400 x 600	0,35 Mbps												
Navigation dans le menu Démarrer	0,49 Mbps												
Défilement d'une page entière de texte	1,23 Mbps												
Exécution de l'écran de veille Maze en 3D	1,55 Mbps												

QUESTION	REPONSE
Quelle est la connexion la moins rapide (débit de bande passante le plus faible) avec laquelle Dominion KX II peut fonctionner ?	Une vitesse de 33 Kbps ou supérieure est recommandée pour obtenir des performances KX acceptables sur une connexion par modem.
Quelle est la vitesse des interfaces Ethernet de Dominion KX II ?	Dominion KX II prend en charge Gigabit et 10/100 Ethernet. KX II prend en charge deux interfaces Ethernet de vitesse 10/100/1000, avec possibilité de configurer la vitesse et les paramètres duplex (détectés automatiquement ou définis manuellement).
Est-il possible d'accéder à Dominion KX II via une connexion sans fil ?	Oui. Dominion KX II n'utilise pas seulement l'interface Ethernet standard, mais également une bande passante très classique de très haute qualité vidéo. Par conséquent, si vous disposez d'un client sans fil équipé d'une connectivité réseau à Dominion KX II, vous pouvez configurer et gérer vos serveurs au niveau du BIOS sans fil.
Est-il possible d'utiliser Dominion KX II sur un réseau étendu (Internet) ou uniquement sur le réseau local d'une entreprise ?	Que ce soit par un réseau LAN rapide, par un réseau étendu moins prévisible (Internet), par un modem câblé ou par un modem d'accès à distance, la technologie KVM sur IP de Dominion KX II s'adapte à votre type de connexion.
Est-il possible d'utiliser Dominion KX II sur un réseau VPN ?	Oui. Dominion KX II utilise les technologies IP (protocole Internet) standard de la couche 1 à 4. L'encombrement peut être facilement canalisé via des réseaux VPN standard.
Combien de ports TCP doivent être activés sur mon pare-feu pour autoriser l'accès réseau à Dominion KX II ? Ces ports sont-ils configurables ?	Un seul. Dominion KX II a besoin d'accéder à un seul port TCP en fonctionnement pour assurer la sécurité de votre réseau. Pour plus de sécurité, ce port est entièrement configurable. Notez que pour pouvoir utiliser la fonction du navigateur Web en option de Dominion KX II, le port 443 HTTPS standard doit, bien évidemment, aussi être activé.
Dominion KX II requiert-il un serveur d'authentification externe pour fonctionner ?	Non. Dominion KX II est une application entièrement autonome. Une fois une adresse IP affectée à un Dominion KX II, ce dernier est prêt à l'emploi avec un navigateur Web et des fonctions d'authentification entièrement intégrés. Si vous utilisez un serveur d'authentification externe (tel que LDAP, Active Directory, RADIUS, etc.), Dominion KX II vous le permet et basculera même sur son propre réseau d'authentification interne en cas d'indisponibilité de votre serveur d'authentification externe. La philosophie de conception de Dominion KX II est ainsi optimisée pour offrir une facilité d'installation, une indépendance totale vis-à-vis de tout serveur externe et un maximum de flexibilité.

QUESTION	REPONSE
Dominion KX II peut-il être utilisé avec CITRIX ?	Dominion KX II peut fonctionner avec des produits d'accès à distance tels que CITRIX si la configuration est effectuée correctement. Raritan ne peut cependant pas garantir que les performances de fonctionnement soient acceptables. Les produits tels que CITRIX utilisent des technologies de réacheminement vidéo dont le concept est similaire à celui des commutateurs KVM, si bien que deux technologies KVM par IP sont utilisées simultanément.
Dominion KX II peut-il utiliser l'adressage DHCP ?	L'adressage DHCP peut être utilisé, mais Raritan recommande l'utilisation d'un adressage fixe. En effet, Dominion KX II est un dispositif d'infrastructure et l'accès et l'administration sont réalisés plus efficacement au moyen d'une adresse IP fixe.
J'ai des problèmes à me connecter à Dominion KX II via mon réseau IP. Quel pourrait être le problème ?	<p>Dominion KX II s'appuie sur votre réseau local/Internet. Les éventuels problèmes incluent :</p> <ul style="list-style-type: none"> • Négociation automatique d'Ethernet. Sur certains réseaux, la négociation automatique 10/100 ne fonctionne pas correctement et l'unité KX II doit alors être réglée sur 100 Mo/full duplex (ou sur une option adaptée au réseau). • Doublet au niveau des adresses IP. Si l'adresse IP de Dominion KX II est la même que celle d'un autre dispositif, il est possible que la connectivité du réseau ne soit pas fiable. • Conflits au niveau du port 5000. Si un autre dispositif utilise le port 5000, le port par défaut de Dominion KX II doit être modifié (ou le port de l'autre dispositif doit être modifié). • Lors de la modification de l'adresse IP d'une unité KX II ou du passage à une nouvelle unité KX II, vous devez attendre suffisamment longtemps pour que ses adresses MAC et IP soient reconnues par les réseaux des couches 2 et 3.

Serveurs

QUESTION	REPONSE
<p>Dominion KX II dépend-il d'un serveur Windows pour fonctionner ?</p>	<p>Absolument pas. Du fait que vous dépendez de votre infrastructure KVM pour être toujours disponible dans n'importe quelle situation de travail (et que vous devrez probablement utiliser cette infrastructure pour résoudre les éventuels problèmes), Dominion KX II est conçu pour être entièrement indépendant par rapport à tout serveur externe.</p> <p>Par exemple, si votre centre de données est attaqué par un ver ou un virus Windows, vous devrez utiliser votre solution KVM pour résoudre le problème. Par conséquent, il est essentiel que cette solution KVM ne dépende d'aucun de ces serveurs Windows (ou de tout autre serveur) pour être opérationnelle afin que la solution KVM fonctionne.</p> <p>Pour cette raison, Dominion KX II est entièrement indépendant. Même si vous choisissez de configurer Dominion KX pour permettre l'authentification par un serveur Active Directory, en cas d'indisponibilité de ce dernier, l'authentification propre à Dominion KX II sera activée et entièrement opérationnelle.</p>
<p>Dois-je installer un serveur Web tel que Microsoft Internet Information Services (IIS) pour pouvoir utiliser la fonction de navigateur Web de Dominion KX II ?</p>	<p>Non. Dominion KX II est une application entièrement autonome. Une fois une adresse IP affectée à Dominion KX II, ce dernier est prêt à l'emploi avec un navigateur Web et des fonctions d'authentification entièrement intégrés.</p>
<p>Quel logiciel dois-je installer pour accéder à Dominion KX II depuis un poste de travail donné ?</p>	<p>Aucun. Dominion KX II est entièrement accessible par un navigateur Web (même si un client installé en option est fourni sur le site Web de Raritan www.raritan.com pour permettre l'accès à Dominion KX II par modem). Un client utilisant Java est désormais disponible pour les utilisateurs qui n'ont pas de système Windows.</p>
<p>Que dois-je faire pour préparer la connexion d'un serveur à Dominion KX II ?</p>	<p>Régalez simplement les paramètres souris de manière à fournir aux utilisateurs la meilleure synchronisation de souris lors des connexions à distance et désactivez les fonctions de gestion d'alimentation électrique qui affectent l'affichage de l'écran. Toutefois, si vous utilisez le nouvel adaptateur D2CIM-VUSB (prenant en charge Absolute Mouse Synchronization™), vous n'avez pas besoin de régler manuellement les paramètres de souris.</p>
<p>Que contient le coffret Dominion KX II ?</p>	<p>Il comprend les éléments suivants : (a) l'unité Dominion KX II, (b) le guide de configuration rapide, (c) les supports de fixation de montage en rack 19 po standard, (d) le CD-ROM du manuel d'utilisation, (e) un câble réseau, (f) un câble croisé, (g) un cordon de raccordement CA localisé, (h) un certificat de garantie et d'autres documents.</p>

Installation

QUESTION	REPONSE
À part l'unité elle-même, que dois-je commander à Raritan pour installer Dominion KX II ?	Chaque serveur connecté à Dominion KX II requiert un module d'interface pour ordinateur (CIM) Paragon ou Dominion, et un adaptateur qui se branche directement sur les ports clavier, écran et souris du serveur.
Quel type de câble Cat5 dois-je utiliser pour mon installation ?	Dominion KX II peut utiliser n'importe quel câble UTP (à paire torsadée) standard : Cat5, Cat5e ou Cat6. Dans nos manuels et brochures publicitaires, Raritan ne mentionne bien souvent que le câble « Cat5 ». En réalité, n'importe quel câble marqué UTP convient pour Dominion KX II.
Quels types de serveur peuvent être connectés à Dominion KX II ?	Dominion KX II est entièrement indépendant des fabricants. N'importe quel serveur avec ports clavier, vidéo et souris conformes aux normes peut être connecté.
Comment connecter les serveurs à Dominion KX II ?	Les serveurs connectés à Dominion KX II requièrent un module d'interface pour ordinateur (CIM) Paragon ou Dominion qui se branche directement sur les ports clavier, écran et souris du serveur. Connectez ensuite chaque CIM à Dominion KX II au moyen d'un câble UTP (à paire torsadée) standard : Cat5, Cat5e ou Cat6.
Quelle est la distance maximale autorisée entre mes serveurs et Dominion KX II ?	En général les serveurs peuvent être distants de 45 mètres de Dominion KX II, selon le type de serveur. (Please refer to the Raritan Web site or Distance de connexion et résolution vidéo du serveur cible for more information.) For the new D2CIM-VUSB CIM that supports virtual media and Absolute Mouse Synchronization, a 100 (30 m) foot range is recommended.
Certains systèmes d'exploitation se bloquent lorsque je déconnecte un clavier ou une souris pendant le fonctionnement. Que faut-il faire pour éviter aux serveurs connectés à Dominion KX II de se bloquer lorsque je m'en déconnecte ?	Chaque clé électronique du module d'interface pour ordinateur Dominion (DCIM) se comporte comme un clavier et une souris virtuels vis-à-vis du serveur auquel elle est connectée. Cette technologie est appelée KME (émulation clavier/souris). La technologie KME de Raritan est adaptée aux centres de données, testée contre les éventuelles attaques et d'une fiabilité nettement supérieure à celle des commutateurs KVM bas de gamme : forte de plus de 15 années d'expérience, elle a été installée sur des millions de serveurs dans le monde entier.
Ne faut-il pas installer des agents sur les serveurs connectés à Dominion KX II ?	Dominion KX II étant directement connecté par voie matérielle aux ports clavier, vidéo et souris des serveurs, les serveurs connectés à Dominion KX II ne nécessitent l'installation d'aucun agent logiciel.
Combien de serveurs peuvent être connectés à chaque unité Dominion KX II ?	La gamme des modèles Dominion KX II permet l'accès de 16 à 32 ports de serveur par unité dans un châssis 2U. C'est le commutateur KVM numérique offrant la densité de ports la plus élevée de l'industrie.

QUESTION	REPONSE
<p>Que se passe-t-il si je déconnecte un serveur de Dominion KX II pour le reconnecter à une autre unité Dominion KX II ou à un autre port sur la même unité ?</p>	<p>Dominion KX II met automatiquement à jour les noms de port du serveur lorsque les serveurs sont déplacés d'un port à l'autre. De plus, cette mise à jour automatique n'affecte pas seulement le port d'accès local, mais également tous les clients distants et la console de gestion CommandCenter Secure Gateway en option.</p>
<p>Comment dois-je connecter un dispositif contrôlé en série (RS-232) à Dominion KX II, tel qu'un routeur/commutateur Cisco ou un serveur Sun headless ?</p>	<p>S'il y a peu de dispositifs contrôlés en série, ils peuvent être connectés à un Dominion KX II via l'adaptateur série de Raritan, AUATC ou le nouveau convertisseur série P2CIM-SER.</p> <p>Toutefois, si vous disposez de quatre dispositifs contrôlés en série, ou davantage, nous vous recommandons d'utiliser la gamme Dominion SX de Raritan des serveurs de console sécurisée. Pour plusieurs dispositifs contrôlés en série, Dominion SX propose plus de fonctions série à un meilleur prix que Dominion KX II. Ce Dominion SX est simple à utiliser, à configurer et à gérer et peut être entièrement intégré au déploiement d'une série Dominion. En particulier, de nombreux administrateurs UNIX et de réseau apprécient l'utilisation du protocole SSH pour établir une connexion directe avec une unité Dominion SX.</p>

Port local

QUESTION	REPOSE
Est-il possible d'accéder à mes serveurs directement depuis le rack ?	Oui. Les fonctions sur rack de Dominion KX II se comportent comme un commutateur KVM traditionnel, vous permettant de contrôler jusqu'à 64 serveurs au moyen d'un seul clavier, écran et souris.
L'accès à distance aux serveurs d'autres utilisateurs est-il bloqué lorsque j'utilise le port local ?	Non, le port local de Dominion KX II dispose d'un chemin d'accès aux serveurs entièrement indépendant. Cela signifie qu'un utilisateur peut accéder localement aux serveurs sur le rack, sans affecter le nombre d'utilisateurs qui accèdent simultanément au rack à distance.
Est-il possible d'utiliser un clavier ou une souris USB sur le port local ?	Oui. Dominion KX II offre à la fois des ports clavier et de souris PS/2 et USB sur le port local. Notez que les ports USB sont des ports USB v1.1 et ne supportent que les claviers et souris, et non des dispositifs USB tels que des scanners ou des imprimantes.
Existe-t-il un affichage à l'écran pour l'accès sur le rack local ?	Oui, mais les performances d'accès sur le rack de Dominion KX II sont largement supérieures aux affichages écran classiques. Doté de l'interface navigateur la plus aboutie de l'industrie en matière d'accès sur le rack, le port local de KX II utilise la même interface pour l'accès local et distant. Par ailleurs, la plupart des fonctions d'administration sont disponibles sur le rack.
Comment sélectionner les serveurs tout en utilisant le port local ?	Le port local affiche les serveurs connectés à l'aide de la même interface utilisateur que celle du client distant. Connectez-vous à un serveur d'un simple clic de souris.
Comment s'assurer que seuls les utilisateurs autorisés peuvent accéder aux serveurs depuis le port local ?	<p>Les utilisateurs essayant d'utiliser le port local doivent subir le même niveau d'authentification que les utilisateurs à distance. En d'autres termes :</p> <ul style="list-style-type: none"> • Si votre Dominion KX II est configuré pour interagir avec un serveur RADIUS, LDAP ou Active Directory externe, les utilisateurs essayant d'accéder au port local seront authentifiés par le même serveur. • Si les serveurs d'authentification externe ne sont pas disponibles, Dominion KX II active sa base de données d'authentification interne. <p>Dominion KX II possède sa propre authentification autonome, offrant une installation instantanée, prête à l'emploi.</p>
En cas d'utilisation du port local pour modifier le nom d'un serveur connecté, est-ce que cela affecte également les clients d'accès distant ? La console CommandCenter en option est-elle affectée ?	Oui. La présentation du port local est identique et entièrement synchronisée avec les clients d'accès distant et la console de gestion CommandCenter Secure Gateway en option de Raritan. Plus simplement, si vous modifiez le nom d'un serveur sur l'affichage à l'écran Dominion KX II, cela met à jour en temps réel tous les clients à distance et les serveurs de gestion externes.

QUESTION	REPONSE
En cas d'utilisation des outils d'administration à distance de Dominion KX II pour modifier le nom d'un serveur connecté, est-ce que cela affecte également l'affichage à l'écran du port local ?	Oui. Si vous modifiez le nom du serveur à distance ou au moyen de la console de gestion CommandCenter Secure Gateway en option de Raritan, cette mise à jour affecte immédiatement l'affichage à l'écran de Dominion KX II.
Parfois je vois des « ombres » sur l'interface utilisateur du port local. Quelle en est l'origine ?	Ces ombres/effets de réplication peuvent apparaître sur les écrans LCD qui sont restés activés longtemps. Les propriétés LCD et la charge électrique/statique peuvent générer ces effets lorsque l'écran est sous tension sur une longue période.

Gestion de l'alimentation

QUESTION	REPOSE
Dominion KX II propose-t-il l'option de double alimentation ?	Tous les modèles Dominion KX II sont équipés d'arrivées CA et d'alimentations en double avec basculement automatique. En cas de défaillance au niveau d'une arrivée électrique ou de l'alimentation électrique, KX II commute automatiquement sur l'autre système.
Les paramètres de tension sont-ils automatiquement détectés par l'alimentation de Dominion KX II ?	Oui. L'alimentation de Dominion KX II peut être utilisée sur une tension alternative comprise entre 100 et 240 volts, à 50 – 60 Hz.
Suis-je informé en cas de coupure de courant ou de défaillance au niveau d'une arrivée électrique ?	Le voyant DEL situé sur le panneau frontal de KX II permet de notifier à l'utilisateur toute panne de courant. Une entrée est également envoyée dans le Journal d'audit et affichée dans l'interface utilisateur Remote Client de KX II. Des événements SNMP ou Syslog sont également générés, si les options correspondantes ont été configurées par l'administrateur.
Quelles sont les fonctions de gestion de l'alimentation offertes par Dominion KX II ?	Les barrettes d'alimentation de gestion d'alimentation à distance de Raritan peuvent être branchées sur le Dominion KX II pour gérer l'alimentation électrique des serveurs cible. Après une simple opération de configuration unique, il vous suffit de cliquer avec le bouton droit de la souris sur le nom du serveur pour démarrer, mettre hors tension ou recycler un serveur bloqué. Notez que redémarrer physiquement équivaut à débrancher le serveur de la prise de courant, puis à le rebrancher.
Dominion KX II prend-il en charge les serveurs à alimentations multiples ? Que se passe-t-il si chaque alimentation est branchée sur une barrette d'alimentation différente ?	Oui. Dominion KX II peut être facilement configuré pour prendre en charge des alimentations multiples branchées sur plusieurs barrettes d'alimentation. Jusqu'à huit (8) barrettes d'alimentation peuvent être connectées au dispositif KX II. Quatre alimentations peuvent être connectées par serveur cible sur plusieurs barrettes d'alimentation.
La gestion de l'alimentation à distance nécessite-t-elle une configuration spéciale du serveur ?	Certains serveurs sont livrés avec des paramètres BIOS par défaut qui rendent impossible le redémarrage automatique du serveur après une coupure de l'alimentation et son rétablissement. Pour plus de détails, consultez le manuel d'utilisation du serveur.
Quelles sont les barrettes d'alimentation prises en charge par Dominion KX II ?	Pour tirer parti de l'interface utilisateur de gestion de l'alimentation intégrée de Dominion KX II et encore plus de la sécurité intégrée, utilisez les barrettes d'alimentation de Remote Power Control (RPC) de Raritan. RPC est livré avec de nombreuses combinaisons de prises, connecteurs et tensions. Vous devez acquérir le module D2CIM-PWR pour pouvoir connecter RPC à KX II.

Évolutivité

QUESTION	REPOSE
<p>Comment puis-je interconnecter plusieurs dispositifs Dominion KX II pour avoir une solution unique ?</p>	<p>Les unités multiples Dominion KX II ne nécessitent aucune interconnexion physique. En effet, toutes les unités Dominion KX II sont connectées au réseau et fonctionnent simultanément comme une solution unique lorsqu'elles sont déployées avec la console de gestion CommandCenter Secure Gateway (CC-SG) en option de Raritan. CC-SG sert de point d'accès et de gestion à distance unique. CC-SG offre tout un ensemble d'outils pratiques, tels que le regroupement de la configuration et de la mise à jour des firmwares, ainsi qu'une base de données d'authentification et d'autorisation unique.</p> <p>De plus, CC-SG permet un tri des serveurs, des autorisations et une fonction d'accès avancés. Si le déploiement de la console de gestion CC-SG de Raritan n'est pas en option, les unités multiples Dominion KX II continuent d'interagir et de gérer automatiquement : L'interface utilisateur distante de KX II et le Client MPC détecteront automatiquement les unités Dominion KX II. Vous pouvez accéder aux unités Dominion KX II qui n'ont pas été détectées au moyen d'un profil défini par l'utilisateur.</p>
<p>Est-il possible de connecter un commutateur analogique KVM existant à Dominion KX II ?</p>	<p>Oui. Les commutateurs KVM analogiques peuvent être connectés à l'un des ports de serveur de Dominion KX II. Il vous suffit d'utiliser un module d'interface pour ordinateur (CIM - Computer Interface Module) PS/2 et de le connecter aux ports utilisateur du commutateur KVM analogique existant. Notez que les caractéristiques des commutateurs KVM varient, et que Raritan ne peut pas garantir l'interopérabilité d'un commutateur KVM analogique tiers particulier. Contactez le support technique Raritan pour obtenir de plus amples informations. Les commutateurs analogiques Paragon[®] et Paragon II de Raritan prennent en charge le protocole IP par le biais de la famille de produits d'accès à distance IP-Reach[®].</p>

Modules d'interface pour ordinateurs

QUESTION	REPOSE
<p>Est-il possible d'utiliser des modules d'interface pour ordinateurs (CIM - Computer Interface Module) venant du commutateur analogique matriciel KVM de Raritan, Paragon, avec Dominion KX II ?</p>	<p>Oui. Certains modules d'interface pour ordinateurs Paragon peuvent être compatibles avec Dominion KX II (consultez les notes de publication de Dominion KX II sur le site Web de Raritan pour obtenir la dernière liste de ces modules certifiés).</p> <p>Toutefois, les modules d'interface pour ordinateurs (CIM - Computer Interface Module) Paragon étant plus chers que les modules Dominion KX II (en raison de leur technologie de transmission vidéo intégrée sur une distance allant jusqu'à 300 mètres), il n'est pas conseillé d'acheter les modules Paragon pour les utiliser avec Dominion KX II. Notez également que lorsque les modules d'interface pour ordinateurs Paragon sont connectés à Dominion KX II, leur transmission vidéo est limitée à 15 mètres, égalant les performances de transmission des modules Dominion KX II, et n'est plus de 300 mètres comme lorsqu'ils sont connectés à Paragon.</p>
<p>Est-il possible d'utiliser des modules d'interface pour ordinateurs (CIM - Computer Interface Module) Dominion KX II avec le commutateur analogique matriciel KVM de Raritan, Paragon ?</p>	<p>Non. Les modules d'interface pour ordinateurs Dominion KX II offrent une transmission vidéo sur une distance de 15 à 45 mètres et par conséquent, ne sont pas compatibles avec Paragon, qui nécessite des modules avec transmission vidéo sur une distance de 300 mètres. Pour que tous les clients de Raritan bénéficient de la qualité vidéo la plus performante qui soit de l'industrie, une caractéristique consistante de Raritan, les modules d'interface pour ordinateurs (CIM - Computer Interface Module) de série Dominion ne sont pas compatibles avec Paragon.</p>

Sécurité

QUESTION	REPONSE														
Quel type de chiffrement est utilisé par Dominion KX II ?	Dominion KX II utilise un système de chiffrement RC4 ou AES à 128 bits standard (extrêmement sûr) pour ses communications SSL et son propre flux de données. Littéralement, aucune donnée n'est transmise entre les clients distants et Dominion KX II si elle n'est pas chiffrée et complètement sécurisée.														
Dominion KX II supporte-t-il le chiffrement AES comme recommandé par les normes FIP et NIST du gouvernement américain ?	Dominion KX II utilise le chiffrement AES (Advanced Encryption Standard) pour une sécurité accrue. AES est un algorithme de cryptage approuvé par le gouvernement américain et recommandé par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) dans la Norme FIPS 197.														
Le dispositif Dominion KX II permet-il le cryptage de données vidéo ? Ou effectue-t-il uniquement le chiffrement des données de clavier et de souris ?	Contrairement aux solutions concurrentes, qui ne chiffrent que les données de clavier et de souris, Dominion KX II ne met pas votre sécurité en danger. Il permet de chiffrer les données de clavier, souris et vidéo.														
Comment Dominion KX II intègre-t-il les serveurs d'authentification externes tels que Active Directory®, RADIUS ou LDAP ?	Grâce à une configuration très simple, il est possible de programmer Dominion KX II pour renvoyer toutes les demandes d'authentification vers un serveur externe tel que LDAP, Active Directory ou RADIUS. Pour chaque utilisateur authentifié, le serveur d'authentification transmet à Dominion KX II le groupe d'utilisateurs auquel appartient l'utilisateur concerné. Dominion KX II détermine ensuite les autorisations d'accès de l'utilisateur en fonction du groupe auquel il appartient.														
Comment sont stockés les noms d'utilisateur et mots de passe ?	En cas d'utilisation des fonctions d'authentification interne de Dominion KX II, toutes les informations critiques telles que les noms d'utilisateur et mots de passe sont stockées sous une forme cryptée. En d'autres termes, personne y compris le support technique ou les services d'ingénierie de produit Raritan, ne peut récupérer ces noms d'utilisateur et mots de passe.														
Dominion KX II prend-il en charge le mot de passe sécurisé obligatoire ?	Oui. Dominion KX II dispose de la fonction de vérification stricte du mot de passe, configurable par l'administrateur, afin de garantir que les mots de passe créés par les utilisateurs répondent aux normes gouvernementales et/ou d'entreprise et résistent au piratage de force.														
Si le mode de chiffrement de Dominion KX II est défini sur Automatique, quel est le niveau de chiffrement obtenu ?	Le niveau de chiffrement qui est négocié automatiquement est tributaire du navigateur en cours d'utilisation : <table border="1" data-bbox="574 1648 1099 1850"> <thead> <tr> <th>Navigateur</th> <th>Niveau de chiffrement</th> </tr> </thead> <tbody> <tr> <td>Internet Explorer 6</td> <td>RC4</td> </tr> <tr> <td>Internet Explorer 7</td> <td>AES-128</td> </tr> <tr> <td>Firefox 1.5</td> <td>RC4</td> </tr> <tr> <td>Firefox 2.0</td> <td>RC4</td> </tr> <tr> <td>Mozilla 1.7</td> <td>RC4</td> </tr> <tr> <td>Safari 2.0.4</td> <td>AES-128</td> </tr> </tbody> </table>	Navigateur	Niveau de chiffrement	Internet Explorer 6	RC4	Internet Explorer 7	AES-128	Firefox 1.5	RC4	Firefox 2.0	RC4	Mozilla 1.7	RC4	Safari 2.0.4	AES-128
Navigateur	Niveau de chiffrement														
Internet Explorer 6	RC4														
Internet Explorer 7	AES-128														
Firefox 1.5	RC4														
Firefox 2.0	RC4														
Mozilla 1.7	RC4														
Safari 2.0.4	AES-128														

Capacités de gestion

QUESTION	REPOSE
Est-il possible de gérer et de configurer à distance Dominion KX II via un navigateur Web ?	<p>Oui. Dominion KX II peut être entièrement configuré à distance via un navigateur Web. Pour cela, votre poste de travail doit disposer d'une version de Java Runtime Environment (JRE) appropriée.</p> <p>Il est possible de configurer entièrement la solution sur le réseau à l'exception du paramètre initial de l'adresse IP de Dominion KX II. (En fait, vous pouvez même configurer les paramètres initiaux au moyen d'un câble Ethernet croisé et de l'adresse IP par défaut de Dominion KX II via un navigateur Web.)</p>
Est-il possible de sauvegarder et de restaurer la configuration de Dominion KX II ?	<p>Oui. Il est possible de sauvegarder entièrement les configurations de l'utilisateur et du dispositif Dominion KX II pour une restauration ultérieure en cas de catastrophe.</p> <p>La fonction de sauvegarde et de restauration de Dominion KX II peut être utilisée à distance sur le réseau ou via un navigateur Web.</p>
Quels sont les journaux d'audit et enregistrements offerts par Dominion KX ?	<p>Pour une responsabilité optimale, Dominion KX II enregistre tous les événements utilisateur principaux avec datage et marque horaire. Par exemple, les événements rapportés comprennent (liste non exhaustive) : connexion de l'utilisateur, déconnexion de l'utilisateur, accès utilisateur à un serveur particulier, échec de connexion, modifications de configuration, etc.</p>
Est-il possible d'intégrer Dominion KX II au serveur Syslog ?	<p>Oui. Dominion KX II peut également, en plus de ses propres fonctions d'enregistrement interne, envoyer tous les événements enregistrés vers un serveur Syslog centralisé.</p>
Est-il possible d'intégrer Dominion KX II avec SNMP ?	<p>Oui. Dominion KX II peut également, en plus de ses propres fonctions d'enregistrement interne, envoyer des traps SNMP vers les systèmes de gestion SNMP comme HP Openview et CC-NOC de Raritan.</p>
Est-il possible de synchroniser l'horloge interne de Dominion KX II avec un serveur de temps ?	<p>Oui. Dominion KX II supporte le protocole NTP standard pour se synchroniser avec le serveur de temps de votre entreprise ou avec n'importe quel serveur de temps public (en partant du principe que le pare-feu de votre entreprise autorise les demandes NTP sortantes).</p>

Divers

QUESTION	REPONSE
Quelle est l'adresse IP par défaut de Dominion KX II ?	192.168.0.192
Quels sont le nom d'utilisateur et le mot de passe par défaut de Dominion KX II ?	Le nom d'utilisateur et le mot de passe par défaut de KXII sont admin/raritan [tout en minuscules]. Cependant, au niveau de sécurité le plus élevé, KX II force l'administrateur à changer le nom d'utilisateur et le mot de passe administratifs par défaut de Dominion KX II lorsque l'unité est lancée pour la première fois.
En cas de modification et d'oubli du mot de passe administratif de Dominion KX II, vous est-il possible de le récupérer ?	KX II comporte une fonction de réinitialisation matérielle qui peut être utilisée pour réinitialiser les paramètres par défaut du dispositif et réinitialiser par la même occasion le mot de passe administratif sur le dispositif.

Guide de dépannage

QUESTION	REPONSE
<p>Je suis connecté au Dominion KX II par l'intermédiaire de Firefox et j'ai ouvert un autre navigateur Firefox. Je suis connecté automatiquement au même Dominion KX II avec le deuxième navigateur Firefox. Est-ce normal ?</p>	<p>Oui, cela est normal. C'est le résultat direct des méthodes de fonctionnement des navigateurs et des cookies.</p>
<p>Je suis connecté au Dominion KX II à l'aide de Firefox et j'essaie de me connecter à un autre Dominion KX II par l'intermédiaire d'une autre session du navigateur Firefox à partir du même client. Je suis déconnecté des deux KX II, ce comportement est-il normal ?</p>	<p>Oui, pour accéder à deux dispositifs Dominion KX II distincts, vous devez soit fermer la première session, soit utiliser un autre PC client.</p>
<p>Lorsque je lance une session de KVM en utilisant Firefox comme navigateur et que certaines fenêtres sont ouvertes dans Virtual KVM Client (Connection Properties, Video Settings, etc.), le navigateur (même les autres sessions Firefox) semble se bloquer. Que dois-je faire ?</p>	<p>C'est normal : avec Firefox, toutes les sessions sont associées. Fermez la fenêtre Virtual KVM Client pour débloquer Firefox.</p>

255-62-4023-00

World Headquarters

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tél. : (732) 764-8886
Fax : (732) 764-8887
E-mail : sales@raritan.com
Web : www.raritan.com

Raritan Amérique

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tél. : (732) 764-8886
Fax : (732) 764-8887
E-mail : sales@raritan.com
Web : www.raritan.com

Bureaux dans la région Asie Pacifique

Raritan Asia Pacific, Inc.
5F, 121, Lane 235, Pao-Chiao Road,
Hsin Tien 231,
Taipei, Taiwan, ROC
Tél. : (886) 2 8919-1333
Fax : (886) 2 8919-1338
E-mail : sales.asia@raritan.com
Web : raritan-ap.com

Raritan China Offices

Raritan Beijing
No. 35 Financial St, Xicheng District
Room 1035, Block C,
Corporate Square
Beijing 100032, Chine
Tél. : (86) 10-8809-1890
E-mail : sales.china@raritan.com
Web : raritan.com.cn

Raritan Shanghai
Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai, China
(200030)
Tél. : (86) 21 5425-2499
Fax : (86) 21 5425-3992
E-mail : sales.china@raritan.com
Web : raritan.com.cn

Raritan Guangzhou
1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou (510075), China Raritan
Tél. : (86) 20 8755-5581
Fax : (86) 20 8755-5571
E-mail : sales.china@raritan.com
Web : raritan.com.cn

Raritan Corée

#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Séoul, Corée
Tél. : (82) 2 557-8730
Fax : (82) 2 557-8733
E-mail : sales.korea@raritan.com
Web : raritan.co.kr

Raritan Japon

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku, Tokyo
104-0033
Tél. : (81) 03-3523-5991
Fax : (81) 03-3523-5992
E-mail : sales@raritan.co.jp
Web : raritan.co.jp

Raritan Osaka
3rd Floor,
Osaka Kagaku Sen'I Kaikan Bldg.
4-6-8 Kawara-machi, Chuo-ku,
Osaka 541-0048
Tél. : (81) 03-3523-5953
Fax : (81) 03-3523-5992
Web : raritan.co.jp

Bureaux Raritan en Australie

Raritan Melbourne
Level 2, 448 St Kilda Rd.,
Melbourne, VIC3004
Australie
Tél. : (61) 3-9866-6887
E-mail : sales.au@raritan.com
Web : raritan.com.au

Raritan Sydney
PO BOX A386,
Sydney, NSW2000, Australie
Tél. : (61) 2-9029-2558
E-mail : sales.au@raritan.com
Web : raritan.com.au

Raritan Inde

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli Gurgaon
Rd, Gurgaon 122 002
Haryana, Inde
Tél. : (91) 124 410-7881
Fax : (91) 124 410-7880
E-mail : enquiry.india@raritan.com
Web : raritan.co.in

Raritan Taiwan

5F, 121, Lane 235, Pao-Chiao Road
Hsin-Tien City
Taipei Hsien, Taiwan, ROC
Tél. : (886) 2 8919-1333
Fax : (886) 2 8919-1338
E-mail : sales.taiwan@raritan.com
Web : raritan.com.tw

Raritan Singapour

350 Orchard Road
#11-08, Suite 21, Shaw House
Singapour 238868
Tél. : (65) 6725 9871
Fax : (65) 6725 9872
E-mail : sales.ap@raritan.com
Web : raritan-ap.com

Bureaux européens

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
Pays-Bas
Tél. : (31) 10-284-4040
Fax : (31) 10-284-4049
E-mail : sales.europe@raritan.com
Web : www.raritan.fr
www.raritan.de

Raritan France

120 Rue Jean Jaurès
92300 Levallois-Perret, France
Tél. : (33) 14-756-2039
Fax : (33) 14-756-2061
E-mail : sales.france@raritan.com
Web : www.raritan.fr

Raritan Deutschland GmbH

Lichtstraße 2
D-45127 Essen, Allemagne
Tél. : (49) 201-747-98-0
Fax : (49) 201-747-98-50
E-mail : sales.germany@raritan.com
Web : www.raritan.de

Raritan Italie

Via dei Piatti 4
20123 Milan
Italie
Tél. : (39) 02-454-76813
Fax : (39) 02-861-749
E-mail : sales.italy@raritan.com
Web : raritan.it
www.raritan.info

Raritan Canada

Raritan, Inc.
4 Robert Speck Pkwy., Suite 1500
Mississauga, ON L4Z 1S1
Canada
Tél. : (1) 905-949-3650
E-mail : sales.canada@raritan.com
Web : raritan.ca

Raritan Royaume-Uni

9th Floor, 12-20 Camomile St
London EC3A 7EX, Royaume-Uni
Tél. : (44) (0)-20-7614-7700
E-mail : sales.uk@raritan.com
Web : raritan.co.uk