Dominion KX II

Manuel d'utilisation
Version 2.5.0

DKX2-v2.5.0-0P-F

Mai 2012

255-62-4023-00

Informations FCC

Le présent équipement a été soumis à des essais, de manière à établir sa conformité avec les limites afférentes à un appareil numérique de classe A, en vertu de la section 15 des réglementations de la FCC. Ces limites sont destinées à assurer une protection raisonnable contre les interférences nocives dans une installation commerciale. Cet appareil génère, utilise et émet de l'énergie de fréquences radio et peut, en cas d'installation ou d'utilisation non conforme aux instructions, engendrer des interférences nuisibles au niveau des 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 causés à ce produit suite à un accident, un désastre, une mauvaise utilisation, un abus d'utilisation, une modification non Raritan apportée au produit, ou à d'autres événements échappant au contrôle raisonnable de Raritan ou ne résultant pas de conditions normales de fonctionnement.

CE c UL us LISTED 1F61 I.T.E.

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 **Caractéristiques**.
- Assurez-vous que la circulation d'air dans l'environnement de rack est suffisante.
- Montez l'équipement dans le rack avec précaution de façon à éviter tout chargement bancal des composants mécaniques.
- Branchez l'équipement au circuit d'alimentation avec précaution afin d'éviter une surcharge des circuits.
- Mettez tout l'équipement correctement à la terre sur le circuit terminal, notamment les raccords d'alimentation tels que les barrettes d'alimentation (autres que celles branchées directement).

Table des matières

Chapitre 7 Gestion des utilisateurs 148

Chapitre 8 Gestion des dispositifs 176

Chapitre 1 Introduction

Dans ce chapitre

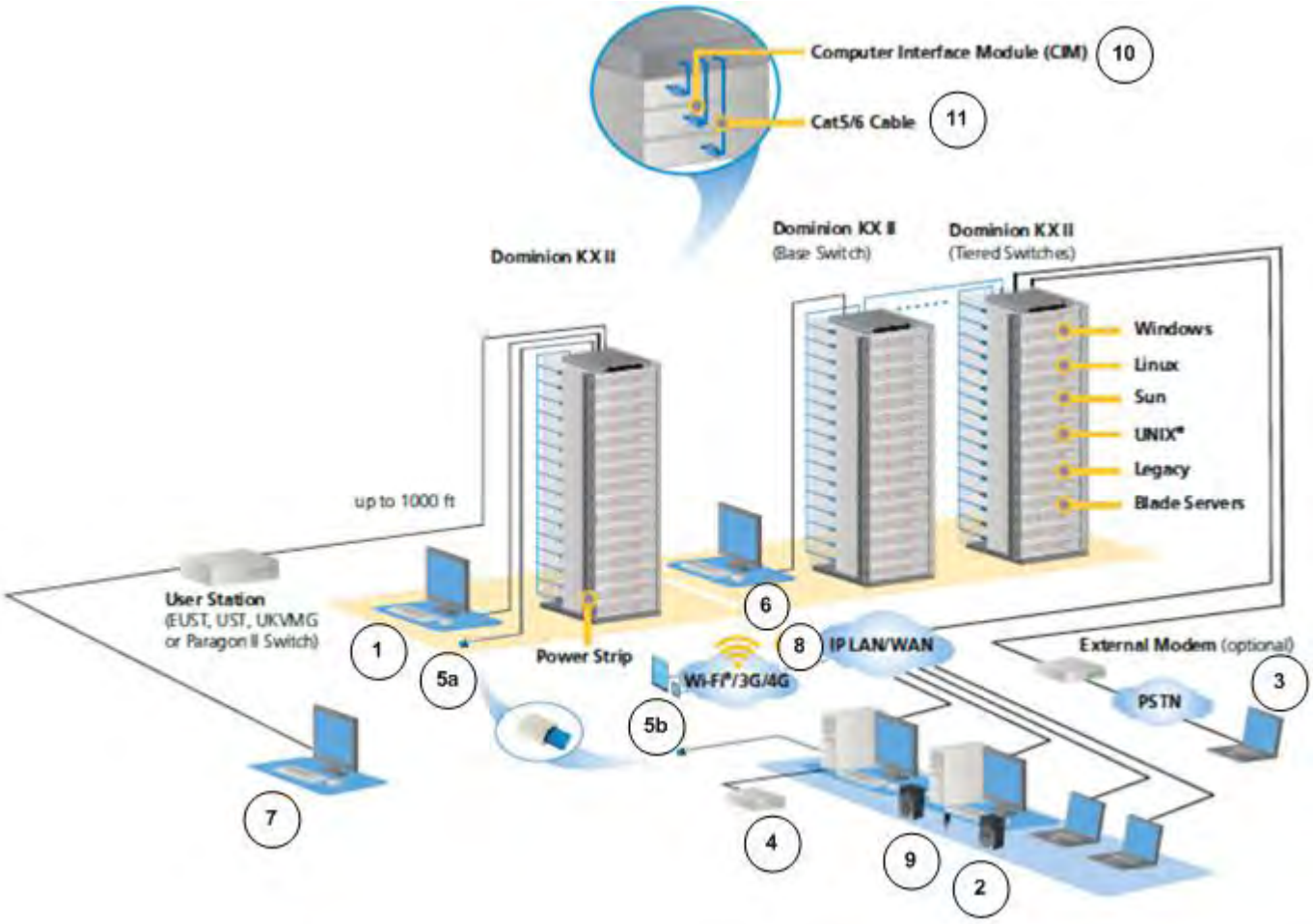
KX II - Présentation

KX II Dominion de Raritan est un commutateur KVM (écran-clavier-souris) numérique sécurisé conçu pour l'entreprise, qui offre un accès au niveau du BIOS (et au-dessus) et permet de gérer des serveurs, où que vous vous trouviez dans le monde, par l'intermédiaire d'un navigateur Web. 64 serveurs au plus peuvent être contrôlés avec une unité KX II standard. Pour le modèle KX II pour huit utilisateurs, 32 serveurs au plus peuvent être contrôlés avec KX2-832 et jusqu'à 64 serveurs avec KX2-864. Une fonction de balayage vous permet de localiser et d'afficher jusqu'à 32 cibles. Les cibles sont affichées sous forme de miniatures dans un diaporama à partir duquel les utilisateurs se connectent à chaque cible.

KX II prend en charge jusqu'à huit canaux vidéo, et permet à tout moment à huit utilisateurs de se connecter simultanément à huit cibles vidéo différentes. Les dispositifs audionumériques sont pris en charge, ce qui vous permet de vous connecter à des dispositifs de lecture et d'enregistrement à partir du PC client distant au serveur cible. Sur le rack, KX II permet de contrôler au niveau du BIOS jusqu'à 64 serveurs et autres dispositifs informatiques depuis un ensemble clavier, écran et souris unique. Les fonctions d'accès à distance intégrées à KX II procurent le même niveau de contrôle des serveurs via un navigateur Web.

L'installation de KX II est facilitée par l'utilisation d'un câblage UTP (Cat5/5e/6) standard. Ses caractéristiques clés sont les suivantes : support virtuel, chiffrement 256 bits, double alimentation, gestion de l'alimentation à distance, Ethernet double, LDAP, RADIUS, Active Directory®, intégration de Syslog, capacités de modem externe et gestion Web. Le modèle KX II pour huit utilisateurs dispose également d'un port local étendu à l'arrière du dispositif. Ces fonctions permettent d'améliorer les temps d'exploitation, la productivité et la sécurité, n'importe où, n'importe quand.

Les produits 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 dispositifs KX II (associés à des dispositifs Dominion SX pour l'accès à distance à une console série, et Dominion KSX pour la gestion des bureaux distants et des filiales) peuvent être intégrés dans une solution logique unique à l'aide de la console de gestion CommandCenter Secure Gateway (CC-SG) de Raritan.


Computer Interface Module (CIM)
10
Cat5/6 Cable
11
Dominion KX II
Dominion KX II
(Base Switch)
Dominion KX II
(Tiered Switches)
Windows
Linux
Sun
UNIX®
Legacy
Blade Servers
up to 1000 ft
User Station
(EUST, UST, UKVMG
or Paragon II Switch)
1
5a
Power Strip
6
8
IP LAN/WAN
Wi-Fi®/3G/4G
5b
External Modem (optional)
3
PSTN
7
4
9
2

Légende			
1	Accès au port local	6	Mise en niveau
2	Accès réseau IP	7	Port local étendu
3	Modem	8	Accès mobile via iPhone® et iPad® avec CC-SG
4	Support virtuel	9	Audionumérique
5a	Accès par carte à puce au rack	10	CIM
5b	Accès par carte à puce distant	11	Câble Cat5/6

Aide KX II

L'aide KX II explique comment installer, paramétrer et configurer KX II. Elle comprend également des informations sur l'accès aux serveurs cible, à l'aide des supports virtuels, sur la gestion des utilisateurs et de la sécurité, ainsi que sur la maintenance et les diagnostics du produit KX II.

Reportez-vous aux notes de version de KX II pour obtenir des informations importantes sur la version en cours avant d'utiliser KX II.

Une version PDF de l'aide peut être téléchargée de la page **Firmware and Documentation** du site Web de Raritan. Raritan vous recommande de consulter son site Web pour obtenir les derniers manuels d'utilisation disponibles.

Pour utiliser l'aide en ligne, Active Content (Contenu actif) doit être activé dans votre navigateur. Si vous utilisez Internet Explorer 7, vous devez activer Scriptlets. Consultez l'aide de votre navigateur pour en savoir plus sur l'activation de ces fonctions.

Nouveautés de l'aide

Les informations suivantes ont été ajoutées à cause d'améliorations et de modifications apportées à l'équipement et/ou à la documentation utilisateur.

- Nouveau modèle KX2-808 avec 8 ports KVM, 1 port local, 1 port local étendu et prise en charge de 8 utilisateurs distants via le réseau

Reportez-vous aux notes de version de KX II pour obtenir une explication plus détaillée des modifications apportées à l'appareil et à cette version de l'aide.

Documentation connexe

L'aide KX II est accompagnée du manuel de configuration rapide KX II, qui se trouve sur la page **Firmware and Documentation** du ***site Web de Raritan*** (***http://www.raritan.com/support/firmware-and-documentation***).

Les exigences et les instructions d'installation des applications clientes utilisées avec KX II se trouvent dans le **manuel des clients d'accès KVM et série**, également présent sur le site Web de Raritan. Le cas échéant, des fonctions clientes particulières utilisées avec KX II sont incluses dans l'aide.

Applications clientes KX II

Les applications clientes suivantes peuvent être utilisées dans KX II :

Produit	Fonctionne avec...				
	MPC	AKC	VKC	RSC	RRC
KX II (deuxième génération)	✓		✓		
KX II 2.2 (ou supérieur)	✓	✓	✓		

Reportez-vous au **manuel des clients KVM et série** pour en savoir plus sur les applications clientes. Reportez-vous également à la section ***Utilisation des serveurs cible*** (à la page 49) du présent manuel, qui contient des informations sur l'utilisation des clients avec KX II.

Remarque : MPC et VKC requièrent Java™ Runtime Environment (JRE™). AKC est basé .NET.

Support virtuel

Tous les modèles KX II prennent en charge la fonction Support virtuel. Chaque KX II est équipé de la fonction Support virtuel pour autoriser la gestion à distance des tâches à l'aide d'une vaste gamme de lecteurs de CD ou de DVD, USB, de dispositifs de lecture et d'enregistrement audio internes et distants, et d'images. KX II prend en charge l'accès par support virtuel des disques durs et des images montées à distance.

Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement 256 bits AES ou RC4.

Les CIM numériques, D2CIM-VUSB et D2CIM-DVUSB prennent en charge les sessions sur support virtuel pour les serveurs cible KVM disposant de l'interface USB 2.0. Ces CIM prennent également en charge la synchronisation absolue de la souris et la fonction Support virtuel, ainsi que la mise à jour du firmware à distance.

Remarque : le connecteur noir du CIM DVUSB est utilisé pour le clavier et la souris. Le connecteur gris est utilisé pour le support virtuel. Laissez les deux prises du CIM branchées sur le dispositif. Le dispositif risque de ne pas fonctionner correctement si les deux prises ne sont pas branchées sur le serveur cible.

Photos du dispositif KX II

KX II

KX2-808

KX2-832

KX2-864

Reportez-vous à ***Dimensions et spécifications physiques de KX II*** (voir "***Spécifications physiques de KX II***" à la page 337) pour obtenir les spécifications du produit. Reportez-vous à ***Spécifications des modules d'interface pour ordinateur (CIM) pris en charge*** (voir "***Spécifications des CIM pris en charge***" à la page 343) pour des spécifications et des images de CIM.

Caractéristiques du produit

Matériel

- Accès distant KVM sur IP intégré
- Montage en rack 1U ou 2U (supports de fixation fournis)
- Double alimentation avec fonction de basculement automatique, alimentation à commutation automatique avec avertissement de panne de courant
- Prise en charge de la fonction multiniveau où un dispositif KX II de base est utilisé pour accéder à plusieurs autres dispositifs en niveau. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.
- Fonction pour utilisateurs multiples (1/2/4/8 utilisateurs distants, 1 utilisateur local)
- Câblage de serveur UTP (Cat5/5e/6)
- Ports Ethernet doubles (10/100/1000 LAN) à protection par basculement
- Améliorable en clientèle
- Port utilisateur local pour accès en rack
  - Les ports clavier/souris PS/2 sur KX2-808, KX2-832 et KX2-864 sont USB uniquement.
  - Un port USB 2.0 sur le panneau avant et trois sur le panneau arrière pour les dispositifs USB pris en charge
  - Simultanéité complète avec l'accès utilisateur à distance
  - Interface graphique utilisateur (GUI) locale pour l'administration
- Un port local étendu offre une portée étendue pour un accès en rack sur les dispositifs KX2 8xx.
- Sécurité de l'accès centralisé
- Gestion de l'alimentation intégrée
- Voyants indiquant le statut de la double alimentation, l'activité du réseau et le statut des utilisateurs distants
- Bouton de réinitialisation matérielle
- Port série pour la connexion à un modem externe.
- Utilisateurs et ports pris en charge par modèle :

Modèle	Utilisateurs distants	Ports
KX II-864	8	64
KX II-832	8	32

Modèle	Utilisateurs distants	Ports
KX II-808	8	8
KX II-464	4	64
KX II-432	4	32
KX II-416	4	16
KX II-232	2	32
KX II-216	2	16
KX II-132	1	32
KX II-116	1	16
KX II-108	1	8

Logiciel

- Prise en charge des supports virtuels dans les environnements Windows®, Mac® et Linux® avec les CIM D2CIM-VUSB, D2CIM-DVUSB et numériques
- Prise en charge audionumérique via USB
- Balayage des ports et vue en miniature de 32 cibles au maximum avec jeu de balayage configurable
- Synchronisation absolue de la souris avec les CIM D2CIM-VUSB, D2CIM-DVUSB et numériques
- Plug and Play
- Gestion et accès Web
- Interface utilisateur graphique intuitive
- Prise en charge de la sortie vidéo sur deux ports
- Chiffrement 256 bits de l'ensemble du signal KVM, signal vidéo et support virtuel inclus
- LDAP, Active Directory®, RADIUS ou authentification et autorisation internes
- Adressage DHCP ou IP fixe
- Authentification par carte à puce/CAC
- Gestion SNMP, SNMP3 et Syslog
- Prise en charge d'IPv4 et d'IPv6
- Gestion de l'alimentation associée directement aux serveurs pour éviter les erreurs
- Intégration avec l'unité de gestion CommandCenter Secure Gateway (CC-SG) de Raritan
- Fonction CC Unmanage pour suspendre la gestion d'un dispositif par CC-SG.
- Prise en charge des appareils Raritan PX1 et PX2

Terminologie

L'aide utilise la terminologie ci-après pour les composants standard de KX II :

Légende du schéma	
1	TCP/IP IPv4 et/ou IPv6
2	KVM (clavier/vidéo/souris)
3	Câble UTP (Cat5/5e/6)
A	KX II
B	Console d'accès local (Local Access Console) Utilisateur local - Console utilisateur facultative (constituée d'un clavier, d'une souris et d'un écran VGA Multisync) directement reliée à KX II pour gérer des serveurs cible KVM (directement au niveau du rack et non par l'intermédiaire du réseau). Un lecteur de cartes à puce USB peut également être branché au port local pour être monté sur un serveur cible. Un port local étendu est également fourni sur les modèles DKX2-808, DKX2-832 et DKX2-864.
C	Ordinateur distant (Remote PC) Ordinateurs mis en réseau utilisés pour accéder aux serveurs cible connectés à KX II et les gérer. Un lecteur de cartes à puce USB peut également être branché au PC distant et relié à un serveur cible via KX II.
D	CIM Clés connectées sur chacun des serveurs cible ou chacune des PDU de rack (barrette d'alimentation). Disponibles pour tous les systèmes d'exploitation pris en charge.
E	Serveurs cible (Target Servers) Serveurs cible KVM - Serveurs disposant de cartes vidéo et d'interfaces utilisateur (par exemple, système d'exploitation Windows®, Linux®, Solaris™, etc.) et accessibles à distance via KX II.
F	PDU de rack Dominion PX (Barrettes d'alimentation) PDU de rack Raritan accessibles à distance via KX II.

Reportez-vous à **Systèmes d'exploitation et CIM pris en charge (serveurs cible)** pour obtenir la liste des systèmes d'exploitation et CIM pris en charge, et à ***Systèmes d'exploitation pris en charge (clients)*** (à la page 340) pour obtenir la liste des systèmes d'exploitation pris en charge par KX II à distance.

Contenu de l'emballage

Chaque KX II est un produit autonome entièrement configuré, dans un châssis de montage en rack 1U (2U pour DKX2-864) 19 pouces standard. Chaque dispositif KX II est livré avec les éléments suivants :

Quantité	Elément
1	Dispositif KX II
1	Manuel de configuration rapide KX II
1	Kit de montage en rack
2	Cordon d'alimentation secteur
2	Câble réseau Cat5
1	Câble réseau croisé Cat5
1	Ensemble de 4 pieds en caoutchouc (pour utilisation sur un bureau)
1	Note d'application
1	Carte de garantie

Chapitre 2 Installation et configuration

Dans ce chapitre

Présentation

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

Pour installer et configurer KX II :

- ***Etape 1 : Configuration des serveurs cible KVM*** (à la page 19)
- ***Etape 2 : Configuration des paramètres du pare-feu de réseau*** (à la page 34)
- ***Etape 3 : Connexion de l'équipement*** (à la page 35)
- ***Etape 4 : Configuration de KX II*** (à la page 39)
- ***Etape 5 : Lancement de la console distante de KX II*** (à la page 46)
- ***Etape 6 : Configuration de la langue du clavier (facultatif)*** (à la page 47)
- ***Etape 7 : Configuration de la fonction multiniveau (facultatif)*** (voir "***Etape 7 : Configuration de la fonction multiniveau (facultatif)***" à la page 48)

Vous trouverez également dans cette section les données de connexion par défaut dont vous aurez besoin. Particulièrement, l'adresse IP, le nom d'utilisateur et le mot de passe par défaut. Reportez-vous à ***Données de connexion par défaut*** (à la page 18).

Montage en rack

KX II peut être monté dans 1U (1,75 po, 4,4 cm) d'espace vertical sur un rack d'équipement standard de 19 pouces.

Montage avant

Remarque : le dispositif Raritan utilisé dans les schémas présentés ici est un exemple et n'est pas nécessairement le dispositif KX II. Toutefois, les instructions de montage sont identiques.

Les étapes correspondent aux chiffres indiqués sur les schémas du montage en rack avant.

1. Fixez la barre de support de câble à l'arrière des pattes latérales à l'aide de deux des vis fournies.
2. Faites glisser la station utilisateur ou le commutateur KVM entre les pattes latérales, panneau arrière face à la barre de support de câble, jusqu'à que le panneau avant soit aligné sur les « oreilles » des pattes latérales.
3. Fixez la station utilisateur ou le commutateur aux pattes latérales à l'aide des vis restantes (trois de chaque côté).
4. Montez l'assemblage sur le rack et fixez les oreilles des pattes latérales sur les rails avant du rack à l'aide de vos propres vis, boulons, écrous à cage, etc.
5. Lorsque vous branchez des câbles au panneau arrière de la station utilisateur ou du commutateur, drapez-les sur la barre de support de câble.

Montage en rack avant

Montage en rack avant

Montage arrière

Remarque : le dispositif Raritan utilisé dans les schémas présentés ici est un exemple et n'est pas nécessairement le dispositif KX II. Toutefois, les instructions de montage sont identiques.

Les étapes correspondent aux chiffres indiqués sur les schémas du montage en rack arrière.

1. Fixez la barre de support de câble à l'avant des pattes latérales, près des « oreilles », à l'aide de deux des vis fournies.
2. Faites glisser la station utilisateur ou le commutateur KVM entre les pattes latérales, panneau arrière face à la barre de support de câble, jusqu'à que le panneau avant soit aligné sur les bords arrière des pattes latérales.
3. Fixez la station utilisateur ou le commutateur aux pattes latérales à l'aide des vis restantes (trois de chaque côté).
4. Montez l'assemblage sur le rack et fixez les oreilles des pattes latérales sur les rails avant du rack à l'aide de vos propres vis, boulons, écrous à cage, etc.
5. Lorsque vous branchez des câbles au panneau arrière de la station utilisateur ou du commutateur, drapez-les sur la barre de support de câble.

Montage en rack arrière

Montage en rack arrière

Données de connexion par défaut

Valeur par défaut	Valeur
Nom d'utilisateur	Le nom d'utilisateur par défaut est admin. Cet utilisateur dispose de droits d'administrateur.
Mot de passe	Le mot de passe par défaut est raritan. Les mots de passe respectent la casse, 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 KX II, il vous est demandé de changer le mot de passe par défaut.
IP address (Adresse IP)	KX II est fourni avec l'adresse IP par défaut 192.168.0.192.

Valeur par défaut	Valeur
Important : à des fins de sauvegarde et de continuité des opérations, il est fortement recommandé de créer un nom d'utilisateur et un mot de passe de secours pour l'administrateur, et de conserver ces données dans un endroit sûr.	

Mise en route

Etape 1 : Configuration des serveurs cible KVM

Les serveurs cible KVM sont des ordinateurs accessibles et contrôlés via KX II. Avant d'installer KX II, configurez tous les serveurs cible KVM afin d'obtenir des performances optimales. Cette configuration s'applique aux serveurs cible KVM uniquement, non aux postes de travail clients (ordinateurs distants) utilisés pour accéder à distance à KX II. Reportez-vous à **Terminologie** (à la page 12) pour plus d'informations.

Papier peint du Bureau

Pour une utilisation de bande passante et une qualité vidéo optimales, les serveurs cible KVM qui exécutent des interfaces utilisateur graphiques telles que Windows®, Linux®, X-Windows, Solaris™ et KDE peuvent nécessiter une configuration. 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

KX II fonctionne en modes Absolute Mouse Mode™ (mode souris absolue), Intelligent Mouse Mode (mode souris intelligente) et Standard Mouse Mode (mode souris standard).

Les paramètres de souris n'ont pas besoin d'être modifiés pour la synchronisation absolue de la souris mais un CIM D2CIM-VUSB, D2CIM-DVUSB ou numérique est requis. Quel que soit le mode souris suivant : standard ou intelligente, les paramètres de la souris doivent être configurés sur des valeurs spécifiques. Les configurations de souris varient selon les différents systèmes d'exploitation cible. Reportez-vous à la documentation de votre système d'exploitation pour de plus amples informations.

Le mode souris intelligente fonctionne bien sur la plupart des plates-formes Windows, mais peut produire des résultats imprévisibles lorsque Active Desktop est défini sur la cible. N'utilisez pas de souris animée pour le mode souris intelligente. Pour plus d'informations sur les paramètres du mode Souris intelligente, reportez-vous à ***Mode Souris intelligente*** (à la page 95).

Les serveurs disposant de commutateurs KVM internes dans un châssis à lame ne prennent habituellement pas en charge la technologie de souris absolue.

Paramètres Windows XP, Windows 2003 et Windows 2008

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Microsoft® Windows XP®, le système d'exploitation Windows 2003® ou les systèmes d'exploitation Windows 2008® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Panneau de configuration > Souris.
   b. Cliquez sur l'onglet Options du pointeur.
   c. Dans la partie Mouvement du pointeur :

- Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
- Désactivez l'option Améliorer la précision du pointeur.
- Désactivez l'option Alignement.
- Cliquez sur OK.

Remarque : lorsque vous exécutez Windows 2003 sur votre serveur cible et que vous accédez au serveur via KVM et effectuez l'une des actions répertoriées ci-dessous, la synchronisation de la souris peut être perdue si elle était déjà activée. Il vous faudra sélectionner la commande Synchronize Mouse (Synchroniser la souris) dans le menu Mouse (Souris) du client pour la réactiver. Les actions ci-après peuvent provoquer ce problème :

- Ouvrir un éditeur de texte.

- Accéder aux propriétés de la souris, du clavier et options de modem et de téléphonie à partir du Panneau de configuration Windows.

2. Désactivez les effets de transition :
   a. Sélectionnez l'option Affichage du Panneau de configuration.
   b. Cliquez sur l'onglet Apparence.
   c. Cliquez sur Effets.
   d. Désélectionnez la case Utiliser l'effet de transition suivant pour les menus et les info-bulles.
   e. Cliquez sur OK.
3. Fermez le Panneau de configuration.

Remarque : pour les serveurs cible KVM exécutant Windows XP, Windows 2000 ou Windows 2008, vous pouvez créer un nom d'utilisateur qui servira uniquement pour les connexions à distance via KX II. Vous pourrez ainsi réserver aux connexions KX II les paramètres d'accélération/de mouvement lent du pointeur de la souris définis pour le serveur cible.

Les pages de connexion de Windows XP, 2000 et 2008 rétablissent les paramètres prédéfinis de la souris qui diffèrent de ceux suggérés pour des performances optimales de l'unité KX II. En conséquence, il est possible que la synchronisation de la souris ne soit pas optimale pour ces écrans.

Remarque : Effectuez cette opération uniquement si vous êtes capable de manipuler le Registre des serveurs cible KVM Windows. Vous pouvez obtenir une meilleure synchronisation de la souris KX II aux pages de connexion en utilisant l'éditeur du Registre Windows pour modifier les paramètres suivants : HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Paramètres Windows 7 et Windows Vista

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Windows Vista® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Paramètres > Panneau de configuration > Souris.
   b. Sélectionnez Paramètres système avancés dans le panneau de navigation à gauche. La boîte de dialogue Propriétés système s'affiche.
   c. Cliquez sur l'onglet Options du pointeur.
   d. Dans la partie Mouvement du pointeur :
      - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
      - Désactivez l'option Améliorer la précision du pointeur.
      - Cliquez sur OK.
2. Désactivez les effets de fondu et d'animation :
   a. Sélectionnez l'option Système à partir du Panneau de configuration.
   b. Sélectionnez Informations sur les performances et Outils > Outils avancés > Ajuster pour régler l'apparence et les performances de Windows.
   c. Cliquez sur l'onglet Avancé.
   d. Cliquez sur Paramètres dans le groupe Performances pour ouvrir la boîte de dialogue Options de performances.
   e. Sous les options Personnalisation, désélectionnez les cases à cocher suivantes :
   - Options d'animation :
     - Animer les commandes et les éléments à l'intérieur des fenêtres
     - Animer les fenêtres lors de la réduction et de l'agrandissement
   - Options de fondu :

- Fondre ou faire glisser les menus dans la zone de visualisation
- Fondre ou faire glisser les info-bulles dans la zone de visualisation
- Fermer en fondu les commandes de menu après le clic de souris

3. Cliquez sur OK et fermez le Panneau de configuration.

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Windows 7® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Panneau de configuration > Matériel et audio > Souris.
   b. Cliquez sur l'onglet Options du pointeur.
   c. Dans la partie Mouvement du pointeur :
      - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
      - Désactivez l'option Améliorer la précision du pointeur.
      - Cliquez sur OK.
2. Désactivez les effets de fondu et d'animation :
   a. Sélectionnez Panneau de configuration > Système et sécurité.
   b. Sélectionnez Système, puis Paramètres système avancés dans le panneau de navigation à gauche. La fenêtre Propriétés système s'affiche.
   c. Cliquez sur l'onglet Avancé.
   d. Cliquez sur le bouton Paramètres du groupe Performances pour ouvrir la boîte de dialogue Options de performances.
   e. Sous les options Personnalisation, désélectionnez les cases à cocher suivantes :
   - Options d'animation :
     - Animer les commandes et les éléments à l'intérieur des fenêtres
     - Animer les fenêtres lors de la réduction et de l'agrandissement
   - Options de fondu :

- Fondre ou faire glisser les menus dans la zone de visualisation
- Fondre ou faire glisser les info-bulles dans la zone de visualisation
- Fermer en fondu les commandes de menu après le clic de souris

3. Cliquez sur OK et fermez le Panneau de configuration.

Paramètres Windows 2000

Pour configurer les serveurs cible KVM exécutant le système d'exploitation Microsoft Windows® 2000® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Panneau de configuration > Souris.
   b. Cliquez sur l'onglet Motion (Mouvement).
      - Définissez l'accélération du pointeur sur 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 Affichage du Panneau de configuration.
   b. Cliquez sur l'onglet Effets.
      - Désélectionnez la case Utiliser l'effet de transition suivant pour les menus et les info-bulles.
3. Cliquez sur OK et fermez le Panneau de configuration.

Remarque : pour les serveurs cible KVM exécutant Windows XP, Windows 2000 ou Windows 2008, vous pouvez créer un nom d'utilisateur qui servira uniquement pour les connexions à distance via KX II. Vous pourrez ainsi réserver aux connexions KX II les paramètres d'accélération/de mouvement lent du pointeur de la souris définis pour le serveur cible.

Les pages de connexion de Windows XP, 2000 et 2008 rétablissent les paramètres prédéfinis de la souris qui diffèrent de ceux suggérés pour des performances optimales de l'unité KX II. En conséquence, il est possible que la synchronisation de la souris ne soit pas optimale pour ces écrans.

Remarque : Effectuez cette opération uniquement si vous êtes capable de manipuler le Registre des serveurs cible KVM Windows. Vous pouvez obtenir une meilleure synchronisation de la souris KX II aux pages de connexion en utilisant l'éditeur du Registre Windows pour modifier les paramètres suivants : HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Paramètres Linux (Red Hat 4 et 5, et Fedora 14)

Remarque : les paramètres suivants sont optimisés uniquement pour le mode souris standard.

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

1. Définissez les paramètres de la souris :
   a. Choisissez Main Menu > Preferences > Mouse (Menu principal > Préférences > Souris). La boîte de dialogue des préférences de la souris s'affiche.
   b. Cliquez sur l'onglet Motion (Mouvement).
   c. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
   d. Dans la même section, définissez également une faible sensibilité.
   e. Dans la section du glisser-déposer, définissez un seuil faible.
   f. Fermez la boîte de dialogue des préférences de la souris.

   Remarque : si ces étapes ne fonctionnent pas, saisissez la commande xset mouse 1 1, comme décrit dans les instructions de ligne de commande Linux.

2. Définissez la résolution d'écran :
   a. Choisissez Main Menu > System Settings > Display (Menu principal > Paramètres système > Affichage). La boîte de dialogue des paramètres d'affichage apparaît.

b. Dans l'onglet Display (Affichage), sélectionnez une résolution prise en charge par KX II.

c. Dans l'onglet Advanced (Avancé), vérifiez que le taux de rafraîchissement est pris en charge par KX II.

Remarque : dans la plupart des environnement graphiques Linux, une fois que la connexion au serveur cible est établie, la commande <Ctrl> <Alt> <+> change la résolution vidéo en faisant défiler toutes les résolutions disponibles activées dans le fichier XF86Config ou /etc/X11/xorg.conf, suivant la distribution de votre serveur X.

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

1. Définissez l'accélération du pointeur de la souris et le seuil exactement sur 1. Entrez la commande suivante : *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 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 % :
   a. Localisez le fichier de configuration Xfree86 (XF86Config).
   b. Désactivez toutes les résolutions qui ne sont pas prises en charge par KX II à l'aide d'un éditeur de texte.
   c. Désactivez la fonctionnalité de bureau virtuel (non prise en charge par KX II).
   d. Vérifiez les temps de passage en blanc (valeurs VESA standard +/- 40 %).
   e. Redémarrez l'ordinateur.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Remarque concernant les serveurs cible KVM Red Hat et Fedora

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

Conseil : ces étapes peuvent se révéler nécessaires même après une installation propre du SE.

Pour configurer les serveurs Red Hat à l'aide de CIM USB :

1. Recherchez le fichier de configuration (généralement /etc/modules.conf) sur le système.
2. Ouvrez l'éditeur de votre choix et 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 soient appliquées.

Paramètres Linux (pour le mode souris standard)

Remarque : les paramètres suivants sont optimisés uniquement pour le mode souris standard.

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

1. Définissez les paramètres de la souris :
   a. Pour les utilisateurs de Red Hat 5 : Choisissez Main Menu > Preferences > Mouse (Menu principal > Préférences > Souris). Pour les utilisateurs de Red Hat 4 : Choisissez Main Menu > Preferences > Mouse (Menu principal > Préférences > Souris). La boîte de dialogue des préférences de la souris s'affiche.
   b. Cliquez sur l'onglet Mouvement.
   c. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
   d. Dans la même section, définissez également une faible sensibilité.
   e. Dans la section du glisser-déposer, définissez un seuil faible.

f. Fermez la boîte de dialogue des préférences de la souris.

Remarque : si ces étapes ne fonctionnent pas, saisissez la commande xset mouse 1 1, comme décrit dans les instructions de ligne de commande Linux.

2. Définissez la résolution d'écran :
   a. Choisissez Main Menu > System Settings > Display (Menu principal > Paramètres système > Affichage). La boîte de dialogue des paramètres d'affichage apparaît.
   b. Dans l'onglet Settings (Paramètres), sélectionnez une résolution prise en charge par KX II.
   c. Cliquez sur OK.

Remarque : dans la plupart des environnement graphiques Linux, une fois que la connexion au serveur cible est établie, la commande <Ctrl> <Alt> <+> change la résolution vidéo en faisant défiler toutes les résolutions disponibles activées dans le fichier XF86Config ou /etc/X11/xorg.conf, suivant la distribution de votre serveur X.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Paramètres SUSE Linux 10.1

Remarque : n'essayez pas de synchroniser la souris à l'invite de connexion SUSE Linux®. Vous devez être connecté au serveur cible pour synchroniser les curseurs de souris.

Pour configurer les paramètres de la souris :

1. Choisissez Desktop > Control Center (Bureau > Centre de contrôle). La boîte de dialogue des préférences du bureau s'affiche.
2. Cliquez sur Mouse (Souris). La boîte de dialogue des préférences de la souris s'affiche.
3. Ouvrez l'onglet Motion (Mouvement).
4. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
5. Dans la même section, définissez également une faible sensibilité.
6. Dans la section du glisser-déposer, définissez un seuil faible.
7. Cliquez sur Fermer.

Pour configurer la vidéo :

1. Choisissez Desktop Preferences > Graphics Card and Monitor (Préférences du bureau > Carte graphique et moniteur). La boîte de dialogue des propriétés de la carte et du moniteur s'affiche.
2. Vérifiez que la résolution et le taux de rafraîchissement utilisés sont pris en charge par KX II. Reportez-vous à **Résolutions vidéo prises en charge** (à la page 341) pour plus d'informations.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Rendre les paramètres Linux permanents

Remarque : ces étapes peuvent varier légèrement selon la version de Linux® utilisée.

Pour rendre vos paramètres dans Linux permanents (invite) :

1. Choisissez System Menu > Preferences > Personal > Sessions (Menu système > Préférences > Personnel > Sessions).
2. Cliquez sur l'onglet Session Options (Options de session).
3. Activez l'option Prompt on log off (Invite à la déconnexion), puis cliquez sur OK. Cette option vous invite à enregistrer la session en cours lorsque vous vous déconnectez.
4. Au moment de la déconnexion, activez l'option Save current setup (Enregistrer la configuration actuelle) dans la boîte de dialogue.
5. Cliquez sur OK.

Conseil : pour empêcher que cette invite ne s'affiche lorsque vous vous déconnectez, exécutez la procédure suivante.

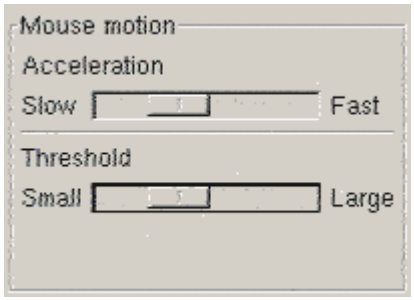
Pour rendre vos paramètres dans Linux permanents (sans invite) :

1. Choisissez Desktop (Bureau) > Control Center (Centre de contrôle) > System (Système) > Sessions.
2. Cliquez sur l'onglet Session Options (Options de session).
3. Désactivez la case à cocher Prompt on the log off (Invite à la déconnexion).
4. Activez l'option Automatically save changes to the session (Enregistrer automatiquement les modifications de la session), puis cliquez sur OK. Cette option enregistre automatiquement votre session actuelle au moment de la déconnexion.

Paramètres Sun Solaris

Pour configurer les serveurs cible KVM exécutant Sun™ Solaris™ :

1. 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 ;



   - à partir de la ligne de commande *xset mouse a t* où *a* représente l'accélération et *t*, le seuil.
2. Tous les serveurs cible KVM doivent être configurés en utilisant l'une des résolutions d'affichage prises en charge par KX II. Les résolutions les plus courantes sur les ordinateurs Sun sont :

Résolution d'affichage	Taux de rafraîchissement vertical	Rapport hauteur/largeur
1600 x 1200	60 Hz	4:3
1280 x 1024	60, 75, 85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60, 70, 75, 85 Hz	4:3
800 x 600	56, 60, 72, 75, 85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60, 72, 75, 85 Hz	4:3

3. Les serveurs cible KVM 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 revendeur Raritan.

Si vous avez	Utilisez cet adaptateur de sortie vidéo
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 prendre en charge la synchronisation composite.
Sun HD15 avec une sortie synchronisée de manière séparée	convertisseur APKMSUN Guardian.

Remarque : certains écrans d'arrière-plan Sun ne se centrent pas toujours précisément sur les serveurs Sun ayant des bordures sombres. Utilisez un autre arrière-plan ou une icône de couleur claire dans le coin supérieur gauche.

Paramètres de souris

Pour configurer les paramètres de la souris (Sun Solaris 10.1) :

1. Choisissez Launcher (Lancement). Application Manager - Desktop Controls (Gestionnaire d'applications - Contrôles de bureau) apparaît.
2. Sélectionnez Mouse Style Manager (Gestionnaire du style de souris). La boîte de dialogue Style Manager - Mouse (Gestionnaire de style - Souris) apparaît.
3. Définissez Acceleration sur 1.0.
4. Définissez Threshold (Seuil) sur 1.0.
5. Cliquez sur OK.

Accès à la ligne de commande

1. Cliquez avec le bouton droit de la souris.
2. Sélectionnez Tools (Outils) > Terminal. Une fenêtre de terminal s'ouvre. (Il est préférable de se trouver à la racine pour lancer des commandes.)

Paramètres vidéo (POST)

Les systèmes Sun ont deux paramètres de résolution différents : une résolution POST et une résolution GUI. Exécutez ces commandes depuis la ligne de commande.

Remarque : les valeurs 1024x768x75 sont utilisées ici à titre d'exemple. Remplacez ces paramètres par la résolution et le taux de rafraîchissement que vous utilisez.

Pour vérifier la résolution POST actuelle :

- Exécutez la commande suivante à la racine : `# eeprom output-device`

Pour modifier la résolution POST :

1. Exécutez `# eeprom output-device=screen:r1024x768x75`.
2. Déconnectez-vous ou redémarrez l'ordinateur.

Paramètres vidéo (GUI)

La résolution GUI peut être vérifiée et définie à l'aide de différentes commandes selon la carte vidéo utilisée. Exécutez ces commandes depuis la ligne de commande.

Remarque : les valeurs 1024x768x75 sont utilisées ici à titre d'exemple. Remplacez ces paramètres par la résolution et le taux de rafraîchissement que vous utilisez.

Carte	Pour vérifier la résolution :	Pour modifier la résolution :
32 bits	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.
64 bits	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.
32 bits et 64 bits	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.

Paramètres IBM AIX 5.3

Suivez la procédure ci-après pour configurer les serveurs cible KVM exécutant IBM® AIX™ 5.3.

Pour configurer la souris :

1. Démarrez le lanceur.
2. Sélectionnez Style Manager (Gestionnaire de style).
3. Cliquez sur Mouse (Souris). La boîte de dialogue Style Manager - Mouse (Gestionnaire de style - Souris) apparaît.
4. Définissez Mouse acceleration (Accélération de la souris) sur 1.0 et Threshold (Seuil) sur 1.0.
5. Cliquez sur OK.

Pour configurer la vidéo :

1. Depuis le lanceur, sélectionnez Application Manager (Gestionnaire d'applications).
2. Sélectionnez System_Admin.
3. Sélectionnez Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate (Smit > Dispositifs > Affichages graphiques > Sélectionner la résolution d'affichage et le taux de rafraîchissement).
4. Sélectionnez la carte vidéo utilisée.
5. Cliquez sur List. Une liste de modes d'affichage apparaît.
6. Sélectionnez une résolution et un taux de rafraîchissement pris en charge par KX II. Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 341) pour plus d'informations.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Rendre les paramètres UNIX permanents

Remarque : ces étapes peuvent varier légèrement selon le type d'UNIX® (par exemple, Solaris™, IBM® AIX™) et la version utilisée.

---

1. Sélectionnez Style Manager (Gestionnaire de style) > Startup (Démarrage). La boîte de dialogue Style Manager - Startup (Gestionnaire de style - Démarrage) apparaît.
2. Dans la fenêtre Logout Confirmation (Confirmation de connexion), sélectionnez l'option On (Activé). Cette option vous invite à enregistrer la session en cours lorsque vous vous déconnectez.

Paramètres Apple Macintosh

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

Remarque : l'option USB Profile Mac OS-X, version 10.4.9 and later (Profil USB Mac OS X, versions 10.4.9 et supérieure) doit être sélectionnée dans le menu USB Profile (Profil USB) ou dans la page Port Configuration (Configuration des ports).

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

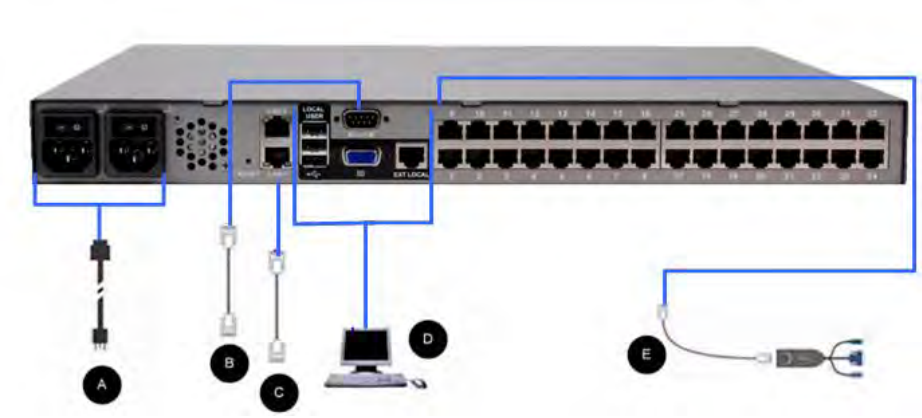
Pour accéder à KX II à travers un pare-feu de réseau par l'intermédiaire de Multi-Platform Client ou de la page Port Access (Accès aux ports), le pare-feu doit autoriser la communication sur TCP Port 5000 ou sur un autre port de votre choix.

Pour tirer parti de KX II :	**Le pare-feu doit permettre la communication en amont sur :**
Fonctionnalités d'accès Web	Port 443 : port TCP standard pour la communication HTTPS
Redirection automatique des requêtes HTTP vers HTTPS (l'adresse plus courante http://xxx.xxx.xxx.xxx peut être utilisée à la place de https://xxx.xxx.xxx.xxx.)	Port 80 : port TCP standard pour la communication HTTP

Reportez-vous à ***Paramètres réseau*** (à la page 176) pour plus d'informations sur la désignation d'un autre port de détection.

Etape 3 : Connexion de l'équipement

Branchez KX II sur l'alimentation, le réseau, le PC local, l'écran vidéo local, le clavier et la souris, et les serveurs cible. Les lettres du schéma correspondent aux rubriques de description de la connexion dans cette section.



A. Alimentation CA

Pour connecter l'alimentation :

1. Raccordez le cordon d'alimentation CA fourni avec KX II et branchez-le sur une prise électrique.
2. Pour une alimentation à double protection par basculement, raccordez le second cordon d'alimentation fourni et branchez-le à une source d'alimentation différente de celle auquel le premier cordon est raccordé.

Remarque : si vous ne connectez qu'un cordon, le voyant d'alimentation sur le panneau avant de KX II est rouge car le système n'est pas configuré pour détecter les deux sources automatiquement. Reportez-vous à **Configuration de l'alimentation** *(à la page 206) pour obtenir des informations sur la désactivation de la fonction de détection automatique de la source d'alimentation non utilisée.*

B. Port du modem (facultatif)

KX II dispose d'un port modem dédié qui permet l'accès à distance même lorsque le réseau local/réseau étendu n'est pas disponible. Utilisez un câble série à brochage direct (RS-232) pour relier un modem série externe au port libellé MODEM à l'arrière de KX II. Reportez-vous à Spécifications pour obtenir la liste des modems agréés et à ***Configuration des paramètres de modem*** (à la page 193) pour plus d'informations sur la configuration du modem.

Remarque : Raritan recommande de configurer le modem en activant le paramètre CD (carrier detect).

C. Port réseau

KX II dispose de deux ports Ethernet pour les basculements (et non pour l'équilibrage des charges). Par défaut, seul LAN1 est actif et le basculement automatique est désactivé. S'il est activé et que l'interface réseau interne de l'unité KX II ou le commutateur réseau auquel elle est connectée n'est plus disponible, LAN2 est activé avec la même adresse IP.

Remarque : les ports de basculement n'étant pas activés avant un basculement effectif, Raritan recommande de ne pas surveiller ces ports ou de le faire après un basculement.

Pour connecter le réseau :

1. Reliez un câble Ethernet standard (fourni) du port réseau LAN1 à un commutateur, concentrateur ou routeur Ethernet.
2. Pour utiliser les capacités de basculement Ethernet facultatives de KX II :
   - Reliez un câble Ethernet standard du port réseau libellé LAN2 à un commutateur, concentrateur ou routeur Ethernet.
   - Activez Automatic Failover (Basculement automatique) sur l'écran Network Configuration (Configuration réseau).

Remarque : n'utilisez les deux ports réseau que si l'un doit servir de port de basculement.

D. Port pour accès local (écran vidéo local, clavier et souris)

Pour accéder facilement aux serveurs cible sur le rack, utilisez le port d'accès local de KX II. Si le port d'accès local est obligatoire pour l'installation et le paramétrage, il est facultatif par la suite. Le port d'accès local fournit également une interface utilisateur graphique depuis la console locale de KX II pour l'administration et l'accès au serveur cible.

KX2-808, KX2-832 et KX2-864 fournissent également un port Extended Local, libellé EXT LOCAL à l'arrière du dispositif, pour accéder aux serveurs cible sur le rack. Ce port n'est pas requis pour l'installation et le paramétrage initiaux. Il n'est pas activé par défaut mais est configuré depuis les consoles locale et distante. Reportez-vous à ***Configuration des paramètres du port local de KX II*** (à la page 246) pour plus d'informations.

Pour connecter le port local :

- Reliez un écran MultiSync VGA, une souris et un clavier aux ports libellés Local User (Utilisateur local) respectifs. Utilisez un clavier et une souris PS/2 ou USB (KX2-808, DKX2-832 et DKX2-864 offrent l'USB uniquement). Les connexions physiques des ports Local User (Utilisateur local) et Extended Local (Local étendu) se trouvent sur le panneau arrière de KX II.

Connexion	Description
Ecran	Branchez un écran VGA Multisync standard sur le port vidéo HD15 (femelle).
Clavier	Branchez un clavier PS/2 standard sur un port clavier Mini-DIN6 (femelle) ou un clavier USB standard sur un des ports USB de type A (femelle).
Souris	Branchez une souris PS/2 standard sur un port souris Mini-DIN6 (femelle) ou une souris USB standard sur un des ports USB de type A (femelle).

Remarque : les futurs modèles KX II offriront des ports USB et non des ports locaux PS/2.

E. Ports de serveur cible

KX II utilise un câblage UTP standard (Cat5/5e/6) pour sa connexion à chaque serveur cible. Reportez-vous à ***Distance de connexion du serveur cible/taux de rafraîchissement/résolution vidéo pris en charge*** (voir "***Distance de connexion et résolution vidéo du serveur cible prises en charge***" à la page 343) pour plus d'informations sur les distances acceptées entre KX II et le serveur cible. Si vous utilisez des CIM numériques (DCIM), reportez-vous à ***Synchronisation et résolution vidéo du serveur cible des CIM numériques*** (à la page 347).

Pour connecter un serveur cible à KX II :

1. Utilisez les modules CIM (module d'interface pour ordinateur) ou DCIM (module d'interface numérique pour ordinateur). Reportez-vous à ***Spécifications des modules d'interface pour ordinateur (CIM) pris en charge*** (voir "***Spécifications des CIM pris en charge***" à la page 343) pour plus d'informations sur les CIM à utiliser avec chaque système d'exploitation.
2. Raccordez le connecteur vidéo HD15 de votre CIM/DCIM au port du serveur cible. Vérifiez que l'écran du serveur cible est déjà configuré sur une résolution et un taux de rafraîchissement pris en charge. Pour les serveurs Sun, assurez-vous que la carte vidéo du serveur cible est paramétrée sur une sortie VGA standard (Sync H-et-V) et non Sync Composite.
3. Reliez le connecteur clavier/souris de votre CIM/DCIM aux ports correspondants du serveur cible. Utilisez un DCIM si vous vous connectez à KX II depuis le port vidéo du serveur cible.
4. Reliez le CIM à un port disponible du serveur à l'arrière du dispositif KX II. Utilisez un câble UTP à brochage direct standard (Cat5/5e/6) pour les CIM ou un câble USB standard pour les DCIM.

Remarque : DCIM-USB G2 présente un petit commutateur à l'arrière du CIM. Placez ce commutateur sur P pour les serveurs cible USB PC. Placez ce commutateur sur S pour les serveurs cible USB Sun.

Une nouvelle position de commutateur ne prend effet qu'après l'alimentation cyclique du CIM. Pour effectuer l'alimentation cyclique du CIM, retirez le connecteur USB du serveur cible, puis rebranchez-le quelques secondes plus tard.

Etape 4 : Configuration de KX II

A la première mise sous tension du dispositif KX II, vous devez effectuer des opérations de configuration initiale via la console locale de KX II :

- Modifier le mot de passe par défaut
- Affecter l'adresse IP
- Configuration des paramètres de date et heure (facultatif)
- Désigner les serveurs cible KVM

KX II est configurable à distance via un navigateur Web. Votre poste de travail doit donc disposer d'une version de Java Runtime Environment (JRE) appropriée.

Modification du mot de passe par défaut

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

Pour changer le mot de passe par défaut :

1. Une fois l'unité amorcée, entrez le nom d'utilisateur (admin) et le mot de passe (raritan) par défaut. Cliquez sur Login (Se connecter).
2. Entrez l'ancien mot de passe (raritan), le nouveau mot de passe, puis encore le nouveau. Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques et caractères spéciaux (présents sur un clavier anglais). Cliquez sur Apply (Appliquer). Cliquez sur OK sur la page Confirmation.
3. Remarque : le mot de passe par défaut peut également être modifié à partir de Multi-Platform Client (MPC) de Raritan.

Remarque : le mot de passe par défaut peut également être modifié à partir de Multi-Platform Client (MPC) de Raritan.

Affectation d'une adresse IP

Ces procédures décrivent comment affecter une adresse IP sur la page Network Settings (Paramètres réseau). Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à ***Paramètres réseau*** (à la page 176).

Pour affecter une adresse IP :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Indiquez un nom de dispositif significatif pour votre unité KX II. 32 caractères alphanumériques au plus, avec des caractères spéciaux valides et aucun espace.

3. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :
   a. Entrez l'adresse IP si nécessaire. L'adresse IP par défaut est 192.168.0.192.
   b. Entrez le masque de sous-réseau. Le masque de sous-réseau par défaut est 255.255.255.0.
   c. Entrez la passerelle par défaut si None (Néant) est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).
   d. Entrez le nom d'hôte DHCP préféré si DHCP est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).
   e. Sélectionnez la configuration IP automatique. Les options suivantes sont disponibles :

   - None (Static IP) (Néant (IP statique)) : cette option nécessite que vous indiquiez manuellement les paramètres réseau.

     Cette option est recommandée car KX II est un dispositif d'infrastructure et son adresse IP ne doit pas être modifiée.
   - 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.

     Avec cette option, les paramètres réseau sont attribués par le serveur DHCP. Si DHCP est utilisé, entrez le nom d'hôte préféré (DHCP uniquement). Maximum de 63 caractères.

4. Si IPv6 doit être utilisé, entrez ou sélectionnez les paramètres réseau spécifiques à IPv6 appropriés dans la section IPv6 :
   a. Cochez la case IPv6 pour activer les champs de la section.
   b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à KX II.
   c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.
   d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).
   e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**
   f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

g. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Néant) - 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.

  Lorsqu'elle est sélectionnée pour la configuration IP automatique, les champs Network Basic Settings (Paramètres réseau de base) sont activés : Global/Unique IP Address (Adresse IP globale/unique), Prefix Length (Longueur de préfixe) et Gateway IP Address (Adresse IP de la passerelle). Vous pouvez paramétrer manuellement la configuration IP.

- Router Discovery (Détection de routeur) - Utilisez cette option pour affecter automatiquement des adresses IPv6 ayant une portée « Global » ou « Unique Local » au-delà des adresses « Link Local » qui ne s'appliquent qu'à un sous-réseau connecté directement.

5. Si l'option DHCP est activée et que le champ Obtain DNS Server Address Automatically (Obtenir l'adresse du serveur DNS automatiquement) est accessible, sélectionnez-le. Les données DNS fournies par le serveur DHCP seront alors utilisées.
6. Si l'option Use the Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée, que DHCP soit sélectionné ou non, les adresses saisies dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les données suivantes si l'option Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée. Il s'agit des adresses DNS primaire et secondaire qui seront utilisées si la connexion au serveur DNS primaire est perdue lors d'une panne.

   a. Adresse IP du serveur DNS primaire

   b. Adresse IP du serveur DNS secondaire.

7. Lorsque vous avez terminé, cliquez sur OK.

Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 180) pour plus d'informations sur la configuration de cette section de la page Network Settings (Paramètres réseau).

Remarque : dans certains environnements, le paramètre par défaut du champ LAN Interface Speed & Duplex (Vitesse d'interface LAN & Duplex), Autodetect (auto-détection), ne définit pas correctement les paramètres réseau, ce qui entraîne des problèmes sur le réseau. Dans ce cas, paramétrez le champ LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN) de KX II sur 100 Mbps/Full Duplex (Bidirectionnel simultané) (ou toute option appropriée à votre réseau) pour résoudre le problème. Reportez-vous à la page **Paramètres réseau** *(à la page 176) pour plus d'informations.*

Configuration des paramètres de date et heure (facultatif)

Le cas échéant, configurez les paramètres de date et d'heure. Notez que ces paramètres affectent la validation du certificat SSL si LDAPS est activé.

Pour définir la date et l'heure :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Date/Time (Date/heure). La page Date/Time Settings (Paramètres de date/heure) s'ouvre.
2. Sélectionnez votre fuseau horaire dans la liste déroulante Time Zone (Fuseau horaire).
3. Pour prendre en compte l'heure d'été, cochez la case Adjust for daylight savings time (Régler selon les changements d'heure).
4. Choisissez la méthode que vous souhaitez utiliser pour définir la date et l'heure :
   - User Specified Time - Sélectionnez cette option pour saisir la date et l'heure manuellement. Pour l'option User Specified Time (Heure spécifiée par l'utilisateur), entrez la date et l'heure. Pour l'heure, utilisez le format hh:mm (système de 24 heures).
   - Synchronize with NTP Server - Sélectionnez cette option pour synchroniser la date et l'heure avec le serveur NTP.
5. Pour l'option Synchronize with NTP Server (Synchroniser avec le serveur NTP) :
   a. Entrez une adresse IP dans le champ Primary Time server (Serveur d'horloge principal).
   b. Renseignez le champ Secondary Time server (Serveur d'horloge secondaire). **Facultatif**
6. Cliquez sur OK.

Nommage des serveurs cible

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à **Etape 3 : Connexion de l'équipement** (à la page 35) pour obtenir une description de la connexion de l'équipement.
2. A l'aide de la console locale KX II, choisissez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports), cliquez sur le nom du port du serveur cible à nommer.
3. Entrez le nom du serveur, qui peut comporter jusqu'à 32 caractères alphanumériques et spéciaux. Cliquez sur OK.

Caractères spéciaux valides pour les noms de cibles

Caractère	Description	Caractère	Description
!	Point d'exclamation	;	Point-virgule
"	Guillemet	=	Signe égal
#	Dièse	>	Signe supérieur à
$	Symbole du dollar	?	Point d'interrogation
%	Symbole du pourcentage	@	Arobas
&	« Et » commercial	[	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
:	Deux-points		

Spécification de la détection automatique de l'alimentation

KX II offre une double alimentation. Par ailleurs, elle peut détecter et notifier automatiquement l'état de ces alimentations. Une configuration appropriée garantit l'envoi de notifications adéquates par KX II en cas de panne de courant.

La page Power Supply Setup (Configuration de l'alimentation) est configurée de manière à détecter automatiquement les deux sources d'alimentation lorsque deux sources sont utilisées. Si une seule source d'alimentation est utilisée dans votre configuration, vous pouvez désactiver la détection automatique sur la page de configuration de l'alimentation.

Pour activer la détection automatique des alimentations utilisées :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation). La page Power Supply Setup s'ouvre.
2. Si vous branchez une arrivée électrique dans l'alimentation numéro un (alimentation la plus à gauche à l'arrière du dispositif), cochez la case Powerln1 Auto Detect (Détection automatique Powerln1).
3. Si vous branchez une arrivée électrique dans l'alimentation numéro deux (alimentation la plus à droite à l'arrière du dispositif), cochez la case Powerln2 Auto Detect (Détection automatique Powerln2).
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 d'alimentation non utilisée :

1. Depuis la console locale de KX II, sélectionnez Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation). La page Power Supply Setup s'ouvre.
2. Désactivez la détection automatique de l'alimentation que vous n'utilisez pas.

Pour plus d'informations, reportez-vous à ***Configuration de l'alimentation*** (à la page 206).

Remarque aux utilisateurs de CC-SG

Si vous utilisez KX II dans une configuration CC-SG, suivez la procédure d'installation. Celle-ci terminée, consultez le **manuel d'utilisation**, **manuel de l'administrateur** ou **guide de déploiement** de CommandCenter Secure Gateway pour poursuivre (tous se trouvent sur le site Web de Raritan, www.raritan.com, sous Support).

Remarque : la suite de cette aide s'applique essentiellement au déploiement des dispositifs KX II sans utiliser les fonctions d'intégration de CC-SG.

Authentification à distance

Remarque aux utilisateurs de CC-SG

Lorsque KX II est géré par CommandCenter Secure Gateway, CC-SG authentifie les utilisateurs et les groupes, à l'exception des utilisateurs locaux requérant l'accès au port local. Lorsque CC-SG assure la gestion de KX II, les utilisateurs du port local sont authentifiés par rapport à la base de données des utilisateurs locaux ou au serveur d'authentification à distance (LDAP/LDAPS ou RADIUS) configurés sur KX II. Ils ne sont pas authentifiés par rapport à la base de données des utilisateurs de CC-SG.

Pour plus d'informations sur l'authentification de CC-SG, consultez le manuel d'utilisation, le manuel de l'administrateur ou le guide de déploiement de CommandCenter Secure Gateway, disponibles par téléchargement dans la section Support du ***site Web de Raritan http://www.raritan.com***.

Protocoles pris en charge

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

Remarque relative à Microsoft Active Directory

Microsoft® Active Directory® utilise le protocole LDAP/LDAPS de manière native et peut servir de source d'authentification et serveur LDAP/LDAPS avec 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.

Création de groupes d'utilisateurs et d'utilisateurs

Dans le cadre de la configuration initiale, vous devez définir des groupes d'utilisateurs et des utilisateurs pour permettre à ces derniers d'accéder à KX II.

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.

Un nom d'utilisateur et un mot de passe sont nécessaires pour accéder à KX II. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre KX II. Reportez-vous à **Gestion des utilisateurs (à la page 148) pour plus d'informations sur l'ajout et la modification des groupes d'utilisateurs et des utilisateurs.**

Etape 5 : Lancement de la console distante de KX II

Pour démarrer la console distante de KX II :

1. Connectez-vous à KX II depuis un poste de travail doté d'une connectivité réseau et de Microsoft .NET® et/ou Java Runtime Environment® (JRE® est disponible sur le ***site Web de Java http://java.sun.com/***).
2. Démarrez un navigateur Web pris en charge, tel qu'Internet Explorer® ou Firefox®.
3. Entrez l'URL : *http://ADRESSE-IP* ou *http://ADRESSE-IP/akc* pour .NET, où ADRESSE-IP correspond à l'adresse IP affectée au dispositif KX II. Vous pouvez aussi utiliser https, le nom DNS de KX II attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou simplement saisir l'adresse IP dans le navigateur (KX II redirige toujours l'adresse IP de HTTP vers HTTPS).
4. Entrez vos nom d'utilisateur et mot de passe. Cliquez sur Login (Se connecter).

Accès et gestion des serveurs cible à distance

La page Port Access (Accès aux ports) de KX II fournit la liste de tous les ports du produit, des serveurs cible connectés, de leur état et de leur disponibilité.

Accès à un serveur cible

Pour accéder à un serveur cible :

1. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.
2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. Une fenêtre KVM s'ouvre, qui contient une connexion à la cible.

Commutation entre les serveurs cible

Pour commuter entre des serveurs cible KVM :

1. Si vous utilisez déjà un serveur cible, accédez à la page Port Access de KX II.
2. Cliquez sur le nom du port associé à la cible à laquelle vous souhaitez accéder. Le menu Port Action (Action des ports) apparaît.
3. Sélectionnez Switch From (Commuter depuis) dans le menu d'action des ports. Le nouveau serveur cible sélectionné est affiché.

Déconnexion d'un serveur cible

Pour déconnecter un serveur cible :

- Cliquez sur le nom de port de la cible que vous souhaitez déconnecter. Lorsque le menu Port Action (Action des ports) apparaît, cliquez sur Disconnect (Déconnecter).

Etape 6 : Configuration de la langue du clavier (facultatif)

Remarque : cette étape n'est pas obligatoire si vous utilisez un clavier américain/international.

Si vous utilisez une langue autre que l'anglais américain, le clavier doit être configuré pour celle-ci. De plus, la langue du clavier de l'ordinateur client et des serveurs cible KVM doit être la même.

Consultez la documentation de votre système d'exploitation pour plus d'informations sur la modification de la disposition du clavier.

Modification du code de disposition de clavier (cibles Sun)

Suivez cette procédure si vous disposez d'un DCIM-SUSB et souhaitez utiliser une disposition de 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 sur le poste de travail Sun™.
2. Assurez-vous que la touche Verr num est active, et appuyez sur la touche Ctrl située à gauche et sur la touche Suppr du clavier. Le voyant du verrouillage des majuscules clignote 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).`
3. Saisissez le code de disposition souhaité (par exemple, *31* pour le clavier japonais).
4. Appuyez sur Entrée.

5. Mettez le dispositif hors tension, puis à nouveau sous tension. Le DCIM-SUSB procède à une réinitialisation (alimentation cyclique).
6. Vérifiez que les caractères sont corrects.

Etape 7 : Configuration de la fonction multiniveau (facultatif)

La fonction multiniveau facultative permet de relier des dispositifs KX II en niveau à un dispositif KX II de base. Vous pouvez alors accéder aux serveurs et aux PDU PX localement et à distance au moyen de la base. Reportez-vous à la section **Gestion des dispositifs** (à la page 176) de l'**aide de KX II** pour en savoir plus sur cette fonction.

Connectez depuis un port de serveur cible sur le dispositif de base aux ports vidéo/clavier/souris du port Local Access du KX II en niveau à l'aide d'un D2CIM-DVUSB.

Si le dispositif en niveau est un dispositif KX2-808, KX2-832 ou KX2-864, effectuez la connection depuis un port du serveur cible sur le dispositif de base directement au port Extended Local du KX2-808/KX2-832/KX2-864 en niveau.

Pour activer la fonction multiniveau :

1. Depuis la base du niveau, choisissez Device Settings > Device Services (Paramètres du dispositif > Services du dispositif). La page de paramétrage Device Services (Services du dispositif) apparaît.
2. Sélectionnez Enable Tiering as Base (Activer la fonction multiniveau comme base).
3. Dans le champ Base Secret (Secret de la base), entrez le secret partagé entre la base et les dispositifs en niveau. Ce secret est exigé pour permettre aux dispositifs en niveau d'authentifier le dispositif de base. Vous entrerez le même mot secret pour le dispositif en niveau.
4. Cliquez sur OK.
5. Activez les dispositifs en niveau. Depuis le dispositif en niveau, choisissez Device Settings > Local Port Settings (Paramètres du dispositif > Paramètres du port local).
6. Dans la section Enable Local Ports (Activer les ports locaux) de la page, sélectionnez Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local).
7. Dans le champ Tier Secret (Secret du niveau), entrez le mot secret entré pour le dispositif de base sur la page Device Settings (Paramètres du dispositif).
8. Cliquez sur OK.

Chapitre 3 Utilisation des serveurs cible

Dans ce chapitre

Interfaces KX II

KX II dispose de plusieurs interfaces utilisateur qui fournissent un accès aisé aux cibles à tout moment, où que vous soyez. Ces interfaces incluent la console locale de KX II, la console distante de KX II, Virtual KVM Client (VKC), Active KVM Client (AKC) et Multi-Platform Client (MPC). Le tableau ci-après décrit les interfaces et leur utilisation pour l'accès aux serveurs cible et la gestion de ces derniers localement et à distance :

Interface utilisateur	Locale		Distante	
	distant	Admin	distant	Admin
Console locale de KX II	✓	✓		
Console distante de KX II			✓	✓
Virtual KVM Client (VKC)			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

Les sections suivantes de l'aide contiennent des informations sur l'utilisation d'interfaces particulières pour accéder à KX II et gérer les cibles :

- Console locale
- Console distante
- Virtual KVM Client
- Multi-Platform Client

Interface de la console locale de KX II : Dispositifs KX II

Lorsque vous êtes situé au niveau du rack du serveur, KX II permet une gestion KVM standard via la console locale de KX II. La console locale de KX II offre une connexion (analogique) KVM directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Les interfaces graphiques utilisateur de la console locale de KX II et de la console distante de KX II présentent de nombreuses ressemblances. Les éventuelles différences sont indiquées dans l'aide.

L'option Factory Reset (Rétablir les valeurs usine) est disponible sur la console locale de KX II et non sur la console distante de KX II.

Interface de la console distante de KX II

La console distante de KX II est une interface graphique utilisateur navigateur qui vous permet de vous connecter aux serveurs cible KVM et aux cibles série connectés à KX II, et de gérer KX II à distance.

Elle offre une connexion numérique à vos serveurs cible KVM connectés. Lorsque vous accédez à un serveur cible KVM à l'aide de la console distante de KX II, une fenêtre Virtual KVM Client s'ouvre.

Il existe de nombreuses ressemblances entre les interfaces utilisateur graphiques de la console locale de KX II et de la console distante de KX II. Les éventuelles différences sont indiquées dans le manuel d'utilisation. Les options suivantes sont disponibles sur la console distante de KX II mais non sur la console locale de KX II :

- Support virtuel
- Favorites (Favoris)
- Backup/Restore (Sauvegarde/Restauration)
- Firmware Upgrade (Mise à niveau du firmware)
- Certificats SSL
- Audio

Lancement de la console distante de KX II

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

Selon le navigateur utilisé et les paramètres de sécurité, 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 de KX II.

Vous pouvez 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 :

- 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 démarrer la console distante de KX II :

1. Connectez-vous à KX II depuis un poste de travail doté d'une connectivité réseau et de Microsoft .NET® et/ou Java Runtime Environment® (JRE® est disponible sur le ***site Web de Java http://java.sun.com/***).
2. Démarrez un navigateur Web pris en charge, tel qu'Internet Explorer® ou Firefox®.
3. Entrez l'URL : *http:///ADRESSE-IP* ou *http:///ADRESSE-IP/akc* pour .NET, où ADRESSE-IP correspond à l'adresse IP affectée au dispositif KX II. Vous pouvez aussi utiliser https, le nom DNS de KX II attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou simplement saisir l'adresse IP dans le navigateur (KX II redirige toujours l'adresse IP de HTTP vers HTTPS).
4. Tapez votre nom d'utilisateur et votre mot de passe. S'il s'agit de la première connexion, utilisez le nom d'utilisateur (admin) et le mot de passe (raritan, en minuscules) par défaut usine. Il vous est alors demandé de modifier le mot de passe par défaut. Cliquez sur Login (Se connecter).

Remarque : si l'administrateur exige la lecture et/ou l'acceptation d'un accord de sécurité pour l'accès au dispositif, une bannière de sécurité s'affiche lorsque vous entrez vos informations d'identification et cliquez sur Login (Connexion).

Reportez-vous à ***Virtual KVM Client (VKC) et Active KVM Client (AKC)*** (à la page 70) pour plus d'informations sur les fonctions KX II disponibles via la console distante.

Interface et navigation

Interface KX II

Les interfaces des consoles distante et locale de KX II présentent toutes les deux une interface Web pour la configuration et l'administration de dispositifs, ainsi qu'une liste et des fonctions de sélection des serveurs cible. Les options sont organisées dans différents onglets.

Une fois la connexion réussie, la page d'accès aux ports s'affiche avec la liste de tous les ports ainsi que leur statut et leur disponibilité. Quatre onglets sont présents sur la page et permettent un affichage par port, par groupe ou par recherche. Vous pouvez effectuer un tri par numéro de port, nom de port, état (activé ou non) et disponibilité (inactif, connecté, occupé, indisponible ou en cours de connexion) en cliquant sur un en-tête de colonne. Reportez-vous à ***Page Port Access (Affichage de la console distante)*** (à la page 56) pour plus d'informations.

Utilisez l'onglet Set Scan (Balayage d'ensemble) pour balayer jusqu'à 32 cibles connectées à KX II. Reportez-vous à ***Balayage des ports*** (à la page 61).

Panneau gauche

Le panneau gauche de l'interface KX II contient les informations suivantes. Notez que certaines d'entre elles sont conditionnelles et ne s'afficheront que si vous êtes un utilisateur particulier, utilisez certaines fonctions, etc. Les informations conditionnelles sont indiquées ici.

Information	Description	Affichée quand ?
Time & Session (Heure & session)	Date et heure de début de la session en cours.	Toujours
Utilisateur	Nom d'utilisateur	Toujours
State (Etat)	Etat actuel de l'application, inactive ou active. Si l'application est active, elle suit et affiche la durée d'inactivité de la session.	Toujours
Your IP (Votre IP)	Adresse IP utilisée pour accéder à KX II.	Toujours
Last Login (Dernière connexion)	Date et heure de la dernière connexion.	Toujours
Under CC-SG Management (Géré par CC-SG)	Adresse IP du dispositif CC-SG assurant la gestion de KX II.	Quand KX II est géré par CC-SG.
Device Information (Informations sur le dispositif)	Information spécifique au KX II que vous utilisez.	Toujours
Device Name (Nom du dispositif)	Nom affecté au dispositif.	Toujours
IP Address (Adresse IP)	Adresse IP du KX II.	Toujours
Firmware	Version actuelle du firmware.	Toujours
Device Model (Modèle du dispositif)	Modèle du KX II	Toujours
Numéro de série	Numéro de série de KX II	Toujours
Réseau	Nom attribué au réseau en cours.	Toujours

Information	Description	Affichée quand ?
PowerIn1	Statut de la connexion de la prise 1 d'alimentation. Sous tension ou hors tension, ou détection automatique désactivée.	Toujours
PowerIn2	Statut de la connexion de la prise 2 d'alimentation. Sous tension ou hors tension, ou détection automatique désactivée.	Toujours
Configured As Base or Configured As Tiered (Configuré comme base ou Configuré comme niveau)	Si vous utilisez une configuration multiniveau, ceci indique si le KX II auquel vous accédez est le dispositif de base ou un dispositif en niveau.	Lorsque KX II fait partie d'une configuration multiniveau
Port States (Etats des ports)	Statut des ports utilisés par KX II.	Toujours
Connect Users (Utilisateurs connectés)	Utilisateurs, identifiés par leur nom d'utilisateur et adresse IP, actuellement connectés au KX II.	Toujours
Aide en ligne	Liens vers l'aide en ligne.	Toujours
Favorite Devices (Dispositifs favoris)	Reportez-vous à ***Gestion des favoris*** (à la page 64).	Toujours
FIPS Mode (Mode FIPS)	Mode FIPS : Activé Certificat SSL : compatible avec le mode FIPS	Quand le mode FIPS est activé

Le panneau gauche peut être réduit pour augmenter la zone d'affichage de la page.

Pour réduire le panneau gauche :

- Cliquez sur la flèche bleue vers la gauche située vers le milieu du côté gauche du panneau. Une fois le panneau réduit, cliquez à nouveau sur la flèche bleue pour le développer.

Navigation dans la console KX II

Les interfaces de la console KX II offrent plusieurs méthodes de navigation et de sélection.

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

- Cliquez sur un onglet. Une page d'options disponibles apparaît.
- Placez le curseur sur un onglet puis sélectionnez l'option souhaitée dans le menu.
- Cliquez sur l'option directement dans la hiérarchie de menu affichée (fils d'Ariane).

Pour faire défiler les pages plus longues que l'écran :

- Utilisez les touches PageSup et PageInf sur votre clavier ;
- utilisez la barre de défilement à droite de l'écran.

Page Port Access (Affichage de la console distante)

Une fois la connexion à la console distante de KX II établie, l'onglet View by Port (Affichage par port) de la page Port Access (Accès aux ports) s'ouvre. Cette page répertorie tous les ports de KX II et les serveurs cibles, groupes de ports et châssis de lames connectés à ces ports.

Par défaut, les données sont triées par numéro de port, mais vous pouvez modifier l'affichage pour trier sur n'importe quelle colonne disponible en cliquant sur un en-tête de colonne. Pour augmenter ou réduire le nombre de rangées affichées simultanément dans un onglet, renseignez le champ Rows per Page (Rangées par page) et cliquez sur Set (Définir).

Les données concernant chaque port affichées dans cette page sont les suivantes :

- Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif KX II.

  Remarque : les ports connectés aux barrettes d'alimentation ne sont pas répertoriés, ce qui génère des trous dans la séquence des numéros de port.

- Port Name (Nom de port) - Nom du port de KX II. Initialement, ce champ est paramétré sur Dominion-KX2-Port# mais vous pouvez remplacer ce nom par un autre plus parlant.
- Status (Statut) - Statut des serveurs, activé ou désactivé.
- Type - Type de serveur ou CIM/DCIM.

  Pour les châssis de lames, ce type peut être Blade Chassis, Blade, BladeChassisAdmin et BladeChassisURL.

Les groupes de deux ports vidéo apparaissent sur la page Port Access comme types Dual Port. Les ports principal et secondaire faisant partie du groupe de ports apparaissent sur la page Port Access comme Dual Port(P) et Dual Port(S), respectivement. Par exemple, si le type du CIM est DCIM, DCIM Dual Port (P) est affiché.

No.	Name	Type	Status	Availability
1	Dominion_KX2_Port1	Not Available	down	idle
2	winXP-primary	Dual-VM Dual Port (P)	up	idle
3	Dominion_KX2_Port3	Not Available	down	idle
5	win7-secondary	DVM-HDMI Dual Port (S)	up	idle
6	Dominion_KX2_Port6	Not Available	down	idle
7	win7-primary	VM Dual Port (P)	up	idle
8	winXP-secondary	DVM-DVI Dual Port (S)	up	idle
9	Ananth	Not Available	down	idle
10	Dominion_KX2_Port10	Not Available	down	idle
11	Dominion_KX2_Port11	Not Available	down	idle
12	Dominion_KX2_Port12	Not Available	down	idle
13	Dominion_KX2_Port13	Not Available	down	idle

Pour vous connecter à un serveur cible disponible ou à deux écrans :

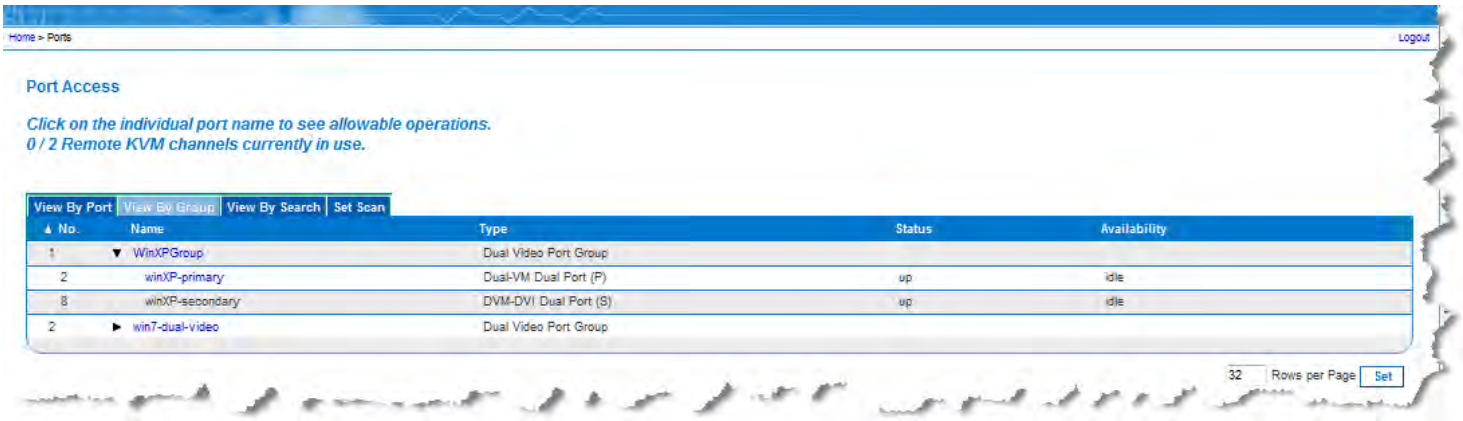
1. Cliquez sur le nom du port. Le menu Port Action (Action des ports) s'ouvre.
2. Cliquez sur Connect (Connecter). Lorsque vous êtes connecté à une cible ou à un serveur cible à deux écrans, cliquez sur le nom du groupe de ports, puis sur Disconnect pour vous déconnecter.

Reportez-vous à ***Port Action Menu (Menu d'action de ports)*** (à la page 60) pour plus d'informations sur les options de menu supplémentaires disponibles.

Onglet View by Group (Afficher par groupe)

L'onglet View by Group (Afficher par groupe) présente les châssis de lames, les groupes de ports standard et de deux ports vidéo. Cliquez sur l'icône Expand Arrow ▶ en regard d'un groupe pour afficher les ports qui lui sont affectés.

Reportez-vous à ***Gestion des dispositifs*** (à la page 176) pour obtenir des informations sur la création de chaque type de groupes de ports.



Onglet View by Search (Afficher par recherche)

L'onglet View by Search (Afficher par recherche) vous permet d'effectuer une recherche par nom de port. La fonction de recherche prend en charge l'utilisation d'un astérisque (*) comme caractère joker, et les noms entiers ou partiels.

Onglet Set Scan (Balayage d'ensemble)

La fonction de balayage des ports est accessible depuis l'onglet Set Scan (Balayage d'ensemble) de la page Port Access (Accès aux ports). Elle vous permet de définir un ensemble de cibles à balayer. Des vues en miniature des cibles balayées sont également disponibles. Sélectionnez une miniature pour ouvrir la cible correspondante dans sa fenêtre Virtual KVM Client.

Reportez-vous à ***Balayage des ports*** (à la page 61) pour plus d'informations.

Dispositifs en niveau - Page Port Access

Si vous utilisez une configuration multiniveau où un dispositif KX II de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, vous pouvez afficher les dispositifs en niveau sur la page Port Access (Accès aux ports) en cliquant sur l'icône Expand Arrow ▶ (flèche de développement) à gauche du nom du dispositif en niveau. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.

Châssis de lames - Page Port Access

Le châssis de lames s'affiche dans une liste hiérarchique extensible sur la page Port Access ; le châssis de lames est placé à la racine de la hiérarchie et chaque lame est libellée et affichée sous la racine. Utilisez l'icône Expand Arrow (flèche de développement) ▶ en regard du châssis racine pour afficher les lames individuelles.

Remarque : pour afficher le châssis de lames dans l'ordre hiérarchique, ses sous-types doivent être configurés.

Groupes de deux ports vidéo - Page Port Access

Les groupes de deux ports vidéo apparaissent sur la page Port Access comme types Dual Port. Les ports principal et secondaire faisant partie du groupe de ports apparaissent sur la page Port Access comme Dual Port(P) et Dual Port(S), respectivement. Par exemple, si le type du CIM est DCIM, DCIM Dual Port (P) est affiché.

Lorsque vous accédez à un groupe de deux ports vidéo depuis le client distant, vous vous connectez au port principal, qui ouvre une fenêtre de connexion KVM aux ports principal et secondaire du groupe.

Remarque : le port principal est défini à la création du groupe.

Remarque : Deux canaux KVM sont nécessaires pour la connexion à distance au groupe de deux ports vidéo en cliquant sur le port principal. Si ces deux canaux ne sont pas disponibles, le lien Connect n'apparaît pas.

Remarque : le menu Action ne s'affiche pas lorsque vous cliquez sur un port secondaire dans un groupe de deux ports vidéo.

Remarque : vous ne pouvez pas vous connecter simultanément aux ports principal et secondaire depuis le port local.

Port Action Menu (Menu d'action de ports)

Lorsque vous cliquez sur un nom de port dans la liste Port Access, le menu d'action des ports s'affiche. Choisissez l'option de menu souhaitée pour ce port afin de l'exécuter. Notez que seules les options actuellement disponibles, suivant l'état et la disponibilité du port, sont répertoriées dans le menu d'actions des ports :

- Connect (Connecter) - Crée une nouvelle connexion au serveur cible. Pour la console distante de KX II, une nouvelle page Virtual KVM Client apparaît. Pour la console locale de KX II, l'affichage passe de l'interface utilisateur locale au serveur cible. Sur le port local, l'interface de la console locale de KX II doit être visible pour pouvoir procéder à la commutation. La commutation par raccourci-clavier est également disponible à partir du port local.

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

- Switch From (Basculer depuis) : permet de basculer d'une connexion existante au port sélectionné (serveur cible KVM). Cette option de menu n'est disponible que pour les cibles KVM. Elle n'est visible que si un client KVM virtuel est ouvert.

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

- Disconnect : déconnecte ce port et ferme la page du client virtuel KVM correspondant à ce serveur cible. Cette option de menu est disponible uniquement lorsque l'état du port est actif et connecté, ou actif et occupé.

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

- Power On : met le serveur cible sous tension via la prise associée. Cette option est visible uniquement lorsqu'il existe une ou plusieurs associations d'alimentation à cette cible.
- Power Off : met le serveur cible hors tension via les prises associées. Cette option est visible uniquement lorsqu'il existe une ou plusieurs associations d'alimentation à cette cible, que la cible est sous tension (statut du port actif) et que l'utilisateur est autorisé à opérer ce service.
- Power Cycle : 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 à cette cible et que l'utilisateur est autorisé à opérer ce service.

Balayage des ports

KX II offre une fonction de balayage des ports qui recherche les cibles sélectionnées et les affiche dans une vue en diaporama, ce qui vous permet de contrôler jusqu'à 32 cibles simultanément. Vous pouvez vous connecter aux cibles ou sélectionner une cible spécifique le cas échéant. Les balayages peuvent inclure des cibles standard, des serveurs lames, des dispositifs Dominion en niveau et des ports de commutateurs KVM. Configurez les paramètres de balayage du client KVM virtuel (VKC) ou du client KVM actif (AKC). Reportez-vous à ***Configuration des paramètres de balayage dans VKC et AKC*** (à la page 101) pour plus d'informations.

Remarque : Dans les groupes de deux ports vidéo, le port principal est inclus dans un balayage de ports, mais non le port secondaire lors de la connexion depuis un client distant. Les deux ports peuvent être inclus dans le balayage depuis le port local. Les groupes de deux ports vidéo sont pris en charge par KX II 2.5.0 (et supérieur).

Remarque : le balayage des dispositifs en niveau n'est pas pris en charge par Multi-Platform Client (MPC).

Lorsque vous démarrez un balayage, la fenêtre Port Scan (Balayage des ports) s'ouvre. Au fur et à mesure de la détection d'une cible, celle-ci est affichée sous forme de miniature dans un diaporama. Le diaporama parcourt les miniatures des cibles selon l'intervalle par défaut de 10 secondes ou par l'intervalle que vous indiquez. Au fur et à mesure du balayage des cibles, celle qui est sélectionnée dans le diaporama s'affiche au centre de la page. Reportez-vous à ***Configuration des paramètres de balayage dans VKC et AKC*** (à la page 101).

Modifiez le délai de rotation des miniatures dans le diaporama, l'intervalle de sélection d'une miniature et les paramètres d'affichage de la page dans l'onglet Scan Settings (Paramètres de balayage) de la boîte de dialogue Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC) Tools > Options (Outils VKC, AKC et MPC > Options). Reportez-vous à ***Configuration des paramètres de balayage dans VKC et AKC*** (à la page 101).

Le nom de la cible s'affiche sous sa miniature et dans la barre de tâches au bas de la fenêtre. Si une cible est occupée, un écran vide apparaît au lieu de la page d'accès au serveur cible.

Le statut de chaque cible est indiqué par des voyants vert, jaune et rouge affichés sous la miniature de la cible, et lorsque la cible est sélectionnée dans la rotation, dans la barre de tâches. Les voyants indiquent les statuts suivants :

- Vert : la cible est activée/inactive ou activée/connectée.
- Jaune : la cible est désactivée mais connectée.
- Rouge : la cible est désactivée/inactive, occupée ou non accessible.

Cette fonction est disponible depuis le port local, Virtual KVM Client (VKC), Active KVM Client (AKC) et Multi-Platform Client (MPC).

Remarque : MPC utilise une méthode différente des autres clients Raritan pour déclencher un balayage. Reportez-vous à ***Set Scan Group*** *(Groupe de balayage d'ensemble) dans le* ***guide des clients KVM et série*** *pour plus d'informations. Les résultats et les options de balayage de la console distante et de la console locale sont différents. Reportez-vous à* **Balayage des ports - Console locale** *(à la page 317).*

Pour effectuer le balayage de cibles :

1. Cliquez sur l'onglet Set Scan (Balayage d'ensemble) dans la page Port Access (Accès aux ports).
2. Sélectionnez les cibles à inclure au balayage en cochant la case située à gauche de chacune, ou cochez la case au sommet de la colonne des cibles pour les sélectionner toutes.
3. Laissez la case Up Only (Activées seulement) cochée si vous ne souhaitez inclure au balayage que les cibles activées. Décochez-la pour inclure toutes les cibles, activées ou désactivées.
4. Cliquez sur Scan (Balayer) pour démarrer le balayage. Au fur et à mesure du balayage, chaque cible est affiché dans la vue en diaporama de la page.
5. Cliquez sur Options > Pause pour interrompre le diaporama et arrêter son mouvement entre les cibles. Cliquez sur Options > Resume (Reprendre) pour reprendre le diaporama.
6. Cliquez sur une miniature de cible pour procéder à son balayage.
7. Connectez-vous à une cible en double-cliquant sur sa miniature.

Utilisation des options de balayage

Les options suivantes sont disponibles pour le balayage des cibles. A l'exception de l'icône Expand/Collapse (Développer/Réduire), toutes ces options sont sélectionnées à partir du menu Options en haut à gauche de l'afficheur Port Scan (Balayage des ports). Les valeurs par défaut des options sont rétablies lorsque vous fermez la fenêtre.

Remarque : configurez les paramètres de balayage tels que l'intervalle d'affichage dans le client KVM virtuel (VKC) ou dans le client KVM actif (AKC). Reportez-vous à **Configuration des paramètres de balayage dans VKC et AKC** *(à la page 101) pour plus d'informations.*

Masquer ou afficher les miniatures

- Utilisez l'icône Expand/Collapse (Développer/Réduire)  en haut à gauche de la fenêtre pour masquer ou afficher les miniatures. Par défaut, la vue est développée.

Interrompre le diaporama des miniatures

- Pour interrompre la rotation des miniatures entre deux cibles, sélectionnez Options > Pause. La rotation des miniatures est le paramètre par défaut.

Reprendre le diaporama des miniatures

- Pour reprendre la rotation des miniatures, sélectionnez Options > Resume (Reprendre).

Dimensionner les miniatures dans l'afficheur Port Scan (Balayage des ports)

- Pour agrandir les miniatures, sélectionnez Options > Size (Taille) > 360x240.
- Pour réduire les miniatures, sélectionnez Options > Size (Taille) > 160x120. Il s'agit de la taille par défaut des miniatures.

Modifier l'orientation de l'afficheur Port Scan (Balayage des ports)

- Pour afficher les miniatures le long du bas de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Horizontal.
- Pour afficher les miniatures le long du côté droit de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Vertical. Il s'agit de la vue par défaut.

Gestion des favoris

Une fonction Favorites (Favoris) intégrée permet d'organiser les dispositifs que vous utilisez fréquemment et d'y accéder rapidement. La section Favorite Devices (Dispositifs favoris) se trouve dans la partie inférieure gauche (cadre) de la page Port Access et permet les opérations suivantes :

- créer et gérer une liste de dispositifs favoris ;
- accéder rapidement aux dispositifs fréquemment utilisés ;
- répertorier vos favoris par nom de dispositif, adresse IP ou nom d'hôte DNS ;
- détecter les dispositifs KX II sur le sous-réseau (avant et après la connexion) ;
- récupérer les dispositifs KX II détectés à partir du dispositif Dominion connecté (après la connexion).

Pour accéder à un dispositif KX II favori :

- Cliquez sur le nom du dispositif (liste figurant sous Favorite Devices). Un nouveau navigateur s'ouvre pour le dispositif en question.

Pour afficher les favoris en fonction de leur nom :

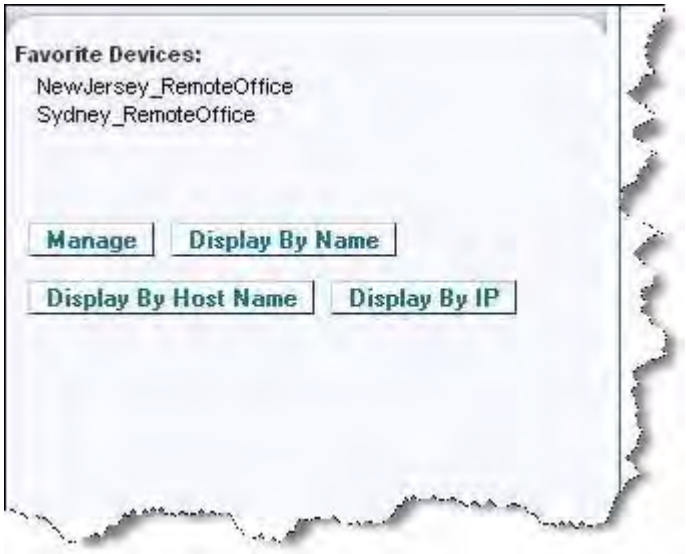
- Cliquez sur Display by Name (Afficher par nom).

Pour afficher les favoris en fonction de leur adresse IP :

- Cliquez sur Display by IP (Afficher par adresse IP).

Pour afficher les favoris en fonction du nom d'hôte :

- Cliquez sur Display by Host Name (Afficher par nom d'hôte).



Page Manage Favorites (Gérer les favoris)

Pour ouvrir la page Manage Favorites :

- Cliquez sur Manage (Gérer) dans le panneau de gauche. La page Manage Favorites (Gérer les favoris) qui s'ouvre contient les éléments suivants :

Utilisez :	Pour :
Liste des favoris (Favorites List)	Gérer la liste de vos dispositifs favoris.
Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local)	Détecter les dispositifs Raritan sur le sous-réseau local du PC client.
Discover Devices - KX II Subnet (Détecter les dispositifs - Sous-réseau de KX II)	Détecter les dispositifs Raritan sur le sous-réseau du dispositif KX II.
Add New Device to Favorites (Ajouter un nouveau dispositif aux favoris)	Ajouter, modifier et supprimer des dispositifs dans votre liste de favoris.

Page Favorites List (Liste des favoris)

A partir de la page Favorites List, vous pouvez ajouter, modifier et supprimer des dispositifs dans votre liste de favoris.

Pour ouvrir la page Favorites List :

- Sélectionnez Manage (Gérer) > Favorites List (Liste des favoris). La page Favorites List s'ouvre.

Détection des dispositifs sur le sous-réseau local

Cette option détecte les dispositifs sur votre sous-réseau local, c'est-à-dire le sous-réseau sur lequel la console distante de KX II est exécutée. Ces dispositifs sont accessibles directement à partir de cette page ou vous pouvez les ajouter à votre liste de favoris. Reportez-vous à ***Page Favorites List (Liste des favoris)*** (à la page 66).

Pour détecter des dispositifs sur le sous-réseau local :

1. Sélectionnez Manage (Gérer) > Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local). La page Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local) apparaît.
2. Choisissez le port de détection approprié :
   - Pour utiliser le port de détection par défaut, sélectionnez la case Use Default Port 5000 (Utiliser le port 5000 par défaut).
   - Pour utiliser un port de détection différent :
     a. Désélectionnez la case Use Default Port 5000 (Utiliser le port 5000 par défaut).
     b. Entrez le numéro de port dans le champ Discover on Port (Détecter sur 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).

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 sur le sous-réseau de KX II

Cette option détecte les dispositifs sur le sous-réseau du dispositif, c'est-à-dire le sous-réseau de l'adresse IP du dispositif KX II même. Vous pouvez accéder à ces dispositifs directement à partir de la page Subnet (Sous-réseau) ou les ajouter à votre liste de favoris. Reportez-vous à ***Page Favorites List (Liste des favoris)*** (à la page 66).

Cette fonction permet à plusieurs dispositifs KX II d'interagir et de se mettre en corrélation automatiquement. La console distante de KX II détecte automatiquement les dispositifs KX II, et n'importe quel autre dispositif Raritan, sur le sous-réseau de KX II.

Pour détecter des dispositifs sur le sous-réseau du dispositif :

1. Choisissez Manage (Gérer) > Discover Devices - KX II Subnet (Détecter les dispositifs - Sous-réseau de KX II). La page Discover Devices - KX II Subnet (Détecter les dispositifs - Sous-réseau de KX II) apparaît.
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).

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.

Ajout, suppression et modification des favoris

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 aux favoris). La page Add New Favorite (Ajouter un nouveau favori) apparaît.
2. Saisissez une description significative.
3. Entrez l'adresse IP ou le nom d'hôte du dispositif.
4. Modifiez le port de détection (le cas échéant).
5. Sélectionnez le type de produit.
6. Cliquez sur OK. Le dispositif est ajouté à votre liste de favoris.

Pour modifier un favori :

1. Dans la page Favorites List (Liste des favoris), cochez la case située en regard du dispositif KX II approprié.
2. Cliquez sur Modifier. La page Edit (Modifier) apparaît.
3. Mettez à jour les champs, le cas échéant :
   - Description
   - IP Address/Host Name (Adresse IP/Nom d'hôte) - Entrez l'adresse IP du dispositif KX II.
   - Port (si nécessaire)
   - Product Type (Type de produit).
4. Cliquez sur OK.

Pour supprimer un favori :

Important : soyez prudent lorsque vous supprimez des favoris. Vous êtes invité à en confirmer la suppression.

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

Se déconnecter

Pour quitter KX II :

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

Remarque : la déconnexion ferme également toutes les sessions ouvertes de Virtual KVM Client, ainsi que les sessions client série.

Configuration du serveur proxy à utiliser avec MPC, VKC et AKC

Lorsque l'utilisation d'un serveur proxy est requise, un proxy SOCKS doit également être fourni et configuré sur le PC client distant.

Remarque : si le serveur proxy installé n'accepte que le protocole proxy HTTP, vous ne pourrez pas vous connecter.

Pour configurer le proxy SOCKS :

1. Sur le client, sélectionnez Panneau de configuration > Options Internet.

a. Sur l'onglet Connexions, cliquez sur Paramètres réseau. La boîte de dialogue Paramètres du réseau local s'ouvre.

b. Cochez Utiliser un serveur proxy pour votre réseau local.

c. Cliquez sur Avancé. La boîte de dialogue Paramètres du proxy s'ouvre.

d. Configurez les serveurs proxy pour tous les protocoles. IMPORTANT : ne cochez pas la case Utiliser le même serveur proxy pour tous les protocoles.

Remarque : le port par défaut d'un proxy SOCKS (1080) est différent de celui du proxy HTTP (3128).

2. Cliquez sur OK dans chaque boîte de dialogue pour appliquer les paramètres.

3. Configurez ensuite les proxys des applets Java™ en sélectionnant Panneau de configuration > Java.

e. Sur l'onglet Général, cliquez sur Paramètres réseau. La boîte de dialogue Paramètres réseau s'ouvre.

f. Sélectionnez Utiliser un serveur proxy.

g. Cliquez sur Avancé. La boîte de dialogue Paramètres réseau avancés s'ouvre.

h. Configurez les serveurs proxy pour tous les protocoles. IMPORTANT : ne cochez pas la case Utiliser le même serveur proxy pour tous les protocoles.

Remarque : le port par défaut d'un proxy SOCKS (1080) est différent de celui du proxy HTTP (3128).

4. Si vous utilisez MPC autonome, vous devez également effectuer les opérations suivantes :

i. Ouvrez le fichier start.bat du répertoire MPC à l'aide d'un éditeur de texte.

j. Insérez les paramètres suivants à la ligne de commande. Ajoutez-les avant "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

Les paramètres doivent ressembler à ce qui suit :

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Virtual KVM Client (VKC) et Active KVM Client (AKC)

Virtual KVM Client (VKC) et Active KVM Client (AKC) sont des interfaces permettant d'accéder à des cibles distantes. AKC et VKC offrent des fonctions similaires à l'exception des suivantes :

- Configuration système minimale requise
- Systèmes d'exploitation et navigateurs pris en charge
- Les macros de clavier créées dans AKC ne peuvent pas être utilisées dans VKC.
- Configuration de l'accès direct aux ports (reportez-vous à **Activation d'un accès direct aux ports via URL**.)
- Configuration de la validation de certification du serveur AKC (reportez-vous à **Conditions requises pour l'utilisation d'AKC** (voir "**Prerequisites for Using AKC**" à la page 72).)

A propos d'Active KVM Client

AKC est basé sur la technologie Microsoft Windows .NET et permet d'exécuter le client dans des environnements Windows sans utiliser Java Runtime Environment (JRE), qui est obligatoire pour exécuter Virtual KVM Client (VKC) et Multi-Platform Client (MPC) de Raritan. AKC fonctionne également avec CC-SG.

Remarque : si vous utilisez l'accès direct aux ports avec AKC, vous devez ouvrir une nouvelle fenêtre de navigateur ou un autre onglet de navigateur pour chaque cible à laquelle vous souhaitez accéder. Si vous tentez d'accéder à une autre cible en entrant l'URL de DPA dans la même fenêtre de navigateur ou le même onglet à partir desquels vous accédez actuellement à une cible, vous ne pourrez pas vous connecter et risquez d'obtenir une erreur.

Systèmes d'exploitation, .NET Framework et navigateurs pris en charge par AKC

.NET Framework

AKC requiert la version 3.5 ou 4.0 de Windows .NET®. AKC fonctionne avec les deux versions, 3.5 et 4.0, installées.

Systèmes d'exploitation

Lorsqu'il est lancé depuis Internet Explorer®, AKC permet d'atteindre les serveurs cible via KX II 2.2 (ou supérieur) et LX 2.4.5 (et supérieur) AKC est compatible avec les plates-formes suivantes exécutant .NET Framework 3.5 :

- système d'exploitation Windows XP®
- système d'exploitation Windows Vista® (jusqu'à 64 bits)
- système d'exploitation Windows 7® (jusqu'à 64 bits)

Remarque : vous devez utiliser Windows 7 si WINDOWS PC FIPs est activé et que vous accédez à une cible à l'aide d'AKC et d'une carte à puce.

.NET est requis pour exécuter AKC. S'il n'est pas installé ou si la version installée n'est pas prise en charge, vous recevrez un message vous demandant de vérifier la version de .NET.

Remarque : Raritan recommande aux utilisateurs du système d'exploitation Windows XP® de vérifier qu'une version opérationnelle de .NET 3.5 ou 4.0 est déjà installée avant de lancer AKC. Sinon, vous serez invité à télécharger un fichier au lieu de recevoir le message par défaut indiquant de vérifier la version de .NET.

Navigateur

- Internet Explorer 6 ou supérieur

Si vous tentez d'ouvrir AKC à partir d'un navigateur autre qu'IE 6 ou supérieur, vous recevrez un message d'erreur vous demandant de vérifier votre navigateur et d'utiliser Internet Explorer.

Prerequisites for Using AKC

In order to use AKC:

- Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.
- Les utilisateurs de serveurs Windows Vista, Windows 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur et que le mode protégé n'est pas activé lors de l'accès au dispositif.

Enable AKC Download Server Certificate Validation

If the device (or CC-SG) administrator has enabled the Enable AKC Download Server Certificate Validation option:

- Les administrateurs doivent téléverser un certificat valide sur le dispositif ou générer un certificat auto-signé sur celui-ci. Le certificat doit désigner un hôte valide.
- Chaque utilisateur doit ajouter le certificat AC (ou une copie du certificat auto-signé) dans la liste Autorités de certification racines de confiance de leur navigateur.

When launching AKC from the CC-SG Admin Client, you must have JRE™ 1.6.0_10 or above.

Boutons de barre d'outils et icônes de barre d'état

Bouton	Nom du bouton	Description
	Propriétés de connexion	Ouvre la boîte de dialogue Modify Connection Properties (Modifier les propriétés de connexion) à partir de laquelle vous pouvez manuellement définir les options de bande passante (telles que la vitesse de connexion, le nombre de couleurs, etc.).
	Video Settings (Paramètres vidéo)	Ouvre la boîte de dialogue Video Settings (Paramètres vidéo) qui permet de définir manuellement les paramètres de conversion des signaux vidéo.
	Color Calibration (Calibrage des couleurs)	Ajuste les paramètres de couleur de manière à réduire le bruit de couleur superflu. Revient à choisir Video > Color Calibrate (Calibrage des couleurs). *Remarque : non disponible dans KX II-101-V2.*

Bouton	Nom du bouton	Description
	Target Screenshot (Capture d'écran de la cible)	Cliquez pour effectuer une capture d'écran du serveur cible et l'enregistrer dans un fichier de votre choix.
	Audio	Ouvre une boîte de dialogue qui permet d'effectuer une sélection dans une liste de dispositifs audio reliés à un PC client. Une fois les dispositifs audio connectés à la cible, sélectionnez cette option pour les déconnecter. *Remarque : cette fonction est disponible sur KX II 2.4.0 (et supérieur).* *Remarque : cette fonction n'est pas prise en charge par LX.*
	Synchronize Mouse (Synchroniser la souris)	En mode souris double, force le réalignement du pointeur de la souris du serveur cible sur le pointeur de la souris. Remarque : non disponible si le mode souris absolue est sélectionnée.
	Refresh Screen (Actualiser l'écran)	Force le rafraîchissement de l'écran vidéo.
	Auto-sense Video Settings (Détection automatique des paramètres vidéo)	Force le rafraîchissement des paramètres vidéo (résolution, taux de rafraîchissement).
	Smart Card (Carte à puce)	Ouvre une boîte de dialogue qui permet d'effectuer une sélection dans une liste de lecteurs de cartes à puce reliés à un PC client. *Remarque : Cette fonction est disponible uniquement sur KSX II 2.3.0 (et supérieur) et sur KX II 2.1.10 (et supérieur).* *Remarque : cette fonction n'est pas prise en charge par LX.*

Bouton	Nom du bouton	Description
	Send Ctrl+Alt+Del (Envoyer Ctrl+Alt+Supr)	Envoie la combinaison de touches de raccourci Ctrl+Alt+Suppr au serveur cible.
	Single Cursor Mode (Mode curseur simple)	Démarre le mode curseur simple par lequel le pointeur de souris locale n'apparaît plus à l'écran. Pour quitter ce mode, appuyez sur CTRL+ALT+O. *Remarque : non disponible dans KX II-101-V2.*
	Mode Full Screen (Mode Plein écran)	Agrandit la zone de l'écran afin d'afficher le Bureau du serveur cible.
	Scaling (Mise à l'échelle)	Augmente ou réduit la taille de la vidéo cible de manière à afficher la totalité du contenu de la fenêtre du serveur cible sans l'aide de la barre de défilement.

Icône	Nom de l'icône	Description
	Speaker (Haut-parleur)	Située dans la barre d'état au bas de la fenêtre du client. Des ondulations vertes clignotantes indiquent qu'une session de lecture audio est diffusée en continu. Une icône Haut-parleur noire s'affiche lorsque le son de la session est coupé. L'icône est estompée lorsqu'aucun dispositif audio n'est connecté. *Remarque : l'audio est pris en charge par KX II 2.4.0 (et supérieur).*
	Microphone	Située dans la barre d'état au bas de la fenêtre du client. Des ondulations rouges clignotantes indiquent qu'une session de capture audio est en cours. L'icône Haut-parleur, qui indique qu'une session de lecture est diffusée en continu, est également affichée. Une icône Microphone noire s'affiche lorsque le son de la session est coupé. L'icône est estompée lorsqu'aucun dispositif audio n'est connecté. *Remarque : la capture audio est prise en charge par KX II 2.5.0 (et supérieur).*

Connection Properties (Propriétés de la connexion)

Les algorithmes de compression vidéo dynamique maintiennent le caractère convivial des consoles KVM avec différents types de bande passante. Les dispositifs optimisent la sortie KVM pour l'utilisation dans un réseau local, mais également pour l'utilisation dans un réseau étendu. Ces dispositifs peuvent également contrôler le nombre de couleurs et limiter la sortie vidéo permettant ainsi un équilibre optimal entre qualité vidéo et réactivité du système pour n'importe quelle bande passante.

Les paramètres de la boîte de dialogue Properties (Propriétés) peuvent être optimisés pour répondre à vos critères spécifiques selon les différents environnements d'exploitation. Les propriétés de connexion sont enregistrées pour les connexions suivantes sur des dispositifs de deuxième génération une fois paramétrées et enregistrées.

Pour définir les propriétés de connexion :

1. Choisissez Connection (Connexion) > Properties (Propriétés) ou cliquez sur le bouton Connection Properties (Propriétés de connexion)  de la barre d'outils. La boîte de dialogue Properties (Propriétés) s'ouvre.

Remarque : KX II-101 ne prend pas en charge Ethernet 1G.

2. Sélectionnez une valeur dans la liste déroulante Connection Speed (Vitesse de connexion). Le dispositif peut détecter automatiquement la basse passante disponible et ne pas en restreindre l'utilisation. Cependant, vous pouvez également en régler l'utilisation en fonction des limitations de 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 (RNIS double)
- 56 Ko (Modem ISP)
- 33 Ko (Modem rapide)
- 24 Ko (Modem lent)

Notez 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 une valeur dans la liste déroulante Color Depth (Nombre de couleurs). Le dispositif peut adapter de manière dynamique le nombre de couleurs transmis aux utilisateurs distants afin d'optimiser la convivialité pour toutes les bandes passantes.
   - 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.), l'ensemble du spectre de couleurs 24 bits ou 32 bits disponible avec la plupart des cartes graphiques modernes n'est pas nécessaire. Les tentatives de transmission d'un nombre de couleurs aussi élevé entraîne une perte de bande passante du réseau.

4. Utilisez le curseur 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 conserver ces propriétés.

Informations sur la connexion

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

- Sélectionnez Connection (Connexion) > Info... La fenêtre d'informations sur la connexion s'affiche alors.

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

- Device Name : nom du dispositif.
- IP Address : adresse IP du dispositif.
- Port : port TCP/IP de communication KVM utilisé pour l'accès au dispositif cible.
- Data In/Second : débit des données en entrée.
- Data Out/Second : débit des données en sortie.
- Connect Time : durée du temps de connexion.
- FPS : nombre d'images par seconde transmises pour la vidéo.
- Horizontal Resolution : résolution d'écran horizontale.
- Vertical Resolution : résolution d'écran verticale.
- Refresh Rate : fréquence à laquelle l'écran est actualisé.
- Protocol Version : 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.

Options de clavier

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. Aussi, si vous utilisez un autre PC, vous ne voyez pas vos macros. Par ailleurs, si un autre utilisateur utilise votre PC et se connecte sous un nom différent, il 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. Toutefois, les macros de clavier créées dans Active KVM Client (AKC) ne peuvent pas être utilisées dans VKC ou MPC, et inversement.

Remarque : KX II-101 ne prend pas en charge AKC.

Importation/exportation de macros de clavier

Les macros exportées d'Active KVM Client (AKC) ne peuvent pas être importées dans Multi-Platform Client (MPC) ou Virtual KVM Client (VKC). Les macros exportées de MPC ou VKC ne peuvent pas être importées dans AKC.

Remarque : KX II-101 ne prend pas en charge AKC.

Pour importer des macros :

1. Choisissez Keyboard > Import Keyboard Macros (Clavier > Importer des macros de clavier) pour ouvrir la boîte de dialogue Import Macros (Importation de macros). Accédez à l'emplacement du dossier du fichier de macro.
2. Cliquez sur le fichier de macro et cliquez sur Ouvrir pour importer la macro.
   a. Si le fichier comporte trop de macros, un message d'erreur s'affiche et l'importation s'interrompt lorsque vous cliquez sur OK.
   b. Si l'importation échoue, une boîte de dialogue d'erreur apparaît contenant un message indiquant le motif de l'échec. Sélectionnez OK pour continuer l'importation en évitant les macros ne pouvant pas être traitées.
3. Sélectionnez les macros à importer en cochant la case correspondante ou en utilisant les options Select All (Tout sélectionner) ou Deselect All (Tout désélectionner).

4. Cliquez sur OK pour démarrer l'importation.
   a. Si une macro en double est détectée, la boîte de dialogue Import Macros (Importer des macros) apparaît. Effectuez une des opérations suivantes :
      - Cliquez sur Yes (Oui) pour remplacer la macro existante par la version importée.
      - Cliquez sur Yes to All (Oui pour tout) pour remplacer la macro sélectionnée et toutes les autres en double éventuellement détectées.
      - Cliquez sur No (Non) pour conserver la macro d'origine et passer à la suivante.
      - Cliquez sur No to All (Non pour tout) pour conserver la macro d'origine et passer à la suivante. Les autres doubles détectés sont également ignorés.
      - Cliquez sur Cancel (Annuler) pour arrêter l'importation.
      - Vous pouvez également cliquer sur Rename pour renommer la macro et l'importer. La boîte de dialogue Rename Macro (Renommage de la macro) apparaît. Entrez le nouveau nom de la macro dans le champ et cliquez sur OK. La boîte de dialogue se ferme et la procédure continue. Si le nom entré est le double d'une macro, une alerte apparaît et vous devez donner un autre nom à la macro.
   b. Si, au cours de l'importation, le nombre de macros importées autorisé est dépassé, une boîte de dialogue apparaît. Cliquez sur OK pour tenter de poursuivre l'importation des macros ou cliquez sur Cancel (Annuler) pour l'arrêter.

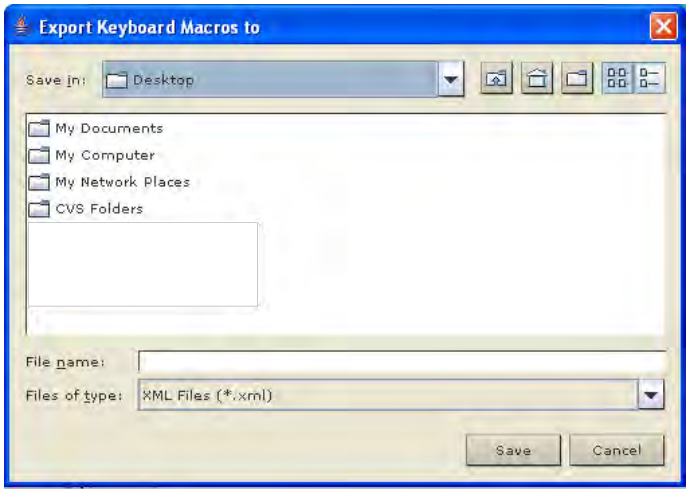
Les macros sont alors importées. Si une macro importée contient un raccourci-clavier existant, celui-ci est éliminé.

Pour exporter des macros :

1. Choisissez Tools > Export Macros (Outils > Exportation de macros) pour ouvrir la boîte de dialogue Select Keyboard Macros to Export (Sélectionnez les macros de clavier à exporter).

2. Sélectionnez les macros à exporter en cochant la case correspondante ou en utilisant les options Select All (Tout sélectionner) ou Deselect All (Tout désélectionner).
3. Cliquez sur OK. Une boîte de dialogue apparaît permettant de localiser et de sélectionner le fichier de macro. Par défaut, la macro existe sur votre bureau.

4. Sélectionnez le dossier d'enregistrement du fichier de macro, entrez le nom du fichier et cliquez sur Save (Enregistrer). Si la macro existe déjà, vous recevez un message d'alerte. Sélectionnez Yes (Oui) pour écraser la macro existante ou No (Non) pour fermer l'alerte sans écraser la macro.



Définition d'une macro de clavier

Pour définir une macro :

1. Sélectionnez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Cliquez sur Add (Ajouter). La boîte de dialogue Add Keyboard Macro (Ajouter une macro de clavier) s'affiche.
3. Saisissez un nom dans le champ Keyboard Macro Name (Nom de la macro de clavier). Ce nom apparaît dans le menu Keyboard (Clavier) après sa création.
4. Dans la liste déroulante du champ Hot-Key Combination (Raccourci-clavier), sélectionnez un raccourci-clavier. Ceci vous permet d'exécuter la macro avec une touche prédéfinie. **Facultatif**
5. Dans la liste déroulante Keys to Press (Touches à enfoncer), sélectionnez les touches que vous souhaitez utiliser pour émuler la séquence de touches utilisée pour effectuer la commande. Sélectionnez les touches dans l'ordre où elles doivent être enfoncées. Après chaque sélection, sélectionnez Add Key (Ajouter la touche). Chaque touche sélectionnée apparaît dans le champ Macro Sequence (Séquence de la macro) et une commande Release Key (Relâcher la touche) est automatiquement ajoutée après chaque sélection.

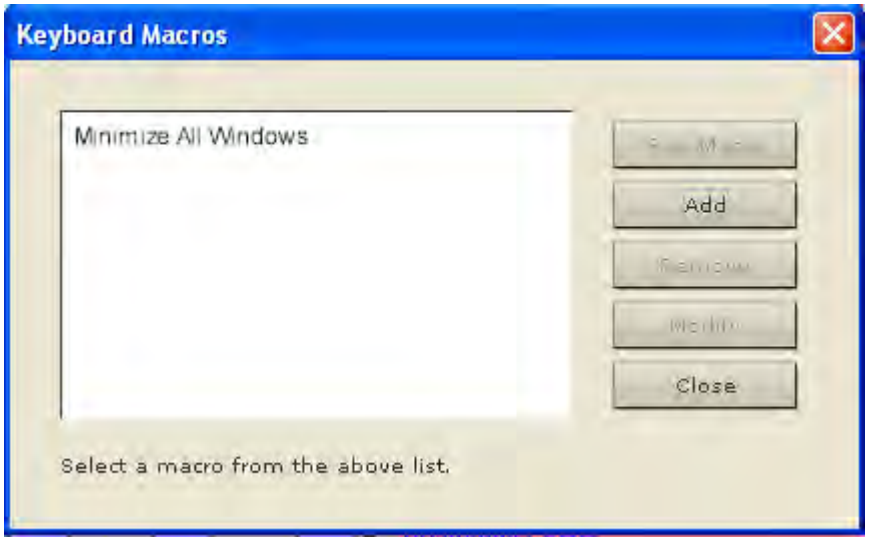
6. Pour utiliser la fonction Send Text to Target (Envoyer un texte à la cible) pour la macro, cliquez sur le bouton Construct Macro from Text (Créer la macro à partir du texte).
7. Par exemple, créez une macro pour fermer une fenêtre en sélectionnant Ctrl de gauche+Echap. Ceci apparaît dans la case Macro Sequence (Séquence de la macro) comme suit :

   Press Left Alt (Appuyer sur Alt gauche)

   Press F4 (Appuyer sur F4)

   Release F4 (Relâcher F4)

   Release Left Alt (Relâcher Alt gauche)
8. Relisez le champ Macro Sequence pour vous assurer que la séquence de la macro est définie correctement.
   a. Pour supprimer une étape de la séquence, sélectionnez-la et cliquez sur Remove (Supprimer).
   b. Pour changer l'ordre des étapes de la séquence, cliquez sur l'étape, puis sur les boutons fléchés haut et bas pour réorganiser les étapes comme vous le souhaitez.
9. Cliquez sur OK pour enregistrer la macro. Cliquez sur Clear (Effacer) pour effacer le contenu du champ et recommencer. Si vous cliquez sur OK, la fenêtre Keyboard Macros (Macros de clavier) s'affiche et présente la nouvelle macro de clavier.
10. Cliquez sur Close (Fermer) pour fermer la boîte de dialogue Keyboard Macros. La macro apparaît maintenant dans le menu Keyboard (Clavier) de l'application. Sélectionnez la nouvelle macro dans le menu pour l'exécuter ou utilisez les touches affectées à la macro.



Lancement d'une macro de clavier

Une fois que vous avez créé une macro de clavier, exécutez-la à l'aide de la macro de clavier que vous lui avez affectée ou en la choisissant dans le menu Keyboard (Clavier).

Exécution d'une macro à partir de la barre de menus

Lorsque vous créez une macro, elle s'affiche dans le menu Keyboard (Clavier). Exécutez la macro du clavier en cliquant sur son nom dans le menu Keyboard (Clavier).

Exécution d'une macro avec une combinaison de touches

Si vous avez attribué une combinaison de touches à une macro lors de sa création, vous pouvez exécuter la macro en appuyant sur les touches correspondantes. Par exemple, appuyez simultanément sur les touches Ctrl+Alt+0 pour réduire toutes les fenêtres sur un serveur cible Windows.

Modification et suppression des macros de clavier

Pour modifier une macro :

1. Choisissez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Choisissez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur Modify (Modifier). La fenêtre d'ajout/de modification de la macro apparaît.
4. Effectuez vos modifications.
5. Cliquez sur OK.

Pour supprimer une macro :

1. Choisissez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Choisissez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur Remove (Supprimer). La macro est supprimée.

Macro Ctrl+Alt+Suppr

En raison de son utilisation fréquente, une macro Ctrl+Alt+Suppr est préprogrammée. Lorsque vous cliquez sur le bouton Ctrl+Alt+Suppr 

de la barre d'outils, cette séquence de touches est envoyée au serveur ou au commutateur KVM auquel vous êtes actuellement connecté.

En revanche, si vous appuyiez physiquement sur les touches Ctrl+Alt+Suppr, la commande serait d'abord interceptée par votre propre ordinateur en raison de la structure du système d'exploitation Windows, au lieu d'être envoyée au serveur cible comme prévu.

Paramétrage des options clavier/souris CIM

Pour accéder au menu de configuration de DCIM-USBG2 :

1. Mettez en surbrillance à l'aide de la souris une fenêtre telle que Notepad (système d'exploitation Windows®) ou son équivalent.
2. Sélectionnez les options Set CIM Keyboard/Mouse options (Définir les options clavier/souris CIM). Ceci correspond à l'envoi de touche Ctrl gauche et Verr Num à la cible. Les options du menu de paramètres CIM sont alors affichées.
3. Définissez la langue et les paramètres de souris.
4. Quittez le menu pour retourner à la fonctionnalité CIM normale.

Propriétés vidéo

Actualisation de l'écran

La commande Refresh Screen (Actualiser l'écran) force le rafraîchissement de l'écran vidéo. Les paramètres vidéo peuvent être actualisés automatiquement de plusieurs manières :

- La commande Refresh Screen (Actualiser l'écran) force le rafraîchissement de l'écran vidéo.
- La commande Auto-sense Video Settings (Détection automatique des paramètres vidéo) permet de détecter automatiquement les paramètres vidéo du serveur cible.
- La commande Calibrate Color (Calibrer les couleurs) permet de procéder au calibrage de la vidéo afin d'optimiser les couleurs affichées.

Vous pouvez également régler les paramètres manuellement à l'aide de la commande Video Settings (Paramètres vidéo).

Pour actualiser les paramètres vidéo, effectuez l'une des opérations suivantes :

- Choisissez Video > Refresh Screen (Actualiser l'écran) ou cliquez sur le bouton Refresh Screen  de la barre d'outils.

Détection automatique des paramètres vidéo

La commande Auto-sense Video Settings force une nouvelle détection des paramètres vidéo (résolution, taux de rafraîchissement) et redessine l'écran vidéo.

Pour détecter automatiquement les paramètres vidéo :

- Choisissez Video > Auto-sense Video Settings (Détection automatique des paramètres vidéo) ou cliquez sur le bouton Auto-Sense Video Settings  de la barre d'outils. Un message s'affiche pour indiquer que le réglage automatique est en cours.

Calibrage de la couleur

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

Remarque : la commande Calibrate Color (Calibrer les couleurs) s'applique à la connexion en cours uniquement.

Remarque : KX II-101 ne prend pas en charge le calibrage des couleurs.

Pour calibrer la couleur :

- Choisissez Video > Calibrate Color (Calibrer les couleurs) ou cliquez sur le bouton Calibrate Color  de la barre d'outils. Le calibrage des couleurs de l'écran du dispositif cible est mis à jour.

Ajustement des paramètres vidéo

Utilisez la commande Video Settings (Paramètres vidéo) pour ajuster manuellement les paramètres vidéo.

Pour modifier les paramètres vidéo :

1. Choisissez Video > Video Settings ou cliquez sur le bouton Video Settings  de la barre d'outils pour ouvrir la boîte de dialogue du même nom.
2. Définissez les paramètres ci-après, le cas échéant. Les effets sont visibles dès que vous définissez les paramètres :
   a. Noise Filter (Filtre antiparasite)

      Le dispositif ProductName peut supprimer les interférences électriques de la sortie vidéo des cartes graphiques. Cette fonction optimise la qualité des images et réduit la bande passante. 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.
      Un seuil plus bas permet de transmettre le plus de changements de pixels. Si ce seuil est défini de manière trop faible, l'utilisation de la bande passante risque d'être plus importante.

   b. PLL Settings (Paramètres PPL)

Clock (Horloge) : contrôle la vitesse d'affichage des pixels vidéo sur l'écran vidéo. Les modifications apportées aux paramètres d'horloge entraînent l'étirement ou la réduction de l'image vidéo sur le plan horizontal. Nous vous recommandons d'utiliser 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-vous à la valeur de phase qui produit la meilleure image vidéo pour le serveur cible actif.

c. Brightness : utilisez cette option pour ajuster la luminosité de l'écran du serveur cible.

d. Brightness Red : contrôle la luminosité de l'écran du serveur cible pour le signal rouge.

e. Brightness Green : contrôle la luminosité du signal vert.

f. Brightness Blue : contrôle la luminosité du signal bleu.

g. Contrast Red : contrôle le contraste du signal rouge.

h. Contrast Green : contrôle le signal vert.

i. Contrast Blue : contrôle le signal bleu.

Si l'image vidéo semble très floue ou que sa mise au point ne semble pas correcte, les paramètres d'horloge et de phase peuvent être ajustés jusqu'à ce qu'une image de meilleure qualité s'affiche sur le serveur cible actif.

Avertissement : soyez prudent lorsque vous modifiez les paramètres Clock and Phase (Horloge et phase) ; en effet ces modifications peuvent entraîner des pertes ou des distorsions vidéo et vous risquez de ne plus pouvoir rétablir l'état précédent. Contactez l'assistance technique Raritan avant d'effectuer tout changement.

---

j. Horizontal Offset (Décalage horizontal) : contrôle le positionnement horizontal de l'affichage du serveur cible sur votre écran.

k. Vertical Offset (Décalage vertical) : contrôle le positionnement vertical de l'affichage du serveur cible sur votre écran.

3. Sélectionnez Automatic Color Calibration (Calibrage automatique des couleurs) pour activer cette fonction.

4. Sélectionnez le mode de détection vidéo :

   - Best possible video mode (Mode vidéo optimal) :

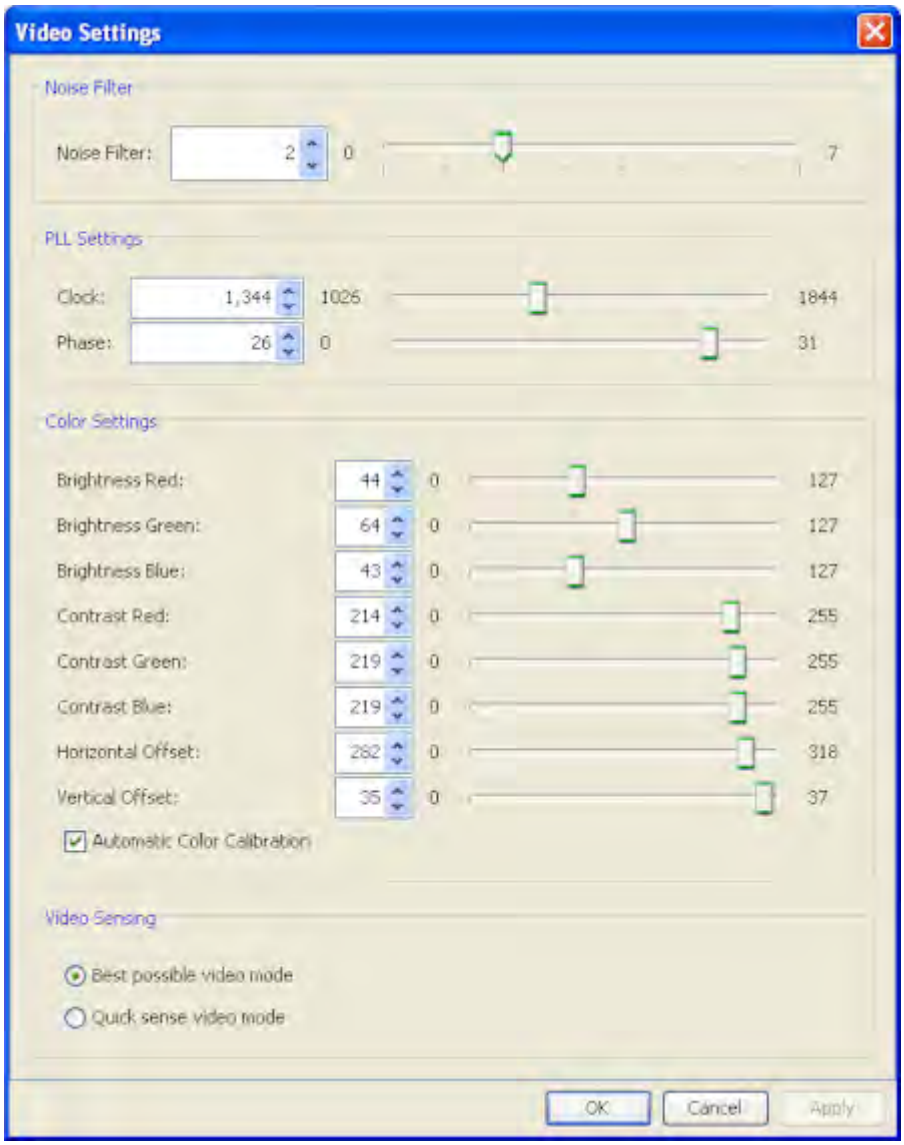
   le dispositif effectue la totalité du processus de détection automatique lorsque vous changez de cibles ou de résolutions cible. La sélection de cette option calibre la vidéo pour obtenir la qualité d'image optimale.

- Quick sense video mode (Détection rapide du mode vidéo) :

  avec cette option, le dispositif utilise la détection rapide automatique du mode vidéo pour 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.

5. Cliquez sur OK pour appliquer les paramètres et fermer la boîte de dialogue. Cliquez sur Apply pour appliquer les paramètres sans fermer la boîte de dialogue.

Remarque : certains écrans d'arrière-plan Sun, tels que les écrans à bord très sombres, risquent de ne pas se centrer 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.

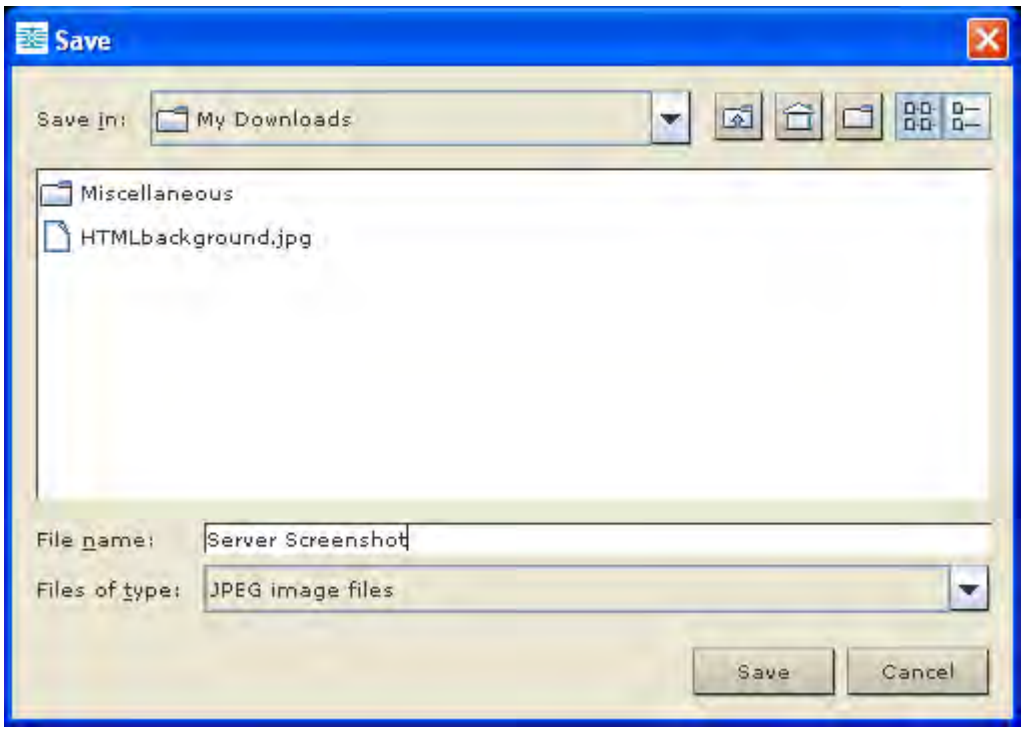


Utilisation de la commande Screenshot from Target

La commande serveur Screenshot from Target (Capture d'écran de la cible) vous permet d'effectuer une capture d'écran du serveur cible. Au besoin, enregistrez cette capture d'écran à un emplacement de votre choix dans un fichier bitmap, JPEG ou PNG.

Pour effectuer une capture d'écran du serveur cible :

1. Sélectionnez Video (Vidéo) > Screenshot from Target (Capture d'écran de la cible) ou cliquez sur le bouton  dans la barre d'outils.
2. Dans la boîte de dialogue Save (Enregistrer), choisissez l'emplacement de sauvegarde du fichier, nommez le fichier et sélectionnez un format dans la liste déroulante Type de fichiers.
3. Cliquez sur Save (Enregistrer) pour enregistrer la capture.



Modification du taux de rafraîchissement maximum

Si la carte vidéo dont vous disposez utilise un logiciel personnalisé et que vous accédez à la cible par l'intermédiaire de MPC ou de VKC, il vous faudra sans doute modifier le taux maximum de rafraîchissement de l'écran pour que celui-ci prenne effet sur la cible.

Pour régler le taux de rafraîchissement de l'écran :

1. Sous Windows®, sélectionnez Propriétés d'affichage < Paramètres < Avancé pour ouvrir la boîte de dialogue Plug-and-Play.
2. Cliquez sur l'onglet Moniteur.
3. Définissez la fréquence de rafraîchissement du moniteur.
4. Cliquez sur OK, puis à nouveau sur OK pour appliquer le paramètre.

Options de souris

Lors de la gestion d'un serveur cible, la console distante 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 de souris simple, soit en mode de souris double. En mode souris double, et à condition que l'option soit correctement configurée, les curseurs s'alignent.

En présence de deux curseurs de souris, le dispositif propose plusieurs modes de souris :

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

Synchronisation des pointeurs de souris

Lorsque vous affichez à distance un serveur cible utilisant une souris, deux curseurs de souris apparaissent : 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 est légèrement en avance sur celui de la souris de la cible en raison des paramètres d'accélération de souris.

Avec des connexions de réseau local rapides, vous pouvez 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 souris (simple et double).

Conseils de synchronisation de la souris

Veillez à suivre ces étapes lorsque vous configurez la synchronisation des souris :

1. Vérifiez que la résolution vidéo et le taux de rafraîchissement sélectionnés sont pris en charge par le dispositif. La boîte de dialogue Virtual KVM Client Connection Info (Informations sur la connexion de Virtual KVM Client) affiche les valeurs réellement observées par le dispositif.
2. Pour les dispositifs KX II et LX, assurez-vous que la longueur de câble se trouve dans les limites spécifiées pour la résolution vidéo sélectionnée.
3. Vérifiez que la souris et la vidéo ont été configurées correctement au cours de l'installation.
4. Forcez la détection automatique en cliquant sur le bouton de détection automatique de Virtual KVM Client.
5. Si cela n'améliore pas la synchronisation de la souris (pour des serveurs cible KVM Linux, UNIX et Solaris) :
   a. Ouvrez une fenêtre de terminal.
   b. Entrez la commande suivante : `xset mouse 1 1.`
   c. Fermez la fenêtre de terminal.
6. Cliquez sur le bouton de synchronisation de la souris de Virtual KVM Client  .

Remarques supplémentaires sur le mode souris intelligente

- Aucune icône ou application ne doit se trouver dans la partie supérieure gauche de l'écran dans la mesure où la routine de synchronisation a lieu à cet emplacement.
- N'utilisez pas de souris animée.
- Désactivez le bureau actif sur les serveurs cible KVM.

Synchronize Mouse (Synchroniser la souris)

En mode souris double, la commande Synchronize Mouse (Synchroniser la souris) force un nouvel alignement du pointeur de la souris du serveur cible avec le pointeur de la souris de Virtual KVM Client.

Pour synchroniser la souris, effectuez l'une des opérations suivantes :

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

Remarque : Cette option est disponible uniquement pour les modes de souris standard et intelligente.

Mode souris standard

Le mode souris standard utilise un algorithme de synchronisation de souris standard reprenant les positions de souris relatives. Le mode souris standard requiert la désactivation de l'accélération de la souris et que les autres paramètres de souris soient configurés correctement afin que la souris du client et celle du serveur restent synchronisées.

Pour entrer en mode souris standard :

- Choisissez Mouse (Souris) > Standard.

Mode souris intelligente

En mode souris intelligente, le dispositif peut détecter les paramètres de la souris cible et synchroniser les curseurs de souris en conséquence, permettant une accélération de la souris au niveau de la cible. Le mode de souris intelligente est le mode par défaut des cibles non-VM.

Au cours de la synchronisation, le curseur de souris effectue une « danse » dans le coin supérieur gauche de l'écran et calcule l'accélération. Pour que ce mode fonctionne correctement, certaines conditions doivent être remplies.

Pour entrer en mode souris intelligente :

- Sélectionnez Mouse (Souris) > Intelligent (Intelligente).

Conditions de synchronisation d'une souris intelligente

La commande Intelligent Mouse Synchronization (Synchronisation de souris intelligente), disponible dans le menu Mouse (Souris) synchronise automatiquement les curseurs de souris lors des moments d'inactivité. Cependant, pour que cette option fonctionne correctement, les conditions suivantes doivent être remplies :

- Le bureau actif doit être désactivé sur le serveur cible.
- Aucune fenêtre ne doit apparaître dans le coin supérieur gauche de la page cible.
- Le coin supérieur gauche de la page cible ne doit pas comporter d'arrière-plan animé.
- La forme du pointeur de la souris cible doit être normale et non animée.
- La vitesse de déplacement du pointeur de souris du serveur cible ne doit pas être réglée sur une valeur très basse ou très élevée.
- Les propriétés de souris avancées, telles que Enhanced pointer precision (Améliorer la précision du pointeur) ou Snap mouse to default button in dialogs (Déplacer automatiquement le pointeur sur le bouton par défaut dans les boîtes de dialogue) doivent être désactivées.
- Les utilisateurs doivent sélectionner l'option Best Possible Video Mode (Mode vidéo optimal) dans la fenêtre Video Settings (Paramètres vidéo).
- Les bords de l'affichage vidéo du serveur cible doivent être clairement visibles (une bordure noire doit être visible entre le bureau de la cible et la fenêtre de la console KVM distante lorsque vous affichez un bord de l'image vidéo de la cible).

- La fonction de synchronisation de la souris intelligente risque de ne pas fonctionner correctement si vous avez une icône de fichier ou de dossier dans le coin supérieur gauche du bureau. Pour éviter tout problème avec cette fonction, Raritan vous recommande de ne pas avoir d'icônes de fichier ou de dossier dans le coin supérieur gauche de votre bureau.

Après avoir exécuté la fonction de détection automatique des paramètres vidéo, exécutez manuellement la synchronisation de la souris en cliquant sur le bouton Synchronize Mouse (Synchroniser la souris) dans la barre d'outils. Cette recommandation est également valable si la résolution du serveur cible est modifiée, entraînant une désynchronisation des pointeurs de souris.

Si la synchronisation de souris intelligente échoue, la souris reprend son comportement standard.

Notez que les configurations de souris varient selon le système d'exploitation cible. Reportez-vous aux instructions de votre système d'exploitation pour de plus amples informations. Notez également que la synchronisation intelligente de la souris ne fonctionne pas avec les cibles UNIX.

Mode souris absolue

Dans ce mode, des coordonnées absolues sont utilisées pour maintenir la synchronisation des curseurs client et cible, même si l'accélération ou la vitesse de la souris cible est configurée sur une valeur différente. Ce mode est pris en charge sur les serveurs avec ports USB et il s'agit du mode par défaut pour les cibles VM et VM doubles.

Pour entrer en mode souris absolue :

- Sélectionnez Mouse (Souris) > Absolute (Absolue).

Remarque : pour KX II, la synchronisation absolue de la souris est disponible uniquement pour les CIM USB pour lesquels le support virtuel est activé (D2CIM-VUSB et D2CIM-DVUSB) et les CIM numériques.

Mode de souris unique

Le mode souris simple utilise uniquement le curseur de la souris du serveur cible ; le pointeur de souris locale n'apparaît plus à l'écran. Si vous êtes en mode souris simple, la commande Synchronize Mouse n'est pas disponible (il n'est pas nécessaire de synchroniser un curseur de souris simple).

Remarque : le mode souris simple ne fonctionne pas sur les cibles Windows ou Linux lorsque le client est exécuté sur une machine virtuelle.

Pour passer en mode souris simple, procédez comme suit :

1. Sélectionnez Mouse (Souris) > Single Mouse Cursor (Curseur de souris simple).
2. Cliquez sur le bouton Single/Double Mouse Cursor (Curseur de souris simple/double) dans la barre d'outils.

Pour quitter le mode souris simple :

- Appuyez sur Ctrl+Alt+O sur le clavier pour quitter le mode souris simple.

Options d'outils

Paramètres généraux

Pour définir les options d'outils :

1. Cliquez sur Tools (Outils) > Options. La boîte de dialogue Options s'affiche.

2. Cochez la case Enable Logging (Activer la journalisation) uniquement si l'assistance technique vous y invite. 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). Les options incluent :
   - US/International (Anglais Etats-Unis/international)
   - Français (France)
   - Allemand (Allemagne)
   - Japonais
   - Royaume-Uni
   - Coréen (Corée)
   - Français (Belgique)
   - Norvégien (Norvège)
   - Portugais (Portugal)
   - Danois (Danemark)
   - Suédois (Suède)
   - Allemand (Suisse)
   - Hongrois (Hongrie)
   - Espagnol (Espagne)
   - Italien (Italie)
   - Slovène
   - Traduction : Français - US
   - Traduction : Français - US International

   dans AKC, le type de clavier provient par défaut du client local, cette option ne s'applique donc pas. En outre, KX II-101 et KX II-101-V2 ne prenant pas en charge le mode de curseur simple, la fonction Exit Single Cursor Mode (Quitter le mode de curseur simple) ne s'applique pas pour ces dispositifs.
4. Configurez les raccourcis-clavier :
   - Exit Full Screen Mode - Hotkey (Quitter le mode Plein écran - Raccourci-clavier). Lorsque vous entrez en mode Plein écran, 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.
   - Exit Single Cursor Mode - Hotkey (Quitter le mode de curseur simple - Raccourci-clavier). Lorsque vous entrez en mode de curseur simple, seul le curseur de souris du serveur cible est visible. Il s'agit du raccourci-clavier utilisé pour quitter le mode de curseur simple et rétablir le curseur de souris du client.

- Disconnect from Target - Hotkey (Se déconnecter de la cible - Raccourci-clavier). Activez ce raccourci-clavier pour permettre aux utilisateurs de se déconnecter rapidement de la cible.

Pour les raccourcis-clavier, l'application n'autorise pas l'affectation de la même combinaison à plusieurs fonctions. Par exemple, si la touche Q est déjà appliquée à la fonction Disconnect from Target (Se déconnecter de la cible), elle ne sera pas disponible pour la fonction Exit Full Screen Mode (Quitter le mode Plein écran). En outre, si un raccourci-clavier est ajouté à l'application en raison d'une mise à niveau et que la valeur par défaut pour la touche est déjà utilisée, la valeur disponible suivante est appliquée à la fonction à la place.

5. Cliquez sur OK.

Restrictions concernant les claviers

Claviers turcs

Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

Claviers slovènes

La touche < ne fonctionne pas sur les claviers slovènes à cause d'une restriction JRE.

Configuration des langues étrangères sous Linux

Comme Sun JRE sous Linux a des difficultés à générer les événements clés corrects pour les claviers étrangers configurés à l'aide des préférences du système, Raritan recommande de configurer ces claviers étrangers à l'aide des méthodes utilisées dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Français	Indicateur de clavier
Allemand	Paramètres système (centre de contrôle)
Japonais	Paramètres système (centre de contrôle)
Anglais britannique	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Belge	Indicateur de clavier
Norvégien	Indicateur de clavier
Danois	Indicateur de clavier
Suédois	Indicateur de clavier

Langue/clavier	Méthode de configuration
Hongrois	Paramètres système (centre de contrôle)
Espagnol	Paramètres système (centre de contrôle)
Italien	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Portugais	Paramètres système (centre de contrôle)

Remarque : l'indicateur de clavier doit être utilisé sur les systèmes Linux utilisant l'environnement de bureau Gnome.

Paramètres de lancement client

Les utilisateurs de KX II peuvent configurer des paramètres de lancement client permettant de définir les paramètres d'écran d'une session KVM.

Pour configurer les paramètres de lancement client :

1. Cliquez sur Tools (Outils) > Options. La boîte de dialogue Options s'affiche.
2. Cliquez sur l'onglet Client Launch Settings (Paramètres de lancement client).
   - Pour configurer les paramètres de la fenêtre cible :
   a. Sélectionnez Standard - sized to target Resolution (Standard - dimension de la résolution cible) pour ouvrir la fenêtre en utilisant la résolution actuelle de la cible. Si la résolution cible est supérieure à celle du client, la fenêtre cible couvre autant de surface à l'écran que possible et des barres de défilement sont ajoutées (le cas échéant).
   b. Sélectionnez Full Screen (Plein écran) pour ouvrir la fenêtre cible en mode Plein écran.
   - Pour configurer le moniteur de lancement de l'afficheur cible :
   a. Sélectionnez Monitor Client Was Launched from (Moniteur de lancement du client) si vous souhaitez lancer l'afficheur cible à l'aide du même affichage que l'application utilisée sur le client (un navigateur ou une applet Web, par exemple).
   b. Utilisez Select From Detected Monitors (Sélectionner parmi les moniteurs détectés) pour effectuer une sélection dans la liste des moniteurs détectés par l'application. Si un moniteur sélectionné précédemment n'est plus détecté, la mention Currently Selected Monitor Not Detected (Moniteur sélectionné non détecté) apparaît.

- Pour configurer des paramètres de lancement supplémentaires :

a. Sélectionnez Enable Single Cursor Mode (Activer le mode de curseur simple) pour activer par défaut le mode de curseur simple lors de l'accès au serveur.

b. Sélectionnez Enable Scale Video (Mise à l'échelle de la vidéo) pour mettre à l'échelle automatiquement l'affichage sur le serveur cible lors de l'accès à celui-ci.

c. Sélectionnez Pin Menu Toolbar (Epingler la barre d'outils de menu) si vous souhaitez que la barre d'outils reste visible sur la cible en mode Plein écran. Par défaut, lorsque la cible est en mode Plein écran, le menu n'est visible que lorsque vous faites passer la souris le long du haut de l'écran.

3. Cliquez sur OK.

Configuration des paramètres de balayage dans VKC et AKC

KX II offre une fonction de balayage des ports qui recherche les cibles sélectionnées et les affiche dans une vue en diaporama, ce qui vous permet de contrôler jusqu'à 32 cibles simultanément. Vous pouvez vous connecter aux cibles ou sélectionner une cible spécifique le cas échéant. Les balayages peuvent inclure des cibles standard, des serveurs lames, des dispositifs Dominion en niveau et des ports de commutateurs KVM. Configurez les paramètres de balayage du client KVM virtuel (VKC) ou du client KVM actif (AKC). Reportez-vous à ***Configuration des paramètres de balayage dans VKC et AKC*** (à la page 101) pour plus d'informations. Reportez-vous à ***Balayage des ports*** (à la page 61). L'onglet Scan Settings (Paramètres de balayage) permet de personnaliser l'intervalle de balayage et les options d'affichage par défaut.

Pour définir les paramètres de balayage :

1. Cliquez sur Tools (Outils) > Options. La boîte de dialogue Options s'affiche.
2. Sélectionnez l'onglet Scan Settings (Paramètres de balayage).
3. Dans le champ Display Interval (10-255 sec) (Intervalle d'affichage (10 à 255 s), indiquez le nombre de secondes pendant lesquelles la cible sélectionnée doit rester affichée au centre de la fenêtre Port Scan (Balayage des ports).
4. Dans le champ Interval Between Ports (10 - 255 sec) (Intervalle entre les ports (10 à 255 s), indiquez l'intervalle de pause que doit respecter le dispositif entre les ports.
5. Dans la section Display (Affichage), modifiez les options d'affichage par défaut pour la taille des miniatures et l'orientation de la division de la fenêtre Port Scan (Balayage des ports).
6. Cliquez sur OK.

Options d'affichage

View Toolbar (Afficher la barre d'outils)

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

Pour afficher et masquer la barre d'outils :

- Choisissez View > View Toolbar (Affichage > Afficher la barre d'outils).

View Status Bar (Afficher la barre d'état)

Par défaut, la barre d'état s'affiche au bas de la fenêtre cible.

Pour masquer la barre d'état :

- Cliquez sur View > Status Bar (Afficher > Barre d'état) pour la désélectionner.

Pour restaurer la barre d'état :

- Cliquez sur View > Status Bar (Afficher > Barre d'état) pour la sélectionner.

Scaling (Mise à l'échelle)

La mise à l'échelle de votre fenêtre 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 tienne dans la fenêtre du 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 :

- Choisissez View > Scaling (Affichage > Mise à l'échelle).

Mode Full Screen (Mode Plein écran)

Lorsque vous passez au mode Plein écran, le plein écran de la cible s'affiche et utilise la même résolution que le serveur cible. Le raccourci-clavier utilisé pour quitter ce mode est spécifié dans la boîte de dialogue Options ; reportez-vous à ***Options d'outils*** (à la page 97).

En mode Plein écran, placez la souris au sommet de l'écran pour afficher la barre de menus du mode Plein écran. Pour que la barre de menus reste visible en mode Plein écran, activez l'option Pin Menu Toolbar (Epingler la barre d'outils de menu) de la boîte de dialogue Tool Options (Options d'outils). Reportez-vous à ***Options d'outils*** (à la page 97).

Pour entrer en mode Plein écran :

- Choisissez View > Full Screen (Affichage > Plein écran).

Pour quitter le mode Plein écran :

- Appuyez sur le raccourci clavier configuré dans la boîte de dialogue Options du menu Tools (Outils). Il s'agit par défaut de Ctrl+Alt+M.

Si vous souhaitez systématiquement accéder à la cible en mode Plein écran, désignez ce dernier comme mode par défaut.

Pour définir le mode Plein écran comme mode par défaut :

1. Cliquez sur Tools > Options (Outils > Options) pour ouvrir la boîte de dialogue Options.
2. Sélectionnez Enable Launch in Full Screen Mode (Activer le lancement en mode Plein écran) et cliquez sur OK.

Audionumérique

KX II prend en charge les connexions audionumériques bidirectionnelles de bout en bout pour les dispositifs audionumériques de lecture et de capture entre un client distant et un serveur cible. Les dispositifs audio sont accessibles via une connexion USB. D2CIM-DVUSB et le firmware à jour du dispositif sont requis.

La fonction audionumérique prend en charge :

- ***Enregistrement des paramètres audio*** (à la page 105)
- ***Connexion à plusieurs cibles depuis un client distant unique*** (à la page 106)
- ***Connexion à un serveur cible unique depuis plusieurs clients distants*** (à la page 107)
- ***Connexion et déconnexion d'un dispositif audionumérique*** (à la page 108)
- ***Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio)*** (à la page 111)

Les systèmes d'exploitation Windows®, Linux® et Mac® sont pris en charge. Les clients Virtual KVM Client (VKC), Active KVM Client (AKC) et Multi-Platform Client (MPC) prennent en charge les connexions aux dispositifs audio.

Remarque : les CD audio ne sont pas pris en charge par les supports virtuels et ne fonctionnent donc pas avec la fonction audio.

Avant d'utiliser la fonction audio, Raritan vous recommande de consulter les informations à ce sujet dans les sections suivantes de l'aide :

- ***Formats de dispositifs audio pris en charge*** (à la page 357)
- ***Recommandations en matière de ports vidéo doubles*** (à la page 373)
- ***Modes souris pris en charge*** (à la page 373)
- ***CIM requis pour la prise en charge de vidéo double*** (à la page 374)
- ***Remarques d'informations*** **(à la page 389),** ***Audio*** (à la page 399)

Enregistrement des paramètres audio

Les paramètres de dispositifs audio sont appliqués par dispositif KX II. Une fois ces paramètres configurés et enregistrés sur KX II, ils lui sont appliqués.

Par exemple, vous pouvez configurer un dispositif audio Windows® afin d'utiliser un format stéréo 16 bits, 44,1 K. Lorsque vous vous connectez à des cibles différentes et utilisez ce dispositif audio Windows, le format stéréo 16 bits, 44,1 K est appliqué à chaque serveur cible.

Pour les dispositifs de lecture et d'enregistrement, le type et le format de dispositif, et les paramètres de mémoire-tampon appliqués au dispositif sont enregistrés.

Reportez-vous à ***Connexion et déconnexion d'un dispositif audionumérique*** (à la page 108) pour obtenir des informations sur la connexion à et la configuration d'un dispositif audio, et à ***Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio)*** (à la page 111) pour en savoir plus sur les paramètres de la mémoire-tampon des dispositifs audio.

Si vous utilisez la fonction audio lors de l'exécution des modes PC Share et VM Share afin de permettre à plusieurs utilisateurs d'accéder simultanément au même dispositif audio d'une cible, les paramètres de dispositif audio de l'utilisateur qui a démarré la session sont appliqués à tous les utilisateurs qui ont rejoint celle-ci.

Ainsi, lorsqu'un utilisateur rejoint une session audio, les paramètres de la machine cible sont utilisés. Reportez-vous à ***Connexion à un serveur cible unique depuis plusieurs clients distants*** (à la page 107).

Connexion à plusieurs cibles depuis un client distant unique

KX II 2.5.0 (et supérieur) permet d'écouter du son sur quatre (4) serveurs cible simultanément depuis un client unique distant. Reportez-vous à ***Connexion et déconnexion d'un dispositif audionumérique*** (à la page 108) pour obtenir des informations sur la connexion à des dispositifs audio.

Remarque : lorsqu'une session audio est en cours, gardez-la active ou changez le délai de temporisation pour inactivité de KX II afin que la session audio continue.

Le tableau ci-après indique les clients Raritan prenant en charge la fonction de lecture et capture audio pour un système d'exploitation donné :

Système d'exploitation	Lecture et capture audio prises en charge par :
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC) • Multi-Platform Client (MPC)
Linux®	• Virtual KVM Client (VKC) • Multi-Platform Client (MPC)
Mac®	• Virtual KVM Client (VKC) • Multi-Platform Client (MPC)

Une icône de haut-parleur  s'affiche dans la barre d'état au bas de la fenêtre du client. Elle est estompée lorsque le son n'est pas utilisé.

Lorsque cette icône et l'icône de micro  sont affichées dans la barre d'état, la session est capturée pendant sa diffusion en continu.

Connexion à un serveur cible unique depuis plusieurs clients distants

KX II 2.5.0 (et supérieur) permet à huit (8) utilisateurs au plus sur des clients distants différents de se connecter simultanément au même serveur cible pour écouter la session audio.

Pour utiliser cette fonction, les modes PC Share et VM Share doivent être activés pour la cible. Reportez-vous à ***Encryption & Share (Chiffrement et partage)*** (à la page 268) pour en savoir plus sur l'activation des modes PC Share et VM Share.

Remarque : si vous utilisez la fonction audio lors de l'exécution des modes PC Share et VM Share, reportez-vous à **Recommandations et exigences en matière de lecture et de capture audio** *(à la page 357).*

Lorsque des utilisateurs rejoignent une session audio sur la même cible, les paramètres du dispositif audio de la personne qui a démarré la session sont utilisés. Par exemple, si l'utilisateur qui a configuré à l'origine le dispositif audio lui applique un format stéréo 16 bits, 44,1 K, ce format sera utilisé chaque fois que des utilisateurs accèdent au dispositif audio du serveur cible pendant une session partagée.

Ces paramètres sont configurés pour la cible lors de l'ajout initial du dispositif audio et ne peuvent pas être modifiés par les utilisateurs. Ces derniers peuvent toutefois régler les paramètres de mémoire-tampon de capture et de lecture afin de les adapter à leur propre configuration réseau. Ils peuvent, par exemple, augmenter la taille de la mémoire-tampon pour améliorer la qualité du son. Reportez-vous à ***Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio)*** (à la page 111).

Chaque participant à la session se connecte à la cible via VKC, AKC ou MPC de la même manière qu'aux dispositifs audio. Reportez-vous à ***Connexion et déconnexion d'un dispositif audionumérique*** (à la page 108).

Une icône de haut-parleur  s'affiche dans la barre d'état au bas de la fenêtre du client. Elle est estompée lorsque le son n'est pas utilisé.

Lorsque cette icône et l'icône de micro  sont affichées dans la barre d'état, la session est capturée pendant sa diffusion en continu.

Remarque : lorsqu'une session audio est en cours, gardez-la active ou changez le délai de temporisation pour inactivité de KX II afin que la session audio continue.

Connexion et déconnexion d'un dispositif audionumérique

Les paramètres de dispositifs audio sont appliqués par dispositif KX II. Une fois ces paramètres configurés et enregistrés sur KX II, ils lui sont appliqués. Reportez-vous à ***Enregistrement des paramètres audio*** (à la page 105) pour plus d'informations.

Remarque : si vous utilisez la fonction audio lors de l'exécution des modes PC Share et VM Share, reportez-vous à **Recommandations et exigences en matière de lecture et de capture audio** *(à la page 357). Reportez-vous également à* **Connexion à un serveur cible unique depuis plusieurs clients distants** *(à la page 107).*

Remarque : si vous vous connectez simultanément à plusieurs dispositifs audio de serveur cible depuis un client distant unique, vérifiez les clients Raritan prenant en charge la fonction de lecture et capture audio pour un système d'exploitation donné. Reportez-vous à **Connexion à plusieurs cibles depuis un client distant unique** *(à la page 106).*

Remarque : lorsqu'une session audio est en cours, gardez-la active ou changez le délai de temporisation pour inactivité de KX II afin que la session audio continue.

Pour vous connecter à un dispositif audio :

1. Connectez le dispositif audio au PC client distant avant de lancer la connexion par navigateur à KX II.
2. Connectez-vous à la cible à partir de la page Port Access (Accès aux ports).
3. Une fois connecté, cliquez sur l'icône Audio  dans la barre d'outils. La boîte de dialogue Connect Audio Device (Connexion au dispositif audio) apparaît. Une liste des dispositifs audio disponibles connectés au PC client distant s'affiche.

   Remarque : si aucun dispositif audio disponible n'est connecté au PC client distant, l'icône Audio est estompée. .

4. Cochez Connect Playback Device (Connexion à un dispositif de lecture) si vous vous connectez à un dispositif de lecture.
5. Dans la liste déroulante, sélectionnez le dispositif à connecter.
6. Sélectionnez le format audio du dispositif de lecture dans la la liste déroulante Format:.

   Remarque : sélectionnez le format que vous souhaitez utiliser en fonction de la bande passante réseau disponible. Les formats à taux d'échantillonnage plus bas consomment moins de bande passante et peuvent tolérer une congestion du réseau plus importante.

7. Cochez Connect Recording Device (Connexion à un dispositif d'enregistrement) si vous vous connectez à un dispositif d'enregistrement.

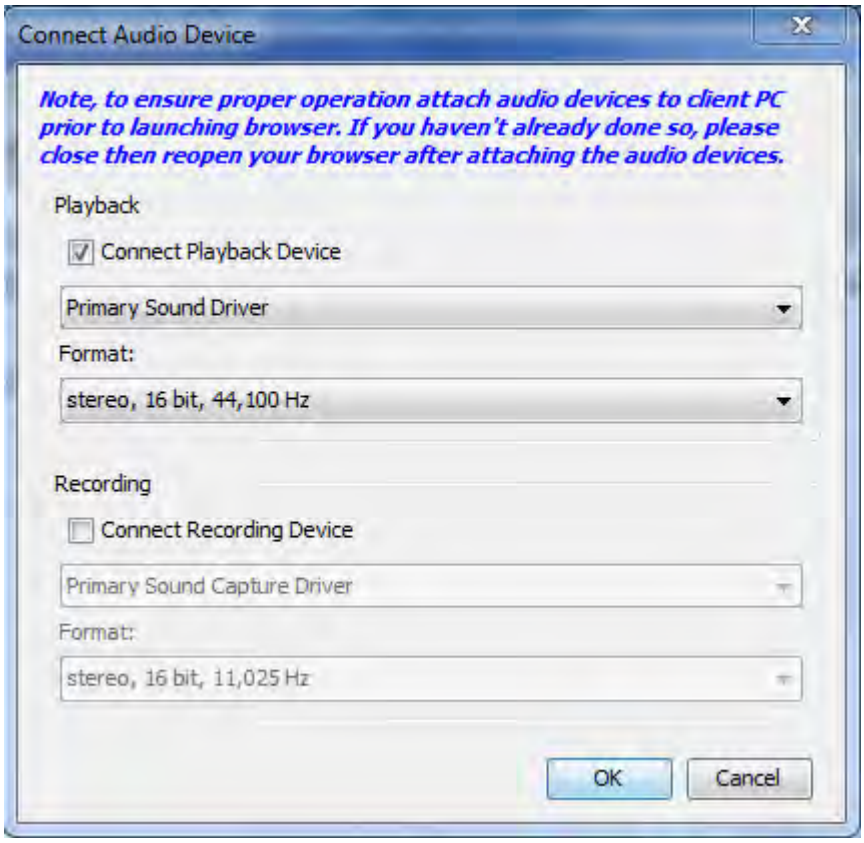
   Remarque : Le nom des dispositifs recensés dans la liste déroulante Connect Recording Device (Connexion d'un dispositif d'enregistrement) est tronqué à 30 caractères au plus pour les clients Java.

8. Dans la liste déroulante, sélectionnez le dispositif à connecter.
9. Sélectionnez le format audio du dispositif d'enregistrement dans la la liste déroulante Format:.
10. Cliquez sur OK. Si la connexion audio est établie, un message de confirmation apparaît. Cliquez sur OK.

    Si la connexion n'est pas établie, un message d'erreur apparaît.

    Une fois la connexion audio établie, le menu Audio devient Disconnect Audio (Déconnexion audio). De plus, les paramètres du dispositif audio sont enregistrés et lui sont appliqués.

Une icône de haut-parleur s'affiche dans la barre d'état au bas de la fenêtre du client. Elle est estompée lorsque le son n'est pas utilisé. Lorsque cette icône et l'icône de micro sont affichées dans la barre d'état, la session est capturée pendant sa diffusion en continu.



Pour vous déconnecter du dispositif audio :

- Cliquez sur l'icône Audio de la barre d'outils et sélectionnez OK lorsque vous êtes invité à confirmer la déconnexion. Un message de confirmation apparaît. Cliquez sur OK.

Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio)

Lorsqu'un dispositif audio est connecté, la taille de la mémoire-tampon de capture et de lecture peut être ajustée si nécessaire. Cette fonction permet de contrôler la qualité du son, qui peut être affectée par les limitations de bande passante ou les pointes de réseau.

Augmenter la taille de la mémoire-tampon améliore la qualité audio mais risque d'affecter le débit. La taille de mémoire-tampon maximum est de 400 millisecondes ; une taille supérieure affecterait énormément la qualité audio.

Elle peut être ajustée lorsque nécessaire, pendant une session audio notamment.

Les paramètres audio sont configurés dans les clients AKC, VKC ou MPC.

Pour régler les paramètres audio :

1. Sélectionnez Audio Settings dans le menu Audio. La boîte de dialogue Audio Settings s'ouvre.
2. Réglez la taille de la mémoire-tampon de capture et/ou de lecture, le cas échéant. Cliquez sur OK.

Cartes à puce

Avec KX II, vous pouvez monter un lecteur de cartes à puce sur un serveur cible pour prendre en charge l'authentification par carte à puce et les applications annexes.

Pour obtenir la liste des cartes à puce et des lecteurs de cartes à puce pris en charge, ainsi que les exigences système supplémentaires, reportez-vous à ***Lecteurs de cartes à puce pris en charge ou non*** (à la page 114).

Remarque : Le jeton de carte à puce USB (eToken NG-OTP) est uniquement pris en charge depuis le client distant.

Lorsque vous accédez à un serveur à distance, vous avez la possibilité de sélectionner un lecteur de cartes à puce branché et de le monter sur le serveur. L'authentification par carte à puce est utilisée avec le serveur cible, et non pour se connecter au dispositif. Aussi, les modifications apportées aux codes PIN et aux informations d'authentification ne nécessitent pas de mises à jour des comptes de dispositifs.

Une fois montés sur le serveur cible, le lecteur de cartes et la carte à puce forceront le serveur à se comporter comme s'ils étaient directement connectés. Le retrait de la carte à puce ou du lecteur de cartes entraînera le verrouillage de la session utilisateur ou vous serez déconnecté suivant la stratégie de retrait de la carte définie dans le système d'exploitation du serveur cible. Lorsque la session KVM est arrêtée, parce qu'elle a été fermée ou parce que vous êtes passé sur une autre cible, le lecteur de cartes à puce est automatiquement démonté du serveur cible.

Lorsque le mode PC-Share est activé sur le dispositif, plusieurs utilisateurs peuvent partager l'accès à un serveur cible. Cependant, lorsqu'un lecteur de cartes à puce est connecté à une cible, le dispositif imposera la confidentialité quel que soit le paramètre du mode PC-Share. De plus, si vous rejoignez une session partagée sur un serveur cible, le montage du lecteur de cartes à puce sera désactivé jusqu'à ce qu'un accès exclusif au serveur cible soit disponible.

Une fois qu'une session KVM est établie vers le serveur cible, un menu et un bouton Smart Card (Carte à puce) sont disponibles sur Virtual KVM Client (VKC), Active KVM Client (AKC) et Multi-Platform Client (MPC). Lorsque le menu est ouvert ou que le bouton Smart Card est sélectionné, les lecteurs de cartes à puce détectés comme branchés au client distant s'affichent. A partir de cette boîte de dialogue, vous pouvez relier des lecteurs de cartes à puce supplémentaires, actualiser la liste de lecteurs de cartes à puce reliés à la cible et déconnecter ces derniers. Vous pouvez également retirer ou réinsérer une carte à puce. Cette fonction permet d'envoyer une notification au système d'exploitation d'un serveur cible qui nécessite le retrait ou la réinsertion afin d'afficher la boîte de dialogue de connexion qui convient. L'utilisation de cette fonction permet l'envoi de la notification vers une cible unique sans affecter les autres sessions KVM actives.

Pour monter un lecteur de cartes à puce :

1. Cliquez sur le menu Smart Card, puis sélectionnez Smart Card Reader (Lecteur de cartes à puce). Vous pouvez également cliquer sur le bouton Smart Card  de la barre d'outils.
2. Sélectionnez le lecteur de cartes à puce dans la boîte de dialogue Select Smart Card Reader (Sélectionner un lecteur de cartes à puce).
3. Cliquez sur Mount (Monter).
4. Une boîte de dialogue de progression s'ouvre. Cochez la case Mount selected card reader automatically on connection to targets (Monter le lecteur de cartes à puce sélectionné automatiquement lors de la connexion aux cibles) pour monter le lecteur automatiquement la prochaine fois que vous vous connectez à une cible. Cliquez sur OK pour démarrer le montage.

Pour mettre à jour la carte à puce dans la boîte de dialogue Select Smart Card Reader :

- Cliquez sur Refresh List (Actualiser la liste) si un lecteur de cartes à puce a été branché sur le PC client.

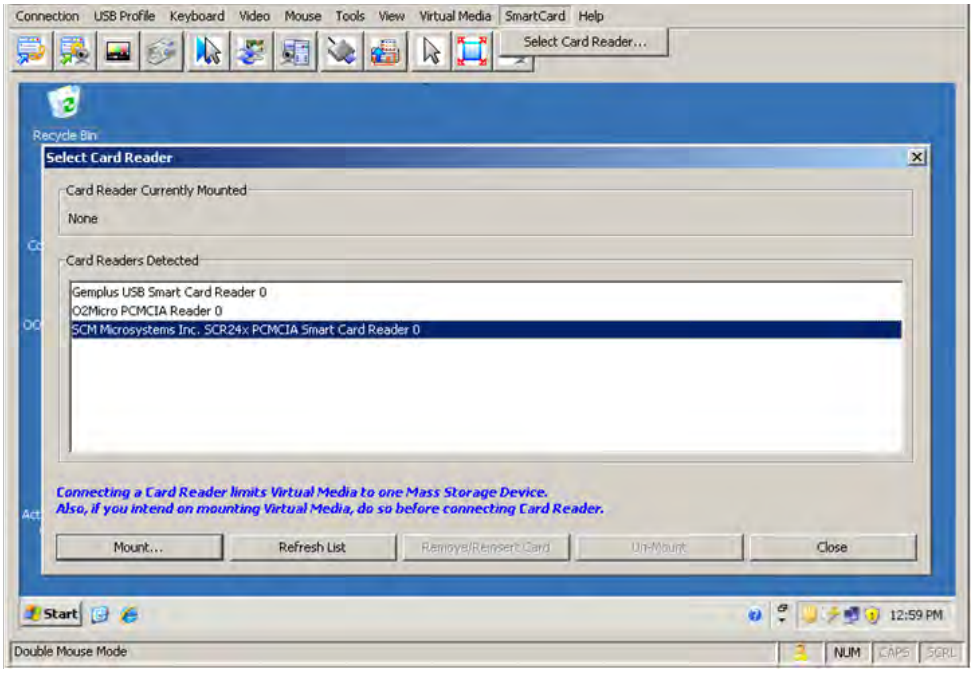
Pour envoyer des notifications de retrait et de réinsertion de la carte à puce à la cible :

- Sélectionnez le lecteur de cartes à puce monté actuellement et cliquez sur le bouton Remove/Reinsert (Retirer/Réinsérer).

Pour démonter un lecteur de cartes à puce :

- Sélectionnez le lecteur de cartes à puce à démonter et cliquez sur le bouton Unmount (Démonter).

Le montage des lecteurs de cartes à puce est également pris en charge depuis la console locale. Reportez-vous à ***Accès par carte à puce à la console locale*** (à la page 319).



Lecteurs de cartes à puce pris en charge ou non

Les lecteurs de cartes à puce USB externes sont pris en charge.

Lecteurs de cartes à puce pris en charge

Type	Fabricant	Modèle	Vérifié
USB	SCM Microsystems	SCR331	Vérifié en local et à distance
USB	ActivIdentity®	Lecteur USB v2.0 ActivIdentity	Vérifié en local et à distance
USB	ActivIdentity	Lecteur USB v3.0 ActivIdentity	Vérifié en local et à distance
USB	Gemalto®	GemPC USB-SW	Vérifié en local et à distance
Clavier avec lecteur de cartes USB	Dell®	Clavier/Lecteur de cartes à puce USB	Vérifié en local et à distance
Clavier avec lecteur de cartes USB	Cherry GmbH	G83-6744 SmartBoard	Vérifié en local et à distance
Lecteur USB de cartes SIM	Omnikey	6121	Vérifié en local et à distance
Intégré (Dell Latitude D620)	O2Micro	OZ776	En local uniquement
PCMCIA	ActivIdentity	Lecteur PCMCIA ActivIdentity	En local uniquement
PCMCIA	SCM Microsystems	SCR243	En local uniquement

Remarque : les lecteurs de cartes à puce SCR331 SCM Microsystems doivent utiliser le firmware SCM Microsystems v5.25.

Lecteurs de cartes à puce non pris en charge

Ce tableau contient la liste des lecteurs testés par Raritan qui ne fonctionnent pas avec le dispositif Raritan et ne sont donc pas pris en charge. Si un lecteur de cartes à puce n'apparaît ni dans le tableau des lecteurs pris en charge ni dans celui des lecteurs non pris en charge, Raritan ne peut pas garantir qu'il fonctionne avec le dispositif.

Type	Fabricant	Modèle	Remarques
Clavier avec lecteur de cartes USB	HP®	ED707A	Point de terminaison sans interruption => non compatible avec pilote Microsoft®
Clavier avec lecteur de cartes USB	SCM Microsystems	SCR338	Mise en œuvre de lecteur de cartes propriétaire (non

Type	Fabricant	Modèle	Remarques
			compatible CCID)
Jeton USB	Aladdin®	eToken PRO™	Mise en œuvre propriétaire

Options 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 :

1. Sélectionnez Help > About Raritan Virtual KVM Client (Aide > A propos de Virtual KVM Client de Raritan).
2. Utilisez le bouton Copy to Clipboard (Copier dans le Presse-papiers) pour copier les informations contenues dans la boîte de dialogue dans un fichier de presse-papiers afin qu'elles soient accessibles ultérieurement lorsque vous communiquez avec le support (le cas échéant).

Multi-Platform Client (MPC)

Multi-Platform Client (MPC) de Raritan est une interface graphique utilisateur pour les lignes de produits Raritan qui permet un accès à distance aux serveurs cible connectés à Raritan KVM via des dispostifs IP. Pour plus d'informations sur l'utilisation de MPC, reportez-vous au **manuel des clients d'accès KVM et série** disponible sur le site Web de Raritan à la même page que le manuel d'utilisation. Des instructions sur le lancement de MPC sont fournies ici.

Notez que ce client est utilisé par divers produits Raritan. Aussi, des références à d'autres produits peuvent apparaître dans cette section de l'aide.

Lancement de MPC à partir d'un navigateur Web

Important : quel que soit le navigateur utilisé, vous devez autoriser l'affichage des fenêtres contextuelles à partir de l'adresse IP du dispositif Dominion pour lancer MPC.

Important : seuls Mac 10.5 et 10.6 avec un processeur Intel® peuvent exécuter JRE 1.6 et donc, être utilisés en tant que client. Mac 10.5.8 ne prend pas en charge MPC en tant que client autonome.

1. Pour ouvrir MPC à partir d'un client exécutant n'importe quel type de navigateur pris en charge, tapez http://ADRESSE-IP/mpc dans la ligne d'adresse, où ADRESSE-IP correspond à l'adresse IP de votre dispositif Raritan. MPC s'ouvre dans une nouvelle fenêtre.

   Remarque : la commande Alt+Tab permet de basculer entre des fenêtres sur le système local uniquement.

   Lorsque MPC s'ouvre, les dispositifs Raritan détectés automatiquement qui se trouvent sur votre sous-réseau s'affichent en arborescence dans le navigateur.

2. Si le nom de votre dispositif n'apparaît pas dans le navigateur, ajoutez-le manuellement :

   a. Choisissez Connection (Connexion) > New Profile (Nouveau profil). La fenêtre Add Connection (Ajouter une connexion) s'affiche.

   b. Entrez-y la description d'un dispositif, indiquez un type de connexion, ajoutez l'adresse IP du dispositif, puis cliquez sur OK. Vous pouvez modifier ces spécifications ultérieurement.

3. Dans le panneau de navigation situé à gauche de la page, double-cliquez sur l'icône qui correspond à votre dispositif Raritan pour vous y connecter.

Remarque : selon le navigateur utilisé et ses paramètres de sécurité, plusieurs vérifications de sécurité et de certificats, ainsi que des messages d'avertissement peuvent s'afficher. Vous devez accepter les options pour ouvrir MPC.

Remarque : si vous utilisez Firefox 3.0.3, vous pouvez rencontrer des problèmes de lancement de l'application. Si cela se produit, effacez la mémoire cache du navigateur et lancez l'application à nouveau.

Chapitre 4 Gestion des prises des PDU de rack (barrettes d'alimentation)

Dans ce chapitre

Présentation

KX II permet de contrôler les prises de PDU (barrettes d'alimentation) de rack des séries PX et RPC de Raritan. connectées à KX II via D2CIM-PWR.

Une fois l'unité de la série PX ou RPC paramétrée puis connectée à KX II, la PDU de rack et ses prises peuvent être contrôlées depuis la page Powerstrip (Barrette d'alimentation) de l'interface de KX II. Pour accéder à cette page, cliquez sur le menu Power (Alimentation) en haut de la page.

La page Powerstrip affiche les PDU de rack connectées au KX II pour lequel l'utilisateur dispose des autorisations appropriées d'accès aux ports. Dans le cas des configurations multiniveaux, la page Powerstrip (Barrette d'alimentation) affiche les PDU de rack connectées à la base et aux KX II multiniveaux, pour lesquels l'utilisateur dispose des autorisations appropriées d'accès aux ports.

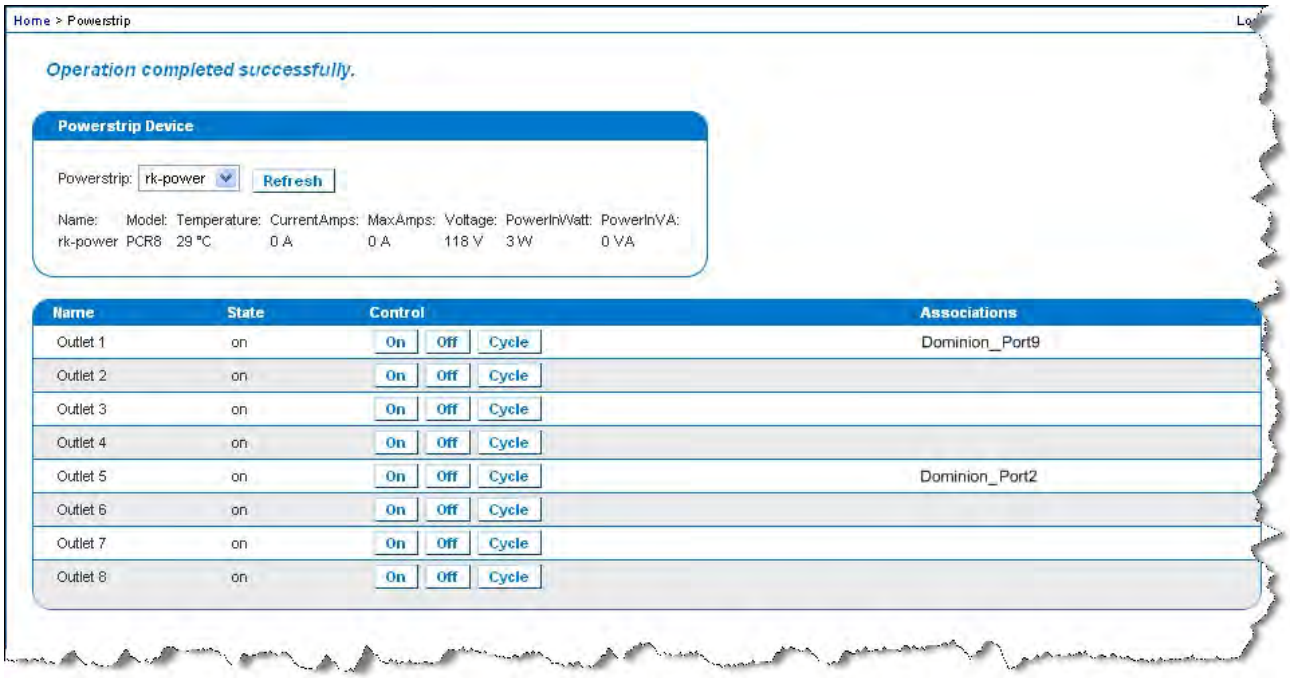
Remarque : pour plus d'informations sur le paramétrage d'une unité PX, reportez-vous au ***manuel d'utilisation de Dominion PX****.*

Sur la page Powerstrip, vous pouvez mettre les prises sous et hors tension, et effectuer leur alimentation cyclique. Vous pouvez également visualiser les informations suivantes relatives à la barrette d'alimentation et aux prises :

- Informations sur le dispositif de barrette d'alimentation :
  - Nom
  - Modèle
  - Température
  - Current Amps (Courant en ampères)
  - Maximum Amps (Courant maximal en ampères)
  - Voltage (Tension)
  - Power in Watts (Puissance en watts)
  - Power in Volts Ampere (Puissance en voltampère)

- Informations sur l'affichage des prises :
  - Name (Nom) - Il s'agit du nom affecté à la prise lors de sa configuration.
  - State (Etat) - Etat sous ou hors tension de la prise.
  - Control (Contrôle) - Permet de mettre les prises sous ou hors tension, ou d'effectuer leur alimentation cyclique.
  - Association - Il s'agit des ports associés à la prise.

Initialement, lorsque vous ouvrez la page Powerstrip, les barrettes d'alimentation actuellement connectées à KX II s'affichent dans la liste déroulante Powerstrip. En outre, les informations relatives à la barrette d'alimentation sélectionnée s'affichent. Si aucune barrette d'alimentation n'est connectée à KX II, un message indiquant « No powerstrips found » (Aucune barrette d'alimentation détectée) s'affiche dans la section Powerstrip Device (Dispositif de barrette d'alimentation) de la page.

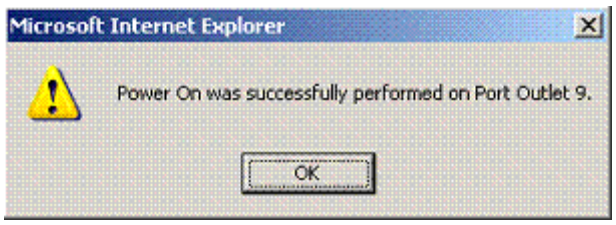


Mise sous/hors tension des prises et alimentation cyclique

Pour mettre une prise sous tension :

1. Cliquez sur le menu Power (Alimentation) pour accéder à la page Powerstrip (Barrette d'alimentation).
2. Dans la liste déroulante Powerstrip, sélectionnez la PDU de rack (barrette d'alimentation) PX que vous souhaitez mettre sous tension.

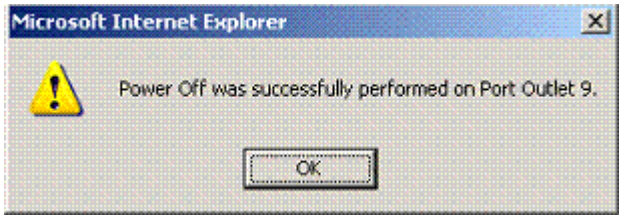
3. Cliquez sur Refresh (Actualiser) pour afficher les contrôles d'alimentation.
4. Cliquez sur On (Sous tension).
5. Cliquez sur OK pour fermer la boîte de dialogue de confirmation Power On (Sous tension). La prise est mise sous tension et son état indique on.



Pour mettre une prise hors tension :

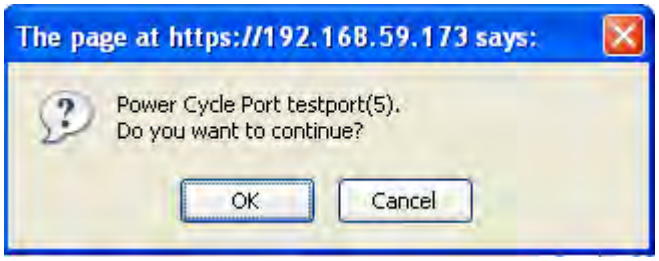
1. Cliquez sur Off (Hors tension).
2. Cliquez sur OK dans la boîte de dialogue Power Off (Hors tension).

3. Cliquez sur OK dans la boîte de dialogue de confirmation Power Off (Hors tension). La prise est mise hors tension et son état indique off.

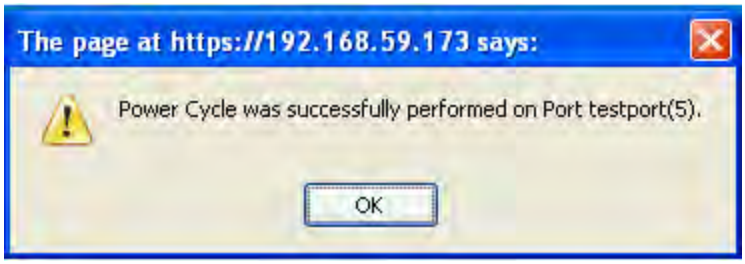


Pour effectuer l'alimentation cyclique d'une prise :

1. Cliquez sur Cycle. La boîte de dialogue Power Cycle Port (Port d'alimentation cyclique) s'ouvre.



2. Cliquez sur OK. L'alimentation cyclique de la prise débute alors (notez qu'elle peut prendre plusieurs secondes).



3. Une fois l'alimentation cyclique terminée, la boîte de dialogue s'ouvre. Cliquez sur OK pour fermer la boîte de dialogue.

Chapitre 5 Support virtuel

Dans ce chapitre

Présentation

La fonction Support virtuel prolonge les capacités KVM en permettant aux serveurs cible KVM d'accéder à distance aux supports des serveurs de fichiers de PC clients et réseau. KX II prend en charge l'accès par support virtuel des disques durs et des images montées à distance. Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement 256 bits AES ou RC4.

Grâce à cette fonction, les supports montés sur les serveurs de fichiers de PC clients et réseau sont intégrés virtuellement au serveur cible. Le serveur cible peut ensuite lire et écrire sur ce support comme si ce dernier lui était physiquement connecté. Outre la prise en charge des fichiers de données via support virtuel, les fichiers sont supportés par support virtuel via une connexion USB.

Les CIM numériques, D2CIM-VUSB et D2CIM-DVUSB prennent en charge les sessions sur support virtuel pour les serveurs cible KVM disposant de l'interface USB 2.0. Ces CIM prennent également en charge la synchronisation absolue de la souris, ainsi que la mise à jour du firmware à distance.

Les supports virtuels permettent d'effectuer des tâches à distance, telles que :

- le transfert de fichiers ;
- la réalisation de diagnostics ;
- l'installation ou la correction d'applications ;
- l'installation complète du système d'exploitation ;
- l'enregistrement et la lecture audionumériques*.

Les types de supports virtuels sont pris en charge pour les clients Windows®, Mac® et Linux™ :

- lecteurs CD et DVD internes et montés sur USB ;
- dispositifs de stockage de masse USB ;
- disques durs de PC ;
- images ISO (images disque) ;
- dispositifs audionumériques*.

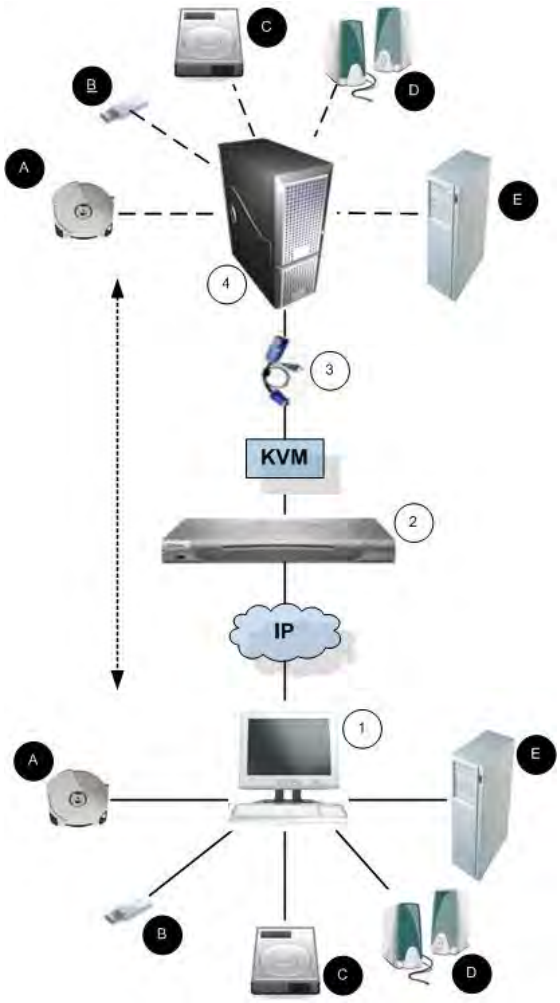
Remarque : ISO9660 est la norme prise en charge par Raritan. D'autres normes ISO peuvent cependant être utilisées.

Les systèmes d'exploitation clients suivants sont pris en charge :

- Serveurs
- Mac OS X 10.5, 10.6 et 10.7
- Red Hat Desktop 4.0 et 5.0
- Open SUSE 10, 11

- Fedora 13 et 14

Virtual KVM Client (VKC) et Multi-Platform Client (MPC) peuvent être utilisés pour monter des types de supports virtuels, à l'exception de Mac OS X 10.5, qui est pris en charge exclusivement par MPC.



Légende			
1	Ordinateur de bureau	B	Dispositif de stockage de masse USB
2	KX II	C	Disque dur de l'ordinateur
3	CIM	D	Haut-parleurs audio
4	Serveur cible	E	Serveur de fichiers à distance (images ISO)
A	Lecteur CD/DVD		

Conditions requises pour l'utilisation des supports virtuels

Grâce à la fonction de support virtuel, vous pouvez monter jusqu'à deux lecteurs (de différents types) pris en charge par le profil USB appliqué actuellement à la cible. 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 support virtuel CD-ROM demeure ouvert pour vous permettre de monter un autre CD-ROM virtuellement. Ces « canaux » de support virtuel restent ouverts jusqu'à la fermeture de la session KVM tant qu'elle est prise en charge par le profil USB.

Pour utiliser un support visuel, connectez/reliez-le au serveur de fichiers client ou réseau auquel vous souhaitez accéder à partir du serveur cible. Ce n'est pas nécessairement la première étape à effectuer, mais elle doit se dérouler avant de tenter d'accéder à ce support.

Pour utiliser les supports virtuels, les conditions suivantes doivent être remplies :

Dispositif Dominion

- Pour les utilisateurs ayant besoin d'accéder aux supports virtuels, des autorisations de dispositif doivent être définies pour permettre l'accès aux ports concernés, ainsi que l'accès aux supports virtuels pour ces ports (Autorisations des ports d'accès aux supports virtuels). Les permissions des ports sont définies au niveau du groupe.
- Il doit exister une connexion USB entre le dispositif et le serveur cible.
- Pour utiliser PC-Share, des paramètres de sécurité doivent également être activés sur la page Security Settings. **Facultatif**
- Vous devez choisir le profil USB correct pour le serveur cible KVM auquel vous vous connectez.

PC client

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

Remarque : si vous utilisez Microsoft Vista ou Windows 7, désactivez Contrôle de compte d'utilisateur ou sélectionnez Exécuter en tant qu'administrateur lorsque vous démarrez Internet Explorer. Pour cela, cliquez sur le menu Démarrer, recherchez Internet Explorer, cliquez dessus avec le bouton droit de la souris et sélectionnez Exécuter en tant qu'administrateur.

Serveur cible

- Les serveurs cible KVM doivent prendre en charge les lecteurs connectés USB.
- Tous les patchs récents doivent être installés sur les serveurs cible KVM qui exécutent Windows 2000.
- Les ports USB 2.0 sont plus rapides et donc préférables.

Supports virtuels dans un environnement Windows XP

Si vous exécutez Virtual KVM Client ou Active KVM Client dans un environnement Windows® XP, les utilisateurs doivent disposer de droits Administrateur pour accéder à n'importe quel type de support virtuel autre que les connexions CD-ROM, les ISO et les images ISO.

Supports virtuels dans un environnement Linux

Les informations importantes suivantes relatives à l'emploi des supports virtuels s'adressent aux utilisateurs Linux®.

Exigence en matière d'autorisation pour utilisateur racine

Votre connexion au support virtuel peut être fermée si vous montez un CD-ROM depuis un client Linux à une cible, puis le démontez. La connexion se ferme également lorsqu'un lecteur de disquette a été monté et qu'une disquette est ensuite retirée. Pour éviter ces problèmes, vous devez être utilisateur racine.

Remarque : Les lecteurs mappés à partir des clients Mac® et Linux® ne sont pas verrouillés lorsqu'ils sont montés sur des cibles connectées. Ceci ne concerne que KX II 2.4.0 et (supérieur) et LX 2.4.5 (et supérieur) qui offrent une prise en charge de Mac et de Linux.

Autorisations

Les utilisateurs doivent disposer des autorisations d'accès appropriées pour connecter le lecteur/CD-ROM à la cible. Pour vérifier si c'est le cas :

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0

brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

Dans l'exemple ci-dessus, l'autorisation doit être modifiée pour permettre l'accès en lecture.

Dans un système prenant en charge les LCA dans ses utilitaires de fichiers, la commande ls change de comportement de la manière suivante :

- Pour les fichiers dotés d'une LCA par défaut, ou d'une LCA contenant plus d'entrées que les trois LCA obligatoires, l'utilitaire ls(1) dans la forme longue produite par ls -l affiche un signe plus (+) après la chaîne d'autorisation.

Ceci est indiqué dans l'exemple fourni ici pour /dev/sr0, utilisez getfacl –a /dev/sr0 pour vérifier si l'accès a été accordé à l'utilisateur dans le cadre d'une LCA. C'est le cas ici et il peut donc connecter le cd-rom au serveur cible, même si la sortie de la commande ls –l peut indiquer le contraire.

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

Une vérification similaire des autorisations concernant un dispositif amovible indique :

```
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1


guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
&gt;    getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---
```

Ceci requiert que l'utilisateur reçoive des autorisations en lecture seule pour le dispositif amovible :

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

Le lecteur est alors disponible pour la connexion à la cible.

Supports virtuels dans un environnement Mac

KX II 2.4.0 (et supérieur) et LX 2.4.5 (et supérieur) prennent en charge les supports virtuels dans un environnement Linux. Les informations importantes suivantes relatives à l'emploi des supports virtuels s'adressent aux utilisateurs Mac®.

Partitions système actives

- Vous ne pouvez pas utiliser de supports virtuels pour le montage de partitions système actives sur un client Mac.

Partitions de lecteur

- Les limites en matière de partition de lecteur suivantes existent à travers les systèmes d'exploitation :
  - Les cibles Windows et Mac ne peuvent pas lire les partitions formatées Linux.
  - Windows® et Linux® ne peuvent pas lire les partitions formatées Mac.
  - Seules les partitions FAT Windows sont prises en charge par Linux.
  - FAT et NTFS Windows sont pris en charge par Mac.
- Les utilisateurs Mac doivent démonter les dispositifs déjà montés pour se connecter à un serveur cible. Utilisez >diskutil umount /dev/disk1s1 pour démonter le dispositif et diskutil mount /dev/disk1s1 pour le remonter.

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

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

- pour les clients Linux® et Mac®
- 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)

Utilisation des supports virtuels

Reportez-vous à ***Conditions requises pour l'utilisation des supports virtuels*** (à la page 126) avant d'utiliser le support virtuel.

Pour utiliser les supports virtuels :

1. Si vous souhaitez accéder à des images ISO de serveur de fichiers, identifiez ces images et ces serveurs de fichiers par le biais de la page Remote Console File Server Setup (Configuration des serveurs de fichiers de la console distante). Reportez-vous à ***Configuration du serveur de fichiers du support virtuel (Images ISO du serveur de fichiers uniquement)*** (à la page 132).

   Remarque : le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

2. Ouvrez une session KVM avec le serveur cible adéquat.
   a. Ouvrez la page Port Access (Accès aux ports) depuis la console distante.
   b. Connectez-vous au serveur cible à partir de la page Port Access (Accès aux ports) :
   - Cliquez sur le nom du port (Port Name) du serveur approprié.
   - Choisissez la commande Connect (Connecter) dans le menu d'action des ports. Le serveur cible s'ouvre dans une fenêtre Virtual KVM Client.
3. Connectez-vous au support virtuel.

Pour :	Sélectionnez cette option VM :
Lecteurs locaux	Connect Drive
Lecteurs de CD/DVD locaux	Connect CD-ROM/ISO (Connecter CD-ROM/ISO)
Images ISO	Connect CD-ROM/ISO (Connecter CD-ROM/ISO)
Images ISO de serveur de fichiers	Connect CD-ROM/ISO (Connecter CD-ROM/ISO)

Une fois vos tâches terminées, déconnectez le support virtuel. Reportez-vous à ***Déconnexion des supports virtuels*** (à la page 137).

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

Remarque : cette fonction est requise uniquement lors de l'utilisation de supports virtuels pour accéder aux images ISO du serveur de fichiers. le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

Remarque : La prise en charge de SMB/CIFS est requise sur le serveur de fichiers.

Utilisez la page File Server Setup (Configuration des serveurs de fichiers) de la console distante pour spécifier les serveurs de fichiers et les chemins d'accès aux images auxquelles vous souhaitez accéder à l'aide de la fonction Support virtuel. Les images ISO de serveurs de fichiers spécifiées ici sont disponibles dans les listes déroulantes Remote Server ISO Image Hostname (Nom d'hôte des images ISO de serveur distant) et Image de la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels). Reportez-vous à ***Montage des images CD-ROM/DVD-ROM/ISO*** (à la page 135).

Pour désigner les images ISO de serveur de fichiers pour l'accès aux supports virtuels :

1. Sélectionnez Virtual Media (Supports virtuels) dans la console distante. La page File Server Setup (Configuration des serveurs de fichiers) s'ouvre.
2. Cochez la case Selected (Sélectionné) pour tous les supports qui seront accessibles comme supports virtuels.
3. Entrez les informations relatives aux images ISO de serveur de fichiers auxquelles vous souhaitez accéder :
   - IP Address/Host Name - Nom d'hôte ou adresse IP du serveur de fichiers.
   - Image Path - Nom complet du chemin d'accès à l'emplacement de l'image ISO. Par exemple, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, etc.

   Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.
4. Cliquez sur Save (Enregistrer). Tous les supports indiqués ici peuvent maintenant être sélectionnés dans la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels).

Remarque : vous ne pouvez pas accéder à une image ISO distante via les supports virtuels à l'aide d'une adresse IPv6 à cause des limites techniques du logiciel tiers utilisé par le dispositif LX, KX, KSX ou KX101 G2.

Remarque : si vous vous connectez à un serveur Windows 2003® et tentez de charger une image ISO du serveur, un message d'erreur peut s'afficher pour indiquer que le montage des supports virtuels sur le port a échoué, que la connexion au serveur est impossible, ou que le nom d'utilisateur et le mot de passe pour le serveur de fichiers sont incorrects. Dans ce cas, désactivez Serveur réseau Microsoft : communications signées numériquement.

Remarque : si vous vous connectez à un serveur Windows 2003 et tentez de charger une image ISO à partir de ce serveur, vous risquez de recevoir un message d'erreur indiquant : « Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password » (Echec du montage du support virtuel. Impossible de connecter le serveur de fichiers ou nom d'utilisateur et mot de passe du serveur de fichiers erroné). Dans ce cas, désactivez l'option Serveur réseau Microsoft : communications signées numériquement sur le serveur sous les stratégies Contrôleurs de domaine.

Connexion aux supports virtuels

Montage des lecteurs locaux

Cette option permet de monter un lecteur entier, ce qui signifie que le lecteur de disque entier est monté virtuellement sur le serveur cible. Utilisez-la uniquement pour les disques durs et les lecteurs externes. Ceux-ci ne comprennent pas les lecteurs réseau, CD-ROM ou DVD-ROM. Il s'agit de la seule option pour laquelle la fonction Read-Write (Lecture/écriture) est disponible.

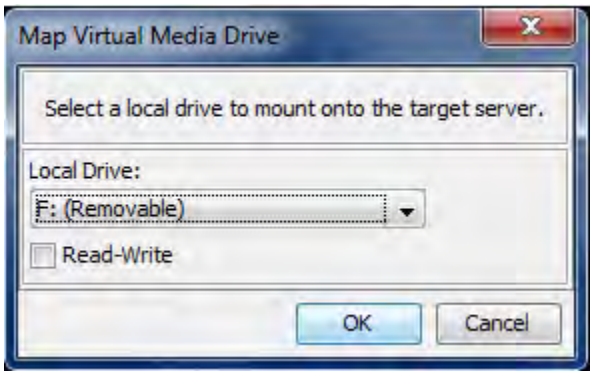
Remarque : les serveurs cible KVM exécutant le système d'exploitation Windows XP® risquent de ne pas accepter les nouvelles connexions de stockage en masse après la redirection vers eux d'une partition de format NTFS (par exemple, le disque C local).

Dans ce cas, fermez la console distante, puis reconnectez-vous avant de rediriger un autre dispositif de support virtuel. Si d'autres utilisateurs sont connectés au même serveur cible, ils doivent également fermer leur connexion au serveur cible.

Remarque : dans KX II 2.1.0 (et supérieur), lorsque vous montez un lecteur externe, tel qu'un lecteur de disquettes, le voyant reste allumé parce que le dispositif vérifie le lecteur toutes les 500 millisecondes afin de s'assurer qu'il est toujours monté.

Pour accéder à un lecteur de l'ordinateur client :

1. Dans Virtual KVM Client, sélectionnez Virtual Media (Supports virtuels) > Connect Drive (Connecter le lecteur). La boîte de dialogue Map Virtual Media Drive (Mapper le lecteur de support virtuel) s'affiche. ()



2. Sélectionnez le lecteur dans la liste déroulante Local Drive (Lecteur local).

3. Pour disposer d'un accès en lecture et en écriture, cochez la case Read-Write (Lecture-écriture). Cette option est désactivée pour les lecteurs non amovibles. Reportez-vous à ***Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible*** (à la page 130) pour plus d'informations. Lorsque cette case est cochée, vous aurez accès en lecture et en écriture au disque USB connecté.

   AVERTISSEMENT : l'activation de la fonction Lecture-écriture peut être dangereuse. L'accès simultané à un même lecteur à partir de plusieurs entités peut altérer les données. Si vous n'avez pas besoin d'un accès en écriture, ne sélectionnez pas cette option.

4. Cliquez sur Connect (Connecter). Le support est monté sur le serveur cible virtuellement. Vous pouvez y accéder de la même manière que pour tous les autres lecteurs.

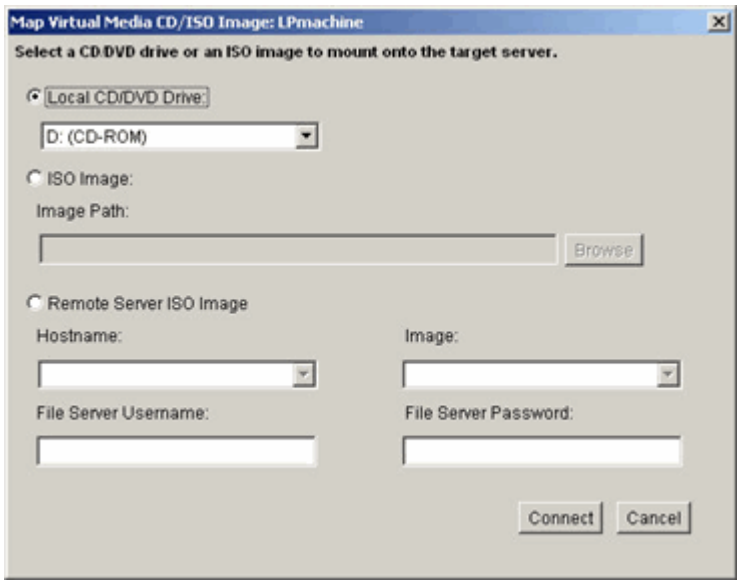
Montage des images CD-ROM/DVD-ROM/ISO

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

Remarque : le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

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

1. Dans Virtual KVM Client, sélectionnez Virtual Media > Connect CD-ROM/ISO Image (Supports virtuels > Connecter l'image ISO/CD-ROM). La boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image ISO/CD de support virtuel) s'affiche.



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 Browse (Parcourir).

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 un nom d'hôte et une image dans la liste déroulante. Les chemins d'accès aux images et les serveurs de fichiers disponibles sont ceux que vous avez configurés via la page File Server Setup (Configuration des serveurs de fichiers). Seuls les éléments que vous avez configurés à l'aide de cette page figurent dans la liste déroulante.

c. File Server Username - Nom d'utilisateur requis pour l'accès au serveur de fichiers. Le nom peut comprendre le nom du domaine, tel que mondomaine/nomutilisateur.

d. File Server Password - Mot de passe requis pour l'accès au serveur de fichiers (le champ est masqué lorsque vous tapez).

e. Cliquez sur Connect (Connecter).

Le support est monté sur le serveur cible virtuellement. Vous pouvez y accéder de la même manière que pour tous les autres lecteurs.

Remarque : si vous travaillez avec des fichiers sur une cible Linux®, utilisez la commande Sync de Linux après la copie des fichiers à l'aide des supports virtuels afin d'afficher les fichiers copiés. Les fichiers risquent de ne pas apparaître si la synchronisation n'est pas effectuée.

Remarque : si vous utilisez le système d'exploitation Windows 7®, Disque amovible n'apparaît pas par défaut dans le dossier Poste de travail de Windows lorsque vous montez un lecteur de CD/DVD local, ou une image ISO locale ou distante. Pour afficher le lecteur de CD/DVD local, ou l'image ISO locale ou distante dans ce dossier, sélectionnez Outils > Options des dossiers > Affichage et désélectionnez Masquer les dossiers vides dans le dossier Ordinateur.

Remarque : vous ne pouvez pas accéder à une image ISO distante via les supports virtuels à l'aide d'une adresse IPv6 à cause des limites techniques du logiciel tiers.

Déconnexion des supports virtuels

Pour déconnecter les lecteurs de supports virtuels :

- Pour les lecteurs locaux, sélectionnez Virtual Media (Supports virtuels) > Disconnect Drive (Déconnecter le lecteur).
- Pour les images ISO, CD et DVD, sélectionnez Virtual Media (Supports Virtuels) > Disconnect CD-ROM/ISO Image (Déconnecter l'image ISO/CD-ROM)

Remarque : outre la commande Disconnect (Déconnecter), la simple fermeture de la connexion KVM entraîne la déconnexion du support virtuel.

Chapitre 6 Profils USB

Dans ce chapitre

Présentation

Pour élargir la compatibilité de KX II avec différents serveurs cible KVM, Raritan fournit une sélection standard de profils de configuration USB pour des implémentations de serveurs sur une grande variété de systèmes d'exploitation et de niveaux de BIOS.

Le profil USB générique (défaut) répond aux besoins de la grande majorité des configurations de serveurs cible KVM déployées. Des profils supplémentaires sont fournis pour répondre aux besoins spécifiques d'autres configurations de serveurs déployées courantes (par exemple, Linux® et MAC OS X®). Un certain nombre de profils (désignés par nom de plate-forme et révision de BIOS) permet également d'améliorer la compatibilité de la fonction Support virtuel avec le serveur cible ; par exemple, lors d'un fonctionnement au niveau du BIOS.

Les profils USB sont configurés sur la page Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) > Port des consoles distantes et locales de KX II. Un administrateur de dispositifs peut configurer le port avec les profils répondant le mieux aux besoins de l'utilisateur et de la configuration des serveurs cible.

Un utilisateur qui se connecte à un serveur cible KVM choisit parmi les profils présélectionnés dans Virtual KVM Client, suivant l'état de fonctionnement du serveur cible KVM. Par exemple, si le serveur est lancé et que l'utilisateur souhaite se servir du système d'exploitation Windows®, il est recommandé d'utiliser le profil générique. Mais si l'utilisateur souhaite modifier les paramètres du menu du BIOS ou effectuer le démarrage à partir d'un lecteur de support virtuel, suivant le modèle du serveur cible, un profil BIOS est sans doute plus adéquat.

Si aucun des profils USB standard fournis par Raritan ne fonctionne avec une cible KVM précise, veuillez contactez l'assistance technique de Raritan.

Compatibilité CIM

Pour utiliser les profils USB, vous devez disposer d'un CIM numérique, d'un D2CIM-VUSB ou d'un D2CIM-DVUSB dont le firmware est à jour. Un VM-CIM dont le firmware n'est pas à niveau prend en charge une large gamme de configurations (clavier, souris, CD-ROM et lecteur amovible) mais ne pourra pas utiliser les profils optimisés pour des configurations cible particulières. Les VM-CIM existants doivent donc être mis à niveau avec le dernier firmware pour accéder aux profils USB. Tant qu'ils ne le seront pas, ils fourniront des fonctionnalités équivalentes à celles du profil générique.

Le firmware VM-CIM est automatiquement mis à niveau lors d'une mise à niveau de firmware, mais les VM-CIM dont le firmware n'est pas actualisé peuvent l'être tel que décrit dans ***Mise à niveau des CIM*** (à la page 289).

Reportez-vous à ***Spécifications des modules d'interface pour ordinateur (CIM) pris en charge*** (voir "***Spécifications des CIM pris en charge***" à la page 343) pour plus d'informations.

Profils USB disponibles

La version actuelle de KX II comporte une sélection de profils USB décrits dans le tableau ci-après. Les nouveaux profils sont inclus avec chaque mise à niveau de firmware fournie par Raritan. Lorsque des nouveaux profils sont ajoutés, ils sont décrits dans l'aide.

Profil USB	Description
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	BIOS Dell PowerEdge 1950/2950/2970/6950/R200 Utilisez ce profil ou le profil générique pour le BIOS Dell PowerEdge 1950/2950/2970/6950/R200. Restrictions : • Néant
BIOS Dell OptiPlex ™ clavier uniquement	Accès BIOS Dell Optiplex (clavier uniquement) Utilisez ce profil pour disposer de la fonctionnalité de clavier pour le BIOS Dell OptiPlex lors de l'utilisation de D2CIM-VUSB. Avec le nouveau D2CIM-DVUSB, utilisez le profil générique. Avis : • Optiplex 210L/280/745/GX620

Profil USB	Description
	nécessite D2CIM-DVUSB avec le profil générique pour prendre en charge les supports virtuels. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Fonction Supports virtuels non prise en charge
BIOS DellPowerEdge Keyboard Only	Accès BIOS Dell PowerEdge (clavier uniquement) Utilisez ce profil pour disposer de la fonctionnalité de clavier pour le BIOS Dell PowerEdge lors de l'utilisation de D2CIM-VUSB. Avec le nouveau D2CIM-DVUSB, utilisez le profil générique. Avis : • PowerEdge 650/1650/1750/2600/2650 BIOS ne prend pas en charge les lecteurs USB CD-ROM et les disques durs comme service armorçable • PowerEdge 750/850/860/1850/2850/SC1425 BIOS nécessite D2CIM-DVUSB avec le profil générique pour prendre en charge les supports virtuels. • Utilisez BIOS Dell PowerEdge 1950/2950/2970/6950/R200 ou le profil générique pour PowerEdge 1950/2950/2970/6950/R200 lors d'un fonctionnement dans le BIOS. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Fonction Supports virtuels non prise en charge

Profil USB	Description
Carte-mère BIOS ASUS P4C800	Utilisez ce profil pour accéder au BIOS et démarrer depuis Virtual Media sur des systèmes Asus P4C800. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS Generic	BIOS Generic Utilisez ce profil lorsque le profil générique du système d'exploitation ne fonctionne pas sur le BIOS. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Utilisez ce profil pour HP Proliant DL145 PhoenixBIOS pendant l'installation du système d'exploitation. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Utilisez ce profil pour démarrer les ordinateurs de la série HP Compaq DC7100/DC7600 à partir du support virtuel. Restrictions :

Profil USB	Description
	• Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS IBM ThinkCentre Lenovo	BIOS IBM Thinkcentre Lenovo Utilisez le profil pour la carte principale IBM® Thinkcentre Lenovo (modèle 828841U) pendant les opérations du BIOS. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
IBM BladeCenter H avec Advanced Management Module	Utilisez ce profil pour activer la fonctionnalité de support virtuel lorsque D2CIM-VUSB ou D2CIM-DVUSB est connecté au module AMM. Restrictions : • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 et X61 (démarrage à partir du support virtuel) Utilisez ce profil pour démarrer les ordinateurs portables des séries T61 et X61 à partir du support virtuel. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
BIOS Mac	BIOS Mac Utilisez ce profil pour le BIOS Mac®. Restrictions : • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.

Profil USB	Description
Générique	Le profil USB générique se comporte comme dans la version du KX2 original. Utilisez-le pour les systèmes d'exploitation Windows 2000®, Windows XP®, Windows Vista® et ultérieur. Restrictions : • Néant
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Utilisez ce profil pour le serveur HP Proliant DL360/DL380 série G4 lors de l'installation du système d'exploitation à l'aide de HP SmartStart CD. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge
HP Proliant DL360/DL380 G4 (Installation Windows 2003® Server)	HP Proliant DL360/DL380 G4 (Installation Windows 2003 Server) Utilisez ce profil pour le serveur HP Proliant DL360/DL380 série G4 lors de l'installation de Windows 2003 Server sans HP SmartStart CD. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
Linux®	Profil Linux générique Il s'agit du profil Linux générique ; utilisez-le pour Redhat Enterprise Linux, SuSE Linux Enterprise Desktop et distributions semblables. Restrictions : • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge
MAC OS X® (10.4.9 et supérieur)	MAC OS X, versions 10.4.9 et supérieure Ce profil compense la mise à l'échelle

Profil USB	Description
	des coordonnées de la souris présente dans les versions récentes de Mac OS X. Sélectionnez-le si les positions de la souris distante et locale sont désynchronisées près des bordures du bureau. Restrictions : • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Carte-mère industrielle RUBY (AwardBIOS)	Carte-mère industrielle RUBY (AwardBIOS) Utilisez ce profil pour les cartes mères industrielles de la série RUBY-9715VG2A avec Phoenix/AwardBIOS v6.00PG. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Supermicro Mainboard Phoenix (AwardBIOS)	Carte-mère Supermicro Phoenix (AwardBIOS) Utilisez ce profil pour les cartes-mères de la série Supermicro avec Phoenix AwardBIOS. Restrictions : • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Suse 9.2	SuSE Linux 9.2 Utilisez-le pour la distribution SuSE Linux 9.2. Restrictions : • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Vitesse du bus USB limitée à plein régime (12 Mbps)

Profil USB	Description
Troubleshooting 1	Dépannage de profil 1 • Stockage en masse en premier • Clavier et souris (Type 1) • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Troubleshooting 2	Dépannage de profil 2 • Clavier et souris (Type 2) en premier • Stockage en masse • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Troubleshooting 3	Dépannage de profil 3 • Stockage en masse en premier • Clavier et souris (Type 2) • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.

Profil USB	Description
Utiliser le plein régime pour le CIM de support virtuel	Utiliser le plein régime pour le CIM de support virtuel Ce profil se comporte comme dans la version du KX2 original lorsque l'option Full Speed for Virtual Media CIM (Plein régime pour le CIM de support virtuel) est activée. Utile pour le BIOS qui ne peut pas traiter les dispositifs USB High Speed. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
Utiliser le plein régime pour USB clavier et souris	Ce profil paramètre l'interface USB clavier et souris du CIM Dual-VM sur Full Speed (Plein régime). Utile pour les dispositifs qui ne peuvent pas fonctionner correctement avec les paramètres USB Low Speed (Faible régime). Restrictions : • Vitesse du bus USB définie sur plein régime (12 Mbps) dans l'interface USB clavier et souris

Sélection des profils pour un port KVM

KX II est fourni avec un ensemble des profils USB que vous pouvez affecter à un port KVM suivant les caractéristiques du serveur cible KVM auquel il se connecte. Vous attribuez des profils USB à un port KVM sur la page Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) > Port de la console distante ou locale de KX II.

L'administrateur désigne les profils les plus susceptibles d'être utilisés pour une cible spécifique. Ces profils peuvent alors être sélectionnés via MPC, AKC et VKC. Si un profil n'est pas disponible, vous pouvez accéder à n'importe quel profil disponible en sélectionnant USB Profile (Profil USB) > Other Profiles (Autres profils).

L'affectation de profils USB à un port KVM met ceux-ci à la disposition d'un utilisateur connecté à un serveur cible KVM. Le cas échéant, l'utilisateur peut sélectionner un profil USB dans le menu USB Profile de VKC, AKC ou MPC.

Pour plus d'informations sur l'affectation de profils USB à un port KVM, reportez-vous à ***Configuration des profils USB (page Port)*** (à la page 243).

Modes de souris lors de l'utilisation du profil USB Mac OS X avec DCIM-VUSB

Si vous utilisez DCIM-VUSB, avec un profil USB Mac OS-X®, en exécutant Mac OS X 10.4.9 (ou supérieur), vous devez passer en mode de souris unique lors du redémarrage pour utiliser la souris dans le menu Boot (Amorçage).

Pour configurer la souris pour qu'elle fonctionne dans le menu Boot :

1. Redémarrez le Mac et appuyez sur la touche Option pendant le redémarrage pour ouvrir le menu Boot. La souris ne répond pas à ce moment.
2. Sélectionnez le mode de souris intelligente, puis le mode de souris unique. La souris répond.

   Remarque : la souris peut être lente en mode de souris unique.

3. Une fois que vous avez quitté le menu Boot et avez amorcé le système d'exploitation, quittez le mode de souris unique et repassez en mode de souris absolue pour obtenir de meilleures performances de la souris.

Chapitre 7 Gestion des utilisateurs

Dans ce chapitre

Groupes d'utilisateurs

KX II stocke une liste interne de tous les noms des utilisateurs et des groupes pour déterminer les autorisations et permissions d'accès. Ces informations sont stockées de manière interne dans un format chiffré. Il existe plusieurs formes d'authentification et celle-ci est connue sous le nom d'authentification locale. Tous les utilisateurs doivent être authentifiés. Si KX II est configuré pour LDAP/LDAPS ou RADIUS, cette authentification est traitée en premier, suivie par l'authentification locale.

Tous les dispositifs KX II sont livrés avec trois groupes d'utilisateurs par défaut. Ces groupes ne peuvent être supprimés :

Utilisateur	Description
Admin	Les membres de ce groupe disposent de droits d'administrateur complets. L'utilisateur par défaut usine est membre de ce groupe et dispose de la totalité des droits de système. De plus, l'utilisateur Admin doit être membre du groupe Admin.
Unknown (Inconnu)	Il s'agit du groupe par défaut pour les utilisateurs authentifiés en externe à l'aide de LDAP/LDAPS ou RADIUS, ou que le système ne connaît pas. Si le serveur externe LDAP/LDAPS ou RADIUS ne peut pas identifier un groupe d'utilisateurs valide, le groupe Unknown est alors utilisé. De plus, tout utilisateur qui vient d'être créé est automatiquement affecté à ce groupe en attendant d'être transféré dans un autre.
Individual Group (Groupe individuel)	Un groupe individuel ne comporte en fait qu'un seul membre. Cet utilisateur spécifique est donc dans son propre groupe et non affilié à d'autres groupes réels. Les groupes individuels sont repérables par leur nom qui comporte le signe @. Le groupe individuel permet à un compte d'utilisateur de bénéficier des mêmes droits qu'un groupe.

Vous pouvez créer jusqu'à 254 groupes d'utilisateurs dans KX II. Vous pouvez créer jusqu'à 254 groupes d'utilisateurs dans le KX II.

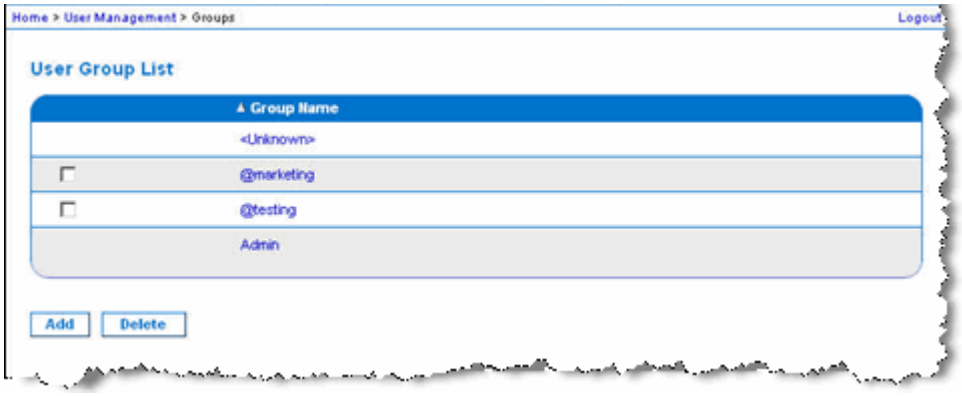
Liste des groupes d'utilisateurs

Les groupes d'utilisateurs sont utilisés avec une authentification à distance et locale (par l'intermédiaire de RADIUS ou de LDAP/LDAPS). Il est recommandé de définir les groupes avant de créer les différents utilisateurs car lorsque vous ajoutez un utilisateur, vous devez l'affecter 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. Ceux-ci peuvent être triés dans l'ordre croissant ou décroissant en cliquant sur l'en-tête de colonne Group Name. A partir de la page User Group List, vous pouvez ajouter, modifier ou supprimer des groupes d'utilisateurs.

Pour répertorier les groupes d'utilisateurs :

- Sélectionnez User Management (Gestion des utilisateurs) > User Group List (Liste des groupes d'utilisateurs). La page User Group List s'ouvre.



Relation entre les utilisateurs et les groupes

Les utilisateurs appartiennent à un groupe et les groupes disposent de droits. La répartition en groupes des utilisateurs de votre unité KX II offre un gain de temps, puisqu'elle permet 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 des utilisateurs particuliers à des groupes. Vous avez alors la possibilité de classer l'utilisateur comme « individuel ».

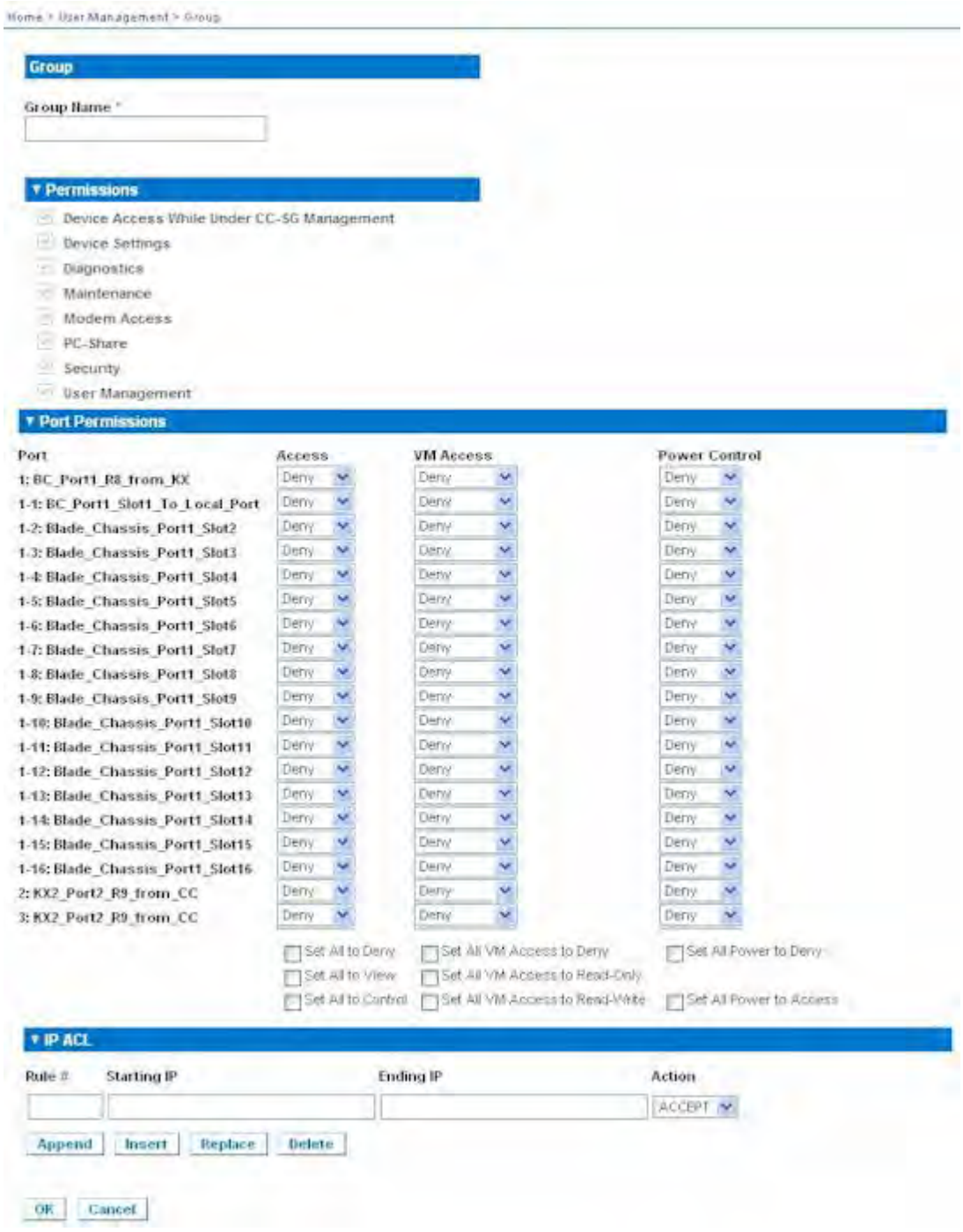
Lorsqu'un utilisateur est authentifié, le dispositif utilise les informations relatives au groupe auquel il appartient pour déterminer ses autorisations : ports de serveur accessibles, autorisation éventuelle de redémarrer l'unité, etc.

Ajout d'un nouveau groupe d'utilisateurs

Pour ajouter un nouveau groupe d'utilisateurs :

1. Sélectionnez User Management > Add New User Group (Gestion des utilisateurs > Ajouter un nouveau groupe d'utilisateurs) ou cliquez sur Add (Ajouter) dans la page User Group List (Liste des groupes d'utilisateurs).
2. Entrez un nom descriptif pour le nouveau groupe d'utilisateurs dans le champ Group Name (64 caractères au plus).
3. Cochez les cases situées en regard des autorisations que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à ***Configuration des autorisations*** (à la page 152).
4. Indiquez les ports de serveur et le type d'accès pour chaque utilisateur appartenant à ce groupe. Reportez-vous à ***Configuration des autorisations d'accès aux ports*** (à la page 153).
5. Configurez la liste de contrôle d'accès IP (IP ACL). Cette fonction limite l'accès au dispositif KX II par le biais de la spécification d'adresses IP. Cette fonction s'applique uniquement aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste de contrôle d'accès IP qui s'applique à toutes les tentatives d'accès au dispositif (et est prioritaire). Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 155). **Facultatif**
6. Cliquez sur OK.

Remarque : plusieurs fonctions d'administration sont disponibles dans MPC et à partir de la console locale de KX II. Elles sont disponibles uniquement pour les membres du groupe par défaut Admin.



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
Device Access While Under CC-SG Management (Accès au dispositif sous la gestion de CC-SG)	Permet aux utilisateurs et aux groupes d'utilisateurs ayant cette autorisation d'accéder directement à KX II à l'aide d'une adresse IP lorsque l'accès local est activé pour le dispositif dans CC-SG. Le dispositif est accessible à partir de la console locale, de la console distante, de MPC, de VKC et de AKC. Lorsque vous accédez à un dispositif directement alors qu'il est géré par CC-SG, l'activité d'accès et de connexion est consignée dans KX II. L'authentification de l'utilisateur est effectuée suivant les paramètres d'authentification de KX II. *Remarque : le groupe d'utilisateurs Admin dispose de cette autorisation par défaut.*
Device Settings (Paramètres du dispositif)	Paramètres réseau, paramètres date/heure, configuration des ports (nom de canal, association d'alimentation), gestion des événements (SNMP, Syslog), configurations de serveur de fichiers du support virtuel.
Diagnostics	Etat d'interface réseau, statistiques de réseau, envoi d'une commande Ping à un hôte, tracer l'itinéraire jusqu'à un hôte, diagnostics de l'unité KX II.
Maintenance	Sauvegarde et restauration de base des données, mise à niveau du firmware, réinitialisation des paramètres usine, redémarrage.
Modem Access (Accès par modem)	Autorisation d'utiliser le modem pour la connexion au dispositif KX II.
PC-Share	Accès simultané à la même cible par plusieurs utilisateurs. Si vous utilisez une configuration multiniveau où un dispositif KX II de base est utilisé pour

Autorisation	Description
	accéder à plusieurs autres dispositifs en niveau, tous les dispositifs doivent partager le même paramètre PC-Share. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.
Sécurité	Certificat SSL, paramètres de sécurité (VM Share, PC-Share), LCA IP.
Gestion des utilisateurs	Gestion des utilisateurs et des groupes, authentification à distance (LDAP/LDAPS/RADIUS), paramètres de connexion. Si vous utilisez une configuration multiniveau où un dispositif KX II de base permet d'accéder à plusieurs autres dispositifs en niveau, les paramètres d'utilisateur, de groupe d'utilisateurs et d'authentification à distance doivent être cohérents à travers tous les dispositifs. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.

Configuration des autorisations d'accès aux ports

Pour chaque port de serveur, vous pouvez spécifier le type d'accès du groupe, ainsi que le type d'accès aux ports du support virtuel et la gestion de l'alimentation. Veuillez noter que le paramètre par défaut de toutes les autorisations est Deny (Refuser).

Port Access (Accès aux ports)	
option	**Description**
Deny (Refuser)	Accès refusé complètement
View (Afficher)	Afficher (mais non interagir avec) le serveur cible connecté.
Control (Contrôler)	Contrôle le serveur cible connecté. Le contrôle doit être affecté au groupe si l'accès du support virtuel et de gestion d'alimentation est également accordé. Pour permettre à tous les utilisateurs d'un groupe de voir les commutateurs KVM ajoutés, un accès Control doit être accordé à chacun. S'ils ne disposent pas de

	cette autorisation et qu'un commutateur KVM est ajouté ultérieurement, ils ne pourront pas le voir. L'accès Control doit être accordé pour que les contrôles associés à l'audio ou aux cartes à puce soient actifs.

VM access (Accès au support virtuel)	
option	**Description**
Deny (Refuser)	L'autorisation d'accès au support virtuel est totalement refusée pour le port.
Read-Only (Lecture seule)	L'accès au support virtuel est limité à l'accès en lecture uniquement.
Read-Write (Lecture-écriture)	Accès total (en lecture, en écriture) au support virtuel.
Power control access (Accès à la gestion d'alimentation)	
option	**Description**
Deny (Refuser)	Refuser la gestion d'alimentation au serveur cible
distant	Autorisation totale de gestion d'alimentation sur un serveur cible

Dans le cas d'un châssis de lames, les autorisations d'accès aux ports contrôleront l'accès aux URL configurées pour ce châssis. Les options sont Deny (Refuser) ou Control (Contrôler). De plus, chaque lame hébergée par le châssis utilise son propre paramètre Port Permissions indépendant.

Si vous utilisez une configuration multiniveau où un dispositif KX II de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, le dispositif en niveau applique des niveaux spécifiques de gestion des ports. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.

Définition des autorisations pour un groupe individuel

Pour configurer des autorisations attribuées à un groupe d'utilisateurs individuel :

1. Localisez le groupe parmi ceux 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) s'ouvre.
3. Sélectionnez les autorisations appropriées.
4. Cliquez sur OK.

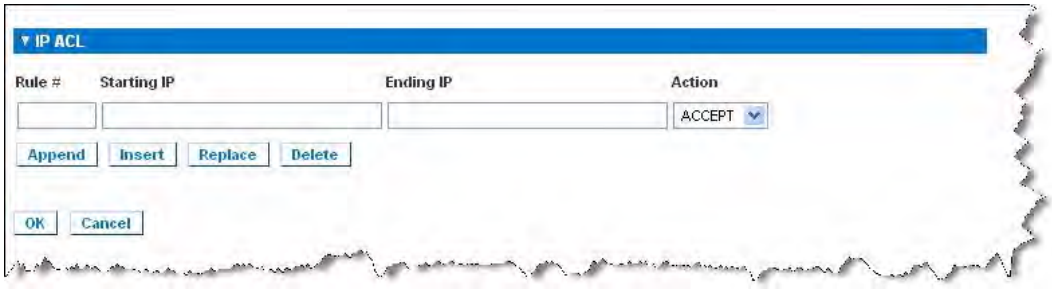
LCA (liste de contrôle d'accès) IP de groupes

Important : soyez prudent lorsque vous utilisez le contrôle d'accès IP applicable à des groupes. L'accès à KX II risque d'être verrouillé si votre adresse IP se trouve dans la plage des adresses à laquelle l'accès a été refusé.

Cette fonction limite à certaines adresses IP l'accès au dispositif KX II pour les utilisateurs appartenant au groupe sélectionné. Elle s'applique uniquement aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste de contrôle d'accès IP qui s'applique à toutes les tentatives d'accès au dispositif, est traitée en premier, et est donc prioritaire).

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de KX II et ne peut pas être verrouillée.

Utilisez la section IP ACL (LCA IP) de la page Group pour ajouter, insérer, remplacer et supprimer les règles de contrôle d'accès au niveau des groupes.



Pour ajouter des règles :

1. Saisissez la première adresse IP dans le champ Starting IP (Adresse IP de départ).

2. Entrez la dernière adresse IP dans le champ Ending IP (Adresse IP de fin).
3. Choisissez l'action à effectuer dans la liste des options disponibles :
   - Accept - Les adresses IP paramétrées sur Accept sont autorisées à accéder au dispositif KX II.
   - Drop - Les adresses IP paramétrées sur Drop ne sont pas autorisées à accéder au dispositif KX II.
4. Cliquez sur Append (Ajouter). La règle est ajoutée au bas de la liste des règles. Répétez les étapes 1 à 4 pour chacune des règles à entrer.

Pour insérer une règle :

1. Entrez un numéro de règle (#). Ce numéro est requis lorsque vous utilisez la commande Insert (Insérer).
2. Renseignez les champs Starting IP et Ending IP.
3. Choisissez une option dans la liste déroulante Action.
4. Cliquez sur Insert (Insérer). Si le numéro de règle que vous venez d'entrer est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont descendues d'un rang.

Pour remplacer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez remplacer.
2. Renseignez les champs Starting IP et Ending IP.
3. Choisissez une option dans la liste déroulante Action.
4. Cliquez sur Replace (Remplacer). Votre nouvelle règle remplace la règle d'origine dont elle conserve le numéro.

Pour supprimer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).
3. Lorsque 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 présenté ici, les deux règles LCA étaient inversées, Dominion n'accepterait aucune communication.

Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP

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

Modification d'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 Group, modifiez les champs appropriés et définissez les autorisations adéquates.
2. Définissez les permissions pour le groupe. Cochez les cases situées en regard des permissions que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à ***Configuration des autorisations*** (à la page 152).
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 ***Configuration des autorisations d'accès aux ports*** (à la page 153).
4. Configurez la liste de contrôle d'accès IP (IP ACL) (facultatif). Cette fonction limite l'accès au dispositif KX II par le biais de la spécification d'adresses IP. Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 155).
5. Cliquez sur OK.

Pour supprimer un groupe d'utilisateurs :

Important : si vous supprimez un groupe contenant des utilisateurs, ces derniers sont automatiquement affectés au groupe d'utilisateurs <unknown> (inconnu).

Conseil : pour déterminer quels utilisateurs appartiennent à un groupe particulier, triez la User List (Liste des utilisateurs) par User Group (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 Delete (Supprimer).
3. Lorsque vous êtes invité à confirmer la suppression, cliquez sur OK.

Utilisateurs

Les utilisateurs doivent disposer de noms d'utilisateur et de mots de passe pour accéder à KX II. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité KX II. Vous pouvez créer jusqu'à 254 utilisateurs pour chaque groupe.

Si vous utilisez une configuration multiniveau où un dispositif KX II de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, les utilisateurs auront besoin d'autorisations d'accès au dispositif de base et à chaque dispositif en niveau (selon les besoins). Lorsqu'un utilisateur se connecte au dispositif de base, chaque dispositif en niveau est interrogé et l'utilisateur peut accéder à chaque serveur cible pour lequel il dispose d'autorisations. Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.

Affichage de la liste des utilisateurs de KX II

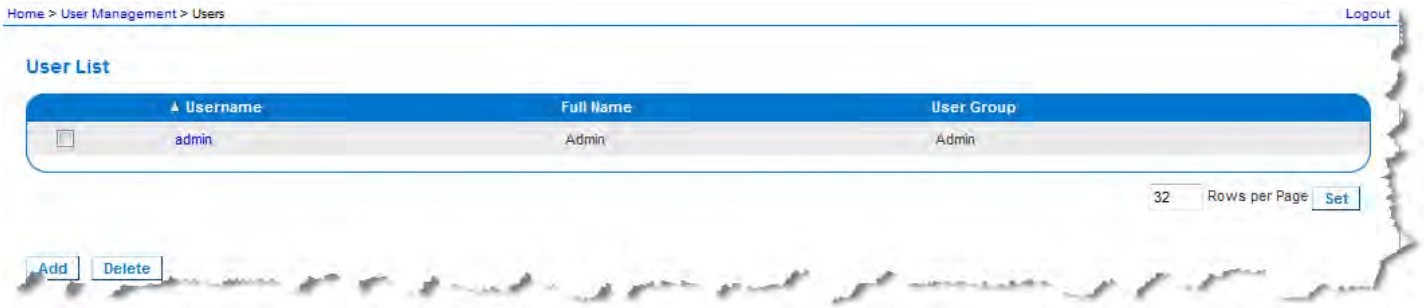
La page User List (Liste des utilisateurs) affiche une liste de tous les utilisateurs, avec leur nom d'utilisateur, leur nom complet et le groupe d'utilisateurs auquel ils appartiennent. Pour trier cette liste en fonction d'une colonne, cliquez sur le nom de celle-ci. A partir de la page User List, vous pouvez ajouter, modifier ou supprimer des utilisateurs.

Les utilisateurs KX II disposant de privilèges User Management (Gestion des utilisateurs) peuvent déconnecter d'autres utilisateurs des ports ou forcer leur déconnexion le cas échéant. Reportez-vous à ***Déconnexion d'utilisateurs des ports*** (à la page 159) et ***Fermeture de la session des utilisateurs de KX II (Déconnexion forcée)*** (à la page 160) respectivement.

Pour afficher les ports cible auxquels chaque utilisateur est connecté, reportez-vous à ***Affichage des utilisateurs par port*** (à la page 159).

Pour afficher la liste des utilisateurs :

- Sélectionnez User Management (Gestion des utilisateurs) > User List (Liste des utilisateurs). La page User List (Liste des utilisateurs) s'ouvre.



Affichage des utilisateurs par port

La page Users By Port (Utilisateurs par port) répertorie tous les utilisateurs locaux et distants authentifiés et les ports auxquels ils sont connectés. Seules les connexions permanentes aux ports sont recensées. Les ports auxquels on accède par balayage ne sont pas indiqués.

Si un même utilisateur est connecté depuis plusieurs clients, son nom d'utilisateur apparaît sur la page pour chaque connexion établie. S'il s'est connecté, par exemple, depuis deux (2) clients différents, son nom est indiqué deux fois.

Cette page contient les données d'utilisateur et de port suivantes :

- Port Number - numéro affecté au port auquel l'utilisateur est connecté.
- Port Number - nom affecté au port auquel l'utilisateur est connecté.

  Remarque : si l'utilisateur n'est pas connecté à une cible, Local Console ou Remote Console (Console distante) apparaît sous le nom du port.

- Username - nom d'utilisateur servant aux connexions d'utilisateur et de cible.
- Access From - adresse IP de KX II auquel l'utilisateur accède.
- Status - statut actuel de la connexion, Active ou Inactive.

Pour afficher les utilisateurs par port :

- Sélectionnez User Management > Users by Port (Gestion des utilisateurs > Utilisateurs par port). La page Users by Port s'ouvre.

Déconnexion d'utilisateurs des ports

Cette opération permet de déconnecter les utilisateurs du port cible mais sans fermer leur session KX II.

Remarque : la fermeture de session déconnecte l'utilisateur du port cible et de KX II. Reportez-vous à **Fermeture de la session des utilisateurs de KX II (Déconnexion forcée)** *(à la page 160) pour en savoir plus sur la déconnexion forcée des utilisateurs.*

Pour déconnecter des utilisateurs d'un port :

1. Sélectionnez User Management > Users by Port (Gestion des utilisateurs > Utilisateurs par port). La page Users by Port s'ouvre.
2. Cochez la case en regard du nom de l'utilisateur que vous souhaitez déconnecter de la cible.
3. Cliquez sur Disconnect User from Port (Déconnecter l'utilisateur du port).

4. Cliquez sur OK dans le message de confirmation pour déconnecter l'utilisateur.
5. Un message de confirmation indique que l'utilisateur est déconnecté.

Fermeture de la session des utilisateurs de KX II (Déconnexion forcée)

Si vous êtes administrateur, vous pouvez fermer la session d'un autre utilisateur authentifié localement qui est connecté à KX II. Les utilisateurs peuvent également être déconnectés au niveau du port. Reportez-vous à ***Déconnexion d'utilisateurs des ports*** (à la page 159).

Pour fermer la session d'un utilisateur de KX II :

1. Sélectionnez User Management > Users by Port (Gestion des utilisateurs > Utilisateurs par port). La page Users by Port s'ouvre.
2. Cochez la case en regard du nom de l'utilisateur que vous souhaitez déconnecter de la cible.
3. Cliquez sur Force User Logoff (Forcer la déconnexion de l'utilisateur).
4. Cliquez sur OK dans le message de confirmation Logoff User.

Ajout d'un nouvel utilisateur

Il est recommandé de définir les groupes d'utilisateurs avant de créer des utilisateurs KX II, car lorsque vous ajoutez un utilisateur, vous devez l'affecter à un groupe d'utilisateurs existant. Reportez-vous à **Ajout d'un nouveau groupe d'utilisateurs** (à la page 150).

Vous pouvez ajouter de nouveaux utilisateurs, modifier leurs informations et réactiver des utilisateurs sur la page User.

Remarque : un nom d'utilisateur peut être désactivé lorsque le nombre de tentatives de connexion qui ont échoué a atteint la limite définie dans la page Security Settings (Paramètres de sécurité). Reportez-vous à **Paramètres de sécurité** *(voir "***Security Settings (Paramètres de sécurité)***" à la page 262).*

Pour ajouter un nouvel utilisateur :

1. Sélectionnez User Management > Add New User (Gestion des utilisateurs > Ajouter un nouvel utilisateur) ou cliquez sur Add (Ajouter) dans la page User List (Liste des utilisateurs).
2. Tapez un nom unique dans le champ Username (Nom d'utilisateur) (16 caractères au maximum).
3. Tapez le nom complet de la personne dans le champ Full Name (Nom complet) (64 caractères au maximum).

4. Tapez un mot de passe dans le champ Password, puis entrez-le à nouveau dans le champ Confirm Password (Confirmer le mot de passe) (64 caractères au maximum).
5. Choisissez un groupe dans la liste déroulante User Group (Groupe d'utilisateurs).

   Si vous ne souhaitez pas affecter cet utilisateur à un groupe d'utilisateurs existant, sélectionnez Individual Group (Groupe individuel) dans la liste déroulante. Pour plus d'informations sur les autorisations associées à un groupe individuel, reportez-vous à ***Définition des autorisations pour un groupe individuel*** (à la page 155).
6. Pour activer le nouvel utilisateur, laissez la case Active cochée. Cliquez sur OK.

Modification d'un utilisateur existant

Pour modifier un utilisateur existant :

1. Ouvrez la page User List (Liste des utilisateurs) en choisissant User Management (Gestion des utilisateurs) > User List.
2. Localisez l'utilisateur parmi ceux répertoriés sur la page User List.
3. Cliquez sur le nom d'utilisateur. La page User (Utilisateur) s'ouvre.
4. Sur la page User (Utilisateur), modifiez les champs appropriés. Reportez-vous à ***Ajout d'un nouvel utilisateur*** (à la page 160) pour plus d'informations sur les méthodes d'accès à la page User.
5. Pour supprimer un utilisateur, cliquez sur Delete. Vous êtes invité à confirmer la suppression.
6. Cliquez sur OK.

Paramètres d'authentification

L'authentification est un processus qui consiste à vérifier l'identité d'un utilisateur. Une fois l'utilisateur authentifié, son groupe permet de déterminer ses autorisations d'accès aux ports et au système. Les droits accordés à l'utilisateur déterminent le type d'accès autorisé. Cela s'appelle l'autorisation.

Lorsque KX II est configuré pour l'authentification à distance, le serveur d'authentification externe est utilisé principalement à des fins d'authentification et non d'autorisation.

Si vous utilisez une configuration multiniveau où un dispositif KX II de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, le dispositif de base et les dispositifs en niveau doivent utiliser les mêmes paramètres d'authentification.

Sur la page Authentication Settings (Paramètres d'authentification), vous pouvez configurer le type d'authentification utilisé pour l'accès à KX II.

Remarque : lorsque l'authentification à distance (LDAP/LDAPS ou RADIUS) est sélectionnée, si l'utilisateur est introuvable, la base de données d'authentification locale est également vérifiée.

Pour configurer l'authentification :

1. Choisissez User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification). La page Authentication Settings s'ouvre :
2. Choisissez le protocole d'authentification que vous souhaitez utiliser (Local Authentication [Authentification locale], LDAP/LDAPS ou RADIUS). L'option LDAP active les champs LDAP restants ; l'option RADIUS active les champs RADIUS restants.
3. Si vous sélectionnez Local Authentication (Authentification locale), passez à l'étape 6.
4. Si vous sélectionnez LDAP/LDAPS, lisez la section intitulée Implémentation de l'authentification à distance LDAP pour obtenir des informations sur la façon de renseigner les champs dans la section LDAP de la page Authentication Settings (Paramètres d'authentification).
5. Si vous sélectionnez RADIUS, lisez la section intitulée Implémentation de l'authentification à distance RADIUS pour obtenir des informations sur la façon de renseigner les champs dans la section RADIUS de la page Authentication Settings (Paramètres d'authentification).
6. Cliquez sur OK pour enregistrer.

Pour réinitialiser les paramètres par défaut usine :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Implémentation de l'authentification à distance LDAP/LDAPS

LDAP (Lightweight Directory Access Protocol, protocole allégé d'accès à un annuaire) est un protocole de mise en réseau pour la recherche et la modification de services d'annuaires fonctionnant sur TCP/IP. Un client démarre une session LDAP en se connectant à un serveur LDAP/LDAPS (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 serveur d'authentification LDAP/LDAPS.

Pour utiliser le protocole d'authentification LDAP :

1. Cliquez sur User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification) pour ouvrir la page Authentication Settings.
2. Sélectionnez le bouton radio LDAP pour activer la section LDAP de la page.
3. Cliquez sur l'icône 

pour développer la section LDAP de la page.

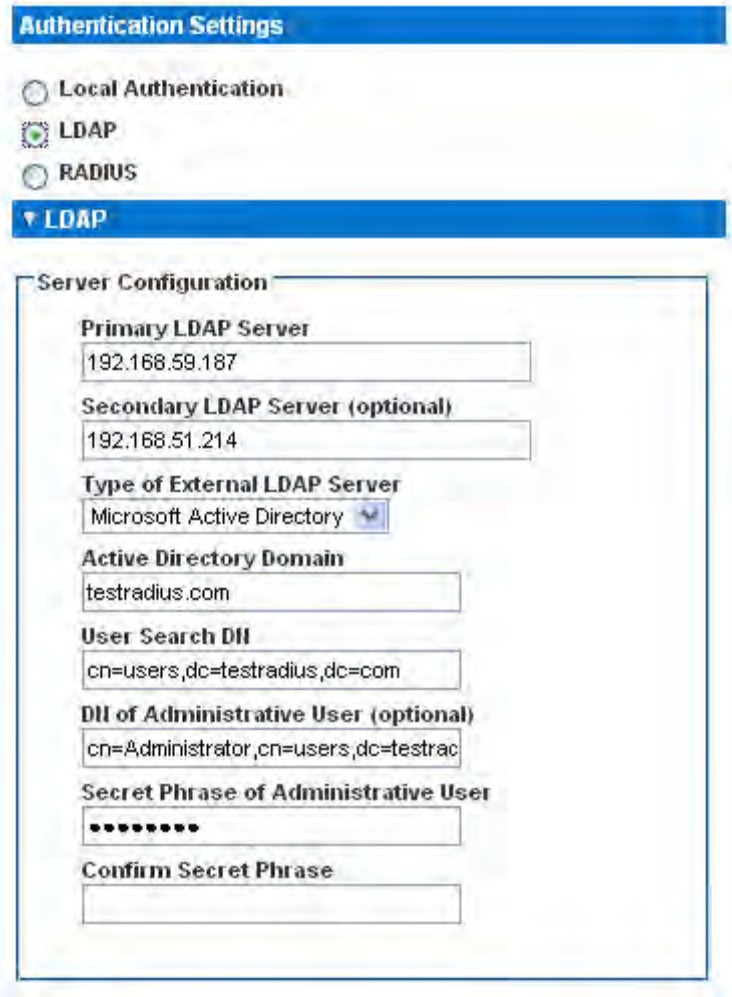
   Configuration du serveur

4. Dans le champ Primary LDAP Server (Serveur LDAP principal), entrez l'adresse IP ou le nom DNS de votre serveur d'authentification à distance LDAP/LDAPS (256 caractères au plus). Lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée avec l'option Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS), le nom DNS doit être utilisé pour vérifier le certificat du serveur LDAP du CN.
5. Dans le champ Secondary LDAP Server (Serveur LDAP secondaire), entrez l'adresse IP ou le nom DNS de votre serveur de sauvegarde LDAP/LDAPS (256 caractères au plus). Lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) sélectionnée, le nom DNS doit être utilisé. Notez que les champs restants comportent les mêmes paramètres que le champ Primary LDAP Server. **Facultatif**
6. Type de serveur LDAP externe.
7. Sélectionnez le serveur LDAP/LDAPS externe. Sélectionnez-le parmi les options disponibles :
   - Serveur LDAP générique.

- Microsoft Active Directory. Active Directory est une implémentation des services d'annuaires LDAP/LDAPS par Microsoft à utiliser dans les environnements Windows.

8. Entrez le nom du domaine Active Directory si vous avez sélectionné Microsoft Active Directory. Par exemple, *acme.com*. Consultez l'administrateur Active Directory pour obtenir un nom de domaine spécifique.
9. Dans le champ User Search DN (ND de recherche d'utilisateur), entrez le ND de l'emplacement dans la base de données LDAP où la recherche d'informations d'utilisateur doit commencer. Vous pouvez entrer jusqu'à 64 caractères. Exemple de valeur de recherche de base : `cn=Users,dc=raritan,dc=com`. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ces champs.
10. Entrez le Distinguished Name de l'utilisateur administratif dans le champ DN of Administrative User (64 caractères au plus). Renseignez ce champ si votre serveur LDAP autorise uniquement les administrateurs à rechercher des informations d'utilisateur à l'aide du rôle Administrative User. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ce champ. Exemple de valeur de ND d'utilisateur administratif : `cn=Administrator,cn=Users,dc=testradius,dc=com`. **Facultatif**

11. Si vous avez entré un Distinguished Name pour l'utilisateur administratif, vous devez entrer le mot de passe qui sera utilisé pour authentifier le ND de l'utilisateur administratif par comparaison avec le serveur d'authentification à distance. Entrez le mot de passe dans le champ Secret Phrase (Expression secrète) et à nouveau dans le champ Confirm Secret Phrase (Confirmer l'expression secrète) (128 caractères au plus).



LDAP/LDAP Secure (LDAP/LDAP sécurisé)

12. Cochez la case Enable Secure LDAP (Activer le LDAP sécurisé) si vous souhaitez utiliser SSL. Ceci coche la case Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS). SSL (Secure Sockets Layer) est un protocole cryptographique qui permet à KX II de communiquer en toute sécurité avec le serveur LDAP/LDAPS.
13. Le port par défaut est 389. Utilisez le port LDAP TCP standard ou spécifiez un autre port.

14. Le port LDAP sécurisé par défaut est 636. Utilisez le port par défaut ou spécifiez un autre port. Ce champ est utilisé uniquement lorsque la case Enable Secure LDAP (Activer le LDAP sécurisé) est cochée.
15. Cochez la case Enable LDAPS Server Certificate Validation afin d'utiliser le fichier de certificat de l'autorité de certification (AC) racine téléversé précédemment pour valider le certificat fourni par le serveur. Si vous ne souhaitez pas utiliser le fichier de certificat, désactivez la case à cocher. Désactiver cette fonction revient à accepter un certificat signé par une autorité de certification inconnue. Cette case à cocher est uniquement disponible lorsque la case Enable Secure LDAP est cochée.

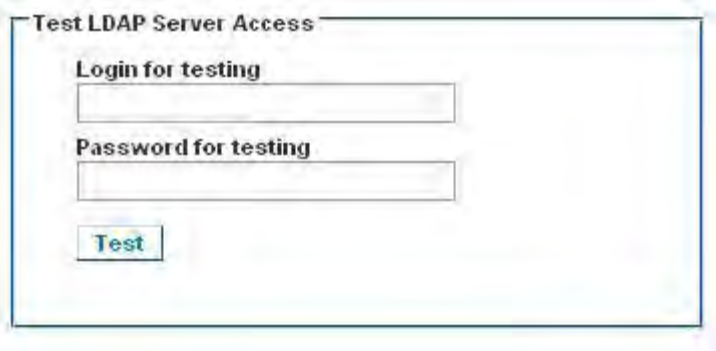
Remarque : lorsque l'option Enable LDAPS Server Certificate Validation est sélectionnée, outre l'utilisation du certificat de l'AC racine pour la validation, le nom d'hôte du serveur doit correspondre au nom commun fourni dans le certificat du serveur.

16. Le cas échéant, téléversez le fichier de certificat de l'AC racine. Ce champ est activé lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée. 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/LDAPS. Utilisez Browse (Parcourir) pour accéder au fichier du certificat. Si vous remplacez un certificat pour un serveur LDAP/LDAPS par un nouveau, vous devez redémarrer KX II pour que ce nouveau certificat prenne effet.

Test LDAP Server Access (Test de l'accès à un serveur LDAP)

17. KX II permet de tester la configuration LDAP dans la page Authentication Settings (Paramètres d'authentification) à cause de la difficulté à configurer correctement le serveur LDAP et KX II pour l'authentification à distance. Pour tester la configuration LDAP, entrez le nom et le mot de passe de connexion dans les champs Login for testing (Nom de connexion pour le test) et Password for testing (Mot de passe pour le test) respectivement. Il s'agit des nom d'utilisateur et de mot de passe entrés pour accéder à KX II et que le serveur LDAP utilisera pour vous authentifier. Cliquez sur Test.

    Une fois le test terminé, un message s'affiche pour indiquer si le test a réussi ou s'il a échoué, un message d'erreur détaillé apparaît. Un message de réussite ou détaillé d'erreur, en cas d'échec, apparaît. Il donne également des informations de groupe extraites du serveur LDAP distant pour l'utilisateur du test en cas de réussite.



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

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 sur le 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.

IMPORTANT : si vous êtes déjà client de Raritan, Inc. et que vous avez configuré le serveur Active Directory en modifiant le schéma AD, KX II continue de prendre 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/LDAPS, reportez-vous à *Mise à jour du schéma LDAP* (à la page 381).

Pour activer le serveur AD sur KX II :

1. A l'aide de KX II, créez des groupes spéciaux et attribuez-leur les autorisations et privilèges appropriés. Par exemple, créez des groupes tels que KVM_Admin et KVM_Operator.

2. Sur le serveur Active Directory, créez des groupes portant le même nom qu'à l'étape précédente.
3. Sur votre serveur AD, affectez les utilisateurs de l'unité KX II aux groupes créés au cours de l'étape 2.
4. A partir de KX II, activez et configurez le serveur AD comme il se doit. Reportez-vous à ***Implémentation de l'authentification à distance LDAP/LDAPS*** (à la page 163).

Remarques importantes :

- Le nom de groupe est sensible à la casse.
- KX II fournit les groupes par défaut suivants qui ne peuvent pas être modifiés ni supprimés : Admin et <Unknown (Inconnu)>. Vérifiez que le serveur Active Directory n'utilise pas les mêmes noms de groupe.
- Si les informations de groupe renvoyées par le serveur Active Directory ne correspondent pas à une configuration de groupe KX II, ce dernier attribue automatiquement le groupe <Unknown> (Inconnu) aux utilisateurs qui ont réussi à s'authentifier.
- Si vous utilisez un numéro de rappel, vous devez entrer la chaîne sensible à la casse suivante : *msRADIUSCallbackNumber.*
- D'après les recommandations de Microsoft, il vaut mieux utiliser les groupes globaux avec les comptes d'utilisateurs, non les groupes locaux de domaines.

Implémentation de l'authentification à distance RADIUS

RADIUS (Remote Authentication Dial-in User Service) est un protocole d'authentification, d'autorisation et de gestion destiné aux applications d'accès aux réseaux.

Pour utiliser le protocole d'authentification RADIUS :

1. Cliquez sur User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification) pour ouvrir la page Authentication Settings.
2. Cliquez sur le bouton radio RADIUS pour activer la section RADIUS de la page.
3. Cliquez sur l'icône 

pour développer la section RADIUS de la page.
4. Dans les champs Primary Radius Server (Serveur Radius principal) et Secondary Radius Server (Serveur Radius secondaire), entrez l'adresse IP des serveurs d'authentification à distance principal et secondaire facultatif, respectivement (256 caractères au plus).
5. Dans les champs Shared Secret (Secret partagé), entrez le secret du serveur utilisé pour l'authentification (128 caractères au plus).

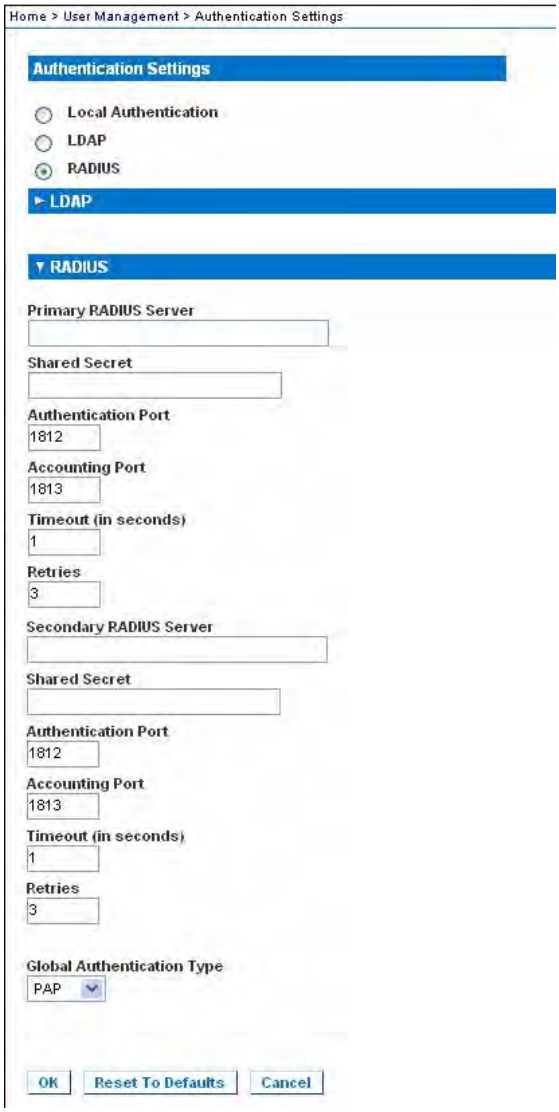
Le secret partagé est constitué d'une chaîne de caractères devant être connus à la fois par KX II et le serveur RADIUS afin de leur permettre de communiquer en toute sécurité. C'est en fait un mot de passe.

6. La valeur par défaut Authentication Port (Port d'authentification) est 1812 mais peut être modifiée si nécessaire.
7. La valeur par défaut Accounting Port (Port de gestion) est 1813 mais peut être modifiée si nécessaire.
8. La valeur Timeout (Délai d'attente) est enregistrée en secondes et le délai d'attente par défaut est 1 seconde, mais peut être modifiée si nécessaire.

   Le délai d'attente correspond au laps de temps utilisé par KX II pour obtenir une réponse du serveur RADIUS avant d'envoyer une autre requête d'authentification.
9. Le nombre de tentatives par défaut est 3.

   Il s'agit du nombre de tentatives accordées à KX II pour envoyer une requête d'authentification au serveur RADIUS.
10. Sélectionnez une option dans la liste déroulante Global Authentication Type (Type d'authentification globale) :
    - PAP - Avec le protocole PAP, les mots de passe sont envoyés en texte brut. Le protocole 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 - Avec le protocole CHAP, l'authentification peut être demandée par le serveur à tout moment. Le protocole CHAP est plus sûr que le protocole PAP.



Cisco ACS 5.x pour l'authentification RADIUS

Si vous utilisez un serveur Cisco ACS 5.x, effectuez les opérations suivantes sur celui-ci après avoir configuré KX II pour l'authentification RADIUS.

Remarque : les opérations suivantes incluent les menus et les options Cisco utilisés pour accéder à chaque page. Reportez-vous à la documentation Cisco pour obtenir les informations les plus récentes sur chaque opération et plus de détails sur leur exécution.

- Ajoutez KX II en tant que client AAA (**obligatoire**) - Network Resources > Network Device Group > Network Device and AAA Clients (Ressources réseau > Groupe de dispositifs réseau > Dispositif réseau et clients AAA).
- Ajoutez/modifiez les utilisateurs (**obligatoire**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users (Ressources réseau > Utilisateurs et magasins d'identités > Magasins d'identités internes > Utilisateurs).
- Configurez l'accès réseau par défaut pour activer le protocole CHAP (**facultatif**) - Policies > Access Services > Default Network Access (Stratégies > Services d'accès > Accès réseau par défaut).
- Créez des règles de stratégie d'autorisation pour contrôler l'accès (**obligatoire**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles (Eléments de stratégie > Autorisation et permissions > Accès réseau > Profils d'autorisation).
  - Type de dictionnaire : RADIUS-IETF
  - Attribut RADIUS : Filter-ID
  - Type d'attribut : Chaîne
  - Attribute Value: Raritan:G{KVM_Admin} (où KVM_Admin est le nom du groupe créé localement sur le commutateur KVM Dominion KVM). Sensible à la casse.
- Configurez les conditions de sessions (date et heure) (**obligatoire**) - Policy Elements > Session Conditions > Date and Time (Eléments de stratégie > Conditions de session > Date et heure).
- Configurez/créez la stratégie d'autorisation d'accès réseau (**obligatoire**) - Access Policies > Access Services > Default Network Access>Authorization (Stratégies d'accès > Services d'accès > Accès réseau par défaut > Autorisation).

Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS

Lorsqu'une demande d'authentification RADIUS est acceptée, KX II détermine les autorisations accordées à un utilisateur donné en fonction des autorisations du groupe auquel il appartient.

Votre serveur RADIUS distant peut fournir ces noms de groupes d'utilisateurs en retournant un attribut, implémenté comme FILTER-ID (ID FILTRE) RADIUS. Le format du FILTER-ID (ID FILTRE) doit être le suivant : Raritan:G{*NOM_GROUPE*} où *NOM_GROUPE* est une chaîne indiquant le nom du groupe auquel l'utilisateur appartient.

```
Raritan:G{NOM_GROUPE}:D{Numéro de rappel}
```

ou NOM_GROUPE est une chaîne indiquant le nom du groupe auquel appartient l'utilisateur et Numéro de rappel est le numéro associé au compte de l'utilisateur dont le modem KX II se servira pour rappeler le compte de l'utilisateur.

Spécifications des échanges de communication RADIUS

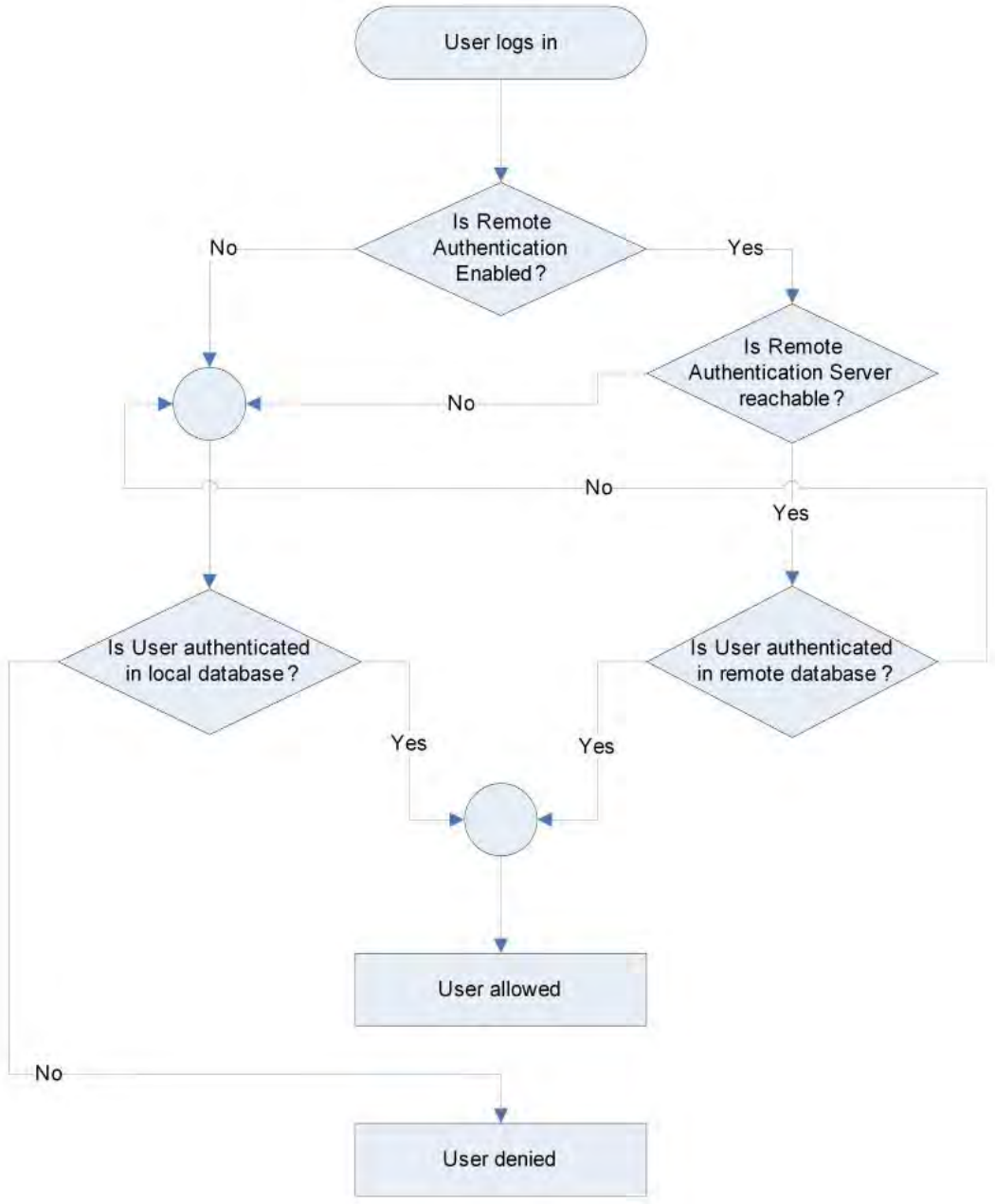
KX II envoie les attributs RADIUS suivants à votre serveur RADIUS :

Attribut	Données
Connexion	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-IP-Address (4)	Adresse IP de KX II.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.
User-Password(2)	Mot de passe chiffré.
Accounting-Request(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 (4)	Adresse IP de KX II.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Attribut Déconnexion	Données
Accounting-Request(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 (4)	Adresse IP de KX II.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Processus d'authentification de l'utilisateur

L'authentification à distance suit le processus défini dans le diagramme ci-dessous :

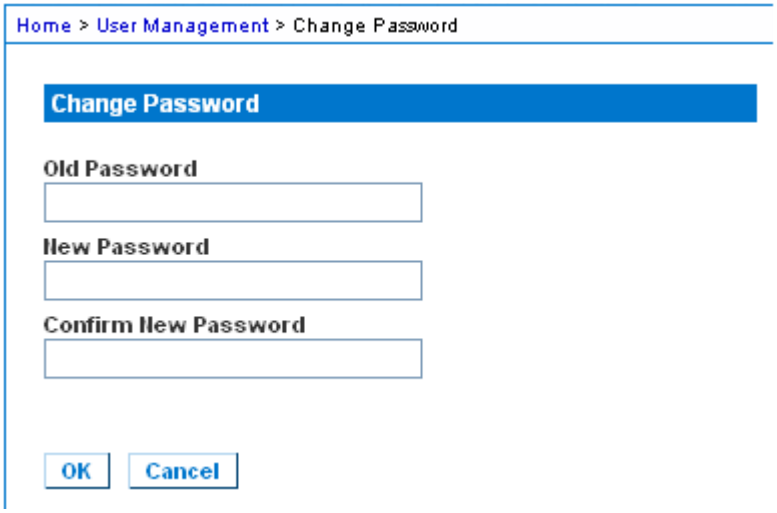


Modification d'un mot de passe

Pour modifier votre mot de passe :

1. Sélectionnez User Management (Gestion des utilisateurs) > Change Password (Modifier le mot de passe). La page Change Password (Modifier le mot de passe) s'ouvre.
2. Entrez 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. Retapez-le dans le champ Confirm New Password (Confirmer le nouveau mot de passe). Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques et caractères spéciaux (présents sur un clavier anglais).
4. Cliquez sur OK.
5. Vous recevrez confirmation que le mot de passe a bien été changé. Cliquez sur OK.

Remarque : si des mots de passe sécurisés sont utilisés, cette page affiche des informations sur le format requis pour ces mots de passe. Pour plus d'informations sur les mots de passe et les mots de passe sécurisés, reportez-vous à **Mots de passe sécurisés** *(à la page 265).*



Chapitre 8 Gestion des dispositifs

Dans ce chapitre

Paramètres réseau

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

Deux options permettent de paramétrer votre configuration IP :

- None (Néant) (valeur par défaut) : il s'agit de l'option recommandée (IP statique). Comme 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 : avec cette option, l'adresse IP est automatiquement attribuée par un serveur DHCP.

Pour modifier la configuration de réseau :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Mettez à jour les paramètres réseau de base. Reportez-vous à ***Paramètres réseau de base*** (à la page 177).
3. Mettez à jour les paramètres relatifs à l'interface LAN. Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 180).
4. Cliquez sur OK pour confirmer ces configurations. Si vos modifications nécessitent le redémarrage du dispositif, un message de redémarrage apparaît.

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Paramètres réseau de base

Ces procédures décrivent comment affecter une adresse IP sur la page Network Settings (Paramètres réseau). Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à ***Paramètres réseau*** (à la page 176).

Pour affecter une adresse IP :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Indiquez un nom de dispositif significatif pour votre unité KX II. 32 caractères alphanumériques au plus, avec des caractères spéciaux valides et aucun espace.
3. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :
   a. Entrez l'adresse IP si nécessaire. L'adresse IP par défaut est 192.168.0.192.
   b. Entrez le masque de sous-réseau. Le masque de sous-réseau par défaut est 255.255.255.0.
   c. Entrez la passerelle par défaut si None (Néant) est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).
   d. Entrez le nom d'hôte DHCP préféré si DHCP est sélectionné dans la liste déroulante IP Auto Configuration (Configuration IP automatique).
   e. Sélectionnez la configuration IP automatique. Les options suivantes sont disponibles :
   - None (Static IP) (Néant (IP statique)) : cette option nécessite que vous indiquiez manuellement les paramètres réseau.

     Cette option est recommandée car KX II est un dispositif d'infrastructure et son adresse IP ne doit pas être modifiée.
   - 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.

     Avec cette option, les paramètres réseau sont attribués par le serveur DHCP. Si DHCP est utilisé, entrez le nom d'hôte préféré (DHCP uniquement). Maximum de 63 caractères.
4. Si IPv6 doit être utilisé, entrez ou sélectionnez les paramètres réseau spécifiques à IPv6 appropriés dans la section IPv6 :
   a. Cochez la case IPv6 pour activer les champs de la section.
   b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à KX II.

c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.

d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).

e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**

f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

g. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Néant) - 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.

  Lorsqu'elle est sélectionnée pour la configuration IP automatique, les champs Network Basic Settings (Paramètres réseau de base) sont activés : Global/Unique IP Address (Adresse IP globale/unique), Prefix Length (Longueur de préfixe) et Gateway IP Address (Adresse IP de la passerelle). Vous pouvez paramétrer manuellement la configuration IP.

- Router Discovery (Détection de routeur) - Utilisez cette option pour affecter automatiquement des adresses IPv6 ayant une portée « Global » ou « Unique Local » au-delà des adresses « Link Local » qui ne s'appliquent qu'à un sous-réseau connecté directement.

5. Si l'option DHCP est activée et que le champ Obtain DNS Server Address Automatically (Obtenir l'adresse du serveur DNS automatiquement) est accessible, sélectionnez-le. Les données DNS fournies par le serveur DHCP seront alors utilisées.

6. Si l'option Use the Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée, que DHCP soit sélectionné ou non, les adresses saisies dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les données suivantes si l'option Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée. Il s'agit des adresses DNS primaire et secondaire qui seront utilisées si la connexion au serveur DNS primaire est perdue lors d'une panne.

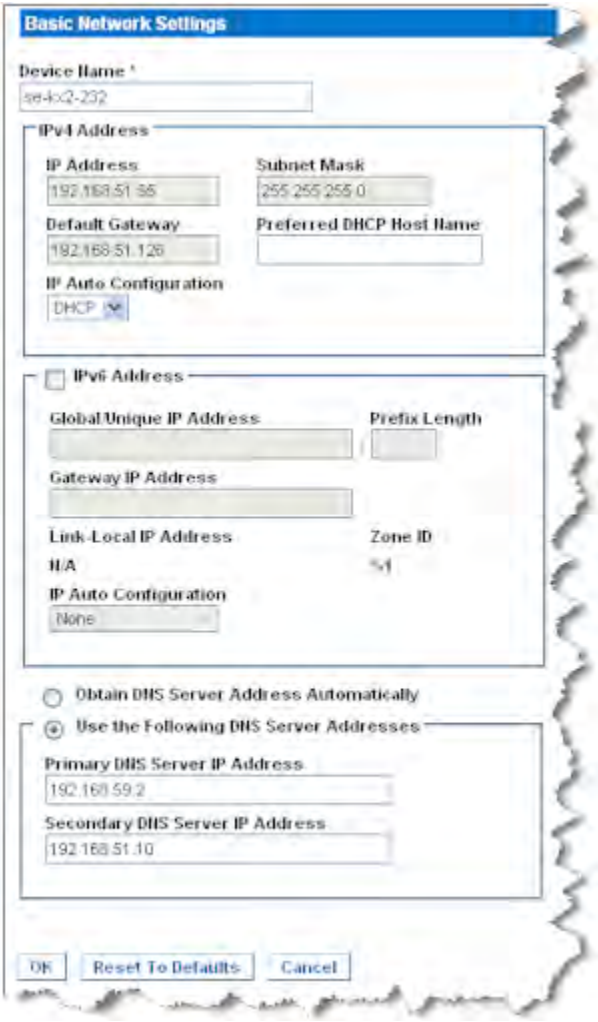
   a. Adresse IP du serveur DNS primaire

   b. Adresse IP du serveur DNS secondaire.

7. Lorsque vous avez terminé, cliquez sur OK.

Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 180) pour plus d'informations sur la configuration de cette section de la page Network Settings (Paramètres réseau).

Remarque : dans certains environnements, le paramètre par défaut du champ LAN Interface Speed & Duplex (Vitesse d'interface LAN & Duplex), Autodetect (auto-détection), ne définit pas correctement les paramètres réseau, ce qui entraîne des problèmes sur le réseau. Dans ce cas, paramétrez le champ LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN) de KX II sur 100 Mbps/Full Duplex (Bidirectionnel simultané) (ou toute option appropriée à votre réseau) pour résoudre le problème. Reportez-vous à la page **Paramètres réseau** *(à la page 176) pour plus d'informations.*



Paramètres de l'interface LAN

Les paramètres actuels sont identifiés dans le champ Current LAN interface parameters (Paramètres actuels de l'interface LAN).

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Renseignez le champ LAN Interface Speed & Duplex (Vitesse et duplex de l'interface LAN) en sélectionnant une des options suivantes :
   - Autodetect (Détection automatique) (option par défaut)
   - 10 Mbps/Half - Les deux témoins clignotent.
   - 10 Mbps/Full - Les deux témoins clignotent.
   - 100 Mbps/Half - Le témoin jaune clignote.
   - 100 Mbps/Full - Le témoin jaune clignote.
   - 1000 Mbps/Full (gigabit) - Le témoin vert clignote.
   - 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 Mbps en half duplex ou en full duplex. Dans ce cas, essayez un autre paramètre de vitesse et de duplex.

   Reportez-vous à ***Paramètres de vitesse réseau*** (à la page 364) pour plus d'informations.
3. Cochez la case Enable Automatic Failover (Activer le basculement automatique) pour permettre à KX II de récupérer automatiquement sa connexion réseau via un second port réseau en cas de panne du port réseau actif.

   Remarque : les ports de basculement n'étant pas activés avant un basculement effectif, Raritan recommande de ne pas surveiller ces ports ou de le faire après un basculement.

   Lorsque cette option est activée, les deux champs ci-après sont utilisés :
   - Ping Interval (seconds) - L'intervalle ping détermine la fréquence à laquelle KX II vérifie l'état du chemin réseau d'accès à la passerelle désignée. L'intervalle ping par défaut est de 30 secondes.
   - Timeout (seconds) - La temporisation détermine la durée pendant laquelle une passerelle désignée reste injoignable via la connexion réseau avant qu'un basculement ne se produise.

Remarque : l'intervalle ping et la temporisation peuvent être configurés pour répondre au mieux aux conditions du réseau local. La temporisation doit être définie pour permettre la transmission de deux demandes ping au moins et le retour des réponses. Par exemple, si une fréquence élevée de basculement est observée en raison d'une utilisation importante du réseau, la temporisation doit être prolongée pour atteindre trois ou quatre fois l'intervalle ping.

4. Sélectionnez la bande passante.
5. Cliquez sur OK pour appliquer les paramètres LAN.

Services du dispositif

La page Device Services vous autorise à configurer les fonctions suivantes :

- activer l'accès SSH
- activer la fonction multiniveau pour le KX II de base
- entrer le port de détection
- activer l'accès direct aux ports
- activer la fonction de validation du certificat du serveur de téléchargement AKC si vous utilisez AKC

Activation de SSH

Activez l'accès SSH pour permettre aux administrateurs d'accéder à KX II via l'application SSH v2.

Pour activer l'accès SSH :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Cochez la case Enable SSH Access.
3. Renseignez le champ SSH Port. Le numéro de port TCP SSH standard est 22 mais ce numéro peut être changé pour offrir un niveau supérieur d'opérations de sécurité.
4. Cliquez sur OK.

Paramètres des ports HTTP et HTTPS

Vous pouvez configurer les ports HTTP et/ou HTTPS utilisés par l'unité KX II. Par exemple, si vous utilisez le port HTTP 80 par défaut pour autre chose, le remplacement du port garantit que le dispositif ne tentera pas de l'utiliser.

Pour modifier les paramètres des ports HTTP et/ou HTTPS :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Entrez les nouveaux ports dans les champs HTTP Port et/ou HTTPS Port.
3. Cliquez sur OK.

Saisie du port de détection

La détection de KX II s'effectue sur un port TCP unique et configurable. Le port par défaut est le port 5000 mais vous pouvez configurer ce paramètre de manière à utiliser le port TCP de votre choix à l'exception des ports 80 et 443. Pour accéder à 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 autre port configuré ici.

Pour activer le port de détection :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Renseignez le champ Discovery Port (Port de détection).
3. Cliquez sur OK.

Configuration et activation de la fonction multiniveau

La fonction multiniveau vous permet d'accéder aux cibles et PDU KX II par l'intermédiaire d'un dispositif KX II de base. Cette fonction est disponible pour les dispositifs KX II standard, ainsi que pour les dispositifs KX2-808, KX2-832 et KX2-864.

Remarque : les dispositifs de base et en niveau doivent tous utiliser la même version de firmware.

Remarque : les cibles des groupes de deux ports vidéo liés à un dispositif en niveau doivent être accessibles uniquement via ce dispositif et non via le dispositif en niveau de base. Reportez-vous à Création d'un groupe de deux ports vidéo.

Des dispositifs peuvent être ajoutés et supprimés d'une configuration selon les besoins, pour obtenir un maximum de deux niveaux étagés.

Lors du paramétrage des dispositifs, vous utiliserez des CIM spécifiques pour des configurations particulières. Reportez-vous à ***Fonction multiniveau - Types de cibles, CIM pris en charge et mise en niveau de configurations*** (à la page 185) pour obtenir une description des cibles pouvant être incluses à une configuration multiniveau, et des informations sur la compatibilité des CIM et la configuration des dispositifs.

Avant d'ajouter des dispositifs en niveau, vous devez activer la fonction multiniveau pour le dispositif de base et les dispositifs en niveau. L'activation des dispositifs de base s'effectue sur la page Device Settings (Paramètres du dispositif). L'activation des dispositifs en niveau s'effectue sur la page Local Port Settings (Paramètres du port local). Une fois les dispositifs activés et configurés, ils apparaissent sur la page Port Access (Accès aux ports).

Lorsque KX II est configuré pour servir de dispositif de base ou en niveau, il apparaît comme suit :

- Configured As Base Device (Configuré comme dispositif de base) dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'interface du KX II pour les dispositifs de base.
- Configured As Tier Device (Configuré comme dispositif en niveau) dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'interface du KX II pour les dispositifs en niveau.
- Le dispositif de base sera identifié par Base dans le panneau gauche de l'interface du dispositif en niveau sous Connect User (Utilisateur connecté).
- Les connexions cible vers un port en niveau depuis la base seront affichés sous la forme de 2 ports connectés.

Le dispositif de base fournit un accès à distance et local via une liste de ports consolidée de la page Port Access. Les dispositifs en niveau offrent un accès à distance depuis leur propre liste de ports. L'accès local n'est pas disponible sur les dispositifs en niveau lorsque la fonction multiniveau est activée.

La configuration des ports, dont la modification du nom du CIM, doit être effectuée directement depuis chaque dispositif et non depuis le dispositif de base des ports cible en niveau.

La fonction multiniveau prend également en charge les commutateurs KVM pour alterner entre les serveurs. Reportez-vous à ***Configuration des commutateurs KVM*** (à la page 210).

Activation de la fonction multiniveau

Connectez depuis un port de serveur cible sur le dispositif de base aux ports vidéo/clavier/souris du port Local Access du KX II en niveau à l'aide d'un D2CIM-DVUSB.

Si le dispositif en niveau est un dispositif KX2-808, KX2-832 ou KX2-864, effectuez la connection depuis un port du serveur cible sur le dispositif de base directement au port Extended Local du KX2-808/KX2-832/KX2-864 en niveau.

Pour activer la fonction multiniveau :

1. Depuis la base du niveau, choisissez Device Settings > Device Services (Paramètres du dispositif > Services du dispositif). La page de paramétrage Device Services (Services du dispositif) apparaît.
2. Sélectionnez Enable Tiering as Base (Activer la fonction multiniveau comme base).
3. Dans le champ Base Secret (Secret de la base), entrez le secret partagé entre la base et les dispositifs en niveau. Ce secret est exigé pour permettre aux dispositifs en niveau d'authentifier le dispositif de base. Vous entrerez le même mot secret pour le dispositif en niveau.
4. Cliquez sur OK.
5. Activez les dispositifs en niveau. Depuis le dispositif en niveau, choisissez Device Settings > Local Port Settings (Paramètres du dispositif > Paramètres du port local).
6. Dans la section Enable Local Ports (Activer les ports locaux) de la page, sélectionnez Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local).
7. Dans le champ Tier Secret (Secret du niveau), entrez le mot secret entré pour le dispositif de base sur la page Device Settings (Paramètres du dispositif).
8. Cliquez sur OK.

Fonction multiniveau - Types de cibles, CIM pris en charge et mise en niveau de configurations

Châssis de lames

Les châssis de lames connectés directement à la base sont accessibles.

Gestion de l'alimentation

Vous pouvez mettre sous et hors tension les cibles intégrées à la configuration multiniveau. L'accès de ces cibles s'effectue depuis la page Port Access.

Les prises de PDU KX II sont accessibles et contrôlées via une configuration multiniveau avec KX II, ou les modèles KX2-808, KX2-832 et KX2-864. Si des cibles et des prises sont associées, la gestion de l'alimentation est disponible depuis la page Port Access. Les associations cibles et prises de PDU sont limitées à celles connectées au même KX II.

Les PDU connectées aux KX II de base ou en niveau sont affichées dans la liste déroulante de la page Power, ainsi que les statistiques relatives à la barrette d'alimentation sélectionnée.

La gestion au niveau des prises est également disponible. Précisément, vous pouvez mettre sous et hors tension les prises actuellement activées, mais vous ne pouvez pas effectuer l'alimentation cyclique des prises actuellement désactivées.

CIM compatibles avec la configuration des ports locaux KX II à KX II ou KX2-8xx

Les CIM suivants sont compatibles lorsque vous configurez un KX II de base pour l'accès et la gestion d'un KX II supplémentaire, ou des modèles KX2-808, KX2-832 et KX2-864, ainsi que des PDU KX II et châssis de lames.

Si vous utilisez une configuration KX II à KX II, D2CIM-DVUSB doit être utilisé. Si vous utilisez une configuration KX II à KX2-8xx, seul le port local étendu peut être utilisé.

Si vous utilisez une configuration constituée d'un KX II et de KX2-808, KX2-832 ou KX2-864, chaque dispositif doit exécuter la même version de firmware. Lorsque les châssis de lames font partie d'une configuration, chaque châssis compte pour un port cible.

Fonctions non prises en charge et limitées sur les cibles en niveau

Les fonctions suivantes ne sont pas prises en charge sur les cibles en niveau :

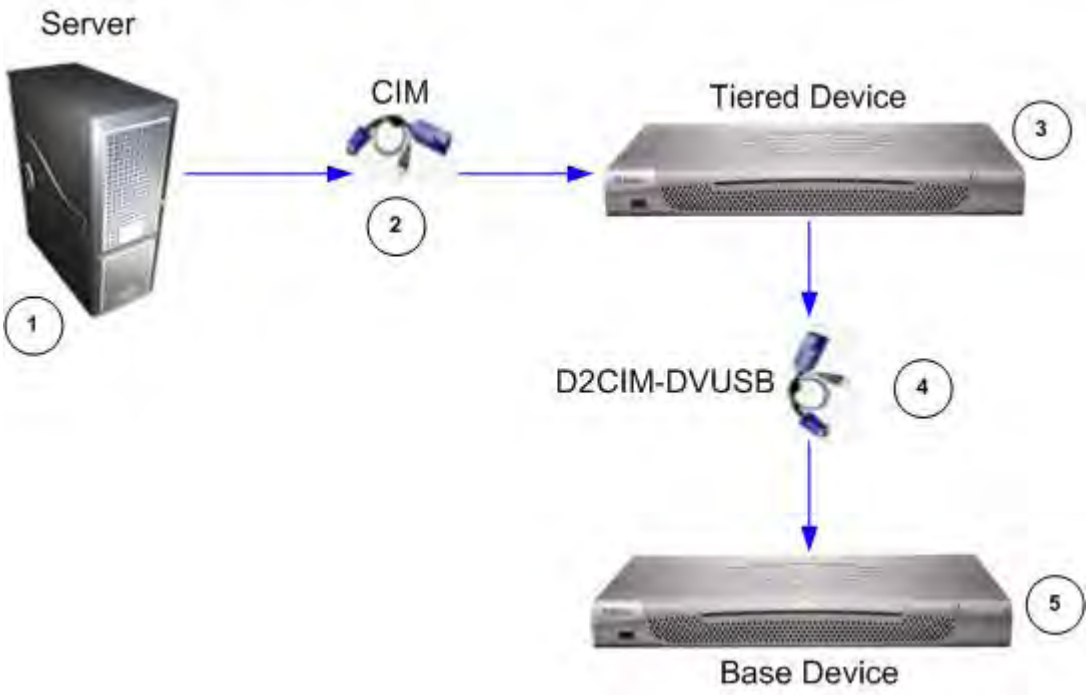
- Châssis de lames sur les dispositifs en niveau
- Audio sur les dispositifs en niveau
- Cartes à puce sur les dispositifs en niveau
- Dispositifs en niveau de support virtuel
- MCCAT comme dispositif en niveau

La gestion des groupes de ports est limitée à la création de groupes de ports de membres connectés directement à la base.

Exemple de câble dans les configurations multiniveaux

Le diagramme suivant illustre les configurations de câblage entre un dispositif en niveau KX II et un dispositif de base KX II. Connectez depuis un port de serveur cible sur le dispositif de base aux ports vidéo/clavier/souris du port Local Access du KX II en niveau à l'aide d'un D2CIM-DVUSB.

Si le dispositif en niveau est un dispositif KX2-808, KX2-832 ou KX2-864, effectuez la connection depuis un port du serveur cible sur le dispositif de base directement au port Extended Local du KX2-808/KX2-832/KX2-864 en niveau.



Légende	
1	Serveur cible

Légende	
2	CIM du serveur cible au dispositif en niveau KX II
3	Dispositif en niveau KX II
4	CIM D2CIM-DVUSB du dispositif en niveau KX II au dispositif de base KX II
5	Dispositif de base KX II

Activation d'un accès direct aux ports via URL

L'accès direct aux ports permet aux utilisateurs d'éviter les pages de connexion et d'accès aux ports du dispositif. Cette fonction permet également d'entrer un nom d'utilisateur et un mot de passe directement, et d'accéder à la cible si le nom d'utilisateur et le mot de passe ne sont pas contenus dans l'URL.

Vous trouverez ci-après des informations d'URL importantes concernant l'accès direct aux ports :

Si vous utilisez VKC et l'accès direct aux ports :

- https://IPaddress/dpa.asp?username=nom d'utilisateur&password=mot de passe&port=numéro de port

Si vous utilisez AKC et l'accès direct aux ports :

- https://IPaddress/dpa.asp?username=nom d'utilisateur&password=mot de passe&port=numéro de port&client=akc

Où :

- Nom d'utilisateur et mot de passe sont facultatifs. S'ils ne sont pas fournis, une boîte de dialogue de connexion apparaît et, après avoir été authentifié, l'utilisateur est connecté directement à la cible.
- Le port peut être un numéro ou un nom de port. Si vous utilisez un nom de port, il doit être unique ou une erreur est signalée. Si le port est totalement omis, une erreur est signalée.
- Pour les châssis de lames, le port est désigné par <numéro de port>'-'<numéro de connecteur>. Par exemple, 1-2 pour un châssis de lames connecté au port 1, connecteur 2.
- Client=akc est facultatif sauf si vous utilisez un client AKC. Si client=akc n'est pas inclus, VKC est utilisé comme client.

Si vous accédez à une cible faisant partie d'un groupe de deux ports vidéo, l'accès aux ports direct utilise le port principal pour lancer les ports principal et secondaire. Les connexions directes au port secondaire sont rejetées et les règles d'autorisation habituelles s'appliquent.
Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 259) pour plus d'informations à ce sujet.

Pour activer l'accès direct aux ports :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Cochez la case Enable Direct Port Access via URL (Activer l'accès direct aux ports via URL) pour accorder aux utilisateurs un accès direct à une cible via le dispositif Dominion par transmission des paramètres nécessaires dans l'URL.

3. Cliquez sur OK.

Activation de la validation du certificat du serveur de téléchargement AKC

Si vous utilisez le client AKC, vous pouvez décider d'utiliser ou non la fonction Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC).

Remarque : lorsque Microsoft® ClickOnce® fonctionne en mode double pile IPv4 et IPv6 avec la fonction Enable AKC Download Server Certificate Validation, le CN du certificat de serveur ne doit pas contenir de forme à zéros compressés de l'adresse IPv6. Sinon, vous ne pourrez pas télécharger et lancer AKC. Toutefois, ceci peut entraîner un conflit avec les préférences de navigateur pour la forme de l'adresse IPv6. Utilisez le nom d'hôte du serveur dans le nom commun (CN) ou entrez des formes compressées et non compressées de l'adresse IPv6 dans le champ Subject Alternative Name (Autre nom du sujet).

Option 1 : Ne pas activer la validation du certificat du serveur de téléchargement AKC (paramètre par défaut)

Si vous n'activez pas la validation du certificat du serveur de téléchargement AKC, tous les utilisateurs du dispositif Dominion et de CC-SG Bookmark and Access Client doivent :

- Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.
- Les utilisateurs de serveurs Windows Vista, Windows 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur et que le mode protégé n'est pas activé lors de l'accès au dispositif.

Option 2 : Activer la validation du certificat du serveur de téléchargement AKC

Si vous activez la validation du certificat du serveur de téléchargement AKC :

- Les administrateurs doivent téléverser un certificat valide sur le dispositif ou générer un certificat auto-signé sur celui-ci. Le certificat doit désigner un hôte valide.
- Chaque utilisateur doit ajouter le certificat AC (ou une copie du certificat auto-signé) dans la liste Autorités de certification racines de confiance de leur navigateur.

Pour installer le certificat auto-signé dans les systèmes d'exploitation Windows Vista® et Windows 7® :

1. Ajoutez l'adresse IP de KX II dans la zone Site de confiance et assurez-vous que le mode protégé est désactivé.

2. Lancez Internet Explorer® en indiquant comme URL l'adresse IP de KX II. Un message Erreur de certificat apparaît.
3. Sélectionnez Afficher les certificats.
4. Sur l'onglet Général, cliquez sur Installer le certificat. Le certificat est alors installé dans la liste Autorités de certification racines de confiance.
5. Une fois le certificat installé, l'adresse IP de KX II peut être supprimé de la zone Site de confiance.

Pour activer la validation du certificat du serveur de téléchargement AKC :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Vous pouvez cocher la case Enable AKC Download Server Certificate Validation ou laisser la fonction désactivée (valeur par défaut).
3. Cliquez sur OK.

Configuration des agents SNMP

Les dispositifs conformes à SNMP, appelés agents, stockent les données qui les concernent dans des bases de données MIB et renvoient ces données aux gestionnaires SNMP. Reportez-vous à ***Affichage du MIB de KX II*** (à la page 202) pour plus d'informations sur la consultation du MIB de KX II.

KX II prend en charge la journalisation de SNMP v1/v2c et/ou v3. SNMP v1/v2c définit le format des messages et les opérations de protocole lorsque la journalisation SNMP est activée. SNMP v3 est une extension de sécurité de SNMP qui permet l'authentification des utilisateurs, la gestion et le chiffrement des mots de passe.

Remarque : les données SNMP v3 sécurisées sont distinctes du mode FIPS sécurisé de KX II.

Pour configurer des agents SNMP :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Entrez les données d'identification de l'agent SNMP ci-après pour les objets MIB-II System Group :
   a. System Name - nom de l'agent SNMP ou du dispositif
   b. System Contact - nom du contact associé au dispositif
   c. System Location - emplacement du dispositif

3. Sélectionnez Enable SNMP v1/v2c (Activer SNMP v1/v2c) et/ou Enable SNMP v3 (Activer SNMP v3). Une des options au moins doit être sélectionnée. **Obligatoire**
4. Renseignez les champs ci-après pour SNMP v1/v2c (le cas échéant) :
   a. Community - chaîne de communauté du dispositif
   b. Community Type - pour accorder l'accès Read-Only (Lecture seule) ou Read-Write (Lecture-Ecriture) aux utilisateurs de la communauté

   Remarque : Une communauté SNMP est le groupe auquel les dispositifs et les postes de gestion exécutant SNMP appartiennent. Elle aide à définir le destinataire des informations. Le nom de la communauté permet d'identifier le groupe. Le dispositif ou agent SNMP peut appartenir à plusieurs communautés SNMP.
5. Renseignez les champs ci-après pour SNMP v3 (le cas échéant) :
   a. Sélectionnez Use Auth Passphrase (Utiliser une phrase de passe d'authentification) si nécessaire. Si une phrase de passe de confidentialité est requise, Use Auth Passphrase permet d'utiliser la même phrase sans avoir à l'entrer à nouveau.
   b. Security Name - nom d'utilisateur ou de compte de service de l'entité communiquant avec l'agent SNMP (32 caractères au plus)
   c. Authentication Protocol - protocole d'authentification MD5 ou SHA utilisé par l'agent SNMP v3
   d. Authentication Passphrase - phrase de passe requise pour accéder à l'agent SNMP v3 (64 caractères au plus)
   e. Privacy Protocol - le cas échéant, algorithme AES ou DES utilisé pour chiffrer les données de PDU et de contexte
   f. Privacy Passphrase - phrase de passe servant à accéder à l'algorithme de protocole de confidentialité (64 caractères au plus)
6. Cliquez sur OK pour démarrer le service de l'agent SNMP.

Pour réinitialiser les valeurs par défaut usine :

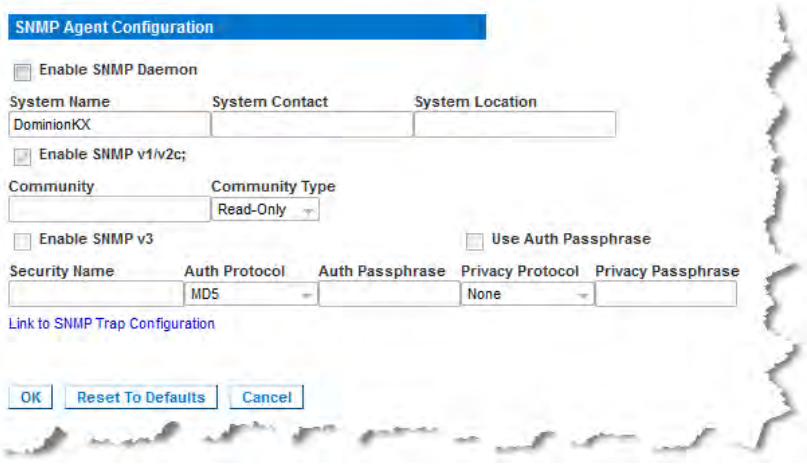
- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut). Tous les éléments de la page récupèrent leurs valeurs par défaut.

Configurez les traps SNMP sur la page Event Management - Settings (Gestion des événements - Paramètres). Reportez-vous à ***Configuration des traps SNMP*** (à la page 196) pour obtenir des informations sur la création des traps SNMP et ***Liste des traps SNMP de KX II*** (à la page 199) pour obtenir la liste des traps SNMP de KX II disponibles.

Conseil : cliquez sur le lien Link to SNMP Trap Configuration (Lien vers la configuration des traps SNMP) pour arriver rapidement à la page Event Management - Settings.

Les événements capturés une fois le trap SNMP configuré sont sélectionnés sur la page Event Management - Destination (Gestion des événements - Destination). Reportez-vous à ***Configuration de la page Event Management - Destinations*** (voir "***Configuration de la gestion des événements - Destinations***" à la page 204).

AVERTISSEMENT : lorsque vous utilisez les traps SNMP via UDP, il est possible que KX II et le routeur auquel elle est reliée se désynchronisent au moment où KX II redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.



Configuration des paramètres de modem

Pour configurer les paramètres de modem :

1. Cliquez sur Device Settings (Paramètres du dispositif) > Modem Settings (Paramètres de modem) pour ouvrir la page Modem Settings.
2. Cochez la case Enable Modem (Activer le modem). Les champs Serial Line Speed (Vitesse de la ligne série) et Modem Init String (Chaîne initiale du modem) sont activés.
3. Le champ Serial Line Speed du modem est paramétré sur 115200.
4. Renseignez le champ Modem Init String. Si la chaîne du modem est laissée vide, la chaîne suivante est envoyée par défaut au modem : ATZ OK AT OK.

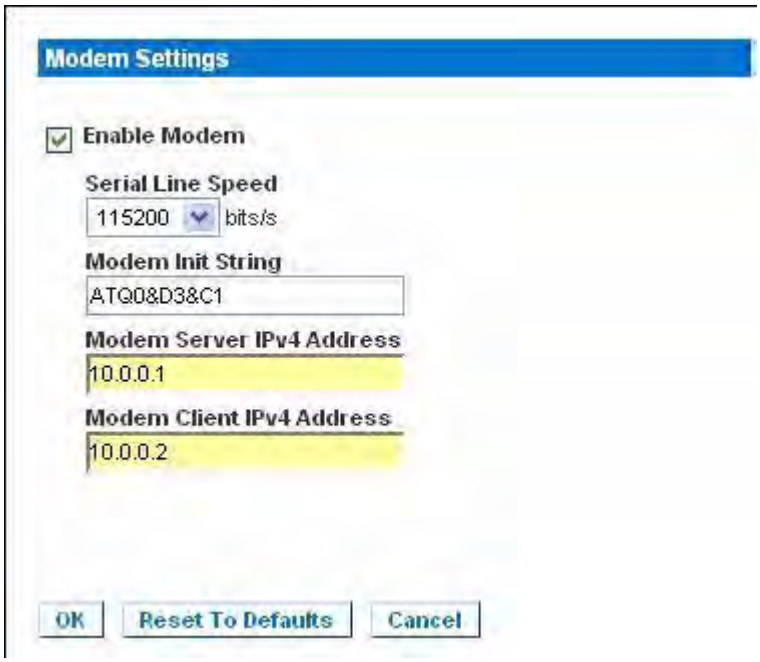
   Cette information est utilisée pour configurer les paramètres du modem. Comme chaque modem paramètre ces valeurs à sa manière, ce document n'indique pas comme définir ces valeurs. L'utilisateur doit se référer au modem pour créer la chaîne appropriée.

   a. Paramètres de modem :

      - Activation du contrôle de flux RTS/CTS (demande pour émettre/prêt à émettre)
      - Envoi de données à l'ordinateur dès la réception de RTS
      - CTS devrait être configuré de manière à abandonner uniquement lorsque le contrôle de flux le demande.
      - DTR devrait être configuré pour les réinitialisations de modem avec basculement DTR.
      - DSR devrait toujours être activé.
      - DCD devrait être configuré comme étant activé après la détection d'un signal porteur. (DCD ne devrait être activé que lorsque la connexion du modem est établie avec le côté distant.)
5. Renseignez le champ Modem Server IPv4 Address (Adresse IPv4 du serveur de modem) et le champ Modem Client IPv4 Address (Adresse IPv4 du client de modem).

Remarque : les adresses IP des client et serveur du modem doivent provenir du même sous-réseau et ne peuvent pas chevaucher le sous-réseau LAN du dispositif.

6. Cliquez sur OK pour appliquer vos changements ou sur Reset to Defaults (Restaurer les paramètres par défaut) pour rétablir les valeurs par défaut des paramètres.



Reportez-vous à ***Modems certifiés*** (à la page 359) pour plus d'informations sur les modems certifiés qui fonctionnent avec KX II. Pour plus d'informations sur les paramètres qui permettront les meilleures performances lors de la connexion à KX II par modem, reportez-vous à **Création, modification et suppression des profils dans MPC - Dispositifs de la deuxième génération** dans le **manuel des clients d'accès KVM et série**.

Remarque : l'accès direct par modem à l'interface HTML de KX II n'est pas prise en charge. Vous devez utiliser le MPC autonome pour accéder à KX II par modem.

Configuration des paramètres de date et heure

La page Date/Time Settings (Paramètres de date/heure) permet d'indiquer la date et l'heure de KX II. Il existe deux méthodes pour ce faire :

- Définir la date et l'heure manuellement ou
- les 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 Date/Time Settings (Paramètres de date/heure) s'ouvre.
2. Sélectionnez votre fuseau horaire dans la liste déroulante Time Zone (Fuseau horaire).
3. Pour prendre en compte l'heure d'été, cochez la case Adjust for daylight savings time (Régler selon les changements d'heure).
4. Choisissez la méthode que vous souhaitez utiliser pour définir la date et l'heure :
   - User Specified Time - Sélectionnez cette option pour saisir la date et l'heure manuellement. Pour l'option User Specified Time (Heure spécifiée par l'utilisateur), entrez la date et l'heure. Pour l'heure, utilisez le format hh:mm (système de 24 heures).
   - Synchronize with NTP Server - Sélectionnez cette option pour synchroniser la date et l'heure avec le serveur NTP.
5. Pour l'option Synchronize with NTP Server (Synchroniser avec le serveur NTP) :
   a. Entrez une adresse IP dans le champ Primary Time server (Serveur d'horloge principal).
   b. Renseignez le champ Secondary Time server (Serveur d'horloge secondaire). **Facultatif**

Cliquez sur OK.

Gestion des événements

La fonction de gestion des événements de KX II permet d'activer et de désactiver la distribution des événements système aux gestionnaires SNMP, Syslog et au journal d'audit. Ces événements sont regroupés dans différentes catégories et vous pouvez décider d'envoyer chacun vers une ou plusieurs destinations.

Configuration de la gestion des événements - Paramètres

Effectuez la configuration des traps SNMP et de syslog sur la page Event Management - Settings (Gestion des événements - Paramètres). Reportez-vous à ***Configuration des traps SNMP*** (à la page 196).

Une fois la configuration effectuée, activez les traps SNMP sur la page Event Management - Settings. Reportez-vous à ***Configuration de la page Event Management - Destinations*** (voir "***Configuration de la gestion des événements - Destinations***" à la page 204).

Configuration des traps SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole qui gouverne la gestion du réseau et la surveillance des dispositifs réseau ainsi que leurs fonctions. Les traps SNMP sont envoyés sur un réseau pour collecter des informations. Ils sont configurés sur la page Event Management - Settings (Gestion des événements - Paramètres). Reportez-vous à ***Liste des traps SNMP de KX II*** (à la page 199).

Les dispositifs compatibles SNMP, appelés agents, stockent les données qui les concernent dans des bases de données de gestion MIB et répondent au trap SNMP. Ces agents sont configurés sur la page Device Services (Services du dispositif). Reportez-vous à ***Configuration des agents SNMP*** (à la page 190) et à ***Affichage du MIB de KX II*** (à la page 202) pour en savoir plus à ce sujet.

Pour configurer SNMP (permettre la journalisation de SNMP) :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Settings (Gestion des événements - Paramètres). La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre :
2. Sélectionnez SNMP Logging Enabled (Journalisation SNMP activée) pour activer les champs SNMP restants. **Obligatoire**
3. Cochez SNMP v1/v2c Traps Enabled et/ou SNMP Trap v3 Enabled. Une des options au moins doit être sélectionnée. A ce moment, tous les champs associés sont activés. **Obligatoire**
4. Renseignez les champs ci-après pour SNMP v1/v2c (le cas échéant) :
   a. Destination IP/Hostname - adresse IP ou nom d'hôte du gestionnaire SNMP. Cinq (5) gestionnaires SNMP au maximum peuvent être créés.

   Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

   b. Port Number - numéro de port utilisé par le gestionnaire SNMP.

c. Community - chaîne de communauté du dispositif

Remarque : Une communauté SNMP est le groupe auquel les dispositifs et les postes de gestion exécutant SNMP appartiennent. Elle aide à définir le destinataire des informations. Le nom de la communauté permet d'identifier le groupe. Le dispositif ou agent SNMP peut appartenir à plusieurs communautés SNMP.

5. Si ce n'est pas encore fait, cochez la case SNMP Trap v3 Enabled pour activer les champs suivants. Renseignez les champs ci-après pour SNMP v3 (le cas échéant) :

   a. Destination IP/Hostname - adresse IP ou nom d'hôte du gestionnaire SNMP. Cinq (5) gestionnaires SNMP au maximum peuvent être créés.

   Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

   b. Port Number - numéro de port utilisé par le gestionnaire SNMP.

   c. Security Name - nom d'utilisateur ou de compte de service de l'entité communiquant avec l'agent SNMP (32 caractères au plus)

   d. Authentication Protocol - protocole d'authentification MD5 ou SHA utilisé par l'agent SNMP v3

   e. Authentication Passphrase - phrase de passe requise pour accéder à l'agent SNMP v3 (64 caractères au plus)

   f. Privacy Protocol - le cas échéant, algorithme AES ou DES utilisé pour chiffrer les données de PDU et de contexte

   g. Privacy Passphrase - phrase de passe servant à accéder à l'algorithme de protocole de confidentialité (64 caractères au plus)

   Remarque : si vous accédez à la page Event Management - Settings depuis la console locale et utilisez une résolution d'écran inférieure à 1280 x 1024, la colonne Privacy Passphrase (Phrase de passe de confidentialité) ne s'affiche pas sur cette page. Dans ce cas, masquez le panneau gauche de KX II. Reportez-vous à **Panneau gauche** *(à la page 53).*

6. Cliquez sur OK pour créer les traps SNMP.

Conseil : utilisez le lien Link to SNMP Agent Configuration (Lien vers la configuration des agents SNMP) pour parvenir rapidement à la page Devices Services depuis la page Event Management - Settings.

Les événements capturés une fois le trap SNMP configuré sont sélectionnés sur la page Event Management - Destination (Gestion des événements - Destination). Reportez-vous à ***Configuration de la page Event Management - Destinations*** (voir "***Configuration de la gestion des événements - Destinations***" à la page 204).

KX II prend en charge la journalisation de SNMP v1/v2c et/ou v3. SNMP v1/v2c définit le format des messages et les opérations de protocole lorsque la journalisation SNMP est activée. SNMP v3 est une extension de sécurité de SNMP qui permet l'authentification des utilisateurs, la gestion et le chiffrement des mots de passe.

Remarque : les données SNMP v3 sécurisées sont distinctes du mode FIPS sécurisé de KX II.

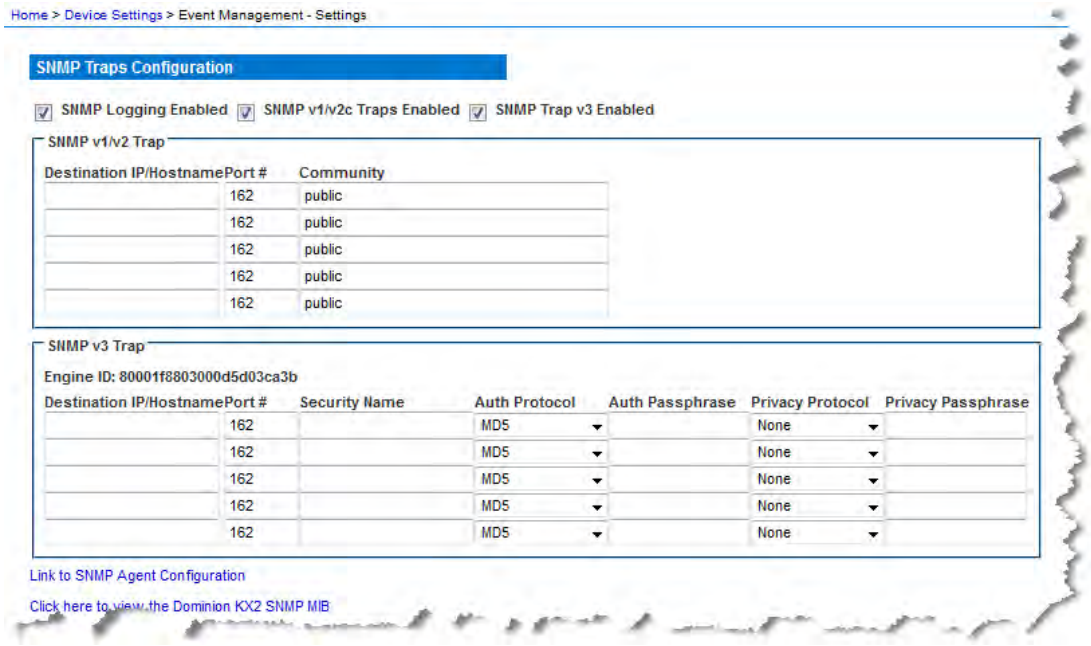
Pour modifier des traps SNMP existants :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Settings (Gestion des événements - Paramètres). La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre :
2. Effectuez les modifications nécessaires et cliquez sur OK pour les enregistrer.

Remarque : si vous désactivez les paramètres SNMP, les données SNMP sont conservées. Vous n'avez pas à les entrer à nouveau lorsque vous réactivez les paramètres.

Pour supprimer des traps SNMP :

- Effacez tous les champs de traps SNMP et enregistrez.



Utilisez la fonction de réinitialisation aux valeurs par défaut usine pour supprimer la configuration SNMP et rétablir les paramètres usine par défaut de KX II.

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

AVERTISSEMENT : lorsque vous utilisez les traps SNMP via UDP, il est possible que KX II et le routeur auquel elle est reliée se désynchronisent au moment où KX II redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Liste des traps SNMP de KX II

SNMP permet d'envoyer des traps, ou notifications, pour prévenir un administrateur qu'une ou plusieurs conditions ont été remplies. Le tableau suivant répertorie les traps SNMP de KX II :

Nom de trap	Description
bladeChassisCommError	Une erreur de communication avec le dispositif

Nom de trap	Description
	avec châssis de lames connecté à ce port a été détectée. *Remarque : pas de prise en charge par KX II-101 ou LX.*
cimConnected	Le CIM est connecté.
cimDisconnected	Le CIM est déconnecté.
cimUpdateStarted	La mise à jour du CIM est en cours.
cimUpdateCompleted	La mise à jour du CIM est terminée.
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	KX II a effectué la mise à jour via un fichier RFP.
deviceUpgradeStarted	KX II a commencé la mise à jour via un fichier RFP.
factoryReset	Les valeurs par défaut usine du dispositif ont été rétablies.
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	Les paramètres réseau ont été modifiés.
networkParameterChangedv2	Les paramètres réseau de KX II-101-V2 ont été modifiés.
passwordSettingsChanged	Les paramètres des mots de passe sécurisés ont été modifiés.
portConnect	Un utilisateur authentifié au préalable a démarré une session KVM.

Nom de trap	Description
portConnectv2	Un utilisateur de KX II-101-V2 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.
portDisconnectv2	Un utilisateur de KX II-101-V2 engagé dans une session KVM ferme la session correctement.
portStatusChange	Le port n'est plus disponible.
powerNotification	Notification de l'état de la prise d'alimentation : 1=Active, 0=Inactive.
powerOutletNotification	Notification du statut d'une prise de barrette d'alimentation.
rebootCompleted	Le redémarrage de KX II est terminé.
rebootStarted	KX II a commencé à redémarrer lors de l'alimentation cyclique du système ou lors d'un redémarrage à chaud à partir du système d'exploitation.
scanStarted	Un balayage de serveur cible a démarré.
scanStopped	Un balayage de serveur cible s'est arrêté.
securityBannerAction	La bannière de sécurité a été acceptée ou refusée.
securityBannerChanged	La bannière de sécurité a été modifiée.
securityViolation	Violation de sécurité.
setDateTime	Les date et heure du dispositif ont été définies.
setFIPSMode	Le mode FIPS a été activé. *Remarque : FIPS n'est pas pris en charge par LX.*
startCCManagement	Le dispositif a été placé sous la gestion de CommandCenter.
stopCCManagement	Le dispositif a été retiré de la gestion de 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 corrects.
userConnectionLost	Un utilisateur avec une session active a subi une interruption anormale de session.
userDeleted	Un compte d'utilisateur a été supprimé.

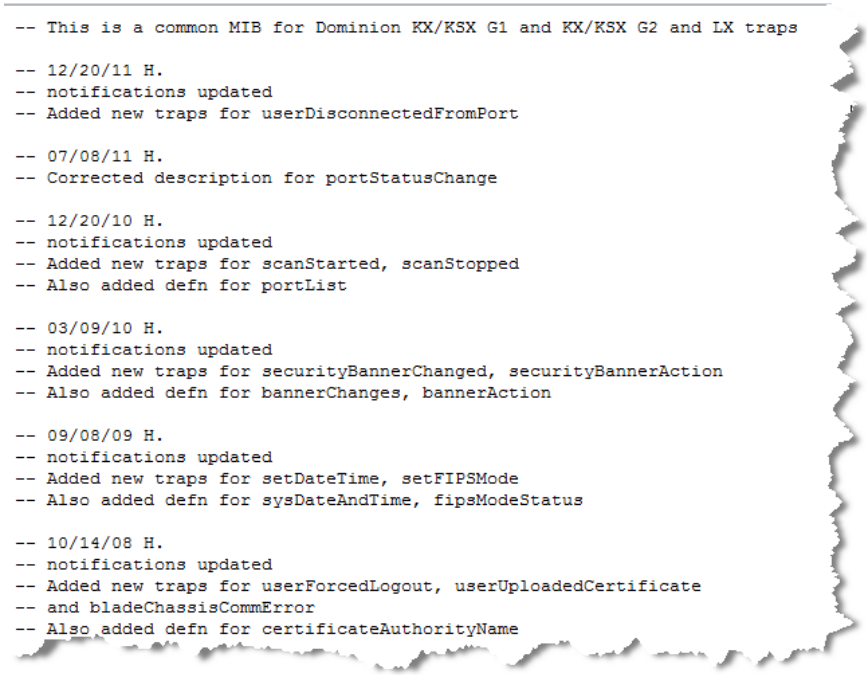
Nom de trap	Description
userForcedLogout	Un utilisateur a été déconnecté de force par Admin.
userLogin	Un utilisateur s'est connecté à KX II et a été authentifié.
userLogout	Un utilisateur s'est déconnecté correctement de KX II.
userModified	Un compte d'utilisateur a été modifié.
userPasswordChanged	Cet événement est déclenché lorsque le mot de passe de n'importe quel utilisateur du dispositif est modifié.
userSessionTimeout	Un utilisateur avec une session active a subi une interruption de session en raison du délai d'attente.
userUploadedCertificate	Un utilisateur a téléversé un certificat SSL.
vmImageConnected	Un utilisateur a tenté de monter un dispositif ou une image sur la cible à l'aide de la fonction Support virtuel. Pour chaque tentative de mappage (montage) de dispositif/image, cet événement est généré.
vmImageDisconnected	Un utilisateur a tenté de démonter un dispositif ou une image sur la cible à l'aide de la fonction Support virtuel.

Affichage du MIB de KX II

Pour afficher le MIB de KX II :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Settings (Gestion des événements - Paramètres). La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre :
2. Cliquez sur le lien Click here to view the Dominion KX2 SNMP MIB (Cliquer ici pour afficher le MIB SNMP de Dominion KX2). Le fichier MIB s'ouvre dans une fenêtre de navigateur.

Remarque : si vous disposez d'un accès en lecture/écriture au fichier MIB, utilisez un éditeur MIB pour le modifier.



```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps

-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateTime, setFIPSMode
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

Configuration de Syslog

Pour configurer Syslog (activer le transfert Syslog) :

1. Sélectionnez Enable Syslog Forwarding (Activer le transfert Syslog) pour consigner les messages du dispositif sur un serveur Syslog distant.
2. Entrez l'adresse IP ou le nom d'hôte de votre serveur Syslog dans le champ IP Address.
3. Cliquez sur OK.

Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

Utilisez la fonction de réinitialisation aux valeurs par défaut usine pour supprimer la configuration syslog et rétablir les paramètres usine par défaut de KX II.

Pour réinitialiser les valeurs par défaut usine :

1. Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

Configuration de la gestion des événements - Destinations

Les événements système, si l'option correspondante est activée, génèrent des événements de notification SNMP (traps) ou peuvent être consignés dans Syslog ou dans le journal d'audit. Utilisez la page Event Management - Destinations (Gestion des événements - Destinations) pour sélectionner les événements système à suivre et l'emplacement vers lequel envoyer les informations.

Remarque : des traps SNMP seront générés uniquement si l'option SNMP Logging Enabled (Journalisation SNMP activée) est sélectionnée. Des événements Syslog sont générés uniquement si l'option Enable Syslog Forwarding (Activer le transfert Syslog) est sélectionnée. Ces deux options se trouvent sur la page Event Management - Settings (Gestion des événements - Paramètres). Reportez-vous à **Configuration de la gestion des événements - Paramètres)** *(voir "***Configuration de la gestion des événements - Paramètres***" à la page 196).*

Pour sélectionner des événements et leurs destinations :

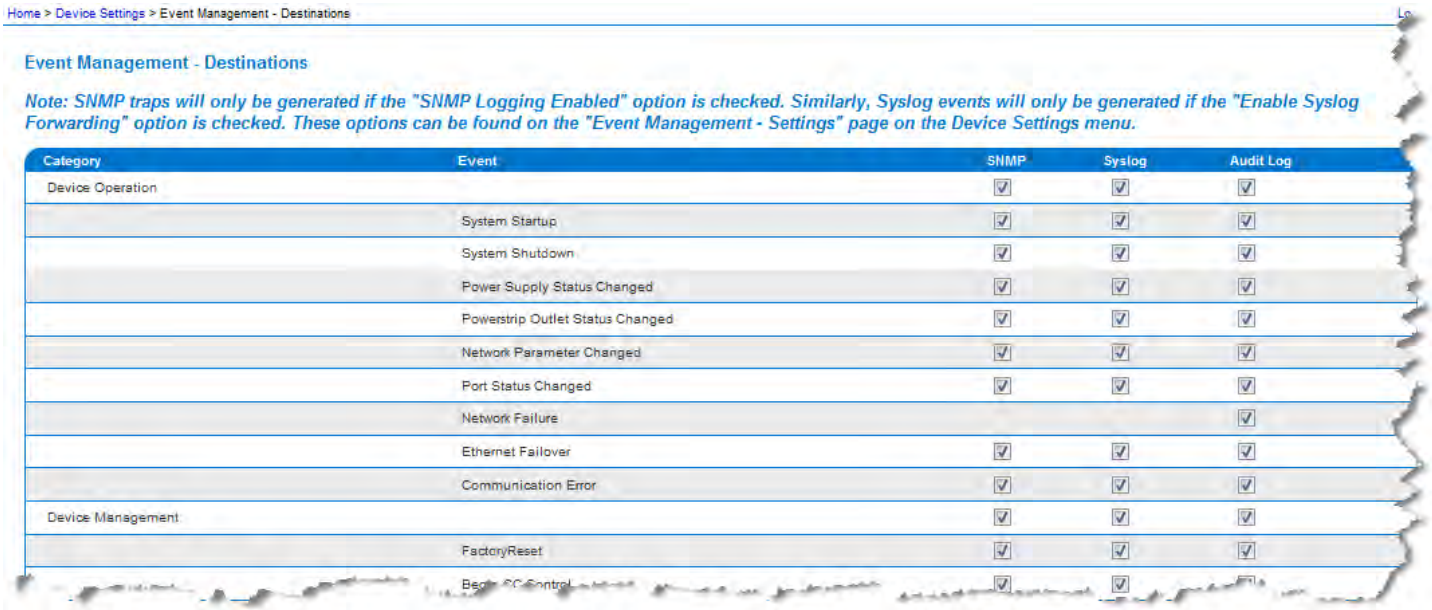
1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Destinations (Gestion des événements - Destinations). La page correspondante s'ouvre.

   Les événements système sont regroupés en plusieurs catégories : Device Operation (Opération sur les dispositifs), Device Management (Gestion des dispositifs), Security, User Activity et User Group Administration.

2. Cochez les cases en regard des éléments de la ligne d'événement pour indiquer ceux que vous souhaitez activer ou désactiver, et pour préciser l'emplacement où vous souhaitez envoyer les informations.

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

3. Cliquez sur OK.



Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

AVERTISSEMENT : lorsque vous utilisez les traps SNMP via UDP, il est possible que KX II et le routeur auquel elle est reliée se désynchronisent au moment où KX II redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Configuration de l'alimentation

L'unité KX II offre une double alimentation. Elle peut détecter et indiquer automatiquement l'état de ces alimentations. Utilisez la page Power Supply Setup (Configuration de l'alimentation) pour préciser si vous utilisez une source d'alimentation ou deux. Une configuration appropriée garantit l'envoi de notifications adéquates par KX II en cas de panne de courant. Par exemple, si l'alimentation numéro un tombe en panne, le voyant d'alimentation situé à l'avant de l'unité devient rouge.

Pour activer la détection automatique des alimentations utilisées :

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

2. Si vous branchez une arrivée électrique dans l'alimentation numéro un (la plus à gauche à l'arrière de l'unité), sélectionnez l'option PowerIn1 Auto Detect (Détection automatique PowerIn1).
3. Si vous branchez une arrivée électrique dans l'alimentation numéro deux (la plus à droite à l'arrière de l'unité), sélectionnez l'option PowerIn2 Auto Detect (Détection automatique PowerIn2).
4. Cliquez sur OK.

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

Pour désactiver la détection automatique :

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

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

Remarque : KX II NE génère PAS de rapport sur l'état de l'alimentation pour CommandCenter. Dominion I (génération 1), en revanche, établit des rapports sur l'état d'alimentation pour CommandCenter.

Configuration des ports

La page Port Configuration (Configuration des ports) affiche la liste des ports de l'unité KX II. Les ports connectés aux serveurs cible KVM (serveurs lames et standard) et aux PDU de rack (barrettes d'alimentation) sont affichés en bleu et peuvent être modifiés. Pour les ports sans CIM connecté ou avec un nom CIM vide, un nom de port par défaut Dominion-KX2_Port# est affecté, où Port# est le numéro du port physique de l'unité KX II.

Lorsque le statut d'un port est désactivé, Not Available (Non disponible) apparaît comme statut. Un port peut être désactivé lorsque son CIM a été retiré ou mis hors tension.

Remarque : un châssis de lames peut être renommé, mais non ses connecteurs de lames.

Une fois le port renommé, utilisez la fonction Reset to Default (Restaurer les paramètres par défaut) à tout moment pour rétablir le nom du port par défaut. Toutes les associations d'alimentation existantes sont alors supprimées et, si le port appartient à un groupe, il en est retiré.

Pour accéder à la configuration d'un port :

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

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

   - Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif KX II.
   - Port Name - Nom attribué au port.

Ou, renommez les ports non connectés à KX II via un CIM et donc, dotés du statut Not Available (Non disponible). Pour renommer un port dont le statut est Not Available, effectuez une des opérations suivantes :

- Renommez le port. Lorsqu'un CIM est connecté, son nom est utilisé.
- Renommez le port et sélectionnez Persist name on Next CIM Insertion (Conserver le nom pour l'insertion de CIM suivante). Lorsqu'un CIM est connecté, le nom qui a été affecté sera copié dans le CIM.
- Réinitialisez le port, nom inclus, aux valeurs par défaut usine en sélectionnant Reset to Defaults. Lorsqu'un CIM est connecté, son nom est utilisé.

Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

- Type de port :
  - DCIM - CIM Dominion
  - Non disponible - Aucun CIM connecté
  - MCUTP - Master Console MCUTP, CIM dans un câble
  - PCIM - CIM Paragon
  - PowerStrip (PDU de rack) - Barrette d'alimentation connectée
  - Dual - VM - CIM de support virtuel (D2CIM-VUSB et D2CIM-DVUSB)
  - Blade Chassis - Châssis de lames et les lames qui lui sont associées (affichés dans un ordre hiérarchique).
  - KVM Switch - Connexion de commutateur KVM générique
  - DVM-DP - Port d'affichage
  - DVM-HDMI - CIM HDMI
  - DVM-DVI - CIM DVI

2. Cliquez sur le nom du port que vous souhaitez modifier.
   - Pour les ports KVM, la page Port des ports KVM et de châssis de lames est ouverte.
   - Pour les PDU de rack, la page Port pour les PDU de rack (barrettes d'alimentation) est ouverte. A partir de cette page, vous pouvez nommer les PDU de rack et leurs prises.

Configuration des serveurs cible standard

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 35) pour obtenir une description de la connexion de l'équipement.
2. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
3. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
4. Sélectionnez Standard KVM Port comme sous-type du port.
5. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.
6. Dans la section Power Association (Association d'alimentation), associez une barre d'alimentation au port, le cas échéant.
7. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
8. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.

9. Cliquez sur OK.

Configuration des commutateurs KVM

KX II prend également en charge l'utilisation des séquences de raccourcis-clavier pour alterner entre les cibles. Outre l'utilisation de séquences de raccourcis-clavier avec les serveurs standard, la commutation KVM est prise en charge par les châssis de lames et dans les configurations multiniveaux.

Important : Pour permettre aux groupes d'utilisateurs de voir le commutateur KVM que vous créez, vous devez d'abord créer le commutateur, puis le groupe. Si un groupe d'utilisateurs existant doit voir le commutateur KVM que vous créez, vous devez créer à nouveau le groupe d'utilisateurs.

Pour configurer des commutateurs KVM :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.

3. Sélectionnez KVM Switch.
4. Sélectionnez le modèle de commutateur KVM (KVM Switch Model).

Remarque : un commutateur seulement apparaîtra dans la liste déroulante.

5. Sélectionnez la séquence de raccourcis-clavier du commutateur KVM (KVM Switch Hot Key Sequence).
6. Entrez le nombre maximum de ports cible (2 à 32).
7. Dans le champ KVM Switch Name, entrez le nom à utiliser pour faire référence à cette connexion de port.
8. Activez les cibles auxquelles la séquence de raccourcis-clavier de commutateur KVM sera appliquée. Indiquez les ports de commutateur KVM auxquels des cibles sont reliées en sélectionnant Active pour chacun des ports.
9. Dans la section KVM Managed Links (Liens gérés de KVM) de la page, vous pouvez configurer la connexion à une interface de navigateur Web si elle est disponible.
   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.
   b. URL Name - Entrez l'URL de l'interface.
   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.
   d. Password - Entrez le mot de passe utilisé à accéder à l'interface.
   e. Username Field - Entrez le paramètre username qui sera utilisé dans l'URL. Par exemple *username*=admin, où *username* est le champ username.
   f. Password Field - Entrez le paramètre password qui sera utilisé dans l'URL. Par exemple, *password*=raritan, où *password* est le champ password.
10. Cliquez sur OK.

Pour modifier le statut actif d'un port ou d'une URL de commutateur KVM :

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

2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Désactivez la case à cocher Active en regard du port ou de l'URL cible de commutateur KVM pour modifier son statut actif.
4. Cliquez sur OK.

Configuration des ports CIM

KX II prend en charge l'utilisation des CIM standard et numériques pour la connexion à un serveur.

Pour configurer un CIM :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Sélectionnez Standard KVM Port comme sous-type du port.
4. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.
5. Dans la section Power Association (Association d'alimentation), associez une barre d'alimentation au port, le cas échéant.
6. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
7. Pour les CIM numériques, sélectionnez une résolution dans la liste déroulante Display Native Resolution (Résolution native d'affichage) pour que la résolution de la cible corresponde à celle du moniteur. Il s'agira du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM. Si aucune sélection n'est effectuée, la résolution par défaut 1280 x 1024 est utilisée.
8. Si vous utilisez un CIM HDMI, certaines combinaisons système d'exploitation/carte vidéo offrent une plage limitée de valeurs RVB. Améliorez les couleurs en cochant la case DVI Compatibility Mode (Mode de compatibilité DVI).
9. Cliquez sur OK.

Configuration des cibles de PDU de rack (barrette d'alimentation)

KX II permet de connecter des PDU de rack (barrettes d'alimentation) à des ports KX II. La configuration des PDU de rack KX II est effectuée à partir de la page Port Configuration de KX II.

Connexion d'une PDU de rack

Les PDU (barrettes d'alimentation) de rack de la série PX de Raritan sont connectées au dispositif Dominion à l'aide du CIM D2CIM-PWR.

Pour connecter la PDU de rack :

1. Branchez le connecteur mâle RJ-45 du module D2CIM-PWR au connecteur RJ-45 femelle du port série de la PDU de rack.
2. Branchez le connecteur RJ-45 femelle du module D2CIM-PWR à n'importe quel connecteur femelle du port système du dispositif KX II au moyen d'un câble Cat 5 droit.
3. Branchez un cordon d'alimentation CA au serveur cible et à une prise de PDU de rack disponible.
4. Connectez la PDU de rack à une source d'alimentation CA.
5. Allumez le dispositif.

Appellation des PDU de rack (page Port pour les barrettes d'alimentation)

Remarque : les PDU de rack PX (barrettes d'alimentation) peuvent être nommées dans PX, ainsi que dans KX II.

Lorsque la PDU de rack à distance Raritan est connectée à KX II, elle apparaîtra dans la page Port Configuration. Cliquez sur le nom du port d'alimentation pour y accéder. Les champs Type et Name sont déjà renseignés.

Remarque : le type de CIM ne peut pas être modifié.

Les données suivantes sont affichées pour chaque prise de la PDU de rack : [Outlet] Number (Numéro [de prise]), Name (Nom) et Port Association (Association de port).

Utilisez cette page pour nommer la PDU de rack et ses prises. Les noms peuvent comporter jusqu'à 32 caractères alphanumériques et spéciaux.

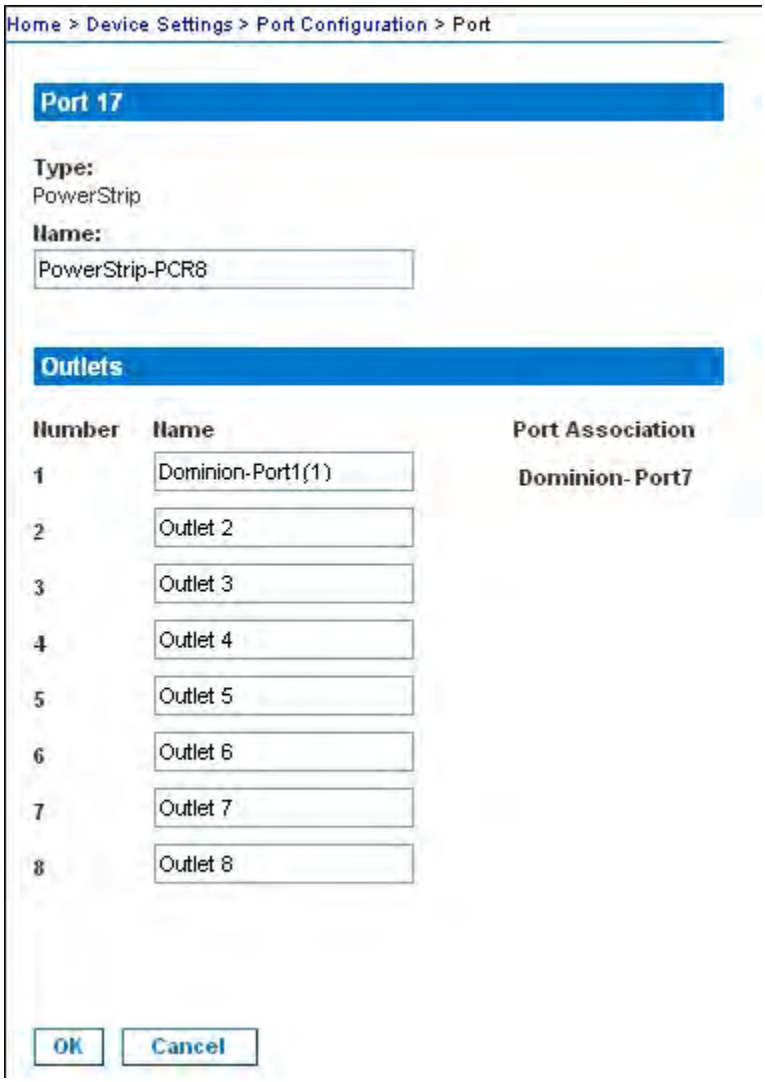
Remarque : lorsqu'une PDU de rack est associée à un serveur cible (port), le nom de la prise est remplacé par celui du serveur cible même si vous avez donné un autre nom à la prise.

Pour nommer la PDU de rack et ses prises :

Remarque : CommandCenter Secure Gateway ne reconnaît pas les noms de PDU de rack contenant des espaces.

1. Entrez le nom de la PDU de rack (si nécessaire).
2. Modifiez le nom de la prise, le cas échéant. (Le nom des prises est par défaut leur numéro.)

3. Cliquez sur OK.



Association de prises à des serveurs cible

La page Port s'ouvre lorsque vous cliquez sur un port de la page Port Configuration (Configuration des ports). Depuis cette page, vous pouvez effectuer des associations d'alimentation, remplacer le nom du port par un autre plus parlant et mettre à jour les paramètres du serveur cible si vous utilisez le module CIM D2CIM-VUSB. Les champs (CIM) Type (Type (de CIM)) et (Port) Name (Nom (du port)) sont déjà renseignés ; notez que le type de CIM n'est modifiable.

Un serveur peut avoir jusqu'à quatre prises d'alimentation et vous pouvez associer une PDU de rack (barrette d'alimentation) différente à chacune d'elles. Depuis cette page, vous pouvez définir des associations permettant de mettre sous tension, hors tension le serveur ou d'en effectuer l'alimentation cyclique à partir de la page Port Access (Accès aux ports).

Pour utiliser cette fonction, vous aurez besoin des éléments suivants :

- PDU de rack à distance Raritan
- CIM d'alimentation (D2CIM-PWR)

Pour effectuer des associations d'alimentation (associer des prises de PDU de rack à des serveurs cible KVM) :

Remarque : lorsqu'une PDU de rack est associée à un serveur cible (port), le nom de la prise est remplacé par celui du serveur cible (même si vous avez donné un autre nom à la prise).

1. Choisissez la PDU de rack dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
2. Pour cette PDU de rack, choisissez la prise dans la liste Outlet Name (Nom de prise).
3. Répétez les étapes 1 et 2 pour toutes les associations d'alimentation souhaitées.
4. Cliquez sur OK. Un message de confirmation s'affiche.

Pour renommer le port :

1. Tapez un nom descriptif dans le champ Name ; le nom du serveur cible, par exemple. Ce nom peut comporter jusqu'à 32 caractères alphanumériques et spéciaux.
2. Cliquez sur OK.

Suppression des associations d'alimentation

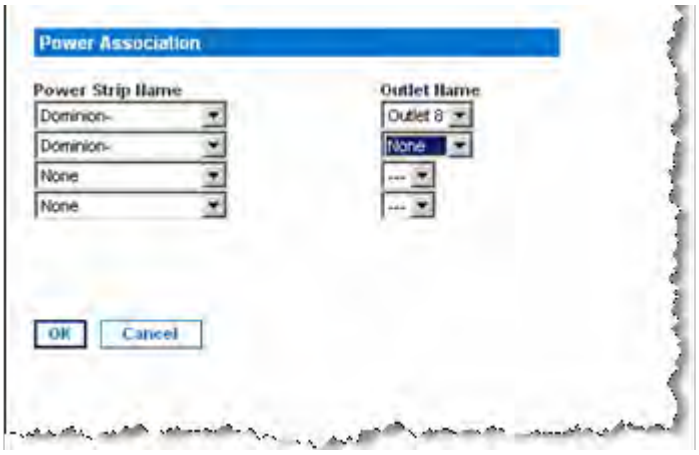
Lors de la déconnexion des serveurs cible et/ou des PDU de rack du dispositif, toutes les associations d'alimentation doivent être supprimées en premier lieu. Lorsqu'une cible est associée à une PDU de rack et que la première est supprimée du dispositif, l'association d'alimentation demeure. Vous ne pouvez alors pas accéder à la configuration des ports pour ce serveur cible déconnecté dans Device Settings (Paramètres du dispositif) afin de supprimer correctement l'association d'alimentation.

Pour supprimer une association de PDU de rack :

1. Sélectionnez la PDU de rack concernée dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
2. Pour cette PDU de rack, sélectionnez la prise souhaitée dans la liste Outlet Name (Nom de prise).
3. Dans la liste déroulante Outlet Name, sélectionnez None (Néant).
4. Cliquez sur OK. L'association PDU de rack-prise est supprimée et un message de confirmation s'affiche.

Pour supprimer l'association d'une PDU de rack si cette dernière a été supprimée de la cible :

1. Cliquez sur Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports), puis sur la cible active.
2. Associez la cible active au port d'alimentation déconnecté. Ceci rompra l'association d'alimentation de la cible déconnectée.
3. Enfin, associez la cible active au port d'alimentation correct.



Configuration des châssis de lames

Outre les serveurs standard et les PDU de rack (barrettes d'alimentation), vous pouvez gérer les châssis de lames branchés sur un port de dispositif KX II. Huit châssis de lames au plus peuvent être gérés à un moment donné.

Le châssis de lames doit être configuré comme sous-type de châssis de lames. S'il est pris en charge, le type du châssis de lames est détecté automatiquement à sa connexion. Sinon, la lame doit être configurée manuellement.

Lorsqu'un châssis de serveurs lames est détecté, un nom par défaut lui est attribué et il s'affiche sur la page Port Access avec les serveurs cible standard et les PDU de rack. Reportez-vous à ***Page Port Access (Affichage de la console distante)*** (à la page 56).

Le châssis de lames s'affiche dans une liste hiérarchique extensible sur la page Port Access ; le châssis de lames est placé à la racine de la hiérarchie et chaque lame est libellée et affichée sous la racine. Utilisez l'icône Expand Arrow (flèche de développement) ▸ en regard du châssis racine pour afficher les lames individuelles.

Remarque : pour afficher le châssis de lames dans l'ordre hiérarchique, ses sous-types doivent être configurés.

A l'exception des châssis de lames HP et UCS de Cisco®, les châssis de lames génériques, IBM® et Dell® sont configurés sur la page Port. Le port connecté au châssis de lames doit être configuré avec le modèle du châssis. Les informations spécifiques que vous pouvez configurer dépendent de sa marque du serveur lames que vous utilisez. Pour obtenir des informations particulières concernant chaque châssis de lame pris en charge, reportez-vous à la rubrique correspondante dans cette section de l'aide.

Les châssis de lames ci-après sont pris en charge :

- IBM BladeCenter® modèles E et H
- Dell PowerEdge® 1855, 1955 et M1000e

Une option Generic permet de configurer un châssis de lame qui ne figure pas dans la liste qui précède. Les serveurs lames HP BladeSystem c3000 et c7000, et Cisco UCS sont pris en charge via des connexions individuelles du dispositif Dominion à chaque lame. Les ports sont regroupés dans une représentation de châssis à l'aide de la fonction Port Group Management (Gestion des groupes de ports).

Remarque : les lames Dell PowerEdge 1855/1955 permettent également une connexion de chaque lame à un port du dispositif Dominion. Dans ce cas, les lames peuvent également être rassemblées pour créer des groupes de serveurs lames.

Deux modes d'opération sont possibles pour les châssis de lames : la configuration manuelle et la détection automatique, selon les capacités du châssis de lames. Lorsqu'un châssis de lames est configuré pour la détection automatique, le dispositif Dominion effectue un suivi et une mise à jour des actions suivantes :

- lorsqu'un nouveau serveur lame est ajouté au châssis ;
- lorsqu'un serveur lame existant est retiré du châssis.

Remarque : dans le cas des modèles E et H d'IBM Blade Center, KX II prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

L'utilisation des séquences de raccourcis-clavier pour commuter l'accès KVM sur un châssis de lames est également prise en charge. Lorsqu'un châssis de lames permet aux utilisateurs de sélectionner une séquence de raccourcis-clavier, ces options seront fournies sur la page Port Configuration. Lorsqu'un châssis de lames est fourni avec des séquences de raccourcis-clavier prédéfinies, ces séquences seront entrées sur la page Port Configuration lorsque le châssis sera sélectionné. Par exemple, la séquence de raccourcis-clavier pour commuter l'accès KVM sur une unité IBM BladeCenter H est Verr num+ Verr num + Numéro de connecteur, cette séquence est donc appliquée par défaut lorsqu'une unité IBM BladeCenter H est sélectionnée pendant la configuration. Consultez la documentation de votre châssis de lames pour plus d'informations sur les séquences de raccourcis-clavier.

Vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Au niveau du châssis, quatre liens au plus peuvent être définis. Le premier est réservé à la connexion à l'interface utilisateur graphique du module d'administration du châssis de lames. Par exemple, ce lien peut être utilisé par l'assistance technique pour vérifier rapidement la configuration d'un châssis.

Les châssis de lames peuvent être gérés à partir de Virtual KVM Client (VKC), d'Active KVM Client (AKC), de Multi-Platform Client (MPC) de Raritan et de CC-SG. La gestion des serveurs lames via VKC, AKC et MPC est identique à la gestion des serveurs cible standard. Reportez-vous à **Utilisation des serveurs cible** (à la page 49) et au **manuel de l'administrateur de CC-SG** pour en savoir plus. Les changements apportés à la configuration du châssis de lames seront reportés dans ces applications clientes.

Important : lorsque le CIM reliant le châssis de lames au dispositif Dominion est mis hors tension ou déconnecté du dispositif, toutes les connexions au châssis de lames établies seront abandonnées. Lorsque le CIM est reconnecté ou mis sous tension, vous devrez établir à nouveau les connexions.

Important : Si vous déplacez un châssis de lames d'un port Dominion à un autre, les interfaces ajoutées au nœud du châssis

dans CC-SG seront perdues dans ce dernier. Toutes les autres informations seront conservées.

Configuration des châssis de lames génériques

La sélection de Generic Blade Chassis (Châssis de lames génériques) ne permet qu'une configuration manuelle. Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 235), ***CIM pris en charge pour les châssis de lames*** (à la page 236) et ***Configurations requises et recommandées de châssis de lames*** (à la page 239) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 357) pour plus d'informations à ce sujet lors de l'utilisation des châssis Dell® avec KX II.

Pour configurer un châssis :

1. Connectez le châssis de lames à KX II. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 35) pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez Generic dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).
6. Configurez le châssis de lames, le cas échéant.
   a. Switch Hot Key Sequence - Définissez la séquence de raccourcis-clavier qui permettra de commuter de KVM au châssis de lames. La séquence de raccourcis-clavier de commutation doit correspondre à celle utilisée par le module KVM dans le châssis de lames.
   b. Administrative Module Primary IP Address/Host Name - Sans objet.
   c. Maximum Number of Slots - Entrez le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames.
   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.
   e. Username - Sans objet.
   f. Password - Sans objet.
7. Modifiez le nom du châssis de lames, le cas échéant.

8. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.
9. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   ---

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.
   b. URL - Entrez l'URL de l'interface. **Obligatoire**
   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface. **Facultatif**
   d. Password - Entrez le mot de passe utilisé à accéder à l'interface. **Facultatif**

   Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

   ---

   e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 231) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web. **Facultatif**
10. Les informations de profil USB ne s'appliquent pas à une configuration générique.

11. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
12. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.
13. Sélectionnez la résolution d'affichage native des CIM dans la liste déroulante Display Native Resolution. Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM. Si aucune sélection n'est effectuée, la résolution par défaut 1280 x 1024 est utilisée.
14. Cliquez sur OK pour enregistrer la configuration.

Configuration des châssis de lames Dell

Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 235), ***CIM pris en charge pour les châssis de lames*** (à la page 236) et ***Configurations requises et recommandées de châssis de lames*** (à la page 239) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 357) pour plus d'informations à ce sujet lors de l'utilisation des châssis Dell® avec KX II.

Pour ajouter un châssis de lame :

1. Connectez le châssis de lames à KX II. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 35) pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez le modèle de châssis de lames Dell dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).

Pour configurer un Dell PowerEdge M1000e :

1. Si vous avez sélectionné Dell PowerEdge™ M1000e, la détection automatique est disponible. Configurez le châssis de lames, le cas échéant. Avant de configurer un châssis de lames pouvant être détecté automatiquement, celui-ci doit accepter les connexions SSH sur le numéro de port désigné (reportez-vous à ***Services du dispositif*** (à la page 181)). De plus, il faut créer au préalable un compte d'utilisateur disposant d'informations d'authentification sur le châssis de lames.
   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames. La séquence de raccourcis-clavier de commutation doit correspondre à celle utilisée par le module KVM dans le châssis de lames.
   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.
   c. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. **Obligatoire pour le mode de détection automatique**
   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Changez ce numéro, le cas échéant. **Obligatoire pour le mode de détection automatique**
   e. Username - Entrez le nom d'utilisateur servant à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**
   f. Password - Entrez le mot de passe utilisé à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**
2. Si vous souhaitez que KX II détecte automatiquement les lames du châssis, cochez la case Blade Auto-Discovery (Détection automatique des lames), puis cliquez sur Discover Blades on Chassis Now (Détecter les lames sur le châssis maintenant). Lorsque les lames sont détectées, elles s'affichent sur la page.
3. Modifiez le nom du châssis de lames, le cas échéant. Si le châssis porte déjà un nom, ce champ est automatiquement renseigné. Sinon, KX II attribue un nom au châssis. La convention d'appellation par défaut pour les châssis de lames par KX II est Blade_Chassis_Port#.
4. En mode manuel, indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

En mode de détection automatique, la case Installed affiche les connecteurs contenant des lames pendant la détection.

5. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

   b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 241) pour obtenir des exemples de configuration pour le Dell M1000e.

   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

   d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

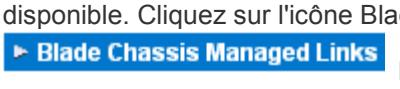
   Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

   e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 231) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

6. Les profils USB ne s'appliquent pas aux châssis Dell.

7. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
8. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.
9. Sélectionnez la résolution d'affichage native des CIM dans la liste déroulante Display Native Resolution. Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM. Si aucune sélection n'est effectuée, la résolution par défaut 1280 x 1024 est utilisée.
10. Cliquez sur OK pour enregistrer la configuration.

Pour configurer un Dell PowerEdge 1855/1955 :

1. Si vous avez sélectionné Dell 1855/1955, la détection automatique *n'est pas disponible*. Configurez le châssis de lames, le cas échéant.
   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames. Pour les modèles Dell 1855/1955, KX II bloque toutes les séquences de raccourci-clavier existantes. Si vous appliquez une configuration générique au Dell 1855, seul un raccourci-clavier existant est bloqué.
   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.
   c. Administrative Module Primary IP Address/Host Name - Sans objet.
   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.
   e. Username - Sans objet.
   f. Password - Sans objet.
2. Modifiez le nom du châssis de lames, le cas échéant.
3. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.
4. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à Exemples de formats d'URL de châssis de lames pour obtenir des exemples de configuration pour le Dell PowerEdge 1855/1955.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 231) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

5. Les profils USB ne s'appliquent pas aux châssis Dell.

6. Cliquez sur OK pour enregistrer la configuration.

Configuration des châssis de lames génériques IBM

Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 235), ***CIM pris en charge pour les châssis de lames*** (à la page 236) et ***Configurations requises et recommandées de châssis de lames*** (à la page 239) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 357) pour plus d'informations à ce sujet lors de l'utilisation des châssis Dell® avec KX II.

Pour ajouter un châssis de lame :

1. Connectez le châssis de lames à KX II. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 35) pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez le modèle de châssis de lames IBM® dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).

Pour configurer un IBM BladeCenter H et E :

1. Si vous avez sélectionné IBM BladeCenter® H ou E, la détection automatique est disponible. Configurez le châssis de lames, le cas échéant. Avant de configurer un châssis de lames pouvant être détecté automatiquement, celui-ci doit accepter les connexions SSH sur le numéro de port désigné (reportez-vous à ***Services du dispositif*** (à la page 181)). De plus, il faut créer au préalable un compte d'utilisateur disposant d'informations d'authentification sur le châssis de lames. KX II ne prend en charge la détection automatique que pour AMM[1].
   a. Switch Hot Key Sequence - Prédéfinie.
   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.
   c. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. **Obligatoire pour le mode de détection automatique**

d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Changez ce numéro, le cas échéant. **Obligatoire pour le mode de détection automatique**

e. Username - Entrez le nom d'utilisateur servant à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

f. Password - Entrez le mot de passe utilisé à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

2. Si vous souhaitez que KX II détecte automatiquement les lames du châssis, cochez la case Blade Auto-Discovery (Détection automatique des lames), puis cliquez sur Discover Blades on Chassis Now (Détecter les lames sur le châssis maintenant). Lorsque les lames sont détectées, elles s'affichent sur la page.

3. Modifiez le nom du châssis de lames, le cas échéant. Si le châssis porte déjà un nom, ce champ est automatiquement renseigné. Sinon, KX II attribue un nom au châssis. La convention d'appellation par défaut pour les châssis de lames par KX II est Blade_Chassis_Port#.

4. En mode manuel, indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

   En mode de détection automatique, la case Installed affiche les connecteurs contenant des lames pendant la détection.

5. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

---

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 241) pour obtenir des exemples de configuration pour l'IBM BladeCenter.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 231) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

6. Le cas échéant, définissez le profil USB pour le châssis de lames ou sélectionnez un profil USB existant. Cliquez sur l'icône USB Profiles for Port (Profils USB pour le port) 

ou sur l'icône Apply Select Profiles to Other Ports (Appliquer les profils sélectionnés aux autres ports)


pour développer ces sections de la page. Reportez-vous à ***Configuration des profils USB (page Port)*** (à la page 243).

7. Cliquez sur OK pour enregistrer la configuration.

Pour configurer un IBM BladeCenter (autre) :

1. Si vous avez sélectionné IBM BladeCenter (Other), la détection automatique *n'est pas* disponible. Configurez le châssis de lames, le cas échéant.

   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames.

b. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames.Sans objet.

c. Maximum Number of Slots - Entrez le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames.

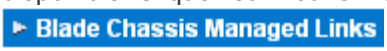
d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.

e. Username - Sans objet.

f. Password - Sans objet.

2. Modifiez le nom du châssis de lames, le cas échéant.

3. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames. S'ils ne sont pas nommés, KX II leur attribue un nom. La convention d'appellation par défaut des serveurs lames est Blade_Chassis_Port#_Slot#.

4. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

---

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 241) pour obtenir des exemples de configuration pour l'IBM BladeCenter.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 231) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

5. Les profils USB ne sont pas utilisés par les configurations IBM (Other).
6. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
7. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.
8. Sélectionnez la résolution d'affichage native des CIM dans la liste déroulante Display Native Resolution. Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM. Si aucune sélection n'est effectuée, la résolution par défaut 1280 x 1024 est utilisée.
9. Cliquez sur OK pour enregistrer la configuration.

Astuces pour ajouter une interface Navigateur Web

Vous pouvez ajouter une interface navigateur Web pour créer une connexion à un dispositif intégrant un serveur Web. Une interface navigateur Web permet également la connexion à une application Web quelconque, telle que celle associée à une carte de processeur RSA, DRAC ou ILO.

DNS doit être configuré pour résoudre les URL. Les adresses IP ne requièrent pas la configuration de DNS.

Pour ajouter une interface navigateur Web :

1. Le nom par défaut d'une interface navigateur Web est fourni. Les cas échéant, vous pouvez modifier le nom dans le champ Name.
2. Entrez l'URL ou le nom du domaine de l'application Web dans le champ URL. Vous devez entrer l'URL à laquelle l'application Web doit lire le nom d'utilisateur et le mot de passe.

Suivez les exemples ci-après pour entrer des formats corrects :

- http(s)://192.168.1.1/login.asp
- http(s)://www.example.com/cgi/login
- http(s)://example.com/home.html

3. Entrez les nom d'utilisateur et mot de passe autorisant l'accès à cette interface. **Facultatif**
4. Si un nom d'utilisateur et un mot de passe ont été entrés, dans Username Field et Password Field, tapez le nom des champs de nom d'utilisateur et de mot de passe utilisés dans l'écran de connexion de l'application Web. Vous devez visualiser la source HTML de l'écran de connexion pour trouver le nom des champs, et non leur libellé.

Astuce pour repérer le nom des champs :

- Dans le code source HTML de la page de connexion de l'application Web, recherchez le libellé du champ, tel que Username et Password.
- Examinez ensuite le code adjacent pour trouver une balise ressemblant à : name="user". Le mot entre guillemets est le nom du champ.

Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)

KX II prend en charge l'agrégation des ports connectés à certains types de lames dans un groupe représentant le châssis de lames ; particulièrement, les lames Cisco® USC, HP® BladeServer et Dell® PowerEdge™ 1855/1955 lorsque le Dell PowerEdge 1855/1955 est connecté de chaque lame à un port de KX II.

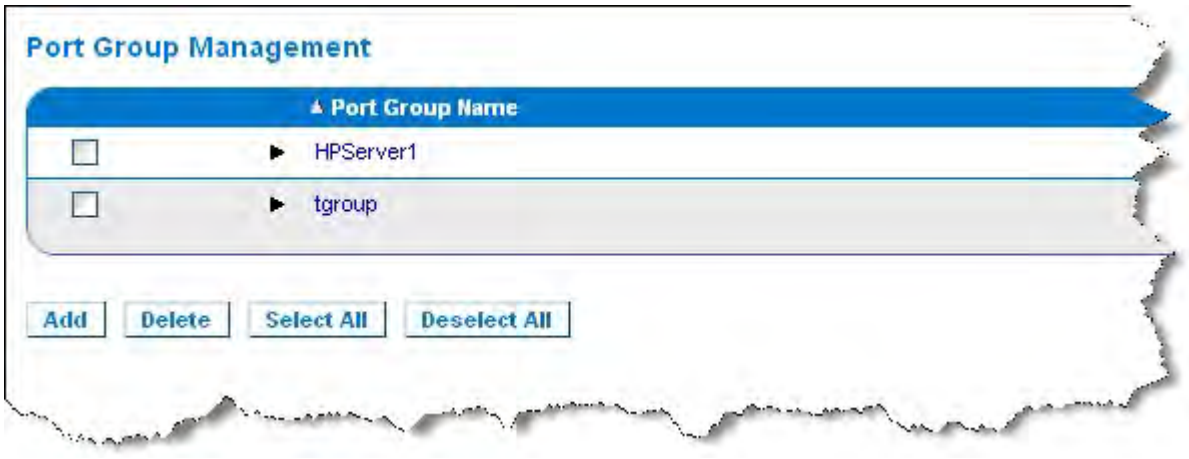
Le châssis est identifié par un nom de groupe de ports et ce groupe est désigné comme Blade Server Group (Groupe de serveurs lames) sur la page Port Group Management (Gestion des groupes de ports). Les groupes de ports comprennent uniquement des ports configurés comme ports KVM standard, non des ports configurés comme châssis de lames. Un port ne peut être membre que d'un seul groupe.

Les ports connectés aux modules KVM intégrés dans un châssis de lames sont configurés comme sous-types de châssis de lames. Ces ports peuvent être inclus dans des groupes de ports.

Lorsque les ports KX II sont connectés à des modules KVM intégrés dans un châssis de lames et à des lames individuelles, ils sont configurés comme sous-types de châssis de lames. Ces ports ne peuvent pas être inclus dans des groupes de ports et n'apparaissent pas dans la liste Available (Disponibles) de la section Select Ports for Group (Sélectionner des ports pour le groupe).

Lorsqu'un port KVM standard a été inclus dans un groupe de ports, puis réorienté pour être utilisé comme sous-type de châssis de lames, il doit d'abord être supprimé du groupe de ports.

Les groupes de ports sont restaurés à l'aide de l'option Backup and Restore (Sauvegarde et restauration) (reportez-vous à ***Backup and Restore (Sauvegarde et restauration)*** (à la page 285)).



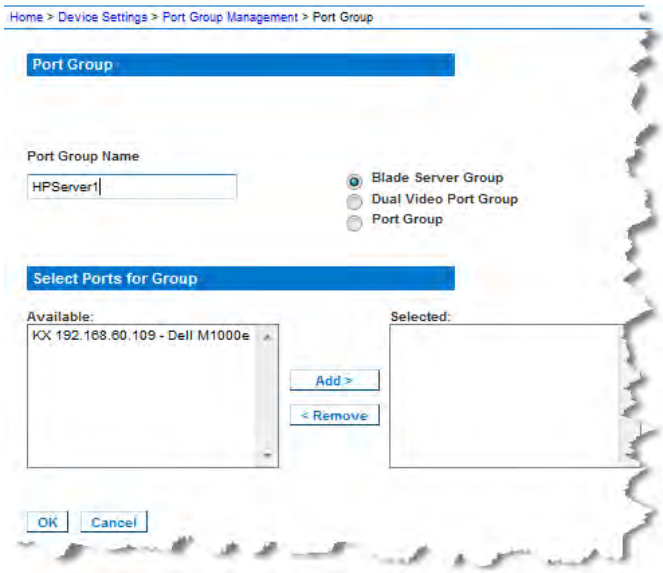
Pour ajouter un groupe de ports :

1. Cliquez sur Device Settings (Paramètres du dispositif) > Port Group Management (Gestion des groupes de ports) pour ouvrir la page Port Group Management.
2. Cliquez sur Add (Ajouter) pour ouvrir la page Port Group (Groupe de ports).
3. Entrez un nom de groupe de ports. Les noms de groupes de ports ne sont pas sensibles à la casse et peuvent contenir jusqu'à 32 caractères.
4. Cochez la case Blade Server Group (Groupe de serveurs lames).

   Si vous souhaitez indiquer que ces ports sont reliés à des lames hébergées dans un châssis de lames (par exemple, HP c3000 ou Dell PowerEdge 1855), sélectionnez la case à cocher Blade Server Group.

   Remarque : ceci est particulièrement important pour les utilisateurs de CC-SG qui souhaitent organiser les lames HP par châssis, même si chaque lame a sa propre connexion à un port de KX II.

5. Cliquez sur un port dans le champ Available (Disponibles) de la section Select Ports for Group (Sélectionner des ports pour le groupe). Cliquez sur Add pour ajouter le port au groupe. Le port est placé dans le champ Selected (Sélectionnés).
6. Cliquez sur OK pour ajouter le groupe de ports.



Pour modifier les informations relatives à un groupe de ports :

1. Sur la page Port Group Management (Gestion des groupes de ports), cliquez sur le lien du groupe de ports que vous souhaitez modifier. La page Port Group (Groupe de ports) s'ouvre.
2. Modifiez les informations selon les besoins.
3. Cliquez sur OK pour enregistrer les modifications.

Pour supprimer un groupe de ports :

1. Cliquez sur la page Port Group Management (Gestion des groupes de ports), cochez la case du groupe de ports que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).
3. Cliquez sur OK dans le message d'avertissement.

Modèles de châssis de lames pris en charge

Ce tableau présente des modèles de châssis de lames pris en charge par KX II et les profils correspondant qui devraient être sélectionnés selon le modèle de châssis lors de leur configuration dans l'application KX II. Une liste de ces modèles peut être sélectionnée sur la page Port Configuration (Configuration des ports) dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames), qui apparaît lorsque le bouton radio Blade Chassis est sélectionné. Pour obtenir des informations concernant la configuration de chaque châssis de lames, reportez-vous à la rubrique correspondante dans cette section de l'aide.

Modèle de châssis de lames	Profil de KX II
Cisco® USC	Configurez à l'aide des fonctions de gestion des groupes de ports. Reportez-vous à ***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)*** (à la page 233).
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (autre)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (autre)
IBM BladeCenter HT	IBM (autre)

Modèle de châssis de lames	Profil de KX II
IBM BladeCenter E	IBM BladeCenter E
HP®	Configurez à l'aide des fonctions de gestion des groupes de ports. Reportez-vous à ***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)*** (à la page 233).

CIM pris en charge pour les châssis de lames

Les CIM suivants sont pris en charge pour les châssis de lames gérés via KX II:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Le tableau suivant contient les CIM pris en charge pour chaque modèle de châssis de lames supporté par KX II.

Châssis de lames	Méthode de connexion	CIM recommandés
Générique	Si un D2CIM-VUSB ou D2CIM-DVUSB est utilisé lors de la connexion à un châssis de lames configuré en tant que Générique, vous pouvez sélectionner les profils USB sur la page Port Configuration (Configuration des ports) et le menu USB Profile du client. Toutefois, la fonction Support virtuel n'est pas prise en charge pour les châssis de lames génériques et le menu Virtual Media est désactivé sur le client.	• DCIM-PS2 • DCIM-USBG2
Cisco® UCS Server Chassis	Le câble Cisco KVM (N20-BKVM) vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide d'installation de Cisco UCS 5108 Server Chassis*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB

Châssis de lames	Méthode de connexion	CIM recommandés
Dell® PowerEdge™ 1855	Inclut un des trois modules KVM : • Module de commutateur Ethernet KVM analogique (standard) • Module de commutateur KVM à accès numérique (facultatif) • Module de commutateur KVM (standard sur les systèmes antérieurs à avril 2005) Ces commutateurs présentent un connecteur personnalisé autorisant la connexion de deux dispositifs PS/2 et d'un dispositif vidéo au système. Source : *Manuel d'utilisation de Dell PowerEdge 1855*	• DCIM-PS2
Dell PowerEdge 1955	Un des deux types de modules KVM peut être installé : • Module de commutateur KVM analogique • Module de commutateur KVM à accès numérique Ces deux modules autorisent la connexion d'un clavier, d'une souris et d'un écran PS/2 compatibles au système (à l'aide d'un câble personnalisé fourni avec le système). Source : *Manuel d'utilisation de Dell PowerEdge 1955*	• DCIM-PS2
Dell PowerEdge M1000e	Le module commutateur KVM (iKVM) est intégré à ce châssis. L'iKVM est compatible avec les périphériques suivants : • claviers USB, dispositifs de pointage USB • écrans VGA avec prise en charge DDC Source : *Guide d'utilisation du contrôleur de gestion de châssis Dell, version de firmware 1.0*	• DCIM-USBG2
HP® BladeSystem c3000	Le câble HP c-Class Blade SUV vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des châssis de lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide de maintenance et de service du serveur lame HP ProLiant™ BL480c*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (pour un fonctionnement de port KVM standard sans option KVM)

Châssis de lames	Méthode de connexion	CIM recommandés
HP BladeSystem c7000	Le câble HP c-Class Blade SUV vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide de maintenance et de service du serveur lame HP ProLiant BL480c*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (pour un fonctionnement de port KVM standard)
IBM® BladeCenter® S	Le module AMM (de gestion avancée) offre des fonctions de gestion du système et de multiplexage de clavier/vidéo/souris (KVM) pour tous les châssis de lames. Les connexions AMM incluent : un port série, une connexion vidéo, un port de gestion à distance (Ethernet) et deux ports USB v2.0 pour un clavier et une souris. Source : *Mise en œuvre du châssis IBM BladeCenter S*	• DCIM-USBG2
IBM BladeCenter H	Le châssis BladeCenter H est livré en standard avec un module AMM. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	Le modèle de châssis actuel BladeCenter E (8677-3Rx) est livré en standard avec un module AMM. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	Le châssis BladeCenter T est livré en standard avec un module AMM. Contrairement au châssis BladeCenter standard, le module KVM et le module de gestion du châssis BladeCenter T sont des composants distincts. L'avant du module de gestion ne comporte des voyants que pour l'affichage de l'état. Toutes les connexions Ethernet et KVM sont alimentées par l'arrière aux modules LAN et KVM. Le module KVM est un module à remplacement à chaud à l'arrière du châssis, fournissant deux connecteurs PS/2 pour un clavier et une souris, un panneau d'état du système et un connecteur vidéo HD-15. Source : *Produits et technologie IBM*	• DCIM-PS2

Châssis de lames	Méthode de connexion	CIM recommandés
	BladeCenter	
IBM BladeCenter HT	Le châssis BladeCenter HT est livré en standard avec un module AMM. Ce module permet de gérer le châssis et offre la fonction KVM locale. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2

Remarque : pour prendre en charge la détection automatique, les modèles H et E d'IBM BladeCenter doivent utiliser AMM avec la version de firmware BPET36K ou supérieure.

Remarque : dans le cas des modèles E et H d'IBM Blade Center, KX II prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Remarque : L'audio est désactivé pour toutes les cibles de commutateur KVM.

Configurations requises et recommandées de châssis de lames

Ce tableau contient des informations sur les limitations et les contraintes qui s'appliquent à la configuration des châssis de lames pour qu'ils fonctionnent avec le dispositif KX II. Raritan vous recommande de suivre toutes les informations suivantes.

Châssis de lames	Action requise/recommandée
Dell® PowerEdge™ M1000e	• Désactivez l'écran de veille de l'interface utilisateur d'iKVM. Sinon, une boîte de dialogue d'autorisation s'affiche et empêche le fonctionnement correct d'iKVM. • Quittez le menu de l'interface utilisateur d'iKVM avant de connecter le châssis Dell à un CIM Raritan. Sinon, iKVM risque de ne pas fonctionner correctement. • Configurez le menu principal de l'interface utilisateur d'iKVM pour sélectionner les lames cible par connecteur, et non par nom. Sinon, iKVM risque de ne pas fonctionner correctement. • *Ne désignez aucun* connecteur pour les opérations d'analyse dans le menu Setup Scan (Paramétrage de l'analyse) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. • *Ne désignez aucun* connecteur pour les opérations de clavier/souris de diffusion dans le menu Setup Broadcast (Paramétrage de la diffusion) de l'interface utilisateur d'iKVM.

Châssis de lames	Action requise/recommandée
	Sinon, iKVM risque de ne pas fonctionner correctement. • Désignez une seule séquence de touches pour appeler l'interface utilisateur d'iKVM. Cette séquence doit également être identifiée au cours de la configuration des ports de KX II. Sinon, iKVM risque de fonctionner de manière erratique après une saisie sur le client. • Assurez-vous que l'option Front Panel USB/Video Enabled (USB/Vidéo du panneau avant activés) *n'est pas* sélectionnée au cours de la configuration d'iKVM via l'interface utilisateur de Dell CMC. Sinon, les connexions effectuées à l'avant du châssis auront priorité sur la connexion de KX II à l'arrière, ce qui empêcherait un fonctionnement correct d'iKVM. Un message s'affichera indiquant User has been disabled as front panel is currently active. (L'utilisateur a été désactivé car le panneau avant est actif.). • Assurez-vous que l'option Allow access to CMC CLI from iKVM (Autoriser l'accès à la CLI CMC depuis iKVM) *n'est pas* sélectionnée au cours de la configuration d'iKVM via l'interface utilisateur de Dell CMC. • Pour empêcher l'affichage de l'interface utilisateur iKVM lors de la connexion au châssis de lames, définissez l'option Screen Delay Time (Délai d'écran) sur 8 secondes. • La sélection de Timed (Différé) et Displayed (Affiché) est recommandé au cours du paramétrage de l'indicateur (Flag Setup) dans l'interface utilisateur d'iKVM. Vous pouvez ainsi confirmer visuellement la connexion au connecteur de lame souhaité.
Dell PowerEdge 1855/1955	• Désactivez l'écran de veille de l'interface utilisateur d'iKVM. Sinon, une boîte de dialogue d'autorisation s'affiche et empêche le fonctionnement correct d'iKVM. • Quittez le menu de l'interface utilisateur d'iKVM avant de connecter le châssis Dell à un CIM Raritan. Sinon, iKVM risque de ne pas fonctionner correctement. • Configurez le menu principal de l'interface utilisateur d'iKVM pour sélectionner les lames cible par connecteur, et non par nom. Sinon, iKVM risque de ne pas fonctionner correctement. • *Ne désignez aucun* connecteur pour les opérations d'analyse dans le menu Setup Scan (Paramétrage de l'analyse) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. • Pour empêcher l'affichage de l'interface utilisateur iKVM lors de la connexion au châssis de lames, définissez l'option Screen Delay Time (Délai d'écran) sur 8 secondes.

Châssis de lames	Action requise/recommandée
	• La sélection de Timed (Différé) et Displayed (Affiché) est recommandé au cours du paramétrage de l'indicateur (Flag Setup) dans l'interface utilisateur d'iKVM. Vous pouvez ainsi confirmer visuellement la connexion au connecteur de lame souhaité.
Détection automatique IBM®/Dell®	• Il est recommandé d'activer l'option Auto-Discovery (Détection automatique) lors de l'application des autorisations d'accès au niveau des lames. Sinon, définissez des autorisations d'accès au niveau du châssis de lames. • Secure Shell (SSH) doit être activé sur le module de gestion des châssis de lames. • Le port SSH configuré dans le module de gestion des châssis de lames doit correspondre au numéro de port saisi sur la page Port Configuration (Configuration des ports).
Support virtuel IBM KX2	• La fonction Support virtuel de KX II de Raritan n'est prise en charge que sur les modèles H et E d'IBM BladeCenter®. Elle requiert l'utilisation de D2CIM-DVUSB. Le connecteur USB à faible vitesse D2CIM-DVUSB noir est relié au module AMM (Administrative Management Module) à l'arrière de l'unité. Le connecteur USB à haute vitesse D2CIM-DVUSB gris est relié au tiroir de support (MT) à l'avant de l'unité. Un câble d'extension USB est nécessaire.
Cisco® UCS Server Chassis	• Le câble Cisco KVM (N20-BKVM) vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. • Source : Guide d'installation de Cisco UCS 5108 Server Chassis- DCIM-USBG2- D2CIM-VUSB- D2CIM-DVUSB

Remarque : tous les IBM BladeCenters utilisant AMM doivent utiliser la version de firmware BPET36K ou supérieure pour fonctionner avec KX II.

Remarque : dans le cas des modèles E et H d'IBM Blade Center, KX II prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Exemples de formats d'URL de châssis de lames

Ce tableau contient des exemples de formats d'URL de châssis de lames configurés dans KX II.

Châssis de lames	Exemple de format d'URL
Dell® M1000e	• URL : https://192.168.60.44/cgi-bin/webcgi/login

Châssis de lames	Exemple de format d'URL
	• Username (Nom d'utilisateur) : root • Username Field (Champ du nom d'utilisateur) : user • Password: calvin • Password Field (Champ du mot de passe) : password
Dell 1855	• URL : https://192.168.60.33/Forms/f_login • Username (Nom d'utilisateur) : root • Username Field (Champ du nom d'utilisateur) : TEXT_USER_NAME • Password: calvin • Password Field (Champ du mot de passe) : TEXT_PASSWORD
IBM® BladeCenter® E ou H	• http://192.168.84.217/private/welcome.ssi

Configuration des profils USB (page Port)

La sélection des profils USB disponibles pour un port s'effectue dans la section Select USB Profiles for Port de la page Port. Les profils USB choisis dans la page Port deviennent les profils disponibles à l'utilisateur dans VKC lors de la connexion à un serveur cible KVM depuis le port. Il s'agit par défaut du profil des systèmes d'exploitation Windows 2000®, Windows XP®, Windows Vista®. Pour plus d'informations sur les profils USB, reportez-vous à ***Profils USB*** (à la page 138).

Remarque : pour définir les profils USB d'un port, un CIM numérique, VM-CIM ou Dual VM-CIM doit être connecté et équipé d'un firmware compatible avec la version de firmware courante de KX II. Reportez-vous à **Mise à niveau des CIM** *(à la page 289).*

Les profils disponibles à affecter à un port apparaissent dans la liste Available (Disponibles) à gauche. Les profils sélectionnés pour une utilisation avec un port apparaissent dans la liste Selected à droite. Lorsque vous sélectionnez un profil dans une des listes, sa description et son utilisation apparaissent dans le champ Profile Description (Description du profil).

Outre la sélection d'un ensemble de profils pour les mettre à la disposition d'un port KVM, vous pouvez également spécifier le profil privilégié pour le port et appliquer les paramètres définis pour un port à d'autres ports KVM.

Remarque : reportez-vous à **Modes de souris lors de l'utilisation du profil USB Mac OS X avec DCIM-VUSB** *(à la page 147) pour plus d'informations sur l'utilisation du profil USB Mac OS-X® avec DCIM-VUSB ou DCIM-DVUSB.*

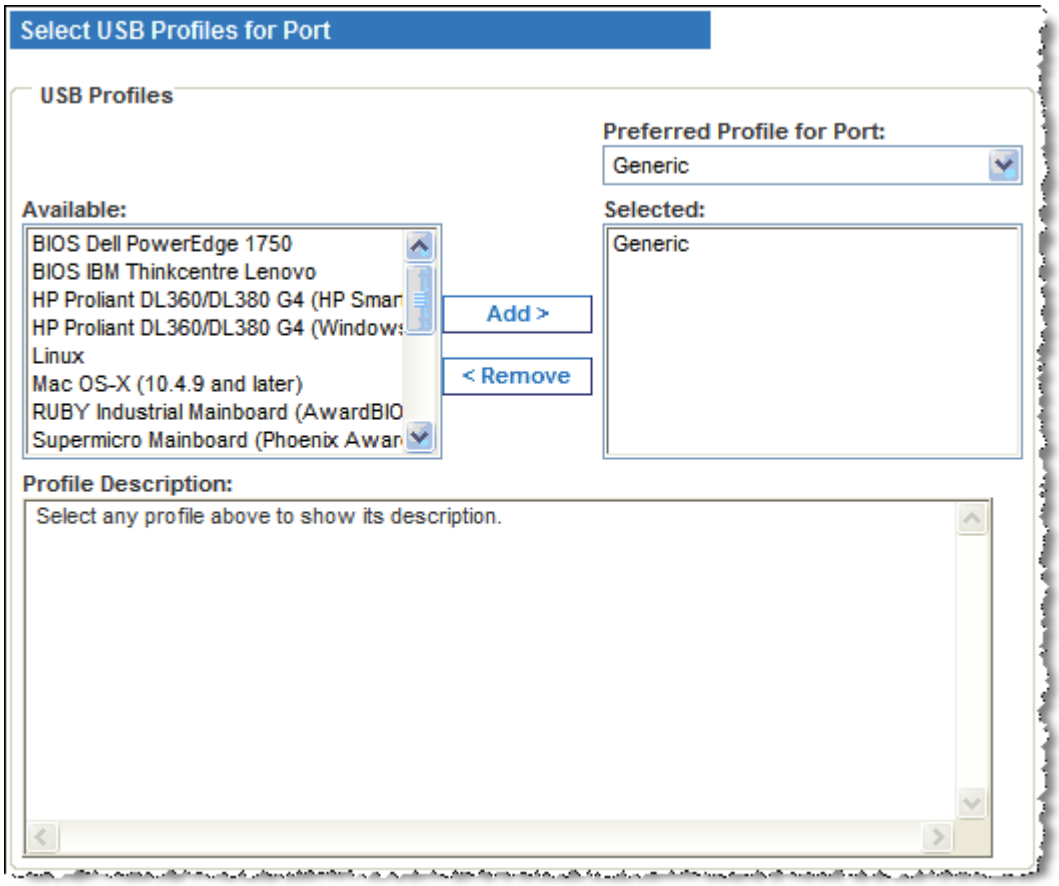
Pour ouvrir la page Port :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port KVM que vous souhaitez modifier. La page Port s'ouvre.

Pour sélectionner les profils USB d'un port KVM :

1. Dans la section Select USB Profiles for Port (Sélectionner les profils USB du port), choisissez un ou plusieurs profils USB dans la liste Available (Disponibles).
   - Appuyez sur la touche Maj+cliquez, et faites glisser pour sélectionner plusieurs profils contigus.

- Appuyez sur la touche Ctrl+cliquez pour sélectionner plusieurs profils non contigus.



2. Cliquez sur Add (Ajouter). Les profils sélectionnés apparaissent dans la liste Selected. Ces profils peuvent être utilisés pour le serveur cible KVM connecté au port.

Pour spécifier un profil USB privilégié :

1. Après avoir sélectionné les profils disponibles pour un port, choisissez-en un dans le menu Preferred Profile for Port (Profil privilégié pour le port). La valeur par défaut est Generic (Générique). Le profil sélectionné est utilisé lors de la connexion au serveur cible KVM. Le cas échéant, vous pouvez le remplacer par n'importe quel autre profil USB.

Pour retirer les profils USB sélectionnés :

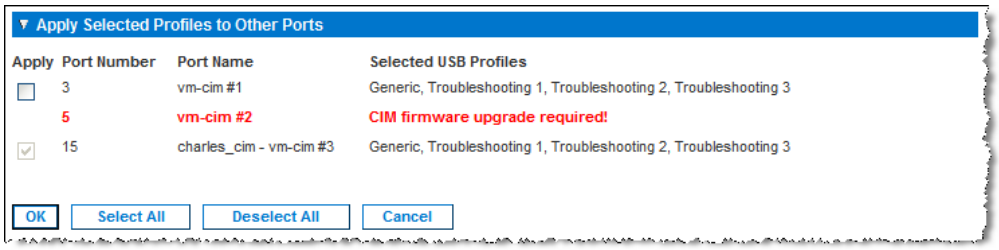
1. Dans la section Select USB Profiles for Port (Sélectionner les profils USB du port), choisissez un ou plusieurs profils USB dans la liste Selected (Sélectionnés).

- Appuyez sur la touche Maj+cliquez, et faites glisser pour sélectionner plusieurs profils contigus.
- Appuyez sur la touche Ctrl+cliquez pour sélectionner plusieurs profils non contigus.

2. Cliquez sur Remove (Supprimer). Les profils sélectionnés apparaissent dans la liste Available (Disponibles). Ils ne sont plus disponibles pour un serveur cible KVM connecté à ce port.

Pour appliquer une sélection de profils à plusieurs ports :

1. Dans la section Apply Selected Profiles to Other Ports (Appliquer les profils sélectionnés à d'autres ports), cochez la case Apply (Appliquer) pour chaque port KVM auquel vous souhaitez appliquer l'ensemble en cours de profils USB sélectionnés.



- Pour sélectionner tous les ports KVM, cliquez sur Select All (Tout sélectionner).
- Pour désélectionner tous les ports KVM, cliquez sur Deselect All (Tout désélectionner).

Configuration des paramètres du port local de KX II

A partir de la page de paramétrage du port local, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale de KX II, notamment le clavier, les raccourcis-clavier, 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 locale. De plus, vous pouvez modifier un profil USB depuis un port local.

Pour KX2-808, KX2-832 et KX2-864, vous pouvez également configurer le port local étendu sur la page Local Port Settings (Paramètres du port local). Le port local étendu peut être connecté à un commutateur ou à une station utilisateur Paragon pour prolonger le port local. Comme pour le port local standard, vous pouvez configurer les paramètres suivants : clavier, raccourcis-clavier, délai de commutation de l'écran, mode d'économie d'alimentation, résolution de l'interface utilisateur locale et authentification d'utilisateur locale. Le port local étendu peut être configuré depuis la console distante et la console locale. Reportez-vous à ***Paramètres des ports locaux standard et étendu de KX2-808, KX2-832 et KX2-864*** (à la page 250) pour en savoir plus sur le port local standard et sur le port local étendu.

Remarque : si le port local étendu est activé sur KX2-808, KX2-832 et KX2-864, et que rien n'est connecté au port, un délai de deux à trois secondes s'écoulera lors du passage à une cible via le port local.

Pour configurer les paramètres du port local :

Remarque : certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage doit se produire lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

1. Sélectionnez Device Settings (Paramètres du dispositif) > Local Port Configuration (Configuration du port local). La page des paramètres du port local s'ouvre.
2. Cochez la case en regard d'Enable Standard Local Port (Activer le port local standard) pour l'activer. Désélectionnez la case à cocher pour le désactiver. Par défaut, le port local standard est activé, mais peut être désactivé selon les besoins. Le navigateur redémarrera lorsque cette modification sera effectuée. Si vous utilisez la fonction multiniveau, cette fonction sera désactivée car les deux ne peuvent pas être utilisées simultanément.
3. Si vous utilisez un dispositif KX2-808, KX2-832 ou KX2-864, cochez la case en regard du port local étendu pour l'activer. Décochez les cases pour le désactiver. Si vous utilisez la fonction Carte à puce, le port local étendu doit être désactivé. Le navigateur redémarrera lorsque cette modification sera effectuée.

Si le port local standard et le port local étendu sont désactivés, les ports locaux ne sont pas accessibles. Si vous tentez d'accéder à un dispositif KX2-808, KX2-832 ou KX2-864 via un port local désactivé, un message indique que le dispositif est géré à distance et que la connexion est désactivée.

Remarque : si vous utilisez KX2-808, KX2-832 et KX2-864 comme dispositifs en niveau, vous devez les connecter au KX II de base via le port local étendu.

4. Si vous utilisez la fonction multiniveau, cochez la case Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local) et entrez le mot secret dans le champ Tier Secret (Secret du niveau). Pour paramétrer la fonction multiniveau, vous devez également configurer le dispositif de base sur la page Device Services (Services du dispositif). Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 183) pour plus d'informations sur la fonction multiniveau.
5. Le cas échéant, configurez les paramètres Local Port Scan Mode (Mode de balayage du port local). Ces paramètres s'appliquent à la fonction Scan Settings (Paramètres de balayage) accessible depuis la page Port. Reportez-vous à ***Balayage des ports*** (à la page 61).
   - Dans le champ Display Interval (10-255 sec) (Intervalle d'affichage (10 à 255 s), indiquez le nombre de secondes pendant lesquelles la cible sélectionnée doit rester affichée au centre de la fenêtre Port Scan (Balayage des ports).
   - Dans le champ Interval Between Ports (10 - 255 sec) (Intervalle entre les ports (10 à 255 s), indiquez l'intervalle de pause que doit respecter le dispositif entre les ports.
6. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - US
   - US/International (Anglais Etats-Unis/international)
   - United Kingdom
   - Français (France)
   - Allemand (Allemagne)
   - Japonais (JIS)
   - Chinois simplifié
   - Chinois traditionnel
   - Dubeolsik Hangul (Coréen)
   - Allemand (Suisse)
   - Portugais (Portugal)

- Norvégien (Norvège)
- Suédois (Suède)
- Danois (Danemark)
- Belge (Belgique)

Remarque : l'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de KX II.

Remarque : Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

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

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur 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

8. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre. Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local. Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à ***Exemples de touches de connexion*** (à la page 322) pour obtenir des exemples de séquences de touches de connexion. La touche de connexion fonctionne pour les serveurs standard et les châssis de lames.

9. 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).
10. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique :
    a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).
    b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.
11. Sélectionnez la résolution de la console locale de KX II dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
    - 800 x 600
    - 1024 x 768
    - 1280 x 1024
12. Sélectionnez le taux de rafraîchissement dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
    - 60 Hz
    - 75 Hz
13. Sélectionnez le type d'authentification d'utilisateur locale.
    - Local/LDAP/RADIUS. Il s'agit de l'option recommandée. Pour plus d'informations sur l'authentification, reportez-vous à ***Authentification à distance*** (à la page 45).
    - Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale. Cette option est recommandée pour les environnements sécurisés uniquement.
    - Cochez la case Ignore CC managed mode on local port (Ignorer le mode géré par CC sur le port local) si vous souhaitez un accès utilisateur local à KX II même si le dispositif est géré par CC-SG.

Remarque : si vous choisissez au départ d'ignorer le mode CC Manage (Gestion par CC) sur le port local, mais souhaitez par la suite un accès au port local, vous devez désactiver la gestion par CC-SG (depuis CC-SG) du dispositif. Vous pourrez alors cocher cette case.

Remarque : pour utiliser le port local standard et le port local étendu alors que KX II est géré par CC-SG, l'option Ignore CC managed mode on local port (Ignorer le mode géré par CC sur le port local) doit être sélectionnée. Cochez la case Ignore CC managed mode on local port si vous souhaitez un accès utilisateur local, via le port local standard ou étendu, à KX II même si le dispositif est géré par CC-SG. Ou, utilisez la fonction d'accès direct au dispositif sous la gestion de CC-SG.

14. Cliquez sur OK.

Paramètres des ports locaux standard et étendu de KX2-808, KX2-832 et KX2-864

KX2-808, KX2-832 et KX2-864 vous offrent deux options pour le port local : le port local standard et le port local étendu. Chacune de ces options de port est activée et désactivée depuis la console distante ou depuis la console locale sur la page Local Port Settings (Paramètres du port local). Pour en savoir plus, reportez-vous à ***Configuration des paramètres du port local de KX II*** (à la page 246).

Par défaut, le port local standard est activé et le port local étendu est désactivé. Si vous souhaitez prolonger le port local, activez le port local étendu et utilisez un câble Cat5/5e/6 pour effectuer la connexion à KX2-808, KX2-832 ou DKX2-864 depuis une unité Paragon II UMT, EUST, UST ou URKVMG.

Remarque : si le port local étendu est activé sur KX2-808, KX2-832 et KX2-864, et que rien n'est connecté au port, un délai de deux à trois secondes s'écoulera lors du passage à une cible via le port local.

Vous devez disposer des droits d'administrateur pour configurer ces options. Pour accéder à un port, vous ne devez entrer vos nom d'utilisateur et mot de passe qu'une seule fois. Vous n'avez pas à les entrer pour chaque port auquel vous accédez.

Reportez-vous à la section ***Spécifications*** (à la page 337) pour en savoir plus sur les dispositifs pris en charge par le port local étendu, les spécifications de distance et les CIM pris en charge.

Limitations de connexion de KX2-808, KX2-832 et KX2-864

Les ports locaux standard et étendu partagent l'accès à une cible. Lorsqu'ils sont tous les deux activés, ils se partagent le clavier, le moniteur et la souris. Ils seront tous les deux connectés à la cible ou déconnectés.

Lorsque le port local standard ou le port local étendu est désactivé, le clavier, le moniteur et la souris de ces ports sont désactivés et un message vous indique que les ports locaux sont désactivés.

Scripts de connexion et de déconnexion

KX II offre la possibilité d'exécuter des scripts de macros lors de la connexion à ou de la déconnexion d'une cible. Ces scripts sont définis et gérés depuis la page Connection Scripts (Scripts de connexion).

Vous pouvez créer et modifier vos propres scripts dans la page Connection Script afin d'effectuer des actions supplémentaires lors de la connexion aux ou de la déconnexion des cibles. Vous pouvez également importer des scripts de connexion existants au format de fichier XML. Les scripts que vous créez dans KX II peuvent également être exportés au format de fichier XML. KX II peut comporter jusqu'à 16 scripts au total.

Application et retrait des scripts

Pour appliquer un script à des cibles :

1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à appliquer aux cibles. Un script On Connect (A la connexion) et un script On Disconnect (A la déconnexion) peuvent être appliqués à une cible.

Remarque : seul un script à la fois peut être ajouté aux cibles.

3. Dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports), sélectionnez les cibles auxquelles vous souhaitez appliquer le script. Pour cela, utilisez le bouton Select All (Tout sélectionner) ou cochez la case à gauche de chaque cible pour appliquer le script à certaines seulement.
4. Cliquez sur Apply Scripts (Appliquer les scripts). Une fois le script ajouté à la cible, il apparaît dans la colonne Scripts Currently in Use (Scripts utilisés actuellement) dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports).

Pour retirer un script à des cibles :

1. Dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports), sélectionnez les cibles auxquelles vous souhaitez retirer le script. Pour cela, utilisez le bouton Select All (Tout sélectionner) ou cochez la case à gauche de chaque cible pour retirer le script à certaines seulement.
2. Cliquez sur Remove Connect Scripts pour retirer des scripts de connexion ou sur Remove Disconnect Scripts pour retirer des scripts de déconnexion.

Ajout de scripts

Remarque : vous pouvez également ajouter des scripts créés en dehors de KX II et les importer sous forme de fichiers XML. Reportez-vous à **Importation et exportation de scripts** *(à la page 255).*

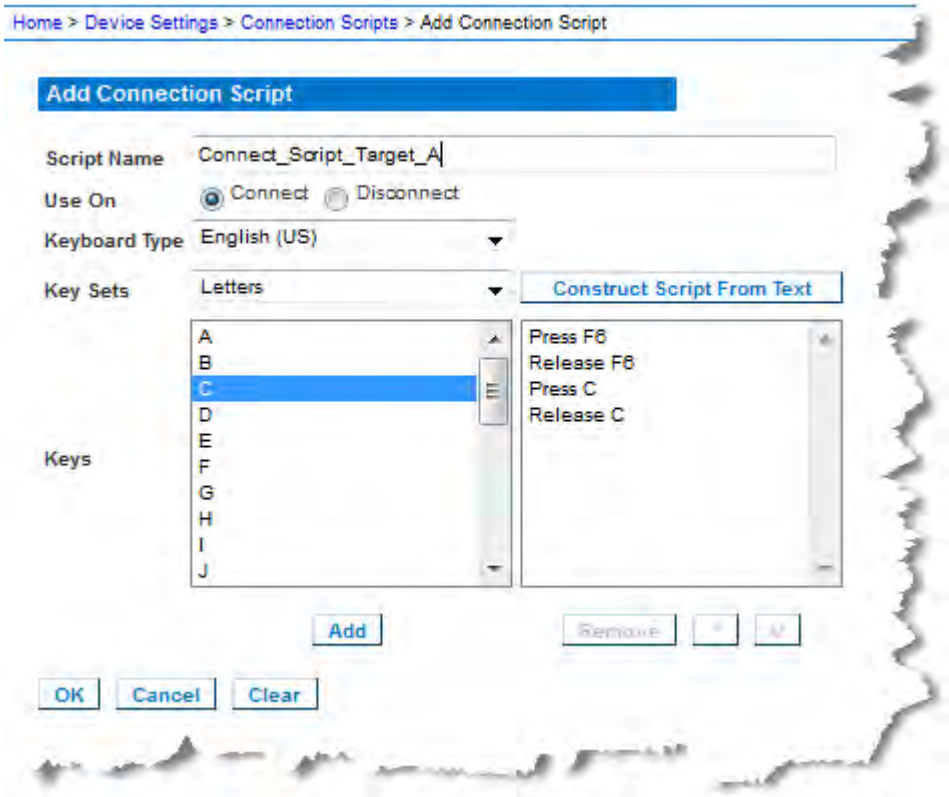
Pour créer un script :

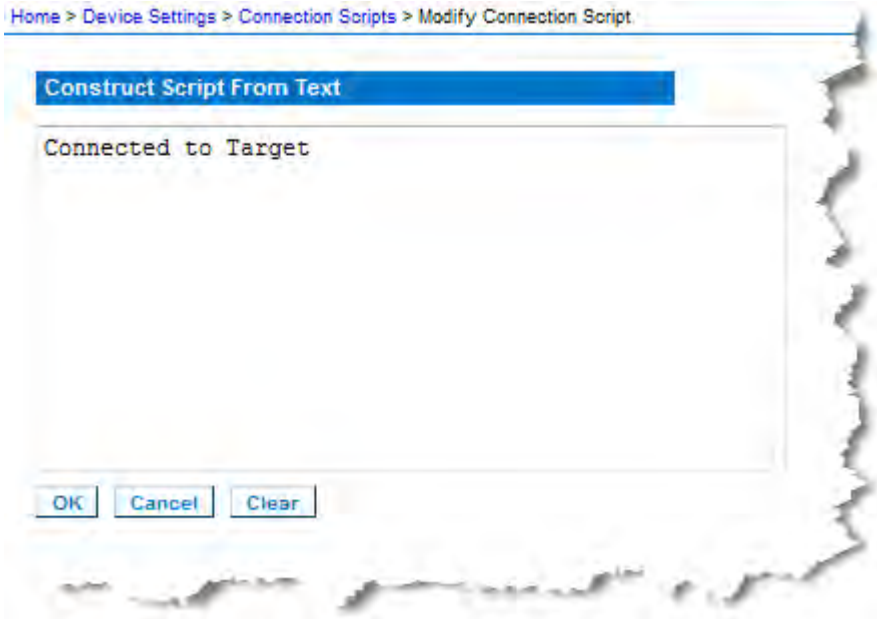
1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), cliquez sur Add (Ajouter). La page Add Connection Scripts (Ajout de scripts de connexion) s'ouvre.
3. Entrez un nom de 32 caractères au maximum pour le script. Ce nom apparaît dans la section Available Connection Scripts (Scripts de connexion disponibles) de la page Configure Scripts (Configurer des scripts) une fois le script créé.
4. Sélectionnez le type de script que vous créez, Connect (Connexion) ou Disconnect (Déconnexion). Les scripts de connexion sont utilisés sur une nouvelle connexion ou lors du passage à une cible.
5. Sélectionnez le type de clavier requis pour la cible que vous utilisez.

6. Dans la liste déroulante Key Sets (Jeux de touches), choisissez les jeux de touches de clavier que vous souhaitez utiliser pour créer le script. Le champ Add (Ajout) sous la liste déroulante Key Sets est alimenté à l'aide des options de jeux de touches sélectionnés.
7. Sélectionnez une touche dans le champ Add et cliquez sur Add (Ajouter) pour la placer dans le champ Script. Pour supprimer une touche du champ Script, sélectionnez-le en cliquant sur Remove (Retirer). Réorganisez les touches en les sélectionnant et en utilisant les icônes Up (Haut) et Down (Bas).

   Le script peut être constitué d'une ou de plusieurs touches. En outre, vous pouvez combiner les touches à utiliser dans le script.

   Par exemple, sélectionnez F1-F16 pour afficher le jeu de touches de fonction dans le champ Add (Ajouter). Sélectionnez une touche de fonction et ajoutez-la au champ Script. Sélectionnez ensuite Letters (Lettres) dans la liste déroulante Key Sets (Jeux de touches) et ajoutez une touche alphabétique au script.
8. Le cas échéant, ajoutez le texte qui s'affichera à l'exécution du script.
   a. Cliquez sur Construct Script From Text (Construire un script à partir du texte) pour ouvrir la page correspondante.
   b. Entrez le script dans la zone de texte. Par exemple, entrez Connecté à la cible.
   c. Cliquez sur OK dans la page Construct Script From Text.
9. Cliquez sur OK pour créer le script.


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

Modification des scripts

Pour modifier des scripts existants :

1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à modifier et cliquez sur Modify. La page est maintenant en mode d'édition.
3. Apportez les modifications nécessaires. Cliquez sur OK lorsque vous avez terminé.

Importation et exportation de scripts

Vous pouvez importer et exporter les scripts de connexion et de déconnexion qui sont au format de fichier XML. Les macros de clavier ne peuvent être ni importées ni exportées.

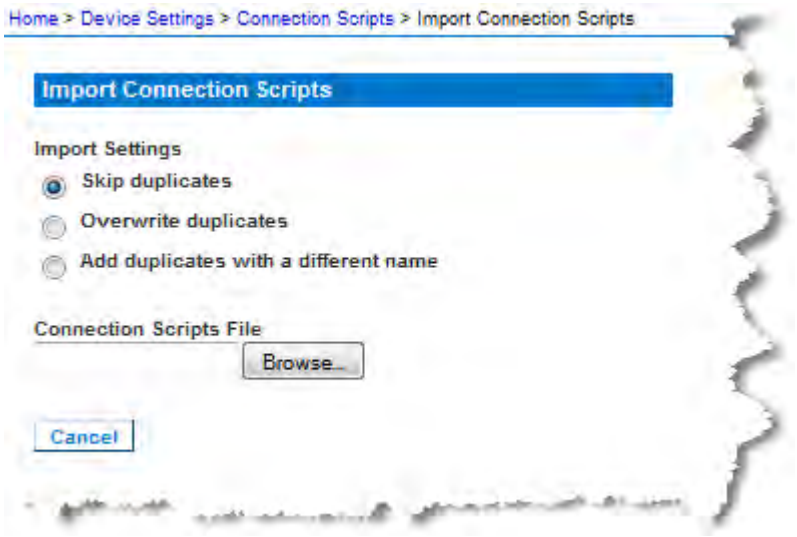
Remarque : la fonction d'importation et d'exportation n'est pas disponible depuis la console locale.

Les scripts importés peuvent être modifiés dans KX II à l'aide de la fonction Modify. Toutefois, une fois qu'un script importé est associé à un port, il n'est plus modifiable. Retirez le script du port pour le modifier. Reportez-vous à ***Application et retrait des scripts*** (à la page 251).

Pour importer un script :

1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), cliquez sur Import (Importer). La page Import Connection Scripts (Importation de scripts de connexion) s'ouvre.
3. Sélectionnez le paramètre d'importation.
   - Skip duplicates (Omettre les doubles) : les scripts existant déjà dans KX II ne sont pas inclus à l'importation.
   - Overwrite duplicates (Ecraser les doubles) : les scripts existant déjà dans KX II sont écrasés par le nouveau script importé.
   - Add duplicates with a different name (Ajouter les doubles sous un nom différent) : les scripts en double seront renommés au cours de l'importation et n'écraseront pas les scripts existants. KX II affecte un numéro au nom du fichier pour le distinguer de l'original.
4. Utilisez la fonction Parcourir pour localiser les fichiers de script XML à importer.

5. Cliquez sur Import (Importer). La page Configuration Scripts (Scripts de configuration) s'ouvre et les scripts importés sont affichés.



Pour exporter un script de déconnexion :

1. Cliquez sur Device Settings > Configuration Scripts (Paramètres du dispositif > Scripts de configuration). La page Configuration Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à exporter et cliquez sur Export. Une boîte de dialogue vous invitant à ouvrir ou à enregistrer le fichier XML apparaît.
3. Enregistrez le fichier XML ou ouvrez-le dans un éditeur XML. Si vous enregistrez le fichier XML, il est enregistré dans votre dossier Download par défaut.

Port Group Management (Gestion des groupes de ports)

La gestion des groupes de ports fait référence aux éléments suivants :

- Groupe de serveurs lames : agrégation des ports connectés à certains types de lames dans un groupe représentant le châssis de lames. Reportez-vous à ***Configuration des châssis de lames HP et Cisco (Gestion des groupes de ports)*** (voir "***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)***" à la page 233).
- Groupe de deux ports vidéo : création de groupes de ports offrant des configurations de bureau étendu sur les serveurs cible. Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 259).
- Groupe de ports : création de groupes de ports « standard » où des paramètres concernant un port principal sont appliqués à tous les ports secondaires du groupe. Reportez-vous à ***Création de groupes de ports*** (à la page 258).

Création de groupes de ports

KX II prend en charge l'agrégation de plusieurs ports dans un même groupe. Les groupes de ports sont constitués uniquement de ports configurés comme ports KVM standard. Un port ne peut être membre que d'un seul groupe.

Les ports pouvant être inclus à un groupe sont affichés dans la liste Select Port for Group > Available (Sélectionner un port pour le groupe > Disponible). Une fois un port ajouté à un groupe, il n'est plus disponible pour un autre. Vous devez le retirer de son groupe actuel pour l'utiliser dans un autre.

Les actions de connexion et de déconnexion exécutées depuis le port principal sont appliquées aux ports secondaires, hormis celles concernant la gestion de l'alimentation.

Les groupes de ports sont restaurés à l'aide de l'option Backup and Restore (Sauvegarde et restauration) (reportez-vous à ***Backup and Restore (Sauvegarde et restauration)*** (à la page 285)).

Remarque : reportez-vous à **Configuration des châssis de lames HP et Cisco (Gestion des groupes de ports)** *(voir "***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)***" à la page 233) pour plus d'informations sur la création de groupes de ports pour un châssis de lames, et à Création de groupes de deux ports vidéo pour plus d'informations à ce sujet.*

Pour créer un groupe de ports :

1. Sélectionnez Device Settings > Port Group Management (Paramètres du dispositif > Gestion des groupes de ports). La page Port Group Management (Gestion des groupes de ports) s'ouvre. Les groupes de ports existants sont affichés.
2. Cliquez sur Add (Ajouter). La page est rafraîchie et affiche toutes les options de groupes de ports disponibles.
3. Sélectionnez le bouton radio Port Group (Groupe de ports).
4. Sélectionnez les ports à ajouter au groupe en cliquant dessus dans la zone de texte Available (Disponible), puis sur Add pour l'ajouter à la zone de texte Selected (Sélectionné).
5. Cliquez sur OK pour créer le groupe de ports. Le groupe de ports apparaît maintenant sur la page Port Group Management (Gestion des groupes de ports).

Création d'un groupe de deux ports vidéo

La fonction des groupes de deux ports vidéo vous permet de réunir deux ports vidéo dans un même groupe. Utilisez cette fonction lorsque vous devez vous connecter à un serveur doté de deux cartes/ports vidéo, et que vous souhaitez accéder aux deux ports simultanément depuis le même client distant.

Remarque : les groupes de deux ports vidéo ne sont pas pris en charge par les modèles KX II dotés d'un seul canal KVM, tels que KX2-108 et KX2-116.

Remarque : une fois le groupe de deux ports vidéo créé, il est disponible depuis la console locale, ainsi que depuis le client distant. Toutefois, le bureau étendu n'est pas pris en charge sur la console locale.

Les groupes de deux ports vidéo apparaissent sur la page Port Access comme types Dual Port. Les ports principal et secondaire faisant partie du groupe de ports apparaissent sur la page Port Access comme Dual Port(P) et Dual Port(S), respectivement. Par exemple, si le type du CIM est DCIM, DCIM Dual Port (P) est affiché.

Chaque groupe doit contenir un port principal et un port secondaire. La configuration appliquée au port principal l'est également à tous les ports secondaires du groupe. Si un port est retiré du groupe, il est considéré indépendant et une nouvelle configuration peut lui être appliquée.

Lorsque vous accédez à un groupe de deux ports vidéo depuis le client distant, vous vous connectez au port principal, qui ouvre une fenêtre de connexion KVM aux ports principal et secondaire du groupe.

Au besoin, les sessions peuvent être lancées et visualisées depuis le client distant sur un ou plusieurs écrans.

Le paramètre d'orientation configuré sur KX II pour la cible doit correspondre à la configuration réelle du système d'exploitation de la cible. Il est recommandé d'utiliser autant que possible la même orientation d'écran sur le client de connexion.

Important : consultez les informations de la section *Groupes de deux ports vidéo* (à la page 367) pour prendre connaissance des restrictions, recommandations, etc. pouvant affecter votre environnement.

Pour créer un groupe de deux ports vidéo :

1. Sélectionnez Device Settings > Port Group Management (Paramètres du dispositif > Gestion des groupes de ports). La page Port Group Management (Gestion des groupes de ports) s'ouvre. Les groupes de ports existants sont affichés.

2. Cliquez sur Add (Ajouter). La page Port Group (Groupe de ports) s'ouvre et tous les ports disponibles apparaissent dans la section Select Ports for Group (Sélectionner des ports pour le groupe).

   Remarque : si un port appartient déjà à un groupe de ports de serveur lame, à un autre groupe de deux ports vidéo ou à un groupe de ports « standard », il ne peut pas être sélectionné. En effet, les ports ne peuvent appartenir qu'à un seul groupe de ports à la fois.

3. Sélectionnez le bouton radio Dual Video Port Group (Groupe de deux ports vidéo).
4. Dans la section Select Ports for Group (Sélectionner des ports pour le groupe), cliquez sur le port désigné comme port principal, puis sur Add pour l'ajouter à la zone de texte Selected (Sélectionné). Veillez à ajouter le port principal en premier.

   Remarque : idéalement, les autorisations appliquées à chaque port du groupe doivent être identiques. Sinon, les autorisations les plus restrictives seront appliquées au groupe. Par exemple, si VM Access Deny (Accès refusé) est appliqué à un port et VM Access Read-Write (Accès en lecture-écriture) à un autre, VM Access Deny est appliqué au groupe. Reportez-vous à **Autorisations et accès aux groupes de deux ports vidéo** *(à la page 376) pour plus d'informations sur l'impact des autorisations relatives aux ports sur les groupes de deux ports vidéo.*

5. Cliquez sur le port désigné comme port secondaire, puis sur Add pour l'ajouter à la zone de texte Selected.
6. Sélectionnez l'orientation de la page. Sélectionnez l'orientation la mieux adaptée à la configuration de l'écran.
7. Cliquez sur OK pour créer le groupe de ports.

   Les groupes de deux ports vidéo apparaissent sur la page Port Access comme types Dual Port. Les ports principal et secondaire faisant partie du groupe de ports apparaissent sur la page Port Access comme Dual Port(P) et Dual Port(S), respectivement. Par exemple, si le type du CIM est DCIM, DCIM Dual Port (P) est affiché.

Remarque : les cibles des groupes de deux ports vidéo liés à un dispositif en niveau doivent être accessibles uniquement via ce dispositif et non via le dispositif en niveau de base.

Modification du paramètre de langue de l'interface utilisateur par défaut

L'interface utilisateur de KX II prend en charge les langues suivantes :

- Japonais
- Chinois simplifié
- Chinois traditionnel

Pour modifier la langue de l'interface utilisateur :

1. Sélectionnez Device Settings > Language (Paramètres du dispositif > Langue). La page Language Settings (Paramètres de langue) s'ouvre :
2. Dans la liste déroulante Language, sélectionnez la langue à appliquer à l'interface utilisateur.
3. Cliquez sur Apply (Appliquer). Cliquez sur Reset Defaults (Rétablir les valeurs par défaut) pour retourner à l'anglais.

Remarque : lorsque vous appliquez une nouvelle langue, l'aide en ligne apparaît dans la langue sélectionnée.

Chapitre 9 Gestion de la sécurité

Dans ce chapitre

Security Settings (Paramètres de sécurité)

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

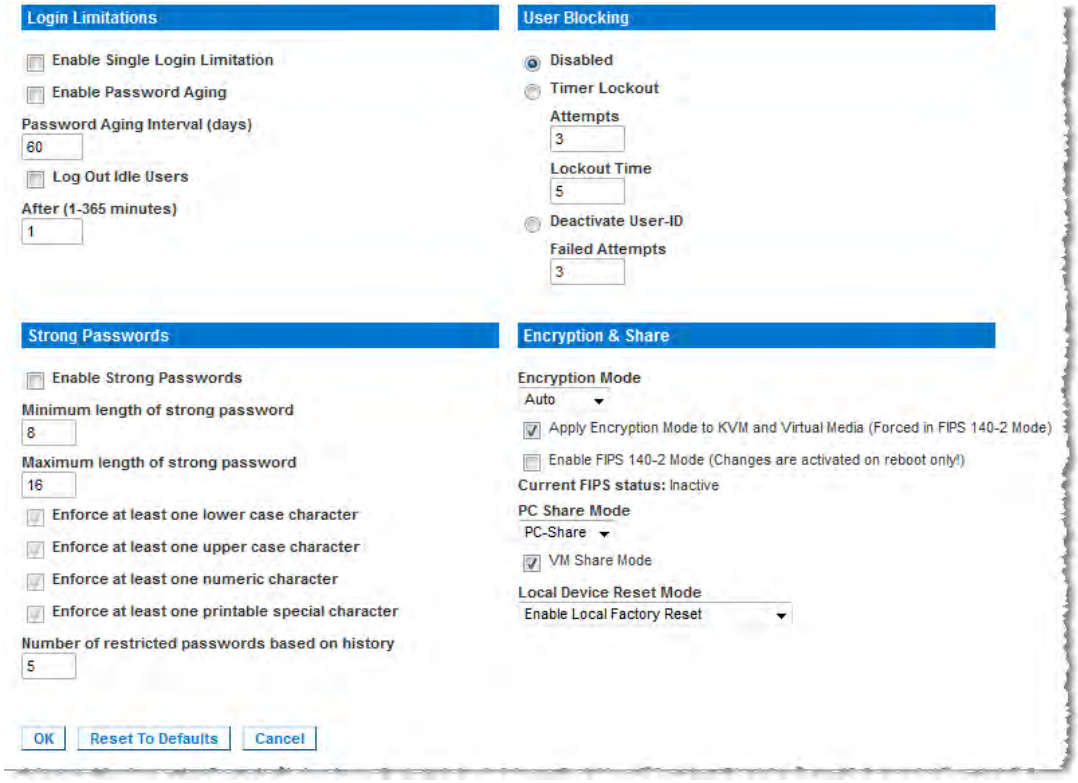
Les certificats SSL Raritan sont utilisés pour des échanges de clés publiques et privées. Ils fournissent un niveau de sécurité supplémentaire. Les certificats de serveur Web Raritan sont auto-signés. Les certificats d'applet Java sont signés par VeriSign. Le chiffrement garantit la sécurité de vos informations en les protégeant contre l'interception frauduleuse. Ces certificats garantissent que l'entité est bien Raritan, Inc.

Pour configurer les paramètres de sécurité :

1. Sélectionnez Security > Security Settings (Sécurité > Paramètres de sécurité). La page Security Settings s'ouvre.
2. Mettez à jour les paramètres de ***limitations de connexion*** (à la page 263) en fonction de vos besoins.
3. Mettez à jour les paramètres de ***mots de passe sécurisés*** (à la page 265) en fonction de vos besoins.
4. Mettez à jour les paramètres de ***blocage des utilisateurs*** (à la page 266) en fonction de vos besoins.
5. Mettez à jour les paramètres de chiffrement & partage en fonction de vos besoins.
6. Cliquez sur OK.

Pour rétablir les paramètres par défaut :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

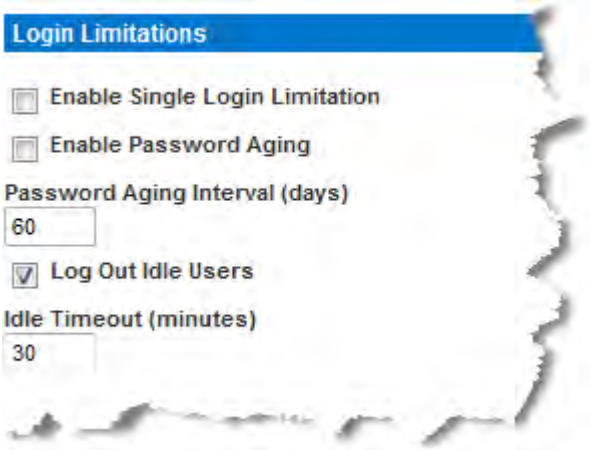


Limitations de connexion

A l'aide des limitations de connexion, spécifiez les restrictions en matière de connexion unique, de vieillissement de mot de passe et de déconnexion des utilisateurs inactifs.

Limitation	Description
Enable Single Login Limitation (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. En revanche, si elle est désélectionnée, une combinaison nom d'utilisateur/mot de passe donnée peut être connectée au dispositif à partir de plusieurs postes de travail clients simultanément.
Enable Password Aging (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 Password Aging

Limitation	Description
	Interval (Intervalle de vieillissement du mot de passe). Ce champ est activé et obligatoire lorsque la case Enable Password Aging (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.
Log off idle users, After (1-365 minutes) (Déconnecter les utilisateurs inactifs, Après)	Cochez la case Log off idle users pour déconnecter automatiquement les utilisateurs après le délai spécifié dans le champ After (1-365 minutes). En l'absence d'activité du clavier ou de la souris, toutes les sessions et toutes les ressources sont déconnectées. En revanche, si une session de support virtuel est en cours, elle n'expire pas. Le champ After (Après) permet de définir le délai (en minutes) après lequel un utilisateur inactif est déconnecté. Ce champ est activé lorsque l'option Log Out Idle Users (Déconnecter les utilisateurs inactifs) est sélectionnée. La valeur saisie dans le champ peut aller jusqu'à 365 minutes.



Mots de passe sécurisés

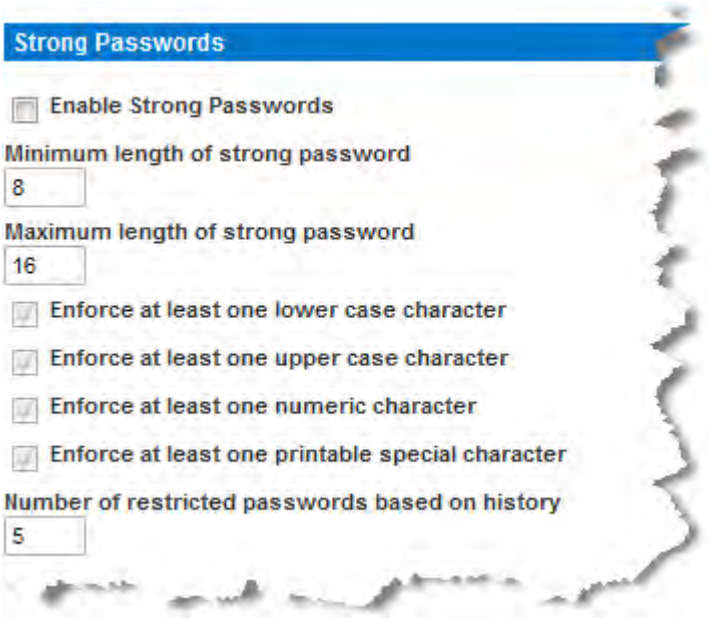
Les mots de passe sécurisés fournissent une authentification locale du système accrue. Utilisez les mots de passe sécurisés pour spécifier le format des mots de passe locaux valides de KX II, tel que la longueur minimum et maximum, les caractères obligatoires et la conservation de l'historique des mots de passe.

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

Si cette option est sélectionnée, les règles des mots de passe sécurisés sont appliquées. Les utilisateurs dont les mots de passe ne répondent pas aux critères de mot de passe sécurisé sont automatiquement invités à modifier leur mot de passe lors de la connexion suivante. Si l'option est désélectionnée, seule la validation du format standard est appliquée. Lorsqu'elle est sélectionnée, les champs suivants sont activés et obligatoires :

Champ	Description
Minimum length of strong password (Longueur minimale du mot de passe sécurisé)	Le mot de passe doit compter au moins 8 caractères. La valeur par défaut est 8, mais vous pouvez entrer jusqu'à 63 caractères.
Maximum length of strong password (Longueur maximale du mot de passe sécurisé)	La valeur par défaut est de 8 au minimum et de 16 au maximum.
Enforce at least one lower case character (Imposer au moins un caractère minuscule)	Lorsqu'elle est cochée, cette option impose au moins un caractère minuscule dans le mot de passe.
Enforce at least one upper case character (Imposer au moins un caractère majuscule)	Lorsqu'elle est cochée, cette option impose au moins un caractère majuscule dans le mot de passe.
Enforce at least one numeric character (Imposer au moins un caractère numérique)	Lorsqu'elle est cochée, cette option impose au moins un caractère numérique dans le mot de passe.
Enforce at least one printable special character (Imposer au moins un caractère spécial imprimable)	Lorsqu'elle est cochée, cette option impose au moins un caractère spécial (imprimable) dans le mot de passe.

Champ	Description
Number of restricted passwords based on history (Nombre de mots de passe restreints en fonction de l'historique)	Ce champ représente la profondeur de l'historique des mots de passe ; c'est-à-dire le nombre de mots de passe précédents ne pouvant pas être répétés. La plage va de 1 à 12, la valeur par défaut étant 5.



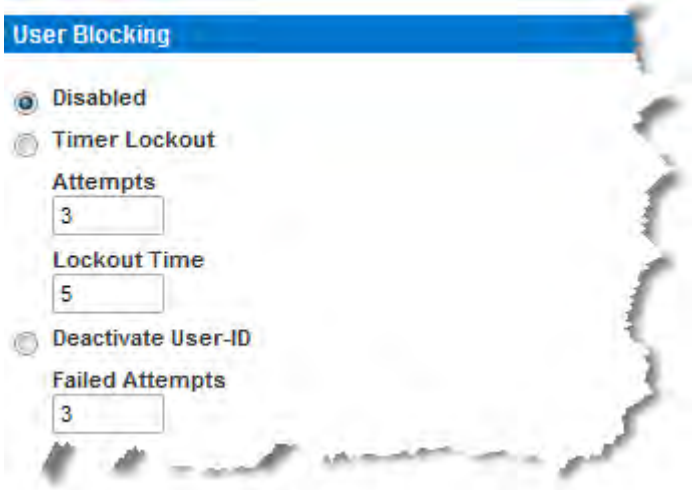
Blocage des utilisateurs

Les options de blocage d'utilisateurs spécifient les critères selon lesquels les utilisateurs se voient refuser l'accès au système après un nombre spécifique d'échecs de connexion.

Les trois options s'excluent les unes les autres :

Option	Description
Disabled (Désactivé)	Il s'agit de l'option par défaut. Les utilisateurs ne sont pas bloqués quel que soit le nombre d'échecs d'authentification.

Option	Description
Timer Lockout (Période de verrouillage)	Les utilisateurs se voient refuser l'accès au système après avoir dépassé le nombre d'échecs de connexion autorisé. Lorsque cette option est sélectionnée, les champs suivants sont activés : ▪ Attempts (Tentatives) - Il s'agit du 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. ▪ Lockout Time (Durée de verrouillage) - Il s'agit du 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. *Remarque : les utilisateurs dotés du rôle Administrateur ne sont pas concernés par les paramètres de période de verrouillage.*
Deactivate User-ID (Désactiver l'ID de l'utilisateur)	Sélectionnée, cette option indique que l'utilisateur ne peut plus accéder au système après un nombre spécifique de tentatives de connexion échouées, défini dans le champ Failed Attempts (Tentatives échouées) : ▪ Failed Attempts (Tentatives échouées) - Il s'agit du nombre d'échecs de connexion après lequel l'ID de l'utilisateur est désactivé. Le champ est activé lorsque l'option Deactivate User-ID (Désactiver l'ID de l'utilisateur) est sélectionnée. Les valeurs autorisées sont comprises entre 1 et 10. Lorsque l'ID d'un utilisateur est désactivé 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 celui-ci en cochant la case Active (Actif) dans la page User (Utilisateur).



Encryption & Share (Chiffrement et partage)

A l'aide des paramètres de chiffrement et de partage, vous pouvez spécifier le type de chiffrement utilisé, les modes de partage PC et VM, ainsi que le type de réinitialisation effectuée lorsque le bouton Reset de KX II est enfoncé.

AVERTISSEMENT : si vous sélectionnez un mode de chiffrement non pris en charge par votre navigateur, vous ne pourrez pas utiliser ce dernier pour accéder à KX II.

Pour configurer le chiffrement et le partage :

1. Sélectionnez une option dans la liste déroulante Encryption Mode (Mode de chiffrement). Lorsqu'un mode de chiffrement est sélectionné, un avertissement s'affiche si votre navigateur ne prend pas en charge ce mode. Dans ce cas, vous ne serez pas en mesure de vous connecter à KX II. L'avertissement indique « When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the KX II. » (Lorsque le mode de chiffrement est spécifié, assurez-vous que votre navigateur le prend en charge ; sinon, vous ne pourrez pas vous connecter à KX II.).

Mode de chiffrement	Description
Auto	Il s'agit de l'option recommandée. KX II négocie automatiquement au niveau le plus élevé de chiffrement possible. Vous *devez* sélectionner Auto pour que le dispositif et le client négocient avec succès

Mode de chiffrement	Description
	l'utilisation des algorithmes compatibles FIPS.
RC4	Permet de sécuriser les noms d'utilisateur, les mots de passe et les données KVM, notamment les transmissions vidéo, à l'aide de la méthode de chiffrement RSA RC4. Le protocole Secure Socket Layer (SSL) à 128 bits fournit un canal de communication privé entre le dispositif KX II et l'ordinateur distant lors de l'authentification de la connexion initiale. Si vous activez le mode FIPS 140-2 et que RC4 est sélectionné, vous recevrez un message d'erreur. RC4 n'est pas disponible en mode FIPS 140-2.
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 l'option AES-128 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 272) pour plus d'informations.
AES-256	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 256). Si l'option AES-256 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 272) pour plus d'informations.

Remarque : MPC négocie systématiquement au niveau le plus élevé de chiffrement et s'adapte au mode de chiffrement paramétré s'il n'est pas défini sur Auto.

Remarque : si vous exécutez le système d'exploitation Windows XP® avec Service Pack 2, Internet Explorer® 7 ne peut pas se connecter à distance à KX II à l'aide du chiffrement AES-128.

2. Apply Encryption Mode to KVM and Virtual Media (Appliquer le mode de chiffrement à KVM et aux supports virtuels). Lorsqu'elle est sélectionnée, cette option applique le mode de chiffrement sélectionné à la fois à KVM et aux supports virtuels. Après authentification, les données KVM et support virtuel sont également transférées avec un chiffrement de 128 bits.
3. Pour les organismes gouvernementaux et autres environnements de haute sécurité, activez le mode FIPS 140-2 en cochant la case Enable FIPS 140-2 (Activer FIPS 140-2). Reportez-vous à ***Activation de FIPS 140-2*** (à la page 272) pour en savoir plus à ce sujet.
4. PC Share Mode - Détermine l'accès KVM à distance simultané global, permettant ainsi à huit utilisateurs distants au maximum de se connecter simultanément à une unité KX II et d'afficher et gérer, en même temps, le même serveur cible par l'intermédiaire du dispositif. Cliquez sur la liste déroulante pour sélectionner une des options suivantes :
   - Private - No PC share (Privé - Pas de PC-Share). 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 KVM. Chaque utilisateur distant dispose du même contrôle au niveau du clavier et de la souris. Notez toutefois que le contrôle n'est pas homogène si un utilisateur n'arrête pas de taper ou de déplacer la souris.
5. En cas de besoin, sélectionnez VM Share Mode (Mode de partage du support virtuel). Cette option est activée uniquement si le mode PC-Share est activé. Lorsqu'elle est sélectionnée, cette option permet le partage des supports virtuels entre plusieurs utilisateurs ; cela signifie que de multiples utilisateurs peuvent accéder à la même session de supports virtuels. Par défaut, ce mode est désactivé.
6. Le cas échéant, sélectionnez Local Device Reset Mode (Mode Réinitialisation du dispositif local). Cette option spécifie les actions entreprises lorsque le bouton Reset (situé à l'arrière du dispositif) est enfoncé. Pour plus d'informations, reportez-vous à ***Réinitialisation de KX II à l'aide du bouton de réinitialisation*** (à la page 335). Sélectionnez une des options suivantes :

Mode Réinitialisation du dispositif local	Description
Enable Local Factory Reset (Activer la réinitialisation locale des paramètres d'usine) (valeur par défaut).	Le dispositif 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 raritan est rétabli.
Disable All Local Resets (Désactiver toutes les réinitialisations locales)	Aucune action de réinitialisation n'est entreprise.

Remarque : lorsque P2CIM-AUSBDUAL ou P2CIM-APS2DUAL est utilisé pour connecter une cible à deux KX II, si l'accès Private aux cibles est requis, le mode de partage PC des deux commutateurs KVM doit être défini sur Private.

Reportez-vous à ***CIM Paragon et configurations pris en charge*** (à la page 349) pour plus d'informations sur l'utilisation des CIM Paragon avec KX II.

Vérification de la prise en charge du chiffrement AES par votre navigateur

KX II prend en charge AES-256. Pour savoir si votre navigateur utilise le chiffrement AES, vérifiez auprès de l'éditeur du navigateur ou consultez le site Web https://www.fortify.net/sslcheck.html à l'aide du navigateur avec la méthode de chiffrement que vous souhaitez vérifier. Ce site Web détecte la méthode de chiffrement de votre navigateur et fournit un rapport.

Remarque : Internet Explorer® 6 ne prend pas en charge le chiffrement AES 128 bits, ni le chiffrement AES 256 bits.

Chiffrement AES 256 bits : conditions préalables et configurations prises en charge

Le chiffrement AES 256 bits est pris en charge uniquement sur les navigateurs Web suivants :

- Firefox® 2.0.0.x et 3.0.x (et supérieur)
- Internet Explorer 7 et 8

Outre la prise en charge par le navigateur utilisé, le chiffrement AES 256 bits nécessite l'installation des fichiers Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy.

Selon la version de JRE™ utilisée, ces fichiers peuvent être téléchargés à la rubrique « other downloads » des pages suivantes dont voici les liens :

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp

Activation de FIPS 140-2

Pour les organismes gouvernementaux et autres environnements de haute sécurité, l'activation du mode FIPS 140-2 est souhaitable. KX II utilise un module cryptographique validé FIPS 140-2 s'exécutant sur une plate-forme Linux® selon la section G.5 des directives de mise en œuvre de FIPS 140-2. Une fois ce mode activé, la clé privée utilisée pour produire les certificats SSL doit être générée en interne ; elle ne peut être ni téléchargée ni exportée.

Pour activer FIPS 140-2 :

1. Accédez à la page Security Settings (Paramètres de sécurité).
2. Pour activer le mode FIPS 140-2, cochez la case Enable FIPS 140-2 dans la section Encryption & Share (Chiffrement & partage) de la page Security Settings (Paramètres de sécurité). Vous utiliserez alors les algorithmes approuvés FIPS 140-2 pour les communications externes. Le module cryptographique FIPS sert au chiffrement du trafic de session KVM constitué de données vidéo, de clavier, de souris, de support virtuel et de carte à puce.
3. Redémarrez KX II **Obligatoire**

Une fois le mode FIPS activé, la mention FIPS Mode: Enabled apparaît dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'écran.

Pour plus de sécurité, vous pouvez également créer une demande de signature de certificat une fois le mode FIPS activé. Elle sera créée à l'aide des chiffres de clé requis. Téléversez le certificat après sa signature ou créez un certificat auto-signé. Le statut du certificat SSL passe de Not FIPS Mode Compliant (Non compatible au mode FIPS) à FIPS Mode Compliant (Compatible au mode FIPS).

Lorsque le mode FIPS est activé, les fichiers de clé ne peuvent être ni téléchargés ni téléversés. La demande de signature de certificat la plus récente sera associée en interne au fichier de clé. En outre, le certificat SSL émanant de l'autorité de certification et la clé privée de celui-ci ne sont pas inclus dans la restauration totale du fichier sauvegardé. La clé ne peut pas être exportée de KX II.

Exigences en matière de prise en charge de FIPS 140-2

KX II prend en charge l'utilisation des algorithmes de chiffrement approuvés FIPS 140-20. Ceci permet à un serveur et à un client SSL de négocier la suite de chiffrement utilisée pour la session chiffrée lorsqu'un client est configuré pour le mode FIPS 140-2 seul.

Les recommandations relatives à l'utilisation de FIPS 140-2 avec KX II figurent ci-après :

KX II

- Paramétrez Encryption & Share (Chiffrement & Partage) sur Auto sur la page Security Settings (Paramètres de sécurité). Reportez-vous à ***Encryption & Share (Chiffrement et partage)*** (à la page 268).

Microsoft Client

- FIPS 140-2 doit être activé sur l'ordinateur client et dans Internet Explorer.

▶ **Pour activer FIPS 140-2 sur un client Windows :**

1. Sélectionnez Panneau de configuration > Outils d'administration > Stratégie de sécurité locale pour ouvrir la boîte de dialogue Paramètres de sécurité locaux.
2. Dans l'arborescence de navigation, sélectionnez Stratégies locales > Options de sécurité.
3. Activez l'option Cryptographie système : utilisez des algorithmes compatibles FIPS pour le cryptage, le hachage et la signature.
4. Redémarrez l'ordinateur client.

Pour activer FIPS 140-2 dans Internet Explorer :

1. Dans Internet Explorer, sélectionnez Outils > Options Internet et cliquez sur l'onglet Avancé.
2. Cochez la case Utiliser TLS 1.0.
3. Redémarrez le navigateur.

Configuration du contrôle d'accès IP

A l'aide du contrôle d'accès IP, vous régulez l'accès à votre KX II. Notez que le contrôle de l'accès par IP empêche n'importe quel trafic d'accéder à KX II ; l'accès à ce dispositif doit donc être accordé aux serveurs NTP, hôtes RADIUS, hôtes DNS, etc.

Le fait de configurer une liste de contrôle d'accès (LCA) globale 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 du dispositif KX II. Cependant, vous pouvez également contrôler l'accès à votre dispositif au niveau du groupe. Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 155) pour plus d'informations sur le contrôle au niveau du groupe.

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

Pour utiliser le contrôle d'accès IP :

1. Sélectionnez Security (Sécurité) > IP Access Control pour ouvrir la page IP Access Control (Contrôle d'accès IP).
2. Sélectionnez la case Enable IP Access Control (Activer le contrôle de l'accès par IP) et les champs restants de la page.
3. Sélectionnez la stratégie par défaut (Default Policy). Cette action concerne les adresses IP qui ne figurent pas dans les plages spécifiées.
   - Accept (Accepter) - Les adresses IP sont autorisées à accéder au dispositif KX II.
   - Drop (Abandonner) - Les adresses IP ne sont pas autorisées à accéder au dispositif KX II.

Pour ajouter des règles :

1. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).

Remarque : l'adresse IP doit être saisie à l'aide de la notation CIDR (Classless Inter-Domain Routing, dans laquelle les 24 premiers bits sont utilisés comme adresse réseau).

2. Sélectionnez la stratégie dans la liste déroulante Policy.
3. Cliquez sur Append (Ajouter). La règle est ajoutée au bas de la liste des règles.

Pour insérer une règle :

1. Tapez un numéro de règle (Rule #). Un numéro de règle est requis lorsque vous utilisez la commande Insert (Insérer).
2. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).
3. Sélectionnez la stratégie dans la liste déroulante Policy.
4. Cliquez sur Insert (Insérer). Si le numéro de règle que vous venez d'entrer est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont descendues d'un rang.

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

Pour remplacer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez remplacer.
2. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).
3. Sélectionnez la stratégie dans la liste déroulante Policy.
4. Cliquez sur Replace (Remplacer). Votre nouvelle règle remplace la règle d'origine portant le même numéro.

Pour supprimer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).

3. Vous êtes invité à confirmer la suppression. Cliquez sur OK.

Certificats SSL

KX II utilise le protocole SSL (Secure Socket Layer) pour le trafic réseau chiffré entre lui-même et un client connecté. A l'établissement d'une connexion, KX II doit s'identifier à un client à l'aide d'un certificat de chiffrement.

Il est possible de générer une demande de signature de certificat (CSR) et d'installer un certificat signé par l'autorité de certification (CA) sur KX II. L'autorité vérifie l'identité de l'auteur de la demande. Elle retourne alors un certificat contenant sa signature à l'auteur. Le certificat, portant la signature de l'autorité de certification reconnue, est utilisé pour confirmer l'identité du détenteur du certificat.

Important : assurez-vous que la date et l'heure de KX II sont définies correctement.

Lorsqu'un certificat auto-signé est créé, la date et l'heure de KX II sont utilisées pour calculer la période de validité. Si elles sont inexactes, les dates de début et de fin de validité du certificat risquent d'être incorrectes et d'entraîner l'échec de la validation du certificat. Reportez-vous à ***Configuration des paramètres de date et d'heure*** (voir "***Configuration des paramètres de date et heure***" à la page 195).

Remarque : la demande de signature de certificat (CSR) doit être générée sur KX II.

Remarque : lors de la mise à niveau du firmware, le certificat actif et la demande de signature de certificat ne sont pas remplacés.

Pour créer et installer un certificat SSL :

1. Sélectionnez Security (Sécurité) > SSL Certificate (Certificat SSL).
2. Remplissez les champs suivants :
   a. Common name (Nom courant) - Il s'agit du nom réseau de KX II une fois qu'il est installé sur le réseau (en règle générale, le nom de domaine complet qualifié). Il est identique au nom utilisé pour accéder à KX II avec un navigateur Web, mais sans le préfixe http://. Si le nom indiqué ici diffère du nom de réseau, le navigateur affiche un avertissement de sécurité lors de l'accès à KX II par le biais du protocole HTTPS.
   b. Organizational unit (Unité organisationnelle) - Ce champ permet de spécifier le service, au sein d'une organisation, auquel KX II appartient.
   c. Organization (Organisation) - Il s'agit du nom de l'organisation à laquelle KX II appartient.
   d. Locality/City (Localité/Ville) - Il s'agit de la ville où se situe l'organisation.
   e. State/Province (Etat/Province) - Il s'agit de l'Etat ou de la province où se situe l'organisation.
   f. Country (ISO code) (Pays (code ISO)) - Il s'agit du pays où se situe l'organisation. Il s'agit du code ISO de deux lettres ; par exemple, DE pour l'Allemagne ou US pour les Etats-Unis.
   g. Challenge Password (Mot de passe challenge) - Certaines autorités de certification requièrent un mot de passe challenge pour autoriser des modifications ultérieures au certificat (par exemple, la révocation du certificat). Entrez-en un le cas échéant.
   h. Confirm Challenge Password (Confirmer le mot de passe challenge) - Il s'agit de la confirmation du mot de passe challenge.
   i. Email (Courriel) - Il s'agit de l'adresse électronique d'un contact responsable du dispositif KX II et de sa sécurité.

j. Key length (Longueur de la clé) - Il s'agit de la longueur de la clé générée en bits. 1024 est la valeur par défaut.

3. Effectuez une des opérations suivantes :

a. Cochez la case Create a Self-Signed Certificate (Créer un certificat auto-signé) si vous devez générer un certificat auto-signé. Lorsque vous sélectionnez cette option, KX II génère le certificat en fonction des données saisies, et sert d'autorité de certification. Il n'est pas nécessaire d'exporter la demande de signature afin de l'utiliser pour générer un certificat signé.

b. Indiquez le nombre de jours de la durée de validité. Assurez-vous que la date et l'heure de KX II sont exactes ; sinon, une date incorrecte risque d'être utilisée pour créer la durée de validité du certificat.

c. Cliquez sur Create (Créer).

d. Une boîte de dialogue de confirmation s'affiche. Cliquez sur OK pour la fermer.

e. Redémarrez KX II pour activer la demande de signature de certificat.

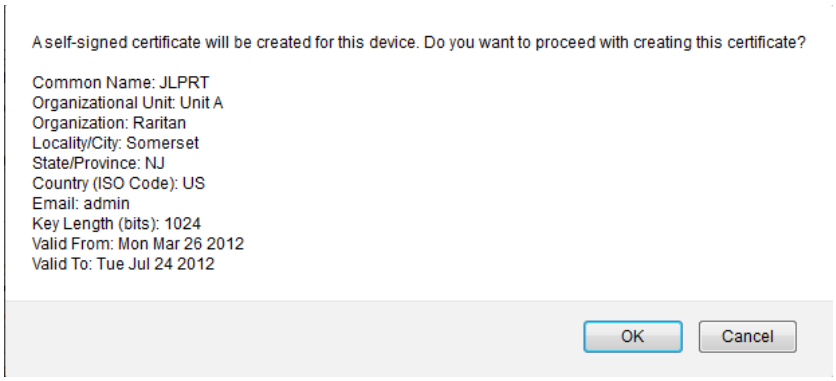
Ou

f. Indiquez le nombre de jours de la durée de validité. Assurez-vous que la date et l'heure de KX II sont exactes ; sinon, une date incorrecte risque d'être utilisée pour créer la durée de validité du certificat.

g. Cliquez sur Create (Créer).

h. Une boîte de dialogue contenant toutes les informations que vous avez entrées, ainsi que les dates de début et de fin de validité du certificat, apparaît. Si les informations sont correctes, cliquez sur OK pour générer la demande de signature de certificat.

i. Redémarrez KX II pour activer la demande de signature de certificat.



Pour télécharger un certificat CSR :

1. La demande et le fichier contenant la clé privée utilisée lors de sa génération peuvent être téléchargés en cliquant sur Download.

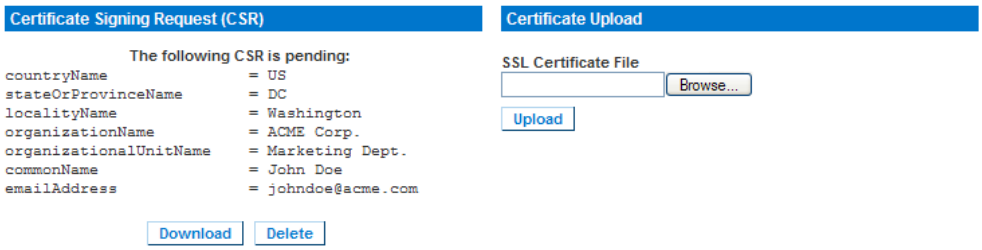
Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.

2. Envoyez la demande enregistrée à une autorité de certification pour confirmation. Vous recevrez le nouveau certificat de l'autorité de certification.

Pour téléverser un certificat auto-signé :

1. Téléversez le certificat dans KX II en cliquant sur Upload.

Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.



Une fois ces étapes effectuées, KX II dispose de son propre certificat permettant d'identifier la carte auprès de ses clients.

Important : si vous détruisez la demande de signature de certificat sur KX II, il n'existe aucun moyen de la récupérer ! Si vous l'avez supprimée par mégarde, vous devez répéter les trois étapes décrites ci-dessus. Pour éviter ceci, utilisez la fonction de téléchargement pour disposer d'une copie de la demande et de sa clé privée.

Bannière de sécurité

KX II vous offre la possibilité d'ajouter une bannière de sécurité au processus de connexion de KX II. Cette fonction oblige les utilisateurs à accepter ou à refuser un accord de sécurité avant d'accéder au KX II. Les informations fournies dans une bannière de sécurité seront affichées dans une boîte de dialogue Restricted Service Agreement (Accord de services limités) après que les utilisateurs auront accédé à KX II à l'aide de leurs informations d'identification.

L'en-tête et le contenu de la bannière de sécurité peuvent être personnalisés, ou le texte par défaut peut être utilisé. En outre, la bannière de sécurité peut être configurée pour exiger d'un utilisateur qu'il accepte l'accord de sécurité avant de pouvoir accéder au KX II ou elle peut être uniquement affichée après le processus de connexion. Si la fonction d'acceptation ou de refus est activée, la sélection de l'utilisateur est consignée dans le journal d'audit.

Pour configurer une bannière de sécurité :

1. Cliquez sur Security > Banner (Sécurité > Bannière) pour ouvrir la page Banner.
2. Cochez la case Display Restricted Service Banner (Afficher la bannière de services limités) pour activer la fonction.
3. Pour obliger les utilisateurs à prendre acte de la bannière avant de poursuivre le processus de connexion, sélectionnez Require Acceptance of Restricted Service Banner (Exiger l'acceptation de la bannière de services limités). Pour prendre acte de la bannière, les utilisateurs cocheront une case. Si vous n'activez pas ce paramètre, la bannière de sécurité n'apparaîtra qu'après la connexion de l'utilisateur et ne l'obligera à la reconnaître.
4. Le cas échéant, modifiez le titre de la bannière. Ces informations apparaîtront aux utilisateurs dans le cadre de la bannière. Vous pouvez entrer jusqu'à 64 caractères.
5. Modifiez les informations de la zone de texte Restricted Services Banner Message (Message de la bannière de services limités). Vous pouvez entrer jusqu'à 6000 caractères ou les télécharger depuis un fichier texte. Pour ce faire, effectuez l'une des opérations suivantes :
   a. Modifiez le texte en tapant dans la zone de texte. Cliquez sur OK.
   b. Téléchargez les informations d'un fichier .txt en sélectionnant le bouton radio Restricted Services Banner File (Fichier de la bannière de services limités) et en utilisant la fonction Parcourir pour localiser et téléverser le fichier. Cliquez sur OK. Une fois le fichier téléversé, son texte apparaîtra dans la zone de texte Restricted Services Banner Message.

Remarque : vous ne pouvez pas téléverser de fichier texte depuis le port local.

Chapitre 10 Maintenance

Dans ce chapitre

Journal d'audit

Un journal des événements du système KX II est créé. Le journal d'audit peut contenir jusqu'à 2 Ko de données avant de commencer à écraser les entrées les plus anciennes. Pour éviter de perdre des données de journal d'audit, exportez-les sur un serveur syslog ou un gestionnaire SNMP. Configurez le serveur syslog ou le gestionnaire SNMP depuis la page Device Settings > Event Management (Paramètres du dispositif > Gestion des événements). Reportez-vous à ***Evénements capturés dans le journal d'audit et dans Syslog*** (à la page 364) pour plus d'informations sur ce qui est capturé dans le journal d'audit et dans syslog.

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

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

   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 : date et heure auxquelles l'événement s'est produit (système de 24 heures).
   - Event : nom de l'événement tel que répertorié dans la page Event Management (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 de KX II et non sur la console locale.

1. Cliquez sur Save to File (Enregistrer dans le fichier). Une boîte de dialogue Save File (Enregistrer le fichier) apparaît.

2. Choisissez le nom et l'emplacement du fichier, 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).

Device Information (Informations sur le dispositif)

La page Device Information fournit des informations détaillées sur votre dispositif KX II et sur les CIM en cours d'utilisation. Ces informations sont utiles si vous avez besoin de contacter l'assistance technique Raritan.

Pour afficher les informations sur votre KX II et ses CIM :

- Sélectionnez Maintenance > Device Information (Informations sur le dispositif). La page des informations relatives au dispositif s'ouvre.

Les informations suivantes relatives à KX II sont fournies :

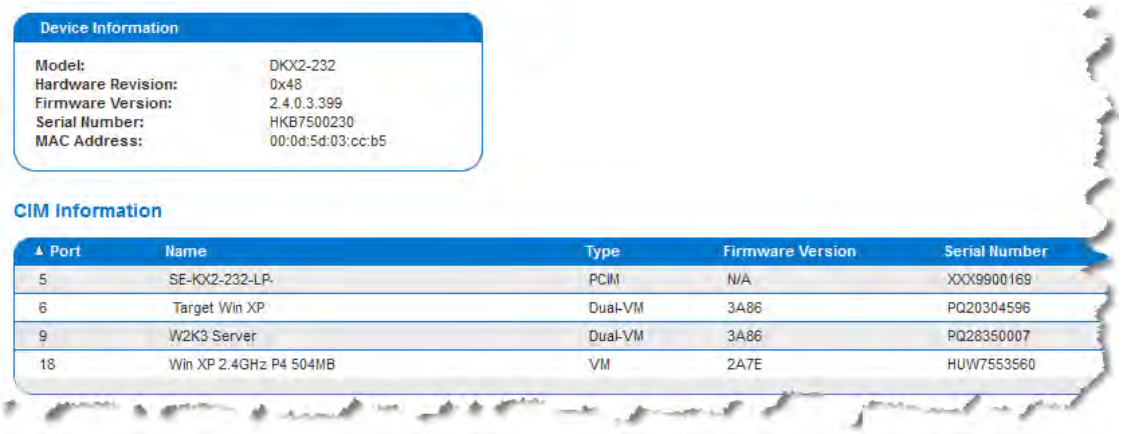
- Modèle
- Numéro de version du matériel
- Version de firmware
- Numéro de série
- Adresse MAC

Les informations suivantes relatives aux CIM en cours d'utilisation sont fournies :

- (Numéro de) port
- Nom
- Type of CIM - DCIM, PCIM, PDU de rack, VM, DVM-DP, DVM-HDMI, DVM-DVI
- Version de firmware
- Numéro de série du CIM - ce numéro provient directement des CIM pris en charge.
  - P2CIM-PS2
  - P2CIM-APS2DUAL
  - P2CIM-AUSBDUAL
  - P2CIM-AUSB
  - P2CIM-SUN
  - P2CIM-SUSB
  - P2CIM-SER
  - DCIM-PS2

- DCIM-USB
- DCIM-USBG2
- DCIM-SUN
- DCIM-SUSB
- DVM-DP
- DVM-HDMI
- DVM-DVI

Remarque : seule la partie numérique ou les numéros de série sont affichés pour les CIM DCIM-USB, DCIM-PS2 et DCIM-USB G2. Par exemple, XXX1234567 est affiché. Le préfixe GN du numéro de série est affiché pour les CIM dotés d'un numéro de série configuré sur site.



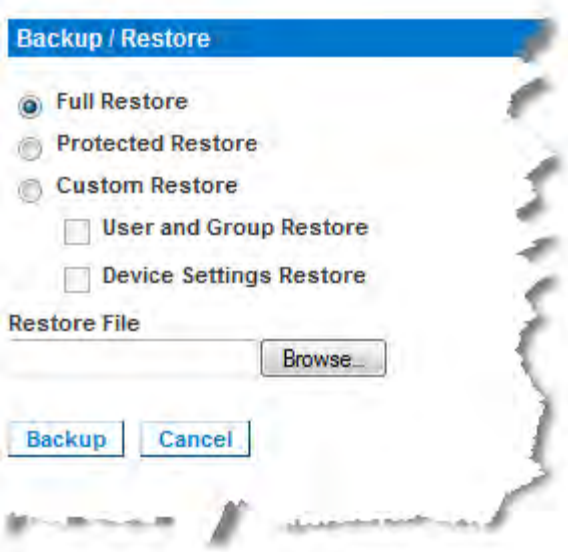
Backup and Restore (Sauvegarde et restauration)

La page Backup/Restore (Sauvegarder/Restaurer) vous permet de sauvegarder et de restaurer les paramètres et la configuration de votre KX II.

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

Pour accéder à la page de sauvegarde/restauration :

- Sélectionnez Maintenance > Backup/Restore (Sauvegarder/Restaurer). La page Backup/Restore (Sauvegarder/Restaurer) s'ouvre.



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

Pour effectuer une copie de sauvegarde de KX II, si vous utilisez Firefox® ou Internet Explorer® 5 ou précédent :

1. Cliquez sur Backup (Sauvegarder). La boîte de dialogue File Download (Téléchargement de fichiers) s'ouvre.
2. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer 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'affiche.
4. Cliquez sur Fermer. Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour effectuer une copie de sauvegarde de KX II, si vous utilisez Internet Explorer 6 ou supérieur :

1. Cliquez sur Backup (Sauvegarder). Une boîte de dialogue File Download (Téléchargement de fichier) contenant un bouton Open (Ouvrir) apparaît. Ne cliquez pas sur Open.

   Dans IE 6 (et supérieur), IE est utilisé comme application par défaut pour ouvrir les fichiers ; vous êtes donc invité à ouvrir le fichier au lieu de l'enregistrer. Pour éviter ce problème, vous devez remplacer l'application utilisée par défaut pour ouvrir les fichiers par WordPad®.
2. Pour ce faire :
   a. Enregistrez le fichier de sauvegarde. Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.
   b. Une fois le fichier enregistré, localisez-le et cliquez dessus avec le bouton droit. Sélectionnez Propriétés.
   c. Dans l'onglet Général, cliquez sur Modifier et sélectionnez WordPad.

Pour restaurer votre KX II :

AVERTISSEMENT : soyez prudent lorsque vous restaurez une version antérieure de votre KX II. Les noms d'utilisateur et mots de passe spécifiés au moment de la sauvegarde sont restaurés. En cas d'oubli des anciens noms d'utilisateur et mots de passe administratifs, vous n'aurez 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, procédez 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. Généralement utilisée à des fins de sauvegarde et de restauration traditionnelles.

- Protected Restore (Restauration protégée) - Tout est restauré, hormis les informations spécifiques au dispositif : adresse IP, nom, etc. Cette option vous permet également de configurer un KX II et de copier sa configuration dans plusieurs dispositifs KX II.
- Custom Restore (Restauration personnalisée) - Avec cette option, vous pouvez sélectionner User and Group Restore (Restauration des utilisateurs et des groupes) et/ou Device Settings Restore (Restauration des paramètres du dispositif).
  - User and Group Restore (Restauration des utilisateurs et des groupes) - Cette option inclut uniquement les informations relatives aux utilisateurs et aux groupes. Cette option *ne restaure pas* le certificat et les fichiers de clé privée. Utilisez cette option pour configurer rapidement des utilisateurs sur un autre KX II.
  - Device Settings Restore (Restauration des paramètres du dispositif) - Cette option n'inclut que les paramètres du dispositif : associations d'alimentation, profils USB, paramètres de configuration relatifs au châssis de lames et les affectations de groupes de ports. Utilisez cette option pour copier rapidement les informations relatives au dispositif.

2. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
3. Localisez et sélectionnez le fichier de sauvegarde approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ Restore File (Restaurer le fichier).
4. Cliquez sur Restore (Restaurer). La configuration (en fonction du type de restauration sélectionnée) est restaurée.

USB Profile Management (Gestion des profils USB)

Depuis la page USB Profile Management, vous pouvez téléverser les profils personnalisés fournis par l'assistance technique Raritan. Ces profils sont conçus pour répondre aux besoins de la configuration du serveur cible, si l'ensemble de profils standard ne suffisait pas. L'assistance technique Raritan vous fournira le profil personnalisé et travaillera avec vous pour vérifier si les besoins spécifiques du serveur cible sont couverts.

Pour accéder à la page USB Profile Management :

- Sélectionnez Maintenance > USB Profile Management (Gestion des profils USB). La page USB Profile Management s'ouvre.

Pour téléverser un profil personnalisé dans KX II :

1. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
2. Localisez et sélectionnez le fichier de profil personnalisé approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ USB Profile File (Fichier de profil USB).
3. Cliquez sur Upload (Téléverser). Le profil personnalisé sera téléversé et affiché dans le tableau Profile (Profil).

Remarque : si une erreur ou un avertissement apparaît pendant le téléversement (par exemple, écrasement d'un profil personnalisé existant), vous pouvez poursuivre l'opération en cliquant sur Upload ou l'annuler en cliquant sur Cancel.

Pour supprimer un profil personnalisé de KX II :

1. Cochez la case correspondant à la rangée du tableau contenant le profil personnalisé à supprimer.

2. Cliquez sur Delete (Supprimer). Le profil personnalisé est supprimé et retiré du tableau Profile (Profil).

Comme indiqué, vous pouvez supprimer un profil personnalisé du système, alors qu'il est toujours désigné comme étant actif. Les éventuelles sessions Support virtuel en place seront alors interrompues.

Gestion des conflits dans les noms de profil

Un conflit d'appellation entre les profils USB personnalisés et standard peut se produire au cours d'une mise à niveau de firmware. Cela peut se produire si un profil personnalisé créé et incorporé à la liste des profils standard porte le nom d'un nouveau profil USB téléchargé dans le cadre de la mise à niveau du firmware.

Dans ce cas, le profil personnalisé préexistant sera marqué old_. Par exemple, si un profil personnalisé appelé GenericUSBProfile5 a été créé et un profil du même nom est téléchargé au cours d'une mise à niveau de firmware, le fichier existant sera alors appelé old_GenericUSBProfile5.

Le cas échéant, vous pouvez supprimer le profil existant. Reportez-vous à ***USB Profile Management (Gestion des profils USB)*** (à la page 288) pour plus d'informations.

Mise à niveau des CIM

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

Pour utiliser les profils USB, vous devez disposer d'un CIM numérique, d'un D2CIM-VUSB ou d'un D2CIM-DVUSB dont le firmware est à jour. Un VM-CIM dont le firmware n'est pas mis à niveau prendra en charge une large gamme de configurations (Windows®, clavier, souris, CD-ROM et lecteur amovible) mais ne pourra pas utiliser les profils optimisés pour des configurations cible particulières. Les VM-CIM existants doivent donc être mis à niveau avec le firmware le plus récent pour accéder aux profils USB. Tant qu'ils ne le seront pas, ils fourniront des fonctionnalités équivalentes à celles du profil générique.

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

1. Sélectionnez Maintenance > CIM Firmware Upgrade (Mise à niveau du firmware du CIM). La page CIM Upgrade from (Mise à niveau du CIM à partir de) s'ouvre.

   Le (numéro de) port, 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.

2. Cochez la case Selected (Sélectionné) pour chacun des CIM que vous voulez mettre à niveau.
3. Cliquez sur Upgrade (Mettre à niveau). Vous êtes invité à confirmer la mise à niveau.
4. Cliquez sur OK pour continuer la mise à niveau. Des barres de progression s'affichent lors de la mise à niveau. La mise à niveau prend environ 2 minutes (ou moins) par CIM.

Mise à niveau du firmware

La page Firmware Upgrade (Mise à niveau du firmware) permet de mettre à niveau le firmware de votre KX II et de tous les CIM reliés. Cette page est disponible sur la console distante de KX II uniquement.

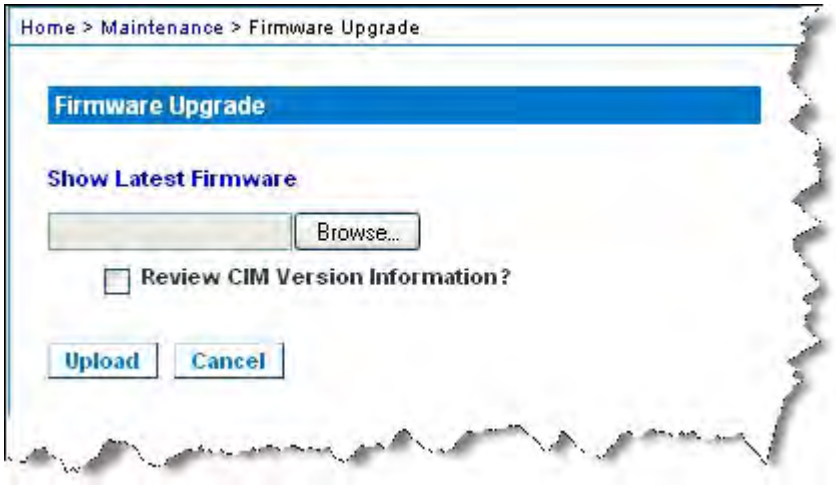
Important : ne mettez pas votre KX II hors tension et ne déconnectez pas les CIM pendant la mise à niveau ; cela risque fortement d'endommager l'unité ou les CIM.

Pour mettre à niveau votre unité KX II :

1. Localisez le fichier de distribution du firmware Raritan (*.RFP) sur la page des mises à niveau du firmware du ***site Web de Raritan http://www.raritan.com*** :
2. Décompressez le fichier. Lisez attentivement l'ensemble des instructions incluses dans les fichiers ZIP du firmware avant de procéder à la mise à niveau.

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

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



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

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

7. Cliquez sur Upgrade (Mettre à niveau). Patientez jusqu'à la fin de la mise à niveau. Des informations sur l'état et des 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 la fin du redémarrage).

A l'invite, fermez le navigateur et attendez environ 5 minutes avant de vous connecter de nouveau à KX II. Pour plus d'informations sur la mise à niveau du firmware du dispositif à l'aide de Multi-Platform Client, reportez-vous à **Mise à niveau du firmware du dispositif** dans le **manuel des clients d'accès KVM et série**.

Remarque : les mises à niveau de firmware ne sont pas prises en charge via modem.

Remarque : Si vous utilisez une configuration multiniveau où un dispositif KX II de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, vous risquez de recevoir une erreur indiquant une mémoire insuffisante lors de la mise à niveau du firmware si vous avez un nombre important de groupes d'utilisateurs. Si vous recevez cette erreur, redémarrez le dispositif, puis effectuez à nouveau la mise à niveau. Si l'erreur persiste après le redémarrage, désactivez la fonction multiniveau sur le dispositif de base et relancez la mise à niveau.

Remarque : lors de la mise à niveau du firmware, le certificat actif et la demande de signature de certificat ne sont pas remplacés.

Historique des mises à niveau

KX II fournit des informations sur les mises à niveau effectuées sur KX II et les CIM reliés.

Pour afficher l'historique des mises à niveau :

- Sélectionnez Maintenance > Upgrade History (Historique des mises à niveau). La page Upgrade History (Historique des mises à niveau) s'ouvre.

Les informations fournies concernent les mises à niveau de KX II exécutées, l'état final de la mise à niveau, les heures de début et de fin, et les versions de firmware précédente et courante. Des informations relatives aux CIM sont également fournies ; pour les obtenir, cliquez sur le lien show (afficher) correspondant à une mise à niveau. Les informations relatives aux CIM fournies sont les suivantes :

- Type - Type du CIM.
- Port - Indique le port sur lequel est connecté le CIM.
- User - Indique l'utilisateur qui a effectué la mise à niveau.
- IP - Indiquez l'adresse IP de l'emplacement du firmware.
- Start Time - Indique l'heure de début de la mise à niveau.
- End Time - Indique l'heure de fin de la mise à niveau.
- Previous Version - Indique la version précédente du firmware de CIM.
- Upgrade Version - Indique la version courante du firmware de CIM.
- CIMs - Indique les CIM mis à niveau.
- Result - Résultat de la mise à niveau (réussite ou échec).

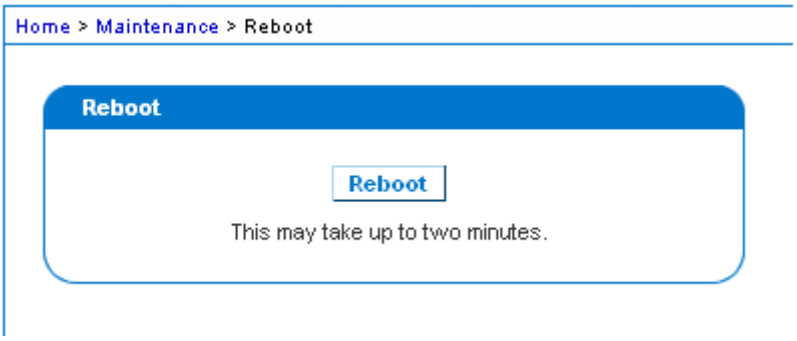
Redémarrage de KX II

La page Reboot (Redémarrer) offre une manière sûre et contrôlée de redémarrer votre KX II. Il s'agit de la méthode recommandée pour le redémarrage.

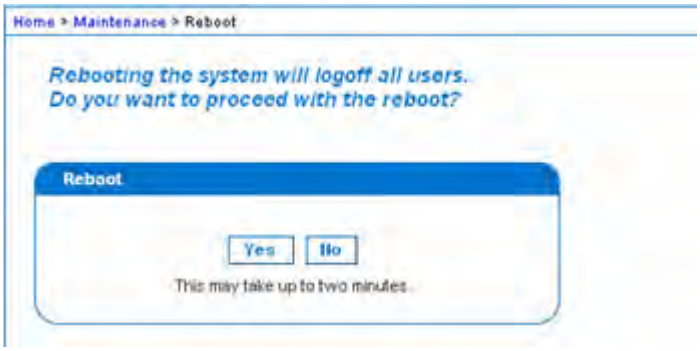
Important : toutes les connexions KVM et série sont fermées et tous les utilisateurs déconnectés.

Pour redémarrer votre KX II :

1. Sélectionnez Maintenance > Reboot (Redémarrer). La page Reboot (Redémarrer) s'ouvre.



2. Cliquez sur Reboot. Vous êtes invité à confirmer l'action. Cliquez sur Yes (Oui) pour procéder au redémarrage.



Arrêt de la gestion par CC-SG

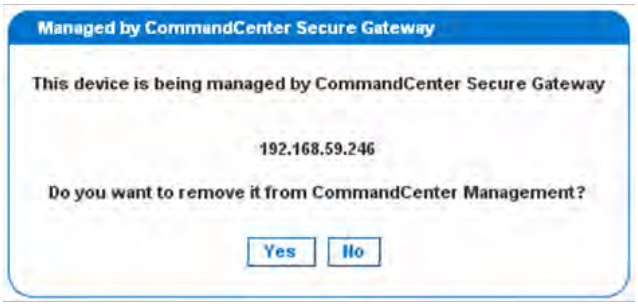
Pendant que KX II est géré par CC-SG, si vous tentez d'accéder au dispositif directement, vous êtes averti que CC-SG assure son contrôle.

Si vous gérez KX II via CC-SG et que la connectivité entre CC-SG et KX II est perdue après un délai spécifié (10 minutes en général), vous pouvez mettre fin à la session de gestion par CC-SG depuis la console de KX II.

Remarque : vous devez disposer des autorisations appropriées pour mettre fin à la gestion par CC-SG de KX II. En outre, l'option Stop CC-SG Management (Arrêter la gestion par CC-SG) n'est accessible que si vous utilisez actuellement CC-SG pour gérer KX II.

Pour arrêter la gestion de KX II par CC-SG :

1. Cliquez sur Maintenance > Stop CC-SG Management (Arrêter la gestion par CC-SG). Un message indiquant que le dispositif est géré par CC-SG s'affiche. Une option permettant de retirer le dispositif de la gestion par CC-SG apparaît également.



2. Cliquez sur Yes (Oui) pour débuter le traitement de retrait du dispositif de la gestion par CC-SG. Un message apparaît alors vous demandant de confirmer le retrait du dispositif de la gestion par CC-SG.

3. Cliquez sur Yes (Oui) pour retirer le dispositif de la gestion par CC-SG. Une fois la gestion par CC-SG terminée, une confirmation apparaît.

Chapitre 11 Diagnostics

Dans ce chapitre

Page Network Interface

KX II offre des informations relatives au statut de votre interface réseau.

Pour afficher les informations relatives à votre interface réseau :

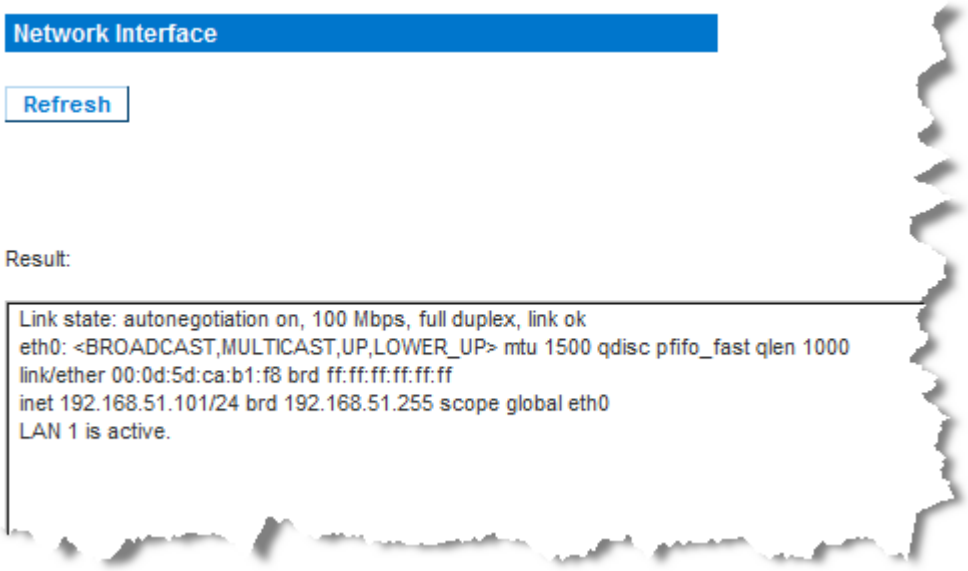
- Choisissez Diagnostics > Network Interface (Diagnostics > Interface réseau). La page Network Interface s'ouvre.

Les informations suivantes s'affichent :

- si l'interface Ethernet est active ou non ;
- si la commande ping peut être émise sur la passerelle ou non ;
- si le port LAN est actuellement actif.

Pour actualiser ces informations :

- Cliquez sur Refresh (Actualiser).



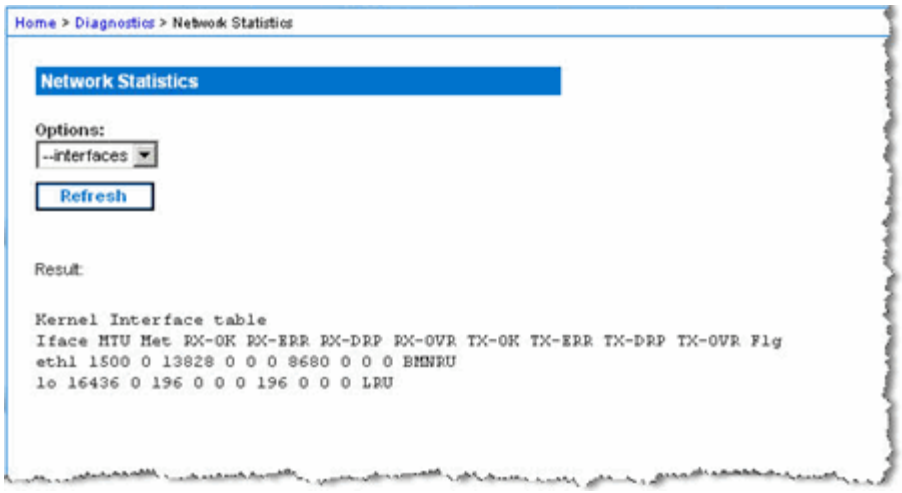
Page Network Statistics (Statistiques réseau)

KX II fournit des statistiques sur votre interface réseau.

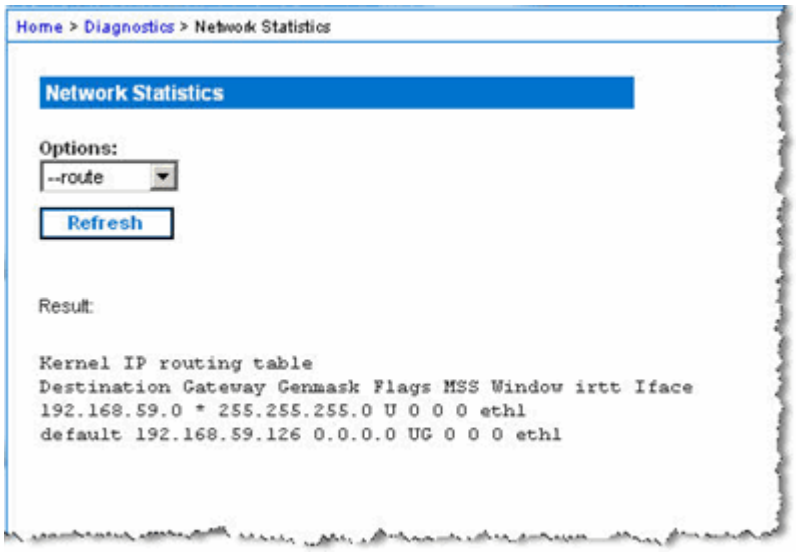
Pour afficher les statistiques relatives à votre interface réseau :

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 - Génère une page similaire à celle affichée ici.

- Interfaces - Génère une page similaire à celle affichée ici.



- Route - Génère une page similaire à celle affichée ici.



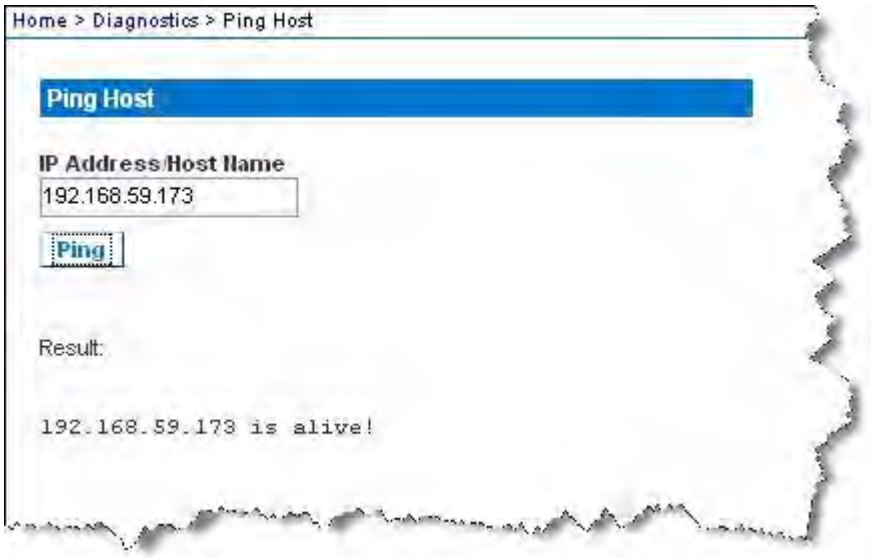
3. Cliquez sur Refresh (Actualiser). Les informations concernées sont affichées dans le champ Result (Résultat).

Page Ping Host (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 la page Ping Host (Envoyer une commande Ping à l'hôte), vous pouvez déterminer si un serveur cible ou un autre 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 (Envoyer une commande Ping à l'hôte) apparaît.



2. Tapez le nom de l'hôte ou l'adresse IP dans le champ IP Address/Host Name.

Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Cliquez sur Ping. Les résultats de la commande Ping sont affichés dans le champ Result (Résultat).

Page Trace Route to Host

Trace Route est un outil réseau permettant de déterminer l'itinéraire emprunté jusqu'au nom d'hôte ou jusqu'à l'adresse IP fournis.

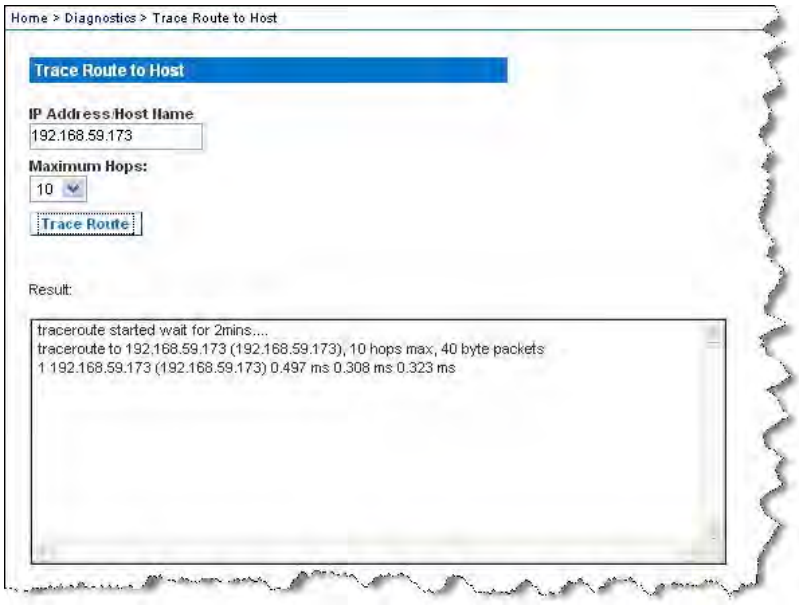
Pour déterminer l'itinéraire jusqu'à l'hôte :

1. Choisissez Diagnostics > Trace Route to Host (Diagnostics > Déterminer l'itinéraire jusqu'à l'hôte). La page Trace Route to Host s'ouvre.

2. Tapez l'adresse IP ou le nom de l'hôte dans le champ IP Address/Host Name.

   Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Sélectionnez une valeur dans la liste déroulante Maximum Hops (Sauts maximum) (de 5 à 50 par incréments de 5).
4. Cliquez sur Trace Route. La commande est exécutée pour le nom d'hôte ou l'adresse IP, et le nombre de sauts maximum donnés. Les données de détermination d'itinéraire sont affichées dans le champ Result (Résultat).



Page Device Diagnostics (Diagnostics du dispositif)

Remarque : cette page est en principe destinée aux techniciens de l'assistance. Vous pouvez l'utiliser lorsque l'assistance technique Raritan vous y invite directement.

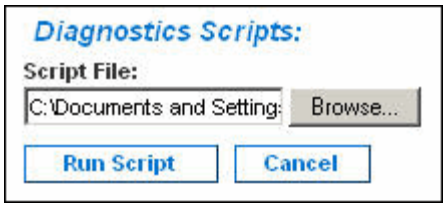
La page Device Diagnostics (Diagnostics du dispositif) télécharge les informations de diagnostic de KX II vers l'ordinateur client. Deux opérations peuvent être effectuées sur cette page :

- Exécutez un script de diagnostics spécial fourni par le support technique Raritan lors d'une session de débogage d'erreurs critiques. Le script est téléversé sur le dispositif et exécuté. Une fois le script exécuté, vous pouvez télécharger les messages de diagnostics à l'aide de la fonction Save to File (Enregistrer dans le fichier).
- Téléchargez le journal de diagnostic du dispositif pour obtenir un instantané des messages de diagnostics de KX II vers le client. Ce fichier chiffré est ensuite envoyé à l'assistance technique Raritan. Seul Raritan peut interpréter ce fichier.

Remarque : cette page n'est accessible qu'aux utilisateurs disposant de droits d'administration.

Pour exécuter les diagnostics du système KX II :

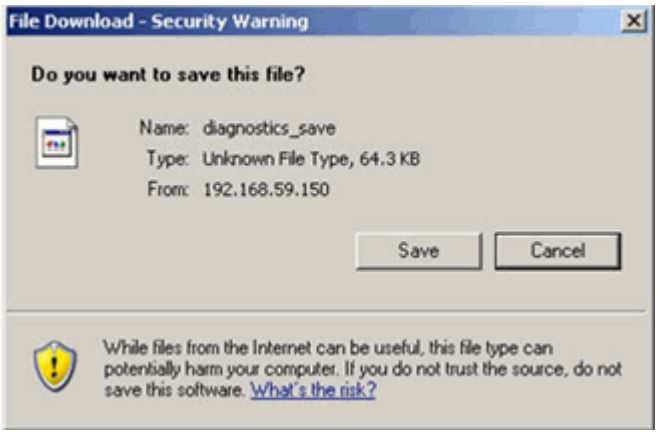
1. Sélectionnez Diagnostics > KX II Diagnostics (Diagnostics de KX II). La page de diagnostics de KX II s'ouvre.
2. Pour exécuter un fichier de script de diagnostics qui vous a été envoyé par courrier électronique par l'assistance technique Raritan :
   a. Récupérez le fichier de diagnostics fourni par Raritan et décompressez-le si nécessaire.
   b. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
   c. Localisez et sélectionnez le fichier de diagnostics.
   d. Cliquez sur Open (Ouvrir). Le fichier s'affiche dans le champ Script File (Fichier de script).



   e. Cliquez sur Run Script (Exécuter le script). Envoyez ce fichier à l'assistance technique Raritan.

3. Pour créer un fichier de diagnostics à envoyer à l'assistance technique Raritan :

   a. Cliquez sur Save to File (Enregistrer dans le fichier). La boîte de dialogue File Download (Téléchargement de fichier) s'ouvre.



   b. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) s'affiche.

   c. Localisez le répertoire voulu puis cliquez sur Save (Enregistrer).

   d. Envoyez ce fichier par courrier électronique à l'assistance technique Raritan.

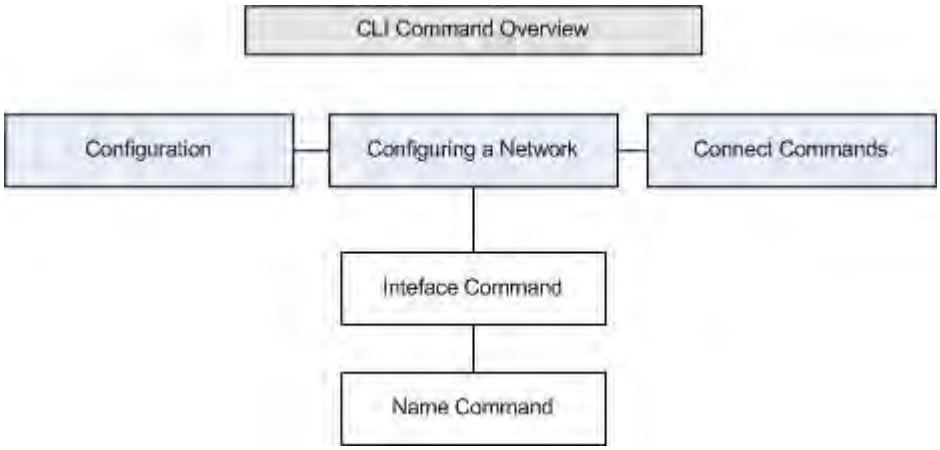
Chapitre 12 Interface de ligne de commande (CLI)

Dans ce chapitre

Présentation

L'interface de ligne de commande (CLI) permet de configurer l'interface réseau de KX II et d'effectuer des fonctions de diagnostic si vous disposez des autorisations appropriées pour cela.

Les figures suivantes présentent les commandes CLI. Reportez-vous à ***Commandes CLI*** (à la page 309) pour consulter une liste de commandes, de définitions et de liens vers les sections de ce chapitre comportant des exemples de ces commandes.



Les commandes courantes suivantes peuvent être utilisées depuis tous les niveaux du CLI : top (haut), history (historique), log off (déconnecter), quit (quitter), show (afficher) et help (aide).

Accès à KX II à l'aide de la CLI

Pour accéder à KX II, choisissez l'une des méthodes suivantes :

- SSH via connexion IP

Un certain nombre de clients SSH sont disponibles et peuvent être obtenus sur les sites suivants :

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client depuis ssh.com - ***www.ssh.com http://www.ssh.com***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

Connexion SSH à KX II

Utilisez un client SSH prenant en charge SSHv2 pour effectuer la connexion à KX II. Vous devez activer l'accès SSH dans la page Device Services (Services du dispositif).

Remarque : pour des raisons de sécurité, les connexions SSH V1 ne sont pas prises en charge par le dispositif KX II.

Accès SSH depuis un PC Windows

Pour ouvrir une session SSH depuis un PC Windows® :

1. Lancez le logiciel client SSH.
2. Entrez l'adresse IP du serveur de KX II. Par exemple, 192.168.0.192.
3. Choisissez SSH, qui utilise le port de configuration 22 par défaut.
4. Cliquez sur Open (Ouvrir).

L'invite `login as:` apparaît.

Reportez-vous à ***Connexion*** (à la page 306).

Accès SSH depuis un poste de travail UNIX/Linux

Pour ouvrir une session SSH depuis un poste de travail UNIX®/Linux® et vous connecter comme administrateur, entrez la commande suivante :

```
ssh -l admin 192.168.30.222
```

L'invite Password (Mot de passe) s'affiche.

Reportez-vous à ***Connexion*** (à la page 306).

Connexion

Pour vous connecter, entrez le nom d'utilisateur admin, comme indiqué ci-après :

1. Connectez-vous sous `admin`.
2. L'invite Password (Mot de passe) s'affiche. Entrez le mot de passe par défaut : *raritan*

   Le message de bienvenue s'affiche. Vous êtes maintenant connecté en tant qu'administrateur.

Après avoir pris connaissance de la section ***Navigation de la CLI*** (à la page 306), effectuez les tâches de configuration initiale.

Navigation de la CLI

Pour utiliser la CLI, il est essentiel d'en comprendre la navigation et la syntaxe. Certaines combinaisons de touches simplifient également l'utilisation de la CLI.

Saisie automatique des commandes

La CLI complète les commandes partiellement entrées. Entrez les premiers caractères d'une entrée et appuyez sur la touche Tab. Si les caractères forment une correspondance unique, la CLI complétera la saisie.

- Si aucune correspondance n'est trouvée, la CLI affiche les entrées valides pour ce niveau.
- S'il existe plusieurs correspondances, la CLI affiche toutes les entrées valides.

Entrez des caractères supplémentaires jusqu'à ce que l'entrée soit unique et appuyez sur la touche Tab pour compléter la saisie.

Syntaxe CLI - Conseils et raccourcis

Conseils

- Les commandes sont répertoriées par ordre alphabétique.
- Les commandes ne sont pas sensibles à la casse.
- Les noms de paramètre sont composés d'un seul mot, sans trait de soulignement.
- Les commandes sans arguments affichent par défaut les paramètres actuels de la commande.
- Si vous entrez un point d'interrogation (?) après une commande, l'aide correspondant à celle-ci s'affiche.
- Une ligne verticale (|) indique un choix parmi un ensemble de mots-clés ou d'arguments facultatifs ou obligatoires.

Raccourcis

- Appuyez sur la flèche Haut pour afficher la dernière entrée.
- Appuyez sur la touche Retour arrière pour supprimer le dernier caractère tapé.
- Utilisez Ctrl + C pour interrompre une commande ou l'annuler si vous avez saisi des paramètres erronés.
- Utilisez la touche Entrée pour exécuter la commande.
- Appuyez sur la touche Tab pour compléter automatiquement une commande. Par exemple, `Admin Port > Conf` Le système affiche ensuite l'invite `Admin Port > Config >`.

Commandes courantes pour tous les niveaux de la CLI

Les commandes disponibles à tous les niveaux du CLI sont indiquées ci-après. Ces commandes permettent également de parcourir la CLI.

Commandes	Description
top	Revient au niveau supérieur de la hiérarchie CLI, ou à l'invite username.
history	Affiche les 200 dernières commandes entrées par l'utilisateur dans la CLI de KX II.
help	Affiche une présentation de la syntaxe CLI.
quit	Fait revenir l'utilisateur au niveau précédent.
logout	Déconnecte la session utilisateur.

Configuration initiale à l'aide de la CLI

Remarque : ces étapes, qui utilisent la CLI, sont facultatives car cette même configuration peut être effectuée via KVM. Reportez-vous à **Mise en route** *(à la page 19) pour plus d'informations.*

Les dispositifs KX II sont livrés avec les paramètres usine par défaut. Lorsque vous mettez sous tension le dispositif et vous y connectez pour la première fois, vous devez définir les paramètres de base suivants, pour permettre un accès sécurisé au dispositif depuis le réseau :

1. Réinitialisez le mot de passe administrateur. Tous les dispositifs KX II sont livrés avec le même mot de passe par défaut. Pour éviter toute intrusion, il est donc impératif de remplacer le mot de passe admin raritan par un mot de passe personnalisé pour les administrateurs qui assureront la gestion du dispositif KX II.
2. Affectez l'adresse IP, le masque de sous-réseau et l'adresse IP de passerelle pour autoriser l'accès à distance.

Définition des paramètres

Pour définir les paramètres, vous devez être connecté avec des privilèges d'administration. Au niveau supérieur, vous verrez l'invite `Username>`, qui pour la configuration initiale est `admin`. Entrez la commande top pour retourner au niveau de menu supérieur.

Remarque : si vous êtes connecté sous un nom d'utilisateur différent, ce nom apparaîtra au lieu d'admin.

Définition des paramètres réseau

Les paramètres réseau sont configurés à l'aide de la commande d'interface.

```
Admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

Lorsque la commande est acceptée, le dispositif abandonne automatiquement la connexion. Vous devez vous reconnecter au dispositif à l'aide de la nouvelle adresse IP, et du nom d'utilisateur et du mot de passe que vous avez créés dans la section de réinitialisation de mot de passe usine par défaut.

Important : en cas d'oubli du mot de passe, KX II doit être réinitialisé à la valeur par défaut usine à l'aide du bouton Reset à l'arrière de KX II. Les tâches de configuration initiale doivent être alors exécutées à nouveau.

KX II est maintenant doté d'une configuration de base et est accessible à distance via SSH, l'interface utilisateur ou localement à l'aide du port série local. L'administrateur doit configurer les utilisateurs et groupes, les services, la sécurité et les ports série par lesquels les cibles série sont connectées au KX II.

Invites CLI

L'invite CLI indique le niveau de commande actuel. La partie racine de l'invite est le nom de connexion. Pour une connexion de port série admin directe avec une application d'émulation de terminal, Admin Port est la partie racine d'une commande.

```
admin >
```

Commandes CLI

- Entrez `admin > help`.

Commande	Description
config	Passe au sous-menu config.
diagnostics	Passe au sous-menu diag.
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
listports	Répertorie les ports accessibles.
logout	Déconnecte de la session CLI actuelle.
top	Revient au menu racine.
userlist	Répertorie les sessions utilisateur actives.

- Entrez `admin > config > network`.

Commande	Description
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
interface	Définit/Extrait les paramètres réseau.
ipv6_interface	Définit/Extrait les paramètres réseau IPv6.
logout	Déconnecte de la session CLI actuelle.
name	Configuration du nom de dispositif.
quit	Revient au menu précédent.
stop	Revient au menu racine.

Problèmes de sécurité

Eléments à considérer en matière de sécurité pour les serveurs de console :

- Chiffrement le trafic des données envoyées entre la console de l'opérateur et le dispositif KX II.
- Authentification et autorisation des utilisateurs.
- Profil de sécurité.

KX II prend en charge chacun de ces éléments ; toutefois, ils doivent être configurés avant l'utilisation générale.

Administration des commandes de configuration du serveur de console de KX II

Remarque : les commandes CLI sont les mêmes pour les sessions SSH et Port local.

La commande Network est accessible depuis le menu Configuration de KX II.

Configuration du réseau

Les commandes du menu Network permettent de configurer l'adaptateur réseau de KX II.

Commandes	Description
interface	Configure l'interface réseau du dispositif KX II.
name	Configuration du nom du réseau.
ipv6	Définit/Extrait les paramètres réseau IPv6.

Commande interface

La commande interface permet de configurer l'interface réseau de KX II. La syntaxe de la commande interface est la suivante :

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> Adresse IP

mask <subnetmask> Masque de sous-réseau

gw <ipaddress> Adresse IP de passerelle

mode <mode> Set Ethernet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Exemple d'utilisation de la commande interface

La commande suivante activer l'interface numéro 1, définit l'adresse IP, le masque et les adresses de passerelle. Elle définit également le mode sur détection automatique.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

Commande name

La commande name permet de configurer le nom de réseau. La syntaxe de la commande name est la suivante :

```
name [devicename <nomDispositif>] [hostname <nomHôte>]
```

Configuration du nom de dispositif.

```
devicename <devicename>   Nom du dispositif

hostname   <hostname>     Nom d'hôte privilégié (DHCP
uniquement)
```

Exemple d'utilisation de la commande name

La commande suivante définit le nom de réseau :

```
Admin > Config > Network > name devicename My-KSX2
```

Commande IPv6

Utilisez IPv6_command pour définir des paramètres réseau IPv6 et extraire les paramètres IPv6 existants.

Chapitre 13 Console locale de KX II

Dans ce chapitre

Présentation

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 de KX II offre une connexion analogique directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur. La console locale de KX II fournit les mêmes fonctionnalités d'administration que la console distante KX II.

Utilisateurs simultanés

La console locale KX II offre un chemin d'accès indépendant aux serveurs cible KVM 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 à KX II, vous pouvez toujours accéder à vos serveurs simultanément à partir du rack via la console locale.

Interface de la console locale de KX II : Dispositifs KX II

Lorsque vous êtes situé au niveau du rack du serveur, KX II permet une gestion KVM standard via la console locale de KX II. La console locale de KX II offre une connexion (analogique) KVM directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Les interfaces graphiques utilisateur de la console locale de KX II et de la console distante de KX II présentent de nombreuses ressemblances. Les éventuelles différences sont indiquées dans l'aide.

L'option Factory Reset (Rétablir les valeurs usine) est disponible sur la console locale de KX II et non sur la console distante de KX II.

Sécurité et authentification

Pour utiliser la console locale de KX II, vous devez d'abord vous authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe valides. KX II dispose d'un schéma d'authentification et de sécurité entièrement intégré que votre accès passe par le réseau ou le port local. Dans ces deux cas, KX II ne permet l'accès qu'aux serveurs pour lesquels un utilisateur dispose de permissions. Reportez-vous à ***Gestion des utilisateurs*** (à la page 148) pour plus d'informations sur la définition des paramètres d'accès et de sécurité des serveurs.

Si votre KX II a été configuré pour des services d'authentification externe (LDAP/LDAPS, RADIUS ou Active Directory), les tentatives d'authentification au niveau 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 de KX II :

1. Branchez un clavier, une souris et un affichage vidéo sur les ports locaux situés à l'arrière de KX II.
2. Démarrez KX II L'interface de la console locale de KX II s'affiche.

Résolutions disponibles

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

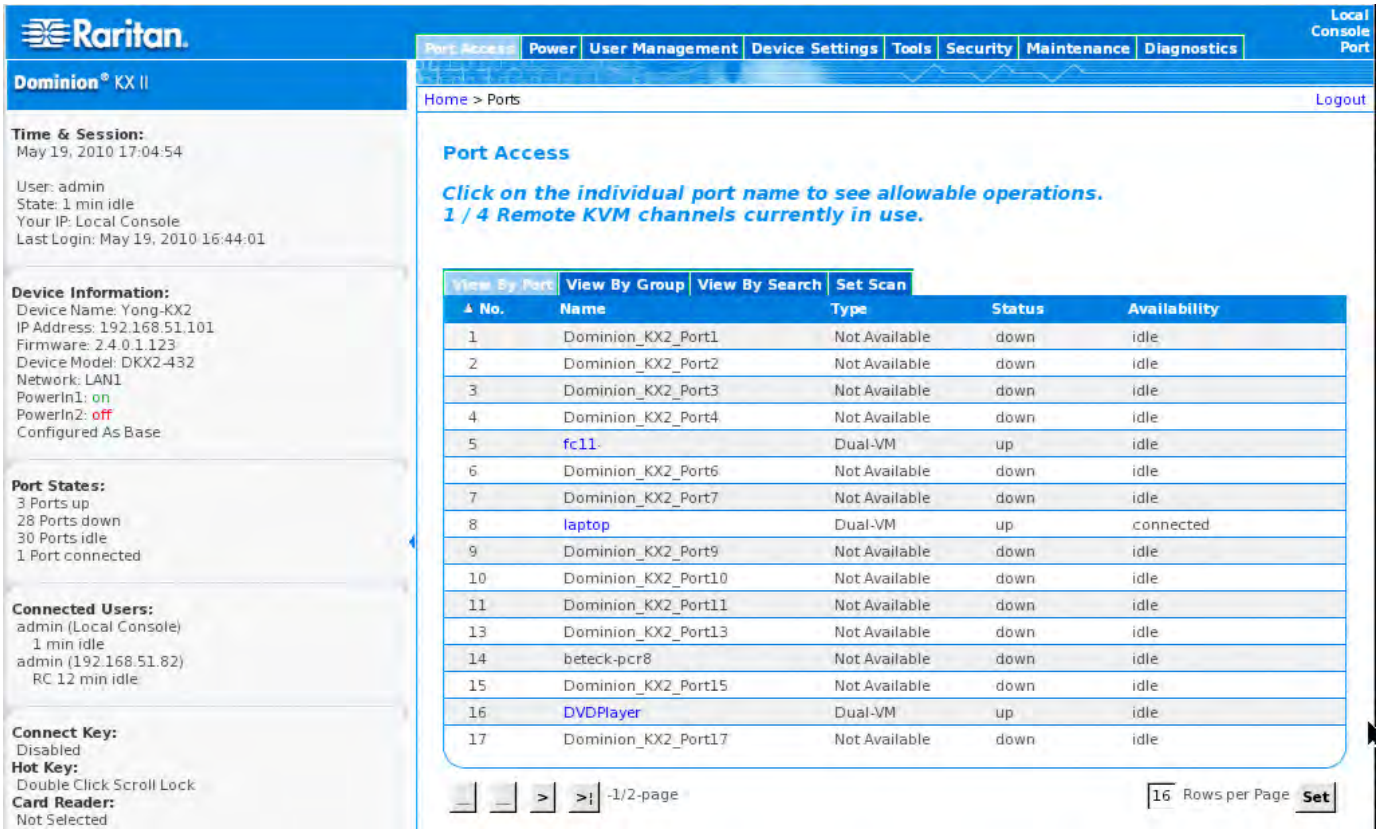
- 800 x 600
- 1024 x 768
- 1280 x 1024

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

Page Port Access (affichage de serveur de la console locale)

Une fois que vous êtes connecté à la console locale de KX II, la page d'accès aux ports s'ouvre. Cette page répertorie tous les ports de KX II et les serveurs cibles, groupes de ports et châssis de lames connectés à ces ports.

Que vous accédiez à la page Port Access (Accès aux ports) depuis la console distante ou la console locale, elle contient les mêmes informations. En outre, vous pouvez naviguer sur la page et accéder aux cibles et aux groupes de ports de la même manière. Reportez-vous à ***Page Port Access (Affichage de la console distante)*** (à la page 56) pour plus d'informations.



Accès à un serveur cible

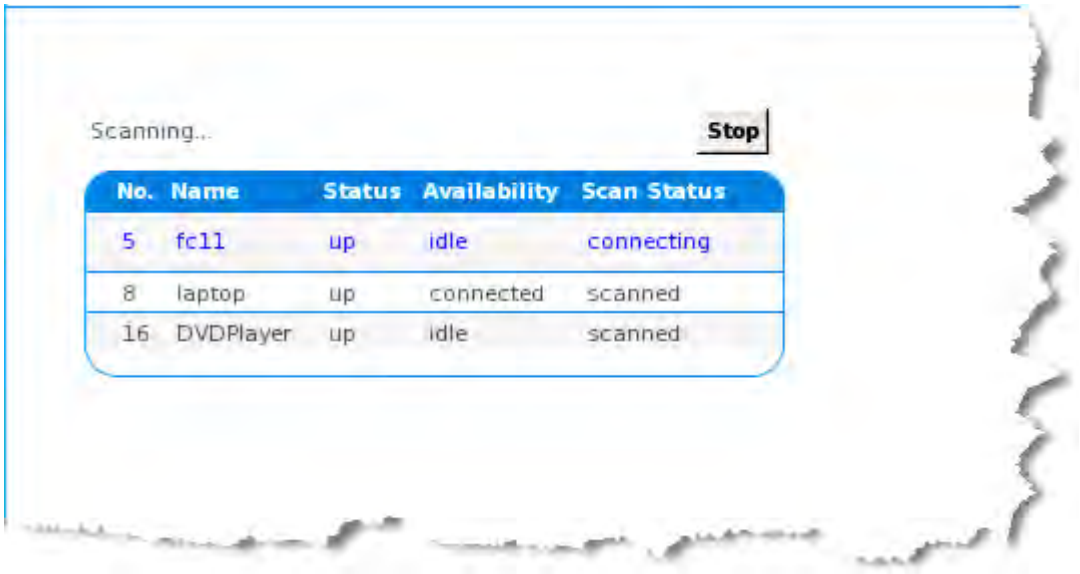
Pour accéder à un serveur cible :

1. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.

2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. L'affichage vidéo bascule sur l'interface du serveur cible.

Balayage des ports - Console locale

La fonction de balayage de KX II est prise en charge par la console locale. Les cibles détectées lors du balayage sont affichées dans la page Scan une par une, ce qui est différent du diaporama des ports de la console distante. Chaque cible est affichée sur la page pendant dix secondes par défaut, ce qui vous permet de la visualiser et de vous y connecter. Utilisez la séquence Local Port ConnectKey (Touche de connexion du port local) pour vous connecter à une cible lorsqu'elle est affichée et la séquence DisconnectKey (Touche de déconnexion) pour vous déconnecter.



Pour effectuer le balayage de cibles :

1. Depuis la console locale, cliquez sur l'onglet Set Scan (Balayage d'ensemble) dans la page Port Access (Accès aux ports).
2. Sélectionnez les cibles à inclure au balayage en cochant la case située à gauche de chacune, ou cochez la case au sommet de la colonne des cibles pour les sélectionner toutes.
3. Laissez la case Up Only (Activées seulement) cochée si vous ne souhaitez inclure au balayage que les cibles activées. Décochez-la pour inclure toutes les cibles, activées ou désactivées.
4. Cliquez sur Scan (Balayer) pour démarrer le balayage. Une fenêtre Port Scan (Balayage des ports) s'ouvre. Au fur et à mesure qu'une cible est détectée, elle est affichée dans la fenêtre.
5. Connectez-vous à une cible lorsqu'elle est affichée en utilisant la séquence ConnectKey.

6. Cliquez sur Stop Scan (Arrêter le balayage) pour arrêter le balayage.

Utilisation des options de balayage

Les options suivantes sont disponibles pour le balayage des cibles. A l'exception de l'icône Expand/Collapse (Développer/Réduire), toutes ces options sont sélectionnées à partir du menu Options en haut à gauche de l'afficheur Port Scan (Balayage des ports). Les valeurs par défaut des options sont rétablies lorsque vous fermez la fenêtre.

Remarque : configurez les paramètres de balayage tels que l'intervalle d'affichage dans le client KVM virtuel (VKC) ou dans le client KVM actif (AKC). Reportez-vous à **Configuration des paramètres de balayage dans VKC et AKC** *(à la page 101) pour plus d'informations.*

Masquer ou afficher les miniatures

- Utilisez l'icône Expand/Collapse (Développer/Réduire)  en haut à gauche de la fenêtre pour masquer ou afficher les miniatures. Par défaut, la vue est développée.

Interrompre le diaporama des miniatures

- Pour interrompre la rotation des miniatures entre deux cibles, sélectionnez Options > Pause. La rotation des miniatures est le paramètre par défaut.

Reprendre le diaporama des miniatures

- Pour reprendre la rotation des miniatures, sélectionnez Options > Resume (Reprendre).

Dimensionner les miniatures dans l'afficheur Port Scan (Balayage des ports)

- Pour agrandir les miniatures, sélectionnez Options > Size (Taille) > 360x240.
- Pour réduire les miniatures, sélectionnez Options > Size (Taille) > 160x120. Il s'agit de la taille par défaut des miniatures.

Modifier l'orientation de l'afficheur Port Scan (Balayage des ports)

- Pour afficher les miniatures le long du bas de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Horizontal.
- Pour afficher les miniatures le long du côté droit de l'afficheur Port Scan, sélectionnez Options > Split Orientation (Orientation de la division) > Vertical. Il s'agit de la vue par défaut.

Accès par carte à puce à la console locale

Pour accéder à un serveur au niveau de la console locale à l'aide d'une carte à puce, connectez un lecteur USB à KX II par un des ports USB situés sur le dispositif. Lorsqu'un lecteur de cartes à puce est branché sur ou débranché de KX II, KX II le détecte automatiquement. Pour obtenir la liste des cartes à puce prises en charge et des informations supplémentaires sur la configuration système requise, reportez-vous à ***Lecteurs de cartes à puce pris en charge ou non*** (à la page 114) et ***Configuration système minimale requise pour les cartes à puce*** (voir "***Configuration système minimum pour carte à puce***" à la page 355).

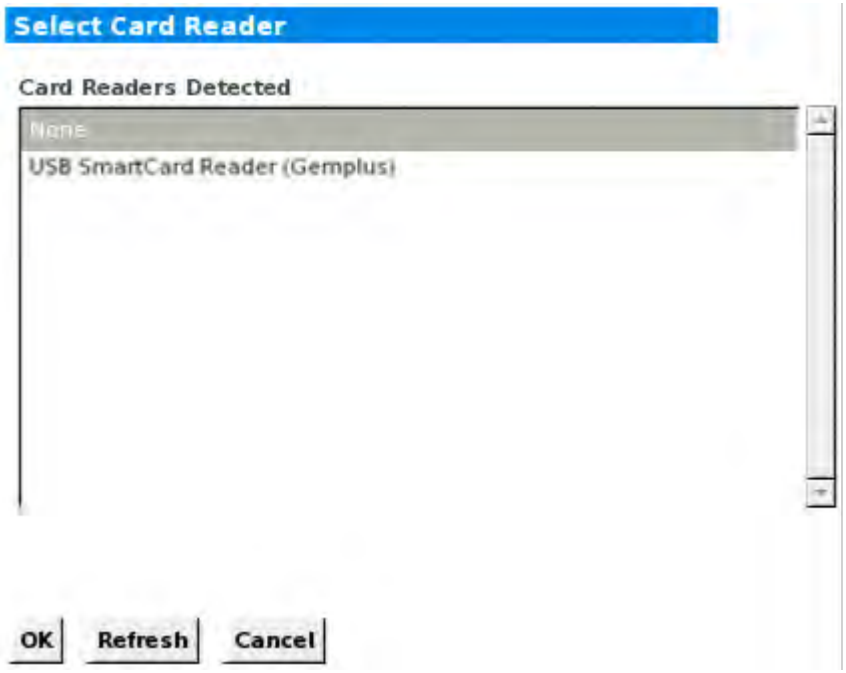
Une fois montés sur le serveur cible, le lecteur de cartes et la carte à puce forceront le serveur à se comporter comme s'ils étaient directement connectés. Le retrait de la carte à puce ou du lecteur de cartes entraînera le verrouillage de la session utilisateur ou vous serez déconnecté suivant la stratégie de retrait de la carte définie dans le système d'exploitation du serveur cible. Lorsque la session KVM est arrêtée, parce qu'elle a été fermée ou parce que vous êtes passé sur une autre cible, le lecteur de cartes à puce est automatiquement démonté du serveur cible.

Pour monter un lecteur de cartes à puce sur une cible via la console locale KX II :

1. Connectez un lecteur de cartes à puce USB à KX II à l'aide d'un des ports USB situés sur le dispositif. Une fois branché, le lecteur sera détecté par KX II.
2. Depuis la console locale, cliquez sur Tools (Outils).
3. Sélectionnez le lecteur dans la liste Card Readers Detected (Lecteurs de cartes détectés). Sélectionnez None (Néant) dans la liste si vous ne souhaitez pas monter de lecteur de cartes à puce.
4. Cliquez sur OK. Une fois le lecteur de cartes à puce ajouté, un message apparaît sur la page pour indiquer que l'opération a abouti. Le statut Selected (Sélectionné) ou Not Selected (Non sélectionné) apparaît dans le panneau gauche de la page sous Card Reader (Lecteur de cartes).

Pour mettre à jour la liste des lecteurs de cartes détectés :

- Cliquez sur Refresh (Actualiser) si un nouveau lecteur de cartes à puce a été monté. La liste Card Readers Detected est rafraîchie pour inclure le lecteur de cartes à puce ajouté.



Accès par carte à puce pour les dispositifs KX2 8xx

Si vous utilisez un lecteur de cartes à puce pour accéder à un serveur depuis la console locale via un dispositif KX2-808, KX2-832 ou KX2-864, le port local étendu (page Local Port Settings (Paramètres du port local)) doit être désactivé. Le port local étendu ne prend pas en charge l'authentification par carte à puce.

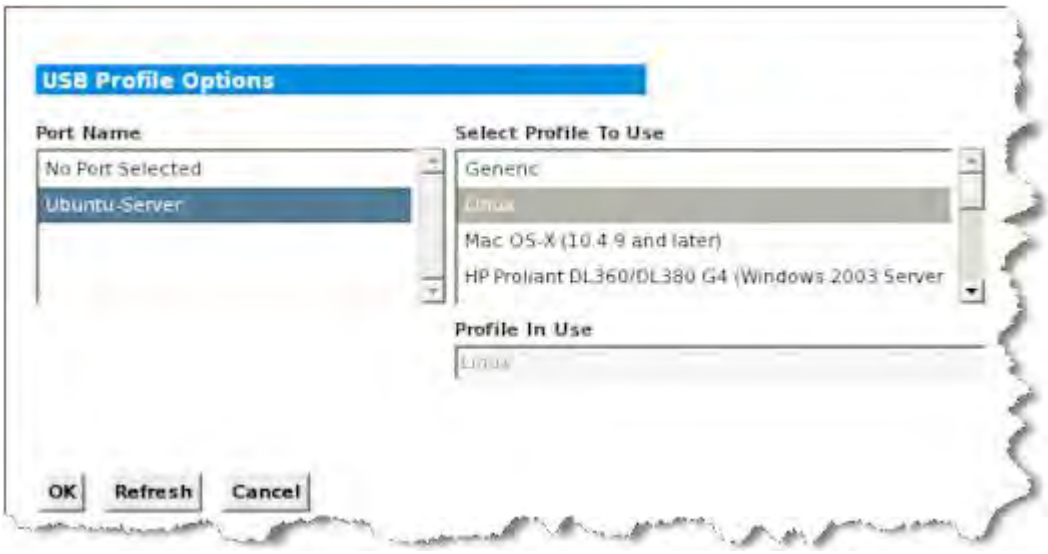
Options de profil USB de la console locale

Dans la section USB Profile Options de la page Tools (Outils), vous pouvez choisir parmi les profils USB disponibles.

Les ports auxquels des profils peuvent être affectés sont affichés dans le champ Port Name et les profils disponibles pour un port apparaissent dans le champ Select Profile To Use (Sélectionner le profil à utiliser) après la sélection du port. Les profils sélectionnés pour l'utilisation avec un port apparaissent dans le champ Profile In Use (Profil utilisé).

Pour appliquer un profil USB à un port de console locale :

1. Dans le champ Port Name, sélectionnez le port auquel vous souhaitez appliquer le profil USB.
2. Dans le champ Select Profile To Use, choisissez le profil à utiliser parmi ceux disponibles pour le port.
3. Cliquez sur OK. Le profil USB sera appliqué au port local et apparaîtra dans le champ Profile In Use.



Raccourcis-clavier et touches de connexion

Comme l'interface de la console locale de KX II est entièrement remplacée par l'interface du serveur cible auquel vous accédez, un raccourci-clavier est utilisé pour vous déconnecter d'une cible et retourner à l'interface utilisateur du port local. Une touche de connexion permet de se connecter à une cible ou de basculer entre plusieurs cibles.

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 une autre combinaison de touches (reportez-vous à la page de paramétrage des ports locaux) comme raccourci-clavier. Reportez-vous à ***Configuration des paramètres de port local de la console locale de KX II*** (voir "***Configuration des paramètres du port local de la console locale de KX II***" à la page 325) pour plus d'informations.

Exemples de touches de connexion

Serveurs standard	
Action de la touche de connexion	**Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accès au port 5 depuis l'interface utilisateur du port local : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Relâchez la touche Alt
Permutation entre les ports	Passer du port cible 5 au port 11 : • Appuyez sur la touche Alt > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Relâchez la touche Alt
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil

Serveurs standard **Action de la touche de connexion** **Châssis de lames** **Action de la touche de connexion**	**Exemple de séquence de touches** **Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accéder au port 5, connecteur 2 : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Appuyez sur la touche - et relâchez-la > Appuyez sur la touche 2 et relâchez-la > Relâchez la touche Alt
Permutation entre les ports	Passer du port cible 5, commutateur 2 au port 5, connecteur 11 : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Appuyez sur la touche - et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Relâchez la touche Alt
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 5, connecteur 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil

•

Combinaisons de touches Sun spéciales

Les combinaisons de touches suivantes pour les touches spéciales du serveur Sun™ Microsystems fonctionnent sur le port local. Ces touches spéciales sont disponibles dans le menu Clavier lorsque vous vous connectez à un serveur cible Sun :

Touche Sun	Combinaison de touches de port local
Again	Ctrl + Alt + F2
Props	Ctrl + Alt + F3
Undo	Ctrl + Alt + F4

Touche Sun	Combinaison de touches de port local
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Muet	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	Aucune combinaison de touches
Alimentation	Aucune combinaison de touches

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 Local Port Settings (Paramètres du port local). Reportez-vous à *Configuration des paramètres du port local de KX II depuis la console locale* (à la page 329).

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

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

Administration du port local

KX II peut être géré par la console locale ou par la console distante. Notez que la console locale de KX II donne également accès à :

- Factory Reset (Réinitialisation des paramètres d'usine)
- Paramètres du port local(disponible également dans la console distante)

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

Configuration des paramètres du port local de la console locale de KX II

A partir de la page de paramétrage du port local, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale de KX II, notamment le clavier, les raccourcis-clavier, 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 locale.

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

Pour configurer les paramètres du port local :

Remarque : certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage doit se produire lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

1. Sélectionnez Device Settings (Paramètres du dispositif) > Local Port Configuration (Configuration du port local). La page des paramètres du port local s'ouvre.
2. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - US
   - US/International (Anglais Etats-Unis/international)
   - United Kingdom
   - Français (France)
   - Allemand (Allemagne)
   - Japonais (JIS)
   - Chinois simplifié

- Chinois traditionnel
- Dubeolsik Hangul (Coréen)
- Allemand (Suisse)
- Portugais (Portugal)
- Norvégien (Norvège)
- Suédois (Suède)
- Danois (Danemark)
- Belge (Belgique)

Remarque : l'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de KX II.

Remarque : Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

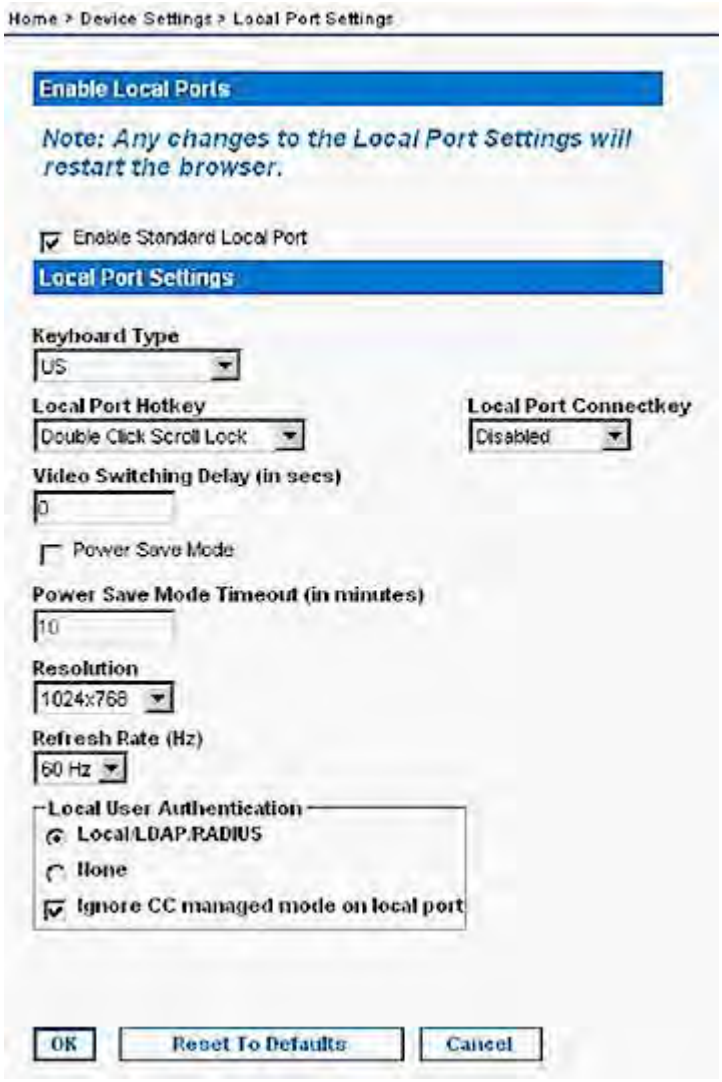
3. Sélectionnez le raccourci-clavier du port local. Le raccourci-clavier du port local vous permet de retourner à l'interface de la console locale de KX II lorsque l'interface d'un serveur cible est affichée. Le paramètre par défaut est Double Click Scroll Lock (Double-clic sur Arrêt défil), mais vous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

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur 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. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre. Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local. Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à ***Exemples de touches de connexion*** (à la page 322) pour obtenir des exemples de séquences de touches de connexion. La touche de connexion fonctionne pour les serveurs standard et les châssis de lames.
5. 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).
6. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique :
   a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).
   b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.
7. Sélectionnez la résolution de la console locale de KX II dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - 800 x 600
   - 1024 x 768
   - 1280 x 1024
8. Sélectionnez le taux de rafraîchissement dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - 60 Hz
   - 75 Hz
9. Sélectionnez le type d'authentification d'utilisateur locale.
   - Local/LDAP/RADIUS. Il s'agit de l'option recommandée. Pour plus d'informations sur l'authentification, reportez-vous à ***Authentification à distance*** (à la page 45).
   - Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale. Cette option est recommandée pour les environnements sécurisés uniquement.
   - Cochez la case Ignore CC managed mode on local port (Ignorer le mode géré par CC sur le port local) si vous souhaitez un accès utilisateur local à KX II même si le dispositif est géré par CC-SG.

Remarque : si vous choisissez au départ d'ignorer le mode CC Manage (Gestion par CC) sur le port local, mais souhaitez par la suite un accès au port local, vous devez désactiver la gestion par CC-SG (depuis CC-SG) du dispositif. Vous pourrez alors cocher cette case.

10. Cliquez sur OK.



Configuration des paramètres du port local de KX II depuis la console locale

Les ports locaux standard et étendu peuvent être configurés depuis la console distante sur la page Port Configuration ou depuis la console locale sur la page Local Port Settings (Paramètres du port local). Reportez-vous à ***Configuration des paramètres du port local de KX II*** (à la page 246) pour en savoir plus sur la configuration de ces ports.

Réinitialisation des paramètres d'usine de la console locale de KX II

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

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

Remarque : il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à ***Journal d'audit*** *(à la page 282).*

Pour procéder à une réinitialisation des paramètres d'usine :

1. Choisissez Maintenance > Factory Reset (Maintenance > Réinitialisation des paramètres usine). La page de réinitialisation des paramètres d'usine s'ouvre.
2. Choisissez l'option de réinitialisation appropriée parmi les suivantes :
   - Full Factory Reset (Réinitialisation intégrale des paramètres d'usine) : supprime la totalité de la configuration et rétablit complètement les paramètres d'usine du dispositif. Notez que toute association de gestion avec CommandCenter est interrompue. En raison du caractère intégral de cette réinitialisation, vous êtes invité à confirmer la réinitialisation des paramètres d'usine.
   - Network Parameter Reset (Réinitialisation des paramètres réseau) : rétablit les paramètres réseau du dispositif aux valeurs par défaut (cliquez sur Device Settings (Paramètres du dispositif) > Network Settings (Paramètres réseau) pour accéder à ces informations) :

- IP auto configuration (Configuration IP automatique)
- IP address (Adresse IP)
- Subnet mask (masque de sous-réseau)
- Gateway IP address (Adresse IP de passerelle)
- Primary DNS server IP address (Adresse IP du serveur DNS primaire)
- Adresse IP du serveur DNS secondaire (Adresse IP du serveur DNS secondaire)
- Discovery port (Port de détection)
- Bandwidth limit (Limite de bande passante)
- LAN interface speed & duplex (Vitesse & duplex de l'interface LAN).
- Enable automatic failover (Activer le basculement automatique)
- Ping interval (seconds) (Intervalle Ping (secondes))
- Timeout (seconds) (Temporisation (secondes))

3. Cliquez sur Reset (Réinitialiser) pour continuer. Vous êtes invité à confirmer la réinitialisation des paramètres d'usine car tous les paramètres réseau seront effacés définitivement.
4. Cliquez sur OK pour continuer. Quand vous avez terminé, le dispositif KX II est automatiquement redémarré.

Scripts de connexion et de déconnexion

KX II offre la possibilité d'exécuter des scripts de macros lors de la connexion à ou de la déconnexion d'une cible. Ces scripts sont définis et gérés depuis la page Connection Scripts (Scripts de connexion).

Vous pouvez créer et modifier vos propres scripts dans la page Connection Script afin d'effectuer des actions supplémentaires lors de la connexion aux ou de la déconnexion des cibles. Vous pouvez également importer des scripts de connexion existants au format de fichier XML. Les scripts que vous créez dans KX II peuvent également être exportés au format de fichier XML. KX II peut comporter jusqu'à 16 scripts au total.

Application et retrait des scripts

Pour appliquer un script à des cibles :

1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à appliquer aux cibles. Un script On Connect (A la connexion) et un script On Disconnect (A la déconnexion) peuvent être appliqués à une cible.

Remarque : seul un script à la fois peut être ajouté aux cibles.

3. Dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports), sélectionnez les cibles auxquelles vous souhaitez appliquer le script. Pour cela, utilisez le bouton Select All (Tout sélectionner) ou cochez la case à gauche de chaque cible pour appliquer le script à certaines seulement.
4. Cliquez sur Apply Scripts (Appliquer les scripts). Une fois le script ajouté à la cible, il apparaît dans la colonne Scripts Currently in Use (Scripts utilisés actuellement) dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports).

Pour retirer un script à des cibles :

1. Dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports), sélectionnez les cibles auxquelles vous souhaitez retirer le script. Pour cela, utilisez le bouton Select All (Tout sélectionner) ou cochez la case à gauche de chaque cible pour retirer le script à certaines seulement.
2. Cliquez sur Remove Connect Scripts pour retirer des scripts de connexion ou sur Remove Disconnect Scripts pour retirer des scripts de déconnexion.

Ajout de scripts

Remarque : vous pouvez également ajouter des scripts créés en dehors de KX II et les importer sous forme de fichiers XML. Reportez-vous à **Importation et exportation de scripts** *(à la page 255).*

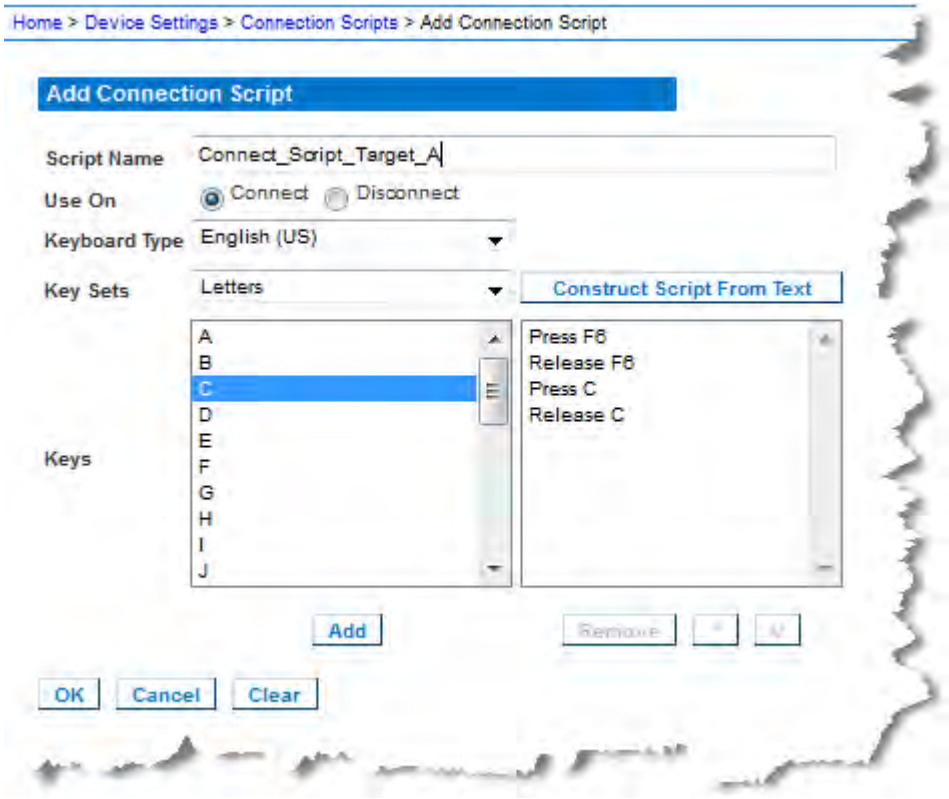
Pour créer un script :

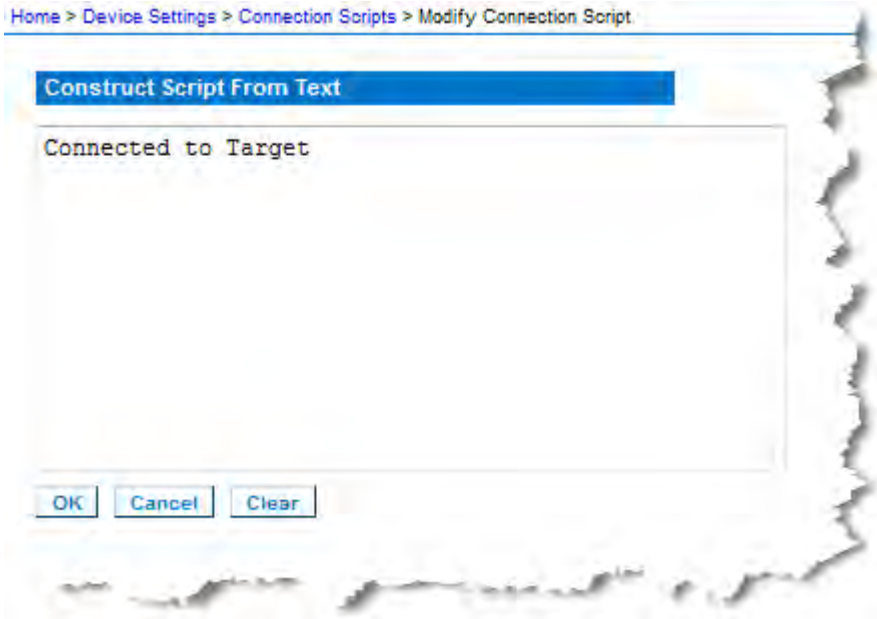
1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), cliquez sur Add (Ajouter). La page Add Connection Scripts (Ajout de scripts de connexion) s'ouvre.
3. Entrez un nom de 32 caractères au maximum pour le script. Ce nom apparaît dans la section Available Connection Scripts (Scripts de connexion disponibles) de la page Configure Scripts (Configurer des scripts) une fois le script créé.
4. Sélectionnez le type de script que vous créez, Connect (Connexion) ou Disconnect (Déconnexion). Les scripts de connexion sont utilisés sur une nouvelle connexion ou lors du passage à une cible.
5. Sélectionnez le type de clavier requis pour la cible que vous utilisez.

6. Dans la liste déroulante Key Sets (Jeux de touches), choisissez les jeux de touches de clavier que vous souhaitez utiliser pour créer le script. Le champ Add (Ajout) sous la liste déroulante Key Sets est alimenté à l'aide des options de jeux de touches sélectionnés.
7. Sélectionnez une touche dans le champ Add et cliquez sur Add (Ajouter) pour la placer dans le champ Script. Pour supprimer une touche du champ Script, sélectionnez-le en cliquant sur Remove (Retirer). Réorganisez les touches en les sélectionnant et en utilisant les icônes Up (Haut) et Down (Bas).

   Le script peut être constitué d'une ou de plusieurs touches. En outre, vous pouvez combiner les touches à utiliser dans le script.

   Par exemple, sélectionnez F1-F16 pour afficher le jeu de touches de fonction dans le champ Add (Ajouter). Sélectionnez une touche de fonction et ajoutez-la au champ Script. Sélectionnez ensuite Letters (Lettres) dans la liste déroulante Key Sets (Jeux de touches) et ajoutez une touche alphabétique au script.
8. Le cas échéant, ajoutez le texte qui s'affichera à l'exécution du script.
   a. Cliquez sur Construct Script From Text (Construire un script à partir du texte) pour ouvrir la page correspondante.
   b. Entrez le script dans la zone de texte. Par exemple, entrez Connecté à la cible.
   c. Cliquez sur OK dans la page Construct Script From Text.
9. Cliquez sur OK pour créer le script.


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

Modification des scripts

Pour modifier des scripts existants :

1. Cliquez sur Device Settings > Connection Scripts (Paramètres du dispositif > Scripts de connexion). La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à modifier et cliquez sur Modify. La page est maintenant en mode d'édition.
3. Apportez les modifications nécessaires. Cliquez sur OK lorsque vous avez terminé.

Réinitialisation de KX II à l'aide du bouton de réinitialisation

Sur le panneau arrière du dispositif figure un bouton Reset (Réinitialiser). Il est encastré pour éviter les réinitialisations accidentelles (vous aurez besoin d'un objet pointu pour utiliser ce bouton). Les opérations effectuées lorsque le bouton de réinitialisation est enfoncé sont définies sur la page Encryption & Share (Chiffrement et partage). Reportez-vous à ***Encryption & Share (Chiffrement et partage)*** (à la page 268).

Remarque : il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à **Journal d'audit** *(à la page 282).*

Pour réinitialiser le dispositif :

1. Mettez KX II hors tension.
2. Utilisez un objet pointu pour appuyer sur le bouton Reset (Réinitialiser) et pour le maintenir.
3. Tout en continuant à maintenir enfoncé le bouton Reset, mettez à nouveau sous tension le dispositif KX II.

4. Continuez de maintenir le bouton enfoncé pendant 10 secondes. Une fois l'unité réinitialisée, deux bips courts signalent la fin de l'opération.

Annexe A Spécifications

Dans ce chapitre

Spécifications physiques de KX II

DKX2-832 - Double alimentation CA 100 V/240 V, ports USB locaux, port de modem, port local étendu, Accès Ethernet double 10/100/1000, VGA de port local, câblage UTP de 32 ports KVM (Cat5/5e/6)

DKX2-864 - Double alimentation CA 100 V/240 V, ports USB locaux, port de modem, port local étendu, Accès Ethernet double 10/100/1000, VGA de port local, câblage UTP de 64 ports KVM (Cat5/5e/6)

Modèle de Dominion KX II	Description	Dimensions (LxPxH)	Poids	Dissipation de puissance et thermique
DKX2-864	64 ports de serveur, 8 utilisateurs distants, 1 port local + port local étendu	17,3" x 13,8" x 3,5" ; 439 x 360 x 88 mm	12,88 lbs ; 5,8 kg	Double alimentation 100 V/240 V 47/63 Hz 1,2 A 67 W 58 KCAL

Modèle de Dominion KX II	Description	Dimensions (LxPxH)	Poids	Dissipation de puissance et thermique
DKX2-832	32 ports de serveur, 8 utilisateurs distants, 1 port local + port local étendu	17,3" x 13,8" x 1,75" 439 x 360 x 44 mm	10,40 lbs ; 4,7 kg	Double alimentation 100 V/240 V 47/63 Hz 1 A 55 W 47 KCAL
DKX2-808	8 ports de serveur, 8 utilisateurs distants, 1 port local + port local étendu	17,3" x 13,8" x 1,75" 439 x 360 x 44 mm	10,40 lbs ; 4,7 kg	Double alimentation 100 V/240 V 47/63 Hz 1 A 55 W 47 KCAL
DKX2-464	64 ports de serveur, 4 utilisateurs distants, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 3,5" ; 439 x 290 x 90 mm	13,73 lbs ; 6,24 kg	Double alimentation 100 V/240 V 47/63 Hz 1,5 A 64 W 55 KCAL
DKX2-432	32 ports de serveur, 4 utilisateurs distants, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 1,75" ; 439 x 290 x 44 mm	9,48 lbs ; 4,3 kg	Double alimentation 100 V/240 V 47/63 Hz 1 A 63 W 54 KCAL
DKX2-416	16 ports de serveur, 4 utilisateurs distants, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 1,75" ; 439 x 290 x 44 mm	9,04 lbs ; 4,1 kg	Double alimentation 100 V/240 V 47/63 Hz 1 A 63 W 54 KCAL
DKX2-232	32 ports de serveur, 2 utilisateurs distants, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 1,75" ; 439 x 290 x 44 mm	9,0 lbs ; 4,1 kg	Double alimentation 100 V/240 V 47/63 Hz 0,6 A 63 W 54 KCAL
DKX2-216	16 ports de serveur, 2 utilisateurs distants, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 1,75" ; 439 x 290 x 44 mm	8,65 lbs ; 3,9 kg	Double alimentation 100 V/240 V 47/63 Hz 0,6 A 62 W 53 KCAL
DKX2-132	32 ports de serveur, 1	17,3" x 11,4" x 1,75" ;	9,0 lbs ; 4,1 kg	Double alimentation 100 V/240 V 47/63 Hz

Modèle de Dominion KX II	Description	Dimensions (LxPxH)	Poids	Dissipation de puissance et thermique
	utilisateur distant, 1 port local pour une utilisation sur le rack	439 x 290 x 44 mm		0,6 A 62 W 53 KCAL
DKX2-116	16 ports de serveur, 1 utilisateur distant, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 1,75" ; 439 x 290 x 44 mm	8,65 lbs ; 3,9 kg	Double alimentation 100 V/240 V 47/63 Hz 0,6 A 62 W 53 KCAL
DKX2-108	8 ports de serveur, 1 utilisateur distant, 1 port local pour une utilisation sur le rack	17,3" x 11,4" x 1,75" ; 439 x 290 x 44 mm	8,58 lbs ; 3,9 kg	Double alimentation 100 V/240 V 47/63 Hz 0,6 A 61 W 53 KCAL

Spécifications pour tous les modèles de Dominion KX II	
Facteur de forme	Montage en rack 1U ou 2U pleine largeur (supports de fixation fournis)
Température d'exploitation	0º - 40º C (32º - 104º F)
Humidité	20 à 85 % HR
Connexion à distance	Accès Ethernet double 10/100/1000 gigabits ; double pile : IPv4 et IPv6
Modem réseau	DB9(F) DTE
Protocoles de port	TCP/IP, HTTP, HTTPS, UDP, RADIUS, SNTP, DHCP, PAP, CHAP, LDAP, SNMP v2 et v3
Accès au port local	
Vidéo	HD15(F) VGA
Clavier/souris	USB(F), 1 USB avant, 3 USB arrière
Garantie	Deux ans standard avec remplacement anticipé*

Systèmes d'exploitation pris en charge (Clients)

Les systèmes d'exploitation suivants sont pris en charge sur Virtual KVM Client et Multi-Platform Client (MPC) :

Système d'exploitation client	Prise en charge des supports virtuels (VM) sur client ?
Windows 7®	Oui
Windows XP®	Oui
Windows 2008®	Oui
Windows Vista®	Oui
Windows 2000® SP4 Server	Oui
Windows 2003® Server	Oui
Windows 2008® Server	Oui
Red Hat® Desktop 5.0	Oui
Red Hat Desktop 4.0	Oui
Open SUSE 10, 11	Oui
Fedora® 13 et 14	Oui
Mac® OS	Oui
Solaris™	Non
Linux®	Oui

Le plug-in JRE™ est disponible pour les systèmes d'exploitation Windows® 32 bits et 64 bits. MPC et VKC peuvent être lancés uniquement à partir d'un navigateur 32 bits, ou d'un navigateur 64 bits IE7 ou IE8.

Les prérequis des systèmes d'exploitation Windows Java™ 32 bits et 64 bits sont donnés ci-après.

Mode	Système d'exploitation	Navigateur
Windows x64 mode 32 bits	Windows XP®	• Internet Explorer® 6.0 SP1+ ou 7.0, IE 8 • Firefox® 1.06 - 3

Mode	Système d'exploitation	Navigateur
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Firefox 1.06 - 3
	Windows Vista®	• Internet Explorer 7.0 ou 8.0
	Windows 7®	• Internet Explorer 9.0 • Firefox 1.06 - 3
Windows x64 mode 64 bits	Windows XP	SE 64 bits, navigateurs 32 bits : • Internet Explorer 6.0 SP1+, 7.0 ou 8.0 • Firefox 1.06 - 3 Mode 64 bits, navigateurs 64 bits : • Internet Explorer 7.0 ou 8.0
	Windows XP Professionnel®	
	Windows XP Edition Tablet PC®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

Résolutions vidéo prises en charge

Assurez-vous que la résolution vidéo et le taux de rafraîchissement de chaque serveur cible sont pris en charge par l'unité KX II, et que le signal est non entrelacé.

La résolution vidéo et la longueur de câble sont des facteurs importants dans la réalisation de la synchronisation de la souris.

L'unité KX II prend en charge ces résolutions :

Résolutions	
640 x 350 à 70Hz	1024 x768 à 85
640 x 350 à 85Hz	1024 x 768 à 75Hz
640 x 400 à 56Hz	1024 x 768 à 90Hz
640 x 400 à 84Hz	1024 x 768 à 100Hz
640 x 400 à 85Hz	1152 x 864 à 60Hz
640 x 480 à 60Hz	1152 x 864 à 70Hz
640 x 480 à 66,6Hz	1152 x 864 à 75Hz

Résolutions	
640 x 480 à 72Hz	1152 x 864 à 85Hz
640 x 480 à 75Hz	1152 x 870 à 75,1Hz
640 x 480 à 85Hz	1152 x 900 à 66Hz
720 x 400 à 70Hz	1152 x 900 à 76Hz
720 x 400 à 84Hz	1280 x 720 à 60Hz
720 x 400 à 85Hz	1280 x 960 à 60Hz
800 x 600 à 56Hz	1280 x 960 à 85Hz
800 x 600 à 60Hz	1280 x 1024 à 60Hz
800 x 600 à 70Hz	1280 x 1024 à 75Hz
800 x 600 à 72Hz	1280 x 1024 à 85Hz
800 x 600 à 75Hz	1360 x 768 à 60Hz
800 x 600 à 85Hz	1366 x 768 à 60Hz
800 x 600 à 90Hz	1368 x 768 à 60Hz
800 x 600 à 100Hz	1400 x 1050 à 60Hz
832 x 624 à 75,1Hz	1440 x 900 à 60Hz
1024 x 768 à 60Hz	1600 x 1200 à 60Hz
1024 x 768 à 70	1680 x 1050 à 60Hz
1024 x 768 à 72	1920 x 1080 à 60Hz

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

Remarque : certaines résolutions ne sont peut-être pas disponibles par défaut. Si une résolution n'apparaît pas, branchez d'abord le moniteur, débranchez-le, puis branchez le CIM.

Remarque : si les résolutions 1440x900 et 1680x1050 ne s'affichent pas, mais sont prises en charge par la carte graphique du serveur cible, un adaptateur DDC-1440 ou DDC-1680 peut être nécessaire.

Distance de connexion et résolution vidéo du serveur cible prises en charge

La distance maximale prise en charge dépend de plusieurs facteurs, notamment le type/la qualité du câble Cat5, le type et 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 :

Résolution vidéo	Taux de rafraîchissement	Distance maximale
1920 x 1080	60	50 ft. (15 m)
1600 x 1200	60	50 ft. (15 m)
1280 x 1024	60	100 ft. (30 m)
1024 x 768	60	150 ft. (45 m)

Remarque : 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*** (à la page 341) pour connaître les résolutions vidéo prises en charge par KX II.

Navigateurs pris en charge

KX II prend en charge les navigateurs suivants :

- Internet Explorer® 6 à 9
- Firefox® 1.5, 2.0, 3.0 (jusqu'à la version 3.6.17) et 4.0
- Safari® 3 ou supérieur

Spécifications des CIM pris en charge

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
D2CIM-DVUSB	CIM double USB pour support virtuel BIOS, carte à puce/CAC, audio et synchronisation absolue de la souris	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
			
D2CIM-VUSB	CIM USB pour support virtuel et synchronisation absolue de la souris 	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0,20 lb ; 0,09 kg
DCIM-PS2	CIM pour PS/2 	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0,20 lb ; 0,09 kg
DCIM-SUN	CIM pour Sun 	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0,20 lb ; 0,09 kg
DCIM-USBG2	CIM pour USB et Sun USB	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0,20 lb ; 0,09 kg

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
			
D2CIM-PWR	CIM pour gestion de l'alimentation à distance 	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0,20 lb ; 0,09 kg
P2CIM-SER	CIM Paragon II/Dominion KX II pour dispositifs série (ASCII) 	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0,20 lb ; 0,09 kg
DVM-DVI	CIM numérique qui permet la conversion numérique-analogique et prend en charge support virtuel, carte à puce/CAC, audio, synchronisations absolue et relative de la souris 	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
D2CIM-DVUSB-DP (port d'affichage)	CIM numérique qui permet la conversion numérique-analogique et prend en charge support virtuel, carte à puce/CAC, audio, synchronisations absolue et relative de la souris 	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg
DVM-HDMI USB	CIM numérique qui permet la conversion numérique-analogique et prend en charge support virtuel, carte à puce/CAC, audio, synchronisations absolue et relative de la souris 	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg

Remarque : les CIM numériques sont pris en charge par KX II 2.5.0 (et supérieur)

Synchronisation et résolution vidéo du serveur cible des CIM numériques

Les CIM numériques prennent en charge les canaux de données d'affichage (DDC) et les données d'identification d'affichage étendues améliorées (E-EDID). Reportez-vous à ***Spécifications des modules d'interface pour ordinateur (CIM) pris en charge*** (voir "***Spécifications des CIM pris en charge***" à la page 343) pour plus d'informations.

Modes de synchronisation

Vous trouverez ci-dessous les modes de synchronisation par défaut utilisés par KX II pour communiquer avec une source vidéo par le biais d'un CIM numérique. Le mode de synchronisation utilisé dépend de la résolution native de la source vidéo.

- 1920 x 1080 à 60 Hz
- 1600 x 1200 à 60 Hz
- 1280 x 1024 à 60 Hz (résolution par défaut appliquée aux CIM numériques)
- 1440 x 900 à 60 Hz

Modes établis et standard

Les résolutions et modes de synchronisation établis et standard supplémentaires ci-après sont pris en charge par KX II 2.5.0 (et supérieur).

Modes établis

- 720 x 400 à 70 Hz IBM, VGA
- 640 x 480 à 60 Hz IBM, VGA
- 640 x 480 à 67 Hz Apple, Mac II
- 640 x 480 à 72 Hz VESA
- 640 x 480 à 75 Hz VESA
- 800 x 600 à 56 Hz VESA
- 800 x 600 à 60 Hz VESA
- 800 x 600 à 72 Hz VESA
- 800 x 600 à 75 Hz VESA
- 832 x 624 à 75 Hz Apple, Mac II
- 1024 x 768 à 60 Hz VESA
- 1024 x 768 à 70 Hz VESA
- 1024 x 768 à 75 Hz VESA
- 1024 x 1024 à 75 Hz VESA
- 1152 x 870 à 75 Hz Apple, Mac II

Modes standard

- 1152 x 864 à 75 Hz VESA
- 1280 x 960 à 60 Hz VESA
- 1280 x 1024 à 60 Hz VESA
- 1360 x 768 à 60 Hz VESA
- 1400 x 1050 à 60 Hz VESA
- 1440 x 900 à 60 Hz VESA
- 1600 x 1200 à 60 Hz VESA
- 1680 x 1050 à 60 Hz VESA
- 1920 x 1080 à 60 Hz VESA

Résolution native d'affichage

Vous pouvez sélectionner la résolution native du CIM sur la page Port Configuration (Configuration des ports) dans le menu déroulant Display Native Resolution (Résolution native d'affichage). Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM. Si aucune sélection n'est effectuée, la résolution par défaut 1280 x 1024 est utilisée.Reportez-vous à ***Configuration des ports CIM*** (à la page 212).

Mode de compatibilité DVI

Le mode de compatibilité DVI est utilisé si vous vous connectez à une cible Dell Optiplex dotée d'une carte vidéo Intel ou à un Mac® Mini doté d'un contrôleur HDMI à l'aide d'un CIM HDMI. La sélection de ce mode assure une bonne qualité vidéo sur les cibles. Reportez-vous à ***Configuration des ports CIM*** (à la page 212).

CIM Paragon et configurations pris en charge

L'unité KX II prend en charge les CIM P2CIM-APS2DUAL et P2CIM-AUSBDUAL, qui fournissent deux connexions RJ45 à des commutateurs KVM différents. La prise en charge de ces CIM offre un second chemin d'accès à la cible au cas où l'un des commutateurs KVM est bloqué ou tombe en panne.

CIM Paragon	Prend en charge	Ne prend pas en charge
P2CIM-APS2DUAL	• Serveurs avec ports clavier et souris IBM® PS/2 • Compensation d'inclinaison automatique (lorsque les CIM sont connectés à Paragon II, non depuis KX II) • Mode Souris intelligente • Mode Souris standard	• Support virtuel • Cartes à puce • Mode Souris absolue • Utilisation avec châssis de lames • Configuration KVM en cascade
P2CIM-AUSBDUAL	• Serveurs avec ports clavier et souris USB ou Sun™ USB • Compensation d'inclinaison automatique (lorsque les CIM sont connectés à Paragon II, non depuis KX II) • Mode Souris intelligente • Mode Souris standard	• Support virtuel • Cartes à puce • Mode Souris absolue • Utilisation avec châssis de lames • Configuration KVM en cascade

KX II à KX II - Directives

Les directives de configuration système ci-après doivent être respectées si vous utilisez des CIM Paragon dans une configuration KX II à KX II :

Accès simultané

Les deux commutateurs KVM KX II doivent utiliser la même stratégie pour l'accès simultané aux cibles, PC-Share ou Private.

Si l'accès Private aux cibles est nécessaire, les deux commutateurs KVM doivent être configurés en conséquence :

- Dans le menu Security > Security Settings > Encryption & Share (Sécurité > Paramètres de sécurité > Chiffrement & Partager), paramètrez l'option PC Share sur Private (Privé).

Ceci garantit que l'accès simultané aux cibles est interdit pour toutes les cibles par tous les groupes d'utilisateurs.

KX II permet une gestion plus modulaire de l'accès simultané aux cibles par groupe d'utilisateurs. Ceci est effectué par le paramétrage des autorisations PC Share du groupe d'utilisateurs. Cependant, ceci est uniquement appliqué dans le cadre d'une unité KX II. Les autorisations PC Share de groupe d'utilisateurs ne suffisent pas à garantir la confidentialité si le CIM P2CIM-APS2DUAL ou P2CIM-AUSBDUAL est utilisé avec KX II.

Mises à jour des noms de CIM

Le nom des CIM P2CIM-APS2 et P2CIM-AUSB est stocké dans leur mémoire. Deux emplacements de mémoire sont fournis pour prendre en compte la convention de nommage Paragon (12 caractères) et celle de KX II (32 caractères).

Lors de la première connexion à KX II, le nom Paragon est extrait de la mémoire et inscrit à l'emplacement de la mémoire du CIM utilisé par KX II. Les demandes suivantes du nom de CIM ou les mises à jour de ce nom provenant du KX II seront effectuées à l'emplacement de la mémoire utilisé par KX II. Les mises à jour ne seront pas effectuées par KX II à l'emplacement de mémoire utilisé par Paragon II.

Lorsque le nom du CIM est mis à jour par une unité KX II, l'autre unité KX II détecte et extrait le nouveau nom à la tentative suivante de connexion à cette cible. Avant cela, le nom n'est pas mis à jour sur l'autre unité KX II.

Statut et disponibilité des ports

Le statut du port, affiché sur la page Port Access (Accès aux ports) de l'unité KX II comme Up (Connecté) ou Down (Déconnecté), est actualisé pour indiquer si le CIM est sous tension et connecté au port KX II.

La disponibilité du port, affichée sur la page Port Access (Accès aux ports) de l'unité KX II comme Idle (Ralenti), Busy (Occupé) ou Connected (Connecté), est uniquement mise à jour pour refléter l'activité sur une cible lancée depuis cette même unité KX II.

Si une connexion est en place entre l'autre unité KX II et la cible, la disponibilité est vérifiée lors de la tentative de connexion. L'accès est refusé ou autorisé suivant la stratégie PC-Share définie pour l'unité KX II. Avant cela, la disponibilité n'est pas mise à jour sur l'autre unité KX II.

Si l'accès est refusé parce que la cible est occupée, une notification s'affiche.

Travail depuis CC-SG

Les opérations lancées depuis CC-SG sont basées sur les statut, disponibilité et nom de CIM indiqués par l'unité KX II gérée. Lorsque la cible est connectée à deux unités KX II gérées et que ces dispositifs sont ajoutés à CC-SG, deux nœuds sont créés. Chaque nœud sera associé à sa propre interface oob-kvm. Un nœud unique peut également être configuré avec une interface oob-kvm provenant de chaque unité KX II.

Si les unités KX II sont configurées pour le mode Private (Privé), à la deuxième tentative de connexion, l'utilisateur est prévenu qu'il ne peut pas se connecter et que l'accès est refusé.

Lorsqu'un nom de port est modifié via un volet CC-SG Port Profile (Profil de port CC-SG), le nouveau nom est répercuté sur l'unité KX II gérée. Le nom de port correspondant de l'autre unité KX II n'est mis à jour dans CC-SG qu'après une tentative de connexion au port cible via l'interface oob-kvm de l'autre unité KX II.

KX II à Paragon II - Directives

Le CIM P2CIM-APS2DUAL ou P2CIM-AUSBDUAL peut être connecté à une unité KX II et à Paragon II.

Accès simultané

Les deux unités KX II et Paragon II doivent utiliser la même stratégie pour l'accès simultané aux cibles.

Mode de fonctionnement de Paragon II	Description du mode	Prise en charge ?
Private (Privé)	Un serveur ou un autre dispositif sur un port de canal spécifique est accessible exclusivement par un seul utilisateur à la fois.	Oui. Paragon II et l'unité KX II doivent être paramétrés sur Private. Le paramètre Private est appliqué au dispositif KX II, non selon le

Mode de fonctionnement de Paragon II	Description du mode	Prise en charge ?
		groupe d'utilisateurs. Paragon II utilise la couleur rouge pour indiquer occupé ou la couleur verte pour indiquer disponible.
PC-Share	Un serveur ou un autre dispositif sur un port de canal spécifique peut être sélectionné et contrôlé par plusieurs utilisateurs, mais un seul utilisateur détient le contrôle du clavier et de la souris.	Oui. Toutefois, la fonction PC Share Idle Timeout (Temporisation pour inactivité), configurée sur Paragon II, n'est pas prise en charge. Deux utilisateurs détiennent simultanément le contrôle du clavier et de la souris. Paragon II utilise la couleur verte pour indiquer disponible, ce qui est aussi vrai si un autre utilisateur accède déjà à la cible.
Public View (Affichage public)	Alors qu'un utilisateur accède à un serveur ou à un autre dispositif sur un port de canal spécifique, d'autres utilisateurs peuvent sélectionner ce port de canal et visualiser la sortie vidéo de ce dispositif. Cependant, seul le premier utilisateur détient le contrôle du clavier et de la souris jusqu'à ce qu'il se déconnecte ou change de dispositif.	Non. Ce mode ne peut pas être utilisé lors de la connexion du CIM à Paragon II et au KX II. Paragon II utilise la couleur jaune pour indiquer qu'il est en mode P-View.

Mises à jour des noms de CIM

- Les noms de CIM mis à jour depuis Paragon II sont stockés et extraits de l'emplacement de mémoire de CIM correspondant à la convention d'appellation de Paragon.
- Les noms de CIM mis à jour depuis KX II sont stockés et extraits de l'emplacement de mémoire de CIM correspondant à la convention d'appellation de ce produit.
- Les mises à jour de nom de CIM ne sont pas transmises entre Paragon II et l'unité KX II.

Distance prise en charge pour l'intégration de KX II

Lorsque KX II est utilisé comme élément frontal d'un système Paragon, nous vous recommandons de limiter la longueur de câble (distance) pour obtenir une bonne qualité vidéo.

La distance prise en charge entre la station utilisateur Paragon et le serveur cible est de 152 m de câble. Si la distance est plus importante, les performances vidéo risquent d'être altérées.

La distance prise en charge entre KX II et la station utilisateur Paragon est de 45 m de câble.

Lecteurs de cartes à puce

Lecteurs de cartes à puce pris en charge ou non

Les lecteurs de cartes à puce USB externes sont pris en charge.

Lecteurs de cartes à puce pris en charge

Type	Fabricant	Modèle	Vérifié
USB	SCM Microsystems	SCR331	Vérifié en local et à distance
USB	ActivIdentity®	Lecteur USB v2.0 ActivIdentity	Vérifié en local et à distance
USB	ActivIdentity	Lecteur USB v3.0 ActivIdentity	Vérifié en local et à distance
USB	Gemalto®	GemPC USB-SW	Vérifié en local et à distance
Clavier avec lecteur de cartes USB	Dell®	Clavier/Lecteur de cartes à puce USB	Vérifié en local et à distance

Type	Fabricant	Modèle	Vérifié
USB	SCM Microsystems	SCR331	Vérifié en local et à distance
Clavier avec lecteur de cartes USB	Cherry GmbH	G83-6744 SmartBoard	Vérifié en local et à distance
Lecteur USB de cartes SIM	Omnikey	6121	Vérifié en local et à distance
Intégré (Dell Latitude D620)	O2Micro	OZ776	En local uniquement
PCMCIA	ActivIdentity	Lecteur PCMCIA ActivIdentity	En local uniquement
PCMCIA	SCM Microsystems	SCR243	En local uniquement

Remarque : les lecteurs de cartes à puce SCR331 SCM Microsystems doivent utiliser le firmware SCM Microsystems v5.25.

Lecteurs de cartes à puce non pris en charge

Ce tableau contient la liste des lecteurs testés par Raritan qui ne fonctionnent pas avec le dispositif Raritan et ne sont donc pas pris en charge. Si un lecteur de cartes à puce n'apparaît ni dans le tableau des lecteurs pris en charge ni dans celui des lecteurs non pris en charge, Raritan ne peut pas garantir qu'il fonctionne avec le dispositif.

Type	Fabricant	Modèle	Remarques
Clavier avec lecteur de cartes USB	HP®	ED707A	Point de terminaison sans interruption => non compatible avec pilote Microsoft®
Clavier avec lecteur de cartes USB	SCM Microsystems	SCR338	Mise en œuvre de lecteur de cartes propriétaire (non compatible CCID)
Jeton USB	Aladdin®	eToken PRO™	Mise en œuvre propriétaire

Configuration système minimum pour carte à puce

Exigences en matière de port local

L'exigence en matière d'interopérabilité de base pour la connexion du port local au KX II est la suivante :

- Tous les dispositifs (lecteur de cartes à puce ou jeton) connectés localement doivent être compatibles USB CCID.

Exigences en matière de serveur cible

Pour l'utilisation de lecteurs de cartes à puce, les exigences de base en matière d'interopérabilité au niveau du serveur cible sont les suivantes :

- Le gestionnaire IFD (lecteur de cartes à puce) doit être un pilote de périphérique CCID USB standard (comparable au pilote CCID USB Microsoft® générique).
- Un CIM numérique ou D2CIM-DVUSB (CIM double VM) est nécessaire et doit utiliser la version de firmware 3A6E ou supérieure.
- Les connexions de serveurs avec châssis de lames, où un CIM par lame est utilisé, sont prises en charge.
- Ce type de connexions, où un CIM par châssis est utilisé, n'est pris en charge que pour les modèles E et H d'IBM BladeCenter® où la détection automatique est activée.

Cibles Windows XP

Les cibles Windows XP® doivent exécuter Windows XP SP3 afin d'utiliser des cartes à puce avec KX II. Si vous travaillez avec .NET 3.5 dans un environnement Windows XP sur le serveur cible, vous devez utiliser SP1.

Cibles Linux

Si vous utilisez une cible Linux®, les exigences suivantes doivent être respectées pour permettre l'utilisation de lecteurs de cartes à puce avec le dispositif Raritan.

- Exigences CCID

  Si D2CIM-DVUSB VM/CCID Raritan n'est pas reconnu en tant que lecteur de cartes à puce par votre cible Linux, il vous faudra peut-être mettre à jour la version du pilote CCID à 1.3.8 ou supérieure, et le fichier de configuration du pilote (Info.plist).

Système d'exploitation	Exigences CCID
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12

Fedora® Core 10	ccid-1.3.8-1.fc10.i386

Exigences en matière de client distant

Les exigences de base en matière d'interopérabilité au niveau du client distant sont les suivantes :

- Le gestionnaire IFD (lecteur de cartes à puce) doit être un pilote de périphérique compatible PC/SC.
- Le gestionnaire de ressources ICC (carte à puce) doit être disponible et compatible PC/SC.
- Le programme JRE™ 1.6.x avec interface API pour carte à puce doit être disponible pour être utilisé par l'application cliente Raritan.

Clients Linux

Si vous utilisez un client Linux®, les exigences suivantes doivent être respectées pour permettre l'utilisation de lecteurs de cartes à puce avec le dispositif Raritan.

Remarque : la connexion de l'utilisateur au client, à l'insertion d'une carte à puce, peut durer plus longtemps si une ou plusieurs sessions KVM sont actives vers les cibles. Le processus de connexion à ces cibles est en effet en cours.

- Exigences PC/SC

Système d'exploitation	PC/SC requis
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Créer un lien vers la bibliothèque Java™

  Un lien symbolique doit être créé vers libpcsclite.so après la mise à niveau de RHEL 4, RHEL 5 et FC 10. Par exemple, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, en supposant que l'installation du progiciel ait placé les bibliothèques dans /usr/lib ou /user/local/lib.

- Démon PC/SC

  Lorsque le démon pcsc (gestionnaire de ressources dans framework) est redémarré, relancez le navigateur et MPC.

Longueurs de câbles et résolutions vidéo pour châssis Dell

Afin de maintenir la qualité vidéo, Raritan recommande l'utilisation des longueurs de câbles et les résolutions vidéo suivantes lorsque vous êtes connecté à un châssis de lames Dell® depuis KX II :

Longueur de câble	Résolution vidéo
1 524,00 cm	1024 x 768 x 60
1 524,00 cm	1280 x 1024 x 60
914,40 cm	1600 x 1200 x 60

Audio

Formats de dispositifs audio pris en charge

KX II prend en charge un dispositif de lecture et de capture, et un dispositif d'enregistrement simultanément. Les formats de dispositifs audio suivants sont pris en charge :

- Stéréo 16 bits, 44,1 K
- Mono 16 bits, 44,1 K
- Stéréo 16 bits, 22,05 K
- Mono 16 bits, 22,05 K
- Stéréo 16 bits, 11,025 K
- Mono 16 bits, 11,025 K

Recommandations et exigences en matière de lecture et de capture audio

Niveau sonore

Réglez le son de la cible à un niveau intermédiaire. Par exemple, sur un client Windows®, réglez-le sur 50 ou plus bas. Ce paramètre doit être configuré depuis le dispositif audio de lecture ou de capture, et non depuis le contrôle du dispositif audio du client.

Recommandations en matière de connexions audio lorsque le mode PC Share est activé

Si vous utilisez la fonction audio lors de l'exécution du mode PC Share, la lecture et la capture audio sont interrompues si un dispositif audio supplémentaire est connecté à la cible.

Par exemple, l'utilisateur A connecte un dispositif de lecture à Cible1 et exécute une application de lecture audio ; l'utilisateur B connecte ensuite un dispositif de capture à la même cible. La session de lecture de l'utilisateur A est interrompue et l'application audio devra peut-être redémarrée.

L'interruption a lieu car le dispositif USB doit être énuméré à nouveau avec la configuration du nouveau dispositif. L'installation d'un pilote pour le nouveau dispositif par la cible peut prendre du temps. Les applications audio peuvent arrêter complètement la lecture, passer à la piste suivante ou poursuivre la lecture. Le comportement exact dépend de la façon dont l'application audio est conçue pour traiter un événement de déconnexion/reconnexion.

Exigences en matière de bande passante

Le tableau ci-dessous détaille les exigences en matière de bande passante de lecture et de capture audio pour le transport du son sur chaque format sélectionné.

Format audio	Bande passante réseau requise
44,1 KHz, stéréo 16 bits	176 Ko/s
44,1 KHz, mono 16 bits	88,2 Ko/s
2,05 KHz, stéréo 16 bits	88,2 Ko/s
22,05 KHz, mono 16 bits	44,1 Ko/s
11,025 KHz, stéréo 16 bits	44,1 Ko/s
11,025 KHz, mono 16 bits	Audio 22,05 Ko/s

Dans la pratique, la bande passante utilisée pour connecter un dispositif audio à une cible est plus importante en raison des données de clavier et vidéo consommées lors de l'ouverture et de l'utilisation d'une application audio sur la cible.

En règle générale, nous vous recommandons une connexion d'au moins 1,5 Mo avant d'exécuter la lecture et la capture. Toutefois, un contenu vidéo important, des connexions en couleurs avec des résolutions d'écran élevées sur la cible consomment beaucoup plus de bande passante et affectent considérablement la qualité sonore. Les paramètres clients recommandés permettent de réduire l'effet de la vidéo sur la qualité sonore avec des bandes passantes inférieures :

- Connectez les dispositifs de lecture audio à des formats de qualité inférieure. La consommation de bande passante par la vidéo affecte moins les performances avec des connexions de 11k que de 44k.
- Paramétrez la vitesse de connexion sous Connection Properties (Propriétés de connexion) sur une valeur correspondant le mieux à la connexion client-serveur.
- Sous Connection Properties, paramétrez le nombre de couleurs sur la valeur la plus basse possible. La réduction à une couleur de 8 bits réduit la consommation de bande passante.
- Paramétrez le lissage sur High (Elevé). Ceci améliorera l'apparence de la vidéo cible en réduisant le bruit de la vidéo affichée.
- Sous Video settings (Paramètres vidéo), paramétrez Noise Filter (Filtre antiparasite) sur 7 (valeur maximale) afin de réduire l'utilisation de bande passante pour les changements d'écran cible.

Nombre de connexions audio/supports virtuels et cartes à puce prises en charge

Vous trouverez ci-après le nombre de connexions audio/supports virtuels et cartes à puce simultanées possibles entre un client et une cible :

- 1 carte à puce
- 1 supports virtuels
- 1 carte à puce et 1 support virtuel
- 2 supports virtuels

Modems certifiés

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

Dispositifs pris en charge par le port local étendu

Le port local étendu prend en charge la connexion des dispositifs suivants :

- Station utilisateur Paragon II (P2-UST) connectée directement au port local étendu
- Station utilisateur optimisée Paragon II (P2-EUST) connectée directement au port local étendu
- Récepteur URKVMG Cat5Reach connecté directement au port local étendu
- Port cible de commutateur KVM analogique Paragon II (UMT) connecté directement au port local étendu. Permet un accès supplémentaire au port local étendu, lorsqu'il est utilisé avec la station utilisateur optimisée Paragon II.

Distances maximales recommandées pour le port local étendu de KX2 8xx

Dispositif étendu	1 024 x 768 à 60 Hz	1280 x 1024 à 60 Hz
Paragon II UMT avec EUST	1000	900
Paragon EUST	500	400
URKVM	650	250
Paragon UST	500	200

Connexions à distance prises en charge

Connexion à distance	Détails
Réseau	Ethernet 10BASE-T, 100BASE-T et 1000BASE-T (Gigabit)
Protocoles	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Langues de clavier prises en charge

L'unité KX II fournit un support clavier pour les langues indiquées dans le tableau suivant.

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 de KX II. Pour plus d'informations sur les claviers non US, reportez-vous à **Remarques d'informations** *(à la page 389).*

Remarque : Raritan recommande d'utiliser système-config-clavier pour modifier les langues si vous travaillez dans un environnement Linux.

Langue	Régions	Configuration du clavier
Anglais (Etats-Unis)	Etats-Unis d'Amérique et la plupart des pays anglophones : Canada, Australie et Nouvelle-Zélande, par exemple.	Clavier américain
Anglais international	Etats-Unis d'Amérique et la plupart des pays où l'anglais est utilisé : les Pays-Bas par exemple.	Clavier américain
Anglais britannique	Royaume-Uni	Clavier britannique
Chinois traditionnel	Hong Kong R.A.S., République de Chine (Taïwan)	Chinois traditionnel
Chinois simplifié	République populaire de Chine (continentale)	Chinois simplifié
Coréen	Corée du Sud	Hangeul Dubeolsik
Japonais	Japon	Clavier JIS
Français	France	Clavier AZERTY français.
Allemand	Allemagne et Autriche	Clavier QWERTZ allemand
Français	Belgique	Belge
Norvégien	Norvège	Norvégien
Danois	Danemark	Danois
Suédois	Suède	Suédois
Hongrois	Hongrie	Hongrois

Langue	Régions	Configuration du clavier
Slovène	Slovénie	Slovène
Italien	Italie	Italien
Espagnol	Espagne et la plupart des pays hispanophones	Espagnol
Portugais	Portugal	Portugais

Ports TCP et UDP utilisés

Port	Description
HTTP, Port 80	Ce port peut être configuré selon les besoins. Reportez-vous à ***Paramètres des ports HTTP et HTTPS*** (à la page 182). Toutes les requêtes reçues par KX II via HTTP (port 80) sont automatiquement transmises à HTTPS pour garantir une sécurité complète. Pour plus de facilité, KX II répond au port 80 (les utilisateurs n'ont ainsi pas à taper explicitement dans le champ URL pour accéder à KX II) tout en préservant un niveau complet de sécurité.
HTTPS, Port 443	Ce port peut être configuré selon les besoins. Reportez-vous à ***Paramètres des ports HTTP et HTTPS*** (à la page 182). Par défaut, ce port est utilisé à diverses fins, notamment pour le serveur Web du client HTML, le téléchargement du logiciel client (MPC/VKC) sur l'hôte du client et le transfert de flux de données KVM et de support virtuel vers le client.
Protocole KX II (Raritan KVM sur IP), Port 5000 configurable	Ce port est utilisé pour détecter d'autres dispositifs Dominion et pour la communication entre les dispositifs et les systèmes Raritan, notamment CC-SG pour les dispositifs pour lesquels la gestion CC-SG est disponible. Le port défini par défaut est le port 5000. Vous pouvez néanmoins configurer ce paramètre pour utiliser tout port TCP libre. Pour plus de détails sur la façon de configurer ce paramètre, reportez-vous à ***Paramètres réseau*** (à la page 176).
SNTP (serveur d'horloge) sur le port UDP configurable 123	KX II offre la fonction facultative de synchroniser son horloge interne sur un serveur d'horloge 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. **Facultatif**
LDAP/LDAPS sur les ports configurables 389 ou 636	Si KX II est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole LDAP, les ports 386 ou 636 sont utilisés. Le système peut également être configuré pour utiliser le port de votre choix. **Facultatif**
RADIUS sur le port configurable 1812	Si KX II est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole RADIUS, le port 1812 est utilisé. Le système peut également être configuré pour utiliser le port de votre choix. **Facultatif**
Gestion RADIUS sur le port configurable 1813	Si KX II est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole RADIUS et qu'il utilise également Gestion RADIUS pour la consignation 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 configurable 514	Si 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 UDP par défaut SNMP	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. **Facultatif**

Port TCP 21	Le port 21 est utilisé pour l'interface de ligne de commande de KX II (lorsque vous travaillez avec l'assistance technique Raritan).

Evénements capturés dans le journal d'audit et dans Syslog

Vous trouverez ci-après la liste et la description des événements capturés par le journal d'audit et syslog de KX II.

- Access Login (Connexion d'accès) - Un utilisateur s'est connecté à KX II.
- Access Logout (Déconnexion d'accès) - Un utilisateur s'est déconnecté de KX II.
- Active USB Profile - Le profil USB est actif.
- CIM Connected - Un CIM a été connecté.
- CIM Disconnected - Un CIM a été déconnecté.
- Connection Lost - La connexion à la cible a été perdue.
- Disconnected User - Un utilisateur a été déconnecté d'un port.
- End CC Control - La gestion par CC-SG est terminée.
- Login Failed - La connexion de l'utilisateur a échoué.
- Password Changed - Le mot de passe a été modifié.
- Port Connect - Le port a été connecté.
- Port Disconnect - Le port a été déconnecté.
- Port Status Change - Modification du statut du port
- Scan Started - Un balayage de cible a été démarré.
- Scan Stopped - Un balayage de cible a été arrêté.
- Session Timeout - Un délai d'inactivité de session a expiré.
- VM Image Connected - Une image VM a été connectée.
- VM Image Disconnected - Une image VM a été déconnectée.

Paramètres de vitesse réseau

Paramètre de vitesse réseau KX II

Paramètre de port de commutateur réseau	**Auto**	**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
		Vitesse disponible maximale	1000/Full	KX II : 100/Full Commutateur : 100/Half	100/Half	KX II : 10/Full Commutateur : 10/Half	10/Half

Paramètre de vitesse réseau KX II						
1000/Full	1000/Full	1000/Full	Aucune communication	Aucune communication	Aucune communication	Aucune communication
100/Full	KX II : 100/Half Commutateur : 100/Full	KX II : 100/Half Commutateur : 100/Full	100/Full	KX II : 100/Half Commutateur : 100/Full	Aucune communication	Aucune communication
100/Half	100/Half	100/Half	KX II : 100/Full Commutateur : 100/Half	100/Half	Aucune communication	Aucune communication
10/Full	KX II : 10/Half Commutateur : 10/Full	Aucune communication	Aucune communication	Aucune communication	10/Full	KX II : 10/Half Commutateur : 10/Full
10/Half	10/Half	Aucune communication	Aucune communication	Aucune communication	KX II : 10/Full Commutateur : 10/Half	10/Half

Légende :

Ne fonctionne pas comme prévu

Pris en charge

Fonctionne ; non recommandé

NON pris en charge par la spécification Ethernet ; le produit peut communiquer mais des collisions se produisent.

Selon la spécification Ethernet, « aucune communication » ne devrait se produire ; notez toutefois que le comportement KX II diffère du comportement attendu.

Remarque : pour assurer une communication réseau fiable, configurez KX II et le commutateur LAN sur les mêmes valeurs de vitesse d'interface de réseau local et duplex. Par exemple, configurez KX II et le commutateur LAN sur Autodetect (détection automatique) (recommandé) ou sur une vitesse fixe/duplex, comme 100Mo/s/Full.

Annexe B Groupes de deux ports vidéo

Dans ce chapitre

Présentation

Les serveurs dotés de deux cartes vidéo sont accessibles à distance avec une configuration de bureau étendu, disponible aux utilisateurs distants. Pour ce faire, vous devez créer des groupes de deux ports vidéo.

La configuration de bureau étendu vous permet d'afficher le bureau du serveur cible sur deux écrans, au lieu d'un affichage standard sur un écran. Une fois le groupe de deux ports vidéo sélectionné, tous les canaux de port de ce groupe s'ouvrent simultanément. Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 259) pour en savoir plus à ce sujet.

Consultez les informations de cette section pour obtenir des informations importantes sur la création de groupes de deux ports vidéo.

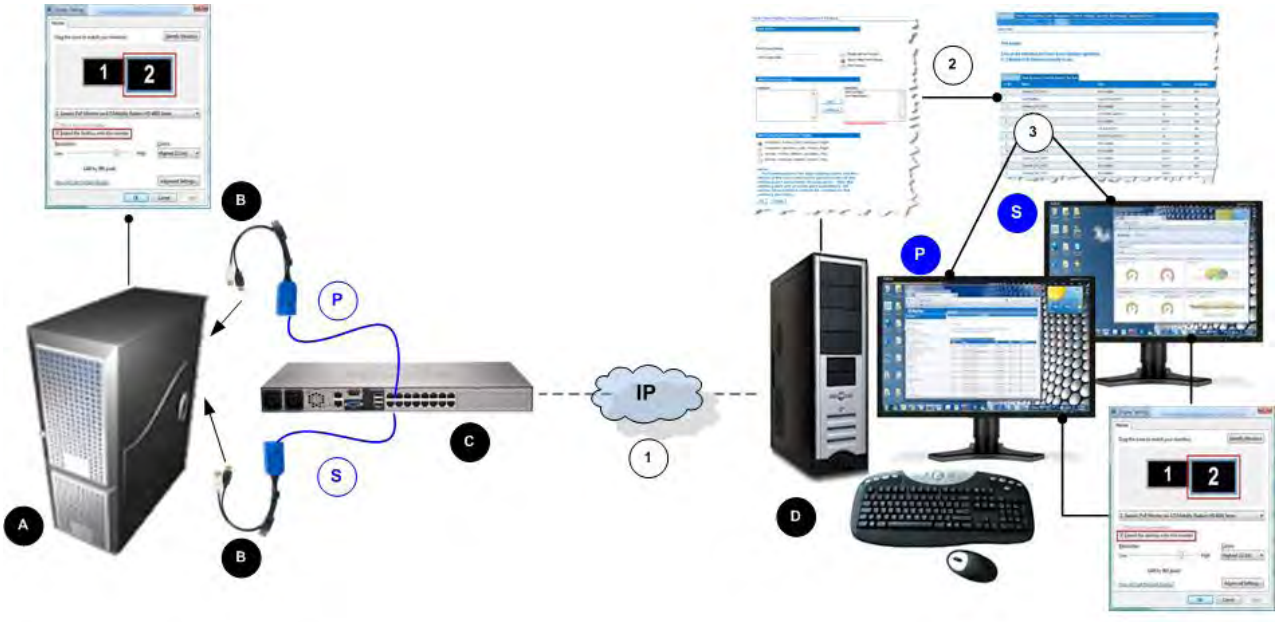
Remarque : les groupes de deux ports vidéo ne sont pas pris en charge par les modèles KX II dotés d'un seul canal KVM, tels que KX2-108 et KX2-116.

Exemple de configuration de groupe de deux ports vidéo

Les étapes suivantes sont fournies à titre d'exemple général. Votre configuration peut varier selon le type de CIM utilisé, le port désigné comme port principal, les ports du KX II auxquels vous vous connectez, etc.

Dans cet exemple, nous utilisons :

- Un serveur cible avec deux ports vidéo
- Port vidéo 1 du serveur cible comme port principal et port vidéo 2 du serveur cible comme port secondaire
- Un dispositif KX II-832
- Un CIM D2CIM-DVUSB-DP
- Un serveur cible et un client distant exécutant le système d'exploitation Microsoft® Windows 7®
- Mode souris intelligente
- Une vue bureau étendu sur le serveur cible et le client distant ; nous configurons donc KX II pour prendre en charge l'orientation d'affichage Horizontal - Primary (Left), Secondary (Right) (Horizontal - Principal (gauche), Secondaire (droite)



Légende	
A	Serveur cible

Légende	
B	CIM numériques
C	KX II
D	Client distant
P	Connexion du premier port vidéo de la cible à KX II
S	Connexion du second port vidéo de la cible à KX II
1	Connexion IP entre KX II et le client distant
2	Création de groupes de deux ports vidéo dans KX II
3	Lancement du groupe de deux ports vidéo
P	Affichage du port principal (défini sur la page Port Group Management (Gestion des groupes de ports) dans KX II)
S	Affichage du port secondaire (défini sur la page Port Group Management (Gestion des groupes de ports) dans KX II)

Etape 1 : Configuration de l'affichage du serveur cible

Le paramètre d'orientation configuré sur KX II pour la cible doit correspondre à la configuration réelle du système d'exploitation de la cible. Il est recommandé d'utiliser autant que possible la même orientation d'écran sur le client de connexion.

Reportez-vous à Orientation, alignement de l'affichage et modes souris des groupes de deux ports vidéo pour plus d'informations sur les orientations d'affichage et les modes souris.

Remarque : reportez-vous à la documentation utilisateur du serveur cible ou du système d'exploitation pour obtenir les procédures exactes de configuration des paramètres d'affichage.

Pour configurer les paramètres d'affichage et de souris du serveur cible :

1. Sur le serveur cible, configurez l'orientation d'affichage du serveur cible pour chaque port vidéo en fonction de celle du client distant.

Par exemple, si vous utilisez une orientation bureau étendu de gauche à droite sur deux écrans sur le client distant, définissez la même orientation d'affichage sur le serveur cible.

2. Vérifiez que l'écran du serveur cible est déjà défini sur une résolution et un taux de rafraîchissement pris en charge. Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 341).

Remarque : Si les affichages principal et secondaire de la cible sont définis sur des résolutions différentes, la souris ne restera pas synchronisée. Il faudra donc la synchroniser à nouveau régulièrement à partir de la fenêtre cible supérieure gauche.

Etape 2 : Connexion du serveur cible à KX II

Des groupes de deux ports vidéo peuvent être créés à partir de connexions de port existantes ou nouvelles. La procédure fournie ici suppose la création de nouvelles connexions. Si vous créez un groupe de deux ports vidéo à partir de connexions existantes, reportez-vous à ***Etape 4 : Création d'un groupe de deux ports vidéo*** (voir "***Etape 4 : Création du groupe de deux ports vidéo***" à la page 371).

Pour connecter l'équipement :

1. Le cas échéant, installez et mettez sous tension le serveur cible selon les instructions du fabricant.
2. Raccordez le connecteur vidéo de chaque CIM à chacun des ports de sortie vidéo de la cible et connectez les câbles USB aux ports USB disponibles sur la cible.
3. Connectez chaque CIM à KX II à l'aide d'un câble CAT5/6.
4. Le cas échéant, reliez KX II à une source d'alimentation CA à l'aide du câble d'alimentation fourni, connectez-vous au port réseau et au port local (au besoin) de KX II, et configurez KX II. Reportez-vous à ***Mise en route*** (à la page 19) pour obtenir les étapes nécessaires à l'utilisation initiale de KX II.
5. Connectez-vous à KX II depuis un poste de travail doté d'une connectivité réseau et de Microsoft .NET® et/ou Java Runtime Environment® (JRE® est disponible sur le ***site Web de Java http://java.sun.com/***).
6. Démarrez un navigateur Web pris en charge, tel qu'Internet Explorer® ou Firefox®.

7. Entrez l'URL : *http://ADRESSE-IP* ou *http://ADRESSE-IP/akc* pour .NET, où ADRESSE-IP correspond à l'adresse IP affectée au dispositif KX II. Vous pouvez aussi utiliser https, le nom DNS de KX II attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou simplement saisir l'adresse IP dans le navigateur (KX II redirige toujours l'adresse IP de HTTP vers HTTPS).
8. Entrez vos nom d'utilisateur et mot de passe. Cliquez sur Login (Se connecter).
9. Configurez le mode souris du serveur cible.

   Par exemple, définissez le mode souris intelligente sur le serveur si vous l'utilisez sur le client distant. Reportez-vous à ***Paramètres de souris*** (à la page 20) pour obtenir les paramètres de souris à appliquer en fonction du système d'exploitation utilisé.

Etape 3 : Configuration du mode souris et des ports

Une fois le serveur cible connecté via ses ports vidéo à KX II, ce dernier détecte la connexion et affiche les ports sur la page Port Configuration. Reportez-vous à ***Configuration des serveurs cible standard*** (à la page 209) pour obtenir des instructions.

Une fois les ports configurés, ils peuvent être réunis dans un groupe de deux ports vidéo.

Remarque : il n'est pas nécessaire de configurer les ports existants si vous l'avez déjà fait. Reportez-vous à **Création d'un groupe de deux ports vidéo** *(à la page 259) pour en savoir plus à ce sujet.*

Configurez le mode souris du serveur cible une fois la connexion à la cible établie. Par exemple, définissez le mode souris intelligente sur le serveur si vous l'utilisez sur le client distant. Reportez-vous à ***Paramètres de souris*** (à la page 20) pour obtenir les paramètres de souris à appliquer en fonction du système d'exploitation utilisé.

Etape 4 : Création du groupe de deux ports vidéo

Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 259).

Etape 5 : Lancement d'un groupe de deux ports vidéo

Une fois le groupe de deux ports vidéo créé, il est disponible sur la page Port Access (Accès aux ports). Deux canaux KVM sont nécessaires pour la connexion à distance au groupe de deux ports vidéo en cliquant sur le port principal. Si ces deux canaux ne sont pas disponibles, le lien Connect n'apparaît pas.

Les délais d'inactivité de session configurés sur KX II sont appliqués aux deux ports d'un groupe de ports vidéo.

Pour lancer un groupe de deux ports :

- Sur la page Port Access (Accès aux ports), cliquez sur le nom de port principal, puis sur Connect (Connecter). Les deux connexions sont lancées en même temps et affichées dans deux fenêtres différentes.

Une fois les fenêtres affichées, elles peuvent être déplacées selon le paramétrage d'affichage utilisé. Par exemple, si vous utilisez le mode bureau étendu, les fenêtres de ports peuvent être déplacées entre les écrans.

Recommandations en matière de ports vidéo doubles

Réglez les écrans principal et secondaire du serveur cible sur la même résolution vidéo afin de maintenir la synchronisation de la souris et de réduire la fréquence de resynchronisation.

Selon l'orientation souhaitée, l'écran supérieur (orientation verticale) ou gauche (orientation horizontale) doit être désigné comme affichage principal. Vous activez ainsi la sélection de menu pour les opérations de support virtuel, audio, carte à puce et souris.

Pour permettre les mouvements et le contrôle intuitifs de la souris, les éléments suivants doivent être dotés de la même orientation : les écrans principal et secondaire du PC client, la configuration du groupe de deux ports vidéo de KX II, et les écrans principal et secondaire du serveur cible.

Seuls les paramètres de lancement du client ci-après seront appliqués aux affichages vidéo à ports doubles :

- Sélectionnez l'affichage standard ou mode Plein écran lors du lancement du client KVM.
- Activez la mise à l'échelle vidéo.
- Activez l'épinglage de la barre d'outils de menu en mode Plein écran.

L'utilisation du mode souris simple n'est pas recommandée lors de l'affichage des ports vidéo doubles en mode Plein écran sur un écran client unique. Vous devrez quitter ce mode pour accéder à l'autre écran et l'afficher.

Modes souris pris en charge

Systèmes d'exploitation cible	Modes souris pris en charge	Commentaires
Tous les systèmes d'exploitation Windows®	Modes souris intelligente, standard et unique	Si le mode Etirer (Stretch) est pris en charge par la carte vidéo du serveur cible, le mode souris absolue fonctionnera correctement. En mode Etirer, le serveur cible gère l'affichage double comme un affichage virtuel contigu unique. En revanche, en mode Etendu (Extended), le serveur considérera les deux écrans comme indépendants. Le

Systèmes d'exploitation cible	Modes souris pris en charge	Commentaires
		mode souris intelligente est recommandé en mode Etendu.
Linux®	Modes souris intelligente et standard	Les utilisateurs de Linux® VKC/MPC peuvent rencontrer des problèmes d'affichage et de mouvement de la souris en mode souris unique. Raritan recommande aux utilisateurs de Linux de ne pas l'employer.
Système d'exploitation Mac®	Mode souris unique	La synchronisation de la souris ne fonctionne pas sur les cibles à ports vidéo doubles.

CIM requis pour la prise en charge de vidéo double

Les CIM numériques suivants prennent en charge la fonction de port vidéo double :

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

Reportez-vous à ***Synchronisation et résolution vidéo du serveur cible des CIM numériques*** (à la page 347) pour obtenir des informations importantes concernant les CIM numériques. Reportez-vous à ***Spécifications des modules d'interface pour ordinateur (CIM) pris en charge*** (voir "***Spécifications des CIM pris en charge***" à la page 343) pour plus d'informations.

Si le CIM d'origine relié à un port vidéo principal ou secondaire est déconnecté et remplacé par un autre, le port est retiré du groupe de deux ports vidéo. Au besoin, ajoutez à nouveau le port au groupe.

Remarque : le CIM utilisé dépend des exigences du serveur cible.

Remarques relatives à l'utilisation des groupes de deux ports vidéo

Les fonctions suivantes sont affectées par l'utilisation de la fonction de groupe de deux ports vidéo.

- Les paramètres de lancement client configurés sur les clients VKC, AKC et MPC au moyen de Tools > Options > Client Launch Settings (Outils > Options > Paramètres de lancement client) seront appliqués aux groupes de deux ports vidéo comme suit :
  - Les paramètres de mode fenêtre seront appliqués.
  - Les paramètres d'écran NE SERONT PAS appliqués. L'orientation d'affichage (Display Orientation) configurée sur la page Port Group Management (Gestion des groupes de ports) sera appliquée à la place.
  - Le paramètre Other - Enable Single Mouse Cursor (Autre - Activer le curseur de souris simple) NE SERA PAS appliqué.
  - Le paramètre Other - Enable Scale Video (Autre - Activer la mise à l'échelle de la vidéo) sera appliqué.
  - Le paramètre Other - Pin Menu Toolbar (Autre - Epingler la barre d'outils de menu) sera appliqué.
- Le glissement et le déplacement d'éléments entre les fenêtres principale et secondaire de la cible requièrent de relâcher et d'enfoncer le bouton de la souris lorsque l'élément passe d'une fenêtre à l'autre.
- Sur les serveurs cible Linux® et Mac®, lorsque le verrouillage numérique et des majuscules est activé, l'indicateur de verrouillage des majuscules apparaît dans la barre de statut de la fenêtre du port principal, mais pas nécessairement dans celle du port secondaire.
- Les MPC peuvent ne pas être activés lorsque les cibles à port double sont ouvertes en mode Plein écran. Pour activer les menus, basculez sur les fenêtres de l'autre port, puis retournez à la fenêtre du port d'origine.

Autorisations et accès aux groupes de deux ports vidéo

idéalement, les autorisations appliquées à chaque port du groupe doivent être identiques. Sinon, les autorisations les plus restrictives seront appliquées au groupe.

Par exemple, si VM Access Deny (Accès refusé) est appliqué à un port et VM Access Read-Write (Accès en lecture-écriture) à un autre, VM Access Deny est appliqué au groupe.

Si un utilisateur ne dispose pas des autorisations appropriées pour accéder à un port faisant partie d'un groupe de deux ports vidéo, seul le port auquel il a accès est affiché. S'il n'est autorisé à accéder à aucun port, l'accès est refusé.

En cas de tentative d'accès, un message s'affiche indiquant que le port n'est pas disponible ou que l'utilisateur n'est pas autorisé à y accéder.

Navigation client Raritan lors de l'utilisation des groupes de deux ports vidéo

Navigation

Pour alterner entre deux ports lorsque le mode Plein écran est utilisé sur les clients :

- VKC

  Appuyez sur Alt+Tab.

  Pour les clients Mac®, appuyez sur F3, puis sélectionnez l'affichage du port.

- AKC

  Cliquez en dehors de la fenêtre d'affichage et appuyez sur Alt+Tab.

- MPC

  Sélectionnez des ports dans la barre d'outils Connected server(s) (Serveurs connectés).

Accès direct aux ports et groupes de deux ports vidéo

L'accès direct aux ports permet aux utilisateurs d'éviter les pages de connexion et d'accès aux ports du dispositif. Cette fonction permet également d'entrer un nom d'utilisateur et un mot de passe directement, et d'accéder à la cible si le nom d'utilisateur et le mot de passe ne sont pas contenus dans l'URL.

Si vous accédez à une cible faisant partie d'un groupe de deux ports vidéo, l'accès aux ports direct utilise le port principal pour lancer les ports principal et secondaire. Les connexions directes au port secondaire sont rejetées et les règles d'autorisation habituelles s'appliquent. Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 259) pour plus d'informations à ce sujet. Reportez-vous à ***Activation d'un accès direct aux ports via URL*** (à la page 188) pour plus d'informations.

Groupes de deux ports vidéo affichés sur la page Ports

Remarque : le port principal est défini à la création du groupe.

Remarque : Deux canaux KVM sont nécessaires pour la connexion à distance au groupe de deux ports vidéo en cliquant sur le port principal. Si ces deux canaux ne sont pas disponibles, le lien Connect n'apparaît pas.

Dans les groupes de deux ports vidéo, le port principal est inclus dans un balayage de ports, mais non le port secondaire lors de la connexion depuis un client distant. Les deux ports peuvent être inclus dans le balayage depuis le port local.

Reportez-vous à ***Page Port Access (affichage de la console distante)*** (à la page 56) pour plus d'informations sur le contenu affiché sur la page Ports et à ***Balayage des ports*** (à la page 61) pour plus d'informations sur l'exécution de balayages.

Annexe C Utilisation de KX II pour accéder à Paragon II

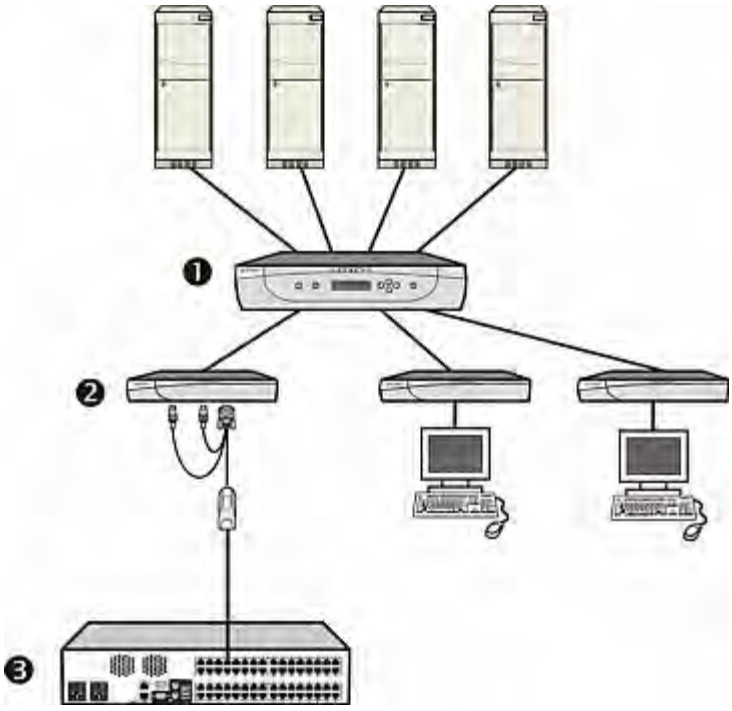
Dans ce chapitre

Présentation

Si vous ne disposez pas du dispositif P2SC, vous pouvez connecter le système Paragon II à un dispositif KX II géré par CC-SG afin de permettre l'accès à Paragon II depuis CC-SG. Pour assurer une compatibilité complète, il est recommandé que le dispositif KX II connecté à Paragon II exécute la version 2.1 ou supérieure.

Remarque : Paragon II est également accessible à distance sur IP via P2-USTIP. Toutefois, P2-USTIP ne prend pas en charge l'intégration aux plates-formes d'authentification/autorisation (AA), telles que LDAP ou Active Directory. KX II ne prend en charge ni ces plates-formes ni d'autres plates-formes AA.

Ce diagramme indique la configuration intégrant KX II.



❶	Système Paragon II impliquant des commutateurs, des serveurs et des stations utilisateur Paragon
❷	Station utilisateur reliée à DCIM-USB-G2 ou DCIM-PS2
❸	KX II

Lorsque vous accédez au système Paragon depuis KX II ou CC-SG (si KX II est géré par CC-SG), l'écran de connexion de l'interface utilisateur Paragon apparaît pour vous permettre d'ouvrir une session.

Dans cette intégration, vous pouvez exécuter toutes les fonctions d'interface utilisateur à l'écran mises en œuvre avec un firmware Paragon à jour, ou toutes les fonctions KX II mises en œuvre avec un firmware KX II à jour, hormis la fonction de support virtuel.

Lorsque vous accédez à l'interface utilisateur à l'écran de Paragon via KX II, NE TENTEZ PAS de synchroniser la souris manuellement. La souris n'est pas nécessaire sur l'écran de l'interface utilisateur et sa synchronisation retardera la réponse du clavier de quelques secondes.

Reportez-vous à ***CIM Paragon et configurations pris en charge*** (à la page 349) pour plus d'informations.

Connexion de Paragon II à KX II

Pour connecter le système Paragon II à KX II :

1. Assurez-vous que la version 4.6 ou supérieure du firmware est mise en œuvre sur la station utilisateur à connecter à KX II. Si tel n'est pas le cas, effectuez la mise à niveau. Reportez-vous à Mise à niveau du firmware pour obtenir des instructions. La station utilisateur peut être une des suivantes :
   - P2-UST
   - P2-EUST
   - P2-EUST/C
2. Connectez un DCIM compatible à cette station utilisateur. S'il s'agit d'un système à deux ou trois niveaux, assurez-vous que la station utilisateur est l'une de celles connectées à l'unité de base (premier niveau).

   Seuls deux types de DCIM sont pris en charge dans cette intégration :
   - Si vous utilisez DCIM-USB-G2, branchez ses connecteurs sur les ports USB et vidéo de la station utilisateur.
   - Si vous utilisez DCIM-PS2, branchez ses connecteurs sur les ports PS/2 et vidéo de la station utilisateur.
3. Connectez la station utilisateur à un dispositif KX II via un câble UTP Cat5 de 45 m au maximum.

- Branchez l'une des extrémités du câble sur le port RJ-45 du DCIM et l'autre, sur un des ports de canal du dispositif KX II.

4. Si vous souhaitez de disposer de chemins d'accès supplémentaires au même système Paragon II dans KX II ou CC-SG, répétez les étapes 1 à 3 pour connecter d'autres stations utilisateur à KX II.

Annexe D Mise à jour du schéma LDAP

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

Dans ce chapitre

Renvoi des informations relatives aux groupes d'utilisateurs

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

Depuis LDAP/LDAPS

Lorsqu'une demande d'authentification LDAP/LDAPS aboutit, >ProductName< détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel il appartient. 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/LDAPS. Consultez l'administrateur de votre serveur d'authentification pour activer cet attribut.

De plus, pour Microsoft® Active Directory®, le memberOf LDAP standard est utilisé.

A partir d'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 le serveur du système d'exploitation Windows 2000® nécessite la mise à jour du schéma LDAP/LDAPS. Reportez-vous à la documentation Microsoft pour plus d'informations.

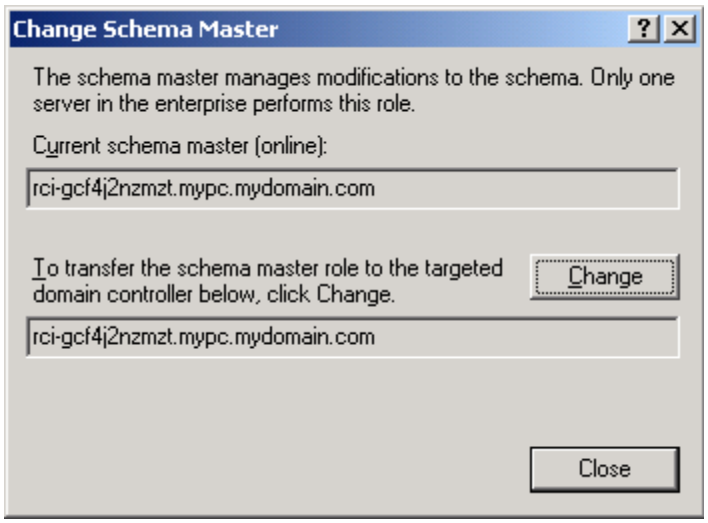
1. Installez le plug-in de schéma pour Active Directory. Reportez-vous à la documentation de Microsoft Active Directory pour obtenir des instructions.
2. Lancez la console Active Directory et sélectionnez Active Directory Schema (Schéma Active Directory).

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.

Pour permettre les opérations d'écriture sur le schéma :

1. Cliquez avec le bouton droit de la souris sur le nœud racine Schéma Active Directory® dans le volet de gauche de la fenêtre, puis cliquez sur Maître d'opérations. La boîte de dialogue Changer le contrôleur de schéma s'affiche.



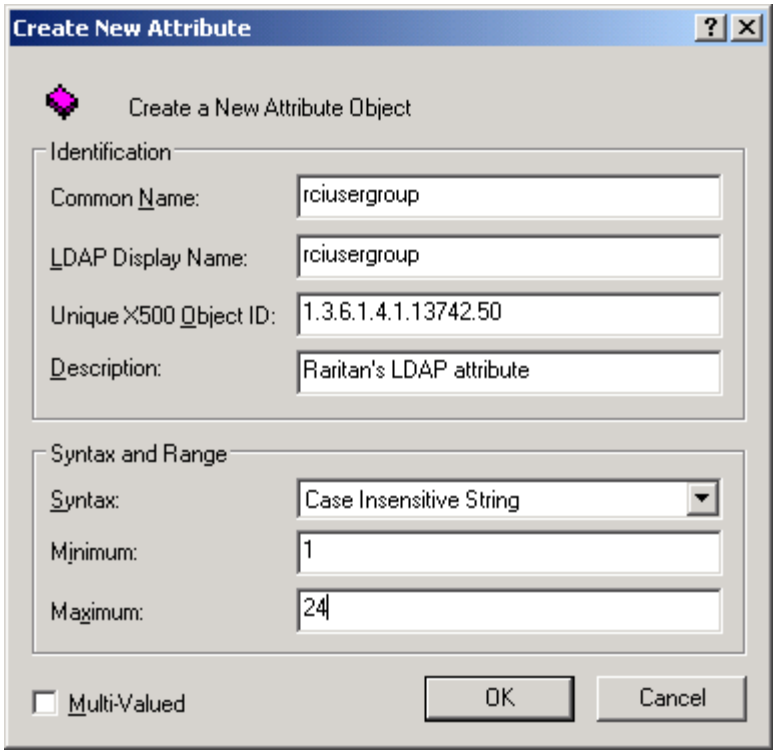
2. Cochez la case Le schéma peut être modifié sur ce contrôleur de domaine. **Facultatif**

3. Cliquez sur OK.

Création d'un attribut

Pour créer des attributs pour la classe rciusergroup :

1. Cliquez sur le symbole + en regard de Schéma Active Directory® dans le volet de gauche de la fenêtre.
2. Cliquez avec le bouton droit de la souris sur Attributs dans le volet de gauche.
3. Cliquez sur Nouveau, puis sélectionnez Attribut. Lorsque le message d'avertissement apparaît, cliquez sur Continuer ; la boîte de dialogue Créer un nouvel attribut s'affiche.



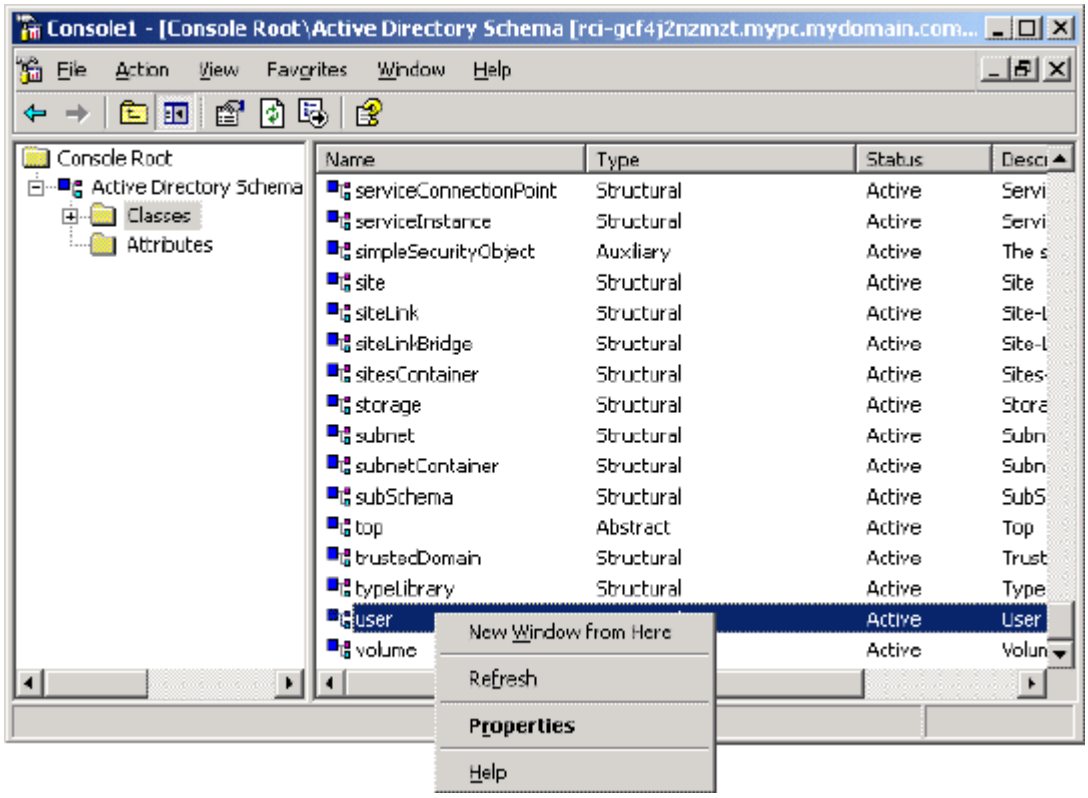
4. Tapez *rciusergroup* dans le champ Nom commun.
5. Tapez *rciusergroup* dans le champ Nom LDAP affiché.
6. Tapez *1.3.6.1.4.1.13742.50* dans le champ ID d'objet X.500 unique.
7. Entrez une description significative dans le champ Description.
8. Cliquez sur la flèche de la liste déroulante Syntaxe et sélectionnez Chaîne insensible à la casse dans la liste.
9. Tapez *1* dans le champ Minimum.
10. Tapez *24* dans le champ Maximum.

11. Cliquez sur OK pour créer l'attribut.

Ajout d'attributs à la classe

Pour ajouter des attributs à la classe :

1. Cliquez sur Classes dans le volet de gauche de la fenêtre.
2. Faites défiler le volet droit jusqu'à la classe user et cliquez dessus avec le bouton droit de la souris.



3. Sélectionnez Propriétés dans le menu. La fenêtre Propriétés de user s'affiche.
4. Cliquez sur l'onglet Attributs pour l'ouvrir.
5. Cliquez sur Add (Ajouter).

6. Sélectionnez rciusergroup dans la liste Sélectionnez l'objet Schéma.

7. Cliquez sur OK dans la boîte de dialogue Sélectionnez l'objet Schéma.
8. Cliquez sur OK dans la boîte de dialogue Propriétés de user.

Mise à jour du cache de schéma

Pour mettre à jour le cache du schéma :

1. Cliquez avec le bouton droit de la souris sur Schéma Active Directory® dans le volet de gauche de la fenêtre et sélectionnez Recharger le schéma.
2. Réduisez la console Active Directory Schema MMC (Microsoft® Management Console).

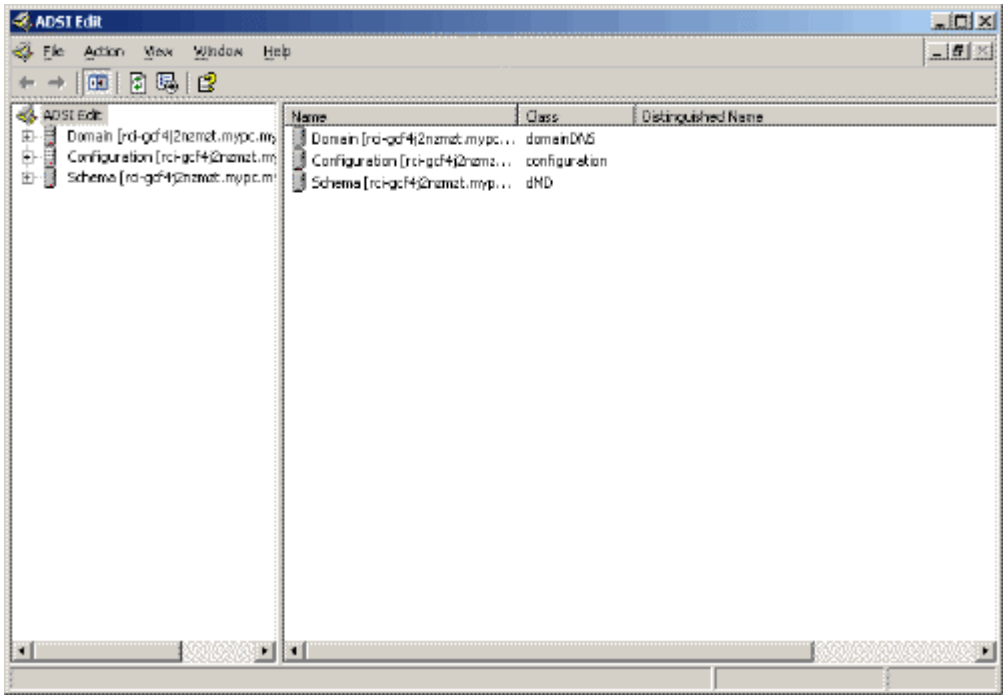
Modification des attributs rciusergroup pour les membres utilisateurs

Pour exécuter un script Active Directory® sur un serveur Windows 2003®, utilisez le script fourni par Microsoft® (disponible sur le CD d'installation de Windows Server 2003). 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 modifier les attributs d'un utilisateur individuel au sein du groupe rciusergroup, procédez comme suit :

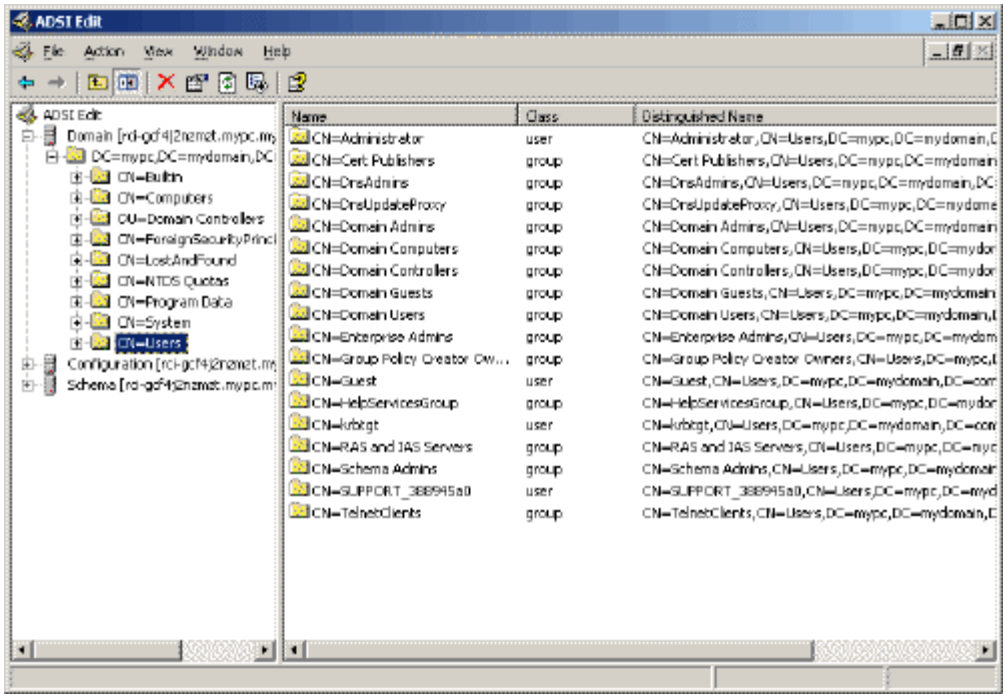
1. Sur le CD d'installation, sélectionnez Support > Tools (Outils).

2. Cliquez deux fois sur SUPTOOLS.MSI pour installer les outils de support.
3. Ouvrez le répertoire dans lequel les outils de support sont installés. Exécutez adsiedit.msc. La fenêtre Editeur ADSI s'ouvre.



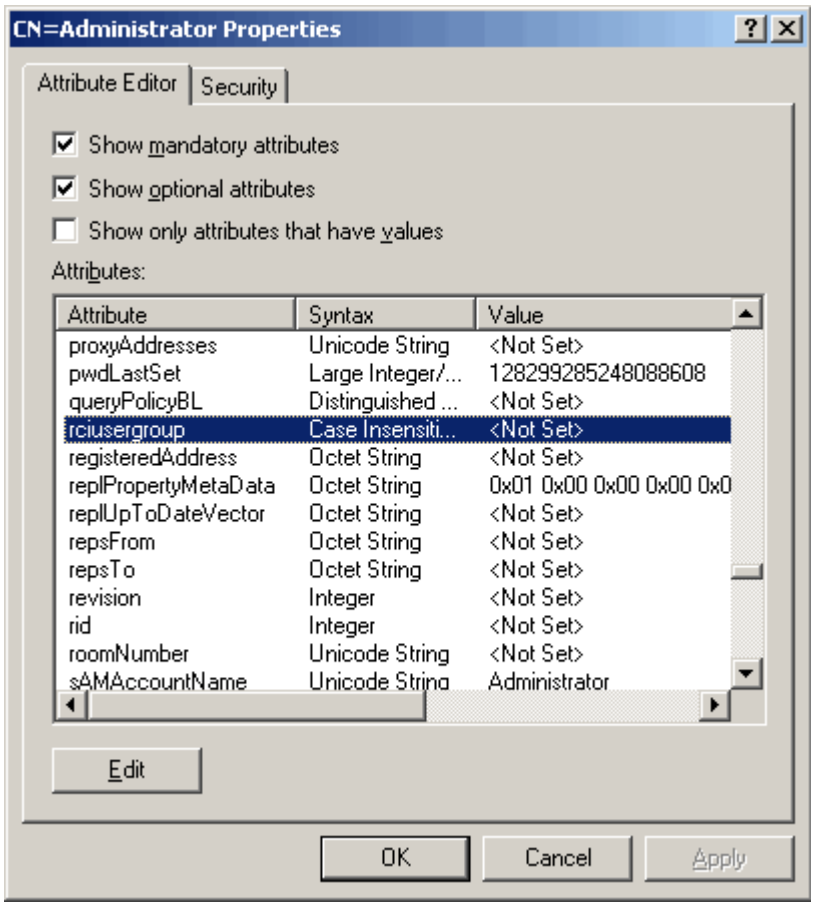
4. Ouvrez le domaine.

5. Dans le volet gauche de la fenêtre, sélectionnez le dossier CN=Users.

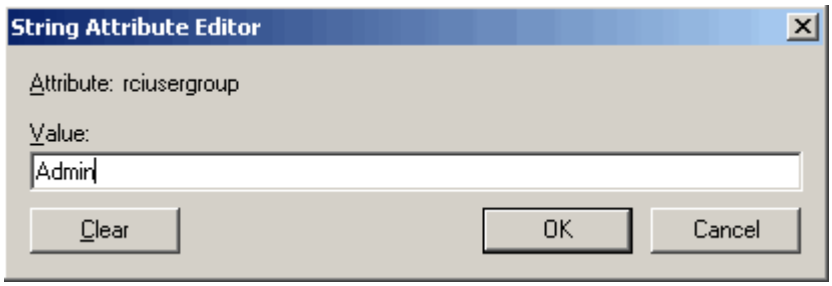


6. Recherchez le nom d'utilisateur dont vous souhaitez régler les propriétés dans le volet de droite. Cliquez avec le bouton droit sur le nom d'utilisateur et sélectionnez Propriétés.

7. Cliquez sur l'onglet Editeur d'attribut s'il n'est pas déjà ouvert. Sélectionnez rciusergroup dans la liste Attributs.



8. Cliquez sur Modifier. La boîte de dialogue Editeur d'attribut de chaîne apparaît.
9. Tapez le groupe d'utilisateurs (créé dans KX II) dans le champ Modifier l'attribut. Cliquez sur OK.



Annexe E Remarques d'informations

Dans ce chapitre

Présentation

Cette section comporte des remarques importantes sur l'utilisation de KX II. Les mises à jour à venir seront rapportées et disponibles en ligne via le lien d'aide de l'interface de la console distante de KX II.

Remarque : Certaines rubriques de cette section traitent de plusieurs autres dispositifs Raritan car divers dispositifs sont concernés par ces informations.

Java Runtime Environment (JRE)

Important : il est recommandé de désactiver la mise en mémoire cache de Java™ et d'effacer la mémoire cache de celui-ci. Reportez-vous à la documentation Java ou au manuel des clients d'accès KVM et série pour plus d'informations.

La console locale de LX, KX II, KX II-101 et KX II-101-V2 et MPC requièrent Java Runtime Environment™ (JRE™) pour fonctionner car la console distante vérifie la version Java. Si la version est incorrecte ou obsolète, vous êtes invité à télécharger une version compatible.

Raritan vous recommande d'utiliser la version 1.6 de JRE pour garantir des performances optimales. La console distante et MPC fonctionnent cependant avec la version 1.6.x ou supérieure de ce programme, à l'exception de la version 1.6.2.

Remarque : pour que les claviers multilingues fonctionnent dans la console distante de LX, KX II, KX II-101 et KX II-101-V2 (Virtual KVM Client), installez la version multilingue de JRE.

Remarques sur la prise en charge d'IPv6

Java

Java™ 1.6 prend en charge IPv6 pour :

- Solaris™ 10 (et supérieur)
- Linux® kernel 2.1.2 (et supérieur)/RedHat 6.1 (et supérieur)

Java 5.0 et supérieur prennent en charge IPv6 pour :

- Solaris 10 (et supérieur)
- Linux kernel 2.1.2 (et supérieur), kernel 2.4.0 (et supérieur) recommandés pour une meilleure prise en charge d'IPv6
- Systèmes d'exploitation Windows XP® SP1, Windows 2003® et Windows Vista®

Les configurations IPv6 suivantes *ne sont pas* prises en charge par Java :

- J2SE 1.4 ne prend pas en charge IPv6 sous Microsoft® Windows®.

Linux

- Linux kernel 2.4.0 ou supérieur est recommandé pour l'utilisation d'IPv6.
- Un noyau compatible IPv6 doit être installé ou le noyau doit être reconstruit avec les options IPv6 activées.
- Plusieurs utilitaires réseau doivent également être installés pour Linux si IPv6 est utilisé. Pour plus d'informations, reportez-vous à http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

Windows

- Les utilisateurs de Windows XP et Windows 2003 doivent installer le service pack Microsoft IPV6 pour activer IPV6.
- Pour AKC avec IPv6 sous Windows XP, ajoutez l'exécutable kxgui.exe à la liste d'exceptions du pare-feu. Affichez le fichier journal sur le client pour identifier le chemin d'accès complet au fichier kxgui.exe.

Mac Leopard

- IPv6 n'est pas pris en charge dans la version 2.0.20 de KX II pour Mac® Leopard®.

Samba

- IPv6 n'est pas pris en charge pour une utilisation avec les supports virtuels sous Samba.

Problèmes de performances de connexion en double pile

Si vous utilisez KX II dans une configuration en double pile, il est important de configurer le système de noms de domaine (DNS) correctement dans KX II afin d'éviter les retards lors de la connexion. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 231) pour plus d'informations sur la configuration de DNS dans KX II.

Remarques sur Mac

Touches de commandes BIOS sur Mac Mini

Les commandes BIOS suivantes ont été testées sur des serveurs cible MAC® Mini connectés à KX II avec des CIM D2CIM-DVUSB et D2CIM-VUSB.

Touches	Description	D2CIM-DVUSB (5A89)	D2CIM-VUSB (4A7F)
Appuyez sur D au démarrage.	Démarrage dans Apple Hardware Test (AHT)	Echoue	Echoue
Appuyez sur Option-Commande-P-R jusqu'à ce que vous entendiez le signal de démarrage une deuxième fois.	Réinitialisation de la NVRAM	Fonctionne	Fonctionne
Appuyez sur Option au démarrage.	Démarrage dans le Gestionnaire de démarrage, où vous pouvez sélectionner un volume Mac OS X pour le démarrage. Remarque : appuyez sur N pour faire apparaître le premier volume réseau amorçable également.	Echoue	Fonctionne
Appuyez sur Ejecter, F12, ou maintenez le bouton de la souris ou du pavé tactile.	Ejection de tout support amovible, un disque optique par exemple.	Fonctionne	Fonctionne
Appuyez sur N au démarrage.	Tentative de démarrage depuis un serveur réseau compatible (NetBoot).	Fonctionne	Fonctionne

Touches	Description	D2CIM-DVUSB (5A89)	D2CIM-VUSB (4A7F)
Appuyez sur T au démarrage.	Démarrage en mode disque cible.	Fonctionne	Fonctionne
Appuyez sur Maj au démarrage.	Démarrage en mode de démarrage sans échec et désactivation temporaire des éléments de connexion.	Echoue	Fonctionne
Appuyez sur Commande-V au démarrage.	Démarrage en mode Verbose (Détaillé).	Fonctionne	Fonctionne
Appuyez sur Commande-S au démarrage.	Démarrage en mode utilisateur unique.	Fonctionne	Fonctionne
Appuyez sur Option-N au démarrage.	Démarrage depuis un serveur NetBoot à l'aide de l'image amorçable par défaut.	Fonctionne	Fonctionne
Appuyez sur Commande-R au démarrage.	Démarrage depuis Lion Recovery1.		T

Lancement de MPC sur des clients Mac Lion

Si vous utilisez Mac® Lion sur votre client, Multi-Platform Client (MPC) Raritan ne peut pas être lancé. Contournez le problème comme suit afin de lancer MPC.

Supprimez JavaApplicationStub de l'installation et créez un lien depuis le processus JavaApplicationStub correct.

- rm /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub
- ln -s /System/Library/Frameworks/JavaVM.framework/Resources/MacOS/JavaApplicationStub /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub

Pour l'exécuter, utilisez :

- /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub

Claviers

Claviers non américains

Clavier français

Caret (clients Linux® uniquement)

Virtual KVM Client et Multi-Platform Client (MPC) ne traitent pas la combinaison de touches Alt Gr + 9 comme le caret (^) lorsqu'un clavier français est utilisé avec des clients Linux.

Pour obtenir le caret :

Sur un clavier français, appuyez sur la touche ^ (à droite de la touche P), puis immédiatement sur la barre d'espacement.

Ou, créez une macro constituée des commandes suivantes :

1. Appuyez sur la touche Alt Gr.
2. Appuyez sur la touche 9.
3. Relâchez la touche 9.
4. Relâchez la touche Alt Gr.

Remarque : ces procédures ne s'appliquent pas à l'accent circonflexe (au-dessus des voyelles). Dans tous les cas, la touche ^ (à droite de la touche P) fonctionne sur les claviers français pour créer l'accent circonflexe, lorsqu'elle est utilisée en combinaison avec un autre caractère.

Accent (clients Windows XP® seulement)

Depuis Virtual KVM Client et Multi-Platform Client, la combinaison de touches Alt Gr + 7 entraîne l'affichage en double du caractère accentué lors de l'utilisation d'un clavier français avec les clients Windows XP.

Remarque : ceci ne se produit pas avec les clients Linux.

Pavé numérique

Depuis Virtual KVM Client et Multi-Platform Client, les symboles du pavé numérique s'affichent comme suit lors de l'utilisation d'un clavier français :

Symbole du pavé numérique	Affiche
/	;

.	;

Tilde

Depuis Virtual KVM Client et Multi-Platform Client, la combinaison de touches Alt Gr + 2 ne produit pas le tilde (~) lors de l'utilisation d'un clavier français.

Pour obtenir le tilde :

Créez une macro constituée des commandes suivantes :

- Appuyez sur la touche Alt Gr.
- Appuyez sur la touche 2.
- Relâchez la touche 2.
- Relâchez la touche Alt Gr.

Préférence de la langue du clavier (clients Fedora Linux)

Etant donné que Sun™ JRE™ sous Linux® a des difficultés à générer les événements KeyEvents corrects pour les claviers dans d'autres langues configurés à l'aide des préférences système, Raritan recommande de configurer ces claviers à l'aide des méthodes décrites dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Anglais britannique	Paramètres système (centre de contrôle)
Français	Indicateur de clavier
Allemand	Indicateur de clavier
Hongrois	Paramètres système (centre de contrôle)
Espagnol	Paramètres système (centre de contrôle)
Allemand (Suisse)	Paramètres système (centre de contrôle)
Norvégien	Indicateur de clavier
Suédois	Indicateur de clavier
Danois	Indicateur de clavier
Japonais	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Italien	Paramètres système (centre de contrôle)

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Portugais	Paramètres système (centre de contrôle)

Remarque : l'indicateur de clavier doit être utilisé sur les systèmes Linux utilisant l'environnement de bureau Gnome.

Sur un clavier hongrois depuis un client Linux, les lettres U et O avec deux accents aigus ne fonctionnent qu'avec JRE 1.6.

Plusieurs méthodes permettent de définir les préférences de langue de clavier sur les clients Fedora® Linux. La méthode suivante est obligatoire pour le mappage correct des touches des Virtual KVM Client et Multi-Platform Client (MPC).

Pour définir la langue du clavier à l'aide des paramètres système :

1. Depuis la barre d'outils, choisissez Système > Préférences > Clavier.
2. Ouvrez l'onglet Agencements.
3. Ajoutez ou sélectionnez la langue appropriée.
4. Cliquez sur Fermer.

Pour définir la langue du clavier à l'aide de l'indicateur de clavier :

1. Cliquez avec le bouton droit sur la barre de tâches et choisissez Ajouter au tableau de bord.
2. Dans la boîte de dialogue Ajouter au tableau de bord, cliquez avec le bouton sur Indicateur de clavier, et dans le menu, choisissez Ouvrir les préférences clavier.
3. Dans la boîte de dialogue Préférences clavier, cliquez sur l'onglet Agencements.
4. Ajoutez et enlevez des langues selon les besoins.

Clavier Macintosh

Lorsqu'un Macintosh® est utilisé comme client, les touches suivantes du clavier ne sont pas capturées par Java™ Runtime Environment (JRE™) :

- F9
- F10
- F11
- F14
- F15
- Monter le volume
- Descendre le volume
- Muet
- Ejection

En conséquence, Virtual KVM Client et Multi-Platform Client (MPC) ne sont pas en mesure de traiter ces touches d'un clavier de client Mac.

Fedora

Résolution du focus de Fedora Core

Lors de l'utilisation de Multi-Platform Client (MPC), il est parfois impossible de se connecter à un dispositif LX, KX II ou KSX II, ou d'accéder aux serveurs cible KVM (Windows®, SUSE, etc.). En outre, la combinaison de touches Ctrl+Alt+M n'affiche peut-être pas le menu des raccourcis-clavier. Cette situation se produit avec la configuration client suivante : Fedora® Core 6 et Firefox® 1.5 ou 2.0.

Des tests ont permis de déterminer que l'installation de libXp résolvait les problèmes de focus de fenêtre avec Fedora Core 6. Raritan a effectué les tests avec libXp-1.0.0.8.i386.rpm ; tous les problèmes de focus de clavier et de menus contextuels.

Remarque : libXp est également requis pour permettre le fonctionnement du navigateur SeaMonkey (précédemment Mozilla®) avec le plug-in Java™.

Synchronisation des pointeurs de souris (Fedora)

Lors d'une connexion en mode souris double à un serveur cible exécutant Fedora® 7, si les pointeurs des souris cible et locale perdent leur synchronisation, faire passer le mode de souris de ou vers Intelligent ou Standard peut améliorer la synchronisation. Le mode de souris unique peut également fournir un meilleur contrôle.

Pour resynchroniser les curseurs de souris :

- Utiliser l'option Synchronize Mouse (Synchroniser la souris) de Virtual KVM Client.

Connexions par carte à puce VKC et MPC aux serveurs Fedora

Si vous utilisez une carte à puce pour vous connecter à un serveur Fedora® via MPC ou VKC, effectuez une mise à niveau de la bibliothèque pcsc-lite vers 1.4.102-3 ou supérieur.

Remarque : cette fonction est disponible uniquement sur KSX II 2.3.0 (et supérieur) et sur KX II 2.1.10 (et supérieur).

Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora

Si vous accédez à Firefox® et que vous utilisez un serveur Fedora®, Firefox risque de se bloquer à l'ouverture. Pour résoudre ce problème, installez le plug-in libnpjp2.so Java™ sur le serveur.

Modes et résolutions vidéo

Modes vidéo SUSE/VESA

L'outil de configuration SaX2 de SuSE X.org génère des modes vidéo à l'aide des entrées ModeLine du fichier de configuration X.org. Ces modes vidéo ne correspondent pas exactement au minutage du mode vidéo VESA (même si un écran VESA est sélectionné). KX II, en revanche, s'appuie sur le minutage du monde VESA exact pour une synchronisation parfaite. Cette disparité peut entraîner des bordures noires, des sections d'image absentes et des parasites.

Pour configurer l'affichage vidéo SUSE :

1. Le fichier de configuration généré /etc/X11/xorg.conf inclut une section Monitor comportant une option appelée UseModes. Par exemple,
   UseModes "Modes[0]"
2. Mettez cette ligne en commentaire (à l'aide de #) ou supprimez-la complètement.

3. Redémarrez le serveur X.

Grâce à cette modification, le minutage du mode vidéo interne du serveur X sera utilisé et correspondra exactement au minutage du mode vidéo VESA, entraînant un affichage vidéo correct sur KX II.

Résolutions vidéo prises en charge non affichées

Lorsque vous utilisez un CIM, certaines résolutions vidéo, indiquées dans ***Résolutions vidéo prises en charge*** (à la page 341), peuvent ne pas être disponibles à la sélection par défaut.

Pour afficher toutes les résolutions vidéo disponibles si elles n'apparaissent pas :

1. Branchez le moniteur.
2. Débranchez ensuite le moniteur et branchez le CIM. Toutes les résolutions vidéo sont à présent disponibles et peuvent être utilisées.

Audio

Problèmes en matière de lecture et de capture audio

Fonctions pouvant interrompre une connexion audio

Si vous utilisez une des fonctions ci-après lors de la connexion à un dispositif audio, votre connexion audio peut être interrompue. Raritan vous recommande de ne pas utiliser ces fonctions si vous êtes connecté à un dispositif audio :

- Détection automatique de la vidéo
- Utilisation extensive du port local
- Ajout d'utilisateurs

Problèmes lors de l'utilisation simultanée d'un dispositif de capture et d'un dispositif de lecture sur une cible

Sur certaines cibles, la connexion simultanée de dispositifs de capture et de lecture risque de ne pas fonctionner en raison du contrôleur de concentrateur USB et son mode de gestion des ports USB. Prévoyez de sélectionner un format audio nécessitant moins de bande passante.

Si ceci ne résout pas le problème, branchez le connecteur de clavier et souris du CIM D2CIM-DVUSB sur un port différent de la cible. Si ceci ne résout pas le problème, branchez le dispositif sur un concentrateur USB et connectez ce dernier à la cible.

Audio dans un environnement Linux

Vous trouverez ci-après les problèmes répertoriés lors de l'utilisation de la fonction audio dans un environnement Linux®.

- Utilisateurs Linux® : utilisez le dispositif audio par défaut pour la lecture. Le son risque de ne pas passer si une carte son autre que celle par défaut est sélectionnée.
- Les clients SuSE 11 requièrent l'installation de Javas_1_6_0-sun-alsa (prise en charge ALSA pour java-1_6_0-sun) via YAST.
- Pour les casques Logitech avec micro incorporé, seule l'option Mono Capture est disponible.
- Si vous exécutez SUSE 11 et utilisez un pilote ALSA, déconnectez-vous de KX II, puis reconnectez-vous pour afficher le dispositif. En outre, si vous connectez et déconnectez le dispositif audio plusieurs fois, il risque d'être répertorié plusieurs fois, au lieu d'une comme il devrait l'être.
- L'utilisation de la fonction audio avec une cible Fedora Core 13 paramétrée sur mono 16 bits, 44k peut entraîner des interférences importantes pendant la lecture.

Audio dans un environnement Mac

Vous trouverez ci-dessous les problèmes répertoriés dans un environnement Mac®.

- Sur les clients Mac, un seul dispositif de lecture apparaît sur le panneau Connect Audio lors de l'accès au dispositif via Virtual KVM Client (VKC) et Multi-Platform Client (MPC). Il s'agit du dispositif par défaut et il est affiché sur le panneau Connect Audio sous Java Sound Audio Engine (Moteur audio).
- Le son utilisé sur une cible Mac via Skype® risque d'être altéré.

Audio dans un environnement Windows

Sur les clients Windows® 64 bits, un seul dispositif de lecture apparaît sur le panneau Connect Audio lors de l'accès au dispositif via Virtual KVM Client (VKC) et Multi-Platform Client (MPC). Il s'agit du dispositif audio par défaut et il est affiché sur le panneau Connect Audio sous Java Sound Audio Engine (Moteur audio).

Ports et profils USB

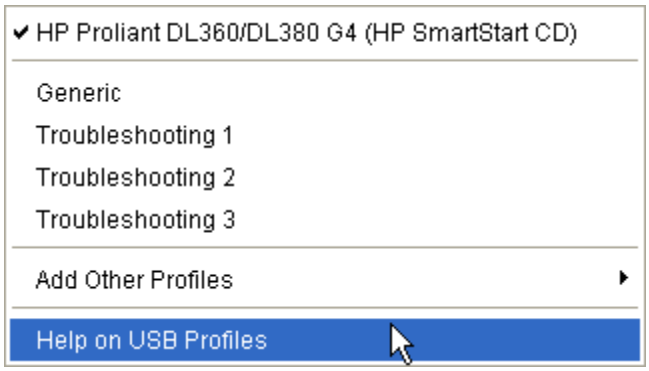
Ports USB VM-CIM et DL360

Les serveurs HP® DL360 sont dotés d'un port USB à l'arrière et d'un autre à l'avant. Avec DL360, les deux ports ne peuvent pas être utilisés simultanément. Aussi, un VM-CIM double ne peut pas être utilisé sur les serveurs DL360.

Toutefois, pour contourner ce problème, un concentrateur USB2 peut être connecté au port USB à l'arrière du dispositif et un VM-CIM double peut être connecté au concentrateur.

Aide pour la sélection des profils USB

Lorsque vous êtes connecté à un serveur cible KVM via Virtual KVM Client (VKC), vous pouvez afficher des informations relatives aux profils USB via l'aide sur la commande USB Profiles (Profils USB) du menu USB Profile (Profil USB).



L'aide relative aux profils USB apparaît dans la fenêtre USB Profile Help. Pour plus d'informations sur des profils USB spécifiques, reportez-vous à ***Profils USB disponibles*** (à la page 139).

Raritan propose une sélection standard de profils de configuration USB pour des implémentations de serveurs sur une grande variété de systèmes d'exploitation et de niveaux de BIOS. Ces profils sont conçus pour offrir une adéquation optimale entre les configurations des dispositifs USB distants et des serveurs cible.

Le profil Generic (Générique) répond aux besoins des configurations de serveurs cible déployées les plus fréquentes.

Des profils supplémentaires sont disponibles pour répondre aux besoins spécifiques d'autres configurations de serveurs déployées courantes (par exemple, Linux®, Mac OS X®).

Un certain nombre de profils (désignés par nom de plate-forme et révision de BIOS) ont également été adaptés pour améliorer la compatibilité de la fonction Support virtuel avec le serveur cible ; par exemple, lors d'un fonctionnement au niveau du BIOS.

L'option Add Other Profiles (Ajouter d'autres profils) permet d'accéder aux autres profils disponibles sur le système. Les profils sélectionnés dans cette liste sont ajoutés au menu USB Profile (Profil USB). Sont inclus des profils de dépannage (Troubleshooting) conçus pour identifier les limites des configurations.

Les options du menu USB Profile sont configurables via la page Console Device Settings > Port Configuration (Paramètres du dispositif de console > Configuration des ports).

Si les profils USB standard fournis par Raritan ne répondent pas aux conditions requises de votre serveur cible, l'assistance technique Raritan peut vous aider à trouver une solution adaptée à cette cible. Raritan vous recommande d'effectuer les opérations suivantes :

1. Consultez les notes de publication les plus récentes sur le site Web de Raritan (www.raritan.com) sur la page des mises à jour de firmware pour vérifier s'il n'existe pas de solution pour votre configuration.
2. Dans le cas contraire, fournissez les informations lorsque vous contactez l'assistance technique Raritan :
    a. Informations sur le serveur cible : fabricant, modèle, BIOS, fabricant et version.
    b. Usage envisagé (par exemple, redirection d'une image pour recharger le système d'exploitation d'un serveur depuis le CD).

Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce

Dans certains cas, vous serez amené à modifier le profil USB d'un serveur cible. Vous aurez par exemple à remplacer la vitesse de connexion par Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du support virtuel) lorsque la cible rencontre des difficultés avec la vitesse de connexion High Speed USB (USB à haut débit).

A la modification d'un profil, vous recevrez, le cas échéant, un message Nouveau matériel détecté et devrez vous connecter à la cible avec des droits d'administrateur afin de réinstaller le pilote USB. Ceci ne se produira probablement que les premières fois où la cible détectera les nouveaux paramètres du périphérique USB. Elle sélectionnera correctement le pilote par la suite.

Remarque : cette fonction est disponible sur KX II 2.4.0 (et supérieur).

Support virtuel

Utilisation du support virtuel via VKC et AKC dans un environnement Windows

Les droits Administrateur et utilisateur standard dans le système d'exploitation Windows XP® varient de ceux des systèmes d'exploitation Windows Vista® et Windows 7®.

Lorsqu'elle est activée dans Vista ou dans Windows 7, la fonction Contrôle d'accès d'utilisateur fournit le niveau de droits le plus bas dont un utilisateur a besoin pour une application. Par exemple, l'option Exécuter en tant qu'administrateur est fournie dans Internet Explorer® pour autoriser explicitement les utilisateurs à effectuer des tâches de niveau Administrateur, sinon celles-ci ne sont pas accessibles même si l'utilisateur dispose d'une connexion administrateur.

Ces deux fonctions affectent le type de supports virtuels accessibles aux utilisateurs via Virtual KVM Client (VKC) et Active KVM Client (AKC). Consultez l'aide Microsoft® pour en savoir plus sur ces fonctions et comment les utiliser.

La liste suivante répertorie des types de supports virtuels accessibles via VKC et AKC dans un environnement Windows. Ces fonctions sont classées par client, puis par rôle utilisateur Windows.

Windows XP

Si vous utilisez VKC et AKC dans un environnement Windows XP, les utilisateurs doivent disposer de droits Administrateur pour accéder à n'importe quel type de support virtuel autre que les connexions CD-ROM, les ISO et les images ISO.

Windows Vista et Windows 7

Si vous utilisez VKC et AKC dans un environnement Windows Vista ou Windows 7 et que la fonction Contrôle d'accès d'utilisateur est activée, les types de supports virtuels suivants sont accessibles suivant le rôle Windows de l'utilisateur :

Client	Administrateur	Utilisateur standard

Client	Administrateur	Utilisateur standard
AKC et VKC	Accès : • Lecteurs fixes et partitions de lecteurs fixes • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes	Accès : • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes

Support virtuel non rafraîchi après l'ajout de fichiers

Après le montage d'un lecteur de support virtuel, si vous ajoutez des fichiers à ce lecteur, ces fichiers peuvent ne pas apparaître immédiatement sur le serveur cible. Supprimez, puis rétablissez la connexion de support virtuel.

Partitions système actives

Vous ne pouvez pas monter de partitions système actives à partir d'un client Mac ou Linux.

Les partitions de lecteur Ext3/4 Linux doivent être démontées à l'aide de umount /dev/<libellé de dispositif> avant d'établir une connexion au support virtuel.

Partitions de lecteur

Les limites en matière de partition de lecteur suivantes existent à travers les systèmes d'exploitation :

- Les cibles Windows et Mac ne peuvent pas lire les partitions formatées Linux.
- Windows® et Linux® ne peuvent pas lire les partitions formatées Mac.
- Seules les partitions FAT Windows sont prises en charge par Linux.
- FAT et NTFS Windows sont pris en charge par Mac.
- Les utilisateurs Mac doivent démonter les dispositifs déjà montés pour se connecter à un serveur cible. Utilisez >diskutil umount /dev/disk1s1 pour démonter le dispositif et diskutil mount /dev/disk1s1 pour le remonter.

Lecteur virtuel Linux répertorié deux fois

Pour les utilisateurs de KX II 2.4.0 (et supérieur) et de LX 2.4.5 (et supérieur) connectés aux clients Linux™ en tant qu'utilisateurs racine, les lecteurs sont répertoriés deux fois dans la liste déroulante Local Drive (Lecteur local). Vous verrez par exemple eg /dev/sdc et eg /dev/sdc1 où le premier lecteur est le secteur d'amorçage et le second, la première partition du disque.

Lecteurs mappés verrouillés Mac et Linux

Les lecteurs mappés à partir des clients Mac® et Linux® ne sont pas verrouillés lorsqu'ils sont montés sur des cibles connectées. Ceci ne concerne que KX II 2.4.0 et (supérieur) et LX 2.4.5 (et supérieur) qui offrent une prise en charge de Mac et de Linux.

Accès au support virtuel sur un serveur Windows 2000 utilisant un D2CIM-VUSB

Un lecteur local de support virtuel n'est pas accessible sur un serveur Windows 2000® utilisant un D2CIM-VUSB.

Durée d'amorçage du BIOS cible avec les supports virtuels

L'amorçage du BIOS de certaines cibles peut durer plus longtemps sur le support est monté virtuellement à la cible.

Pour raccourcir la durée d'amorçage :

1. Fermez Virtual KVM Client pour libérer complètement les lecteurs de supports virtuels.
2. Redémarrez la cible.

Echec de connexion des supports virtuels lors de l'utilisation du haut débit

Dans certains cas, il peut être nécessaire de sélectionner l'option Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du support virtuel) lorsque la cible rencontre des difficultés avec la vitesse de connexion High Speed USB (USB à haut débit) ou qu'elle connaît des erreurs de protocole USB en raison d'une dégradation du signal due à la présence de connecteurs et de câbles supplémentaires. (par exemple, une connexion à un serveur lame via une clé électronique).

CIM

Souris à 3 boutons Windows sur les cibles Linux

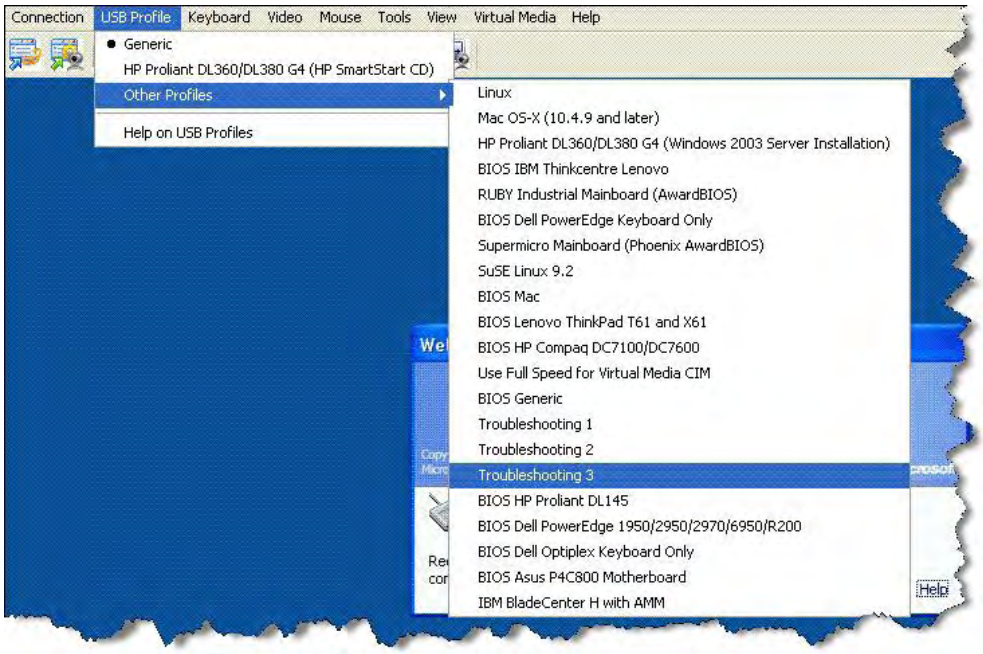
Lorsque vous utilisez une souris à 3 boutons sur un client Windows® connecté à une cible Linux®, le bouton gauche peut être mappé sur le bouton central de la souris à 3 boutons du client Windows.

Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel

Le système d'exploitation Windows 2000® ne prend pas en charge les dispositifs USB composites, comme D2CIM-VUSB de Raritan, de la même façon que les dispositifs USB non composites.

En conséquence, l'icône de la barre d'état Supprimer le périphérique en toute sécurité n'apparaît pas pour les lecteurs mappés par D2CIM-VUSB et un message d'avertissement peut s'afficher lors de la déconnexion du dispositif. Raritan n'a toutefois constaté aucun problème à la suite de ce message.

Le service technique de Raritan aux Etats-Unis a mis au point une configuration prenant en charge l'icône Supprimer le périphérique en toute sécurité et évitant ce message Windows. Cette configuration requiert l'utilisation de l'adaptateur de supports virtuels D2CIM-DVUSB et le profil USB Troubleshooting 3, qui configure D2CIM-DVUSB en tant que dispositif USB non composite prenant en charge une connexion de supports virtuels unique. Raritan a testé cette configuration avec succès aux Etats-Unis et au Japon.



CC-SG

Version de Virtual KVM Client non reconnue par le mode proxy CC-SG

Lorsque Virtual KVM Client est démarré depuis CommandCenter Secure Gateway (CC-SG) en mode proxy, la version de Virtual KVM Client est inconnue. Dans la boîte de dialogue About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan), la version est indiquée comme inconnue.

Mode souris simple - Connexion à une cible contrôlée par CC-SG via VKC utilisant Firefox

Si vous utilisez Firefox® pour vous connecter à une cible KX II ou KSX II contrôlée par CC-SG à l'aide de DCIM-PS2 ou DCIM-USBG2, et que vous passez au mode souris simple dans Virtual KVM Client, le focus ne sera plus sur la fenêtre VKC et la souris ne répondra pas. Dans ce cas, cliquez ou appuyez sur Alt+Tab pour rétablir le focus sur la fenêtre VKC.

Mode proxy et MPC

Si vous utilisez KX II dans une configuration CC-SG, ne vous servez pas du mode proxy CC-SG si vous avez l'intention d'utiliser Multi-Platform Client (MPC).

Déplacement entre ports sur un dispositif

Si vous effectuez un déplacement entre ports du même dispositif Raritan et reprenez la gestion au bout d'une minute, CC-SG peut afficher un message d'erreur. Si vous reprenez la gestion, l'affichage est mis à jour.

Annexe F Foire aux questions

Dans ce chapitre

Foire aux questions générale

Question	Réponse
Qu'est-ce que Dominion KX II ?	Dominion KX II est un commutateur KVM (clavier, vidéo, souris) numérique de la seconde génération qui permet à un, deux, quatre ou huit administrateurs informatiques d'accéder à et de gérer 8, 16, 32 ou 64 serveurs sur le réseau grâce à des fonctionnalités 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. 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 depuis n'importe quel poste de travail mis en réseau, ainsi que depuis un iPhone® et un iPad®.

Question	Réponse
En quoi Dominion KX II diffère-t-il d'un logiciel de contrôle à distance ?	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 : Ne dépend ni du système d'exploitation ni du matériel - Dominion KX II peut être utilisé pour gérer des serveurs exécutant de nombreux systèmes d'exploitation courants, notamment Intel®, Sun®, PowerPC exécutant Windows, Linux®, Solaris™, etc. Ne dépend pas de l'état ou d'un serveur sans agent – Dominion KX II n'a pas besoin que le système d'exploitation du serveur géré soit activé, 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.
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 ne mesure que 1U de hauteur (à l'exception de KX2-864 et KX2-464 qui mesurent 2U), s'adapte dans un rack standard de 19 pouces et ne mesure que 29 cm de profondeur. Dominion KX2-832 et KX2-864 mesurent 36 cm de profondeur.

Accès à distance

Question	Réponse
Combien d'utilisateurs peuvent accéder à distance aux serveurs sur chaque Dominion KX II ?	Les modèles Dominion KX II permettent la connexion distante de huit utilisateurs au maximum par canal d'utilisateur 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, huit utilisateurs distants au maximum peuvent utiliser et gérer le serveur sur le canal un et huit autres utilisateurs au maximum sur le canal deux. En ce qui concerne les dispositifs à quatre canaux, huit utilisateurs au maximum par canal, pour un total de 32 (8 x 4) utilisateurs, peuvent accéder à quatre serveurs et les gérer. De même, pour les dispositifs à huit canaux, huit utilisateurs au maximum peuvent accéder à un seul serveur, jusqu'à un total maximum de 32 utilisateurs sur huit canaux.
Puis-je accéder à distance aux serveurs depuis mon iPhone ou iPad ?	Oui. Depuis les versions 2.4 de Dominion KX II et 5.2 de CC-SG, les utilisateurs peuvent accéder aux serveurs connectés à KX II à l'aide de leur iPhone ou iPad.
Deux utilisateurs peuvent-ils visualiser le même serveur simultanément ?	Oui. En fait, huit personnes au maximum 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 » à distance. Le port local peut accéder au même serveur grâce à la fonctionnalité PC-Share.

<table>
<tr><th>Question</th><th>Réponse</th></tr>
<tr><td>Quels sont les matériel, logiciel ou configuration réseau nécessaires pour accéder à Dominion KX II à partir d'un ordinateur client ?</td><td>Dominion KX II étant entièrement accessible par le Web, il ne requiert l'installation d'aucun logiciel spécifique sur les clients utilisés pour y accéder. (Un client installé facultatif est disponible sur Raritan.com. Il est obligatoire pour l'accès par modem externe.)

Il est possible d'accéder à Dominion KX II par le biais des principaux navigateurs Web : Internet Explorer® et Firefox®. Dominion KX II est accessible sur les ordinateurs Windows, Linux et Macintosh® par l'intermédiaire du client Windows de Raritan et des clients Multiplatform et Virtual KVM™ Java™.

Les administrateurs Dominion KX II peuvent également effectuer une gestion à distance (définir des mots de passe et la sécurité, renommer des serveurs, modifier des adresses IP, etc.) grâce à une interface navigateur pratique.</td></tr>
<tr><td>Quelle est la taille du fichier de l'applet utilisée pour accéder à Dominion KX II ? Combien de temps faut-il pour l'extraire ?</td><td>La taille de l'applet Virtual KVM Client (VKC) utilisée 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 :

<table>
<tr><td>100 Mbps</td><td>Vitesse réseau théorique
100 mégabits</td><td>0,05 seconde</td></tr>
<tr><td>60 Mbps</td><td>Vitesse réseau pratique probable
100 mégabits</td><td>0,08 seconde</td></tr>
<tr><td>10 Mbps</td><td>Vitesse réseau théorique
10 mégabits</td><td>0,4 seconde</td></tr>
<tr><td>6 Mbps</td><td>Vitesse réseau pratique probable
10 mégabits</td><td>0,8 seconde</td></tr>
<tr><td>512 Kbps</td><td>Vitesse de téléchargement (type) d'un modem câblé</td><td>8 seconde</td></tr>
</table>
</td></tr>
</table>

Question	Réponse
Comment puis-je accéder aux serveurs connectés à Dominion KX II en cas d'indisponibilité du réseau ?	Vous pouvez accéder aux serveurs sur rack ou par modem. Dominion KX II offre un port de modem dédié pour connecter un modem externe.
Disposez-vous d'un client KVM Windows ?	Oui. Nous avons un client Windows .NET natif appelé Active KVM Client (AKC) de Raritan.
Disposez-vous d'un client KVM non-Windows ?	Oui. Virtual KVM Client (VKC) et Multiplatform Client (MPC) permettent aux utilisateurs non-Windows de se connecter à des serveurs cible dans le centre de données. MPC peut être exécuté via des navigateurs Web et en mode autonome, et peut accéder à des serveurs connectés aux commutateurs Dominion KX I et KX II. Reportez-vous aux manuels d'utilisation de Dominion KX II et de KVM Client de Raritan pour plus d'informations.
Vos clients KVM offrent-ils une prise en charge multilingue ?	Oui. L'interface utilisateur HTML de Dominion KX II et les clients KVM prennent en charge le japonais, le chinois simplifié et le chinois traditionnel. Ceci est disponible en mode autonome et via CC-SG.
Vos clients KVM prennent-ils en charge les écrans LCD doubles ?	Oui. Pour les clients qui souhaitent améliorer leur productivité en utilisant plusieurs écrans LCD sur leur bureau, Dominion KX II peut lancer des sessions KVM sur plusieurs écrans, en modes plein écran ou standard.
Prenez-vous en charge les serveurs dotés de cartes vidéo doubles ?	Oui, depuis la version 2.5, les serveurs dotés de cartes vidéo doubles sont pris en charge via une configuration bureau étendu disponible à l'utilisateur distant.

Support virtuel universel

Question	Réponse
Quels sont les modèles Dominion KX II qui prennent en charge les supports virtuels ?	Tous les modèles Dominion KX II prennent en charge les médias virtuels. Ils sont disponibles en mode autonome et via CommandCenter® Secure Gateway, la console de gestion centralisée de Raritan.

Question	Réponse
Quels types de supports virtuels Dominion KX II prend-il en charge ?	Dominion KX II prend en charge les types de supports suivants : lecteurs CD/DVD internes et connectés USB, dispositifs de stockage de masse USB, lecteurs de disque dur PC et images ISO.
Quelles sont les conditions requises pour l'utilisation du support virtuel ?	Un CIM de support virtuel Dominion KX II est requis : un CIM virtuel, D2CIM-VUSB ou D2CIM-DVUSB. D2CIM-VUSB est doté d'un connecteur USB simple et est destiné aux clients souhaitant utiliser le support virtuel au niveau du système d'exploitation. D2CIM-DVUSB est doté de connecteurs USB double et est destiné aux clients souhaitant utiliser le support virtuel au niveau du BIOS. D2CIM-DVUSB est également requis pour l'authentification par carte à puce, la mise en niveau/en cascade et l'audionumérique. Ces deux CIM prennent en charge des sessions de support virtuel sur les serveurs cible supportant l'interface USB 2.0. Disponibles en coffrets économiques de 32 et 64 CIM, ces CIM prennent en charge la synchronisation absolue de la souris Absolute Mouse Synchronization™, ainsi que la mise à jour du firmware à distance. A l'origine, nos CIM prenaient en charge la vidéo VGA analogique. Trois nouveaux CIM de support virtuel double prennent en charge les formats vidéo numérique, notamment DVI, HDMI et DisplayPort. Il s'agit de D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI et D2CIM-DVUSB-DP.
Le support virtuel est-il fiable ?	Oui. Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement 256 bits, 128 bits AES ou 128 bits RC4.

Question	Réponse
Les supports virtuels prennent-ils réellement en charge la fonction audio ?	Oui. La lecture et l'enregistrement audio sur un serveur connecté à Dominion KX II sont pris en charge. Vous pouvez écouter les sons provenant d'un serveur distant du centre de données à l'aide des haut-parleurs branchés sur votre PC ou ordinateur portable. Vous pouvez également effectuer des enregistrements sur le serveur distant à l'aide d'un microphone branché sur votre PC ou ordinateur portable. Un CIM numéro ou le CIM de support virtuel double D2CIM-DVUSB est requis.
Qu'est-ce qu'un profil USB ?	Certains serveurs requièrent une interface USB configurée de manière spécifique pour les services USB, tels que les supports virtuels. Le profil USB adapte l'interface USB de KX II au serveur pour prendre en compte les caractéristiques spécifiques de ce dernier.
En quoi un profil USB peut-il m'être utile ?	Les profils USB sont le plus souvent exigés au niveau du BIOS, où la spécification USB n'est peut-être pas totalement prise en charge lors de l'accès aux lecteurs de support virtuel. Toutefois, les profils sont parfois utilisés au niveau du système d'exploitation, par exemple, pour la synchronisation de la souris des serveurs Macintosh et Linux.
Comment un profil USB est-il utilisé ?	Les ports peuvent être configurés individuellement ou par groupe par l'administrateur pour utiliser un profil USB spécifique sur la page de configuration des ports de KX II. Un profil USB peut également être sélectionné dans le client KX II en cas de besoin. Pour plus d'informations, consultez le manuel d'utilisation.
Dois-je systématiquement définir un profil USB si j'utilise la fonction Support virtuel ?	Non. Dans de nombreux cas, le profil USB par défaut est suffisant pour l'utilisation de la fonction Support virtuel au niveau du système d'exploitation, ou pour le fonctionnement au niveau du BIOS sans accès aux supports virtuels.

Question	Réponse
Quels profils sont disponibles ? Où puis-je trouver des informations supplémentaires ?	Reportez-vous au manuel d'utilisation pour obtenir les profils disponibles et pour plus d'informations.

Bande passante et performance KVM-sur-IP

Question	Réponse
Comment la bande passante est-elle utilisée dans les systèmes KVM sur IP ?	Dominion KX II offre la technologie KVM sur 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. Dominion KX II numérise, compresse et chiffre les signaux du clavier, de l'écran et de la souris provenant du serveur cible et transmet des paquets IP via le réseau IP au client distant afin de créer une session distante pour l'utilisateur. KX II offre une expérience sur le rack basée sur ses algorithmes de traitement vidéo de pointe. Les changements d'écran, notamment vidéo, représentent la majorité de la bande passante utilisée ; l'activité du clavier et de la souris est considérablement inférieure. Il est important de noter que la bande passante n'est employée que lorsque l'utilisateur est actif. La quantité de bande passante utilisée est basée sur le volume de changements se produisant à l'écran vidéo du serveur. En l'absence de changement à l'écran vidéo, l'utilisateur n'interagit pas avec le serveur, la bande passante n'est pas utilisée. Si l'utilisateur déplace la souris ou tape un caractère, la quantité de bande passante utilisée est réduite. Si l'affichage exécute un écran de veille complexe ou lit une vidéo, la bande passante utilisée peut être plus conséquente.

Question	Réponse
Comment la bande passante affecte-t-elle les performances KVM sur IP ?	En général, il existe un compromis entre bande passante et performances. Plus la bande passante disponible est importante, plus les performances sont bonnes. Dans les environnements à bande passante réduite, les performances peuvent se dégrader. Dominion KX II a été optimisé pour fournir des performances solides dans une grande variété d'environnements.
Quels facteurs affectent la bande passante ?	De nombreux facteurs déterminent la quantité de bande passante utilisée. Le facteur principal, comme indiqué précédemment, est la quantité de changements se produisant dans l'affichage vidéo du serveur cible. Il dépend des tâches et actions de l'utilisateur. Parmi les autres facteurs figurent la résolution vidéo du serveur, la vitesse et les caractéristiques du réseau, les ressources du client PC et le bruit de la carte vidéo. Dominion KX II dispose d'algorithmes de traitement vidéo très élaborés qui optimisent la bande passante et les performances pour des environnements divers. En outre, ils sont hautement configurables; de nombreux paramètres permettent d'optimiser l'usage de la bande passante. Le paramètre de vitesse de connexion des clients distants (VKC, MPC) en particulier peut être défini pour réduire la bande passante utilisée. Contrairement à KX I, le paramètre Noise Filter (Filtre antiparasite) ne joue généralement pas un rôle important dans la réduction de la bande passante ou l'amélioration des performances de Dominion KX II.

<table>
<tr><th>Question</th><th>Réponse</th></tr>
<tr><td>Quelle est la quantité de bande passante utilisée par KX II pour les tâches courantes ?</td><td>La bande passante dépend principalement des tâches et actions de l'utilisateur. Plus l'écran vidéo du serveur change, plus le débit de bande passante utilisée est important.

Le tableau ci-dessous résume des cas d'utilisation standard avec les valeurs par défaut de Dominion KX II et deux paramètres de bande passante réduite (paramètre de vitesse de connexion d'1 Mo avec couleur 15 et 8 bits) sur un serveur cible Windows XP (résolution de 1024 x 768) sur un réseau local de 100 Mbits/s :
<table>
<tr><th>Tâche utilisateur</th><th>Valeur par défaut</th><th>Vitesse d'1Mb et couleurs 15 bits</th><th>Vitesse d'1Mb et couleurs 8 bits</th></tr>
<tr><td>Bureau de Windows inactif</td><td>0 Ko/s</td><td>0 Ko/s</td><td>0 Ko/s</td></tr>
<tr><td>Déplacement du curseur de la souris</td><td>5 à 15 Ko/s</td><td>2 à 6 Ko/s</td><td>2 à 3 Ko/s</td></tr>
<tr><td>Glissement d'icône</td><td>40 à 70 Ko/s</td><td>10 à 25 Ko/s</td><td>5 à 15 Ko/s</td></tr>
<tr><td>Glissement de dossier</td><td>10 à 40 Ko/s</td><td>5 à 20 Ko/s</td><td>5 à 10 Ko/s</td></tr>
<tr><td>Ouverture d'une fenêtre de texte</td><td>50 à 100 Ko/s</td><td>25 à 50 Ko/s</td><td>10 à 15 Ko/s</td></tr>
<tr><td>Frappe en continu</td><td>1 Ko/s</td><td>0,5 à 1 Ko/s</td><td>0,2 à 0,5 Ko/s</td></tr>
<tr><td>Défilement d'une fenêtre de texte</td><td>1050 Ko/s</td><td>5 à 25 Ko/s</td><td>2 à 10 Ko/s</td></tr>
<tr><td>Fermeture d'une fenêtre de texte</td><td>50 à 100 Ko/s</td><td>20 à 40 Ko/s</td><td>10 à 15 Ko/s</td></tr>
<tr><td>Ouverture d'un panneau</td><td>50 à 100 Ko/s</td><td>60 à 70 Ko/s</td><td>20 à 30 Ko/s</td></tr>
<tr><td>Changement d'onglet</td><td>40 à 50 Ko/s</td><td>20 à 50 Ko/s</td><td>10 à 20 Ko/s</td></tr>
</table>
</td></tr>
</table>

Question	Réponse
Comment puis-je réduire la bande passante ?	KX II offre divers paramètres dans vos clients distants pour permettre à l'utilisateur d'optimiser la bande passante et les performances. Les paramètres par défaut fournissent un niveau de performances sur le rack dans les environnements de réseau local/étendu avec une utilisation économique de la bande passante. Les paramètres de gestion de la bande passante incluent la vitesse de connexion et le nombre de couleurs. Pour réduire la bande passante : Vitesse de connexion. La réduction de la vitesse de connexion peut considérablement diminuer la bande passante utilisée. Dans les environnements de réseau local/étendu, la définition de la vitesse de connexion sur 1,5 ou 1 Mb par seconde réduit la bande passante en maintenant des performances correctes. Les paramètres au-dessous réduiront davantage la bande passante et conviennent aux connexions par bande passante à faible débit. Nombre de couleurs. La réduction du nombre de couleurs diminue la bande passante et augmente les performances considérablement. Toutefois, étant donné qu'un nombre inférieur de couleurs est utilisé, la vidéo s'en trouve dégradée. Ceci peut être acceptable pour certaines tâches d'administration système. Pour les connexions Internet lentes, l'utilisation de la couleur 8 bits ou d'un nombre inférieur de bits peut réduire la bande passante et améliorer les performances. Autres astuces pour réduire la bande passante : Utilisez un papier peint uni pour le Bureau au lieu d'une image complexe. Désactivez les écrans de veille. Utilisez une résolution plus basse sur le serveur cible. Désactivez l'option Afficher le contenu des fenêtres pendant leur déplacement dans Windows. Utilisez des images, thèmes et bureaux simples (par exemple, Windows

Question	Réponse
Que dois-je faire sur les connexions par bande passante à faible débit ?	Les paramètres de vitesse de connexion et de nombre de couleurs peuvent être peaufinés pour optimiser les performances des connexions par bande passante à faible débit. Par exemple, dans Multiplatform Client ou Virtual KVM Client, définissez la vitesse de connexion sur 1,5 Mb ou 1 Mb, et le nombre de couleurs sur 8 bits. Des paramètres de vitesse de connexion et de nombre de couleurs plus bas encore peuvent être utilisés en cas de bande passante à très faible débit. Pour les connexions par modem, KX II passe automatiquement par défaut à une vitesse de connexion très basse et à un nombre de couleurs réduit pour optimiser les performances.
Je souhaite me connecter via Internet. A quel type de performance dois-je m'attendre ?	Ceci dépend de la bande passante et de la latence de la connexion Internet entre votre client distant et KX II. Avec une connexion par modem câble ou ADSL à haut débit, vos performances peuvent être très similaires à une connexion par réseau local/étendu. Pour les connexions plus lentes, utilisez les suggestions ci-dessus pour améliorer les performances.
Mon environnement dispose d'une bande passante à haut débit. Comment puis-je optimiser les performances ?	Les paramètres par défaut fournissent des performances solides dans un environnement à bande passante à haut débit. Assurez-vous que la vitesse de connexion est paramétrée sur 100 Mb ou 1 Gb, et le nombre de couleurs sur Couleur RVB 15 bits.

Question	Réponse
Quelle est la résolution vidéo distante (sur IP) maximale prise en charge ?	Dominion KX II est le seul commutateur KVM-sur-IP à prendre en charge la résolution vidéo distante haute définition (HD) 1920 x 1080. De plus, des formats grand écran courants sont pris en charge, comme 1600 x 1200, 1680 x 1050 et 1440 x 900, les utilisateurs distants peuvent donc travailler sur les écrans actuels à résolution supérieure.
Quelle quantité de bande passante est utilisée pour le son ?	Cela dépend du type de format audio utilisé, mais il faut environ 1,5 Mbps pour écouter du son de qualité CD.
Et pour les serveurs à ports DVI ?	Les serveurs à ports DVI prenant en charge DVI-A (analogique) et DVI-I (analogique et numérique intégrés) peuvent utiliser un adaptateur passif peu coûteux tel qu'ADVI-VGA de Raritan pour convertir le port DVI du serveur en prise VGA qui peut être connectée à la prise VGA d'un CIM de KX II. Les serveurs dotés de ports DVI prenant en charge DVI-I ou DVI-D (numérique) peuvent utiliser le nouveau CIM D2CIM-DVUSB-DVI.

Ethernet et mise en réseau IP

Question	Réponse
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).

Question	Réponse
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.
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 ?	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.
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 par des réseaux VPN standard.
Puis-je utiliser KX II avec un serveur proxy ?	Oui. KX II peut être utilisé avec un serveur proxy SOCKS, à condition que le PC client distant soit configuré correctement. Consultez la documentation de l'utilisateur ou l'aide en ligne pour en savoir plus.
Combien de ports TCP doivent être activés sur mon pare-feu pour autoriser l'accès réseau à Dominion KX II ?	Deux ports sont requis : un port 5000 TCP pour détecter d'autres dispositifs Dominion, et pour la communication entre les dispositifs Raritan et CC-SG ; et, bien entendu, le port 443 pour la communication HTTPS.
Ces ports sont-ils configurables ?	Oui. Les ports TCP de Dominion KX II sont configurables par l'administrateur.

Question	Réponse
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 clients doivent se rendre compte que 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 sur 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 ?	Dominion KX II s'appuie sur votre réseau local/Internet. Les éventuels problèmes incluent : Négociation automatique d'Ethernet. Sur certains réseaux, la négociation automatique 10/100 ne fonctionne pas correctement et l'unité Dominion KX II doit alors être réglée sur 100 Mb/full duplex ou sur l'option adaptée au réseau. Doublon 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 (ou le port de l'autre dispositif) doit être modifié. Lors de la modification de l'adresse IP de Dominion KX II ou du passage à une nouvelle unité KX II, vous devez attendre suffisamment longtemps pour que ses adresses IP et Mac® soient reconnues par les réseaux des couches 2 et 3.

Gestion de réseau IPv6

Question	Réponse
Qu'est-ce qu'IPv6 ?	IPv6 est l'acronyme d'Internet Protocol Version 6. Il s'agit du protocole IP nouvelle génération qui remplacera la version 4 (IPv4) actuelle du protocole IP. IPv6 corrige certains problèmes constatés dans IPv4, comme le nombre limité d'adresses IPv4. Il améliore également IPv4 dans des domaines, tels que le routage et la configuration automatique du réseau. IPv6 devrait remplacer IPv4 graduellement, les deux coexistant pendant quelques années. IPv6 résout l'un des problèmes les plus épineux rencontrés par l'administrateur : la configuration et la gestion d'un réseau IP.
Pourquoi Dominion KX II prend-il en charge la gestion de réseau IPv6 ?	Les organismes publics et le ministère de la Défense américains sont maintenant dans l'obligation d'acheter des produits compatibles IPv6. En outre, de nombreuses entreprises et de nombreux pays, tels que la Chine, effectueront la transition à IPv6 au cours des prochaines années.
Qu'est-ce que la « double pile » et pourquoi est-elle nécessaire ?	La double pile consiste à prendre en charge simultanément les protocoles IPv4 et IPv6. Etant donné la transition graduelle d'IPv4 à IPv6, la double pile est un prérequis fondamental pour la prise en charge d'IPv6.
Comment puis-je activer IPv6 sur Dominion KX II?	Utilisez la page Network Settings (Paramètres réseau), disponible depuis l'onglet Device Settings (Paramètres du dispositif). Activez l'adressage IPv6 et choisissez la configuration manuelle ou automatique. Pour plus d'informations, consultez le manuel d'utilisation.

Question	Réponse
Et si je dispose d'un serveur externe avec une adresse IPv6 que je souhaite utiliser avec mon dispositif Dominion KX II?	Dominion KX II peut accéder aux serveurs externes via leurs adresses IPv6 ; par exemple, un gestionnaire SNMP, un serveur Syslog ou un serveur LDAP. Grâce à l'architecture à double pile de Dominion KX II, ces serveurs externes sont accessibles via (1) une adresse IPv4, (2) une adresse IPv6 ou (3) un nom d'hôte. Dominion KX II prend donc en charge l'environnement mixte IPv4/IPv6 dont de nombreux clients disposent.
Dominion KX I (la génération précédente de KX) prend-il en charge IPv6 ?	Non. Dominion KX I ne prend pas en charge les adresses IPv6.
Et si mon réseau ne prend pas en charge IPv6 ?	La gestion de réseau par défaut de Dominion KX II est définie en usine pour IPv4 uniquement. Dès que vous êtes prêt à utiliser IPv6, suivez les instructions ci-dessous pour activer le fonctionnement à double pile IPv4/IPv6.
Où puis-je obtenir des informations supplémentaires sur IPv6 ?	Consultez www.ipv6.org pour obtenir des informations générales sur IPv6. Le manuel d'utilisation de Dominion KX II décrit la prise en charge de IPv6.

Serveurs

Question	Réponse
Dominion KX II dépend-il d'un serveur Windows pour fonctionner ?	Absolument pas. Les utilisateurs dépendant de la disponibilité permanente de leur infrastructure KVM dans n'importe quelle situation de travail (car ils en auront certainement besoin pour résoudre des problèmes éventuels), Dominion KX II est conçu pour être entièrement indépendant de tous les serveurs externes.

Question	Réponse
Dois-je installer un serveur Web tel que Microsoft Internet Information Services (IIS) pour utiliser la fonction de navigateur Web de Dominion KX II ?	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 des fonctionnalités de navigateur Web et d'authentification entièrement intégrées.
Quel logiciel dois-je installer pour accéder à Dominion KX II depuis un poste de travail donné ?	Aucun. Dominion KX II est entièrement accessible par un navigateur Web (même si un client installé facultatif est fourni sur le site Web de Raritan, www.raritan.com, requis pour les connexions par modem). Un client Java est maintenant disponible pour les utilisateurs non-Windows.
Que dois-je faire pour préparer la connexion d'un serveur à Dominion KX II ?	Réglez les paramètres souris de manière à fournir aux utilisateurs la meilleure synchronisation de souris et désactivez les écrans de veille et les fonctions de gestion d'alimentation qui affectent l'affichage de l'écran.
Et pour la synchronisation de la souris ?	Auparavant, la synchronisation de souris dans KVM sur IP était une expérience frustrante. La synchronisation absolue de la souris sur Dominion KX II offre une souris parfaitement synchronisée sans modification des paramètres de la souris sur des serveurs Windows et Mac Apple®. Pour d'autres serveurs, le mode Intelligent Mouse (souris intelligente) ou le mode de souris unique rapide évite la modification des paramètres de la souris du serveur.
Que contient le coffret Dominion KX II ?	Il comprend les éléments suivants : (1) l'unité Dominion KX II, (2) le guide de configuration rapide, (3) les pattes de fixation de montage en rack 19 po standard, (4) le CD-ROM du manuel d'utilisation, (5) un câble réseau, (6) un câble croisé, (7) un cordon de raccordement CA localisé et (8) un certificat de garantie et d'autres documents.

Serveurs lames

Question	Réponse

Question	Réponse
Puis-je connecter des serveurs lames à Dominion KX II ?	Oui. Dominion KX II prend en charge les modèles courants de serveurs lames des principaux fabricants : HP®, IBM®, Dell® et Cisco®.
Quels serveurs lames sont pris en charge ?	Les modèles suivants sont pris en charge : Dell PowerEdge® 1855, 1955 et M1000e ; HP BladeSystem c3000 et c7000 ; IBM BladeCenter® H, E et S ; et Cisco UCS B-Series.
Les CIM lames Paragon® sont-ils utilisés ?	Non. Dominion KX II n'exige pas l'utilisation de CIM spéciaux pour serveurs lames, comme Paragon II.
Quel CIM dois-je utiliser ?	Tout dépend du type de ports KVM figurant sur la marque et le modèle spécifiques du serveur lame que vous utilisez. Les CIM suivants sont pris en charge : DCIM-PS2, DCIM-USBG2, D2CIM-VUSB et D2CIM-DVUSB.
Quels types d'accès et de contrôle sont disponibles ?	Dominion KX II offre un accès KVM automatisé et sécurisé : (1) sur rack, (2) à distance sur IP, (3) via CommandCenter et (4) par modem.
Dois-je utiliser des raccourcis-clavier pour permuter entre les lames ?	Certains serveurs lames requièrent l'utilisation de raccourcis-clavier pour permuter entre les lames. Avec Dominion KX II, ces raccourcis-clavier sont inutiles. Il vous suffit de cliquer sur le nom du serveur lame pour que Dominion KX II passe automatiquement sur cette lame sans l'utilisation explicite du raccourci-clavier.
Puis-je accéder au module de gestion du serveur lame ?	Oui. Vous pouvez définir l'URL du module de gestion et y accéder depuis Dominion KX II ou depuis CommandCenter Secure Gateway. S'il est configuré, l'accès en un clic est disponible.

Question	**Réponse**
Combien de serveurs lames puis-je connecter à Dominion KX II ?	Aux fins de performances et de fiabilité, vous pouvez connecter jusqu'à 8 châssis de lames à un Dominion KX II, indépendamment du modèle. Raritan recommande de connecter jusqu'à deux fois le nombre de connexions à distance prises en charge par le dispositif. Par exemple, avec un KX2-216 doté de deux canaux à distance, nous vous recommandons de connecter jusqu'à quatre châssis de serveurs lames. Vous pouvez bien entendu connecter des serveurs individuels aux ports de serveur restants.
Je suis un client SMB possédant quelques Dominion KX II. Dois-je utiliser votre station de gestion CommandCenter Secure Gateway ?	Non, vous n'y êtes pas obligé. Les clients SMB n'ont pas à utiliser CommandCenter Secure Gateway pour exploiter les nouvelles fonctions de lames.
Je suis un client professionnel utilisant CommandCenter Secure Gateway. Puis-je accéder aux serveurs lames via CommandCenter Secure Gateway ?	Oui. Une fois les serveurs lames configurés sur Dominion KX II, l'utilisateur CommandCenter Secure Gateway peut y accéder via des connexions KVM. En outre, les serveurs lames sont organisés par châssis, ainsi que par vues personnalisées CommandCenter Secure Gateway.
Et si je souhaite également un accès KVM en bande ou intégré ?	L'accès en bande et intégré aux serveurs lames peut être configuré au sein de CommandCenter Secure Gateway.
J'exécute VMware® sur certains serveurs lames. Est-ce pris en charge ?	Oui. Oui, avec CommandCenter Secure Gateway, vous pouvez afficher les machines virtuelles exécutées sur les serveurs lames, et y accéder.
Le support virtuel est-il pris en charge ?	Tout dépend du serveur lame. Les lames HP peuvent prendre en charge le support virtuel. S'il est configuré de manière appropriée, IBM BladeCenter (hormis BladeCenter T) prend en charge le support virtuel. Un CIM de support virtuel, D2CIM-VUSB ou D2CIM-DVUSB, doit être utilisé.

Question	Réponse
La synchronisation absolue de la souris est-elle prise en charge ?	Les serveurs disposant de commutateurs KVM internes dans un châssis à lame ne prennent habituellement pas en charge la technologie de souris absolue. Pour les lames HP et certains serveurs lames Dell, un CIM peut être connecté à chaque lame ; la synchronisation absolue de la souris est donc prise en charge.
L'accès aux lames est-il sécurisé ?	Oui. Oui, l'accès aux lames utilisent toutes les fonctions de sécurité standard de Dominion KX II, telles que le chiffrement 128 bits ou 256 bits. En outre, il existe des fonctions de sécurité spécifiques aux lames, telles que les autorisations d'accès par lame et le blocage des raccourcis-clavier qui interdit l'accès non autorisé.
Les dispositifs Dominion KSX II ou KX II-101 prennent-ils en charge les serveurs lames ?	Pour le moment, ces produits ne prennent pas en charge les serveurs lames.

Installation

Question	Réponse
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) Dominion ou Paragon, et un adaptateur qui se branche directement sur les ports clavier, vidéo 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 (paire torsadée non blindée) standard : Cat5, Cat5e ou Cat6. Dans nos manuels et brochures publicitaires, Raritan n'indique que câble « Cat5 ». En réalité, n'importe quel câble UTP convient pour Dominion KX II.

Question	Réponse
Quels types de serveurs 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 normalisés peut être connecté. En outre, les serveurs dotés de ports série peuvent être contrôlés à l'aide du CIM P2CIM-SER.
Comment connecter les serveurs à Dominion KX II ?	Les serveurs connectés à Dominion KX II requièrent un CIM Dominion ou Paragon 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 (paire torsadée blindée) 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 au maximum de Dominion KX II, suivant leur type. (Reportez-vous à la documentation utilisateur sur le site Web de Raritan.) Pour le CIM D2CIM-VUSB qui prend en charge les fonctions Support virtuel et Synchronisation absolue de la souris, une distance de 30 m est recommandée.
Certains systèmes d'exploitation se bloquent lorsque je déconnecte un clavier ou une souris pendant le fonctionnement. Que faut-il faire pour éviter qu'un serveur connecté à Dominion KX II ne se bloque lorsque je passe à un autre ?	Chaque clé électronique de 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 : fruit de plus de 15 années d'expérience, elle a été déployée 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.

Question	Réponse
Combien de serveurs peuvent être connectés à chaque unité Dominion KX II ?	Les modèles Dominion KX II offrent 8, 16 ou 32 ports de serveur dans un châssis 1U, et jusqu'à 64 dans un châssis 2U. Ce commutateur KVM numérique offre la densité de ports la plus élevée du secteur.
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 ?	Dominion KX II met automatiquement à jour les noms de ports de serveurs 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 l'appareil de gestion CommandCenter Secure Gateway en option.
Comment dois-je connecter un dispositif contrôlé en série (RS-232), tel qu'un routeur/commutateur Cisco ou un serveur Sun headless, à Dominion KX II ?	Si le nombre de dispositifs contrôlés en série est réduit, ils peuvent être connectés à Dominion KX II via le convertisseur série P2CIM-SER de Raritan. Les clients peuvent également envisager le déploiement de Dominion KSX II, commutateur KVM et série intégré. DKSX-144 offre quatre ports KVM sur IP et quatre ports série. DKSX-188 offre huit ports KVM sur IP et huit ports série. Toutefois, si vous disposez de nombreux dispositifs contrôlés en série, nous vous recommandons d'utiliser la gamme Dominion SX de Raritan des serveurs de console sécurisée. Dominion SX propose plus de fonctions série à un meilleur prix que Dominion KX II. SX est simple à utiliser, à configurer et à gérer, et peut être entièrement intégré au déploiement d'une série Dominion.

Port local

Question	Réponse
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 de clavier, écran et souris uniques. Vous pouvez basculer d'un serveur à l'autre via l'interface utilisateur basée navigateur ou un raccourci-clavier.
Puis-je regrouper les ports locaux de plusieurs unités KX II ?	Oui. Vous pouvez connecter les ports locaux de plusieurs commutateurs KX II à un autre KX II à l'aide de la fonction multiniveau. Vous pouvez alors accéder aux serveurs connectés à vos dispositifs KX II d'un point unique du centre de données via une liste de regroupement de ports.
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 est doté de ports clavier et souris USB sur le port local. Notez que depuis avril 2011, les commutateurs Dominion KX II ne sont plus équipés de ports locaux PS/2. Les clients possédant des claviers et souris PS/2 doivent utiliser un adaptateur PS/2-USB.
Existe-t-il un affichage à l'écran pour l'accès local sur le rack ?	Oui, mais l'accès sur le rack de Dominion KX II dépasse largement les possibilités des 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 Dominion KX II utilise la même interface pour l'accès local et l'accès distant. Par ailleurs, la plupart des fonctions d'administration sont disponibles sur le rack.

Question	Réponse
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. Les utilisateurs se connectent à un serveur d'un simple clic de la souris ou via un raccourci-clavier.
Comment s'assurer que seuls les utilisateurs autorisés peuvent accéder aux serveurs depuis le port local ?	Les utilisateurs essayant d'utiliser le port local doivent subir le même niveau d'authentification que les utilisateurs à distance. En d'autres termes : 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 bascule sur sa base de données d'authentification interne. Dominion KX II possède sa propre authentification autonome, offrant une installation instantanée, prête à l'emploi.
En cas d'utilisation du port local pour renommer 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 l'appareil de gestion CommandCenter Secure Gateway de Raritan. Plus simplement, si le nom d'un serveur sur l'affichage à l'écran Dominion KX II est modifié, tous les clients à distance et les serveurs de gestion externes sont mis à jour en temps réel.
Si j'utilise les outils d'administration à distance de Dominion KX II pour modifier le nom d'un serveur connecté, l'affichage à l'écran du port local est-il également affecté ?	Oui. Si vous modifiez le nom du serveur à distance ou au moyen de l'appareil de gestion CommandCenter Secure Gateway en option de Raritan, l'affichage à l'écran de Dominion KX II est immédiatement mis à jour.

Port local étendu (modèles Dominion KX2-832 et KX2-864 uniquement)

Question	Réponse
Qu'est-ce que le port local étendu ?	Dominion KX2-832 et KX2-864 comportent un port local étendu. Les modèles huit utilisateurs de KX II sont dotés d'un port local standard, et d'un nouveau port local étendu qui prolonge le port local, via un câble Cat5, au-delà du rack vers une salle de contrôle, un autre point du centre de données ou un commutateur Dominion KX II ou Paragon II.
Puis-je connecter le port local étendu à une autre unité KX II ?	Oui, vous pouvez connecter le port local étendu à un port de serveur d'une autre unité KX II à l'aide de la fonction multiniveau de KX II.
Le port local étendu requiert-il une station utilisateur ?	Oui. Les dispositifs suivants peuvent servir de « station utilisateur » pour le port local étendu : Paragon II EUST, Paragon II UST et le dispositif Cat5 Reach® URKVMG. En outre, le port local étendu peut être connecté via un câble Cat5 à un port serveur sur un commutateur Dominion KX II ou Paragon II. Cette configuration peut être utilisée pour consolider les ports locaux de nombreux dispositifs KX2-8xxx sur un seul commutateur.
Quelle est la distance maximale autorisée entre la station utilisateur et Dominion KX II ?	La distance est de 61 à 304 m, mais varie selon le type de station utilisateur, la résolution vidéo, le type et la qualité du câble. Pour plus d'informations, consultez le manuel d'utilisation ou les notes de version.
Un CIM est-il nécessaire ?	Aucun CIM n'est nécessaire. Il vous suffit de connecter un câble Cat5.
Dois-je utiliser le port local étendu ?	Non. Le port local étendu est une fonction facultative, désactivée par défaut. Utilisez la page Local Port Settings (Paramètres du port local) pour l'activer. Pour plus de sécurité, vous pouvez également désactiver le port local standard si vous ne l'utilisez pas.
Double alimentation	

Question	Réponse
Dominion KX II propose-t-il l'option de double alimentation ?	Oui. Tous les modèles Dominion KX II sont équipés d'arrivées et d'alimentations CA 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, de 50 à 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 avant de Dominion KX II permet d'avertir l'utilisateur d'une panne de courant. Une entrée est également envoyée dans le journal d'audit et affichée dans l'interface utilisateur du client distant de KX II. Des événements SNMP ou Syslog sont également générés, si les options correspondantes ont été configurées par l'administrateur.

Contrôle des unités de distribution d'alimentation (PDU)

Question	Réponse
Quel type de fonctions de gestion de l'alimentation à distance Dominion KX II offre-t-il ?	Les PDU intelligentes de Raritan peuvent être connectées à Dominion KX II pour permettre la gestion de l'alimentation des serveurs cible et d'autres équipements. Pour les serveurs, après une simple opération de configuration unique, il vous suffit de cliquer sur le nom du serveur pour mettre sous ou hors tension un serveur bloqué ou en effectuer l'alimentation cyclique.

Question	Réponse
Quelles sont les barrettes d'alimentation prises en charge par Dominion KX II ?	Les barrettes d'alimentation Dominion PX™ et Remote Power Control (RPC) de Raritan. Elles sont livrées avec de nombreuses variations de prises, connecteurs et tensions. Notez que vous ne devez pas connecter des barrettes d'alimentation de la série PM à Dominion KX II car elles ne permettent pas la commutation au niveau des prises.
Combien de PDU peuvent être connectées à chaque unité Dominion KX II ?	Vous pouvez connecter jusqu'à huit PDU à un dispositif Dominion KX II.
Comment puis-je connecter la PDU à Dominion KX II ?	D2CIM-PWR permet de connecter la barrette d'alimentation à Dominion KX II. D2CIM-PWR est vendu séparément ; il n'est pas fourni avec la PDU.
Dominion KX II prend-il en charge les serveurs à alimentations multiples ?	Oui. Dominion KX II peut être facilement configuré pour prendre en charge des serveurs à alimentations multiples branchés sur plusieurs barrettes d'alimentation. Quatre alimentations peuvent être connectées par serveur cible.
Dominion KX II affiche-t-il des statistiques et des mesures provenant de la PDU ?	Oui. Les statistiques d'alimentation au niveau de la PDU, comprenant l'alimentation, le courant et la tension, sont extraites de la PDU et affichées pour l'utilisateur.
La gestion de l'alimentation à distance nécessite-t-elle une configuration spéciale des serveurs reliés ?	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. Consultez la documentation du serveur pour modifier ce paramètre.
Que se passe-t-il lorsque j'effectue l'alimentation cyclique d'un serveur ?	Notez que ceci équivaut physiquement à débrancher le serveur de la prise de courant, puis à le rebrancher.
Puis-je mettre sous/hors tension un autre équipement (non-serveurs) connecté à une PDU ?	Oui. Vous pouvez mettre sous tension et hors tension d'autres équipements reliés à la PDU par prise depuis l'interface du navigateur de Dominion KX II.

Groupement, fonction multiniveau et mise en cascade des ports locaux

Question	Réponse
Comment puis-je connecter physiquement plusieurs dispositifs Dominion KX II entre eux pour disposer d'une solution unique ?	Pour connecter physiquement plusieurs dispositifs KX II entre eux et permettre un accès local groupé, vous pouvez relier les ports locaux de plusieurs commutateurs KX II en niveau (ou en cascade) à un KX II de base à l'aide de la fonction multiniveau de KX II. Vous pouvez alors accéder aux serveurs connectés à vos dispositifs KX II d'un point unique du centre de données via une liste de regroupement de ports. Le CIM D2CIM-DVUSB est nécessaire pour relier le commutateur KX II en niveau au commutateur de base. Ou pour KX2-832 et KX2-864, le port local étendu peut être connecté via un câble CAT5/6 (aucun CIM requis) au commutateur KX II de base. Un accès via la liste de regroupement de ports est disponible dans le centre de données ou même à partir d'un PC distant. Tous les serveurs connectés aux KX II en niveau sont accessibles via une liste hiérarchisée de ports ou via une recherche (avec caractères joker). Deux niveaux sont pris en charge ; 1024 dispositifs au plus sont accessibles dans une configuration multiniveau. La gestion de l'alimentation à distance est également prise en charge. L'accès multiniveau aux supports virtuels, aux cartes à puce et aux serveurs lames sera pris en charge dans une prochaine version. Ces fonctions sont évidemment accessibles via une connexion distante standard. Même si l'accès au serveur IP distant via la liste de regroupement de ports est disponible pour des raisons de commodité, l'accès à distance au serveur en niveau depuis CommandCenter, ou via l'unité KX II à laquelle le serveur est connecté, est recommandé pour des performances optimales.

Question	Réponse
Dois-je connecter physiquement les dispositifs Dominion KX II entre eux ?	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 automatiquement comme une solution unique lorsqu'elles sont déployées avec l'appareil de gestion CommandCenter Secure Gateway (CC-SG) 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 firmware, ainsi qu'une base de données d'authentification et d'autorisation unique. Les clients qui utilisent CC-SG pour un accès distant centralisé peuvent profiter de la fonction multiniveau (cascade) de KX II pour regrouper les ports locaux de plusieurs commutateurs KX II et accéder à 1024 serveurs au plus à partir d'une console unique dans le centre de données.
CC-SG est-il requis ?	Pour les clients souhaitant un usage autonome (sans système central de gestion), plusieurs unités Dominion KX II interagissent encore et se mettent en corrélation via le réseau IP. Plusieurs commutateurs Dominion KX II sont accessibles depuis l'interface utilisateur Web KX II et depuis Multiplatform Client (MPC).

Question	Réponse
Est-il possible de connecter un commutateur analogique KVM existant à Dominion KX II ?	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) PS/2 ou USB, et de le connecter aux ports utilisateur du commutateur KVM analogique existant. Les commuteurs KVM analogiques prenant en charge la commutation par raccourci-clavier sur leurs ports locaux peuvent être mis en niveau sur un commutateur Dominion KX II et commutés via une liste de regroupement de ports, à distance et dans le centre de données. 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.

Modules d'interface pour ordinateur (CIM)

Question	Réponse
Quel type de vidéo vos CIM prennent-ils en charge ?	A l'origine, nos CIM prenaient en charge la vidéo VGA analogique. Trois nouveaux CIM prennent en charge les formats de vidéo numérique, notamment DVI, HDMI et DisplayPort. Il s'agit de D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI et D2CIM-DVUSB-DP.

Question	Réponse
Est-il possible d'utiliser des modules d'interface pour ordinateur (CIM) venant du commutateur analogique matriciel KVM de Raritan Paragon avec Dominion KX II ?	Oui. Il est possible que certains CIM Paragon fonctionnent avec Dominion KX II. (Consultez les notes de version de Dominion KX II Raritan sur le site Web pour obtenir la liste la plus récente des CIM agréés.) Toutefois, les modules d'interface pour ordinateurs (CIM) 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 304 mètres), il n'est pas conseillé d'acheter les modules Paragon pour les utiliser avec Dominion KX II. Notez également que lorsque les CIM 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 304 mètres comme lorsqu'ils sont connectés à Paragon.
Est-il possible d'utiliser des modules d'interface pour ordinateurs (CIM) Dominion KX II avec le commutateur analogique matriciel KVM de Raritan Paragon ?	Non. Les modules d'interface pour ordinateurs (CIM) Dominion KX II offrent une transmission vidéo sur une distance de 15 à 46 mètres et, par conséquent, ne sont pas compatibles avec Paragon qui nécessite des CIM avec transmission vidéo sur une distance de 304 mètres. Pour que tous les clients de Raritan bénéficient de la qualité vidéo la plus performante qui soit, une caractéristique constante de Raritan, les CIM de série Dominion ne sont pas compatibles avec Paragon.

Question	Réponse
Dominion KX II prend-il en charge les CIM doubles Paragon ?	Oui. Dominion KX II prend maintenant en charge les CIM doubles Paragon II (P2CIM-APS2DUAL et P2CIM-AUSBDUAL) qui peuvent connecter des serveurs du centre de données à deux commutateurs Dominion KX II différents. Lorsqu'un commutateur KX II n'est pas disponible, le serveur est accessible au moyen du second commutateur KX II, ce qui offre un accès redondant et double le niveau de l'accès KVM à distance. Notez qu'il s'agit de CIM Paragon, ils ne prennent donc pas en charge les fonctions avancées de KX II telles que le support virtuel, la souris absolue, etc.

Sécurité

Question	Réponse
Dominion KX II est-il certifié FIPS 140-2 ?	Dominion KX II utilise un module cryptographique validé FIPS 140-2 s'exécutant sur une plate-forme Linux selon les directives de mise en œuvre de FIPS 140-2. Ce module cryptographique sert au chiffrement du trafic de session KVM constitué de données vidéo, de clavier, de souris, de support virtuel et de carte à puce.
Quel type de chiffrement est utilisé par Dominion KX II ?	Dominion KX II utilise un système de chiffrement AES à 256 bits, AES à 128 bits ou 128 bits standard (et 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.

Question	Réponse
Dominion KX II prend-il en charge le chiffrement AES comme recommandé par les normes NIST et FIPS du gouvernement américain ?	Oui. Dominion KX II utilise le chiffrement AES (Advanced Encryption Standard) pour une sécurité accrue. AES est disponible pour 256 bits et 128 bits. AES est un algorithme de chiffrement 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 chiffrement 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, vidéo et support virtuel.
Comment Dominion KX II intègre-t-il les serveurs d'authentification externes tels qu'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 chiffrée. Personne, y compris l'assistance 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 les mots de passe forts ?	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.

Question	Réponse
Est-il possible de téléverser son propre certificat numérique sur Dominion KX II ?	Oui. Les clients peuvent téléverser des certificats auto-signés ou numériques fournis par une autorité de certification sur Dominion KX II pour une authentification améliorée et des communications sécurisées.
KX II prend-il en charge une bannière de sécurité configurable ?	Oui. Pour le gouvernement, les forces armées et autres clients requérant un message de sécurité avant l'ouverture de session de l'utilisateur, KX II peut afficher un message de bannière configurable par l'utilisateur et éventuellement demander une acceptation.
Ma stratégie de sécurité ne permet pas l'utilisation de numéros de port TCP standard. Est-il possible de les modifier ?	Oui. Pour les clients souhaitant éviter les numéros de port TCP/IP standard pour augmenter la sécurité, Dominion KX II permet à l'administrateur de configurer d'autres numéros de port.

Authentification par cartes à puce et CAC

Question	Réponse
Dominion KX II prend-il en charge l'authentification par cartes à puce et CAC ?	Oui. L'authentification par cartes à puce et DoD Common Access Card (CAC) sur les serveurs cible est prise en charge depuis la version 2.1.10.
Qu'est-ce que CAC ?	Suivant la directive présidentielle relative à la sécurité intérieure 12 (HSPD-12), CAC est un type de carte à puce créée par le gouvernement américain et utilisé par les personnels militaires et gouvernementaux américains. Il s'agit d'une carte multitechnologie, polyvalente dont le but est de disposer d'une carte d'identification unique. Pour plus d'informations, reportez-vous aux normes FIPS 201.
Quels modèles de KX II prennent en charge les cartes à puce/CAC ?	Tous les modèles de Dominion KX II les prennent en charge. Dominion KSX II et KX2-101 ne prennent pas pour le moment en charge les cartes à puce et CAC.

Question	Réponse
Les clients entreprise et SMB utilisent-ils également des cartes à puce ?	Oui. Cependant, le déploiement le plus agressif de cartes à puce est effectué par le gouvernement fédéral des Etats-Unis.
Quels CIM prennent en charge les cartes à puce/CAC ?	D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI et D2CIM-DVUSB-DP représentent les CIM requis.
Quels lecteurs de cartes à puce sont pris en charge ?	Les normes de lecteur requises sont CCID USB et PC/SC. Consultez la documentation pour obtenir la liste des lecteurs agréés et des informations supplémentaires.
L'authentification par carte à puce/CAC fonctionne-t-elle sur le port local et via CommandCenter ?	Oui. L'authentification par carte à puce/CAC fonctionne sur le port local et via CommandCenter. Pour le port local, connectez un lecteur de cartes à puce compatible au port USB de Dominion KX II.
Les UST et CIM Paragon habilités carte à puce sont-ils utilisés ?	Non. P2-EUST/C et P2CIM-AUSB-C ne sont pas intégrés à la solution Dominion KX II.
Où puis-je obtenir des informations supplémentaires sur la prise en charge des cartes à puce par KX II ?	Consultez les notes de version et le manuel d'utilisation de Dominion KX II pour plus d'informations.

Capacités de gestion

Question	Réponse
Est-il possible de gérer et de configurer à distance Dominion KX II via un navigateur Web ?	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. 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.)

Question	Réponse
Est-il possible de sauvegarder et de restaurer la configuration de Dominion KX II ?	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. La fonction de sauvegarde et de restauration de Dominion KX II peut être utilisée à distance sur le réseau ou via un navigateur Web.
Quelles fonctions d'audit et de consignation Dominion KX II offre-t-il ?	Pour une responsabilité optimale, Dominion KX II consigne tous les événements utilisateur principaux avec horodatage. 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.
Est-il possible d'intégrer Dominion KX II au serveur Syslog ?	Oui. Dominion KX II peut également, en plus de ses propres fonctions de consignation interne, envoyer tous les événements enregistrés à un serveur Syslog centralisé.
Est-il possible d'intégrer Dominion KX II avec SNMP ?	Oui. Dominion KX II peut également, en plus de ses propres fonctions de consignation interne, envoyer des traps SNMP aux systèmes de gestion SNMP. SNMP v2 et v3 sont pris en charge.
Un administrateur peut-il fermer la session d'un utilisateur ?	Oui, les administrateurs peuvent vérifier à quel port un utilisateur est connecté, et le déconnecter au besoin d'un port spécifique ou du dispositif.
Est-il possible de synchroniser l'horloge interne de Dominion KX II avec un serveur de temps ?	Oui. Dominion KX II prend en charge le protocole NTP standard pour se synchroniser avec le serveur de temps de votre entreprise ou avec n'importe quel serveur de temps public (si le pare-feu de votre entreprise autorise les demandes NTP sortantes).

Documentation et assistance

Question	Réponse
Comment puis-je trouver de la documentation sur Dominion KX II?	La documentation est disponible sur raritan.com à la page de firmware et de documentation de KX II : http://www.raritan.com/support/dominion-kx-ii. Elle est classée par version de firmware.
Quelle documentation est disponible ?	Un guide de configuration rapide, un manuel d'utilisation et un manuel des clients KVM et série, ainsi que des notes de version et d'autres informations sont disponibles.
Existe-t-il une aide en ligne ?	Oui. Une aide en ligne est disponible sur raritan.com avec la documentation et depuis l'interface utilisateur de KX II.
Quel CIM dois-je utiliser avec un serveur particulier ?	Consultez le manuel sur les CIM fourni avec la documentation KX II. Notez que les normes vidéo DVI, HDMI et DisplayPort sont prises en charge avec les nouveaux CIM vidéo numériques, disponibles depuis la version 2.5.
Quelle est la durée de la garantie de KX II ?	Dominion KX II est fourni avec une garantie standard de deux ans, qui peut être prolongée à cinq ans.

Divers

Question	Réponse
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 Dominion KX II sont admin/raritan (tout en minuscules). Cependant, pour offrir le 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.

Question	Réponse
En cas de modification et d'oubli du mot de passe administratif de Dominion KX II, vous est-il possible de le récupérer ?	Dominion KX II comporte une fonction de réinitialisation matérielle qui peut être utilisée pour réinitialiser les paramètres par défaut du dispositif et rétablir par la même occasion le mot de passe administratif par défaut.
Comment dois-je procéder à la migration de Dominion KX I à Dominion KX II ?	De manière générale, les utilisateurs de KX I peuvent continuer à utiliser leurs commutateurs existants pendant de nombreuses années. A mesure que leurs centres de données se développent, les clients peuvent acheter et utiliser les nouveaux modèles KX II. L'appareil de gestion centralisée de Raritan, CommandCenter Secure Gateway (CC-SG) ainsi que le client MPC (Multi-Platform Client), prennent tous les deux en charge les commutateurs KX I et KX II de manière transparente.
Mes CIM KX I existants vont-ils fonctionner avec les commutateurs 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 de Paragaon I désireux de passer à KVM sur IP d'effectuer la migration en toute facilité vers KX II. Toutefois, vous pouvez également utiliser les CIM D2CIM-VUSB et D2CIM-DVUSB qui prennent en charge le support virtuel et la synchronisation absolue de la souris. En outre, des CIM vidéo numériques prenant en charge DVI, HDMI et DisplayPort sont également disponibles.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

Etats-Unis/Canada/Amérique latine

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

Chine

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

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

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

Inde

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

Japon

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5991
E-mail : support.japan@raritan.com

Europe

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

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

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

Allemagne
Lundi - Vendredi
8h30 - 17h30, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0
E-mail : rg-support@raritan.com

Melbourne, Australie

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

Taiwan

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