



Dominion KX II-101-V2

Manuel d'utilisation
Version 3.5.0

Copyright © 2012 Raritan, Inc.

KX2101V2-v3.5.0-D-F

Septembre 2012

255-62-3059-00

Le présent document contient des informations protégées par le droit d'auteur. Tous droits réservés. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans approbation écrite préalable de Raritan, Inc.

© Copyright 2012 Raritan, Inc. Tous les logiciels et matériels tiers mentionnés dans le présent document sont des marques commerciales déposées ou non de leurs détenteurs respectifs et leur propriété.

Informations FCC (Etats-Unis seulement)

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

Informations VCCI (Japon)

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

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

Si un câble d'alimentation est fourni avec ce produit, il doit être utilisé exclusivement pour ce dernier.



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 1 Introduction	1
KX II-101-V2 - Présentation	2
Aide KX II-101-V2	3
Nouveautés de l'aide	4
Documentation connexe	4
Photos du produit	5
Caractéristiques du produit	5
Interfaces	5
Configuration réseau	5
Caractéristiques du système de gestion	6
Caractéristiques d'administration	6
Caractéristiques utilisateur	7
Alimentation	7
Résolution vidéo	7
Montage	7
Terminologie	7
Contenu de l'emballage	8
Chapitre 2 Installation et configuration	9
Présentation	9
Données de connexion par défaut	9
Mise en route	10
Étape 1 : Configuration du serveur cible	10
Étape 2 : Configuration des paramètres du pare-feu de réseau	23
Étape 3 : Connexion de l'équipement	24
Étape 4 : Configuration du dispositif KX II-101-V2	29
Chapitre 3 Utilisation des serveurs cible	38
Interfaces	38
Interface de la console distante KX II-101-V2	38
Multi-Platform Client (MPC)	47
Virtual KVM Client (VKC)	47
Présentation	47
Connexion à un serveur cible KVM	48
Boutons de barre d'outils et icônes de barre d'état	48
Gestion de l'alimentation d'un serveur cible	50
Déconnexion des serveurs cible KVM	51
Connexion Properties (Propriétés de la connexion)	51
Informations sur la connexion	53
Options de clavier	54

Propriétés vidéo.....	60
Options de souris.....	65
Supports virtuels VKC	69
Options d'outils	70
Options d'affichage	74
Options d'aide	76
Chapitre 4 Support virtuel	77
Présentation.....	78
Conditions requises pour l'utilisation des supports virtuels	80
Supports virtuels dans un environnement Windows XP.....	81
Supports virtuels dans un environnement Linux	82
Supports virtuels dans un environnement Mac	84
Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible	84
Utilisation des supports virtuels	85
Connexion aux supports virtuels.....	86
Lecteurs locaux.....	86
Montage des images CD-ROM/DVD-ROM/ISO	87
Déconnexion des supports virtuels	88
Chapitre 5 Gestion des utilisateurs	89
Groupes d'utilisateurs	89
Liste des groupes d'utilisateurs	90
Relation entre les utilisateurs et les groupes.....	90
Ajout d'un nouveau groupe d'utilisateurs.....	91
Modification d'un groupe d'utilisateurs existant	95
Utilisateurs	96
Affichage de la liste des utilisateurs de KX II-101-V2.....	97
Affichage des utilisateurs par port	97
Déconnexion d'utilisateurs des ports	98
Fermeture de la session des utilisateurs de KX II-101-V2 (Déconnexion forcée)	98
Ajout d'un nouvel utilisateur.....	99
Modification d'un utilisateur existant.....	99
Blocage et déblocage des utilisateurs	100
Paramètres d'authentification	101
Implémentation de l'authentification à distance LDAP/LDAPS	102
Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory	106
Implémentation de l'authentification à distance RADIUS	107
Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS	110
Spécifications des échanges de communication RADIUS	110
Processus d'authentification d'utilisateur.....	112
Modification d'un mot de passe	114
Chapitre 6 Gestion des dispositifs	115
Paramètres réseau	115
Paramètres réseau de base	116
LAN Interface Settings (Paramètres de l'interface LAN)	119

Table des matières

Services du dispositif	120
Activation de Telnet	120
Activation de SSH.....	120
Paramètres des ports HTTP et HTTPS.....	121
Saisie du port de détection	121
Activation de l'accès direct aux ports via URL.....	122
Configuration des agents SNMP	122
Configuration du clavier/de la souris.....	125
Paramètres de port série	125
Port Admin	126
Gestion des barrettes d'alimentation Raritan	126
Modem.....	126
Configuration des paramètres de date et heure	128
Gestion des événements	128
Configuration de la gestion des événements - Paramètres	129
Configuration de la gestion des événements - Destinations	136
Configuration des ports.....	137
Gestion des serveurs cible KVM (page Port)	138
Gestion de l'alimentation	140
Commutateur KVM analogique.....	145
Réinitialisation de KX II-101-V2 à l'aide du bouton de réinitialisation.....	147
Modification du paramètre de langue de l'interface utilisateur par défaut	148

Chapitre 7 Gestion des connexions USB 149

Présentation	150
Paramètres de connexion USB	151
Paramètres des connexions USB avancées	152

Chapitre 8 Gestion de la sécurité 154

Security Settings (Paramètres de sécurité)	154
Limitations de connexion	154
Mots de passe sécurisés	156
Blocage des utilisateurs.....	157
Encryption & Share (Chiffrement et partage)	159
Activation de FIPS 140-2.....	163

Configuration du contrôle d'accès IP	165
Certificats SSL	168
Bannière de sécurité	171

Chapitre 9 Maintenance **173**

Journal d'audit.....	173
Informations sur le dispositif	174
Backup and Restore (Sauvegarde et restauration)	175
Mise à niveau du firmware	177
Historique des mises à niveau	179
Factory Reset (Restauration des valeurs d'usine)	179
Redémarrage de KX II-101-V2	180
Arrêt de la gestion par CC-SG	181

Chapitre 10 Diagnostics **183**

Page d'interface réseau	183
Page Network Statistics (Statistiques réseau)	183
Page Ping Host (Envoyer une commande Ping à l'hôte)	186
Page Trace Route to Host	186
Page Device Diagnostics (Diagnostics du dispositif).....	188

Chapitre 11 Interface de ligne de commande (CLI) **190**

Présentation	190
Accès à l'unité KX II-101-V2 à l'aide du CLI	191
Connexion SSH à KX II-101-V2.....	191
Accès SSH depuis un PC Windows	191
Accès SSH depuis un poste de travail UNIX/Linux	192
Connexion	192
Navigation de la CLI.....	192
Invites CLI	192
Saisie automatique des commandes.....	193
Syntaxe CLI - Conseils et raccourcis.....	193
Commandes courantes pour tous les niveaux de la CLI	194
Commandes CLI	194
Diagnostics	195
Configuration	197
Commande listports.....	199
Commande Userlist	199

Chapitre 12	Gestion CC-SG	200
	Présentation	200
	Suspension de la gestion du dispositif KX II-101-V2 par CC-SG	201
	Utilisation de CC-SG en mode proxy	202
Annexe A	Caractéristiques	203
	Spécifications physiques	203
	Systèmes d'exploitation pris en charge (Clients)	204
	Navigateurs pris en charge	205
	Connecteurs	206
	Modems certifiés	206
	Résolutions vidéo prises en charge	206
	Langues des claviers pris en charge	208
	Ports TCP et UDP utilisés	209
	Paramètres de vitesse réseau	211
	Brochage à 9 broches	212
Annexe B	Mise à jour du schéma LDAP	213
	Renvoi des informations relatives aux groupes d'utilisateurs	213
	A partir de LDAP	213
	A partir d'Active Directory (AD) de Microsoft	213
	Définition du Registre pour autoriser les opérations d'écriture sur le schéma	214
	Création d'un attribut	214
	Ajout d'attributs à la classe	215
	Mise à jour du cache de schéma	217
	Modification des attributs rciusergroup pour les membres utilisateurs	217
Annexe C	Montage en rack	221
	Attachez la fixation en L au dispositif KX II-101-V2 pour un montage horizontal	221
Annexe D	Remarques informatives	223
	Java Runtime Environment (JRE)	223
	Remarques sur la prise en charge d'IPv6	224
	Remarques sur la prise en charge d'IPv6 par système d'exploitation	224
	Remarques concernant le clavier, la vidéo et la souris	224
	Restriction de Sun Blade quant à la prise en charge de la vidéo, du clavier et de la souris	225
	Restriction d'accès au BIOS depuis un clavier local	225
	Configuration clavier et souris HP UX RX 1600	226
	Restriction du mode de souris pour serveurs Compaq Alpha et IBM P	226
	Restrictions des serveurs Windows 2000 et Windows 2003 quant au clavier	227
	CC-SG	227
	Mode proxy et MPC	227

Annexe E FAQ	228
<hr/>	
Foire aux questions générale	228
Gestion de réseau IPv6	229
Index	231
<hr/>	

Chapitre 1 Introduction

Dans ce chapitre

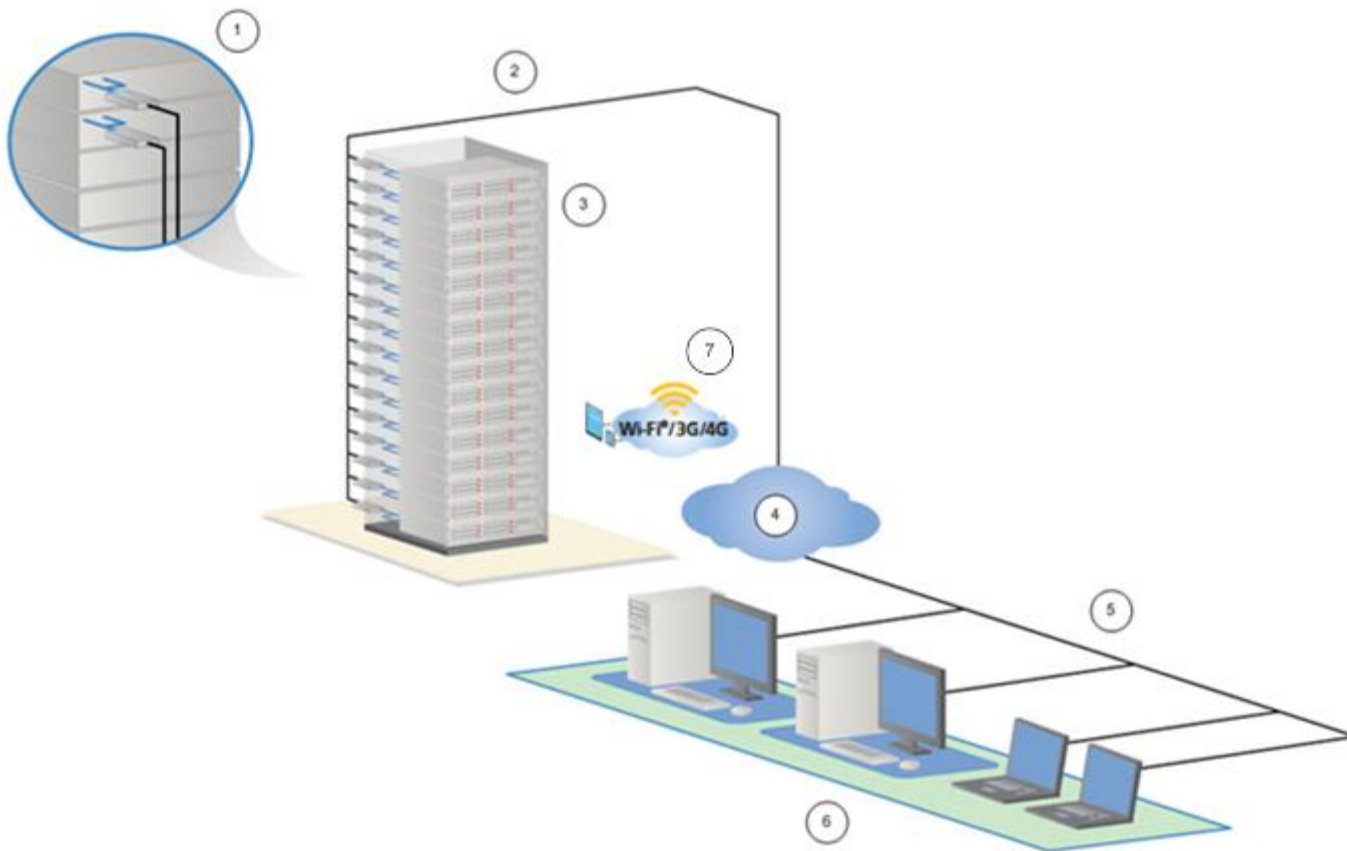
KX II-101-V2 - Présentation.....	2
Aide KX II-101-V2.....	3
Photos du produit	5
Caractéristiques du produit.....	5
Terminologie.....	7
Contenu de l'emballage.....	8

KX II-101-V2 - Présentation

Merci d'avoir acheté Dominion KX II-101-V2. KX II-101-V2 est composé d'un seul port (KVM) clavier, écran et souris pour la connexion à un serveur cible et d'un seul port IP pour la connexion à un réseau IP. Au sein du dispositif KX II-101-V2, les signaux KVM de votre serveur sont convertis au format IP et compressés pour la transmission via un réseau IP.

Le facteur de forme de la clé de l'unité KX II-101-V2 facilite son installation près du serveur cible, et chaque dispositif KX II-101-V2 a sa propre adresse IP. Chaque dispositif est alimenté via un bloc d'alimentation secteur externe.

KX II-101-V2 peut fonctionner comme appareil autonome ou être intégré à une solution logique, avec d'autres produits d'accès Raritan, à l'aide de la console de gestion CommandCenter Secure Gateway (CC-SG) 5.4 ou supérieure de Raritan.



Légende	
1	KX II-101-V2
2	LAN
3	Serveurs Windows®, Linux® et Sun™
4	TCP/IP
5	LAN
6	Accès distant (réseau)
7	Accès mobile via iPhone® et iPad® avec CC-SG

Aide KX II-101-V2

L'aide KX II-101-V2 explique comment installer, paramétrer et configurer KX II-101-V2. 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-101-V2.

Reportez-vous aux notes de version de KX II-101-V2 pour obtenir des informations importantes sur la version en cours avant d'utiliser KX II-101-V2.

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.

- Prise en charge du chiffrement FIPS 140-2
- Prise en charge d'une bannière de sécurité de connexion
- Accès mobile depuis un iPad® et un iPhone® à des serveurs connectés à une unité KX II-101-V2 gérée par CC-SG
- Prise en charge de SNMPv3
- Possibilité de téléverser votre propre certificat SSL sur l'unité KX II-101-V2
- Prise en charge pour les résolutions vidéo 1920 x 1080 et grand écran
- Numéros de ports TCP/IP configurables (mode Stealth)
- Accès direct à l'unité KX II-101-V2 gérée par CC-SG 5.4 ou supérieur
- Prise en charge de la fonction Virtual Media (Supports virtuels) pour Linux® et Mac®
- Prise en charge de l'interface utilisateur en japonais, chinois traditionnel et chinois simplifié
- Prise en charge pour IPv4 et IPv6 dans un environnement en double pile
- Déconnexion d'utilisateurs des ports
- Déconnexion forcée d'utilisateurs
- Mises à jour vers l'interface utilisateur de trap SNMP et d'agent SNMP dans KX II-101-V2

Reportez-vous aux notes de version de KX II-101-V2 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-101-V2 est accompagnée du manuel de configuration rapide KX II-101-V2, 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-101-V2 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-101-V2 sont incluses dans l'aide.

Photos du produit



KX II-101-V2

Caractéristiques du produit

Interfaces

- Connexion PS/2 KVM intégrée
- Connexion USB pour contrôle et support virtuel
- Port série Admin pour la configuration initiale du dispositif et des diagnostics, ainsi que l'utilisation avec un accès par modem externe et une gestion des barrettes d'alimentation Raritan
- Port local pour la connexion de l'écran
- Port LAN Ethernet prenant en charge une détection automatique 10/100-base-T, bidirectionnelle simultanée

Configuration réseau

- Adresse de dispositif IP DHCP ou statique

Caractéristiques du système de gestion

- Firmware susceptible d'être mis à niveau via Ethernet
- Fonctionnalité de mise à niveau de firmware sécurisée en cas de défaillance
- Horloge pouvant être réglée manuellement ou par synchronisation avec Network Time Protocol (NTP/SNTP)
- Agent SNMP V2 pour le journal d'activités de l'administrateur avec marque horaire locale, susceptible d'être désactivé par l'administrateur
- Prise en charge des protocoles d'authentification RADIUS et LDAP/LDAPS

Caractéristiques d'administration

- Gestion Web
- LDAP, Active Directory®, RADIUS ou authentification et autorisation internes
- Adressage DHCP ou IP fixe
- Intégration avec l'unité de gestion CommandCenter Secure Gateway (CC-SG) de Raritan
- Accès mobile depuis un iPad® et un iPhone® à des serveurs connectés à une unité KX II-101-V2 gérée par CC-SG
- Prise en charge de FIPS 140-2
- Prise en charge d'une bannière de sécurité de connexion
- Prise en charge de SNMPv3
- Possibilité de téléverser votre propre certificat SSL sur l'unité KX II-101-V2
- Numéros de ports TCP/IP configurables (mode Stealth)
- Prise en charge pour IPv4 et IPv6 dans un environnement en double pile
- Déconnexion d'utilisateurs des ports
- Déconnexion forcée d'utilisateurs

Caractéristiques utilisateur

- Accès Web via les navigateurs courants
- Interface utilisateur graphique intuitive
- Mode PC Share, qui permet à plusieurs utilisateurs distants de se connecter à la cible
- Communication TCP
- Interface utilisateur et aide en anglais, japonais, chinois traditionnel et chinois simplifié
- Accès aux supports virtuels
- Synchronisation absolue de la souris™
- Plug and Play
- Chiffrement 256 bits de l'ensemble du signal KVM, signal vidéo et support virtuel inclus

Alimentation

- Alimentation par un adaptateur AC/DC externe

Résolution vidéo

- Résolutions vidéo jusqu'à 1920 x 1080 à 60 Hz maximum et grand écran

Montage

- Support de fixation de montage en rack

Terminologie

Terme	Description
Serveur cible	Serveur auquel vous accédez à distance via KX II-101-V2 et sa configuration KVM connectée.
Ordinateur distant (Remote PC)	Ordinateur Windows®, Linux® ou Apple Macintosh® utilisé pour accéder aux serveurs cible connectés à KX II-101-V2 et les contrôler.
Port série Admin	Utilisez le port série Admin pour la connexion au port série du PC au moyen d'un câble DB9 mâle. Utilisez ensuite un progiciel d'émulation standard (par exemple HyperTerminal) pour accéder au port série Admin. Ce port est utilisé pour la configuration réseau.
Port Local User (Utilisateur local)	Permet à un utilisateur situé à proximité immédiate du serveur cible d'utiliser le clavier et la souris natifs sans débrancher KX II-101-V2.

Terme	Description
Support virtuel	Permet à un serveur cible KVM d'accéder, à distance, à un support depuis le PC client et les serveurs de fichiers réseau.

Contenu de l'emballage

Chaque dispositif KX II-101-V2 est fourni avec :

- KX II-101-V2 - KVM sur IP
- Câble KVM
- Adaptateur d'alimentation - AC/DC 5VDC avec adaptateur universel
- Kit de fixation de montage
- Guide de configuration rapide imprimé
- Notes de version d'application imprimées (le cas échéant)
- Notes techniques imprimées (le cas échéant)

Chapitre 2 Installation et configuration

Dans ce chapitre

Présentation	9
Données de connexion par défaut	9
Mise en route	10

Présentation

Ce chapitre décrit l'installation et la configuration de l'unité KX II-101-V2. L'installation et la configuration comprend les étapes suivantes :

- **Etape 1 : Configuration du serveur cible** (à la page 10)
- **Etape 2 : Configuration des paramètres réseau de pare-feu** (voir "**Etape 2 : Configuration des paramètres du pare-feu de réseau**" à la page 23).
- **Etape 3 : Connexion de l'équipement** (voir "**Etape 3 : Connexion de l'équipement**" à la page 24)
- **Etape 4 : Configuration du dispositif KX II-101-V2** (voir "**Etape 4 : Configuration du dispositif KX II-101-V2**" à la page 29)

Avant d'installer le dispositif KX II-101-V2, configurez le serveur cible auquel vous souhaitez accéder via KX II-101-V2 afin d'obtenir des performances optimales. Notez que les étapes de configuration suivantes s'appliquent uniquement au serveur cible, et non aux ordinateurs que vous utiliserez pour accéder au dispositif KX II-101-V2 à distance.

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-101-V2, il vous est demandé de changer le mot de passe par défaut.
IP address (Adresse IP)	KX II-101-V2 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

Si vous utilisez KX II-101-V2 avec Microsoft® Internet Explorer® version 6 ou Windows 2000®, vous devez effectuer une mise à niveau au Service Pack 4 (SP4) ou supérieur.

KX II-101-V2 est livré avec une adresse IP statique par défaut. Sur un réseau sans serveur DHCP, vous devez configurer une nouvelle adresse IP statique, un nouveau masque réseau et une nouvelle adresse de passerelle, soit en utilisant la console d'administration série de l'unité KX II-101-V2, soit la console distante de KX II-101-V2.

Reportez-vous à **Attribution d'une adresse IP** (voir "**Affectation d'une adresse IP**" à la page 30) pour plus d'informations sur l'attribution d'une adresse IP à KX II-101-V2 à l'aide de la console distante. Reportez-vous à **Configuration de KX II-101-V2 à l'aide d'un programme d'émulation de terminal (facultatif)** (à la page 35) pour en savoir plus sur le paramétrage d'une adresse IP à l'aide de la console série Admin.

Étape 1 : Configuration du serveur cible

Avant d'installer le dispositif KX II-101-V2, configurez le serveur cible auquel vous souhaitez accéder via KX II-101-V2 afin d'obtenir des performances optimales. Notez que les étapes de configuration suivantes s'appliquent uniquement au serveur cible, et non aux ordinateurs que vous utiliserez pour accéder au dispositif KX II-101-V2 à distance.

Configuration de la résolution vidéo du serveur

Afin d'optimiser l'efficacité de la bande passante et les performances vidéo, vous devez configurer un serveur cible exécutant une interface utilisateur graphique, telle que Windows®, X-Windows®, Solaris® et KDE, avec un papier peint de Bureau comportant une image unie et uniforme de couleur claire. Evitez les papiers peints représentant des photos ou avec des dégradés complexes.

Assurez-vous que la résolution vidéo et le taux de rafraîchissement du serveur sont pris en charge par l'unité KX II-101-V2, et que le signal est non entrelacé. L'unité KX II-101-V2 prend en charge ces résolutions :

Résolutions	
640 x 350 à 70Hz	1024 x 768 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
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

Résolutions	
1024 x 768 à 70	1680 x 1050 à 60Hz
1024 x 768 à 72	1920 x 1080 à 60Hz

Résolution vidéo Sun

Les systèmes Sun™ ont deux paramètres de résolution, pour la ligne de commande et pour l'interface graphique utilisateur. Pour plus d'informations sur les résolutions prises en charge par le dispositif KX II-101-V2, reportez-vous à **Configuration de la résolution vidéo du serveur** (à la page 11).

Remarque : si aucune des résolutions prises en charge ne fonctionne, vérifiez si l'écran est Multisync. Certains écrans ne fonctionnent pas avec une synchronisation H&V.

Résolution de la ligne de commande

► **Pour vérifier la résolution de la ligne de commande :**

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

► **Pour changer la résolution de la ligne de commande :**

1. Exécutez la commande suivante : `# eeprom output-device=screen:r1024x768x75` où `1024x768x75` représente une résolution quelconque prise en charge par KX II-101-V2.
2. Redémarrez l'ordinateur.

Résolution de l'interface utilisateur graphique/32 bits

► **Pour vérifier la résolution de l'interface utilisateur graphique sur des cartes 32 bits :**

1. Exécutez la commande suivante : `# /usr/sbin/pgxconfig -prconf`

► **Pour modifier la résolution de l'interface utilisateur graphique sur des cartes 32 bits :**

1. Exécutez la commande suivante : `# /usr/sbin/pgxconfig -res1024x768x75` où `1024x768x75` représente une résolution quelconque prise en charge par KX II-101-V2.
2. Redémarrez l'ordinateur.

Résolution de l'interface utilisateur graphique/64 bits

► **Pour vérifier la résolution de l'interface utilisateur graphique sur des cartes 64 bits :**

1. Exécutez la commande suivante : `# /usr/sbin/m64config -prconf`

► **Pour modifier la résolution sur des cartes 64 bits :**

1. Exécutez la commande suivante : `# /usr/sbin/m64config -res1024x768x75` où `1024x768x75` représente une résolution quelconque prise en charge par KX II-101-V2.
2. Redémarrez l'ordinateur.

Résolution de l'interface utilisateur graphique/Solaris 8

► **Pour vérifier la résolution sur Solaris™ 8 pour des cartes 32 et 64 bits :**

1. Exécutez la commande suivante : `# /usr/sbin/fbconfig -prconf`

► **Pour modifier la résolution sur Solaris 8 pour des cartes 32 et 64 bits :**

1. Exécutez la commande suivante : `# /usr/sbin/fbconfig -res1024x768x75` où `1024x768x75` représente une résolution quelconque prise en charge par KX II-101-V2.
2. Redémarrez l'ordinateur.

Paramètres de souris

Plusieurs modes de souris sont disponibles pour l'unité KX II-101-V2 : Absolute Mouse Synchronization™ (Synchronisation absolue de la souris), mode souris Intelligent et mode souris Standard.

Remarque : n'utilisez pas de souris animée en mode souris Intelligent.

Les paramètres de souris ne doivent pas être modifiés pour la synchronisation absolue de la souris. Pour les modes souris Standard ou Intelligent, les paramètres de la souris doivent être configurés sur des valeurs spécifiques décrites dans la présente section.

Les configurations de souris varient suivant les différents systèmes d'exploitation cible. Reportez-vous à la documentation de votre système d'exploitation pour de plus amples informations.

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-101-V2. Vous pourrez ainsi réserver aux connexions KX II-101-V2 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-101-V2. 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-101-V2 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-101-V2. Vous pourrez ainsi réserver aux connexions KX II-101-V2 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-101-V2. 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-101-V2 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-101-V2.
- c. Dans l'onglet Advanced (Avancé), vérifiez que le taux de rafraîchissement est pris en charge par KX II-101-V2.

Remarque : dans la plupart des environnements 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 être réglé pour être exécuté lors de la connexion.
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-101-V2.
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-101-V2 à l'aide d'un éditeur de texte.
 - c. Désactivez la fonctionnalité de bureau virtuel (non prise en charge par KX II-101-V2).
 - 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. Localisez le fichier de configuration (généralement `/etc/modules.conf`) sur le système.
2. Avec l'éditeur de votre choix, assurez-vous que la ligne alias `usb-controller` du fichier `modules.conf` est comme suit :

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

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

3. Enregistrez le fichier.
4. Redémarrez le système pour que les modifications 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 > Préférences > Mouse (Menu principal > Préférences > Souris). Pour les utilisateurs de Red Hat 4 : Choisissez Main Menu > Préférences > 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-101-V2.
 - c. Cliquez sur OK.

Remarque : dans la plupart des environnements 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.

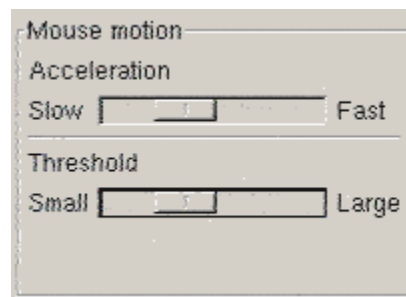
Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Paramètres Sun Solaris

Un serveur cible Solaris™ doit être configuré en utilisant l'une des résolutions d'affichage prises en charge par KX II-101-V2. Les résolutions les plus courantes sur les ordinateurs Sun™ sont :

Résolution
1024 x 768 à 60 Hz
1024 x 768 à 70 Hz
1024 x 768 à 75 Hz
1024 x 768 à 85 Hz
1280 x 1024 à 60 Hz

Définissez la valeur d'accélération du pointeur de la souris et le seuil exactement sur 1. Un serveur cible exécutant le système d'exploitation Solaris doit utiliser une sortie vidéo VGA (signaux H-Sync et V-Sync, pas à synchronisation composite). Définissez ces paramètres sur l'interface graphique utilisateur ou à l'aide de la ligne de commande `xset mouse a t` où `a` correspond à l'accélération et `t`, au seuil.



► **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 `#eeprom output-device=screen:r1024x768x75` pour modifier la résolution de sortie.
3. Lancez la commande `boot` pour redémarrer le serveur.

Vous pouvez également vous procurer un adaptateur de sortie vidéo auprès de votre représentant Raritan. Les serveurs Sun avec une sortie synchronisée de manière composite ont besoin de APSSUN II Raritan Guardian pour être utilisés avec KX II-101-V2. Les serveurs Sun HD15 avec une sortie synchronisée de manière séparée ont besoin de APKMSUN Raritan Guardian pour être utilisés avec KX II-101-V2.

Paramètres Apple Macintosh

KX II-101-V2 est prêt à l'emploi sur Mac®. Vous devez toutefois utiliser Absolute Mouse Synchronization (Synchronisation absolue de la souris) et activer le mode Absolute Mouse et le facteur d'échelle souris pour les serveurs Mac sur la page Port de KX II-101-V2.

► **Pour activer ce paramètre :**

1. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration (Configuration des ports) s'ouvre.
2. Cliquez sur le nom du port que vous souhaitez modifier.

3. Dans la section USB Connection Settings (Paramètres de connexion USB), cochez la case Enable Absolute Mouse (Activer le mode Souris absolue) et la case Enable Absolute mouse scaling for MAC server (Activer le facteur d'échelle Souris absolue pour serveur MAC). Cliquez sur OK.

Reportez-vous à **Configuration des ports** (à la page 137).

Paramètres IBM AIX

1. Accédez au Style Manager (Gestionnaire de style).
2. Cliquez sur Mouse Settings (Paramètres de souris) et réglez Mouse Acceleration (Accélération de la souris) sur 1.0 et Threshold (Seuil) sur 3.0.

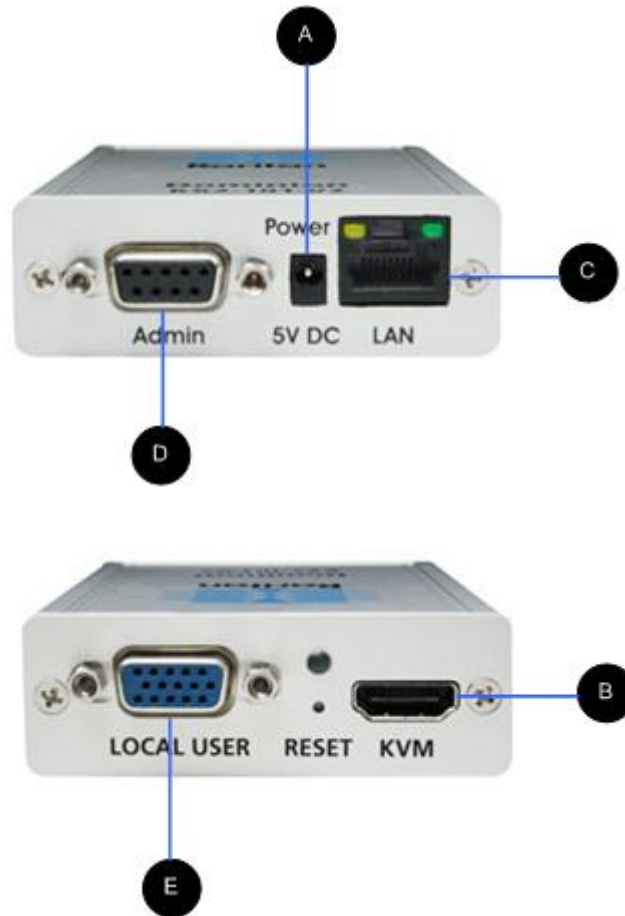
Etape 2 : Configuration des paramètres du pare-feu de réseau

Pour que vous puissiez accéder à l'unité KX II-101-V2 via un pare-feu réseau, votre pare-feu doit permettre la communication sur le port TCP 5000. Vous pouvez également configurer l'unité KX II-101-V2 de façon à ce qu'elle utilise un port TCP différent, que vous aurez déterminé.

Pour vous permettre de bénéficier des fonctionnalités d'accès Web de KX II-101-V2, le pare-feu doit autoriser les communications entrantes sur le port TCP 443, port TCP standard pour les communications HTTPS. Pour vous permettre de bénéficier de la redirection par KX II-101-V2 des requêtes HTTP vers HTTPS (afin que les utilisateurs puissent saisir `http://xxx.xxx.xxx.xxx`, comme ils en ont l'habitude, au lieu de `https://xxx.xxx.xxx.xxx`), le pare-feu doit autoriser les communications entrantes sur le port TCP 80, port TCP standard pour les communications HTTP.

Etape 3 : Connexion de l'équipement

Le dispositif KX II-101-V2 est doté des connexions physiques décrites dans le schéma ci-après : chaque lettre du schéma correspond à une étape de la procédure de connexion de l'équipement décrite ici.



Légende		
A	Connecteur d'alimentation	Adaptateur d'alimentation unique
B	Câble KVM avec écran, connecteurs PS/2 et USB (inclus)	Reliez le câble KVM fourni aux ports clavier, vidéo et souris du serveur cible.
C	LAN Ethernet	Fournit une connectivité LAN.

Légende		
D	Port Admin	Utilisez-le pour effectuer l'une des opérations suivantes : <ul style="list-style-type: none"> • Configurer et gérer le dispositif avec un programme d'émulation de terminal sur votre PC. • Configurer et gérer une barrette d'alimentation (nécessite un adaptateur, non fourni). • Connecter un modem externe pour composer le numéro dans le dispositif.
E	Utilisateur local	Le port local relie à un écran.

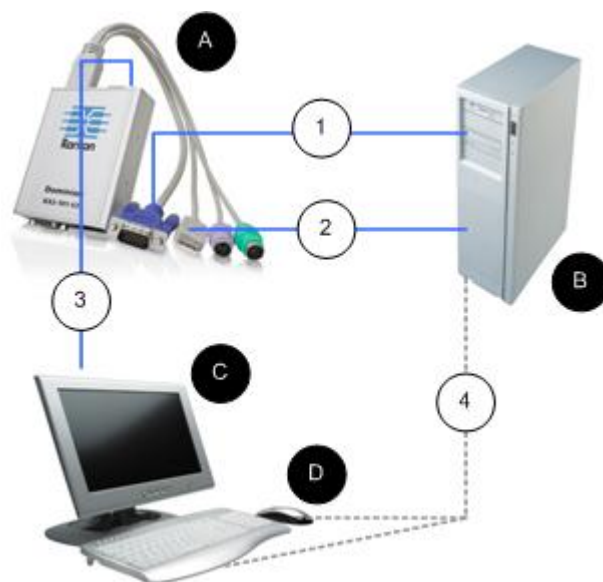
A : Alimentation

Le dispositif KX II-101-V2 est alimenté par un adaptateur d'alimentation 100-240V CA en entrée et 5VDC en sortie fourni. Pour l'alimentation CA standard, branchez le kit d'adaptateur d'alimentation CA dans le port d'alimentation, et branchez l'autre extrémité sur une prise CA proche.

B : Serveur cible

Utilisez PS/2 ou USB pour la connexion à la cible. Auparavant, définissez la configuration vidéo du serveur cible sur une résolution prise en charge. Utilisez la connexion USB si vous employez les supports virtuels ou le mode de souris Absolu.

Configuration USB



► **Pour configurer l'unité KX II-101-V2 en vue de son utilisation avec un serveur cible USB :**

1. Utilisez le câble vidéo relié pour connecter KX II-101-V2 au port vidéo cible.
2. Branchez le connecteur USB du câble KVM sur l'unité KX II-101-V2 et sur un port USB du serveur cible.
3. Connectez un écran au port pour utilisateur local de l'unité KX II-101-V2 si vous avez besoin de la vidéo locale. **Facultatif**
4. Connectez le clavier et la souris USB directement à la cible. **Facultatif**

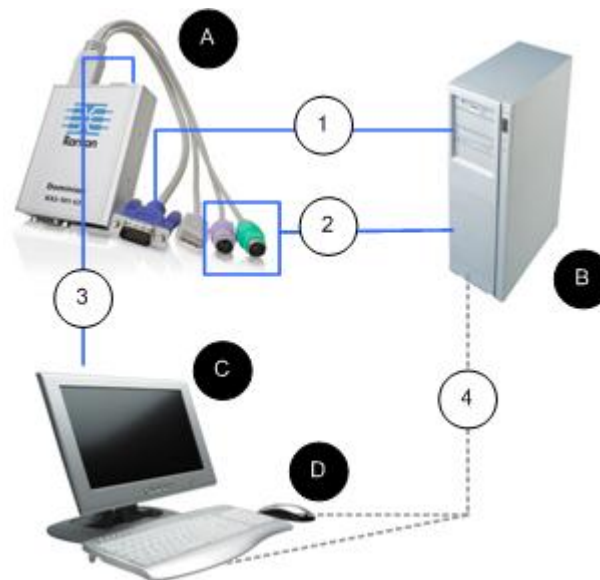
Remarque : si vous utilisez des supports virtuels, vous devez employer la connexion USB.

Légende de la connexion USB

A	KX II-101-V2
B	Serveur cible
C	Ecran local (facultatif)
D	Souris et clavier locaux (facultatif)

Légende de la connexion USB	
1	Connexion vidéo de l'unité KX II-101-V2 à la cible
2	Connexion USB de l'unité KX II-101-V2 à la cible
3	Connexion écran facultative du port utilisateur local de l'unité KX II-101-V2 à l'écran
4	Connexion USB facultative du serveur cible à la souris et au clavier (câble non fourni)









Configuration PS/2



► Pour configurer l'unité KX II-101-V2 en vue de son utilisation avec un serveur cible PS/2 :

1. Utilisez le câble vidéo relié pour connecter KX II-101-V2 au port vidéo cible.
2. Branchez le connecteur PS/2 du câble KVM au port PS/2 de la cible.
3. Connectez un écran au port pour utilisateur local de l'unité KX II-101-V2 si vous avez besoin de la vidéo locale. **Facultatif**
4. Si vous disposez d'un clavier et d'une souris PS/2, utilisez un adaptateur PS/2-USB (non fourni) pour les connecter directement au port USB de la cible. **Facultatif**

Remarque : si vous utilisez des supports virtuels, vous devez employer la connexion USB.

Légende pour les connexions PS/2	
	KX II-101-V2
	Serveur cible
	Ecran local
	Souris et clavier locaux (facultatif)
	Connexion vidéo de l'unité KX II-101-V2 à la cible
	Connexion de câble KVM de l'unité KX II-101-V2 au serveur cible
	Connexion facultative de l'unité KX II-101-V2 à l'écran
	Connexion facultative de l'adaptateur PS/2-USB (câble non fourni) de la cible au clavier et à la souris

C : Réseau

Branchez un câble Ethernet standard entre le port réseau LAN et un routeur, un concentrateur ou un commutateur Ethernet. Les voyants LAN qui apparaissent au-dessus de la connexion Ethernet indiquent une activité Ethernet. Le voyant jaune clignote lorsque le dispositif KX II-101-V2 est utilisé, indiquant ainsi un trafic IP à 10 Mbps. Le voyant vert indique une vitesse de connexion de 100 Mbps.

D : Port Admin

Le port Admin vous permet d'effectuer la configuration et le paramétrage de l'unité KX II-101-V2 à l'aide d'un programme d'émulation de terminal tel que HyperTerminal. Utilisez un câble série droit DB9M-DB9F pour la connexion de KX II-101-V2 au port série de votre PC ou de votre portable. Les paramètres de communication du port série doivent être configurés comme suit :

- 115 200 bauds
- 8 bits de données
- 1 bit d'arrêt
- Aucune parité
- Aucun contrôle de flux

E : Port d'utilisateur local

Le port Local User sert de passerelle vers la vidéo du serveur cible pour le connecter directement à l'écran. Les clavier et souris locaux doivent être connectés directement au serveur cible.

Pour les configurations USB, seul l'écran local se connecte au serveur cible via le port Local User (Utilisateur local). Le clavier et la souris se branchent directement sur les ports USB du serveur cible.

Etape 4 : Configuration du dispositif KX II-101-V2

Remarque : vous devez utiliser un câble croisé entre KX II-101-V2 et le client si vous configurez KX II-101-V2 via un navigateur Web.

Configuration de KX II-101-V2 à l'aide de la console à distance

La console distante de KX II-101-V2 est une application Web qui vous permet de configurer le dispositif avant son utilisation, et de le gérer après sa configuration. Avant de configurer le dispositif KX II-101-V2 à l'aide de la console distante, vous devez vous assurer que votre poste de travail et le dispositif sont connectés à un réseau.

Vous pouvez également utiliser un programme d'émulation de terminal afin de configurer KX II-101-V2. Reportez-vous à **Configuration de KX II-101-V2 à l'aide d'un programme d'émulation de terminal (facultatif)** (à la page 35).

Définition d'un nouveau mot de passe

La première fois que vous vous connectez à la console distante, le système vous invite à définir un nouveau mot de passe pour remplacer celui qui a été configuré par défaut. Vous pouvez ensuite configurer l'unité KX II-101-V2.

1. Connectez-vous à un poste de travail doté d'une connectivité réseau à votre dispositif KX II-101-V2.
2. Démarrez un navigateur Web pris en charge, tel que Internet Explorer® (IE) ou Firefox®.
3. Dans le champ d'adresse du navigateur, entrez l'adresse IP par défaut du dispositif : 192.168.0.192.
4. Appuyez sur Entrée. La page de connexion s'ouvre.
5. Saisissez `admin` comme nom d'utilisateur et `raritan` comme mot de passe.
6. Cliquez sur Login (Se connecter). L'écran Change Password (Modifier le mot de passe) s'affiche.
7. Dans le champ Old Password (Ancien mot de passe), saisissez `raritan`.
8. Entrez un nouveau mot de passe dans les champs New Password et Confirm New Password (Confirmer le nouveau mot de passe). Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques (caractères présents sur un clavier anglais et caractères spéciaux imprimables).
9. Cliquez sur Apply (Appliquer). Un message s'affiche pour confirmer la modification du mot de passe.
10. Cliquez sur OK. La page Port Access (Accès aux ports) s'ouvre.

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 115).

► 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-101-V2. 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-101-V2 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-101-V2.
 - 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** (voir "**LAN Interface Settings (Paramètres de l'interface LAN)**") à la page 119) 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-101-V2 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 115) pour plus d'informations.*

Désignation du serveur cible

1. Reliez KX II-101-V2 au serveur cible.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration (Configuration des ports) s'ouvre.
3. Cliquez sur le nom du port pour le serveur cible. La page Port s'ouvre.
4. Saisissez un nom contenant un maximum de 32 caractères alphanumériques et spéciaux.
5. Cliquez sur OK.

Port 1

Type:
KVM

Name:

Power Association

Power Strip Name	Outlet Name
<input style="width: 50px;" type="text" value="None"/>	<input 5px;"="" padding:="" style="width: 40px;" type="text" value="---</input></td> </tr> <tr> <td></td> <td style="/> <input 5px;"="" padding:="" style="width: 40px;" type="text" value="---</input></td> </tr> <tr> <td></td> <td style="/> <input 5px;"="" padding:="" style="width: 40px;" type="text" value="---</input></td> </tr> <tr> <td></td> <td style="/> <input #0070c0;="" 10px;="" 5px;="" background-color:="" color:="" display:="" flex;="" justify-content:="" margin-top:="" padding:="" space-between;"="" style="width: 40px;" type="text" value="---</input></td> </tr> </tbody> </table> <div style=" white;=""/> ▶ USB Connection Settings

▶ Advanced USB Connection Settings

Authentification à distance

Note aux utilisateurs de CC-SG

Lorsque le dispositif KX II-101-V2 est géré par l'unité CommandCenter Secure Gateway, celle-ci authentifie les utilisateurs et les groupes.

Pour en savoir plus sur l'authentification par CC-SG, reportez-vous aux **manuels d'utilisation et d'administration de CommandCenter Secure Gateway** ou au **guide de déploiement**, téléchargeables depuis la section Support du site Web de Raritan (www.raritan.com).

Protocoles pris en charge

Afin de simplifier la gestion des noms d'utilisateur et des mots de passe, KX II-101-V2 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-101-V2. 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-101-V2.

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-101-V2. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre KX II-101-V2. Reportez-vous à **Gestion des utilisateurs (à la page 89) pour plus d'informations sur l'ajout et la modification des groupes d'utilisateurs et des utilisateurs.**

Configuration de KX II-101-V2 à l'aide d'un programme d'émulation de terminal (facultatif)

Vous pouvez utiliser la console série Admin avec un programme d'émulation de terminal, tel que HyperTerminal, afin de définir les paramètres de configuration suivants pour l'unité KX II-101-V2 :

- IP address (Adresse IP)
- Adresse du masque de sous-réseau
- Adresse de la passerelle
- Autoconfiguration IP
- Vitesse LAN
- Mode d'interface LAN

Pour utiliser un programme d'émulation de terminal avec KX II-101-V2, vous devez d'abord brancher le câble série RS-232 fourni entre le port Admin de l'unité KX II-101-V2 et le port COM de votre PC.

Dans les exemples de cette section, nous avons utilisé le programme d'émulation de terminal HyperTerminal. Mais vous pouvez utiliser n'importe quel programme d'émulation de terminal.

► Pour utiliser un programme d'émulation de terminal afin de configurer l'unité KX II-101-V2 :

1. Reliez KX II-101-V2 à un PC local.
2. Connectez le câble au port Admin de l'unité KX II-101-V2 et au port COM1 du PC.
3. Démarrez le programme d'émulation de terminal à utiliser pour configurer l'unité KX II-101-V2.
4. Définissez les paramètres de port suivants dans le programme d'émulation de terminal :
 - Bits par seconde - 115200
 - Bits de données - 8
 - Parité - Aucune
 - Bits d'arrêt - 1
 - Contrôle de flux - Aucun
5. Connectez-vous à KX II-101-V2. La page de connexion s'ouvre.
6. Entrez le nom d'utilisateur de l'administrateur et appuyez sur Entrée. Le système vous invite à saisir votre mot de passe.
7. Entrez le nom par défaut de l'administrateur *admin* et appuyez sur Entrée. Le système vous invite à entrer votre mot de passe.
8. A l'invite Admin Port (Port Admin) >, tapez *config* et appuyez sur Entrée.

9. A l'invite Config >, tapez *network* et appuyez sur Entrée.
10. Pour configurer de nouveaux paramètres de réseau, à la suite de l'invite Network (Réseau), tapez *interface*, puis l'une des commandes suivantes et l'argument approprié (option). Appuyez sur Entrée.

Commande	Argument	Options
ipauto	none dhcp	<p>none (aucune) - Vous permet de spécifier manuellement une adresse IP pour le dispositif. Vous devez faire suivre cette option de la commande ip et de l'adresse IP, comme illustré dans l'exemple suivant :</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p>dhcp - Attribue automatiquement une adresse IP au dispositif lors du démarrage.</p> <pre>interface ipauto dhcp</pre>
ip	IP address (Adresse IP)	<p>L'adresse IP à attribuer au dispositif. Lorsque vous définissez manuellement une adresse IP pour la première fois, cette commande doit être utilisée avec la commande ipauto et l'option none (aucune). Reportez-vous à ipauto pour plus d'informations. Une fois que l'adresse IP a été attribuée une première fois, vous pouvez utiliser la commande ip seule pour changer cette adresse.</p>
mask	subnet mask (masque de sous-réseau)	<p>La colonne de commande doit être interface</p> <pre>interface ip ... interface mask Adresse IP du masque de</pre>

Commande	Argument	Options
		sous-réseau interface gw Adresse IP de la passerelle interface mode
gw	IP address (adresse IP)	L'adresse IP de la passerelle.
mode	mode	Le mode Ethernet. Vous disposez des possibilités suivantes : <ul style="list-style-type: none"> ▪ auto - Définit automatiquement la vitesse et le mode d'interface en fonction du réseau. ▪ 10hdx - 10 Mo/s, half duplex. ▪ 10fdx - 10 Mo/s, full duplex. ▪ 100hdx - 100 Mo/s, half duplex. ▪ 100fdx - 100 Mo/s, full duplex.

Une fois le paramètre modifié, un message de confirmation similaire au suivant s'affiche :

```
Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.126
Network interface configuration successful.
```

Une fois la configuration de l'unité KX II-101-V2 terminée, saisissez *logout* à la suite de l'invite de commande, puis appuyez sur Entrée. Vous êtes alors déconnecté de l'interface de ligne de commande.

Chapitre 3 Utilisation des serveurs cible

Dans ce chapitre

Interfaces	38
Virtual KVM Client (VKC).....	47

Interfaces

Interface de la console distante KX II-101-V2

La console distante de KX II-101-V2 est une interface utilisateur graphique basée sur un navigateur qui vous permet d'accéder aux serveurs cible et cibles série KVM connectés à KX II-101-V2 et d'administrer à distance KX II-101-V2.

Elle offre une connexion numérique à vos serveurs cible KVM connectés. Chaque fois que vous accédez à un serveur cible KVM à l'aide de la console distante de KX II-101-V2, une fenêtre Virtual KVM Client s'ouvre.

Remarque : si vous utilisez Internet Explorer® 7, vous pouvez rencontrer des problèmes d'autorisation lorsque vous tentez de vous connecter à un serveur cible. Pour les éviter, procédez comme suit :

1. Dans Internet Explorer, cliquez sur Outils > Options Internet pour ouvrir la boîte de dialogue Options Internet.
 2. Dans la section Fichiers Internet temporaires, cliquez sur Paramètres. La boîte de dialogue Paramètres s'ouvre.
 3. Dans la section Vérifier s'il existe une version plus récente des pages enregistrées, sélectionnez Automatiquement.
 4. Cliquez sur OK pour appliquer les paramètres.
-

Activation de l'accès direct aux ports

L'accès direct aux ports vous permet d'accéder au client distant de KX II-101-V2 sans avoir à passer par la page de connexion habituelle. Lorsque l'accès direct aux ports est activé, vous pouvez définir une URL de façon à atteindre directement la page Port Access (Accès aux ports).

► **Pour autoriser l'accès direct aux ports :**

1. Démarrez la console distante de KX II-101-V2.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Device Services (Services du dispositif). La page Device Services (Services du dispositif) s'ouvre.

3. Cochez la case Enable Direct Port Access via URL (Activer l'accès direct aux ports via URL).
4. Cliquez sur Save (Enregistrer).

► **Pour définir une URL d'accès direct à un port :**

- Définissez une URL avec l'adresse IP, le nom d'utilisateur, le mot de passe et, si nécessaire, le numéro de port de KX II-101-V2.

Le format d'une URL d'accès direct à un port est le suivant :

`https://adresse`

`IP/dpa.asp?username=nomutilisateur&password=motdepasse`

Conseil : définissez une URL d'accès direct au port une première fois, puis enregistrez-la dans votre navigateur Web comme signet afin de pouvoir la réutiliser plus facilement.

Navigation dans la console KX II-101-V2

Les interfaces de la console KX II-101-V2 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.

Panneau gauche

Le panneau gauche de l'interface KX II-101-V2 contient les informations suivantes. Notez que certaines d'entre elles sont conditionnelles, ce qui signifie qu'elles ne s'afficheront que si vous êtes un utilisateur particulier, utilisez certaines fonctions, etc. Les informations conditionnelles sont indiquées ici.

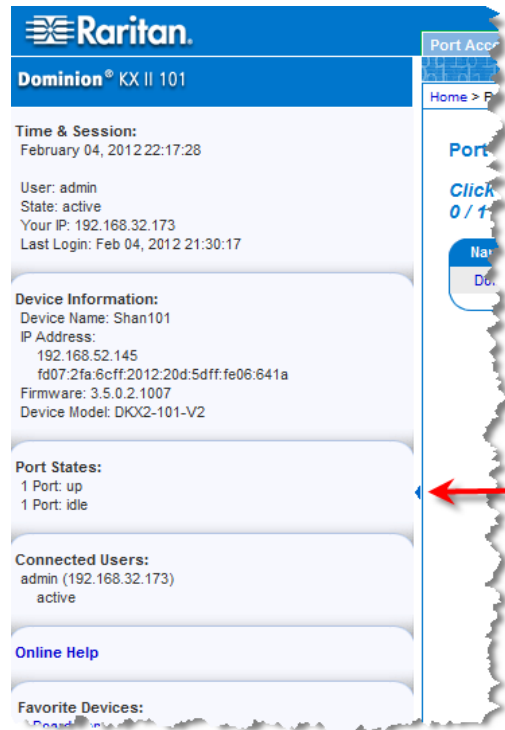
Information	Description	Affichée quand ?
Time & Session (Heure & session)	Date et heure actuelles.	Toujours
Utilisateur	Nom d'utilisateur de l'utilisateur actuel	Toujours

Information	Description	Affichée quand ?
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-101-V2.	Toujours
Last Login (Dernière connexion)	Date et heure de la dernière connexion de l'utilisateur actuel.	Toujours
Under CC-SG Management (Géré par CC-SG)	Adresse IP du dispositif CC-SG assurant la gestion de KX II-101-V2.	Quand KX II-101-V2 est géré par CC-SG
Device Information (Informations sur le dispositif)	Information spécifique au KX II-101-V2 que vous utilisez.	Toujours
Device Name (Nom du dispositif)	Nom affecté au dispositif.	Toujours
IP Address (Adresse IP)	Adresse IP du KX II-101-V2.	Toujours IPv4, et IPv6 si configuré
Firmware	Version actuelle du firmware.	Toujours
Device Model (Modèle du dispositif)	Modèle du KX II-101-V2	Toujours
Port States (Etats des ports)	Statuts du port utilisé par KX II-101-V2.	Toujours
Connect Users (Utilisateurs connectés)	Utilisateurs, identifiés par leurs nom d'utilisateur et adresse IP, actuellement connectés à KX II-101-V2.	Toujours
Aide en ligne	Liens vers l'aide en ligne.	Toujours
Favorite Devices (Dispositifs favoris)	Reportez-vous à Gestion des favoris.	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.



Page Port Access

Une fois connecté à la console distante de KX II-101-V2, la page Port Access (Accès aux ports) s'ouvre. Cette page indique le port KX II-101-V2, le serveur cible KVM connecté et sa disponibilité. La page Port Access (Accès aux ports) indique le chemin permettant d'accéder au serveur cible connecté à KX II-101-V2. Les serveurs cible KVM sont des serveurs que vous souhaitez gérer via le dispositif KX II-101-V2. Ils sont connectés aux ports de KX II-101-V2 placés à l'arrière du dispositif.

► **Pour utiliser la page Port Access :**

1. Dans la console distante de KX II-101-V2, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche. Les informations suivantes s'affichent :

- Port Name (Nom de port) - Nom du port de KX II-101-V2. Initialement, ce champ est paramétré sur Dominion_KX2_101_Port1 mais vous pouvez remplacer ce nom par un autre plus parlant. Lorsque vous cliquez sur un lien Port Name (Nom du port), le menu d'action des ports (Port Action Menu) s'affiche.
 - Availability (Disponibilité) - La disponibilité peut être Idle (Inactif), Connected (Connecté) ou Busy (Occupé).
2. Cliquez sur le nom du port du serveur cible auquel vous souhaitez accéder. Le menu d'action des ports (Port Action Menu) apparaît. Reportez-vous à **Port Action Menu (Menu d'action de ports)** (à la page 42) pour plus d'informations sur les options de menu disponibles.
 3. Sélectionnez la commande souhaitée dans le menu d'action des ports.

Port Action Menu (Menu d'action de ports)

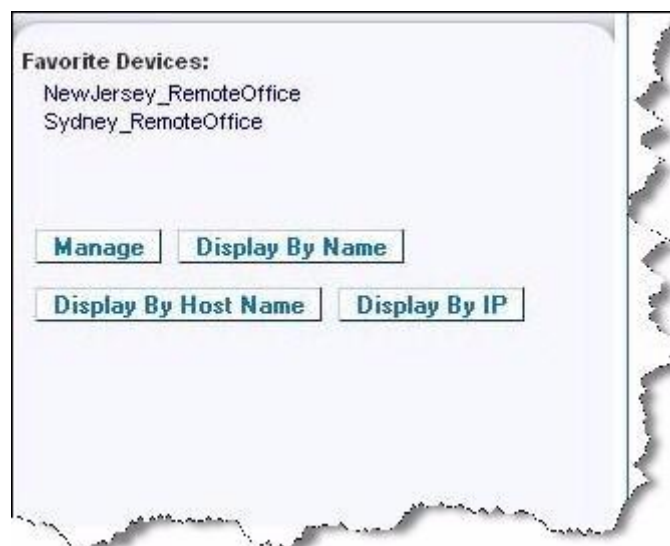
Lorsque vous cliquez sur un nom de port dans la liste Port Access, le menu d'action des ports s'affiche. Choisissez l'option de menu souhaitée pour ce port afin de l'exécuter. Notez que seules les options actuellement disponibles, suivant l'état et la disponibilité du port, sont répertoriées dans le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

- Connect (Connecter) - Crée une nouvelle connexion au serveur cible. Pour la console distante de KX II-101-V2, une nouvelle page **Virtual KVM Client (VKC)** (à la page 47) apparaît.
- 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.
- Power On (Mettre sous tension) : permet de mettre le serveur cible sous tension par l'intermédiaire de la prise associée. Cette option est visible uniquement lorsqu'il existe au moins une association d'alimentation à la cible et lorsque l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.
- Power Off (Mettre hors tension) : permet de mettre le serveur cible hors tension par l'intermédiaire des prises associées. Cette option est visible uniquement lorsqu'il existe au moins une association d'alimentation à la cible, lorsque la cible est activée (état du port actif) et lorsque l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.
- Power Cycle (Alimentation cyclique) : permet d'éteindre puis de rallumer le serveur cible par l'intermédiaire des prises associées. Cette option est visible uniquement lorsqu'il existe au moins une association d'alimentation à la cible et lorsque l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.

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-101-V2 sur le sous-réseau (avant et après la connexion) ;
 - récupérer les dispositifs KX II-101-V2 détectés à partir du dispositif Dominion connecté (après la connexion).
- **Pour accéder à un dispositif KX II-101-V2 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-101-V2 Subnet (Détecter les dispositifs - Sous-réseau de KX II-101-V2)	Détecter les dispositifs Raritan sur le sous-réseau du dispositif KX II-101-V2.
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 Raritan 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-101-V2 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 44).

► **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 Raritan sur le sous-réseau du dispositif KX II-101-V2

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-101-V2 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 44).

Cette fonction permet à plusieurs dispositifs KX II-101-V2 d'interagir et de se mettre en corrélation automatiquement. La console distante de KX II-101-V2 détecte automatiquement les dispositifs KX II-101-V2, et n'importe quel autre dispositif Raritan, sur le sous-réseau de KX II-101-V2.

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

1. Choisissez Manage (Gérer) > Discover Devices - KX II-101-V2 Subnet (Détecter les dispositifs - Sous-réseau de KX II-101-V2). La page Discover Devices - KX II-101-V2 Subnet (Détecter les dispositifs - Sous-réseau de KX II-101-V2) 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, modification et suppression 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-101-V2 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-101-V2.
 - 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-101-V2 approprié.
2. Cliquez sur Delete (Supprimer). Le favori est supprimé de la liste.

Se déconnecter

► Pour quitter KX II-101-V2 :

- 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.

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 dispositifs 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.

Virtual KVM Client (VKC)

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.

Présentation

Chaque fois que vous accédez à un serveur cible à l'aide de la console distante, une fenêtre Virtual KVM Client (VKC) s'ouvre. Il existe une fenêtre Virtual KVM Client pour le serveur cible auquel vous êtes connecté. Cette fenêtre est accessible via la barre de tâches Windows®.

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

Remarque : le rafraîchissement de votre navigateur HTML entraîne la fermeture de la connexion de Virtual KVM Client ; faites donc attention.






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.







Connexion à un serveur cible KVM



► Pour se connecter à un serveur cible KVM :

1. Dans la console distante de KX II-101-V2, cliquez sur l'onglet Port Access (Accès aux ports) pour l'ouvrir. La page Port Access s'affiche.
2. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu Port Action (Action des ports) apparaît.
3. Cliquez sur Connect (Connecter). Une fenêtre du client virtuel KVM s'ouvre pour le serveur cible connecté à ce port.

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, le lissage, 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). <hr/> <i>Remarque : non disponible dans KX II-101-V2.</i>
	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. <hr/> <i>Remarque : cette fonction est disponible sur KX</i>

Bouton	Nom du bouton	Description
		<p>II 2.4.0 (et supérieur).</p> <p>Remarque : cette fonction n'est pas prise en charge par LX. Cette fonction n'est pas prise en charge par KX II-101-V2.</p>
	Synchronize Mouse (Synchroniser la souris)	<p>En mode souris double, force le réalignement du pointeur de la souris du serveur cible sur le pointeur de la souris.</p> <p>Remarque : non disponible si le mode souris absolue est sélectionnée.</p>
	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)	<p>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.</p> <p>Remarque : Cette fonction est disponible uniquement sur KSX II 2.3.0 (et supérieur) et sur KX II 2.1.10 (et supérieur).</p> <p>Remarque : cette fonction n'est pas prise en charge par LX. Cette fonction n'est pas prise en charge par KX II-101-V2.</p>
	Send Ctrl+Alt+Del (Envoyer Ctrl+Alt+Suppr)	Envoie la combinaison de touches de raccourci Ctrl+Alt+Suppr au serveur cible.
	Single Cursor Mode (Mode curseur simple)	<p>Démarre le mode curseur simple par lequel le pointeur de souris locale n'apparaît plus à l'écran.</p> <p>Pour quitter ce mode, appuyez sur CTRL+ALT+O.</p>

Bouton	Nom du bouton	Description
	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.

Gestion de l'alimentation d'un serveur cible

Remarque : ces fonctions sont disponibles uniquement si vous avez effectué des associations d'alimentation.

► **Pour effectuer l'alimentation cyclique d'un serveur cible KVM :**

1. Dans la console distante de KX II-101-V2, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.
2. Cliquez sur le nom du port du serveur cible souhaité. Le menu Port Action (Action des ports) apparaît.
3. Choisissez Power Cycle (Alimentation cyclique). Un message de confirmation apparaît.

► **Pour mettre sous tension un serveur cible :**

1. Dans la console distante de KX II-101-V2, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.
2. Cliquez sur le nom du port du serveur cible souhaité. Le menu Port Action (Action des ports) apparaît.
3. Choisissez Power On (Mettre sous tension). Un message de confirmation apparaît.

► **Pour mettre un serveur cible hors tension :**

1. Dans la console distante de KX II-101-V2, cliquez sur l'onglet Port Access (Accès aux ports) pour l'ouvrir. La page Port Access s'affiche.
2. Cliquez sur le nom du port du serveur cible souhaité. Le menu Port Action (Action des ports) apparaît.
3. Choisissez Power Off (Mettre hors tension). Un message de confirmation apparaît.

Déconnexion des serveurs cible KVM

► 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).


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

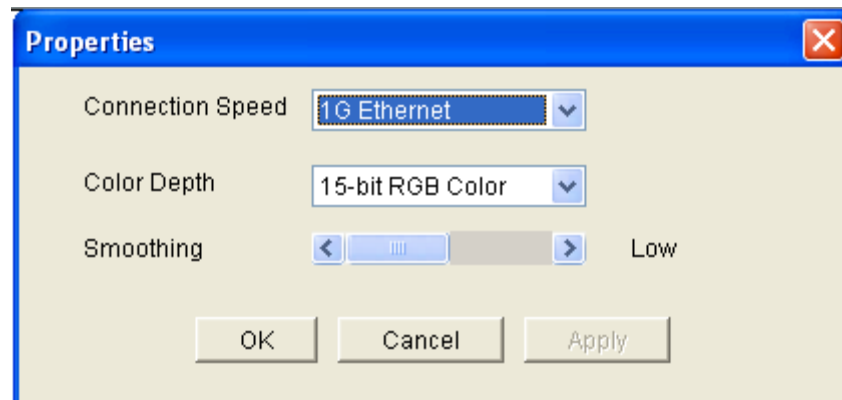
Connection Properties (Propriétés de la connexion)

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 (Informations). La fenêtre Connection Info (Informations sur la connexion) s'ouvre.

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

- Device Name (Nom de dispositif) - Nom du dispositif.
- IP Address (Adresse IP) - Adresse IP du dispositif.
- Port - Port TCP/IP de communication KVM utilisé pour l'accès au dispositif cible.
- Data In/Second (Entrée de données/seconde) - Débit en entrée.
- Data Out/Second (Sortie de données/seconde) - Débit en sortie.
- Connect Time (Temps de connexion) - Durée de connexion.
- FPS - Images par seconde transmises pour la vidéo.
- Horizontal Resolution - Résolution d'écran horizontale.
- Vertical Resolution - Résolution d'écran verticale.
- Refresh Rate (Taux de rafraîchissement) - Fréquence à laquelle l'écran est actualisé.
- Protocol Version (Version du protocole) - Version du protocole RFB.

► **Pour copier ces informations :**

- Cliquez sur Copy to Clipboard (Copier dans Presse-papiers). Ces informations peuvent maintenant être collées 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 :

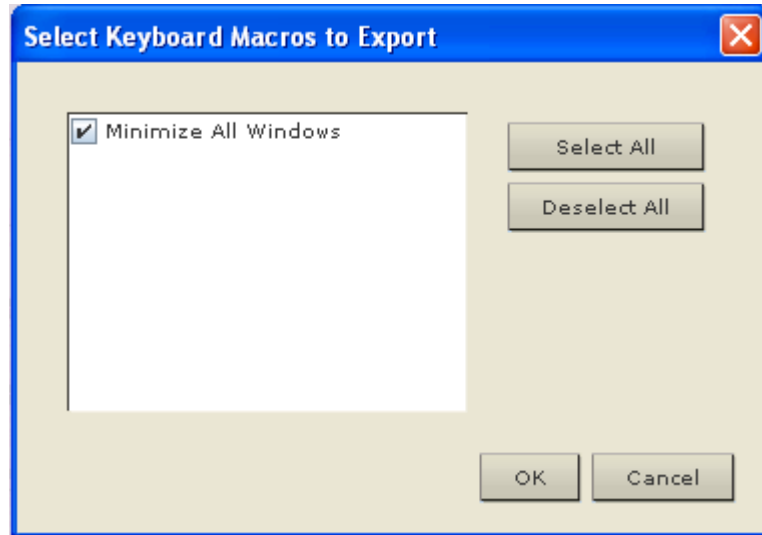
1. Choisissez Keyboard > Import Keyboard Macros (Clavier > Importer des macros de clavier) pour ouvrir la boîte de dialogue Import Macros (Importation de macros). Accédez à l'emplacement du dossier du fichier de macro.
2. Cliquez sur le fichier de macro et cliquez sur Ouvrir pour importer la macro.
 - 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.

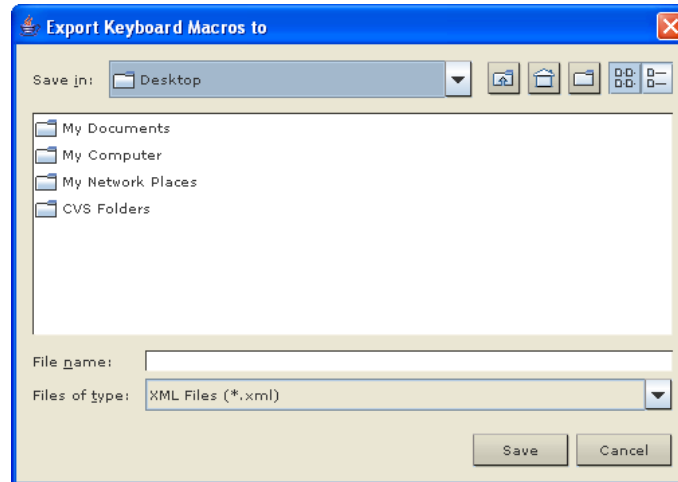
► **Pour exporter des macros :**

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 Export Keyboard Macros to (Exporter les macros clavier vers) s'affiche. Recherchez et sélectionnez 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.

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 :

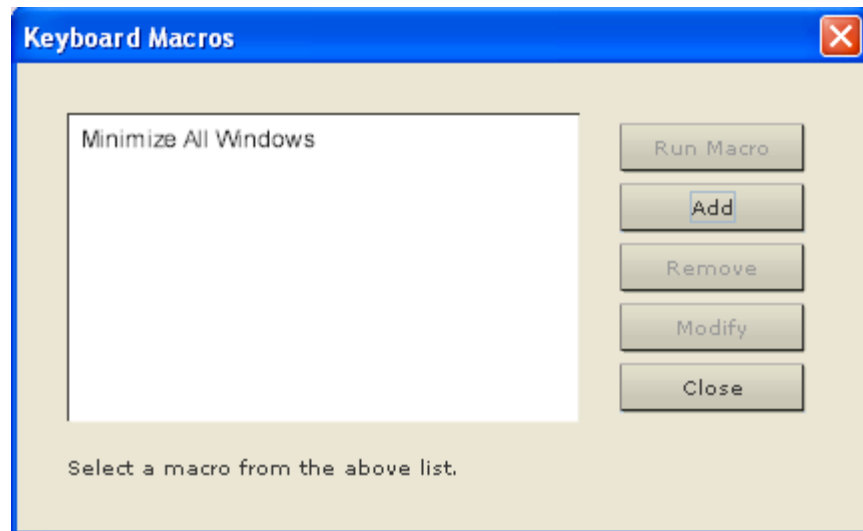
Press Left Alt (Appuyer sur Alt gauche)

Press F4 (Appuyer sur F4)

Release F4 (Relâcher F4)

Release Left Alt (Relâcher Alt gauche)

6. 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.
7. Cliquez sur OK pour enregistrer la macro. Cliquez sur Clear (Effacer) pour effacer le contenu des champs et recommencer. Si vous cliquez sur OK, la fenêtre Keyboard Macros (Macros de clavier) s'affiche et présente la nouvelle macro de clavier.
8. 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.



► **Pour utiliser la fonction Send Text to Target (Envoyer un texte à la cible) pour la macro :**

1. Cliquez sur Keyboard (Clavier) > Sent Text to Target (Envoyer un texte à la cible). La boîte de dialogue correspondante s'ouvre.
2. Entrez le texte à envoyer à la cible.

Remarque : les caractères non utilisés en anglais ne sont pas pris en charge par la fonction Send Text to Target (Envoyer un texte à la cible).

3. Si la cible utilise une configuration de clavier E.U./International, cochez la case Target system is set to the US/International keyboard layout (Le système cible utilise la configuration de clavier E.U./International).
4. Cliquez sur OK.

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.

Les combinaisons de touches qui coïncident avec les séquences de touches de commutation de châssis de lames ne sont pas envoyées aux lames hébergées par ces châssis.

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.

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.

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.

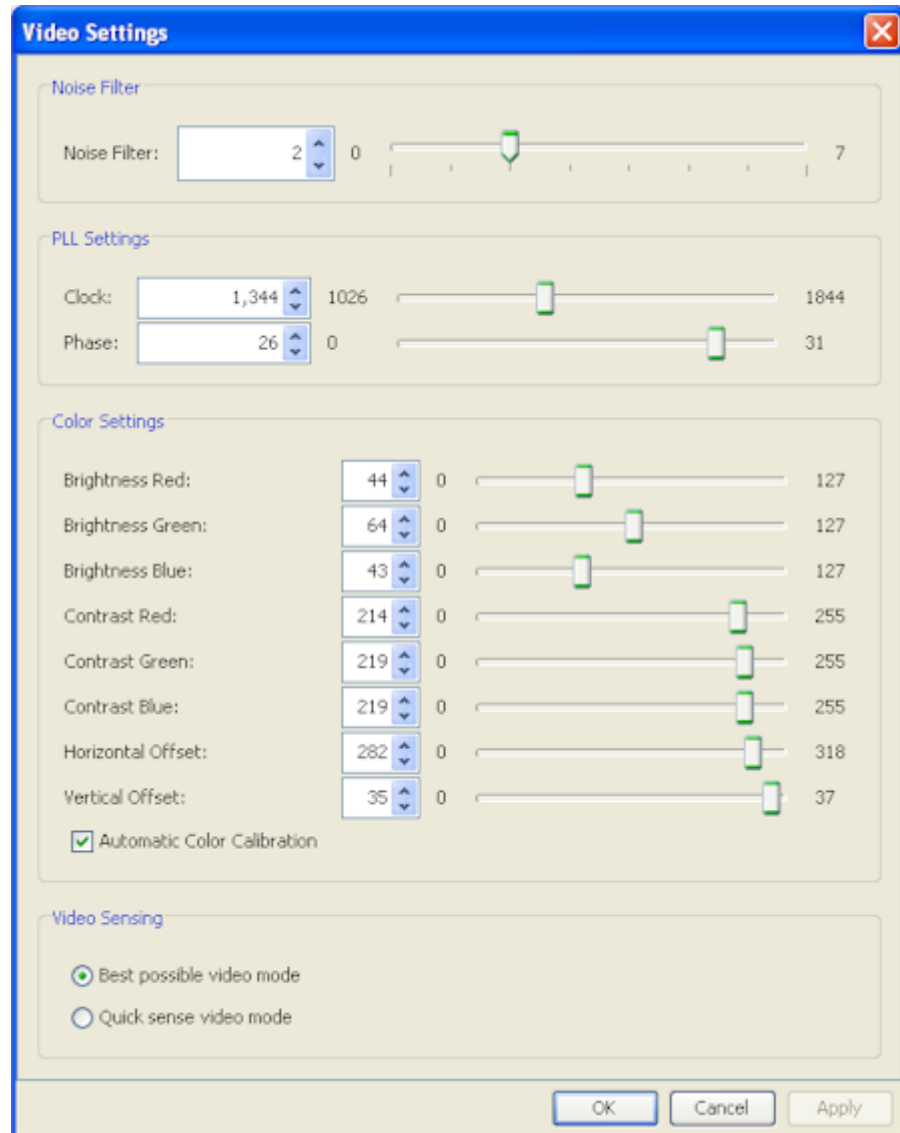
- i. Contrast Blue : contrôle le signal bleu.

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.

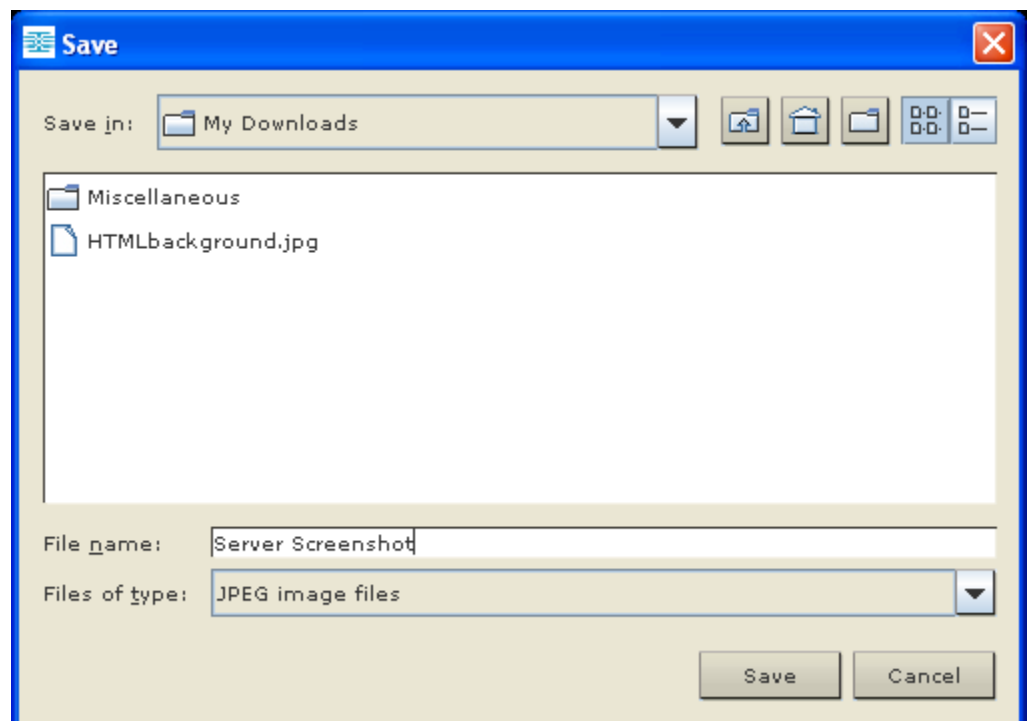


Utilisation de la commande Screenshot from Target

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 : le paramètre de souris absolue nécessite un système cible USB. Il est recommandé pour KX II-101.

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).

Supports virtuels VKC

Reportez-vous au chapitre sur les **supports virtuels** (voir "**Support virtuel**" à la page 77) pour obtenir des informations complètes sur la configuration et l'utilisation des supports virtuels.

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
- Français (France)
- Allemand (Allemagne)
- Japonais
- Royaume-Uni
- Coréen (Corée)
- Belge (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)

Langue/clavier	Méthode de configuration
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
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

La configuration des paramètres de lancement client vous permet de définir les paramètres d'écran pour une session KVM.

Remarque : les dispositifs LX prennent en charge cette fonction dans MPC. LX ne prend pas en charge le paramètre de lancement du client dans VKC et AKC.

► 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 (Épingler 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 et LX fournissent 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 pour plus d'informations. Reportez-vous à Balayage des ports. 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 70).

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 (Épingler 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 70).

► 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.

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).

Chapitre 4 Support virtuel

Dans ce chapitre

Présentation	78
Utilisation des supports virtuels	85
Connexion aux supports virtuels	86
Déconnexion des supports virtuels	88

Présentation

Les supports virtuels étendent les fonctionnalités KVM en permettant aux serveurs cible KVM d'accéder à distance à des supports à partir du PC client et des serveurs de fichiers réseau. Grâce à cette fonction, les supports installés sur le PC client et sur les serveurs de fichiers réseau sont au fond installés virtuellement sur le serveur cible. Le serveur cible peut ensuite lire et écrire sur ces supports comme s'ils étaient physiquement connectés au serveur cible lui-même. Les supports virtuels peuvent inclure des lecteurs CD/DVD USB et internes, des dispositifs de stockage de masse USB, des disques durs et des lecteurs de disquette, ainsi que des images ISO (images disque).

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

- Transférer des fichiers.
- Réaliser des diagnostics.
- Installer ou corriger des applications.
- Installer complètement le système d'exploitation (s'il est pris en charge par le BIOS).
- Ce contrôle KVM étendu élimine la plupart des consultations du centre de données, ce qui vous permet d'économiser du temps et de l'argent.

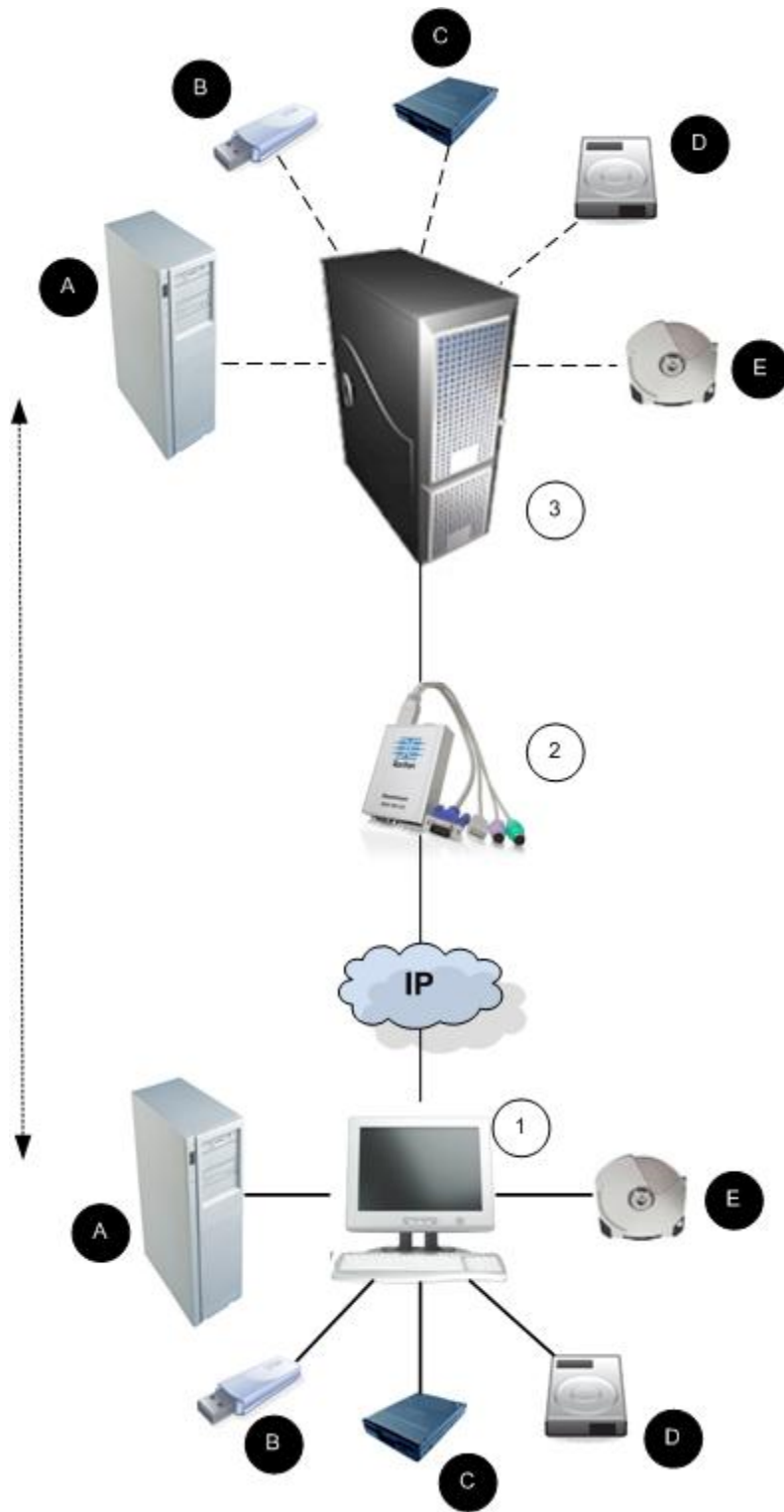
Les types de supports virtuels sont pris en charge pour les clients Windows®, Mac® et Linux™ :

- 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 :

- Windows
- 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



Remarque : si vous utilisez des supports virtuels, vous devez employer la connexion USB.

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 Virtual KVM Client est exécuté 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.

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
> 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

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 monter des 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 80) 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).

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 (Connecter le lecteur)
Lecteurs de CD/DVD locaux	Connect CD-ROM/ISO Image (Connecter l'image ISO/CD-ROM)
Images ISO	Connect CD-ROM/ISO Image (Connecter l'image ISO/CD-ROM)
Images ISO de serveur de fichiers	Connect CD-ROM/ISO Image (Connecter l'image ISO/CD-ROM)

Une fois vos tâches terminées, déconnectez le support virtuel.
Reportez-vous à **Déconnexion des supports virtuels** (à la page 88).

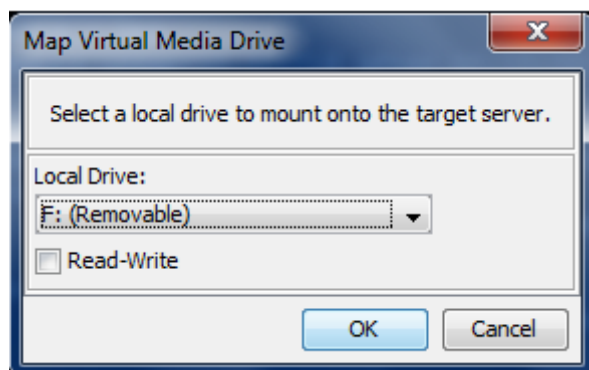
Connexion aux supports virtuels

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.

► **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 84) 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 OK. 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 5 Gestion des utilisateurs

Dans ce chapitre

Groupes d'utilisateurs	89
Utilisateurs	96
Paramètres d'authentification	101
Modification d'un mot de passe	114

Groupes d'utilisateurs

Tous les dispositifs KX II-101-V2 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-101-V2.

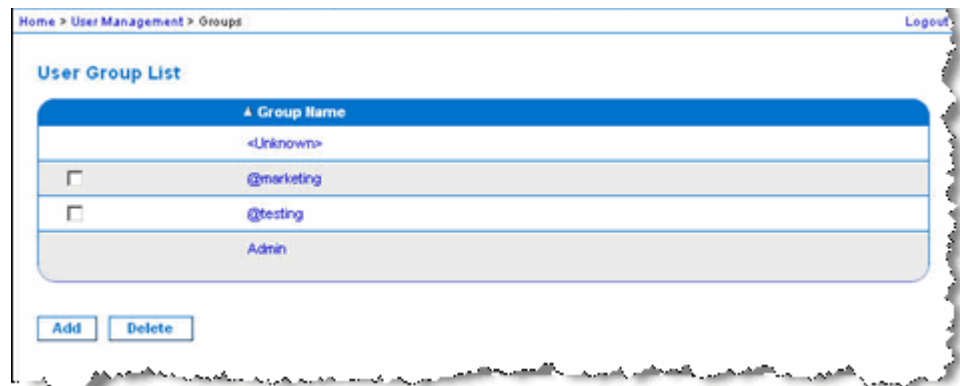
Liste des groupes d'utilisateurs

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-101-V2 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 94).

Définition 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.

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	Accès total (en lecture, en écriture) au support virtuel.

VM access (Accès au support virtuel)	
(Lecture-écriture)	
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

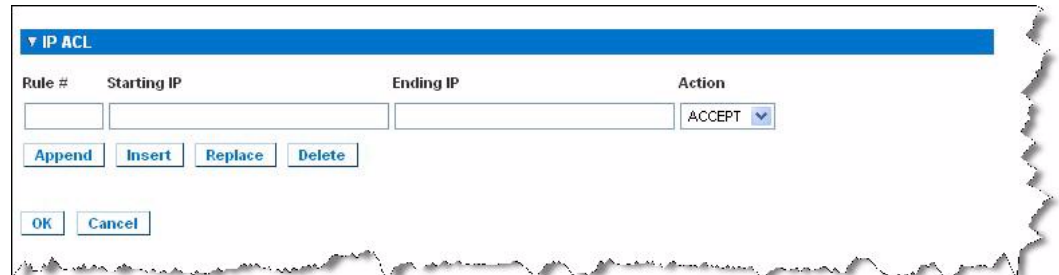
LCA (liste de contrôle d'accès) IP de groupes

Important : soyez prudent lorsque vous utilisez le contrôle d'accès IP applicable à des groupes. L'accès à KX II-101-V2 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-101-V2 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-101-V2 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-101-V2.
 - Drop - Les adresses IP paramétrées sur Drop ne sont pas autorisées à accéder au dispositif KX II-101-V2.
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.

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)	<p>Permet aux utilisateurs et aux groupes d'utilisateurs ayant cette autorisation d'accéder directement à KX II-101-V2 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 distante, de MPC, de VKC et d'AKC.</p> <p>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-101-V2. L'authentification de l'utilisateur est effectuée suivant les paramètres d'authentification de KX II-101-V2.</p> <p><i>Remarque : le groupe d'utilisateurs Admin dispose de cette autorisation par défaut.</i></p>
Device Settings (Paramètres du dispositif)	Paramètres réseau, paramètres date/heure, configuration des ports (nom de canal, association d'alimentation), gestion des événements (SNMP, Syslog), configuration du serveur de fichiers du 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-101-V2

Autorisation	Description
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-101-V2.
PC-Share	Accès simultané à la même cible par plusieurs utilisateurs
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

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.

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 (autorisations) 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 94).

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** (voir "**Définition des autorisations d'accès aux ports**" à la page 91).
4. Configurez la liste de contrôle d'accès IP (IP ACL) (facultatif). Cette fonction limite l'accès au dispositif KX II-101-V2 par le biais de la spécification d'adresses IP. Reportez-vous à **LCA (liste de contrôle d'accès) IP de groupes** (à la page 92).
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-101-V2. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité KX II-101-V2.

Affichage de la liste des utilisateurs de KX II-101-V2

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.

Pour afficher les ports auxquels chaque utilisateur est connecté, reportez-vous à Affichage des utilisateurs par port.

► 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.

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 Name - 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-101-V2 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-101-V2.

*Remarque : la fermeture de session déconnecte l'utilisateur du port cible et de KX II-101-V2. Reportez-vous à **Fermeture de la session des utilisateurs de KX II-101-V2 (Déconnexion forcée)** (à la page 98) 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-101-V2 (Déconnexion forcée)

Si vous êtes administrateur, vous pouvez fermer la session d'un autre utilisateur authentifié localement qui est connecté à KX II-101-V2. Les utilisateurs peuvent également être déconnectés au niveau du port. Reportez-vous à **Déconnexion d'utilisateurs des ports** (à la page 98).

► **Pour fermer la session d'un utilisateur de KX II-101-V2 :**

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-101-V2, 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**.

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 154).*

► 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 95).

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 99) 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.

Blocage et déblocage des utilisateurs

L'accès d'un utilisateur au système peut être bloqué par l'administrateur ou bloqué automatiquement en fonction des paramètres de sécurité. Reportez-vous à **Blocage des utilisateurs** (à la page 157). Un utilisateur bloqué devient inactif et peut être débloqué par l'administrateur, qui a la possibilité de le rendre actif à nouveau.

► **Pour bloquer ou débloquer un utilisateur :**

1. Sélectionnez User Management (Gestion des utilisateurs) > User List (Liste des utilisateurs). La page User List (Liste des utilisateurs) s'ouvre :
2. Cochez ou décochez la case Active (Actif).
 - Si cette case est cochée, l'utilisateur devient actif et peut accéder à l'unité KX II-101-V2.
 - Si cette case est décochée, l'utilisateur devient inactif et ne peut pas accéder à l'unité KX II-101-V2.
3. Cliquez sur OK. L'état actif de l'utilisateur est mis à jour.

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-101-V2 est configuré pour l'authentification à distance, le serveur d'authentification externe est utilisé principalement à des fins d'authentification et non d'autorisation.

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) est 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).

Authentication Settings

Local Authentication

LDAP

RADIUS

LDAP

Server Configuration

Primary LDAP Server
192.168.59.187

Secondary LDAP Server (optional)
192.168.51.214

Type of External LDAP Server
Microsoft Active Directory

Active Directory Domain
testradius.com

User Search DN
cn=users,dc=testradius,dc=com

DN of Administrative User (optional)
cn=Administrator,cn=users,dc=testrac

Secret Phrase of Administrative User
••••••••

Confirm Secret Phrase

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-101-V2 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-101-V2 pour que ce nouveau certificat prenne effet.

LDAP / Secure LDAP

Enable Secure LDAP

Port

Secure LDAP Port

Enable LDAPS Server Certificate Validation

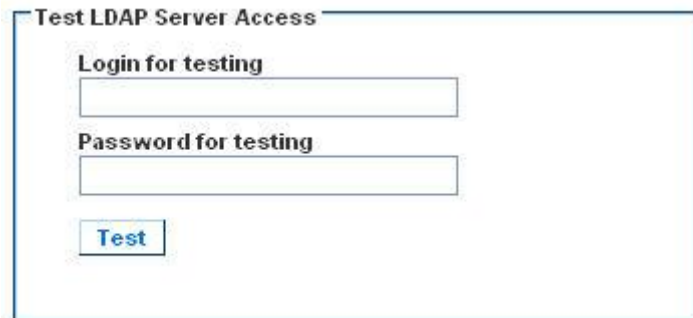
Root CA Certificate File

Note: Reboot device after certificate file is uploaded.

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

17. KX II-101-V2 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-101-V2 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-101-V2 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.



The screenshot shows a web form titled "Test LDAP Server Access". It contains two text input fields. The first is labeled "Login for testing" and the second is labeled "Password for testing". Below these fields is a blue button labeled "Test".

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

KX II-101-V2 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-101-V2. 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-101-V2 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-101-V2 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.

► **Pour activer le serveur AD sur KX II-101-V2 :**

1. A l'aide de KX II-101-V2, 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-101-V2 aux groupes créés au cours de l'étape 2.
4. A partir de KX II-101-V2, activez et configurez le serveur AD comme il se doit. Reportez-vous à **Implémentation de l'authentification à distance LDAP/LDAPS** (à la page 102).


Remarques importantes :

- Le nom de groupe est sensible à la casse.
- KX II-101-V2 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-101-V2, ce dernier attribue automatiquement le groupe <Unknown> (Inconnu) aux utilisateurs qui ont réussi à s'authentifier.

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-101-V2 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-101-V2 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-101-V2 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.

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
 LDAP
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type
 ▼

Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS

Lorsqu'une demande d'authentification RADIUS est acceptée, KX II-101-V2 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.

Spécifications des échanges de communication RADIUS

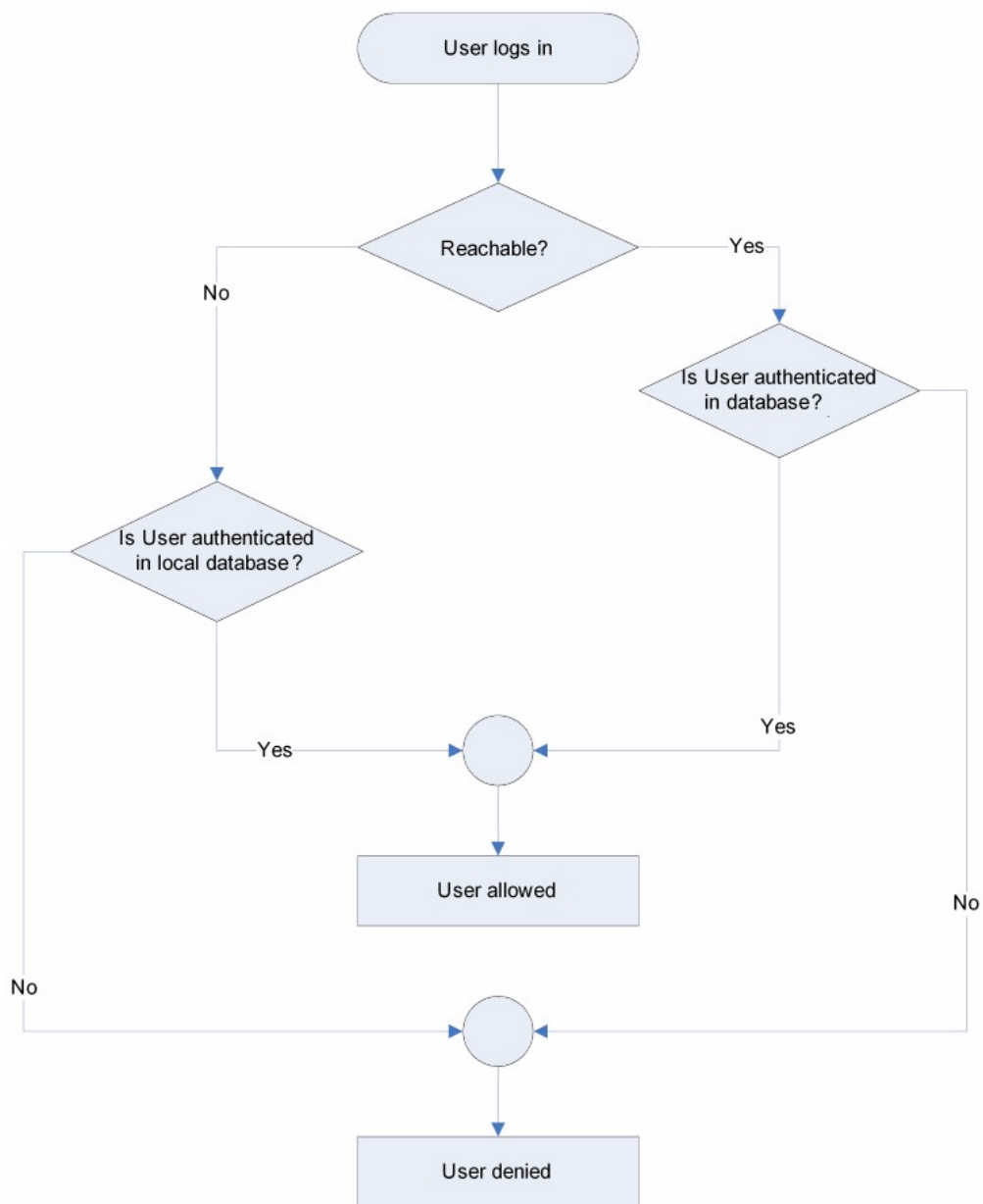
KX II-101-V2 envoie les attributs RADIUS suivants à votre serveur RADIUS :

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-101-V2.
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-101-V2.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.
Déconnexion	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Met fin à la gestion.

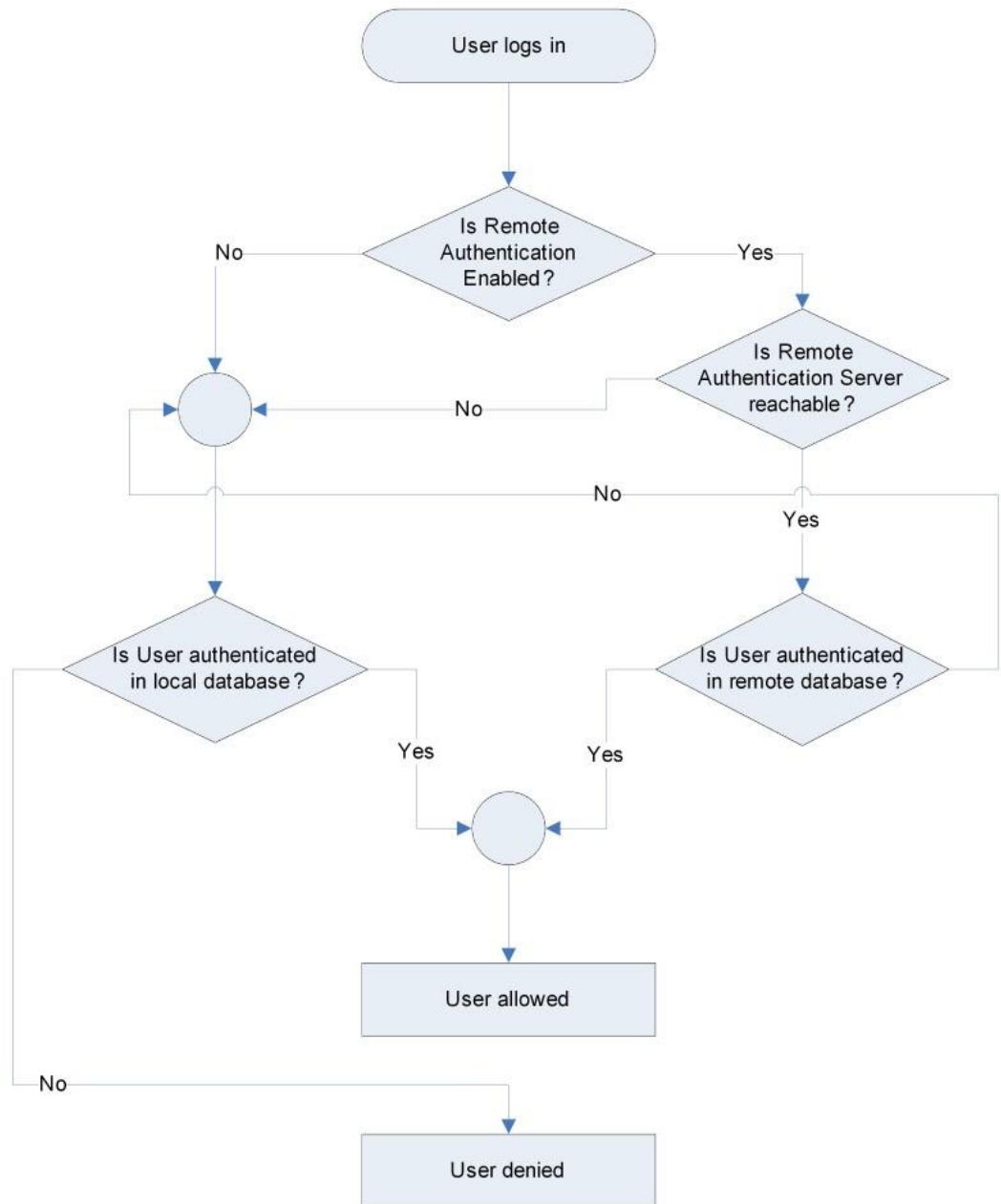
Attribut	Données
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0.
NAS-IP-Address (4)	Adresse IP de KX II-101-V2.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Processus d'authentification d'utilisateur

Lorsque le dispositif est configuré pour authentifier et autoriser les utilisateurs locaux, l'ordre de validation des informations d'identification de l'utilisateur suit le processus suivant :



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 156).*

The screenshot shows a web application interface for changing a password. At the top, there is a breadcrumb trail: "Home > User Management > Change Password". Below this is a blue header bar with the text "Change Password". The form contains three input fields: "Old Password", "New Password", and "Confirm New Password". At the bottom of the form, there are two buttons: "OK" and "Cancel".

Chapitre 6 Gestion des dispositifs

Dans ce chapitre

Paramètres réseau	115
Services du dispositif	120
Configuration du clavier/de la souris	125
Paramètres de port série	125
Configuration des paramètres de date et heure	128
Gestion des événements	128
Configuration des ports	137
Commutateur KVM analogique	145
Réinitialisation de KX II-101-V2 à l'aide du bouton de réinitialisation ...	147
Modification du paramètre de langue de l'interface utilisateur par défaut	148

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-101-V2.

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-101-V2 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 116).
3. Mettez à jour les paramètres relatifs à l'interface LAN. Reportez-vous à **Paramètres de l'interface LAN** (voir "**LAN Interface Settings (Paramètres de l'interface LAN)**" à la page 119).
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 115).

► 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-101-V2. 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-101-V2 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-101-V2.
 - 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** (voir "**LAN Interface Settings (Paramètres de l'interface LAN)**" à la page 119) 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-101-V2 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 115) pour plus d'informations.*

Basic Network Settings

Device Name *
se-kx2-232

IPv4 Address

IP Address	Subnet Mask
192.168.51.55	255.255.255.0
Default Gateway	Preferred DHCP Host Name
192.168.51.126	

IP Auto Configuration
DHCP

IPv6 Address

Global Unique IP Address	Prefix Length
Gateway IP Address	
Link-Local IP Address	Zone ID
N/A	%1

IP Auto Configuration
None

Obtain DNS Server Address Automatically

Use the Following DNS Server Addresses

Primary DNS Server IP Address
192.168.59.2
Secondary DNS Server IP Address
192.168.51.10

OK Reset To Defaults Cancel

LAN Interface Settings (Paramètres de l'interface LAN)

Les paramètres actuels de l'interface LAN sont identifiés dans le champ Current LAN interface parameters (Paramètres actuels de l'interface LAN).

- Sélectionnez les paramètres LAN Interface Speed & Duplex (Vitesse de l'interface LAN & Duplex).
 - Autodetect (Détection automatique) (option par défaut)
 - 10 Mbps/Half : le voyant jaune clignote.
 - 10 Mbps/Full : le voyant jaune clignote.
 - 100 Mbps/Half : le voyant jaune clignote et le voyant vert reste allumé.
 - 100 Mbps/Full : le voyant jaune clignote et le voyant vert reste allumé.

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 Mbit/s en half duplex ou en full duplex. Si vous rencontrez des problèmes, veuillez sélectionner une autre vitesse et un autre duplex.

Reportez-vous à **Paramètres de vitesse réseau** (à la page 211).

- Sélectionnez la limite de bande passante.
 - No Limit (Aucune limite)
 - 128 kilobits
 - 256 kilobits
 - 512 kilobits
 - 2 mégabits
 - 5 mégabits
 - 10 mégabits
 - 100 mégabits

NEED NEW SCREENSHOT

Services du dispositif

La page Device Services vous autorise à configurer les fonctions suivantes :

- Activer l'accès SSH
- Entrer le port de détection.
- Activer l'accès direct aux ports
- Activer l'accès Telnet
- Configurer les paramètres HTTP et HTTPS
- Configuration des agents SNMP

Activation de Telnet

Si vous souhaitez utiliser Telnet pour accéder à KX II-101-V2, accédez-y d'abord depuis la CLI ou un navigateur.

► **Pour activer Telnet :**

1. Sélectionnez Device Settings > Device Services (Paramètres du dispositif > Services du dispositif), puis cochez la case Enable TELNET Access (Activer l'accès TELNET).
2. Entrez le port Telnet.
3. Cliquez sur OK.

Une fois l'accès Telnet activé, vous pouvez l'utiliser pour accéder à KX II-101-V2 et configurer les paramètres restants.

Activation de SSH

Activez l'accès SSH pour permettre aux administrateurs d'accéder à KX II-101-V2 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-101-V2. 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-101-V2 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-101-V2 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.

Activation de l'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`

► Pour autoriser 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.

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-101-V2** (à la page 135) pour plus d'informations sur la consultation du MIB de KX II-101-V2.

KX II-101-V2 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.

► 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.

Configurez des traps SNMP dans la page Event Management - Settings (Gestion des événements - Paramètres), accessible rapidement en cliquant sur le lien SNMP Trap Configuration (Configuration des traps SNMP). Reportez-vous à Configuration des traps SNMP pour obtenir des informations sur la création des traps SNMP et Liste des traps SNMP de KX II-101-V2 pour obtenir la liste des traps SNMP de KX II-101-V2 disponibles.

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.

SNMP Agent Configuration

Enable SNMP Daemon

System Name: DominionKX System Contact: System Location:

Enable SNMP v1/v2c;

Community: Community Type: Read-Only

Enable SNMP v3 Use Auth Passphrase

Security Name	Auth Protocol	Auth Passphrase	Privacy Protocol	Privacy Passphrase
	MD5		None	

[Link to SNMP Trap Configuration](#)

OK Reset To Defaults Cancel

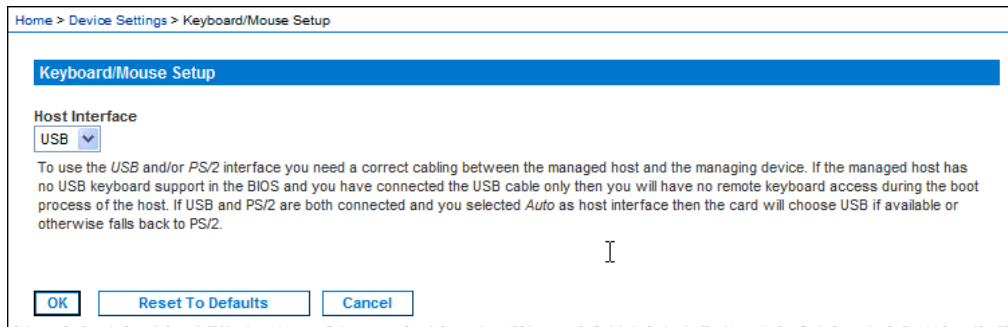
► **Pour réinitialiser les valeurs par défaut usine :**

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut). Tous les éléments de la page récupèrent leurs valeurs par défaut.

AVERTISSEMENT : lorsque vous utilisez les traps SNMP sur UDP, il est possible que l'unité KX II-101-V2 et le routeur auquel elle est reliée se désynchronisent au moment où KX II-101-V2 redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Configuration du clavier/de la souris

La page Keyboard/Mouse Setup (Configuration du clavier/de la souris) permet de configurer l'interface du clavier et de la souris entre KX II-101-V2 et le dispositif hôte.



1. Cliquez sur Device Settings > Keyboard/Mouse (Paramètres du dispositif > Clavier/Souris).
2. Sélectionnez l'interface hôte. Cette sélection détermine si KX II-101-V2 envoie les données de clavier et de souris via les connexions PS/2 ou USB.
 - Auto : avec ce paramètre, KX II-101-V2 utilisera une connexion USB, si elle est disponible, ou PS/2, dans le cas contraire.
 - USB : oblige KX II-101-V2 à utiliser la connexion USB pour envoyer les données de clavier et de souris au dispositif hôte.
 - PS/2 : oblige KX II-101-V2 à utiliser la connexion PS/2 pour envoyer les données de clavier et de souris au dispositif hôte.

*Remarque : si vous utilisez un commutateur Raritan frontal avec KX II-101-V2, vous devez définir l'interface hôte sur PS/2 pour que la configuration fonctionne correctement. Reportez-vous à **Commutateur KVM analogique** (à la page 145).*

3. Cliquez sur OK.
 - ▶ **Pour restaurer les paramètres d'usine par défaut :**
 - Cliquez sur Reset to Defaults (Restaurer les paramètres par défaut).

Paramètres de port série

La page Serial Port Settings (Paramètres de port série) permet de configurer l'utilisation du port série intégré par KX II-101-V2.

Port Admin

► **Pour configurer le port série admin :**

1. Sélectionnez Device Settings (Paramètres du dispositif) > Serial Port (Port série). La page Serial Port Settings (Paramètres du port série) apparaît.
2. Sélectionnez le bouton radio Admin Port (Port Admin).
3. Choisissez une de ces options pour vous connecter à KX II-101-V2 directement depuis un PC client et accéder à l'interface de ligne de commande au moyen d'un programme comme Hyperterminal. Reportez-vous à **Interface de ligne de commande (CLI)** (à la page 190).
4. Dans la section Serial Settings (Paramètres série), configurez les champs suivants :
 - Speed (Vitesse)
 - Stop bits (Bits d'arrêt)
 - Data bits (Bits de données)
 - Handshake (Etablissement de liaison)
 - Parity (Parité)
5. Cliquez sur OK.

Gestion des barrettes d'alimentation Raritan

► **Pour configurer le port série de barrette d'alimentation :**

1. Sélectionnez Device Settings (Paramètres du dispositif) > Serial Port (Port série). La page Serial Port Settings (Paramètres du port série) s'ouvre.
2. Sélectionnez la case d'option PowerStrip Control (Gestion de la barrette d'alimentation). Sélectionnez cette option lorsque vous connectez KX II-101-V2 à une barrette d'alimentation Raritan.
3. Cliquez sur OK.

Modem

► **Pour configurer le port série de modem :**

1. Sélectionnez Device Settings (Paramètres du dispositif) > Serial Port (Port série). La page Serial Port Settings (Paramètres du port série) s'ouvre.
2. Sélectionnez le bouton radio Modem. Sélectionnez cette option lorsque vous reliez un modem externe à KX II-101-V2 afin de disposer d'un accès par liaison commutée.

3. Dans la section Modem Settings (Paramètres de modem), configurez les champs suivants :
 - Serial line speed (Vitesse de la ligne série)
 - Modem init string (Chaîne d'initialisation du modem) - La chaîne par défaut affichée dans le champ doit être utilisée pour activer l'accès par modem.
 - Modem server IP address (Adresse IP du serveur de modem) - Adresse entrée par l'utilisateur pour accéder à l'interface Web de l'unité KX II-101-V2 une fois connecté via le modem.
 - Modem client IP address (Adresse IP du client de modem) - Adresse attribuée à l'utilisateur une fois connecté via modem.
4. Cliquez sur OK.

Reportez-vous à **Connexions de câbles d'accès par modem** (voir "**Connexions de câble pour l'accès par modem**" à la page 127) pour en savoir plus sur la connexion de câbles pour l'accès par modem et à **Modems certifiés** (à la page 206) pour en savoir plus sur les modems certifiés fonctionnant avec KX II-101-V2. Pour plus d'informations sur les paramètres qui permettront les meilleures performances lors de la connexion à KX II-101-V2 par modem, reportez-vous à **Création, modification et suppression des profils dans MPC** dans le **manuel des clients d'accès KVM et série**.

Connexions de câble pour l'accès par modem

Utilisez la configuration de connexion de câbles suivante pour relier KX II-101-V2 à un modem :

1. Branchez un câble série admin à KX II-101-V2.
2. Branchez un changeur de genre mâle/mâle à 9 broches au câble série admin.
3. Connectez un câble de modem null à l'autre extrémité du changeur de genre.
4. Branchez le changeur de genre mâle/mâle à 9 broches à l'autre extrémité du câble modem nul.
5. Branchez un câble de modem DB9-mâle DB25 entre le câble modem nul et le 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-101-V2. 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**
6. Cliquez sur OK.

Gestion des événements

La fonction de gestion des événements de KX II-101-V2 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.

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.

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-101-V2.

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 122) et à **Affichage du MIB de KX II-101-V2** (à la page 135) 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 cases à cocher restantes. <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)
6. Cliquez sur OK pour créer les trapps SNMP.

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](#).

KX II-101-V2 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.

► **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-101-V2.

AVERTISSEMENT : lorsque vous utilisez les traps SNMP sur UDP, il est possible que l'unité KX II-101-V2 et le routeur auquel elle est reliée se désynchronisent au moment où KX II-101-V2 redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Home > Device Settings > Event Management - Settings

SNMP Traps Configuration

SNMP Logging Enabled SNMP v1/v2c Traps Enabled SNMP Trap v3 Enabled

SNMP v1/v2 Trap

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

SNMP v3 Trap

Engine ID: 80001f8803000d5d03ca3b

Destination IP/Hostname	Port #	Security Name	Auth Protocol	Auth Passphrase	Privacy Protocol	Privacy Passphrase
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	

[Link to SNMP Agent Configuration](#)

[Click here to view the Dominion KX2 SNMP MIB](#)

Liste des traps SNMP de KX II-101-V2

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-101-V2 :

Nom de trap	Description
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.

Nom de trap	Description
deviceUpgradeCompleted	KX II-101-V2 a effectué la mise à jour via un fichier RFP.
deviceUpgradeStarted	KX II-101-V2 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-101-V2.
groupDeleted	Un groupe a été supprimé du système.
groupModified	Un groupe a été modifié.
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.
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-101-V2 est terminé.
rebootStarted	KX II-101-V2 a commencé à redémarrer lors de l'alimentation cyclique du système ou lors d'un

Nom de trap	Description
	redémarrage à chaud à partir du système d'exploitation.
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.
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.
userForcedLogout	Un utilisateur a été déconnecté de force par Admin.
userLogin	Un utilisateur s'est connecté à KX II-101-V2 et a été authentifié.
userLogout	Un utilisateur s'est déconnecté correctement de KX II-101-V2.
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

Nom de trap	Description
	Support virtuel.

Affichage du MIB de KX II-101-V2

► Pour afficher le MIB de KX II-101-V2 :

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 setDateAndTime, 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-101-V2.

► **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 129).

► **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 sur UDP, il est possible que l'unité KX II-101-V2 et le routeur auquel elle est reliée se désynchronisent au moment où KX II-101-V2 redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Configuration des ports

La page Port Configuration (Configuration des ports) affiche la liste des ports de l'unité KX II-101-V2. Les ports connectés aux serveurs cible KVM ou aux barrettes d'alimentation sont affichés en bleu et peuvent être modifiés.

► **Pour modifier la configuration d'un port :**

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

Tri

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 Name - Nom attribué au port. Un nom de port affiché en noir indique que ce nom ou ce port ne peut pas être modifié. Les noms de port affichés en bleu sont modifiables.

Remarque : n'utilisez pas d'apostrophes pour le nom de port.

- Port Type - Type de cible connectée au port :

Type de port	Description
PowerStrip	Barrette d'alimentation/PDU
KVM	Cible KVM

► **Pour modifier le nom d'un port :**

1. Cliquez sur l'option Port Name (Nom du port) associée au port que vous souhaitez modifier.
 - Pour les ports KVM, la page Port s'ouvre. Dans cette page, vous pouvez nommer les ports, créer des associations d'alimentation et définir les paramètres des serveurs cible.

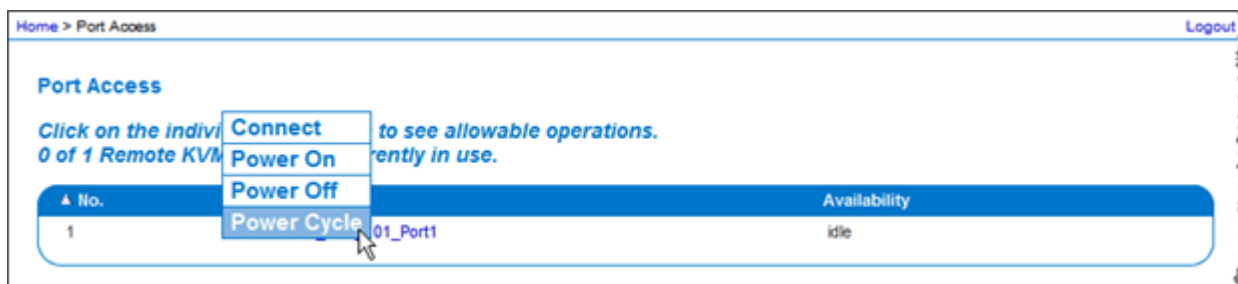
- Pour les barrettes d'alimentation, la page Port des barrettes d'alimentation s'ouvre. Dans cette page, vous pouvez nommer les barrettes d'alimentation et leurs prises. Reportez-vous à **Gestion de l'alimentation électrique** (voir "**Gestion de l'alimentation**" à la page 140).

Remarque : le lien Power Port 1 (Port d'alimentation 1) est activé uniquement lorsqu'une barrette d'alimentation Raritan est connectée à KX II-101-V2 et configurée. Dans le cas contraire, ce lien est désactivé.

Gestion des serveurs cible KVM (page Port)

La page Port s'ouvre lorsque vous sélectionnez un port connecté à un serveur cible dans la page Port Configuration (Configuration des ports). Dans cette page, vous pouvez procéder à des associations d'alimentation et remplacer le nom de port à votre convenance.

Un serveur peut avoir jusqu'à quatre prises d'alimentation et vous pouvez associer une barrette d'alimentation différente à chacune d'elle. Dans cette page, vous pouvez définir ces associations de façon à pouvoir mettre sous tension, hors tension, éteindre et rallumer le serveur dans la page Port Access (Accès aux ports), comme illustré ci-après.



Remarque : pour que vous puissiez utiliser cette fonction, une barrette d'alimentation Raritan Dominion PX doit être reliée au dispositif. Reportez-vous à Connexion de la barrette d'alimentation.

► Pour accéder à la configuration d'un port :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration (Configuration des ports) s'ouvre.
2. Cliquez sur le nom du port que vous souhaitez modifier.

Remarque : le lien Power Port 1 (Port d'alimentation 1) est activé uniquement lorsqu'une barrette d'alimentation Raritan est connectée au dispositif KX II-101-V2 et configurée. Dans le cas contraire, ce lien est désactivé.

Renommage d'un port**► Pour modifier le nom du port :**

1. Saisissez un nom descriptif, par exemple le nom du serveur cible. Ce nom peut être composé de 32 caractères alphanumériques maximum et inclure des caractères spéciaux.

Remarque : n'utilisez pas d'apostrophes pour le nom de port.

2. Cliquez sur OK.

Caractères spéciaux acceptés

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		

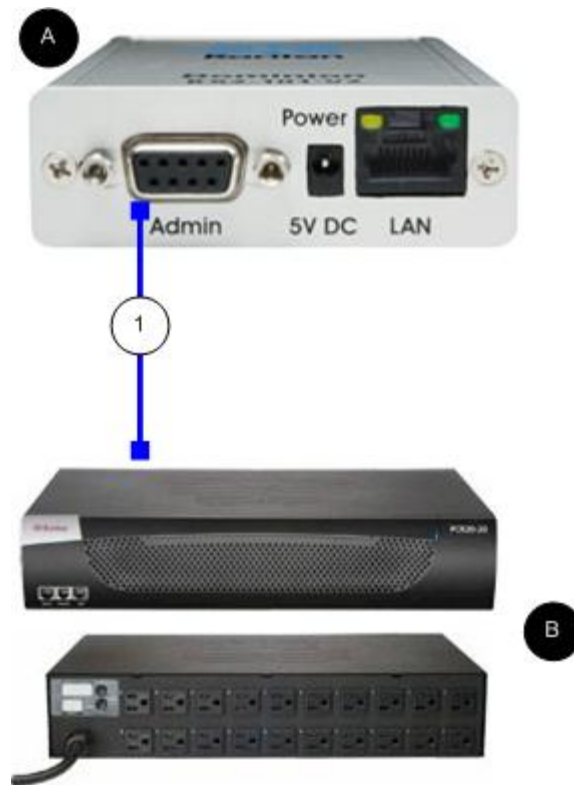
Gestion de l'alimentation

L'unité KX II-101-V2 permet la gestion de l'alimentation à distance d'un serveur cible. Pour utiliser cette fonction, vous devez disposer d'une barrette d'alimentation distante Raritan.

► **Pour utiliser la fonction de gestion de l'alimentation de l'unité KX II-101-V2 :**

- Branchez la barrette d'alimentation sur votre serveur cible à l'aide du connecteur DKX2-101-V2-PDU (non fourni mais disponible auprès de votre revendeur ou de Raritan). Reportez-vous à Brancher la barrette d'alimentation.
- Nommez la barrette d'alimentation (non fournie mais disponible auprès de votre revendeur ou de Raritan. Reportez-vous à **Nommer la barrette d'alimentation (Page Port pour les barrettes d'alimentation)** (voir "**Nommage de la barrette d'alimentation (Page Port pour les barrettes d'alimentation)**" à la page 142).
- Associez une prise de la barrette d'alimentation au serveur cible. Reportez-vous à **Gestion des services cible KVM (Page Port)** (voir "**Gestion des serveurs cible KVM (page Port)**" à la page 138).
- Activez et désactivez les prises de la barrette d'alimentation dans la page Power Strip Device (Dispositif de barrette d'alimentation). Reportez-vous à Contrôle d'un dispositif de barrette d'alimentation.

Branchement de la barrette d'alimentation



Légende	
A	KX II-101-V2
B	Barrette d'alimentation Raritan.
1	Connecteur DKX2-101-V2-PDU (adaptateur DB9-RJ45) (non fourni) de l'unité KX II-101-V2 à une barrette d'alimentation Raritan.

► **Pour brancher l'unité KX II-101-V2 à une barrette d'alimentation Raritan :**

1. Reliez le câble DKX2-101-V2-PDU (adaptateur DB9-RJ45) au port Admin de l'unité KX II-101-V2.
2. Connectez DKX2-101-V2-PDU au connecteur du port série de la barrette d'alimentation Raritan à l'aide d'un câble Cat5.
3. Reliez un cordon d'alimentation CA au serveur cible et à une prise de barrette d'alimentation disponible.

4. Branchez la barrette à une source d'alimentation CA.
5. Mettez sous tension la barrette d'alimentation Raritan.
6. Cliquez sur Device Settings (Paramètres du dispositif) > Serial Port (Port série) pour ouvrir la page Serial Port.
7. Sélectionnez le bouton radio Power Strip Control (Gestion des barrettes d'alimentation) et cliquez sur OK. Ceci fait, le menu Power (Alimentation) est disponible sur la console distante.

Nommage de la barrette d'alimentation (Page Port pour les barrettes d'alimentation)

Une fois le dispositif KX II-101-V2 connecté à une barrette d'alimentation distante Raritan, le port est affiché dans la page Port et vous pouvez ouvrir ce port depuis la page de configuration des ports. Les champs Type et Name (Nom) sont déjà renseignés. Les informations suivantes s'affichent pour chaque prise de barrette d'alimentation : numéro, nom et association des ports pour les prises.

Utilisez cette page pour nommer la barrette d'alimentation et ses prises. Tous les noms peuvent être composés de 32 caractères alphanumériques maximum et inclure des caractères spéciaux.

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

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

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

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

► **Pour quitter sans enregistrer les modifications :**

- Cliquez sur Cancel (Annuler).

Home > Device Settings > Port Configuration > Port

Port 2

Type:
PowerStrip

Name:
Power Port 1

Outlets

Number	Name	Port Association
1	Outlet 1	
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	

OK Cancel

© 2008 Raritan, Inc.

Gestion des associations d'alimentation

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

Remarque : lorsqu'une barrette d'alimentation est associée au serveur cible (port), le nom de la prise est remplacé par celui du port. Vous pouvez modifier ce nom dans la page Port 2.

1. Sélectionnez la barrette d'alimentation dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
2. Sélectionnez la prise dans la liste déroulante Outlet Name (Nom de prise).
3. Répétez les étapes 1 et 2 pour chaque association d'alimentation voulue.
4. Cliquez sur OK. Un message de confirmation apparaît.

► **Pour supprimer une association de barrettes d'alimentation :**

1. Sélectionnez la barrette d'alimentation appropriée dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
2. Pour cette barrette d'alimentation, sélectionnez la prise appropriée dans la liste déroulante Outlet Name (Nom de prise).
3. Dans la liste déroulante Outlet Name (Nom de prise), sélectionnez None (Aucun).
4. Cliquez sur OK. Cette association de barrettes d'alimentation/prises est supprimée. Un message de confirmation apparaît.

► **Pour afficher la configuration des ports d'alimentation :**

- Sélectionnez Home (Accueil) > Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) > [nom du port d'alimentation]. Les associations de prises pour la barrette d'alimentation figurent sous Outlets (Prises).

► **Pour modifier la configuration des ports d'alimentation :**

1. Modifiez le nom du port dans le champ de nom du port.
2. Remplacez le nom de la prise en modifiant le champ Name (Nom) des prises associées. Le nom de la prise apparaît dans la page Powerstrip Device (Dispositif de barrette d'alimentation). Reportez-vous à Gestion d'un dispositif de barrette d'alimentation.
3. Modifiez l'association de prises en cliquant sur le lien Port Association (Association de ports) en regard du nom de la prise et en le remplaçant dans la page Port 1.

Contrôle d'un dispositif de barrette d'alimentation

Contrôlez le dispositif de barrette d'alimentation à l'aide de la page Power Strip Device (Dispositif de barrette d'alimentation). Cette page vous permet d'activer et de désactiver chaque prise de la barrette d'alimentation.

► **Pour contrôler la barrette d'alimentation connectée à KX II-101-V2 :**

1. Sélectionnez Home (Accueil) > Powerstrip (Barrette d'alimentation). La page Power Strip Device (Dispositif de barrette d'alimentation) s'ouvre.
2. Cliquez sur le bouton On (Actif) ou Off (Inactif) pour chaque prise pour l'activer ou la désactiver.
3. A l'invite, cliquez sur OK pour confirmer votre choix.

Remarque : KX II-101-V2 peut gérer une seule barrette d'alimentation. Vous ne pouvez pas sélectionner d'autres barrettes d'alimentation dans le menu Powerstrip (Barrette d'alimentation).

Commutateur KVM analogique

Vous pouvez configurer un commutateur KVM analogique Raritan pour qu'il fonctionne avec KX II-101-V2.

La compatibilité de KX II-101-V2 avec les commutateurs KVM Raritan suivants a été vérifiée :

- SwitchMan SW2, SW4 et SW8
- Master Console MX416 et MXU

Des produits similaires de Raritan ou d'autres fabricants peuvent être compatibles, mais la prise en charge n'est pas garantie.

Remarque : pour permettre le fonctionnement de KX II-101-V2 avec des commutateurs KVM analogiques, le raccourci clavier du commutateur servant à alterner entre les cibles doit être défini sur la valeur par défaut Arrêt défil.

► Pour configurer un commutateur KVM analogique Raritan :

1. Définissez l'interface hôte sur PS/2 dans la page Keyboard/Mouse Setup (Configuration du clavier/de la souris). Si vous tentez de configurer un commutateur KVM analogique sans effectuer cette opération, le message d'erreur « PS/2 is needed to access the KVM Switch. Please enable PS/2 first! » (L'accès au commutateur KVM requiert PS/2. Activez d'abord PS/2.) apparaîtra dans la page Analog KVM Switch Configuration (Configuration du commutateur KVM analogique). Reportez-vous à **Configuration du clavier/de la souris** (à la page 125).
2. Cliquez sur Device Settings > Analog KVM Switch (Paramètres du dispositif > Commutateur KVM analogique). La page Analog KVM Switch Configuration (Configuration du commutateur KVM analogique) s'ouvre.
3. Cochez la case Use Analog KVM Switch (Utiliser un commutateur KVM analogique) pour activer ces champs.
4. Sélectionnez le type de commutateur Raritan dans le menu déroulant Switch Type :
 - Raritan MCC
 - Raritan MX
 - Raritan MXU
 - Raritan Switchman

5. Dans le champ Port Count, entrez le nombre de ports disponibles selon le type de commutateur sélectionné. Modifiez le nombre de ports le cas échéant ou utilisez la valeur par défaut. Les valeurs par défaut de sélection du commutateur et du nombre de ports sont les suivantes :
 - Raritan MCC - 8
 - Raritan MX - 16
 - Raritan MXU - 16
 - Raritan Switchman - 2
6. Cochez la case Security Setting (Définition de la sécurité) pour activer la sécurité.
7. Entrez le mot de passe utilisé pour accéder au commutateur KVM.
8. Cliquez sur OK pour configurer le commutateur KVM analogique.

► **Pour restaurer les valeurs par défaut du commutateur KVM analogique :**

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

Analog KVM Switch Configuration

Note: Changing one of the following options will close all kvm and virtual media sessions.

Use Analog KVM Switch

Switch Type

Raritan MCC

Port Count

8

Security Setting

Password

OK

Reset To Defaults

Cancel

Réinitialisation de KX II-101-V2 à l'aide du bouton de réinitialisation

Sur le haut 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 dans l'interface utilisateur graphique. Reportez-vous à **Encryption & Share (Chiffrement et partage)**.

► **Pour réinitialiser le dispositif :**

1. Mettez KX II-101-V2 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-101-V2.
4. Continuez de maintenir le bouton enfoncé pendant 10 secondes.
5. Relâchez le bouton Reset et KX II-101-V2 redémarre. Ceci prend généralement trois minutes.

Remarque : si KX II-101-V2 est paramétré pour rétablir les valeurs par défaut usine à la réinitialisation, l'adresse IP, le nom d'utilisateur et d'autres options seront définis en conséquence.



Modification du paramètre de langue de l'interface utilisateur par défaut

L'interface utilisateur de KX II-101-V2 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 7 Gestion des connexions USB

Dans ce chapitre

Présentation	150
Paramètres de connexion USB	151
Paramètres des connexions USB avancées	152

Présentation

Pour élargir la compatibilité du dispositif KX II-101-V2 avec différents serveurs cible KVM, Raritan fournit une sélection en temps réel définie par l'utilisateur d'options de profils de configuration USB pour un large éventail de mises en œuvre de serveurs de système d'exploitation et au niveau du BIOS.

Les paramètres de connexion USB par défaut répondent aux besoins de la grande majorité des configurations de serveurs cible KVM déployés. Des éléments de configuration supplémentaires sont fournis pour répondre aux besoins particuliers d'autres configurations de serveurs habituels (par exemple, Linux® et Mac OS X. Il existe également des éléments de configuration, désignés par nom de plate-forme et par version de BIOS, permettant d'améliorer la compatibilité de la fonction de supports virtuels avec le serveur cible, par exemple, lors d'une exploitation au niveau du BIOS.

Les profils USB sont configurés dans la page Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) > page Port de la console distante KX II-101-V2. Un administrateur de dispositifs peut configurer le port à l'aide des profils le mieux adaptés aux besoins de l'utilisateur et à la configuration du serveur cible.

AVERTISSEMENT : les sélections effectuées dans la section Advanced USB Connection Settings (Paramètres des connexions USB avancées) peuvent parfois poser des problèmes de configuration entre KX II-101-V2 et le serveur cible.

Aussi, Raritan recommande de consulter le lien le plus récent de la table de configuration des profils USB KX II-101-V2 définis par l'utilisateur, accessible directement depuis la section Advanced USB Connection Settings de la page Port. Les informations disponibles au moment de la rédaction de cette publication se trouvent dans la rubrique Profils USB connus.

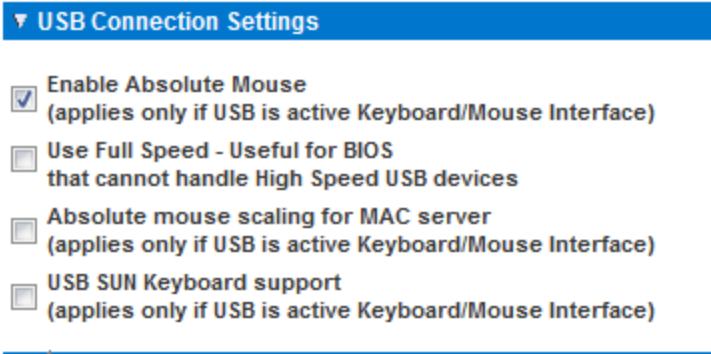
Un utilisateur connecté à un serveur cible KVM choisit parmi ces paramètres de connexion USB suivant l'état fonctionnel de ce serveur. Par exemple, si le serveur est lancé et que l'utilisateur souhaite utiliser le système d'exploitation Windows®, il est recommandé d'utiliser les paramètres par défaut. Si l'utilisateur souhaite modifier les paramètres dans le menu BIOS ou démarrer depuis un lecteur de supports virtuels, suivant le modèle du serveur cible, un paramètre de connexion USB différent conviendrait mieux.

Lorsqu'aucun des paramètres de connexion USB fournis par Raritan ne fonctionne avec une cible KVM particulière, veuillez contacter le support technique Raritan.

Paramètres de connexion USB

► **Pour définir des connexions USB pour le serveur cible :**

1. Cliquez sur Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page correspondante. Cliquez sur le port à configurer.
2. Cliquez sur USB Connection Settings (Paramètres de connexion USB) pour développer la section.
3. Sélectionnez les paramètres de connexion USB que vous souhaitez utiliser :
 - Enable Absolute Mouse (Activer le mode Souris absolue) : s'applique uniquement si l'USB est actif pour l'interface clavier/souris.
 - Use Full Speed (Utiliser le haut débit) : utile pour les BIOS qui ne peuvent pas accueillir les dispositifs USB haute vitesse.
 - Absolute mouse scaling for MAC server (Facteur d'échelle de souris absolue pour serveur MAC) : s'applique uniquement si USB est actif pour l'interface clavier/souris.
 - USB Sun Keyboard support (Prise en charge de clavier Sun USB) : s'applique uniquement si USB est actif pour l'interface clavier/souris.
4. Cliquez sur OK.



▼ USB Connection Settings

- Enable Absolute Mouse
(applies only if USB is active Keyboard/Mouse Interface)
- Use Full Speed - Useful for BIOS
that cannot handle High Speed USB devices
- Absolute mouse scaling for MAC server
(applies only if USB is active Keyboard/Mouse Interface)
- USB SUN Keyboard support
(applies only if USB is active Keyboard/Mouse Interface)

Paramètres des connexions USB avancées

AVERTISSEMENT : les sélections effectuées dans la section Advanced USB Connection Settings (Paramètres des connexions USB avancées) peuvent parfois poser des problèmes de configuration entre KX II-101-V2 et le serveur cible. Aussi, Raritan recommande de consulter la section Profils USB connus ou la table de configuration des profils USB KX II-101-V2 définis par l'utilisateur, accessible directement depuis la section Advanced USB Connection Settings de la page Port.

► **Pour définir des connexions USB avancées pour le serveur cible :**

1. Cliquez sur Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page correspondante. Cliquez sur le port à configurer.
2. Cliquez sur Advanced USB Connection Settings pour développer la section.
3. Cliquez sur le lien de la table de configuration des profils USB KX II-101 définis par l'utilisateur pour accéder aux configurations recommandées à appliquer à la section Advanced USB Connection Settings.
4. Configurez les options suivantes selon les besoins :
 - a. Virtual Media Interface #1 Type (Type de l'interface de supports virtuels n° 2)
 - b. Cochez la case Remove Unused VM Interface #1 From Device Configuration (Retirer l'interface n° 1 inutilisée de la configuration du dispositif) pour supprimer l'interface de type VM (pour n° 2).
 - c. Virtual Media Interface #2 Type (Type de l'interface de supports virtuels n° 2)
 - d. Cochez la case Remove Unused VM Interface #2 From Device Configuration (Retirer l'interface n° 2 inutilisée de la configuration du dispositif) pour supprimer l'interface de type VM (pour n° 2).

5. Cliquez sur OK.

▼ Advanced USB Connection Settings

IMPORTANT: Please follow the reference guide provided at this link.

User Defined KX II-101 USB Profile Configuration Table

Virtual Media Interface #1 Type

CD-ROM ▼

Remove Unused VM Interface #1 From Device Configuration
(useful for BIOS that cannot accommodate empty drives)

Virtual Media Interface #2 Type

Removable Disk ▼

Remove Unused VM Interface #2 From Device Configuration
(useful for BIOS that cannot accommodate empty drives)

Chapitre 8 Gestion de la sécurité

Dans ce chapitre

Security Settings (Paramètres de sécurité).....	154
Configuration du contrôle d'accès IP.....	165
Certificats SSL.....	168
Bannière de sécurité.....	171

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.

► **Pour configurer les paramètres de sécurité :**

1. Sélectionnez Security > Security Settings (Sécurité > Paramètres de sécurité). La page Security Settings (Paramètres de sécurité) s'ouvre.
2. Mettez à jour les paramètres de **limitations de connexion** (à la page 154) en fonction de vos besoins.
3. Mettez à jour les paramètres de **mots de passe sécurisés** (à la page 156) en fonction de vos besoins.
4. Mettez à jour les paramètres de **blocage des utilisateurs** (à la page 157) 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 :**

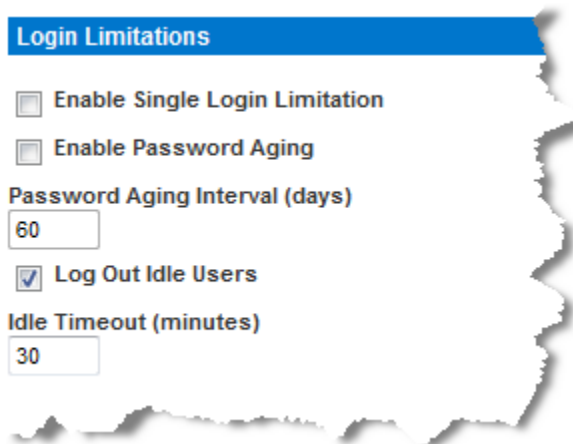
- Cliquez sur Reset to Defaults (Restaurer les paramètres par défaut).

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)	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

Limitation	Description
unique)	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)	<p>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 Interval (Intervalle de vieillissement du mot de passe).</p> <p>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.</p>
Log off idle users, After (1-365 minutes) (Déconnecter les utilisateurs inactifs, Après)	<p>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.</p> <p>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.</p>



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-101-V2, 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 les administrateurs peuvent changer le minimum à 63 caractères.
Maximum length of strong password (Longueur maximale du mot de passe sécurisé)	La longueur minimum par défaut est 8, mais les administrateurs peuvent définir le maximum à une valeur par défaut de 16 caractères. La longueur maximum des mots de passe forts est de 63 caractères.
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	Lorsqu'elle est cochée, cette option impose au moins un caractère spécial

Champ	Description
(Imposer au moins un caractère spécial imprimable)	(imprimable) dans le mot de passe.
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.

Strong Passwords

Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history

5

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
<p>Timer Lockout (Période de verrouillage)</p>	<p>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 :</p> <ul style="list-style-type: none"> ▪ 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. <hr/> <p><i>Remarque : les utilisateurs dotés du rôle Administrateur ne sont pas concernés par les paramètres de période de verrouillage.</i></p>
<p>Deactivate User-ID (Désactiver l'ID de l'utilisateur)</p>	<p>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) :</p> <ul style="list-style-type: none"> ▪ 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. <p>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).</p>

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-101-V2 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-101-V2.

► 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-101-V2. 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-101-V2. » (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-101-V2.).

Mode de chiffrement	Description
Auto	Il s'agit de l'option recommandée. KX II-101-V2 négocie automatiquement au niveau le plus élevé de chiffrement possible. Vous <i>devez</i> sélectionner Auto pour que le

Mode de chiffrement	Description
	dispositif et le client négocient avec succès l'utilisation des algorithmes compatibles FIPS.
RC4	<p>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-101-V2 et l'ordinateur distant lors de l'authentification de la connexion initiale.</p> <p>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.</p>
AES-128	<p>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 163) pour plus d'informations.</p>
AES-256	<p>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 163) pour plus d'informations.</p>

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-101-V2 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 163) pour en savoir plus à ce sujet.
4. PC Share Mode - Détermine l'accès KVM à distance simultanément global, permettant ainsi à huit utilisateurs distants au maximum de se connecter simultanément à une unité KX II-101-V2 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-101-V2 à l'aide du bouton de réinitialisation** (à la page 147). 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-101-V2 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.

Vérification de la prise en charge du chiffrement AES par votre navigateur

KX II-101-V2 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 :

- JRE1.7 - javase/downloads/jce-7-download-432124.html

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-101-V2 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-101-V2 <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-101-V2.

Exigences en matière de prise en charge de FIPS 140-2

KX II-101-V2 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-101-V2 figurent ci-après :

KX II-101-V2

- Paramétrez Encryption & Share (Chiffrement & Partage) sur Auto sur la page Security Settings (Paramètres de sécurité). Reportez-vous à Encryption & Share (Chiffrement et partage).

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 pouvez réguler l'accès à votre KX II-101-V2. 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.

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de KX II-101-V2. Lorsque vous créez une liste de contrôle d'accès IP, si 127.0.0.1 se trouve dans la plage des adresses IP bloquées, vous n'aurez plus accès au port local de KX II-101-V2.

► **Pour utiliser le contrôle d'accès IP :**

1. Ouvrez la page IP Access Control (Contrôle d'accès IP) en sélectionnant Security (Sécurité) > IP Access Control. La page IP Access Control s'ouvre.
2. Cochez la case Enable IP Access Control (Activer le contrôle de l'accès par IP) pour activer le contrôle de l'accès par IP, ainsi que les autres champs 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-101-V2.
 - Drop (Abandonner) - Les adresses IP ne sont pas autorisées à accéder au dispositif KX II-101-V2.

► **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 entrée à l'aide de la notation CIDR (Classless Inter-Domain Routing). Celle-ci comporte deux parties. La partie la plus importante est l'adresse réseau qui identifie un réseau entier ou un sous-réseau. La partie la moins importante est l'identifiant. La longueur du préfixe après le signe / identifie la longueur du masque de sous-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. Entrez un numéro de règle (#). Ce numéro 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 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. Vous êtes invité à confirmer la suppression. Cliquez sur OK.

Home > Security > IP Access Control

IP Access Control

Enable IP Access Control

Default Policy

ACCEPT ▾

Rule #	IPv4/Mask or IPv6/Prefix Length	Policy
<input type="text"/>	<input type="text"/>	ACCEPT ▾

Append

Insert

Replace

Delete

OK

Reset To Defaults

Cancel

Pour autoriser l'accès à une seule adresse IP et bloquer toutes les autres, modifiez le masque de sous-réseau pour la règle à /32. Par exemple, si vous tentez d'exclure tout accès depuis le sous-réseau 192.168.51 et que l'option Default Policy (Stratégie par défaut) est paramétrée sur Accept (Accepter), vous allez ajouter une règle avec l'option IP/MASK définie sur 192.168.51.00/24 et la stratégie DROP. Ou si vous tentez d'exclure tout accès depuis le sous-réseau 192.168.51 à l'exception d'une adresse IP particulière (192.168.51.105) et que la stratégie par défaut est Accept (Accepter), vous allez :

1. Ajouter la règle Rule 1 avec l'option IP/Mask définie sur 192.168.51.105/32 et la stratégie Accept.
2. Ajouter la règle Rule 2 avec l'option IP/Mask définie sur 192.168.51.0/24 et la stratégie Drop (Abandonner).

Si vous intervertissiez Rule 1 et Rule 2, 192.168.51.105 ne pourrait pas non plus accéder à KX II-101-V2 puisqu'elle aurait également été abandonnée par la première règle rencontrée.

Certificats SSL

KX II-101-V2 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-101-V2 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-101-V2. 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-101-V2 sont définies correctement.

Lorsqu'un certificat auto-signé est créé, la date et l'heure de l'unité KX II-101-V2 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 128).

Remarque : la demande de signature de certificat (CSR) doit être générée sur KX II-101-V2.

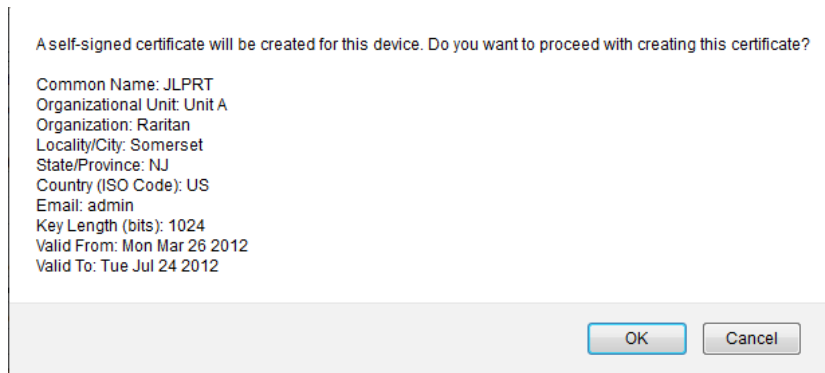
Remarque : lors de la mise à niveau du firmware, le certificat actif et la demande de signature de certificat ne sont pas remplacés.

► **Pour créer et installer un certificat SSL :**

1. Sélectionnez Security (Sécurité) > Certificate (Certificat).
2. Remplissez les champs suivants :
 - a. Common name (Nom courant) - Il s'agit du nom réseau de KX II-101-V2 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-101-V2 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-101-V2 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-101-V2 appartient.
 - c. Organization (Organisation) - Il s'agit du nom de l'organisation à laquelle KX II-101-V2 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-101-V2 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-101-V2 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-101-V2 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-101-V2 pour activer le certificat auto-signé.



Ou

- f. Indiquez le nombre de jours de la durée de validité. Assurez-vous que la date et l'heure de KX II-101-V2 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-101-V2 pour envoyer la demande de signature de certificat (CSR) à une autorité de certification pour le certificat SSL.

► **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 (Télécharger).

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 signé :**

1. Téléversez le certificat dans KX II-101-V2 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.

Certificate Signing Request (CSR)	Certificate Upload
<p>The following CSR is pending:</p> <pre>countryName = US stateOrProvinceName = DC localityName = Washington organizationName = ACME Corp. organizationalUnitName = Marketing Dept. commonName = John Doe emailAddress = johndoe@acme.com</pre> <p style="text-align: center;"> <input type="button" value="Download"/> <input type="button" value="Delete"/> </p>	<p>SSL Certificate File</p> <input type="text"/> <input type="button" value="Browse..."/> <p style="text-align: center;"><input type="button" value="Upload"/></p>

Une fois ces étapes effectuées, KX II-101-V2 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-101-V2, 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-101-V2 vous offre la possibilité d'ajouter une bannière de sécurité au processus de connexion de KX II-101-V2. Cette fonction oblige les utilisateurs à accepter ou à refuser un accord de sécurité avant d'accéder au KX II-101-V2. 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-101-V2 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-101-V2 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.
6. 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.

Chapitre 9 Maintenance

Dans ce chapitre

Journal d'audit	173
Informations sur le dispositif	174
Backup and Restore (Sauvegarde et restauration)	175
Mise à niveau du firmware.....	177
Historique des mises à niveau	179
Factory Reset (Restauration des valeurs d'usine)	179
Redémarrage de KX II-101-V2.....	180
Arrêt de la gestion par CC-SG.....	181

Journal d'audit

Un journal des événements du système KX II-101-V2 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).

► **Pour consulter le journal d'audit de votre unité KX II-101-V2 :**

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 :**

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).

Informations sur le dispositif

La page Device Information (Informations sur le dispositif) contient des données détaillées sur votre unité KX II-101-V2. Ces informations sont utiles si vous avez besoin de contacter le support technique Raritan.

► **Pour afficher les informations sur votre unité KX II-101-V2 :**

- Sélectionnez Maintenance > Device Information (Informations sur le dispositif). La page Device information (Informations sur le dispositif) s'ouvre.

Les informations suivantes sur l'unité KX II-101-V2 sont disponibles :

- Modèle
- Révision du matériel
- Version du firmware
- Numéro de série
- Adresse MAC

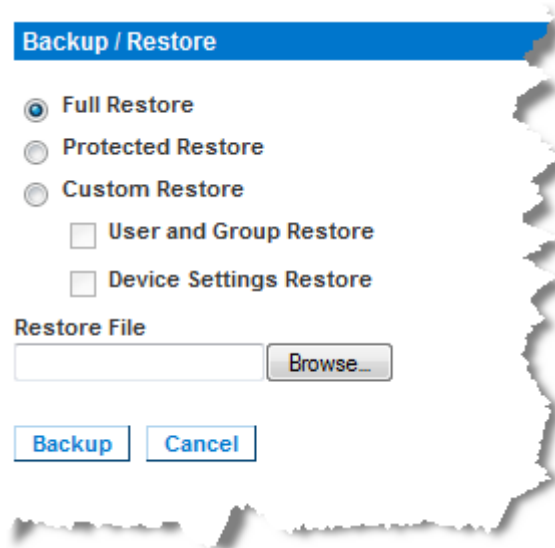
Backup and Restore (Sauvegarde et restauration)

La page Backup/Restore (Sauvegarder/Restaurer) vous permet de sauvegarder et de restaurer les paramètres et la configuration de votre KX II-101-V2.

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-101-V2 en sauvegardant les paramètres de configuration utilisateur du dispositif KX II-101-V2 en cours d'utilisation et en restaurant ces paramètres sur le nouveau KX II-101-V2. Vous pouvez également configurer un KX II-101-V2 et copier sa configuration dans plusieurs dispositifs KX II-101-V2.

► 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 système complètes. Les restaurations, en revanche, peuvent être totales ou partielles selon votre sélection.

► Pour effectuer une copie de sauvegarde de KX II-101-V2, si vous utilisez Internet Explorer 7 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 journal de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.
 - b. Une fois le fichier enregistré, recherchez-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-101-V2 :**

AVERTISSEMENT : soyez prudent lorsque vous restaurez une version antérieure de votre KX II-101-V2. 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-101-V2.

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-101-V2 et de copier sa configuration dans plusieurs dispositifs KX II-101-V2.
 - 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-101-V2.
 - 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.

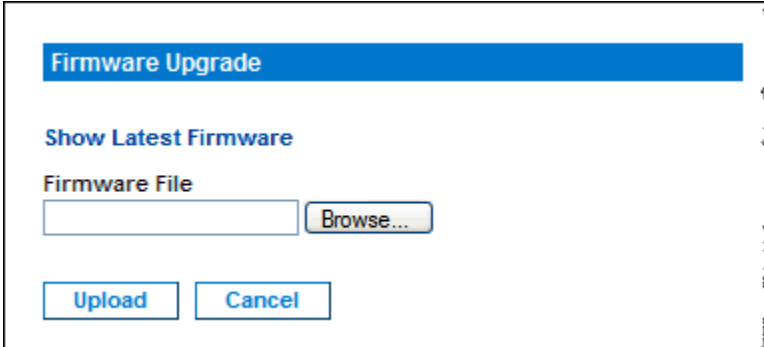
Mise à niveau du firmware

La page Firmware Upgrade (Mise à niveau du firmware) permet de mettre à niveau le firmware de votre unité KX II-101-V2.

Important : n'éteignez pas votre dispositif KX II-101-V2 pendant la mise à niveau, ou vous risquez de l'endommager.

► **Pour mettre à niveau votre dispositif KX II-101-V2 :**

1. Sélectionnez Maintenance > Firmware Upgrade (Mise à niveau du firmware). La page Firmware Upgrade (Mise à niveau du firmware) s'ouvre :



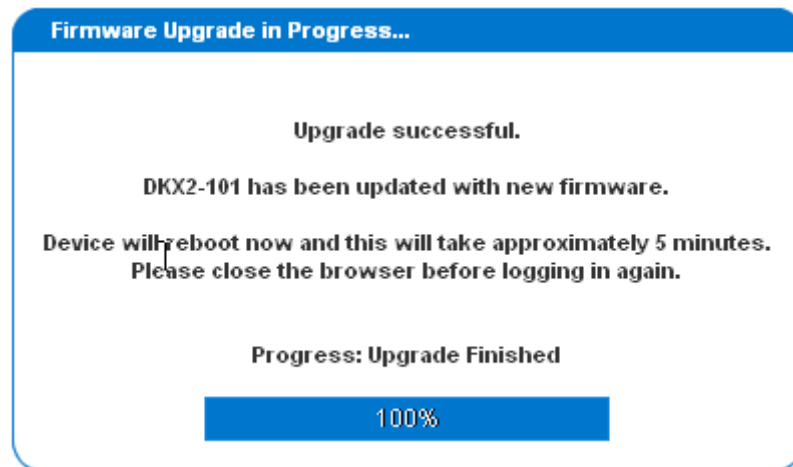
2. Cliquez sur le lien Show Latest Firmware (Afficher le dernier firmware), recherchez le fichier de distribution de firmware Raritan approprié (*.RFP) dans la page Firmware Upgrades (Mises à niveau du firmware) > KX II-101-V2, puis téléchargez le fichier.
3. Décompressez le fichier ZIP et lisez attentivement 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. Cliquez sur Browse (Parcourir) pour accéder au répertoire où vous avez décompressé le fichier de mise à niveau.

4. Cliquez sur Upload (Télécharger) dans la page de mise à niveau du firmware. Des informations concernant le numéro de la mise à niveau et de la version s'affichent.

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

5. Cliquez sur Upgrade (Mettre à niveau). Veuillez attendre la fin de la mise à niveau. Des informations de statut et des barres de progression s'affichent pendant la mise à niveau. Une fois la mise à niveau terminée, le dispositif est redémarré.



6. A l'invite, fermez le navigateur et attendez environ 5 minutes avant de vous connecter de nouveau à KX II-101-V2.

Pour obtenir des informations sur la mise à niveau du firmware du dispositif via le Client MPC (Multi-Platform Client), consultez le **manuel d'utilisation des clients d'accès KVM et série**.

Historique des mises à niveau

KX II-101-V2 fournit des informations sur les mises à niveau effectuées sur le dispositif KX II-101-V2.

► **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.

Factory Reset (Restauration des valeurs d'usine)

*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**.*

► **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) :
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-101-V2 est automatiquement redémarré.

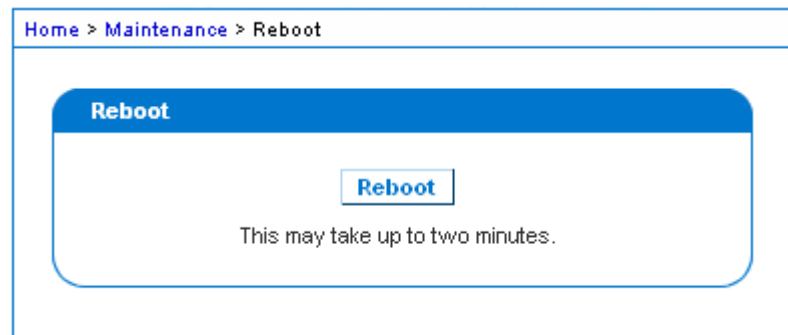
Redémarrage de KX II-101-V2

La page Reboot (Redémarrer) offre une manière sûre et contrôlée de redémarrer votre KX II-101-V2. Il s'agit de la méthode recommandée pour le redémarrage.

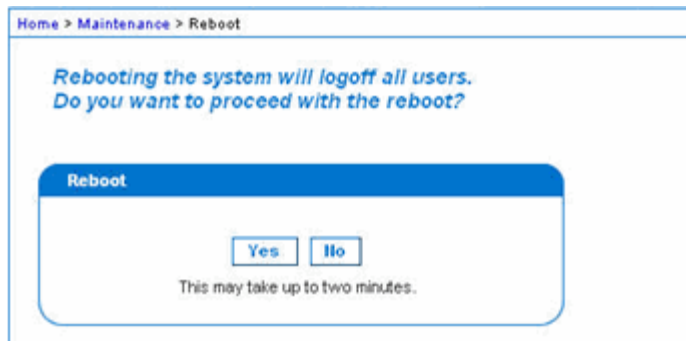
Important : toutes les connexions KVM et série sont fermées et tous les utilisateurs déconnectés.

► **Pour redémarrer votre KX II-101-V2 :**

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

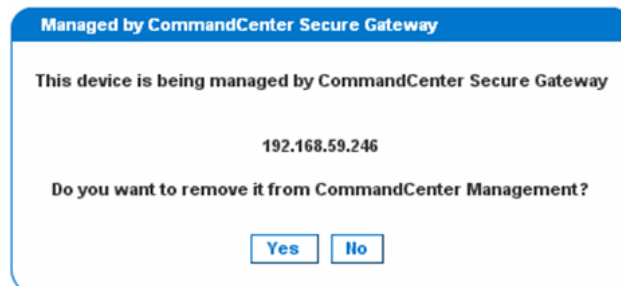
Pendant que KX II-101-V2 est géré par CC-SG, si vous tentez d'accéder au dispositif directement, vous êtes averti que CC-SG assure son contrôle.

Si vous gérez KX II-101-V2 via CC-SG et que la connectivité entre CC-SG et KX II-101-V2 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-101-V2.

Remarque : vous devez disposer des autorisations appropriées pour mettre fin à la gestion par CC-SG de KX II-101-V2. 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-101-V2.

► Pour arrêter la gestion de KX II-101-V2 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 débiter 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 10 Diagnostics

Les pages de diagnostics sont utilisées pour le dépannage et sont destinées avant tout à l'administrateur du dispositif KX II-101-V2. Toutes les pages de diagnostic (sauf Device Diagnostics (Diagnostics du dispositif)) exécutent les commandes de réseau standard ; les informations affichées sont le résultat de ces commandes. Les options suivantes du menu Diagnostics vous permettent de déboguer et de configurer les paramètres réseau.

L'option Device Diagnostics doit être utilisée conjointement à l'assistance technique Raritan.

Dans ce chapitre

Page d'interface réseau.....	183
Page Network Statistics (Statistiques réseau)	183
Page Ping Host (Envoyer une commande Ping à l'hôte)	186
Page Trace Route to Host	186
Page Device Diagnostics (Diagnostics du dispositif)	188

Page d'interface réseau

KX II-101-V2 fournit des informations sur l'état de votre interface réseau.

► **Pour afficher les informations relatives à votre interface réseau :**

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

Les informations suivantes s'affichent :

- l'état de l'interface Ethernet (active ou non) ;
- si la commande ping peut être émise sur la passerelle ;
- le port LAN actif.

► **Pour actualiser ces informations :**

- Cliquez sur Refresh (Actualiser).

Page Network Statistics (Statistiques réseau)

KX II-101-V2 fournit des statistiques sur votre interface réseau.

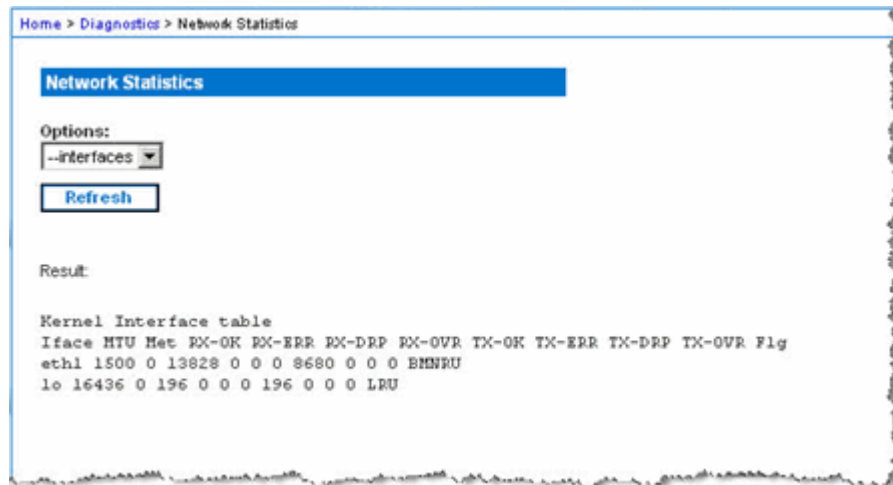
► **Pour afficher les statistiques relatives à votre interface réseau :**

1. Sélectionnez Diagnostics > Network Statistics (Statistiques réseau). La page des statistiques réseau s'ouvre.

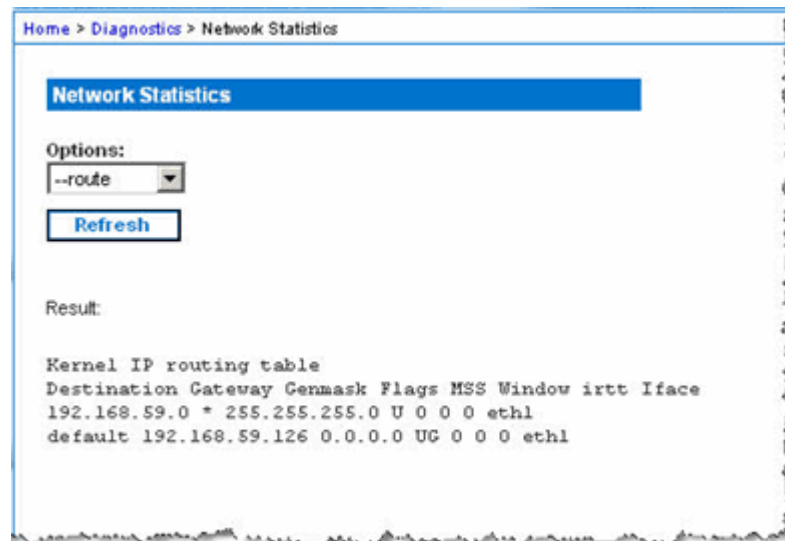
2. Sélectionnez l'option appropriée parmi celles de la liste déroulante Options :
 - Statistics - Génère une page similaire à celle affichée ici.



- Interfaces - Génère une page similaire à celle affichée ici.



- Route - Génère une page similaire à celle affichée ici.



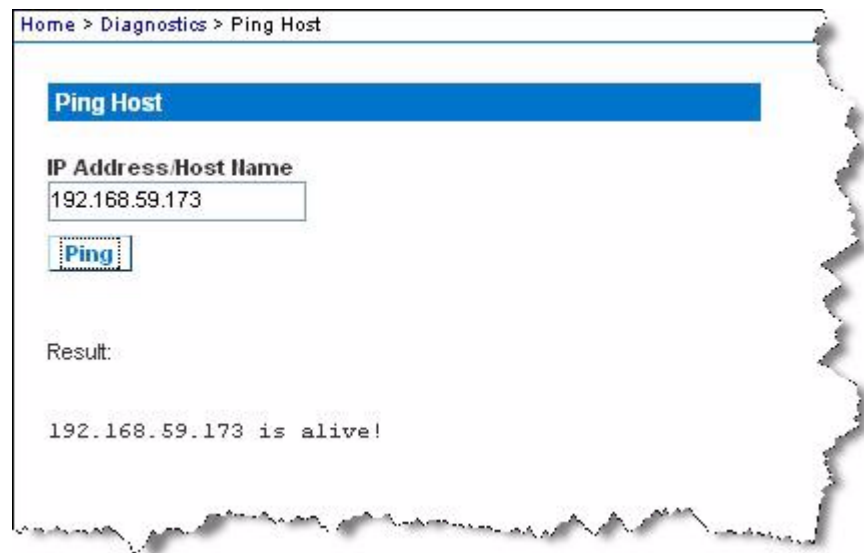
3. Cliquez sur Refresh (Actualiser). Les informations concernées sont affichées dans le champ Result (Résultat).

Page Ping Host (Envoyer une 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-101-V2 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.

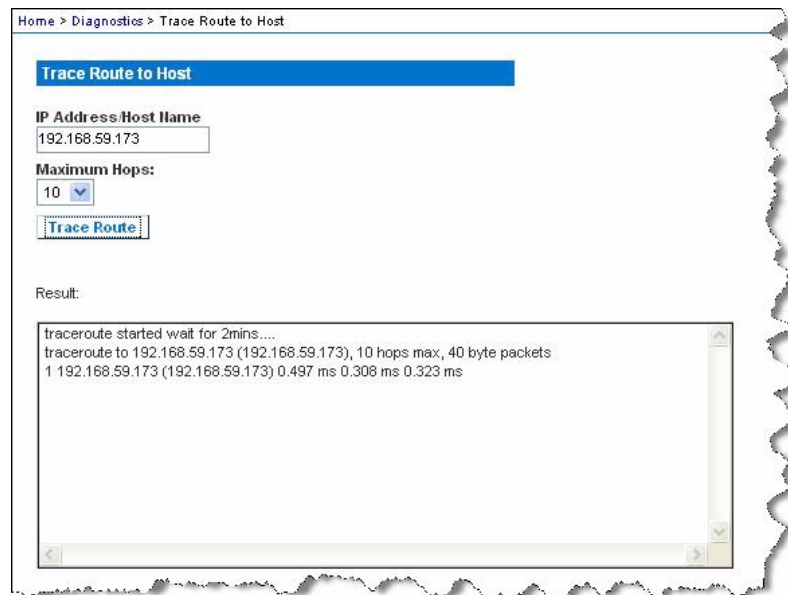
► **Pour déterminer l'itinéraire jusqu'à l'hôte :**

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 à la clientèle. Vous pouvez l'utiliser uniquement lorsque le support technique Raritan vous donne des instructions.

La page Device Diagnostics (Diagnostics du dispositif) télécharge les informations de diagnostic du dispositif KX II-101-V2 vers l'ordinateur client. Un journal de diagnostics du dispositif peut être généré avec ou sans l'exécution d'un script de diagnostics facultatif fourni par le support technique Raritan. Un script de diagnostics donne plus d'informations permettant de diagnostiquer les problèmes.

Utilisez les paramètres suivants :

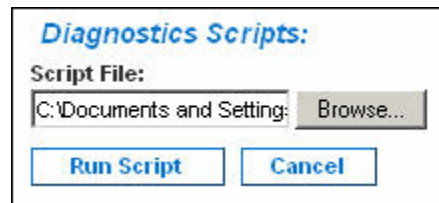
- Diagnostics Scripts (Scripts de diagnostics) : charge un script spécial fourni par le support technique Raritan lors d'une session de débogage d'erreurs critiques. Ce script est téléchargé vers le dispositif et exécuté. **Facultatif**
- Device Diagnostic Log (Journal de diagnostics du dispositif) : télécharge une capture d'écran des messages de diagnostics du dispositif KX II-101-V2 vers le client. Le fichier chiffré est ensuite envoyé au support technique Raritan. Seul Raritan est en mesure d'interpréter ce fichier.

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

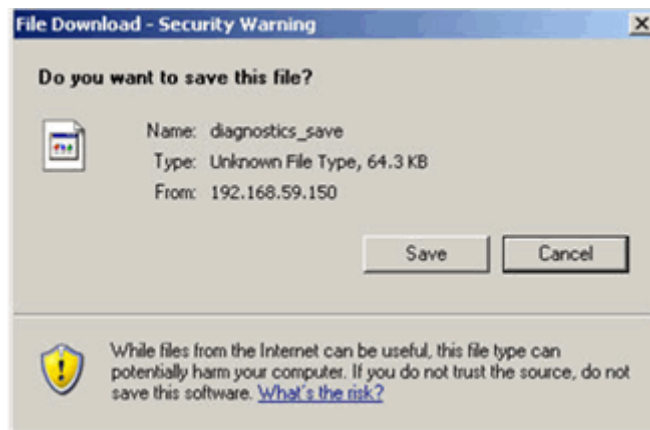
► Pour exécuter les diagnostics du système KX II-101-V2 :

1. Sélectionnez Diagnostics > Device Diagnostics (Diagnostics du dispositif). La page Device Diagnostics (Diagnostics du dispositif) s'ouvre.
2. (Facultatif) Effectuez les opérations suivantes si vous avez reçu un fichier script de diagnostics de la part du support technique Raritan. Sinon, passez à l'étape 3.
 - 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).
3. Créez un fichier de diagnostics à envoyer au support technique Raritan :
 - a. Cliquez sur Save to File (Enregistrer dans un fichier). La boîte de dialogue File Download (Téléchargement de fichiers) s'ouvre.



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

Chapitre 11 Interface de ligne de commande (CLI)

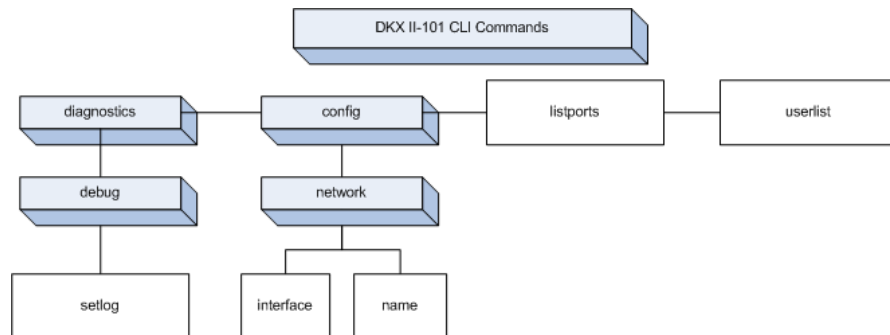
Dans ce chapitre

Présentation	190
Accès à l'unité KX II-101-V2 à l'aide du CLI	191
Connexion SSH à KX II-101-V2	191
Connexion.....	192
Navigation de la CLI	192
Commandes CLI.....	194

Présentation

Ce chapitre présente les commandes CLI susceptibles d'être utilisées avec l'unité KX II-101-V2. Reportez-vous à **Commandes CLI** (à la page 194) pour consulter une liste de commandes, de définitions et de liens vers les sections de ce chapitre comportant des exemples de ces commandes.

Le schéma suivant présente les commandes CLI :



Remarque : les commandes courantes suivantes peuvent être utilisées depuis tous les niveaux du CLI : top (haut), history (historique), logout (déconnexion), quit (quitter) et help (aide).

Accès à l'unité KX II-101-V2 à l'aide du CLI

Pour accéder à KX II-101-V2, choisissez l'une des méthodes suivantes :

- TELNET via connexion IP
- SSH via connexion IP
- Port série admin multifonction via une interface série RS-232 avec le câble fourni et un programme d'émulation de terminal tel que HyperTerminal

Plusieurs clients SSH/TELNET 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>

*Remarque : si vous accédez au CLI via SSH ou TELNET, vous devez configurer l'accès dans la page Device Services (Services du dispositif) du client distant de KX II-101-V2. Reportez-vous à **Services du dispositif** (à la page 120).*

Connexion SSH à KX II-101-V2

Utilisez un client SSH prenant en charge SSHv2 pour effectuer la connexion au dispositif. Vous devez activer l'accès SSH dans la page Device Services (Services du dispositif). Reportez-vous à **Services du dispositif** (à la page 120).

Remarque : pour des raisons de sécurité, les connexions SSH V1 ne sont pas prises en charge par le dispositif KX II-101-V2.

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-101-V2. Par exemple, 192.168.0.192.
3. Choisissez SSH, qui utilise le port de configuration 22 par défaut.
4. Cliquez sur Open (Ouvrir).
5. L'invite `login as:` apparaît.

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.

Connexion

- **Pour vous connecter :**

1. Login: admin
2. L'invite Password (Mot de passe) s'affiche. Saisissez le mot de passe par défaut : *raritan*.

Le message de bienvenue s'affiche. Vous êtes maintenant connecté en tant qu'administrateur.

Après avoir consulté la section **Navigation de la CLI** (à la page 192), vous pouvez effectuer les tâches de configuration initiales décrites dans **Configuration de KX II-101-V2 à l'aide d'un programme d'émulation de terminal (facultatif)** (à la page 35).

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.

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 >
```

Pour Telnet/SSH, admin est la partie racine de la commande :

```
admin > config > network >
```

0

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

CLI Commands (Commandes CLI) répertorie les commandes disponibles à tous les niveaux de la CLI. Ces commandes permettent également de parcourir la CLI.

Commande	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 du dispositif KX II-101-V2.
help	Affiche une présentation de la syntaxe CLI.
quit	Fait revenir l'utilisateur au niveau précédent.
logout	Déconnecte la session utilisateur.

Commandes CLI

Le tableau ci-après répertorie et décrit toutes les commandes CLI disponibles.

Commande	Description
config	Passe au menu Configuration.
diagnostics	Affiche le menu des diagnostics. Reportez-vous à Diagnostics (à la page 195).
debug	Affiche le menu de débogage. Reportez-vous à Déboguer (à la page 195).
help	Affiche une présentation de la syntaxe CLI.
history	Affiche l'historique des lignes de commande de la session actuelle.
interface	Configure l'interface réseau de KX II-101-V2.
ipv6_interface	Définit/Extrait les paramètres réseau IPv6.
listports	Répertorie le port, son nom, son type, son état et sa disponibilité. Reportez-vous à Commande listports (à la page 199).
logout	Déconnecte de la session CLI actuelle.
name	Définit le nom du dispositif. Reportez-vous à Commande name (à la page 198).
network	Affiche la configuration réseau et vous permet de configurer les paramètres réseau. Reportez-vous à

Commande	Description
config	Passe au menu Configuration.
diagnostics	Affiche le menu des diagnostics. Reportez-vous à Diagnositics (à la page 195).
	Réseau (à la page 197).
quit	Revient à la commande précédente.
setlog	Définit les options de journalisation du dispositif. Reportez-vous à Commande setlog (à la page 196).
top	Revient au menu racine.
userlist	Répertorie le nombre d'utilisateurs actifs, les noms d'utilisateur, le port et le statut. Reportez-vous à Commande userlist (à la page 199).

Diagnositics

Le menu Diagnositics vous permet de définir les options de journalisation pour différents modules de l'unité KX II-101-V2. Ne définissez les options de journalisation que sur la demande d'un ingénieur du support technique Raritan. Ces options de journalisation permettent à un ingénieur du support d'obtenir les bonnes informations en vue d'un débogage ou de la résolution d'un problème. L'ingénieur du support vous indiquera alors comment définir ces options et générer un fichier de journalisation à envoyer au support technique Raritan.

Important : ne définissez les options de journalisation que sous la supervision d'un ingénieur du support technique Raritan.

Déboguer

Le menu Diagnositics > Debug (Déboguer) vous permet de choisir la commande Setlog afin de définir les options de journalisation de l'unité KX II-101-V2.

Commande Setlog

La commande Setlog vous permet de définir le niveau de journalisation pour différents modules de l'unité KX II-101-V2 et d'afficher les niveaux de journalisation actuels de chaque module. La syntaxe de la commande setlog est la suivante :

```
setlog [module <module>] [level <level>] [vflag <vflag>] [verbose <on|off>]
Set/Get diag log level
```

Les options de la commande Setlog sont décrites dans le tableau suivant. Le support technique Raritan vous indiquera comment configurer ces paramètres.

Option de commande	Description
module	Le nom du module.
level	Le niveau de diagnostic : <ul style="list-style-type: none"> ▪ err ▪ warn ▪ info ▪ debug ▪ trace
vflag	Le type d'indicateur verbeux : <ul style="list-style-type: none"> ▪ timestamp ▪ module ▪ thread ▪ fileline
verbose [on off]	Active ou désactive la journalisation en mode verbeux.

Exemple d'utilisation de la commande Setlog

La commande Setlog suivante définit le niveau de journalisation de façon à déboguer avec la journalisation verbeuse activée pour le module libpp_serial.

```
Setlog module libpp_serial level debug verbose on
```

Configuration

Le menu Configuration vous permet d'accéder aux commandes du réseau utilisées afin de configurer l'interface réseau et de définir le nom du dispositif.

Réseau

Les commandes Configuration > Network (Réseau) permettent de configurer la connexion réseau et le nom du dispositif KX II-101-V2.

Commande	Description
interface	Configure l'interface réseau du dispositif KX II-101-V2.
name	Définit le nom du dispositif.
ipv6_interface	Définit/Extrait les paramètres réseau IPv6.

Commande interface

La commande interface permet de configurer l'interface réseau de l'unité KX II-101-V2. Lorsque la commande est acceptée, le dispositif abandonne la connexion HTTP/HTTPS et initialise une nouvelle connexion réseau. Tous les utilisateurs HTTP/HTTPS doivent se reconnecter au dispositif à l'aide de la nouvelle adresse IP, ainsi que du nom d'utilisateur et du mot de passe corrects. Reportez-vous à **Installation et configuration** (à la page 9).

La syntaxe de la commande interface est la suivante :

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode
<auto/10hdx/10fdx/100hdx/100fdx>]
```

Les options de la commande interface sont décrites dans le tableau suivant.

Option de commande	Description
ipauto	Adresse IP statique ou dynamique
ip ipaddress	Adresse IP de KX II-101-V2 attribuée pour un accès depuis le réseau IP.
mask subnetmask	Masque de sous-réseau obtenu auprès de l'administrateur IP.
gw ipaddress	Adresse IP de la passerelle obtenue auprès de l'administrateur IP.
mode <auto 100fdx>	Définit le mode Ethernet sur détection

Option de commande	Description
	automatique ou impose 100 Mbit/s full duplex (100fdx).

Exemple d'utilisation de la commande interface

La commande suivante définit l'adresse IP, le masque et les adresses de passerelle. Elle définit également le mode sur détection automatique.

```
Admin Port > Config > Network > interface ipauto none  
ip 192.168.50.12 mask 255.255.255.0 gw 192.168.51.12 mode  
auto
```

Commande name

La commande name permet de configurer le nom de l'unité et de l'hôte.

Syntaxe

```
name [unitname name] [domain name] [force <true|false>]
```

Exemple d'utilisation de la commande name

La commande suivante définit le nom de l'unité :

```
Admin Port > Config > Network > name unitname <unit name>  
domain <host name> force trues
```

Commande IPv6

Utilisez IPv6_command pour définir des paramètres réseau IPv6 et extraire les paramètres IPv6 existants.

```
Ipv6_interface mode enable ipauto none ip  
2001:db8:290c:1291::17 prefixlen 128 gw  
2001:db8:290c:1291::1
```

Commande listports

La commande listports répertorie le nombre d'utilisateurs actifs, les noms d'utilisateur, le port et l'état.

Exemple d'utilisation de la commande listports

```
Admin Port > listports
Port Port                Port Port  Port
No.  Name                Type Status Availability
1 - Dominion_KXII-101_V2_Port KVM  up    idle
```

Commande Userlist

La commande Userlist répertorie le port, son nom, son type, son état et sa disponibilité.

Exemple d'utilisation de la commande Userlist

```
Admin Port > Userlist
Active user number: 1
User Name | From          | Status
-----
-
admin     | Admin Port | active
```


Chapitre 12 Gestion CC-SG

Dans ce chapitre

Présentation	200
Suspension de la gestion du dispositif KX II-101-V2 par CC-SG.....	201
Utilisation de CC-SG en mode proxy	202

Présentation

CC-SG peut gérer KX II-101-V2. Une fois l'unité sous gestion par CC-SG, l'accès mobile à KX II-101-V2 est pris en charge depuis un iPad® ou un iPhone®. Pour en savoir plus sur l'ajout de KX II-101-V2 à la console CC-SG afin que cette dernière gère le dispositif et sur le paramétrage de l'accès mobile au dispositif, consultez la documentation de CC-SG.

Lorsqu'un dispositif KX II-101-V2 est géré par CommandCenter Secure Gateway et que vous tentez d'accéder au dispositif directement à l'aide de la console distante KX II-101-V2, le message suivant s'affiche (après l'entrée d'un nom d'utilisateur et d'un mot de passe valides) :

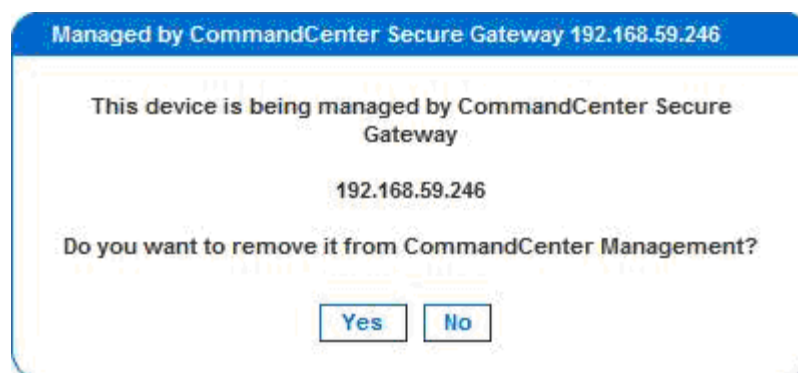


Suspension de la gestion du dispositif KX II-101-V2 par CC-SG

A moins que la gestion de KX II-101-V2 par CC-SG ne soit suspendue, vous ne pouvez pas accéder au dispositif directement. Toutefois, si KX II-101-V2 ne reçoit pas les messages de détection de collision de CommandCenter (par exemple, CommandCenter n'est pas sur le réseau), vous pouvez suspendre la gestion de KX II-101-V2 par CC-SG afin de pouvoir accéder au dispositif. Vous pouvez le faire par l'intermédiaire de la fonction CC Unmanage (Suspendre la gestion par CC).

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

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

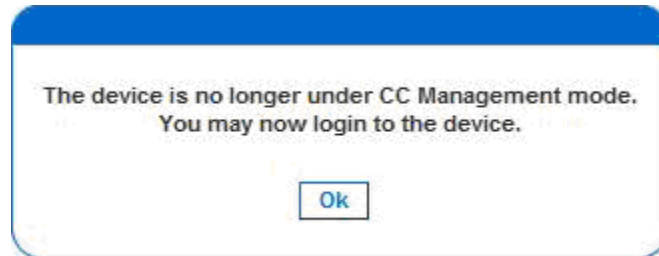


► **Pour suspendre la gestion du dispositif par CC-SG (pour utiliser CC Unmanage) :**

1. Cliquez sur Yes (Oui). Vous êtes invité à confirmer l'action.



2. Cliquez sur Yes (Oui). Un message s'affiche pour confirmer que le dispositif n'est plus placé sous la gestion de CC.



3. Cliquez sur OK. La page de connexion de l'unité KX II-101-V2 s'ouvre.

Utilisation de CC-SG en mode proxy

Version de Virtual KVM Client non reconnue par le mode proxy CC-SG

Lorsque le Virtual KVM Client est démarré depuis 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), « Version Unknown » (Version inconnue) s'affiche.

Mode proxy et MPC

Si vous utilisez l'unité KX II-101-V2 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).

Annexe A Caractéristiques

Dans ce chapitre

Spécifications physiques	203
Systèmes d'exploitation pris en charge (Clients)	204
Navigateurs pris en charge.....	205
Connecteurs	206
Modems certifiés	206
Résolutions vidéo prises en charge	206
Langues des claviers pris en charge.....	208
Ports TCP et UDP utilisés	209
Paramètres de vitesse réseau.....	211
Brochage à 9 broches	212

Spécifications physiques

KX II-101-V2...	Description
Facteur de forme	Facteur de forme zéro-U ; montable sur rack verticalement ou horizontalement (kit de fixation inclus)
Dimensions (PxLxH)	4,055" x 2,913" x 1,063" ; 103 x 74 x 27 mm
Poids	0,6498 lb ; 0,295 kg
Alimentation	Adaptateur d'alimentation AC/DC (100-240 V~/6 VDC) ou par Ethernet (PoE) ; compatible avec IEEE 802.3af Entrée d'alimentation de mi-portée Entrée d'alimentation pour paire de signaux Dispositif alimenté par alimentation de Classe 2 via Ethernet (sous 7 Wts)
Température de fonctionnement	0° - 40° C (32° - 104° F)
Humidité	20 à 85 %
Indicateurs : Logo rétroéclairé bleu RARITAN	Indicateur de démarrage et d'alimentation Indicateur d'activité réseau et de vitesse de connexion
Voyant jaune et vert	
Connexion locale :	1 - Port mini-USB pour clavier/souris USB et connectivité du support virtuel à la cible 1 - Port MiniDIN9 pour port série multifonction des fonctionnalités RS-232, connexion modem et

KX II-101-V2...	Description
	connectivité Dominion PX
Connexion à distance : Protocoles réseau	1 port Ethernet (RJ45) avec indicateur de statut d'activité TCP/IP, TELNET, SSH, HTTP, HTTPS, LDAP sécurisé, RADIUS, LDAP, SNMP v2 et v3, DHCP et SNTP, double pile : IPv4 et IPv6
Garantie	Deux ans 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, pour les images ISO

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®	<ul style="list-style-type: none"> Internet Explorer® 6.0 SP1+ ou 7.0, IE 8 Firefox® 1.06 - 4 ou supérieur
	Windows Server 2003®	<ul style="list-style-type: none"> Internet Explorer 6.0 SP1++, IE 7, IE 8 Firefox 1.06 - 3
	Windows Vista®	<ul style="list-style-type: none"> Internet Explorer 7.0 ou 8.0
	Windows 7®	<ul style="list-style-type: none"> Internet Explorer 9.0 Firefox 1.06 - 4 ou supérieur
Windows x64 mode 64 bits	Windows XP	SE 64 bits, navigateurs 32 bits :
	Windows XP Professionnel®	
	Windows XP Edition Tablet PC®	
	Windows Vista	Mode 64 bits, navigateurs 64 bits :
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	
	<ul style="list-style-type: none"> Internet Explorer 7.0 ou 8.0 	

Navigateurs pris en charge

KX II-101-V2 prend en charge les navigateurs suivants :

- Internet Explorer® 7 à 9
- Firefox® 4 ou supérieur
- Safari® 3 ou supérieur

Connecteurs

Type d'interface	Longueur		Description
	Pouces	Centimètres	
Câble KVM avec PS/2 et USB	15"	38 cm	Câble intégré
MiniDin9(M) vers DB9(F)	72"	182 cm	Câble pour série
DKX2-101-V2-PDU (facultatif)	70,86"	180 cm	Câble pour connexion à un Dominion PX

Modems certifiés

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

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-101-V2, 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-101-V2 prend en charge ces résolutions :

Résolutions	
640 x 350 à 70Hz	1024 x 768 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

Résolutions	
640 x 480 à 66,6Hz	1152 x 864 à 75Hz
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.

Langues des claviers pris en charge

L'unité KX II-101-V2 fournit un support clavier pour les langues indiquées dans le tableau suivant.

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 (Taiwan)	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
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 121). Toutes les requêtes reçues par KX II-101-V2 via HTTP (port 80) sont automatiquement transmises à HTTPS pour garantir une sécurité complète. Pour plus de facilité, KX II-101-V2 répond au port 80 (les utilisateurs n'ont ainsi pas à taper explicitement dans le champ URL pour accéder à KX II-101-V2) 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 121). 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-101-V2 (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 115).
SNTP (serveur d'horloge) sur le port UDP configurable 123	KX II-101-V2 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-101-V2 est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole LDAP, les ports 389 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-101-V2 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-101-V2 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-101-V2 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	Le port 161 est utilisé pour l'accès SNMP entrant/sortant, en

défaut SNMP	lecture/écriture, et le port 162 est utilisé pour le trafic sortant des traps SNMP. Facultatif
Port TCP 22	Le port 22 est utilisé pour l'interface de ligne de commande de KX II-101-V2 (lorsque vous travaillez avec l'assistance technique Raritan).

Paramètres de vitesse réseau

Paramètre de vitesse réseau KX II-101-V2


Paramètre de port de commutateur réseau	Auto	100/Full	100/Half	10/Full	10/Half
Auto	Vitesse disponible maximale	KX II-101-V2 : 100/Full Commutateur : 100/Half	100/Half	KX II-101-V2 : 10/Full Commutateur : 10/Half	10/Half
100/Full	KX II-101-V2 : 100/Half Commutateur : 100/Full	100/Full	KX II-101-V2 : 100/Half Commutateur : 100/Full	Aucune communication	Aucune communication
100/Half	100/Half	KX II-101-V2 : 100/Full Commutateur : 100/Half	100/Half	Aucune communication	Aucune communication
10/Full	KX II-101-V2 : 10/Half Commutateur : 10/Full	Aucune communication	Aucune communication	10/Full	KX II-101-V2 : 10/Half Commutateur : 10/Full
10/Half	10/Half	Aucune communication	Aucune communication	KX II-101-V2 : 10/Full Commutateur : 10/Half	10/Half


Légende :

	Ne fonctionne pas comme prévu
--	-------------------------------

 Prise 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-101-V2 diffère du comportement attendu.

Remarque : pour assurer une communication réseau fiable, configurez KX II-101-V2 et le commutateur LAN sur les mêmes valeurs de vitesse d'interface de réseau local et duplex. Par exemple, configurez KX II-101-V2 et le commutateur LAN sur Autodetect (détection automatique) (recommandé) ou sur une vitesse fixe/duplex, comme 100Mo/s/Full.

Brochage à 9 broches

Désignation de broche	
1	DTR (entrée)
2	TXD (sortie)
3	RXD (entrée)
4	DCD/DSR (entrée) *
5	GND
6	DTR (sortie)
7	CTS (entrée)
8	RTS (sortie)
9	RI (entrée)

Annexe B Mise à jour du schéma LDAP

Remarque : seuls des utilisateurs confirmés devraient effectuer les procédures de ce chapitre.

Dans ce chapitre

Renvoi des informations relatives aux groupes d'utilisateurs	213
Définition du Registre pour autoriser les opérations d'écriture sur le schéma	214
Création d'un attribut	214
Ajout d'attributs à la classe	215
Mise à jour du cache de schéma.....	217
Modification des attributs rciusergroup pour les membres utilisateurs .	217

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.

A partir de LDAP

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.

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.

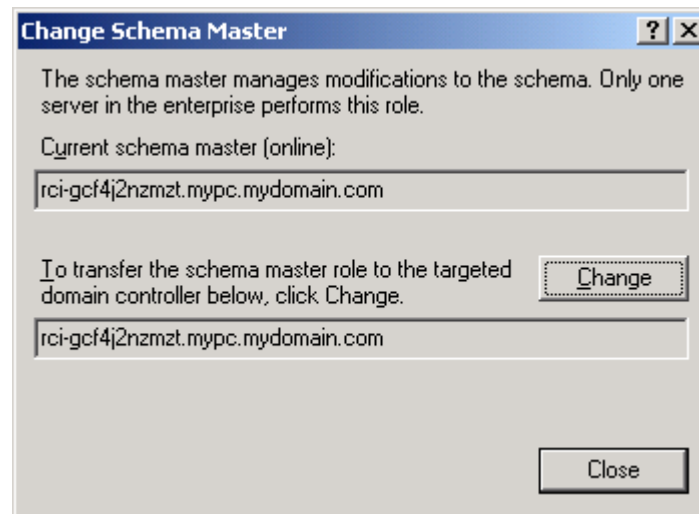
2. Lancez la console Active Directory et sélectionnez Active Directory Schema (Schéma Active Directory).

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 rcigroup :**

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.

Create New Attribute

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

Multi-Valued

OK Cancel

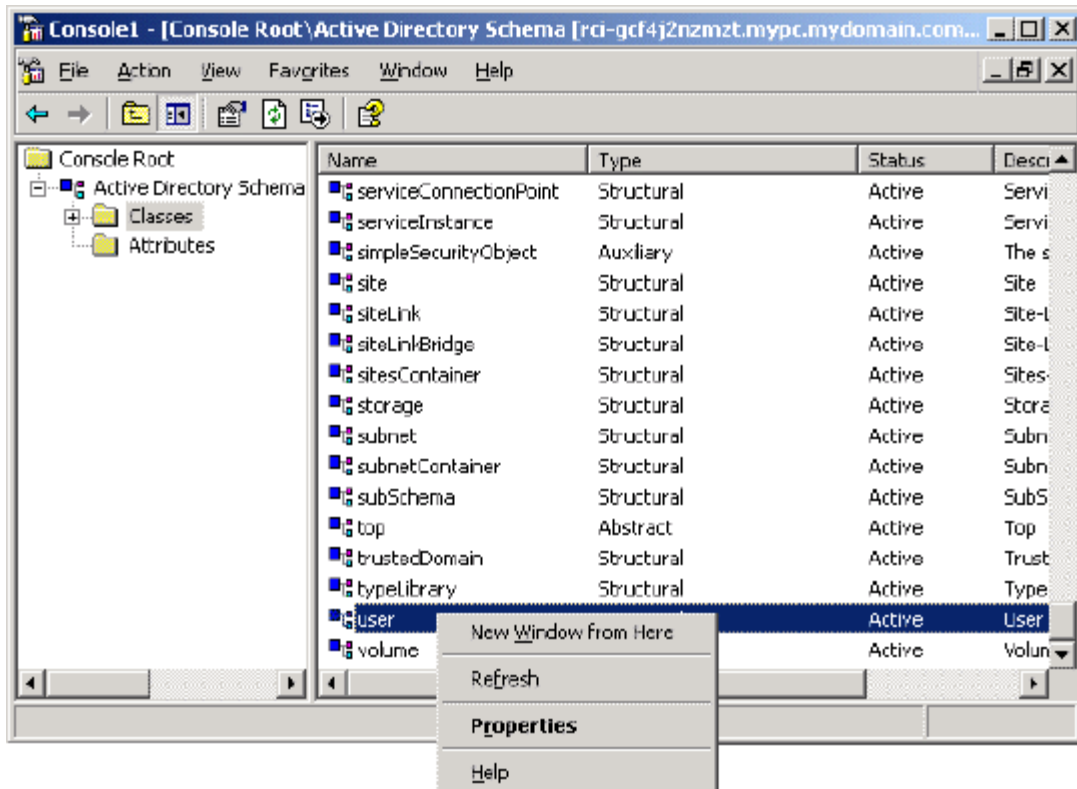
4. Tapez *rciusergroup* dans le champ Nom commun.
5. Tapez *rciusergroup* dans le champ Nom LDAP affiché.
6. Tapez *1.3.6.1.4.1.13742.50* dans le champ ID d'objet X.500 unique.
7. Entrez une description significative dans le champ Description.
8. Cliquez sur la flèche de la liste déroulante Syntaxe et 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 :**

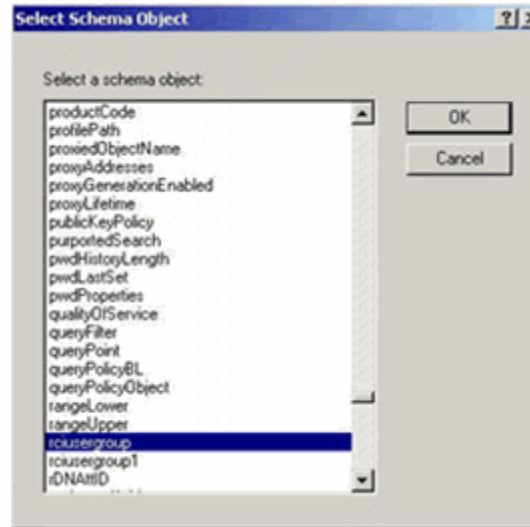
1. Cliquez sur Classes dans le volet de gauche de la fenêtre.

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 rcusergroup 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).

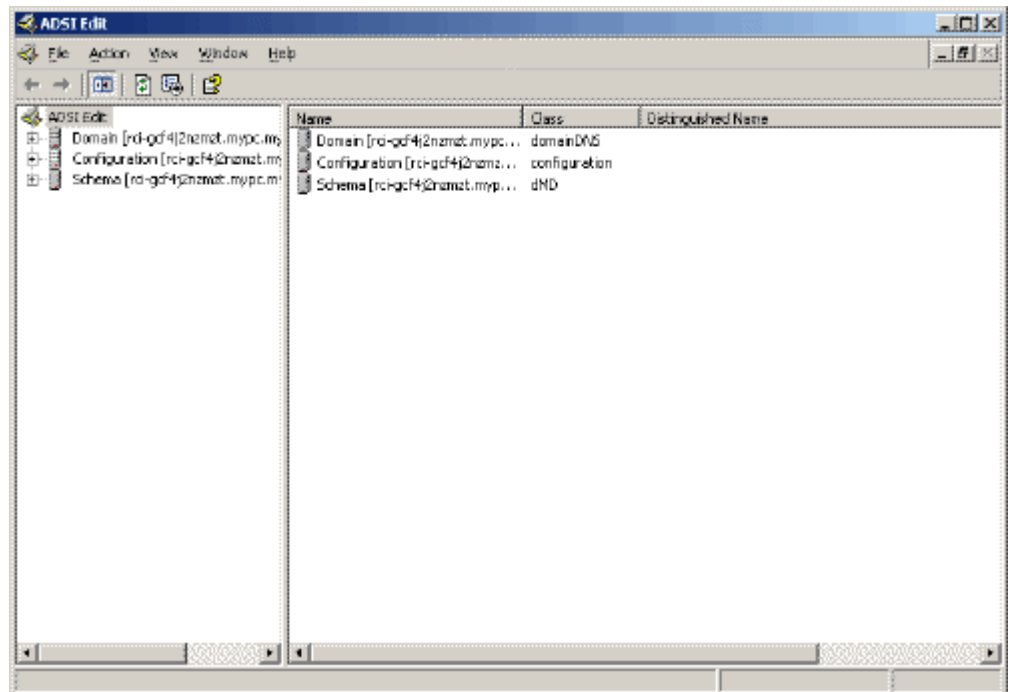
Modification des attributs rcusergroup pour les membres utilisateurs

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 rcusergroup, procédez comme suit :**

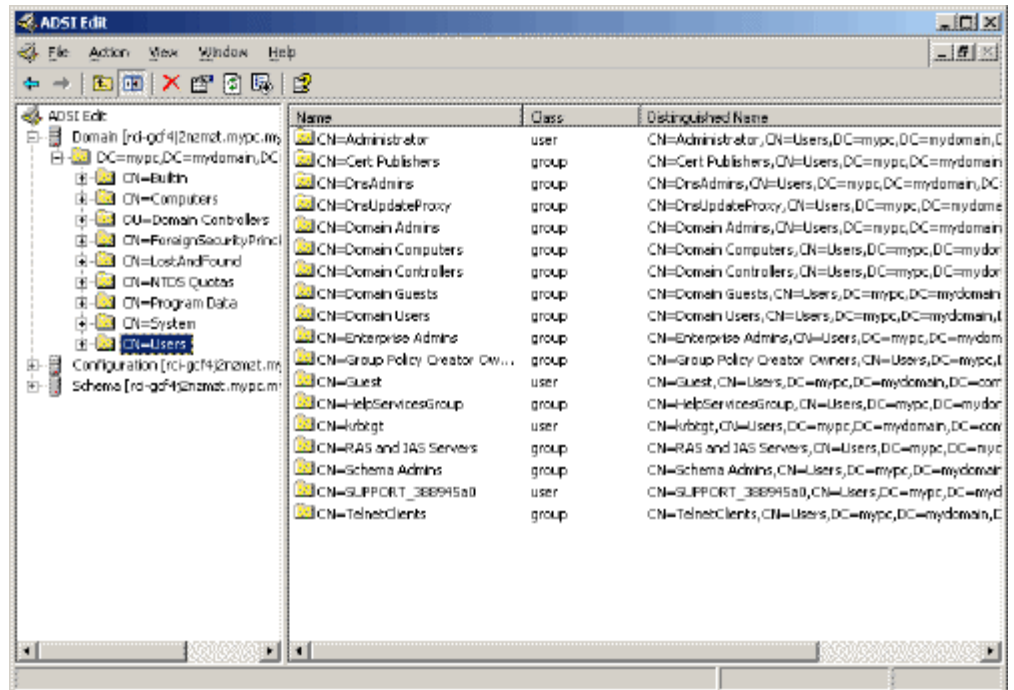
1. Sur le CD d'installation, sélectionnez Support > Outils (Outils).

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.



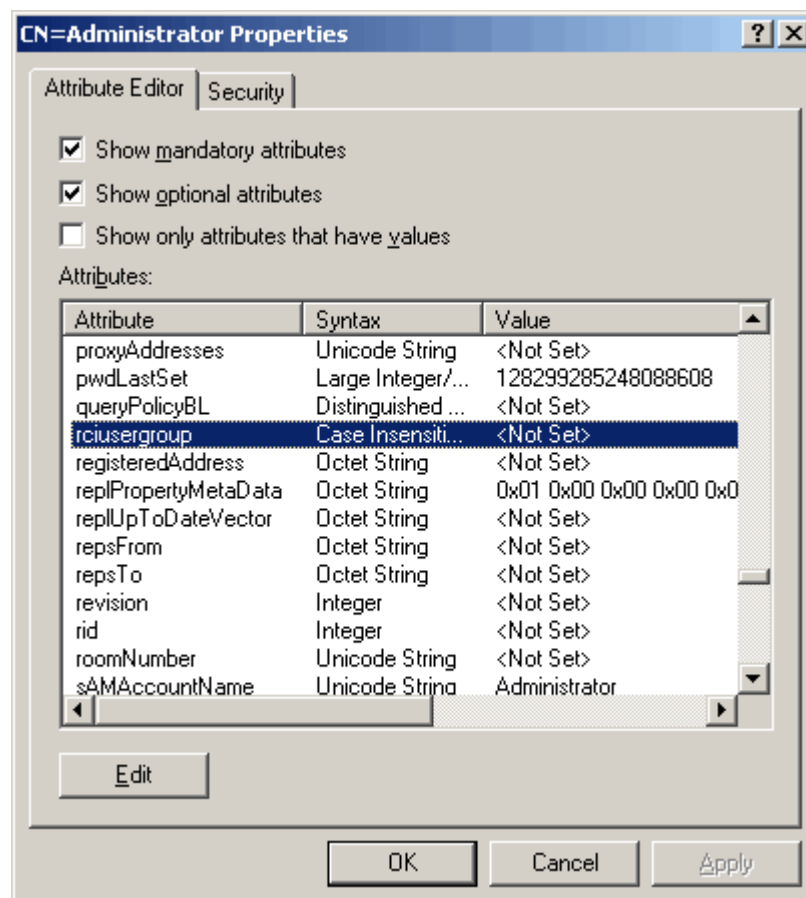
4. Ouvrez le domaine.

5. Dans le volet gauche de la fenêtre, sélectionnez le dossier CN=Users.

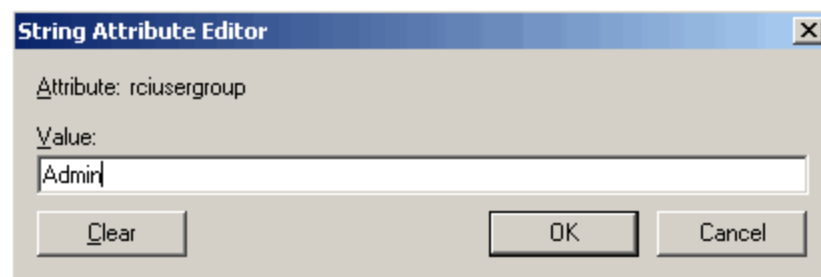


6. Recherchez le nom d'utilisateur dont vous souhaitez régler les propriétés dans le volet de droite. Cliquez avec le bouton droit sur le nom d'utilisateur et sélectionnez Propriétés.

7. Cliquez sur l'onglet Editeur d'attribut s'il n'est pas déjà ouvert. Sélectionnez rcusergroup 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-101-V2) dans le champ Modifier l'attribut. Cliquez sur OK.



Annexe C Montage en rack

Le dispositif KX II-101-V2 peut être monté verticalement ou horizontalement, face à l'avant ou à l'arrière, sur n'importe quel côté d'un rack de serveur. Utilisez les supports de fixation et les vis inclus dans le kit KX II-101-V2.

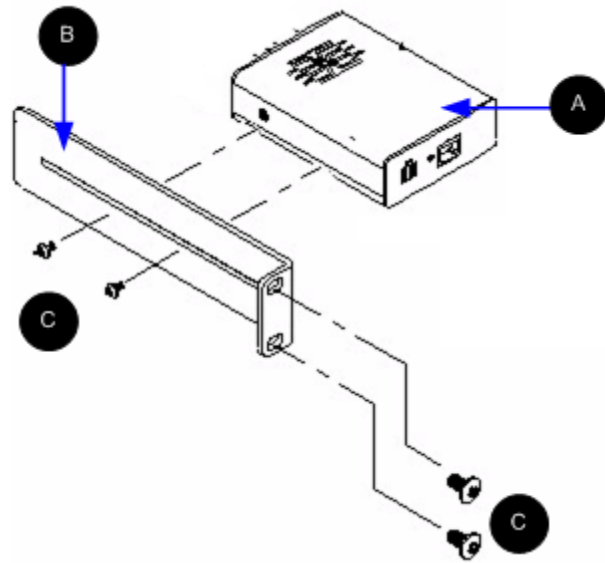
Dans ce chapitre

Attachez la fixation en L au dispositif KX II-101-V2 pour un montage horizontal221

Attachez la fixation en L au dispositif KX II-101-V2 pour un montage horizontal



1. Attachez la fixation en L au dispositif KX II-101-V2 en utilisant les vis incluses. Ajustez le placement des fixations avant de visser.
2. Montez l'assemblage fixation en L sur le rack et fixez le tout avec les vis fournies par le fabricant du rack.

L'image ci-dessous illustre le montage du dispositif KX II-101-V2 sur la gauche. Pour monter le dispositif KX II-101-V2 sur la droite, suivez ces instructions, mais attachez les fixations sur le côté droit.



Légende du schéma

	KX II-101-V2
---	--------------

Légende du schéma	
	Fixation en L
	Vis

Annexe D Remarques informatives

Dans ce chapitre

Java Runtime Environment (JRE)	223
Remarques sur la prise en charge d'IPv6	224
Remarques concernant le clavier, la vidéo et la souris	224
CC-SG	227

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 distante 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 1.7 de JRE pour garantir des performances optimales. La console distante et MPC fonctionnent cependant avec les versions 1.6.x et supérieures 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

Remarques sur la prise en charge d'IPv6 par système d'exploitation

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)

Les configurations IPv6 suivantes *ne sont pas* prises en charge par Java :

- J2SE 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.

Mac Leopard

- IPv6 n'est pas pris en charge dans la version 2.0.20 de KX II pour Mac® Leopard®.

Remarques concernant le clavier, la vidéo et la souris

Les équipements ci-après connaissent certaines restrictions quant au clavier, à la vidéo ou à la souris. Le cas échéant, une solution de contournement est fournie.

Restriction de Sun Blade quant à la prise en charge de la vidéo, du clavier et de la souris

Vidéo

Si vous accédez à Sun™ Blade 100 avec le dispositif KX II-101-V2, la vidéo sur le port local ou une connexion à distance risque de ne pas fonctionner correctement lors du démarrage de Sun Blade. Pour éviter ce problème, utilisez le firmware Sun Open Boot 4.17.1 ou une version supérieure.

Clavier et souris

Sun Blade ne prenant pas en charge plusieurs claviers et aucun port local de clavier ou de souris n'étant fourni, le dispositif KX II-101-V2 et un clavier local ne peuvent pas être utilisés en même temps. Cependant, un clavier et une souris à distance peuvent être utilisés pour Sun Blade.

Restriction d'accès au BIOS depuis un clavier local

Une connexion USB est nécessaire pour la synchronisation de souris absolue. Cependant, les claviers de cette section ne prennent pas en charge la connexion USB au clavier local. Pour accéder au clavier local via le BIOS ou des supports virtuels au moyen du port local, utilisez les configurations suivantes :

Clavier	Configuration à utiliser
Dell® OptiPlex™ GX280 - BIOS A03	Le BIOS et les supports virtuels sont accessibles pour les claviers locaux et à distance à l'aide d'un adaptateur Newlink USB vers PS/2. Réglez l'option Host Interface (Interface hôte) sur PS/2 dans la page Keyboard/Mouse Setup (Configuration du clavier et de la souris). Reportez-vous à Configuration du clavier et de la souris (voir " Configuration du clavier/de la souris " à la page 125).
Dell Dimension 2400– BIOS A05	Réglez l'option Host Interface (Interface hôte) sur PS/2 dans la page Keyboard/Mouse Setup (Configuration du clavier et de la souris). Reportez-vous à Configuration du clavier et de la souris (voir " Configuration du clavier/de la souris " à la page 125).
Dell Optiplex 170L - BIOS A07	PS/2 et adaptateur PS/2 vers USB. Réglez l'option Host Interface (Interface hôte) sur PS/2 dans la page Keyboard/Mouse Setup (Configuration du clavier et de la souris). Reportez-vous à Configuration du clavier et de la souris (voir " Configuration du clavier/de la souris " à la page 125).

Clavier	Configuration à utiliser
Dell Server 1850	<p>Pour que le BIOS version A06 reconnaisse la clé USB de support virtuel amovible, utilisez les connexions PS/2 et USB entre le serveur Dell et le dispositif KX II-101-V2.</p> <p>Réglez l'option Host Interface (Interface hôte) sur PS/2 dans la page Keyboard/Mouse Setup (Configuration du clavier et de la souris). Reportez-vous à Configuration du clavier et de la souris (voir "Configuration du clavier/de la souris" à la page 125).</p>

Configuration clavier et souris HP UX RX 1600

Si vous utilisez HP® UX RX 1600 sous UNIX®, suivez la procédure ci-après pour connecter le dispositif à la cible :

- Vérifiez que vous utilisez bien le firmware KX II-101-V2 2.0.20.5.6964 ou supérieur.
- Utilisez le câble USB fourni avec KX II-101-V2.
- Paramétrez le champ Host Interface (Interface hôte) de la page Keyboard/Mouse Setup (Configuration du clavier/de la souris) sur USB. Reportez-vous à **Configuration du clavier/de la souris** (à la page 125).
- Vérifiez que les cases Enable Absolute Mouse (Activer la souris absolue) et Use Full Speed (Utiliser le plein régime) de la page Port sont cochées.
- Utilisez le mode souris intelligente ou souris standard. N'utilisez pas le mode Absolute Mouse (Souris absolue).

Restriction du mode de souris pour serveurs Compaq Alpha et IBM P

Lorsque vous vous connectez aux serveurs Compaq® Alpha ou IBM® P via KX II-101-V2, vous devez utiliser le mode de souris unique. Reportez-vous à **Utilisation des serveurs cible** (à la page 38).

Restrictions des serveurs Windows 2000 et Windows 2003 quant au clavier

A cause de restriction du système d'exploitation, les combinaisons de touches ci-après ne fonctionnent pas avec un clavier US-International (Anglais international) lorsque vous utilisez le système d'exploitation Windows 2000® et les serveurs Windows 2003®.

- Alt de droite +D
- Alt de droite + I
- Alt de droite + L

Remarque : la touche Alt de droite peut être libellée Alt Gr sur les claviers dont les touches indiquent les fonctions US/International.

CC-SG

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).

Annexe E FAQ

Dans ce chapitre

Foire aux questions générale	228
Gestion de réseau IPv6	229

Foire aux questions générale

Question	Réponse
Quelle est la différence entre Dominion KX II-101-V2 et la génération précédente Dominion KX II-101 ?	Dominion KX II-101-V2 est le modèle économique de la toute dernière génération. V2 prend en charge virtuellement toutes les fonctions de la génération précédente KX II-101, auxquelles s'ajoutent de nombreuses fonctions supplémentaires remarquables. La version V2 ne prend pas en charge l'alimentation par Ethernet (PoE) ou un port local PS2.
Comment fonctionne Dominion KX II-101-V2 ?	Dominion KX II-101-V2 se branche sur les ports clavier, vidéo et souris d'un serveur. Il capture, numérise et comprime le signal vidéo avant de transmettre à un PC client distant à l'aide de la technologie d'acquisition vidéo et de compression performante de Raritan. Dominion KX II-101-V2 offre un ensemble complet de fonctions dans une interface utilisateur intuitive. Il peut également être contrôlé de manière centralisée avec d'autres dispositifs de gestion par CommandCenter® Secure Gateway.
Quels types de serveurs peuvent être contrôlés à distance par Dominion KX II-101-V2 ?	Dominion KX II-101-V2 fonctionne indépendamment du matériel, du système d'exploitation ou des applications d'un serveur cible dont il accède aux dispositifs d'entrée et de sortie principaux, clavier, vidéo et souris. Aussi, tous les matériels prenant en charge les interfaces standard de clavier et de souris PC, et la vidéo PC standard (VGA) peuvent être utilisés avec Dominion KX II-101-V2.
Des fonctions de sécurité permettent-elles de protéger mes serveurs cible d'une connexion à distance non autorisée ?	Oui. KX II-101-V2 offre plusieurs couches de sécurité : authentification de connexion et sécurité du transfert des données pendant une session à distance. Les noms d'utilisateur, les mots de passe et les clés privées servent à authentifier les utilisateurs. Dominion KX II-101-V2 peut authentifier des utilisateurs à l'aide de la base de données qui y réside localement ou à l'aide de serveurs AAA externes (LDAP, Active Directory® ou RADIUS). Toutes les données clavier, vidéo et souris sont chiffrées avec le système AES utilisant jusqu'à 256 bits.
Quels types de supports virtuels Dominion KX II-101-V2 prend-il en charge ?	KX II-101-V2 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 de lecteurs distants.
Le support virtuel est-il fiable ?	Oui. Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement AES de 256 bits.

Question	Réponse
KX2-101-V2 dispose-t-il d'un port local ?	Oui, il dispose d'un port VGA-USB, mais aucun câble de port local n'est nécessaire. Pour obtenir un accès local au serveur connecté, branchez votre écran LCD au port Local VGA de KX2-101-V2. Connectez le clavier et la souris USB directement au serveur cible.
Quelles nouvelles fonctions sont disponibles dans la dernière version ?	<p>Avec la version 3.5 (et supérieur), les fonctions suivantes sont maintenant disponibles :</p> <ul style="list-style-type: none"> • Résolution vidéo 1920 x 1080 • Accès iPad et iPhone (CC-SG obligatoire) • Double pile IPv6 • Module de chiffrement FIPS 140-2 • Déconnexion d'utilisateur et de port • SNMPv3 • Prise en charge supplémentaire de supports virtuels des clients Linux et Mac • Prise en charge de l'interface utilisateur en japonais, chinois traditionnel et chinois simplifié • Menu d'aide • Bannière de connexion • Téléversement du certificat SSL du client • Numéros de port configurables

Gestion de réseau IPv6

Question	Réponse
Qu'est-ce qu'IPv6 ?	<p>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.</p> <p>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.</p> <p>IPv6 résout l'un des problèmes les plus épineux rencontrés par l'administrateur : la configuration et la gestion d'un réseau IP.</p>

Question	Réponse
Pourquoi KX II-101-V2 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 KX II-101-V2 ?	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.
Et si je dispose d'un serveur externe avec une adresse IPv6 que je souhaite utiliser avec KX II-101-V2 ?	<p>KX II-101-V2 peut accéder aux serveurs externes via leurs adresses IPv6 ; par exemple, un gestionnaire SNMP, un serveur Syslog ou un serveur LDAP.</p> <p>Grâce à l'architecture à double pile de KX II-101-V2, ces serveurs externes sont accessibles via (1) une adresse IPv4, (2) une adresse IPv6 ou (3) un nom d'hôte. KX II-101-V2 prend donc en charge l'environnement mixte IPv4-IPv6 dont de nombreux clients disposent.</p>
Et si mon réseau ne prend pas en charge IPv6 ?	La gestion de réseau par défaut de KX II-101-V2 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 KX II-101-V2 décrit la prise en charge d'IPv6 par KX II-101-V2.

Index

A

- A
- Alimentation - 25
- A partir d'Active Directory (AD) de Microsoft - 213
- A partir de LDAP - 213
- Accès à l'unité KX II-101-V2 à l'aide du CLI - 191
- Accès SSH depuis un PC Windows - 191
- Accès SSH depuis un poste de travail UNIX/Linux - 192
- Activation de FIPS 140-2 - 161, 163
- Activation de l'accès direct aux ports - 38
- Activation de l'accès direct aux ports via URL - 122
- Activation de SSH - 120
- Activation de Telnet - 120
- Actualisation de l'écran - 60
- Affectation d'une adresse IP - 10, 30
- Affichage de la liste des utilisateurs de KX II-101-V2 - 97
- Affichage des utilisateurs par port - 97
- Affichage du MIB de KX II-101-V2 - 122, 129, 135
- Aide KX II-101-V2 - 3
- Ajout d'attributs à la classe - 215
- Ajout d'un nouveau groupe d'utilisateurs - 91
- Ajout d'un nouvel utilisateur - 99, 100
- Ajout, modification et suppression des favoris - 46
- Ajustement des paramètres vidéo - 61
- Alimentation - 7
- Arrêt de la gestion par CC-SG - 181
- Attachez la fixation en L au dispositif KX II-101-V2 pour un montage horizontal - 221
- Authentification à distance - 33

B

- B
- Serveur cible - 25
- Backup and Restore (Sauvegarde et restauration) - 175
- Bannière de sécurité - 171
- Blocage des utilisateurs - 100, 154, 157
- Blocage et déblocage des utilisateurs - 100
- Boutons de barre d'outils et icônes de barre d'état - 48

- Branchement de la barrette d'alimentation - 141

- Brochage à 9 broches - 212

C

- C
- Réseau - 28
- Caractéristiques - 203
- Caractéristiques d'administration - 6
- Caractéristiques du produit - 5
- Caractéristiques du système de gestion - 6
- Caractéristiques utilisateur - 7
- CC-SG - 227
- Certificats SSL - 168
- Commande interface - 197
- Commande IPv6 - 198
- Commande listports - 194, 199
- Commande name - 194, 198
- Commande Setlog - 195, 196
- Commande Userlist - 195, 199
- Commandes CLI - 190, 194
- Commandes courantes pour tous les niveaux de la CLI - 194
- Commutateur KVM analogique - 125, 145
- Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible - 84, 86
- Conditions requises pour l'utilisation des supports virtuels - 80, 85
- Configuration - 197
- Configuration clavier et souris HP UX RX 1600 - 226
- Configuration de KX II-101-V2 à l'aide de la console à distance - 29
- Configuration de KX II-101-V2 à l'aide d'un programme d'émulation de terminal (facultatif) - 10, 29, 35, 192
- Configuration de la gestion des événements - Destinations - 136
- Configuration de la gestion des événements - Paramètres - 129, 136
- Configuration de la résolution vidéo du serveur - 11, 12
- Configuration de Syslog - 135
- Configuration des agents SNMP - 122, 129
- Configuration des autorisations - 91, 94, 95
- Configuration des paramètres de balayage dans VKC et AKC - 73

Configuration des paramètres de date et heure - 128, 168
Configuration des ports - 23, 137
Configuration des traps SNMP - 129
Configuration du clavier/de la souris - 125, 145, 225, 226
Configuration du contrôle d'accès IP - 165
Configuration PS/2 - 27
Configuration réseau - 5
Configuration USB - 26
Connecteurs - 206
Connexion Properties (Propriétés de la connexion) - 51
Connexion - 192
Connexion à un serveur cible KVM - 48
Connexion aux supports virtuels - 86
Connexion SSH à KX II-101-V2 - 191
Connexions de câble pour l'accès par modem - 127
Contenu de l'emballage - 8
Contrôle d'un dispositif de barrette d'alimentation - 144
Création de groupes d'utilisateurs et d'utilisateurs - 34
Création d'un attribut - 214

D

D
Port Admin - 29
Déboguer - 194, 195
Déconnexion des serveurs cible KVM - 51
Déconnexion des supports virtuels - 85, 88
Déconnexion d'utilisateurs des ports - 98
Définition des autorisations d'accès aux ports - 91, 96
Définition des autorisations pour un groupe individuel - 95, 99
Définition du Registre pour autoriser les opérations d'écriture sur le schéma - 214
Définition d'un nouveau mot de passe - 30
Définition d'une macro de clavier - 57
Désignation du serveur cible - 33
Détection automatique des paramètres vidéo - 60
Détection des dispositifs Raritan sur le sous-réseau du dispositif KX II-101-V2 - 45
Détection des dispositifs Raritan sur le sous-réseau local - 44
Diagnostics - 183, 194, 195
Documentation connexe - 4
Données de connexion par défaut - 9

E

E
Port d'utilisateur local - 29
Encryption & Share (Chiffrement et partage) - 159
Etape 1
Configuration du serveur cible - 9, 10
Etape 2
Configuration des paramètres du pare-feu de réseau - 9, 23
Etape 3
Connexion de l'équipement - 9, 24
Etape 4
Configuration du dispositif KX II-101-V2 - 9, 29
Exigences en matière de prise en charge de FIPS 140-2 - 164

F

Factory Reset (Restauration des valeurs d'usine) - 179
FAQ - 228
Fermeture de la session des utilisateurs de KX II-101-V2 (Déconnexion forcée) - 98
Foire aux questions générale - 228

G

Gestion CC-SG - 200
Gestion de la sécurité - 154
Gestion de l'alimentation - 138, 140
Gestion de l'alimentation d'un serveur cible - 50
Gestion de réseau IPv6 - 229
Gestion des associations d'alimentation - 143
Gestion des barrettes d'alimentation Raritan - 126
Gestion des connexions USB - 149
Gestion des dispositifs - 115
Gestion des événements - 128
Gestion des favoris - 43
Gestion des serveurs cible KVM (page Port) - 138, 140
Gestion des utilisateurs - 34, 89
Groupes d'utilisateurs - 89

H

Historique des mises à niveau - 179

I

Implémentation de l'authentification à distance LDAP/LDAPS - 102, 107
 Implémentation de l'authentification à distance RADIUS - 107
 Importation/exportation de macros de clavier - 54
 Informations sur la connexion - 53
 Informations sur le dispositif - 174
 Installation et configuration - 9, 197
 Interface de la console distante KX II-101-V2 - 38
 Interface de ligne de commande (CLI) - 126, 190
 Interfaces - 5, 38
 Introduction - 1
 Invites CLI - 192

J

Java Runtime Environment (JRE) - 223
 Journal d'audit - 173

K

KX II-101-V2 - Présentation - 2

L

LAN Interface Settings (Paramètres de l'interface LAN) - 32, 115, 118, 119
 Lancement d'une macro de clavier - 59
 Langues des claviers pris en charge - 208
 LCA (liste de contrôle d'accès) IP de groupes - 92, 96
 Lecteurs locaux - 86
 Limitations de connexion - 154
 Liste des groupes d'utilisateurs - 90
 Liste des traps SNMP de KX II-101-V2 - 132

M

Macros de clavier - 54
 Maintenance - 173
 Mise à jour du cache de schéma - 217
 Mise à jour du schéma LDAP - 213
 Mise à niveau du firmware - 177
 Mise en route - 10
 Mode Full Screen (Mode Plein écran) - 75
 Mode proxy et MPC - 227
 Mode souris absolue - 69
 Mode souris intelligente - 68
 Mode souris standard - 67
 Modem - 126

Modems certifiés - 127, 206
 Modification des attributs rcusergroup pour les membres utilisateurs - 217
 Modification du paramètre de langue de l'interface utilisateur par défaut - 148
 Modification du taux de rafraîchissement maximum - 65
 Modification d'un groupe d'utilisateurs existant - 95
 Modification d'un mot de passe - 114
 Modification d'un utilisateur existant - 99
 Modification et suppression des macros de clavier - 59
 Montage - 7
 Montage des images
 CD-ROM/DVD-ROM/ISO - 87
 Montage en rack - 221
 Mots de passe sécurisés - 114, 154, 156
 Multi-Platform Client (MPC) - 47

N

Navigateurs pris en charge - 205
 Navigation dans la console KX II-101-V2 - 39
 Navigation de la CLI - 192
 Nommage de la barrette d'alimentation (Page Port pour les barrettes d'alimentation) - 140, 142
 Note aux utilisateurs de CC-SG - 33
 Nouveautés de l'aide - 4

O

Options d'affichage - 74
 Options d'aide - 76
 Options de clavier - 54
 Options de souris - 65
 Options d'outils - 70, 75

P

Page Device Diagnostics (Diagnostics du dispositif) - 188
 Page d'interface réseau - 183
 Page Favorites List (Liste des favoris) - 44, 45
 Page Manage Favorites (Gérer les favoris) - 44
 Page Network Statistics (Statistiques réseau) - 183
 Page Ping Host (Envoyer une commande Ping à l'hôte) - 186
 Page Port Access - 41
 Page Trace Route to Host - 186
 Panneau gauche - 39

Index

Paramètres Apple Macintosh - 22
Paramètres d'authentification - 101
Paramètres de connexion USB - 151
Paramètres de lancement client - 72
Paramètres de port série - 125
Paramètres de souris - 13
Paramètres de vitesse réseau - 119, 211
Paramètres des connexions USB avancées - 152
Paramètres des ports HTTP et HTTPS - 121, 210
Paramètres généraux - 70
Paramètres IBM AIX - 23
Paramètres Linux (pour le mode souris standard) - 20
Paramètres Linux (Red Hat 4 et 5, et Fedora 14) - 18
Paramètres réseau - 30, 32, 115, 116, 118, 210
Paramètres réseau de base - 115, 116
Paramètres Sun Solaris - 21
Paramètres Windows 2000 - 17
Paramètres Windows 7 et Windows Vista - 15
Paramètres Windows XP, Windows 2003 et Windows 2008 - 13
Photos du produit - 5
Port Action Menu (Menu d'action de ports) - 42
Port Admin - 126
Ports TCP et UDP utilisés - 209
Présentation - 9, 47, 78, 150, 190, 200
Processus d'authentification d'utilisateur - 112
Propriétés vidéo - 60
Protocoles pris en charge - 34

R

Redémarrage de KX II-101-V2 - 180
Réinitialisation de KX II-101-V2 à l'aide du bouton de réinitialisation - 147, 161
Relation entre les utilisateurs et les groupes - 90
Remarque relative à Microsoft Active Directory - 34
Remarques concernant le clavier, la vidéo et la souris - 224
Remarques informatives - 223
Remarques sur la prise en charge d'IPv6 - 224
Remarques sur la prise en charge d'IPv6 par système d'exploitation - 224
Renommage d'un port - 139

Renvoi des informations relatives aux groupes d'utilisateurs - 213
Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory - 106
Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS - 110
Réseau - 194, 197
Résolution vidéo - 7
Résolution vidéo Sun - 12
Résolutions vidéo prises en charge - 206
Restriction d'accès au BIOS depuis un clavier local - 225
Restriction de Sun Blade quant à la prise en charge de la vidéo, du clavier et de la souris - 225
Restriction du mode de souris pour serveurs Compaq Alpha et IBM P - 226
Restrictions concernant les claviers - 71
Restrictions des serveurs Windows 2000 et Windows 2003 quant au clavier - 227

S

Saisie automatique des commandes - 193
Saisie du port de détection - 121
Scaling (Mise à l'échelle) - 75
Se déconnecter - 47
Security Settings (Paramètres de sécurité) - 99, 154
Services du dispositif - 120, 191
Spécifications des échanges de communication RADIUS - 110
Spécifications physiques - 203
Support virtuel - 69, 77
Supports virtuels dans un environnement Linux - 82
Supports virtuels dans un environnement Mac - 84
Supports virtuels dans un environnement Windows XP - 81
Supports virtuels VKC - 69
Suspension de la gestion du dispositif KX II-101-V2 par CC-SG - 201
Synchronisation des pointeurs de souris - 66
Syntaxe CLI - Conseils et raccourcis - 193
Systèmes d'exploitation pris en charge (Clients) - 204

T

Terminologie - 7

U

- Utilisateurs - 96
- Utilisation de CC-SG en mode proxy - 202
- Utilisation de la commande Screenshot from Target - 64
- Utilisation des serveurs cible - 38, 226
- Utilisation des supports virtuels - 85

V

- Vérification de la prise en charge du chiffrement AES par votre navigateur - 160, 163
- View Status Bar (Afficher la barre d'état) - 74
- View Toolbar (Afficher la barre d'outils) - 74
- Virtual KVM Client (VKC) - 42, 47

▶ Etats-Unis/Canada/Amerique 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