Dominion KX III

Manuel de l'administrateur
Version 3.0.0

Copyright © 2014 Raritan, Inc.

DKX3A-v3.0.0-0B-F

Février 2014

255-62-0002-00

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

© Copyright 2014 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

Présentation 1
Nouveautés de l'aide 1
Contenu de l'emballage 2
Caractéristiques et Photos de l'appareil KX III 2
Matériel 2
Logiciel 3
Dominion KX3-832 4
Dominion KX3-864 6
Utilisateurs et ports pris en charge par modèle 7
Interfaces des consoles KX III locales et à distance 7
Applications Client KVM pour KX III 8
Aide en ligne KX II 8

Chapitre 2 Mise en route 9

Installer et configurer KX III: 9
Autorise les pop-ups : 9
Messages de validation et avertissements de sécurité 9
Avertissement d'accès et Validation de Java 9
Avertissements de Sécurité Supplémentaires 10
Installation d'un certificat 10
Exemple 1 : Importer le certificat dans le navigateur 11
Exemple 2 : Ajouter le KX III aux sites de confiance et importer le certificat 13
Connexion au KX III 14

Chapitre 3 Interface et navigation KX III 16

Présentation 16
Interface de console à distance de KX III 16
Page d'accès aux ports (Affichage de la console à distance) 17
Port Action Menu (Menu d'action de ports) 20
Panneau gauche 23
Navigation dans la console KX III 25
Interface de la console locale KX III 26

Chapitre 4 Aide pour l'administrateur de KX III 27

Présentation 27
Installation et configuration de KX III 28
Montage en rack 28
Données de connexion par défaut 29

Etape 1 : Configuration des paramètres du pare-feu réseau 30
Etape 2 : Configurer les serveurs cible KVM 30
Etape 3 : Connexion de l'équipement 34
Etape 4 : Configurer le KX III 37
Etape 5 : Lancement de la console à distance de KX III 42
Etape 6 : Configuration de la langue du clavier (facultatif) 44
Etape 7 : Créer et installer un certificat SSL 45
Gestion des prises des PDU de rack (barrettes d'alimentation) 46
Présentation 46
Mise sous/hors tension des prises et alimentation cyclique 47
Profils USB 49
Présentation 49
Compatibilité CIM 49
Profils USB disponibles 50
Sélection des profils pour un port KVM 56
User Management (Gestion des utilisateurs) 57
Groupes d'utilisateurs 57
Utilisateurs 66
Paramètres d'authentification 71
Modification d'un mot de passe 84
Gestion des dispositifs 85
Paramètres réseau 85
Configuration des ports 90
Services du dispositif 134
Configuration de l'alimentation 158
Scripts de connexion et de déconnexion 159
Port Group Management (Gestion des groupes de ports) 165
Modification du paramètre de langue de l'interface utilisateur par défaut 169
Gestion de la sécurité 169
Security Settings (Paramètres de sécurité) 169
Configuration du contrôle d'accès IP 181
Certificats SSL 183
Bannière de sécurité 187
Maintenance 188
Journal d'audit 188
Device Information (Informations sur le dispositif) 190
Backup and Restore (Sauvegarde et restauration) 192
USB Profile Management (Gestion des profils USB) 195
Mise à niveau des CIM 196
Mettre à jour le firmware KX III 197
Historique des mises à niveau 198
Redémarrage de KX III 198
Arrêt de la gestion par CC-SG 200
Diagnostics 201
Page d'interface réseau 201
Page Network Statistics (Statistiques réseau) 201
Page Ping Host (Envoi de commande Ping à l'hôte) 204
Page Trace Route to Host 204
Page Device Diagnostics (Diagnostics du dispositif) 206
Console locale KX III 207
Sécurité et authentification 208
Configurer les Paramètres du port local KX III à partir de la Console locale 209

Interface de ligne de commande (CLI) 213
Présentation 213
Accès à KX III à l'aide de la CLI 213
Connexion SSH à KX III 214
Connexion 214
Navigation de la CLI 215
Configuration initiale à l'aide de la CLI 217
Invites CLI 218
Commandes CLI 218
Administration des commandes de configuration du serveur de console de KX III 219
Configuration du réseau 219
Groupes de deux ports vidéo 222
Recommandations en matière de ports vidéo doubles 223
Modes de souris pris en charge pour les groupes de deux ports vidéo 223
CIM requis pour la prise en charge de vidéo double 224
Remarques relatives à l'utilisation des groupes de deux ports vidéo 225
Autorisations et accès aux groupes de deux ports vidéo 225
Exemple de configuration de groupe de deux ports vidéo 226
Etapes de configuration de deux ports vidéo 227
Navigation client Raritan lors de l'utilisation des groupes de deux ports vidéo 230
Accès direct aux ports et groupes de deux ports vidéo 231
Groupes de deux ports vidéo affichés sur la page Ports 231
Mise à jour du schéma LDAP 232
Renvoi des informations relatives aux groupes d'utilisateurs 232
Définition du Registre pour autoriser les opérations d'écriture sur le schéma 233
Création d'un attribut 233
Ajout d'attributs à la classe 234
Mise à jour du cache de schéma 236
Modification des attributs rciusergroup pour les membres utilisateurs 236

Chapitre 5 Aide Virtuelle pour Client KVM (VKC) 240

Présentation 240
Se connecte à un serveur cible 241
Configurer les propriétés de connexion 242
Propriétés d'accès de connexion 242
Concernant les Propriétés de connexion 242
Paramètres de propriétés de connexion par défaut - Optimisé pour de meilleures performances 243
Optimisé pour : Sélections 244
Mode vidéo 244
Noise Filter (Filtre antiparasite) 245
Informations sur la connexion 246
Informations de connexion d'accès et de copie 247
Profils USB 247
Clavier 248
Envoyez le Macro Ctrl+Alt+Suppr 248
Envoyez LeftAlt+Tab 248
Paramétrage des options clavier/souris CIM 248
Envoyer du Texte à la Cible 249
Macros de clavier 249

Définir une nouvelle macro 249
Importer des macros 250
Exporter des macros 252
Propriétés vidéo 253
Actualisation de l'écran 253
Auto-Sense Video Settings (Détection automatique des paramètres vidéo) 253
Calibrage de la couleur 254
Réglage des paramètres vidéo 254
Capture d'écran de la commande cible (Capture d'écran de la cible) 256
Options de souris 257
Modes souris double 258
Mode souris unique 261
Options d'outils 262
Paramètres généraux 262
Paramètres de lancement client 265
Configuration des paramètres de balayage de ports dans VKC et AKC 267
Options d'affichage 268
View Toolbar (Afficher la barre d'outils) 268
View Status Bar (Afficher la barre d'état) 268
Scaling (Mise à l'échelle) 269
Mode Full Screen (Mode Plein écran) 269
Support virtuel 270
Conditions requises pour l'utilisation des supports virtuels 270
Montage des lecteurs locaux 271
Tâches prise en charge Via Support Virtuel 272
Types de supports média virtuels 272
Systèmes d'exploitation pour support média virtuel pris en charge 273
Nombre de disques média virtuel pris en charge 274
Connexion et déconnexion d'un média virtuel 274
Supports virtuels dans un environnement Windows XP 277
Supports virtuels dans un environnement Linux 277
Supports virtuels dans un environnement Mac 278
Configuration du serveur de fichiers du support virtuel (Images ISO du serveur de fichiers uniquement) 278
Cartes à puce 279
Configuration Smart Card minimale requise, CIM et lecteurs de cartes à puce pris en charge/ non supportés. 280
Authentication lors de l'accès à un lecteur de carte à puces 280
Mode PC Partagé et Paramètres de Confidentialité lors de l'utilisation de cartes à puce. 280
Lecteurs de cartes à puce détecté 281
Monter un lecteur de cartes à puce 281
Mettre à jour un lecteur de cartes à puce 282
Pour envoyer des notifications de retrait et de réinsertion de la carte à puce à la cible : 282
Démonter (Retirer) un Lecteur de Carte à Puce 282
Audionumérique 283
Formats de dispositifs audio pris en charge 283
Recommandations et exigences en matière de lecture et de capture audio 284
Niveau sonore 284
Recommandations en matière de connexions audio lorsque le mode PC Share est activé 284
Exigences en matière de bande passante 284
Enregistrement des paramètres audio 286
Connexion à plusieurs cibles depuis un client distant unique 287

Connexion et déconnexion d'un dispositif audionumérique 288
Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio) 290
Informations de version - Virtual KVM Client 291

Chapitre 6 Aide Active pour Client KVM (AKC) 292

Présentation 292
Se connecte à un serveur cible 293
Framework Microsoft NET AKC prise en charge 293
Systèmes d'exploitation pris en charge par AKC 294
Navigateurs pris en charge par AKC 294
Conditions requises pour l'utilisation d'AKC 294
Autoriser les cookies 294
Inclure l'adresse IP de KX III dans la 'Zone des sites de confiance' 294
Désactiver le 'Mode Protégé' 295
Activer la validation du certificat du serveur de téléchargement AKC 295

Chapitre 7 Console locale KX III - Assistance d'utilisateur final KX III 296

Présentation 296
Accès à un serveur cible 296
Résolutions vidéo de la Console locale 297
Utilisateurs simultanés 297
Raccourcis-clavier et touches de connexion 298
Retour à l'interface de la Console locale de KX III - Raccourci-clavier par défaut 298
Exemples de touches de connexion 298
Combinaisons de touches Sun spéciales 300
Balayage des ports - Console locale 301
Diaporama Balayage des ports - Console locale 302
Indicateurs de Statut Cible pendant le balayage des ports - Console locale 304
Configurer les paramètres de balayage de la Console Locale 304
Balayage de Cibles - Console locale 305

Accès par carte à puce à la console locale 306
Options de profil USB de la console locale 307
Réinitialisation des paramètres d'usine de la Console locale KX III 308
Réinitialisation de KX IIII à l'aide du bouton de réinitialisation sur le dispositif 309

Annexe A Connecter un DVI Cat5 Reach et KX III - fournit une fonctionnalité de port local étendue 310

Présentation 310
Concernant le DVI Reach Cat5 310
Connecter un KX III et un DVI Reach Cat5 311

Annexe B Accèder à un Paragon II depuis le KX III 314

Présentation 314
Configurations et CIMs Paragon II pris en charge 315
Directives CIM Paragon KX III-à-KX III 317
Directives KX III-à-Paragon II 318
Distances de connexion entre Paragon II et KX III prises en charge 320
Connexion de Paragon II au KX III 320

Annexe C Gérer KX III dans dcTrack 322

Présentation 322
Localiser de l'espace dans un cabinet pour le KX III 323
Ajouter des dispositifs KX III à dcTrack 324
Ajouter manuellement un KX III à dcTrack 324
Importer des dispositifs KX III dans dcTrack 325
Cloner les dispositifs KX III existants 326
Construire des données et circuits de puissance pour KX III 326
Soumettez une requête d'ajout d'objet pour le KX III 327
Gérer l'ordre de travail KX III 327
Visualisez le KX III dans un cabinet d'élévation et sur une carte d'étage 327
Gérer le cycle de vie de KX III 329
Déplacer un KX III 329
Allumez ou éteignez un KX III 329
Ajouter ou retirer un KX III du site 329
Déclasser un KX III en stockage 329
Déclasser un KX III aux archives 329

Annexe D Spécifications 330

Matériel 330
Dimensions et spécifications physiques de KX III 330
Résolutions de Vidéo de Serveur cible supportées par KX III 334
Distance de connexion, taux de rafraîchissement et résolution vidéo du serveur cible pris en charge 335
Résolutions DVI de Port Local KX III prises en charge 336
Spécifications des CIM pris en charge 336

CIM Vidéo Digital pris en charge par Mac 339
Modes de synchronisation de CIM numériques 339
Modes digital CIM établis et standard 339
Mode de compatibilité DVI 340
Connexions à distance prises en charge 341
Paramètres de vitesse réseau 341
Longueurs de câbles et résolutions vidéo pour châssis Dell 342
Configuration système minimum pour carte à puce 343
Lecteurs de cartes à puce pris en charge 344
Lecteurs de cartes à puce non pris en charge 345
Recommandations et exigences en matière de lecture et de capture audio 346
Nombre de connexions audio/supports virtuels et cartes à puce prises en charge 348
KX III Langues de clavier prises en charge 348
Touches de commandes BIOS sur Mac Mini 349
Utiliser un clavier Windows pour accéder à des cibles Mac 351
Ports TCP et UDP utilisés 351
Logiciel 352
Systèmes d'exploitation et navigateurs pris en charge 352
Exigences Java et Microsoft .NET 354
Exigence de clavier multi-langue JRE 354
Evénements capturés dans le journal d'audit et dans Syslog 355

Annexe E Remarques d'informations 356

Présentation 356
Remarques sur l'environnement d'éxécution de Java (JRE) 356
Désactiver la mise en mémoire cache de Java et effacer le cache de Java 356
Java ne chargeant pas correctement sur Mac 357
Remarques sur la prise en charge d'IPv6 358
Remarques sur la prise en charge du système d'exploitation d'IPv6 358
Notes de version Ipv6 pour téléchargement de la Validation de Certification du Serveur AKC 359
Problèmes de performances de connexion en double pile 359
Remarques CIM 359
Souris à 3 boutons Windows sur les cibles Linux 359
Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel 360
Remarques sur le support virtuel 361
Ne peut pas se connecter aux lecteurs de clients Linux 361
Ne peut pas écrire sur/à partir d'un fichier de Client Mac 361
Utilisation du support virtuel via VKC et AKC dans un environnement Windows 362
Support virtuel non rafraîchi après l'ajout de fichiers 363
Lecteur virtuel Linux répertorié deux fois 363
Accès à Virtual Media sur Windows 2000 363
Déconnecter les Lecteurs USB Virtuels Mac et Linux 363
Durée d'amorçage du BIOS cible avec les supports virtuels 363
Echec de connexion des supports virtuels lors de l'utilisation du haut débit 364
Remarques sur les ports et profils USB 364
Ports USB VM-CIM et DL360 364
Aide pour la sélection des profils USB 364
Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce 366

Modes et résolutions vidéo 366
L'image vidéo est foncée sous Mac 366
Bandes noires/barres affichées sur le Port local 366
Synch Vidéo Sun Composite 366
Modes vidéo SUSE/VESA 367
Remarques clavier 367
Clavier français 367
Préférence de la langue du clavier (clients Fedora Linux) 369
Macros ne s'enregistrant pas sur serveurs cible Linux 370
Touches clavier non prises en charge pour accès à distance 370
Remarques souris 371
Synchronisation des pointeurs de souris (Fedora) 371
Mode souris simple - lors de la Connexion à une cible contrôlée par CC-SG 371
Audio 372
Problèmes en matière de lecture et de capture audio 372
Audio dans un environnement Linux 372
Audio dans un environnement Windows 373
Remarques sur les cartes à puce 373
Connexions par carte à puce Virtual KVM Client (VKC) aux serveurs Fedora 373
Remarques CC-SG 373
Version de Virtual KVM Client non reconnue par le mode proxy CC-SG 373
Déplacement entre ports sur un dispositif 373
Remarques Navigateur 374
Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora 374

Annexe F Foire aux questions 375

FAQ - Généralités 375
Accès à distance 379
Support virtuel universel 382
Bande passante et performance KVM-sur-IP 384
Gestion de réseau IPv6 388
Windows 390
Serveurs lames 391
Installation 393
Port Local - KX III 395
Port local étendu 396
Double alimentation 397
Contrôle des unités de distribution d'alimentation (PDU) 397
Ethernet et mise en réseau IP 399
Groupement, fonction multiniveau et mise en cascade des ports locaux 401
Modules d'interface pour ordinateur (CIM) 404
Sécurité 405
Authentification par cartes à puce et CAC 407
Capacités de gestion 408
Documentation et assistance 410
Divers 411

Index 413

Chapitre 1 Introduction

Dans ce chapitre

Présentation 1
Nouveautés de l'aide 1
Contenu de l'emballage 2
Caractéristiques et Photos de l'appareil KX III 2
Interfaces des consoles KX III locales et à distance 7
Applications Client KVM pour KX III 8
Aide en ligne KX II 8

Présentation

Dominion KX III est un commutateur KVM sur IP, sécurisé, pour entreprise permettant l'accès à distance au BIOS de 8 à 64 serveurs de 1, 2, 4 ou 8 utilisateurs.

KX III est fourni avec des fonctions standard telles que le support DVI / HDMI / DisplayPort numérique, support de vidéo analogique, audio, média virtuel, carte à puce / CAC, serveur blade et accès mobile.

Déployez KX III individuellement, ou avec le Centre de Commande Sécurisé de Raritan (CC-SG).

Nouveautés de l'aide

- KX III prend en charge ls moniteurs vidéo DVI
- Egalement ajouté dans cette version:
  - Capacité d'étendre la portée de KX III en se connectant au DVI Cat5 Reach de Raritan - consultez ***Connecter un DVI Cat5 Reach et KX III - fournit une fonctionnalité de port local étendue*** (à la page 310)
  - Changements aux propriétés de connexion au Client KVM Virtuel (VKC) et Client KVM Actif (AKC) - consulter ***Configurer les propriétés de connexion*** (à la page 242)
  - Activer et désactiver les Favoris dans le client distant KX III - Reportez-vous à la Gestion des favoris
  - Support pour tous types de disques média virtuels externes

Contenu de l'emballage

Chaque envoi KX III est un produit autonome entièrement configuré, dans un châssis de montage en rack 1U (2U pour KX3-864) 19 pouces standard. Chaque appareil KX III est livré avec les éléments suivants :

Quantité	Elément
1	- Appareil KX III
1	Guide de configuration rapide KX III
1	Kit de montage en rack
2	Cordon d'alimentation secteur
1	Ensemble de 4 pieds en caoutchouc (pour utilisation sur un bureau)
1	Note d'application
1	Carte de garantie

Caractéristiques et Photos de l'appareil KX III

Matériel

- Accès distant KVM sur IP intégré
- Montage en rack 1U ou 2U (supports de fixation fournis)
- Double alimentation avec fonction de basculement automatique, alimentation à commutation automatique avec avertissement de panne de courant
- Prise en charge pour les CIMs suivants :
  - Pour synchronisation absolue de la souris et média virtuel, utilisez l'un des CIM suivants:
    - D2CIM-VUSB
    - D2CIM-DVUSB
    - D2CIM-DVUSB-DVI
    - D2CIM-DVUSB-HDMI
    - D2CIM-DVUSB-DP
  - Obligatoire pour une connexion PS2:

    - DCIM-PS2
- Support moniteur DVI à partir du port local DVI
    - Support VGA via un convertisseur DVI en VGA
    - Support DVI via un câble standard DVI
- Support pour multiniveau dans lequel un appareil KX III de base est utilisé pour accéder à plusieurs autres dispositifs en niveau.
- Fonction pour utilisateurs multiples (1/2/4/8 utilisateurs distants, 1 utilisateur local)
- Câblage de serveur UTP (Cat5/5e/6)
- Ports Ethernet doubles (10/100/1000 LAN) à protection par basculement
- Améliorable en clientèle
- Port utilisateur USB local pour accès en rack
    - Port USB clavier/souris
    - Un panneau avant et trois panneaux de ports USB arrières pour les dispositifs USB pris en charge.
    - Simultanéité complète avec l'accès utilisateur à distance
    - Interface graphique utilisateur (GUI) locale pour l'administration
- Sécurité de l'accès centralisé
- Gestion de l'alimentation intégrée
- Voyants indiquant le statut de la double alimentation, l'activité du réseau et le statut des utilisateurs distants
- Bouton de réinitialisation matérielle

Remarque : La version KX III 3.0.0 ne fournit pas de support modem, mais en fournira dans de futures versions.

Logiciel

- Support média virtuel sous environnements Windows®, Mac® et Linux®.
- Synchronisation absolue de la souris*

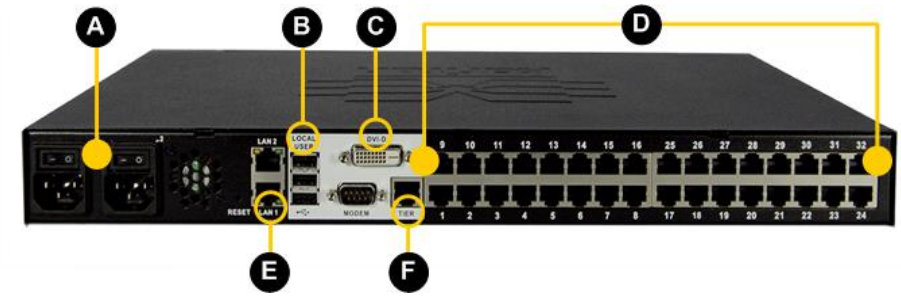
**Remarque : La synchronisation absolue de la souris et les média virtuels requièrent l'utilisation d'un D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI ou D2CIM-DVUSB-DP CIM.*

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

Dominion KX3-832

Photos KX3-832

Fonctions KX3-832



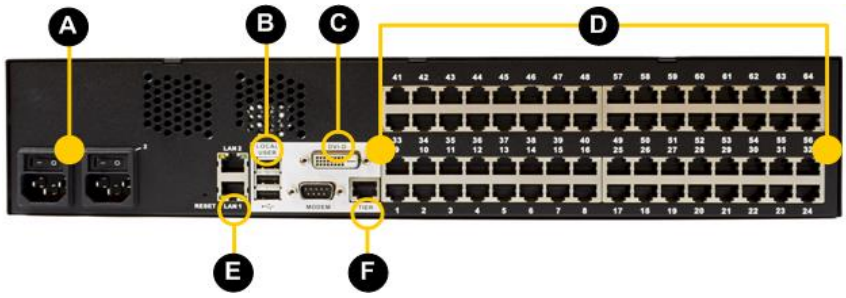
Légende	
A	Alimentation double AC 100V/240V
B	Port locaux USB
C	Port DVI-D
D	32 Ports KVM de câblage UTP (Cat5/5e/6)
E	Accès Ethernet double 10/100/1000
F	Port multiniveau

Remarque : La version KX III 3.0.0 ne fournit pas de support modem, mais en fournira dans de futures versions.

Dominion KX3-864

Photos KX3-864

Fonctions KX3-864



Légende	
A	Alimentation double AC 100V/240V
B	Port locaux USB
C	Port DVI-D
D	64 Ports KVM de câblage UTP (Cat5/5e/6)
E	Accès Ethernet double 10/100/1000
F	Port multiniveau

Légende
Remarque : La version KX III 3.0.0 ne fournit pas de support modem, mais en fournira dans de futures versions.

Utilisateurs et ports pris en charge par modèle

Modèle	Ports	Utilisateurs distants
KX3-864	64	8
KX3-832	32	8
KX3-808	8	8
KX3-464	64	4
KX3-432	32	4
KX3-416	16	4
KX3-232	32	2
KX3-216	16	2
KX3-132	32	1
KX3-116	16	1
KX3-108	8	1

Interfaces des consoles KX III locales et à distance

Utiliser l'interface de la console à distance pour configurer et gérer le KX III via une connexion réseau.

L'interface de la Console Locale donne accès au KX III sur le rack.

Consultez ***l'Interface de console à distance de KX III*** (voir "***Interface de console à distance de KX III***" à la page 16) et ***l'interface de console locale KX III*** (voir "***Interface de la console locale KX III***" à la page 26), respectivement.

Applications Client KVM pour KX III

KX III fonctionne avec le Client KVM Virtuel (VKC) et le client KVM Actif (AKC)

Pour obtenir de l'aide sur l'utilisation des clients, consultez L'***aide concernant le client KVM Virtuel (VKC)*** (voir "***Aide Virtuelle pour Client KVM (VKC)***" à la page 240) et l'***aide concernant le client KVM Actif (AKC)*** (voir "***Aide Active pour Client KVM (AKC)***" à la page 292)

Aide en ligne KX II

L'aide en ligne KX III est considéré comme votre source d'aide principale. Les versions PDF de l'aide sont des ressources secondaires.

Consultez les notes de version de KX III pour obtenir les informations importantes sur la version actuelle avant de commencer à utiliser KX III.

L'aide client KVM est fournie en tant que partie de l'aide en ligne KXIII.

L'aide en ligne est accompagnée par le Guide de configuration rapide KX III, qui peut être trouvé sur la page de Documentation, Mises à jours et Logiciel du ***site web de Raritan*** (***http://www.raritan.com/support/firmware-and-documentation***).

La page de Documentation, Mises à jours et Logiciel contient également une version PDF de les sections de l'aide en ligne pour l'utilisateur final, y compris l'aide pour Client KVM, la console d'aide locale, la console d'aide à distance(si applicable), les spécifications etc..

Remarque : Pour utiliser l'aide en ligne, Active Content (le contenu actif) doit être activé dans votre navigateur.

Chapitre 2 Mise en route

Dans ce chapitre

Installer et configurer KX III: 9
Autorise les pop-ups : 9
Messages de validation et avertissements de sécurité 9
Installation d'un certificat 10
Connexion au KX III 14

Installer et configurer KX III:

Connectez tous les serveurs cible (si vous ne l'avez pas déjà fait).

Consultez le Guide de configuration rapide de KX III fourni avec votre appareil ou téléchargez le à partir du ***site web de support Raritan http://www.raritan.com/support*** ou consultez ***Installation et configuration de KX III*** (à la page 28).

Autorise les pop-ups :

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

Messages de validation et avertissements de sécurité

Lorsque vous vous connectez à KX III, des messages de validation et avertissements de sécurité peuvent apparaître.

Ceux-ci incluent:

- Requêtes et avertissements de sécurité Java™pour valider KX III. Consultez ***Avertissement d'accès et validation de Java*** (à la page 9), et ***Installation d'un certificat*** (à la page 10)
- Avertissements de sécurité supplémentaires selon vos paramètres de navigation et de sécurité. Consultez ***Avertissements de Sécurité Supplémentaires*** (à la page 10)

Avertissement d'accès et Validation de Java

Lorsque vous vous connectez à KX III, Java® 1.7 vous invite à valider KX III, et autorise l'accès à l'application.

Raritan recommande d'installer un certificat SSL sur chaque appareil KX III afin de réduire les avertissements Java et d'améliorer la sécurité. Reportez-vous à ***Certificats SSL*** (à la page 183).

Avertissements de Sécurité Supplémentaires

Même après qu'un certificat SSL soit installé dans le KX II, selon dans les paramètres de sécurité de votre navigateur, des avertissements de sécurité supplémentaires peuvent être affichés lorsque vous vous connectez à KX III.

Il est nécessaire d'accepter ces avertissements pour lancer la Console à Distance de KX III.

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

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

Installation d'un certificat

Vous pouvez être invité par le navigateur à accepter et valider le certificat SSL de KX III.

Selon dans les paramètres de sécurité de votre navigateur, des avertissements de sécurité supplémentaires peuvent être affichés lorsque vous vous connectez à KX III.

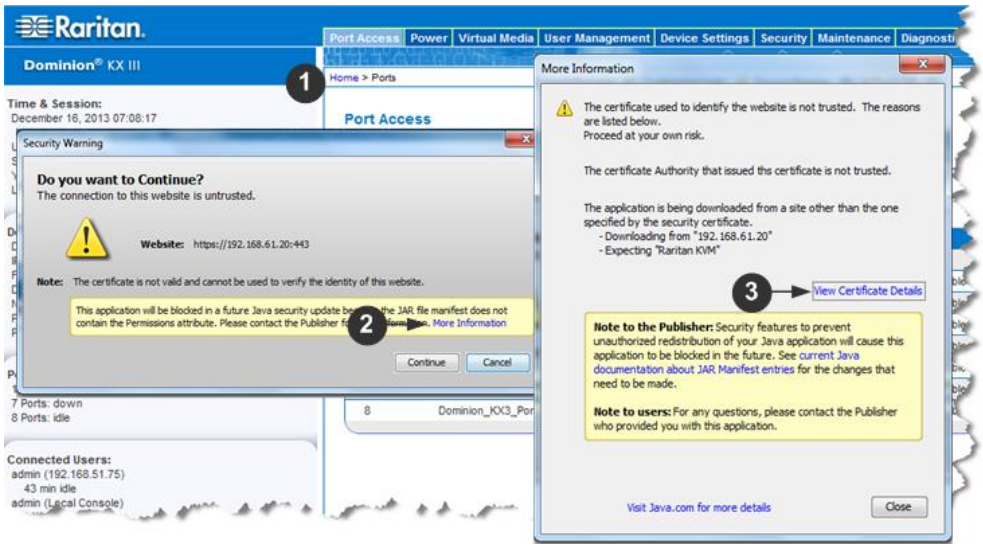
Il est nécessaire d'accepter ces avertissements pour lancer la Console à Distance de KX III. Pour plus d'informations, consultez ***Messages de validation et avertissements de sécurité*** (à la page 9).

Deux méthodes d'échantillon concernant la méthode d'installation d'un Certificat SSL dans le navigateur sont fournis ici, toutes deux utilisant Microsoft Internet Explorer 8® et Windows 7®.

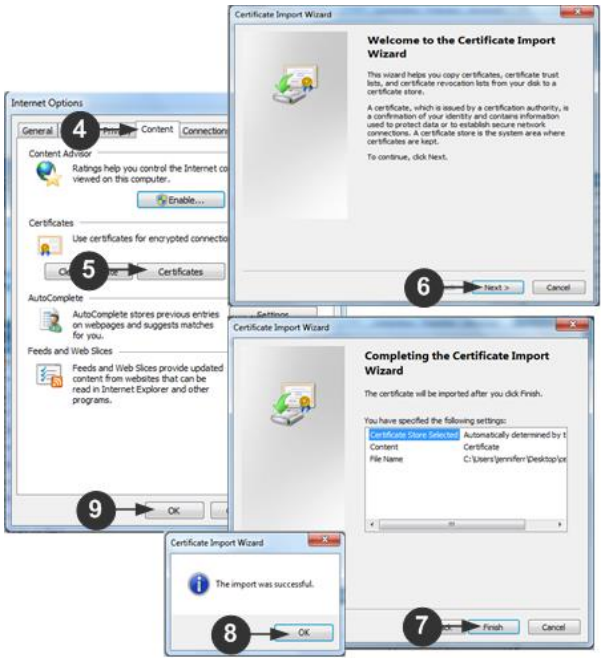
Les méthodes et étapes spécifiques dépendant de votre navigateur et de votre système d'exploitation. Consultez l'aide de votre navigateur et système d'opération pour plus de détails.

Exemple 1 : Importer le certificat dans le navigateur

Dans cet exemple, vous importez le certificat dans le navigateur



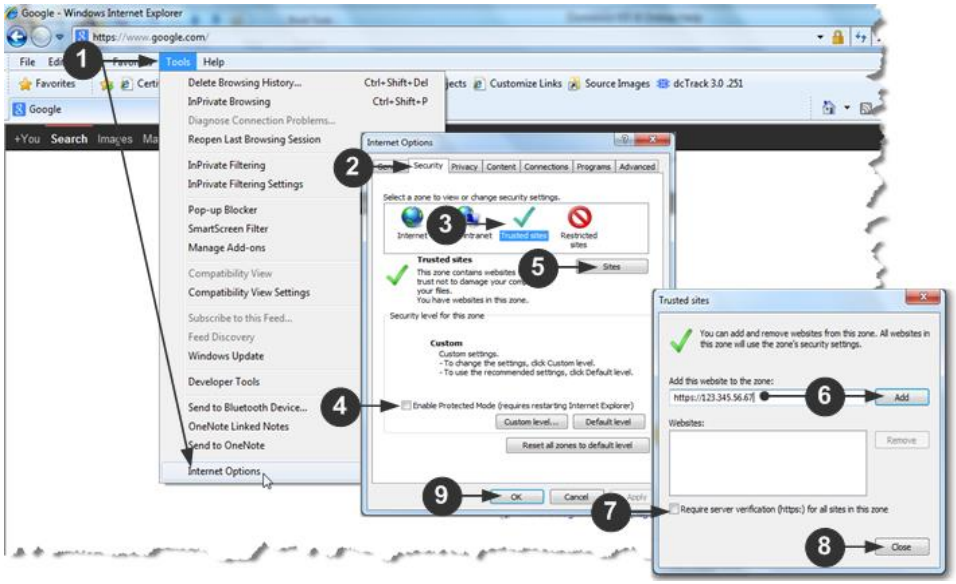
Procédure	
1	Open le navigateur IE, puis connectez-vous à KX III.
2	Cliquez sur Plus d'informations lors du premier avertissement de sécurité Java™.
3	Cliquez sur Afficher les Détails du Certificat dans la boîte de dialogue Plus d'informations. On vous demande d'installer le certificat. Suivez les étapes de l'assistant. *Remarque : Si vous n'êtes pas invités par le navigateur, sélectionnez manuellement Outils > Options Internet pour ouvrir la boîte de dialogue d'Options Internet.*



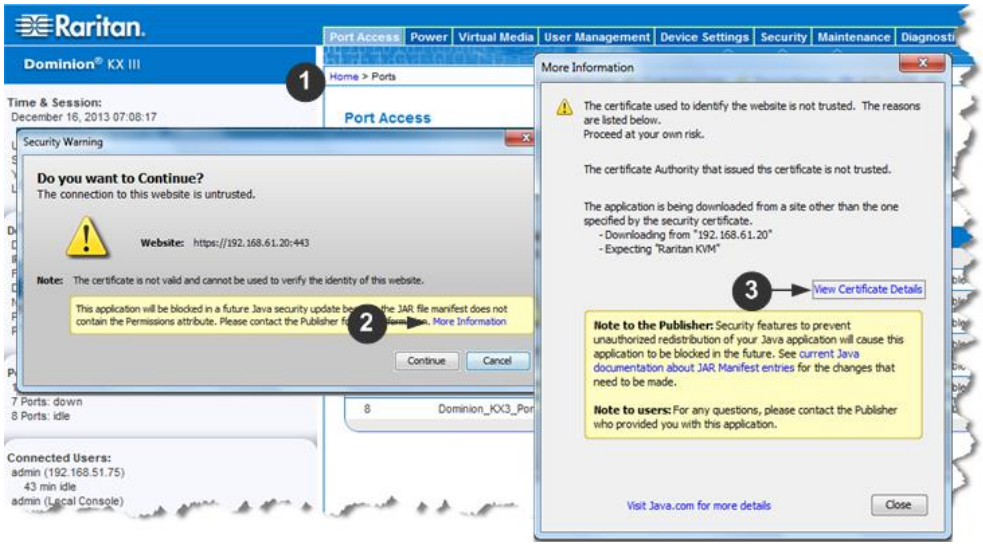
Procédure	
4	Cliquez sur l'onglet Contenu.
5	Cliquez sur Certificats
6	L'assistant d'importation de Certificat s'ouvre et vous guide à travers chaque étape. ▪ Fichier à Importer - Naviguer pour localiser le Certificat ▪ Stockage de Certificat - Sélectionnez la localisation où stocker le Certificat
7	Cliquez sur Terminer lors de la dernière étape de l'Assistant.
8	Le Certificat est importé. Fermer le message de réussite.
9	Cliquez sur OK dans la fenêtre de dialogue d'options Internet pour appliquer les changements, puis fermez et réouvrez le navigateur.

Exemple 2 : Ajouter le KX III aux sites de confiance et importer le certificat

Dans cet exemple, l'URL de KX III est ajoutée en tant que site de Confiance, et le certificat auto-signé est ajouté dans le cadre du process.



Procédure	
1	Ouvrez un navigateur IE, puis sélectionnez Outils > Options Internet pour ouvrir la boîte de dialogue d'Options Internet.
2	Cliquez sur l'onglet de Sécurité.
3	Cliquez sur les Sites de Confiance.
4	Désactivez le Mode Protégé, et acceptez tout avertissement.
5	Cliquez sur Site pour ouvrir la boîte de dialogue contenant les Sites de Confiance.
6	Entrez l'URL de KX III puis cliquez sur Ajouter.
7	Déselectionner la vérification de serveur pour la zone (si applicable).
8	Cliquez sur Fermer.
9	Cliquez sur OK dans la fenêtre de dialogue d'options Internet pour appliquer les changements, puis fermez et réouvrez le navigateur. Ensuite, importez le certificat.



Procédure	
1	Open le navigateur IE, puis connectez-vous à KX III.
2	Cliquez sur Plus d'informations lors du premier avertissement de sécurité Java™.
3	Cliquez sur Afficher les Détails du Certificat dans la boîte de dialogue Plus d'informations. On vous demande d'installer le certificat. Suivez les étapes de l'assistant. Pour plus de détails reportez-vous à ***l'Exemple 1. Importer le certificat dans le navigateur*** (voir "***Exemple 1 : Importer le certificat dans le navigateur***" à la page 11)

Connexion au KX III

Connectez-vous à votre console à distance de KX III depuis un poste de travail doté d'une connectivité réseau et possédant Microsoft.NET® et/ou Java Runtime Environment™ installé.

Se connecter et utiliser KX III nécessite que vous autorisiez les pop-ups.

Pour plus d'informations concernant les messages de validation et avertissements de sécurité, et la procédure pour les réduire ou éliminer, consultez ***Messages de validation et avertissements de sécurité*** (à la page 9)

Pour se connecter au KX III

1. Lancer un navigateur pris en charge.

2. Entrez soit:
   - L'URL - *http://ADRESSE-IP* pour utiliser le client KVM virtuel basé sur Java

     Ou

   - *http://ADRESSE-IP/akc* pour le client KVM actif basé sur .NET

   ADRESSE-IP est l'adresse IP assignée à votre KX III.

   Vous pouvez également l'HTTPS ou le nom DNS du KX III assigné par votre administrateur (si applicable).

   Vous êtes toujours redirigé à l'adresse IP de HTTP à HTTPS.
3. Entrez votre nom d'utilisateur et mot de passe, puis cliquez sur Connexion.
4. Acceptez le contrat d'utilisation (si applicable).
5. Si des avertissements de sécurité apparaissent, acceptez-les et/ou autorisez l'accès.

Chapitre 3 Interface et navigation KX III

Dans ce chapitre

Présentation 16
Interface de console à distance de KX III 16
Interface de la console locale KX III 26

Présentation

Les interfaces de la console distante de KX III et celle de la console locale de KX III présentent toutes les deux une interface Web pour la configuration et l'administration, ainsi qu'une liste et sélection des serveurs cible.

Interface de console à distance de KX III

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

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

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

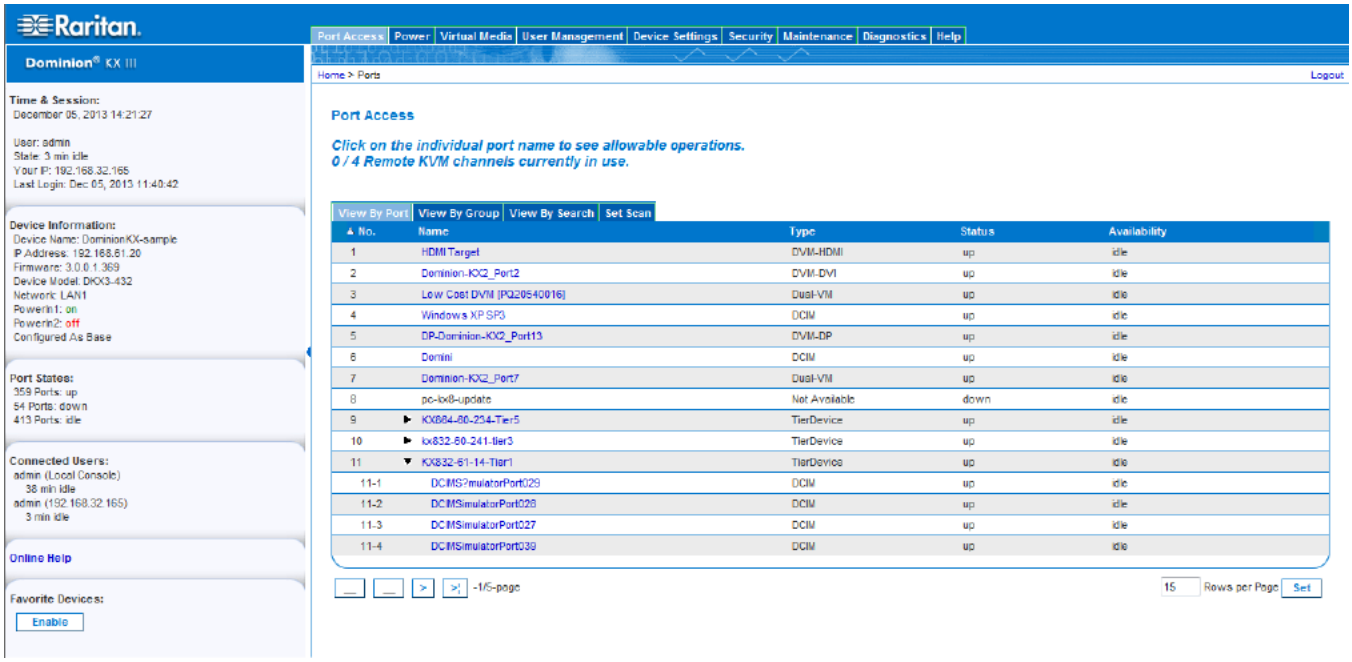
- Support virtuel
- Favorites (Favoris)
- Backup/Restore (Sauvegarde/Restauration)
- Firmware Upgrade (Mise à niveau du firmware)
- Certificats SSL
- Audio

Page d'accès aux ports (Affichage de la console à distance)

Une fois la connexion réussie, la page d'accès aux ports s'affiche avec la liste de tous les ports ainsi que leur statut et leur disponibilité.

Les ports connectés aux serveurs cible KVM (serveurs blades et standard) sont affichés en bleu et peuvent être modifiés. Faites clic droit sur n'importe lequel de ces ports pour ouvrir le menu d'Action de ports. Pour plus d'informations, consultez le ***Menu d'action de ports*** (voir "***Port Action Menu (Menu d'action de ports)***" à la page 20).

Pour les ports sans CIM connectés ou pour lesquels le nom de CIM est vide, un Dominion-KX3_Port# par défaut est assigné, où Port# est le numéro du port physique de KX III.



Quatre onglets sont présents sur la page et permettent un affichage par port, par groupe ou par recherche.

Vous pouvez effectuer un tri par numéro de port, nom de port, état (activé ou non) et disponibilité (inactif, connecté, occupé, indisponible ou en cours de connexion) en cliquant sur un en-tête de colonne.

Utilisez l'onglet Set Scan (Balayage d'ensemble) pour balayer jusqu'à 32 cibles connectées à KX III. Reportez-vous à Balayage des ports - Console à distance

Dispositifs en niveau - Page Port Access

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

Châssis de lames - Page Port Access

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

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

Groupes de deux ports vidéo - Page Port Access

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

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

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

Remarque : Deux canaux KVM sont requis pour la connexion à distance au groupe de deux ports vidéo en cliquant sur le port principal. Si deux canaux ne sont pas disponibles, le lien Connect (Connexion) n'est pas affiché.

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

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

Onglet View by Group (Afficher par groupe)

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

Reportez-vous à Gestion des dispositifs pour obtenir des informations sur la création de chaque type de groupes de ports.

Onglet View by Search (Afficher par recherche)

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

Onglet Set Scan (Balayage d'ensemble)

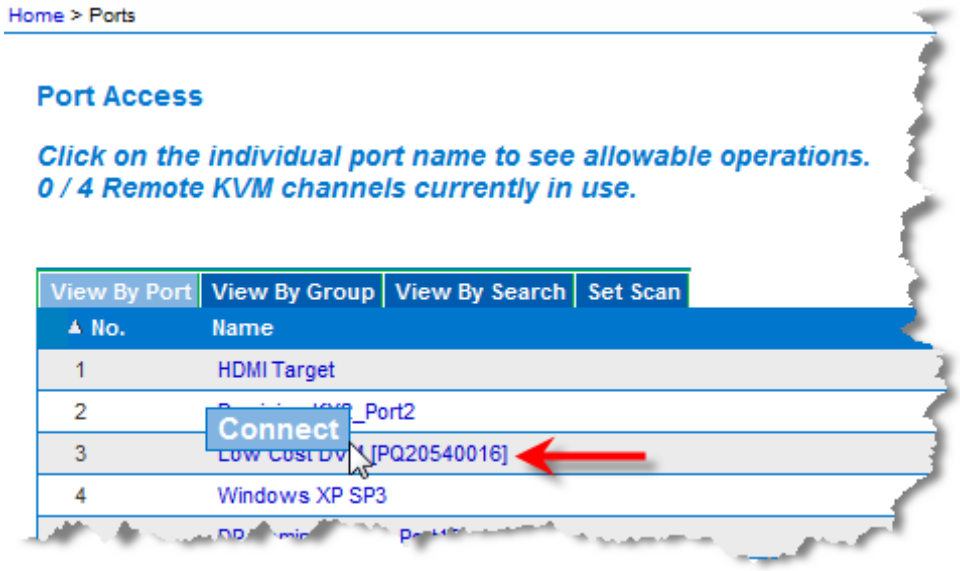
La fonction de balayage des ports est accessible depuis l'onglet Réglage de Balyage sur la page Accès aux ports. Elle vous permet de définir un ensemble de cibles à balayer. Des vues en miniature des cibles balayées sont également disponibles. Sélectionnez une miniature pour ouvrir la cible correspondante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

Reportez-vous à Balayage des ports - Console à distance pour plus d'informations.

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, seront répertoriées dans le menu d'actions des ports :



Connecter

- Connect (Connecter) - Crée une nouvelle connexion au serveur cible.

  Pour la console à distance de KX III, une nouvelle page de Client KVM Virtuel apparaît.

  Pour la console locale de KX III, l'affichage passe de l'interface utilisateur locale au serveur cible.

  Sur le port local, l'interface de la console locale de KX III doit être visible pour pouvoir procéder à la commutation.

  La commutation par raccourci-clavier est également disponible à partir du port local.

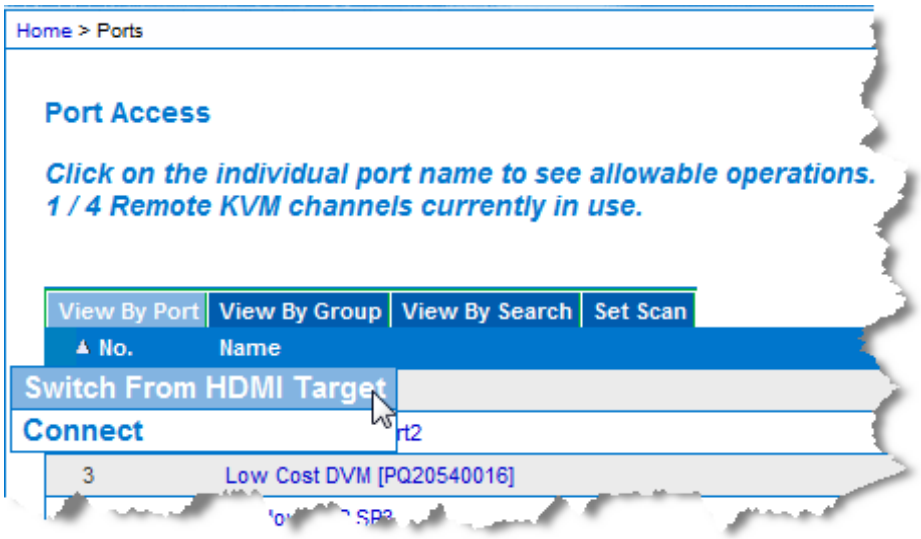
  Remarque : cette option n'apparaît pas pour un port disponible à partir de la console distante KX III si toutes les connexions sont occupées.

Switch From (Basculer à partir de).

- Switch From (Basculer depuis) : permet de basculer d'une connexion existante au port sélectionné (serveur cible KVM).

  Cette option de menu est disponible uniquement pour les cibles KVM et n'est visible que lorsqu'un client KVM virtuel est ouvert.

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

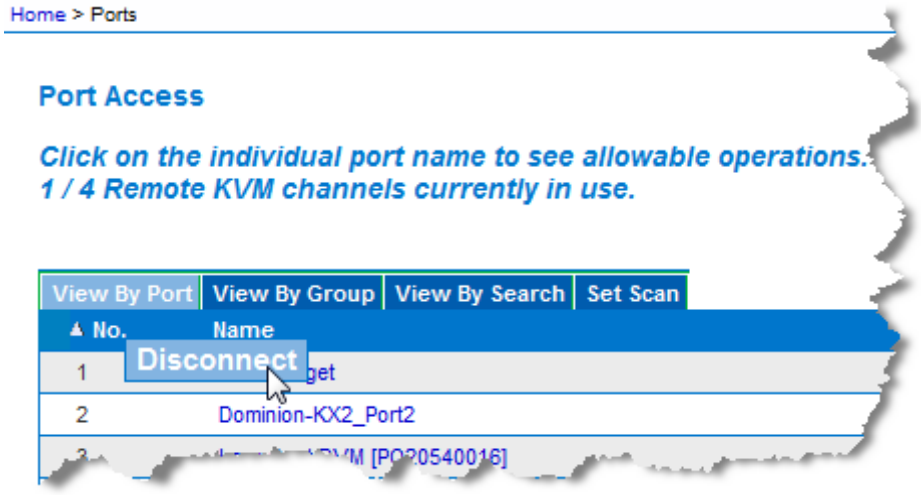


Déconnecter

- Disconnect (Déconnecter) : permet de déconnecter ce port et de fermer la page du client KVM virtuel pour ce serveur cible.

  Cette option de menu est disponible uniquement lorsque l'état du port est actif et connecté, ou actif et occupé.

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



Sous tension

- 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.

Hors tension

- 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.

Cycle d''alimentation

- 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.

Panneau gauche

Le panneau gauche de l'interface KX III contient les informations suivantes.

Notez que certaines informations sont conditionnelles - signifiant qu'elles sont affichées selon votre rôle, les fonctions utilisées etc. Les informations conditionnelles sont indiquées ici.

Information	Description	Quand affichée ?
Temps & session	Date et heure de début de la session en cours.	Toujours
Utilisateur	Nom d'utilisateur	Toujours
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)	L'adresse IP utilisée pour accéder à KX III.	Toujours
Last Login (Dernière connexion)	Date et heure de la dernière connexion	Toujours
Under CC-SG Management (Géré par CC-SG)	L'adresse IP du dispositif CC-SG assurant la gestion de KX III.	Quand le KX III est géré par CC-SG.
Device Information (Informations sur le dispositif)	Information spécifiques au KX III que vous utilisez.	Toujours
Nom du dispositif	Nom affecté au dispositif	Toujours
Adresse IP	L'adresse IP du KX III	Toujours
Firmware	Version actuelle du firmware	Toujours
Device Model (Modèle du dispositif)	Modèle du KX III	Toujours
Numéro de série	Numéro de série de KX III	Toujours
Réseau	Nom attribué au réseau en cours.	Toujours

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

Réduire le panneau gauche

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

Pour réduire le panneau gauche :

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

Navigation dans la console KX III

Les interfaces de la console KX III 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.

Interface de la console locale KX III

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

Pour plus de détails sur l'utilisation de la Console Locale, consultez ***KX III Console locale - KX III assitance d'utilisateur final*** (voir "***Console locale KX III - Assistance d'utilisateur final KX III***" à la page 296).

Chapitre 4 Aide pour l'administrateur de KX III

Dans ce chapitre

Présentation 27
Installation et configuration de KX III 28
Gestion des prises des PDU de rack (barrettes d'alimentation) 46
Profils USB 49
User Management (Gestion des utilisateurs) 57
Gestion des dispositifs 85
Gestion de la sécurité 169
Maintenance 188
Diagnostics 201
Console locale KX III 207
Interface de ligne de commande (CLI) 213
Groupes de deux ports vidéo 222
Mise à jour du schéma LDAP 232

Présentation

L'aide pour l'administrateur contient des informations spécifiques aux fonctions KX III généralement effectuées par les administrateurs de l'application KX III, comme l'installation et la configuration de KX III, la gestion des groupes et des utilisateurs, la gestion de la sécurité etc.

Les fonctions d'administration sont généralement effectuées via la Console à Distance KX III et/ou via la Console Locale.

Les fonctions généralement effectuées par les utilisateurs finaux en utilisant le Client KVM Virtuel ou le Client KVM Actif, et certaines fonctions effectuées vie la Console à Distance ou Console Locale sont décrites dans leurs propres sections de l'aide.

Ces fonctions incluent l'utilisation de média virtuels, la configuration des paramètres de souris, l'utilisation de la fonction de balayage des ports, la configuration d'options vidéo etc.

Installation et configuration de KX III

Consultez le Guide de configuration rapide KX III fourni avec votre appareil ou téléchargez le à partir du site web de support Raritan pour une référence rapide aux étapes de configuration basiques, minimums.

Les informations additionnelles et étapes optionnelles incluses ici mais pas dans le QSG incluent:

- ***Paramètres additionnels de la souris pris en charge*** (à la page 31)
- ***Status LED pendant le démarrage de KX III*** (à la page 34)
- ***Connexion à un Moniteur VGA (Optionnel)*** (voir "***Connexion à un Moniteur VGA (Optionnel).***" à la page 36)
- ***Etape 6 : Configuration de la langue du clavier (facultatif)*** (à la page 44)

Montage en rack

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

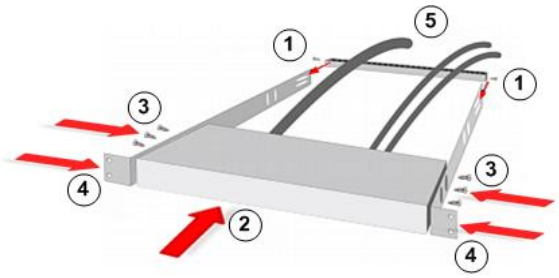
Remarque : Le dispositif Raritan utilisé dans les schémas présentés ici est un exemple et n'est pas nécessairement représentatif de votre appareil. Les instructions de montage sont spécifiques à votre appareil.

Montage avant

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

1. Fixez la barre de support de câble à l'arrière des pattes latérales à l'aide de deux des vis fournies.
2. Faites glisser le KX III entre les pattes latérales, panneau arrière face à la barre de support de câble, jusqu'à que le panneau avant soit aligné sur les « oreilles » des pattes latérales.
3. Sécurisez le KX III aux pattes latérales à l'aide des vis restantes (trois de chaque côté).
4. Montez l'assemblage sur le rack et fixez les oreilles des pattes latérales sur les rails avant du rack à l'aide de vos propres vis, boulons, écrous à cage, etc.

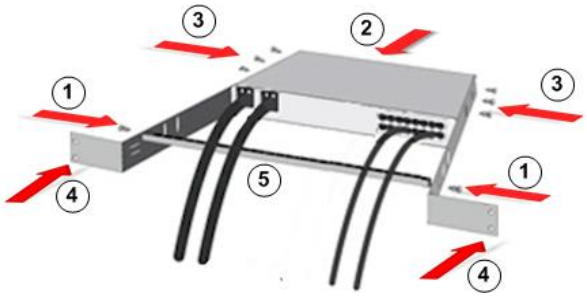
5. Lorsque vous branchez des câbles au panneau arrière du KX III, drapez-les sur la barre de support de câble.



Montage arrière

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

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



Données de connexion par défaut

Valeur par défaut	Valeur
Nom d'utilisateur	*admin*

Valeur par défaut	Valeur
	Cet utilisateur dispose de droits d'administrateur.
Mot de passe	*raritan* La première fois que vous démarrez KX III, il vous est demandé de changer le mot de passe par défaut.
IP address (Adresse IP)	192.168.0.192

Important : A 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.

Etape 1 : Configuration des paramètres du pare-feu réseau

Port TCP 5000

Pour permettre l'accès distant à ProductName, vos réseau et pare-feu doivent autoriser la communication sur le port TCP 5000.

Vous pouvez également configurer l'unité KX III pour utiliser un autre port TCP, puis autoriser la communication sur ce port.

Port TCP 443

Pour accéder à KX III par le biais d'un navigateur Web, votre pare-feu doit également autoriser l'accès au port TCP 443 (port standard HTTPS).

Port TCP 80

L'accès au port TCP 80 (port standard HTTP) permet de rediriger automatiquement les requêtes HTTP vers HTTPS.

Etape 2 : Configurer les serveurs cible KVM

Résolutions de serveur vidéo cible

Pour obtenir une liste des résolutions de serveur vidéo cible supportées, consultez ***Résolutions de Vidéo de Serveur cible supportées par KX III*** (à la page 334) dans l'Aide en ligne KX III..

Paramètres de la souris

Raritan recommende l'utilisation de Synchronisation absolue de la souris pour minimiser les Paramètres de la souris sur les serveurs cibles. Pour d'autres modes de souris, consultez ***Paramètres additionnels de la souris pris en charge*** (à la page 31)

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 CIMs de média virtuel.

Synchronisation absolue de la sourisrequière l'utilisation d'un CIM média virtuel:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Paramètres additionnels de la souris pris en charge

Ces paramètres sont configurés sur votre système d'opération cible sauf contre-indication.

Paramètres de la souris

Voici les paramètres de souris pour différents systèmes d'exploitation.

Ces paramètres sont configurés sur votre système d'opération cible sauf contre-indication.

Reportez-vous à l'aide en ligne ou au manuel d'utilisation de KX III pour obtenir des instructions détaillées sur ces paramètres de souris.

Paramètres Microsoft Windows 7 et Windows Vista

Configurer ces paramètres de souris sous Windows 7® et Windows Vista®:

Configurer les paramètres de mouvement:

- Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
- Désélectionnez la case Améliorer la précision du pointeur.

Désactivez les effets de fondu et d'animation :

- Animer les commandes et les éléments à l'intérieur des fenêtres
- Animer les fenêtres lors de la réduction et de l'agrandissement
- 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

Paramètres Windows XP, Windows 2003 et Windows 2008

Configurer ces paramètres de souris sous Windows XP®, Windows 2003® et Windows 2008®:

Configurer les paramètres de mouvement:

- 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.

Désactivez les effets de transition :

- Désélectionnez l'option 'Utiliser l'effet de transition suivant pour les menus et les info-bulles'.

Paramètres de souris Windows 2000

Configurer les paramètres de souris Windows 2000®:

Configurer les paramètres de mouvement:

- Définissez l'accélération du pointeur sur Aucune.
- Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.

Désactivez les effets de transition :

- Désélectionnez l'option 'Utiliser l'effet de transition suivant pour les menus et les info-bulles'.

Paramètres de la souris Mac d'Apple

Configurer ces paramètres de la souris Mac® d'Apple:

La synchronisation de souris absolue est requise pour une synchronisation de souris correcte sur les serveurs KVM cibles utilisant un système d'exploitation Mac®.

Afin qu'une synchronisation absolue fonctionne, un CIM média virtuel est requis. Pour une liste des CIMS pris en charge, consultez ***Spécifications des CIM pris en charge*** (à la page 336).

Une fois que vous avea terminé l'installation de votre KX III, activez le profil USB Mac. Si vous n'activez pas ce profil, la souris ne se synchronise pas sous OS X.

Pour ce faire, effectuez l'une des opérations suivantes :

1. Connectez-vous à la cible MAC à partir du client KVM Raritan.
2. Sélectionner Profil USB > Autre Profiles > Mac OS-X (10.4.9 et ultérieur).

   Ou

3. Dans KX III, sélectionnez Paramètres du dispositif > Configuration des ports puis cliquez ensuite sur le nom de la cible pour ouvrir la page des ports.
4. Elargissez la section 'Sélectionner des profils USB pour les ports'.
5. Sélectionnez 'Mac OS-X (10.4.9) et supérieur' dans la boîte Disponible, puis cliquez sur Ajouter pour l'ajouter à la boîte Sélectionné.
6. Cliquez sur 'Mac OS-X (10.4.9) et supérieur' dans la boîte Sélectionné. Cela l'ajoute automatiquement à la liste déroulante des profils préférés.
7. Sélectionnez 'Mac OS-X (10.4.9) et supérieur' dans la liste déroulante des profiles préférés, puis cochez la case sous 'Définir comme profil actif en tant que profil préféré'.

- Cliquez sur OK pour appliquer.

Paramètres de la souris Linux

Configurer ces paramètres de la souris Linux®:

- (Mode souris standard uniquement) Définissez l'accélération de la souris et le seuil exactement sur 1. Entrez la commande suivante:`xset mouse 1 1`. Ce paramètre doit est réglé pour être exécuté lorsque vous vous connectez.

Paramètres de la souris Sun Solaris

Configurer ces paramètres de la souris Sun® Solaris™:

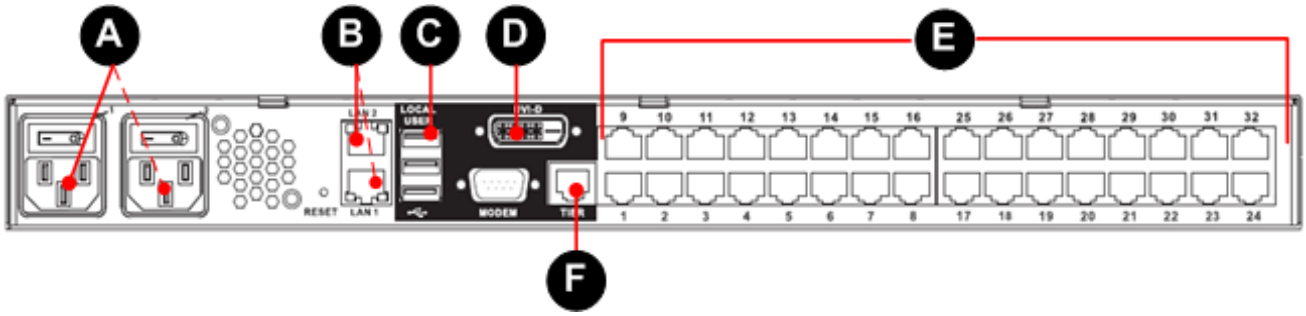
- Définissez la valeur d'accélération du pointeur de la souris et le seuil exactement sur 1.
- Assurez-vous que votre carte vidéo est configurée sur une résolution prise en charge et pour une sortie VGA, non à synchronisation composite.

Paramètres de souris IBM AIX

Configurer ces paramètres de souris IBM AIX®:

- Accédez au Gestionnaire de style, cliquez sur Paramètres de souris et réglez l'accélération de la souris sur 1.0 et Threshold (Seuil) sur 3.0.

Etape 3 : Connexion de l'équipement



A Alimentation CA

Connectez les source(s) d'alimentation:

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

Status LED pendant le démarrage de KX III

Lorsque vous démarrez le KX III, les LED lumineuses agissent de la manière suivante:

- Lors de la première mise sous tension:
  - Toutes les LED de canal sont allumées
  - La LED d'alimentation est éteinte

- Lors du démarrage:
  - Toutes les LED de canal sont éteintes
  - Si les deux sources d'énergie sont allumées, la LED d'alimentation est bleue
  - Si une seule source d'énergie est allumée, la LED d'alimentation est rouge

B Port réseau

KX III dispose de deux ports Ethernet pour les basculements - et non pour l'équilibrage des charges.

Par défaut, seul LAN1 est actif et le basculement automatique est désactivé.

Autorisez le basculement de réseau si vous voulez que LAN2 utilise la même adresse IP si jamais l'interface de réseau interne de KX III ou le commutateur réseau auquel elle est connecté devient indisponible.

Pour se connecter au réseau:

1. Reliez un câble Ethernet standard du port réseau libellé LAN1 à un commutateur, concentrateur ou routeur Ethernet.
2. Pour utiliser les capacités de basculement Ethernet optionnelles de ProductName :
   a. Reliez un câble Ethernet standard du port réseau libellé LAN2 à un commutateur, concentrateur ou routeur Ethernet.
   b. Activez le 'Basculement automatique' sur la page de 'Configuration réseau' de KX III.

C. Port d'utilisateur local (Console Locale)

Pour connecter le clavier et la souris:

- Connectez un clavier et une souris USB au ports de l'Utilisateur Local respectifs au dos de KX III.

Utilisez le port d'utilisateur locale de KX III pour un accès administratif et au serveur cible sur le rack via une interface d'utilisateur graphique.

Si le port local d'utilisateur est obligatoire pour l'installation et le paramétrage, il est facultatif par la suite.

D. Port DVI-D local

Un câble DVI standard est utilisé pour se connecter à un moniteur DVI local ou à un plateau de clavier (non fourni avec le KX III).

Connectez-vous au port DVI sur le plateau de clavier Raritan T1700-LED.

Utilisez un convertisseur DVI-D en VGA pour vous connecter aux moniteurs VGA.

Se connecter à un Moniteur DVI

Le moniteur local doit supporter une résolution minimum de 1024 x 768.

Pour se connecter à un moniteur DVI:

1. Connectez un clavier et une souris USB au ports de l'Utilisateur Local respectifs au dos de KX III.
2. Branchez une extremité d'un câble DVI dans le port DVI-D à l'arrière du KX III.
3. Connectez l'autre extrémité du câble DVI dans le port DVI du moniteur DVI.

Connexion à un Moniteur VGA (Optionnel).

Pour connecter à un moniteur VGA:

1. Connectez un clavier et une souris USB au ports de l'Utilisateur Local respectifs au dos de KX III.
2. Branchez le convertisseur DVI-D en VGA dans le port DVI-D au dos de KX III et sécurisez le en tournant les vis de chaque côté dans le sens des aiguilles d'une montre.
3. Connectez un câble VGA au convertisseur DVI-D en VGA, connectez l'autre extremité à votre moniteur VGA et sécurisez en renforçant les vis.

Remarque : Le convertisseur DVI-D en VGA n'est pas inclus avec le KX III. Contactez le service Ventes de Raritan pour plus d'informations.

E. Connexion des serveurs cibles au KX III

Pour connecter un serveur cible à KX III :

1. Connectez les prises clavier, souris et vidéo sur le CIM aux ports correspondants sur le serveur cible.
2. Reliez le CIM à un port cible disponible du serveur à l'arrière du dispositif KX III via un câble Cat5/5e/6.

F. Multiniveau (Facultatif)

Reportez-vous à ***Configuration et activation de la fonction multiniveau*** (à la page 136, ***http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#33184***)

Etape 4 : Configurer le KX III

Pour les étapes suivantes, vous devez changer le mot de passe par défaut et assigner son adresse IP de la Console Locale au KX III.

Toutes les autres étapes peuvent être effectuées soit via la Console Locale, ou de la Console à distance de KX III via un navigateur web pris en charge en utilisant l'adresse IP par défaut de KX III.

Java® 1.7 (ou plus élevé) ou Microsoft .NET® 3.5 (ou version ultérieure) est obligatoire pour utiliser KX III.

Modification du mot de passe par défaut

La première fois que vous démarrez KX III, il vous est demandé de changer le mot de passe par défaut.

Pour changer le mot de passe par défaut :

1. Une fois que l'unité a été démarrée, entrez le nom d'utilisateur *admin* et mot de passe *raritan* par défaut. Cliquez sur Login (Se connecter).
2. Entrez l'ancien mot de passe *raritan*, puis entrez et ré-entrez 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).
3. Cliquez sur Appliquer. Cliquez sur OK sur la page de Confirmation.

Assigner une adresse IP au KX III

Pour assigner une adresse IP au KX III:

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 III.

   Contenant un maximum de 32 caractères alphanumériques et caractères valides, sans espaces entre les caractères.
3. Ensuite, configurez les paramètres IPv4, Ipv6 et DNS.

Configurer les paramètres Ipv4

1. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :

a. Le cas échéant, entrez l'adresse IP. L'adresse IP par défaut est 192.168.0.192.

b. Renseignez le champ Subnet Mask (Masque de sous-réseau). Le masque de sous-réseau par défaut est 255.255.255.0.

c. Renseignez le champ Default Gateway (Passerelle par défaut) si l'option None (Néant) est sélectionnée dans la liste déroulante IP Auto Configuration (Configuration automatique IP).

d. Renseignez le champ Preferred DHCP Host Name (Nom de l'hôte DHCP privilégié) si l'option DHCP est sélectionnée dans la liste déroulante IP Auto Configuration (Configuration automatique IP).

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

- Aucune (IP Statique) - Cette option requiert une saisie manuelle des paramètres réseau.

  Il s'agit de l'option recommandée car KX III est un dispositif d'infrastructure et son adresse IP ne devrait pas changer.

  Sélectionnez cette option si vous souhaiter assurer des capacités de basculement redondants dans le cas où le port ethernet primaire (ou le commutateur / routeur auquel il est connecté) échoue. Si cela échoue, KX III échoue sur le port de réseau secondaire avec la même adresse IP, assurant qu'il n'y ait pas d'interruption.

- 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 du serveur DHCP.

  Avec cette option, les paramètres réseau sont affectés par le serveur DHCP.

  Si DHCP est utilisé, entrez le nom d'hôte privilégié (DHCP uniquement). 63 caractères au plus.

2. Ensuite, configurer les paramètres IPv6 et/ou DNS.

Configurer les paramètres IPv6

1. Si vous utilisez IPv6, 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 et IPv6 sur le dispositif.

   b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à KX III.

   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, et 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. Sélection d'une Configuration IP automatique:

- Aucune (IP Statique) - Cette option requiert une saisie manuelle des paramètres réseau.

  Il s'agit de l'option recommandée car KX III est un dispositif d'infrastructure et son adresse IP ne devrait pas changer.

  Sélectionnez cette option si vous souhaiter assurer des capacités de basculement redondants dans le cas où le port ethernet primaire (ou le commutateur / routeur auquel il est connecté) échoue. Si cela échoue, KX III bascule sur le port du réseau secondaire avec la même adresse IP, assurant qu'il n'y ait pas d'interruption.

  Si Aucun est sélectionné, les champs de Paramètres Réseau de Base suivants 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.

2. Ensuite, configurer les paramètres DNS.

Configurer la paramètres DNS

1. 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.

2. Si l'option Utiliser les adresses de serveurs DNS suivantes est activée, que le DHCP soit sélectionné ou non, les adresses saisies dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les informationssuivantes si l'option 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.

3. Lorsque vous avez terminé, cliquez sur OK.

Votre KX III est maintenant accessible depuis le réseau.

Nommez vos serveurs cibles

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait.
2. Sélectionnez Paramètres du dispositif > Configuration du port, puis cliquez sur le nom du port du serveur cible que vous souhaitez nommer.
3. Entrez un nom pour le serveur.

   Contenant un maximum de 32 caractères alphanumériques et spéciaux.
4. Cliquez sur OK.

Spécification de la détection automatique de l'alimentation

Le KX III fournit des sources d'alimentation doubles.

Lorsque les deux sources d'énergie sont utilisées, le KX III les détecte automatiquement et vous notifie de leur statut.

En outre, les cases à détection automatique Powerln1 et Powerln2 sont automatiquement sélectionnées sur la Page de configuration de l'alimentation.

Si vous n'utilisez qu'une source d'alimentation, vous pouvez activer la détection automatique pour la source d'énergie en cours d'utilisation.

Pour activer la détection automatique des alimentations utilisées :

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

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

Configuration des paramètres de date et heure (facultatif)

Le cas échéant, configurez les paramètres de date et d'heure.

Les paramètres de date et heure affectent la validation du certificat SSL si LDAPS est activé.

Pour définir la date et l'heure :

1. Sélectionnez Paramètres du dispositif > 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 « Ajuster à l'heure d'été ».
4. Choisissez la méthode à utiliser pour définir la date et l'heure :
   - User Specified Time (Heure spécifiée par l'utilisateur) - utilisez 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).
   - Synchronisation avec le Serveur NTP - utilisez cette option pour synchroniser la date et l'heure avec le Serveur de Protocole Temps Réseau (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. Entrez l'adresse IP du Serveur d'horloge secondaire. **Facultatif**

   Remarque : Si DHCP est sélectionné pour les Paramètres réseau sur la Page Réseau, l'adresse IP du serveur NTP est automatiquement récupérée à partir du serveur DHCP par défaut.

   Entrez manuellement l'adresse IP du serveur NTP en sélectionnant la case Ecraser DHCP.
6. Cliquez sur OK.

Création de groupes d'utilisateurs et d'utilisateurs

Remarque aux utilisateurs de CC-SG

Lorsque KX III est géré par CommandCenter Secure Gateway, CC-SG authentifie les utilisateurs et les groupes, à l'exception des utilisateurs locaux requérant l'accès au port local.

Lorsque CC-SG assure la gestion de KX III, les utilisateurs du port local sont authentifiés par rapport à la base de données des utilisateurs locaux ou au serveur d'authentification à distance (LDAP/LDAPS ou RADIUS) configurés sur ProductName. Ils ne sont pas authentifiés par rapport à la base de données des utilisateurs de CC-SG.

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

Protocoles pris en charge

Afin de simplifier la gestion des noms d'utilisateur et des mots de passe, KX III 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 III. 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.

Etape 5 : Lancement de la console à distance de KX III

Connectez-vous à votre console à distance KX III depuis un poste de travail doté d'une connectivité réseau et possédant Microsoft.NET® et/ou Java Runtime Environment® installé.

Pour démarrer la console distante de KX III :

1. Lancer un navigateur pris en charge.
2. Entrez soit:
   - L'URL - *http://ADRESSE-IP* pour utiliser le client KVM virtuel basé sur Java

     Ou

   - *http://ADRESSE-IP/akc* pour le client KVM actif basé sur .NET

   ADRESSE-IP est l'adresse IP assignée à votre KX III.

Vous pouvez également l'HTTPS ou le nom DNS du KX III assigné par votre administrateur (si applicable).

3. Vous êtes toujours redirigé à l'adresse IP de HTTP à HTTPS.
4. Entrez vos nom d'utilisateur et mot de passe. Cliquez sur Login (Se connecter).

Accès et gestion des serveurs cible à distance

La page d'Accès aux ports de KX III fournit la liste de tous les ports du produit, des serveurs cible connectés, de leur état et leur disponibilité.

Accès à un serveur cible depuis KX III

Pour accéder à un serveur cible :

1. Dans la page d'accès aux ports de KX III, cliquez sur l'option Nom du port associée à la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.

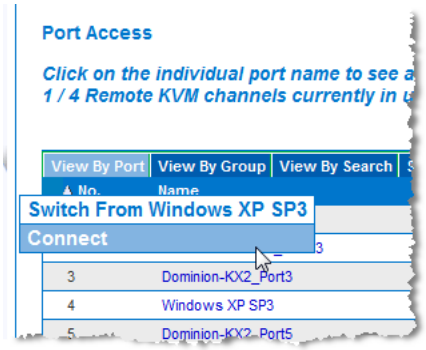
2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. Une fenêtre KVM s'ouvre, qui contient une connexion à la cible.

Commutation entre les serveurs cible

Pour commuter entre des serveurs cible KVM :

1. Si vous utilisez déjà un serveur cible, accédez à la page Port Access de KX III.
2. Cliquez sur le nom du port associé à la cible à laquelle vous souhaitez accéder. Le menu Port Action (Action des ports) apparaît.

3. Sélectionnez Switch From (Commuter depuis) dans le menu d'action des ports. Le nouveau serveur cible sélectionné est affiché.



Déconnexion d'un serveur cible

Pour déconnecter un serveur cible :

- Sur la page d'accès aux ports, cliquez sur le Nom du port associée à la cible de laquelle vous souhaitez vous déconnecter, cliquez ensuite sur Déconnecter dans le menu d'Action de Port lorsqu'il apparait.

  Ou

- Fermer la fenêtre client KVM

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

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

Si vous utilisez une langue autre que l'anglais américain, le clavier doit être configuré pour celle-ci.

De plus, la langue du clavier de l'ordinateur client et des serveurs cibles KVM doit être la même.

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

Modification du code de disposition de clavier (cibles Sun)

Suivez cette procédure si vous disposez d'un DCIM-SUSB et souhaitez utiliser une disposition de clavier dans une autre langue.

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

1. Ouvrez une fenêtre de l'éditeur de texte sur le poste de travail Sun™.

2. Assurez-vous que la touche Verr num soit active, et appuyez sur la touche Ctrl située à gauche et sur la touche Suppr du clavier, ou sélectionnez l'option « définir les options clavir/souris CIM » à partir du menu du clavier.

   Le voyant du verrouillage des majuscules clignote pour indiquer que le CIM est en mode de modification du code de disposition.

   La fenêtre de texte affiche les informations suivantes : `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).`

3. Saisissez le code de disposition souhaité (par exemple, *31* pour le clavier japonais). Appuyez sur Entrée.
4. Mettez le dispositif hors tension, puis à nouveau sous tension. Le DCIM-SUSB procède à une réinitialisation (alimentation cyclique).
5. Vérifiez que les caractères sont corrects.

Etape 7 : Créer et installer un certificat SSL

Raritan vous recommande fortement d'installer votre propre Certificat SSL sur tout dispositif KX III.

Cette pratique de sécurité réduit le nombre de messages d'avertissement de Java®, et évite les attaques intermédiaires.

Cela évite également les futures versions de Java et du navigateur de bloquer l'accès à votre dispositif KX III.

Pour des informations concernant la création et l'installation de certificats SSL, consultez ***Certificats SSL*** (à la page 183).

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

Présentation

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

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

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

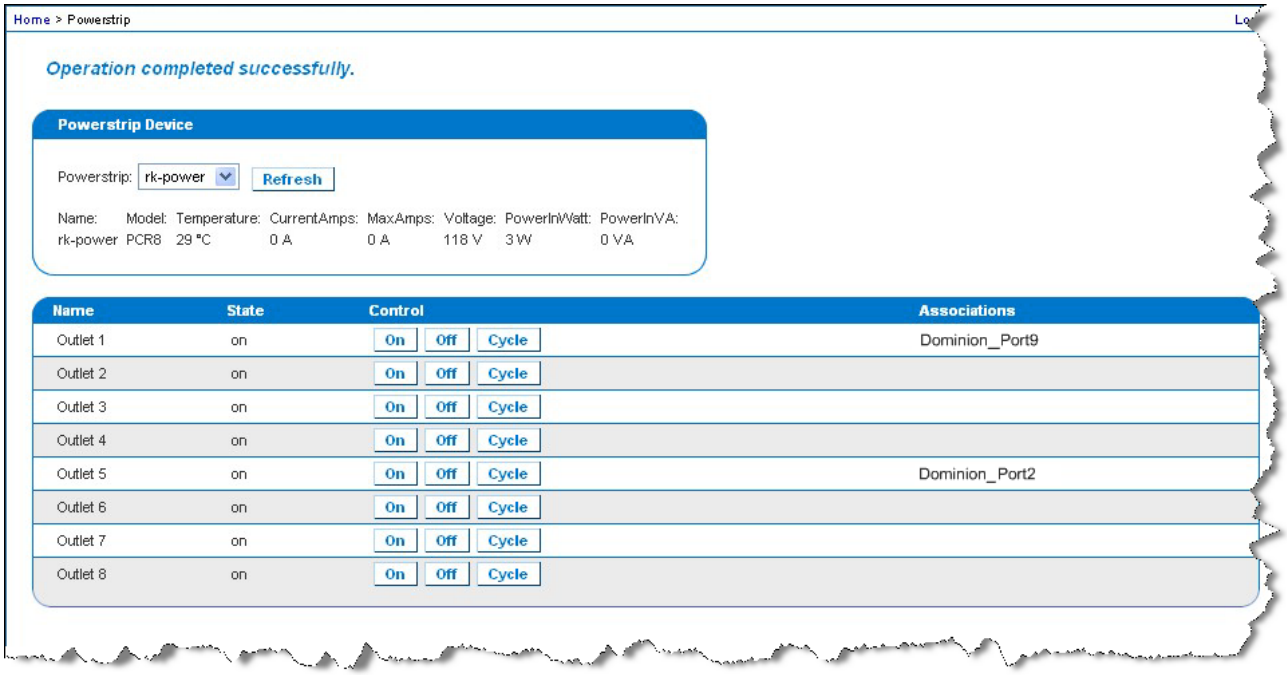
*Remarque : Pour plus d'informations sur le paramétrage d'une unité PX, reportez-vous au **manuel d'utilisation de Raritan PX**.*

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

- Informations sur le dispositif de barrette d'alimentation :
  - Nom
  - Modèle
  - Température
  - Current Amps (Courant en ampères)
  - Maximum Amps (Courant maximal en ampères)
  - Voltage (Tension)
  - Power in Watts (Puissance en watts)
  - Power in Volts Ampere (Puissance en voltampère)
- Informations sur l'affichage des prises :
  - Name (Nom) - Il s'agit du nom affecté à la prise lors de sa configuration.
  - State (Etat) - Etat sous ou hors tension de la prise.
  - Control (Contrôle) - Permet de mettre les prises sous ou hors tension, ou d'effectuer leur alimentation cyclique.

- Association - Il s'agit des ports associés à la prise.

Initialement, lorsque vous ouvrez la page Powerstrip, les barrettes d'alimentation actuellement connectées à KX III s'affichent dans la liste déroulante Powerstrip. En outre, les informations relatives à la barrette d'alimentation sélectionnée s'affichent. Si aucune barrette d'alimentation n'est connectée àKX III, un message indiquant «Aucune barrette d'alimentation détectée » s'affiche dans la section Dispositif de barrette d'alimentation de la page.



Mise sous/hors tension des prises et alimentation cyclique

Pour mettre une prise sous tension :

1. Cliquez sur le menu Power (Alimentation) pour accéder à la page Powerstrip (Barrette d'alimentation).
2. Dans la liste déroulante Powerstrip, sélectionnez la PDU de rack (barrette d'alimentation) PX que vous souhaitez mettre sous tension.
3. Cliquez sur Refresh (Actualiser) pour afficher les contrôles d'alimentation.
4. Cliquez sur On (Sous tension) juste à côté de la prise que vous souhaitez mettre sous tension.
5. Cliquez sur OK pour fermer la boîte de dialogue de confirmation Power On (Sous tension). La prise est mise sous tension et son état indique on.

Pour mettre une prise hors tension :

1. Cliquez sur Off (Hors tension) juste à côté de la prise que vous souhaitez mettre hors tension.
2. Cliquez sur OK dans la boîte de dialogue Power Off (Hors tension).
3. Cliquez sur OK dans la boîte de dialogue de confirmation Power Off (Hors tension). La prise est mise hors tension et son état indique off.

Pour effectuer l'alimentation cyclique d'une prise :

1. Cliquez sur Cycle juste à côté de la prise que vous souhaitez mettre sous cycle. La boîte de dialogue Power Cycle Port (Port d'alimentation cyclique) s'ouvre.
2. Cliquez sur OK. L'alimentation cyclique de la prise débute alors (notez qu'elle peut prendre plusieurs secondes).
3. Une fois l'alimentation cyclique terminée, la boîte de dialogue s'ouvre. Cliquez sur OK pour fermer la boîte de dialogue.

Profils USB

Présentation

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

Le profil USB générique (défaut) répond aux besoins de la grande majorité des configurations de serveurs cible KVM déployées.

Des profils supplémentaires sont fournis pour répondre aux besoins spécifiques d'autres configurations de serveurs déployées courantes (par exemple, Linux® et MAC OS X®).

Un certain nombre de profils (désignés par nom de plate-forme et révision de BIOS) permet également d'améliorer la compatibilité de la fonction Support virtuel avec le serveur cible ; par exemple, lors d'un fonctionnement au niveau du BIOS.

Les profils USB sont configurés sur la page Paramètres du dispositif > Configuration des ports > Port des consoles distantes et locales de KX III.

Un administrateur peut configurer le port avec les profils USB répondant le mieux aux besoins de l'utilisateur et de la configuration des serveurs cible.

Un utilisateur qui se connecte à un serveur cible KVM choisit parmi les profils présélectionnés dans Virtual KVM Client, suivant l'état de fonctionnement du serveur cible KVM.

Par exemple, si le serveur est lancé sur le système d'exploitation Windows®, il est recommandé d'utiliser le profil générique.

Mais si l'utilisateur souhaite modifier les paramètres du menu du BIOS ou effectuer le démarrage à partir d'un lecteur de support virtuel, suivant le modèle du serveur cible, un profil BIOS est sans doute plus adéquat.

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

Compatibilité CIM

Pour utiliser les profils USB, vous devez disposer d'un CIM média virtuel dont le firmware est mis à jour. Pour une liste des CIM média virtuels, consultez ***Spécifications des CIM pris en charge*** (à la page 336).

Profils USB disponibles

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

Profil USB	Description
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	BIOS Dell PowerEdge 1950/2950/2970/6950/R200 Utilisez ce profil ou le profil générique pour le BIOS Dell PowerEdge 1950/2950/2970/6950/R200. Restrictions : ▪ Néant
BIOS Dell OptiPlex ™ Clavier et Souris seulement	Accès BIOS Dell Optiplex (clavier et souris uniquement) Utilisez ce profil pour disposer de la fonctionnalité de clavier pour le BIOS Dell OptiPlex lors de l'utilisation de D2CIM-VUSB. Avec le nouveau D2CIM-DVUSB, utilisez le profil générique. Avis : ▪ Optiplex 210L/280/745/GX620 nécessite D2CIM-DVUSB avec le profil générique pour prendre en charge les supports virtuels. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Fonction Supports virtuels non prise en charge
BIOS Dell OptiPlex 790	Utilisez ce profil pour Dell Optiplex 790 pendant les opérations BIOS. Avertissement : ▪ L'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Synchronisation absolue de la souris non supportée ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.

Profil USB	Description
BIOS Dell OptiPlex 790 Clavier seulement	Utilisez ce profil pour Dell Optiplex 790 pendant l'utilisation de Macros clavier lors d'opérations BIOS. Seul le clavier est activé avec ce profil. Restrictions : ▪ La souris est désactivée. ▪ Les lecteurs de CD-ROM et disques durs virtuels sont désactivés.
BIOS DellPowerEdge clavier et souris uniquement	Accès BIOS DellPowerEdge clavier et souris uniquement Utilisez ce profil pour disposer de la fonctionnalité de clavier pour le BIOS Dell PowerEdge lors de l'utilisation de D2CIM-VUSB. Avec le nouveau D2CIM-DVUSB, utilisez le profil générique. Avis : ▪ PowerEdge 650/1650/1750/2600/2650 BIOS ne prend pas en charge les lecteurs USB CD-ROM et les disques durs comme service armorçable ▪ PowerEdge 750/850/860/1850/2850/SC1425 BIOS nécessite D2CIM-DVUSB avec le profil générique pour prendre en charge les supports virtuels. ▪ Utilisez BIOS Dell PowerEdge 1950/2950/2970/6950/R200 ou le profil générique pour PowerEdge 1950/2950/2970/6950/R200 lors d'un fonctionnement dans le BIOS. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Synchronisation™ absolue de la souris non supportée ▪ Fonction Supports virtuels non prise en charge
Carte-mère BIOS ASUS P4C800	Utilisez ce profil pour accéder au BIOS et démarrer depuis Virtual Media sur des systèmes Asus P4C800. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.

Profil USB	Description
BIOS Generic	BIOS Generic Utilisez ce profil lorsque le profil générique du système d'exploitation ne fonctionne pas sur le BIOS. AVERTISSEMENT : L'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Synchronisation™ absolue de la souris non supportée ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Utilisez ce profil pour HP Proliant DL145 PhoenixBIOS pendant l'installation du système d'exploitation. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Utilisez ce profil pour démarrer les ordinateurs de la série HP Compaq DC7100/DC7600 à partir du support virtuel. Restrictions : ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS IBM ThinkCentre Lenovo	BIOS IBM Thinkcentre Lenovo Utilisez le profil pour la carte principale IBM® Thinkcentre Lenovo (modèle 828841U) pendant les opérations du BIOS. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
IBM BladeCenter H avec Advanced Management Module	Utilisez ce profil pour activer la fonctionnalité de support virtuel lorsque D2CIM-VUSB ou D2CIM-DVUSB est connecté au module AMM. Restrictions : ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.

Profil USB	Description
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 et X61 (démarrage à partir du support virtuel) Utilisez ce profil pour démarrer les ordinateurs portables des séries T61 et X61 à partir du support virtuel. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps)
Générique	Le profil USB générique se comporte comme dans la version originale du KX3. Utilisez-le pour les systèmes d'exploitation Windows 2000®, Windows XP®, Windows Vista® et ultérieur. Restrictions : ▪ Néant
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Utilisez ce profil pour le serveur HP Proliant DL360/DL380 série G4 lors de l'installation du système d'exploitation à l'aide de HP SmartStart CD. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Synchronisation™ absolue de la souris non supportée
HP Proliant DL360/DL380 G4 (Serveur d'installation Windows 2003®)	HP Proliant DL360/DL380 G4 (Installation Windows 2003 Server) Utilisez ce profil pour le serveur HP Proliant DL360/DL380 série G4 lors de l'installation de Windows 2003 Server sans HP SmartStart CD. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps)
Linux®	Profil Linux générique Il s'agit du profil Linux générique ; utilisez-le pour Redhat Enterprise Linux, SuSE Linux Enterprise Desktop et distributions semblables. Restrictions : ▪ Synchronisation™ absolue de la souris non supportée
BIOS Mac®	BIOS Mac Utilisez ce profil pour le BIOS Mac. Restrictions : ▪ Synchronisation™ absolue de la souris non supportée ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. Si vous voyez ce profil USB, consultez ***Modes de souris lors de***

Profil USB	Description
	l'utilisation du Menu de Démarrage Mac (à la page 56)pour des informations sur les modes de souris lors de l'utilisation du Menu de démarrage Mac
MAC OS X® 10.4.9 (et supérieur)	Mac OS X version 10.4.9 (et supérieur) Ce profil compense la graduation des coordonnées de souris introduite dans les récentes versions de Mac OS X. Sélectionnez-le si les positions de la souris distante et locale sont désynchronisées près des bordures du bureau. Restrictions : ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Carte-mère industrielle RUBY (AwardBIOS)	Carte-mère industrielle RUBY (AwardBIOS) Utilisez ce profil pour les cartes mères industrielles de la série RUBY-9715VG2A avec Phoenix/AwardBIOS v6.00PG. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Supermicro Mainboard Phoenix (AwardBIOS)	Carte-mère Supermicro Phoenix (AwardBIOS) Utilisez ce profil pour les cartes-mères de la série Supermicro avec Phoenix AwardBIOS. Restrictions : ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Suse 9.2	SuSE Linux 9.2 Utilisez-le pour la distribution SuSE Linux 9.2. Restrictions : ▪ Synchronisation™ absolue de la souris non supportée ▪ Vitesse du bus USB limitée à plein régime (12 Mbps)
Troubleshooting 1	Dépannage de profil 1 ▪ Stockage en masse en premier ▪ Clavier et souris (Type 1) ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : L'énumération USB se déclenche dès

Profil USB	Description
	que le support virtuel est connecté ou déconnecté.
Troubleshooting 2	Profil de dépannage 2 ▪ Clavier et souris (Type 2) en premier ▪ Stockage en masse ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : L'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Troubleshooting 3	Profil de dépannage 3 ▪ Stockage en masse en premier ▪ Clavier et souris (Type 2) ▪ Vitesse du bus USB limitée à plein régime (12 Mbps) ▪ Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : L'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Utiliser le plein régime pour le CIM de support virtuel	Utiliser le plein régime pour le CIM de support virtuel Ce profil se comporte comme dans la version originale KX3 lorsque l'option Full Speed for Virtual Media CIM (Plein régime pour le CIM de support virtuel) est activée. Utile pour le BIOS qui ne peut pas traiter les dispositifs USB High Speed. Restrictions : ▪ Vitesse du bus USB limitée à plein régime (12 Mbps)
Utiliser le plein régime pour USB clavier et souris	Ce profil paramètre l'interface USB clavier et souris du CIM Dual-VM sur Full Speed (Plein régime). Utile pour les dispositifs qui ne peuvent pas fonctionner correctement avec les paramètres USB Low Speed (Faible régime). Restrictions : ▪ Vitesse du bus USB définie sur plein régime (12 Mbps) dans l'interface USB clavier et souris

Modes de souris lors de l'utilisation du menu de démarrage Mac

Lors de l'utilisation de profils USB, afin d'utiliser la Souris dans le Menu de Démarrage Mac, vous devez utiliser le Mode de Souris Unique car le Mode de Souris Absolue n'est pas supporté dans le BIOS.

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

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

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

3. Une fois que vous avez quitté le menu de démarrage et êtes de retour aux système d'exploitation X, quittez le mode de souris unique et repassez en mode de souris absolue.

Sélection des profils pour un port KVM

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

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

L'affectation de profils USB à un port KVM met ceux-ci à la disposition d'un utilisateur connecté à un serveur cible KVM. Si besoin, l'utilisateur peut sélectionner un profil USB dans le menu Profil USB dans Virtual KVM Client (VKC).

Pour plus d'informations sur l'affectation de profils USB à un port KVM, reportez-vous à ***Configuration des profils USB (page Port)*** (à la page 127).

User Management (Gestion des utilisateurs)

Groupes d'utilisateurs

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

Chaque KX III est livré 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 III. Vous pouvez créer jusqu'à 254 groupes d'utilisateurs dans le KX III.

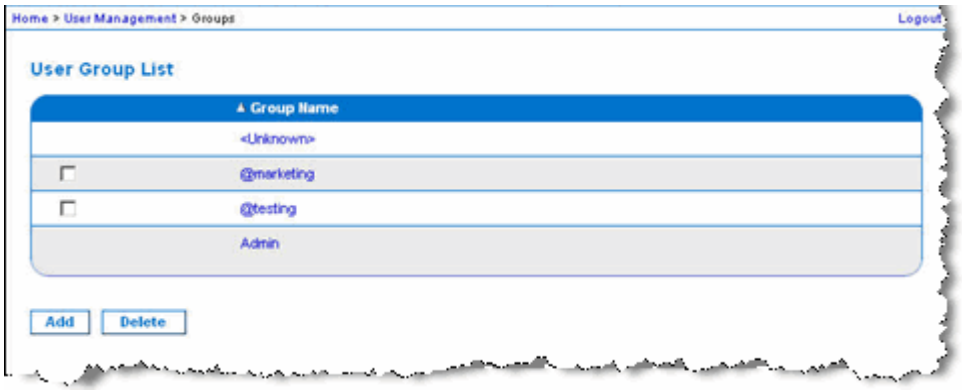
Liste des groupes d'utilisateurs

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 III 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 ».

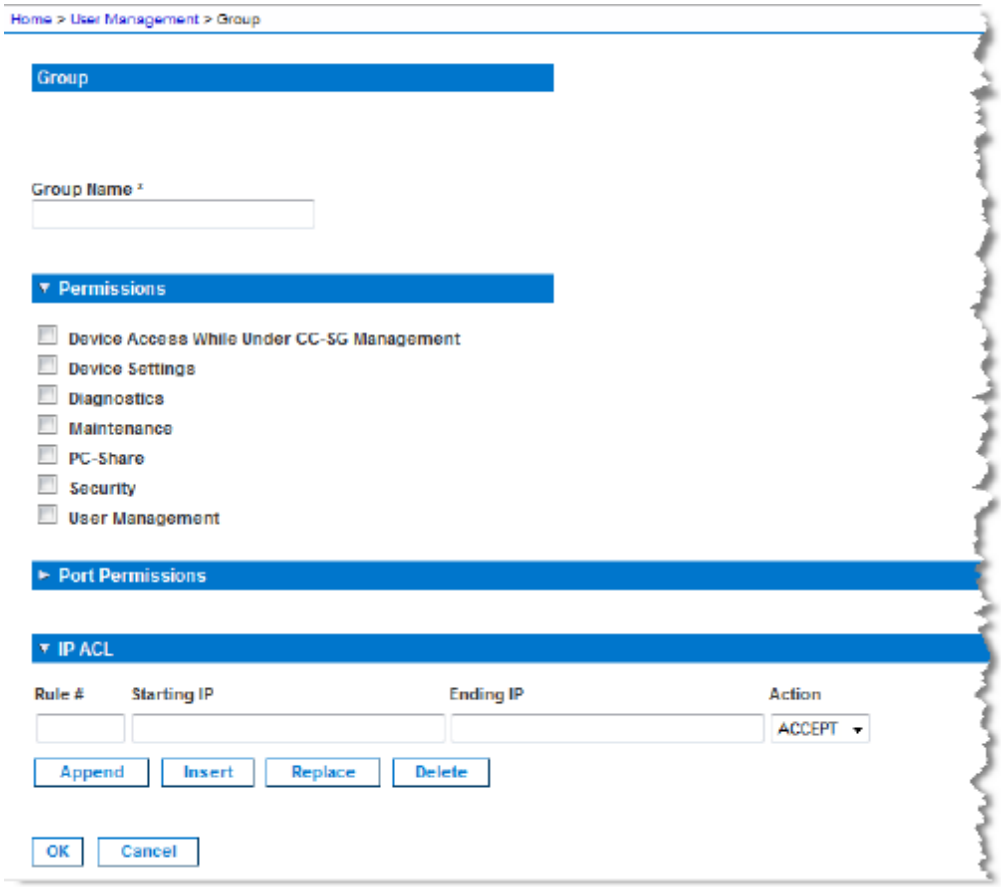
Lorsqu'un utilisateur est authentifié, le dispositif utilise les informations relatives au groupe auquel il appartient pour déterminer ses autorisations : ports de serveur accessibles, autorisation éventuelle de redémarrer l'unité, etc.

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.
4. Indiquez les ports de serveur et le type d'accès pour chaque utilisateur appartenant à ce groupe. Reportez-vous à ***Configuration des autorisations d'accès aux ports*** (à la page 62).
5. Configurez la liste de contrôle d'accès IP (IP ACL). Cette fonction limite l'accès au dispositif KX III par le biais de la spécification d'adresses IP. Cette fonction s'applique uniquement aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste de contrôle d'accès IP qui s'applique à toutes les tentatives d'accès au dispositif (et est prioritaire). Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 63). **Facultatif**

6. Cliquez sur OK.



Configuration des autorisations

Autorisation	Description
Device Access While Under CC-SG Management (Accès au dispositif sous la gestion de CC-SG)	Permet aux utilisateurs et aux groupes d'utilisateurs ayant cette autorisation d'accéder directement à KX III 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 . 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 III. L'authentification de l'utilisateur est effectuée suivant les paramètres d'authentification de KX III. *Remarque : Le groupe d'utilisateurs Admin*

Autorisation	Description
	dispose de cette autorisation par défaut.
Device Settings (Paramètres du dispositif)	Paramètres réseau, paramètres date/heure, configuration des ports (nom de canal, association d'alimentation), gestion des événements (SNMP, Syslog), configurations de serveur de fichiers du support virtuel.
Diagnostics	Etat de l'interface réseau, statistiques de réseau, envoi d'une commande ping à un hôte, traçage d'itinéraire jusqu'à un hôte, diagnostiques de KX III.
Maintenance	Sauvegarde et restauration de base des données, mise à niveau du firmware, réinitialisation des paramètres usine, redémarrage.
PC-Share	Accès simultané à la même cible par plusieurs utilisateurs. Si vous utilisez une configuration multiniveau où un dispositif KX III de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, tous les dispositifs doivent partager le même paramètrage PC-Share. Reportez-vous à Configuration et activation de la fonction multiniveau pour plus d'informations sur la fonction multiniveau.
Sécurité	Certificat SSL, paramètres de sécurité (VM Share, PC-Share), LCA IP.
User Management (Gestion des utilisateurs)	Gestion des utilisateurs et des groupes, authentification à distance (LDAP/LDAPS/RADIUS), paramètres de connexion. Si vous utilisez une configuration multiniveau où un dispositif KX III de base permet d'accéder à plusieurs autres dispositifs en niveau, les paramètres d'utilisateur, de groupe d'utilisateurs et d'authentification à distance doivent être cohérents à travers tous les dispositifs. Reportez-vous à Configuration et activation de la fonction multiniveau pour plus d'informations sur la fonction multiniveau.

Configuration des autorisations d'accès aux ports

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

Port Access (Accès aux ports)	
option	**Description**
Deny (Refuser)	Accès refusé complètement
View (Afficher)	Afficher (mais non interagir avec) le serveur cible connecté.
Control (Contrôler)	Contrôle le serveur cible connecté. Le contrôle doit être affecté au groupe si l'accès du support virtuel et de gestion d'alimentation est également accordé. Pour permettre à tous les utilisateurs d'un groupe de voir les commutateurs KVM ajoutés, un accès Control doit être accordé à chacun. S'ils ne disposent pas de cette autorisation et qu'un commutateur KVM est ajouté ultérieurement, ils ne pourront pas le voir. L'accès Control doit être accordé pour que les contrôles associés à l'audio ou aux cartes à puce soient actifs.

VM access (Accès au support virtuel)	
option	**Description**
Deny (Refuser)	L'autorisation d'accès au support virtuel est entièrement refusée pour le port.
Read-Only (Lecture seule)	L'accès au support virtuel est limité à l'accès en lecture uniquement.
Read-Write (Lecture-écriture)	Accès total (en lecture, en écriture) au support virtuel

VM access (Accès au support virtuel) Power control access (Accès à la gestion d'alimentation)	
option	**Description**
Deny (Refuser)	Refuser la gestion d'alimentation au serveur cible
distant	Autorisation totale de gestion d'alimentation sur un serveur cible

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

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

Définition des autorisations pour un groupe individuel

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

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

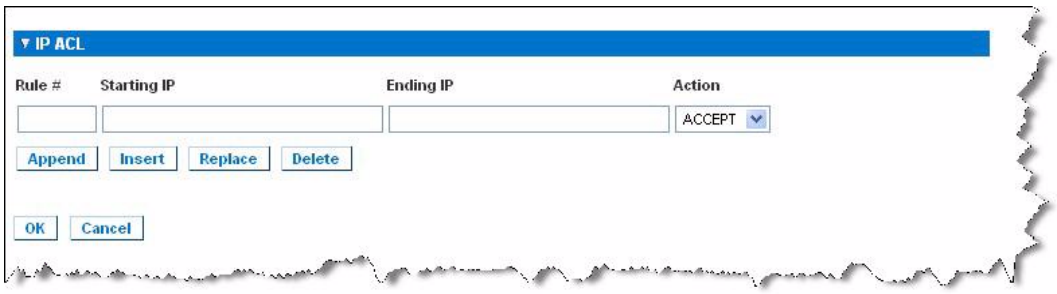
LCA (liste de contrôle d'accès) IP de groupes

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

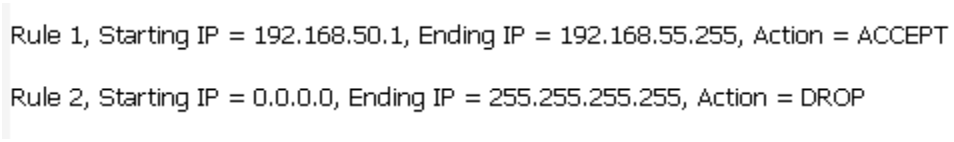
Pour remplacer une règle :

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.



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

Modification d'un groupe d'utilisateurs existant

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

Pour modifier un groupe d'utilisateurs existant :

1. A partir de la page Group, modifiez les champs appropriés et définissez les autorisations adéquates.
2. Définissez les permissions pour le groupe. Cochez les cases situées en regard des permissions que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à Configuration des autorisations.

3. Définissez les autorisations d'accès aux ports. Spécifiez les ports de serveur auxquels peuvent accéder les utilisateurs appartenant à ce groupe (et le type d'accès). Reportez-vous à ***Configuration des autorisations d'accès aux ports*** (à la page 62).
4. Configurez la liste de contrôle d'accès IP (IP ACL) (facultatif). Cette fonction limite l'accès au dispositif KX III par le biais de la spécification d'adresses IP. Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 63).
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>.

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 III. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité KX III.

Vous pouvez créer jusqu'à 254 utilisateurs pour chaque groupe.

Si vous utilisez une configuration multiniveau où un dispositif KX III de base est utilisé pour accéder à plusieurs autres dispositifs en niveau, les utilisateurs auront besoin d'autorisations d'accès au dispositif de base et à chaque dispositif en niveau (selon les besoins).

Lorsqu'un utilisateur se connecte au dispositif de base, chaque dispositif en niveau est interrogé et l'utilisateur peut accéder à chaque serveur cible pour lequel il dispose d'autorisations. Reportez-vous à Configuration et activation de la fonction multiniveau pour plus d'informations sur la fonction multiniveau.

Ajout d'un nouvel utilisateur

Il est recommandé de définir les groupes d'utilisateurs avant de créer des utilisateurs KX III, 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 169).*

Pour ajouter un nouvel utilisateur :

1. Sélectionnez Gestion des utilisateurs > Ajouter un nouvel utilisateur ou cliquez sur Ajouter sur la page de la liste d'utilisateur.
2. Tapez un nom unique dans le champ du 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. Entrez un mot de passe dans le champ Mot de passe, puis entrez-le à nouveau dans le champ 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 63).
6. Pour activer le nouvel utilisateur, laissez la case Active cochée. Cliquez sur OK.

Affichage de la liste des utilisateurs de KX III

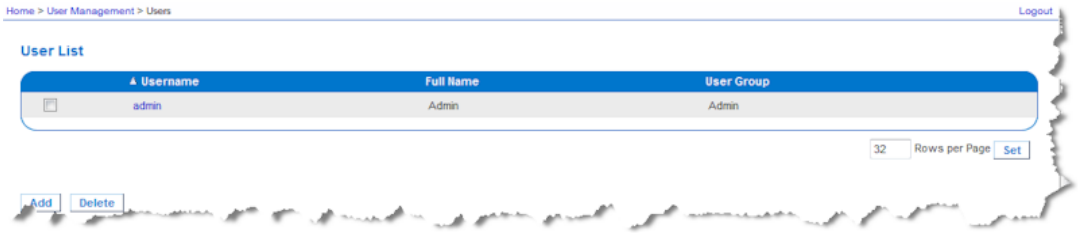
La page User List (Liste des utilisateurs) affiche une liste de tous les utilisateurs, avec leur nom d'utilisateur, leur nom complet et le groupe d'utilisateurs auquel ils appartiennent. Pour trier cette liste en fonction d'une colonne, cliquez sur le nom de celle-ci. A partir de la page User List, vous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

Les utilisateurs KX III disposant de privilèges de Gestion des utilisateurs peuvent déconnecter d'autres utilisateurs des ports ou forcer leur déconnexion le cas échéant. Reportez-vous à ***Déconnexion d'utilisateurs des ports*** (à la page 69) et ***Fermeture de la session des utilisateurs de KX III (Déconnexion forcée)*** (à la page 70) respectivement.

Pour afficher les ports cible auxquels chaque utilisateur est connecté, reportez-vous à ***Affichage des utilisateurs par port*** (à la page 69).

Pour afficher la liste des utilisateurs :

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



Affichage des utilisateurs par port

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

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

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

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

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

- Username - nom d'utilisateur servant aux connexions d'utilisateur et de cible.
- Accès depuis - adresse IP du PC client accédant au KX III.
- Status - statut actuel de la connexion, Active ou Inactive.

Pour afficher les utilisateurs par port :

- Choisissez 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 III.

Remarque : la fermeture de session déconnecte l'utilisateur du port cible et de KX III. Reportez-vous à **Fermeture de la session des utilisateurs de KX III (Déconnexion forcée)** *(à la page 70) 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 III (Déconnexion forcée)

Si vous êtes administrateur, vous pouvez fermer la session d'un autre utilisateur authentifié localement qui est connecté à KX III. Les utilisateurs peuvent également être déconnectés au niveau du port. Reportez-vous à ***Déconnexion d'utilisateurs des ports*** (à la page 69).

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

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.

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 67) pour plus d'informations sur les méthodes d'accès à la page User.
5. Pour supprimer un utilisateur, cliquez sur Delete. Vous êtes invité à confirmer la suppression.
6. Cliquez sur OK.

Paramètres d'authentification

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

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

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

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

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

Pour configurer l'authentification :

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

Pour réinitialiser les paramètres par défaut usine :

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

Implémentation de l'authentification à distance LDAP/LDAPS

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

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

Pour utiliser le protocole d'authentification LDAP :

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

pour développer la section LDAP de la page.

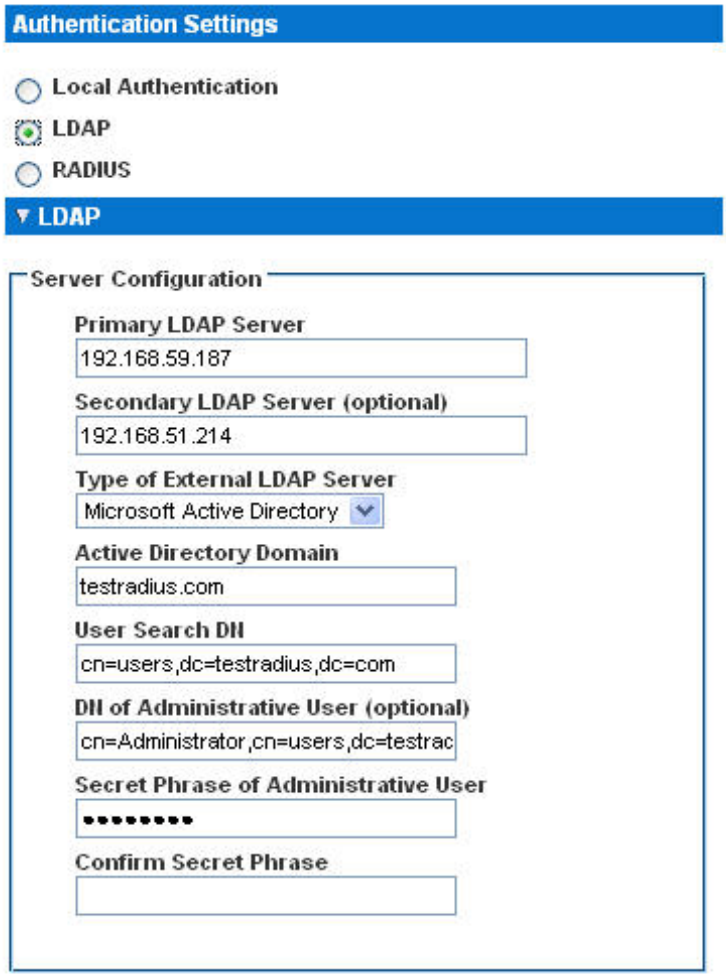
   Configuration du serveur

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

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

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

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



LDAP/LDAP Secure (LDAP/LDAP sécurisé)

12. Cochez la case Enable Secure LDAP (Activer le LDAP sécurisé) si vous souhaitez utiliser SSL. Ceci coche la case Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS). SSL (Secure Sockets Layer) est un protocole cryptographique qui permet à KX III 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.

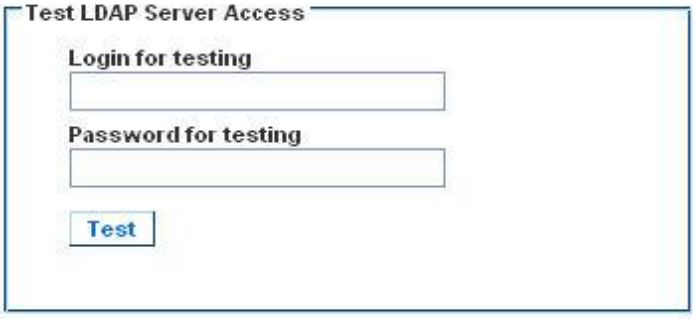
---

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 III pour que ce nouveau certificat prenne effet.

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

17. KX III 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 III 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 III et que le serveur LDAP utilisera pour vous authentifier. Cliquez sur Test.

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



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

KX III 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 III. 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 III 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 III 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 III :

1. A l'aide de KX III, 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 III aux groupes créés au cours de l'étape 2.
4. A partir de KX III, activez et configurez le serveur AD comme il se doit. Reportez-vous à ***Implémentation de l'authentification à distance LDAP/LDAPS*** (à la page 72).

Remarques importantes :

- Le nom de groupe est sensible à la casse.
- KX III 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 III, ce dernier attribue automatiquement le groupe <Unknown> (Inconnu) aux utilisateurs qui ont réussi à s'authentifier.
- Si vous utilisez un numéro de rappel, vous devez entrer la chaîne de caractère sensible aux majuscules suivante :*msRADIUSCallbackNumber*.
- D'après les recommandations de Microsoft, il vaut mieux utiliser les groupes globaux avec les comptes d'utilisateurs, non les groupes locaux de domaines.

Implémentation de l'authentification à distance RADIUS

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

Pour utiliser le protocole d'authentification RADIUS :

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

pour développer la section RADIUS de la page.

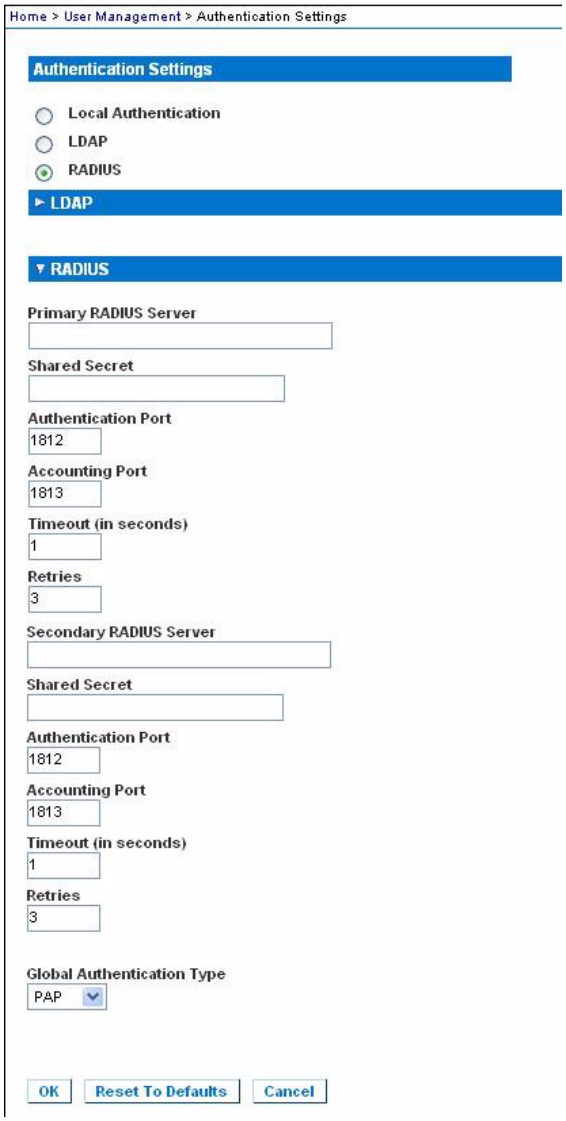
4. Dans les champs Primary Radius Server (Serveur Radius principal) et Secondary Radius Server (Serveur Radius secondaire), entrez l'adresse IP des serveurs d'authentification à distance principal et secondaire facultatif, respectivement (256 caractères au plus).
5. Dans les champs Shared Secret (Secret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

   Le secret partagé est constitué d'une chaîne de caractères devant être connus à la fois par KX III 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 III 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 III pour envoyer une requête d'authentification au serveur RADIUS.
10. Sélectionnez une option dans la liste déroulante Global Authentication Type (Type d'authentification globale) :
    - PAP - Avec le protocole PAP, les mots de passe sont envoyés en texte brut. Le protocole PAP n'est pas interactif. Le nom d'utilisateur et le mot de passe sont envoyés en un ensemble unique de données une fois la connexion établie, et non sous la forme d'une invite de connexion suivie de l'attente d'une réponse.

- CHAP - Avec le protocole CHAP, l'authentification peut être demandée par le serveur à tout moment. Le protocole CHAP est plus sûr que le protocole PAP.



Cisco ACS 5.x pour l'authentification RADIUS

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

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

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

Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS

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

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

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

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

Spécifications des échanges de communication RADIUS

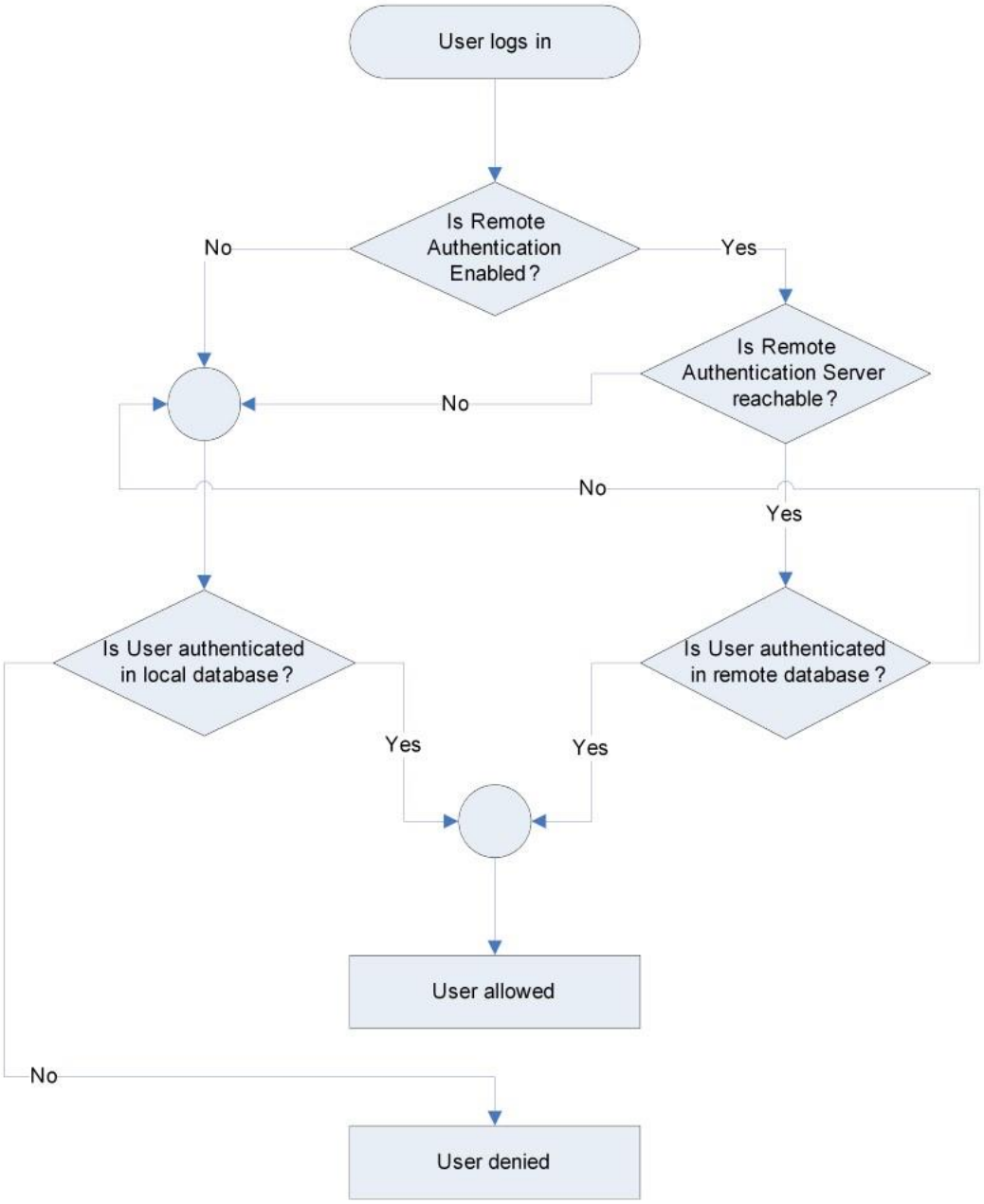
KX III envoie les attributs RADIUS suivants à votre serveur RADIUS :

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

Attribut	Données
Déconnexion	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Met fin à la gestion.
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0.
NAS-IP-Address (4)	Adresse IP de KX III.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Processus d'authentification de l'utilisateur

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

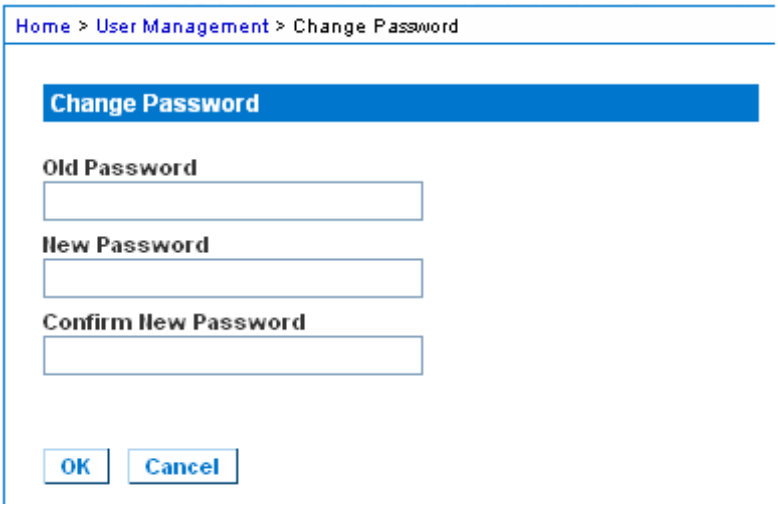


Modification d'un mot de passe

Pour changer votre mot de passe KX III:

1. Sélectionnez Gestion des utilisateurs > Changer de mot de passe. La page Modifier le mot de passe s'ouvre.
2. Entrez votre mot de passe actuel dans le champ 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 172) dans l'aide en ligne.*



Gestion des dispositifs

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 III.

Deux options permettent de paramétrer votre configuration IP :

- None (Néant) (valeur par défaut) : il s'agit de l'option recommandée (IP statique). Comme KX III 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 85).
3. Mettez à jour les paramètres relatifs à l'interface LAN. Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 89).
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 85).

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 III. 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 III 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 III.
   c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.
   d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).
   e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**
   f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

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

- None (Néant) - Utilisez cette option si vous ne souhaitez pas de configuration IP automatique et préférez définir l'adresse IP vous-même (IP statique). Cette option par défaut est recommandée.

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

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

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

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

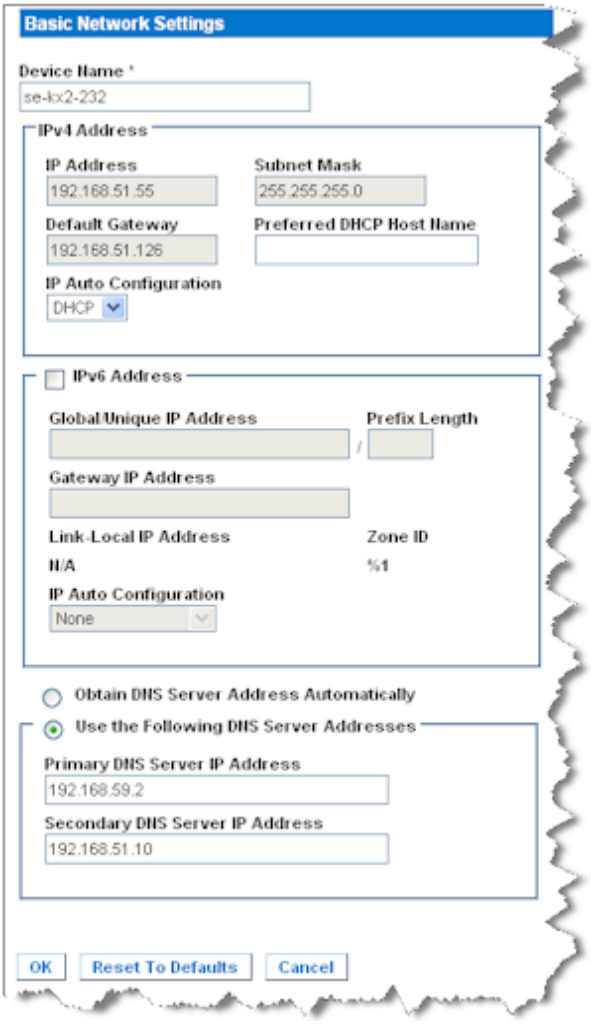
   a. Adresse IP du serveur DNS primaire

   b. Adresse IP du serveur DNS secondaire.

7. Lorsque vous avez terminé, cliquez sur OK.

Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 89) 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 III 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 85) pour plus d'informations.*



Paramètres de l'interface LAN

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

1. Sélectionnez Paramètres du dispositif > Réseau. La page Network Settings (Paramètres réseau) s'ouvre.
2. Choisissez la vitesse d'interface LAN et le Duplex parmi les options suivantes:
   - Autodetect (Détection automatique) (option par défaut)
   - 10 Mbps/Half - Les deux témoins clignotent.
   - 10 Mbps/Full - Les deux témoins clignotent.
   - 100 Mbps/Half - Le témoin jaune clignote.
   - 100 Mbps/Full - Le témoin jaune clignote.
   - 1000 Mbps/Full (gigabit) - Le témoin vert clignote.
   - Half-duplex permet la communication dans les deux directions, mais seulement une direction à la fois (non simultanément).
   - Full-duplex permet la communication dans les deux directions simultanément.

   Remarque : Des problèmes surviennent parfois lors de l'exécution à 10 Mbps en half duplex ou en full duplex. Dans ce cas, essayez un autre paramètre de vitesse et de duplex.

   Reportez-vous à ***Paramètres de vitesse réseau*** (à la page 341) pour plus d'informations.
3. Cochez la case Enable Automatic Failover (Activer le basculement automatique) pour permettre à KX III de récupérer automatiquement sa connexion réseau via un second port réseau en cas de panne du port réseau actif.

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

   Lorsque cette option est activée, les deux champs ci-après sont utilisés :
   - Ping Interval (seconds) - L'intervalle ping détermine la fréquence à laquelle KX III vérifie l'état du chemin réseau d'accès à la passerelle désignée. L'intervalle ping par défaut est de 30 secondes.
   - Timeout (seconds) - La temporisation détermine la durée pendant laquelle une passerelle désignée reste injoignable via la connexion réseau avant qu'un basculement ne se produise.

Remarque : l'intervalle ping et la temporisation peuvent être configurés pour répondre au mieux aux conditions du réseau local. La temporisation doit être définie pour permettre la transmission de deux demandes ping au moins et le retour des réponses. Par exemple, si une fréquence élevée de basculement est observée en raison d'une utilisation importante du réseau, la temporisation doit être prolongée pour atteindre trois ou quatre fois l'intervalle ping.

4. Sélectionnez la bande passante.
5. Cliquez sur OK pour appliquer les paramètres LAN.

Configuration des ports

Accès à la page de Configuration des ports

Pour accéder à la configuration d'un port :

1. Sélectionnez Paramètres du dispositif > Configuration du port. La page Port Configuration s'ouvre.

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

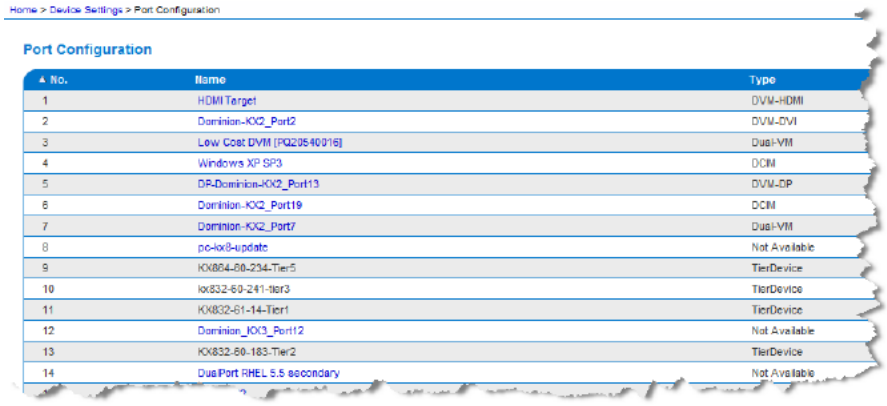
2. Cliquez sur le nom du port que vous souhaitez modifier.
   - Pour les ports KVM, la page Port des ports KVM et de châssis de lames est ouverte.
   - Pour les PDU de rack, la page Port pour les PDU de rack (barrettes d'alimentation) est ouverte. A partir de cette page, vous pouvez nommer les PDU de rack et leurs prises.

Page de configuration des ports

La page de Configuration des ports affiche la liste des ports de l'unité KX III.

Lorsque le statut d'un port est désactivé, Non disponible apparaît comme statut. Un port peut être désactivé lorsque son CIM a été retiré ou mis hors tension.

Remarque : Un châssis de lames peut être renommé, mais non ses connecteurs de lames.



Numéro de port

Numérotés de 1 au nombre total de ports disponibles pour le dispositif KX III.

Nom du port

Pour les ports sans CIM connectés ou pour lesquels le nom de CIM est vide, un par défaut est assigné, où Port# est le numéro du port physique de KX III.

Les ports actuellement connectés au KX III via un CIM ont un statut Non Disponible.

Pour renommer un port dont le statut est Not Available, effectuez une des opérations suivantes :

- Renommez le port. Lorsqu'un CIM est connecté, son nom est utilisé.
- Renommez le port et sélectionnez Persist name on Next CIM Insertion (Conserver le nom pour l'insertion de CIM suivante). Lorsqu'un CIM est connecté, le nom qui a été affecté sera copié dans le CIM.
- Réinitialisez le port, nom inclus, aux valeurs par défaut usine en sélectionnant Reset to Defaults. Lorsqu'un CIM est connecté, son nom est utilisé.

Remarque : N'utilisez pas d'apostrophe pour le nom de port (CIM).

Une fois le port renommé, utilisez la fonction Reset to Default (Restaurer les paramètres par défaut) à tout moment pour rétablir le nom du port par défaut.

Toutes les associations d'alimentation existantes sont alors supprimées et, si le port appartient à un groupe, il en est retiré.

Port Type (Type de port)

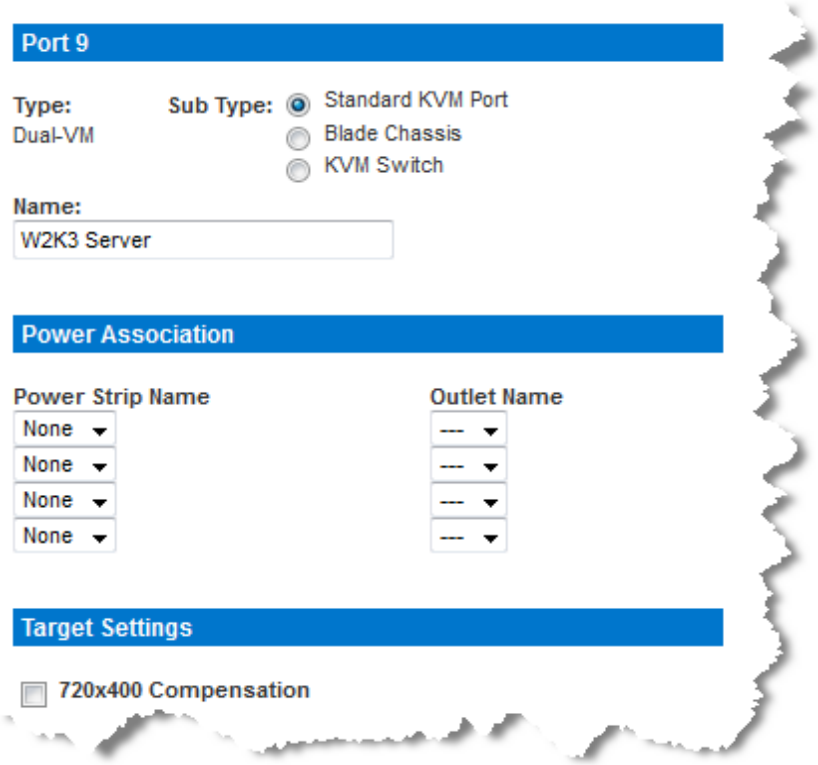
Les types de port incluent:

- DCIM - CIM Dominion
- TierDevice - Dispositif multiniveau
- Non disponible - Aucun CIM connecté
- DVM-DP - Port d'affichage
- DVM-HDMI - CIM HDMI
- DVM-DVI - CIM DVI
- PowerStrip (PDU de rack) - Barrette d'alimentation connectée
- VM - D2CIM - VUSB CIM
- Dual - VM - D2CIM-DVUSB CIM
- Blade Chassis - Châssis de lames et les lames qui lui sont associées (affichés dans un ordre hiérarchique).
- KVM Switch - Connexion de commutateur KVM générique
- PCIM - CIM Paragon

Configuration des serveurs cible standard

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à Etape 3 : Connexion de l'équipement pour obtenir une description de la connexion de l'équipement.
2. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
3. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
4. Sélectionnez Standard KVM Port comme sous-type du port.
5. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.
6. Cliquez sur OK.



Configuration des commutateurs KVM

KX III prend également en charge l'utilisation des séquences de raccourcis-clavier pour alterner entre les cibles. Outre l'utilisation de séquences de raccourcis-clavier avec les serveurs standard, la commutation KVM est prise en charge par les châssis de lames et dans les configurations multiniveaux.

Important : Pour permettre aux groupes d'utilisateurs de voir le commutateur KVM que vous créez, vous devez d'abord créer le commutateur, puis le groupe. Si un groupe d'utilisateurs existant doit voir le commutateur KVM que vous créez, vous devez créer à nouveau le groupe d'utilisateurs.

Pour configurer des commutateurs KVM :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Sélectionnez KVM Switch.
4. Sélectionnez le modèle de commutateur KVM (KVM Switch Model).

   Remarque : un commutateur seulement apparaîtra dans la liste déroulante.
5. Sélectionnez la séquence de raccourcis-clavier du commutateur KVM (KVM Switch Hot Key Sequence).
6. Entrez le nombre maximum de ports cible (2 à 32).
7. Dans le champ KVM Switch Name, entrez le nom à utiliser pour faire référence à cette connexion de port.
8. Activez les cibles auxquelles la séquence de raccourcis-clavier de commutateur KVM sera appliquée. Indiquez les ports de commutateur KVM auxquels des cibles sont reliées en sélectionnant Active pour chacun des ports.
9. Dans la section KVM Managed Links (Liens gérés de KVM) de la page, vous pouvez configurer la connexion à une interface de navigateur Web si elle est disponible.

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL Name - Entrez l'URL de l'interface.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

e. Username Field - Entrez le paramètre username qui sera utilisé dans l'URL. Par exemple *username*=admin, où *username* est le champ username.

f. Password Field - Entrez le paramètre password qui sera utilisé dans l'URL. Par exemple, *password*=raritan, où *password* est le champ password.

10. Cliquez sur OK.

Pour modifier le statut actif d'un port ou d'une URL de commutateur KVM :

1. Sélectionnez Device Settings > Port Configuration (Paramètres du dispositif > Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Désactivez la case à cocher Active en regard du port ou de l'URL cible de commutateur KVM pour modifier son statut actif.
4. Cliquez sur OK.

Configuration des ports CIM

Le KX III prend en charge l'utilisation de CIMs standards et numériques pour la connexion d'un serveur à KX III.

Pour configurer un CIM :

1. Sélectionnez Paramètres du dispositif > Configuration du port. La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
3. Sélectionnez Standard KVM Port comme sous-type du port.
4. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.

5. Dans la section Power Association (Association d'alimentation), associez une barre d'alimentation au port, le cas échéant.
6. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
7. Pour les CIM numériques, sélectionnez une résolution dans la liste déroulante Display Native Resolution (Résolution native d'affichage) pour que la résolution de la cible corresponde à celle du moniteur d'origine.

   Si vous utilisez un CIM HDMI, certaines combinaisons système d'exploitation/carte vidéo offrent une plage limitée de valeurs RVB. Améliorez les couleurs en cochant la case DVI Compatibility Mode (Mode de compatibilité DVI).
8. Cliquez sur OK.

Configuration des cibles de PDU de rack (barrette d'alimentation)

Le KX II vous permet de connecter des PDU de rack (barrettes d'alimentation) à des ports KX II.

La configuration des PDU de rack KX II est effectuée à partir de la page de Configuration des ports de KX II.

Remarque : Raritan recommande non moins de huits (8) PDU de rack (barrettes d'alimentation) connectés à KX III à la fois car les perfomances peuvent être affectées.

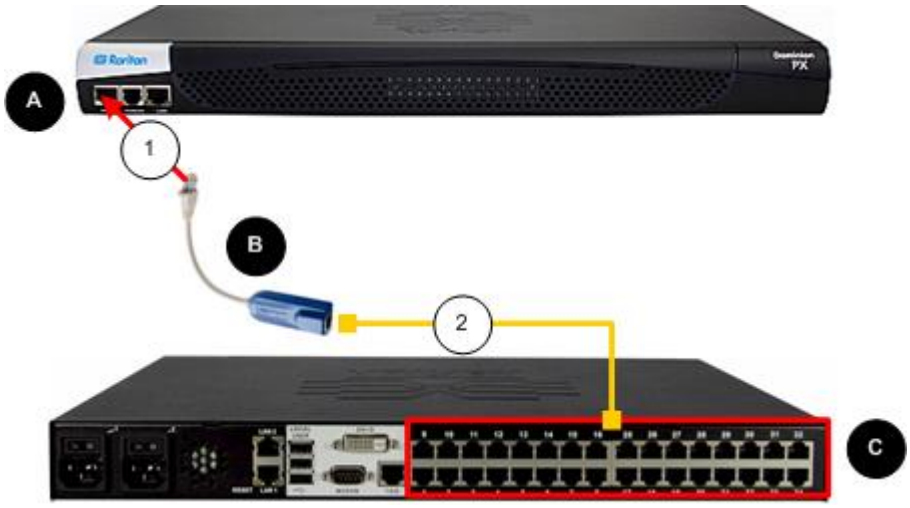
Connexion d'une PDU de rack

Les PDU (barrettes d'alimentation) de rack de la série PX de Raritan sont connectées au dispositif Dominion à l'aide du CIM D2CIM-PWR.

Pour connecter la PDU de rack :

1. Branchez la fiche RJ-45 mâle du D2CIM-PWR au connecteur RJ-45 femelle du port série de la PDU de rack.
2. Branchez le connecteur RJ-45 femelle du D2CIM-PWR à l'un des connecteurs de port système femelles disponible sur l'unité KX III à l'aide d'un câble Cat5 à brochage direct.
3. Branchez un cordon d'alimentation CA au serveur cible et à une prise de PDU de rack disponible.
4. Connectez la PDU de rack à une source d'alimentation CA.

5. Mettez le dispositif sous tension.



Légende	
A	PX rack PDU avec port série
B	D2CIM-PWR
C	KX III
1	Connexion D2CIM-PWR au rack port série PDU
2	D2CIM-PWR au serveur cible KX III via Câble Cat5

Appellation des PDU de rack (page Port pour les barrettes d'alimentation)

Remarque : Les PDU de rack PX (barrettes d'alimentation) peuvent être nommées dans le PX, ainsi que dans KX III.

Lorsque la PDU de rack à distance Raritan est connectée à KX III, elle apparaîtra dans la page Port Configuration. Cliquez sur le nom du port d'alimentation pour y accéder. Les champs Type et Name (Nom) sont déjà renseignés.

Remarque : Le champ Type (CIM) ne peut pas être modifié.

Les données suivantes sont affichées pour chaque prise de la PDU de rack : Numéro de [Outlet], nom et association de port.

Utilisez cette page pour nommer la PDU de rack et ses prises. Les noms peuvent comporter jusqu'à 32 caractères alphanumériques et spéciaux.

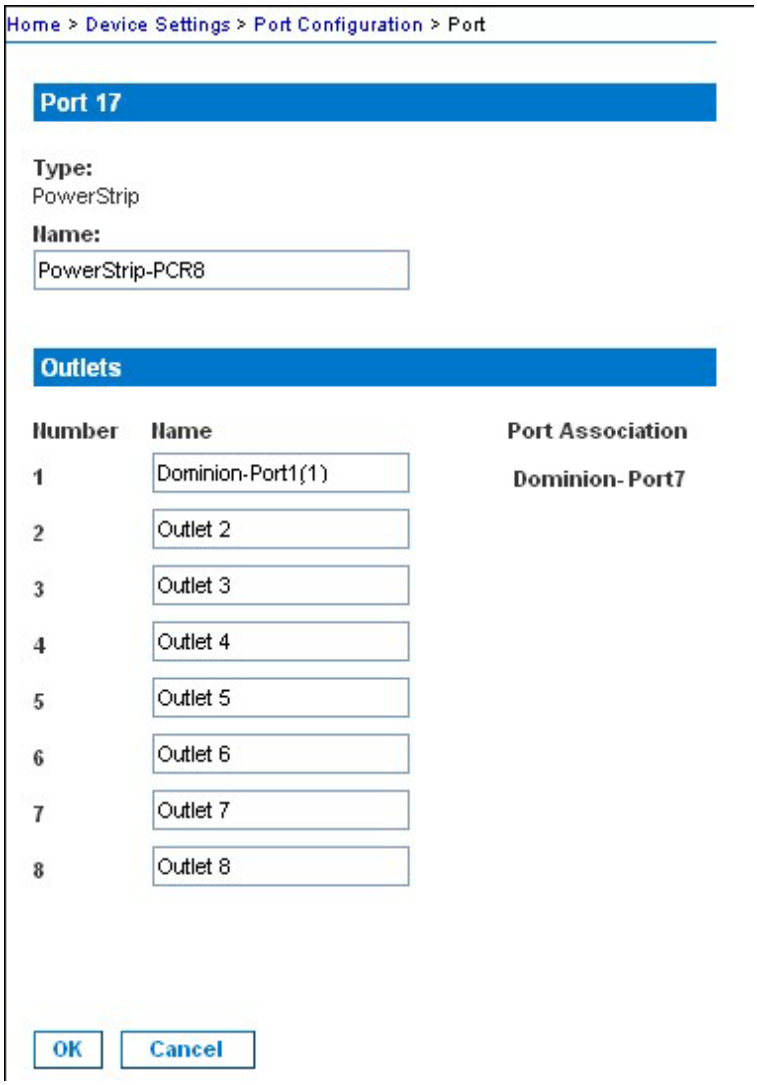
Remarque : Lorsqu'une PDU de rack est associée à un serveur cible (port), le nom de la prise est remplacé par celui du serveur cible même si vous avez donné un autre nom à la prise.

Pour nommer la PDU de rack et ses prises :

Remarque : CommandCenter Secure Gateway ne reconnaît pas les noms de PDU de rack contenant des espaces.

1. Entrez le nom de la PDU de rack (si nécessaire).
2. Modifiez le nom de [Outlet] si vous le souhaitez. (Le nom par défaut d'une prise est son numéro.)

3. Cliquez sur OK.



Association de prises à des serveurs cible

La page Port s'ouvre lorsque vous cliquez sur un port sur la page Port Configuration (Configuration des ports).

If une prise est connectée au même serveur que le port auquel elle est connectée, une association d'alimentation peut être faite avec le serveur cible.

Un serveur peut avoir jusqu'à quatre prises d'alimentation et vous pouvez associer une PDU de rack (barrette d'alimentation) différente à chacune d'elles. A partir cette page, définissez les associations de façon à effectuer la mise sous tension, hors tension et l'alimentation cyclique du serveur sur la page Port Access.

Pour utiliser cette fonction, vous avez besoin :

- PDU de rack à distance Raritan
- CIM d'alimentation (D2CIM-PWR).

Faire une association d'alimentation

Pour effectuer des associations d'alimentation (associer des prises de PDU de rack à des serveurs cible KVM) :

Remarque : Lorsqu'une PDU de rack est associée à un serveur cible (port), le nom de la prise est remplacé par celui du serveur cible (même si vous avez donné un autre nom à la prise).

1. Sur la page de configuration des ports, sélectionnez le serveur cible auquel vous associez la PDU.
2. Choisissez la PDU de rack dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
3. Pour cette PDU de rack, choisissez la prise dans la liste Outlet Name (Nom de prise).
4. Répétez les étapes 1 et 2 pour chaque association d'alimentation voulue.
5. Cliquez sur OK. Un message de confirmation s'affiche.

Supprimer une association d'alimentation

Lors de la déconnexion des serveurs cible et/ou des PDU de rack du dispositif, toutes les associations d'alimentation doivent être supprimées en premier lieu. Lorsqu'une cible est associée à une PDU de rack et que la première est supprimée du dispositif, l'association d'alimentation demeure. Lorsque cela se produit, vous ne pouvez pas accéder à la configuration des ports de ce serveur cible déconnecté dans Device Settings (Paramètres du dispositif) pour supprimer correctement l'association d'alimentation.

Pour supprimer une association de PDU de rack :

1. Sélectionnez la PDU de rack concernée dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
2. Pour cette PDU de rack, sélectionnez la prise souhaitée dans la liste Outlet Name (Nom de prise).
3. Sélectionnez None dans la liste déroulante Outlet Name.
4. Cliquez sur OK. L'association PDU de rack-prise est supprimée et un message de confirmation s'affiche.

Pour supprimer l'association d'une PDU de rack si cette dernière a été supprimée de la cible :

1. Cliquez sur Paramètres du dispositif > Configuration des ports, puis sur la cible active.
2. Associez la cible active au port d'alimentation déconnecté. Cette action rompt l'association d'alimentation de la cible déconnectée.
3. Associez ensuite la cible active au port d'alimentation correct.

Configuration des châssis de lames

Outre les serveurs standard et les PDU de rack (barrettes d'alimentation), vous pouvez gérer les châssis de lames branchés sur le port de dispositif KX III. Huit châssis de lames au plus peuvent être gérés à un moment donné.

S'il est pris en charge, le type du châssis de lames est détecté automatiquement à sa connexion.

Lorsqu'un châssis de serveurs lames est détecté, un nom par défaut lui est attribué et il s'affiche sur la page Port Access avec les serveurs cible standard et les PDU de rack.

Sinon, la lame doit être configurée manuellement. Le châssis de lames doit être configuré comme sous-type de châssis de lames.

Pour plus d'informations sur l'affichage des blades, consultez ***Affichage de la console distante*** (voir "***Page d'accès aux ports (Affichage de la console à distance)***" à la page 17).

Options de configuration du chassis blade

A l'exception des châssis de lames HP et UCS de Cisco®, les châssis de lames génériques, IBM® et Dell® sont configurés sur la page Port.

Le port connecté au châssis de lames doit être configuré avec le modèle du châssis.

Les informations spécifiques que vous pouvez configurer dépendent de sa marque du serveur lames que vous utilisez. Pour obtenir des informations particulières concernant chaque châssis de lame pris en charge, reportez-vous à la rubrique correspondante dans cette section de l'aide.

Dell

- Dell PowerEdge® 1855, 1955 et M1000e

  Les lames Dell PowerEdge 1855/1955 permettent également une connexion de chaque lame à un port du dispositif Dominion. Dans ce cas, les lames peuvent également être rassemblées pour créer des groupes de serveurs lames.

IBM

- IBM BladeCenter® Modèles E et H

Générique

- Une option générique vous permet de configurer un châssis blade qui ne soit pas un Dell PowerEdge® 1855, 1955 ou M1000e, ni un IBM BladeCenter® Modèles E et H, ni un HP BladeSystem c3000 et c7000, ou un serveur blade Cisco UCS.

HP

- Les serveurs lames HP BladeSystem c3000 et c7000, et Cisco UCS sont pris en charge via des connexions individuelles du dispositif Dominion à chaque lame.

  Les ports sont regroupés dans une représentation de châssis à l'aide de la fonction Port Group Management (Gestion des groupes de ports).

Configuration Manuelle et Auto-Découverte du châssis de lames

Deux modes d'opération sont possibles pour les châssis de lames: configuration manuelle et auto-découverte, selon les capacités du châssis de lames.

Lorsqu'un châssis de lames est configuré pour la détection automatique, le dispositif Dominion effectue un suivi et une mise à jour des actions suivantes :

- Lorsqu'un nouveau serveur lame est ajouté au châssis ;
- Lorsqu'un serveur lame existant est retiré du châssis.

Remarque : dans le cas des modèles E et H d'IBM Blade Center, KX III prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Raccourci-Clavier Sequences pour l'accès au châssis de lames.

L'utilisation des séquences de raccourcis-clavier pour commuter l'accès KVM sur un châssis de lames est également prise en charge.

Lorsqu'un châssis de lames permet aux utilisateurs de sélectionner une séquence de raccourcis-clavier, ces options seront fournies sur la page Port Configuration.

Lorsqu'un châssis de lames est fourni avec des séquences de raccourcis-clavier prédéfinies, ces séquences seront entrées sur la page Port Configuration lorsque le châssis sera sélectionné.

Par exemple, la séquence de raccourcis-clavier pour commuter l'accès KVM sur une unité IBM BladeCenter H est Verr num+ Verr num + Numéro de connecteur, cette séquence est donc appliquée par défaut lorsqu'une unité IBM BladeCenter H est sélectionnée pendant la configuration. Consultez la documentation de votre châssis de lames pour plus d'informations sur les séquences de raccourcis-clavier.

Lien à l'interface du châssis de lames.

Vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Au niveau du châssis, quatre liens au plus peuvent être définis.

Le premier est réservé à la connexion à l'interface utilisateur graphique du module d'administration du châssis de lames.

Par exemple, ce lien peut être utilisé par l'assistance technique pour vérifier rapidement la configuration d'un châssis.

Gérer les châssis de lames

Les châssis de lames peuvent être gérés à partir de Virtual KVM Client (VKC), d'Active KVM Client (AKC) et de CC-SG.

Gérer les serveurs de lames via VKC et MPC est identique à la gestion des serveurs cible standard.

Reportez-vous à l'aide de l'utilisateur et au **manuel de l'administrateur de CC-SG** pour en savoir plus.

Remarque : Les changements apportés à la configuration du châssis de lames seront reportés dans ces applications clientes.

Important : Lorsque le CIM reliant le châssis de lames au dispositif Dominion est mis hors tension ou déconnecté du dispositif, toutes les connexions au châssis de lames établies seront abandonnées. Lorsque le CIM est reconnecté ou mis sous tension, vous devrez établir à nouveau les connexions.

Configuration des châssis de lames génériques

La sélection de Generic Blade Chassis (Châssis de lames génériques) ne permet qu'une configuration manuelle. Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 119), ***CIM pris en charge pour les châssis de lames*** (à la page 120) et ***Configurations requises et recommandées de châssis de lames*** (à la page 123) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 342) pour plus d'informations à ce sujet lors de l'utilisation des châssis Dell® avec KX III.

Pour configurer un châssis :

1. Connectez le châssis de lames à KX III. Reportez-vous à Etape 3 : Connexion de l'équipement pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez Generic dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).
6. Configurez le châssis de lames, le cas échéant.

a. Switch Hot Key Sequence - Définissez la séquence de raccourcis-clavier qui permettra de commuter de KVM au châssis de lames. La séquence de raccourcis-clavier de commutation doit correspondre à celle utilisée par le module KVM dans le châssis de lames.

b. Administrative Module Primary IP Address/Host Name - Sans objet.

c. Maximum Number of Slots - Entrez le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames.

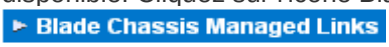
d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.

e. Username - Sans objet.

f. Password - Sans objet.

7. Modifiez le nom du châssis de lames, le cas échéant.

8. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

9. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   ---

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

   b. URL - Entrez l'URL de l'interface. **Obligatoire**

   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface. **Facultatif**

   d. Password - Entrez le mot de passe utilisé à accéder à l'interface. **Facultatif**

Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 115) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web. **Facultatif**

10. Les informations de profil USB ne s'appliquent pas à une configuration générique.
11. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
12. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.

Sélectionnez la résolution d'affichage native des CIM dans la liste déroulante Display Native Resolution. Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM.

1. Si aucune sélection n'est effectuée, la résolution par défaut de 1280x1024@60Hz est utilisée.
2. Cliquez sur OK pour enregistrer la configuration.

Configuration des châssis de lames Dell

Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 119), ***CIM pris en charge pour les châssis de lames*** (à la page 120) et ***Configurations requises et recommandées de châssis de lames*** (à la page 123) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 342) pour plus d'informations à ce sujet lors de l'utilisation des châssis Dell® avec KX III.

Pour ajouter un châssis de lame :

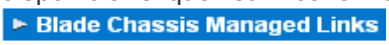
1. Connectez le châssis de lames à KX III. Reportez-vous à Etape 3 : Connexion de l'équipement pour plus d'informations.

2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez le modèle de châssis de lames Dell dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).

Pour configurer un Dell PowerEdge M1000e :

1. Si vous avez sélectionné Dell PowerEdge™ M1000e, la détection automatique est disponible. Configurez le châssis de lames, le cas échéant. Avant de configurer un châssis de lames pouvant être détecté automatiquement, celui-ci doit accepter les connexions SSH sur le numéro de port désigné (reportez-vous à Services du dispositif). De plus, il faut créer au préalable un compte d'utilisateur disposant d'informations d'authentification sur le châssis de lames.
   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames. La séquence de raccourcis-clavier de commutation doit correspondre à celle utilisée par le module KVM dans le châssis de lames.
   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.
   c. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. **Obligatoire pour le mode de détection automatique**
   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Changez ce numéro, le cas échéant. **Obligatoire pour le mode de détection automatique**
   e. Username - Entrez le nom d'utilisateur servant à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**
   f. Password - Entrez le mot de passe utilisé à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**
2. Si vous souhaitez que KX III détecte automatiquement les lames du châssis, cochez la case Blade Auto-Discovery (Détection automatique des lames), puis cliquez sur Discover Blades on Chassis Now (Détecter les lames sur le châssis maintenant). Lorsque les lames sont détectées, elles s'affichent sur la page.

3. Modifiez le nom du châssis de lames, le cas échéant. Si le châssis porte déjà un nom, ce champ est automatiquement renseigné. Sinon, KX III attribue un nom au châssis. La convention d'appellation par défaut pour les châssis de lames par KX III est Blade_Chassis_Port#.
4. En mode manuel, indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

   En mode de détection automatique, la case Installed affiche les connecteurs contenant des lames pendant la détection.
5. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.
   b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 125) pour obtenir des exemples de configuration pour le Dell M1000e.
   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.
   d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

   Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 115) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

6. Les profils USB ne s'appliquent pas aux châssis Dell.
7. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
8. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.

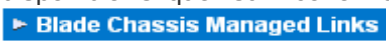
Sélectionnez la résolution d'affichage native des CIM dans la liste déroulante Display Native Resolution. Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM.

1. Si aucune sélection n'est effectuée, la résolution par défaut de 1280x1024@60Hz est utilisée.
2. Cliquez sur OK pour enregistrer la configuration.

Pour configurer un Dell PowerEdge 1855/1955 :

1. Si vous avez sélectionné Dell 1855/1955, la détection automatique *n'est pas disponible*. Configurez le châssis de lames, le cas échéant.
   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames. Pour les modèles Dell 1855/1955, KX III bloque toutes les séquences de raccourci-clavier existantes. Si vous appliquez une configuration générique au Dell 1855, seul un raccourci-clavier existant est bloqué.
   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.
   c. Administrative Module Primary IP Address/Host Name - Sans objet.
   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.
   e. Username - Sans objet.

f. Password - Sans objet.

2. Modifiez le nom du châssis de lames, le cas échéant.
3. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.
4. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

   b. URL - Entrez l'URL de l'interface. Reportez-vous à Exemples de formats d'URL de châssis de lames pour obtenir des exemples de configuration pour le Dell PowerEdge 1855/1955.

   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

   d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

   Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 115) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

5. Les profils USB ne s'appliquent pas aux châssis Dell.
6. Cliquez sur OK pour enregistrer la configuration.

Configuration des châssis de lames génériques IBM

Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 119), ***CIM pris en charge pour les châssis de lames*** (à la page 120) et ***Configurations requises et recommandées de châssis de lames*** (à la page 123) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 342) pour plus d'informations à ce sujet lors de l'utilisation des châssis Dell® avec KX III.

Pour ajouter un châssis de lame :

1. Connectez le châssis de lames à KX III. Reportez-vous à Etape 3 : Connexion de l'équipement pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez le modèle de châssis de lames IBM® dans la liste déroulante de Modèle de châssis de serveurs lames.

Pour configurer un IBM BladeCenter H et E :

1. Si vous avez sélectionné IBM BladeCenter H ou E, la détection automatique est disponible. Configurez le châssis de lames, le cas échéant. Avant de configurer un châssis de lames pouvant être détecté automatiquement, celui-ci doit accepter les connexions SSH sur le numéro de port désigné (reportez-vous à Services du dispositif). De plus, il faut créer au préalable un compte d'utilisateur disposant d'informations d'authentification sur le châssis de lames. KX III ne prend en charge la détection automatique que pour AMM[1].

a. Switch Hot Key Sequence - Prédéfinie.

b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.

c. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. **Obligatoire pour le mode de détection automatique**

d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Changez ce numéro, le cas échéant. **Obligatoire pour le mode de détection automatique**

e. Username - Entrez le nom d'utilisateur servant à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

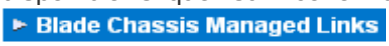
f. Password - Entrez le mot de passe utilisé à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

2. Si vous souhaitez que KX III détecte automatiquement les lames du châssis, cochez la case Blade Auto-Discovery (Détection automatique des lames), puis cliquez sur Discover Blades on Chassis Now (Détecter les lames sur le châssis maintenant). Lorsque les lames sont détectées, elles s'affichent sur la page.

3. Modifiez le nom du châssis de lames, le cas échéant. Si le châssis porte déjà un nom, ce champ est automatiquement renseigné. Sinon, KX III attribue un nom au châssis. La convention d'appellation par défaut pour les châssis de lames par KX III est Blade_Chassis_Port#.

4. En mode manuel, indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

   En mode de détection automatique, la case Installed affiche les connecteurs contenant des lames pendant la détection.

5. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 125) pour obtenir des exemples de configuration pour l'IBM BladeCenter.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 115) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

6. Le cas échéant, définissez le profil USB pour le châssis de lames ou sélectionnez un profil USB existant. Cliquez sur l'icône USB Profiles for Port (Profils USB pour le port)

ou sur l'icône Apply Select Profiles to Other Ports (Appliquer les profils sélectionnés aux autres ports)

pour développer ces sections de la page. Reportez-vous à ***Configuration des profils USB (page Port)*** (à la page 127).

7. Cliquez sur OK pour enregistrer la configuration.

Pour configurer un IBM BladeCenter (autre) :

1. Si vous avez sélectionné IBM BladeCenter (Other), la détection automatique *n'est pas* disponible. Configurez le châssis de lames, le cas échéant.

a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames.

b. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. Sans objet.

c. Maximum Number of Slots - Entrez le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames.

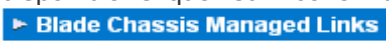
d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.

e. Username - Sans objet.

f. Password - Sans objet.

2. Modifiez le nom du châssis de lames, le cas échéant.

3. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames. S'ils ne sont pas nommés, KX III leur attribue un nom. La convention d'appellation par défaut des serveurs lames est Blade_Chassis_Port#_Slot#.

4. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links 

pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   ---

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

   b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 125) pour obtenir des exemples de configuration pour l'IBM BladeCenter.

   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

Remarque : laissez les champs Username et Password vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 115) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

5. Les profils USB ne sont pas utilisés par les configurations IBM (Other).
6. Dans la section Target Settings (Paramètres de la cible), sélectionnez la compensation 720 x 400 si l'affichage connaît des difficultés lorsque la cible utilise cette résolution.
7. Sélectionnez Use international keyboard for scan code set 3 (Utiliser le clavier international pour le jeu de codes de balayage 3) si la connexion à la cible s'effectue via un DCIM-PS2 et exige l'utilisation du jeu de codes de balayage 3 avec un clavier international.

Sélectionnez la résolution d'affichage native des CIM dans la liste déroulante Display Native Resolution. Il s'agit du mode de résolution et de synchronisation privilégié du CIM numérique. Lorsque la résolution est sélectionnée, elle est appliquée au CIM.

1. Si aucune sélection n'est effectuée, la résolution par défaut de 1280x1024@60Hz est utilisée.
2. Cliquez sur OK pour enregistrer la configuration.

Astuces pour ajouter une interface Navigateur Web

Vous pouvez ajouter une interface navigateur Web pour créer une connexion à un dispositif intégrant un serveur Web. Une interface navigateur Web permet également la connexion à une application Web quelconque, telle que celle associée à une carte de processeur RSA, DRAC ou ILO.

DNS doit être configuré pour résoudre les URL. Les adresses IP ne requièrent pas la configuration de DNS.

Pour ajouter une interface navigateur Web :

1. Le nom par défaut d'une interface navigateur Web est fourni. Les cas échéant, vous pouvez modifier le nom dans le champ Name.

2. Entrez l'URL ou le nom du domaine de l'application Web dans le champ URL. Vous devez entrer l'URL à laquelle l'application Web doit lire le nom d'utilisateur et le mot de passe.

   Suivez les exemples ci-après pour entrer des formats corrects :

   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html

3. Entrez les nom d'utilisateur et mot de passe autorisant l'accès à cette interface. **Facultatif**
4. Si un nom d'utilisateur et un mot de passe ont été entrés, dans Username Field et Password Field, tapez le nom des champs de nom d'utilisateur et de mot de passe utilisés dans l'écran de connexion de l'application Web. Vous devez visualiser la source HTML de l'écran de connexion pour trouver le nom des champs, et non leur libellé.

Astuce pour repérer le nom des champs :

- Dans le code source HTML de la page de connexion de l'application Web, recherchez le libellé du champ, tel que Username et Password.
- Examinez ensuite le code adjacent pour trouver une balise ressemblant à : name="user". Le mot entre guillemets est le nom du champ.

Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports).

KX III prend en charge l'agrégation des ports connectés à certains types de lames dans un groupe représentant le châssis de lames ; Particulièrement, les lames HP® BladeServer et Dell® PowerEdge 1855/1955 lorsque le DellPowerEdge 1855/1955 est connecté de chaque lame au port sur KX III.

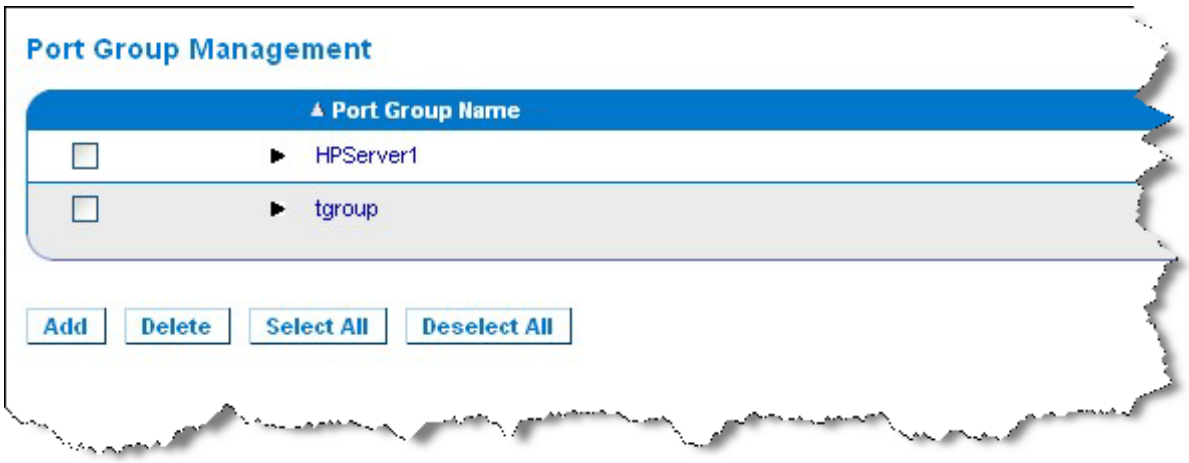
Le châssis est identifié par un nom de groupe de ports et ce groupe est désigné comme Blade Server Group (Groupe de serveurs lames) sur la page Port Group Management (Gestion des groupes de ports). Les groupes de ports comprennent uniquement des ports configurés comme ports KVM standard, non des ports configurés comme châssis de lames. Un port ne peut être membre que d'un seul groupe.

Les ports connectés aux modules KVM intégrés dans un châssis de lames sont configurés comme sous-types de châssis de lames. Ces ports peuvent être inclus dans des groupes de ports.

Lorsque les ports de KX III sont connectés à des modules KVM intégrés dans un châssis de lames et à des lames individuelles, ils sont configurés comme sous-types de châssis de lames. Ces ports ne peuvent pas être inclus dans des groupes de ports et n'apparaissent pas dans la liste Available (Disponibles) de la section Select Ports for Group (Sélectionner des ports pour le groupe).

Lorsqu'un port KVM standard a été inclus dans un groupe de ports, puis réorienté pour être utilisé comme sous-type de châssis de lames, il doit d'abord être supprimé du groupe de ports.

Les groupes de ports sont restaurés à l'aide de l'option Backup and Restore (Sauvegarde et restauration) (reportez-vous à ***Backup and Restore*** (voir "***Backup and Restore (Sauvegarde et restauration)***" à la page 192) (Sauvegarde et restauration)).



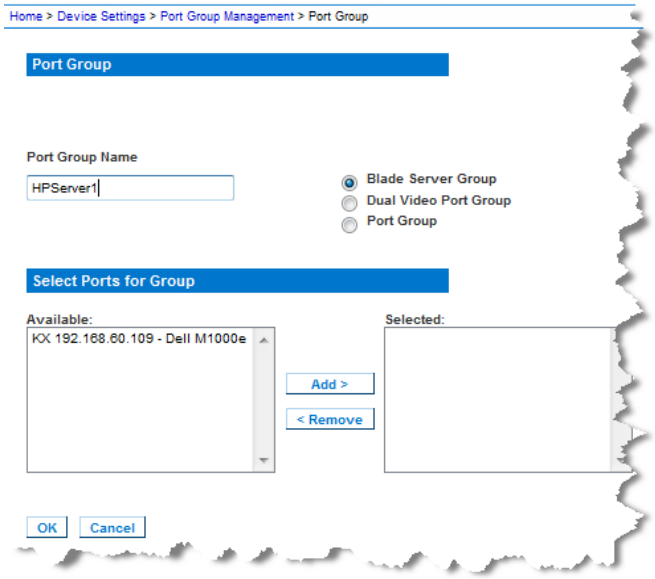
Pour ajouter un groupe de ports :

1. Cliquez sur Paramètres du dispositif > Gestion des groupes de ports pour ouvrir la page de Gestion des groupes de ports.
2. Cliquez sur Add (Ajouter) pour ouvrir la page Port Group (Groupe de ports).
3. Entrez un nom de groupe de ports. Les noms de groupes de ports ne sont pas sensibles à la casse et peuvent contenir jusqu'à 32 caractères.
4. Cochez la case Blade Server Group (Groupe de serveurs lames).

   Si vous souhaitez indiquer que ces ports sont reliés à des lames hébergées dans un châssis de lames (par exemple, HP c3000 ou Dell PowerEdge 1855), sélectionnez la case à cocher Blade Server Group.

   Remarque : Ceci est particulièrement important pour les utilisateurs de CC-SG qui souhaitent organiser les lames HP par châssis, même si chaque lame a sa propre connexion à un port de KX III.

5. Cliquez sur un port dans le champ Available (Disponibles) de la section Select Ports for Group (Sélectionner des ports pour le groupe). Cliquez sur Add pour ajouter le port au groupe. Le port est placé dans le champ Selected (Sélectionnés).
6. Cliquez sur OK pour ajouter le groupe de ports.



Pour modifier les informations relatives à un groupe de ports :

1. Sur la page Port Group Management (Gestion des groupes de ports), cliquez sur le lien du groupe de ports que vous souhaitez modifier. La page Port Group (Groupe de ports) s'ouvre.
2. Modifiez les informations selon les besoins.
3. Cliquez sur OK pour enregistrer les modifications.

Pour supprimer un groupe de ports :

1. Cliquez sur la page Port Group Management (Gestion des groupes de ports), cochez la case du groupe de ports que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).
3. Cliquez sur OK dans le message d'avertissement.

Modèles de châssis de lames pris en charge

Ce tableau présente les modèles de châssis de lames pris en charge par KX III et les profils correspondant qui devraient être sélectionnés selon le modèle de châssis lors de leur configuration dans l'application KX III. Une liste de ces modèles peut être sélectionnée sur la page Port Configuration (Configuration des ports) dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames), qui apparaît lorsque le bouton radio Blade Chassis est sélectionné. Pour obtenir des informations concernant la configuration de chaque châssis de lames, reportez-vous à la rubrique correspondante dans cette section de l'aide.

Modèle de châssis de lames	Profil de KX III
UCS Cisco®	Configurez à l'aide des fonctions de gestion des groupes de ports. Consultez ***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)*** (voir "***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports).***" à la page 117).
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
BladeCenter® IBM® S	IBM (autre)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (autre)
IBM BladeCenter HT	IBM (autre)

Modèle de châssis de lames	Profil de KX III
IBM BladeCenter E	IBM BladeCenter E
HP®	Configurez à l'aide des fonctions de gestion des groupes de ports. Consultez ***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports)*** (voir "***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports).***" à la page 117).

CIM pris en charge pour les châssis de lames

Les CIM suivants sont pris en charge pour les châssis de lames gérés via KX III:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Le tableau suivant contient les CIM pris en charge pour chaque modèle de châssis de lames supporté par KX III.

Châssis de lames	Méthode de connexion	CIM recommandés
Générique	Si un D2CIM-VUSB ou D2CIM-DVUSB est utilisé lors de la connexion à un châssis de lames configuré en tant que Générique, vous pouvez sélectionner les profils USB sur la page Port Configuration (Configuration des ports) et le menu USB Profile du client. Toutefois, la fonction Support virtuel n'est pas prise en charge pour les châssis de lames génériques et le menu Virtual Media est désactivé sur le client.	• DCIM-PS2 • DCIM-USBG2
Cisco® UCS Server Chassis	Le câble Cisco KVM (N20-BKVM) vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide d'installation de Cisco UCS 5108 Server Chassis*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB

Châssis de lames	Méthode de connexion	CIM recommandés
Dell® PowerEdge™ 1855	Inclut un des trois modules KVM : • Module de commutateur Ethernet KVM analogique (standard) • Module de commutateur KVM à accès numérique (facultatif) • Module de commutateur KVM (standard sur les systèmes antérieurs à avril 2005) Ces commutateurs présentent un connecteur personnalisé autorisant la connexion de deux dispositifs PS/2 et d'un dispositif vidéo au système. Source : *Manuel d'utilisation de Dell PowerEdge 1855*	• DCIM-PS2
Dell PowerEdge 1955	Un des deux types de modules KVM peut être installé : • Module de commutateur KVM analogique • Module de commutateur KVM à accès numérique Ces deux modules autorisent la connexion d'un clavier, d'une souris et d'un écran PS/2 compatibles au système (à l'aide d'un câble personnalisé fourni avec le système). Source : *Manuel d'utilisation de Dell PowerEdge 1955*	• DCIM-PS2
Dell PowerEdge M1000e	Le module commutateur KVM (iKVM) est intégré à ce châssis. L'iKVM est compatible avec les périphériques suivants : • claviers USB, dispositifs de pointage USB • écrans VGA avec prise en charge DDC Source : *Guide d'utilisation du contrôleur de gestion de châssis Dell, version de firmware 1.0*	• DCIM-USBG2
HP® BladeSystem c3000	Le câble HP c-Class Blade SUV vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des châssis de lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide de maintenance et de service du serveur lame HP ProLiant™ BL480c*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (pour un fonctionnement de port KVM standard sans option KVM)

Châssis de lames	Méthode de connexion	CIM recommandés
HP BladeSystem c7000	Le câble HP c-Class Blade SUV vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide de maintenance et de service du serveur lame HP ProLiant BL480c*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (pour un fonctionnement de port KVM standard)
IBM® BladeCenter® S	Le module AMM (de gestion avancée) offre des fonctions de gestion du système et de multiplexage de clavier/vidéo/souris (KVM) pour tous les châssis de lames. Les connexions AMM incluent : un port série, une connexion vidéo, un port de gestion à distance (Ethernet) et deux ports USB v2.0 pour un clavier et une souris. Source : *Mise en œuvre du châssis IBM BladeCenter S*	• DCIM-USBG2
IBM BladeCenter H	Le châssis BladeCenter H est livré en standard avec un module AMM. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	Le modèle de châssis actuel BladeCenter E (8677-3Rx) est livré en standard avec un module AMM. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	Le châssis BladeCenter T est livré en standard avec un module AMM. Contrairement au châssis BladeCenter standard, le module KVM et le module de gestion du châssis BladeCenter T sont des composants distincts. L'avant du module de gestion ne comporte des voyants que pour l'affichage de l'état. Toutes les connexions Ethernet et KVM sont alimentées par l'arrière aux modules LAN et KVM. Le module KVM est un module à remplacement à chaud à l'arrière du châssis, fournissant deux connecteurs PS/2 pour un clavier et une souris, un panneau d'état du système et un connecteur vidéo HD-15. Source : *Produits et technologie IBM*	• DCIM-PS2

Châssis de lames	Méthode de connexion	CIM recommandés
	BladeCenter	
IBM BladeCenter HT	Le châssis BladeCenter HT est livré en standard avec un module AMM. Ce module permet de gérer le châssis et offre la fonction KVM locale. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2

Remarque : pour prendre en charge la détection automatique, les modèles H et E d'IBM BladeCenter doivent utiliser AMM avec la version de firmware BPET36K ou supérieure.

Remarque : dans le cas des modèles E et H d'IBM Blade Center, KX III prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Remarque : L'audio est désactivé pour toutes les cibles de commutateur KVM.

Configurations requises et recommandées de châssis de lames

Ce tableau contient des informations sur les limitations et les contraintes qui s'appliquent à la configuration des châssis blade pour qu'ils fonctionnent avec le dispositif KX III. Raritan vous recommande de suivre toutes les informations suivantes.

Châssis de lames	Action requise/recommandée
Dell® PowerEdge™ M1000e	▪ Désactivez l'écran de veille de l'interface utilisateur d'iKVM. Sinon, une boîte de dialogue d'autorisation s'affiche et empêche le fonctionnement correct d'iKVM. ▪ Quittez le menu de l'interface utilisateur d'iKVM avant de connecter le châssis Dell à un CIM Raritan. iKVM ne fonctionnera pas correctement si cela n'est pas fait. ▪ Configurez le menu principal de l'interface utilisateur d'iKVM pour sélectionner les lames cible par connecteur, et non par nom. iKVM ne fonctionnera pas correctement si cela n'est pas fait. ▪ *Ne désignez aucun* connecteur pour les opérations d'analyse dans le menu Setup Sans (Paramétrage de l'analyse) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. ▪ *Ne désignez aucun* connecteur pour les opérations de clavier/souris de diffusion dans le menu Setup Broadcast

Châssis de lames	Action requise/recommandée
	(Paramétrage de la diffusion) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. ▪ Désignez une seule séquence de touches pour appeler l'interface utilisateur d'iKVM. Ce séquence doit être identifié pendant la configuration des ports KX III. Sinon, iKVM risque de fonctionner de manière erratique après une saisie sur le client. ▪ Assurez-vous que l'option Front Panel USB/Video Enabled (USB/Vidéo du panneau avant activés) ne soit *pas* sélectionnée au cours de la configuration d'iKVM via l'interface utilisateur de Dell CMC. Sinon, les connexions effectuées sur le devant du châssis l'emporteront sur la connexion arrière du KX III, empêchant le fonctionnement correct de l'iKVM. Un message s'affichera indiquant User has been disabled as front panel is currently active. (L'utilisateur a été désactivé car le panneau avant est actif.). ▪ Assurez-vous que l'option Allow access to CMC CLI from iKVM (Autoriser l'accès à la CLI CMC depuis iKVM) *n'est pas* sélectionnée au cours de la configuration d'iKVM via l'interface utilisateur de Dell CMC. ▪ Pour empêcher l'affichage de l'interface utilisateur iKVM lors de la connexion au châssis de lames, définissez l'option Screen Delay Time (Délai d'écran) sur 8 secondes. ▪ La sélection de Timed (Différé) et Displayed (Affiché) est recommandé au cours du paramétrage de l'indicateur (Flag Setup) dans l'interface utilisateur d'iKVM. Vous pouvez ainsi confirmer visuellement la connexion au connecteur de lame souhaité.
Dell PowerEdge 1855/1955	▪ Désactivez l'écran de veille de l'interface utilisateur d'iKVM. Sinon, une boîte de dialogue d'autorisation s'affiche et empêche le fonctionnement correct d'iKVM. ▪ Quittez le menu de l'interface utilisateur d'iKVM avant de connecter le châssis Dell à un CIM Raritan. iKVM ne fonctionnera pas correctement si cela n'est pas fait. ▪ Configurez le menu principal de l'interface utilisateur d'iKVM pour sélectionner les lames cible par connecteur, et non par nom. iKVM ne fonctionnera pas correctement si cela n'est pas fait. ▪ *Ne désignez aucun* connecteur pour les opérations d'analyse dans le menu Setup Scan (Paramétrage de l'analyse) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. ▪ Pour empêcher l'affichage de l'interface utilisateur iKVM lors de la connexion au châssis de lames, définissez l'option Screen Delay Time (Délai d'écran) sur 8 secondes.

Châssis de lames	Action requise/recommandée
	▪ La sélection de Timed (Différé) et Displayed (Affiché) est recommandé au cours du paramétrage de l'indicateur (Flag Setup) dans l'interface utilisateur d'iKVM. Vous pouvez ainsi confirmer visuellement la connexion au connecteur de lame souhaité.
Détection automatique IBM®/Dell®	▪ Il est recommandé d'activer l'option Auto-Discovery (Détection automatique) lors de l'application des autorisations d'accès au niveau des lames. Sinon, définissez des autorisations d'accès au niveau du châssis de lames. ▪ Secure Shell (SSH) doit être activé sur le module de gestion des châssis de lames. ▪ Le port SSH configuré dans le module de gestion des châssis de lames doit correspondre au numéro de port saisi sur la page Port Configuration (Configuration des ports).
Media Virtuel KX3 IBM	▪ Le media virtuel KX III Raritan est seulement supporté par les modèles H et E dans le BladeCenter® IBM. Cela requiert l'utilisation de D2CIM-DVUSB. Le connecteur USB à faible vitesse D2CIM-DVUSB noir est relié au module AMM (Administrative Management Module) à l'arrière de l'unité. Le connecteur USB à haute vitesse D2CIM-DVUSB gris est relié au tiroir de support (MT) à l'avant de l'unité. Un câble d'extension USB est nécessaire.
Châssis de serveur UCS Cisco®	▪ Le câble Cisco KVM (N20-BKVM) vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. ▪ Source : *Guide d'installation de Châssis de Serveur Cisco UCS 5108-DCIM-USBG2, D2CIM-VUSB, D2CIM-DVUSB*

Remarque : Tous les BladeCenters IBM utilisant AMM doivent utiliser la version de firmware AMM BPET36K ou supérieure pour fonctionner avec KX III.

Remarque : dans le cas des modèles E et H d'IBM Blade Center, KX III prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Exemples de formats d'URL de châssis de lames

Ce tableau contient des exemples de formats d'URL de châssis de lames configurés dans KX III.

Châssis de lames	Exemple de format d'URL
Dell® M1000e	• URL : https://192.168.60.44/cgi-bin/webcgi/login • Username (Nom d'utilisateur) : root

Châssis de lames	Exemple de format d'URL
	• Username Field (Champ du nom d'utilisateur) : user • Password: calvin • Password Field (Champ du mot de passe) : password
Dell 1855	• URL : https://192.168.60.33/Forms/f_login • Username (Nom d'utilisateur) : root • Username Field (Champ du nom d'utilisateur) : TEXT_USER_NAME • Password: calvin • Password Field (Champ du mot de passe) : TEXT_PASSWORD
IBM® BladeCenter® E ou H	• http://192.168.84.217/private/welcome.ssi

Configuration des profils USB (page Port)

La sélection des profils USB disponibles pour un port s'effectue dans la section Select USB Profiles for Port de la page Port. Les profils USB choisis dans la page Port deviennent les profils disponibles à l'utilisateur dans VKC lors de la connexion à un serveur cible KVM depuis le port. Il s'agit par défaut du profil des systèmes d'exploitation Windows 2000®, Windows XP®, Windows Vista®. Pour plus d'informations sur les profils USB, reportez-vous à Profils USB.

Remarque : Pour définir les profils USB d'un port, un CIM numérique, VM-CIM ou Dual VM-CIM doit être connecté et équipé d'un firmware compatible avec la version de firmware courante de KX III. Reportez-vous à **Mise à niveau des CIM** *(à la page 196).*

Les profils disponibles à affecter à un port apparaissent dans la liste Available (Disponibles) à gauche. Les profils sélectionnés pour une utilisation avec un port apparaissent dans la liste Selected à droite. Lorsque vous sélectionnez un profil dans une des listes, sa description et son utilisation apparaissent dans le champ Profile Description (Description du profil).

Outre la sélection d'un ensemble de profils à mettre à la disposition d'un port KVM, vous pouvez également spécifier le profil privilégié pour le port et appliquer les paramètres définis pour un port à d'autres ports KVM.

Remarque : Reportez-vous à **Modes de souris lors de l'utilisation du Menu de démarrage Mac** *(à la page 56) pour plus d'informations sur l'utilisation du profil USB Mac OS-X® avec DCIM-VUSB ou DCIM-DVUSB.*

Pour ouvrir la page Port :

1. Sélectionnez Paramètres du dispositif > Configuration du port. La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port KVM que vous souhaitez modifier. La page Port s'ouvre.

Pour sélectionner les profils USB d'un port KVM :

1. Dans la section Select USB Profiles for Port (Sélectionner les profils USB du port), choisissez un ou plusieurs profils USB dans la liste Available (Disponibles).
   - Appuyez sur la touche Maj+cliquez, et faites glisser pour sélectionner plusieurs profils contigus.
   - Appuyez sur la touche Ctrl+cliquez pour sélectionner plusieurs profils non contigus.
2. Cliquez sur Add (Ajouter). Les profils sélectionnés apparaissent dans la liste Selected. Ces profils peuvent être utilisés pour le serveur cible KVM connecté au port.

Pour spécifier un profil USB privilégié :

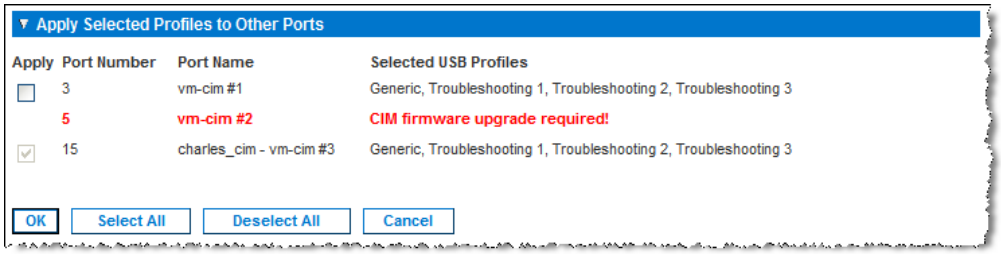
1. Après avoir sélectionné les profils disponibles pour un port, choisissez-en un dans le menu Preferred Profile for Port (Profil privilégié pour le port). La valeur par défaut est Generic (Générique). Le profil sélectionné est utilisé lors de la connexion au serveur cible KVM. Le cas échéant, vous pouvez le remplacer par n'importe quel autre profil USB.
2. Si le profil actif défini en tant que profil préféré est sélectionné, cet USB préféré est également utilisé comme profil actif.

Pour retirer les profils USB sélectionnés :

1. Dans la section Select USB Profiles for Port (Sélectionner les profils USB du port), choisissez un ou plusieurs profils USB dans la liste Selected (Sélectionnés).
   - Appuyez sur la touche Maj+cliquez, et faites glisser pour sélectionner plusieurs profils contigus.
   - Appuyez sur la touche Ctrl+cliquez pour sélectionner plusieurs profils non contigus.
2. Cliquez sur Remove (Supprimer). Les profils sélectionnés apparaissent dans la liste Available (Disponibles). Ils ne sont plus disponibles pour un serveur cible KVM connecté à ce port.

Pour appliquer une sélection de profils à plusieurs ports :

1. Dans la section Apply Selected Profiles to Other Ports (Appliquer les profils sélectionnés à d'autres ports), cochez la case Apply (Appliquer) pour chaque port KVM auquel vous souhaitez appliquer l'ensemble en cours de profils USB sélectionnés.



   - Pour sélectionner tous les ports KVM, cliquez sur Select All (Tout sélectionner).
   - Pour désélectionner tous les ports KVM, cliquez sur Deselect All (Tout désélectionner).

Configurer les Paramètres du port local KX III

Remarque : Certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage de navigateur se produit lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

Pour configurer les paramètres du port local :

- Choisissez Paramètres du dispositif > Paramètres du port local La page des paramètres du port local s'ouvre.

Activer le Port Local standard

1. Cochez la case en regard d'Enable Standard Local Port (Activer le port local standard) pour l'activer. Désélectionnez la case à cocher pour le désactiver.

   Par défaut, le port local standard est activé, mais peut être désactivé selon les besoins.

   Le navigateur redémarre lorsque cette modification est effectuée.

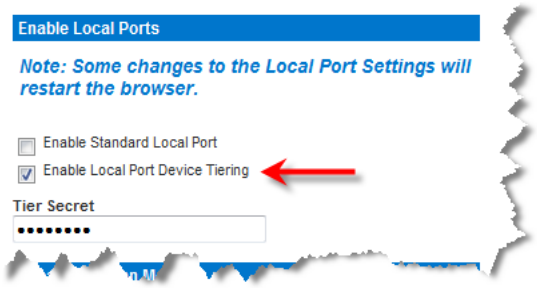
   Remarque : Si vous utilisez la fonction multiniveau, la fonction Port Local Standard sera désactivée car les deux ne peuvent pas être utilisées simultanément.

Activer la fonction multiniveau sur le dispositif du port local

1. Si vous utilisez la fonction multiniveau, cochez la case Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local) et entrez le mot secret dans le champ Tier Secret (Secret du niveau).

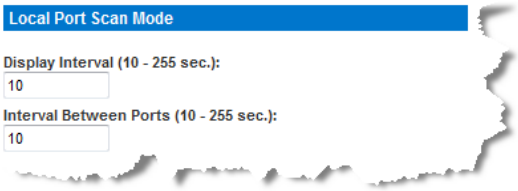
   Pour paramétrer la fonction multiniveau, vous devez également configurer le dispositif de base sur la page Device Services (Services du dispositif).

Reportez-vous à Configuration et activation de la fonction multiniveau pour plus d'informations sur la fonction multiniveau.



Configurer les paramètres du Mode de balayage du Port Local

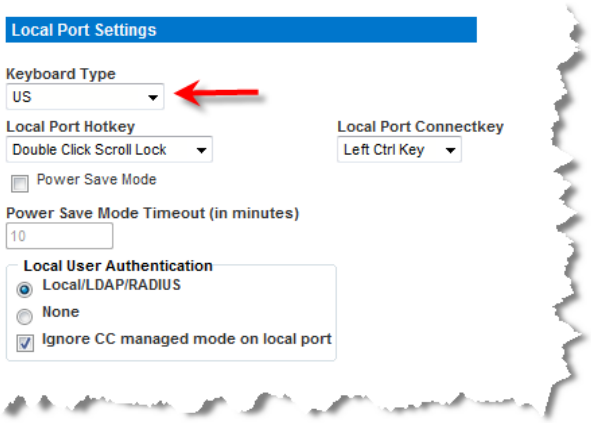
1. Le cas échéant, configurez les paramètres Local Port Scan Mode (Mode de balayage du port local). Ces paramètres s'appliquent à la fonction Scan Settings (Paramètres de balayage) accessible depuis la page Port. Reportez-vous à Balayage des ports.
   - Dans le champ Display Interval (10-255 sec) (Intervalle d'affichage (10 à 255 s), indiquez le nombre de secondes pendant lesquelles la cible sélectionnée doit rester affichée au centre de la fenêtre Port Scan (Balayage des ports).
   - Dans le champ Interval Between Ports (10 - 255 sec) (Intervalle entre les ports (10 à 255 s), indiquez l'intervalle de pause que doit respecter le dispositif entre les ports.



Sélectionnez le type de clavier de la Console locale

1. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante.

Le navigateur redémarrera lorsque cette modification sera effectuée.



- US
- US/International
- United Kingdom
- Français (France)
- Allemand (Allemagne)
- Allemand (Suisse)
- Chinois simplifié
- Chinois traditionnel
- Dubeolsik Hangul (Coréen)
- Japonais (JIS)
- Portugais (Portugal)
- Norvégien (Norvège)
- Suédois (Suède)
- Danois (Danemark)
- Belge (Belgique)
- Hongrois
- Espagnol
- Italien
- Slovène

Remarque : L'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de KX III.

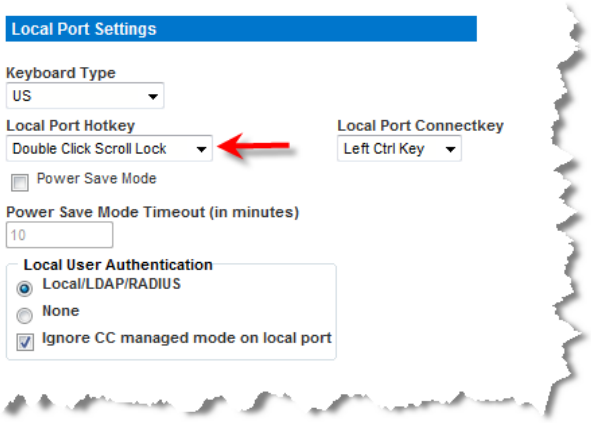
Remarque : Si vous utilisez un clavier turc, vous devez vous connecter à un serveur cible via Active KVM Client (AKC). Il n'est pas pris en charge par les autres clients Raritan.

Sélectionnez le raccourci-clavier du port local.

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

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans

Raccourci-clavier :	Appuyez sur :
	interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption



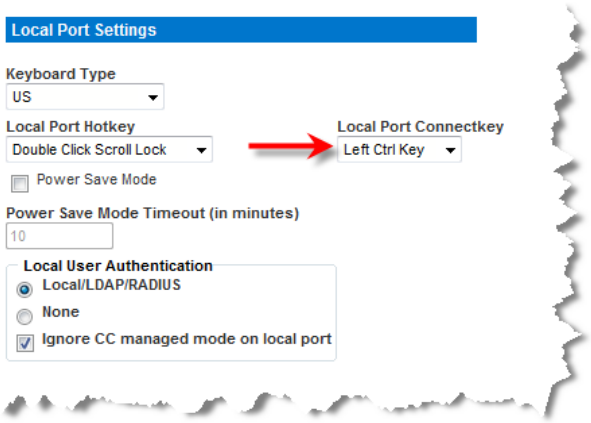
Sélectionnez la touche de connexion du port local.

1. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre.

   Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local.

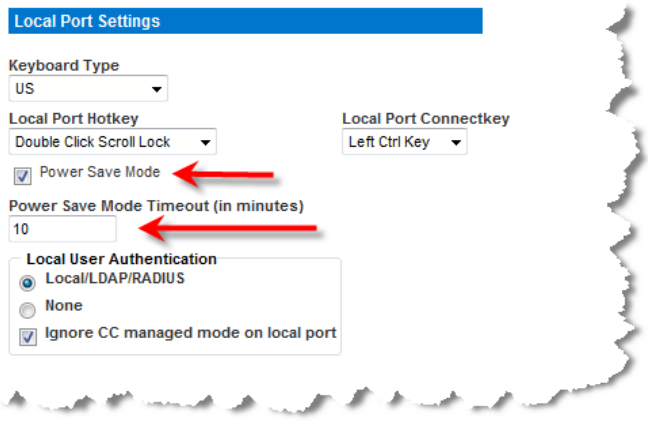
   Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à ***Exemples de touches de connexion*** (à la page 298) pour obtenir des exemples de séquences de touches de connexion.

La touche de connexion fonctionne pour les serveurs standard et les châssis de lames.



Configurer l'option d'Economie d'énergie (optionnel)

1. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique :
   a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).
   b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.

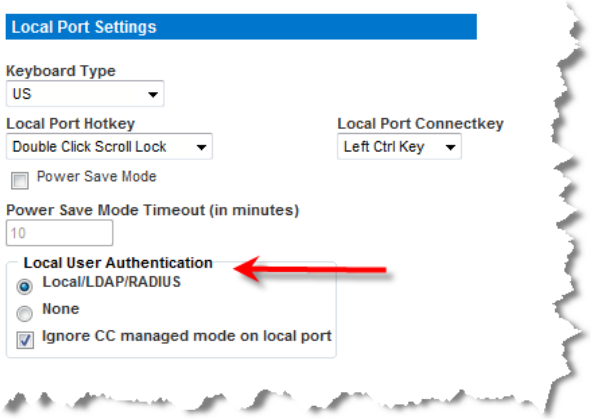


Sélectionnez l'authentification des utilisateurs locaux

1. Sélectionnez le type d'authentification d'utilisateur locale.
   - Local/LDAP/RADIUS. Il s'agit de l'option recommandée.

     Pour plus d'informations sur l'authentification, reportez-vous à Authentification à distance.
   - Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale.

Cette option est recommandée pour les environnements sécurisés uniquement.



Services du dispositif

Activation de SSH

Activez l'accès SSH pour permettre aux administrateurs d'accéder à KX III 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 III. 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 III 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 III par-delà un pare-feu, les paramètres du pare-feu doivent permettre la communication bidirectionnelle par l'intermédiaire du port 5000 par défaut ou d'un autre port configuré ici.

Pour activer le port de détection :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Renseignez le champ Discovery Port (Port de détection).
3. Cliquez sur OK.

Configuration et activation de la fonction multiniveau

La fonction multiniveau vous permet d'accéder aux cibles et PDU KX III par l'intermédiaire d'un dispositif KX III de base.

Des dispositifs peuvent être ajoutés et supprimés d'une configuration multiniveau selon les besoins, pour obtenir un maximum de deux niveaux étagés.

Lors du paramétrage des dispositifs, vous utiliserez des CIM spécifiques pour des configurations particulières.

Reportez-vous à Fonction multiniveau - Types de cibles, CIM pris en charge et mise en niveau de configurations pour obtenir une description des cibles pouvant être incluses à une configuration multiniveau, et des informations sur la compatibilité des CIM et la configuration des dispositifs.

La configuration des ports, dont la modification du nom du CIM, doit être effectuée directement depuis chaque dispositif Cela ne peut être fait à partir du dispositif de base des ports cible en niveau.

La fonction multiniveau prend également en charge les commutateurs KVM pour alterner entre les serveurs. Reportez-vous à ***Configuration des commutateurs KVM*** (à la page 94).

Une fois configuré, les dispositifs base et multiniveaux sont affichés sur la Page d'accès aux ports Reportez-vous aux ***Dispositifs Multiniveaux - Page d'accès aux ports*** (voir "***Dispositifs en niveau - Page Port Access***" à la page 18)

Avant de créer une configuration multiniveau

Avant de créer une configuration multiniveau, revoyez les ***Configurations multiniveau KX III permises*** (à la page 137) et les fonctions limitées et non-supportées en cibles multiniveau.

Avant d'ajouter des appareils multiniveau à une configuration KX III multiniveau:

- Les appareils de base et multiniveau doivent tous être opérés sous la même révision de firmaware.
- L'activation des dispositifs de base s'effectue sur la page Device Settings (Paramètres du dispositif). Consultez Configuration des serveurs cible standard
- L'activation des dispositifs en niveau s'effectue sur la page Local Port Settings (Paramètres du port local). Consultez ***Configurer les Paramètres du port local KX III*** (à la page 129), puis ***Autoriser le multiniveau du disposif de port local*** (voir "***Activer la fonction multiniveau sur le dispositif du port local***" à la page 129)
- Activer le multiniveau pour l'appareil de base, et les appareils multiniveau. Consultez ***Activation de la fonction multiniveau*** (à la page 139)

Configurations multiniveau KX III permises

Avant de rendre un appareil multiniveau, revoyez ***Avant de créer une configuration multiniveau*** (à la page 137).

Voici les configurations multiniveau permises pour KX III:

- Dispositif KXIII de base> dispositifs KX III multiniveau
- Dispositif KXIII de base> dispositifs KX III multiniveau
- Les cibles à deux ports vidéo attachés à un appareil à niveau doivent être connectés via des appareils à niveau.

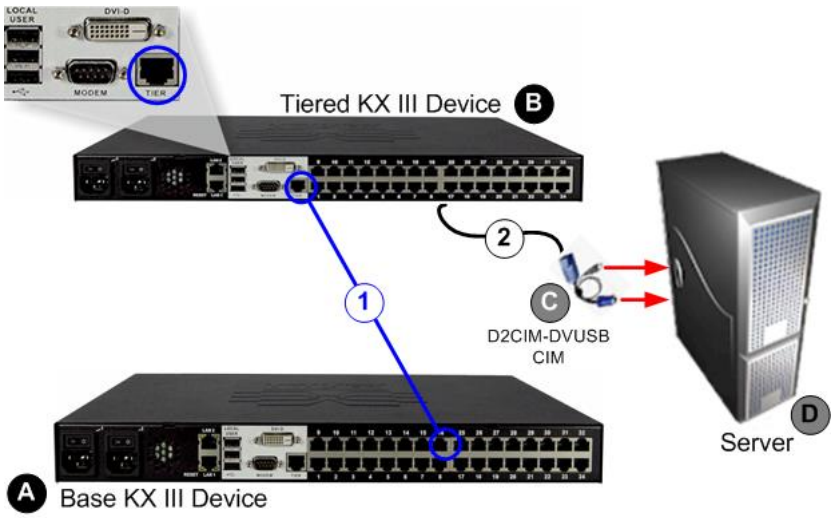
Fonctions non prises en charge et limitées sur les cibles en niveau

Les fonctions suivantes ne sont pas prises en charge sur les cibles en niveau :

- Châssis de lames sur les dispositifs en niveau
- Audio sur les dispositifs en niveau
- Cartes à puce sur les dispositifs en niveau
- Dispositifs en niveau de support virtuel
- MCCAT comme dispositif en niveau
- La gestion des groupes de ports est limitée à la création de groupes de ports de membres connectés directement à la base.
- Les cibles à deux ports vidéo attachés à un appareil à niveau doivent être connectés via des appareils à niveau.
- La synchronisation absolue de la souris peut ne pas être effectuée correctement si la configuration multiniveau est un mélange de dispositifs KX III et KX II
- Dispositif KX II de base> dispositifs KX III multiniveau

Exemple de connexion multiniveau KX III

Le diagramme suivant illustre les configurations de câblage entre un dispositif KX III multiniveau et un dispositif de KX III de base.



Procédure	
A	Dispositif KXIII de base
B	Dispositif KX III multiniveau
C	CIM à connecter au serveur cible du dispositif multiniveau de KX III.
D	Serveur cible
1	Port à niveau d'un dispositif de base à un dispositif multiniveau Connexion au port à niveau: ▪ Connectez l'une des extremités d'un câble Cat5/5e/6 à un port de serveur cible sur un dispositif KX III de base. ▪ Connectez l'autre extrémité du câble dans le port à niveau du dispositif KX III multiniveau.
2	La connexion d'un dispositif multiniveau aux ports clavier/vidéo/souris d'un serveur cible: ▪ Connectez l'une des extremités d'un câble Cat5/5e/6 à un port de serveur cible sur un dispositif KX III de base, et l'autre extremité dans un CIM pris en charge tel qu'un D2CIM-DVUSB. ▪ Connectez les prises clavier, souris et vidéo sur le CIM aux ports correspondants sur le serveur cible.

Activation de la fonction multiniveau

Pour activer la fonction multiniveau :

1. A partir du dispositf multiniveau, sélectionnez Paramètres de l'appareil > Services de l'appareil pour ouvrir la page de Paramètres des services de l'Appareil.
2. Sélectionnez Enable Tiering as Base (Activer la fonction multiniveau comme base).
3. Dans le champ Base Secret (Secret de la base), entrez le secret partagé entre la base et les dispositifs en niveau. Ce secret est exigé pour permettre aux dispositifs en niveau d'authentifier le dispositif de base. Vous entrerez le même mot secret pour le dispositif en niveau. Cliquez sur OK.
4. Activez les dispositifs en niveau. Depuis le dispositif en niveau, choisissez Paramètres du dispositif > Paramètres du port local.

5. Dans la section Enable Local Ports (Activer les ports locaux) de la page, sélectionnez Enable Local Port Device Tiering (Activer la fonction multiniveau sur le dispositif du port local).
6. Dans le champ Tier Secret (Secret du niveau), entrez le mot secret entré pour le dispositif de base sur la page Device Settings (Paramètres du dispositif). Cliquez sur OK.

Une fois les dispositifs activés et configurés, ils apparaissent sur la page Port Access (Accès aux ports).

Lorsque KX III est configuré pour servir de dispositif de base ou multiniveau, il apparaît comme suit :

- Configured As Base Device (Configuré comme dispositif de base) dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'interface du KX III pour les dispositifs de base.
- Configured As Tier Device (Configuré comme dispositif en niveau) dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'interface du KX III pour les dispositifs multiniveau.
- Le dispositif de base sera identifié comme 'Base' dans le panneau gauche de l'interface du dispositif multiniveau sous Connect User (Utilisateur connecté).
- Les connexions cible vers un port en niveau depuis la base seront affichés sous la forme de 2 ports connectés.

Accès local et à distance d'appareil multiniveau

Le dispositif de base fournit un accès à distance et local via une liste de ports consolidée de la page Port Access.

Les dispositifs en niveau offrent un accès à distance depuis leur propre liste de ports.

L'accès local n'est pas disponible sur les dispositifs en niveau lorsque la fonction multiniveau est activée.

Accèder à un châssis de lames à partir d'un dispositif de base

Des châssis de lames attachés directement à un dispositif KX III de base sont accessibles.

Gestion de l'alimentation de dispositifs multiniveau

Vous pouvez mettre sous et hors tension les cibles intégrées à la configuration multiniveau.

L'accès de ces cibles s'effectue depuis la page Port Access.

Si des cibles et des prises sont associées, la gestion de l'alimentation est disponible depuis la page Port Access.

Les associations cibles et prises de PDU sont limitées à celles connectées au même KX III.

Les PDU connectées aux KX III de base ou multiniveau sont affichées dans la liste déroulante de la page Puissance, ainsi que les statistiques relatives à la barrette d'alimentation sélectionnée.

La gestion du niveau des prises est également disponible.

Précisément, vous pouvez mettre sous et hors tension les prises actuellement activées, mais vous ne pouvez pas effectuer l'alimentation cyclique des prises actuellement désactivées.

Activation d'un accès direct aux ports via URL

L'accès direct aux ports permet aux utilisateurs d'éviter les pages de connexion et d'accès aux ports du dispositif.

Cette fonction permet également d'entrer un nom d'utilisateur et un mot de passe directement, et d'accéder à la cible si le nom d'utilisateur et le mot de passe ne sont pas contenus dans l'URL.

Syntaxe URL d'accès direct au port pour le client KVM Virtuel (VKC)

Si vous utilisez le Virtual KVM Client (VKC) et l'accès direct aux ports, utilisez l'une des syntaxes suivantes pour les ports standards:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

  Ou

- https://IPaddress/dpa.asp?username=username&password=password&portname=port name

Pour les châssis de lames, le port est désigné par le numéro de port et le numéro de connecteur.

- https://IPaddress/dpa.asp?username=username&password=password&port=port number-slot number

  Par exemple, le numéro de port est 1-2 lorsque le châssis de lames est connecté au port 1, connecteur 2

- https://IPaddress/dpa.asp?username=username&password=password&port=port name-slot number

  Par exemple, le numéro de port est 1-2 lorsque le châssis de lames est connecté au port 1, connecteur 2

Le nom d'utilisateur et mot de passe sont facultatifs.

S'ils ne sont pas fournis, une boîte de dialogue de connexion apparaît et, après avoir été authentifié, l'utilisateur est connecté directement à la cible.

Le port peut être un numéro ou un nom de port.

Si vous utilisez un nom de port, il doit être unique ou une erreur est signalée.

Si le port est totalement omis, une erreur est signalée.

Si vous accédez à une cible faisant partie d'un groupe de deux ports vidéo, l'accès aux ports direct utilise le port principal pour lancer les ports principal et secondaire.

Les connexions directes au port secondaire sont rejetées et les règles d'autorisation habituelles s'appliquent.

Reportez-vous à **Création d'un groupe de deux ports vidéo** (à la page 167) pour plus d'informations à ce sujet. .

Syntaxe URL d'accès direct au port pour le client KVM Actif (AKC)

Si vous utilisez le Active KVM Client (AKC) et l'accès direct aux ports, utilisez:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

  Ou

- https://IPaddress/dpa.asp?username=username&password=password&port=port name&client=akc

Pour les châssis de lames, le port est désigné par le numéro de port et le numéro de connecteur.

- https://IPaddress/dpa.asp?username=username&password=password&port=port number-slot number=akc

  Par exemple, le numéro de port est 1-2 lorsque le châssis de lames est connecté au port 1, connecteur 2

- https://IPaddress/dpa.asp?username=username&password=password&port=port name-slot number=akc

  Par exemple, le numéro de port est 1-2 lorsque le châssis de lames est connecté au port 1, connecteur 2

Le nom d'utilisateur et mot de passe sont facultatifs.

S'ils ne sont pas fournis, une boîte de dialogue de connexion apparaît et, après avoir été authentifié, l'utilisateur est connecté directement à la cible.

Le port peut être un numéro ou un nom de port.

Si vous utilisez un nom de port, il doit être unique ou une erreur est signalée.

Si le port est totalement omis, une erreur est signalée.

Client=akc est facultatif sauf si vous utilisez un client AKC.

Si client=akc n'est pas inclus, le Client KVM Virtuel (VKC) est utilisé comme client.

Si vous accédez à une cible faisant partie d'un groupe de deux ports vidéo, l'accès aux ports direct utilise le port principal pour lancer les ports principal et secondaire.

Les connexions directes au port secondaire sont rejetées et les règles d'autorisation habituelles s'appliquent.

Reportez-vous à **Création d'un groupe de deux ports vidéo** (à la page 167) pour plus d'informations à ce sujet. .

Activer l'accès direct aux ports.

Pour activer l'accès direct aux ports :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Cochez la case Enable Direct Port Access via URL (Activer l'accès direct aux ports via URL) pour accorder aux utilisateurs un accès direct à une cible via le dispositif Dominion par transmission des paramètres nécessaires dans l'URL.
3. Cliquez sur OK.

Activation de la validation du certificat du serveur de téléchargement AKC

Si vous utilisez le client AKC, vous pouvez décider d'utiliser ou non la fonction Activer la validation du certificat du serveur de téléchargement AKC.

Remarque : Lorsque Microsoft® ClickOnce® fonctionne en mode double pile IPv4 et IPv6 avec la fonction 'Auotoriser le téléchargement du serveur AKC, Validation de Certificat', le CN du certificat de serveur ne doit pas contenir de forme à zéros compressés de l'adresse IPv6.

Sinon, vous ne pourrez pas télécharger et lancer AKC.

Toutefois, ceci peut entraîner un conflit avec les préférences du navigateur concernant la forme de l'adresse IPv6.

Utilisez le nom d'hôte du serveur dans le nom commun (CN) ou entrez des formes compressées et non compressées de l'adresse IPv6 dans le champ Subject Alternative Name (Autre nom du sujet).

Option 1 : vous n'activez pas la validation du certificat du serveur de téléchargement AKC (paramètre par défaut)

Si vous n'activez pas cette fonction, tous les utilisateurs du dispositif Dominion et de CC-SG Bookmark and Access Client doivent :

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

Option 2 : Activer la validation du certificat du serveur de téléchargement AKC

Si vous activez la validation du certificat du serveur de téléchargement AKC :

- Les administrateurs doivent téléverser un certificat valide sur le dispositif ou générer un certificat auto-signé sur celui-ci. Le certificat doit désigner un hôte valide.
- Chaque utilisateur doit ajouter le certificat AC (ou une copie du certificat auto-signé) dans la liste Autorités de certification racines de confiance de leur navigateur.
- Lorsque vous utilisez les quartiers CC-SG, vous devez activer AKC sur chacun des membres du quartier.

Pour installer le certificat auto-signé avec les systèmes d'exploitation Windows Vista® et Windows 7® :

1. Incluez l'adresse IP de KX III dans la zone Sites de confiance et assurez-vous que le mode protégé est désactivé.
2. Lancez Internet Explorer® en utilisant l'adresse IP de KX III comme URL. Un message d'erreur de certificat s'affiche.
3. Sélectionnez Afficher les certificats.
4. Dans l'onglet Général, cliquez sur Installer le certificat. Le certificat est alors installé dans la liste Autorités de certification racines de confiance.
5. Après l'installation du certificat, l'adresse IP de KX III devrait être retirée de la zone Sites de confiance.

Pour activer la validation du certificat du serveur de téléchargement AKC :

1. Sélectionnez Paramètres du dispositif > Device Services (Services du dispositif). La page Device Service Settings (Paramètres des services du dispositif) s'ouvre.
2. Cochez la case Activer la validation du certificat du serveur de téléchargement AKC ou laissez la fonction désactivée (défaut).
3. Cliquez sur OK.

Si vous vous connectez à un dispositif autonome KX III et que la prise en charge de la validation du certificat du serveur de téléchargement AKC est activée, le format IPv6 valable pour générer le certificat est :

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` où figure un 0 non significatif

  ou

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` où l'adresse n'est pas compressée

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 III*** (voir "***Affichage du MIB de Productname***" à la page 155) pour plus d'informations sur la consultation du MIB de KX III.

KX III prend en charge l'enregistrement 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). Au moins une des options 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)

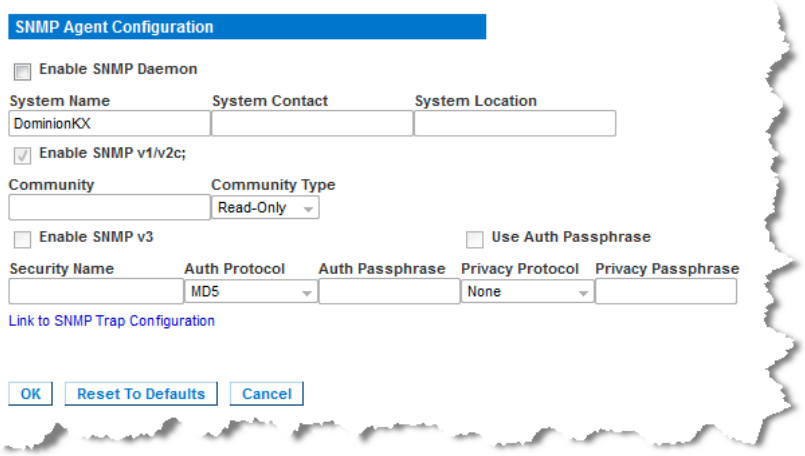
e. Privacy Protocol - le cas échéant, algorithme AES ou DES utilisé pour chiffrer les données de PDU et de contexte

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.

<e> Configurez les traps SNMP sur la page Gestion des événements - Paramètres, qui peut être rapidement accédé en cliquant sur le lien de Configuration des traps SNMP. Reportez-vous à ***Configuration des traps SNMP*** (à la page 149) pour obtenir des informations sur la création des traps SNMP et Liste des traps SNMP de KX III pour obtenir la liste des traps SNMP de KX III 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*** (voir "***Configuration de la gestion des événements - Destinations***" à la page 157).



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 III et le routeur auquel elle est reliée se désynchronisent au moment où KX III redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Configuration des paramètres de modem

Remarque : La version KX III 3.0.0 ne fournit pas de support modem, mais en fournira dans de futures versions.

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 III. 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 Paramètres du dispositif > 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 « Ajuster à l'heure d'été ».
4. Choisissez la méthode à utiliser pour définir la date et l'heure :
   - User Specified Time (Heure spécifiée par l'utilisateur) - utilisez 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).
   - Synchronisation avec le Serveur NTP - utilisez cette option pour synchroniser la date et l'heure avec le Serveur de Protocole Temps Réseau (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. Entrez l'adresse IP du Serveur d'horloge secondaire. **Facultatif**

6. Cliquez sur OK.

Gestion des événements

La fonction de gestion des événements de KX III permet d'activer et de désactiver la distribution des événements système aux gestionnaires SNMP, Syslog et au journal d'audit. Ces événements sont regroupés dans différentes catégories et vous pouvez décider d'envoyer chacun vers une ou plusieurs destinations.

Configuration de la gestion des événements - Paramètres

Effectuez la configuration des traps SNMP et de syslog sur la page Event Management - Settings (Gestion des événements - Paramètres). Reportez-vous à ***Configuration des traps SNMP*** (à la page 149).

Une fois la configuration effectuée, activez les traps SNMP sur la page Event Management - Settings. Reportez-vous à ***Configuration de la page Event Management - Destinations*** (voir "***Configuration de la gestion des événements - Destinations***" à la page 157).

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 III pour une liste de traps SNMP KX III .

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 146) pour des informations sur la configuration des agents SNMP et ***Affichage du MIB de KX III*** (voir "***Affichage du MIB de Productname***" à la page 155) pour des informations concernant la visualisation du MIB de KX III.

Pour configurer SNMP (permettre la journalisation de SNMP) :

1. Sélectionnez Paramètres du dispositif > Gestion des événements – Paramètres. La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre :
2. Sélectionnez la Journalisation SNMP activée pour activer les champs SNMP restants dans la section. **Obligatoire**

3. Cochez SNMP v1/v2c Traps Enabled et/ou SNMP Trap v3 Enabled. Une des options au moins doit être sélectionnée.

   Une fois sélectionnée, tous les champs liés sont activés. **Obligatoire**

4. Renseignez les champs ci-après pour SNMP v1/v2c (le cas échéant) :

   a. Destination IP/Hostname - adresse IP ou nom d'hôte du gestionnaire SNMP. Cinq (5) gestionnaires SNMP au maximum peuvent être créés.

   Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

   b. Port Number - numéro de port utilisé par le gestionnaire SNMP.

   c. Community - chaîne de communauté du dispositif

   Remarque : une communauté SNMP est le groupe auquel les dispositifs et les postes de gestion exécutant SNMP appartiennent. Elle aide à définir le destinataire des informations. Le nom de la communauté permet d'identifier le groupe. Le dispositif ou agent SNMP peut appartenir à plusieurs communautés SNMP.

5. Si ce n'est pas encore fait, cochez la case SNMP Trap v3 Enabled pour activer les champs suivants. Renseignez les champs ci-après pour SNMP v3 (le cas échéant) :

   a. Destination IP/Hostname - adresse IP ou nom d'hôte du gestionnaire SNMP. Cinq (5) gestionnaires SNMP au maximum peuvent être créés.

   Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

   b. Port Number - numéro de port utilisé par le gestionnaire SNMP.

   c. Security Name - nom d'utilisateur ou de compte de service de l'entité communiquant avec l'agent SNMP (32 caractères au plus)

   d. Authentication Protocol - protocole d'authentification MD5 ou SHA utilisé par l'agent SNMP v3

   e. Authentication Passphrase - phrase de passe requise pour accéder à l'agent SNMP v3 (64 caractères au plus)

   f. Privacy Protocol - le cas échéant, algorithme AES ou DES utilisé pour chiffrer les données de PDU et de contexte

   g. Privacy Passphrase - phrase de passe servant à accéder à l'algorithme de protocole de confidentialité (64 caractères au plus)

Remarque : Si vous accédez à la page Event Management - Settings depuis la console locale et utilisez une résolution d'écran inférieure à 1280 x 1024, la colonne Privacy Passphrase (Phrase de passe de confidentialité) ne s'affiche pas sur cette page. Dans ce cas, masquez le panneau gauche de KX III. Reportez-vous à Panneau gauche.

6. Cliquez sur OK pour créer les traps 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*** (voir "***Configuration de la gestion des événements - Destinations***" à la page 157).

KX III prend en charge l'enregistrement 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.

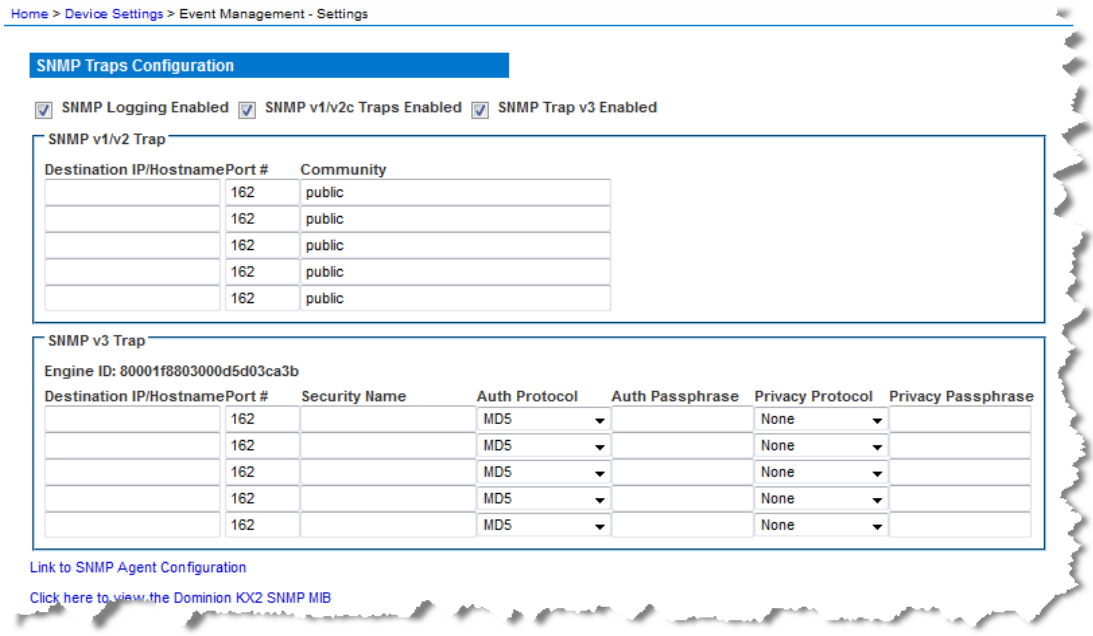
Pour modifier des traps SNMP existants :

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 d'usine par défaut de KX III.

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 III et le routeur auquel elle est reliée se désynchronisent au moment où KX III redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Liste des traps SNMP de KX III

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 III :

Nom de trap	Description
bladeChassisCommError	Une erreur de communication avec le dispositif avec châssis de lames connecté à ce port a été détectée.
cimConnected	Le CIM est connecté.
cimDisconnected	Le CIM est déconnecté.
cimUpdateStarted	La mise à jour du CIM est en cours.
cimUpdateCompleted	La mise à jour du CIM est terminée.
configBackup	La configuration du dispositif a été sauvegardée.
configRestore	La configuration du dispositif a été restaurée.
deviceUpdateFailed	La mise à jour du dispositif a échoué.
deviceUpgradeCompleted	Le KX III a effectué la mise à jour via un fichier RFP.
deviceUpgradeStarted	Le KX III 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 III.
groupDeleted	Un groupe a été supprimé du système.
groupModified	Un groupe a été modifié.
ipConflictDetected	Un conflit d'adresse IP a été détecté.
ipConflictResolved	Un conflit d'adresse IP a été résolu.
networkFailure	Une interface Ethernet du produit ne peut plus communiquer via le réseau.
networkParameterChanged	Une modification a été appliquée aux paramètres réseau.
passwordSettingsChanged	Les paramètres des mots de passe sécurisés ont été modifiés.

Nom de trap	Description
portConnect	Un utilisateur authentifié au préalable a démarré une session KVM.
portConnectionDenied	Une connexion au port cible a été refusée.
portDisconnect	Un utilisateur engagé dans une session KVM ferme la session correctement.
portStatusChange	Le port n'est plus disponible.
powerNotification	Notification de l'état de la prise d'alimentation : 1=Active, 0=Inactive.
powerOutletNotification	Notification de l'état d'une prise de barrette d'alimentation.
rebootCompleted	Le redémarrage de KX III est terminé.
rebootStarted	KX III a commencé à redémarrer lors de l'alimentation cyclique du système ou lors d'un redémarrage à chaud à partir du système d'exploitation.
scanStarted	Un balayage de serveur cible a démarré.
scanStopped	Un balayage de serveur cible s'est arrêté.
securityBannerAction	La bannière de sécurité a été acceptée ou refusée.
securityBannerChanged	La bannière de sécurité a été modifiée.
securityViolation	Violation de sécurité.
setDateTime	Les date et heure du dispositif ont été définies.
setFIPSMode	Le mode FIPS a été activé.
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.

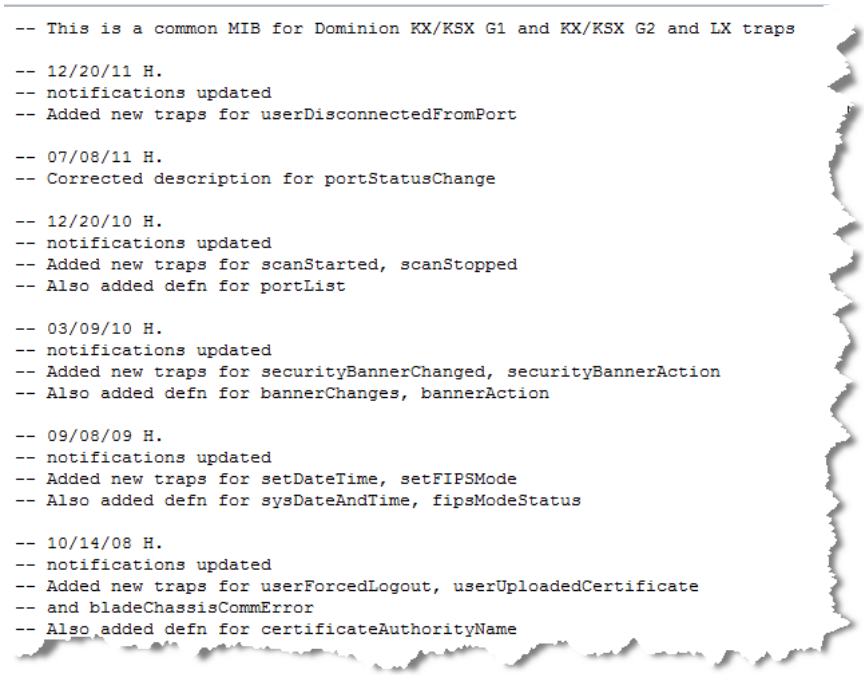
Nom de trap	Description
userLogin	Un utilisateur s'est connecté avec succès à KX III et a été authentifié.
userLogout	Un utilisateur s'est déconnecté avec succès de KX III.
userModified	Un compte d'utilisateur a été modifié.
userPasswordChanged	Cet événement est déclenché lorsque le mot de passe de n'importe quel utilisateur du dispositif est modifié.
userSessionTimeout	Un utilisateur avec une session active a subi une interruption de session en raison du délai d'attente.
userUploadedCertificate	Un utilisateur a téléversé un certificat SSL.
vmImageConnected	Un utilisateur a tenté de monter un dispositif ou une image sur la cible à l'aide de la fonction Support virtuel. Pour chaque tentative de mappage (montage) de dispositif/image, cet événement est généré.
vmImageDisconnected	Un utilisateur a tenté de démonter un dispositif ou une image sur la cible à l'aide de la fonction Support virtuel.

Affichage du MIB de Productname

Pour afficher le MIB de Productname :

1. Sélectionnez Paramètres du dispositif > Gestion des événements – Paramètres. La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre :
2. Cliquez le lien 'Cliquer ici pour afficher le MIB SNMP de Dominion KX3'. Le fichier MIB s'ouvre dans une fenêtre de navigateur.

Remarque : Si vous disposez d'un accès en lecture/écriture au fichier MIB, utilisez un éditeur MIB pour le modifier.



```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps

-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateTime, setFIPSMode
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

Configuration de Syslog

Pour configurer Syslog (activer le transfert Syslog) :

1. Sélectionnez Enable Syslog Forwarding (Activer le transfert Syslog) pour consigner les messages du dispositif sur un serveur Syslog distant.
2. Entrez l'adresse IP ou le nom d'hôte de votre serveur Syslog dans le champ IP Address.
3. Cliquez sur OK.

Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

Utilisez la fonction de réinitialisation aux valeurs par défaut pour supprimer la configuration syslog.

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 149).*

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).

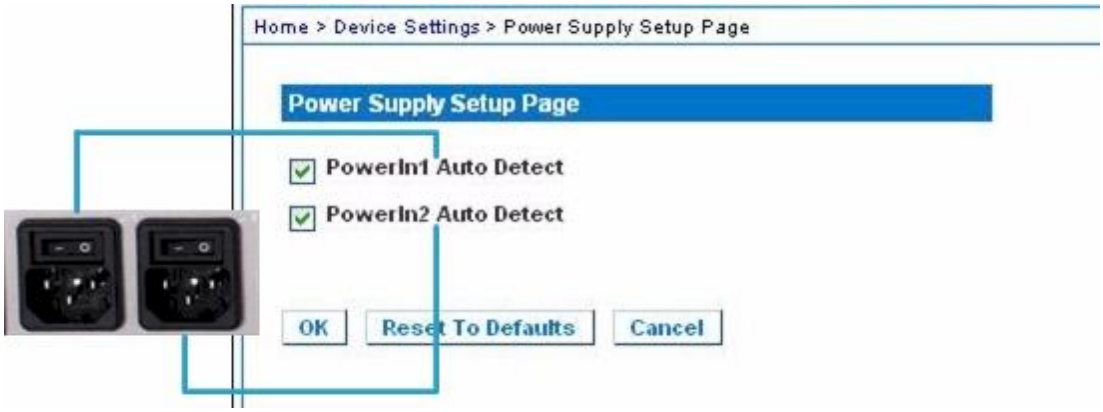
AVERTISSEMENT : lorsque vous utilisez les traps SNMP sur UDP, il est possible que l'unité KX III et le routeur auquel elle est reliée se désynchronisent au moment où KX III redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Configuration de l'alimentation

L'unité KX III offre une double alimentation. Elle peut détecter et indiquer automatiquement l'état de ces alimentations. Utilisez la page Power Supply Setup (Configuration de l'alimentation) pour préciser si vous utilisez une source d'alimentation ou deux. Une configuration appropriée garantit l'envoi de notifications adéquates par KX III en cas de panne de courant. Par exemple, si l'alimentation numéro un tombe en panne, le voyant d'alimentation situé à l'avant de l'unité devient rouge.

Pour activer la détection automatique des alimentations utilisées :

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



2. Si vous branchez une arrivée électrique dans l'alimentation numéro un (la plus à gauche à l'arrière de l'unité), sélectionnez l'option PowerIn1 Auto Detect (Détection automatique PowerIn1).
3. Si vous branchez une arrivée électrique dans l'alimentation numéro deux (la plus à droite à l'arrière de l'unité), sélectionnez l'option PowerIn2 Auto Detect (Détection automatique PowerIn2).
4. Cliquez sur OK.

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

Pour désactiver la détection automatique :

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

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

Remarque : KX III NE génère PAS de rapport sur l'état de l'alimentation pour CommandCenter. Dominion I (génération 1), en revanche, établit des rapports sur l'état d'alimentation pour CommandCenter.

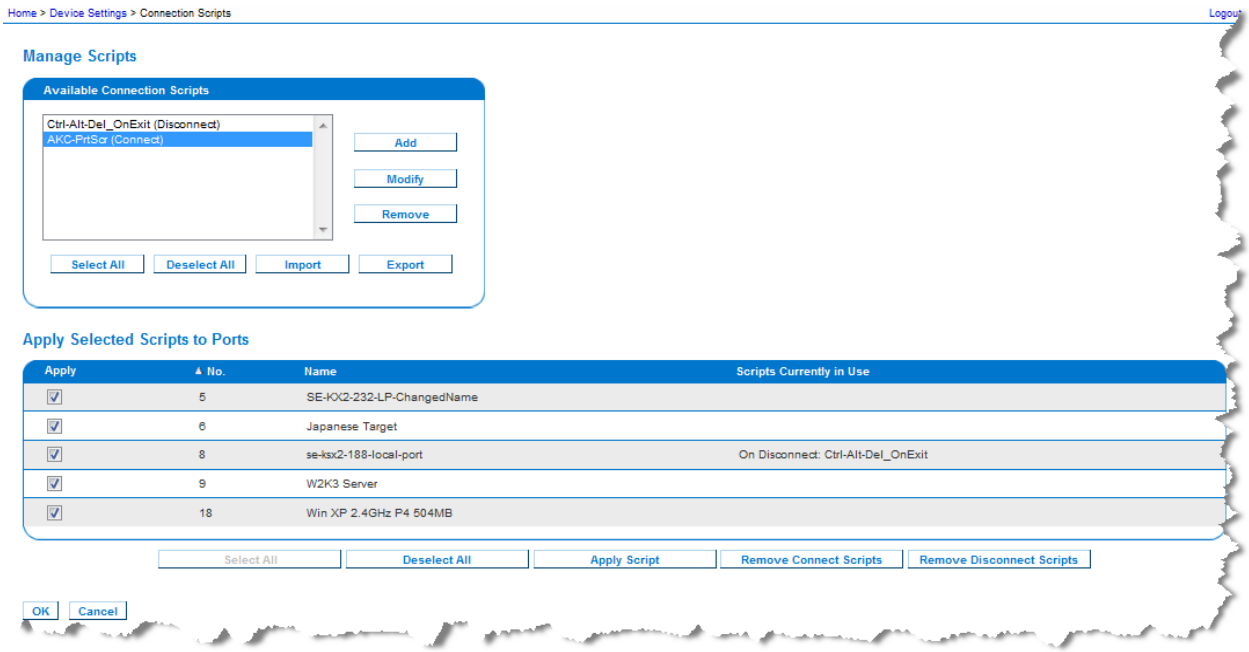
Scripts de connexion et de déconnexion

Le KX III offre la possibilité d'exécuter des scripts de macros lors de la connexion à ou de la déconnexion d'une cible.

Vous pouvez créer et modifier vos propres scripts dans la page Connection Script afin d'effectuer des actions supplémentaires lors de la connexion aux ou de la déconnexion des cibles.

Vous pouvez également importer des scripts de connexion existants au format de fichier XML. Les scripts que vous créez dans KX III peuvent également être exportés au format de fichier XML.

KX III peut comporter jusqu'à 16 scripts au total.



Application et retrait des scripts

Pour appliquer un script à des cibles :

1. Cliquez sur Paramètres du dispositif > Scripts de connexion. La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à appliquer aux cibles. Un script On Connect (A la connexion) et un script On Disconnect (A la déconnexion) peuvent être appliqués à une cible.

   Remarque : Un seul script à la fois peut être ajouté aux cibles.

3. Dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports), sélectionnez les cibles auxquelles vous souhaitez appliquer le script. Pour cela, utilisez le bouton Select All (Tout sélectionner) ou cochez la case à gauche de chaque cible pour appliquer le script à certaines seulement.
4. Cliquez sur Apply Scripts (Appliquer les scripts). Une fois le script ajouté à la cible, il apparaît dans la colonne Scripts Currently in Use (Scripts utilisés actuellement) dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports).

Pour retirer un script à des cibles :

1. Dans la section Apply Selected Scripts to Ports (Appliquer les scripts sélectionnés aux ports), sélectionnez les cibles auxquelles vous souhaitez retirer le script. Pour cela, utilisez le bouton Select All (Tout sélectionner) ou cochez la case à gauche de chaque cible pour retirer le script à certaines seulement.
2. Cliquez sur Remove Connect Scripts pour retirer des scripts de connexion ou sur Remove Disconnect Scripts pour retirer des scripts de déconnexion.

Ajout de scripts

Remarque : Vous pouvez également ajouter des scripts créés en dehors de KX III et les importer sous forme de fichiers XML. Reportez-vous à **Importation et exportation de scripts** *(à la page 163).*

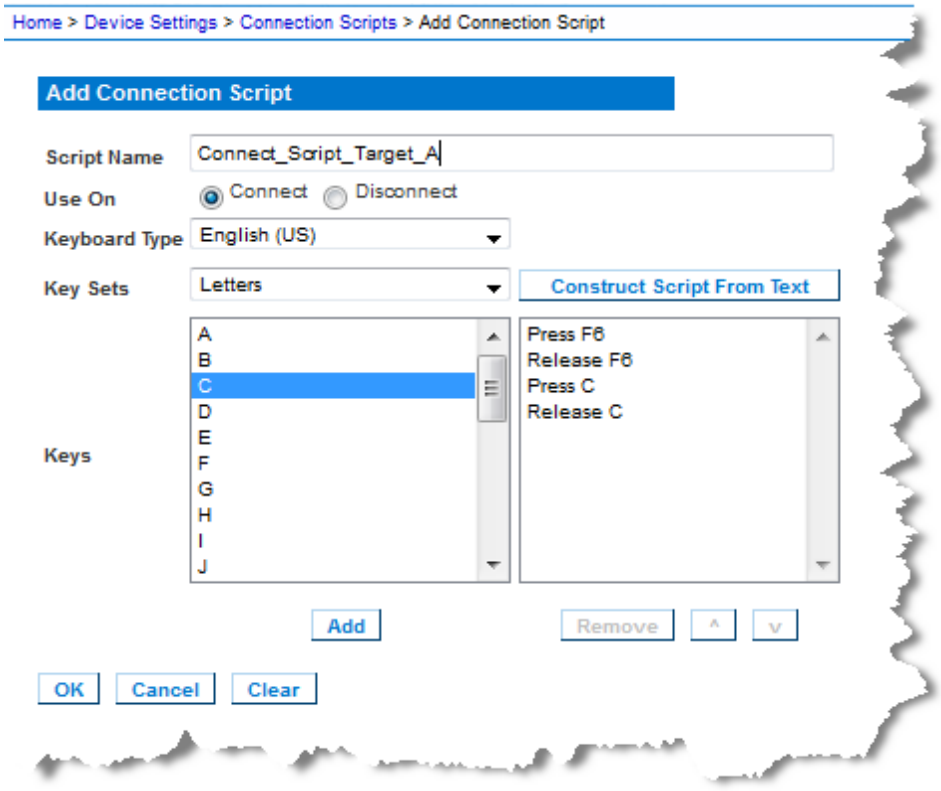
Pour créer un script :

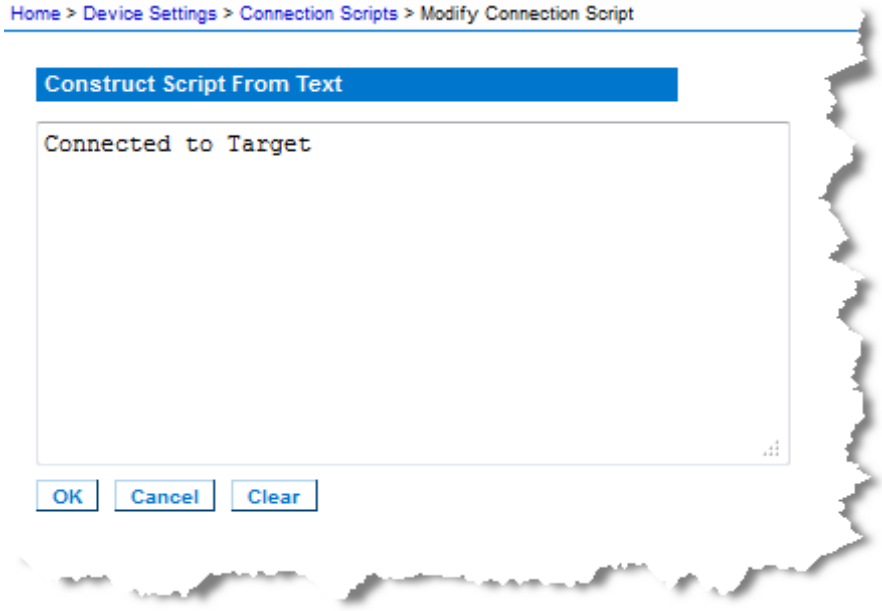
1. Cliquez sur Paramètres du dispositif > Scripts de connexion. La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), cliquez sur Add (Ajouter). La page Add Connection Scripts (Ajout de scripts de connexion) s'ouvre.

3. Entrez un nom de 32 caractères au maximum pour le script. Ce nom apparaît dans la section Available Connection Scripts (Scripts de connexion disponibles) de la page Configure Scripts (Configurer des scripts) une fois le script créé.
4. Sélectionnez le type de script que vous créez, Connect (Connexion) ou Disconnect (Déconnexion). Les scripts de connexion sont utilisés sur une nouvelle connexion ou lors du passage à une cible.
5. Sélectionnez le type de clavier requis pour la cible que vous utilisez.
6. Dans la liste déroulante Key Sets (Jeux de touches), choisissez les jeux de touches de clavier que vous souhaitez utiliser pour créer le script. Le champ Add (Ajout) sous la liste déroulante Key Sets est alimenté à l'aide des options de jeux de touches sélectionnés.
7. Sélectionnez une touche dans le champ Add et cliquez sur Add (Ajouter) pour la placer dans le champ Script. Pour supprimer une touche du champ Script, sélectionnez-le en cliquant sur Remove (Retirer). Réorganisez les touches en les sélectionnant et en utilisant les icônes Up (Haut) et Down (Bas).

   Le script peut être constitué d'une ou de plusieurs touches. En outre, vous pouvez combiner les touches à utiliser dans le script.

   Par exemple, sélectionnez F1-F16 pour afficher le jeu de touches de fonction dans le champ Add (Ajouter). Sélectionnez une touche de fonction et ajoutez-la au champ Script. Sélectionnez ensuite Letters (Lettres) dans la liste déroulante Key Sets (Jeux de touches) et ajoutez une touche alphabétique au script.
8. Le cas échéant, ajoutez le texte qui s'affichera à l'exécution du script.
   a. Cliquez sur Construct Script From Text (Construire un script à partir du texte) pour ouvrir la page correspondante.
   b. Entrez le script dans la zone de texte. Par exemple, entrez Connecté à la cible.
   c. Cliquez sur OK dans la page Construct Script From Text.
9. Cliquez sur OK pour créer le script.


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
^
v
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

Modification des scripts

Pour modifier des scripts existants :

1. Cliquez sur Paramètres du dispositif > Scripts de connexion. La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à modifier et cliquez sur Modify. La page est maintenant en mode d'édition.
3. Effectuez les changements nécessaires. Cliquez sur OK lorsque vous avez terminé.

Importation et exportation de scripts

Vous pouvez importer et exporter les scripts de connexion et de déconnexion qui sont au format de fichier XML. Les macros de clavier ne peuvent être ni importées ni exportées.

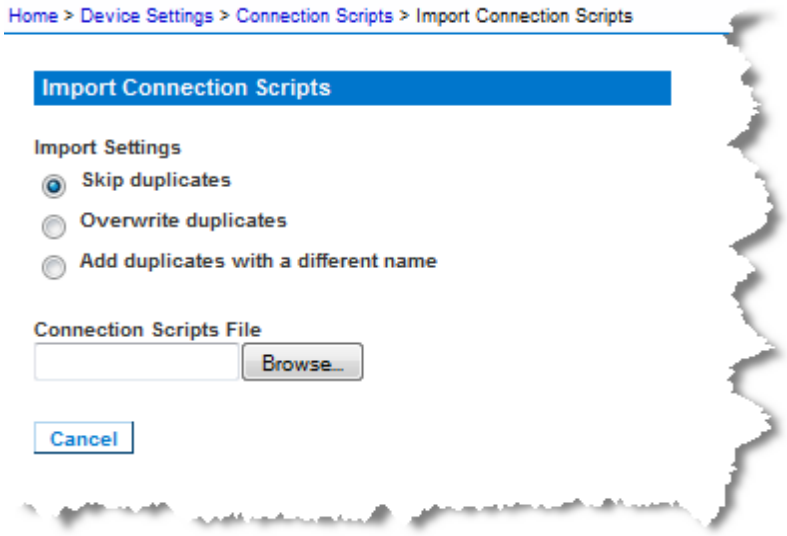
Remarque : La fonction d'importation et d'exportation n'est pas disponible depuis la console locale.

Les scripts importés peuvent être modifiés dans KX III à l'aide de la fonction Modifier. Toutefois, une fois qu'un script importé est associé à un port, il n'est plus modifiable. Retirez le script du port pour le modifier. Reportez-vous à ***Application et retrait des scripts*** (à la page 160).

Pour importer un script :

1. Cliquez sur Paramètres du dispositif > Scripts de connexion. La page Connection Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), cliquez sur Import (Importer). La page Import Connection Scripts (Importation de scripts de connexion) s'ouvre.
3. Sélectionnez le paramètre d'importation.
   - Omettre les doubles - les scripts existant déjà dans KX III ne sont pas inclus dans l'importation.
   - Ecraser les doubles : les scripts existant déjà dans KX III sont écrasés par le nouveau script importé.
   - Ajouter des doubles sous un nom différent : les scripts en double seront renommés au cours de l'importation et n'écraseront pas les scripts existants. KX III assigne un nombre au nom de fichier pour le distinguer de l'original.
4. Utilisez la fonction Parcourir pour localiser les fichiers de script XML à importer.

5. Cliquez sur Importer. La page Configuration Scripts (Scripts de configuration) s'ouvre et les scripts importés sont affichés.



Pour exporter un script de déconnexion :

1. Cliquez sur Paramètres du dispositif > Scripts de configuration. La page Configuration Scripts s'ouvre.
2. Dans la section Available Connection Scripts (Scripts de connexion disponibles), sélectionnez le script à exporter et cliquez sur Export. Une boîte de dialogue vous invitant à ouvrir ou à enregistrer le fichier XML apparaît.
3. Enregistrez le fichier XML ou ouvrez-le dans un éditeur XML. Si vous enregistrez le fichier XML, il est enregistré dans votre dossier Download par défaut.

Port Group Management (Gestion des groupes de ports)

La gestion des groupes de ports fait référence aux éléments suivants :

- Groupe de serveurs lames : agrégation des ports connectés à certains types de lames dans un groupe représentant le châssis de lames. Consultez ***Configuration des châssis de lames USC (Gestion des groupes de ports)*** (voir "***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports).***" à la page 117)pour plus de détails.
- Groupe de deux ports vidéo : création de groupes de ports offrant des configurations de bureau étendu sur les serveurs cible. Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 167).
- Groupe de ports : création de groupes de ports « standard » où des paramètres concernant un port principal sont appliqués à tous les ports secondaires du groupe. Reportez-vous à ***Création de groupes de ports*** (à la page 165).

Création de groupes de ports

KX III prend en charge l'agrégation de plusieurs ports dans un même groupe. Les groupes de ports sont constitués uniquement de ports configurés comme ports KVM standard. Un port ne peut être membre que d'un seul groupe.

Les ports pouvant être inclus dans un groupe de ports sont affichés dans Sélectionner un Port pour Groupe > liste Disponible. Une fois un port ajouté à un groupe, il n'est plus disponible pour un autre. Vous devez le retirer de son groupe actuel pour l'utiliser dans un autre.

Les actions de connexion et de déconnexion exécutées depuis le port principal sont appliquées aux ports secondaires, hormis celles concernant la gestion de l'alimentation.

Les groupes de ports sont restaurés à l'aide de l'option Backup and Restore (Sauvegarde et restauration) (reportez-vous à ***Backup and Restore*** (voir "***Backup and Restore (Sauvegarde et restauration)***" à la page 192) (Sauvegarde et restauration)).

Remarque : Consultez **Configuration des châssis de lames HP et Cisco (Gestion des groupes de ports)** *(voir "***Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports).***" à la page 117) pour plus d'informations sur la création de groupes de ports pour un châssis de lames, et Création de groupes de deux ports vidéo pour plus d'informations à ce sujet.*

Pour créer un groupe de ports :

1. Sélectionnez Paramètres du dispositif > Gestion des groupes de ports. La page Port Group Management (Gestion des groupes de ports) s'ouvre. Les groupes de ports existants sont affichés.

2. Cliquez sur Add (Ajouter). La page est rafraîchie et affiche toutes les options de groupes de ports disponibles.
3. Sélectionnez le bouton radio Port Group (Groupe de ports).
4. Sélectionnez les ports à ajouter au groupe en cliquant dessus dans la zone de texte Available (Disponible), puis sur Add pour l'ajouter à la zone de texte Selected (Sélectionné).
5. Cliquez sur OK pour créer le groupe de ports. Le groupe de ports apparaît maintenant sur la page Port Group Management (Gestion des groupes de ports).

Création d'un groupe de deux ports vidéo

La fonction des groupes de deux ports vidéo vous permet de réunir deux ports vidéo dans un même groupe. Utilisez cette fonction lorsque vous devez vous connecter à un serveur doté de deux cartes/ports vidéo, et que vous souhaitez accéder aux deux ports simultanément depuis le même client distant.

Remarque : Les groupes de deux ports vidéo ne sont pas pris en charge par les modèles n'ayant qu'un seul canal KVM, tels que les modèles KX3-108 et KX3-116.

Remarque : Une fois le groupe de deux ports vidéo créé, il est disponible depuis la console locale, ainsi que depuis le client distant. Toutefois, le bureau étendu n'est pas pris en charge sur la console locale.

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

Chaque groupe doit contenir un port principal et un port secondaire. La configuration appliquée au port principal l'est également à tous les ports secondaires du groupe. Si un port est retiré du groupe, il est considéré indépendant et une nouvelle configuration peut lui être appliquée.

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

Au besoin, les sessions peuvent être lancées et visualisées depuis le client distant sur un ou plusieurs écrans.

Le paramètre d'orientation configuré sur le dispositif pour la cible doit correspondre à la configuration réelle du système d'exploitation de la cible.

Il est recommandé que le client connecté ait la même orientation d'écran dès que possible.

Important : Consultez les informations de la section Groupes de deux ports vidéo pour prendre connaissance des restrictions, recommandations, etc. pouvant affecter votre environnement.

Pour créer un groupe de deux ports vidéo :

1. Sélectionnez Paramètres du dispositif > Gestion des groupes de ports. La page Port Group Management (Gestion des groupes de ports) s'ouvre. Les groupes de ports existants sont affichés.

2. Cliquez sur Add (Ajouter). La page Port Group (Groupe de ports) s'ouvre et tous les ports disponibles apparaissent dans la section Select Ports for Group (Sélectionner des ports pour le groupe).

Remarque : Si un port appartient déjà à un groupe de ports de serveur lame, à un autre groupe de deux ports vidéo ou à un groupe de ports « standard », il ne peut pas être sélectionné. En effet, les ports ne peuvent appartenir qu'à un seul groupe de ports à la fois.

3. Sélectionnez le bouton radio Dual Video Port Group (Groupe de deux ports vidéo).
4. Dans la section Select Ports for Group (Sélectionner des ports pour le groupe), cliquez sur le port désigné comme port principal, puis sur Add pour l'ajouter à la zone de texte Selected (Sélectionné). Veillez à ajouter le port principal en premier.

Remarque : idéalement, les autorisations appliquées à chaque port du groupe doivent être les mêmes. Sinon, les autorisations les plus restrictives d'un port s'appliquent au groupe. Par exemple, si l'option VM Access Deny (Refus d'accès VM) est appliquée à un port et l'option VM Access Read-Write (Accès en lecture-écriture VM) à un autre, la première est appliquée au groupe de ports. Reportez-vous à **Autorisations et accès aux groupes de deux ports vidéo** *(à la page 225) pour savoir comment les autorisations des ports affectent les groupes de deux ports vidéo.*

5. Cliquez sur le port désigné comme port secondaire, puis sur Add pour l'ajouter à la zone de texte Selected.
6. Sélectionnez l'orientation de la page. Sélectionnez l'orientation la mieux adaptée à la configuration de l'écran.
7. Cliquez sur OK pour créer le groupe de ports.

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

Remarque : Les cibles des groupes de deux ports vidéo liés à un dispositif en niveau doivent être accessibles uniquement via ce dispositif et non via le dispositif en niveau de base.

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

L'interface utilisateur de KX III est en anglais par défaut mais prend également en charge les langues suivantes :

- Japonais
- Chinois simplifié
- Chinois traditionnel

Pour modifier la langue de l'interface utilisateur :

1. Sélectionnez Paramètres du dispositif > Date/heure. 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 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.

Gestion de la sécurité

Security Settings (Paramètres de sécurité)

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

Les certificats SSL Raritan sont utilisés pour des échanges de clés publiques et privées. Ils fournissent un niveau de sécurité supplémentaire. Les certificats de serveur Web Raritan sont auto-signés. Les certificats d'applet Java sont signés par VeriSign. Le chiffrement garantit la sécurité de vos informations en les protégeant contre l'interception frauduleuse. Ces certificats garantissent que l'entité est bien Raritan, Inc.

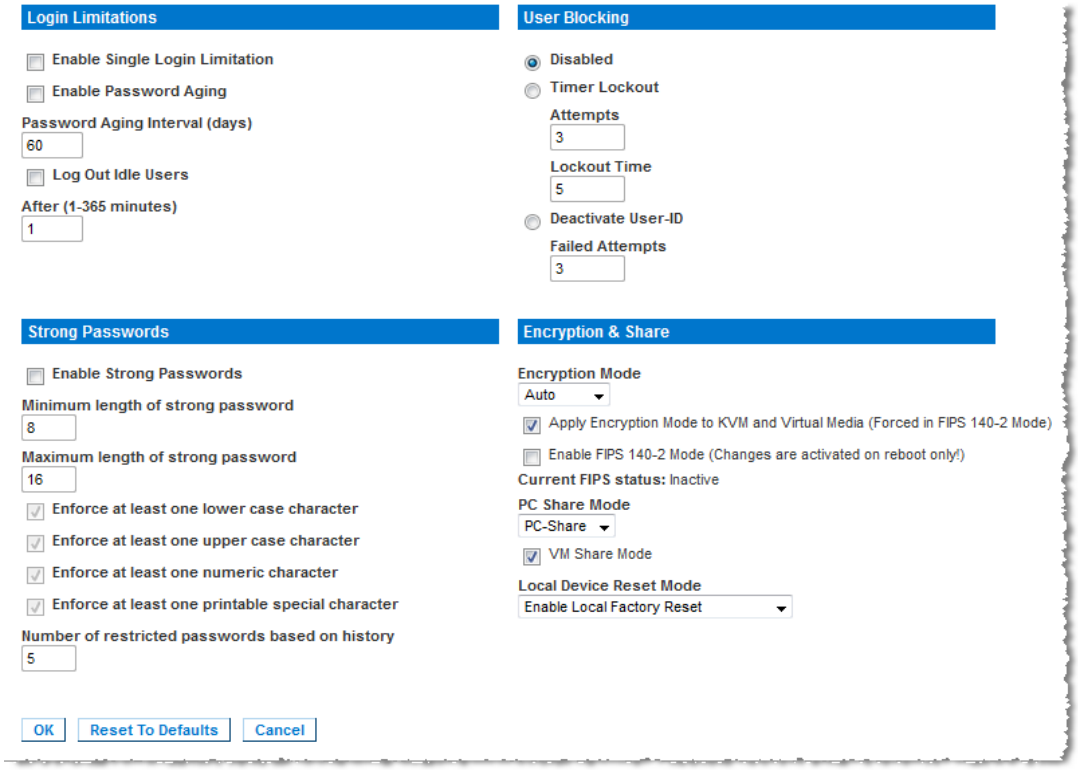
Pour configurer les paramètres de sécurité :

1. Sélectionnez Security > Security Settings (Sécurité > Paramètres de sécurité). La page Security Settings (Paramètres de sécurité) s'ouvre.
2. Mettez à jour les paramètres de ***limitations de connexion*** (à la page 170) en fonction de vos besoins.
3. Mettez à jour les paramètres de ***mots de passe sécurisés*** (à la page 172) en fonction de vos besoins.

4. Mettez à jour les paramètres de ***blocage des utilisateurs*** (à la page 173) 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).

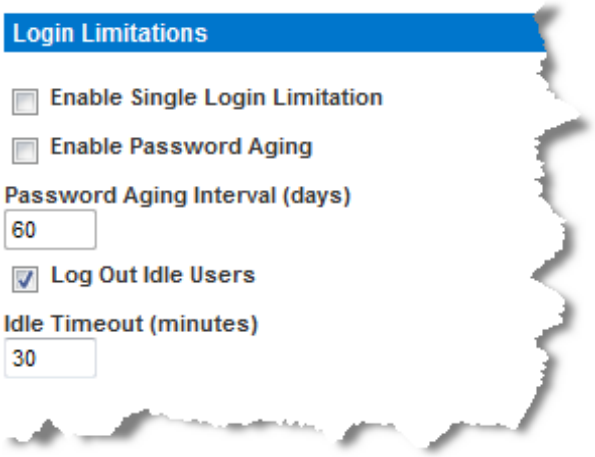


Limitations de connexion

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)	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). Ce champ est activé et obligatoire lorsque la case Enable Password Aging (Activer le vieillissement du mot de passe) est cochée. Entrez le nombre de jours après lequel une modification de mot de passe est requise. Le nombre par défaut est 60 jours.
Log off idle users, After (1-365 minutes) (Déconnecter les utilisateurs inactifs, Après)	Cochez la case Log off idle users pour déconnecter automatiquement les utilisateurs après le délai spécifié dans le champ After (1-365 minutes). En l'absence d'activité du clavier ou de la souris, toutes les sessions et toutes les ressources sont déconnectées. En revanche, si une session de support virtuel est en cours, elle n'expire pas. Le champ After (Après) permet de définir le délai (en minutes) après lequel un utilisateur inactif est déconnecté. Ce champ est activé lorsque l'option Log Out Idle Users (Déconnecter les utilisateurs inactifs) est sélectionnée. La valeur saisie dans le champ peut aller jusqu'à 365 minutes.



Mots de passe sécurisés

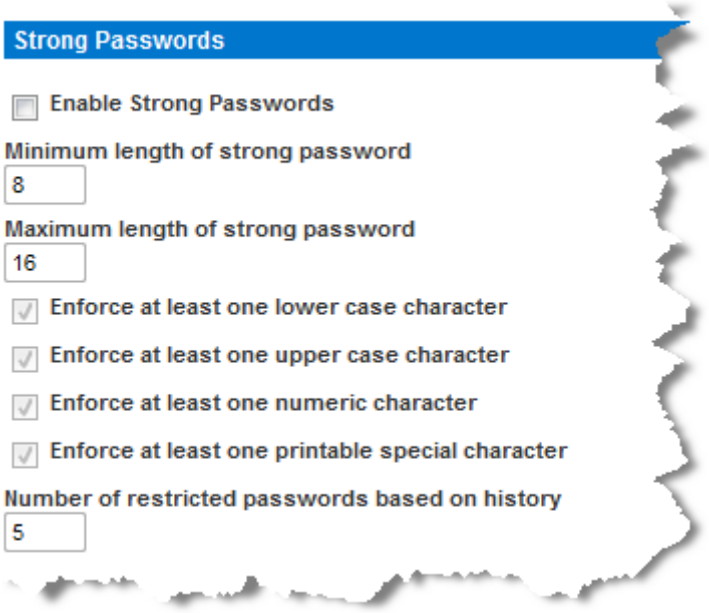
Les mots de passe sécurisés fournissent une authentification locale du système accrue. Utilisez les mots de passe sécurisés pour spécifier le format des mots de passe locaux valides de KX III, tel que la longueur minimum et maximum, les caractères obligatoires et la conservation de l'historique des mots 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.



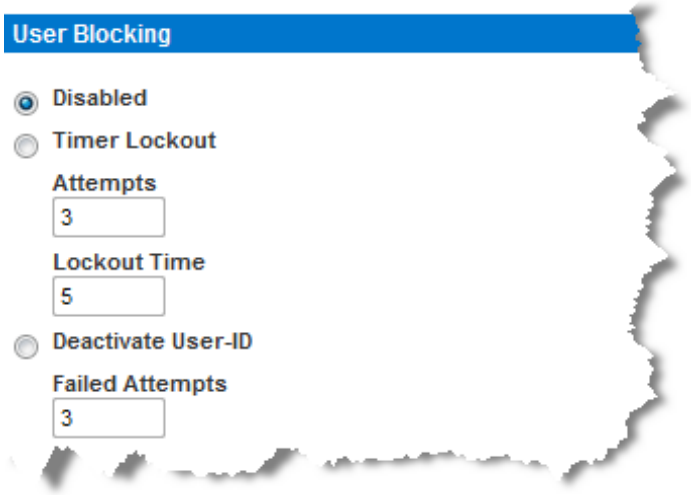
Blocage des utilisateurs

Les options de blocage d'utilisateurs spécifient les critères selon lesquels les utilisateurs se voient refuser l'accès au système après un nombre spécifique d'échecs de connexion.

Les trois options s'excluent les unes les autres :

Option	Description
Disabled (Désactivé)	Il s'agit de l'option par défaut. Les utilisateurs ne sont pas bloqués quel que soit le nombre d'échecs d'authentification.

Option	Description
Timer Lockout (Période de verrouillage)	Les utilisateurs se voient refuser l'accès au système après avoir dépassé le nombre d'échecs de connexion autorisé. Lorsque cette option est sélectionnée, les champs suivants sont activés : ▪ Attempts (Tentatives) - Il s'agit du nombre d'échecs de connexion après lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 10, la valeur par défaut étant 3 tentatives. ▪ Lockout Time (Durée de verrouillage) - Il s'agit du laps de temps pendant lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 1 440 minutes, la valeur par défaut étant 5 minutes. *Remarque : les utilisateurs dotés du rôle Administrateur ne sont pas concernés par les paramètres de période de verrouillage.*
Deactivate User-ID (Désactiver l'ID de l'utilisateur)	Sélectionnée, cette option indique que l'utilisateur ne peut plus accéder au système après un nombre spécifique de tentatives de connexion échouées, défini dans le champ Failed Attempts (Tentatives échouées) : ▪ Failed Attempts (Tentatives échouées) - Il s'agit du nombre d'échecs de connexion après lequel l'ID de l'utilisateur est désactivé. Le champ est activé lorsque l'option Deactivate User-ID (Désactiver l'ID de l'utilisateur) est sélectionnée. Les valeurs autorisées sont comprises entre 1 et 10. Lorsque l'ID d'un utilisateur est désactivé suite à un nombre spécifique d'échecs de connexion, l'administrateur doit modifier le mot de passe de l'utilisateur et activer le compte de celui-ci en cochant la case Active (Actif) dans la page User (Utilisateur).



Cryptage & 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 III 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 III.

Configurer le Cryptage & Partage

Notez que la performance peut être impactée une fois que l'encryption est appliquée. L'étendue de l'impact sur les performances dépend du mode de chiffrement.

Pour les meilleures performances vidéo possibles et rendu, désactiver le chiffrement si votre politique de sécurité le permet.

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 III.

   L'avertissement indique « 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 III. »

Mode de chiffrement	Description
Auto	Il s'agit de l'option recommandée. Le KX III négocie automatiquement au niveau le plus élevé de chiffrement possible. Vous *devez* sélectionner Auto pour que le dispositif et le client négocient avec succès l'utilisation des algorithmes compatibles FIPS.
RC4	Permet de sécuriser les noms d'utilisateur, les mots de passe et les données KVM, notamment les transmissions vidéo, à l'aide de la méthode de chiffrement RSA RC4. Le protocole Secure Socket Layer (SSL) à 128 bits fournit un canal de communication privé entre le dispositif KX III et l'ordinateur distant lors de l'authentification de la connexion initiale. Si vous activez le mode FIPS 140-2 et que RC4 est sélectionné, vous recevrez un message d'erreur. RC4 n'est pas disponible en mode FIPS 140-2.
AES-128	La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 128). Si l'option AES-128 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 179) pour plus d'informations.
AES-256	La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 256). Si l'option AES-256 est sélectionnée, assurez-vous que votre navigateur la prend en charge, sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de***

Mode de chiffrement	Description
	la prise en charge du chiffrement AES par votre navigateur (à la page 179) pour plus d'informations.

Remarque : Si vous exécutez Windows XP® avec le Service Pack 2, Internet Explorer 7 ne peut pas se connecter à distance à KX III 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 179) pour en savoir plus à ce sujet.
4. PC Share Mode - Détermine l'accès KVM à distance simultané global, permettant ainsi à huit utilisateurs distants au maximum de se connecter simultanément à une unité KX III 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 III à l'aide du bouton de réinitialisation. 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 III retrouve les paramètres d'usine par défaut.
Enable Local Admin Password Reset (Activer la réinitialisation locale du mot de passe administrateur)	Permet de réinitialiser le mot de passe d'administrateur local uniquement. Le mot de passe raritan est rétabli.
Disable All Local Resets (Désactiver toutes les réinitialisations locales)	Aucune action de réinitialisation n'est entreprise.

Remarque : Lors de l'utilisation de P2CIM-AUSBDUAL ou P2CIM-APS2DUAL est utilisé pour connecter une cible à deux KX III, si l'accès Privé aux cibles est requis, le mode de partage PC des deux commutateurs KVM doit être défini sur Privé.

Reportez-vous à **CIM Paragon et configurations pris en charge** *(voir "***Configurations et CIMs Paragon II pris en charge***" à la page 315) pour plus d'informations sur l'utilisation des CIM Paragon avec KX III.*

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

Si vous ne savez pas si votre navigateur utilise AES, vérifiez auprès de son fabricant ou ouvrez le site Web https://www.fortify.net/sslcheck.html dans le navigateur comportant la méthode de chiffrement que vous souhaitez vérifier. Ce site Web détecte la méthode de chiffrement de votre navigateur et affiche un rapport.

Le chiffrement AES 256 bits est pris en charge uniquement sur les navigateurs Web suivants :

- Firefox®
- Internet Explorer®

Outre la prise en charge par le navigateur utilisé, le chiffrement AES 256 bits nécessite l'installation des fichiers Java™ Cryptography Extension (JCE®) à niveau illimité.

Les fichiers de jurisdiction pour divers JREs™ sont disponibles dans la section « autres téléchargements » du lien suivant :

- 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 peut être requise.

Le KX III utilise un module cryptographique FIPS 140-2 validé 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.

Notez que la performance peut être impactée une fois que le mode FIPS 140-2 est activé.

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 Activer FIPS 140-2 dans la section Cryptage et partage de la page Paramètres de sécurité.

   Vous utiliserez alors les algorithmes approuvés FIPS 140-2 pour les communications externes.

   Le module cryptographique FIPS sert au cryptage du trafic de session KVM constitué de données vidéo, de clavier, de souris, de support virtuel et de carte à puce.
3. Redémarrez le KX III. **Obligatoire**

Une fois le mode FIPS activé, la mention 'FIPS Mode: Activé' apparaît dans la section 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 III.

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

KX III prend en charge l'utilisation des algorithmes de chiffrement approuvés FIPS 140-2. 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 III figurent ci-après :

KX III

- 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 régulez l'accès à votre KX III. Notez que le contrôle de l'accès par IP empêche n'importe quel trafic d'accéder à KX III ; l'accès à ce dispositif doit donc être accordé aux serveurs NTP, hôtes RADIUS, hôtes DNS, etc.

Le fait de configurer une liste de contrôle d'accès (LCA) globale permet de garantir que votre dispositif ne répondra pas aux paquets envoyés à partir d'adresses IP non autorisées. Le contrôle d'accès IP est global et affecte l'ensemble du dispositif KX III. Cependant, vous pouvez également contrôler l'accès à votre dispositif au niveau du groupe. Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 63) pour plus d'informations sur le contrôle au niveau du groupe.

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de KX III. Lorsque vous créez une liste de contrôle d'accès IP, 127.0.0.1 ne doit pas figurer dans la plage des adresses IP bloquées ou vous n'aurez plus accès au port local de KX III.

Pour utiliser le contrôle d'accès IP :

1. Sélectionnez Security (Sécurité) > IP Access Control pour ouvrir la page IP Access Control (Contrôle d'accès IP).
2. Sélectionnez la case Enable IP Access Control (Activer le contrôle de l'accès par IP) et les champs restants de la page.
3. Sélectionnez la stratégie par défaut (Default Policy). Cette action concerne les adresses IP qui ne figurent pas dans les plages spécifiées.
   - Accept (Accepter) - Les adresses IP sont autorisées à accéder au dispositif KX III.
   - Drop (Abandonner) - Les adresses IP ne sont pas autorisées à accéder au dispositif KX III.

Pour ajouter des règles :

1. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).

Remarque : l'adresse IP doit être saisie à l'aide de la notation CIDR (Classless Inter-Domain Routing, dans laquelle les 24 premiers bits sont utilisés comme adresse réseau).

2. Sélectionnez la stratégie dans la liste déroulante Policy.
3. Cliquez sur Append (Ajouter). La règle est ajoutée au bas de la liste des règles.

Pour insérer une règle :

1. Tapez un numéro de règle (Rule #). Un numéro de règle est requis lorsque vous utilisez la commande Insert (Insérer).
2. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).
3. Sélectionnez la stratégie dans la liste déroulante Policy.
4. Cliquez sur Insert (Insérer). Si le numéro de règle que vous venez d'entrer est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont descendues d'un rang.

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

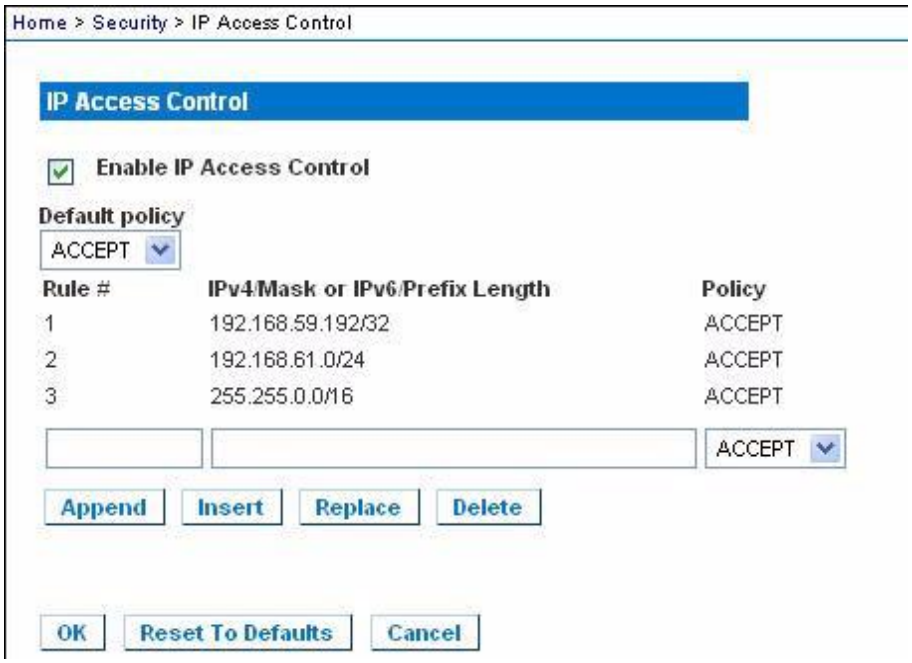
Pour remplacer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez remplacer.
2. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).
3. Sélectionnez la stratégie dans la liste déroulante Policy.
4. Cliquez sur Replace (Remplacer). Votre nouvelle règle remplace la règle d'origine portant le même numéro.

Pour supprimer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).

3. Vous êtes invité à confirmer la suppression. Cliquez sur OK.



Certificats SSL

KX III utilise le protocole SSL (Secure Socket Layer) pour tout trafic réseau chiffré entre lui-même et un client connecté.

A l'établissement d'une connexion, KX III doit s'identifier auprès d'un client à l'aide d'un certificat de cryptage.

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 III.

L'autorité vérifie l'identité de l'auteur de la demande.

L'autorité renvoie 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 III soient définies correctement.

Lorsqu'un certificat auto-signé est créé, la date et l'heure de KX III sont utilisées pour calculer la période de validité. Si la date et l'heure de KX III sont incorrectes, 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 148).

Remarque : La demande de signature du certificat (CSR) doit être générée sur KX III.

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 Securité > Certificat.
2. Remplissez les champs suivants :
   a. Common name (Nom courant) - Il s'agit du nom réseau de KX III 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 III 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 III 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 III appartient.
   c. Organization (Organisation) - Il s'agit du nom de l'organisation à laquelle KX III 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). Applicable lors de la génération d'une demande de signature du certificat (CSR) pour la certification par l'autorité.

h. Confirm Challenge Password (Confirmer le mot de passe challenge) - Il s'agit de la confirmation du mot de passe challenge. Applicable lors de la génération d'une demande de signature du certificat (CSR) pour la certification par l'autorité.

i. Email (Courriel) - Il s'agit de l'adresse électronique d'un contact responsable du dispositif KX III 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. Pour la générer, effectuez une des opérations suivantes :

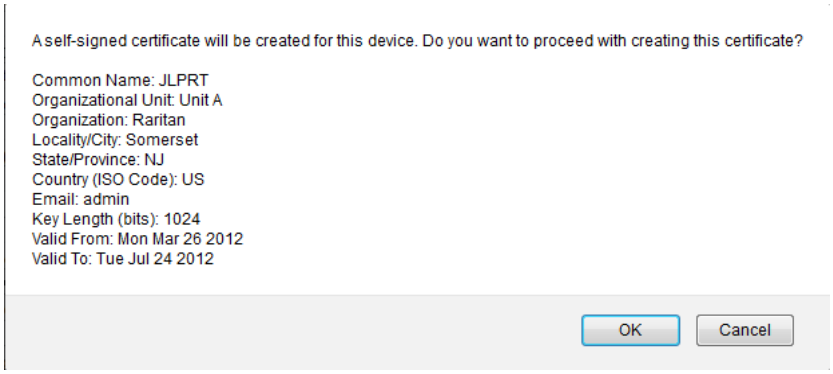
- Pour générer un certificat auto-signé, procédez comme suit :

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 III 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 III 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.

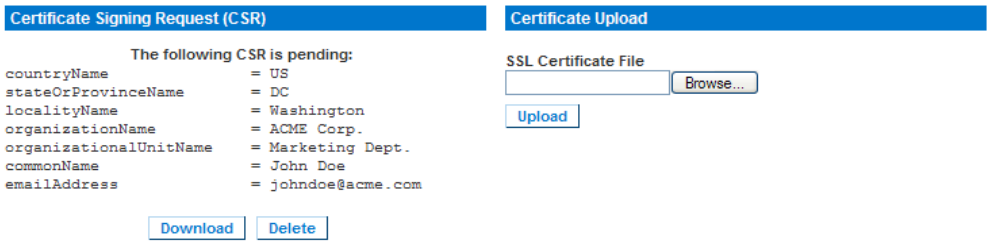


e. Redémarrez KX III pour activer le certificat auto-signé.

- Pour générer une demande de signature de certificat à envoyer à l'autorité pour certification:

a. Cliquez sur Create (Créer).

b. Une boîte de dialogue contenant toutes les informations que vous avez entrées apparaît.



c. La demande de signature de certificat et le fichier contenant la clé privée utilisée lors de sa génération peuvent être téléchargés en cliquant sur Download CSR (Télécharger CSR).

d. Envoyez la demande enregistrée à une autorité de certification pour confirmation. Vous recevrez le nouveau certificat de l'autorité de certification.

Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.

- Une fois que vous obtenez le certificat de la part de l'autorité, téléchargez-le au KX III en cliquant sur Upload.
- Redémarrez KX III pour activer le certificat.

Une fois ces étapes effectuées, KX III 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 III, 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

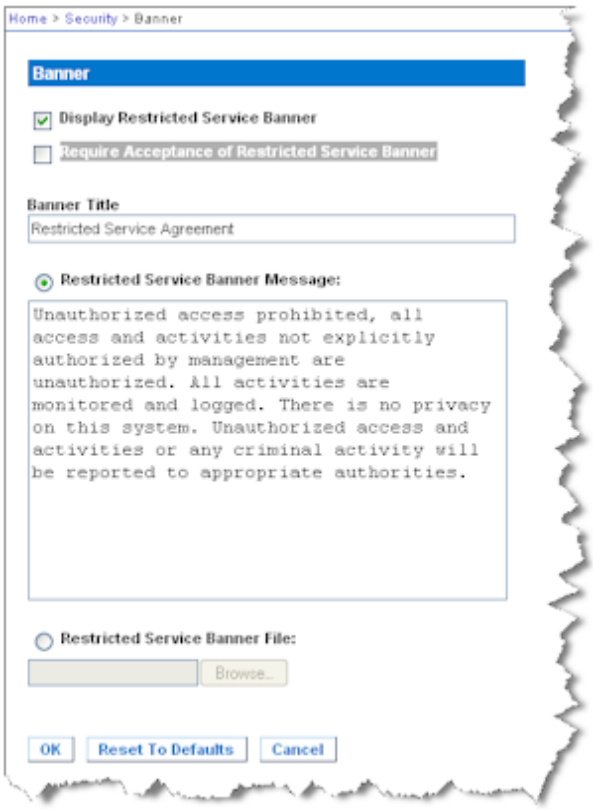
KX III vous offre la possibilité d'ajouter une bannière de sécurité au processus de connexion de KX III. Cette fonction oblige les utilisateurs à accepter ou à refuser un accord de sécurité avant d'accéder au KX III. Les informations fournies dans une bannière de sécurité seront affichées dans une boîte de dialogue Restricted Service Agreement (Accord de services limités) après que les utilisateurs auront accédé à KX III 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 III ou elle peut être uniquement affichée après le processus de connexion. Si la fonction d'acceptation ou de refus est activée, la sélection de l'utilisateur est consignée dans le journal d'audit.

Pour configurer une bannière de sécurité :

1. Cliquez sur Security > Banner (Sécurité > Bannière) pour ouvrir la page Banner.
2. Cochez la case Display Restricted Service Banner (Afficher la bannière de services limités) pour activer la fonction.
3. Pour obliger les utilisateurs à prendre acte de la bannière avant de poursuivre le processus de connexion, sélectionnez Require Acceptance of Restricted Service Banner (Exiger l'acceptation de la bannière de services limités). Pour prendre acte de la bannière, les utilisateurs cocheront une case. Si vous n'activez pas ce paramètre, la bannière de sécurité n'apparaîtra qu'après la connexion de l'utilisateur et ne l'obligera à la reconnaître.
4. Le cas échéant, modifiez le titre de la bannière. Ces informations apparaîtront aux utilisateurs dans le cadre de la bannière. Vous pouvez entrer jusqu'à 64 caractères.
5. Modifiez les informations de la zone de texte Restricted Services Banner Message (Message de la bannière de services limités). Vous pouvez entrer jusqu'à 6000 caractères ou les télécharger depuis un fichier texte. Pour ce faire, effectuez l'une des opérations suivantes :
   a. Modifiez le texte en tapant dans la zone de texte. Cliquez sur OK.
   b. Téléchargez les informations d'un fichier .txt en sélectionnant le bouton radio Restricted Services Banner File (Fichier de la bannière de services limités) et en utilisant la fonction Parcourir pour localiser et téléverser le fichier. Cliquez sur OK. Une fois le fichier téléversé, son texte apparaîtra dans la zone de texte Restricted Services Banner Message.

Remarque : Vous ne pouvez pas téléverser de fichier texte depuis le port local.



Maintenance

Journal d'audit

Un journal des événements du système KX III est créé. Le journal d'audit peut contenir jusqu'à 2 Ko de données avant de commencer à écraser les entrées les plus anciennes. Pour éviter de perdre des données de journal d'audit, exportez-les sur un serveur syslog ou un gestionnaire SNMP. Configurez le serveur syslog ou le gestionnaire SNMP depuis la page Device Settings > Event Management (Paramètres du dispositif > Gestion des événements). Reportez-vous à ***Evénements capturés dans le journal d'audit et dans Syslog*** (à la page 355) pour plus d'informations sur ce qui est capturé dans le journal d'audit et dans syslog.

Pour consulter le journal d'audit de votre unité KX III :

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

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

- Date : date et heure auxquelles l'événement s'est produit (système de 24 heures).
- Event : nom de l'événement tel que répertorié dans la page Event Management (Gestion des événements).
- Description : description détaillée de l'événement.

Pour enregistrer le journal d'audit :

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

1. Cliquez sur Save to File (Enregistrer dans le fichier). Une boîte de dialogue Save File (Enregistrer le fichier) apparaît.
2. Choisissez le nom et l'emplacement du fichier, puis cliquez sur Save (Enregistrer). Le journal d'audit est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour naviguer dans le journal d'audit :

- Utilisez les liens [Older] (Plus ancien) et [Newer] (Plus récent).

Device Information (Informations sur le dispositif)

La page d'informations sur le dispositif fournit des informations détaillées sur votre dispositif KX III et sur les CIM en cours d'utilisation. Ces informations sont utiles si vous avez besoin de contacter l'assistance technique Raritan.

Pour afficher les informations sur votre KX III et ses CIM :

- Sélectionnez Maintenance > Informations relatives au dispositif. La page des informations relatives au dispositif s'ouvre.

Les informations suivantes relatives à KX III sont fournies :

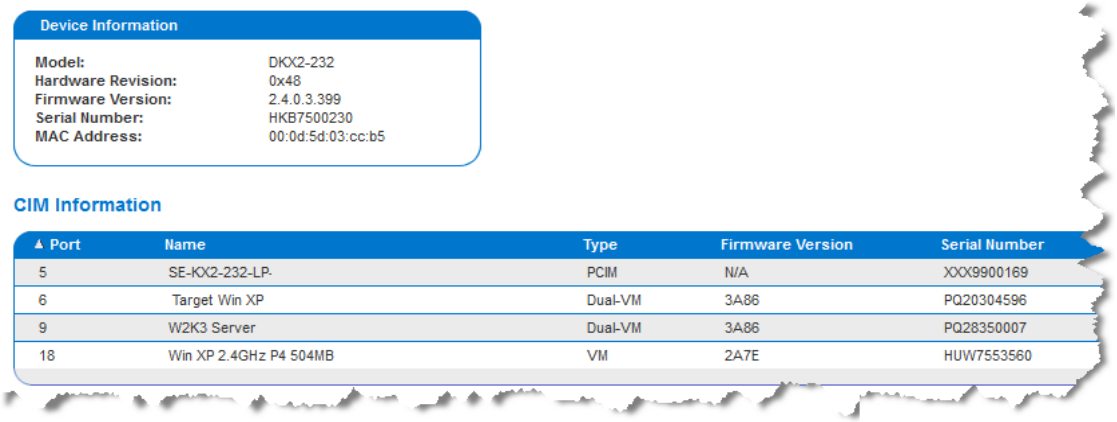
- Modèle
- Numéro de version du matériel
- Version de firmware
- Numéro de série
- Adresse MAC

Les informations suivantes relatives aux CIM en cours d'utilisation sont fournies :

- (Numéro de) port
- Nom
- Type of CIM - DCIM, PCIM, PDU de rack, VM, DVM-DP, DVM-HDMI, DVM-DVI
- Version de firmware
- Numéro de série du CIM - ce numéro provient directement des CIM pris en charge.
  - P2CIM-PS2
  - P2CIM-APS2DUAL
  - P2CIM-AUSBDUAL
  - P2CIM-AUSB
  - P2CIM-SUN
  - P2CIM-SUSB
  - P2CIM-SER
  - DCIM-PS2
  - DCIM-USB
  - DCIM-USBG2
  - DCIM-SUN
  - DCIM-SUSB

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB

Remarque : Seule la portion numérique des numéros de séries est affichée pour les CIMs DCIM-USB, DCIM-PS2 et DCIM-USB. Par exemple, XXX1234567 est affiché. Le préfixe GN du numéro de série est affiché pour les CIM qui ont un numéro de série configuré.



Backup and Restore (Sauvegarde et restauration)

A partir de la page de sauvegarde/restauration, vous pouvez sauvegarder et restaurer les paramètres et la configuration de votre KX III.

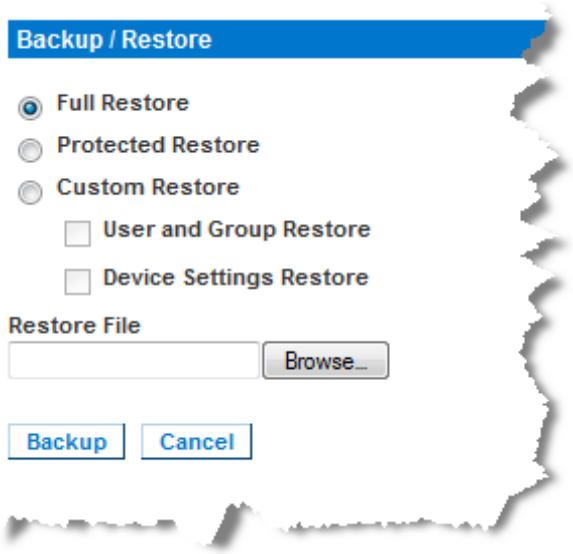
Outre l'utilisation de la sauvegarde et de la restauration pour la continuité des opérations, vous pouvez utiliser cette fonction pour gagner du temps.

Par exemple, vous pouvez donner rapidement un accès à votre équipe à partir d'un autre KX III en sauvegardant les paramètres de configuration utilisateur du dispositif KX III en cours d'utilisation et en restaurant ces paramètres sur le nouveau KX III.

Vous pouvez également configurer un KX III et copier sa configuration dans plusieurs dispositifs KX III.

Pour accéder à la page de sauvegarde/restauration :

- Sélectionnez Maintenance > Sauvegarde/restauration. La page Backup/Restore (Sauvegarder/Restaurer) s'ouvre.



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

Si vous utilisez Internet Explorer 7 ou une version supérieure, pour restaurer votre KX III:

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 7 et supérieur, IE est utilisé comme application par défaut pour ouvrir les fichiers ; vous êtes donc invité à ouvrir le fichier au lieu de l'enregistrer. Pour éviter ce problème, vous devez remplacer l'application utilisée par défaut pour ouvrir les fichiers par Wordpad®.

2. Pour ce faire :
   a. Enregistrez le fichier de sauvegarde. Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.
   b. Une fois le fichier enregistré, localisez-le et cliquez dessus avec le bouton droit. Sélectionnez Propriétés.
   c. Dans l'onglet Général, cliquez sur Modifier et sélectionnez WordPad.

Pour restaurer votre KX III :

AVERTISSEMENT : Soyez prudent lorsque vous restaurez une version antérieure de votre KX III. 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 III.

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 III et de copier sa configuration dans plusieurs dispositifs KX III.
   - 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 III.
- Device Settings Restore (Restauration des paramètres du dispositif) - Cette option n'inclut que les paramètres du dispositif : associations d'alimentation, profils USB, paramètres de configuration relatifs au châssis de lames et les affectations de groupes de ports. Utilisez cette option pour copier rapidement les informations relatives au dispositif.

2. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
3. Localisez et sélectionnez le fichier de sauvegarde approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ Restore File (Restaurer le fichier).
4. Cliquez sur Restore (Restaurer). La configuration (en fonction du type de restauration sélectionnée) est restaurée.

USB Profile Management (Gestion des profils USB)

Depuis la page USB Profile Management, vous pouvez téléverser les profils personnalisés fournis par l'assistance technique Raritan. Ces profils sont conçus pour répondre aux besoins de la configuration du serveur cible, si l'ensemble de profils standard ne suffisait pas. L'assistance technique Raritan vous fournira le profil personnalisé et travaillera avec vous pour vérifier si les besoins spécifiques du serveur cible sont couverts.

Pour accéder à la page USB Profile Management :

- Choisissez > Maintenance > Gestion de Profil USB La page USB Profile Management s'ouvre.

Pour uploader un profil personnalisé à votre KX III:

1. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
2. Localisez et sélectionnez le fichier de profil personnalisé approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ USB Profile File (Fichier de profil USB).
3. Cliquez sur Upload (Téléverser). Le profil personnalisé sera téléversé et affiché dans le tableau Profile (Profil).

Remarque : Si une erreur ou un avertissement apparaît pendant le téléversement (par exemple, écrasement d'un profil personnalisé existant), vous pouvez poursuivre l'opération en cliquant sur Upload ou l'annuler en cliquant sur Cancel.

Pour supprimer un profil personnalisé de votre KX III :

1. Cochez la case correspondant à la rangée du tableau contenant le profil personnalisé à supprimer.
2. Cliquez sur Delete (Supprimer). Le profil personnalisé est supprimé et retiré du tableau Profile (Profil).

Comme indiqué, vous pouvez supprimer un profil personnalisé du système, alors qu'il est toujours désigné comme étant actif. Les éventuelles sessions Support virtuel en place seront alors interrompues.

Gestion des conflits dans les noms de profil

Un conflit d'appellation entre les profils USB personnalisés et standard peut se produire au cours d'une mise à niveau de firmware. Cela peut se produire si un profil personnalisé créé et incorporé à la liste des profils standard porte le nom d'un nouveau profil USB téléchargé dans le cadre de la mise à niveau du firmware.

Dans ce cas, le profil personnalisé préexistant sera marqué old_. Par exemple, si un profil personnalisé appelé GenericUSBProfile5 a été créé et un profil du même nom est téléchargé au cours d'une mise à niveau de firmware, le fichier existant sera alors appelé old_GenericUSBProfile5.

Le cas échéant, vous pouvez supprimer le profil existant. Reportez-vous à ***USB Profile Management (Gestion des profils USB)*** (à la page 195) pour plus d'informations.

Mise à niveau des CIM

Utilisez cette procédure pour mettre à niveau les CIM à l'aide des versions de firmware stockées dans la mémoire de votre dispositif KX III. En général, tous les CIM sont mis à niveau lorsque vous mettez à niveau le firmware du dispositif via la page Firmware Upgrade (Mise à niveau du firmware).

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

1. Sélectionnez Maintenance > Mise à niveau du firmware du CIM. La page CIM Upgrade from (Mise à niveau du CIM à partir de) s'ouvre.

   Le (numéro de) port, le nom, le type, la version actuelle du CIM et la mise à niveau de la version du CIM sont affichés pour faciliter l'identification des CIM.
2. Cochez la case Selected (Sélectionné) pour chacun des CIM que vous voulez mettre à niveau.
3. Cliquez sur Upgrade (Mise à niveau). Vous êtes invité à confirmer la mise à niveau.
4. Cliquez sur OK pour continuer la mise à niveau. Des barres de progression s'affichent lors de la mise à niveau. La mise à niveau prend environ 2 minutes (ou moins) par CIM.

Mettre à jour le firmware KX III

La page de Mise à niveau du firmware permet de mettre à niveau le firmware de votre KX III et de tous les CIM reliés. Cette page est disponible dans la Console à distance du KX III seulement.

Firmware Upgrade (Mise à niveau du firmware)

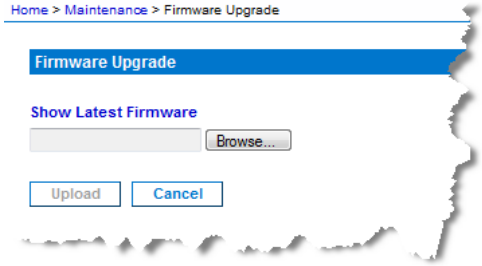
Important : Ne mettez pas votre unité de KX III hors tension et ne déconnectez pas les CIM pendant la mise à niveau ; cela risque fortement d'endommager l'unité ou les CIM.

Pour mettre à niveau votre unité KX III :

1. Localisez le fichier de distribution du firmware Raritan (*.RFP) sur la page des mises à niveau du firmware du ***site Web de Raritan http://www.raritan.com*** :
2. Décompressez le fichier. Lisez attentivement l'ensemble des instructions incluses dans les fichiers ZIP du firmware avant de procéder à la mise à niveau.

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

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



4. Cliquez sur le bouton Parcourir pour accéder au répertoire où vous avez décompressé le fichier de mise à niveau.
5. Cliquez sur Upload (Téléverser) dans la page de mise à niveau du firmware.

   Les informations concernant les numéros de mise à niveau et de version sont affichées pour votre confirmation (si vous avez opté pour la vérification des informations relatives au CIM, ces informations sont également affichées) :

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

6. Cliquez sur Upgrade (Mise à niveau). Patientez jusqu'à la fin de la mise à niveau. Des informations sur l'état et des barres de progression s'affichent pendant la mise à niveau. Une fois la mise à niveau terminée, l'unité redémarre (1 bip est émis pour signaler la fin du redémarrage).
7. Si vous y êtes invités, fermez le navigateur et attendez environ 5 minutes avant de vous connecter de nouveau à KX III.

Historique des mises à niveau

KX III fournit des informations sur les mises à niveau effectuées sur KX III et les CIM reliés.

Pour afficher l'historique des mises à niveau :

- Sélectionnez Maintenance > Upgrade History (Historique des mises à niveau). La page Upgrade History (Historique des mises à niveau) s'ouvre.

Les informations fournies concernent les mises à niveau de KX III exécutées, l'état final de la mise à niveau, les heures de début et de fin, et les versions de firmware précédente et courante. Des informations relatives aux CIM sont également fournies ; pour les obtenir, cliquez sur le lien show (afficher) correspondant à une mise à niveau. Les informations relatives aux CIM fournies sont les suivantes :

- Type - Type du CIM.
- Port - Indique le port sur lequel est connecté le CIM.
- User - Indique l'utilisateur qui a effectué la mise à niveau.
- IP - Indiquez l'adresse IP de l'emplacement du firmware.
- Start Time - Indique l'heure de début de la mise à niveau.
- End Time - Indique l'heure de fin de la mise à niveau.
- Previous Version - Indique la version précédente du firmware de CIM.
- Upgrade Version - Indique la version courante du firmware de CIM.
- CIMs - Indique les CIM mis à niveau.
- Result - Résultat de la mise à niveau (réussite ou échec).

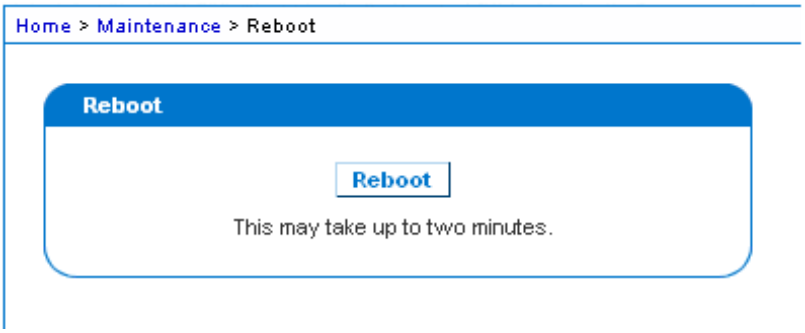
Redémarrage de KX III

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

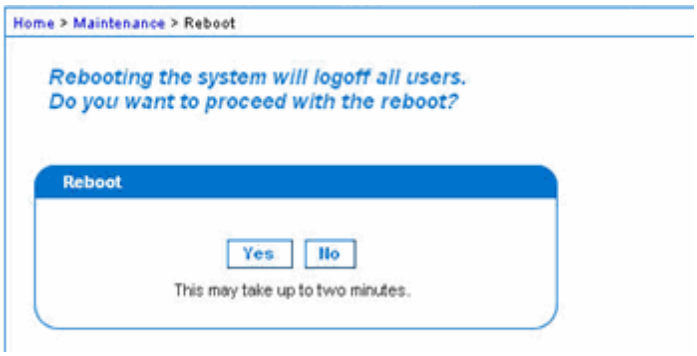
Important : toutes les connexions KVM et série sont fermées et tous les utilisateurs déconnectés.

Pour redémarrer votre KX III :

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

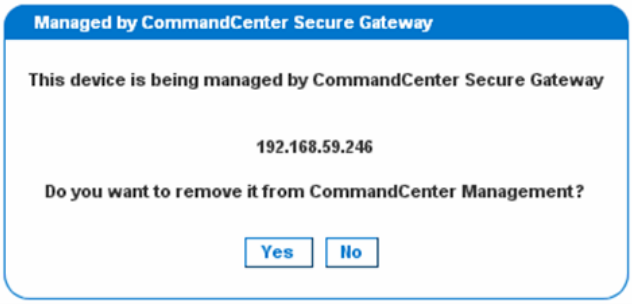
Pendant que KX III est géré par CC-SG, si vous tentez d'accéder au dispositif directement, vous êtes averti que CC-SG assure son contrôle.

Si vous gérez KX III via CC-SG et que la connectivité entre CC-SG et KX III 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 III.

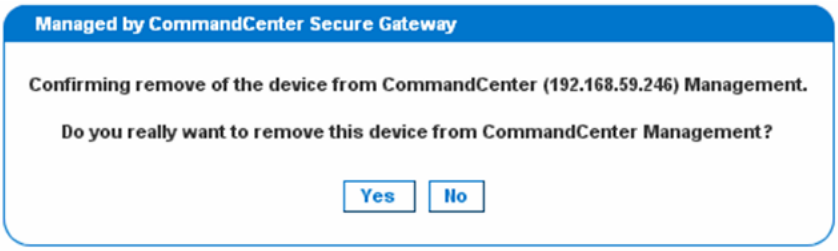
Remarque : Vous devez disposer des autorisations appropriées pour mettre fin à la gestion par CC-SG de KX III. En outre, l'option Stop CC-SG Management (Arrêter la gestion par CC-SG) n'est accessible que si vous utilisez actuellement CC-SG pour gérer KX III.

Pour arrêter la gestion de KX III par CC-SG :

1. Cliquez sur Maintenance > Arrêter la gestion par CC-SG. Un message indiquant que le dispositif est géré par CC-SG s'affiche. Une option permettant de retirer le dispositif de la gestion par CC-SG apparaît également.



2. Cliquez sur Yes (Oui) pour débuter le traitement de retrait du dispositif de la gestion par CC-SG. Un message apparaît alors vous demandant de confirmer le retrait du dispositif de la gestion par CC-SG.



3. Cliquez sur Yes (Oui) pour retirer le dispositif de la gestion par CC-SG. Une fois la gestion par CC-SG terminée, une confirmation apparaît.

Diagnostics

Page d'interface réseau

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

Pour afficher les informations relatives à votre interface réseau :

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

Les informations suivantes s'affichent :

- L'état de l'interface Ethernet est actif 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)

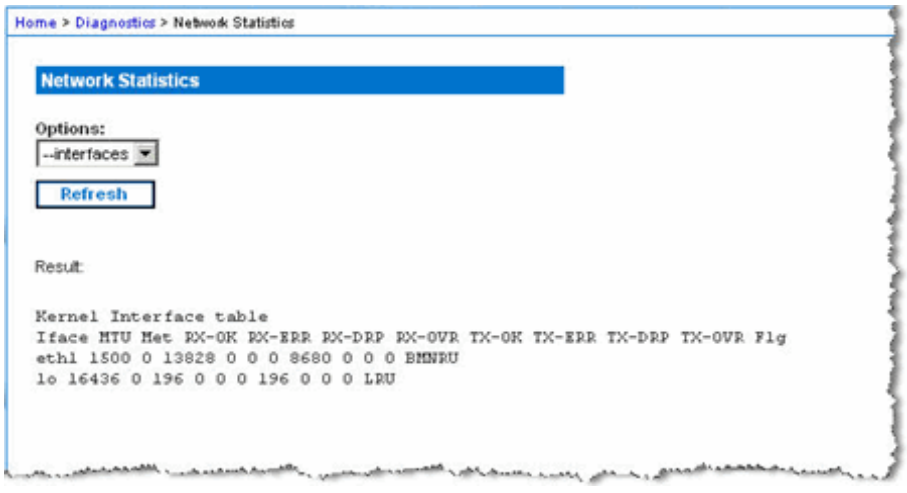
KX III fournit des statistiques sur votre interface réseau.

Pour afficher les statistiques relatives à votre interface réseau :

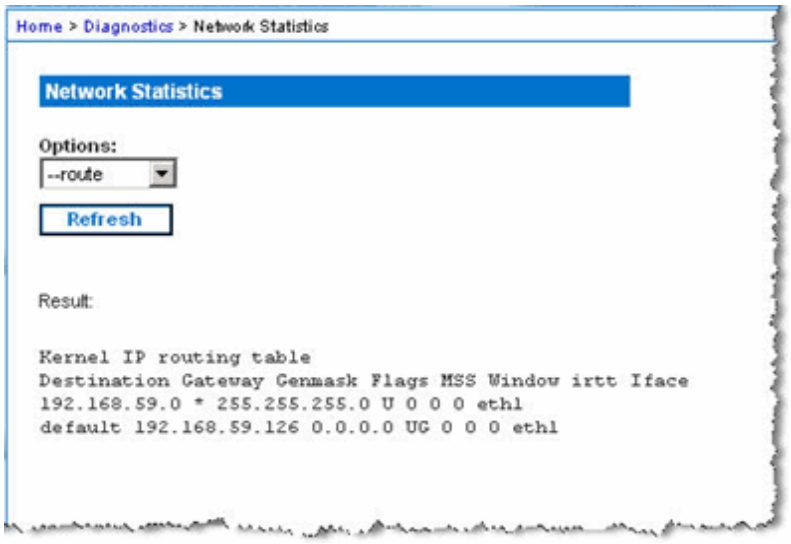
1. Sélectionnez Diagnostics > Network Statistics (Statistiques réseau). La page des statistiques réseau s'ouvre.
2. Sélectionnez l'option appropriée parmi celles de la liste déroulante Options :

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

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



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



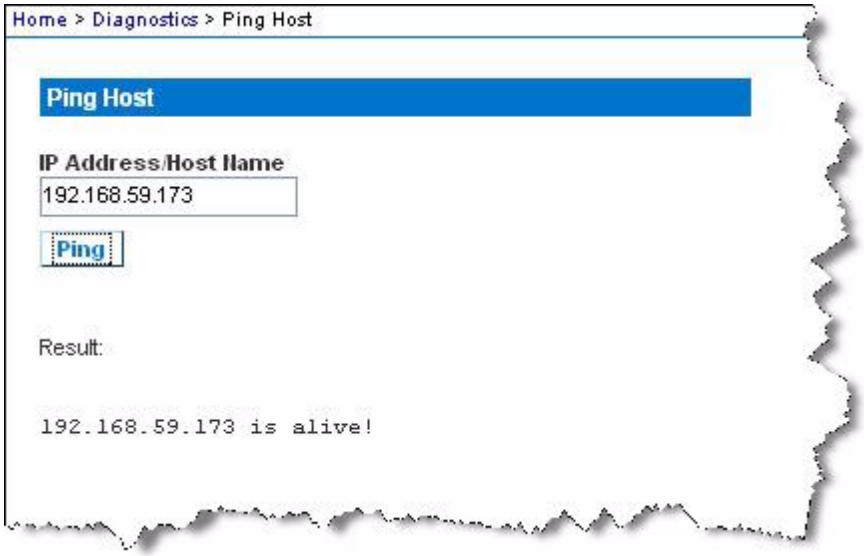
3. Cliquez sur Refresh (Actualiser). Les informations concernées sont affichées dans le champ Result (Résultat).

Page Ping Host (Envoi de commande Ping à l'hôte)

La commande Ping est un outil réseau qui permet de vérifier si un hôte ou une adresse IP spécifique est accessible via un réseau IP. Grâce à la page Ping Host (Envoyer une commande Ping à l'hôte), vous pouvez déterminer si un serveur cible ou un autre KX III est accessible.

Pour envoyer une commande Ping à l'hôte :

1. Sélectionnez Diagnostics > Ping Host (Envoyer une commande Ping à l'hôte). La page Ping Host (Envoyer une commande Ping à l'hôte) apparaît.



2. Tapez le nom de l'hôte ou l'adresse IP dans le champ IP Address/Host Name.

Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Cliquez sur Ping. Les résultats de la commande Ping sont affichés dans le champ Result (Résultat).

Page Trace Route to Host

Trace Route est un outil réseau permettant de déterminer l'itinéraire emprunté jusqu'au nom d'hôte ou jusqu'à l'adresse IP fournis.

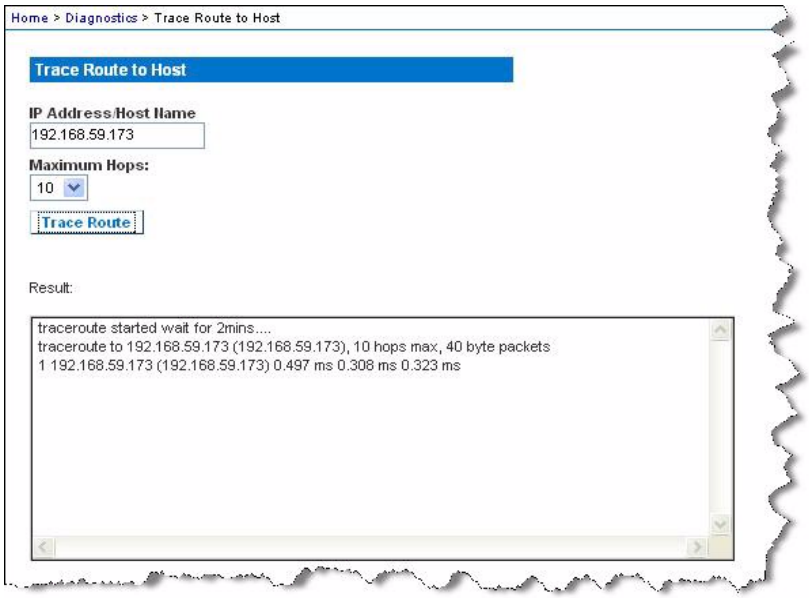
Pour déterminer l'itinéraire jusqu'à l'hôte :

1. Choisissez Diagnostics > Trace Route to Host (Diagnostics > Déterminer l'itinéraire jusqu'à l'hôte). La page Trace Route to Host s'ouvre.

2. Tapez l'adresse IP ou le nom de l'hôte dans le champ IP Address/Host Name.

   Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Sélectionnez une valeur dans la liste déroulante Maximum Hops (Sauts maximum) (de 5 à 50 par incréments de 5).
4. Cliquez sur Trace Route. La commande est exécutée pour le nom d'hôte ou l'adresse IP, et le nombre de sauts maximum donnés. Les données de détermination d'itinéraire sont affichées dans le champ Result (Résultat).



Page Device Diagnostics (Diagnostics du dispositif)

Remarque : cette page est en principe destinée aux techniciens de l'assistance. Vous pouvez l'utiliser lorsque l'assistance technique Raritan vous y invite directement.

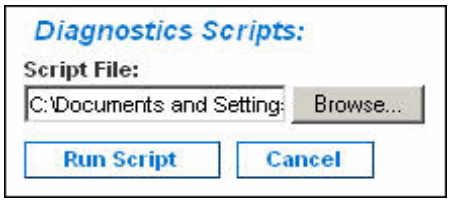
La page Device Diagnostics (Diagnostics du dispositif) télécharge les informations de diagnostic de KX III vers l'ordinateur client. Deux opérations peuvent être effectuées sur cette page :

- Exécutez un script de diagnostics spécial fourni par le support technique Raritan lors d'une session de débogage d'erreurs critiques. Le script est téléversé sur le dispositif et exécuté. Une fois le script exécuté, vous pouvez télécharger les messages de diagnostics à l'aide de la fonction Save to File (Enregistrer dans le fichier).
- Téléchargez le journal de diagnostic du dispositif pour obtenir un instantané des messages de diagnostics de KX III vers le client. Ce fichier chiffré est ensuite envoyé à l'assistance technique Raritan. Seul Raritan peut interpréter ce fichier.

Remarque : cette page n'est accessible qu'aux utilisateurs disposant de droits d'administration.

Pour exécuter les diagnostics du système KX III :

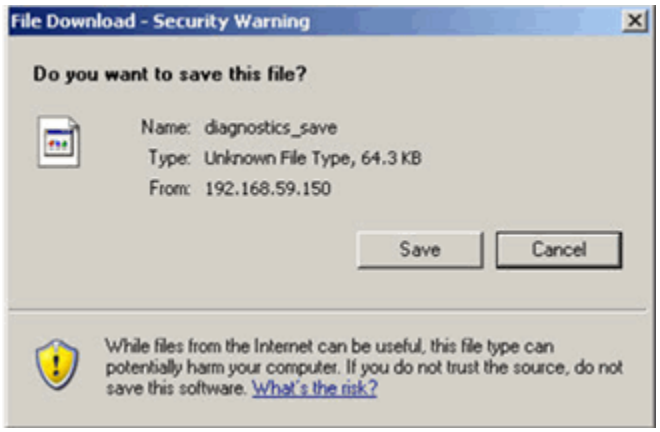
1. Sélectionnez Diagnostics > KX III Diagnostics (Diagnostics de KX III). La page de diagnostics de KX III s'ouvre.
2. Pour exécuter un fichier de script de diagnostics qui vous a été envoyé par courrier électronique par l'assistance technique Raritan :
   a. Récupérez le fichier de diagnostics fourni par Raritan et décompressez-le si nécessaire.
   b. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
   c. Localisez et sélectionnez le fichier de diagnostics.
   d. Cliquez sur Open (Ouvrir). Le fichier s'affiche dans le champ Script File (Fichier de script).



   e. Cliquez sur Run Script (Exécuter le script). Envoyez ce fichier à l'assistance technique Raritan.

3. Pour créer un fichier de diagnostics à envoyer à l'assistance technique Raritan :

   a. Cliquez sur Save to File (Enregistrer dans le fichier). La boîte de dialogue File Download (Téléchargement de fichier) s'ouvre.



   b. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) s'affiche.

   c. Localisez le répertoire voulu puis cliquez sur Save (Enregistrer).

   d. Envoyez ce fichier par courrier électronique à l'assistance technique Raritan.

Console locale KX III

Le KX III fournit un accès et une administration sur le rack via son port local. L'accès aux fonctions KX III est fournie via la Console locale.

La majorité des fonctions d'administration sont généralement effectuées via la Console à Distance KX III sont également effectuées à partir de la Console locale.

Cette section est spécifiques aux tâches d'administrateur. Pour les tâches d'utilisateur final effectuées à partir la Console Locale, consultez l'aide de l'utilisateur.

Sécurité et authentification

Pour utiliser la console locale de KX III, vous devez d'abord vous authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe valides. KX III dispose d'un schéma d'authentification et de sécurité entièrement intégré que votre accès passe par le réseau ou le port local. Dans ces deux cas, KX III ne permet l'accès qu'aux serveurs pour lesquels un utilisateur dispose de permissions. Reportez-vous à Gestion des utilisateurs pour plus d'informations sur la définition des paramètres d'accès et de sécurité des serveurs.

Si votre KX III a été configuré pour des services d'authentification externe (LDAP/LDAPS, RADIUS ou Active Directory), les tentatives d'authentification au niveau de la console locale sont également authentifiées à l'aide du service d'authentification externe.

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

Pour utiliser la console locale de KX III :

1. Branchez un clavier, une souris et un affichage vidéo sur les ports locaux situés à l'arrière de KX III.
2. Démarrez KX III L'interface de la console locale de KX III s'affiche.

Configurer les Paramètres du port local KX III à partir de la Console locale

Les ports locaux standards et étendus peuvent être configurés depuis la Console à Distance sur la page de Configuration des ports, ou depuis la Console Locale sur la page de Paramètres du port local.

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

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

Remarque : Certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage de navigateur se produit lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

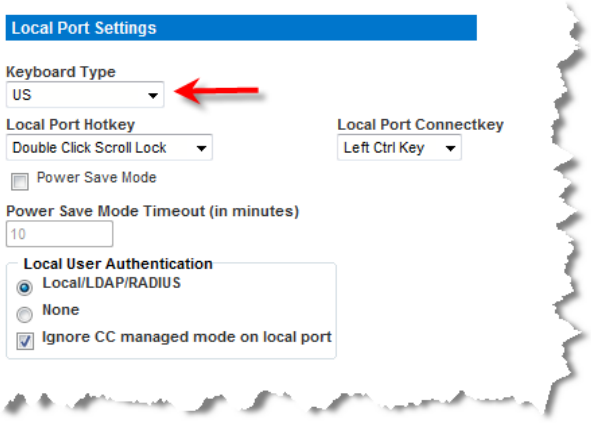
Pour configurer les paramètres du port local :

1. Choisissez Paramètres du dispositif > Paramètres du port local La page des paramètres du port local s'ouvre.

Sélectionnez le type de clavier de la Console locale

1. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante.

   Le navigateur redémarrera lorsque cette modification sera effectuée.



- US
- US/International
- United Kingdom
- Français (France)
- Allemand (Allemagne)
- Allemand (Suisse)
- Chinois simplifié
- Chinois traditionnel
- Dubeolsik Hangul (Coréen)
- Japonais (JIS)
- Portugais (Portugal)
- Norvégien (Norvège)
- Suédois (Suède)
- Danois (Danemark)
- Belge (Belgique)
- Hongrois
- Espagnol
- Italien
- Slovène

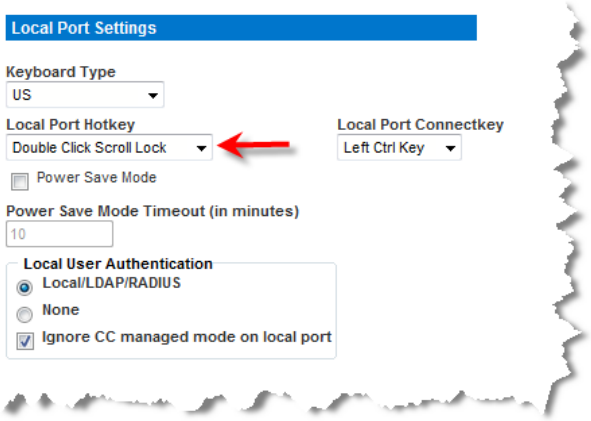
Remarque : L'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de KX III.

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

Sélectionnez le raccourci-clavier du port local.

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

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption



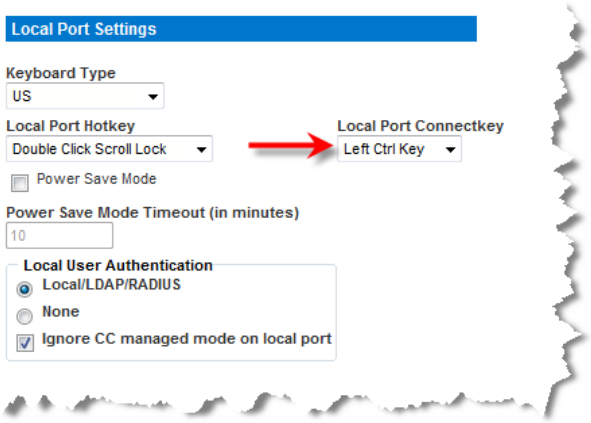
Sélectionnez la touche de connexion du port local.

1. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre.

   Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local.

   Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à ***Exemples de touches de connexion*** (à la page 298) pour obtenir des exemples de séquences de touches de connexion.

   La touche de connexion fonctionne pour les serveurs standard et les châssis de lames.

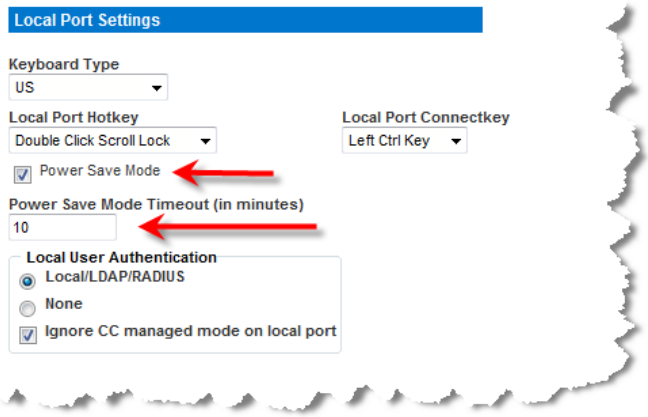


Configurer l'option d'Economie d'énergie (optionnel)

1. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique :

a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).

b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.

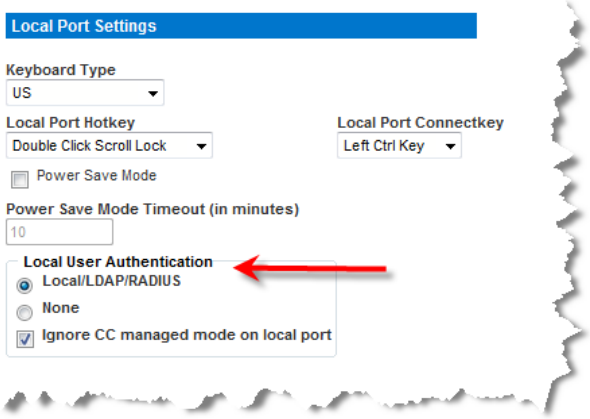


Sélectionnez l'authentification des utilisateurs locaux

1. Sélectionnez le type d'authentification d'utilisateur locale.
   - Local/LDAP/RADIUS. Il s'agit de l'option recommandée.

     Pour plus d'informations sur l'authentification, reportez-vous à Authentification à distance.
   - Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale.

     Cette option est recommandée pour les environnements sécurisés uniquement.

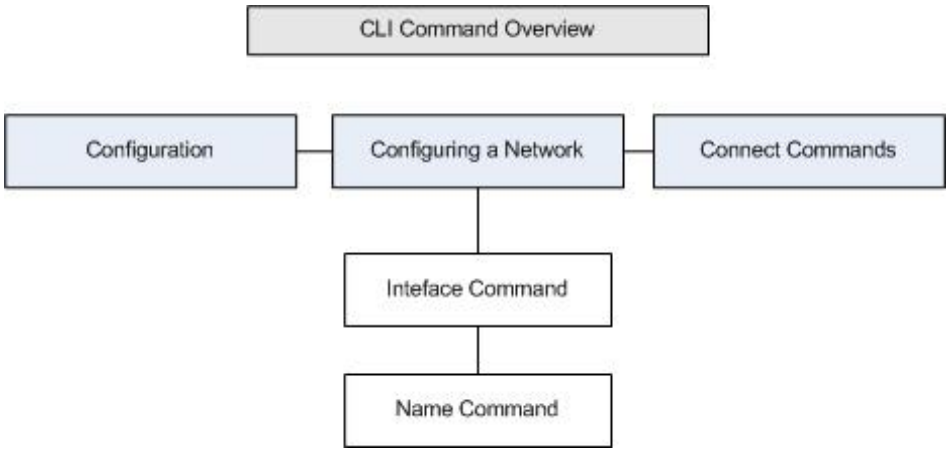


Interface de ligne de commande (CLI)

Présentation

L'interface de ligne de commande (CLI) permet de configurer l'interface réseau de KX III et d'effectuer des fonctions de diagnostic si vous disposez des autorisations appropriées pour cela.

Les figures suivantes présentent les commandes CLI. Reportez-vous à ***Commandes CLI*** (à la page 218) pour consulter une liste de commandes, de définitions et de liens vers les sections de ce chapitre comportant des exemples de ces commandes.



Les commandes courantes suivantes peuvent être utilisées depuis tous les niveaux du CLI : top (haut), history (historique), log off (déconnecter), quit (quitter), show (afficher) et help (aide).

Accès à KX III à l'aide de la CLI

Pour accéder à KX III, choisissez l'une des méthodes suivantes :

- SSH via connexion IP

Un certain nombre de clients SSH sont disponibles et peuvent être obtenus sur les sites suivants :

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client depuis ssh.com - ***www.ssh.com http://www.ssh.com***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

Connexion SSH à KX III

Utilisez un client SSH prenant en charge SSHv2 pour effectuer la connexion à KX III. Vous devez activer l'accès SSH dans la page Device Services (Services du dispositif).

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

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 III. Par exemple, 192.168.0.192.
3. Choisissez SSH, qui utilise le port de configuration 22 par défaut.
4. Cliquez sur Open (Ouvrir).

L'invite `login as:` apparaît.

Reportez-vous à ***Connexion*** (à la page 214).

Accès SSH depuis un poste de travail UNIX/Linux

Pour ouvrir une session SSH depuis un poste de travail UNIX®/Linux® et vous connecter comme administrateur, entrez la commande suivante :

```
ssh -l admin 192.168.30.222
```

L'invite Password (Mot de passe) s'affiche.

Reportez-vous à ***Connexion*** (à la page 214).

Connexion

Pour vous connecter, entrez le nom d'utilisateur admin, comme indiqué ci-après :

1. Connectez-vous sous `admin`.
2. L'invite Password (Mot de passe) s'affiche. Entrez le mot de passe par défaut : *raritan*

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

Après avoir pris connaissance de la section ***Navigation de la CLI*** (à la page 215), effectuez les tâches de configuration initiale.

Navigation de la CLI

Pour utiliser la CLI, il est essentiel d'en comprendre la navigation et la syntaxe. Certaines combinaisons de touches simplifient également l'utilisation de la CLI.

Saisie automatique des commandes

La CLI complète les commandes partiellement entrées. Entrez les premiers caractères d'une entrée et appuyez sur la touche Tab. Si les caractères forment une correspondance unique, la CLI complétera la saisie.

- Si aucune correspondance n'est trouvée, la CLI affiche les entrées valides pour ce niveau.
- S'il existe plusieurs correspondances, la CLI affiche toutes les entrées valides.

Entrez des caractères supplémentaires jusqu'à ce que l'entrée soit unique et appuyez sur la touche Tab pour compléter la saisie.

Syntaxe CLI - Conseils et raccourcis

Conseils

- Les commandes sont répertoriées par ordre alphabétique.
- Les commandes ne sont pas sensibles à la casse.
- Les noms de paramètre sont composés d'un seul mot, sans trait de soulignement.
- Les commandes sans arguments affichent par défaut les paramètres actuels de la commande.
- Si vous entrez un point d'interrogation (?) après une commande, l'aide correspondant à celle-ci s'affiche.
- Une ligne verticale (|) indique un choix parmi un ensemble de mots-clés ou d'arguments facultatifs ou obligatoires.

Raccourcis

- Appuyez sur la flèche Haut pour afficher la dernière entrée.
- Appuyez sur la touche Retour arrière pour supprimer le dernier caractère tapé.
- Utilisez Ctrl + C pour interrompre une commande ou l'annuler si vous avez saisi des paramètres erronés.
- Utilisez la touche Entrée pour exécuter la commande.
- Appuyez sur la touche Tab pour compléter automatiquement une commande. Par exemple, `Admin Port > Conf` Le système affiche ensuite l'invite `Admin Port > Config >`.

Commandes courantes pour tous les niveaux de la CLI

Les commandes disponibles à tous les niveaux du CLI sont indiquées ci-après. Ces commandes permettent également de parcourir la CLI.

Commandes	Description
top	Revient au niveau supérieur de la hiérarchie CLI, ou à l'invite username.
history	Affiche les 200 dernières commandes entrées par l'utilisateur dans la CLI de KX III.
help	Affiche une présentation de la syntaxe CLI.
quit	Fait revenir l'utilisateur au niveau précédent.
logout	Déconnecte la session utilisateur.

Configuration initiale à l'aide de la CLI

Remarque : ces étapes, qui utilisent la CLI, sont facultatives car cette même configuration peut être effectuée via KVM. Reportez-vous à **Mise en route** *(à la page 9) pour plus d'informations.*

Les dispositifs KX III sont livrés avec les paramètres usine par défaut. Lorsque vous mettez sous tension le dispositif et vous y connectez pour la première fois, vous devez définir les paramètres de base suivants, pour permettre un accès sécurisé au dispositif depuis le réseau :

1. Réinitialisez le mot de passe administrateur. Tous les dispositifs KX III sont livrés avec le même mot de passe par défaut. Pour éviter toute intrusion, il est donc impératif de remplacer le mot de passe admin raritan par un mot de passe personnalisé pour les administrateurs qui assureront la gestion du dispositif KX III.
2. Affectez l'adresse IP, le masque de sous-réseau et l'adresse IP de passerelle pour autoriser l'accès à distance.

Définition des paramètres

Pour définir les paramètres, vous devez être connecté avec des privilèges d'administration. Au niveau supérieur, vous verrez l'invite `Username>`, qui pour la configuration initiale est `admin`. Entrez la commande top pour retourner au niveau de menu supérieur.

Remarque : si vous êtes connecté sous un nom d'utilisateur différent, ce nom apparaîtra au lieu d'admin.

Définition des paramètres réseau

Les paramètres réseau sont configurés à l'aide de la commande d'interface.

```
Admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

Lorsque la commande est acceptée, le dispositif abandonne automatiquement la connexion. Vous devez vous reconnecter au dispositif à l'aide de la nouvelle adresse IP, et du nom d'utilisateur et du mot de passe que vous avez créés dans la section de réinitialisation de mot de passe usine par défaut.

Important : en cas d'oubli du mot de passe, KX III doit être réinitialisé à la valeur par défaut usine à l'aide du bouton Reset à l'arrière de KX III. Les tâches de configuration initiale doivent être alors exécutées à nouveau.

KX III est maintenant doté d'une configuration de base et est accessible à distance via SSH, l'interface utilisateur ou localement à l'aide du port série local. L'administrateur doit configurer les utilisateurs et groupes, les services, la sécurité et les ports série par lesquels les cibles série sont connectées au KX III.

Invites CLI

L'invite CLI indique le niveau de commande actuel. La partie racine de l'invite est le nom de connexion. Pour une connexion de port série admin directe avec une application d'émulation de terminal, Admin Port est la partie racine d'une commande.

```
admin >
```

Commandes CLI

- Entrez `admin > help`.

Commande	Description
config	Passe au sous-menu config.
diagnostics	Passe au sous-menu diag.
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
listports	Répertorie les ports accessibles.
logout	Déconnecte de la session CLI actuelle.
top	Revient au menu racine.
userlist	Répertorie les sessions utilisateur actives.

- Entrez `admin > config > network`.

Commande	Description
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
interface	Définit/Extrait les paramètres réseau.
ipv6_interface	Définit/Extrait les paramètres réseau IPv6.
logout	Déconnecte de la session CLI actuelle.
name	Configuration du nom de dispositif.
quit	Revient au menu précédent.
stop	Revient au menu racine.

Problèmes de sécurité

Eléments à considérer en matière de sécurité pour les serveurs de console :

- Chiffrement le trafic des données envoyées entre la console de l'opérateur et le dispositif KX III.
- Authentification et autorisation des utilisateurs.
- Profil de sécurité.

KX III prend en charge chacun de ces éléments ; toutefois, ils doivent être configurés avant l'utilisation générale.

Administration des commandes de configuration du serveur de console de KX III

Remarque : Les commandes CLI sont les mêmes pour les sessions SSH et Port local.

La commande Réseau est accessible depuis le menu Configuration de KX III.

Configuration du réseau

Les commandes du menu Network permettent de configurer l'adaptateur réseau de KX III.

Commandes	Description
interface	Configure l'interface réseau du dispositif KX III.

Commandes	Description
name	Configuration du nom du réseau.
ipv6	Définit/Extrait les paramètres réseau IPv6.

Commande interface

La commande interface permet de configurer l'interface réseau de KX III. La syntaxe de la commande interface est la suivante :

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> Adresse IP

mask <subnetmask> Masque de sous-réseau

gw <ipaddress> Adresse IP de passerelle

mode <mode> Set Ethernet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Exemple d'utilisation de la commande interface

La commande suivante activer l'interface numéro 1, définit l'adresse IP, le masque et les adresses de passerelle. Elle définit également le mode sur détection automatique.

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

Commande name

La commande name permet de configurer le nom de réseau. La syntaxe de la commande name est la suivante :

```
name [devicename <nomDispositif>] [hostname <nomHôte>]
```

Configuration du nom de dispositif.

```
devicename <devicename>   Nom du dispositif

hostname   <hostname>     Nom d'hôte privilégié (DHCP
uniquement)
```

Exemple d'utilisation de la commande name

La commande suivante définit le nom de réseau :

```
Admin > Config > Network > name devicename My-KSX2
```

Commande IPv6

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

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

Groupes de deux ports vidéo

Les serveurs dotés de deux cartes vidéo sont accessibles à distance avec une configuration de bureau étendu, disponible aux utilisateurs distants. Pour ce faire, vous devez créer des groupes de deux ports vidéo.

La configuration de bureau étendu vous permet d'afficher le bureau du serveur cible sur deux écrans, au lieu d'un affichage standard sur un écran.

Une fois le groupe de deux ports vidéo sélectionné, tous les canaux de port de ce groupe s'ouvrent simultanément.

Reportez-vous à **Création d'un groupe de deux ports vidéo** (à la page 167).

Consultez les informations de cette section pour obtenir des informations importantes sur la création de groupes de deux ports vidéo.

Remarque : Les groupes de deux ports vidéo ne sont pas pris en charge par les modèles n'ayant qu'un seul canal KVM, tels que les modèles KX3-108 et KX3-116.

Recommandations en matière de ports vidéo doubles

Réglez les écrans principal et secondaire du serveur cible sur la même résolution vidéo afin de maintenir la synchronisation de la souris et de réduire la fréquence de resynchronisation.

Selon l'orientation souhaitée, l'écran supérieur (orientation verticale) ou gauche (orientation horizontale) doit être désigné comme affichage principal. Vous activez ainsi la sélection de menu pour les opérations de support virtuel, audio, carte à puce et souris.

Afin de fournir des mouvements et un contrôle de souris intuitif, les choses suivantes devraient avoir la même orientation d'écran:

- Ecrans du PC primaires et secondaires du client
- Configuration des groupes de deux ports vidéo KX II/KX III
- Ecrans du serveur cible primaires et secondaires

Seuls les paramètres de lancement du client ci-après seront appliqués aux affichages vidéo à ports doubles :

- Sélectionnez l'affichage standard ou mode Plein écran lors du lancement du client KVM.
- Activez la mise à l'échelle vidéo.
- Activez l'épinglage de la barre d'outils de menu en mode Plein écran.

L'utilisation du mode souris simple n'est pas recommandée lors de l'affichage des ports vidéo doubles en mode Plein écran sur un écran client unique. Vous devrez quitter ce mode pour accéder à l'autre écran et l'afficher.

Modes de souris pris en charge pour les groupes de deux ports vidéo

Systèmes d'exploitation cible	Modes souris pris en charge	Commentaires
Tous les systèmes d'exploitation Windows®	Modes de souris intelligente, standard et unique	Si le mode 'étiré' (Stretch) est pris en charge par la carte vidéo du serveur cible, le mode souris absolue fonctionnera correctement. En mode étiré, le serveur cible gère l'affichage double comme un affichage virtuel contigu unique. En revanche, en mode Etendu (Extended), le serveur considérera les deux écrans comme indépendants. Le mode souris intelligente est

Systèmes d'exploitation cible	Modes souris pris en charge	Commentaires
		recommandé en mode Etendu.
Linux®	Modes souris intelligente et standard	Les utilisateurs de Linux® peuvent rencontrer des problèmes d'affichage et de mouvement de la souris en mode souris unique. Raritan recommande aux utilisateurs de Linux de ne pas l'employer.
Système d'exploitation Mac®	Mode souris unique	Pour les cibles Mac avec plusieurs moniteurs, utilisez une souris standard en mode curseur unique.

CIM requis pour la prise en charge de vidéo double

Les CIM numériques suivants prennent en charge la fonction de port vidéo double :

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

Reportez-vous à Synchronisation et résolution vidéo du serveur cible des CIM numériques pour d'importantes informations concernant les CIM numériques. Consultez Spécifications des CIM pris en charge pour les spécifications CIM.

Si le module CIM d'origine relié à un port principal ou secondaire est déconnecté et remplacé par un autre, le port est retiré du groupe de deux ports vidéo. Au besoin, ajoutez à nouveau le port au groupe.

Remarque : Le CIM utilisé dépend des exigences du serveur cible.

Remarques relatives à l'utilisation des groupes de deux ports vidéo

Les fonctions suivantes sont affectées par l'utilisation de la fonction de groupe de deux ports vidéo.

- Les paramètres de lancement client configurés sur les clients Virtual KVM Client (VKC) et Active KVM Client (AKC) via Outils > Options > Paramètres de lancement client seront appliqués aux groupes de deux ports vidéo comme suit:
  - Les paramètres de mode fenêtre seront appliqués.
  - Les paramètres d'écran NE SERONT PAS appliqués. L'orientation d'affichage (Display Orientation) configurée sur la page Port Group Management (Gestion des groupes de ports) sera appliquée à la place.
  - Le paramètre Other - Enable Single Mouse Cursor (Autre - Activer le curseur de souris simple) NE SERA PAS appliqué.
  - Le paramètre Other - Enable Scale Video (Autre - Activer la mise à l'échelle de la vidéo) sera appliqué.
  - Le paramètre Other - Pin Menu Toolbar (Autre - Epingler la barre d'outils de menu) sera appliqué.
- Le glissement et le déplacement d'éléments entre les fenêtres principale et secondaire de la cible requièrent de relâcher et d'enfoncer le bouton de la souris lorsque l'élément passe d'une fenêtre à l'autre.
- Sur les serveurs cible Linux® et Mac®, lorsque le verrouillage numérique et des majuscules est activé, l'indicateur de verrouillage des majuscules apparaît dans la barre de statut de la fenêtre du port principal, mais pas nécessairement dans celle du port de la fenêtre secondaire.

Autorisations et accès aux groupes de deux ports vidéo

Idéalement, les autorisations appliquées à chaque port du groupe doivent être identiques. Sinon, les autorisations les plus restrictives seront appliquées au groupe.

Par exemple, si VM Access Deny (Accès refusé) est appliqué à un port et VM Access Read-Write (Accès en lecture-écriture) à un autre, VM Access Deny est appliqué au groupe.

Si un utilisateur ne dispose pas des autorisations appropriées pour accéder à un port faisant partie d'un groupe de deux ports vidéo, seul le port auquel il a accès est affiché. S'il n'est autorisé à accéder à aucun port, l'accès est refusé.

En cas de tentative d'accès, un message s'affiche indiquant que le port n'est pas disponible ou que l'utilisateur n'est pas autorisé à y accéder.

Exemple de configuration de groupe de deux ports vidéo

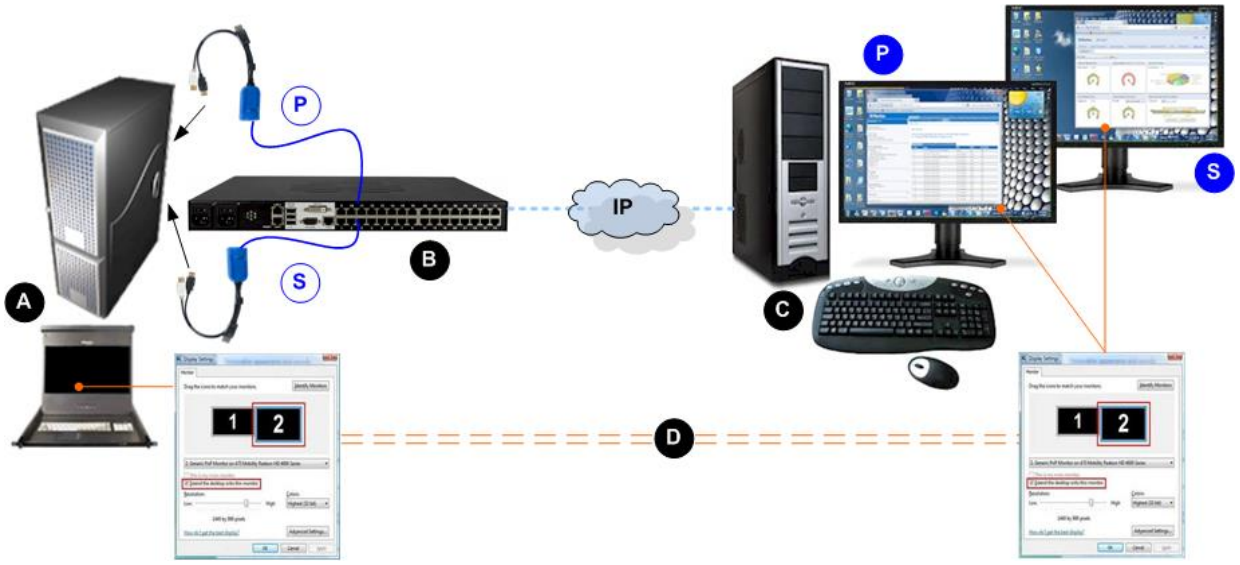
Voici un exemple général.

Votre configuration peut varier selon le type de CIM utilisé, le port désigné comme port principal, les ports du KX III auxquels vous vous connectez, etc.

Dans cet exemple, nous utilisons :

- Un serveur cible avec deux ports vidéo
- Port vidéo 1 du serveur cible comme port principal et port vidéo 2 du serveur cible comme port secondaire
- Un dispositif KX3-832
- Un CIM D2CIM-DVUSB-DP
- Un serveur cible et un client distant exécutant le système d'exploitation Microsoft® Windows 7®
- Mode souris intelligente

Une vue bureau étendue sur le serveur cible et le client distant ; nous configurons donc KX III pour prendre en charge l'orientation d'affichage Horizontal - Primary (Left), Secondary (Right) (Horizontal - Principal (gauche), Secondaire (droite)



Légende	
A	Client à distance - configure le groupe de deux ports vidéo et les paramètres d'affichage
B	KX III

Légende	
P	Connexion à partir d'une cible vidéo primaire (primaire) au KX III
S	Connexion à partir du port vidéo secondaire (second) de la cible à KX III
Connexion IP entre le KX III et le client distant	
C	Serveur cible - configure les paramètres d'affichage et lance le groupe de deux ports vidéo
D	Les paramètres d'affichage sont les mêmes sur le client à distance et le serveur cible (recommandé)
P	Horizontal - Primaire (Gauche) - défini sur la page de gestion des groupes de ports en KX III
S	Secondaire (Droite) - défini sur la page de gestion des groupes de ports en KX III

Etapes de configuration de deux ports vidéo

Etape 1 : Configuration de l'affichage du serveur cible

Le paramètre d'orientation configuré sur le dispositif pour la cible doit correspondre à la configuration réelle du système d'exploitation de la cible.

Il est recommandé que le client connecté ait la même orientation d'écran dès que possible.

Pour plus d'informations sur l'orientation de l'écran et les modes de souris Orientation, alignement de l'affichage et modes souris des groupes de deux ports vidéo

Remarque : Reportez-vous à la documentation utilisateur du serveur cible ou du système d'exploitation pour obtenir les procédures exactes de configuration des paramètres d'affichage.

Pour configurer les paramètres d'affichage et de souris du serveur cible :

1. Sur le serveur cible, configurez l'orientation d'affichage du serveur cible pour chaque port vidéo en fonction de celle du client distant.

   Par exemple, si vous utilisez une orientation bureau étendu de gauche à droite sur deux écrans sur le client distant, définissez la même orientation d'affichage sur le serveur cible.

2. Vérifiez que l'écran du serveur cible est déjà défini sur une résolution et un taux de rafraîchissement pris en charge. Consultez ***Résolutions de serveur vidéo cible*** (voir "***Résolutions de Vidéo de Serveur cible supportées par KX III***" à la page 334, ***http://www.raritan.com/help/kx-iii/v3.0.0/en/index.htm#32872***)

Remarque : Si les affichages principal et secondaire cible sont définis sur des résolutions différentes, la souris ne sera plus synchronisée et devra être resynchronisée depuis la fenêtre supérieure gauche cible.

Etape 2 : Connexion du serveur cible à KX III

Des groupes de deux ports vidéo peuvent être créés à partir de connexions de port existantes ou nouvelles.

La procédure fournie ici suppose la création de nouvelles connexions.

Si vous créez un groupe de deux ports vidéo à partir de connexions existantes, reportez-vous à Etape 4 : Création d'un groupe de deux ports vidéo.

Pour connecter l'équipement :

1. Le cas échéant, installez et mettez sous tension le serveur cible selon les instructions du fabricant.
2. Raccordez le connecteur vidéo de chaque CIM à chacun des ports de sortie vidéo de la cible et connectez les câbles USB aux ports USB disponibles sur la cible.
3. Connectez chaque CIM à KX III à l'aide d'un câble CAT5/6.
4. Si vous ne l'avez pas déjà fait:
   a. Connectez la KX III à une source d'alimentation CA utilisant le câble d'alimentation fourni
   b. Connectez au port réseau KX III et port local (si nécessaire)
   c. Configurer la KX III. Consultez ***Mise en route*** (à la page 9) pour obtenir les étapes nécessaires à l'utilisation initiale du dispositif.
5. Lancer un navigateur pris en charge.
6. Entrez soit:
   - L'URL - *http://ADRESSE-IP* pour utiliser le client KVM virtuel basé sur Java

     Ou

   - *http://ADRESSE-IP/akc* pour le client KVM actif basé sur .NET

   ADRESSE-IP est l'adresse IP assignée à votre KX III.

Vous pouvez également l'HTTPS ou le nom DNS du KX III assigné par votre administrateur (si applicable).

Vous êtes toujours redirigé à l'adresse IP de HTTP à HTTPS.

7. Entrez votre nom d'utilisateur et mot de passe, puis cliquez sur Connexion.
8. Acceptez le contrat d'utilisation (si applicable).
9. Si des avertissements de sécurité apparaissent, acceptez-les et/ou autorisez l'accès.

Etape 3 : Configuration du mode souris et des ports

Une fois que vous avez connecté le serveur cible à la KX III via les ports vidéo du serveur cible, il détecte la connexion et affiche les ports de la page de configuration de Port.

Pour des instructions, consultez **Configuration des serveurs cible standard**

Une fois les ports configurés, ils peuvent être réunis dans un groupe de deux ports vidéo.

---

*Remarque : Il n'est pas nécessaire de configurer les ports existants si vous l'avez déjà fait en créant les groupes de deux ports vidéo. Reportez-vous à **Création d'un groupe de deux ports vidéo** (à la page 167).*

Configurez le mode souris du serveur cible une fois la connexion à la cible établie. Consultez **Modes de souris pris en charge pour les groupes de deux ports vidéo** (à la page 223)

Etape 4 : Création du groupe de deux ports vidéo

Reportez-vous à ***Création d'un groupe de deux ports vidéo*** (à la page 167).

Etape 5 : Lancement d'un groupe de deux ports vidéo

Une fois le groupe de deux ports vidéo créé, il est disponible sur la page Port Access (Accès aux ports).

Deux canaux KVM sont requis pour la connexion à distance au groupe de deux ports vidéo en cliquant sur le port principal. Si deux canaux ne sont pas disponibles, le lien Connect (Connexion) n'est pas affiché.

Les délais d'inactivité de session configurés sur KX III sont appliqués aux deux ports d'un groupe de ports vidéo.

Pour lancer un groupe de deux ports :

- Sur la page Port Access (Accès aux ports), cliquez sur le nom de port principal, puis sur Connect (Connecter).

Les deux connexions sont lancées en même temps et affichées dans deux fenêtres différentes.

Une fois les fenêtres affichées, elles peuvent être déplacées selon le paramétrage d'affichage utilisé. Par exemple, si vous utilisez le mode bureau étendu, les fenêtres de ports peuvent être déplacées entre les écrans.

Navigation client Raritan lors de l'utilisation des groupes de deux ports vidéo

Pour alterner entre deux ports lorsque le mode Plein écran est utilisé sur les clients :

- VKC
  - Appuyez sur Alt+Tab.
  - Pour les clients Mac®, appuyez sur F3, puis sélectionnez l'affichage du port.

- AKC
  - Cliquez en dehors de la fenêtre d'affichage et appuyez sur Alt+Tab.

Accès direct aux ports et groupes de deux ports vidéo

L'accès direct aux ports permet aux utilisateurs d'éviter les pages de connexion et d'accès aux ports du dispositif.

Cette fonction permet également d'entrer un nom d'utilisateur et un mot de passe directement, et d'accéder à la cible si le nom d'utilisateur et le mot de passe ne sont pas contenus dans l'URL.

Si vous accédez à une cible faisant partie d'un groupe de deux ports vidéo, l'accès aux ports direct utilise le port principal pour lancer les ports principal et secondaire.

Les connexions directes au port secondaire sont rejetées et les règles d'autorisation habituelles s'appliquent.

Reportez-vous à **Création d'un groupe de deux ports vidéo** (à la page 167) pour plus d'informations à ce sujet..

Pour plus d'informations sur l'accès direct au port, consultez **Activation d'un accès direct aux ports via URL**.

Groupes de deux ports vidéo affichés sur la page Ports

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

Remarque : Deux canaux KVM sont requis pour la connexion à distance au groupe de deux ports vidéo en cliquant sur le port principal. Si deux canaux ne sont pas disponibles, le lien Connect (Connexion) n'est pas affiché.

Dans les groupes de deux ports vidéo, le port principal est inclus dans un balayage de ports, mais non le port secondaire lors de la connexion depuis un client distant. Les deux ports peuvent être inclus dans le balayage depuis le port local.

Reportez-vous à Page Port Access (affichage de la console distante) pour plus d'informations sur le contenu affiché sur la page Ports et à Balayage des ports pour plus d'informations sur l'exécution de balayages.

Mise à jour du schéma LDAP

Renvoi des informations relatives aux groupes d'utilisateurs

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

Depuis LDAP/LDAPS

Lorsqu'une demande d'authentification LDAP/LDAPS aboutit, >ProductName< détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel il appartient. Votre serveur LDAP distant peut fournir ces noms de groupes d'utilisateurs en renvoyant un attribut désigné de la manière suivante :

rciusergroup attribute type: chaîne

Il est possible que cette opération nécessite une extension de schéma sur votre serveur LDAP/LDAPS. Consultez l'administrateur de votre serveur d'authentification pour activer cet attribut.

De plus, pour Microsoft® Active Directory®, le memberOf LDAP standard est utilisé.

A partir d'Active Directory (AD) de Microsoft

Remarque : Seul un administrateur Active Directory® confirmé doit tenter cette opération.

Le renvoi des informations relatives aux groupes d'utilisateurs à partir de Microsoft Active Directory pour Windows 2000 Server nécessite la mise à jour du schéma LDAP/LDAPS. Reportez-vous à la documentation Microsoft pour plus d'informations.

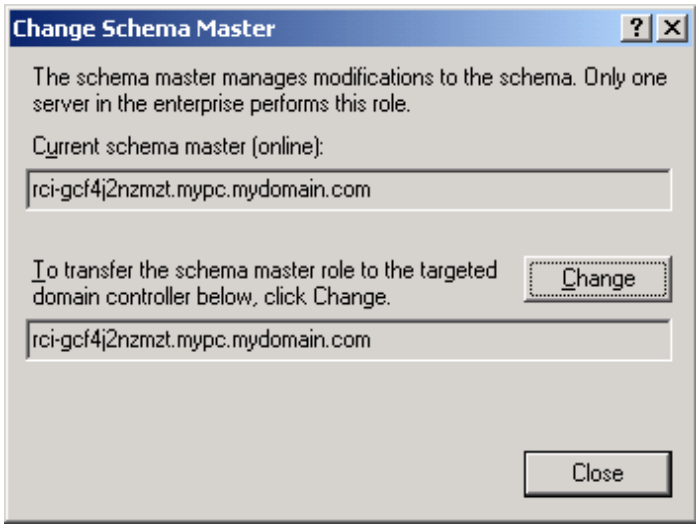
1. Installez le plug-in de schéma pour Active Directory. Reportez-vous à la documentation de Microsoft Active Directory pour obtenir des instructions.
2. Lancez la console Active Directory et sélectionnez Active Directory Schema (Schéma Active Directory).

Définition du Registre pour autoriser les opérations d'écriture sur le schéma

Pour autoriser un contrôleur de domaine à écrire sur le schéma, vous devez définir une entrée de Registre permettant les mises à jour du schéma.

Pour permettre les opérations d'écriture sur le schéma :

1. Cliquez avec le bouton droit de la souris sur le nœud racine Schéma Active Directory® dans le volet de gauche de la fenêtre, puis cliquez sur Maître d'opérations. La boîte de dialogue Changer le contrôleur de schéma s'affiche.



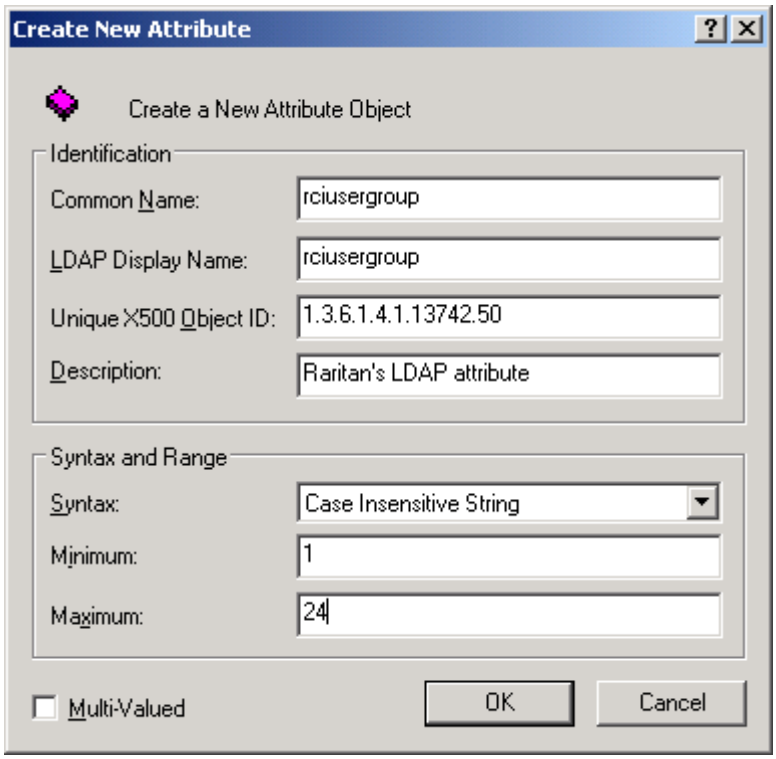
2. Cochez la case Le schéma peut être modifié sur ce contrôleur de domaine. **Facultatif**
3. Cliquez sur OK.

Création d'un attribut

Pour créer des attributs pour la classe rciusergroup :

1. Cliquez sur le symbole + en regard de Schéma Active Directory® dans le volet de gauche de la fenêtre.
2. Cliquez avec le bouton droit de la souris sur Attributs dans le volet de gauche.

3. Cliquez sur Nouveau, puis sélectionnez Attribut. Lorsque le message d'avertissement apparaît, cliquez sur Continuer ; la boîte de dialogue Créer un nouvel attribut s'affiche.



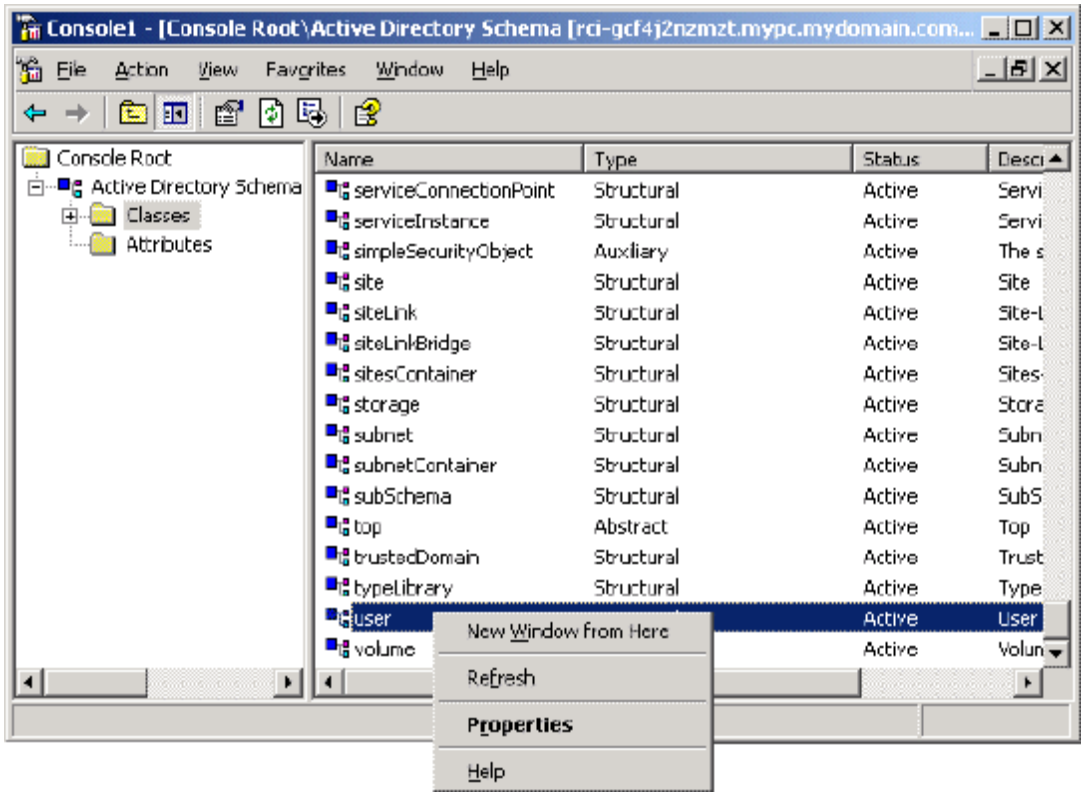
4. Tapez *rciusergroup* dans le champ Nom commun.
5. Tapez *rciusergroup* dans le champ Nom LDAP affiché.
6. Tapez *1.3.6.1.4.1.13742.50* dans le champ ID d'objet X.500 unique.
7. Entrez une description significative dans le champ Description.
8. Cliquez sur la flèche de la liste déroulante Syntaxe et sélectionnez Chaîne insensible à la casse dans la liste.
9. Tapez *1* dans le champ Minimum.
10. Tapez *24* dans le champ Maximum.
11. Cliquez sur OK pour créer l'attribut.

Ajout d'attributs à la classe

Pour ajouter des attributs à la classe :

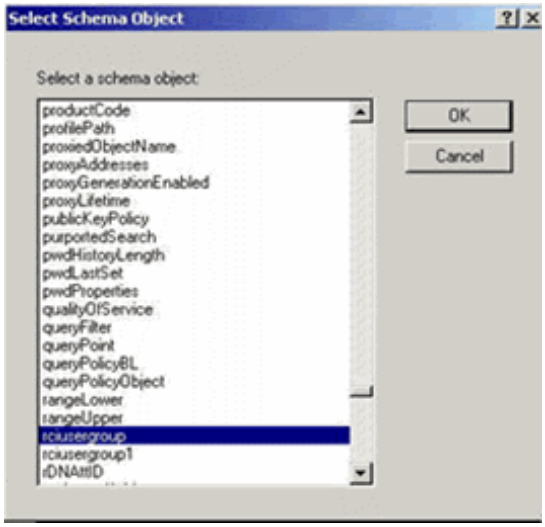
1. Cliquez sur Classes dans le volet de gauche de la fenêtre.

2. Faites défiler le volet droit jusqu'à la classe user et cliquez dessus avec le bouton droit de la souris.



3. Sélectionnez Propriétés dans le menu. La fenêtre Propriétés de user s'affiche.
4. Cliquez sur l'onglet Attributs pour l'ouvrir.
5. Cliquez sur Add (Ajouter).

6. Sélectionnez rciusergroup dans la liste Sélectionnez l'objet Schéma.



7. Cliquez sur OK dans la boîte de dialogue Sélectionnez l'objet Schéma.
8. Cliquez sur OK dans la boîte de dialogue Propriétés de user.

Mise à jour du cache de schéma

Pour mettre à jour le cache du schéma :

1. Cliquez avec le bouton droit de la souris sur Schéma Active Directory® dans le volet de gauche de la fenêtre et sélectionnez Recharger le schéma.
2. Réduisez la console Active Directory Schema MMC (Microsoft® Management Console).

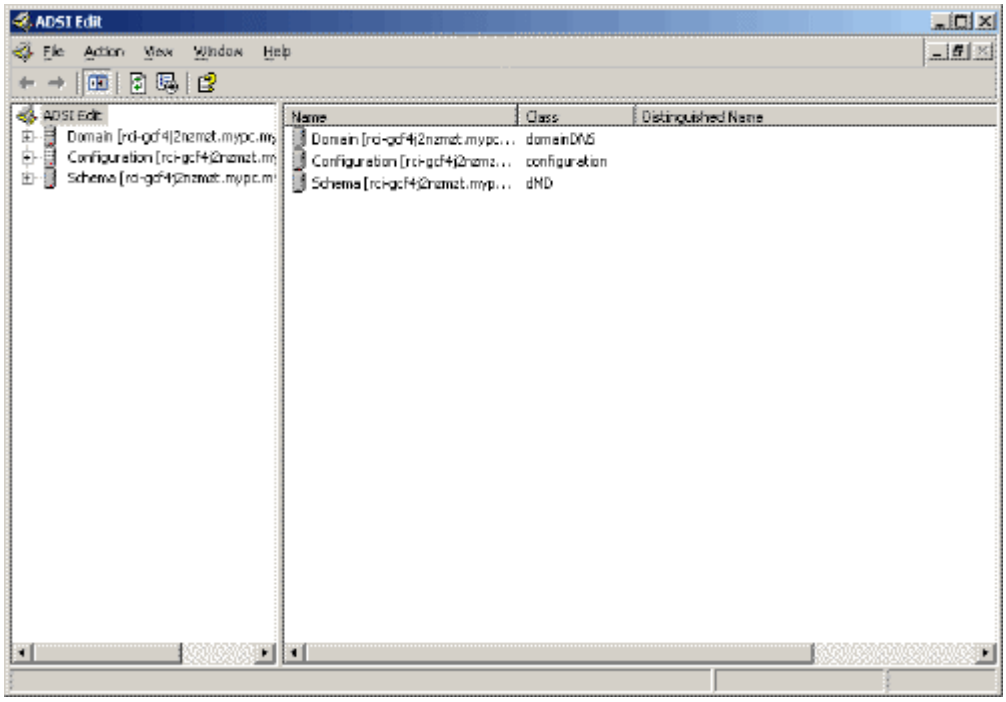
Modification des attributs rciusergroup pour les membres utilisateurs

Pour exécuter un script Active Directory® sur un serveur Windows 2003®, utilisez le script fourni par Microsoft® (disponible sur le CD d'installation de Windows Server 2003). Ces scripts sont chargés sur votre système lors de l'installation de Microsoft® Windows 2003. ADSI (ou Active Directory Service Interface) sert d'éditeur de bas niveau pour Active Directory. Il vous permet d'effectuer des tâches d'administration courantes, telles que l'ajout, la suppression et le déplacement d'objets avec un service d'annuaire.

Pour modifier les attributs d'un utilisateur individuel au sein du groupe rciusergroup, procédez comme suit :

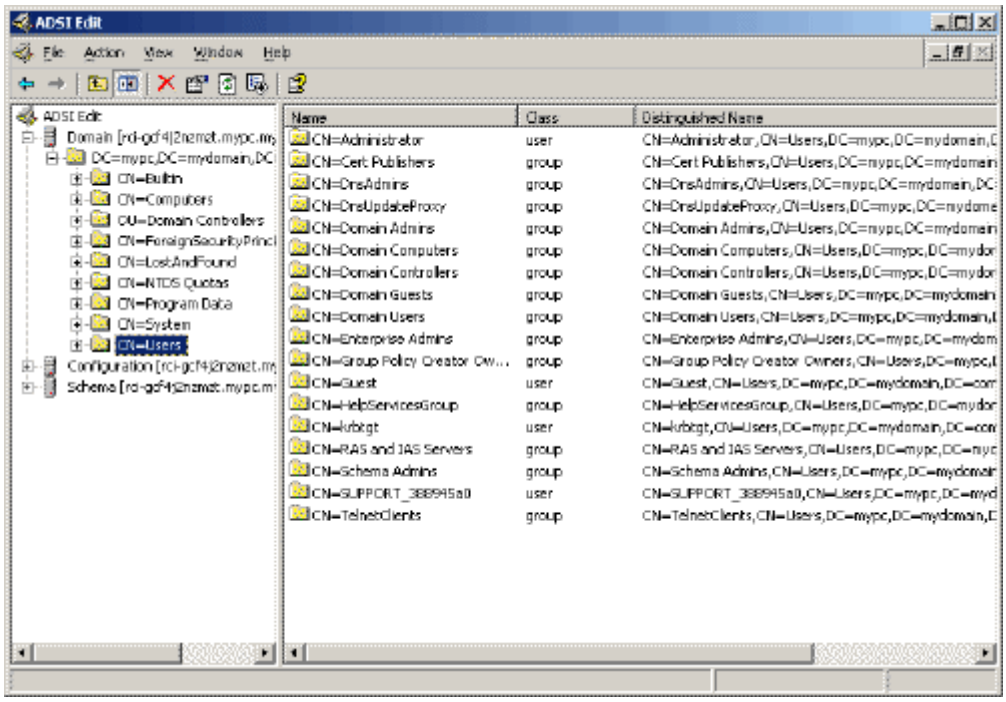
1. Sur le CD d'installation, sélectionnez Support > Tools (Outils).

2. Cliquez deux fois sur SUPTOOLS.MSI pour installer les outils de support.
3. Ouvrez le répertoire dans lequel les outils de support sont installés. Exécutez adsiedit.msc. La fenêtre Editeur ADSI s'ouvre.



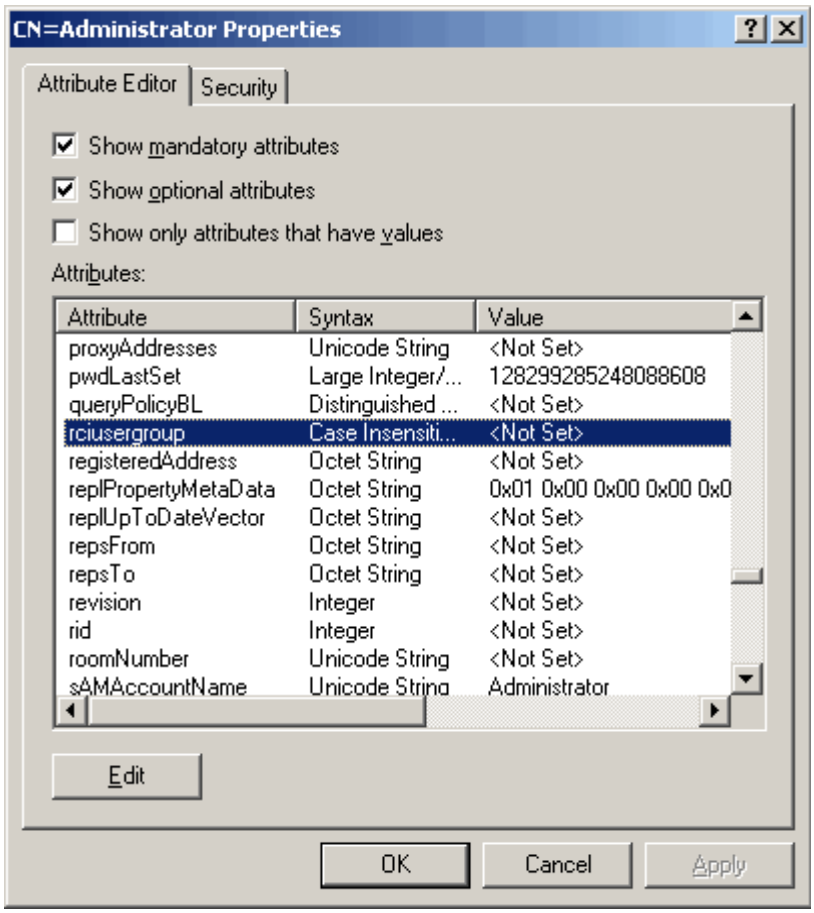
4. Ouvrez le domaine.

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

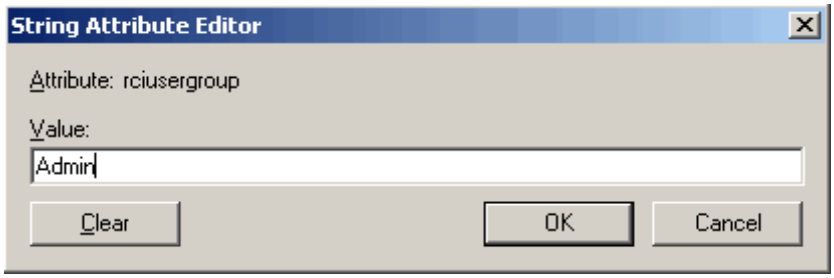


6. Recherchez le nom d'utilisateur dont vous souhaitez régler les propriétés dans le volet de droite. Cliquez avec le bouton droit sur le nom d'utilisateur et sélectionnez Propriétés.

7. Cliquez sur l'onglet Editeur d'attribut s'il n'est pas déjà ouvert. Sélectionnez rciusergroup dans la liste Attributs.



8. Cliquez sur Modifier. La boîte de dialogue Editeur d'attribut de chaîne apparaît.
9. Tapez le groupe d'utilisateurs (créé dans KX III) dans le champ Modifier l'attribut. Cliquez sur OK.



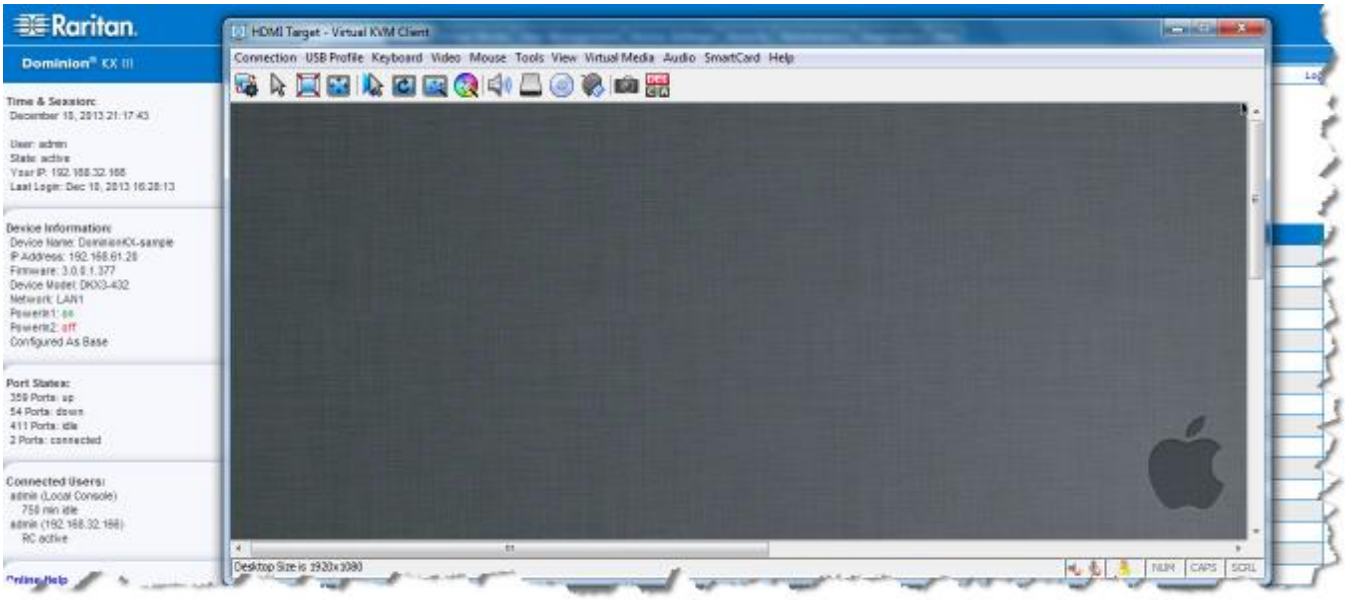
Chapitre 5 Aide Virtuelle pour Client KVM (VKC)

Dans ce chapitre

Présentation 240
Se connecte à un serveur cible 241
Configurer les propriétés de connexion.....242
Informations sur la connexion 246
Profils USB 247
Clavier.....248
Propriétés vidéo.....253
Options de souris.....257
Options d'outils 262
Options d'affichage.....268
Support virtuel 270
Cartes à puce 279
Audionumérique 283
Informations de version - Virtual KVM Client.....291

Présentation

Chaque fois que vous accédez à un serveur cible à l'aide de la page d'Accès au Port de KX III, une fenêtre Virtual KVM Client (VKC) s'ouvre.



A chaque serveur cible connecté correspond une fenêtre Virtual KVM Client.

Elles peuvent être réduites, agrandies et déplacées sur le bureau de votre ordinateur.

IMPORTANT : Le rafraîchissement de votre navigateur HTML entraîne la fermeture de la connexion de Virtual KVM Client, faites donc attention.

Virtual KVM Client (VKC) et Active KVM Client (AKC) sont des interfaces permettant d'accéder à des cibles distantes.

VKC et AKC partage des fonctions similaires à l'exception des suivantes :

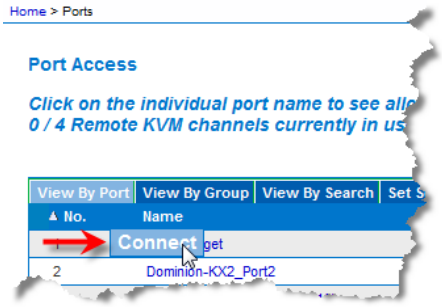
- Configuration système minimale requise
- Systèmes d'exploitation et navigateurs pris en charge
- Les macros de clavier créées dans AKC ne peuvent pas être utilisées dans VKC.
- Configuration de l'accès direct aux ports (reportez-vous à **Activation d'un accès direct aux ports via URL**.)
- Configuration de la validation de certification du serveur AKC (reportez-vous à **Conditions requises pour l'utilisation d'AKC** (à la page 294).)

Se connecte à un serveur cible

Une fois que vous vous êtes connecté au KX III à Distance, accédez aux serveurs cible via le Virtual KVM Client (VKC) ou l'Active KVM Client (AKC).

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

1. Sur la page d'accès au Port, cliquez sur le nom du port du serveur cible auquel vous souhaitez vous connecter. Le menu Port Action (Action des ports) s'ouvre.
2. Cliquez sur Connect (Connecter).



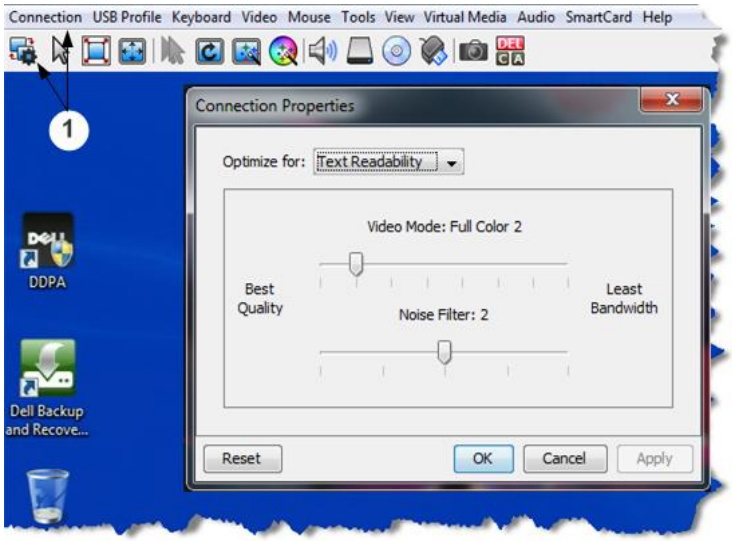
Reportez-vous à ***Port Action Menu (Menu d'action de ports)*** (à la page 20) pour plus d'informations sur les options de menu supplémentaires disponibles.

Configurer les propriétés de connexion

Propriétés d'accès de connexion

Pour accèder aux propriétés de connexion:

1	Cliquez sur Connexion > Propriétés, ou cliquez sur l'icône Connexion pour ouvrir la boîte de dialogue de Propriétés de Connexion.



Concernant les Propriétés de connexion

Le Virtual KVM Client (VKC) et Active KVM Client (AKC) prend en charge la gestion des proppriétés de connexion.

Les propriétés de connexion gèrent la performance de diffusion vidéo par connections à distance à des serveurs cible.

Les propriétés sont appliquées seulement à votre connexion - elles n'impactent pas la connexion d'autres utilisateurs accédant aux mêmes serveurs cible via VKC ou AKC.

Si vous effectuez des changements aux propriétés de connexion, ils sont retenus par VKC et AKC.

Paramètres de propriétés de connexion par défaut - Optimisé pour de meilleures performances

KX III est déjà configuré pour fournir des performances optimales dans la majorité des conditions de diffusion vidéo.

Valeur des paramètres de connexion par défaut sont:

- Optimisé pour : Lisibilité du texte - les modes vidéo sont conçus pour maximiser la lisibilité du texte.

  Ce paramètre est idéal pour des applications informatiques et IT générales, telles que l'administration du serveur.

- Mode vidéo - défauts à couleur complète 2.

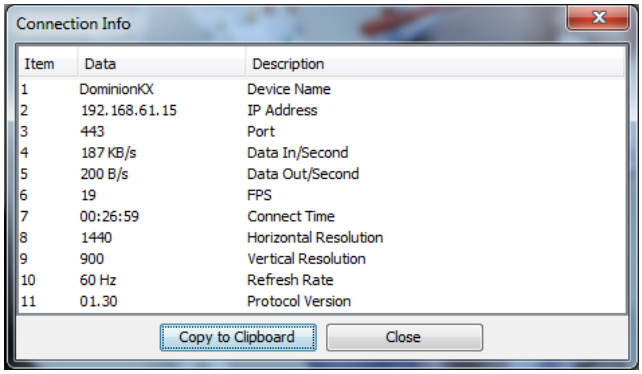
  Les images vidéo sont transmises en haute qualité, en couleurs 24 bits. Ce paramètre convient lorsqu'un réseau local haut débit est utilisé.

- Filtre de bruit - défaut à 2.

  Le paramètre de filtre de bruit n'a pas besoin d'être changé fréquemment.

Cliquez sur le dialogue de Propriétés de Connexion à tout moment pour retourner aux paramètres par défaut.

Conseil : Utilisez les dialogues d'informations de connexion pour contrôle la connexion en temps réel. Consultez **Informations de connexion d'accès et de copie** *(à la page 247)*



Optimisé pour : Sélections

Lisibilité du Texte

Lorsque la lisibilité du texte est sélectionnée, tous les modes vidéo sont désignés pour fournir un texte lisible de haute qualité.

Ce paramètre est idéal lors du travail avec des interfaces utilisateur graphiques comme lors de l'éxécution d'administration de serveur etc.

Lorsque vous travaillez en mode couleur complète de la vidéo, une légère accentuation de contraste est fournie, et le texte est plus net.

En modes de qualité vidéo inférieure, la bande passante est diminuée au dépens de la précision.

Précision de couleur

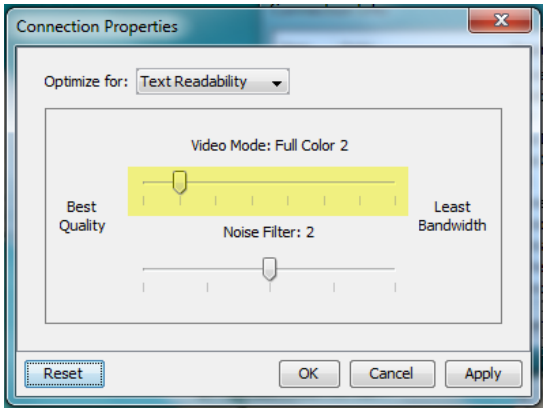
Lorsque la Précision de couleur est sélectionné, tous les modes vidéos sont rendus en couleur complète avec une réponse en couleur plate.

Ce paramètre s'applique à la visualisation de flux vidéo tels que les films ou autres flux de diffusion.

En modes de qualité vidéo inférieure, l'exactitude de fins détails, comme le texte, est sacrifiée.

Mode vidéo

Le slide de Mode vidéo contrôle l'encodage de chaque image vidéo, affectant la qualité de la vidéo, la fréquence et la bande passante.



En généralement, déplacer le slider à gauche entraîne une meilleure qualité au prix d'une plus grande bande passante et dans certains cas, d'une plus petite fréquence.

Déplacer le slider à droite vous permet une compression plus forte, de réduire la bande passante par image, mais la qualité vidéo est réduite.

Dans des situations où la bande passante du système est un facteur limitant, déplacer le slider de mode vidéo à droite peut résulter en de plus hautes fréquences.

Lorsque la Lisibilité du Texte est sélectionné comme paramètre Optimisé, les quatre modes les plus à droite offrent une résolution de couleur réduite ou pas de couleur du tout.

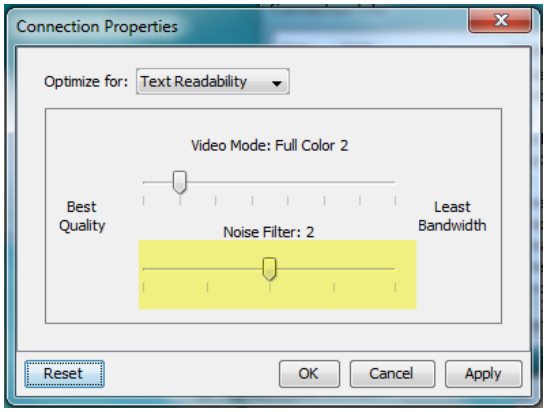
Ces modes sont appropriés pour du travail administratif là où le texte et les éléments de l'interface utilisateur graphique ont la priorité et la bande passante est en prime.

Cliquez sur le dialogue de Propriétés de Connexion à tout moment pour retourner aux paramètres par défaut.

Noise Filter (Filtre antiparasite)

A moins qu'il n'y ait un besoin spécifique de le faire, ne changez pas les paramètres du filtre antiparasite. Le paramètrage par défaut est désigné pour bien fonctionner dans la plupart des situations.

Le filtre antiparasite contrôle la quantité de bruit en interimage absorbée par le KX III.



Déplacer le slide du filtre antiparasite vers des niveaux gauche, le filtre prend une valeur seuil, ce qui entraîne une meilleure qualité vidéo dynamique. Néanmoins plus de bruit est susceptible de passer, résultant en une bande passante plus haute et de plus faibles fréquences.

Déplacer le slider vers la droit, augmente le seuil, permettant moins de bruit et d'utilisation de bande passante. Les artefacts vidéo peuvent être augmentés.

Déplacer le filtre antiparasite sur la droite peut s'avérer utile pour accéder à l'interface d'utilisateur graphique d'un ordinateur via des connexions à bande passante très limitées.

Cliquez sur le dialogue de Propriétés de Connexion à tout moment pour retourner aux paramètres par défaut.

Informations sur la connexion

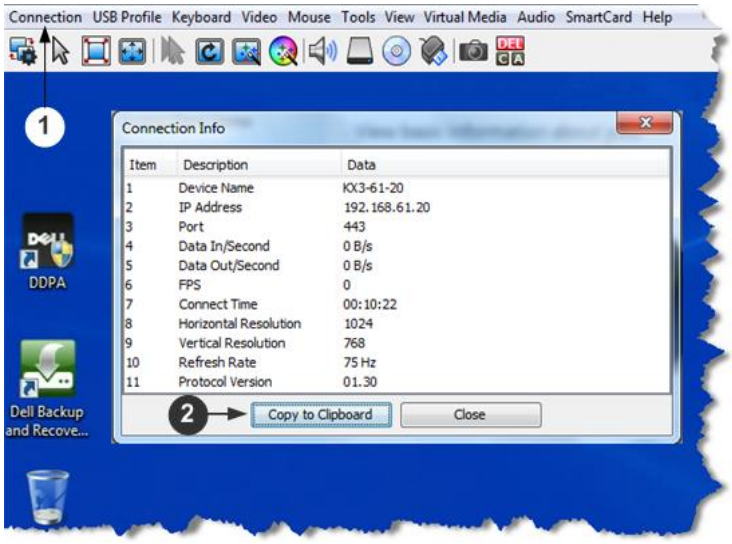
Ouvrez la boîte de dialogue d'Informations sur la connexion pour des informations sur la connexion en temps réel, et copiez les informations de la boîte de dialogue si besoin.

Cela est utile si, par exemple, vous voulez rassembler des informations en temps réel sur votre connexion actuelle. Consultez ***Configurer les propriétés de connexion*** (à la page 242)

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

- Nom KX III - Le nom du KX III.
- Adresse IP - L'adresse IP du KX III.
- Port - Le Port TCP/IP de communication KVM utilisé pour l'accès au KX III.
- Data In/Second (Entrée de données/seconde) - Débit en données par KX III.
- Data Out/Second (Sortie de données/seconde) - Débit en sortie du KX III.
- Connect Time (Temps de connexion) - Durée de connexion.
- FPS - Images vidéo transmises par seconde reçu de KX III.
- Résolution horizontale - La résolution horizontale du serveur cible.
- Résolution verticale - La résolution verticale du serveur cible.
- Taux de rafraîchissement - Taux de rafraîchissement du serveur cible.
- Protocol Version (Version du protocole) - Version des protocoles de communication Raritan.

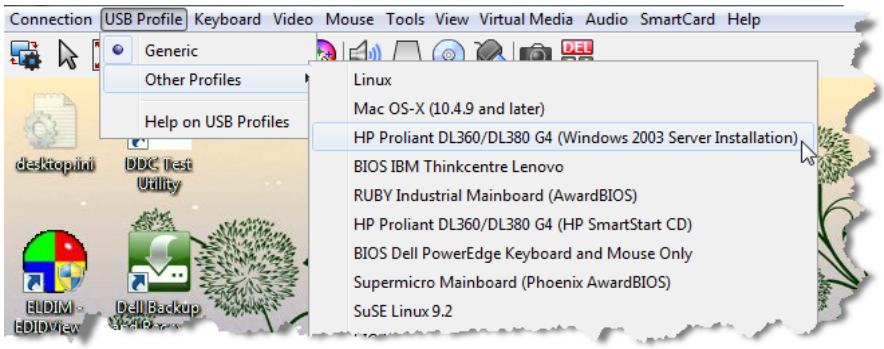
Informations de connexion d'accès et de copie



Procédure	
1	Cliquez sur Connexion > Infos... pour ouvrir la boîte d'infos de connexion.
2	Cliquez sur Copy to Clipboard (Copier dans le Presse-papiers). Collez les informations dans un fichier de votre choix.

Profils USB

Définissez un profil USB pour un serveur cible du Virtual KVM Client (VKC) en cliquant sur Profil USB dans le menu, puis en selectionnant parmi les choix du menu.



Sélectionnez un profil USB qui s'applique le mieux possible au serveur cible KVM.

Par exemple, si le serveur est lancé sur le système d'exploitation Windows®, il est recommandé d'utiliser le profil générique.

Ou si l'utilisateur souhaite modifier les paramètres du menu du BIOS ou effectuer le démarrage à partir d'un lecteur de support virtuel, suivant le modèle du serveur cible, un profil BIOS est sans doute plus adéquat.

Reportez-vous à **Profils USB** (à la page 49) dans l'aide en ligne pour plus d'informations sur les profils USB.

Clavier

Envoyez le Macro Ctrl+Alt+Suppr

En raison de son utilisation fréquente, une macro Ctrl+Alt+Suppr est préprogrammée.

Sélectionnez Clavier > Envoyer Ctrl+Alt+Suppr ou cliquez sur bouton Ctrl+Alt+Delete.

la barre d'outils envoie cette séquence clé au serveur ou au commutateur KVM auquel vous êtes actuellement connecté.

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

Envoyez LeftAlt+Tab

Sélectionnez Clavier > Envoyer LeftAlt + Tab pour basculer entre les fenêtres ouvertes du serveur cible ou du commutateur KVM auquel vous êtes connecté.

Paramétrage des options clavier/souris CIM

Pour accéder au menu de configuration de DCIM-USBG2 :

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

Envoyer du Texte à la Cible

Pour utiliser la fonction Envoyer du Texte à la Cible pour la macro:

1. Cliquez sur Clavier > Envoyer du Texte à la Cible Le texte envoyé à la boîte de dialogue apparaît.
2. Entrez le texte que vous voulez envoyer à la cible.

   Remarque : Les caractères non-anglais ne sont pas pris en charge par la fonction Envoyer du Texte à la Cible.

3. Si la cible utilise une disposition de clavier US/International, cochez la case « le Système cible a une disposition de clavier US/International »
4. Cliquez sur OK.

Macros de clavier

Les macros de clavier garantissent l'envoi des combinaisons de touches destinées au serveur cible et leur interprétation par celui-ci uniquement. Sinon, elles risquent 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. Néanmoins, si vous utilisez un autre PC, vous ne verrez pas vos macros.

Par ailleurs, si une autre personne utilise votre PC et se connecte sous un nom différent, elle verra vos macros puisqu'elles appartiennent à l'ordinateur.

Les macros de clavier crées via le Virtual KVM Client (VKC) ne peuvent pas être utilisés dans l'Active KVM Client (AKC) ou vice versa.

Définir une nouvelle macro

Pour définir une macro :

1. Sélectionnez Clavier > Macros de clavier. La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Cliquez sur Add (Ajouter). La boîte de dialogue 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 devront 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)

   Echap

   Release F4 (Relâcher F4)

   Echap

   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 du champ et recommencer. Si vous cliquez sur OK, la fenêtre Keyboard Macros (Macros de clavier) s'affiche et présente la nouvelle macro de clavier.
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.
9. Sélectionnez la nouvelle macro dans le menu pour l'exécuter ou utilisez les touches affectées à la macro.

Importer des macros

Pour importer des macros :

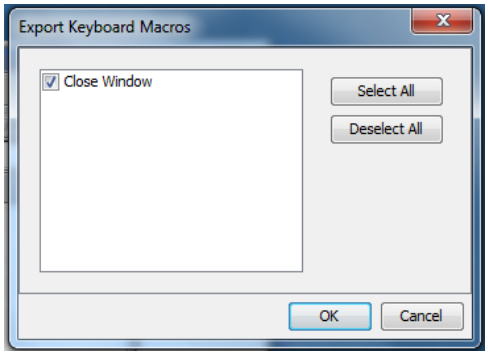
1. Choisissez Clavier > Importer des macros de clavier pour ouvrir la boîte de dialogue Importe des macros. Accédez à l'emplacement du dossier du fichier de macro.

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.

Exporter des macros

1. Choisissez Outils > Exportation de macros pour ouvrir la boîte de dialogue 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 « Exporter des macros de clavier » s'affiche. Localiser et sélectionner le fichier de macro. Par défaut, la macro existe sur votre bureau.
4. Sélectionnez le dossier d'enregistrement du fichier de macro, entrez le nom du fichier et cliquez sur Save (Enregistrer). Si la macro existe déjà, vous recevez un message d'alerte.
5. Sélectionnez Yes (Oui) pour écraser la macro existante ou No (Non) pour fermer l'alerte sans écraser la macro.

Propriétés vidéo

Actualisation de l'écran

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

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

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

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

- Choisissez Vidéo > Actualiser l'écran ou cliquez sur le bouton Actualiser l'écran de la barre d'outils.

Auto-Sense Video Settings (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 Vidéo > Détection automatique des paramètres vidéo ou cliquez sur le bouton Détection automatique des paramètres de la vidéo de la barre d'outils.

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

Calibrage de la couleur

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

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

Pour calibrer la couleur :

- Sélectionnez Vidéo > Calibrer les couleurs ou cliquez sur le bouton de calibrage des couleurs de la barre d'outils.

  Le calibrage des couleurs de l'écran du dispositif cible est mis à jour.

Réglage des paramètres vidéo

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

Pour modifier les paramètres vidéo :

1. Choisissez Vidéo > Paramètres vidéo pour ouvrir la boîte de dialogue de Paramètres vidéo.
2. Définissez les paramètres ci-après, le cas échéant. Les effets sont visibles dès que vous définissez les paramètres :
   a. 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.

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

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

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

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

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

g. Contrast Green : contrôle le signal vert.

h. 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.

---

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

j. 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) :

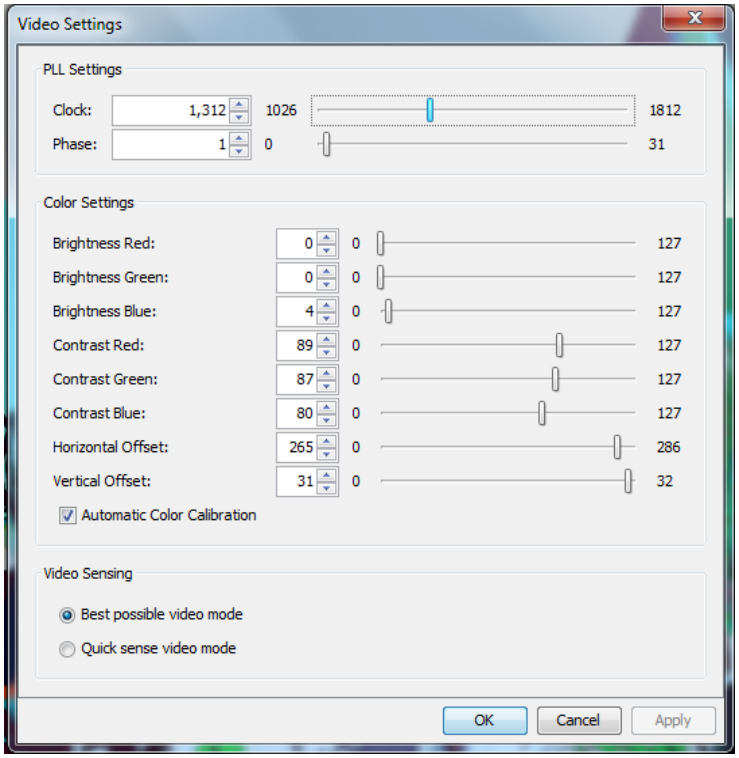
   le dispositif effectue la totalité du processus de détection automatique lorsque vous changez de cibles ou de résolutions cible. La sélection de cette option calibre la vidéo pour obtenir la qualité d'image optimale.

   - 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.



Capture d'écran de la commande cible (Capture d'écran de la cible)

Vous pouvez effectuer une capture d'écran d'un serveur cible à l'aide de la commande serveur Screenshot from Target (Capture d'écran de la cible). Si besoin, enregistrez cette capture d'écran dans une location de votre choix en tant que fichier bitmap, JPEG ou PNG.

Pour effectuer une capture d'écran du serveur cible :

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

Options de souris

En mode souris double et si l'option est configurée correctement, les curseurs de la souris sont alignés.

En mode souris double, lorsque vous contrôlez un serveur cible, la Console distante affiche deux curseurs de souris: l'un appartenant à votre station de travail KX III et l'autre appartenant au serveur cible.

Vous avez la possibilité d'opérer en mode souris simple ou en mode souris double.

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

- Absolue (Synchronisation de la souris)
- Intelligente (Mode souris)
- Standard (Mode souris)

Lorsque le pointeur de votre souris se trouve dans la zone de la fenêtre du serveur cible du client KVM, 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 utiliser le mode souris simple et visualiser seulement le pointeur du serveur cible.

Vous pouvez basculer entre ces deux modes souris (simple et double).

Modes souris double

Synchronisation absolue de la souris

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 CIMs de média virtuel.

Synchronisation absolue de la sourisrequière l'utilisation d'un CIM média virtuel:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Pour entrer en mode synchronisation absolue :

- Sélectionnez Souris > Absolue.

Notez que le connecteur noir des CIM DVUSB est utilisé pour le clavier et la souris. Le connecteur gris est utilisé pour le support virtuel.

Laissez les deux prises du CIM branchées sur le dispositif. Le dispositif risque de ne pas fonctionner correctement si les deux prises ne sont pas branchées sur le serveur cible.

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.

Entrer en mode souris intelligente

Pour entrer en mode souris intelligente :

- Choisissez Souris > 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 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.

Conseils de synchronisation de la souris

Si vous avez un problème de synchronisation de souris:

1. Vérifiez que la résolution vidéo et le taux de rafraîchissement sélectionnés sont pris en charge par le dispositif. La boîte de dialogue d'Infos de Connexion Client KVM affiche les véritables valeurs que le dispositif voit.
2. Forcez la détection automatique en cliquant sur le bouton de détection automatique du Client KVM.
3. 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.
4. Cliquez sur le bouton « Synchronisation de la souris du Client KVM » .

Synchroniser votre souris

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

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

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

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

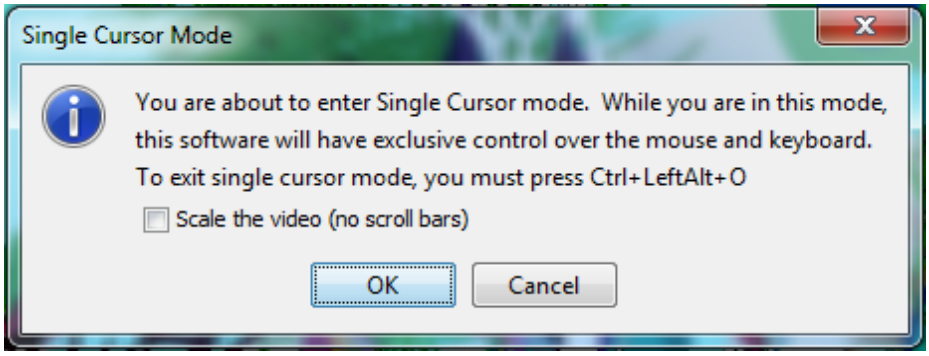
Mode souris unique

Le mode souris simple utilise uniquement le curseur de la souris du serveur cible ; le pointeur de souris locale n'apparaît plus à l'écran.

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

Pour passer en mode souris simple, procédez comme suit :

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



Pour quitter le mode souris simple :

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

Options d'outils

Paramètres généraux

Pour définir les options d'outils :

1. Cliquez sur Outils > Options. La boîte de dialogue Options s'affiche.
2. Cochez la case Enable Logging (Activer la journalisation) uniquement si le support 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
   - United Kingdom
   - Coréen (Corée)
   - Français (Belgique)
   - Norvégien (Norvège)
   - Portugais (Portugal)
   - Danois (Danemark)
   - Suédois (Suède)
   - Allemand (Suisse)
   - Hongrois (Hongrie)
   - Espagnol (Espagne)
   - Italien (Italie)
   - Slovène
   - Traduction : Français - US
   - Traduction : Français - US International

   Dans AKC, le type de clavier provient par défaut du client local, cette option ne s'applique donc pas.
4. Configurez les raccourcis-clavier :

- Exit Full Screen Mode (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).

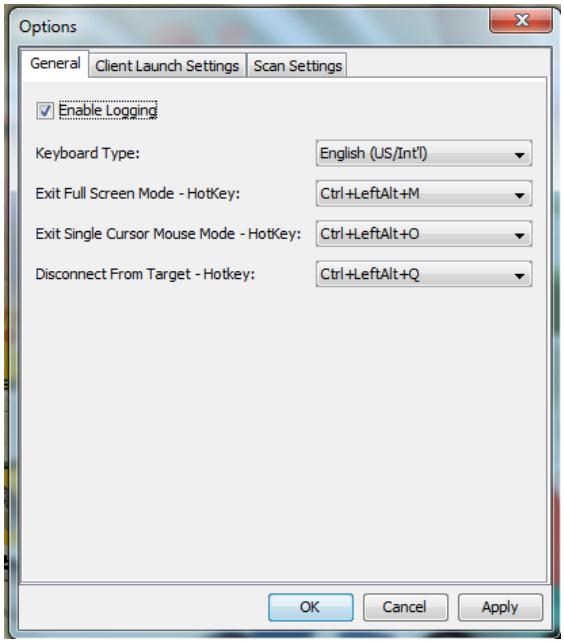
  Activez ce raccourci-clavier pour permettre aux utilisateurs de se déconnecter rapidement de la cible.

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.

Pour configurer les paramètres de lancement client :

1. Cliquez sur 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.

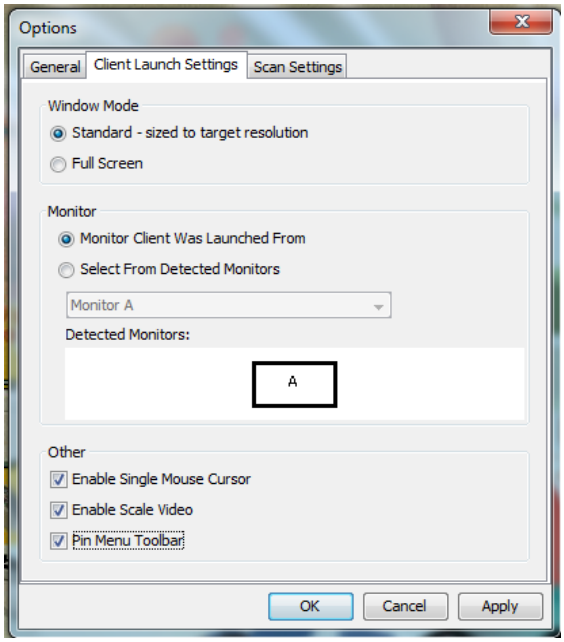
- Pour configurer des paramètres de lancement supplémentaires :

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 automatiquement à l'échelle l'affichage sur le serveur cible lors de l'accès à celui-ci.

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

3. Cliquez sur OK.



Configuration des paramètres de balayage de ports dans VKC et AKC

Configurer des paramètres de balayage de ports dans VKC et AKC s'applique au balayage à partir de la Console KX III à Distance.

Pour configurer les options de balayage de port de la Console Locale, consultez ***Configurer les paramètres de balayage de la Console Locale*** (à la page 304)

Utilisation la fonction de balayage des ports 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 Balayage des ports - Console à distance

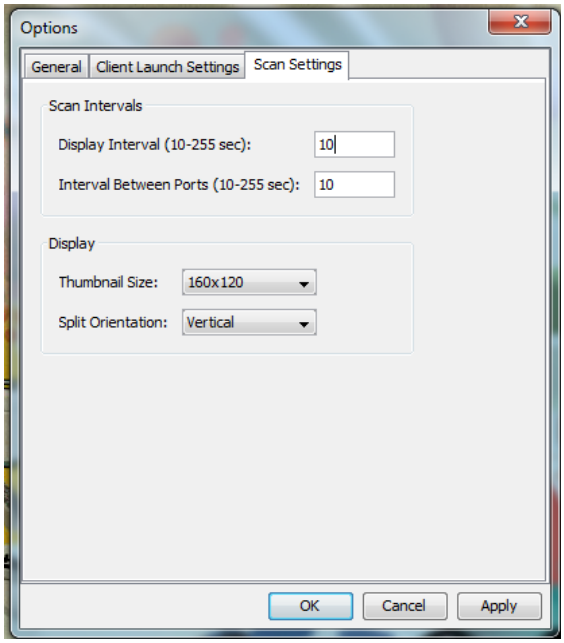
L'onglet Scan Settings (Paramètres de balayage) permet de personnaliser l'intervalle de balayage et des options d'affichage par défaut.

Configurer le balayage des ports

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 Vue > 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 262).

En mode Plein écran, placez la souris au sommet de l'écran pour afficher la barre de menus du mode Plein écran.

Pour que la barre de menus reste visible en mode Plein écran, activez l'option Pin Menu Toolbar (Epingler la barre d'outils de menu) de la boîte de dialogue Tool Options (Options d'outils). Reportez-vous à ***Options d'outils*** (à la page 262).

Pour entrer en mode Plein écran :

- Choisissez Vue > Plein écran, ou cliquez sur le bouton 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.

Support virtuel

Tous les modèles KX III prennent en charge la fonction Support virtuel. La fonction Support virtuel prolonge les capacités KVM en permettant aux serveurs cible KVM d'accéder à distance aux supports des serveurs de fichiers de PC clients et réseau.

Grâce à cette fonction, les supports montés sur les serveurs de fichiers de PC clients et réseau sont « intégrés virtuellement » au serveur cible. Le serveur cible peut ensuite lire et écrire sur ce support comme si ce dernier lui était physiquement connecté.

Chaque KX III est équipé de la fonction Support virtuel pour autoriser la gestion à distance des tâches à l'aide d'une vaste gamme de lecteurs de CD ou de DVD, USB, de dispositifs de lecture et d'enregistrement audio internes et distants, et d'images.

Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement 128 ou 256 bits AES ou RC4.

Conditions requises pour l'utilisation des supports virtuels

Prérequis KX III

- 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.
- Si vous voulez utiliser le Partage de PC lesparamètres de sécurité doivent également être activés sur la page de Paramètres de Sécurité. **Facultatif**
- Vous devez choisir le profil USB correct pour le serveur cible KVM auquel vous vous connectez.

Ordinateur distant (Remote PC)

- Certaines options de supports virtuels 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.
- Les ports USB 2.0 sont rapides et plus appropriés.

CIM requis pour support virtuel

Vous devez utiliser l'un des CIM suivants pour utiliser le support virtuel:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Notez que le connecteur noir des CIM DVUSB est utilisé pour le clavier et la souris. Le connecteur gris est utilisé pour le support virtuel.

Laissez les deux prises du CIM branchées sur le dispositif. Le dispositif risque de ne pas fonctionner correctement si les deux prises ne sont pas branchées sur le serveur cible.

Montage des lecteurs locaux

Cette option permet de monter un lecteur entier, ce qui signifie que le lecteur de disque entier est monté virtuellement sur le serveur cible.

Utilisez-la uniquement pour les disques durs et les lecteurs externes. Ceux-ci ne comprennent pas les lecteurs réseau, CD-ROM ou DVD-ROM.

Notes sur le montage de lecteurs locaux

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

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

Tâches prise en charge Via Support Virtuel

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

- Le transfert de fichiers ;
- La réalisation de diagnostics ;
- L'installation ou la correction d'applications ;
- L'installation complète du système d'exploitation.
- L'enregistrement et la lecture audionumériques.

Types de supports média virtuels

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

- Disques durs internes et externes
- 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.

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 clients Linux® et Mac®
- 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)

Systèmes d'exploitation pour support média virtuel pris en charge

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

- Système d'exploitation Windows® 7
- Système d'exploitation Windows® 8
- Système d'exploitation Windows XP®
- openSUSE® 11.4 Celadon (x86_64)
- Fedora® 18
- RHEL® 6.4
- OSX Mountain Lion® 10.7 (et supérieur)
- Solaris® 10

Le Active KVM Client (AKC) peut être utilisé pour monter plusieurs types de média virtuel mais seulement pour les systèmes d'exploitation Windows.

Nombre de disques média virtuel pris en charge

Avec la fonction Support virtuel, vous pouvez monter jusqu'à deux lecteurs (de types différents) pris en charge par le profil USB actuellement appliqué 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 » de supports virtuels du CD-ROM demeure ouvert afin que vous puissiez monter un autre CD-ROM virtuellement. Ces « canaux » de supports virtuels restent ouverts jusqu'à la fermeture de la session KVM tant que le profil USB la prend en charge.

Pour utiliser le support virtuel, connectez/reliez-le au serveur de fichiers réseau ou client auquel vous souhaitez accéder à partir du serveur cible.

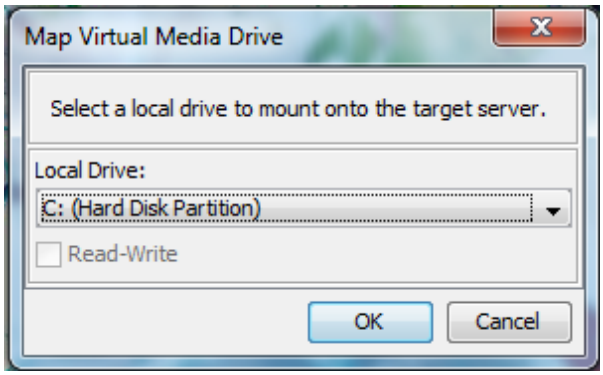
Ceci n'est pas nécessairement la première étape mais elle doit être effectuée avant de tenter d'accéder au support.

Connexion et déconnexion d'un média virtuel

Accès à un disque média virtuel sur un Ordinateur Client

Pour accéder à un lecteur virtuel de l'ordinateur client :

1. Dans le Virtual KVM Client, sélectionnez Supports virtuels > Connecter le lecteur ou cliquez sur le bouton 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).

   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 273) 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.

3. 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 le Virtual KVM Client, sélectionnez Supports virtuels > Connectez l'image CD-ROM/ISO ou cliquez sur le bouton Connecter CD-ROM/ISO . 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 sur des fichiers sur une cible Linux®, utilisez la commande Sync 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®, le 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.

Connexion et déconnexion de disques média virtuels

Pour déconnecter les lecteurs de supports virtuels :

- Pour les lecteurs locaux, sélectionnez Supports virtuels > Déconnecter le lecteur.
- Pour les images ISO, CD-ROM et DVD, sélectionnez Supports Virtuels > 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.

Supports virtuels dans un environnement Windows XP

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

Supports virtuels dans un environnement Linux

Partitions système actives

Vous ne pouvez pas monter de partitions système actives à partir d'un client Linux.

Les partitions de lecteur Ext3/4 Linux doivent être démontées à l'aide du libellé umount /dev/ avant d'établir une connexion au support virtuel.

Partitions de lecteur

Les limites en matière de partition de lecteur suivantes existent à travers les systèmes d'exploitation :

- Les cibles Windows® et Mac ne peuvent pas lire les partitions formatées Linux.
- Windows et Linux ne peuvent pas lire les partitions formatées Mac.
- Seules les partitions FAT Windows sont prises en charge par Linux.

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.

Pour éviter ces problèmes, vous devez être utilisateur racine.

Supports virtuels dans un environnement Mac

Partitions système actives

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

Partitions de lecteur

Les limites en matière de partition de lecteur suivantes existent à travers les systèmes d'exploitation :

- Les cibles Windows® et Mac ne peuvent pas lire les partitions formatées Linux.
- Windows ne peut pas lire les partitions formatées Mac.
- Les formats 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.

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

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

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

Utilisez la page File Server Setup (Configuration des serveurs de fichiers) de la console distante pour spécifier les serveurs de fichiers et les chemins d'accès aux images auxquelles vous souhaitez accéder à l'aide de la fonction Support virtuel. Les images ISO de serveurs de fichiers spécifiées ici sont disponibles dans les listes déroulantes Remote Server ISO Image Hostname (Nom d'hôte des images ISO de serveur distant) et Image de la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels). Reportez-vous à ***Montage des images CD-ROM/DVD-ROM/ISO*** (à la page 275).

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

1. Sélectionnez Virtual Media (Supports virtuels) dans la console distante. La page File Server Setup (Configuration des serveurs de fichiers) s'ouvre.

2. Cochez la case Selected (Sélectionné) pour tous les supports qui seront accessibles comme supports virtuels.
3. Entrez les informations relatives aux images ISO de serveur de fichiers auxquelles vous souhaitez accéder :
   - IP Address/Host Name - Nom d'hôte ou adresse IP du serveur de fichiers.
   - Image Path - Nom complet du chemin d'accès à l'emplacement de l'image ISO. Par exemple, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, etc.

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

Remarque : Si vous vous connectez à un serveur Windows 2003® et tentez de charger une image ISO à partir de ce serveur, vous risquez de recevoir un message d'erreur indiquant : « Echec du montage du support virtuel. Impossible de connecter le serveur de fichiers ou nom d'utilisateur et mot de passe du serveur de fichiers erroné ». Impossible de se connecter au serveur de fichier ou incorrects fichier nom d'utilisateur et mot de passe du serveur ". Si cela se produit, désactiver « Serveur Réseau Microsoft: Communications signées digitalement » option sur le serveur dans les contrôleurs de domaine des politiques.

Cartes à puce

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

Pour obtenir la liste des cartes à puce et des lecteurs de cartes à puce pris en charge, ainsi que des exigences système supplémentaires, reportez-vous à ***Lecteurs de cartes à puce pris en charge ou non et Configuration système minimale requise*** (voir "***Configuration Smart Card minimale requise, CIM et lecteurs de cartes à puce pris en charge/ non supportés.***" à la page 280).

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

Le montage des lecteurs de cartes à puce est également pris en charge depuis la console locale.

Reportez-vous à ***Accès par carte à puce à la console locale*** (à la page 306) dans l'aide de Dominion.

Configuration Smart Card minimale requise, CIM et lecteurs de cartes à puce pris en charge/ non supportés.

Avant que vous commenciez à utiliser un lecteur de cartes à puce, revoyez les choses suivantes:

- ***Configuration système minimum pour carte à puce*** (à la page 343)
- ***Spécifications des CIM pris en charge*** (à la page 336)
- Lecteurs de cartes à puce pris en charge ou non

Authentication lors de l'accès à un lecteur de carte à puces

Lorsque vous accédez à un serveur à distance, vous avez la possibilité de sélectionner un lecteur de cartes à puce branché et de le monter sur le serveur.

L'authentification par carte à puce est utilisée avec le serveur cible, et non pour se connecter au dispositif. Aussi, les modifications apportées aux codes PIN et aux informations d'authentification ne nécessitent pas de mises à jour des comptes de dispositifs.

Mode PC Partagé et Paramètres de Confidentialité lors de l'utilisation de cartes à puce.

Lorsque le mode PC-Share est activé sur le dispositif, plusieurs utilisateurs peuvent partager l'accès à un serveur cible.

Cependant, lorsqu'un lecteur de cartes à puce est connecté à une cible, le dispositif imposera la confidentialité quel que soit le paramètre du mode PC-Share.

De plus, si vous rejoignez une session partagée sur un serveur cible, le montage du lecteur de cartes à puce sera désactivé jusqu'à ce qu'un accès exclusif au serveur cible soit disponible.

Lecteurs de cartes à puce détecté

Une fois qu'une session KVM est établie vers le serveur cible, un menu de Carte à puce et un bouton sont disponibles dans le VKC et AKC.

Lorsque le bouton Carte à puce est sélectionné ou que Carte à puce est selectionné dans le menu, les lecteurs de carte à puce qui sont détectés comme attachés au client distant sont affichés dans une boite de dialogue.

A partir de cette boîte de dialogue, vous pouvez relier des lecteurs de cartes à puce supplémentaires, actualiser la liste de lecteurs de cartes à puce reliés à la cible et déconnecter ces derniers.

Vous pouvez également retirer ou réinsérer une carte à puce. Cette fonction permet d'envoyer une notification au système d'exploitation d'un serveur cible qui nécessite le retrait ou la réinsertion afin d'afficher la boîte de dialogue de connexion qui convient. L'utilisation de cette fonction permet l'envoi de la notification vers une cible unique sans affecter les autres sessions KVM actives.

Monter un lecteur de cartes à puce

Une fois montés sur le serveur cible, le lecteur de cartes et la carte à puce forceront le serveur à se comporter comme s'ils étaient directement connectés.

Le retrait de la carte à puce ou du lecteur de cartes entraînera le verrouillage de la session utilisateur ou vous serez déconnecté suivant la stratégie de retrait de la carte définie dans le système d'exploitation du serveur cible.

Lorsque la session KVM est arrêtée, parce qu'elle a été fermée ou parce que vous êtes passé sur une autre cible, le lecteur de cartes à puce est automatiquement démonté du serveur cible.

Pour monter un lecteur de cartes à puce à partir d'un VKC ou AKC :

1. Cliquez sur le menu Smart Card, puis sélectionnez Smart Card Reader (Lecteur de cartes à puce). Vous pouvez également cliquer sur le bouton Smart Card de la barre d'outils.
2. Sélectionnez le lecteur de cartes à puce dans la boîte de dialogue Select Smart Card Reader (Sélectionner un lecteur de cartes à puce).
3. Cliquez sur Mount (Monter).

4. Une boîte de dialogue de progression s'ouvre. Cochez la case Mount selected card reader automatically on connection to targets (Monter le lecteur de cartes à puce sélectionné automatiquement lors de la connexion aux cibles) pour monter le lecteur automatiquement la prochaine fois que vous vous connectez à une cible. Cliquez sur OK pour démarrer le montage.

Mettre à jour un lecteur de cartes à puce

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

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

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

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

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

Démonter (Retirer) un Lecteur de Carte à Puce

Pour démonter un lecteur de cartes à puce :

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

Audionumérique

Le KX III prend en charge les connexions audionumériques bidirectionnelles de bout en bout pour les dispositifs audionumériques de lecture et de capture entre un client distant et un serveur cible.

Les dispositifs audio sont accessibles via une connexion USB.

Le firmware du dispositif actuel est requis.

L'un des CIM suivants doit être utilisé:

- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

Les systèmes d'exploitation clients Windows®, Linux® et Mac® sont pris en charge : La Virtual KVM Client (VKC) et Active KVM Client (AKC) prend en charge les connexions aux dispositifs audio.

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

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

- ***Formats de dispositifs audio pris en charge*** (à la page 283)
- ***Recommandations en matière de ports vidéo doubles*** (à la page 223)
- ***Modes souris pris en charge*** (voir "***Modes de souris pris en charge pour les groupes de deux ports vidéo***" à la page 223)
- ***CIM requis pour la prise en charge de vidéo double*** (à la page 224)
- Remarques d'informations**, *Audio*** (à la page 372)

Formats de dispositifs audio pris en charge

KX III prend en charge un dispositif de lecture et de capture, et un dispositif d'enregistrement simultanément. Les formats de dispositifs audio suivants sont pris en charge :

- Stéréo 16 bits, 44,1 K
- Mono 16 bits, 44,1 K
- Stéréo 16 bits, 22,05 K
- Mono 16 bits, 22,05 K
- Stéréo 16 bits, 11,025 K
- Mono 16 bits, 11,025 K

Recommandations et exigences en matière de lecture et de capture audio

Niveau sonore

- Réglez le son de la cible à un niveau intermédiaire.

  Par exemple, sur un client Windows®, réglez l'audio à 50 ou moins.

Ce paramètre doit être configuré depuis le dispositif audio de lecture ou de capture, et non depuis le contrôle du dispositif audio du client.

Recommandations en matière de connexions audio lorsque le mode PC Share est activé

Si vous utilisez la fonction audio lors de l'exécution du mode PC Share, la lecture et la capture audio sont interrompues si un dispositif audio supplémentaire est connecté à la cible.

Par exemple, l'utilisateur A connecte un dispositif de lecture à Cible1 et exécute une application de lecture audio ; l'utilisateur B connecte ensuite un dispositif de capture à la même cible. La session de lecture de l'utilisateur A est interrompue et l'application audio devra peut-être redémarrée.

L'interruption a lieu car le dispositif USB doit être énuméré à nouveau avec la configuration du nouveau dispositif.

L'installation d'un pilote pour le nouveau dispositif par la cible peut prendre du temps.

Les applications audio peuvent arrêter complètement la lecture, passer à la piste suivante ou poursuivre la lecture.

Le comportement exact dépend de la façon dont l'application audio est conçue pour traiter un événement de déconnexion/reconnexion.

Exigences en matière de bande passante

Le tableau ci-dessous détaille les exigences en matière de bande passante de lecture et de capture audio pour le transport du son sur chaque format sélectionné.

Format audio	Bande passante réseau requise
44,1 KHz, stéréo 16 bits	176 Ko/s
44,1 KHz, mono 16 bits	88,2 Ko/s
2,05 KHz, stéréo 16 bits	88,2 Ko/s
22,05 KHz, mono 16 bits	44,1 Ko/s
11,025 KHz, stéréo 16 bits	44,1 Ko/s

Format audio	Bande passante réseau requise
11,025 KHz, mono 16 bits	Audio 22,05 Ko/s

Dans la pratique, la bande passante utilisée pour connecter un dispositif audio à une cible est plus importante en raison des données de clavier et vidéo consommées lors de l'ouverture et de l'utilisation d'une application audio sur la cible.

En règle générale, nous vous recommandons une connexion d'au moins 1,5 Mo avant d'exécuter la lecture et la capture.

Toutefois, un contenu vidéo important, des connexions en couleurs avec des résolutions d'écran élevées sur la cible consomment beaucoup plus de bande passante et affectent considérablement la qualité sonore.

Les paramètres clients recommandés permettent de réduire l'effet de la vidéo sur la qualité sonore avec des bandes passantes inférieures :

- Connectez les dispositifs de lecture audio à des formats de qualité inférieure. La consommation de bande passante par la vidéo affecte moins les performances avec des connexions de 11k que de 44k.
- Paramétrez la vitesse de connexion sous Connection Properties (Propriétés de connexion) sur une valeur correspondant le mieux à la connexion client-serveur.
- Sous Connection Properties, paramétrez le nombre de couleurs sur la valeur la plus basse possible. La réduction à une couleur de 8 bits réduit la consommation de bande passante.
- Paramétrez le lissage sur High (Elevé). Ceci améliorera l'apparence de la vidéo cible en réduisant le bruit de la vidéo affichée.
- Sous Video settings (Paramètres vidéo), paramétrez Noise Filter (Filtre antiparasite) sur 7 (valeur maximale) afin de réduire l'utilisation de bande passante pour les changements d'écran cible.

Enregistrement des paramètres audio

Les paramètres de dispositif audio sont appliqués sur la base du produit KX III.

Une fois ces paramètres configurés et enregistrés sur KX III, les même paramètres lui sont appliqués.

Par exemple, vous pouvez configurer un dispositif audio Windows® afin d'utiliser un format stéréo 16 bits, 44.1 K.

Lorsque vous vous connectez à des cibles différentes et utilisez ce dispositif audio Windows, le format stéréo 16 bits, 44,1 K est appliqué à chaque serveur cible.

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

Reportez-vous à ***Connexion et déconnexion d'un dispositif audionumérique*** (à la page 288) pour obtenir des informations sur la connexion et la configuration d'un dispositif audio, et à Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio) pour en savoir plus sur les paramètres de la mémoire-tampon des dispositifs audio.

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

Ainsi, lorsqu'un utilisateur rejoint une session audio, les paramètres de la machine cible sont utilisés. Reportez-vous à ***Connexion à plusieurs cibles depuis un client distant unique*** (à la page 287).

Connexion à plusieurs cibles depuis un client distant unique

Connexion audio jusqu'à quatre (4) serveurs cibles en même temps à partir d'un client à distance unique.

Reportez-vous à ***Connexion et déconnexion d'un dispositif audionumérique*** (à la page 288) pour obtenir des informations sur la connexion à des dispositifs audio.

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

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

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

Système d'exploitation Audio Playback Support

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

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

Connexion et déconnexion d'un dispositif audionumérique

Les paramètres de dispositif audio sont appliqués sur la base du produit KX III.

Une fois ces paramètres configurés et enregistrés sur KX III, les même paramètres lui sont appliqués.

Reportez-vous à ***Enregistrement des paramètres audio*** (à la page 286) pour plus d'informations.

Remarque : Si vous utilisez la fonction audio lors de l'exécution des modes PC Share et VM Share, reportez-vous à **Recommandations et exigences en matière de lecture et de capture audio** *(à la page 284). Consultez également* **Connexion à plusieurs cibles depuis un client distant unique** *(à la page 287).*

Connexion à un Dispositif audio digital

Pour vous connecter à un dispositif audio :

1. Connectez le dispositif audio au PC client distant avant de lancer la connexion par navigateur à KX III.
2. Connectez-vous à la cible à partir de la page Port Access (Accès aux ports).
3. Une fois connecté, cliquez sur le bouton audio de la barre d'outils.

   La boîte de dialogue Connect Audio Device (Connexion au dispositif audio) apparaît. Une liste des dispositifs audio disponibles connectés au PC client distant s'affiche.

   Remarque : Si aucun dispositif audio disponible n'est connecté au PC client distant, l'icône Audio est estompée.
4. Cochez Connect Playback Device (Connexion à un dispositif de lecture) si vous vous connectez à un dispositif de lecture.
5. Dans la liste déroulante, sélectionnez le dispositif à connecter.
6. Sélectionnez le format audio du dispositif de lecture dans la liste déroulante: Format.

   Remarque : Sélectionnez le format que vous souhaitez utiliser en fonction de la bande passante réseau disponible. Les formats à taux d'échantillonnage plus bas consomment moins de bande passante et peuvent tolérer une congestion du réseau plus importante.
7. Cochez Connect Recording Device (Connexion à un dispositif d'enregistrement) si vous vous connectez à un dispositif d'enregistrement.

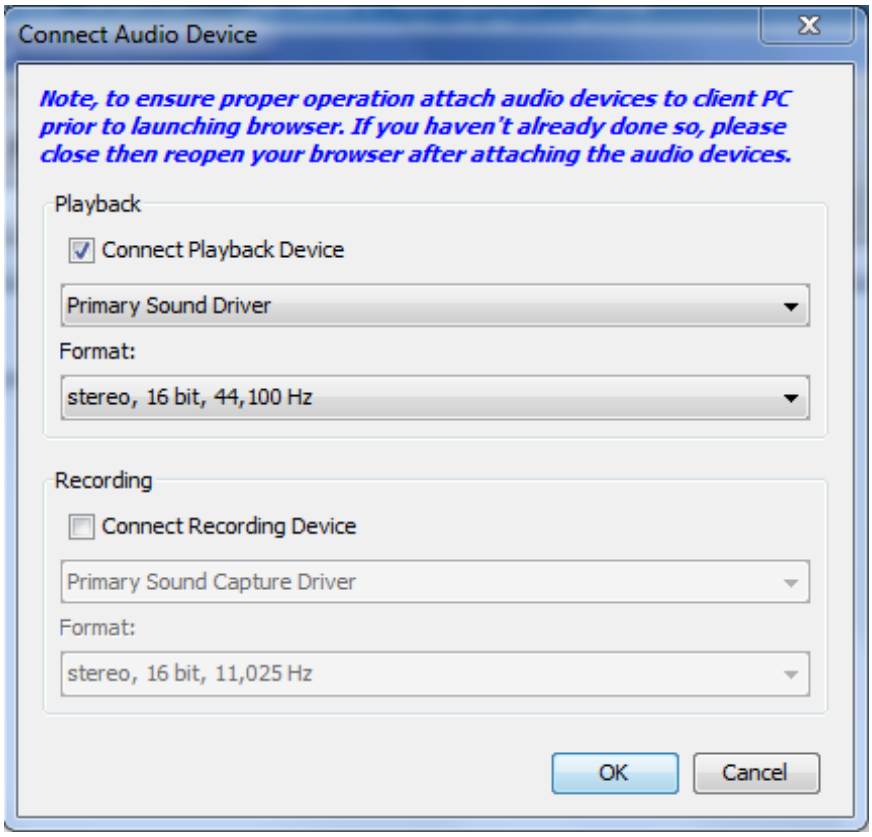
Remarque : Le nom des dispositifs recensés dans la liste déroulante Connect Recording Device (Connexion d'un dispositif d'enregistrement) est tronqué à 30 caractères au plus pour les clients Java.

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

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

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

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



Déconnexion d'un Dispositif audio

Pour vous déconnecter du dispositif audio :

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

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

Lorsqu'un dispositif audio est connecté, la taille de la mémoire-tampon de capture et de lecture peut être ajustée si nécessaire.

Cette fonction permet de contrôler la qualité du son, qui peut être affectée par les limitations de bande passante ou les pointes de réseau.

Augmenter la taille de la mémoire-tampon améliore la qualité audio mais risque d'affecter le débit.

La taille de mémoire-tampon maximum est de 400 millisecondes ; une taille supérieure affecterait énormément la qualité audio.

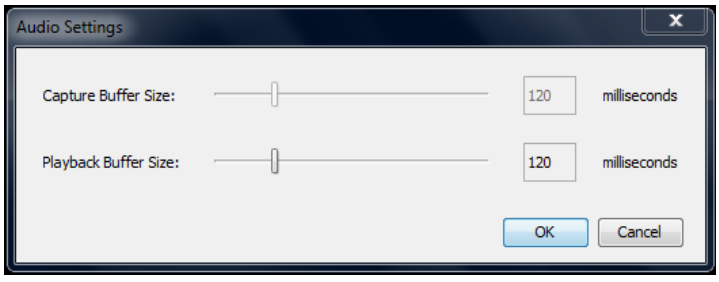
Elle peut être ajustée lorsque nécessaire, pendant une session audio notamment.

Les paramètres audio sont configurés dans le VKC ou AKC.

Ajuster les Paramètres Audio

Pour régler les paramètres audio :

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



Informations de version - Virtual KVM Client

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 6 Aide Active pour Client KVM (AKC)

Dans ce chapitre

Présentation 292
Se connecte à un serveur cible 293
Framework Microsoft NET AKC prise en charge 293
Systèmes d'exploitation pris en charge par AKC 294
Navigateurs pris en charge par AKC 294
Conditions requises pour l'utilisation d'AKC 294

Présentation

L'Active KVM Client (AKC) est basé sur la technologie Microsoft Windows .NET®.

Cela vous permet d'exécuter le client dans des environnements Windows sans utiliser Java Runtime Environment (JRE), qui est obligatoire pour exécuter Virtual KVM Client (VKC) et Multi-Platform Client (MPC) de Raritan..

AKC fonctionne également avec CC-SG.

AKC fournit les mêmes fonctions que VKC à l'exception des suivantes:

- Les macros de clavier créées dans AKC ne peuvent pas être utilisées dans VKC.
- Configuration de l'accès direct aux ports (reportez-vous à Activation d'un accès direct aux ports via URL.)
- Configuration de la validation de certification du serveur AKC (reportez-vous à ***Conditions requises pour l'utilisation d'AKC*** (à la page 294).)
- AKC charge automatiquement les favoris, VKC ne le fait pas. Reportez-vous à Gestion des favoris.

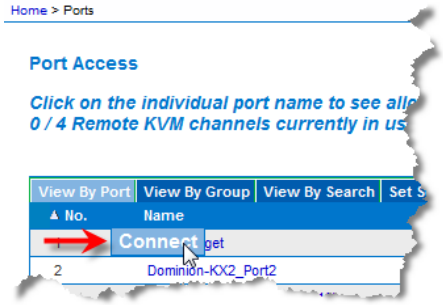
Pour plus de détails sur l'utilisation des fonctions, consultez ***Aide pour Client KVM Virtuel (VKC)*** (voir "***Aide Virtuelle pour Client KVM (VKC)***" à la page 240).

Se connecte à un serveur cible

Une fois que vous vous êtes connecté au KX III à Distance, accédez aux serveurs cible via le Virtual KVM Client (VKC) ou l'Active KVM Client (AKC).

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

1. Sur la page d'accès au Port, cliquez sur le nom du port du serveur cible auquel vous souhaitez vous connecter. Le menu Port Action (Action des ports) s'ouvre.
2. Cliquez sur Connect (Connecter).



Reportez-vous à ***Port Action Menu (Menu d'action de ports)*** (à la page 20) pour plus d'informations sur les options de menu supplémentaires disponibles.

Framework Microsoft NET AKC prise en charge

Le Client Actif KVM (AKC) requiert la version 4.0 ou 4.5 de Windows .NET®. AKC fonctionne avec les deux versions, 3.5 et 4.0, installées.

Systèmes d'exploitation pris en charge par AKC

Lorsqu'il est lancé depuis Internet Explorer®, AKC permet d'atteindre les serveurs cible via KX III.

AKC est compatible avec les plates-formes suivantes :

- Système d'exploitation Windows XP®
- Système d'exploitation Windows Vista® (jusqu'à 64 bits)
- Système d'exploitation Windows 7® (jusqu'à 64 bits)
- Système d'exploitation Windows 8® (jusqu'à 64 bits)

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

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

Remarque : Raritan recommande aux utilisateurs du système d'exploitation Windows XP® de vérifier qu'ils ont une version fonctionnelle de .NET 3.5 ou 4.0 déjà installée avant de lancer AKC. Si vous n'avez pas vérifié votre version de .NET, vous pourrez être invité à télécharger un fichier au lieu de recevoir le message par défaut vous invitant à vérifier votre version .NET.

Navigateurs pris en charge par AKC

- Internet Explorer® 8 (et supérieur)

  Si vous tentez d'ouvrir AKC à partir d'un navigateur autre qu'IE 8 ou supérieur, vous recevrez un message d'erreur vous demandant de vérifier votre navigateur et d'utiliser Internet Explorer.

Conditions requises pour l'utilisation d'AKC

Autoriser les cookies

Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.

Inclure l'adresse IP de KX III dans la 'Zone des sites de confiance'

Les utilisateurs de serveurs Windows Vista®, Windows® 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur.

Désactiver le 'Mode Protégé'

Les utilisateurs de serveurs Windows Vista®, Windows® 7 et Windows 2008 doivent s'assurer que le Mode Protégé n'est pas activé lorsqu'ils accèdent au KX III.

Activer la validation du certificat du serveur de téléchargement AKC

Si l'administrateur du dispositif (ou CC-SG) a activé l'option Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC) :

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

Pour lancer AKC depuis le client Admin CC-SG, vous devez disposer de JRE™ 1.7.x (ou supérieur).

Chapitre 7 Console locale KX III - Assistance d'utilisateur final KX III

Dans ce chapitre

Présentation 296
Accès à un serveur cible 296
Résolutions vidéo de la Console locale....297
Utilisateurs simultanés....297
Raccourcis-clavier et touches de connexion....298
Balayage des ports - Console locale....301
Accès par carte à puce à la console locale....306
Options de profil USB de la console locale....307
Réinitialisation des paramètres d'usine de la Console locale KX III 308
Réinitialisation de KX IIII à l'aide du bouton de réinitialisation sur le dispositif....309

Présentation

L'interface de la Console Locale donne accès au KX III sur le rack.

Cette section contient de l'aide sur les tâches effectuées par les utilisateurs finaux dans la Console locale.

Accès à un serveur cible

Pour accéder à un serveur cible :

1. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.
2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. L'affichage vidéo bascule sur l'interface du serveur cible.

Résolutions vidéo de la Console locale

Une fois qu'un moniteur est connecté à la Console locale KX III, KX III détecte la résolution native du moniteur. Il s'agit typicalement de la plus haute résolution d'écran prise en charge par le moniteur.

Tant que la résolution native du moniteur est prise en charge par la Console locale, KX III utilise cette résolution.

Si la résolution native n'est pas prise en charge par la Console locale, et qu'aucune autre résolution n'est prise en charge par le moniteur et la Console locale, KX III utilise la résolution du dernier moniteur connecté à la Console locale.

Par exemple, vous connectez un moniteur ayant une résolution de 1600x1200 à 60Hz à la Console locale. KX III utilise la résolution étant donné qu'elle est prise en charge par la Console locale.

Si le moniteur que vous connectez ensuite à la Console locale n'est pas défini sur une résolution prise en charge, KX III utilise la résolution de 1024x768@60.

Pour une liste des résolutions vidéo prise en charge par la Console locale, consultez ***Résolutions DVI de Port Local KX III prises en charge*** (à la page 336).

Pensez également à consulter ***Remarques sur les Modes et résolutions vidéo*** (voir "***Modes et résolutions vidéo***" à la page 366) pour plus d'informations.

Utilisateurs simultanés

La console locale KX III offre un chemin d'accès indépendant aux serveurs cible KVM connectés.

L'utilisation de la console locale n'empêche pas les autres utilisateurs de se connecter en même temps sur le réseau. Et même quand des utilisateurs à distance sont connectés au KX III, vous pouvez accéder en simultané à vos serveurs sur le rack via la Console locale.

Raccourcis-clavier et touches de connexion

Etant donné que l'interface de la console locale de KX III est entièrement remplacée par l'interface du serveur cible auquel vous accédez, un raccourci-clavier est utilisé pour vous déconnecter d'une cible et retourner à l'interface utilisateur du port local.

Une touche de connexion permet de se connecter à une cible ou de basculer entre plusieurs cibles.

Le raccourci-clavier du port local vous permet d'accéder rapidement à l'interface utilisateur de la console locale de KX III lorsqu'un serveur cible est en cours d'affichage.

Reportez-vous à Paramètres du port local de la console locale de KX III pour plus d'informations.

Retour à l'interface de la Console locale de KX III - Raccourci-clavier par défaut

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

- Appuyez rapidement deux fois sur la touche Défilement.

  L'affichage écran passe de l'interface du serveur cible à celle de la console locale de KX III.

Cette combinaison de touches peut être modifiée dans la page Local Port Settings (Paramètres du port local). Reportez-vous à **Configuration des paramètres du port local de KX III depuis la console locale**dans l'aide en ligne.

Exemples de touches de connexion

Serveurs standard	
Action de la touche de connexion	**Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accès au port 5 depuis l'interface utilisateur du port local : • Appuyez sur la touche Alt gauche > Appuyez sur la touche 5 et relâchez-la > Relâchez la touche Alt gauche
Permutation entre les ports	Passer du port cible 5 au port 11 : • Appuyez sur la touche Alt gauche > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la >

Serveurs standard	
Action de la touche de connexion	**Exemple de séquence de touches**
	Relâchez la touche Alt gauche
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil
Châssis de lames	
Action de la touche de connexion	**Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accéder au port 5, connecteur 2 : • Appuyez sur la touche Alt gauche > Appuyez sur la touche 5 et relâchez-la > Appuyez sur la touche - et relâchez-la > Appuyez sur la touche 2 et relâchez-la > Relâchez la touche Alt gauche
Permutation entre les ports	Passer du port cible 5, commutateur 2 au port 5, connecteur 11 : • Appuyez sur la touche Alt gauche > Appuyez sur la touche 5 et relâchez-la > Appuyez sur la touche - et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Relâchez la touche Alt gauche
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 5, connecteur 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil

Combinaisons de touches Sun spéciales

Les combinaisons de touches suivantes pour les touches spéciales du serveur Sun™ Microsystems fonctionnent sur le port local. Ces touches spéciales sont disponibles dans le menu Clavier lorsque vous vous connectez à un serveur cible Sun :

Touche Sun	Combinaison de touches de port local
Again	Ctrl + Alt + F2
Props	Ctrl + Alt + F3
Undo	Ctrl + Alt + F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Muet	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	Aucune combinaison de touches
Alimentation	Aucune combinaison de touches

Balayage des ports - Console locale

Utilisez la fonction de balayage des ports pour rechercher les cibles sélectionnées et les affiche dans une vue en diaporama.

Cette fonction vous permet de contrôler jusqu'à 32 cibles à la fois étant donné que vous êtes en mesure de visualiser chaque serveur de cible individuellement telle qu'affichée pendant le diaporama.

Se connecte à des cibles ou se concentre sur une cible spécifique si besoin.

Les balayages peuvent inclure des cibles standard, des serveurs lames, des dispositifs Dominion en niveau et des ports de commutateurs KVM.

Dans les groupes de deux ports vidéo, le port principal est inclus dans un balayage de ports, mais non le port secondaire lors de la connexion depuis un client distant. Les deux ports peuvent être inclus dans le balayage depuis le port local.

Cliquez sur l'aperçu d'un serveur cible pour quitter le mode balayage et vous connecter à la cible, ou utiliser la séquence clé de Connexion au Port Local.

Pour quitter le mode balayage, cliquez sur le bouton Arrêter le Balayage dans la vue miniature, ou utilisez la séquence de raccourci DisconnectKey.

Remarque : Le fonction de balayage des ports est disponible sur la Console à Distance et la Console Locale, mais varie légèrement. Reportez-vous à Balayage des ports - Console à distance

Diaporama Balayage des ports - Console locale

Lorsque vous démarrez un balayage, la fenêtre Port Scan (Balayage des ports) s'ouvre.

Au fur et à mesure de la détection d'une cible, celle-ci est affichée sous forme de miniature dans un diaporama.

Le diaporama parcourt les miniatures des cibles selon l'intervalle par défaut de 10 secondes ou par l'intervalle que vous indiquez.

Au fur et à mesure du balayage des cibles, celle qui est sélectionnée dans le diaporama s'affiche au centre de la page.

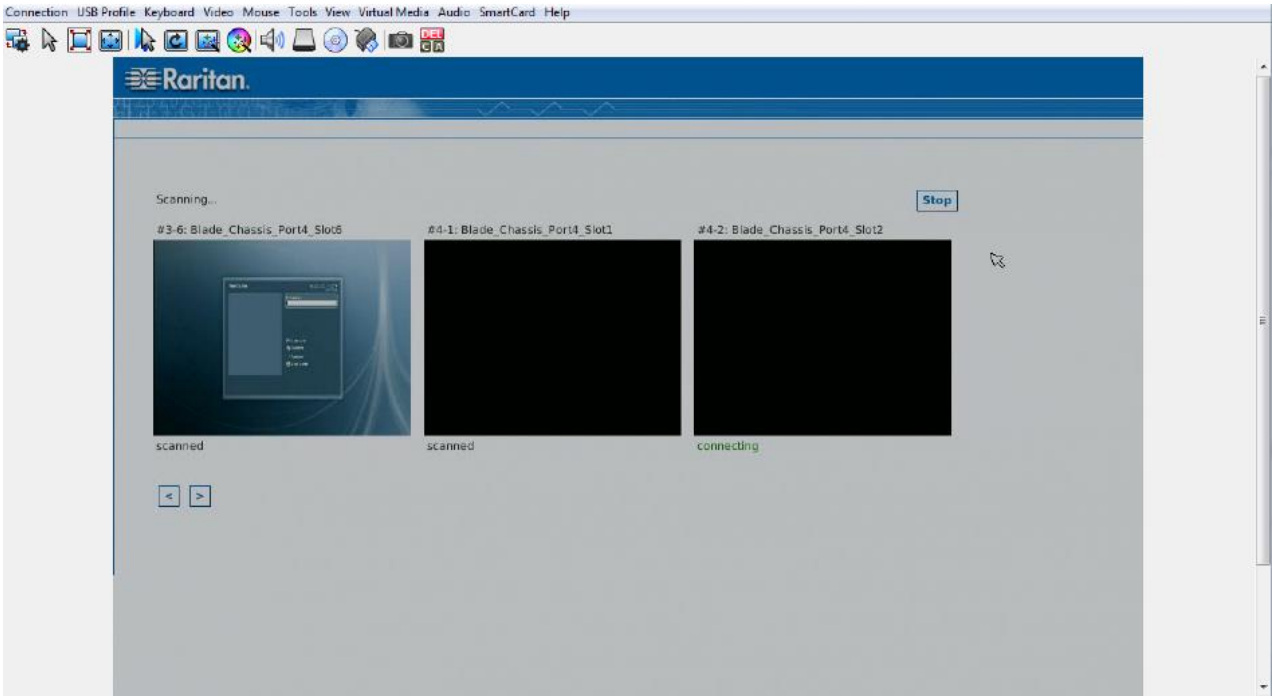
Le nom de la cible s'affiche sous sa miniature et dans la barre de tâches au bas de la fenêtre.

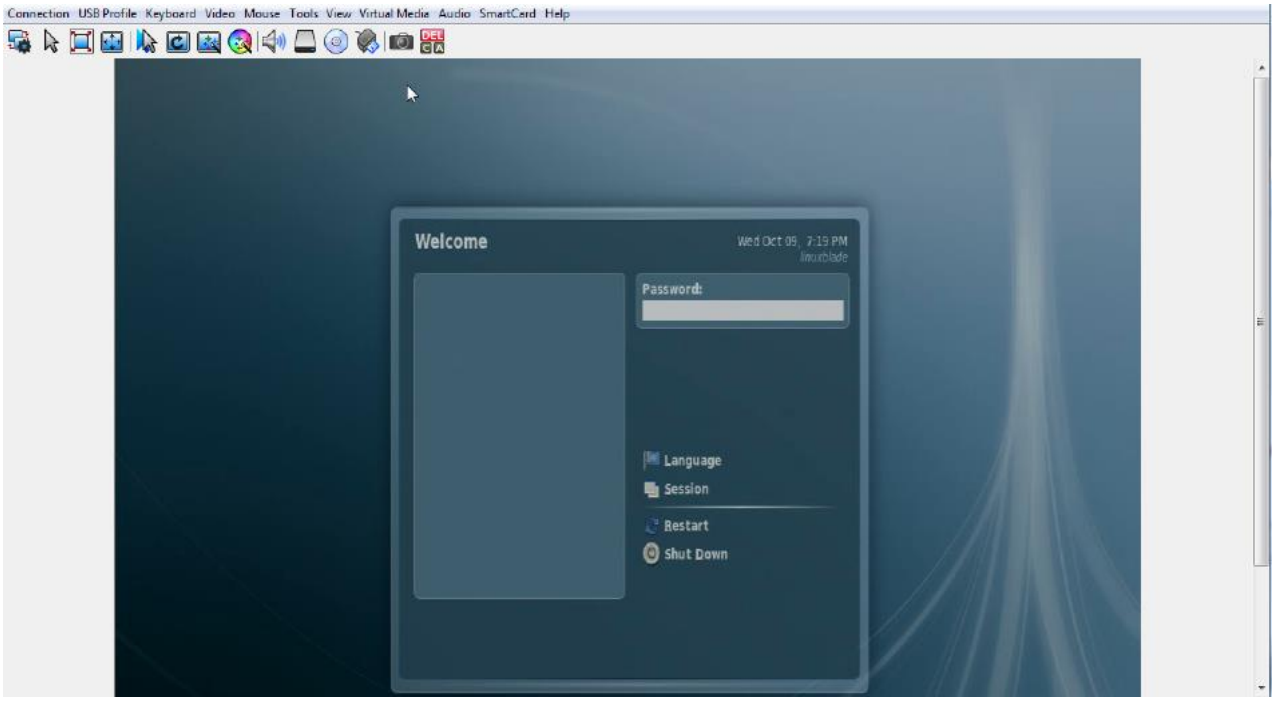
Si une cible est occupée, un écran vide apparaît au lieu de la page d'accès au serveur cible.

Réglez le temps entre les rotations de miniatures dans le diaporama et l'intervalle de mise au point sur page de Paramètres du port local.

Consultez ***Configurer les paramètres de balayage de la Console Locale*** (à la page 304)

Remarque : Configurez les paramètres de balayage du client KVM virtuel (VKC) ou du client KVM actif (AKC). Consultez **Configuration des paramètres de balayage de ports dans VKC et AKC** *(à la page 267)*



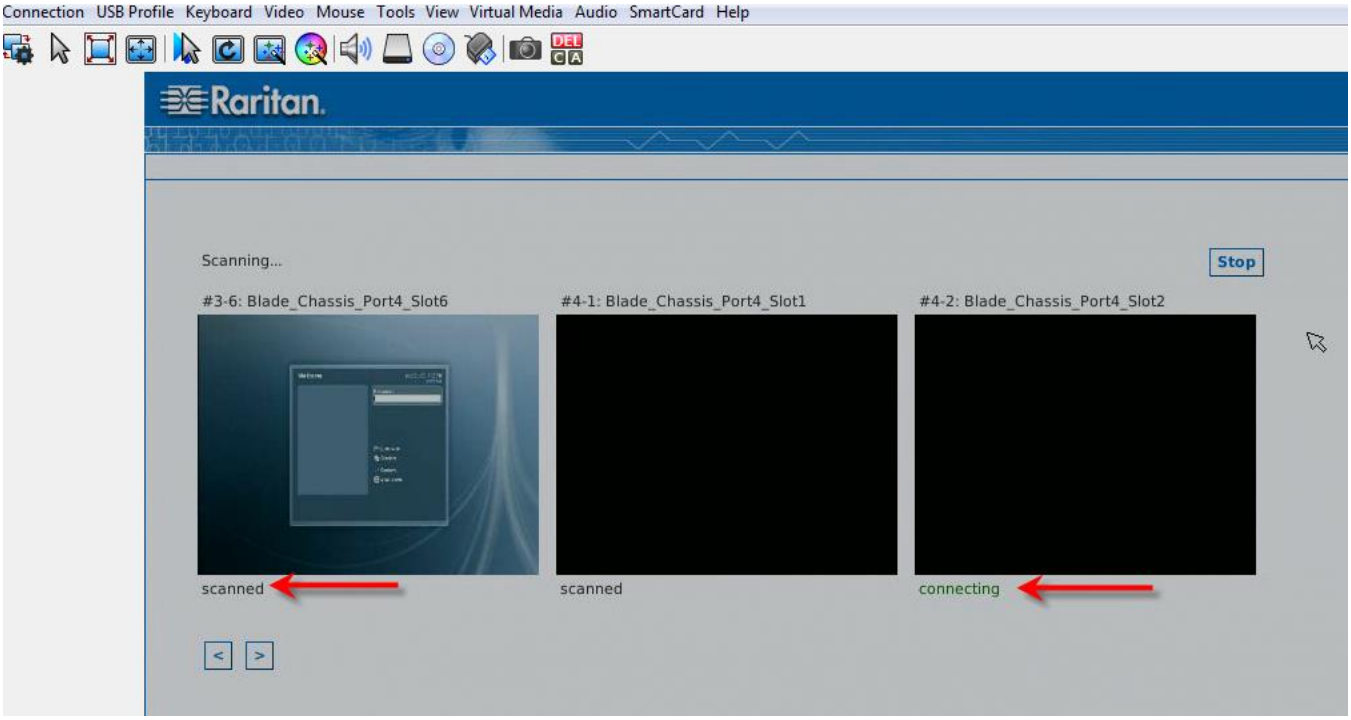

Connection USB Profile Keyboard Video Mouse Tools View Virtual Media Audio SmartCard Help
Welcome
Wed Oct 09, 7:19 PM
linuxblade
Password:
Language
Session
Restart
Shut Down

Indicateurs de Statut Cible pendant le balayage des ports - Console locale

Dans la vue en miniature dans la Console locale, le statut de chaque cible est indiquée sous la miniature de la page jusqu'à ce qu'il soit au centre du diaporama.

Le statut de balayage de chaque cible est affiché ainsi:

- non scanné
- connexion en cours...
- scanné
- passé



Configurer les paramètres de balayage de la Console Locale

Pour configurer les options de balayage de ports de la Console locale faites les choses suivantes.

Remarque : Configurez les paramètres de balayage du client KVM virtuel (VKC) ou du client KVM actif (AKC). Consultez **Configuration des paramètres de balayage de ports dans VKC et AKC** *(à la page 267)*

Pour configurer les paramètres de balayage de la Console Locale :

1. Depuis la console locale, sélectionnez Paramètres du dispositif.

2. Dans la section de Paramètres de port local, sélectionnez Mode de balayage du Port Local.
3. Changez l'intervalle d'affichage nécessaire.
   - Intervalle d'affichage - change l'intervalle d'affichage du scan.
   - Intervalle entre les ports - change l'intervalle entre le basculement ente différents ports pendant le balayage.

Balayage de Cibles - Console locale

Pour effectuer le balayage de cibles :

1. Cliquez sur l'onglet Set Scan (Balayage d'ensemble) dans la page Port Access (Accès aux ports).
2. Sélectionnez les cibles à inclure au balayage en cochant la case située à gauche de chacune, ou cochez la case au sommet de la colonne des cibles pour les sélectionner toutes.
3. Laissez la case Up Only (Activées seulement) cochée si vous ne souhaitez inclure au balayage que les cibles activées. Décochez-la pour inclure toutes les cibles, activées ou désactivées.
4. Cliquez sur Scan (Balayer) pour démarrer le balayage.

   Au fur et à mesure du balayage, chaque cible est affiché dans la vue en diaporama de la page.

Accès par carte à puce à la console locale

Pour accéder à un serveur au niveau de la console locale à l'aide d'une carte à puce, connectez un lecteur USB à KX III par un des ports USB situés sur le KX III.

Une fois qu'un lecteur de cartes à puce est branché sur ou débranché de KX III, KX III le détecte automatiquement.

Pour obtenir la liste des cartes à puce prises en charge et des informations supplémentaires sur la configuration système requise, reportez-vous à Lecteurs de cartes à puce pris en charge ou non et ***Configuration système minimale requise pour les cartes à puce*** (voir "***Configuration système minimum pour carte à puce***" à la page 343).

Une fois montés sur le serveur cible, le lecteur de cartes et la carte à puce forceront le serveur à se comporter comme s'ils étaient directement connectés.

Le retrait de la carte à puce ou du lecteur de cartes entraînera le verrouillage de la session utilisateur ou vous serez déconnecté suivant la stratégie de retrait de la carte définie dans le système d'exploitation du serveur cible.

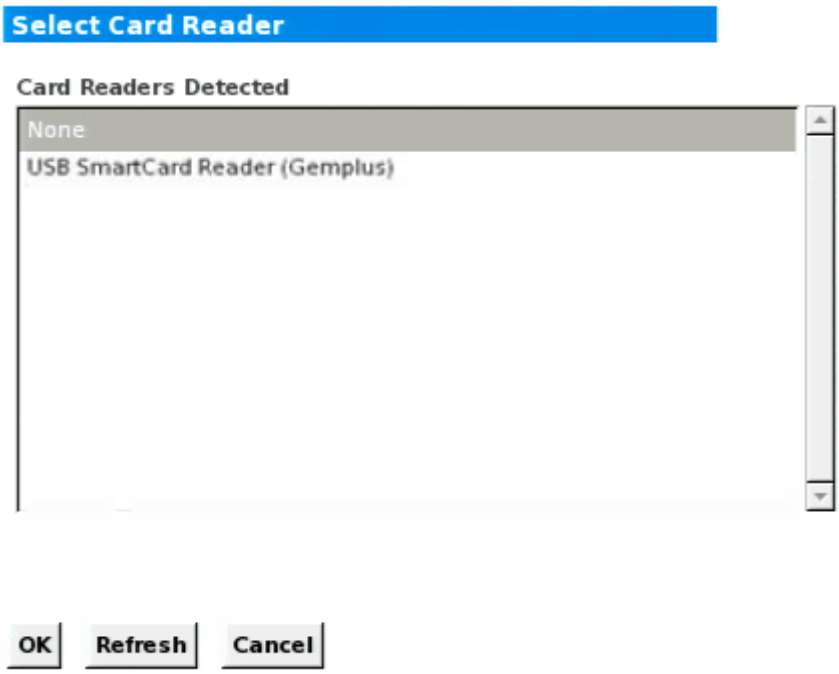
Lorsque la session KVM est arrêtée, parce qu'elle a été fermée ou parce que vous êtes passé sur une autre cible, le lecteur de cartes à puce est automatiquement démonté du serveur cible.

Pour monter un lecteur de cartes à puce sur une cible via la console locale KX III :

1. Connectez un lecteur de cartes à puce USB à KX III à l'aide d'un des ports USB situés sur le dispositif. Une fois branché, le lecteur sera détecté par KX III.
2. Depuis la console locale, cliquez sur Tools (Outils).
3. Sélectionnez le lecteur dans la liste Card Readers Detected (Lecteurs de cartes détectés). Sélectionnez None (Néant) dans la liste si vous ne souhaitez pas monter de lecteur de cartes à puce.
4. Cliquez sur OK. Une fois le lecteur de cartes à puce ajouté, un message apparaît sur la page pour indiquer que l'opération a abouti. Le statut Selected (Sélectionné) ou Not Selected (Non sélectionné) apparaît dans le panneau gauche de la page sous Card Reader (Lecteur de cartes).

Pour mettre à jour la liste des lecteurs de cartes détectés :

- Cliquez sur Refresh (Actualiser) si un nouveau lecteur de cartes à puce a été monté. La liste Card Readers Detected est rafraîchie pour inclure le lecteur de cartes à puce ajouté.



Options de profil USB de la console locale

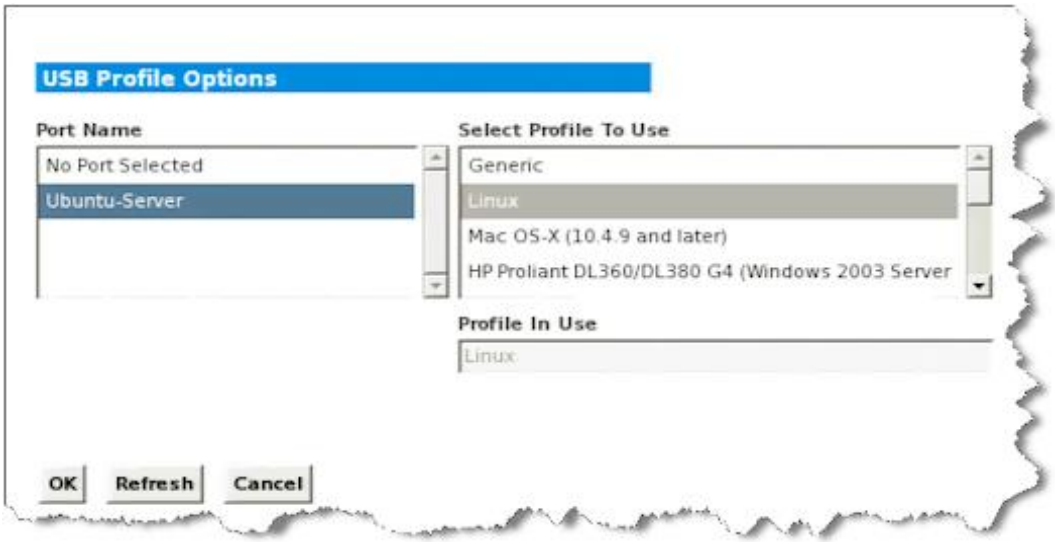
Dans la section USB Profile Options de la page Tools (Outils), vous pouvez choisir parmi les profils USB disponibles.

Les ports auxquels des profils peuvent être affectés sont affichés dans le champ Port Name et les profils disponibles pour un port apparaissent dans le champ Select Profile To Use (Sélectionner le profil à utiliser) après la sélection du port. Les profils sélectionnés pour l'utilisation avec un port apparaissent dans le champ Profile In Use (Profil utilisé).

Pour appliquer un profil USB à un port de console locale :

1. Dans le champ Port Name, sélectionnez le port auquel vous souhaitez appliquer le profil USB.
2. Dans le champ Select Profile To Use, choisissez le profil à utiliser parmi ceux disponibles pour le port.

3. Cliquez sur OK. Le profil USB sera appliqué au port local et apparaîtra dans le champ Profile In Use.



Réinitialisation des paramètres d'usine de la Console locale KX III

Remarque : Il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine.

Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à ***Journal d'audit*** *(à la page 188).*

Pour procéder à une réinitialisation des paramètres d'usine :

1. Sélectionnez Maintenance > Restauration des valeurs d'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.
   - Réinitialisation des paramètres réseau : rétablit les paramètres réseau du dispositif aux valeurs par défaut (cliquez sur Paramètres du dispositif > 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 III est automatiquement redémarré.

Réinitialisation de KX IIII à l'aide du bouton de réinitialisation sur le dispositif

Sur le panneau arrière du dispositif figure un bouton Reset (Réinitialiser). Il est encastré pour éviter les réinitialisations accidentelles (vous aurez besoin d'un objet pointu pour utiliser ce bouton).

Les opérations effectuées lorsque le bouton de réinitialisation est enfoncé sont définies sur la page Chiffrement et partage. Consultez Cryptage & Partage dans l'aide en ligne.

Remarque : Il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine.

Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à ***Journal d'audit*** *(à la page 188).*

Pour réinitialiser le dispositif :

1. Mettez KX III 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 III.
4. Continuez de maintenir le bouton enfoncé pendant 10 secondes.

Annexe A Connecter un DVI Cat5 Reach et KX III - fournit une fonctionnalité de port local étendue

Dans ce chapitre

Présentation 310
Concernant le DVI Reach Cat5 310
Connecter un KX III et un DVI Reach Cat5 311

Présentation

Un port local étendu étend la portée du port local au delà du rack sur lequel le KX II est localisé, par exemple à un autre commutateur KVM.

Ceci peut être effectué en configurant un KX III pour fonctionner avec un transmetteur et receveur Raritan DVI Cat5, qui sont ensuite connectés à une console à distance ou à un autre appareil.

Une fois connecté au DVI Reach Cat5, le KX III peut être accédé jusqu'à 152m de distance.

Connecter le KX III au DVI Reach Cat5 par chaînage des étendus de commutateurs Ethernet peut étendre la portée du KX III jusqu'à 914m.

Concernant le DVI Reach Cat5

Pour plus de détails concernant le DVI Reach Cat5, consultez l'aide en ligne du DVI Reach Cat5 disponible sur la ***page de Support Raritan http://www.raritan.com/support***.

Contactez Raritan (***http://www.raritan.com/contact-us/***) pour des informations supplémentaires concernant le Cat5 Reach DVI, ou pour plus d'informations concernant l'achat.

Connecter un KX III et un DVI Reach Cat5

Remarque : Les images utilisés dans les schémas ne sont pas spécifiques au KX III mais les connexions sont précises.

Cette section présente trois scénarios impliquant des commutateurs KVM.

- Connecter le DVI Reach Cat5 entre tout commutateur KVM et sa console locale.
- Connecter le DVI Reach Cat5 entre deux commutateurs KVM.
- Connecter le DVI Reach Cat5 entre un ordinateur/serveur et un commutateur KVM.

Eteignez tous les appareils avant de faire les connexions.

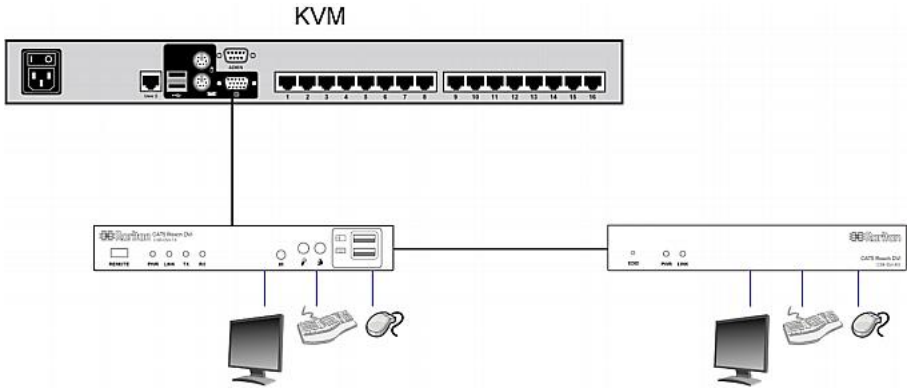
Pour des informations détaillées sur la configuration de consoles locales et à distance, consultez **Se connecter à une source clavier/souris/vidéo** dans l'**aide DVI Reach Cat5** pour plus d'informations.

Pour connecter un KX III et un DVI Reach Cat5:

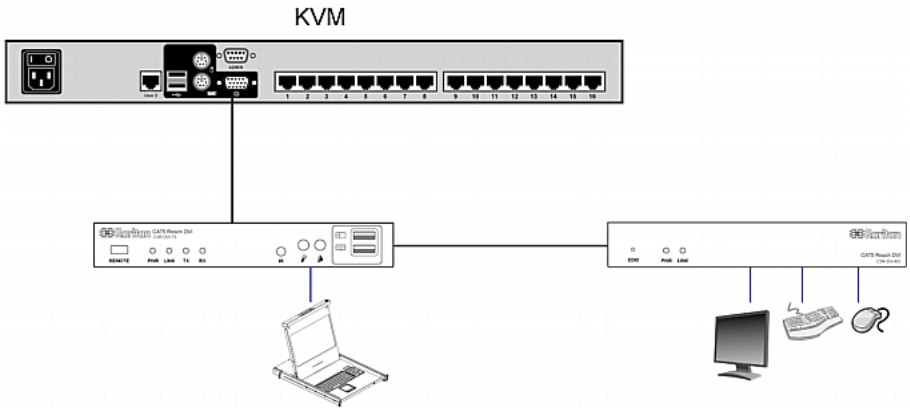
1. Si vous ne l'avez pas déjà fait, configurez les consoles locales et à distance avec le transmetteur et receveur Cat5 Reach DVI, respectivement.

   Consultez **Installation Basique** dans **l'aide Cat5 Reach DVI** pour des informations supplémentaires.
2. Utilisez un câble Cat5e/6 pour connecter le transmetteur et le récepteur.
3. Connectez le transmetteur et le récepteur à une source d'alimentation appropriée respectivement.
4. Connectez les ports de la console locale du commutateur KVM au transmetteur.
   a. Connectez une extremité du câble fourni par Raritan dans le port DVI-I IN dans le transmetteur, et l'autre extremité dans le port vidéo du comumutateur KVM.
   b. Branchez le connecteur USB -B du câble USB fourni par Raritan dans le port USB -B du transmetteur, et l'autre extremité dans le port USB -A du commutateur local KVM.

5. Allumer le commutateur KVM.



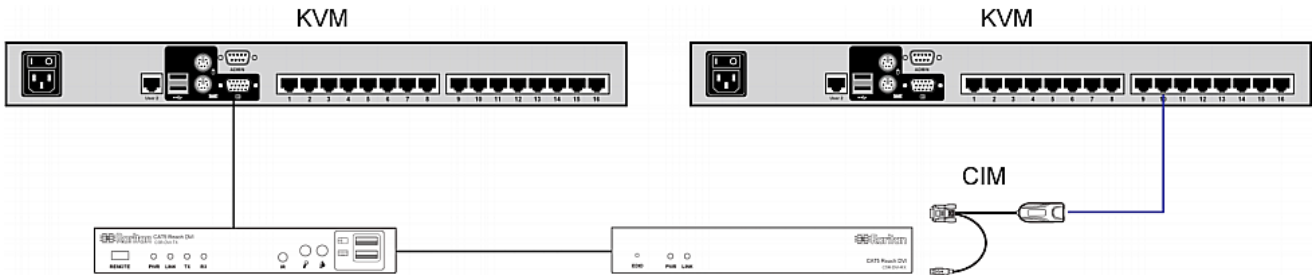
Conseil : La console locale ou distante peut être équipée par un tiroir KVM au lieu d'un ensemble clavier, souris et moniteur. Regardez l'illustration ci-dessous.



Pour augmenter la distance entre deux commutateurs KVM multiniveau:

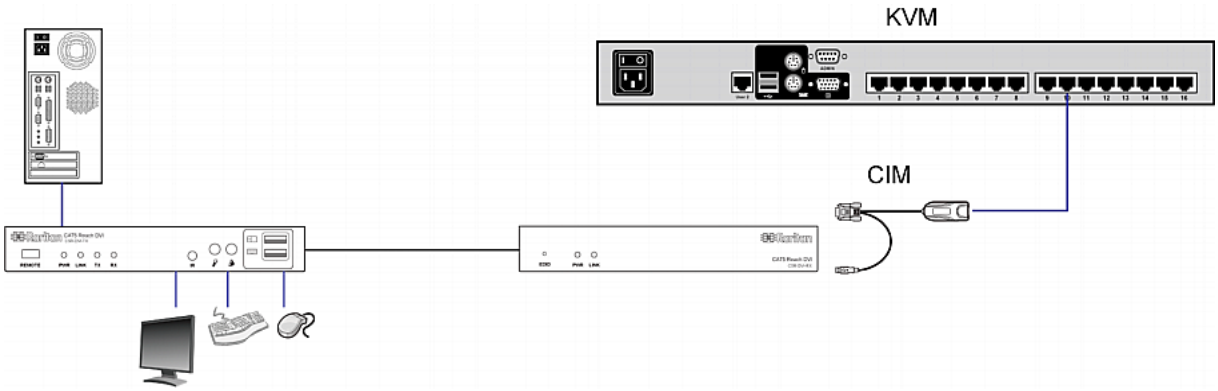
1. Configurez une console à distance en connectant le receveur à un commutateur KVM.
   a. Connectez un CIM USB au receveur.
   b. Connectez ce CIM USB à tout port de canal sur le commutateur KVM via un câble Cat5.
2. Utilisez un câble Cat5e/6 pour connecter le transmetteur et le récepteur.
3. Connectez le transmetteur et le récepteur à une source d'alimentation appropriée respectivement.
4. Connectez le commutateur KVM au transmetteur.

5. Allumez les deux commutateurs KVM.



Pour augmenter la distance entre un ordinateur et un commutateur KVM:

1. Configurez un console locale optionnelle avec le transmetteur.
2. Configurez une console à distance en connectant le receveur à un commutateur KVM.
3. Utilisez un câble Cat5e/6 pour connecter le transmetteur et le récepteur.
4. Connectez le transmetteur et le récepteur à une source d'alimentation appropriée respectivement.
5. Connectez l'ordinateur au transmetteur.
6. Allumez l'ordinateur.



Annexe B Accèder à un Paragon II depuis le KX III

Dans ce chapitre

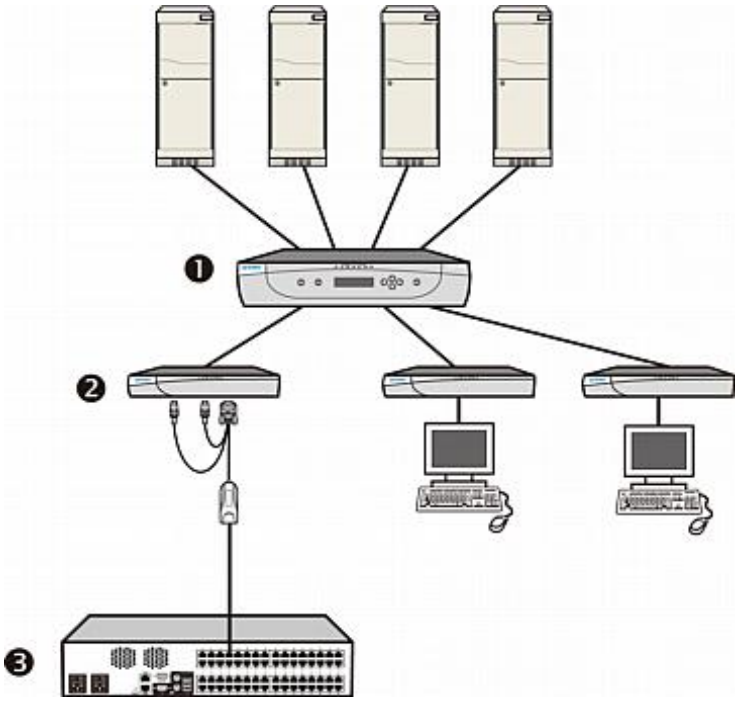
Présentation 314
Configurations et CIMs Paragon II pris en charge 315
Connexion de Paragon II au KX III 320

Présentation

Connectez le système Paragon II à un dispositif KX III qui géré par CC-SG afin que Paragon II soit accessible à partir de CC-SG.

Ce diagramme indique la configuration intégrant KX III.

Remarque : Les images sont à titre d'exemple uniquement, et peuvent ne pas ressembler exactement à votre appareil.



1	Le système Paragon II comportant des commutateurs, serveurs et stations d'utilisateur Paragon II.
2	La station de l'utilisateur avec un DCIM-USB G2 attaché
3	KX III

Lorsque vous accédez au système Paragon II depuis KX III (si la KX III est géré par CC-SG), l'écran de connexion de l'interface utilisateur Paragon II apparaît pour vous permettre d'ouvrir une session.

Dans cette intégration, vous pouvez exécuter toutes les fonctions d'interface utilisateur à l'écran mises en œuvre avec un firmware Paragon II à jour, ou toute fonction KX III mises en œuvre avec un firmware KX III à jour, hormis la fonction de support virtuel.

Lorsque vous accédez à l'interface utilisateur à l'écran de Paragon II via KX III, NE TENTEZ PAS de synchroniser la souris manuellement. La souris n'est pas nécessaire sur l'écran de l'interface utilisateur et sa synchronisation retardera la réponse du clavier de quelques secondes.

Reportez-vous à ***Configurations et CIMs Paragon II pris en charge*** (à la page 315) pour plus d'informations.

Configurations et CIMs Paragon II pris en charge

L'unité KX III prend en charge les CIM P2CIM-APS2DUAL et P2CIM-AUSBDUAL, qui fournissent deux connexions RJ45 à des commutateurs KVM différents.

La prise en charge de ces CIM offre un second chemin d'accès à la cible au cas où l'un des commutateurs KVM est bloqué ou tombe en panne.

CIM Paragon	Prend en charge	Ne prend pas en charge
P2CIM-APS2DUAL	• Serveurs avec ports clavier et souris IBM® PS/2 • Compensation d'inclinaison automatique (lorsque les CIM sont connectés à Paragon II, pas depuis KX III) • Mode Souris intelligente • Mode Souris standard	• Support virtuel • Cartes à puce • Mode Souris absolue • Utilisation avec châssis de lames • Configuration KVM en cascade

CIM Paragon	Prend en charge	Ne prend pas en charge
P2CIM-AUSBDUAL	• Serveurs avec ports clavier et souris USB ou Sun™ USB • Compensation d'inclinaison automatique (lorsque les CIM sont connectés à Paragon II, pas depuis KX III) • Mode Souris intelligente • Mode Souris standard	• Support virtuel • Cartes à puce • Mode Souris absolue • Utilisation avec châssis de lames • Configuration KVM en cascade

Directives CIM Paragon KX III-à-KX III

Les directives de configuration système ci-après doivent être respectées si vous utilisez des CIM Paragon dans une configurationKX III à KX III :

Accès simultané

Les deux commutateurs KVM KX III doivent utiliser la même stratégie pour l'accès simultané aux cibles, PC-Share ou Privées.

Si l'accès Private aux cibles est nécessaire, les deux commutateurs KVM doivent être configurés en conséquence :

- Dans le menu Sécurité > Paramètres de sécurité > Encryption & Partage, définissez le Mode PC Share en 'Privé'.

Ceci garantit que l'accès simultané aux cibles est interdit pour toutes les cibles par tous les groupes d'utilisateurs.

KX III permet une gestion plus modulaire de l'accès simultané aux cibles par groupe d'utilisateurs. Ceci est effectué par le paramétrage des autorisations PC Share du groupe d'utilisateurs. Cependant, ceci est uniquement appliqué dans le cadre d'une unité KX III. Les autorisations PC Share de groupe d'utilisateurs ne suffisent pas à garantir la confidentialité si le CIM P2CIM-APS2DUAL ou P2CIM-AUSBDUAL est utilisé avec KX III.

Mises à jour des noms de CIM

Le nom des CIM P2CIM-APS2 et P2CIM-AUSB est stocké dans leur mémoire. Deux emplacements de mémoire sont fournis pour prendre en compte la convention de nommage Paragon (12 caractères) et celle de KX III (32 caractères).

Lors de la première connexion à KX III, le nom Paragon est extrait de la mémoire et inscrit à l'emplacement de la mémoire du CIM utilisé par KX III. Les demandes suivantes du nom de CIM ou les mises à jour de ce nom provenant du KX III seront effectuées à l'emplacement de la mémoire utilisé par KX III. Les mises à jour ne seront pas effectuées par KX III à l'emplacement de mémoire utilisé par Paragon II.

Lorsque le nom du CIM est mis à jour par une unité KX III, l'autre unité KX III détecte et extrait le nouveau nom à la tentative suivante de connexion à cette cible. Avant cela, le nom n'est pas mis à jour sur l'autre unité KX III.

Statut et disponibilité des ports

Le statut du port, affiché sur la page Port Access (Accès aux ports) de l'unité KX III comme Up (Connecté) ou Down (Déconnecté), est actualisé pour indiquer si le CIM est sous tension et connecté au port KX III.

La disponibilité du port, affichée sur la page Port Access (Accès aux ports) de l'unité KX III comme Idle (Ralenti), Busy (Occupé) ou Connected (Connecté), est uniquement mise à jour pour refléter l'activité sur une cible lancée depuis cette même unité KX III.

Si une connexion est en place entre l'autre unité KX III et la cible, la disponibilité est vérifiée lors de la tentative de connexion. L'accès est refusé ou autorisé suivant la stratégie PC-Share définie pour l'unité KX III. Avant cela, la disponibilité n'est pas mise à jour sur l'autre unité KX III.

Si l'accès est refusé parce que la cible est occupée, une notification s'affiche.

Travail depuis CC-SG

Les opérations lancées depuis CC-SG sont basées sur les statut, disponibilité et nom de CIM indiqués par l'unité KX III gérée. Lorsque la cible est connectée à deux KX III gérés et que ces dispositifs sont ajoutés à CC-SG, deux nœuds seront créés. Chaque nœud sera associé à sa propre interface oob-kvm. Un nœud unique peut également être configuré avec une interface oob-kvm provenant de chaque unité KX III.

Si les unités KX III sont configurées pour le mode Private (Privé), à la deuxième tentative de connexion, l'utilisateur est prévenu qu'il ne peut pas se connecter et que l'accès est refusé.

Lorsqu'un nom de port est modifié via un volet CC-SG Port Profile (Profil de port CC-SG), le nouveau nom est répercuté sur l'unité KX III gérée. Le nom de port correspondant de l'autre unité KX III n'est mis à jour dans CC-SG qu'après une tentative de connexion au port cible via l'interface oob-kvm de l'autre unité KX III.

Directives KX III-à-Paragon II

Le P2CIM-APS2DUAL ou P2CIM-AUSBDUAL peut être connecté à une unité KX III et à Paragon II.

Accès simultané

Les deux unités KX III et Paragon II doivent utiliser la même stratégie pour l'accès simultané aux cibles.

Mode de fonctionnement de Paragon II	Description du mode	Prise en charge ?
Private (Privé)	Un serveur ou un autre dispositif sur un port de canal spécifique est accessible exclusivement par un seul utilisateur à la fois.	Oui. Paragon II et l'unité KX III doivent être paramétrés sur Privé. Le paramètre Private est appliqué au dispositif KX III, non selon le groupe

Mode de fonctionnement de Paragon II	Description du mode	Prise en charge ?
		d'utilisateurs. Paragon II utilise la couleur rouge pour indiquer occupé ou la couleur verte pour indiquer disponible.
PC-Share	Un serveur ou un autre dispositif sur un port de canal spécifique peut être sélectionné et contrôlé par plusieurs utilisateurs, mais un seul utilisateur détient le contrôle du clavier et de la souris.	Oui. Toutefois, la fonction PC Share Idle Timeout (Temporisation pour inactivité), configurée sur Paragon II, n'est pas prise en charge. Deux utilisateurs détiennent simultanément le contrôle du clavier et de la souris. Paragon II utilise la couleur verte pour indiquer disponible, ce qui est aussi vrai si un autre utilisateur accède déjà à la cible.
Public View (Affichage public)	Alors qu'un utilisateur accède à un serveur ou à un autre dispositif sur un port de canal spécifique, d'autres utilisateurs peuvent sélectionner ce port de canal et visualiser la sortie vidéo de ce dispositif. Cependant, seul le premier utilisateur détient le contrôle du clavier et de la souris jusqu'à ce qu'il se déconnecte ou change de dispositif.	Non. Ce mode ne peut pas être utilisé lors de la connexion du CIM à Paragon II et au KX III. Paragon II utilise la couleur jaune pour indiquer qu'il est en mode P-View.

Mises à jour des noms de CIM

- Les noms de CIM mis à jour depuis Paragon II sont stockés et extraits de l'emplacement de mémoire de CIM correspondant à la convention d'appellation de Paragon.
- Les noms de CIM mis à jour depuis KX III sont stockés et extraits de l'emplacement de mémoire de CIM correspondant à la convention d'appellation de KX III.
- Les mises à jour de nom de CIM ne sont pas transmises entre Paragon II et l'unité KX III.

Distances de connexion entre Paragon II et KX III prises en charge

Lors de l'utilisation de KX III en tant qu'extrémité avant d'un système Paragon II, vous devez limiter la longueur du câble (la distance) pour une bonne qualité vidéo.

La distance prise en charge entre la station utilisateur Paragon II et le serveur cible est de 152 m de câble. Si la distance est plus importante, les performances vidéo risquent d'être altérées.

La distance prise en charge entre KX III et la station utilisateur Paragon II est de 45 m de câble.

Connexion de Paragon II au KX III

Pour connecter le système Paragon II à KX III:

1. Vérifiez si la station d'utilisateur Paragon II que vous voulez connecter à KX III soit dotée d'une version de firmware 4.6 (ou supérieure). Si tel n'est pas le cas, effectuez la mise à niveau.

   La station utilisateur Paragon II peut être une des suivantes :

   - P2-UST
   - P2-EUST
   - P2-EUST/C

   Consultez **l'Aide Paragon II** pour des informations concernant la mise à jour.

2. Branchez un DCIM-USB compatible dans les ports USB et vidéo de la station d'utilisateur de Paragon II.

   Si le système est un système de niveau deux ou trois, assurez que la station utilisateur Paragon II soit reliée au dispositif de KX III de base (premier niveau).

3. Connectez la station utilisateur Paragon II à un dispositif KX III via un câble UTP Cat5 de 45 m au maximum.

- Branchez l'une des extrémités du câble sur le port RJ-45 du DCIM et l'autre, sur un des ports de canal du dispositif KX III.

4. Si vous souhaitez de disposer de chemins d'accès supplémentaires au même système Paragon II dans KX III ou CC-SG, répétez les étapes 1 à 3 pour connecter d'autres stations utilisateur à KX III.

Annexe C Gérer KX III dans dcTrack

Dans ce chapitre

Présentation 322
Localiser de l'espace dans un cabinet pour le KX III.....323
Ajouter des dispositifs KX III à dcTrack.....324
Construire des données et circuits de puissance pour KX III.....326
Soumettez une requête d'ajout d'objet pour le KX III 327
Gérer l'ordre de travail KX III 327
Visualisez le KX III dans un cabinet d'élévation et sur une carte d'étage327
Gérer le cycle de vie de KX III 329

Présentation

Le dcTrack® de Raritan est une solution de Gestion d'Infrastructure de Centre de données qui vous fournit des informations en temps réel concernant vos installations, réseaux et IT.

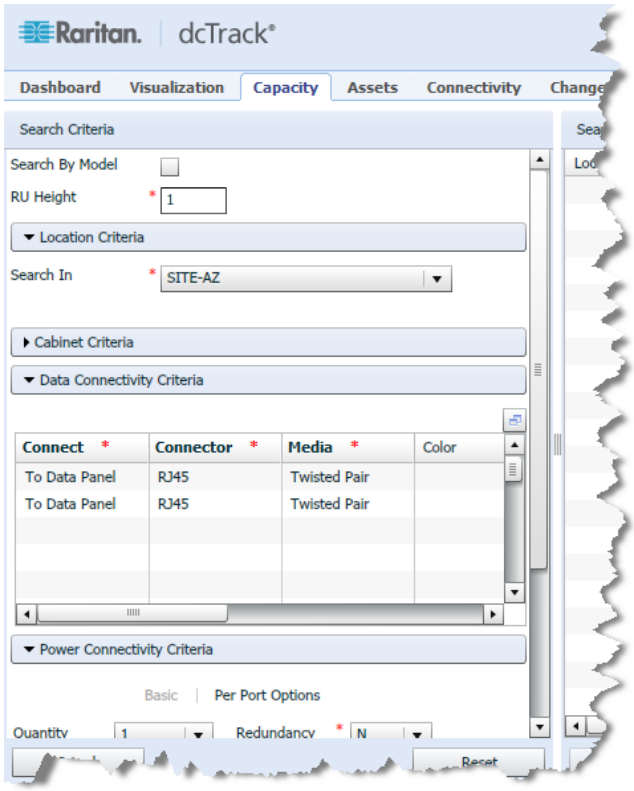
dcTrack visualise votre infrastructure pour aider les gestionnaires de centre de données et d'installations à gérer le placement d'équipes informatiques, à prendre des décisions de gestion de capacités en connaissance, et à garder une trace précise des actifs des centres de données tels que le KX III.

Localiser de l'espace dans un cabinet pour le KX III

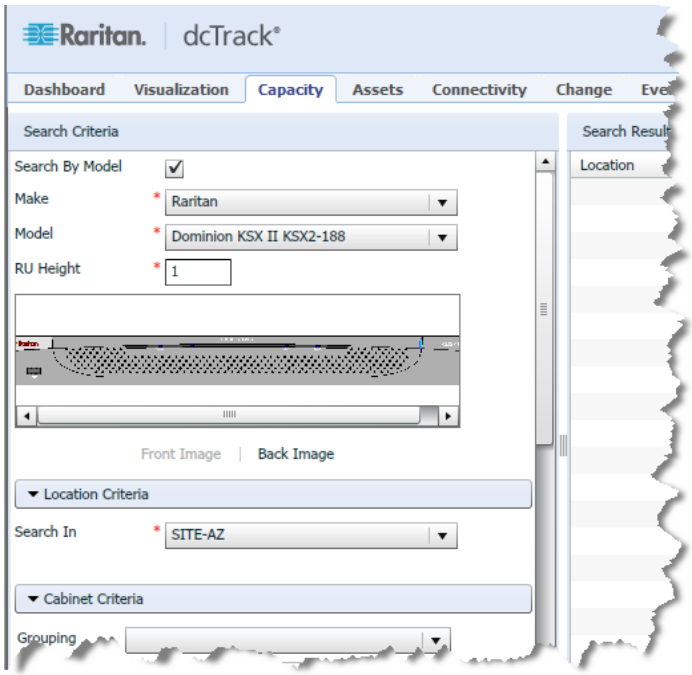
Utiliser la fonction de Gestion de Capacité de dcTrack pour localiser de l'espace dans un cabinet de votre centre de données pour KX III.

Rechercher par:

- Unités rack - dcTrack chercher un cabinet avec assez d'unités de rack prêt à accomoder le KX III.



- Marque et modèle - dcTrack cherche un cabinet avec suffisamment d'espace disponible en fonction des dimensions de la KX III, connecteurs, et ainsi de suite.



Consultez **Gestion de Capacité - Localiser et réserver de l'espace cabinet pour un objet** dans l'**aide dcTrack**.

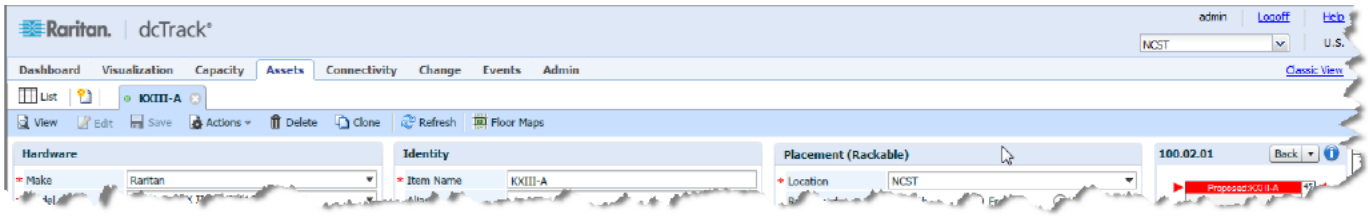
Ajouter des dispositifs KX III à dcTrack

Commencer à gérer des dispositifs KX III dans dcTrack® en les ajoutant à l'application.

Il y a différents moyens d'ajouter des dispositifs à dcTrack selon vos besoins.

Ajouter manuellement un KX III à dcTrack

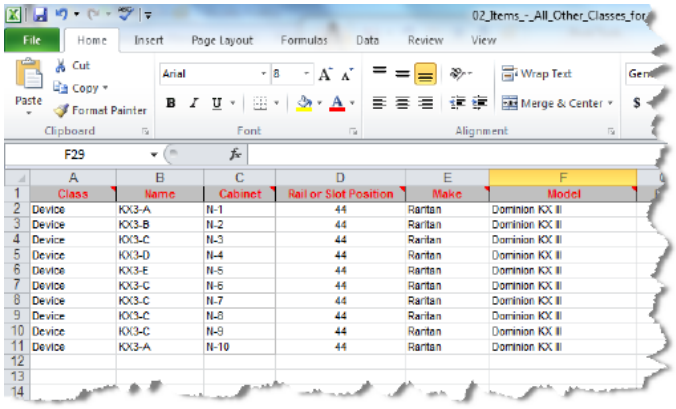
Ajouter manuellement un KX III si vous ajoutez un ou plusieurs dispositifs



Consultez **Créer manuellement de nouveaux objets dans dcTrack** dans l'**aide dcTrack**.

Importer des dispositifs KX III dans dcTrack

Si vous ajoutez un grand nombre de KX III, complétez le tableur 02_Items_-_All_Other_Classes_for_3.x.xls, fourni par Raritan, avec les informations KX III puis importez le tableur dans dcTrack® en utilisant l'assistant d'importation.

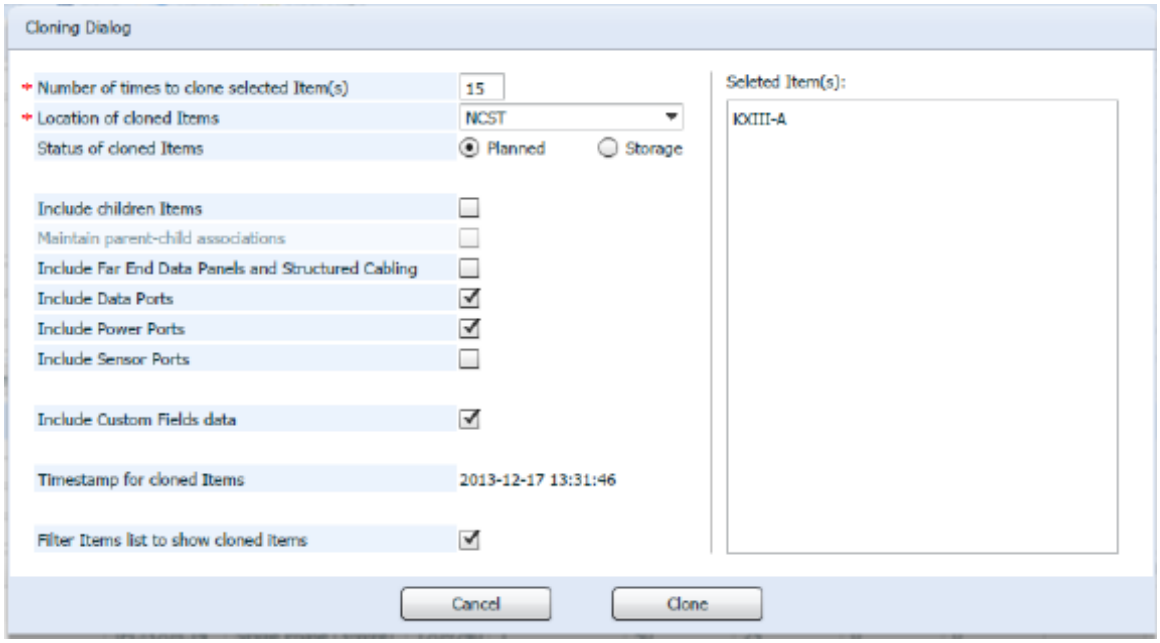


	A	B	C	D	E	F
1	Class	Name	Cabinet	Rail or Slot Position	Make	Model
2	Device	KX3-A	N-1	44	Raritan	Dominion KX II
3	Device	KX3-B	N-2	44	Raritan	Dominion KX II
4	Device	KX3-C	N-3	44	Raritan	Dominion KX II
5	Device	KX3-D	N-4	44	Raritan	Dominion KX II
6	Device	KX3-E	N-5	44	Raritan	Dominion KX II
7	Device	KX3-C	N-6	44	Raritan	Dominion KX II
8	Device	KX3-C	N-7	44	Raritan	Dominion KX II
9	Device	KX3-C	N-8	44	Raritan	Dominion KX II
10	Device	KX3-C	N-9	44	Raritan	Dominion KX II
11	Device	KX3-A	N-10	44	Raritan	Dominion KX II
12						
13						
14						

Consultez **Ajouter de nouveaux objets à dcTrack en utilisant l'assistant d'importation** dans l'**aide dcTrack**.

Cloner les dispositifs KX III existants

Utiliser le clonage si vous avez déjà ajouté un KX III et voulez le cloner avec son alimentation et ces circuits de données (si vous les avez crée), ports champs personnalisés etc.



Notez que les cabinets entiers, avec les éléments du cabinet et de leurs connexions et dispositifs fils, peuvent également être clonés.

Si vous ajoutez un KX III à un cabinet et utilisez la même configuration de cabinet via votre centre de données, vous pouvez cloner le cabinet.

Consultez **Créer des nouveaux objets et cabinets en utilisant le clonage** dans l'**aide dcTrack**.

Construire des données et circuits de puissance pour KX III

Une fois que KX III existe dans le dcTrack®, créez-lui des données et circuits de puissance.

Les circuits peuvent être crées lorsque vous ajoutez le KX III, ou plus tard.

Une fois que les circuits ont été crées, émettez une demande pour les créer dans le centre de données.

Consultez **Construire de nouveaux circuits pour objets** dans l'**aide dcTrack**.

Soumettez une requête d'ajout d'objet pour le KX III

Une fois que vous avez ajouté un KX III à dcTrack®, soumettez une requête d'installation d'objet.

La demande déclenche le processus de contrôle des changements, à commencer par un ordre de travail pour installer physiquement le KX III dans le centre de données.

Consultez **Soumettre une requête d'installation d'objet depuis le Menu d'action** dans l'**aide dcTrack**.

Gérer l'ordre de travail KX III

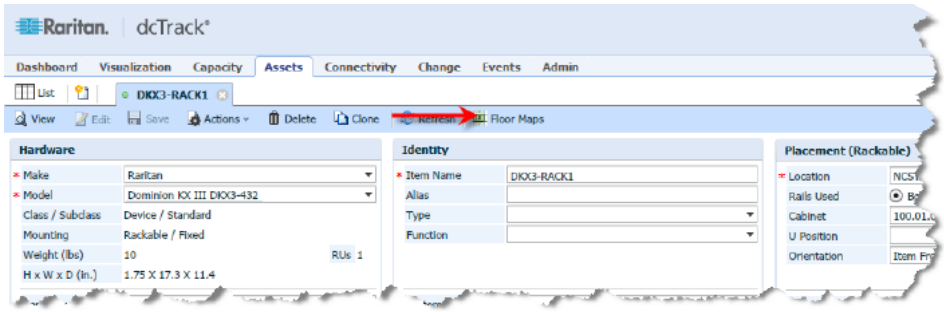
A moins que le mode Request Bypass soit activé, dans quel cas dcTrack® ne gère pas le processus de controle de changement lors d'une demande d'article, l'ordre de travail pour l'installation de KX III est géré par le Gatekeeper dcTrack.

Consultez **Gérer les ordres de travail** ou **Request Bypass** dans l'**aide dcTrack**.

Visualisez le KX III dans un cabinet d'élévation et sur une carte d'étage

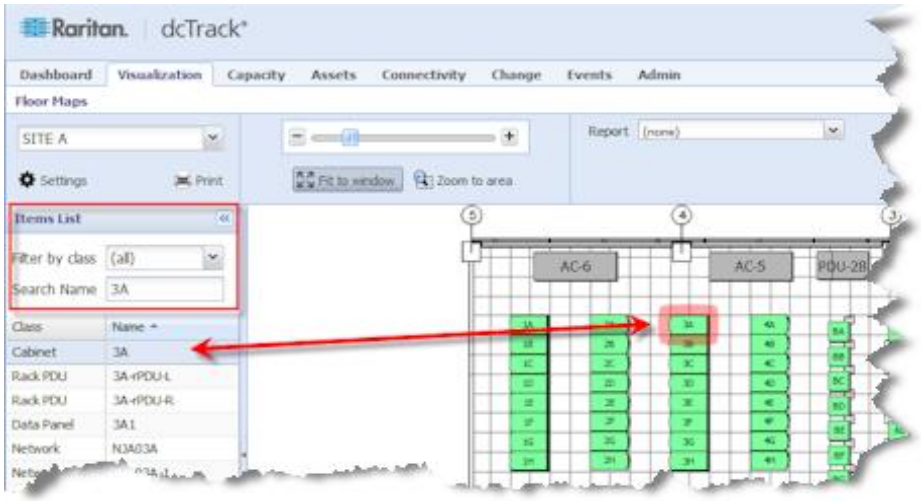
Lorsque vous ajoutez le KX III à dcTrack®, vous le placez dans un cabinet.

Si la localisation du centre de données à laquelle appartient le cabinet a une carte d'étage, et que le cabinet dans lequel KX III est localisé est en lien à un cabinet objet sur la carte d'étage, vous pouvez accéder à la carte d'étage depuis la page KX III dans dcTrack.



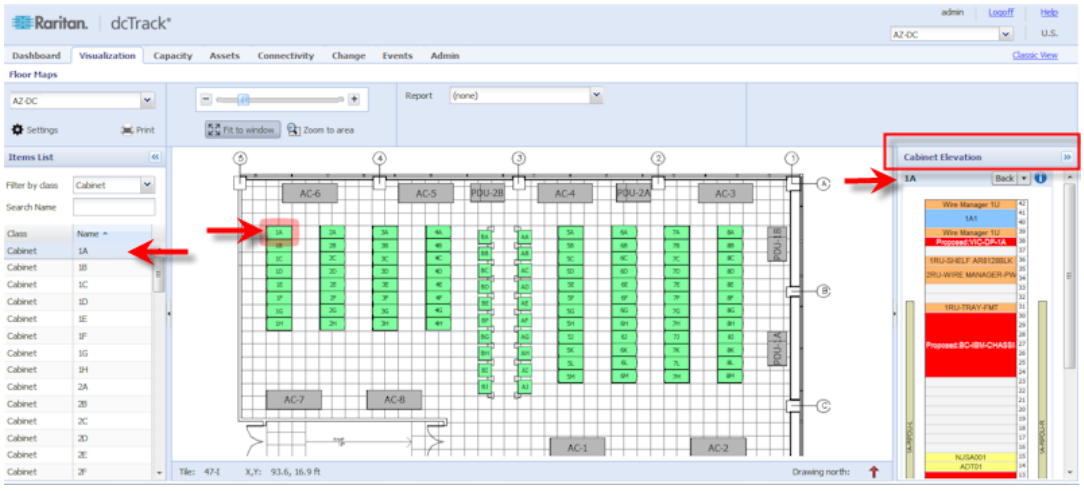
Consultez **Ouvrir une carte d'étage depuis la page objet** dans l'**aide dcTrack**.

Une fois sur la page de la carte d'étage, visualisez la localisation du cabinet dans lequel se trouve le KX III dans la carte d'étage et dans le liste d'objets.



Consultez **Localisez un objet sur la carte d'étage et la liste d'objets (client web)** dans l'**aide dcTrack**.

Vous pouvez également visualiser le KX III dans l'élévation de cabinet de la carte d'étage.



Consultez **Elevations de cabinet - Carte d'étage (client web)** dans l'**aide dcTrack**.

Gérer le cycle de vie de KX III

Une fois que KX III est installé, gérer son cycle de vie via votre centre de données.

Déplacer un KX III

Soumettre une requête pour déplacer un KX III de :

- Un cabinet à un autre cabinet
- Une localisation à une autre localisation
- Une position de rail à une autre position de rail

Consultez **les Requêtes de déplacement d'objet**dans **la Piste d'aide**.

Allumez ou éteignez un KX III

Soumettez des requêtes afin d'allumer ou d'éteindre le KX III, selon vos besoins.

Consultez **l'envoi de requêtes pour allumer ou éteindre les appareils** dans **la Piste d'aide**.

Ajouter ou retirer un KX III du site

Soumettez des requêtes afin d'ajouter ou de retirer le KX III du site, par exemple s'il est temporairement retiré pour des questions de maintenance.

Consultez **l'envoi de requêtes pour ajouter ou retirer des objets du site** dans **la Piste d'aide**.

Déclasser un KX III en stockage

Soumettez une requête afin de déclasser le KX III en stockage si vous prévoyez de le déplacer temporairement dans un endroit hors-site.

Consultez **la Soumission de Requête afin de déclasser un item en stockage** dans **la Piste d'aide**.

Déclasser un KX III aux archives

Soumettez une requête afin de déclasser le KX III aux archives pour le supprimer de votre inventaire à disposition.

Consultez **Déclasser un objet installé aux archives** dans**la piste d'aide**.

Annexe D Spécifications

Dans ce chapitre

Matériel 330
Logiciel 352

Matériel

Dimensions et spécifications physiques de KX III

Modèle Dominion KX III	Description	Puissance et dissipation de chaleur	Dimensions (LxPxH)	Poids	Température de fonctionnement	Humidité
DKX3-108	▪ 8 ports serveur ▪ 1 utilisateur distant ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	8.60lbs 3,9 kg	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-116	▪ 16 ports serveur ▪ 1 utilisateur distant ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	8.60lbs 3,9 kg	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-132	▪ 32 ports serveur ▪ 1 utilisateur distant ▪ 1 port local	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	8.60lbs 3,9 kg	0º - 45º C 32º - 113º F	0-85 % RH

Modèle Dominion KX III	Description	Puissance et dissipation de chaleur	Dimensions (LxPxH)	Poids	Température de fonctionnement	Humidité
	pour une utilisation sur le rack					
DKX3-216	▪ 16 ports serveur ▪ 2 utilisateur distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	9.08lbs 4,12 kg	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-232	▪ 32 ports serveur ▪ 2 utilisateur distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	9.08lbs 4,12 kg	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-416	▪ 16 ports serveur ▪ 4 utilisateur distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	9.08lbs 4,12 kg	0º - 45º C 32º - 113º F	0-85 % RH
DKX3-432	▪ 32 ports serveur ▪ 4 utilisateur distants	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ; 439x334x44 mm	9.08lbs 4,12 kg	0º - 45º C 32º - 113º F	0-85 % RH

Modèle Dominion KX III	Description	Puissance et dissipation de chaleur	Dimensions (LxPxH)	Poids	Température de fonctionnement	Humidité
	▪ 1 port local pour une utilisation sur le rack					
DKX3-464	▪ 64 ports serveur ▪ 4 utilisateur distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,3" x 3,5"	12.39lbs	0º - 45º C	0-85 % RH
			439x338x89 mm	5,62 kg	32º - 113º F	
DKX3-808	▪ 8 ports serveur ▪ 8 utilisateurs distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ;	9.96lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	4,52 kg	32º - 113º F	
DKX3-832	▪ 32 ports serveur ▪ 8 utilisateurs distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,15" x 1,73" ;	9.96lbs	0º - 45º C	0-85 % RH
			439x334x44 mm	4,52 kg	32º - 113º F	

Modèle Dominion KX III	Description	Puissance et dissipation de chaleur	Dimensions (LxPxH)	Poids	Température de fonctionnement	Humidité
DKX3-864	▪ 64 ports serveur ▪ 8 utilisateurs distants ▪ 1 port local pour une utilisation sur le rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17,3" x 13,3" x 3,5"	12.39lbs	0º - 45º C	0-85 % RH
			439x338x89 mm	5,62 kg	32º - 113º F	

Résolutions de Vidéo de Serveur cible supportées par KX III

- 640x350@70Hz
- 640x350@85Hz
- 640x400@56Hz
- 640x400@84Hz
- 640x400@85Hz
- 640x480@60Hz
- 640x480@66,6Hz
- 640x480@72Hz
- 640x480@75Hz
- 640x480@85Hz
- 720x400@70Hz
- 720x400@84Hz
- 720x400@85Hz
- 800x600@56Hz
- 800x600@60Hz
- 800x600@70Hz
- 800x600@72Hz
- 800x600@75Hz
- 800x600@85Hz
- 800x600@90Hz
- 800x600@100Hz
- 832x624@75,1Hz
- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@72Hz
- 1024x768@85Hz
- 1024x768@75Hz
- 1024x768@90Hz
- 1024x768@100Hz
- 1152x864@60Hz
- 1152x864@70Hz
- 1152x864@75Hz
- 1152x864@85Hz
- 1152x870@75,1Hz
- 1280x720@60Hz

- 1280x960@60Hz
- 1280x960@85Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1280x1024@85Hz
- 1360x768@60Hz
- 1366x768@60Hz
- 1368x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz

Distance de connexion, taux de rafraîchissement et résolution vidéo du serveur cible pris en charge

La distance maximale prise en charge dépend de plusieurs facteurs, notamment le type/la qualité du câble Cat5, le type et le fabricant du serveur, le pilote et l'écran vidéo, les conditions de l'environnement et les attentes de l'utilisateur.

Le tableau suivant indique la distance maximale du serveur cible pour différentes résolutions vidéo et taux de rafraîchissement :

Résolution vidéo du serveur cible	Distance maximale
1024x768@60Hz (et en dessous)	150' (45 m)
1280x1024@60Hz	100' (30 m)
1280×720@60Hz	75' (22m)
1600x1200@60Hz	50' (15m)
1920x1080@60Hz	50' (15m)

Reportez-vous à ***Résolutions vidéo du serveur cible prises en charge*** (voir "***Résolutions de Vidéo de Serveur cible supportées par KX III***" à la page 334) pour connaître les résolutions vidéo prises en charge par KX III.

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

Résolutions DVI de Port Local KX III prises en charge

- 1920x1080@60
- 1280x720@60
- 1024x768@60 (par default)
- 1024x768@75
- 1280x1024@60
- 1280x1024@75
- 1600x1200@60
- 800x480@60
- 1280x768@60
- 1366x768@60
- 1360x768@60
- 1680x1050@60
- 1440x900@60

Spécifications des CIM pris en charge

Les CIM numériques prennent en charge les canaux de données d'affichage (DDC) et les données d'identification d'affichage étendues améliorées (E-EDID).

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
D2CIM-DVUSB	CIM double USB pour support virtuel BIOS, carte à puce/CAC, audio et synchronisation absolue de la souris	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg
D2CIM-VUSB	CIM USB pour support virtuel et synchronisation absolue de la souris	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0.20lb; 0,09 kg

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
D2CIM-DVUSB-DVI	CIM numérique qui permet la conversion numérique-analogique et prend en charge support virtuel, carte à puce/CAC, audio, synchronisations absolue et relative de la souris	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg
D2CIM-DVUSB-DP	CIM numérique qui permet la conversion numérique-analogique et prend en charge support virtuel, carte à puce/CAC, audio, synchronisations absolue et relative de la souris	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg

Modèle de CIM	Description	Dimensions (LxPxH)	Poids
D2CIM-DVUSB-HDMI	CIM numérique qui permet la conversion numérique-analogique et prend en charge support virtuel, carte à puce/CAC, audio, synchronisations absolue et relative de la souris	1,7" x 3,5" x 0,8" ; 43 x 90 x 19 mm	0,25 lb ; 0,11 kg
DCIM-PS2	CIM pour PS2	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0.20lb; 0,09 kg
DCIM-USBG2	CIM pour USB et Sun USB	1,3" x 3,0" x 0,6" ; 33 x 76 x 15 mm	0.20lb; 0,09 kg

Notez que le connecteur noir des CIM DVUSB est utilisé pour le clavier et la souris. Le connecteur gris est utilisé pour le support virtuel.

Laissez les deux prises du CIM branchées sur le dispositif. Le dispositif risque de ne pas fonctionner correctement si les deux prises ne sont pas branchées sur le serveur cible.

CIM Vidéo Digital pris en charge par Mac

Utilisez un CIM vidéo digital pour connecter les ports Mac® suivants:

Port Mac	CIM
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort ou Thunderbolt	D2CIM-DVUSB-DP

Si le port HDMI ou vidéo Mac a un mini connecteur, un câble adaptateur passif peut être requis pour se connecter aux prises HDMI et DisplayPort en pleine dimension sur le CIM digital.

Sinon, utilisez l'adaptateur VGA Mac avec le D2CIM-VUSB ou D2CIM-DVUSB. Remarquez que cela peut être moins fiable et que la qualité vidéo peut en pâtir.

Pour plus d'informations sur les modes établis pris en charge par le KX III 2.5.0 (et supérieur) sur Mac, consultez ***Modes digital CIM établis et standard*** (à la page 339).

Modes de synchronisation de CIM numériques

Vous trouverez ci-dessous les modes de synchronisation par défaut utilisés par KX III pour communiquer avec une source vidéo par le biais d'un CIM numérique.

Le mode de synchronisation utilisé dépend de la résolution native de la source vidéo.

- 1920x1080@60Hz
- 1600x1200@60Hz
- 1280 x 1024@60 Hz (résolution par défaut appliquée aux CIM numériques)
- 1440x900@60Hz
- 1024x768@60Hz

Consultez ***Configurer les ports CIM*** (voir "***Configuration des ports CIM***" à la page 95) dans l'aide en ligne pour plus d'informations.

Modes digital CIM établis et standard

Les résolutions et modes de synchronisation établis et standard supplémentaires ci-après sont pris en charge par KX III 3.0.0 (et supérieur).

Modes CIM digital établis

- 720x400@70Hz IBM, VGA
- 640x480@60Hz IBM, VGA
- 640x480@67Hz Apple Mac® II
- 640x480@72Hz VESA
- 640x480@75Hz VESA
- 800x600@56Hz VESA
- 800x600@60Hz VESA
- 800x600@72Hz VESA
- 800x600@75Hz VESA
- 832x624@75Hz Apple Mac II
- 1024x768@60Hz VESA
- 1024x768@70Hz VESA
- 1024x768@75Hz VESA
- 1280x1024@75Hz VESA
- 1152x870@75Hz Apple Mac II

Modes digital CIM standard

- 1152x864@75 Hz VESA
- 1280x960@60 Hz VESA
- 1280x1024@60 Hz VESA
- 1360x768@60 Hz VESA
- 1400x1050@60 Hz VESA
- 1440x900@60 Hz VESA
- 1600x1200@60 Hz VESA
- 1680x1050@60 Hz VESA
- 1920x1080@60 Hz VESA

Mode de compatibilité DVI

Le mode de compatibilité DVI est utilisé si vous vous connectez à une cible Dell Optiplex dotée d'une carte graphique Intel ou à un Mac® Mini doté d'un contrôleur HDMI à l'aide d'un CIM HDMI.

La sélection de ce mode assure une bonne qualité vidéo sur les cibles.

Consultez ***Configurer les ports CIM*** (voir "***Configuration des ports CIM***" à la page 95) dans l'aide en ligne.

Connexions à distance prises en charge

Connexion à distance	Détails
Réseau	Ethernet 10BASE-T, 100BASE-T et 1000BASE-T (Gigabit)
Protocoles	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Paramètres de vitesse réseau

Paramètre de vitesse réseau de KX III

Paramètre de port de commutateur réseau		Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
	Auto	Vitesse disponible maximale	1000/Full	KX III: 100/Full Commutateur : 100/Half	100/Half	KX III: 10/Full Commutateur : 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	Aucune communication	Aucune communication	Aucune communication	Aucune communication
	100/Full	KX III: 100/Half Commutateur : 100/Full	KX III: 100/Half Commutateur : 100/Full	100/Full	KX III: 100/Half Commutateur : 100/Full	Aucune communication	Aucune communication
	100/Half	100/Half	100/Half	KX III: 100/Full Commutateur : 100/Half	100/Half	Aucune communication	Aucune communication
	10/Full	KX III: 10/Half Commutateur : 10/Full	Aucune communication	Aucune communication	Aucune communication	10/Full	KX III: 10/Half Commutateur : 10/Full
	10/Half	10/Half	Aucune communication	Aucune communication	Aucune communication	KX III: 10/Full Commutateur : 10/Half	10/Half

Légende :

Ne fonctionne pas comme prévu

Pris en charge

Fonctionne ; non recommandé

NON pris en charge par la spécification Ethernet ; le produit peut communiquer mais des collisions se produisent.

Selon la spécification Ethernet, « aucune communication » ne devrait se produire ; notez toutefois que le comportement KX III diffère du comportement attendu.

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

Longueurs de câbles et résolutions vidéo pour châssis Dell

Afin de maintenir la qualité vidéo, Raritan recommande l'utilisation des longueurs de câbles et des résolutions vidéo suivantes lorsque vous êtes connecté à un châssis blade Dell® depuis KX III :

Résolution vidéo	Longueur de câble
1024x768@60Hz	50' (15.24m)
1280x1024@60Hz	50' (15.24m)
1600x1200@60Hz	30' (9.14m)

Configuration système minimum pour carte à puce

Exigences en matière de port local

L'exigence en matière d'interopérabilité de base pour la connexion du port local au KX III est la suivante :

- Tous les dispositifs (lecteur de cartes à puce ou jeton) connectés localement doivent être compatibles USB CCID.

Exigences en matière de serveur cible

Pour l'utilisation de lecteurs de cartes à puce, les exigences de base en matière d'interopérabilité au niveau du serveur cible sont les suivantes :

- Le gestionnaire IFD (lecteur de cartes à puce) doit être un pilote de périphérique CCID USB standard (comparable au pilote CCID USB Microsoft générique).
- Un CIM numérique ou D2CIM-DVUSB (CIM double VM) est nécessaire et doit utiliser la version de firmware 3A6E ou supérieure.
- Les connexions de serveurs avec châssis de lames, où un CIM par lame est utilisé, sont prises en charge.
- Les connexions de serveur à châssis de lames, où un CIM par châssis est utilisé, ne sont prises en charge que pour les modèles E et H d'IBM BladeCenter où la détection automatique est activée.

Cibles Windows XP

Les systèmes d'exploitation cibles Windows XP® doivent exécuter Windows XP SP3 afin d'utiliser des cartes à puce avec KX III. Si vous travaillez avec .NET 3.5 dans un environnement Windows XP sur le serveur cible, vous devez utiliser SP1.

Cibles Linux

Si vous utilisez une cible Linux®, les exigences suivantes doivent être respectées pour permettre l'utilisation de lecteurs de cartes à puce avec le dispositif Raritan.

- Exigences CCID

  Si D2CIM-DVUSB VM/CCID Raritan n'est pas reconnu en tant que lecteur de cartes à puce par votre cible Linux, il vous faudra peut-être mettre à jour la version du pilote CCID à 1.3.8 ou supérieure, et le fichier de configuration du pilote (Info.plist).

Système d'exploitation	Exigences CCID
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12

Fedora® Core 10	ccid-1.3.8-1.fc10.i386

Exigences en matière de client distant

Les exigences de base en matière d'interopérabilité au niveau du client distant sont les suivantes :

- Le gestionnaire IFD (lecteur de cartes à puce) doit être un pilote de périphérique compatible PC/SC.
- Le gestionnaire de ressources ICC (carte à puce) doit être disponible et compatible PC/SC.
- Le programme JRE® Java® 1.7 avec interface API pour carte à puce doit être disponible pour être utilisé par l'application cliente Raritan.

Exigences de clients distants Linux

Si vous utilisez un client Linux®, les exigences suivantes doivent être respectées pour permettre l'utilisation de lecteurs de cartes à puce avec le dispositif Raritan.

Remarque : La connexion de l'utilisateur au client, à l'insertion d'une carte à puce, peut durer plus longtemps si 1 ou plusieurs sessions KVM sont actives vers les cibles. Le processus de connexion à ces cibles est en effet en cours.

- Exigences PC/SC

Système d'exploitation	PC/SC requis
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Créer un lien vers la bibliothèque Java®

  Un lien symbolique doit être créé vers libpcsclite.so après la mise à niveau de RHEL 4, RHEL 5 et FC 10. Par exemple, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, en supposant que l'installation du progiciel ait placé les bibliothèques dans /usr/lib ou /user/local/lib.

- Démon PC/SC

  Lorsque le démon pcsc (gestionnaire de ressources dans framework) est redémarré, relancez le navigateur.

Lecteurs de cartes à puce pris en charge

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

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

Lecteurs de cartes à puce non pris en charge

Ce tableau contient la liste des lecteurs testés par Raritan qui ne fonctionnent pas avec le dispositif Raritan et ne sont donc pas pris en charge.

Si un lecteur de cartes à puce n'apparaît ni dans le tableau des lecteurs pris en charge ni dans celui des lecteurs non pris en charge, Raritan ne peut pas garantir qu'il fonctionne avec le dispositif.

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

Type	Fabricant	Modèle	Remarques
		PRO™	propriétaire

Recommandations et exigences en matière de lecture et de capture audio

Niveau sonore

- Réglez le son de la cible à un niveau intermédiaire.

  Par exemple, sur un client Windows®, réglez l'audio à 50 ou moins.

Ce paramètre doit être configuré depuis le dispositif audio de lecture ou de capture, et non depuis le contrôle du dispositif audio du client.

Recommandations en matière de connexions audio lorsque le mode PC Share est activé

Si vous utilisez la fonction audio lors de l'exécution du mode PC Share, la lecture et la capture audio sont interrompues si un dispositif audio supplémentaire est connecté à la cible.

Par exemple, l'utilisateur A connecte un dispositif de lecture à Cible1 et exécute une application de lecture audio ; l'utilisateur B connecte ensuite un dispositif de capture à la même cible. La session de lecture de l'utilisateur A est interrompue et l'application audio devra peut-être redémarrée.

L'interruption a lieu car le dispositif USB doit être énuméré à nouveau avec la configuration du nouveau dispositif.

L'installation d'un pilote pour le nouveau dispositif par la cible peut prendre du temps.

Les applications audio peuvent arrêter complètement la lecture, passer à la piste suivante ou poursuivre la lecture.

Le comportement exact dépend de la façon dont l'application audio est conçue pour traiter un événement de déconnexion/reconnexion.

Exigences en matière de bande passante

Le tableau ci-dessous détaille les exigences en matière de bande passante de lecture et de capture audio pour le transport du son sur chaque format sélectionné.

Format audio	Bande passante réseau requise
44,1 KHz, stéréo 16 bits	176 Ko/s

Format audio	Bande passante réseau requise
44,1 KHz, mono 16 bits	88,2 Ko/s
2,05 KHz, stéréo 16 bits	88,2 Ko/s
22,05 KHz, mono 16 bits	44,1 Ko/s
11,025 KHz, stéréo 16 bits	44,1 Ko/s
11,025 KHz, mono 16 bits	Audio 22,05 Ko/s

Dans la pratique, la bande passante utilisée pour connecter un dispositif audio à une cible est plus importante en raison des données de clavier et vidéo consommées lors de l'ouverture et de l'utilisation d'une application audio sur la cible.

En règle générale, nous vous recommandons une connexion d'au moins 1,5 Mo avant d'exécuter la lecture et la capture.

Toutefois, un contenu vidéo important, des connexions en couleurs avec des résolutions d'écran élevées sur la cible consomment beaucoup plus de bande passante et affectent considérablement la qualité sonore.

Les paramètres clients recommandés permettent de réduire l'effet de la vidéo sur la qualité sonore avec des bandes passantes inférieures :

- Connectez les dispositifs de lecture audio à des formats de qualité inférieure. La consommation de bande passante par la vidéo affecte moins les performances avec des connexions de 11k que de 44k.
- Paramétrez la vitesse de connexion sous Connection Properties (Propriétés de connexion) sur une valeur correspondant le mieux à la connexion client-serveur.
- Sous Connection Properties, paramétrez le nombre de couleurs sur la valeur la plus basse possible. La réduction à une couleur de 8 bits réduit la consommation de bande passante.
- Paramétrez le lissage sur High (Elevé). Ceci améliorera l'apparence de la vidéo cible en réduisant le bruit de la vidéo affichée.
- Sous Video settings (Paramètres vidéo), paramétrez Noise Filter (Filtre antiparasite) sur 7 (valeur maximale) afin de réduire l'utilisation de bande passante pour les changements d'écran cible.

Audio dans un environnement Mac

Vous trouverez ci-dessous les problèmes connus dans un environnement Mac®.

- Sur les clients Mac, un seul dispositif de lecture apparaît sur le panneau Connexion Audio lors de l'accès au dispositif via le Virtual KVM Client (VKC). Il s'agit du dispositif par défaut et il est affiché sur le panneau Connect Audio sous Java Sound Audio Engine (Moteur audio).
- Le son utilisé sur une cible Mac via Skype® risque d'être altéré.

Nombre de connexions audio/supports virtuels et cartes à puce prises en charge

Vous trouverez ci-après le nombre de connexions audio/supports virtuels et cartes à puce simultanées possibles entre un client et une cible :

- 1 carte à puce
- 1 supports virtuels
- 1 carte à puce et 1 support virtuel
- 2 supports virtuels

KX III Langues de clavier prises en charge

L'unité KX III fournit un support clavier pour les langues indiquées dans le tableau suivant.

Remarque : Vous pouvez utiliser le clavier pour le chinois, le japonais et le coréen à des fins d'affichage uniquement ; l'entrée de données dans la langue locale n'est pas prise en charge pour le moment en ce qui concerne les fonctions de la console locale de KX III. Pour plus d'informations sur les claviers non US, reportez-vous à **Remarques d'informations** *(à la page 356).*

Remarque : Raritan recommande d'utiliser système-config-clavier pour modifier les langues si vous travaillez dans un environnement Linux.

Langue	Régions	Configuration du clavier
Anglais (Etats-Unis)	Etats-Unis d'Amérique et la plupart des pays anglophones : Canada, Australie et Nouvelle-Zélande, par exemple.	Clavier américain
Anglais international	Etats-Unis d'Amérique et la plupart des pays où l'anglais est utilisé : les Pays-Bas par exemple.	Clavier américain
Anglais britannique	Royaume-Uni	Clavier britannique
Chinois traditionnel	Hong Kong R.A.S., République de Chine (Taïwan)	Chinois traditionnel
Chinois simplifié	République populaire de Chine (continentale)	Chinois simplifié
Coréen	Corée du Sud	Hangeul Dubeolsik
Japonais	Japon	Clavier JIS

Langue	Régions	Configuration du clavier
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

Touches de commandes BIOS sur Mac Mini

Les commandes BIOS suivantes ont été testées sur des serveurs cibles Mac® Mini basé sur Interl et Mac Lion® tournant sur Mac Snow Leopard®. Les serveurs furent attachés à un KX III avec CIM D2CIM-DVUSB et D2CIM-VUSN. Vérifiez ci-dessous les clés prises en charge et remarques.

Touches	Description	CIM Média Virtuel	CIM Média Virtuel Double	Serveur Mac Lion HDMI CIM
Appuyez sur C au démarrage	Démarrez depuis un CD ou DVD bootable, tel que le disque d'installation Mac OS X	✓	✓	
Appuyez sur D au démarrage.	Démarrage dans Apple Hardware Test (AHT)	✓ Peut nécessiter le profil Mac BIOS pour que la souris fonctionne	✓ Peut nécessiter le profil Mac BIOS pour que la souris fonctionne	✓ Peut nécessiter le profil Mac BIOS pour que la souris fonctionne
Appuyez sur Option-	Réinitialisation de la NVRAM		✓	✓

Touches	Description	CIM Média Virtuel	CIM Média Virtuel Double	Serveur Mac Lion HDMI CIM
Commande-P-R jusqu'à ce que vous entendiez le signal de démarrage une deuxième fois.				
Appuyez sur Option au démarrage.	Démarrage dans le Gestionnaire de démarrage, où vous pouvez sélectionner un volume Mac OS X pour le démarrage.	✓	✓	✓
Appuyez sur Ejecter, F12, ou maintenez le bouton de la souris	Ejecte tout support amovible, comme un disque optique par exemple	✓	✓	
Appuyez sur N au démarrage.	Démarrage depuis un serveur réseau compatible (NetBoot)	✓	✓	✓
Appuyez sur T au démarrage.	Démarrage en mode disque cible.			✓
Appuyez sur Maj au démarrage.	Démarrage en mode de démarrage sans échec et désactivation temporaire des éléments de connexion.	✓	✓	Problème connu avec LION pour démarrer en mode sécurisé. « Mode sécurisé » en rouge n'appraît pas pour Lion
Appuyez sur Commande-V au démarrage.	Démarrage en mode Verbose.admin	✓	✓	✓
Appuyez sur Commande-S au démarrage.	Démarrage en mode utilisateur unique.	✓	✓	✓
Appuyez sur Option-N au démarrage.	Démarrage depuis un serveur NetBoot à l'aide de l'image amorçable par défaut.	✓	✓	✓
Appuyez sur Commande-R au	Démarrage depuis Lion Recovery1.	S/O	S/O	✓

Touches	Description	CIM Média Virtuel	CIM Média Virtuel Double	Serveur Mac Lion HDMI CIM
démarrage.				

Utiliser un clavier Windows pour accéder à des cibles Mac

Un clavier Windows® peut être utilisé pour accéder à un Mac® connecté à un KX III. Les touches Windows sont alors émulées pour utiliser les touches spéciales Mac. Cela revient au même que de connecter un clavier Windows directement sur le Mac.

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 134). Par défaut, toutes les requêtes reçues par KX III via HTTP (port 80) sont automatiquement transmises à HTTPS pour garantir une sécurité complète. Le KX III répond au port 80 pour le confort des utilisateurs, permettant que les utilisateurs n'aient pas à taper explicitement dans le champ URL pour accéder au KX III, tout en préservant un niveau complet de sécurité.
HTTP, Port 443	Ce port peut être configuré selon les besoins. Reportez-vous à ***Paramètres des ports HTTP et HTTPS*** (à la page 134). Par défaut, ce port est utilisé à diverses fins, notamment pour le serveur Web du client HTML, le téléchargement du logiciel client (Virtual KVM Client (VKC)) sur l'hôte du client et le transfert de flux de données KVM et de support virtuel vers le client.
Protocole KX III (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 85).
SNTP (serveur d'horloge) sur le port UDP configurable 123	KX III 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

Port	Description
	choix. **Facultatif**
LDAP/LDAPS sur les ports configurables 389 ou 636	Si KX III est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole LDAP/DAPS, 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 III 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 III 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 III est configuré pour envoyer des messages à un serveur Syslog, les ports indiqués sont utilisés pour la communication -utilise le port UDP 514.
Ports UDP par défaut SNMP	Le port 161 est utilisé pour l'accès SNMP entrant/sortant, en lecture/écriture, et le port 162 est utilisé pour le trafic sortant des traps SNMP. **Facultatif**
Port TCP 22	Le port 22 est utilisé pour l'interface de ligne de commande de KX III (lorsque vous travaillez avec l'assistance technique Raritan).
SSH	(Secure Shell) Le port SSH peut être configuré. Le port par défaut est 22.

Logiciel

Systèmes d'exploitation et navigateurs pris en charge

Systèmes d'exploitation	Navigateurs
Windows 7® Home Premium SP1 64-bit	▪ Internet Explorer® 10 et 11 ▪ Firefox® 25 ▪ Chrome® 31 ▪ Safari® 5.1.7
Windows 7 Ultimate SP1 64-bit	▪ Internet Explorer 8,9,11 ▪ Firefox 25 ▪ Chrome 31
Windows 7 Ultimate 32-bit	▪ Internet Explorer 8

Systèmes d'exploitation	Navigateurs
	▪ Firefox 25 ▪ Chrome 31
Windows 8® 64-bit	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
Serveur Windows 2012® Standard 64-bit	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
Windows XP® Edition Familiale avec SP 3	▪ Internet Explorer 10 ▪ Firefox 25 ▪ Chrome 31
openSUSE® 11.4 Celadon (x86_64)	▪ Firefox 16.0.2
Fedora® 18 (Spherical Cow)	▪ Firefox 24
RHEL 6.4	▪ Firefox 21
OS X Mountain Lion® 10.8.5 *	▪ Firefox 25 (recommandé) ▪ Safari 6.1
Solaris® 10 64-bit	▪ Firefox 3.6.23
Mac® 10.7.5	▪ Safari 6.0.5 ▪ Firefox 25

**Remarque : Lors de la mise à jour de OS X 10.8.2 à OS X 10.8.3, Safari® peut bloquer Java™.*

Exigences JRE et considérations de navigateur pour Mac

Exigences d'environnement d'éxécution Java pour Mac

Installer l'environnement d'éxécution Java 7 (JRE)® sur PC et Mac® en utilisant le Virtual KVM Client (VKC) pour accéder à des serveurs cible via KX III.

Cela garantit de fournir des performances élevées, traitement vidéo KVM-sur-IP à distance lors de l'accès aux serveurs cibles/PC/Mac.

La dernière version de JRE pour Mac peut être téléchargée depuis le Site d'assistance Apple.

Considérations de navigateur pour Mac

Java peut être désactivé par défaut sur certains navigateurs. Active Java et accepte tous les avertissements de sécurité afin d'utiliser KX III.

Certaines versions de Safari® bloquent Java pour des raisons de sécurité. Etant donné que Java est requis pour utiliser KX III, Raritan vous recommande d'utiliser Firefox® à la place.

De plus, il peut vous être demandé de naviguer parmi un nombre de messages. Sélectionnez 'Ne pas bloquer' si ces messages sont affichés.

Exigences Java et Microsoft .NET

Java® 1.7 (ou plus élevé) ou Microsoft .NET® 3.5 (ou version ultérieure) est obligatoire pour utiliser KX III

KX III vérifie votre version actuelle de Java et vous demande de la mettre à jour si elle n'est pas compatible.

Consultez les ***Remarques sur l'environnement d'éxécution de Java (JRE)*** (à la page 356) pour plus d'informations.

Exigence de clavier multi-langue JRE

Pour que les claviers multilingues fonctionnent dans KX III et le Virtual KVM Client (VKC), installez la version multilingue de JRE™.

Evénements capturés dans le journal d'audit et dans Syslog

Vous trouverez ci-après la liste et la description des événements capturés par le journal d'audit et syslog de KX III.

- Connexion d'accès - Un utilisateur s'est connecté à KX III.
- Déconnexion d'accès - Un utilisateur s'est déconnecté de KX III.
- Active USB Profile - Le profil USB est actif.
- CIM Connected - Un CIM a été connecté.
- CIM Disconnected - Un CIM a été déconnecté.
- Connection Lost - La connexion à la cible a été perdue.
- Disconnected User - Un utilisateur a été déconnecté d'un port.
- End CC Control - La gestion par CC-SG est terminée.
- Login Failed - La connexion de l'utilisateur a échoué.
- Password Changed - Le mot de passe a été modifié.
- Port Connect - Le port a été connecté.
- Port Disconnect - Le port a été déconnecté.
- Port Status Change - Modification du statut du port
- Scan Started - Un balayage de cible a été démarré.
- Scan Stopped - Un balayage de cible a été arrêté.
- Session Timeout - Un délai d'inactivité de session a expiré.
- VM Image Connected - Une image VM a été connectée.
- VM Image Disconnected - Une image VM a été déconnectée.

Annexe E Remarques d'informations

Dans ce chapitre

Présentation 356
Remarques sur l'environnement d'éxécution de Java (JRE) 356
Remarques sur la prise en charge d'IPv6 358
Problèmes de performances de connexion en double pile 359
Remarques CIM 359
Remarques sur le support virtuel 361
Remarques sur les ports et profils USB 364
Modes et résolutions vidéo.....366
Remarques clavier.....367
Remarques souris 371
Audio.....372
Remarques sur les cartes à puce.....373
Remarques CC-SG 373
Remarques Navigateur.....374

Présentation

Cette section comporte des remarques importantes sur l'utilisation de KX III. Les mises à jour à venir seront rapportées et disponibles en ligne via le lien d'aide de l'interface de la console distante de KX III.

Remarque : Certaines rubriques de cette section traitent de plusieurs autres dispositifs Raritan car divers dispositifs sont concernés par ces informations.

Remarques sur l'environnement d'éxécution de Java (JRE)

Désactiver la mise en mémoire cache de Java et effacer le cache de Java

Il est recommandé de désactiver la mise en mémoire cache de Java sous Microsoft Windows® et d'effacer le cache de Java™.

Pour désactiver la mise en mémoire cache de Java et effacer le cache:

1. A partir du menu de démarrage Windows, cliquez sur Panneau de Contrôle.
2. Double-cliquez sur l'icône Java pour lancer le programme. Le panneau de contrôle de Java s'affiche.
3. Pour désactiver la mise en mémoire cache de Java :

a. Dans l'onglet Généralités, cliquez sur le bouton Paramètres. La boîte de dialogue de paramètres des fichiers temporaires s'affiche.

b. Cliquez sur le bouton View Applets (Afficher les applets). L'afficheur du cache des applets Java apparaît :

c. Désélectionnez la case Enable Caching (Activer la mise en mémoire cache) si elle est déjà cochée.

d. Cliquez sur OK.

4. Pour effacer le cache de Java :

a. Dans la boîte de dialogue des paramètres de fichiers temporaires, cliquez sur le bouton Delete Files (Supprimer les fichiers). La boîte de dialogue de suppression des fichiers temporaires s'affiche.

b. Sélectionnez les fichiers temporaires que vous souhaitez supprimer.

c. Cliquez sur OK.

Java ne chargeant pas correctement sur Mac

Si vous utilisez un Mac® et voyez le message suivant en vous connectant à un dispositif à partir du Tableau d'Accès au port KX III, Java™ ne charge pas correctement:

« Erreur lors de l'obtention de la liste de cibles ouvertes, veuillez réessayer dans quelques secondes ».

Si cela survient, vérifiez votre installation Java sur ce site web:
http://www.java.com/en/download/testjava.jsp
http://www.java.com/en/download/testjava.jsp

Si votre applet Java est inactif, il peut être activé à partir de cette page. Si cela n'a pas été installé correctement, un message vous en informe et vous pouvez ensuite réinstaller Java.

Remarques sur la prise en charge d'IPv6

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

Java

Java™ 1.7 prend en charge IPv6 pour :

- Solaris™ 10 (et supérieur)
- Linux® kernel 2.1.2 (et supérieur)/RedHat 6.1 (et supérieur)
- Solaris 10 (et supérieur)
- Les systèmes d'exploitation Windows XP® SP1 et Windows 2003®, Windows Vista® et Windows 7

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.
- Pour AKC avec IPv6 sous Windows XP, ajoutez l'exécutable kxgui.exe à la liste d'exceptions du pare-feu. Affichez le fichier journal sur le client pour identifier le chemin d'accès complet au fichier kxgui.exe.

Samba

- IPv6 n'est pas pris en charge pour une utilisation avec les supports virtuels sous Samba.

Notes de version Ipv6 pour téléchargement de la Validation de Certification du Serveur AKC

Si vous vous connectez à un dispositif autonome KX III et que la prise en charge de la validation du certificat du serveur de téléchargement AKC est activée, le format IPv6 valable pour générer le certificat est :

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` où figure un 0 non significatif

  ou

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` où l'adresse n'est pas compressée

Problèmes de performances de connexion en double pile

Si vous utilisez KX III dans une configuration en double pile, il est important de configurer le système de noms de domaine (DNS) correctement dans KX III afin d'éviter les retards lors de la connexion.

Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 115) pour plus d'informations sur la configuration de DNS dans KX III.

Remarques CIM

Souris à 3 boutons Windows sur les cibles Linux

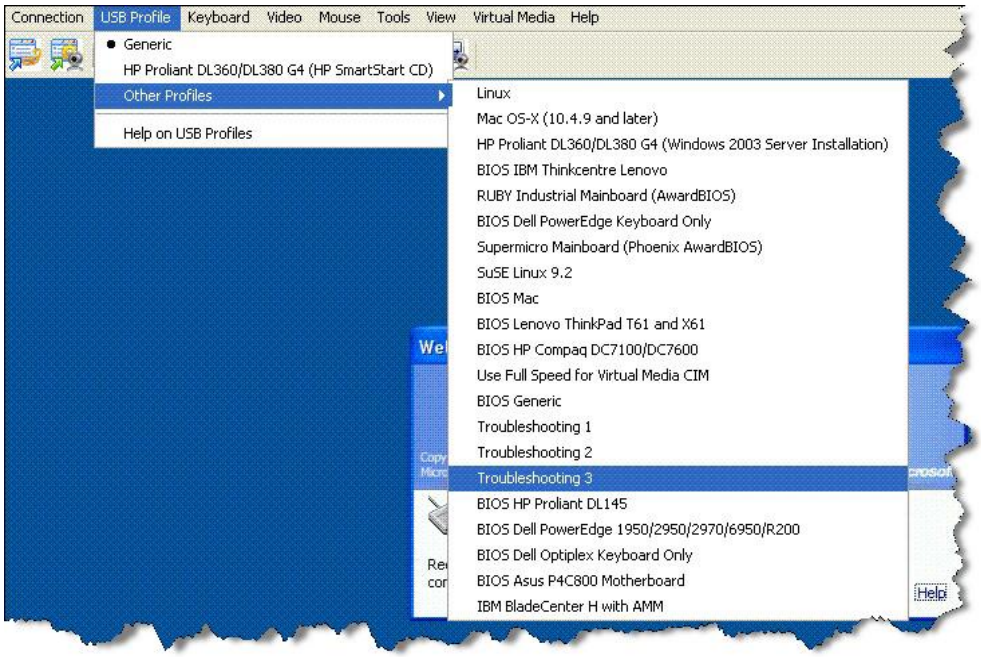
Lorsque vous utilisez une souris à 3 boutons sur un client Windows® connecté à une cible Linux®, le bouton gauche peut être mappé sur le bouton central de la souris à 3 boutons du client Windows.

Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel

Le système d'exploitation Windows 2000® ne prend pas en charge les dispositifs USB composites, comme le D2CIM-VUSB de Raritan, de la même façon que les dispositifs USB non composites.

En conséquence, l'icône de la barre d'état Supprimer le périphérique en toute sécurité n'apparaît pas pour les lecteurs mappés par D2CIM-VUSB et un message d'avertissement peut s'afficher lors de la déconnexion du dispositif. Raritan n'a toutefois constaté aucun problème à la suite de message.

Le service technique de Raritan aux Etats-Unis a mis au point une configuration prenant en charge l'icône Supprimer le périphérique en toute sécurité et évitant ce message Windows. Cette configuration requiert l'utilisation de l'adaptateur de supports virtuels D2CIM-DVUSB et le profil USB Troubleshooting 3, qui configure D2CIM-DVUSB en tant que dispositif USB non composite prenant en charge une connexion de supports virtuels unique. Raritan a testé cette configuration avec succès aux Etats-Unis et au Japon.



Remarques sur le support virtuel

Ne peut pas se connecter aux lecteurs de clients Linux

Si vous ne pouvez pas vous connecter à un lecteur média virtuel lorsque vous vous connectez à un client utilisant Linux® Fedora™ 18 avec Java™ 1.7.0 (mise à jour 45 et supérieure), désactivez SELinux dans Fedora 18 sur le client pour résoudre ce problème.

Ne peut pas écrire sur/à partir d'un fichier de Client Mac

Si vous vous connectez au KX III depuis un client Mac® 10.8.5 éxécutant Safari® 6.1 avec Java™ 1.7 et ne pouvez pas écrire sur/à partir d'un serveur cible ou accéder à un support virtuel, suivez la procédure suivante pour corriger cela:

1. Dans Safari, sélectionnez Préférences.
2. Dans l'onglet Sécurité, sélectionnez Gérer les Paramètres du site web.
3. Cliquez sur « Site web pour KX3 ».
4. Sélectionnez « Executer en mode sécurisé » à partir de la liste défilante.
5. Redémarrez Safari.

Utilisation du support virtuel via VKC et AKC dans un environnement Windows

Les droits Administrateur et utilisateur standard dans le système d'exploitation Windows XP®sont différents de ceux des systèmes d'exploitation Windows Vista® et Windows 7®.

Lorsqu'elle est activée dans Vista ou dans Windows 7, la fonction Contrôle d'accès d'utilisateur fournit le niveau de droits le plus bas dont un utilisateur a besoin pour une application. Par exemple, l'option « Exécuter en tant qu'administrateur » est proposée sous Internet Explorer® pour autoriser explicitement les utilisateurs à effectuer des tâches de niveau Administrateur, sinon celles-ci ne sont pas accessibles même si l'utilisateur dispose d'une connexion administrateur.

Ces deux fonctions affectent le type de supports virtuels accessibles aux utilisateurs via Virtual KVM Client (VKC) et Active KVM Client (AKC). Consultez l'aide Microsoft® pour en savoir plus sur ces fonctions et comment les utiliser.

La liste suivante répertorie des types de supports virtuels accessibles via VKC et AKC dans un environnement Windows. Ces fonctions sont classées par client, puis par rôle utilisateur Windows.

Windows XP

Si vous utilisez VKC et AKC dans un environnement Windows XP, les utilisateurs doivent disposer de droits Administrateur pour accéder à n'importe quel type de support virtuel autre que les connexions CD-ROM, les ISO et les images ISO.

Windows Vista and Windows 7

Si vous utilisez VKC et AKC dans un environnement Windows Vista ou Windows 7 et que la fonction Contrôle d'accès d'utilisateur est activée, les types de supports virtuels suivants sont accessibles suivant le rôle Windows de l'utilisateur :

Client	Administrateur	Utilisateur standard
AKC et VKC	Accès : • Lecteurs fixes et partitions de lecteurs fixes • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes	Accès : • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes

Support virtuel non rafraîchi après l'ajout de fichiers

Après le montage d'un lecteur de support virtuel, si vous ajoutez des fichiers à ce lecteur, ces fichiers peuvent ne pas apparaître immédiatement sur le serveur cible. Supprimez, puis rétablissez la connexion de support virtuel.

Lecteur virtuel Linux répertorié deux fois

Pour KX III, les utilisateurs qui sont enregistrés sous clients Linux™ en tant que super-utilisateur (utilisateur root), les lecteurs sont listés deux fois dans la liste déroulante du Lecteur Local.

Vous verrez par exemple eg /dev/sdc et eg /dev/sdc1 où le premier lecteur est le secteur d'amorçage et le second, la première partition du disque.

Accès à Virtual Media sur Windows 2000

Un lecteur local de support virtuel n'est pas accessible sur un serveur Windows 2000® utilisant un D2CIM-VUSB.

Déconnecter les Lecteurs USB Virtuels Mac et Linux

Dans un environnement Linux® ou Mac®:

- Pour les utilisateurs Linux, si il y a dev/sdb et /dev/sdb1, le client utilise seulement /dev/sdb1 et le considère comme un disque amovible.
- /dev/sdb n'est pas accessible à l'utilisateur.
- Pour les utilisateurs Linux, si il y a /dev/sdb/ mais pas de /dev/sdb1, alors /dev/sdb est utilisé comme disque amovible.
- /dev/disk1 and /dev/disk1s1 sont utilisés pour les utilisateurs Mac.

Durée d'amorçage du BIOS cible avec les supports virtuels

L'amorçage du BIOS de certaines cibles peut durer plus longtemps sur le support est monté virtuellement à la cible.

Pour raccourcir la durée d'amorçage :

1. Fermez Virtual KVM Client pour libérer complètement les lecteurs de supports virtuels.
2. Redémarrez la cible.

Echec de connexion des supports virtuels lors de l'utilisation du haut débit

Dans certains cas, il peut être nécessaire de sélectionner l'option « Utiliser le haut débit pour le CIM du support virtuel » lorsque la cible rencontre des difficultés avec la vitesse de connexion USB à haut débit ou qu'elle connaît des erreurs de protocole USB en raison d'une dégradation du signal due à la présence de connecteurs et de câbles supplémentaires. (par exemple, une connexion à un serveur lame via une clé électronique).

Remarques sur les ports et profils USB

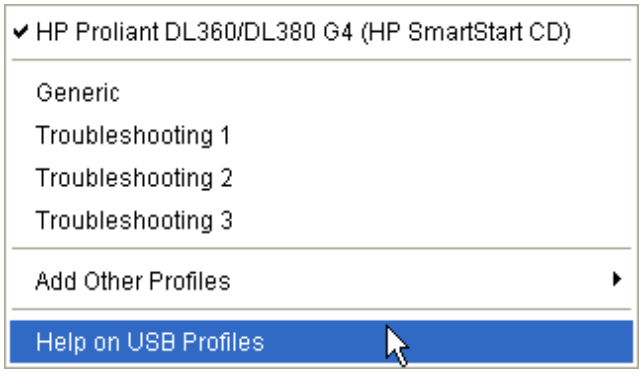
Ports USB VM-CIM et DL360

Les serveurs HP® DL360 sont dotés d'un port USB à l'arrière et d'un autre à l'avant. Avec DL360, les deux ports ne peuvent pas être utilisés simultanément. Aussi, un VM-CIM double ne peut pas être utilisé sur les serveurs DL360.

Toutefois, pour contourner ce problème, un concentrateur USB2 peut être connecté au port USB à l'arrière du dispositif et un VM-CIM double peut être connecté au concentrateur.

Aide pour la sélection des profils USB

Lorsque vous êtes connecté à un serveur cible KVM via Virtual KVM Client (VKC), vous pouvez afficher des informations relatives aux profils USB via l'aide sur la commande USB Profiles (Profils USB) du menu USB Profile (Profil USB).



L'aide relative aux profils USB apparaît dans la fenêtre USB Profile Help. Pour plus d'informations sur des profils USB spécifiques, reportez-vous à Profils USB disponibles.

Raritan propose une sélection standard de profils de configuration USB pour des implémentations de serveurs sur une grande variété de systèmes d'exploitation et de niveaux de BIOS. Ces profils sont conçus pour offrir une adéquation optimale entre les configurations des dispositifs USB distants et des serveurs cible.

Le profil Generic (Générique) répond aux besoins des configurations de serveurs cible déployées les plus fréquentes.

Des profils supplémentaires sont disponibles pour répondre aux besoins spécifiques d'autres configurations de serveurs déployées courantes (par exemple, Linux®, Mac OS X®).

Un certain nombre de profils (désignés par nom de plate-forme et révision de BIOS) ont également été adaptés pour améliorer la compatibilité de la fonction Support virtuel avec le serveur cible ; par exemple, lors d'un fonctionnement au niveau du BIOS.

L'option Add Other Profiles (Ajouter d'autres profils) permet d'accéder aux autres profils disponibles sur le système. Les profils sélectionnés dans cette liste sont ajoutés au menu USB Profile (Profil USB). Sont inclus des profils de dépannage (Troubleshooting) conçus pour identifier les limites des configurations.

Les options du menu Profil USB sont configurables via Paramètres du dispositif de console > Configuration des ports.

Si les profils USB standard fournis par Raritan ne répondent pas aux conditions requises de votre serveur cible, l'assistance technique Raritan peut vous aider à trouver une solution adaptée à cette cible. Raritan vous recommande d'effectuer les opérations suivantes :

1. Consultez les notes de publication les plus récentes sur le site Web de Raritan (www.raritan.com) sur la page des mises à jour de firmware pour vérifier s'il n'existe pas de solution pour votre configuration.
2. Dans le cas contraire, fournissez les informations lorsque vous contactez l'assistance technique Raritan :
    a. Informations sur le serveur cible : fabricant, modèle, BIOS, fabricant et version.
    b. Usage envisagé (par exemple, redirection d'une image pour recharger le système d'exploitation d'un serveur depuis le CD).

Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce

Dans certains cas, vous serez amené à modifier le profil USB d'un serveur cible. Vous aurez par exemple à remplacer la vitesse de connexion par Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du support virtuel) lorsque la cible rencontre des difficultés avec la vitesse de connexion High Speed USB (USB à haut débit).

A la modification d'un profil, vous recevrez, le cas échéant, un message Nouveau matériel détecté et devrez vous connecter à la cible avec des droits d'administrateur afin de réinstaller le pilote USB. Ceci ne se produira probablement que les premières fois où la cible détectera les nouveaux paramètres du périphérique USB. Elle sélectionnera correctement le pilote par la suite.

Modes et résolutions vidéo

L'image vidéo est foncée sous Mac

Si vous utilisez un Mac® avec un port vidéo HDMI et que la vidéo semble trop foncée, activez le Mode de compatibilité DVI sur le CIM pour aider à résoudre le problème.

Reportez-vous à ***Configuration des ports CIM*** (à la page 95).

Bandes noires/barres affichées sur le Port local

Certains serveurs et résolutions vidéo peuvent être affichés sur le port local avec des petites barres noires dans le coin de l'écran.

Si cela se produit:

1. Essayez une résolution différent, ou
2. Si vous utilisez un CIM numérique, alors changez la Résolution de l'écran d'origine sur le page de Configuration des Ports dans une autre résolution, ou
3. Si vous utilisez le CIM HDMI, utilisez le Mode de compatibilité DVI

Contactez l'assistance technique Raritan pour plus d'aide.

Synch Vidéo Sun Composite

La synchronisation vidéo Sun™ composite n'est pas prise en charge.

Modes vidéo SUSE/VESA

L'outil de configuration SaX2 de SuSE X.org génère des modes vidéo à l'aide des entrées ModeLine du fichier de configuration X.org. Ces modes vidéo ne correspondent pas exactement au minutage du mode vidéo VESA (même si un écran VESA est sélectionné). Le KX III, en revanche, s'appuie sur le minutage du monde VESA exact pour une synchronisation parfaite. Cette disparité peut entraîner des bordures noires, des sections d'image absentes et des parasites.

Pour configurer l'affichage vidéo SUSE :

1. Le fichier de configuration généré /etc/X11/xorg.conf inclut une section Monitor comportant une option appelée UseModes. Par exemple,
   UseModes "Modes[0]"
2. Mettez cette ligne en commentaire (à l'aide de #) ou supprimez-la complètement.
3. Redémarrez le serveur X.

Grâce à cette modification, le minutage du mode vidéo interne du serveur X sera utilisé et correspondra exactement au minutage du mode vidéo VESA, entraînant un affichage vidéo correct sur KX III.

Remarques clavier

Clavier français

Caret (clients Linux uniquement)

La Virtual KVM Client (VKC) ne traitent pas la combinaison de touches Alt Gr + 9 comme le caret (^) lorsqu'un clavier français est utilisé avec des clients Linux®.

Pour obtenir le caret :

Sur un clavier français, appuyez sur la touche ^ (à droite de la touche P), puis immédiatement sur la barre d'espacement.

Ou, créez une macro constituée des commandes suivantes :

1. Appuyez sur la touche Alt Gr.
2. Appuyez sur la touche 9.
3. Relâchez la touche 9.
4. Relâchez la touche Alt Gr.

Remarque : Ces procédures ne s'appliquent pas à l'accent circonflexe (au-dessus des voyelles). Dans tous les cas, la touche ^ (à droite de la touche P) fonctionne sur les claviers français pour créer l'accent circonflexe, lorsqu'elle est utilisée en combinaison avec un autre caractère.

Accent (clients avec système d'exploitation Windows XPR seulement)

Depuis Virtual KVM Client (VKC), la combinaison de touches Alt Gr + 7 entraîne l'affichage en double du caractère accentué lors de l'utilisation d'un clavier français avec les clients Windows XP®.

Remarque : Ceci ne se produit pas avec les clients Linux®.

Pavé numérique

Depuis Virtual KVM Client (VKC), les symboles du pavé numérique s'affichent comme suit lors de l'utilisation d'un clavier français :

Symbole du pavé numérique	Affiche
/	;
.	;

Tilde

Depuis Virtual KVM Client (VKC), la combinaison de touches Alt Gr + 2 ne produit pas le tilde (~) lors de l'utilisation d'un clavier français.

Pour obtenir le tilde :

Créez une macro constituée des commandes suivantes :

- Appuyez sur la touche Alt Gr.
- Appuyez sur la touche 2.
- Relâchez la touche 2.
- Relâchez la touche Alt Gr.

Préférence de la langue du clavier (clients Fedora Linux)

Etant donné que le JRE™ de Sun™ sous Linux a des difficultés à générer les événements KeyEvents corrects pour les claviers dans d'autres langues configurés à l'aide des préférences système, Raritan recommande de configurer ces claviers à l'aide des méthodes décrites dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Anglais britannique	Paramètres système (centre de contrôle)
Français	Indicateur de clavier
Allemand	Indicateur de clavier
Hongrois	Paramètres système (centre de contrôle)
Espagnol	Paramètres système (centre de contrôle)
Allemand (Suisse)	Paramètres système (centre de contrôle)
Norvégien	Indicateur de clavier
Suédois	Indicateur de clavier
Danois	Indicateur de clavier
Japonais	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Italien	Paramètres système (centre de contrôle)
Portugais	Paramètres système (centre de contrôle)

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

Sur un clavier hongrois depuis un client Linux, les lettres U et O avec deux accents aigus ne fonctionnent qu'avec JRE 1.6 5(et supérier).

Plusieurs méthodes permettent de définir les préférences de langue de clavier sur les clients Fedora® Linux. La méthode suivante doit être utilisée pour le mappage correct des touches de Virtual KVM Client (VKC).

Pour définir la langue du clavier à l'aide des paramètres système :

1. Depuis la barre d'outils, choisissez Système > Préférences > Clavier.

2. Ouvrez l'onglet Agencements.
3. Ajoutez ou sélectionnez la langue appropriée.
4. Cliquez sur Fermer.

Pour définir la langue du clavier à l'aide de l'indicateur de clavier :

1. Cliquez avec le bouton droit sur la barre de tâches et choisissez Ajouter au tableau de bord.
2. Dans la boîte de dialogue Ajouter au tableau de bord, cliquez avec le bouton sur Indicateur de clavier, et dans le menu, choisissez Ouvrir les préférences clavier.
3. Dans la boîte de dialogue Préférences clavier, cliquez sur l'onglet Agencements.
4. Ajoutez et enlevez des langues selon les besoins.

Macros ne s'enregistrant pas sur serveurs cible Linux

Si vous recevez le message d'erreur suivant lorsque vous créez puis enregistrez un macro sur un serveur cible équipé de Linux® Fedora™ 18 avec Java™ 1.7.0 (mise à jour 45 et supérieure), désactivez SELinux dans Fedora 18 sur le serveur cible pour résoudre le problème.

```
"Une erreur s'est produite lors de l'essai d'écriture des
nouveaux macros clavier. La macro n'a pas été ajoutée"
```

Touches clavier non prises en charge pour accès à distance

Lorsqu'un Mac®est utilisé comme client, les touches suivantes du clavier ne sont pas capturées par Java™ Runtime Environment (JRE™) :

- F9
- F10
- F11
- F14
- F15
- Monter le volume
- Descendre le volume
- Muet
- Ejection

En conséquence, les Virtual KVM Client (VKC) ne sont pas en mesure de traiter ces touches d'un clavier de client Mac.

Remarques souris

Synchronisation des pointeurs de souris (Fedora)

Lors d'une connexion en mode souris double à un serveur cible exécutant Fedora® 7, si les pointeurs des souris cible et locale perdent leur synchronisation, faire passer le mode de souris de ou en Intelligent ou Standard peut améliorer la synchronisation.

Le mode de souris unique peut également fournir un meilleur contrôle.

Pour resynchroniser les curseurs de souris :

- Utiliser l'option Synchroniser la souris de Virtual KVM Client (VKC).

Mode souris simple - lors de la Connexion à une cible contrôlée par CC-SG

Si vous utilisez Firefox® pour vous connecter à une cible KX III contrôlée par CC-SG à l'aide de DCIM-PS2 ou DCIM-USBG2, et que vous passez au mode souris simple dans Virtual KVM Client, le focus ne sera plus sur la fenêtre VKC et la souris ne répondra pas.

Dans ce cas, cliquez ou appuyez sur Alt+Tab pour rétablir le focus sur la fenêtre VKC.

Audio

Problèmes en matière de lecture et de capture audio

Fonctions pouvant interrompre une connexion audio

Si vous utilisez une des fonctions ci-après lors de la connexion à un dispositif audio, votre connexion audio peut être interrompue. Raritan vous recommande de ne pas utiliser ces fonctions si vous êtes connecté à un dispositif audio :

- Détection automatique de la vidéo
- Utilisation extensive du port local
- Ajout d'utilisateurs

Problèmes lors de l'utilisation simultanée d'un dispositif de capture et d'un dispositif de lecture sur une cible

Sur certaines cibles, la connexion simultanée de dispositifs de capture et de lecture risque de ne pas fonctionner en raison du contrôleur de concentrateur USB et son mode de gestion des ports USB. Prévoyez de sélectionner un format audio nécessitant moins de bande passante.

Si ceci ne résout pas le problème, branchez le connecteur de clavier et souris du CIM D2CIM-DVUSB sur un port différent de la cible. Si ceci ne résout pas le problème, branchez le dispositif sur un concentrateur USB et connectez ce dernier à la cible.

Audio dans un environnement Linux

Vous trouverez ci-après les problèmes répertoriés lors de l'utilisation de la fonction audio dans un environnement Linux®.

- Utilisateurs LinuxR : utilisez le dispositif audio par défaut pour la lecture. Le son risque de ne pas passer si une carte son autre que celle par défaut est sélectionnée.
- Les clients SuSE 11 requièrent l'installation de Javas_1_6_0-sun-alsa (prise en charge ALSA pour java-1_6_0-sun) via YAST.
- Pour les casques Logitech avec micro incorporé, seule l'option Mono Capture est disponible.
- Si vous exécutez SUSE 11 et utilisez un pilote ALSA, déconnectez-vous de KX II, puis reconnectez-vous pour afficher le dispositif.

  En outre, si vous connectez et déconnectez le dispositif audio plusieurs fois, il risque d'être répertorié plusieurs fois, au lieu d'une comme il devrait l'être.

- L'utilisation de la fonction audio avec une cible Fedora Core® 13 paramétrée sur mono 16 bits, 44k peut entraîner des interférences importantes pendant la lecture.

Audio dans un environnement Windows

Sur les clients Windows® 64 bits, un seul dispositif de lecture apparaît sur le panneau Connexion Audio lors de l'accès au dispositif via le Virtual KVM Client (VKC).

Il s'agit du dispositif audio par défaut et il est affiché sur le panneau Connect Audio sous Java Sound Audio Engine (Moteur audio).

Remarques sur les cartes à puce

Connexions par carte à puce Virtual KVM Client (VKC) aux serveurs Fedora

Si vous utilisez une carte à puce pour vous connecter à un serveur Fedora® Linux® via Virtual KVM Client (VKC), effectuez une mise à niveau de la bibliothèque pcsc-lite vers 1.4.102-3 ou supérieure.

Remarques CC-SG

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

Lorsque Virtual KVM Client est démarré depuis CommandCenter Secure Gateway (CC-SG) en mode proxy, la version VKC est inconnue.

Dans la boîte de dialogue About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan), la version est indiquée comme inconnue.

Déplacement entre ports sur un dispositif

Si vous effectuez un déplacement entre ports du même dispositif Raritan et reprenez la gestion au bout d'une minute, CC-SG peut afficher un message d'erreur.

Si vous reprenez la gestion, l'affichage est mis à jour.

Remarques Navigateur

Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora

Si vous accédez à Firefox® et que vous utilisez un serveur Fedora®, Firefox risque de se bloquer à l'ouverture.

Pour résoudre ce problème, installez le plug-in libnpjp2. afin que Java™ puisse se connecter sur le serveur.

Annexe F Foire aux questions

Dans ce chapitre

FAQ - Généralités....375
Accès à distance....379
Support virtuel universel....382
Bande passante et performance KVM-sur-IP....384
Gestion de réseau IPv6....388
Windows....390
Serveurs lames....391
Installation....393
Port Local - KX III....395
Port local étendu....396
Double alimentation....397
Contrôle des unités de distribution d'alimentation (PDU)....397
Ethernet et mise en réseau IP....399
Groupement, fonction multiniveau et mise en cascade des ports locaux401
Modules d'interface pour ordinateur (CIM)....404
Sécurité....405
Authentification par cartes à puce et CAC....407
Capacités de gestion....408
Documentation et assistance....410
Divers....411

FAQ - Généralités

Question	Réponse
Qu’est-ce que Dominion KX II ?	Dominion KX II est un commutateur KVM (clavier, vidéo, souris) numérique de troisième génération qui permet à un, deux, quatre ou huit administrateurs informatiques d'accéder à et de gérer 8, 16, 32 ou 64 serveurs sur le réseau grâce à des fonctionnalités au niveau BIOS. Dominion KX II est entièrement indépendant du matériel et du système d'exploitation. Les utilisateurs peuvent donc dépanner et reconfigurer les serveurs même lorsqu'ils sont éteints. Pour le rack, Dominion KX II offre les mêmes fonctionnalités, commodités, économies d'espace et de coût que les commutateurs KVM analogiques traditionnels. Toutefois, Dominion KX II intègre également la technologie KVM sur réseau IP la plus performante du secteur, permettant ainsi à plusieurs administrateurs d'accéder aux consoles des serveurs KVM depuis n'importe quel poste de travail mis en réseau, ainsi que depuis un iPhone® et un iPad®.

Question	Réponse
Qu'est-ce qui différencie KX III de KX II?	KX III est la version nouvelle génération de KX III. Doté d'un design moderne avec d'une puissance de calcul et de stockage améliorée, KX III fournit un accès KVM-sur-IP à l'administration de l'informatique, ainsi que l'accès IP à haute performance pour des applications de diffusion. KX III comprend la quasi-totalité des fonctionnalités de KX II avec les avancés suivantes: Le nouveau moteur de traitement vidéo de KX III prend en charge une large gamme d'applications à partir d'applications informatiques traditionnelles pour les applications de diffusion les plus dynamiques nécessitant 30 images par seconde 1920x1080, des couleurs 24 bits, l'audio numérique, deux moniteurs et DVI, HDMI, DisplayPort et VGA vidéo. Avec le premier port local de l'industrie basé sur DVI, l'interface d'utilisateur commune de KX III fournit de nouveaux niveaux de productivité et de performance pour l'administration au niveau du rack et l'accès au serveur. Tous les modèles KX III dispose d'un port multiniveau pour connecter plusieurs commutateurs Dominion KX III ensembler et accéder aux serveurs liés. Il est possible d'accéder jusqu'à 1024 serveurs via une liste de ports consolidée. KX III prend en charge tous les CIM Dominion et Paragon II pris en charge par KX II.

Question	Réponse
En quoi Dominion KX II diffère-t-il d'un logiciel de contrôle à distance ?	Lors d'une utilisation de Dominion KX III à distance, au premier abord, l'interface peut sembler similaire aux logiciels de gestion à distance pcAnywhere™, Terminal Services/Bureau distant Windows®, VNC, etc. Toutefois, Dominion KX III est une solution matérielle, non logicielle, ce qui le rend beaucoup plus puissant : Ne dépendant ni du système d'exploitation ni du matériel - Dominion KX II peut être utilisé pour gérer des serveurs exécutant de nombreux systèmes d'exploitation courants, notamment Intel®, Sun®, PowerPC exécutant Windows, Linux®, Solaris™, etc. Ne dépend pas de l'état ou d'un serveur " agentless " – Dominion KX II n'a pas besoin que le système d'exploitation du serveur géré soit en marche, ni qu'un logiciel spécial soit installé sur le serveur géré. Hors-bande – Même s'il n'existe pas de connexion disponible sur le réseau même du serveur géré, celui-ci peut quand même être géré par Dominion KX III. Accès au niveau du BIOS – Même si le serveur est bloqué lors du démarrage, il requiert un redémarrage en mode sans échec ou une modification des paramètres BIOS du système, Dominion KX III fonctionne toujours sans faille pour permettre de procéder à ces configurations.
Est-il possible de monter Dominion KX III en rack ?	Oui. Dominion KX II est livré en livraison standard avec des supports de fixation 19". Il peut également être monté en rack par l'arrière de façon à ce que les ports du serveur soient dirigés vers l'avant.
Quelles sont les dimensions de Dominion KX III ?	Dominion KX III ne mesure qu'1U de hauteur (à l'exception de KX2-864 et KX2-464 qui mesurent 2U), s'adapte à un rack standard de 19 pouces et ne mesure que 29 cm de profondeur. Dominion KX2-832 et KX2-864 mesurent 36 cm de profondeur.

Accès à distance

Question	Réponse
Combien d'utilisateurs peuvent accéder à distance aux serveurs sur chaque Dominion KX III ?	Les modèles Dominion KX III permettent la connexion distante de huit utilisateurs au maximum par canal d'utilisateur pour l'accès et la gestion simultanés d'un serveur cible unique. Pour les dispositifs à un canal tels que DKX3-116, un seul serveur cible peut être utilisé et géré par huit utilisateurs distants maximum. Pour les dispositifs à deux canaux tels que DKX3-216, huit utilisateurs distants au maximum peuvent utiliser et gérer le serveur sur le canal un et huit autres utilisateurs au maximum sur le canal deux. En ce qui concerne les dispositifs à quatre canaux, huit utilisateurs au maximum par canal, pour un total de 32 (8 x 4) utilisateurs, peuvent accéder à quatre serveurs et les gérer. De même, pour les dispositifs à huit canaux, huit utilisateurs au maximum peuvent accéder à un seul serveur, jusqu'à un total maximum de 32 utilisateurs sur huit canaux.
Puis-je accéder à distance aux serveurs depuis mon iPhone ou iPad ?	Oui. Les utilisateurs peuvent accéder aux serveurs connectés à KX III à l'aide de leur iPhone ou iPad.
Deux utilisateurs peuvent-ils visualiser le même serveur simultanément ?	Oui. En fait, huit personnes au maximum peuvent utiliser et gérer n'importe quel serveur unique en même temps.
Deux utilisateurs, l'un à distance et l'autre à partir du port local, peuvent-ils accéder au même serveur ?	Oui. Le port local est totalement indépendant des « ports » à distance. Le port local peut accéder au même serveur grâce à la fonctionnalité PC-Share.

Question	Réponse
Quels sont les matériels, logiciels ou la configuration réseau nécessaires pour accéder à Dominion KX III à partir d'un ordinateur client ?	Dominion KX II étant entièrement accessible par le Web, il ne requiert l'installation d'aucun logiciel spécifique sur les clients utilisés pour y accéder. *Remarque : La version KX III 3.0.0 ne fournit pas de support modem, mais en fournira dans de futures versions.* Il est possible d'accéder à Dominion KX III par le biais des principaux navigateurs Web : Internet Explorer® et Firefox®. Dominion KX II est accessible sur les ordinateurs Windows®, Linux® et Mac® par l'intermédiaire du client Windows de Raritan et des clients Multiplatform et Virtual KVM™ Java™. Les administrateurs Dominion KX III peuvent également effectuer une gestion à distance (définir des mots de passe et la sécurité, renommer des serveurs, modifier des adresses IP, etc.) grâce à une interface navigateur pratique.

<table>
<tr><th>Question</th><th>Réponse</th></tr>
<tr><td>Quelle est la taille du fichier de l'applet utilisée pour accéder à Dominion KX III ? Combien de temps faut-il pour l'extraire ?</td><td>La taille de l'applet Virtual KVM Client (VKC) utilisée pour accéder à Dominion KX III est d'environ 500 Ko. Le tableau suivant indique le temps nécessaire pour extraire l’applet de Dominion KX III à différentes vitesses réseau :

<table>
<tr><td>100 Mbps</td><td>Vitesse réseau théorique de 100Mbit</td><td>0,05 secondes</td></tr>
<tr><td>60 Mbps</td><td>Vitesse réseau pratique probable 100 mégabits</td><td>0,08 secondes</td></tr>
<tr><td>10 Mbps</td><td>Vitesse réseau théorique
10 mégabits</td><td>0,4 secondes</td></tr>
<tr><td>6 Mbps</td><td>Vitesse réseau pratique probable 10 mégabits</td><td>0,8 secondes</td></tr>
<tr><td>512 Kbps</td><td>Vitesse de téléchargement (type) d'un modem câblé</td><td>8 secondes</td></tr>
</table></td></tr>
<tr><td>Disposez-vous d'un client KVM Windows ?</td><td>Oui. Nous avons un client Windows .NET natif appelé Active KVM Client (AKC) de Raritan. Consultez Aide Active pour Client KVM (AKC) (à la page 292)</td></tr>
<tr><td>Disposez-vous d'un client KVM non-Windows ?</td><td>Oui. Le Virtual KVM Client (VKC) permet aux non-utilisateurs Windows de se connecter à des serveurs cible dans le centre de données. Consultez l'Aide pour Virtual KVM Client (VKC) (voir "Aide Virtuelle pour Client KVM (VKC)" à la page 240)</td></tr>
<tr><td>Vos clients KVM offrent-ils une prise en charge multilingue ?</td><td>Oui. L'interface utilisateur HTML de Dominion KX III et les clients KVM prennent en charge le japonais, le chinois simplifié et le chinois traditionnel. Ceci est disponible en mode autonome et via CC-SG.</td></tr>
</table>

Question	Réponse
Vos clients KVM prennent-ils en charge les écrans LCD doubles ?	Oui. Pour les clients qui souhaitent améliorer leur productivité en utilisant plusieurs écrans LCD sur leur bureau, Dominion KX III peut lancer des sessions KVM sur plusieurs écrans, en modes plein écran ou standard.
Prenez-vous en charge les serveurs dotés de cartes vidéo doubles ?	Oui, les cartes vidéo doubles sont prises en charge avec une configuration bureau étendue disponible pour l'utilisateur distant.

Support virtuel universel

Question	Réponse
Quels sont les modèles Dominion KX III qui prennent en charge les supports virtuels ?	Tous les modèles Dominion KX III prennent en charge les supports virtuels. Ils sont disponibles en mode autonome et via CommandCenter® Secure Gateway, la console de gestion centralisée de Raritan.
Quels types de supports virtuels Dominion KX III prend-il en charge ?	Dominion KX III prend en charge les types de média suivants: lecteurs CD/DVD internes et connectés USB, dispositifs de stockage de masse USB, lecteurs de disque dur PC et images ISO.

Question	Réponse
Quelles sont les conditions requises pour l'utilisation du support virtuel ?	Un CIM de support virtuel Dominion KX III est requis. Il y a deux CIM basé sur VGA: un D2CIM-VUSB ou D2CIM-DVUSB. D2CIM-VUSB est doté d'un connecteur USB simple et est destiné aux clients souhaitant utiliser le support virtuel au niveau du système d'exploitation. D2CIM-DVUSB est doté de connecteurs USB double et est destiné aux clients souhaitant utiliser le support virtuel au niveau du BIOS. D2CIM-DVUSB est également requis pour l'authentification par carte à puce, la mise en niveau/en cascade et l'audionumérique. Ces deux CIM prennent en charge des sessions de support virtuel sur les serveurs cible supportant l'interface USB 2.0. Disponibles en coffrets économiques de 32 et 64 CIM, ces CIM prennent en charge la synchronisation absolue de la souris Absolute Mouse Synchronization™, ainsi que la mise à jour du firmware à distance. A l'origine, nos CIM prenaient en charge la vidéo VGA analogique. Trois nouveaux CIM de support virtuel double prennent en charge les formats vidéo numérique, notamment DVI, HDMI et DisplayPort. Il s'agit de D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI et D2CIM-DVUSB-DP.
Le support virtuel est-il fiable ?	Oui. Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement 256 bits, 128 bits AES ou 128 bits RC4.
Les supports virtuels prennent-ils réellement en charge la fonction audio ?	Oui. La lecture et l'enregistrement audio sur un serveur connecté à Dominion KX III sont pris en charge. Vous pouvez écouter les sons provenant d'un serveur distant du centre de données à l'aide des haut-parleurs branchés sur votre PC ou ordinateur portable. Vous pouvez également effectuer des enregistrements sur le serveur distant à l'aide d'un microphone branché sur votre PC ou ordinateur portable. Un CIM numéro ou le CIM de support virtuel double D2CIM-DVUSB est requis.

Question	Réponse
Qu'est-ce qu'un profil USB ?	Certains serveurs requièrent une interface USB configurée de manière spécifique pour les services USB, tels que les supports virtuels. Le profil USB adapte l'interface USB de KX III au serveur pour prendre en compte les caractéristiques spécifiques de ce dernier.
En quoi un profil USB peut-il m'être utile ?	Les profils USB sont le plus souvent exigés au niveau du BIOS, où la spécification USB n'est peut-être pas totalement prise en charge lors de l'accès aux lecteurs de support virtuel. Toutefois, les profils sont parfois utilisés au niveau du système d'exploitation, par exemple, pour la synchronisation de la souris des serveurs Max et Linux.
Comment un profil USB est-il utilisé ?	Les ports peuvent être configurés individuellement ou par groupe par l'administrateur pour utiliser un profil USB spécifique sur la page de configuration des ports de KX III. Un profil USB peut également être sélectionné dans le client KX III en cas de besoin. Pour plus d'informations, consultez le manuel d'utilisation.
Dois-je systématiquement définir un profil USB si j'utilise la fonction Support virtuel ?	Non. Dans de nombreux cas, le profil USB par défaut est suffisant pour l'utilisation de la fonction Support virtuel au niveau du système d'exploitation, ou pour le fonctionnement au niveau du BIOS sans accès aux supports virtuels.
Quels profils sont disponibles ? Où puis-je trouver des informations supplémentaires ?	Reportez-vous au manuel d'utilisation pour obtenir les profils disponibles et pour plus d'informations.

Bande passante et performance KVM-sur-IP

Question	Réponse
Comment la bande passante est-elle utilisée dans les systèmes KVM sur IP ?	Dominion KX III offre un traitement vidéo tout à fait nouveau qui offre flexibilité, des vidéos haute performance, une utilisation efficace de la bande passante et un accès à tout moment/n'importe où via LAN, WAN ou Internet. Dominion KX III numérise compresse et crypte les signaux clavier, vidéo et souris de le serveur cible et transmet les paquets IP sur le réseau IP au client distant de la session à distance à l'utilisateur. KX III fournit une expérience au niveau du rack en fonction de ses algorithmes de traitement vidéo de pointe. Les changements d'écran, notamment vidéo, représentent la majorité de la bande passante utilisée ; l'activité du clavier et de la souris est considérablement réduite. Il est important de noter que la bande passante n'est employée que lorsque l'utilisateur est actif. La quantité de bande passante utilisée est basée sur le volume de changements se produisant à l'écran vidéo du serveur. S'il n'y a aucun changement fait à la vidéo - l'utilisateur n'intéragit pas avec le serveur - aucune ou une toute petite partie de la bande passant est utilisée. Si l'utilisateur déplace la souris ou tape un caractère, la quantité de bande passante utilisée est réduite. Si l'affichage exécute un écran de veille complexe ou lit une vidéo, la bande passante utilisée peut être plus conséquente.
Comment la bande passante affecte-t-elle les performances KVM sur IP ?	En général, il existe un compromis entre bande passante et performances. Plus la bande passante disponible est importante, plus les performances sont bonnes. Dans les environnements à bande passante réduite, les performances peuvent se dégrader. Dominion KX II a été optimisé pour fournir des performances solides dans une grande variété d'environnements.

Question	Réponse
Quels facteurs affectent la bande passante ?	De nombreux facteurs déterminent la quantité de bande passante utilisée. Le facteur principal, comme indiqué précédemment, est la quantité de changements se produisant dans l'affichage vidéo du serveur cible. Cela dépend des tâches et des actions de l'utilisateur. Parmi les autres facteurs figurent la résolution vidéo du serveur, la vitesse et les caractéristiques du réseau, les propriétés de connexion du Client KVM, les ressources du client PC et le bruit de la carte vidéo.
Quelle est la quantité de bande passante utilisée par KX II pour les tâches courantes ?	La bande passante dépend principalement des tâches et actions de l'utilisateur. Plus l'écran vidéo du serveur change, plus le débit de bande passante utilisée est important.

Question	Réponse
Comment puis-je optimiser la performance et la bande passante?	KX II offre divers paramètres dans vos clients distants pour permettre à l'utilisateur d'optimiser la bande passante et les performances. Les paramètres par défaut fournissent un niveau de performances sur le rack dans les environnements de réseau local/étendu avec une utilisation économique de la bande passante. **Optimisé pour.** Utiliser ce paramètre pour configurer le moteur vidéo pour des applications informations standard/ordinateurs ou pour des applications vidéo/de diffusion. **Compression.** Déplacez le curseur vers la gauche pour la qualité vidéo la plus haute possible et à droite pour une qualité de bande passante minimum. **Noise Filter (Filtre antiparasite).** Dans la plupart des cas, le paramètrage par défaut sera celui qui fonctionnera le mieux, cependant vous pouvez bouger vers la gauche pour une vidéo plus sensible et vers la droite pour moins de bande passante. Voici quelques autres astuces pour réduire la bande passante: ▪ Utilisez un papier peint uni pour le Bureau au lieu d'une image complexe. ▪ Désactivez les écrans de veille. ▪ Utilisez une résolution plus basse sur le serveur cible. ▪ Désactivez l'option Afficher le contenu des fenêtres pendant leur déplacement dans Windows. ▪ Utilisez des images, thèmes et bureaux simples (par exemple, Windows Classique).

Question	Réponse
Je souhaite me connecter via Internet. A quel type de performance dois-je m'attendre ?	Cela dépend de la bande passante et de la latence de la connexion Internet entre votre client distant et KX III. Avec une connexion par modem câble ou ADSL à haut débit, vos performances peuvent être très similaires à une connexion par réseau local/étendu. Pour les connexions plus lentes, utilisez les suggestions ci-dessus pour améliorer les performances.
Mon environnement dispose d'une bande passante à haut débit. Comment puis-je optimiser les performances ?	Le paramètre par défaut fonctionneront très bien. Vous pouvez déplacer les Propriétés de Connexion vers la gauche pour améliorer la performance vidéo.
Quelle est la résolution vidéo distante (sur IP) maximale prise en charge ?	Dominion KX II est le premier et le seul commutateur KVM-sur-IP à prendre en charge la résolution vidéo distante haute définition (HD) 1920 x 1080 avec une cadence de jusqu'à 30 images par seconde avec audio numérique. De plus, des formats grand écran courants sont pris en charge, comme 1600 x 1200, 1680 x 1050 et 1440 x 900, les utilisateurs distants peuvent donc travailler sur les écrans actuels à résolution supérieure.
Quelle quantité de bande passante est utilisée pour le son ?	Cela dépend du type de format audio utilisé, mais il faut environ 1,5 Mbps pour écouter du son de qualité CD.
Et pour les serveurs à ports DVI ?	Les serveurs à ports DVI prenant en charge DVI-A (analogique) et DVI-I (analogique et numérique intégrés) peuvent utiliser un adaptateur passif peu coûteux tel qu'ADVI-VGA de Raritan pour convertir le port DVI du serveur en prise VGA qui peut être connectée à la prise VGA d'un CIM de KX III. Les serveurs dotés de ports DVI prenant en charge DVI-I ou DVI-D (numérique) peuvent utiliser le nouveau CIM D2CIM-DVUSB-DVI.

Gestion de réseau IPv6

Question	Réponse
Qu'est-ce qu'IPv6 ?	IPv6 est l'acronyme d'Internet Protocol Version 6. IPv6 est le protocole IP « nouvelle génération » qui remplacera la version 4 (IPv4) actuelle du protocole IP. IPv6 règle un certain nombre de problèmes connus sous IPv4, tels que le nombre limité d'adresses IPv4. Il améliore également IPv4 dans des domaines, tels que le routage et la configuration automatique du réseau. IPv6 devra progressivement remplacer IPv4, bien que les deux coexisteront pendant quelques annés. IPv6 résout l'un des problèmes les plus épineux rencontrés par l'administrateur : la configuration et la gestion d'un réseau IP.
Pourquoi KX III 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 III ?	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 address que je souhaite utiliser avec mon dispositif ProductName ?	Le KX III peut accéder aux serveurs externes via leurs adresses IPv6 ; par exemple, un gestionnaire SNMP, un serveur Syslog ou un serveur LDAP. En utilisant l'architecture double pile de KX III, il est possible d'accéder à ces serveurs externes via: (1) une adresse IPv4, (2) une adresse IPv6 ou (3) un nom d'hôte. Donc, le KX III prend en charge l'environnement mixte IPv4/IPv6 dont de nombreux clients disposent.

Question	Réponse
Et si mon réseau ne prend pas en charge IPv6 ?	La gestion de réseau par défaut de KX III 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 III décrit la prise en charge de IPv6 par KX III.

Windows

Question	Réponse
Dominion KX II dépend-il d'un serveur Windows pour fonctionner ?	Absolument pas. Du fait que vous dépendez de votre infrastructure KVM pour être toujours disponible dans n'importe quelle situation de travail (et que vous devrez probablement utiliser cette infrastructure pour résoudre les éventuels problèmes), Dominion KX III est conçu pour être entièrement indépendant par rapport à tout serveur externe.
Que dois-je faire pour préparer la connexion d'un serveur à Dominion KX III ?	Réglez les paramètres souris de manière à fournir aux utilisateurs la meilleure synchronisation de souris et désactivez les écrans de veille et les fonctions de gestion d'alimentation qui affectent l'affichage de l'écran.
Et pour la synchronisation de la souris ?	Auparavant, la synchronisation de souris dans KVM sur IP était une expérience frustrante. La synchronisation absolue de la souris sur Dominion KX III offre une souris parfaitement synchronisée sans modification des paramètres de la souris sur des serveurs Windows et Mac Apple®. Pour d'autres serveurs, le mode Intelligent Mouse (souris intelligente) ou le mode de souris unique rapide évite la modification des paramètres de la souris du serveur.

Question	Réponse
Que contient le coffret Dominion KX III ?	Il comprend les éléments suivants : (1) l'unité Dominion KX III, (2) le guide de configuration rapide, (3) les pattes de fixation de montage en rack 19 pouces standard, (4) le CD-ROM du manuel d'utilisation, (6) un cordon de raccordement CA localisé et (7) un certificat de garantie et d'autres documents.

Serveurs lames

Question	Réponse
Puis-je connecter des serveurs lames à Dominion KX II ?	Oui. Dominion KX III prend en charge les modèles courants de serveurs lames des principaux fabricants : HP®, IBM®, Dell® et Cisco®.
Quels serveurs lames sont pris en charge ?	Les modèles suivants sont pris en charge : Dell PowerEdge® 1855, 1955 et M1000e; HP BladeSystem c3000 et c7000; IBM BladeCenter® H, E et S; et Cisco UCS B-Series.
Quel CIM dois-je utiliser ?	Tout dépend du type de ports KVM figurant sur la marque et le modèle spécifiques du serveur lame que vous utilisez. Les CIM suivants sont pris en charge : DCIM-PS2, DCIM-USBG2, D2CIM-VUSB et D2CIM-DVUSB.
Quels types d'accès et de contrôle sont disponibles ?	Dominion KX III fournit un accès KVM sécurisé et automatisé: (1) sur le rack, (2) à distance sur IP, (3) via le CommandCenter et (4) par modem.
Dois-je utiliser des raccourcis-clavier pour permuter entre les lames ?	Certains serveurs lames requièrent l'utilisation de raccourcis-clavier pour permuter entre les lames. Avec Dominion KX II, ces raccourcis-clavier sont inutiles. Il vous suffit de cliquer sur le nom du serveur lame pour que Dominion KX III passe automatiquement sur cette lame sans l'utilisation explicite du raccourci-clavier.
Puis-je accéder au module de gestion du serveur lame ?	Oui. Vous pouvez définir l'URL du module de gestion et y accéder depuis Dominion KX III ou depuis le CommandCenter Secure Gateway. S'il est configuré, l'accès en un clic est disponible.

Question	Réponse
Combien de serveurs lames puis-je connecter à Dominion KX III ?	Aux fins de performances et de fiabilité, vous pouvez connecter jusqu'à huit châssis de lames à un Dominion KX III, indépendamment du modèle. Raritan recommande de connecter jusqu'à deux fois le nombre de connexions à distance prises en charge par le dispositif. Par exemple, avec un KX3-216 doté de deux canaux à distance, nous vous recommandons de connecter jusqu'à quatre châssis de serveurs lames. Vous pouvez bien entendu connecter des serveurs individuels aux ports de serveur restants.
Je suis un client professionnel utilisant CommandCenter Secure Gateway. Puis-je accéder aux serveurs lames via CommandCenter Secure Gateway ?	Oui. Une fois les serveurs lames configurés sur Dominion KX III, l'utilisateur CommandCenter Secure Gateway peut y accéder via des connexions KVM. En outre, les serveurs lames sont organisés par châssis, ainsi que par vues personnalisées CommandCenter Secure Gateway.
Et si je souhaite également un accès KVM en bande ou intégré ?	L'accès en bande et intégré aux serveurs lames peut être configuré au sein de CommandCenter Secure Gateway.
J'exécute VMware® sur certains de mes serveurs lames. Est-ce pris en charge ?	Oui. Oui, avec CommandCenter Secure Gateway, vous pouvez afficher les machines virtuelles exécutées sur les serveurs lames, et y accéder.
Le support virtuel est-il pris en charge ?	Tout dépend du serveur lame. Les lames HP peuvent prendre en charge le support virtuel. S'il est configuré de manière appropriée, IBM BladeCenter (hormis BladeCenter T) prend en charge le support virtuel. Un CIM de support virtuel, D2CIM-VUSB ou D2CIM-DVUSB, doit être utilisé.
La synchronisation absolue de la souris est-elle prise en charge ?	Les serveurs disposant de commutateurs KVM internes dans un châssis à lame ne prennent habituellement pas en charge la technologie de souris absolue. Pour les lames HP et certains serveurs lames Dell, un CIM peut être connecté à chaque lame ; la synchronisation absolue de la souris est donc prise en charge.

Question	Réponse
L'accès aux lames est-il sécurisé ?	Oui. L'accès aux lames utilisent toutes les fonctions de sécurité standard de Dominion KX III, telles que le chiffrement 128 bits ou 256 bits. En outre, il existe des fonctions de sécurité spécifiques aux lames, telles que les autorisations d'accès par lame et le blocage des raccourcis-clavier qui interdit l'accès non autorisé.
Les dispositifs Dominion KSX II ou KX II-101 prennent-ils en charge les serveurs lames ?	Pour le moment, ces produits ne prennent pas en charge les serveurs lames.

Installation

Question	Réponse
Outre l'unité elle-même, que dois-je commander à Raritan pour installer Dominion KX III ?	Chaque serveur connecté à Dominion KX III requiert un module d'interface pour ordinateur (CIM) Dominion ou Paragon, et un adaptateur qui se branche directement sur les ports clavier, vidéo et souris du serveur.
Quel type de câble Cat5 dois-je utiliser pour mon installation ?	Dominion KX III peut utiliser n'importe quel câble UTP (paire torsadée non blindée) standard : Cat5, Cat5e ou Cat6. Dans nos manuels et brochures publicitaires, Raritan n'indique que câble « Cat5 ». En réalité, n'importe quel câble marqué UTP convient pour Dominion KX III.
Quels types de serveurs et PC peuvent être connectés à Dominion KX III ?	Dominion KX III est entièrement indépendant des fabricants. N'importe quel serveur avec ports clavier, vidéo et souris normalisés peut être connecté. En outre, les serveurs dotés de ports série peuvent être contrôlés à l'aide du CIM P2CIM-SER.
Comment connecter les serveurs à Dominion KX III ?	Les serveurs connectés à Dominion KX III requièrent un CIM Dominion ou Paragon qui se branche directement sur les ports clavier, écran et souris du serveur. Ensuite, connectez ensuite chaque CIM à Dominion KX III au moyen d'un câble UTP (paire torsadée blindée) standard : Cat5, Cat5e ou Cat6.

Question	Réponse
Quelle est la distance maximale autorisée entre mes serveurs et Dominion KX III ?	En général les serveurs peuvent être distants de 45 mètres au maximum de Dominion KX III, suivant leur type. (Consultez ***Taux de rafraîchissement et distances de connexion au serveur cible supportés*** (voir "***Distance de connexion, taux de rafraîchissement et résolution vidéo du serveur cible pris en charge***" à la page 335)) Pour le CIM D2CIM-VUSB qui prend en charge les fonctions Support virtuel et Synchronisation absolue de la souris, une distance de 30 m est recommandée.
Certains systèmes d'exploitation se bloquent lorsque je déconnecte un clavier ou une souris pendant le fonctionnement. Que faut-il faire pour éviter aux serveurs connectés à Dominion KX III de se bloquer lorsque je m'en déconnecte ?	Chaque clé électronique de module d'interface pour ordinateur Dominion (DCIM) se comporte comme un clavier et une souris virtuels vis-à-vis du serveur auquel elle est connectée. Cette technologie est appelée KME (émulation clavier/souris). La technologie KME de Raritan est adaptée aux centres de données, testée contre les éventuelles attaques et d'une fiabilité nettement supérieure à celle des commutateurs KVM bas de gamme : elle incorpore plus de 15 ans d'expérience et a été déployée sur des millions de serveurs dans le monde.
Ne faut-il pas installer des agents sur les serveurs connectés à Dominion KX III ?	Dominion KX III étant directement connecté par voie matérielle aux ports clavier, vidéo et souris des serveurs, les serveurs connectés à Dominion KX III ne nécessitent l'installation d'aucun agent logiciel.
Combien de serveurs peuvent être connectés à chaque unité Dominion KX III ?	Les modèles Dominion KX III offrent 8, 16 ou 32 ports serveurs dans un châssis 1U, et jusqu'à 64 dans un châssis 2U. C'est le commutateur KVM numérique offrant la densité de ports la plus élevée de l'industrie.
Que se passe-t-il si je déconnecte un serveur de Dominion KX III pour le reconnecter à une autre unité Dominion KX III ou à un autre port sur la même unité Dominion KX III ?	Dominion KX III met automatiquement à jour les noms de ports de serveurs lorsque les serveurs sont déplacés d'un port à l'autre. De plus, cette mise à jour automatique n'affecte pas seulement le port d'accès local, mais également tous les clients distants et l'appareil de gestion CommandCenter Secure Gateway en option.

Question	Réponse
Comment dois-je connecter un dispositif contrôlé en série (RS-232), tel qu'un routeur/commutateur Cisco ou un serveur Sun headless, à Dominion KX III ?	Si le nombre de dispositifs contrôlés en série est réduit, ils peuvent être connectés à Dominion KX III via le convertisseur série P2CIM-SER de Raritan. Les clients peuvent également envisager le déploiement de Dominion KSX II, commutateur KVM et série intégré. DKSX-144 offre quatre ports KVM sur IP et quatre ports série. DKSX-188 offre huit ports KVM sur IP et huit ports série. Toutefois, si vous disposez de nombreux dispositifs contrôlés en série, nous vous recommandons d'utiliser la gamme Dominion SX de Raritan des serveurs de console sécurisée. Dominion SX offre plus de fonctionnalité en série à un meilleur prix que Dominion KX III. SX est simple à utiliser, à configurer et à gérer, et peut être entièrement intégré au déploiement d'une série Dominion.

Port Local - KX III

Question	Réponse
Est-il possible d'accéder à mes serveurs directement depuis le rack ?	Oui. Les fonctions sur rack de Dominion KX III se comportent comme un commutateur KVM traditionnel, vous permettant de contrôler jusqu'à 64 serveurs au moyen de clavier, écran et souris uniques. Vous pouvez basculer d'un serveur à l'autre via l'interface utilisateur basée navigateur ou un raccourci-clavier.
Puis-je regrouper les ports locaux de plusieurs unités KX III ?	Oui. Vous pouvez connecter les ports locaux de plusieurs commutateurs KX III à un autre KX III en utilisant la fonction « multiniveau » du KX III. Vous pouvez alors accéder aux serveurs connectés à vos dispositifs KX II d'un point unique du centre de données via une liste de regroupement de ports.
L'accès à distance aux serveurs d'autres utilisateurs est-il bloqué lorsque j'utilise le port local ?	Non. Le port local de Dominion KX III dispose d’un chemin d’accès aux serveurs entièrement indépendant. Cela signifie qu’un utilisateur peut accéder localement aux serveurs sur le rack, sans affecter le nombre d’utilisateurs qui accèdent simultanément au rack à distance.

Question	Réponse
Est-il possible d'utiliser un clavier ou une souris USB sur le port local ?	Oui. Dominion KX III est doté de ports clavier et souris USB sur le port local. Les commutateurs Dominion KX III n'ont pas de ports locaux PS/2. Les clients possédant des claviers et souris PS/2 doivent utiliser un adaptateur PS/2-USB.
Existe-t-il un affichage à l'écran pour l'accès local sur le rack ?	Oui, mais les performances d'accès sur le rack de Dominion KX III sont largement supérieures aux affichages écran classiques. Doté de l'interface navigateur la plus aboutie de l'industrie en matière d'accès sur le rack, le port local de Dominion KX III utilise la même interface pour l'accès local et l'accès distant. Par ailleurs, la plupart des fonctions d'administration sont disponibles sur le rack.
Comment sélectionner les serveurs tout en utilisant le port local ?	Le port local affiche les serveurs connectés à l'aide de la même interface utilisateur que celle du client distant. Les utilisateurs se connectent à un serveur d'un simple clic de la souris ou via un raccourci-clavier.
Comment s'assurer que seuls les utilisateurs autorisés peuvent accéder aux serveurs depuis le port local ?	Les utilisateurs essayant d'utiliser le port local doivent subir le même niveau d'authentification que les utilisateurs à distance. En d'autres termes : Si Dominion KX III est configuré pour interagir avec un serveur RADIUS, LDAP ou Active Directory® externe, les utilisateurs essayant d'accéder au port local seront authentifiés par le même serveur. Si les serveurs d'authentification externes ne sont pas disponibles, Dominion KX III bascule sur sa base de données d'authentification interne. Dominion KX III possède sa propre authentification autonome, offrant une installation instantanée, prête à l'emploi.

Port local étendu

Question	Réponse
Qu'est-ce que le port local étendu ?	Dominion KX2-808, KX2-832 et KX2-864 comportent un port local étendu. Les modèles Dominion KX III correspondants n'ont pas de port local étendu. A la place, tous les modèles KX III ont un port multiniveau. Pour étendre le port digital local KX III, vous pouvez utiliser le produit Raritan Cat5 Reach DVI pour un accès local et distant à plus de 500 mètres. Consultez ***Connecter un DVI Cat5 Reach et KX III - fournit une fonctionnalité de port local étendue*** (à la page 310)

Double alimentation

Question	Réponse
Dominion KX III propose-t-il l'option de double alimentation ?	Oui. Tous les modèles Dominion KX III sont équipés d'arrivées et d'alimentations CA en double avec basculement automatique. En cas de défaillance au niveau d'une arrivée électrique ou de l'alimentation électrique, KX III commute automatiquement sur l'autre système.
Les paramètres de tension sont-ils automatiquement détectés par l'alimentation de Dominion KX III ?	Oui. L'alimentation de Dominion KX III peut être utilisée sur une tension alternative comprise entre 100 et 240 volts, de 50 à 60 Hz.
Suis-je informé en cas de coupure de courant ou de défaillance au niveau d'une arrivée électrique ?	Le voyant DEL situé sur le panneau avant de Dominion KX II permet d'avertir l'utilisateur d'une panne de courant. Une entrée est également envoyée dans le journal d'audit et affichée dans l'interface utilisateur du client distant de KX II. Des événements SNMP ou Syslog sont également générés, si les options correspondantes ont été configurées par l'administrateur.

Contrôle des unités de distribution d'alimentation (PDU)

Question	Réponse
Quel type de fonctions de gestion de l'alimentation à distance Dominion KX III offre-t-il ?	Les PDU intelligentes de Raritan peuvent être connectées à Dominion KX III pour permettre la gestion de l'alimentation des serveurs cible et d'autres équipements. Pour les serveurs, après une simple opération de configuration unique, il vous suffit de cliquer sur le nom du serveur pour mettre sous ou hors tension un serveur bloqué ou en effectuer l'alimentation cyclique.
Quelles sont les barrettes d'alimentation prises en charge par Dominion KX III ?	Les barrettes d'alimentation Dominion PX™ et Remote Power Control (RPC) de Raritan. Elles sont livrées avec de nombreuses variations de prises, connecteurs et tensions. Notez que vous ne devez pas connecter des barrettes d'alimentation de la série PM à Dominion KX III car elles ne permettent pas la commutation au niveau des prises.
Combien de PDU peuvent être connectées à chaque unité Dominion KX III ?	Vous pouvez connecter jusqu'à huit PDU à un dispositif Dominion KX III.
Comment puis-je connecter la PDU à Dominion KX III ?	D2CIM-PWR est utilisé pour connecter la barette d'alimentation à Dominion KX III. D2CIM-PWR est vendu séparément ; il n'est pas fourni avec la PDU.
Dominion KX III prend-il en charge les serveurs à alimentations multiples ?	Oui. Dominion KX III peut être facilement configuré pour prendre en charge des serveurs à alimentations multiples branchés sur plusieurs barrettes d'alimentation. Quatre alimentations peuvent être connectées par serveur cible.
Dominion KX III affiche-t-il des statistiques et des mesures provenant de la PDU ?	Oui. Les statistiques d'alimentation au niveau de la PDU, comprenant l'alimentation, le courant et la tension, sont extraites de la PDU et affichées pour l'utilisateur.
La gestion de l'alimentation à distance nécessite-t-elle une configuration spéciale des serveurs reliés ?	Certains serveurs sont livrés avec des paramètres BIOS par défaut qui rendent impossible le redémarrage automatique du serveur après une coupure de l'alimentation et son rétablissement. Consultez la documentation du serveur pour modifier ce paramètre.

Question	Réponse
Que se passe-t-il lorsque j'effectue l'alimentation cyclique d'un serveur ?	Notez que ceci équivaut physiquement à débrancher le serveur de la prise de courant, puis à le rebrancher.

Ethernet et mise en réseau IP

Question	Réponse
Quelle est la vitesse des interfaces Ethernet de Dominion KX III ?	Dominion KX III prend en charge Gigabit et 10/100 Ethernet. KX III prend en charge deux interfaces Ethernet de vitesse 10/100/1000, avec possibilité de configurer la vitesse et les paramètres duplex (détectés automatiquement ou définis manuellement).
Est-il possible d'accéder à Dominion KX III via une connexion sans fil ?	Oui. Dominion KX III n'utilise pas seulement l'interface Ethernet standard, mais également une bande passante très classique de très haute qualité vidéo. Par conséquent, si vous disposez d'un client sans fil équipé d'une connectivité réseau à Dominion KX III, vous pouvez configurer et gérer vos serveurs au niveau du BIOS sans fil.
Dominion KX III offre-t-il des ports Ethernet doubles d'un gigabit pour fournir une fonction de protection par basculement redondante ou un équilibrage des charges ?	Oui. Dominion KX III comporte des ports Ethernet doubles d'un gigabit pour permettre la protection par basculement redondante. En cas de panne du port Ethernet primaire (ou du commutateur/routeur auquel il est connecté), Dominion KX III bascule sur le port réseau secondaire avec la même adresse IP, empêchant ainsi toute interruption de fonctionnement de votre serveur. Notez que la protection par basculement automatique doit être activée par l'administrateur.
Est-il possible d'utiliser Dominion KX III sur un réseau VPN ?	Oui. Dominion KX III utilise les technologies IP (protocole Internet) standards de la couche 1 à 4. L'encombrement peut être facilement canalisé via des réseaux VPN standard.
Puis-je utiliser KX III avec un serveur proxy ?	Oui. KX III peut être utilisé avec un serveur proxy SOCKS, à condition que le PC client distant soit configuré correctement. Consultez la documentation de l'utilisateur ou l'aide en ligne pour en savoir plus.

Question	Réponse
Combien de ports TCP doivent être activés sur mon pare-feu pour autoriser l'accès réseau à Dominion KX III ?	Deux ports sont requis : un port 5000 TCP pour détecter d'autres dispositifs Dominion, et pour la communication entre les dispositifs Raritan et CC-SG ; et, bien entendu, le port 443 pour la communication HTTPS.
Ces ports sont-ils configurables ?	Oui. Les ports TCP de Dominion KX III sont configurables par l'administrateur.
Dominion KX III peut-il être utilisé avec CITRIX ?	Dominion KX III peut fonctionner avec des produits d'accès à distance tels que Citrix si la configuration est effectuée correctement. Raritan ne peut cependant pas garantir que les performances de fonctionnement soient acceptables. Les clients doivent se rendre compte que les produits tels que Citrix utilisent des technologies de réacheminement vidéo dont le concept est similaire à celui des commutateurs KVM, si bien que deux technologies KVM sur IP sont utilisées simultanément.
Dominion KX III peut-il utiliser l'adressage DHCP ?	L'adressage DHCP peut être utilisé, mais Raritan recommande l'utilisation d'un adressage fixe. En effet, Dominion KX III est un dispositif d'infrastructure et l'accès et l'administration sont réalisés plus efficacement au moyen d'une adresse IP fixe.

Question	Réponse
J’ai des problèmes pour me connecter à Dominion KX III via mon réseau IP. Quel pourrait être le problème ?	Dominion KX III s’appuie sur votre réseau local/Internet. Les éventuels problèmes incluent : Négociation automatique d'Ethernet. Sur certains réseaux, la négociation automatique 10/100 ne fonctionne pas correctement et l'unité Dominion KX III doit alors être réglée sur 100 Mb/full duplex ou sur l'option adaptée au réseau. Doublon au niveau des adresses IP. Si l'adresse IP de Dominion KX III est la même que celle d'un autre dispositif, il est possible que la connectivité du réseau ne soit pas fiable. Conflits au niveau du port 5000. Si un autre dispositif utilise le port 5000, le port par défaut de Dominion KX III (ou le port de l'autre dispositif) doit être modifié. Lors de la modification de l'adresse IP de Dominion KX III ou du passage à une nouvelle unité KX III, vous devez attendre suffisamment longtemps pour que ses adresses IP et Mac® soient reconnues par les réseaux des couches 2 et 3.

Groupement, fonction multiniveau et mise en cascade des ports locaux

Question	Réponse
Comment puis-je connecter physiquement plusieurs dispositifs Dominion KX III entre eux pour disposer d'une solution unique ?	Connecter physiquement plusieurs dispositifs KX III entre eux pour un accès local consolidé, vous pouvez connecter les ports locaux de plusieurs commutateurs KX III à un autre KX III en utilisant la fonction « multiniveau » du KX III. Vous pouvez alors accéder aux serveurs connectés à vos dispositifs KX III d'un point unique du centre de données via une liste de regroupement de ports. Le port multiniveau doit être utilisé pour relier le commutateur KX III en niveau au commutateur de base. L'accès via une liste de port consolidée est disponible dans le centre de données ou même depuis un PC distant. Tous les serveurs connectés aux KX II en niveau sont accessibles via une liste hiérarchisée de ports ou via une recherche (avec caractères joker). Deux niveaux sont pris en charge ; 1024 dispositifs au plus sont accessibles dans une configuration multiniveau. La gestion de l'alimentation à distance est également prise en charge. L'accès multiniveau aux supports virtuels, aux cartes à puce et aux serveurs lames sera pris en charge dans une prochaine version. Ces fonctions sont évidemment accessibles via une connexion distante standard. Même si l'accès au serveur IP distant via la liste de regroupement de ports est disponible pour des raisons de commodité, l'accès à distance au serveur en niveau depuis CommandCenter, ou via l'unité KX III à laquelle le serveur est connecté, est recommandé pour des performances optimales.

Question	Réponse
Dois-je connecter physiquement les dispositifs Dominion KX III entre eux ?	Les unités multiples Dominion KX III ne nécessitent aucune interconnexion physique. En effet, toutes les unités Dominion KX III sont connectées au réseau et fonctionnent automatiquement comme une solution unique lorsqu'elles sont déployées avec l'appareil de gestion CommandCenter Secure Gateway (CC-SG) de Raritan. CC-SG sert de point d'accès et de gestion à distance unique. CC-SG offre tout un ensemble d'outils pratiques, tels que le regroupement de la configuration et de la mise à jour des firmware, ainsi qu'une base de données d'authentification et d'autorisation unique. Les clients qui utilisent CC-SG pour un accès distant centralisé peuvent profiter de la fonction multiniveau (cascade) de KX III pour regrouper les ports locaux de plusieurs commutateurs KX III et accéder à 1024 serveurs au plus à partir d'une console unique dans le centre de données.
CC-SG est-il requis ?	Pour les clients souhaitant un usage autonome (sans système central de gestion), plusieurs unités Dominion KX III interagissent encore et se mettent en corrélation via le réseau IP. Plusieurs commutateurs Dominion KX III sont accessibles depuis l'interface utilisateur basé Web.

Question	Réponse
Est-il possible de connecter un commutateur analogique KVM existant à Dominion KX III ?	Oui. Les commutateurs KVM analogiques peuvent être connectés à l'un des ports de serveur de Dominion KX III. Il vous suffit d'utiliser un module d'interface USB pour ordinateur (CIM), et de le connecter aux ports utilisateur du commutateur KVM analogique existant. Les commuteurs KVM analogiques prenant en charge la commutation par raccourci-clavier sur leurs ports locaux peuvent être mis en niveau sur un commutateur Dominion KX III et commutés via une liste de regroupement de ports, à distance et dans le centre de données. Notez que les caractéristiques des commutateurs KVM varient, et que Raritan ne peut pas garantir l'interopérabilité d'un commutateur KVM analogique tiers particulier. Contactez le support technique Raritan pour obtenir de plus amples informations.

Modules d'interface pour ordinateur (CIM)

Question	Réponse
Quel type de vidéo vos CIM prennent-ils en charge ?	A l'origine, nos CIM prenaient en charge la vidéo VGA analogique. Trois nouveaux CIM prennent en charge les formats de vidéo numérique, notamment DVI, HDMI et DisplayPort. Il s'agit de D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI et D2CIM-DVUSB-DP.

Question	Réponse
Est-il possible d'utiliser des modules d'interface pour ordinateur (CIM) venant du commutateur analogique matriciel KVM de Raritan Paragon avec Dominion KX III ?	Oui. Il est possible que certains modules d''interfaces Paragon (CIM) fonctionnent avec Dominion KX III. (Veuillez consultez les Remarques sur la Version Raritan Dominion KX III sur le site web pour obtenir la dernière list de CIM certifiées.) Néanmoins, du fait que les CIM Paragon coûtent plus cher que les CIM Dominion KX III (du fait qu'elles incorporent des technologie de vidéo transmission jusqu'à 304m), il n'est pas conseillé d'acheter des CIM Paragon pour une utilisation avec Dominion KX III. Notez également que lorsque les CIM Paragon sont connectés à Dominion KX II, leur transmission vidéo est limitée à 15 mètres, égalant les performances de transmission des modules Dominion KX II, et n'est plus de 304 mètres comme lorsqu'ils sont connectés à Paragon.
Dominion KX III prend-il en charge les CIM doubles Paragon ?	Oui. Dominion KX III prend maintenant en charge les CIM doubles Paragon II (P2CIM-APS2DUAL et P2CIM-AUSBDUAL) qui peuvent connecter des serveurs du centre de données à deux commutateurs Dominion KX III différents. Lorsqu'un commutateur KX III n'est pas disponible, le serveur est accessible au moyen du second commutateur KX III, ce qui offre un accès redondant et double le niveau de l'accès KVM à distance. Notez qu'il s'agit de CIM Paragon, ils ne prennent donc pas en charge les fonctions avancées de KX III telles que le support virtuel, la souris absolue, etc.

Sécurité

Question	Réponse
Dominion KX III est-il certifié FIPS 140-2 ?	Dominion KX III utilise un module cryptographique validé FIPS 140-2 s'exécutant sur une plate-forme Linux selon les directives de mise en œuvre de FIPS 140-2. Ce module cryptographique sert au cryptage du trafic de session KVM constitué de données vidéo, de clavier, de souris, de support virtuel et de carte à puce.
Quel type de chiffrement est utilisé par Dominion KX III ?	Dominion KX III utilise un système de chiffrement AES à 256 bits, AES à 128 bits ou 128 bits standard (et extrêmement sûr) pour ses communications SSL et son propre flux de données. Littéralement aucune donnée n'est transmise entre les clients distants et Dominion KX III si elle n'est pas chiffrée et complètement sécurisée.
Dominion KX III prend-il en charge le chiffrement AES comme recommandé par les normes NIST et FIPS du gouvernement américain ?	Oui. Dominion KX III utilise le chiffrement AES (Advanced Encryption Standard) pour une sécurité accrue. Le chiffrement AES 256-bits et 128-bits est disponible. L'AES est un algorithme de chiffrement approuvé par le gouvernement américain et recommandé par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) dans la norme FIPS 197.
Le dispositif Dominion KX II permet-il le cryptage de données vidéo ? Ou effectue-t-il uniquement le chiffrement des données de clavier et de souris ?	Contrairement aux solutions concurrentes qui ne chiffrent que les données de clavier et de souris, Dominion KX III ne met pas votre sécurité en danger- il permet de chiffrer les données de clavier, souris, vidéo et support virtuel.
Comment Dominion KX III intègre-t-il les serveurs d'authentification externes tels qu'Active Directory, RADIUS ou LDAP ?	Grâce à une configuration très simple, il est possible de programmer Dominion KX III pour renvoyer toutes les demandes d'authentification vers un serveur externe tel que LDAP, Active Directory ou RADIUS. Pour chaque utilisateur authentifié, le serveur d'authentification transmet à Dominion KX III le groupe d'utilisateurs auquel appartient l'utilisateur concerné. Dominion KX III détermine ensuite les autorisations d'accès de l'utilisateur en fonction du groupe auquel il appartient.

Question	Réponse
Comment sont stockés les noms d'utilisateur et mots de passe ?	En cas d'utilisation des fonctions d'authentification interne de Dominion KX III, toutes les informations critiques telles que les noms d'utilisateur et mots de passe sont stockées sous une forme chiffrée. Personne, y compris l'assistance technique ou les services d'ingénierie de produit Raritan, ne peut récupérer ces noms d'utilisateur et mots de passe.
Dominion KX III prend-il en charge les mots de passe forts ?	Oui. Dominion KX III dispose de la fonction de vérification stricte du mot de passe, configurable par l'administrateur, afin de garantir que les mots de passe créés par les utilisateurs répondent aux normes gouvernementales et/ou d'entreprise et résistent au piratage de force.
Est-il possible de téléverser son propre certificat numérique sur Dominion KX III ?	Oui. Les clients peuvent téléverser des certificats auto-signés ou numériques fournis par une autorité de certification sur Dominion KX III pour une authentification améliorée et des communications sécurisées.
KX III prend-il en charge une bannière de sécurité configurable ?	Oui. Pour le gouvernement, les forces armées et autres clients requérant un message de sécurité avant l'ouverture de session de l'utilisateur, KX III peut afficher un message de bannière configurable par l'utilisateur et éventuellement demander une acceptation.
Ma stratégie de sécurité ne permet pas l'utilisation de numéros de port TCP standard. Est-il possible de les modifier ?	Oui. Pour les clients souhaitant éviter les numéros de port TCP/IP standard pour augmenter la sécurité, Dominion KX III permet à l'administrateur de configurer d'autres numéros de port.

Authentification par cartes à puce et CAC

Question	Réponse
Dominion KX III prend-il en charge l'authentification par cartes à puce et CAC ?	Oui. L'authentification par cartes à puce et DoD Common Access Card (CAC) sur les serveurs cible est prise en charge.

Question	Réponse
Qu'est-ce que CAC ?	Suivant la directive présidentielle relative à la sécurité intérieure 12 (HSPD-12), CAC est un type de carte à puce créée par le gouvernement américain et utilisé par les personnels militaires et gouvernementaux américains. Il s'agit d'une carte multitechnologie, polyvalente dont le but est de disposer d'une carte d'identification unique. Pour plus d'informations, reportez-vous aux normes FIPS 201.
Quels modèles de KX III prennent en charge les cartes à puce/CAC ?	Tous les modèles de Dominion KX III les prennent en charge. Les modèles Dominion KX III-101 ne prennent actuellement pas en charge les cartes à puce et CAC.
Les clients entreprise et SMB utilisent-ils également des cartes à puce ?	Oui. Cependant, le déploiement le plus agressif de cartes à puce est effectué par le gouvernement fédéral des Etats-Unis.
Quels CIM prennent en charge les cartes à puce/CAC ?	D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI et D2CIM-DVUSB-DP représentent les CIM requis.
Quels lecteurs de cartes à puce sont pris en charge ?	Les normes de lecteur requises sont CCID USB et PC/SC. Consultez la documentation pour obtenir la liste des lecteurs agréés et des informations supplémentaires.
L'authentification par carte à puce/CAC fonctionne-t-elle sur le port local et via CommandCenter ?	Oui. L'authentification par carte à puce/CAC fonctionne sur le port local et via CommandCenter. Pour le port local, connectez un lecteur de cartes à puce compatible au port USB de Dominion KX III.

Capacités de gestion

Question	Réponse
Est-il possible de gérer et de configurer à distance Dominion KX III via un navigateur Web ?	Oui. Dominion KX III peut être entièrement configuré à distance via un navigateur Web. Pour cela, votre poste de travail doit disposer d'une version de Java Runtime Environment (JRE) appropriée. Il est possible de configurer entièrement la solution sur le réseau à l'exception du paramètre initial de l'adresse IP de Dominion KX III. (En fait, vous pouvez même configurer les paramètres initiaux au moyen d'un câble Ethernet croisé et de l'adresse IP par défaut de Dominion KX III via un navigateur Web.)
Est-il possible de sauvegarder et de restaurer la configuration de Dominion KX III ?	Oui. Il est possible de sauvegarder entièrement les configurations de l'utilisateur et du dispositif Dominion KX III pour une restauration ultérieure en cas de catastrophe. La fonction de sauvegarde et de restauration de Dominion KX III peut être utilisée à distance sur le réseau ou via un navigateur Web.
Quels sont les journaux d'audit et enregistrements offerts par Dominion KX III ?	Pour une responsabilité optimale, Dominion KX III enregistre tous les événements utilisateur principaux avec datage et marque horaire. Par exemple, les événements rapportés comprennent (liste non exhaustive) : xonnexion de l'utilisateur, déconnexion de l'utilisateur, accès utilisateur à un serveur particulier, échec de connexion, modifications de configuration, etc.
Est-il possible d'intégrer Dominion KX III au serveur Syslog ?	Oui. Dominion KX III peut également, en plus de ses propres fonctions de consignation interne, envoyer tous les événements enregistrés à un serveur Syslog centralisé.
Est-il possible d'intégrer Dominion KX III avec SNMP ?	Oui. Dominion KX III peut également, en plus de ses propres fonctions de consignation interne, envoyer des traps SNMP aux systèmes de gestion SNMP. SNMP v2 et v3 sont pris en charge.
Un administrateur peut-il fermer la session d'un utilisateur ?	Oui, les administrateurs peuvent vérifier à quel port un utilisateur est connecté, et le déconnecter au besoin d'un port spécifique ou du dispositif.

Question	Réponse
Est-il possible de synchroniser l'horloge interne de Dominion KX III avec un serveur de temps ?	Oui. Dominion KX III prend en charge le protocole NTP standard pour se synchroniser avec le serveur de temps de votre entreprise ou avec n'importe quel serveur de temps public (en partant du principe que le pare-feu de votre entreprise autorise les demandes NTP sortantes).

Documentation et assistance

Question	Réponse
Existe-t-il une aide en ligne ?	Oui. L'aide en ligne est disponible sur raritan.com avec la documentation et depuis l'interface utilisateur de KX II. L'Aide en ligne inclut des informations sur l'administration et l'utilisation final de KX III lors de l'utilisation de la Console distante, du Virtual KVM Client (VKC), du Active KVM Client (AKC) et de la Console locale, ainsi que des spécifications sur KX III, des remarques informatives, sur l'utilisation de KX III avec Paragon II, la connexion de KX III à Car5 Reach DVI, la connexion de KX III à T1700-LED, etc.
Comment puis-je trouver de la documentation sur Dominion KX III?	La documentation est disponible sur raritan.com. Elle est classée par version de firmware.
Quelle documentation est disponible ?	Un guide de configuration rapide, une version PDF de l'aide sous la forme d'un guide d'administrateur et d'un guide d'utilisateur est disponible, ainsi que des notes de version et d'autres informations sont disponibles.
Quel CIM dois-je utiliser avec un serveur particulier ?	Consultez le manuel sur les CIM fourni avec la documentation KX III. Notez que les normes vidéo DVI, HDMI et DisplayPort sont prises en charge avec les nouveaux CIM vidéo numériques.
Quelle est la durée de la garantie de KX III ?	Dominion KX II est fourni avec une garantie standard de deux ans, qui peut être prolongée à 5 ans.

Divers

Question	Réponse
Quelle est l'adresse IP par défaut de Dominion KX III ?	192.168.0.192
Quels sont le nom d'utilisateur et le mot de passe par défaut de Dominion KX III ?	Le nom d'utilisateur et le mot de passe par défaut de Dominion KX II sont admin/raritan (tout en minuscules). Cependant, pour offrir le niveau de sécurité le plus élevé, Dominion KX III force l'administrateur à changer le nom d'utilisateur et le mot de passe administratifs par défaut de Dominion KX III lorsque l'unité est lancée pour la première fois.
J'ai changé et oublié mon mot de passe administratif de Dominion KX II, vous est-il possible de le récupérer pour moi?	Dominion KX III comporte une fonction de réinitialisation matérielle qui peut être utilisée pour réinitialiser les paramètres par défaut du dispositif et rétablir par la même occasion le mot de passe administratif par défaut.
Comment dois-je procéder pour migrer de Dominion KX II à Dominion KX III ?	De manière générale, les utilisateurs de KX II peuvent continuer à utiliser leurs commutateurs existants pendant de nombreuses années. À mesure que leurs centres de données se développent, les clients peuvent acheter et utiliser les nouveaux modèles KX III. La console de gestion centralisée de Raritan, le CommandCenter Secure Gateway (CC-SG) version 6.0 prend en charge les commutateurs KX II et KX III sans différence.
Mes CIM KX II existants vont-ils fonctionner avec les commutateurs Dominion KX III ?	Oui. Les CIM KX II existants fonctionnent avec le commutateur Dominion KX III. De plus, sélectionnez les CIM Paragon fonctionnera avec le KX III. Cela permet aux utilisateurs de Paragaon I désireux de passer à KVM sur IP d'effectuer la migration en toute facilité vers KX II. Toutefois, vous pouvez également utiliser les CIM D2CIM-VUSB et D2CIM-DVUSB qui prennent en charge le support virtuel et la synchronisation absolue de la souris. En outre, des CIM vidéo numériques prenant en charge DVI, HDMI et DisplayPort sont également disponibles.

Index

A

A Alimentation CA - 34
A partir d'Active Directory (AD) de Microsoft - 232
Accèder à un châssis de lames à partir d'un dispositif de base - 140
Accèder à un Paragon II depuis le KX III - 314
Accent (clients avec système d'exploitation Windows XPR seulement) - 368
Accès à distance - 379
Accès à KX III à l'aide de la CLI - 213
Accès à la page de Configuration des ports - 90
Accès à un disque média virtuel sur un Ordinateur Client - 274
Accès à un serveur cible - 296
Accès à un serveur cible depuis KX III - 43
Accès à Virtual Media sur Windows 2000 - 363
Accès direct aux ports et groupes de deux ports vidéo - 231
Accès et gestion des serveurs cible à distance - 43
Accès local et à distance d'appareil multiniveau - 140
Accès par carte à puce à la console locale - 279, 306
Accès SSH depuis un PC Windows - 214
Accès SSH depuis un poste de travail UNIX/Linux - 214
Activation de FIPS 140-2 - 177, 179
Activation de la fonction multiniveau - 137, 139
Activation de la validation du certificat du serveur de téléchargement AKC - 144
Activation de SSH - 134
Activation d'un accès direct aux ports via URL - 141
Activer la fonction multiniveau sur le dispositif du port local - 129, 137
Activer la validation du certificat du serveur de téléchargement AKC - 295
Activer l'accès direct aux ports. - 143
Activer le Port Local standard - 129
Actualisation de l'écran - 253
Administration des commandes de configuration du serveur de console de KX III - 219
Affichage de la liste des utilisateurs de KX III - 68
Affichage des utilisateurs par port - 68, 69
Affichage du MIB de Productname - 146, 149, 155
Aide Active pour Client KVM (AKC) - 8, 292, 381
Aide en ligne KX II - 8
Aide pour la sélection des profils USB - 364
Aide pour l'administrateur de KX III - 27
Aide Virtuelle pour Client KVM (VKC) - 8, 240, 292, 381
Ajout d'attributs à la classe - 234
Ajout de scripts - 160
Ajout d'un nouveau groupe d'utilisateurs - 59
Ajout d'un nouvel utilisateur - 67, 70
Ajouter des dispositifs KX III à dcTrack - 324
Ajouter manuellement un KX III à dcTrack - 324
Ajouter ou retirer un KX III du site - 329
Ajustement de la taille de la mémoire-tampon de capture et de lecture (Paramètres audio) - 290
Ajuster les Paramètres Audio - 290
Allumez ou éteignez un KX III - 329
Appellation des PDU de rack (page Port pour les barrettes d'alimentation) - 98
Application et retrait des scripts - 160, 163
Applications Client KVM pour KX III - 8
Arrêt de la gestion par CC-SG - 200
Assigner une adresse IP au KX III - 37
Association de prises à des serveurs cible - 100
Astuces pour ajouter une interface Navigateur Web - 106, 109, 111, 113, 115, 359
Audio - 283, 372
Audio dans un environnement Linux - 372
Audio dans un environnement Mac - 347
Audio dans un environnement Windows - 373
Audionumérique - 283
Authentication lors de l'accès à un lecteur de carte à puces - 280
Authentification par cartes à puce et CAC - 407
Autorisations et accès aux groupes de deux ports vidéo - 168, 225
Autorise les pop-ups : - 9
Autoriser les cookies - 294

Auto-Sense Video Settings (Détection automatique des paramètres vidéo) - 253
Avant de créer une configuration multiniveau - 137
Avertissement d'accès et Validation de Java - 9
Avertissements de Sécurité Supplémentaires - 9, 10

B

B Port réseau - 35
Backup and Restore (Sauvegarde et restauration) - 117, 165, 192
Balayage de Cibles - Console locale - 305
Balayage des ports - Console locale - 301
Bande passante et performance KVM-sur-IP - 384
Bandes noires/barres affichées sur le Port local - 366
Bannière de sécurité - 187
Blocage des utilisateurs - 170, 173

C

C. Port d'utilisateur local (Console Locale) - 35
Calibrage de la couleur - 254
Capacités de gestion - 408
Capture d'écran de la commande cible (Capture d'écran de la cible) - 256
Caractéristiques et Photos de l'appareil KX III - 2
Caret (clients Linux uniquement) - 367
Cartes à puce - 279
Certificats SSL - 9, 45, 183
Châssis de lames - Page Port Access - 18
CIM pris en charge pour les châssis de lames - 104, 106, 111, 120
CIM requis pour la prise en charge de vidéo double - 224, 283
CIM requis pour support virtuel - 271
CIM Vidéo Digital pris en charge par Mac - 339
Cisco ACS 5.x pour l'authentification RADIUS - 80
Clavier - 248
Clavier français - 367
Cloner les dispositifs KX III existants - 326
Combinaisons de touches Sun spéciales - 300
Commande interface - 220
Commande IPv6 - 221
Commande name - 221
Commandes CLI - 213, 218
Commandes courantes pour tous les niveaux de la CLI - 216
Commutation entre les serveurs cible - 43
Compatibilité CIM - 49
Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel - 360
Concernant le DVI Reach Cat5 - 310
Concernant les Propriétés de connexion - 242
Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible - 273, 275
Conditions de synchronisation d'une souris intelligente - 259
Conditions requises pour l'utilisation d'AKC - 241, 292, 294
Conditions requises pour l'utilisation des supports virtuels - 270
Configuration de la gestion des événements - Destinations - 147, 149, 151, 157
Configuration de la gestion des événements - Paramètres - 149, 157
Configuration de l'alimentation - 158
Configuration de Syslog - 156
Configuration des agents SNMP - 146, 149
Configuration des autorisations - 60
Configuration des autorisations d'accès aux ports - 59, 62, 66
Configuration des châssis de lames - 101
Configuration des châssis de lames Dell - 106
Configuration des châssis de lames génériques - 104
Configuration des châssis de lames génériques IBM - 111
Configuration des châssis de lames HP et Cisco USC (Gestion des groupes de ports). - 117, 119, 120, 165
Configuration des cibles de PDU de rack (barrette d'alimentation) - 96
Configuration des commutateurs KVM - 94, 136
Configuration des paramètres de balayage de ports dans VKC et AKC - 267, 302, 304
Configuration des paramètres de date et heure - 148, 184
Configuration des paramètres de date et heure (facultatif) - 41
Configuration des paramètres de modem - 148
Configuration des ports - 90

Configuration des ports CIM - 95, 339, 340, 366
Configuration des profils USB (page Port) - 56, 113, 127
Configuration des serveurs cible standard - 93
Configuration des traps SNMP - 147, 149
Configuration du contrôle d'accès IP - 181
Configuration du réseau - 219
Configuration du serveur de fichiers du support virtuel (Images ISO du serveur de fichiers uniquement) - 278
Configuration et activation de la fonction multiniveau - 37, 136
Configuration initiale à l'aide de la CLI - 217
Configuration Manuelle et Auto-Découverte du châssis de lames - 103
Configuration Smart Card minimale requise, CIM et lecteurs de cartes à puce pris en charge/ non supportés. - 279, 280
Configuration système minimum pour carte à puce - 280, 306, 343
Configurations et CIMs Paragon II pris en charge - 178, 315
Configurations multiniveau KX III permises - 137
Configurations requises et recommandées de châssis de lames - 104, 106, 111, 123
Configurer la paramètres DNS - 39
Configurer le balayage des ports - 267
Configurer le Cryptage & Partage - 175
Configurer les paramètres de balayage de la Console Locale - 267, 302, 304
Configurer les paramètres du Mode de balayage du Port Local - 130
Configurer les Paramètres du port local KX III - 129, 137
Configurer les Paramètres du port local KX III à partir de la Console locale - 209
Configurer les paramètres Ipv4 - 37
Configurer les paramètres IPv6 - 38
Configurer les propriétés de connexion - 1, 242, 246
Configurer l'option d'Economie d'énergie (optionnel) - 133, 211
Connecter - 20
Connecter un DVI Cat5 Reach et KX III - fournit une fonctionnalité de port local étendue - 1, 310, 397
Connecter un KX III et un DVI Reach Cat5 - 311
Connexion - 214
Connexion à plusieurs cibles depuis un client distant unique - 286, 287, 288
Connexion à un Dispositif audio digital - 288
Connexion à un Moniteur VGA (Optionnel). - 28, 36
Connexion au KX III - 14
Connexion de Paragon II au KX III - 320
Connexion d'une PDU de rack - 96
Connexion et déconnexion de disques média virtuels - 277
Connexion et déconnexion d'un dispositif audionumérique - 286, 287, 288
Connexion et déconnexion d'un média virtuel - 274
Connexion SSH à KX III - 214
Connexions à distance prises en charge - 341
Connexions par carte à puce Virtual KVM Client (VKC) aux serveurs Fedora - 373
Conseils de synchronisation de la souris - 260
Console locale KX III - 207
Console locale KX III - Assistance d'utilisateur final KX III - 26, 296
Construire des données et circuits de puissance pour KX III - 326
Contenu de l'emballage - 2
Contrôle des unités de distribution d'alimentation (PDU) - 397
Création de groupes de ports - 165
Création de groupes d'utilisateurs et d'utilisateurs - 42
Création d'un attribut - 233
Création d'un groupe de deux ports vidéo - 142, 143, 165, 167, 222, 229, 231
Cryptage & Partage - 175
Cycle d''alimentation - 22

D

D. Port DVI-D local - 36
Déclasser un KX III aux archives - 329
Déclasser un KX III en stockage - 329
Déconnecter - 21
Déconnecter les Lecteurs USB Virtuels Mac et Linux - 363
Déconnexion d'un Dispositif audio - 290
Déconnexion d'un serveur cible - 44
Déconnexion d'utilisateurs des ports - 68, 69, 70
Définir une nouvelle macro - 249
Définition des autorisations pour un groupe individuel - 63, 67
Définition des paramètres - 217
Définition des paramètres réseau - 217

Définition du Registre pour autoriser les opérations d'écriture sur le schéma - 233
Dell - 102
Démonter (Retirer) un Lecteur de Carte à Puce - 282
Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora - 374
Déplacement entre ports sur un dispositif - 373
Déplacer un KX III - 329
Depuis LDAP/LDAPS - 232
Désactiver la mise en mémoire cache de Java et effacer le cache de Java - 356
Désactiver le 'Mode Protégé' - 295
Device Information (Informations sur le dispositif) - 190
Diagnostics - 201
Diaporama Balayage des ports - Console locale - 302
Dimensions et spécifications physiques de KX III - 330
Directives CIM Paragon KX III-à-KX III - 317
Directives KX III-à-Paragon II - 318
Dispositifs en niveau - Page Port Access - 18, 136
Distance de connexion, taux de rafraîchissement et résolution vidéo du serveur cible pris en charge - 335, 394
Distances de connexion entre Paragon II et KX III prises en charge - 320
Divers - 411
Documentation et assistance - 410
Dominion KX3-832 - 4
Dominion KX3-864 - 6
Données de connexion par défaut - 29
Double alimentation - 397
Durée d'amorçage du BIOS cible avec les supports virtuels - 363

E

E. Connexion des serveurs cibles au KX III - 36
Echec de connexion des supports virtuels lors de l'utilisation du haut débit - 364
Enregistrement des paramètres audio - 286, 288
Entrer en mode souris intelligente - 258
Envoyer du Texte à la Cible - 249
Envoyez le Macro Ctrl+Alt+Suppr - 248
Envoyez LeftAlt+Tab - 248
Etape 1
  Configuration de l'affichage du serveur cible - 227
  Configuration des paramètres du pare-feu réseau - 30
Etape 2
  Configurer les serveurs cible KVM - 30
  Connexion du serveur cible à KX III - 228
Etape 3
  Configuration du mode souris et des ports - 229
  Connexion de l'équipement - 34
Etape 4
  Configurer le KX III - 37
  Création du groupe de deux ports vidéo - 229
Etape 5
  Lancement de la console à distance de KX III - 42
  Lancement d'un groupe de deux ports vidéo - 230
Etape 6
  Configuration de la langue du clavier (facultatif) - 28, 44
Etape 7
  Créer et installer un certificat SSL - 45
Etapes de configuration de deux ports vidéo - 227
Ethernet et mise en réseau IP - 399
Evénements capturés dans le journal d'audit et dans Syslog - 188, 355
Exemple 1
  Importer le certificat dans le navigateur - 11, 14
Exemple 2
  Ajouter le KX III aux sites de confiance et importer le certificat - 13
Exemple de configuration de groupe de deux ports vidéo - 226
Exemple de connexion multiniveau KX III - 138
Exemples de formats d'URL de châssis de lames - 108, 113, 114, 125
Exemples de touches de connexion - 132, 211, 298
Exigence de clavier multi-langue JRE - 354
Exigence en matière d'autorisation pour utilisateur racine - 277
Exigences de clients distants Linux - 344
Exigences en matière de bande passante - 284, 346
Exigences en matière de client distant - 344

Exigences en matière de port local - 343
Exigences en matière de prise en charge de FIPS 140-2 - 180
Exigences en matière de serveur cible - 343
Exigences Java et Microsoft .NET - 354
Exigences JRE et considérations de navigateur pour Mac - 354
Exporter des macros - 252

F

F. Multiniveau (Facultatif) - 37
Faire une association d'alimentation - 100
FAQ - Généralités - 375
Fermeture de la session des utilisateurs de KX III (Déconnexion forcée) - 68, 69, 70
Firmware Upgrade (Mise à niveau du firmware) - 197
Foire aux questions - 375
Fonctions KX3-832 - 5
Fonctions KX3-864 - 6
Fonctions non prises en charge et limitées sur les cibles en niveau - 138
Formats de dispositifs audio pris en charge - 283
Framework Microsoft NET AKC prise en charge - 293

G

Générique - 102
Gérer KX III dans dcTrack - 322
Gérer le cycle de vie de KX III - 329
Gérer les châssis de lames - 104
Gérer l'ordre de travail KX III - 327
Gestion de la sécurité - 169
Gestion de l'alimentation de dispositifs multiniveau - 141
Gestion de réseau IPv6 - 388
Gestion des conflits dans les noms de profil - 196
Gestion des dispositifs - 85
Gestion des événements - 149
Gestion des prises des PDU de rack (barrettes d'alimentation) - 46
Groupement, fonction multiniveau et mise en cascade des ports locaux - 401
Groupes de deux ports vidéo - 222
Groupes de deux ports vidéo - Page Port Access - 18
Groupes de deux ports vidéo affichés sur la page Ports - 231
Groupes d'utilisateurs - 57

H

Historique des mises à niveau - 198
Hors tension - 22
HP - 102

I

IBM - 102
Implémentation de l'authentification à distance LDAP/LDAPS - 72, 77
Implémentation de l'authentification à distance RADIUS - 77
Importation et exportation de scripts - 160, 163
Importer des dispositifs KX III dans dcTrack - 325
Importer des macros - 250
Inclure l'adresse IP de KX III dans la 'Zone des sites de confiance' - 294
Indicateurs de Statut Cible pendant le balayage des ports - Console locale - 304
Informations de connexion d'accès et de copie - 243, 247
Informations de version - Virtual KVM Client - 291
Informations sur la connexion - 246
Installation - 393
Installation d'un certificat - 9, 10
Installation et configuration de KX III - 9, 28
Installer et configurer KX III: - 9
Interface de console à distance de KX III - 7, 16
Interface de la console locale KX III - 7, 26
Interface de ligne de commande (CLI) - 213
Interface et navigation KX III - 16
Interfaces des consoles KX III locales et à distance - 7
Introduction - 1
Invites CLI - 218

J

Java ne chargeant pas correctement sur Mac - 357
Journal d'audit - 188, 308, 309

K

KX III Langues de clavier prises en charge - 348

L

LCA (liste de contrôle d'accès) IP de groupes - 59, 63, 66, 181

Lecteur virtuel Linux répertorié deux fois - 363
Lecteurs de cartes à puce détecté - 281
Lecteurs de cartes à puce non pris en charge - 345
Lecteurs de cartes à puce pris en charge - 344
Lien à l'interface du châssis de lames. - 103
L'image vidéo est foncée sous Mac - 366
Limitations de connexion - 169, 170
Lisibilité du Texte - 244
Liste des groupes d'utilisateurs - 58
Liste des traps SNMP de KX III - 153
Localiser de l'espace dans un cabinet pour le KX III - 323
Logiciel - 3, 352
Longueurs de câbles et résolutions vidéo pour châssis Dell - 104, 106, 111, 342

M

Macros de clavier - 249
Macros ne s'enregistrant pas sur serveurs cible Linux - 370
Maintenance - 188
Matériel - 2, 330
Messages de validation et avertissements de sécurité - 9, 10, 14
Mettre à jour le firmware KX III - 197
Mettre à jour un lecteur de cartes à puce - 282
Mise à jour du cache de schéma - 236
Mise à jour du schéma LDAP - 232
Mise à niveau des CIM - 127, 196
Mise en route - 9, 217, 228
Mise sous/hors tension des prises et alimentation cyclique - 47
Mode de compatibilité DVI - 340
Mode Full Screen (Mode Plein écran) - 269
Mode PC Partagé et Paramètres de Confidentialité lors de l'utilisation de cartes à puce. - 280
Mode souris intelligente - 258
Mode souris simple - lors de la Connexion à une cible contrôlée par CC-SG - 371
Mode souris standard - 260
Mode souris unique - 261
Mode vidéo - 244
Modèles de châssis de lames pris en charge - 104, 106, 111, 119
Modes CIM digital établis - 340
Modes de souris lors de l'utilisation du menu de démarrage Mac - 53, 56, 127
Modes de souris pris en charge pour les groupes de deux ports vidéo - 223, 229, 283
Modes de synchronisation de CIM numériques - 339
Modes digital CIM établis et standard - 339
Modes digital CIM standard - 340
Modes et résolutions vidéo - 297, 366
Modes souris double - 258
Modes vidéo SUSE/VESA - 367
Modification des attributs rciusergroup pour les membres utilisateurs - 236
Modification des scripts - 163
Modification du code de disposition de clavier (cibles Sun) - 44
Modification du mot de passe par défaut - 37
Modification du paramètre de langue de l'interface utilisateur par défaut - 169
Modification d'un groupe d'utilisateurs existant - 65
Modification d'un mot de passe - 84
Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce - 366
Modification d'un utilisateur existant - 70
Modules d'interface pour ordinateur (CIM) - 404
Montage arrière - 29
Montage avant - 28
Montage des images CD-ROM/DVD-ROM/ISO - 275, 278
Montage des lecteurs locaux - 271
Montage en rack - 28
Monter un lecteur de cartes à puce - 281
Mots de passe sécurisés - 84, 169, 172

N

Navigateurs pris en charge par AKC - 294
Navigation client Raritan lors de l'utilisation des groupes de deux ports vidéo - 230
Navigation dans la console KX III - 25
Navigation de la CLI - 215
Ne peut pas écrire sur/à partir d'un fichier de Client Mac - 361
Ne peut pas se connecter aux lecteurs de clients Linux - 361
Niveau sonore - 284, 346
Noise Filter (Filtre antiparasite) - 245
Nom du port - 92
Nombre de connexions audio/supports virtuels et cartes à puce prises en charge - 348
Nombre de disques média virtuel pris en charge - 274
Nommez vos serveurs cibles - 40

Notes de version Ipv6 pour téléchargement de la Validation de Certification du Serveur AKC - 359
Notes sur le montage de lecteurs locaux - 272
Nouveautés de l'aide - 1
Numéro de port - 91

O

Onglet Set Scan (Balayage d'ensemble) - 19
Onglet View by Group (Afficher par groupe) - 19
Onglet View by Search (Afficher par recherche) - 19
Optimisé pour Sélections - 244
Options d'affichage - 268
Options de configuration du chassis blade - 102
Options de profil USB de la console locale - 307
Options de souris - 257
Options d'outils - 262, 269
Ordinateur distant (Remote PC) - 271

P

Page d'accès aux ports (Affichage de la console à distance) - 17, 101
Page de configuration des ports - 91
Page Device Diagnostics (Diagnostics du dispositif) - 206
Page d'interface réseau - 201
Page Network Statistics (Statistiques réseau) - 201
Page Ping Host (Envoi de commande Ping à l'hôte) - 204
Page Trace Route to Host - 204
Panneau gauche - 23
Paramétrage des options clavier/souris CIM - 248
Paramètres additionnels de la souris pris en charge - 28, 31
Paramètres d'authentification - 71
Paramètres de la souris - 31
Paramètres de la souris Linux - 33
Paramètres de la souris Mac d'Apple - 33
Paramètres de la souris Sun Solaris - 34
Paramètres de lancement client - 265
Paramètres de l'interface LAN - 85, 88, 89
Paramètres de propriétés de connexion par défaut - Optimisé pour de meilleures performances - 243
Paramètres de souris IBM AIX - 34
Paramètres de souris Windows 2000 - 32
Paramètres de vitesse réseau - 89, 341
Paramètres des ports HTTP et HTTPS - 134, 351
Paramètres généraux - 262
Paramètres Microsoft Windows 7 et Windows Vista - 32
Paramètres réseau - 85, 88, 351
Paramètres réseau de base - 85
Paramètres Windows XP, Windows 2003 et Windows 2008 - 32
Partitions de lecteur - 277, 278
Partitions système actives - 277, 278
Pavé numérique - 368
Photos KX3-832 - 4
Photos KX3-864 - 6
Port Action Menu (Menu d'action de ports) - 17, 20, 242, 293
Port Group Management (Gestion des groupes de ports) - 165
Port Local - KX III - 395
Port local étendu - 396
Port TCP 443 - 30
Port TCP 5000 - 30
Port TCP 80 - 30
Port Type (Type de port) - 92
Ports TCP et UDP utilisés - 351
Ports USB VM-CIM et DL360 - 364
Pour envoyer des notifications de retrait et de réinsertion de la carte à puce à la cible : - 282
Précision de couleur - 244
Préférence de la langue du clavier (clients Fedora Linux) - 369
Prérequis KX III - 270
Présentation - 1, 16, 27, 46, 49, 213, 240, 292, 296, 310, 314, 322, 356
Problèmes de performances de connexion en double pile - 359
Problèmes de sécurité - 219
Problèmes en matière de lecture et de capture audio - 372
Processus d'authentification de l'utilisateur - 83
Profils USB - 49, 247, 248
Profils USB disponibles - 50
Propriétés d'accès de connexion - 242
Propriétés vidéo - 253
Protocoles pris en charge - 42

R

Raccourci-Clavier Sequences pour l'accès au châssis de lames. - 103
Raccourcis-clavier et touches de connexion - 298
Recommandations en matière de connexions audio lorsque le mode PC Share est activé - 284, 346
Recommandations en matière de ports vidéo doubles - 223, 283
Recommandations et exigences en matière de lecture et de capture audio - 284, 288, 346
Redémarrage de KX III - 198
Réduire le panneau gauche - 25
Réglage des paramètres vidéo - 254
Réinitialisation de KX IIII à l'aide du bouton de réinitialisation sur le dispositif - 309
Réinitialisation des paramètres d'usine de la Console locale KX III - 308
Relation entre les utilisateurs et les groupes - 58
Remarque aux utilisateurs de CC-SG - 42
Remarque relative à Microsoft Active Directory - 42
Remarques CC-SG - 373
Remarques CIM - 359
Remarques clavier - 367
Remarques d'informations - 348, 356
Remarques Navigateur - 374
Remarques relatives à l'utilisation des groupes de deux ports vidéo - 225
Remarques souris - 371
Remarques sur la prise en charge d'IPv6 - 358
Remarques sur la prise en charge du système d'exploitation d'IPv6 - 358
Remarques sur le support virtuel - 361
Remarques sur l'environnement d'éxécution de Java (JRE) - 354, 356
Remarques sur les cartes à puce - 373
Remarques sur les ports et profils USB - 364
Renvoi des informations relatives aux groupes d'utilisateurs - 232
Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory - 76
Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS - 81
Résolutions de serveur vidéo cible - 30
Résolutions de Vidéo de Serveur cible supportées par KX III - 30, 228, 334, 335
Résolutions DVI de Port Local KX III prises en charge - 297, 336
Résolutions vidéo de la Console locale - 297
Restrictions concernant les claviers - 264
Retour à l'interface de la Console locale de KX III - Raccourci-clavier par défaut - 298

S

Saisie automatique des commandes - 215
Saisie du port de détection - 135
Scaling (Mise à l'échelle) - 269
Scripts de connexion et de déconnexion - 159
Se connecte à un serveur cible - 241, 293
Se connecter à un Moniteur DVI - 36
Sécurité - 405
Sécurité et authentification - 208
Security Settings (Paramètres de sécurité) - 67, 169
Sélection des profils pour un port KVM - 56
Sélectionnez la touche de connexion du port local. - 132, 211
Sélectionnez l'authentification des utilisateurs locaux - 133, 212
Sélectionnez le raccourci-clavier du port local. - 131, 210
Sélectionnez le type de clavier de la Console locale - 130, 209
Serveur cible - 271
Serveurs lames - 391
Services du dispositif - 134
Soumettez une requête d'ajout d'objet pour le KX III - 327
Souris à 3 boutons Windows sur les cibles Linux - 359
Sous tension - 22
Spécification de la détection automatique de l'alimentation - 40
Spécifications - 330
Spécifications des CIM pris en charge - 33, 49, 280, 336
Spécifications des échanges de communication RADIUS - 81
Status LED pendant le démarrage de KX III - 28, 34
Support virtuel - 270
Support virtuel non rafraîchi après l'ajout de fichiers - 363
Support virtuel universel - 382
Supports virtuels dans un environnement Linux - 277

Supports virtuels dans un environnement Mac - 278
Supports virtuels dans un environnement Windows XP - 277
Supprimer une association d'alimentation - 101
Switch From (Basculer à partir de). - 21
Synch Vidéo Sun Composite - 366
Synchronisation absolue de la souris - 258
Synchronisation des pointeurs de souris (Fedora) - 371
Synchroniser votre souris - 261
Syntaxe CLI - Conseils et raccourcis - 216
Syntaxe URL d'accès direct au port pour le client KVM Actif (AKC) - 142
Syntaxe URL d'accès direct au port pour le client KVM Virtuel (VKC) - 141
Système d'exploitation Audio Playback Support - 287
Systèmes d'exploitation et navigateurs pris en charge - 352
Systèmes d'exploitation pour support média virtuel pris en charge - 273
Systèmes d'exploitation pris en charge par AKC - 294

T

Tâches prise en charge Via Support Virtuel - 272
Tilde - 368
Touches clavier non prises en charge pour accès à distance - 370
Touches de commandes BIOS sur Mac Mini - 349
Types de supports média virtuels - 272

U

USB Profile Management (Gestion des profils USB) - 195, 196
User Management (Gestion des utilisateurs) - 57
Utilisateurs - 66
Utilisateurs et ports pris en charge par modèle - 7
Utilisateurs simultanés - 297
Utilisation du support virtuel via VKC et AKC dans un environnement Windows - 362
Utiliser un clavier Windows pour accéder à des cibles Mac - 351

V

Vérification de la prise en charge du chiffrement AES par votre navigateur - 176, 179
Version de Virtual KVM Client non reconnue par le mode proxy CC-SG - 373
View Status Bar (Afficher la barre d'état) - 268
View Toolbar (Afficher la barre d'outils) - 268
Visualisez le KX III dans un cabinet d'élévation et sur une carte d'étage - 327

W

Windows - 390

Etats-Unis/Canada/Amérique latine

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

Chine

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

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

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

Inde

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

Japon

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5991
E-mail : support.japan@raritan.com

Europe

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

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

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

Allemagne
Lundi - Vendredi
8h30 - 17h30, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0
E-mail : rg-support@raritan.com

Melbourne, Australie

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

Taiwan

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